2016/2017

Classe 4 E

Liceo Scientifico E.Fermi
Catanzaro Lido (CZ)

[INFORMATICA 4.E]

Sommario

PRESENTAZIONE

Il presente lavoro è stato realizzato dalla classe 4°E del Liceo Scientifico Enrico Fermi di Catanzaro nell'anno scolastico 2016/2017, sotto indicazione del professore Santi Caltabiano, docente di Informatica della classe. Gli alunni, suddivisi in gruppi di lavoro, coordinati da Talarico Federica e Catanese Claudia, hanno affrontato gli argomenti proposti lasciandosi incuriosire dalla vastità dei temi. Il compito assegnato ha avuto un duplice obiettivo: suscitare interesse nello studente e al tempo stesso contribuire alla personale formazione in questo campo. I ragazzi, quindi, hanno esaminato argomenti riferiti a vari aspetti dell'informatica ripercorrendo l'evoluzione di tale disciplina, apparentemente nota e semplice, che invece si è rivelata complessa e dinamica. Il testo racchiude le varie trattazioni dei work group integrate dalla presenza di immagini che favoriscono la lettura e la comprensione del testo.

Il WEB

Storia

Di Marta Miletta e Arianna Daini

World Wide Web

Il World Wide Web nasce tra la fine del 1990 e il 1991. Fu Tim Berners-Lee a definire il protocollo HTTP (HyperText Transfer Protocol), un sistema che permetteva una lettura ipertestuale, non-sequenziale dei documenti, saltando da un punto all'altro mediante l'utilizzo di link o hyperlink). Il primo browser, dalle caratteristiche simili a quelle odierne, fu il Mosaic, che fu realizzato nel 1993. Esso rivoluzionò il modo di effettuare le ricerche e di comunicare in rete. Nel mese di dicembre furono completate le prime versioni dei software per il server e il browser, il 20 dicembre fu pubblicato il primo sito, che descriveva il progetto WWW all'URL http://info.cern.ch/hypertext/WWW/TheProject.html. Dal 6 agosto 1991 Berners-Lee annunciò pubblicamente su diversi newsgroup l'esistenza del progetto WWW e la disponibilità del software. Con il successo del Web ha inizio la diffusione di Internet degli anni 2000-2010.
Nel 1998 venne introdotto il concetto di eEconomy.

La nascita del Web risale al ***6 agosto 1991***, giorno in cui l'informatico inglese Tim Berners-Lee pubblicò il primo sito web dando vita al "*WWW*" (noto anche come "*tripla W*").

Questo è il computer utilizzato dall'inglese Tim Berners-Lee per realizzare il primo web, oggi esposto nel Museo Microcosm del CERN, a Meyrin (Ginevra), in Svizzera.

L'idea del Web era nata già due anni prima, nel 1989, presso il CERN (Conseil Européen pour la Recherche Nucléaire) di Ginevra, il più importante laboratorio di fisica europeo.
Il ricercatore inglese fu colpito da come alcuni colleghi italiani trasmettevano informazioni da un piano all'altro dell'istituto attraverso una linea telefonica e visualizzando le informazioni sotto forma di video.
Il 12 marzo 1989, Berners-Lee presentò al supervisore il documento *Information Management*: a *Proposal*, una cui copia è esposta presso il CERN, che fu valutato «vago ma interessante».
Il progetto di Berners-Lee e di Robert Cailliau, un suo collega, era quello di elaborare un software con cui condividere documenti scientifici in formato elettronico, che fossero indipendentementi dalla piattaforma informatica utilizzata, il loro obiettivo era quello di migliorare la comunicazione e la cooperazione tra i ricercatori dell'istituto.
Con la creazione del software si iniziò a definire lo standard e i protocolli per scambiare documenti su reti di calcolatori: il linguaggio HTML e il protocollo di rete HTTP.
Questi standard e protocolli inizialmente supportavano solo la gestione di pagine HTML statiche, ossia file ipertestuali -preparati precedentemente- visualizzabili e, soprattutto, navigabili utilizzando opportune applicazioni (browser web).
Il 30 aprile 1993, il CERN decise di mettere il WWW a disposizione del pubblico rinunciando ad ogni diritto d'autore. La semplicità della tecnologia ottenendo un immediato successo: in pochi anni, divenne la modalità più diffusa al mondo per inviare e ricevere dati su Internet. Iniziò così l'"Era del Web".

Dal web statico al web service

Per superare le limitazioni del progetto, furono definiti strumenti capaci di generare pagine HTML dinamiche (ad es. utilizzando dati estratti da un database).

La prima soluzione fu la CGI (Common Gateway Interface), attraverso cui possiamo richiedere ad un web server di chiamare un'applicazione esterna e di presentarne il risultato. Però questa soluzione, sebbene fosse molto semplice da realizzare, presentava numerose limitazioni di progetto (l'applicativo esterno viene eseguito ad ogni richiesta utente e non è prevista alcuna ottimizzazione,

non vi è alcuna gestione dello stato della sessione, etc.). Allora per dare al web una maggiore interattività e dinamicità sono state:

- aumentate le funzionalità dei browser con un'evoluzione del linguaggio HTML e la possibilità d'interpretazione dei linguaggi di scripting (come JavaScript);
- migliorate le qualità di elaborazione dei server grazie ad una nuova generazione di linguaggi integrati con il web server (come JSP, PHP, ASP, etc.), trasformando i web server negli attuali application server.

Queste soluzioni hanno consentito l'utilizzo del web come una piattaforma applicativa che, oggi, trova la sua massima espressione nei Web Service; alla sua realizzazione e diffusione lavorano l'intera industria mondiale del software per la gestione d'azienda, dai grandi nomi commerciali (come SAP e Oracle) fino alle comunità Open Source.

L'utilizzo dei web-service all'interno dell'architettura di integrazione SOA permette alle piccole imprese di gestire i propri processi aziendali.

Lo scopo dei Web Service è quello di limitare le attività di implementazione, consentendo di accedere ai servizi software resi disponibili in rete, assemblarli secondo le proprie necessità e pagarli soltanto per il loro utilizzo effettivo, metodologia nota come pay per use, on demand software, just in time software, on tap software, etc.

I web-service hanno un legame strutturale con i processi aziendali che dovranno supportare nell'ambito di una nuova organizzazione basata sui processi.

Dal web statico al web semantico

Nonostante tutte le sue evoluzioni, il web rimane una biblioteca di pagine HTML statiche on-line.

Se lo standard HTML, da un lato, ha contribuito nell'affermazione del web, dall'altro si è limitato di occuparsi solamente della formattazione dei documenti, tralasciando la struttura e il significato del contenuto.

Questo causò delle difficoltà nel riutilizzo delle informazioni. Eseguendo una ricerca utilizzando un motore di ricerca disponibile in rete noteremo che dai tanti

documenti risultanti dalla query solo pochi sono di nostro interesse; questo rende la ricerca molto difficile.

Allora per risolvere il problema, l'informatico inglese Tim Berners-Lee, che, abbandonato il CERN, ha fondato il consorzio W3C, che assunse il ruolo di governo nello sviluppo di standard e protocolli legati al web.

Nel 1998 Berners-Lee definì lo standard XML (eXtensible Markup Language), un metalinguaggio derivante dall'SGML, che consente di creare nuovi linguaggi di marcatura (ad es. HTML è stato ridefinito in XML come XHTML). La sua caratteristica innovativa fu la possibilità di aggiungere informazioni semantiche sui contenuti grazie ai tag.

Gli obiettivi di XML, dichiarati nell'ottobre 1998, furono: l'utilizzo del linguaggio su Internet, la facilità di creazione dei documenti, supporto di più applicazioni, chiarezza e comprensibilità. Con queste semplici caratteristiche l'XML fornisce un modo semplice per rappresentare i dati, cosicché i programmi software siano in grado di eseguire meglio le ricerche, visualizzando e manipolando le informazioni nascoste.

L'XML è alla base di tutte le nuove tecnologiche distribuite dal W3C ed è stato adottato come standard di rappresentazione dati da tutta l'industria informatica.

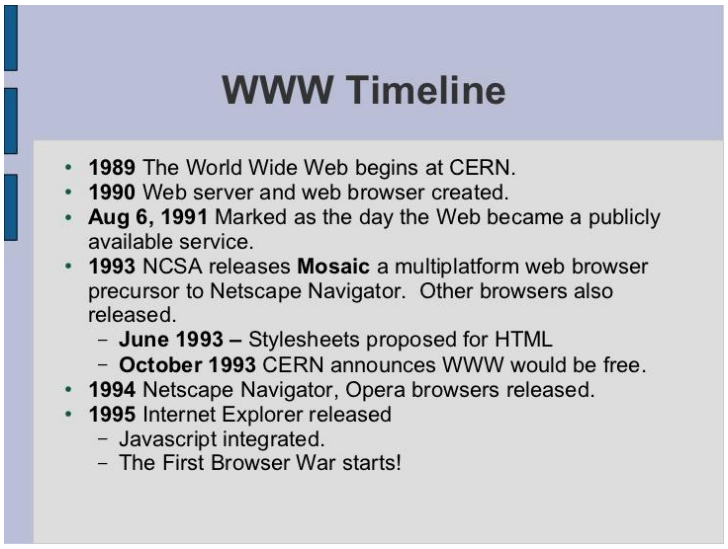
Però XML ha una lacuna molto importante: non definisce alcun meccanismo univoco e condiviso per specificare relazioni tra le informazioni espresse sul web per una loro elaborazione automatica (ad es. più documenti che parlano dello stesso argomento, persona, organizzazione, oggetto), rendendo difficile la condivisione delle informazioni.

La soluzione del problema è avvenuta dal W3C di Berners-Lee, attraverso la formalizzazione del web semantico. Il W3C considera l'ideale evoluzione del web dal machine-representable al machine-understandable. L'idea è quella di generare documenti che possano non solo essere letti e apprezzati da esseri umani, ma anche accessibili e interpretabili da agenti automatici per la ricerca di contenuti.

A tale scopo furono definiti alcuni linguaggi, quali Resource Description Framework (RDF) e Web Ontology Language (OWL), basati su XML, che consentono

di esprimere le relazioni tra le informazioni rifacendosi alla logica dei predicati mutuata dall'intelligenza artificiale. Questi standard sono già disponibili, ma continuano ad essere sviluppati insieme a strumenti per dotare il web di capacità di inferenza. È un processo apparentemente tecnico che ha come obiettivo l'approdo all'intelligenza condivisa del web che promette l'uso più efficiente dei siti internet e un'autentica trasformazione nella natura del software e dei servizi.

L'interesse per queste tecnologie è il fatto che tutti (utenti, produttori di software e di servizi piccoli e grandi) hanno da avvantaggiarsi dalla diffusione questi standard. La formazione nel corpo del web di una rete "semantica" è la condizione chiave per il decollo di un nuovo modo di intendere ed usare il web.



Cos'è il WEB?

Quasi tutti confondiamo Internet con il Web, come se fossero la stessa cosa, invece rimangono due cose ben distinte: "***Internet***" è l'hardware cioè la struttura, mentre, il "***Web***" è il software cioè il contenuto.

Il ***Web*** o ***World Wide Web*** (in italiano "*rete di grandezza mondiale*"), la cui sigla ***WWW***, è uno dei principali servizi di Internet che permette di navigare e usufruire ad un insieme di contenuti amatoriali e professionali (multimediali e non) collegati tra loro attraverso legami (*link*), e ad altri servizi accessibili a tutti o ad una parte selezionata degli utenti di Internet. La diffusione delle informazioni è resa possibile dai protocolli di rete e dalla presenza, diffusione dei motori di ricerca e del web browser in un modello di architettura di rete definito client-server.
Caratteristica principale del Web sono i nodi che la compongono, collegati tra loro tramite i cosiddetti link (collegamenti ipertestuali), formando un enorme ipertesto e i suoi servizi possono essere resi disponibili dagli utenti di Internet. Il Web ha la capacità di offrire a chiunque la possibilità di diventare editore e, con una spesa limitata, di raggiungere un pubblico distribuito in tutto il mondo.

oggi gli standard su cui è basato, in continua evoluzione, sono mantenuti dal World Wide Web Consortium (W3C: www.w3c.org).
La prima proposta di un sistema ipertestuale si può far risalire agli studi di Vannevar Bush, poi pubblicati nell'articolo As We May Think (in italiano "Come potremmo pensare") del 1945.

Il Web è uno spazio elettronico e digitale di Internet utilizzato per la pubblicazione di contenuti multimediali (testi, immagini, audio, video, ipertesti, ipermedia, ecc.), ossia uno strumento utilizzata per implementare servizi, ad esempio, il download di software (programmi, dati, applicazioni, videogiochi, ecc.). Tale spazio elettronico e tali servizi sono resi disponibili grazie a particolari computer di Internet chiamati server web.
I contenuti del Web sono costantemente on-line quindi, fruibili da chiunque disponga di un computer, di un accesso a Internet, e degli opportuni programmi (ossia dei browser web, il programma che permette di "navigare" nel Web, usufruendo dei contenuti e dei servizi del Web.)
Però non tutti i contenuti e i servizi del Web sono disponibili a chiunque poiché il proprietario dello spazio web, o chi ne ha delega di utilizzo, può renderli disponibili solo a determinati utenti, gratuitamente o a pagamento, utilizzando il sistema degli account.
I contenuti principali del Web sono costituiti da testo e grafica rappresentati in un insieme ristretto di standard definito dal W3C. Tali contenuti sono quelli che tutti i browser web devono essere in grado di utilizzare autonomamente senza software aggiuntivo.
I contenuti pubblicati sul Web possono essere però di qualunque tipo e in qualunque standard. Alcuni sono pubblicati per essere utilizzati attraverso il browser web e, non essendo in uno degli standard appartenenti all'insieme definito dal W3C, per poterli fruire attraverso il browser web questo deve essere integrato con i cosiddetti plug-in, software che integrano le funzionalità di un programma i quali sono scaricabili dal Web.
I contenuti del Web sono organizzati nei cosiddetti siti web, i quali sono strutturati nelle pagine web le quali si presentano come composizioni di testo e/o grafica visualizzate sullo schermo del computer dal browser web. Le pagine web sono collegate fra loro in modo non sequenziale, ma attraverso link (anche

chiamati collegamenti), ossia parti di testo e/o grafica di una pagina web che permettono di accedere ad un'altra pagina web, di scaricare contenuti, o di accedere a funzionalità, cliccandoci sopra con il mouse, creando così un ipertesto. Tutti i siti web, sono identificati per mezzo del loro indirizzo web, una sequenza di caratteri univoca chiamata URL che permette la rintracciabilità nel Web.
Nel corso degli anni sono nati i *motori di ricerca*, siti web da cui è possibile ricercare contenuti nel Web in modo automatico sulla base di parole chiave inserite dall'utente, e i *portali web*, siti web da cui è possibile accedere ad ampie quantità di contenuti del Web selezionati dai redattori del portale web attraverso l'utilizzo di motori di ricerca.
Il Web è implementato attraverso un insieme di standard, i principali sono:

- ***HTML***: il linguaggio di markup con cui sono scritte e descritte le pagine web;
- ***HTTP***: il protocollo di rete su cui è basato il Web;
- ***URL***: lo schema di identificazione, ossia di rintracciabilità, dei contenuti e dei servizi del Web.

Funzionamento
La visione di una pagina web inizia con la digitazione dell'URL nell'apposito campo del browser web oppure cliccando su un collegamento ipertestuale presente in una pagina web o in un'altra risorsa come ad esempio un'e-mail. Il browser web a quel punto inizia una serie di messaggi di comunicazione con il web server che ospita quella pagina.
La porzione di server-name dell'URL è risolta in un indirizzo IP usando il database globale, conosciuto come Domain Name System (in sigla DNS). Questo indirizzo IP è necessario per inviare e ricevere pacchetti dal server web.
A questo punto il browser richiede le informazioni inviando una richiesta a quell'indirizzo. In caso di una tipica pagina web, il testo HTML di una pagina è richiesto per primo interpretato dal browser web che poi richiede immagini o file che serviranno per formare la pagina definitiva.
Una volta ricevuti i file richiesti dal web server, il browser formatta la pagina sullo schermo seguendo le specifiche HTML, CSS, o di altri linguaggi web. Ogni immagine e le altre risorse sono incorporate per produrre la pagina web che l'utente vedrà.

Fonti

1. Wikipedia
2. Webhouse.it
3. File PDF Muldimediarchitecture
4. Web in testa
5. Rai Storia

Internet

Di Marta Miletta e Arianna Daini

Storia

Internet nasce intorno i primi anni degli anni sessanta, su iniziativa degli Stati Uniti, che durante la guerra fredda vollero idealizzare un nuovo sistema di difesa e di controspionaggio.
La prima pubblicazione scientifica in cui si teorizza una rete di computer mondiale ad accesso pubblico fu On-line man computer communication nell'agosto 1962, una pubblicazione scientifica degli statunitensi Joseph C.R. Licklider e Welden E. Clark. Nella pubblicazione Licklider e Clark, diedero un nome alla rete da loro teorizzata: "Intergalactic Computer Network".
Tutto divenne realtà solo nel 1991 quando il governo degli Stati Uniti d'America emanò la High performance computing act, la legge con cui per la prima volta venne prevista la possibilità di ampliare la rete Internet.

Arpanet (1969)

Il progenitore della rete Internet è considerato il progetto ARPANET, finanziato dalla Defence Advanced Research Projects Agency (inglese: DARPA, Agenzia per i Progetti di ricerca avanzata per la Difesa), un'agenzia dipendente dal Ministero della Difesa statunitense (Department of Defense o DoD degli Stati Uniti d'America). In una nota del 25 aprile 1963, Licklider aveva espresso l'intenzione di collegare tutti i computer e i sistemi di time-sharing in una rete continentale. Avendo lasciato l'ARPA per un posto all'IBM l'anno seguente, furono i suoi successori che si dedicarono al progetto ARPANET.

Il contratto fu assegnato all'azienda da cui proveniva Licklider, la Bolt, Beranek and Newman (BBN) che utilizzò i minicomputer di Honeywell come supporto. La rete venne costruita nel 1969 collegando quattro nodi: l'Università della California di Los Angeles, l'SRI di Stanford, l'Università della California di Santa Barbara, e l'Università dello Utah. L'ampiezza di banda era di 50 kbps. Furono introdotti i fondamentali Request for Comments, ancora oggi i documenti fondamentali per tutto ciò che riguarda i protocolli informatici della rete e dei loro sviluppi.

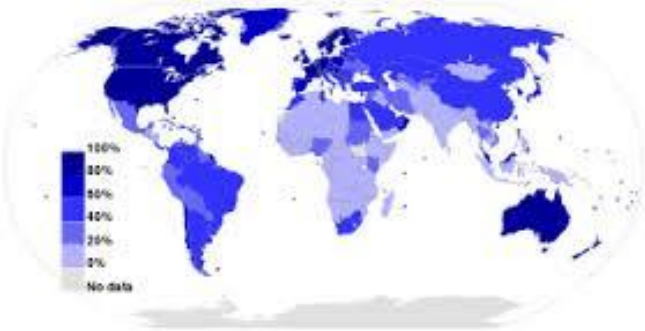
I primi nodi si basavano su un'architettura client/server, e non supportavano connessioni dirette (host-to-host). Le applicazioni eseguite erano

fondamentalmente Telnet e i programmi di File Transfer Protocol (FTP). Il servizio di posta elettronica fu inventata da Ray Tomlinson della BBN nel 1971, derivando il programma da altri due: il SENDMSG per messaggi interni e CPYNET, un programma per il trasferimento dei file. L'anno seguente ARPANET venne presentata al pubblico e divenne subito popolare, grazie anche al contributo di Larry Roberts che aveva sviluppato il primo programma per la gestione della posta elettronica, RD.

Da Arpanet a Internet

In pochi anni, ARPANET allargò i suoi nodi oltreoceano; nacque il primo servizio di invio pacchetti a pagamento: Telenet della BBN.
In Francia si inizia la costruzione della rete CYCLADES sotto la direzione di Louis Pouzin.
In Norvegia fu costruita la rete NORSAR che permise il collegamento di Arpanet con lo University College di Londra.
L'espansione proseguì sempre più rapidamente: il 26 marzo del 1976 la regina Elisabetta II spedì un'email alla sede del Royal Signals and Radar Establishment.
Il 12 aprile 1979 vennero istituite le emoticon, quando Kevin MacKenzie suggerì di inserire un simbolo nelle mail per indicare gli stati d'animo.

Tutto era pronto per il cruciale passaggio a Internet, compreso il primo virus telematico: sperimentando sulla velocità di propagazione delle e-mail, a causa di un errore negli header del messaggio, Arpanet venne totalmente bloccata: era il 27 ottobre 1980. Definendo il Transmission Control Protocol (TCP) e l'Internet Protocol (IP), DCA e ARPA diedero il via ufficialmente a Internet come l'insieme di reti interconnesse tramite questi protocolli.
L'Italia fu il terzo Paese in Europa a connettersi in rete, dopo Norvegia e Inghilterra, grazie ai finanziamenti del Dipartimento della Difesa degli Stati Uniti. La connessione avvenne dall'Università di Pisa, poiché alcuni dei componenti del gruppo avevano lavorato a contatto con quelli che poi sarebbero stati considerati i padri di Internet, Robert Kahn e Vinton Cerf. Fu Kahn a convincere i suoi superiori a finanziare l'acquisto delle tecnologie necessarie per il gruppo di Pisa.
Il collegamento avvenne il 30 aprile 1986.



Diffusione

Fino al 1995 Internet era una rete dedicata solo alle comunicazioni all'interno della comunità scientifica e tra le associazioni governative e amministrative, dopo tale anno si assiste alla diffusione degli accessi alla rete da parte di utenti privati fino al boom degli anni 2000. Furono migliorati e aumentati i contenuti e i servizi offerti dal Web, le modalità di navigazione sempre più usabili, accessibili e user-friendly, ossia a velocità di trasferimento dati a più alta velocità di trasmissione passando dalle connessioni ISDN e V.90 alle attuali connessioni a banda larga tramite sistemi DSL.

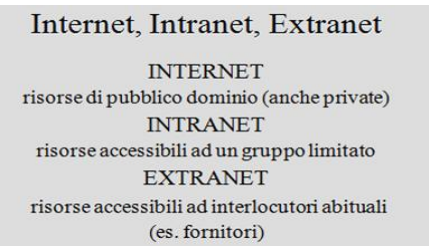
Approfondimenti sull'argomento Internet

Di Giuseppe Timpano

Cos'è una rete?

Prima di parlare del mondo di internet è necessario introdurre il concetto di rete. Con il termine rete, si intende una serie di componenti, sistemi o entità interconnessi tra loro in qualche opportuno modo. Nel mondo dell'informatica, queste componenti sono solitamente computer, modem router e/o semplici stampanti di rete, collegati in qualche tipica maniera tra loro con l'intento di poter fargli scambiare a vicenda informazioni o, piuttosto, condividere determinate risorse. In informatica esistono comunque diverse tipologie di rete ma quelle più importanti sono sostanzialmente due, ovvero: le **LAN**, dall'acronimo inglese di *Local Area Network*, in italiano rete in area locale, che corrispondono a quelle reti realizzate all'interno di un'area piuttosto circoscritta (ad esempio, in una casa, in una scuola o in un ufficio). Mediante la creazione di una rete di questa particolare tipologia si vogliono solitamente condividere determinate risorse hardware, come per esempio una stampante o un semplice scanner, o software, come documenti o, in generale, file di qualsiasi tipo. In ogni caso, il collegamento esistente tra le varie componenti hardware di una LAN può avvenire solitamente o mediante l'utilizzo di speciali cavi, chiamati in gergo "cavi Ethernet", oppure in maniera del tutto wireless ovvero senza l'utilizzo di alcun fastidioso filo. In quest'ultimo caso, tuttavia, piuttosto che di LAN si parla di **WLAN**, dall'acronimo inglese di *Wireless Local Area Network*, cioè di una rete Wi-Fi che non corrisponde altro che ad una speciale LAN protetta da un'opportuna password. Invece le **WAN**, dall'acronimo inglese di *Wide Area Network*, che non sono altro che quelle reti appartenenti ad un'area geografica molto più grande rispetto alle comuni LAN (ad esempio, tra nazioni o, addirittura, tra continenti). Tra tutte le WAN esistenti, quella più grande e, al tempo stesso, più importante, prende il nome di **Internet.**

Cos'è e come funziona internet?



Internet è sostanzialmente definita la "rete delle reti", cioè un insieme di reti di computer sparse in tutto il mondo e collegate tra loro, a cui possono accedere migliaia di utenti per scambiare tra loro

informazioni binarie di vario tipo a definizione. La si può descrivere come un insieme di reti telefoniche locali o nazionali che nel loro insieme formano una immensa rete internazionale in grado di comunicare utilizzando il set di protocolli

TCP/IP. Il funzionamento di Internet è quello di seguire passo passo una comunicazione, cioè il passaggio di un'informazione da un **computer di origine** (o **client**) ad un computer di destinazione (**server**). Va infatti notato che, anche se un computer può comunicare con diversi altri in rapida successione, di fatto questa **comunicazione avviene sempre tra due computer** (**client/server**) di cui il client è l'emittente del messaggio e il server è il suo ricevente, o computer remoto. La parola Internet è una espressione inglese formata da due parole intere, **net** (rete), con cui si indica un collegamento tra due reti (di computer) attraverso una **gateway** (via d'accesso): è questo collegamento che permette a qualsiasi computer di una rete di comunicare con un qualsiasi altro computer di un'altra rete che può essere immaginata come è, un'immensa ragnatela fondata da migliaia di reti di computer sparse in tutto il mondo e tutte collegate tra loro, questo significa che col nostro computer, connesso ad una delle reti, possiamo in teoria comunicare con tutti i milioni di computer che formano la "rete delle reti" o che sono a queste connessi.

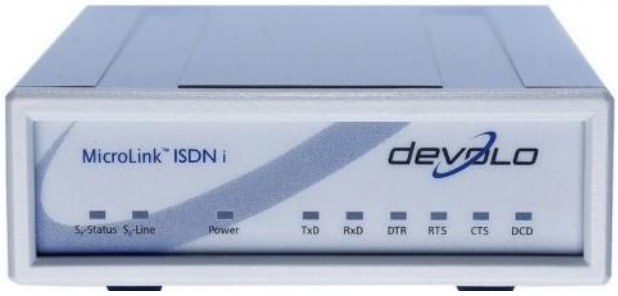
I vari tipi di collegamento ad internet

Per accedere a Internet da un computer (o da uno smartphone per estensione) possiamo usare una grande varietà di tecnologie, messe a disposizione di noi tutti per poter accedere alla grande rete da quasi ogni punto del globo. Le tecnologie sono molte ed hanno tanti nomi diversi, al punto che può essere difficile che tipo di tecnologia adottiamo o siamo in procinto di adottare con un nuovo abbonamento.

1) **Dial-up o modem analogico (in disuso)**: Il modem analogico trasformava i segnali provenienti dalla linea telefonica in segnali digitali per il computer e, viceversa in upload,

trasformava i segnali digitali inviati dal computer in segnali analogici da inviare al provider. Il modem quindi effettua una vera telefonata al fornitore dei servizi, occupando la linea interamente ed impedendo l'uso del normale telefono. Questa connessione è davvero troppo lenta per il Web attuale, ed è definitivamente scomparsa nei paesi industrializzati.

2) **ISDN (quasi in disuso):** La prima evoluzione per aumentare la velocità delle connessioni fu l'introduzione di una linea dedicata: affianco alla normale linea analogica si affiancava un nuovo cavo da usare per la navigazione Web, per il telefono, per le teleconferenze e per il fax, tutti insieme. Era nata **ISDN** (*Integrated Services Digital Network*). Con ISDN ci fu un discreto incremento prestazionale, ma la sua messa in posa e i suoi contratti erano molto costosi, al punto che rimase quasi sempre relegata in ambito business (dove era più conveniente avere connessioni veloci). I dati viaggiavano tutti in digitale, comprese le chiamate e i fax (sui modelli compatibili ovviamente). La velocità era discreta: con il Web 1.0 si caricavano e scaricavano contenuti alla stessa velocità con cui oggi si naviga con una 20 Mega.



3) **xDSL (in uso):** Con l'arrivo dei contratti DSL era possibile far viaggiare i dati su frequenze separate usando sempre la presa telefonica di casa (linea analogica), con il risultato di non dover più tenere il telefono occupato: già solo questo fu quasi una rivoluzione per l'epoca, al di là del cospicuo aumento di velocità (tutt'ora in continuo aumento). **DSL** sta per *Digital Subscriber Line*, ed indica una connessione di tipo digitale ad abbonamento. La sua forma più nota è **ADSL**, dove la A identifica la differenza prestazionale tra le velocità di download e quelle di upload (sempre a favore del download, ecco perché Asimmetrica).

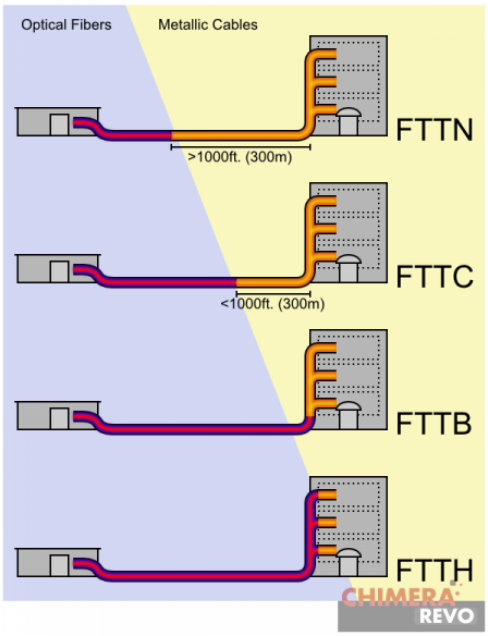
L'ADSL ha un tallone d'Achille non indifferente: utilizza i vecchi cavi analogici per trasmettere i dati, questo indica che una parte della trasmissione sarà giocoforza sullo stesso cavo analogico e sarà soggetta agli stessi problemi di una 56K (interferenze, distanza dalla centrale e degradamento della linea). Molti paesi europei stanno adottando la **VDSL** (un'evoluzione della ADSL) perché riduce a zero il rischio d'interferenze e di sensibilità ai rumori tipica dell'ADSL e promette velocità paragonabili a quelle di una connessione a fibra ottica, con costi inferiori.

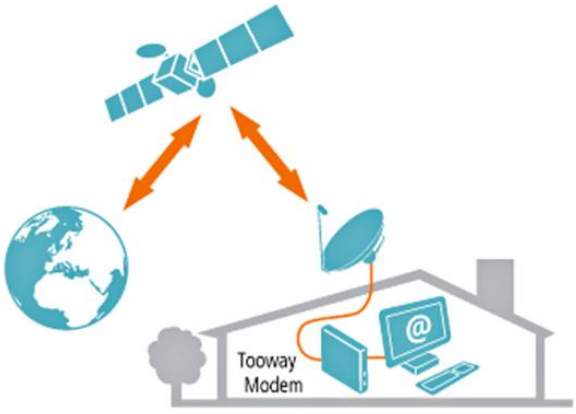
4) **Fibra ottica (in uso):** L'evoluzione più recente delle connessioni Internet è la fibra ottica: esso altro non è che un sottilissimo cavo dove i dati non viaggiano come impulsi elettrici (come invece capita con le tecnologie precedenti), ma come "punti di luce", dove ogni punto di luce equivale ad un bit. Il cuore di questo cavo quindi è una sorta di "tubo di vetro" dove i dati luminosi viaggiano confinati ad elevatissima velocità.

È attualmente la migliore tecnologia per le connessioni di tipo digitale, nonché quella più costosa per via della messa in posa di nuovi cavi e nuove strutture per gestirla. Il funzionamento è di per sé semplicissimo: un'apparecchiatura alla centrale telefonica si occupa di convertire i segnali elettrici in segnali luminosi da inviare lungo la fibra, e viceversa per i segnali luminosi in arrivo, riconvertiti in segnali elettrici gestibili dal modem di casa.

La tecnologia a fibra ottica è molto stabile, quasi del tutto immune alle interferenze e al deterioramento dei cavi (salvo strappi del nucleo di vetro) e offre velocità molto simili al valore contrattuale.

5) **Connessione satellitare (in uso):** Un cenno a parte merita la connessione satellitare, non ordinabile in ordine cronologico per via della sua stessa "natura". Con connessione satellitare intendiamo un tipo di connessione stabilita tramite parabola con un satellite dedicato alla trasmissione dei dati. La particolarità di questo tipo di connessione è data dal fatto che in quasi tutte le offerte casalinghe con la parabola possiamo "solo" ricevere dati, non trasmettere. Una tecnologia che in Italia non ha preso molto piede, anche grazie alla crescita costante della velocità sulle linee analogiche e l'arrivo del **WiMax**, ma che ancora adesso è sfruttata nelle zone difficilmente raggiungibili da un cavo.





6) **WiMax e HyperLAN (in uso):** Anche se parliamo di connessioni di tipo wireless, WiMax e H-LAN rientrano a tutti gli effetti tra le connessioni "fisse", legate quindi a contratti flat per le utenze domestiche. Con questo tipo di connessione sfrutteremo le onde elettromagnetiche in maniera simile al WiFi domestico, ma su lunghe distanze: gli utenti con seria

difficoltà a connettersi in zone digitalmente divise possono così connettersi senza usare la linea analogica ma sfruttando connessioni senza fili. L'ultima evoluzione di tale tecnologia permette di sfruttare **LTE (4G)** al posto del segnale WiMax, con notevole incremento di velocità e copertura.

Come funziona il modem e come avviene la connessione ad Internet?

Va subito chiarito che normalmente l'utente privato non ha il computer fisicamente collegato alla rete Internet chiamato anche **service provider**. Per connetterci a Internet dobbiamo anzitutto collegare, con un modem, il nostro computer ad una linea telefonica che, a sua volta ci collega, sempre con un modem, al computer del provider. Naturalmente il provider presso cui chiediamo l'accesso a Internet per poter sostenere le richieste di più clienti deve possedere più modem che a loro volta devono essere ben più potenti del nostro come capacità di trasmissione. I modem del provider sono a loro volta collegati ad un grosso computer che tecnicamente si chiama **host (ospite)** e che fa la funzione di server rispetto al computer del **cliente (client)**. È importante tenere presente che l'host è fisicamente parte di Internet, cioè è un nodo di una delle tante reti che compongono la "rete delle reti". In questo modo anche il computer del cliente, finché dura la connessione con l'host del provider, viene ad essere fisicamente parte della rete; può quindi usufruire di tutti i servizi che Internet è in grado di offrire, dalla posta elettronica alla ricerca sui cosiddetti motori di ricerca, fino naturalmente alla consultazione delle pagine Web. Vediamo di spiegare in modo più dettagliato che cos'è il Modem:

Il termine modem deriva dalla contrazione di due parole inglesi (MODular e DEModulator), che servono ad indicare due tipi di operazioni:

- **MODulate,** trasformazione degli impulsi digitali del computer in segnali analogici, cioè suoni trasmissibili da una normale linea telefonica;
- **DEModulate**, cioè, all'arrivo, l'operazione contraria di trasformazione di suoni (o segnali analogici) in impulsi digitali leggibili da un computer.

L'unità di misura della velocità di trasmissione di un modem è chiamata bps (bit per second, o bit al secondo) e dal loro numero dipenderà la velocità della trasmissione dei dati. Adesso cercheremo di spiegare in modo più dettagliato che cos'è un **provider**. Dal nostro computer chiediamo via telefono (e modem) ad un provider di connetterci alla rete Internet, quindi bisogna tenere presente che

quando noi ci colleghiamo ad essa o da scuola o da casa via telefono utilizziamo la normale rete telefonica per il tratto tra il proprio modem e il modem del provider pagando la relativa tariffa. Il termine Provider è la semplificazione di un acronimo **IAP** che in inglese sta per *Internet Access Provider* (o fornitore di accessi a Internet), ossia qualcuno che, con un contratto di abbonamento, ci dà la possibilità di collegarci alla rete, essendo egli in possesso di un computer permanentemente funzionante che fa fisicamente parte della rete stessa (cioè di un sito Internet). Oggi, forse più propriamente, si parla di **ISP** (*Internet Service Provider*) che offre altri servizi all'utente, tra cui le pagine Web. C'è qui da ribadire che, una volta attivata la connessione tra il nostro computer e l'host del provider anche il nostro computer fa parte della rete Internet ed è quindi in grado di comunicare con tutti gli altri computer ad essa collegati in tutto il mondo.

Il Protocollo

Arrivati a questo punto è necessario sempre più addentrarci nel mondo di Internet con l'introduzione tecnica di cos'è un **Protocollo**. Abbiamo già spiegato che una rete mondiale è formata da milioni di computer, che tra loro possono essere molto diversi e funzionare con differenti sistemi operativi. C'è quindi da porsi non solo il problema **di come avvenga la trasmissione dei dati** nella rete, ma anche della loro intelligibilità; cioè di come fa un computer a decifrare un messaggio scritto con un computer ed un programma di scrittura completamente diversi. In Internet **due computer connessi possono comunicare tra loro solo utilizzando lo stesso protocollo**, intendendo per protocollo l'insieme delle **regole che ne permettono la comunicazione**: si tratta in pratica di un insieme di convenzioni che definiscono un linguaggio comune, il quale a sua volta rende possibile la comunicazione fra computer dotati di sistemi operativi diversi.

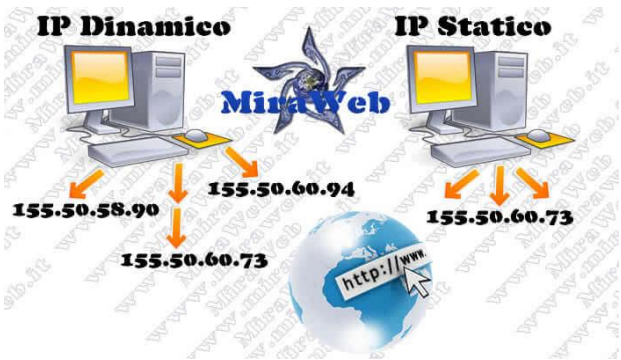
Gli indirizzi

Dopo aver spiegato il funzionamento del Protocollo dobbiamo introdurre un argomento molto importante degli **Indirizzi**. Oggigiorno la quasi totalità dei dispositivi collegati ad una rete, ivi compresa la grande rete globale di Internet, utilizzano infatti il protocollo TCP/IP come standard per la comunicazione digitale. Ma come funziona? I computer utilizzano l'identificativo unico per trovare uno specifico destinatario all'interno del network, esattamente come noi, quando inviamo una lettera, scriviamo l'indirizzo del destinatario sulla busta. Ci sono due

standard per gli indirizzi IP: l'IP versione 4, il cosiddetto **IPv4**, e l'IP versione 6, abbreviato in **IPv6**. I dispositivi collegati in rete possiedono di norma un indirizzo del tipo IPv4 ma da qualche tempo cominciano ad essere utilizzati anche i nuovi indirizzi IPv6. Ma in che cosa si differenziano le due versioni e cosa questo comporta?

- L'IPv4 utilizza una codifica binaria a 32 bit per creare un indirizzo unico sulla rete. Per rendere questa codifica più "leggibile" e facile da utilizzare da parte degli esseri umani, abituati a ragionare in termini decimali (0-9) e non binari (0-1), un indirizzo IPv4 viene espresso con quattro numeri, separati da punti, dove ogni numero è un numero decimale che rappresenta a sua volta un numero binario (a base 2) ad otto bit, chiamato anche ottetto.
- L'IPv6 utilizza invece una codifica binaria a 128 bit per creare un indirizzo unico sulla rete. Questo significa che un indirizzo IPv6 viene espresso con otto gruppi di numeri a base esadecimale (a base 16) separati da due punti (":"). Dato che questa tipologia di numeri può essere abbastanza difficoltoso da utilizzare per un essere umano, anche in questo caso si sono introdotte alcune "semplificazioni", la principale delle quali è costituita dalla possibilità di tralasciare le quadruplette di "0" (0000) contigue.

Nel momento in cui un qualsiasi dispositivo si collega alla rete mondiale ed esso viene assegnato un indirizzo IP, unico ed univoco e, da quel momento, viene abilitato a scambiarsi informazioni, sotto forma di pacchetti di dati, con qualsiasi altro dispositivo presente nella rete. L'indirizzo IP assegnato può assumere la forma di un **indirizzo statico** oppure di un **indirizzo dinamico**. Gli indirizzi del

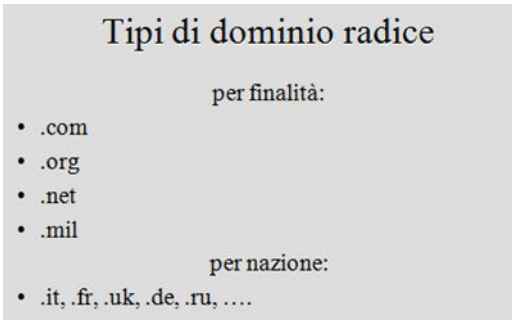


WWW

Un sito internet è un documento elettronico pubblicato su un server web, composto da diverse pagine gerarchicamente collegate, ciascuna con un proprio indirizzo, scritte in linguaggio HTML

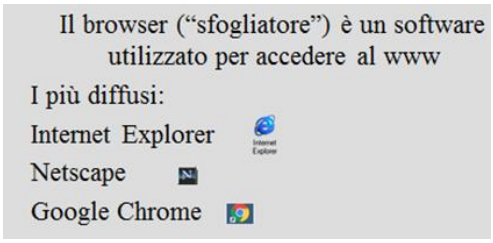
primo tipo sono relativamente rari in quanto richiedono configurazioni del software che gestisce la connessione di rete più complicate ed inoltre richiedono che tale indirizzo IP sia "riservato" a quel particolare dispositivo anche quando esso non è presente in rete (ovvero è disconnesso), il che, come abbiamo visto prima, comporta un serio spreco di risorse. Gli indirizzi del secondo tipo sono di gran lunga i più comuni e vengono assegnati dinamicamente dal **DHCP** (Dynamic Host Configuration Protocol), ovvero dal servizio di rete che si occupa proprio di "staccare" il primo IP disponibile (ovvero non "riservato", come ad esempi o un IP statico) associandolo al dispositivo che ne ha appena fatto richiesta. La caratteristica di questo secondo tipo di IP è quella di essere "dati in prestito" e pertanto sempre "riutilizzabili". In pratica, un dispositivo cui è stato assegnato un indirizzo IP dinamico lo può conservare soltanto per un determinato tempo, scaduto il quale gli viene ritirato dal DHCP che però di solito procede subito a fornirgliene uno nuovo (o, al limite, anche lo stesso di prima). Stessa cosa succede se il dispositivo si disconnette dalla rete per un tempo congruo: il suo indirizzo IP viene "ritirato" dal DHCP che può quindi riutilizzarlo per un diverso dispositivo.

Nella rete Internet incontreremo almeno due tipi di indirizzi: gli **E-mail**, cioè gli indirizzi per la posta elettronica; gli **Url**, cioè un indirizzo che si usa per gli altri protocolli di comunicazione gestiti da un browser, cioè da un programma di gestione di servizi Internet. L'Url permette di arrivare con sicurezza al server, cioè al computer remoto presso cui l'oggetto da noi cercato si trova. I tipi di domini o Url più utilizzati nel mondo hanno le estensioni elencati nella figura al lato:



Il Browser

Internet fornisce una serie di servizi, ciascuno dei quali fino a non molto tempo fa, e in parte ancora adesso, ha bisogno di un suo specifico protocollo e di un suo particolare programma di esecuzione. Oggi tutti questi servizi sono gestiti da un unico programma, detto **browser**, dal verbo inglese to browse, cioè sfogliare (in realtà lo si dovrebbe tradurre in italiano con il termine navigatore): il browser è quindi il programma cliente inizialmente sviluppato per poter visualizzare le pagine



Web, ed esteso poi anche agli altri servizi Internet. Attualmente i browser più conosciuti sono due, entrambi scaricabili direttamente dalla rete. Netscape, Microsoft Internet Explorer, Google Chrome e Firefox. Tecnicamente un browser sarebbe un programma che permette di leggere, ma non di modificare un dato tipo di file: in riferimento specifico a Internet, un browser (o navigatore) è quindi un programma che permette al nostro computer di visualizzare gli oggetti del Web. È cioè il programma che, in base alla Url, permette di accedere ai vari oggetti di Internet.

La posta elettronica

Dopo aver illustrato il funzionamento del Browser è il caso di introdurre la posta elettronica o electronic mail. I vantaggi dell'E-mail rispetto alla posta normale sono: la velocità che rende la trasmissione della comunicazione quasi immediata, cioè praticamente, come si dice, in tempo reale. È stato calcolato che rispetto ai 20 minuti medi di una telefonata e ai 30 minuti di una lettera, per scrivere e mandare una E-mail sono sufficienti meno di 5 minuti e ha un costo molto basso, non solo rispetto alla posta normale ma anche rispetto alla comunicazione via fax; la comunicazione è asincrona, cioè non richiede la contemporanea presenza della persona che manda il messaggio e di chi lo riceve, come invece succede per il telefono (a meno che non si usi la segreteria telefonica);

È evidente che anche per mandare una E-mail ad una persona bisogna conoscerne l'indirizzo a cui si può raggiungerlo sulla rete Internet, cioè il suo E-mail address (o indirizzo di posta elettronica). Facciamo un esempio: marco.verdi@gmail.com questa E-mail è composto dai seguenti elementi: **nome utente** – **dominio**. Il dominio (raggruppamenti di sistemi collegati in rete), individua la categoria del dominio (negli Usa) o la nazione (nel resto del mondo): nel nostro caso il dominio **gmail** significa che l'utente è collegato alla rete con un provider presso il cui sito, l'utente ha l'accesso ad Internet. Il simbolo @ (chiocciola) sta per l'inglese "at", cioè "presso", invece il nome "marco.verdi" evidentemente indica il nome (o lo pseudonimo) della mia posta a cui si vuole fare arrivare il nostro messaggio.

FTP (File Transfer Protocol)

Quando si vuol mandare o ricevere interi file, Internet offre uno strumento che si avvale di un protocollo chiamato **FTP** (*File Transfer Protocol*, protocollo per il trasferimento di file). Il protocollo FTP funziona con il **sistema client-server**, cioè con un computer server in grado di fornire risorse ad altri computer detti client. Per accedere ad un sito FTP basta conoscere il suo indirizzo (IP). Esiste un grande numero di biblioteche che contengono archivi, cioè raccolte di file trasferibili. Si tratta in genere di programmi che vengono offerti in due modi principali:

Vantaggi e svantaggi di internet

Chi avrebbe mai pensato che uno strumento nato per trasferire in modo rapido informazioni militari avrebbe cambiato, in modo ancor più rapido, il mondo intero? Internet, la rete delle reti, ha trasformato il modo di comunicare, ancor più che la televisione, la radio, forse anche più del telegrafo e del telefono, la prima invenzione che permise di far viaggiare le parole velocissimamente.

L'utilizzo di Internet presenta svantaggi e vantaggi per quanto riguarda il nuovo modo di comunicare: Internet è ricco di informazioni e ha un'organizzazione tale da permettere una più alta diffusione del sapere grazie alle numerose enciclopedie in esso presenti e ai numerosi siti culturali accessibili a tutti, senza obblighi nei confronti dei vari sponsor. Tutte le informazioni sono diventate accessibili. Dal paese più piccolo d'Italia puoi collegarti con la più grande biblioteca del mondo e sfogliare (virtualmente) libri che altrimenti non avresti mai potuto consultare. Vedere capolavori custoditi in musei quasi irraggiungibili per la maggioranza degli amanti dell'arte. Conoscere tutto dell'ultimo film dell'attore preferito mentre è ancora in lavorazione; La rete, con la facilità di connessione e i costi comunque contenuti, ha fatto riscoprire il piacere della scrittura. Anche il più pigro ha ripreso a scrivere, senza avere il fastidio di dover poi imbucare la lettera. L'e-mail ha poi il vantaggio di arrivare in tempo reale, senza dover aspettare il postino. Anche se devi chiedere un'informazione su un libro, su uno spettacolo, su un viaggio da fare, basta inviare un messaggio di posta elettronica e nel giro di qualche ora ecco arrivare la risposta. A volte meglio del telefono.

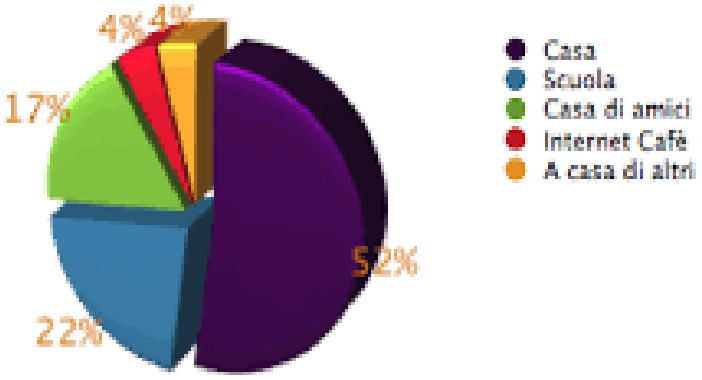
Fonti

1. http://www.informaticapertutti.com/internet-che-cose-come-funziona-e-come-si-usa/
2. http://www.gandalf.it/net/internet.htm
3. http://www.chimerarevo.com/internet/tipi-di-connessione-internet-guida-parte-1-180201/
4. https://it.wikipedia.org/wiki/Internet
5. http://www.fastweb.it/internet/che-cos-e-l-indirizzo-ip/

Rischi del web e come difendersi

Di Marta Miletta e Arianna Daini

Il web, se usato correttamente, ci permette di leggere giornali, informarsi, prenotare visite mediche, comunicare con persone vicine e lontane, pubblicare le nostre storie e promuovere il nostro lavoro, consultare guide e libri digitali. Però se viene usato però senza adeguato senso critico, internet può rappresentare un grande pericolo: spesso, si sente parlare di furti d'identità, di scippi virtuali, oltre che di phishing e di social network utilizzati per danneggiare una persona.



Cyberbullismo

Tra i rischi più pericolosi abbiamo il cyberbullismo o ciberbullismo (ossia «bullismo online») è un tipo di attacco continuo, ripetuto, offensivo e sistematico attuato mediante gli strumenti della Rete.

Il termine cyberbullying fu coniato dall'insegnante canadese Bill Belsey.

Si distinguono due tipi di cyberbullismo:

- il cyberbullying (cyberbullismo), che avviene tra minorenni;
- il cyberharassment ("cybermolestia"), che avviene tra adulti o tra un adulto e un minorenne.

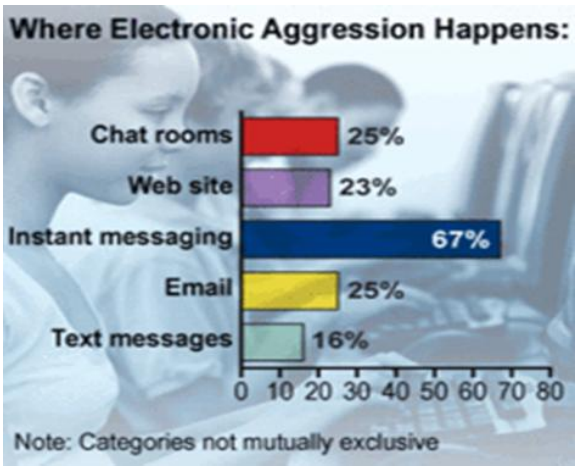
Oggi il 34% del bullismo è online: anche se in forma diversa è una forma di bullismo perché far circolare delle foto spiacevoli o inviare delle mail contenenti materiale offensivo, può costituire un danno psicologico.

Tipi di cyberbullismo:

Esistono diversi tipi di cyberbullismo:

- *Flaming*: quando i messaggi online violenti e volgari sono mirati a suscitare battaglie verbali in un forum;
- *Molestie (harassment)*: quando si inviano ripetuti messaggi insultanti per ferire qualcuno;

- *Denigrazione*: quando si sparla di qualcuno per danneggiare gratuitamente e con cattiveria la sua reputazione, attraverso e-mail, messaggistica istantanea, gruppi su social network, etc.;
- *Sostituzione di persona ("impersonation")*: quando una persona si passare per un'altra persona per spedire messaggi o pubblicare testi reprensibili;
- *Inganno (trickery)*: quando si ottiene la fiducia di qualcuno con l'inganno, per poi pubblicare o condividere con altri le informazioni confidate per mezzi elettronici;
- *Esclusione*: quando si escludere una persona da un gruppo online per provocare in essa un sentimento di emarginazione;
- *Cyber-persecuzione* ("*cyberstalking*"): quando le molestie e le denigrazioni ripetute e minacciose sono mirate a incutere paura;
- *Doxing*: quando si diffondono pubblicamente via internet dati personali e sensibili;
- *Minacce di morte*.



Diffusione del fenomeno

Secondo delle ricerche effettuate tale fenomeno sembra abbracciare sempre più adolescenti e preadolescenti. Il cyberbullismo, sebbene meno diffuso del tradizionale bullismo, può essere suddiviso in sette differenti categorie:

1. SMS;
2. Immagini e video clip (attraverso cellulare);
3. chiamate telefoniche;

4. E-mail;
5. Chat Rooms;
6. Istant messaging (via cellulare);
7. Web Site.

In *Inghilterra*, su uno studio di 129 studenti, il 22% degli studenti hanno riferito di essere stati vittime di cyberbullismo almeno una volta, mentre il 7% è stato vittima per più volte. Le forme più comuni di cyberbullismo sono risultate le telefonate (mute o sgradevoli) e le e-mail offensive, mentre, il bullismo in Chat Rooms è risultato il meno frequente.

In *Norvegia*, in seguito ad una ricerca su 4000 studenti, è stato rilevato che il 3,6% di studenti e il 2% delle studentesse hanno subito cyberbullismo per più volte.

In *Italia*, in una ricerca che ha preso come campione 1387 studenti delle scuole medie superiori e 545 studenti delle scuole medie inferiori, ha rilevato che l'1,3% degli studenti delle superiori e il 3,8% di quelli delle medie hanno dichiarato di essere stati coinvolti in episodi di cyberbullismo. Il 42,7% degli studenti delle medie dice di essere stato oggetto qualche volta di insulti o commenti cattivi o poco gentili via Internet. Il 3,9% degli studenti delle superiori e il 13,8% di quelli delle medie ignorano di conoscere il termine cyberbullismo.

In *Svezia*, hanno svolto un ricerca su 360 adolescenti, la ricerca ha evidenziato che il 12% è stato cyberbullizzato una o due volte, mentre il 10% ha dichiarato di aver agito prepotenze online.

Negli *USA*, in uno studio che ha coinvolto più di 4000 soggetti, ha mostrato che la possibilità di usare servizi di social networking, chat o forum in forma anonima o con pseudonimi rende più facile per soggetti fragili dare avvio ad azioni di cyberbullismo.

In *Finlandia*, in una ricerca rivolta a 6500 studenti ha rilevato che il 2% degli studenti e il 2,4% delle studentesse è vittima di cyberbullismo.

In *Belgio*, ha svolto una ricerca su 2052 studenti, ha rilevato che il 62% è stato vittima di cyberbullismo.

Nei *Paesi Bassi*, hanno svolto una ricerca su 4500 studenti, il 17% ha riferito di essere stato vittima di cyberbullismo una volta al mese ed il 3% una volta a settimana.

In *Grecia*, hanno svolto una ricerca su 544 studenti, le vittime di cyberbullismo sono risultate il 90% (una o due volte al mese), il 6% (due o tre volte al mese), mentre, i cyberbulli il 9% (una o due volte al mese) e il 7% (due o tre volte al mese).

In *Canada*, si è svolto un'indagine su 264 studenti, di cui il 25% riferisce di aver subito cyberbullismo, mentre il 17% afferma di aver cyberbullizzato un coetaneo. In un recente studio la percentuale di studenti vittime di cyberbullismo è salita al 35%.

In *Australia*, si è riscontrato che il 14% di 120 studenti è stato oggetto di cyberbullismo mentre l'11% ha cyberbullizzato un compagno nell'ultimo anno.

Il cyberbullismo in Italia è un reato che non rispetta l'articolo 3 della costituzione italiana. Le cause legali sono un risarcimento economico e la prigione.

Phishing

Il ***phishing*** è un tipo di truffa effettuata su Internet mediante cui un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.

Si tratta di una attività illegale che sfrutta una tecnica di ingegneria sociale: il malintenzionato effettua un invio di messaggi di posta elettronica che imitano, nell'aspetto e nel contenuto, messaggi legittimi di fornitori di servizi; tali messaggi richiedono di fornire informazioni riservate (ad es. il numero della carta di credito o la password per accedere ad un determinato servizio).

Solitamente è una truffa effettuata mediante posta elettronica, ma non mancano casi che sfruttano altri mezzi, quali i messaggi SMS.

Il phishing è una minaccia attuale ad alto rischio sono i social media come Facebook, Twitter, e Google+. Degli hacker potrebbero infatti creare un clone del sito e chiedere all'utente di inserire le sue informazioni personali. Gli hacker traggono vantaggio dal fatto che questi siti vengono utilizzati a casa, al lavoro e nei luoghi pubblici per ottenere le informazioni personali o aziendali.

Il termine phishing allude all'uso di tecniche sempre più sofisticate per "pescare" (da “fishing”) dati finanziari e password di un utente.

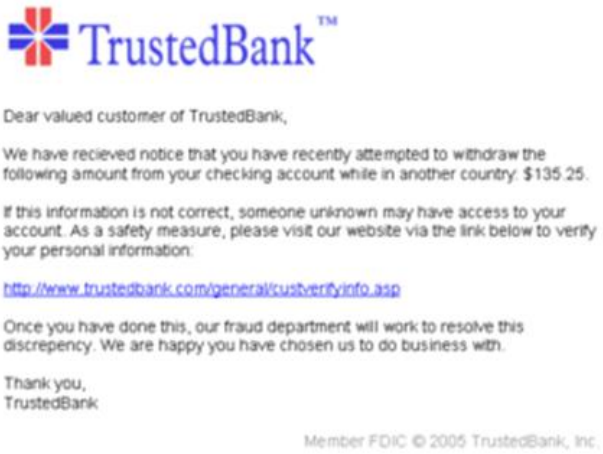
Metodologia generale di attacco

Il processo standard delle metodologie di attacco di phishing è:

- l'utente malintenzionato (phisher) spedisce a un utente un messaggio email simile, nella grafica e nel contenuto, a quello di un'istituzione nota al destinatario (ad es. la sua banca, il suo provider web, un sito di aste online a cui è iscritto);
- l'e-mail contiene quasi sempre avvisi di particolari situazioni o problemi verificatesi con il proprio conto corrente/account (ad es. un addebito enorme, la scadenza dell'account, ecc.) oppure un'offerta di denaro;
- l'e-mail invita il destinatario a seguire un link, presente nel messaggio, per evitare l'addebito e/o per regolarizzare la sua posizione con l'ente o la società di cui il messaggio simula la grafica e l'impostazione (Fake login);
- il link fornito non porta al sito web ufficiale, ma a una copia apparentemente simile al sito ufficiale, situata su un server controllato dal phisher, con lo scopo di richiedere e ottenere dal destinatario dati personali particolari, di solito con la scusa di una conferma o la necessità di effettuare un'autenticazione al sistema; queste informazioni vengono memorizzate dal server gestito dal phisher e poi finiscono nelle mani del malintenzionato;
- il phisher utilizza questi dati per acquistare beni, trasferire somme di denaro o l'utilizza come "ponte" per ulteriori attacchi.

Se l'e-mail contiene l'invito a cogliere una nuova "opportunità di lavoro" (quale operatore finanziario o financial manager), consistente nel fornire le coordinate bancarie del proprio conto online per ricevere l'accredito di somme che vanno poi ri-trasferite all'estero tramite sistemi di money trasfert (Western Union o Money Gram), trattenendo una percentuale dell'importo, che può arrivare a cifre molto alte. In realtà si tratta del denaro rubato con il phishing, per il quale il titolare del conto online beneficiario commette il reato di riciclaggio di denaro sporco. Quest'attività comporta per il phisher la perdita di una certa percentuale di quanto è riuscito a sottrarre, ma esiste un interesse a disperdere il denaro sottratto in molti conti correnti e a fare ritrasferimenti in differenti Paesi, perché così diviene più difficile risalire alla identità del criminale informatico e ricostruire il meccanismo illecito. Se i trasferimenti coinvolgono più Paesi, i tempi per la ricostruzione dei movimenti bancari si allungano, poiché serve una rogatoria e

l'apertura di un procedimento presso la magistratura locale di ogni Paese interessato.



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Storia del phishing

La prima tecnica di phishing fu descritta in un trattato presentato nel 1987 al International HP Users Group, Interex.

Tipi di phishing

- *Spear phishing*: un attacco mirato verso un individuo o una compagnia che è stato denominato spear phishing. Gli attaccanti potrebbero cercare informazioni sull'biettivo per poter incrementare le probabilità di successo. Questa tecnica è la più diffusa su internet, con una quota del 91% degli attacchi;
- *Clone phishing*: è un tipo di phishing in cui una mail legittima viene modificata negli allegati o nei link e rimandata ai riceventi, dichiarando di essere una versione aggiornata. Le parti modificate della mail sono volte a ingannare il ricevente;
- *Whaling*: quando gli attacchi sono rivolti verso figure di spicco (ad es. aziende o entim). Viene mascherata una mail/ pagina web con lo scopo di ottenere delle credenziali di un manager. Sono state utilizzate mail identiche a quelle dell'FBI cercando di forzare il ricevente a scaricare e installare del software;
- *Manipolazione dei link*: è uno dei metodi di phishing più utilizzati degli exploit tecnici per far apparire i link nelle mail come quelli autentici. Altri trucchetti diffusi sono l'utilizzo di URL scritti male, oppure l'utilizzo di sottodomini; un'altra metodologia è registrare un dominio lavorando su lettere visivamente simili;
- *Aggiramento dei filtri*: successivamente, i phisher hanno iniziato a mascherare il testo inserendolo in immagini, in questo modo i filtri anti-phishing hanno più

difficoltà nell'identificazione delle minacce. Questo ha portato però, all'evoluzione dei filtri, ora capaci di trovare testo in immagini. Questi filtri usano OCR (riconoscimento ottico dei caratteri);

- *Contraffazione di un sito web*: quando una vittima visita un sito di phishing l'attacco non è terminato, nella pagina possono essere presenti altri comandi JavaScript per alterarne la barra degli indirizzi. Può essere fatto mettendo un'immagine nella barra degli indirizzi o chiudendo la finestra e aprendone una nuova con l'indirizzo legittimo;
- *Cross-site scripting*: Un attaccante può anche usare un sito fidato e inserire i suoi script malevoli. Questi tipi di attacco sono problematici perché tutto3 sembra legittimo, compresi i certificati di sicurezza. Un attacco di questo tipo è stato utilizzato nel 2006 contro PayPal;Phishing telefonico: non sempre il phishing implica l'utilizzo di un sito web o di mail, vengono infatti inviati messaggi sms agli utenti, i quali dicono che ci sono stati dei problemi con i loro account bancari. Quando il numero indicato (gestito dal phisher e di solito si tratta di un numero Voice over IP) nel messaggio viene chiamato viene chiesto all'utente il proprio PIN. Il Vishing (voice phishing) utilizza un finto numero di chiamante, in modo da dare l'apparenza di un'organizzazione fidata.

Anti-Phishing

Fino al 2007 l'adozione di strategie anti-phishing per proteggere i dati personali e finanziari era bassa. Oggi ci sono molte tecniche per combattere il phishing:

- *Istruzione*: una strategia per combattere il phishing è istruire le persone a riconoscere gli attacchi e ad affrontarli. L'educazione può essere molto efficace, specialmente se vengono enfatizzati alcuni concetti e fornito un feedback diretto. L'Anti-Phishing Working Group, un ente di rinforzo per la sicurezza, ha suggerito che le tecniche di phishing convenzionali potrebbero diventare obsolete in futuro, con la crescente consapevolezza delle persone delle tecniche di social engineering usate dai phisher. Ha inoltre predetto che il pharming e diversi usi di malware diventeranno più comuni per rubare informazioni. Tutti possono aiutare il pubblico incoraggiando pratiche sicure ed evitando quelle pericolose;
- *Risposta tecnica*: misure di anti-phishing sono state implementate nei browsers, come estensioni o toolbar, e come parte delle procedure di login. Sono anche disponibili software contro il phishing.
- *Aiuti nell'identificare i siti legittimi*: la maggior parte dei siti bersaglio del punishing sono protetti da SSL con una forte crittografia, dove l'URL del sito web è usata come identificativo. Questo dovrebbe confermare l'autenticità del sito, ma è facile da aggirare. La vulnerabilità che viene sfruttata sta nella user interface (UI) del browser. Nell'URL del browser viene indicata con dei colori la connessione utilizzata;
- *Browsers*: che allertano l'utente quando visitano siti truffaldini: un altro approccio per combattere il phishing è quello di mantenere una lista dei siti noti per phishing e controllare se l'utente li visita. Tutti i browser popolari incorporano questo tipo di protezione. Alcune implementazioni di questo approccio mandano gli URL visitati a un servizio centrale, che ha suscitato preoccupazione per la privacy. Una protezione di questo tipo può essere applicata anche a livello di DNS, filtrando a monte le richieste pericolose, questo approccio può essere applicato a ogni browser, ed è simile all'uso di un file host (un file in cui si definiscono destinazioni personalizzati per domini);

- *Argomentare i login con password*: il sito di Bank of America è uno dei siti che ha adottato il sistema di far scegliere nel momento dell'iscrizione un'immagine all'utente, e mostrarla ad ogni login successivo. In questo modo essendo l'immagine nota solo all'utente e al sito legittimo in un eventuale attacco di phishing questa sarebbe assente o sbagliata. Però molti studi hanno suggerito che l'utente ignori la mancanza della sua immagine personale e immette la sua password;
- *Eliminazione delle mail di phishing*: si cerca di eliminare le mail attraverso filtri specializzati contro la spam, diminuendo le minacce diminuiscono le possibilità di essere ingannati. I filtri si basano sul machine learning e natural language processing per classificare le mail a rischio;
- *Monitoraggio e blocco*: molte compagnie offrono servizio di monitoraggio e analisi per banche e organizzazioni con lo scopo di bloccare i siti di phishing. Però i singoli individui possono contribuire riportando tentativi di phishing, a servizi come Google, Cyscon o PhishTank. Internet Crime Complaint Center noticeboard raccoglie e gestisce allerte per ransomware e phishing;
- *Verifica a 2 passi delle transazioni*: prima di autorizzare operazioni sensibili viene mandato un messaggio telefonico con un codice di verifica da immettere oltre la password;
- *Limiti della risposta tecnica*: un articolo di Forbes dell'agosto 2014 argomenta che il phishing resiste alle tecnologie anti-phishing perché una tecnologia non può sopperire in modo completo alle incompetenze umane ("un sistema tecnologico per mediare a debolezze umane").

La truffa dei “viaggi fantasma”

Nei periodi di vacanza, estate, Natale, Capodanno, numerose sono le finte offerte di viaggi che offrono pacchetti "last minute" per posti inesistenti.

Come per qualsiasi acquisto in rete, è importante avere alcune cautele basilari: verificare se il sito o la società che gestisce la vendita è affidabile. Se si tratta di privati che inseriscono annunci su siti di compravendita, verificarne le credenziali del venditore, e per cautela non inviare tutti i soldi subito: inviare soltanto una caparra e poi pagare il resto del soggiorno quando si arriva sul posto, dopo aver verificato che è tutto a posto.

Social network e furti d'identità

Molto spesso si sente parlare di persone che si impossessano dell'identità di una persona per diffamarla, denigrarla o distribuire password e numeri di telefono. È possibile anche che qualcuno si impossessi dell'identità di una persona per creare finti profili, in cui li mettono in cattiva luce o utilizzano il nome per compiere atti illeciti o per ricevere benefici. Per cautelarsi la prima regola è quella di non fornire dati personali sensibili (ad esempio indirizzo, data di nascita, luogo di lavoro o scuola frequentata, ect.). La sostituzione di persona, l'accesso abusivo ai sistemi informatici o l'utilizzo non autorizzato del sistema e la detenzione di codici e password sono tutti reati previsti del codice penale e punibili con la reclusione.

Dialer auto installanti

I dialer sono software, solitamente file ".exe", che si autoinstallano sul proprio PC quando si visitano determinati siti Internet. Il Dialer si connette ad un proprio numero, il che comporterà delle spese telefoniche non previste, di elevatissima entità. Visto che i modem dialer sono ormai in disuso, questo tipo di attacco non ha più alcun riscontro.

Spam

Lo "***Spamming***", o lo "***Spam***" è l'invio verso indirizzi generici, non verificati o sconosciuti, di messaggi ripetuti ad alta frequenza da renderli indesiderati (generalmente commerciali o offensivi). È noto anche come posta spazzatura (in inglese junk mail). Può essere attuato attraverso qualunque sistema di comunicazione, ma il più usato è Internet, attraverso messaggi di posta elettronica, chat, tag board, forum, Facebook e altri servizi di rete sociale. Chi invia messaggi spam viene chiamato spammista (spammer in inglese). Lo scopo dello spam è la pubblicità. C'è il pericolo che possa essere a sfondo sessuale più o meno esplicito.

Fonti

1. Wikipedia
2. I Giovani e i Media
3. Polizia di stato
4. Gestweb

Il Deep Web

Di Grasso Dario

Cos'è il Web

Il World Wide Web, letteralmente "rete di grandezza mondiale", abbreviato Web, è uno dei principali servizi di Internet che permette di navigare e usufruire di un insieme vastissimo di contenuti amatoriali e professionali collegati tra loro attraverso legami (link), e di ulteriori servizi accessibili a tutti o ad una parte selezionata degli utenti di Internet. Le caratteristiche che hanno fatto del World Wide Web una vera e propria rivoluzione nel mondo della telematica, possono essere riassunte nei seguenti punti:

- la sua diffusione planetaria;
- la facilità di utilizzazione delle interfacce;
- la sua organizzazione ipertestuale;
- la possibilità di trasmettere/ricevere informazioni multimediali;
- le semplicità di gestione per i fornitori di informazione.

E' necessario sapere che il Web è uno dei servizi di Internet che permette il trasferimento e la visualizzazione dei dati, mentre la rete internet è l'infrastruttura tecnologica dove viaggiano i dati. Internet è il più rivoluzionario sistema di scambio per l'uomo. Può essere visto come un pozzo di risorse, più o meno infinito e, proprio come nella vita reale, presenta determinati luoghi e posti che possono soddisfare qualunque requisito, basta cercare abbastanza in profondità. Secondo le statistiche, oltre il 40% della popolazione mondiale lo usa quotidianamente per diversi scopi, dall'intrattenimento alle comunicazioni. Dalla sua nascita Internet si è espanso rapidamente, arrivando ad essere onnipresente nella vita di miliardi di persone, che possono facilmente accedervi da qualsiasi piattaforma in qualsiasi momento della giornata. La rete cresce ogni minuto sempre di più ed attualmente sono oltre cinquecento milioni i domini registrati su internet, senza contare le pagine secondarie, le 404 e i siti morti. E' estremamente facile e veloce da usare: basta aprire un qualsiasi motore di ricerca, digitare una o più parole chiave e premere invio per ottenere i risultati in pochissimi secondi. I risultati indicizzati dai motori di ricerca costituiscono quello che viene definito Clear Web. Si tratta di informazioni facilmente accessibili, alla

portata di tutti, con un semplice click. Ci sono sempre migliaia, a volte milioni, di risultati, perciò, data questa sovrabbondanza di dati, si potrebbe pensare che ciò che Internet ha da offrire sia tutto qui. Tuttavia esiste un'altra faccia del web. Il Clear web costituisce soltanto il 4% della totalità dei dati presenti su Internet, questo significa che quando si cercano informazioni su Google, non si ottengono nemmeno la metà dei dati presenti online. Basti pensare ad un iceberg: la normale navigazione su internet permette soltanto di vederne la punta emersa, tutto ciò che resta sottacqua invece costituisce il Deep Web.

Clear Web & Deep Web

Nessuno sa con precisione quanto sia vasto il Deep Web, ma si suppone sia il 96% del web, mentre il Clear Web è, come suddetto, il rimanente 4%. Si pensi ad esempio ai dati protetti, come la posta in entrata nelle e-mail o l'Home page di Facebook: per questione di privacy, queste pagine non sono indicizzate, eppure esistono, fanno parte del Deep Web. Questa enorme porzione di Internet costituisce un vasto deposito di informazioni e dati nascosti, non soltanto siti, ma anche forum, immagini e video che attendono di essere recuperati nei recessi più oscuri della rete.

Bisogna però sfatare qualche mito: soprattutto negli ultimi tempi in molti hanno trattato l'argomento del Deep Web, spacciando filmati o immagini forti per contenuti provenienti da esso.

Questo è soltanto in parte vero: in altre parole, navigando su numerosi siti, è facile incontrare qualcuno che afferma di aver recuperato qualcosa di terrificante dal Deep Web. Nella maggior parte dei casi però si tratta di fake con materiale creato ad hoc per alimentare la paura degli utenti più inesperti.

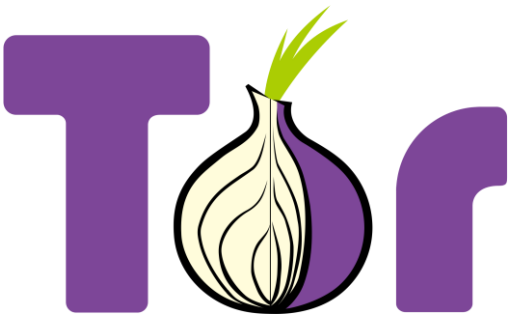
Insomma, non tutto è come appare, e trovare materiali realmente provenienti dal Deep Web non è facile come sembra: bisogna saper cercare. Alle volte, infatti, emerge qualcosa che realmente proviene dal lato oscuro di Internet. Sapendo quali forum frequentare e quali link cliccare, ecco che si accede alla parte più intricata e profonda della rete.

I domini del Deep web sono costantemente controllati e suscettibili ad attacco, per cui non sorprende che nascano e muoiano in pochissimo tempo, ma, data la loro natura segreta e nascosta, è lì che si annidano alcune delle perversioni più amene dell'uomo.

E' sconsigliabile fare ricerche troppo a fondo nel Deep Web, infatti, a meno di non essere Hacker o navigatori molto esperti, è possibile vedere soltanto ciò che il Deep Web vuole mostrare, ossia la sua parte più superficiale. Addentrarsi molto a fondo implicherebbe trovare materiale davvero estremo, e assolutamente illegale.

Come accedere

Navigare nel Deep web non è semplice: occorre avere contatti giusti e sapere come muoversi per non incorrere in problemi con la legge, bisogna utilizzare un browser che sia in grado di fare Onion Routing, ossia mascherare e rendere su diversi livelli anonima la navigazione in rete. Il più famoso è senz'altro Tor, acronimo di "The Onion Router", che funziona come estensione dei normali Browser (ad esempio Firefox, Google Chrome ecc..) e permette di collegarsi al Deep Web mantenendo il quasi totale anonimato. Molti siti del Deep Web usano "Hidden Tor Service" , ma sono anche diffusi I2P, JhonDonym e Freenet.

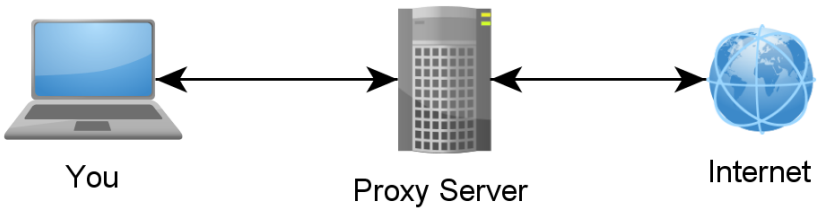


Tor, a prima impressione, sembrerà un qualsiasi altro browser, ma non è così, infatti è facile rendersi conto che non si sta navigando normalmente in Internet. Esso permette di poter navigare in modalità quasi anonima, nei servizi nascosti del Deep Web, nonché quelli che nell'URL hanno come pseudo dominio la scritta ".onion".

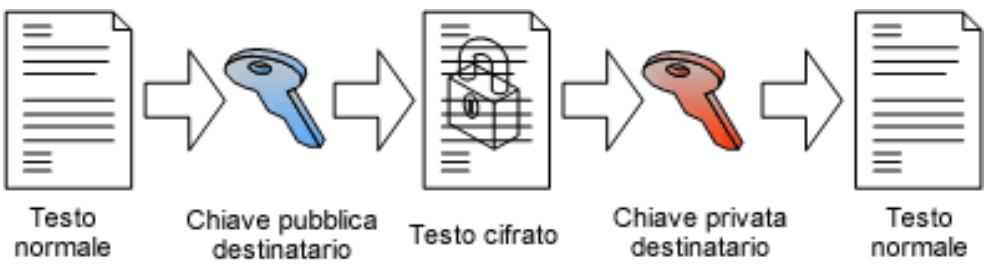
Tor nasce da un progetto militare, precisamente dagli U.S.A Naval Research Laboratory, come strumento per proteggere le comunicazioni della marina militare. Era un servizio primario per la protezione delle comunicazioni governative. Oggi è un progetto open-source, disponibile per chiunque. Viene utilizzato da giornalisti, militari, forze dell'ordine, whistle-blower, infiltrati e soprattutto dagli Hacktivisti (Anonymus).

E' un Browser che si incentra nell'anonimato ed è necessario infatti sapere che utilizza tre elementi:

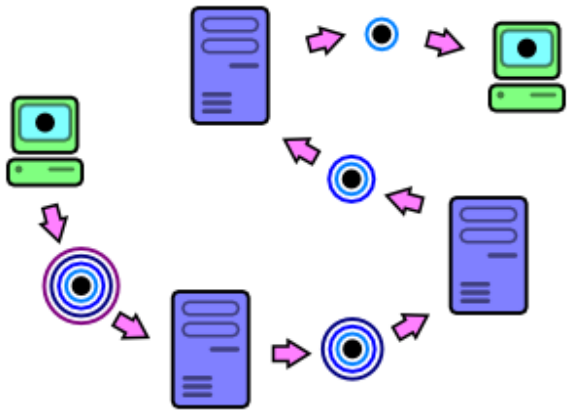
1) Il Server Proxy, impiegato quando si ha la necessità di rimanere anonimi, quindi mascherare il proprio indirizzo IP. E' necessario che il client invii una richiesta al server proxy, che andrà a richiedere i contenuti al server specificato e li restituirà allo stesso;



2) La Crittografia Asimmetrica, cioè una crittografia dove la comunicazione fra due soggetti è associata a una coppia di chiavi: una chiave pubblica e una chiave privata. Teoricamente se con una delle due chiavi si codifica un messaggio, allora quest'ultimo potrà essere decifrato solo con l'altra chiave;



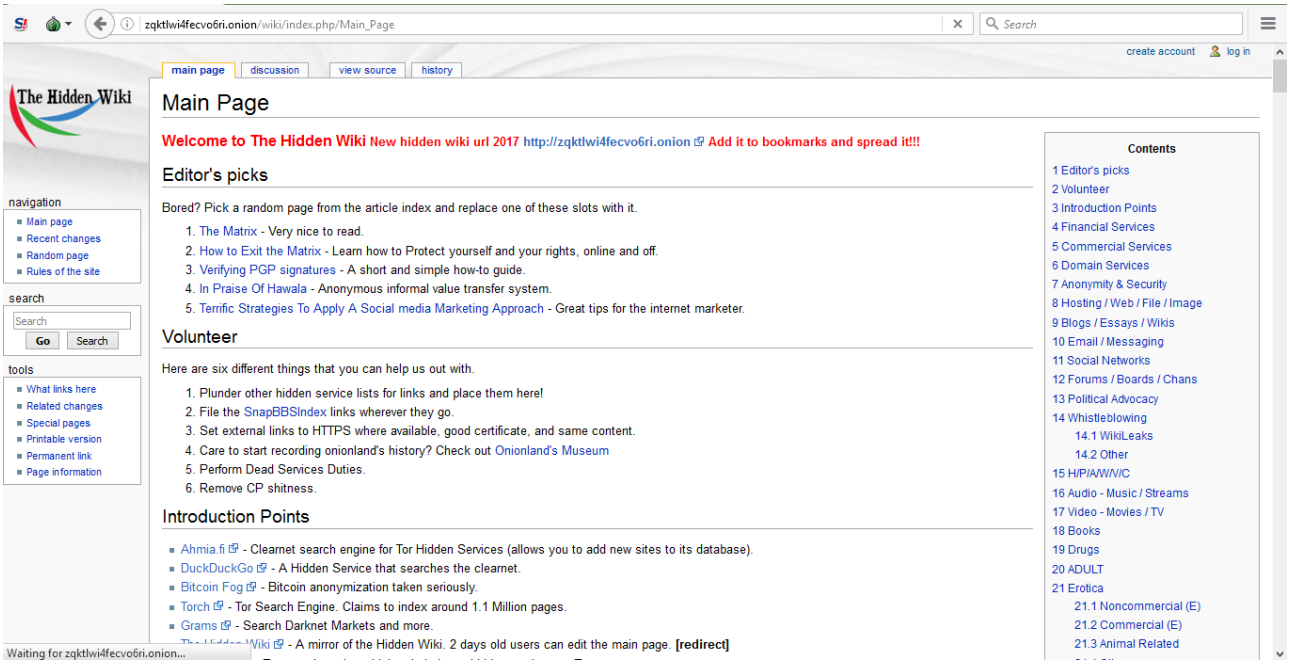
3) L'Onion Routing, ovvero una tecnica di anonimizzazione delle comunicazioni in una rete. Un dato Onion è una struttura a "cipolla" formata da un messaggio che è stato "avvolto" da strati di crittografia, uno successivo all'altro. Questi strati saranno decifrati (ovvero "sbucciati") da tanti intermediari quanti sono gli strati di crittografia, prima di arrivare al destinatario finale. Il mittente rimane anonimo, perché ciascun intermediario conosce solo l'intermediario immediatamente precedente e quello immediatamente successivo.



Navigazione Deep Web

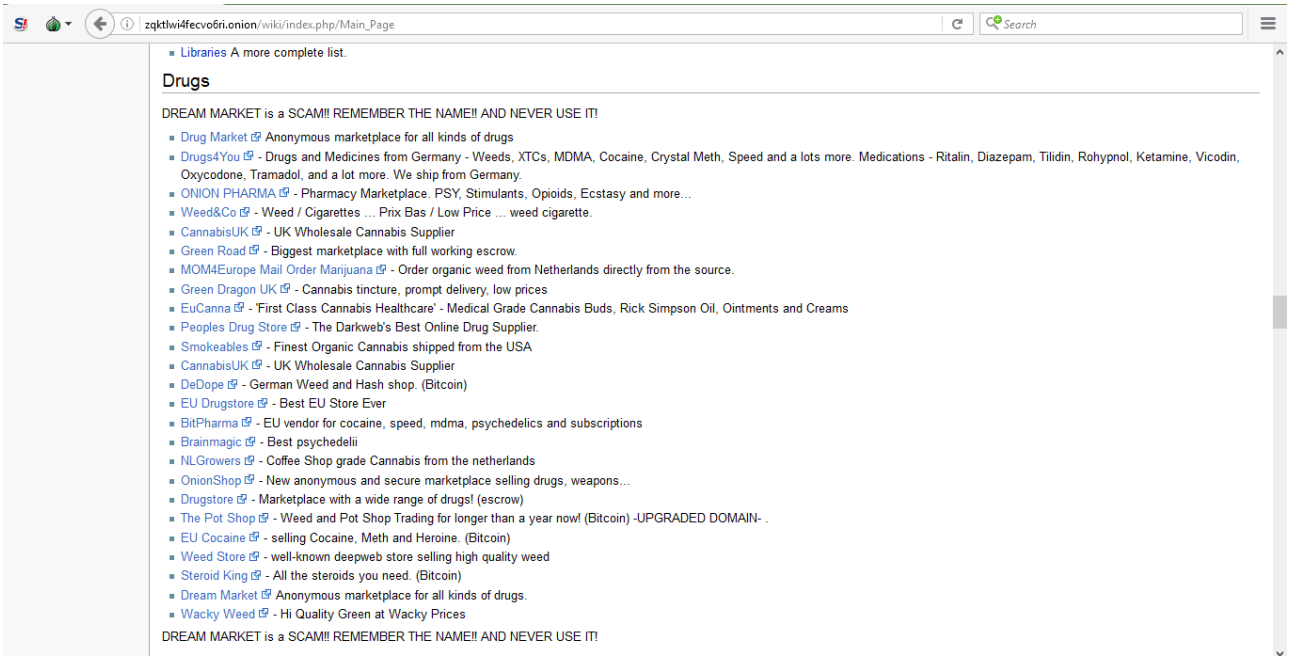
Una volta entrati si può iniziare a scendere nei recessi del web, mediante siti come "The Hidden Wiki", che fornisce una serie di link divisi per categorie. Può essere visto come un sito simile a Wikipedia, ma in realtà è un elenco di altri Hidden Sites suddivisi in categorie.

Infatti, "The Hidden Wiki" tiene conto dei principali indirizzi web più visitati nel Deep Web e i cui indirizzi non sono mai statici, ma cambiano dinamicamente per impedire alle autorità di localizzarli fisicamente. Infatti, numerosi link sono stati individuati e di conseguenza bloccati, chiusi e ora sono solamente accessibili attraverso passaparola nei forum, mediante link alternativi.



Sarà facile notare che la maggior parte dei link elencati finiscono per ".onion", ciò dimostra come l'ambiente di navigazione, per quanto simile, è in realtà diverso dal normale.

A partire da qui si andrà ad attraversare un cancello informatico, oltre il quale si trova soprattutto criminalità. In particolare vengono offerti servizi quali riciclaggio di denaro, il fishing dei numeri di carta di credito, la vendita di armi e lo scambio di droghe.



Ovviamente The Hidden Wiki è solo uno dei tanti siti attraverso i quali si può accedere alle lande più oscure del Deep Web, ma sicuramente è uno dei più stabili.

Deep Web

Il Deep Web è una rete nascosta, accessibile solo attraverso determinati software, che utilizzano dei protocolli di comunicazione codificati o criptati. Circa l'85% dei contenuti in rete si trova in questo mondo nascosto sotto la parte superficiale del Web, alla quale accediamo normalmente attraverso i classici browser, vedendo solo il restante 15%.

Spesso, per rendere l'idea, viene utilizzato l'immagine di un iceberg, perché in superficie è visibile solo una piccola parte di esso e contiene i siti più utilizzati, accessibili attraverso un qualsiasi browser, mentre in profondità l'iceberg nasconde un'enorme porzione di sé.

Nel Deep Web vi sono server non visibili, i quali non necessariamente fanno cose illegali, ma semplicemente vogliono mantenersi nascosti al governo o agli utenti normali. In questa zona vi sono server che contengono documenti di ogni genere, per esempio ricerche scientifiche non ancora divulgabili, informazioni accademiche a cui solo gli esperti possono accedervi, risorse governative o semplicemente utenti normali che condividono alcuni file Peer-To-Peer.

La rete ora conosciuta come Deep Web, in realtà era andata come un progetto negli anni '90 allo scopo di proteggere le telecomunicazioni militari statunitensi, e successivamente sviluppato anche da informatici amatoriali di tutto il mondo, che volevano ottenere una rete più libera, non rintracciabile, come avviene con le normali attività di navigazione.

Dopo qualche anno dalla sua nascita, il Deep Web venne, come ancora oggi, utilizzato per cooperazioni del tutto illegali, depravate e violente. Sempre più spesso si parla di questa rete nascosta e a volte viene anche visto come un mondo quasi leggendario, ma è tutto assolutamente reale e molte delle cose orribili che si sentono in tv, sono state annunciate e preparate qui, da episodi di cronaca violenta ad attentati terroristici. Contrariamente allo scopo per cui è stato ideato, ovvero l'irrintracciabilità, il Deep Web, in paesicome Germania e Stati Uniti, da

diversi anni viene monitorato, controllando gli Hidden Server presenti sui loro territori. Infatti, in Germania, già nel 2006, sono stati chiusi e confiscati moltissimi Tor server, che venivano utilizzati da pedofili per richiedere materiale di ogni genere. Nonostante ciò, la crescente domanda di risorse illegali in rete e la diffusione di nuovi metodi per evadere ai controlli, anche dall'FBI, rende ancora

oggi il Deep Web un cumulo di tenebre informatiche dove si nascondono diversi criminali.

Quindi, da questi presupposti, era nata una rete del tutto nascosta agli occhi delle autorità e che voleva solo essere libera, ma proprio come disse Oscar Wilde: "Le cose peggiori sono sempre state fatte con le migliori intenzioni".

La parte legale del Deep Web

Il Deep Web è solitamente associato a storie inerenti ad attività illegali, ma sul web invisibile si possono trovare anche cose innocue, bizzarre o rivoluzionarie, che tra l'altro sono completamente legali. Infatti, il Web Sommerso è idealmente suddiviso in: Deep Web, costituito da pagine non indicizzate dai comuni motori di ricerca; Dark Web, un sottoinsieme del Deep Web, solitamente irraggiungibile attraverso una normale connessione internet o senza far uso di software particolari, perché giace su una rete definita "Darknet"(maggiormente utilizzata per attività illegali). Il Deep Web "legale" è costituito da siti di persone che amano trascorrere il loro tempo libero a spasso per i tunnel sotterranei, oppure di altre che sono costrette a starci perché vivono sotto regimi dittatoriali. Poi ci sono cose veramente di nicchia, che per qualche motivo non vengono accettate dalla società. "Bright Planet", un gruppo specializzato in intelligence del Deep Web, lo definisce come "qualunque cosa che un motore di ricerca non riesce a trovare." Questo perché i motori di ricerca comuni trovano solamente contenuti indicizzati.

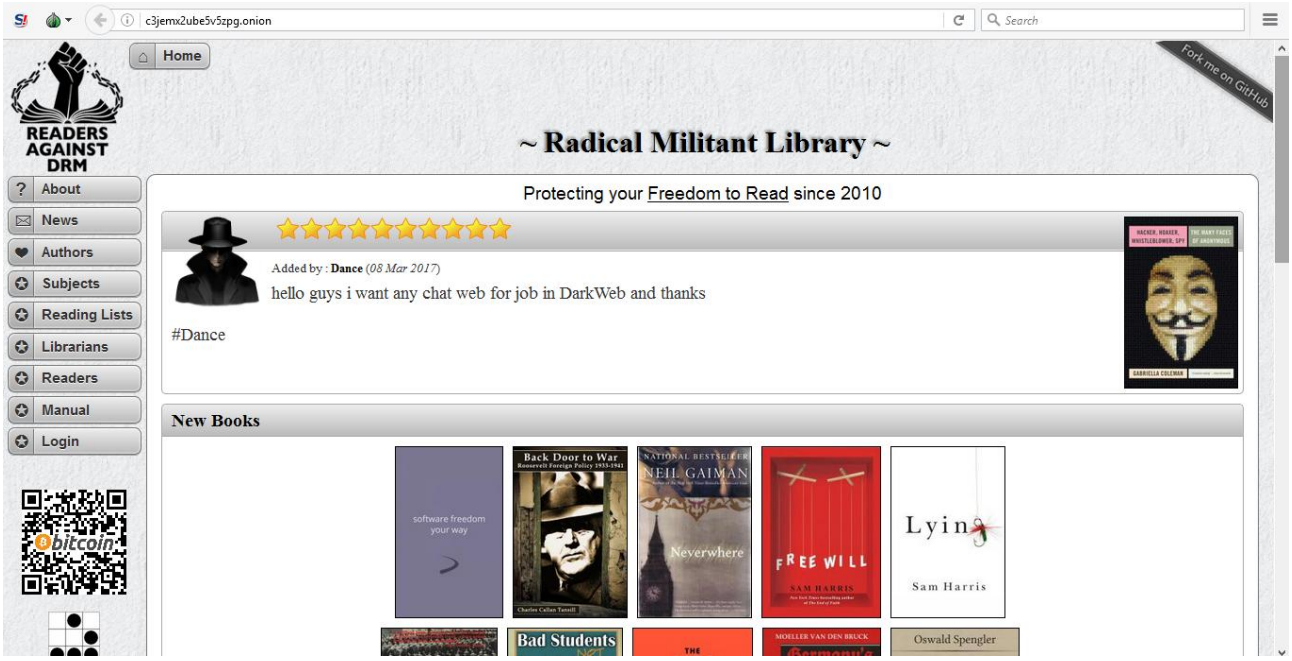
Naturalmente, alcuni di questi sono bloccati. In tal caso, per visualizzare un sito del genere, bisogna conoscere l'URL esatto. Questi URL non indicizzati costituiscono il Deep Web.

Nel 2000, gli URL indicizzati da Google erano un miliardo. Nel 2008, mille miliardi. Oggi, nel 2017, molti di più. Il Deep web non è solo un insieme di cose strane, illegali o divertenti. È pieno di database del calibro della "National Oceanic

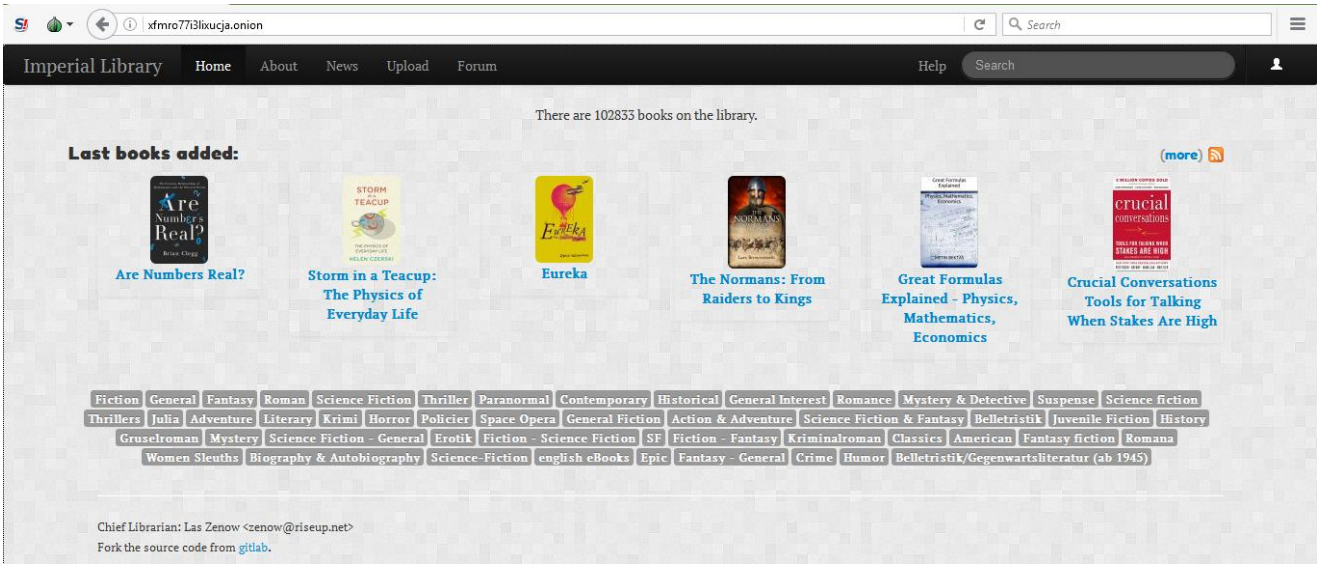
and Atmospheric Administration" degli Stati Uniti, della NASA o dell'Ufficio Brevetti e Marchi. Ci sono anche svariate Intranet (reti interne per compagnie e università), che contengono principalmente informazioni noiose sul personale.

Essendo una tecnologia progettata per nascondere l'identità degli utenti, sono inusuali i numerosi blog di fan fiction erotica, i circoli rivoluzionari, i siti di speleologia e gli archivi di Scientology. Per avere un'idea migliore di tutti gli aspetti del Deep web che non hanno a che fare con droghe e sicari, basta dare un'occhiata alle parti meno nascoste, appena sotto la superficie.

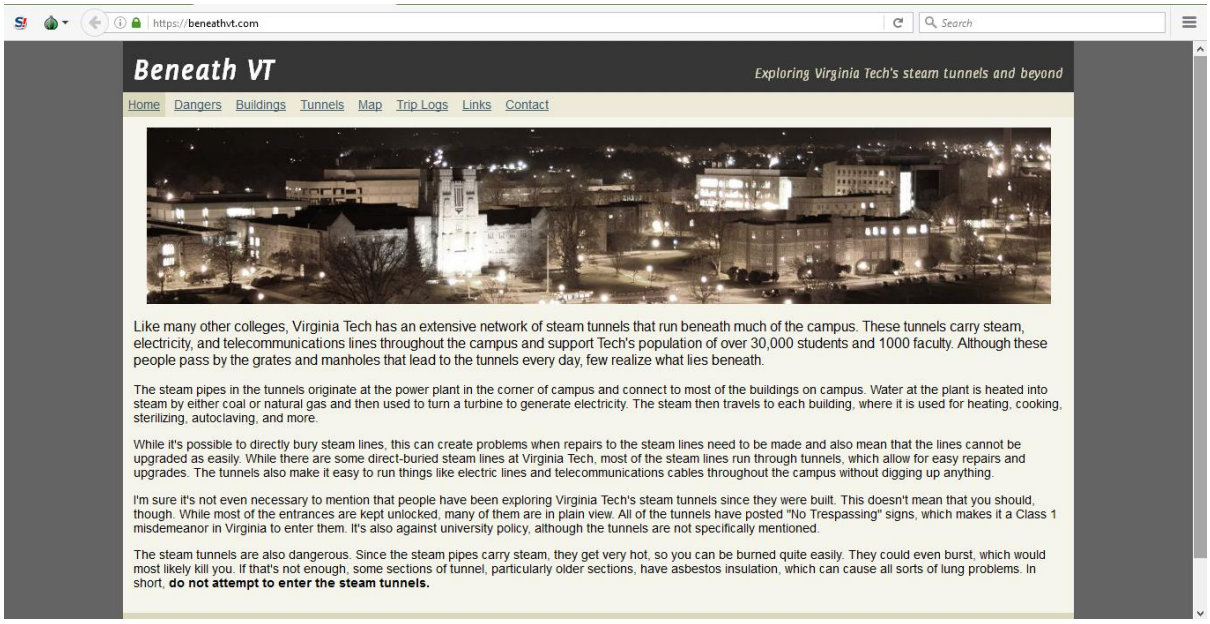
Il "Club di lettura di Jotunbane" è un ottimo esempio. Sulla homepage, vicino all'immagine in stile propaganda sovietica di un pugno che libera un libro dalle catene, si legge chiaramente "Lettori contro la DRM" (gestione dei diritti digitali). I libri più popolari sono sovversivi o di fantascienza.



La "Biblioteca Imperiale di Trantor", dal nome decisamente sinistro, è un sito dedicato a discussioni e dibattiti politici, dove definiscono la Società "prodotto dei nostri desideri, e il governo della nostra malvagità". Anche Dread Pirate Roberts, presunto fondatore di Silk Road, nel 2011 ha avviato un circolo del libro sul Deep web.



A volte ci si domanda se parte del contenuto sul Deep Web debba necessariamente essere anonimo. Un sito che si chiama “Beneath VT” documenta le esplorazioni sotterranee sotto Virginia Tech, nelle quali degli avventurieri esplorano i tunnel sotterranei. I creatori spiegano che “nonostante ogni giorno tutti camminino sopra le grate e i tombini che portano ai tunnel, pochi sanno cosa c’è sotto”.



Siti del genere si trovano anche sul web tradizionale, ma pare che il Deep web offra agli utenti una sorta di conforto simbolico e psicologico. In pratica, ospita una serie di sottoculture formate da persone dai desideri diversi che sono in cerca di persone simili a loro.

Il Deep web ha un grosso potenziale liberatorio; navigare nel completo anonimato provoca sensazioni strane, quasi di euforia, che non sono troppo lontane da quelle che probabilmente hanno provato un quarto di secolo fa i primi utenti di internet.

Può offrire idealismo, spensieratezza e comunità, ma anche l'illegalità, l'immoralità e il grottesco. Il BitCoin, per esempio, ha legami molto forti col Deep web: era inteso come sistema monetario alternativo, ma all'inizio era famoso perché era possibile comprare le droghe online.

È incoraggiante sapere che molti scelgono il Deep web per vivere le loro strane ma innocue vite nell'anonimato. Come diceva Voltaire: "anche se non condivido quello che dici, difenderò fino alla morte il tuo diritto di fantasticare ambiguamente sui miei personaggi Disney preferiti."

Transazioni di denaro

La domanda più frequente è: "Come vengono pagati i servizi offerti nella Dark Net?" La risposta è semplice: il "Bit Coin".

Il Bit Coin è una moneta virtuale ideata per non lasciare traccia delle transazioni effettuate, anche se ora sta prendendo piede la Dark Coin o Dash. Nel "Deep Web" un vastissimo universo di siti, che svolgono le attività economiche più varie, utilizzano principalmente il BitCoin come moneta di scambio. Un gigantesco mercato nero, di attività illecite e spesso illegali.

Tramite Tor, oltre all'anonimato durante la navigazione, è consentito effettuare transazioni attraverso il BitCoin. Bit Coin è il nome di una valuta digitale, che ha la stessa validità del denaro contante, ma è spendibile solamente in Internet. Essa consente di effettuare pagamenti anonimi in sicurezza, grazie all'architettura peer-to-peer.

Questa cripto valuta è stata ideata nel 2009, da un programmatore sconosciuto, in arte Satoshi Nakamoto. Un BitCoin ha un valore di circa 514€ sebbene non esista una quotazione ufficiale. La quotazione la fa il mercato e chiunque può vendere BitCoin in rete al prezzo che desidera.

Il BitCoin è privo di una “banca centrale”. Il registro delle transazioni viene mantenuto da un gruppo di computer o da un singolo server centrale. L’architettura Peer-To-Peer fa si che una copia del registro delle transazioni sia presente su ogni computer connesso alla rete BitCoin. Tale registro viene così costantemente aggiornato, sulla base degli importi spesi da tutti gli account connessi.

La spendibilità dei BitCoin è legata a una chiave di decrittazione, all’interno dei cosiddetti “Wallet”: i portafogli dei singoli utenti. Questi sono protetti da una password (la firma digitale), che assicura che la transazione provenga dal legittimo proprietario dei BitCoin. La firma digitale deve essere differente per ogni transazione. La chiave pubblica e quella privata, assicurano il corretto funzionamento del sistema di pagamenti. L’unica informazione conoscibile è la parola chiave incomprensibile, che funge da indirizzo del Wallet stesso.

Tale meccanismo, unito al sistema di anonimizzazione gratuito offerto da Tor, rappresenta una preziosissima risorsa per tutti quei business fondati su scambi illeciti, che vanno a disegnare il mercato nero globale. All’interno del Deep Web, mediante BitCoin, si possono acquistare documenti falsi, carte di credito rubate, droga, armi, omicidi su commissione, filmati pedopornografici, bambini schiavi e molto altro.

Coloro che effettuano questi tipi di acquisti per fuggire dalla tracciabilità, creano sempre nuovi Wallet per ogni diversa transazione. Ciò rende il BitCoin molto simile al denaro contante e molto appetibile per i businessmen più spregiudicati.

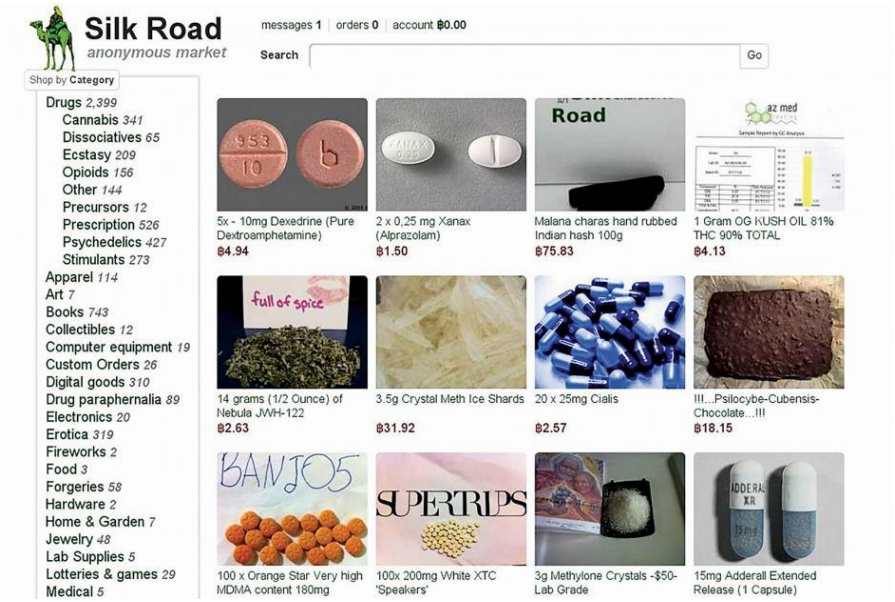
DarkWeb

Andando sempre più in profondità la rete nascosta diventa sempre più complessa e buia, ed è qui che inizia il Dark web, quella porzione di Deep Web più conosciuta e che ha infangato tutti i buoni propositi per cui era nata questa rete. Nel Dark Web agli utenti viene garantito quasi completamente l’anonimato e le autorità, per riuscire a prendere un singolo utente, devono impiegare molte risorse e tempo.

Il Dark Web è la più recondita e profonda parte della rete, dove sono presenti siti contenenti risorse illegali, come filmati pedopornografici, sicari disposti ad

uccidere chiunque e dovunque, droghe che arrivano direttamente a casa, giochi mortali trasmessi in diretta a scopo ludico, maltrattamento di animali, torture su persone reali, vendita di organi, armi di ogni genere e molto altro ancora. Nel Dark Web o Dark Net ogni desiderio più malato, ogni azione illegale ed ogni fantasia più viscida è assolutamente possibile.

Proprio come negli abissi marini, in questa zona oscura si trovano siti ormai famigerati, che si dedicano a mettere in commercio qualunque cosa. Il più famoso è ovviamente Silk Road o "Via della seta" che rappresenta il più grande negozio illegale in rete, una sorta di mercato nero virtuale. È stato chiuso più volte dall'FBI, ma inevitabilmente riaperto in breve tempo. In questo Virtual Market, è possibile acquistare droghe di ogni genere, da quelle più leggere come Marijuana o Hashish, passando a quelle pesanti come Eroina, Crack e Cocaina, fino ad arrivare a droghe in grado di devastare le persone con poche dosi, sia psicologicamente che fisicamente, come la Crocodile, i Sali da Bagno o Metanfetamina.



Se l'intenzione fosse quella di voler acquistare sostanze stupefacenti, basterebbe entrare in uno dei link suggeriti dal sito, registrarsi e selezionare il numero di prodotti. La descrizione della sostanza sarà, nella maggior parte dei casi, spaventosamente minuziosa, con informazioni sulla composizione chimica, la provenienza e anche una sorta di "recensione" sugli effetti della sostanza. In più, c'è una disponibilità a compiere atti illegali, come il recapito degli oggetti desiderati, che è da far spavento. Nella Silk Road non vi sono solamente droghe, ma anche medicine illegali, libri banditi, dipinti trafugati, hardware e software per clonare carte di credito e molto altro ancora. Aperto nel Febbraio 2011 questo mercato virtuale ha capitalizzato, in soli 2 anni, secondo le stime dell'FBI, più di un miliardo di dollari. Uno dei business più redditizi della storia della rete. Ovviamente un colosso del genere non poteva rimanere nascosto per sempre: così, attraverso un pedinamento online, l'FBI è riuscita a trovare il suo fondatore, Ross Ulbricht, noto come "Dread Pirate Roberts", colui che portò lo spaccio di droghe ad un nuovo livello. Ross è stato arrestato nel 2013, con l'accusa di fomentare la distribuzione di droghe, reati informatici, riciclaggio di denaro e la pesantissima accusa di essere la principale causa di morte di 6 persone tossicodipendenti. Nel 2015, dopo una battaglia legale, Ross venne condannato da una giuria di New York all'ergastolo e a pagare un risarcimento di circa 183 milioni di dollari. I giudici sono stati duri per non creare precedenti e scoraggiare altre persone a seguire le sue orme. Purtroppo però la Silk Road, invece di estinguersi, è diventata un marchio, un vero e proprio Brand e ora nella Dark Net, nonostante gli sforzi dell'FBI, sono stati aperti altri siti di commercio illegale come Silk Road 2.0 e Silk Road 3.0 e tantissimi altri come Agora, AlphaBay, Achropolis, Dream Market e molti altri. L'elencazione dei servizi illegali potrebbe andare avanti all'infinito, ma c'è una cosa molto importante da sottolineare: la maggioranza di questi siti sono falsi. Il Deep Web è pieno di Hacker e Scammers, pertanto siti come quelli che promettono la vendita di schiavi a pagamento sono probabilmente truffe; i soldi vengono inviati, ma la droga, le armi, i documenti falsi e gli schiavi non verranno mai consegnati. Questo è anche uno dei motivi per cui i siti di vendite e scambio sono fra i più accessibili: chiunque si celi dietro di essi infatti ha interesse ad attirare clienti creduloni così da guadagnare soldi facili. Accade anche che molti siti siano tranelli architettati dalle attività federali per

catturare eventuali criminali. Naturalmente è impossibile stabilire con precisione quali siano.

Nel Dark Web, oltre alla vendita di stupefacenti e armi, si trovano anche gli Hitman, ossia Sicari che offrono i loro servizi di Killer professionisti. Vi sono tutta una serie di modalità con cui possono essere uccise le persone, ad esempio si possono mettere delle taglie, proprio come nel vecchio Far West, dove veniva pubblicata una foto, con una promessa di risarcimento in denaro per l'uccisione della persona in questione. Esistono infatti diversi siti dove vengono pubblicate persone che si vogliono morte e il primo che invia una foto con la vittima ammazzata prende tutti i soldi promessi. Una nota piuttosto particolare è che in alcuni siti la taglia di una persona continua ad aumentare grazie al contributo di altri utenti che vogliono quella persona morta. Per esempio, nel Novembre 2013, su un sito chiamato Assassination Market, in pochi mesi la taglia per la testa di Keith Alexander (direttore della National Security Agency) era arrivata a 40 BitCoin, mentre il presidente degli Stati Uniti Barack Obama aveva una taglia di 124 BitCoin. Anche altre persone importanti nella struttura finanziaria e governativa dei principali stati del mondo, avevano e hanno ancora oggi, una taglia.

La Parte Macabra del DarkWeb

Ma la mente umana può essere molto più malata di così. Oltre ad assassini e narcotrafficanti, nel Dark Web spopolano i siti contenenti materiali pedopornografici e non solo, vi sono siti che si dedicano alla vendita vera e propria di bambini per essere violentati, torturati e uccisi, pratica diffusa soprattutto in Asia. Sui siti vengono pubblicate le fotografie tristi delle vittime, con tanto di descrizione e prezzo, proprio come se fossero merce: immagini difficili da commentare. Esiste un sito di nome Paraside che si presenta con una grafica tipica del WEB degli albori negli anni novanta e contiene una sterminata lista di File, Link e Torrent. All'apparenza sembra semplicemente un archivio di immagini e scritti pseudo-anarchici , cioè un archivio di materiali che vanno dai tutorial per la produzione di bombe artigianali e droghe, alle istruzioni per portare a termine un atto terroristico, passando per mostrare contenuti nazisti,

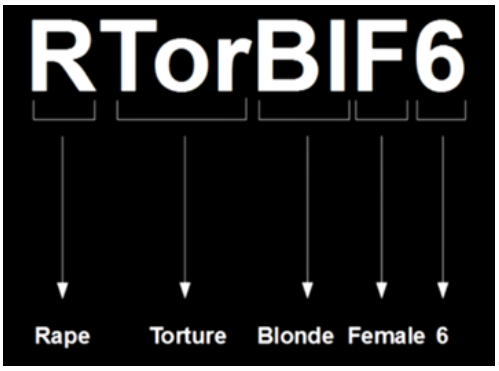
razzisti e criminali nonché materiali relativi alla violenza sessuale, spingendosi fino al cannibalismo.

Il Cannibalismo è una categorie piuttosto comune, dopotutto la follia degli esseri umani non ha limiti : si pensi soltanto che sulla Hidden Wiki è possibile trovare link di siti aventi materiale pedopornografico. Fortunatamente, questi tipi di siti vengono regolarmente controllati e abbattuti dalle autorità, pertanto ne chiudono decine ogni giorno. Qualche tempo fa, inoltre, gli attivisti di Anonymous hanno portato avanti una massiccia azione di boicottaggio nei confronti dei gestori, contribuendo così alla cattura di un gran numero di pedofili. Ma oltre alla pedopornografia il Deep Web offre un'infinità di servizi di Video Sharing o Video Streaming. Molte di queste situazioni, partono dal nucleo familiare, ad esempio un padre garantisce l'accesso alla webcam di sua figlia mentre la ragazza è impegnata in rapporti sessuali: il servizio è a pagamento e vengono offerti diversi tipi di pacchetti tariffe a secondo di quante fotografie o video si vogliano acquistare.

In un altro caso, un ragazzo offre, in cambio di Bit Coin, libero accesso alla webcam situata nella camera da letto della fidanzata, indicando persino gli orari migliori per poterla spiare. Offerte del genere avvengono anche per filmati di stupri, violenze, zoofilia e necrofilia. Qualsiasi perversione esista al mondo, nel Deep Web è presente.

Addentrandosi più in profondità nel Deep Web è possibile trovare ogni tipo di nefandezza, dalla quale emergono servizi raccapriccianti, che per essere raggiunti bisogna avere esperienza e sapersi muovere per non essere rintracciati.

Pagando profumatamente è possibile accedere a collezioni di Torture Porn, dove le vittime vengono seviziate e stuprate, oppure veri e propri Snuff, dove i soggetti vengono uccisi. Se invece capita di imbattersi in un filmato pedopornografico, questo tipo di contenuti saranno solitamente nominati mediante un linguaggio criptato, ad esempio in un contenuto che ha come titolo la seguente sequenza:



E' necessario sapere che non si tratta di lettere e numeri casuali. La R sta per "stupro"(rape in inglese), Tor sta per "tortura"(torture), Bl sta per "bionda"(blonde), F sta per "femmina"(female) e 6 per "sei anni", nonché l'età del soggetto ripreso. E' facile da intuire come questi contenuti siano di natura illegale, chiunque ne detenga il possesso può infatti essere rintracciato e perseguito penalmente , dunque coloro che creano e diffondono questo genere di materiali si accertano che essi rimangano ben nascosti.

Accade però che ogni tanto qualcosa emerga, ad esempio il sito degli NLF, si tratta di un gruppo ben organizzato che si fa chiamare NO LIMITS FUN (Divertimento senza limiti), che sfrutta il Deep Web per vendere materiale Snuff e di Violenza sessuale.

Parlando di casi che fecero balzare il Deep Web agli apici della cronaca mondiale, si può citare la vicenda del Marzo 2001, in cui, il Tedesco Armin Meiwes, pubblicò un annuncio sul forum "The Cannibal Café". L'annuncio diceva "Cerco un ragazzo di buona costituzione dai 18 ai 30 anni, per essere macellato e poi mangiato". Il 9 Marzo, l'Ingegnere Armando Brandes rispose all'annuncio e si recò a casa di Meiwes. Dopo averlo drogato, Brandes venne lasciato dissanguare in una vasca da bagno, dopo essere stato mutilato, mentre Meiwes leggeva un libro tranquillamente al piano di sotto. La vittima infine venne sgozzata e sezionata: i resti di Brandes furono conservati in un congelatore, e quello che ora è conosciuto come il Cannibale di Rotenburg li consumò nel giro di 10 mesi. Questa terribile vicenda non sarebbe mai stata scoperta se tempo dopo Meiwes non avesse pubblicato un nuovo annuncio nel Deep Web, dove ancora una volta cercava carne umana.

Il Deep web, dopotutto, è sempre stato un punto di ritrovo per i feticisti del cannibalismo. Non sempre si tratta di cannibali reali come Meiwes, molto spesso infatti tutto resta a livello teorico, venendo sfruttato solo per soddisfare l'immaginazione o il desiderio sessuale, ciò però non toglie che sia possibile trovare dei veri e propri tutorial sulla macellazione della carne umana, oppure degli scambi di consigli su forum tematici.

Andare troppo a fondo può essere estremamente pericoloso, e non si tratta di virus più o meno dannosi, ma di veri e propri guai con la giustizia. Ciò che è certo è che il Deep web è costantemente controllato dalle autorità, in quanto alcune porzioni di esso contengono materiali illegali.

Su internet è possibile essere ciò che si vuole, sprigionare la propria natura, esprimere se stessi….e questa…è la cosa che spaventa di più.

Conclusioni

Chi cerca trova. E cosa si cerca? Naturalmente ciò che non si trova.

La mente umana è attirata da ciò che non conosce, ma soprattutto da ciò che è proibito. Occultare qualcosa, nasconderla, vietarla, la rende solo più interessante all'occhio di chi, credendo di essere al sicuro dietro uno schermo, vuole saperne sempre di più. Spesso però, la curiosità non fa bene, anzi. E' bello voler superare i propri limiti, ampliare i propri orizzonti, ma quando si comincia a parlare di sette, pedopornografia, cannibalismo, forse ci si dovrebbe fermare per chiedersi "Queste cose fanno davvero per me?".

La risposta dovrebbe essere sempre "No."

L'unica cosa da fare è chiudere il computer e tornare alla propria vita, perché una volta che ci si è immersi fino in fondo, riemergere per prendere una boccata d'aria potrebbe non essere così semplice.

Fonti

1. https://it.wikipedia.org/wiki/Web_sommerso
2. http://www.unicoffee.it/economia/deep-web-bitcoin-un-gigantesco-mercato-nero/
3. http://www.focus.it/natura/cinque-cose-da-sapere-sul-deep-web
4. https://motherboard.vice.com/it/article/un-tour-delle-meraviglie-legali-del-deep-web

L’open source

Storia

Di Lara Cosentino

Introduzione

In informatica, il termine inglese open source (che significa i aperti) indica un software di cui gli autori (più precisamente, i detentori dei diritti) rendono pubblico il codice sorgente, favorendone il libero studio e permettendo a programmatori indipendenti di apportarvi modifiche ed estensioni. Questa possibilità è regolata tramite l'applicazione di apposite licenze d'uso. Il fenomeno ha tratto grande beneficio da Internet, perché esso permette a programmatori distanti di coordinarsi e lavorare allo stesso progetto.

Alla filosofia del movimento open source si ispira il movimento open content (*contenuti aperti*): in questo caso, ad essere liberamente disponibile non è il codice sorgente di un software, ma contenuti editoriali quali testi, immagini, video e musica. Wikipedia è un chiaro esempio dei frutti di questo movimento. Attualmente, l'open source tende ad assumere rilievo filosofico, consistendo in una nuova concezione della vita, aperta e refrattaria ad ogni oscurantismo, che l'open source si propone di superare mediante la condivisione della conoscenza.

Open source e software libero, seppure siano sovente utilizzati come sinonimi, hanno definizioni differenti: l'Open Source Initiative ha definito il termine "open source" per descrivere soprattutto libertà sul codice sorgente di un'opera. Il concetto di software libero descrive più generalmente le libertà applicate ad un'opera, ed è prerequisito che il suo codice sia consultabile e modificabile, rientrando generalmente nella definizione di open source.

Avvenimenti

Negli anni quaranta il problema della condivisione del codice si poneva in termini molto diversi da quelli attuali. Esistevano pochi computer, costruiti spesso in un unico esemplare e con specifiche hardware molto diverse e non compatibili. Basti pensare che solo nel 1951 una ditta metterà a listino un modello di computer, il Ferranti Mark 1. Di conseguenza anche il software che veniva sviluppato caso per caso non poteva essere trasportato su altre macchine e aveva standard di

riferimento a cui attenersi. D'altra parte, le conoscenze di programmazione venivano liberamente condivise in quanto erano considerate più simili alle conoscenze scientifiche che a quelle industriali. Verso la fine degli anni cinquanta, e soprattutto negli anni sessanta, è stato possibile riusare lo stesso codice e distribuirlo anche se in modo oggi ritenuto piuttosto artigianale, ovvero con nastri e schede perforate. Questo fenomeno diventò evidente soprattutto quando si affermò il vantaggio di usare una stessa porzione di codice, il che presupponeva di avere macchine uguali e problemi simili. Fino a tutti gli anni settanta, anche se in misura decrescente, la componente principale e più costosa di un computer era l'hardware, il quale era comunque inutile in assenza di software. Da ciò la scelta dei produttori di hardware di vendere il loro prodotto accompagnato da più software possibile e di facilitarne la diffusione, fenomeno che rendeva più utili le loro macchine e dunque più concorrenziali. Il software, tra l'altro, non poteva avvantaggiare la concorrenza in quanto funzionava solo su un preciso tipo di computer e non su altri, spesso neanche su quelli dello stesso produttore. Un altro fattore che favorì lo sviluppo di software condiviso fu la diffusione di linguaggi di programmazione. Specie in ambito scientifico un programma scritto in Fortran poteva essere scambiato tra diversi ricercatori. La disponibilità del codice sorgente era indispensabile per apportare le piccole modifiche rese necessarie dai "dialetti" adottati dalle varie ditte per il linguaggio di programmazione. Lo sviluppo dei sistemi operativi rese i programmi sempre più portabili, in quanto lo stesso sistema operativo, con gli stessi compilatori veniva offerto dal produttore sui suoi diversi modelli di hardware. La presenza di sistemi operativi funzionanti per macchine di differenti produttori hardware ampliava ulteriormente le possibilità di usare lo stesso codice in modo relativamente indipendente dall'hardware usato. Uno di questi sistemi operativi era Unix, iniziato nel 1969 come progetto all'interno di un'impresa delle telecomunicazioni, la AT&T. Una famosa causa antitrust contro la AT&T le vietò di entrare nel settore dell'informatica. Questo fece sì che Unix venisse distribuito ad un prezzo simbolico a buona parte delle istituzioni universitarie, le quali si ritrovarono ad avere una piattaforma comune, ma senza alcun supporto da parte del produttore. Si creò spontaneamente una rete di collaborazioni attorno al codice di questo sistema operativo, coordinata dall'Università di Berkeley, da dove sarebbe poi

uscita la versione BSD di Unix, che diventa da un lato un centro di sviluppo ed innovazione, dall'altro è la base di partenza per numerosi fork.

La nascita del software proprietario

Considerato che la condivisione del codice è nata insieme all'informatica, piuttosto che di origini dell'Open Source potrebbe essere più appropriato parlare, invece, di origine del software proprietario, ed esaminare il contesto storico in cui questa origine ha avuto luogo.

L'utilità principale delle licenze restrittive consiste nella possibilità di rivendere un programma più volte, se necessario con alcune modifiche purché non rilevanti. Questo presuppone che esistano clienti diversi con esigenze simili, oltre che l'esistenza di più computer sul quale poter far eseguire il programma. Queste condizioni cominciano a determinarsi negli anni sessanta, grazie al fatto che esisteva un maggior numero di utilizzatori con esigenze standardizzabili come lo erano quelle delle organizzazioni economiche nell'area della contabilità, la logistica o delle statistiche.

L'introduzione dei sistemi operativi rese inoltre possibile l'utilizzo dello stesso programma anche su hardware differente aumentando così le possibilità di riutilizzo dello stesso codice e dunque l'utilità nell'impedire la duplicazione non autorizzata dei programmi.

La suddivisione della AT&T in 26 società, le cosiddette *Baby Bell*, permise alla AT&T di usare logiche prettamente commerciali nella distribuzione del suo sistema operativo Unix, innalzando notevolmente i costi delle licenze e impedendo la pratica delle patch. Il 1982 fu anche l'anno della divisione delle diverse versioni commerciali di Unix, portate avanti dai singoli produttori di hardware. Questi ultimi, effettuando delle piccole modifiche alla propria versione del sistema operativo, impedirono ai propri utenti l'utilizzo di altri sistemi, facendo in modo che i programmi scritti per la propria versione di Unix non funzionassero su versioni concorrenti.

Gli anni 90: Internet, Linux e le Open Source Definition

Benché Internet avesse visto la luce già negli anni settanta, è soltanto agli inizi degli anni novanta, con la diffusione del protocollo HTTP e la nascita dei

primi browser, che cominciò ad essere diffuso prima in ambito accademico e poi in modo sempre più capillare anche tra semplici privati.

All'inizio degli anni novanta, il progetto GNU non aveva ancora raggiunto il suo obiettivo principale, mancando di completare il kernel del suo sistema operativo (GNU Hurd). Per sopperire a tale mancanza, William e Lynne Jolitz riuscirono ad effettuare il porting di UNIX BSD su piattaforma Intel 386 nel 1991. Purtroppo, negli anni successivi tale porting si trovò ad affrontare problemi di natura legale USL v. BSDi che ne ritardarono temporaneamente lo sviluppo.

Nello stesso anno, Linus Torvalds, studente al secondo anno di informatica presso l'Università di Helsinki, decise di sviluppare un proprio sistema operativo imitando le funzionalità di Unix su un PC con un processore Intel 386. Tale processore venne scelto per il suo minor costo e per la sua maggiore diffusione rispetto alle piattaforme hardware per le quali erano disponibili i sistemi operativi Unix. Torvalds era spinto dall'insoddisfazione riguardante alcuni applicativi di Minix (un sistema Unix-like su piattaforma PC), dal desiderio di approfondire le proprie conoscenze del processore Intel 386, e dall'entusiasmo per le caratteristiche tecniche di Unix.

Torvalds distribuì il proprio lavoro tramite Internet e ricevette immediatamente un ampio riscontro positivo da parte di altri programmatori, i quali apportarono nuove funzionalità e contribuirono a correggere errori riscontrati. Nacque così il kernel Linux, il quale fu subito distribuito con una licenza libera.

Internet dal canto suo, rende possibile la comunicazione tra persone molto distanti in tempi rapidi e a basso costo. Inoltre rende possibile la distribuzione di software direttamente dalla rete, riducendo ulteriormente i costi di duplicazione e le difficoltà a reperire il software stesso. La diffusione dei CD-ROM come supporto privilegiato di raccolte di software rese possibile il fenomeno delle cosiddette distribuzioni.

Linux può essere considerato come il primo vero progetto "open source" cioè come il primo progetto che faceva affidamento essenzialmente sulla collaborazione via Internet per progredire; fino ad allora, infatti, anche i progetti di software libero come Emacs erano stati sviluppati in maniera centralizzata

seguendo un progetto prestabilito da un ristretto numero di persone, in base cioè ai principi 'standard'di ingegneria del software. Si assumeva valida anche per i progetti open source la 'legge di Brooks', secondo cui "aggiungere sviluppatori a un progetto in corso di implementazione in realtà rallenta il suo sviluppo", legge che ovviamente non è applicabile a un progetto di sviluppo open source.

Agli inizi degli anni novanta, l'idea delle licenze liberali era rappresentata soprattutto da Richard Stallman e la sua FSF, ovvero le licenze liberali per eccellenza erano la GPL e la LGPL che però venivano ritenute "contagiose", in quanto a partire da un codice licenziato con la GPL qualsiasi ulteriore modifica deve essere distribuita con la stessa licenza. Le idee stesse di Stallman venivano viste con sospetto dall'ambiente commerciale statunitense, il che non facilitava la diffusione del software libero. Per favorire dunque l'idea delle licenze liberali nel mondo degli affari, Bruce Perens, Eric S. Raymond, Ockman e altri cominciarono nel 1997 a pensare di creare una sorta di lobby a favore di una ridefinizione ideologica del software libero, evidenziandone cioè i vantaggi pratici per le aziende e coniarono il termine "*Open Source*". Ciò anche al fine di evitare l'equivoco dovuto al doppio significato del termine "free" nella lingua inglese, visto che spesso veniva interpretato come "gratuito" invece che come "libero". L'iniziativa venne portata avanti soprattutto da parte di Raymond che, in occasione della liberalizzazione del codice sorgente di Netscape, voleva utilizzare un tipo di licenza meno restrittivo per le aziende di quanto fosse la GPL.

La scelta a favore dell'Open Source da parte di alcune importanti imprese del settore come la Netscape, l'IBM, la Sun Microsystems e l'HP, facilitarono inoltre l'accettazione del movimento Open Source presso l'industria del software, facendo uscire l'idea della "condivisione del codice" dalla cerchia ristretta nella quale era rimasta relegata fino ad allora. Venne cioè accettata l'idea che l'open source fosse una metodologia di produzione software efficace, nonostante nel suo famoso saggio *La cattedrale e il bazaar*, Eric S. Raymond avesse esplicitamente criticato i tradizionali metodi di ingegneria del software, metodi che fino a quel momento avevano dato buoni frutti. Va notato come i primi programmi 'liberi', come il GCC, seguivano ancora il modello a cattedrale; solo successivamente progetti come EGCS adottarono il modello a baaz.

Studi e ricerche

OSPA (Open Studies for Public Administration) è un gruppo di lavoro dell'Associazione Concreta-Mente orientato a studiare il tema dell'innovazione organizzativa e tecnologica nella Pubblica Amministrazione. Integra competenze verticali di origine accademica e professionale con l'obiettivo di formulare proposte concrete e presentarle ai decisori istituzionali nel contesto di eventi pubblici. Il gruppo di lavoro OSPA organizza annualmente dal 2008 un convegno nel quale sono presentati e discussi con interlocutori di diverse estrazioni i risultati delle ricerche sull'innovazione nelle Pubbliche Amministrazioni. Ad oggi ha coinvolto nelle sue attività: 6 Università e Centri di Ricerca Nazionali, più di 50 aziende del settore privato, oltre 250 Amministrazioni Pubbliche sia locali che centrali.

OSPA 2008 è stato il primo momento in Italia di incontro e confronto tra PA, imprese e università sul tema dell'open source nelle Pubbliche Amministrazioni. L'iniziativa dei convegni OSPA è poi proseguita negli anni successivi.

A partire dagli spunti raccolti nel corso della prima edizione, il convegno OSPA 2009 è stato dedicato a verificare l'esistenza di interrelazioni tra cambiamento organizzativo e adozione di soluzioni open in 16 diverse amministrazioni, e ad approfondirne la natura. I casi di studio esaminati, i risultati della ricerca e le discussioni attivate sono stati raccolti nel volume Open Source nella Pubblica Amministrazione - OSPA '09, che è anche possibile scaricare gratuitamente.

L'edizione OSPA 2010[7] è stata orientata all'approfondimento verticale su due temi di grande rilevanza per la promozione e valutazione dell'innovazione nella PA: il Riuso di soluzioni software tra amministrazioni diverse, e il Total Cost of Ownership, come strumento per supportare le decisioni di adozione. Anche in questo caso, i risultati delle ricerche presentati al convegno e le riflessioni degli esperti intervenuti sono stati raccolti in un volume, OSPA 10 - Strumenti per l'Innovazione nella PA , che si può anche scaricare gratuitamente.

Software open source maggiormente diffusi

I software applicativi open source attualmente più diffusi sono Firefox, VLC, Gimp, 7-Zip, OpenOffice, LibreOffice oltre ad un gran numero di progetti rivolti non all'utente finale ma ad altri programmatori. Sono inoltre

degne di nota le famiglie di sistemi operativi BSD, GNU, Android e il kernel Linux i cui autori e fautori hanno contribuito in modo fondamentale alla nascita del movimento. La comunità open source è molto attiva, comprende decine di migliaia di progetti, numero tendenzialmente in crescita.

Per quanto riguarda il web, oltre l'80% dei siti web utilizza linguaggi di programmazione server-side o client-side open source, come PHP o JavaScript. I server web più diffusi sono open source.

Modelli di business

Lo sviluppo open source ha tra le sue caratteristiche quello di essere quasi sempre gratuito, tanto da creare confusione tra alcuni che credono che "open source" e "gratuito" siano sinonimi (nonostante il termine inglese 'free' non abbia una connotazione precisa relativamente al costo, ma solo alla libertà di utilizzo). Ci si potrebbe chiedere perché delle persone si dedichino allo sviluppo di progetti talvolta semplici, talvolta impegnativi e complessi, senza una remunerazione. In realtà, ci possono essere delle forme di guadagno (anche se non sempre) e si può ricorrere ad una o più strategie per questo scopo. Nella seguente lista, con "sviluppatore" si può intendere sia uno o più soggetti privati, sia un'azienda che crea ed eventualmente si occupa di fare evolvere/mantenere il programma o prodotto software:

- **donazioni**: lo sviluppatore dà la possibilità di fare delle donazioni non obbligatorie a chi usa il suo programma, come ringraziamento o come incoraggiamento per un ulteriore sviluppo;
- **servizio di supporto a pagamento**: il programma è gratuito, ma si paga per avere il supporto dello sviluppatore; se il supporto prevede donazioni, si può ritenere simile al punto precedente;
- **sponsorizzazione**: il programma o il sito che lo ospita può contenere il nome o altro tipo di pubblicità ad un'azienda che supporta economicamente lo sviluppatore; può anche accadere che un'azienda si occupi dello sviluppo di un programma gratuito e conti sulla pubblicità che riscuoterà da esso per farsi conoscere;

- guadagni grazie alla **didattica**: se il prodotto creato è particolarmente complesso, ad esempio nel caso di un nuovo linguaggio di programmazione o di una particolare libreria (o framework ecc.), lo sviluppatore può guadagnare grazie all'organizzazione di corsi di apprendimento del prodotto stesso, la vendita di manuali e libri a supporto ecc. Questo tipo di guadagno può risentire della concorrenza dei manuali che sono o saranno pubblicate gratuitamente in rete da parte di utenti, e può dar vita ad una strategia di mercato piuttosto complessa. Nei casi di librerie (o framework) che vogliono fare concorrenza a prodotti esistenti, si deve convincere gli utilizzatori che essi siano validi al confronto degli altri prodotti disponibili. Il produttore può anche rendere disponibile in rete delle introduzioni all'apprendimento del proprio prodotto, che però non coprono tutte le potenzialità dello stesso, cercando allo stesso tempo di creare una comunità di supporto ed un gergo che l'accomuni. Il gergo può far uso di termini nuovi che rimpiazzano quelli già in uso, giustificati con motivazioni diverse (ad esempio, le "funzioni" in Java sono chiamate "metodi", nonostante compiano azioni o restituiscano un risultato di un'elaborazione). Talvolta può dar vita ad una serie di acronimi che rendono quasi criptico il linguaggio (si veda il framework Spring). In tal modo si riesce a far diminuire il numero degli autodidatti che imparano in rete, spingendo chi vuole apprendere a comprare libri per l'apprendimento e le pratiche ottimali da seguire e/o seguire corsi e contemporaneamente si crea una comunità di sviluppatori fedele nel tempo, spesso unita anche da una "filosofia" di programmazione. Dunque, la caratteristica di questo modello può spingere i manutentori del progetto ad aumentare artificiosamente la complessità del software e diminuire la leggibilità del codice, contrastando almeno in parte i principi della semplicità di condivisione della conoscenza che animano invece altri tipi di progetti, sempre open-source.

Questi modelli di business tipici non sono al momento distinti da una tassonomia condivisa. È anche possibile, dunque, che un certo progetto Open Source venga iniziato sotto un certo modello di business, ma poi prosegua sotto un altro.

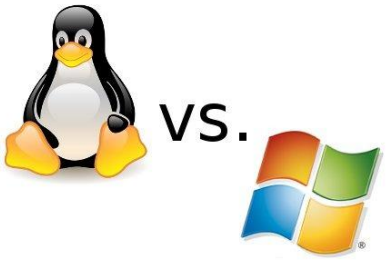
Fonti

1. Wikipedia

Microsoft vs Linux

Di Paone Paola e Cioffi Miriana

Linux e Microsoft sono entrambi due sistemi operativi abbastanza stimati dal mercato, ma per le loro piccole differenze nel tempo si è creato un “dibattito” tra i loro utenti. La competizione tra Microsoft Windows e Linux è iniziata nel 1991, nascita del primo sistema operativo di Linux, ed è proseguita negli anni 2000, in particolare per la diffusione di Windows XP, in contrapposizione a Ubuntu, la distribuzione Linux più diffusa, nata nel 2004. Prima di analizzare le ragioni di tale dibattito storico, andiamo ad esaminare singolarmente i due sistemi operativi.



Fonte: Hosting Linux Vs. Windows: un confronto ragionato

La differenza sostanziale tra i due sistemi operativi sta nel loro settaggio, nella loro base. Linux, detto anche GNU/Linux, è un sistema operativo molto sicuro (è difficilmente attaccabile da un virus), è un sistema economico, è distribuito sotto licenza GPL (General Public License, licenza pubblica generale di GNU) ed infine è Open Source: tutti gli utenti hanno la possibilità di per poter spostare, modificare, scrivere e creare script e programmi semplicemente, senza dover scaricare ambienti di sviluppo contribuendo al suo miglioramento e questo permette un continuo aggiornamento ed evoluzione del sistema. Microsoft, invece, è un sistema operativo distribuito sotto EULA (End User License Agreement, accordo di licenza dell'utente finale), ovvero è software proprietario, chiamato anche privato, non libero, o closed source. E' un software che ha di per sé un’architettura più chiusa e la cui licenza consente al beneficiario il suo utilizzo sotto particolari condizioni ed impedendone altre come la modifica, la condivisione, lo studio, la ridistribuzione. Ora andiamo ad analizzare nel dettaglio le principali differenze dei due sistemi operativi.

Fonte: Tux

Installazione

Nel 2000 le distribuzioni Linux erano considerate difficili da installare, ma nel corso degli anni i processi d'installazione sono stati semplificati. A partire dal

2003, anno in cui fu distribuita la prima versione di Knoppix, la creazione di numerose distro avviabili da LiveCD ha permesso agli utenti di provare Linux prima d'installarlo. Sia il processo d'installazione di Windows che quello di Linux (salvo eccezioni) fanno uso di wizard per aiutare gli utenti durante l'installazione. A differenza delle più comuni distribuzioni Linux, di solito i driver per Windows vengono installati separatamente.

	Microsoft	Linux
Facilità d' installazione	Il processo di installazione è stato notevolmente semplificato, ma può essere necessario l'utilizzo di un floppy disk.	La modalità d'installazione può variare di molto a seconda della distribuzione. Ubuntu, SUSE, Fedora e Mandriva, permettono l'installazione tramite chiavetta USB.
Tempo d' installazione	Il tempo stimato si aggira intorno all'ora in base alla versione di Windows desiderata.	Va da 6 minuti ad un'ora (circa), variabile secondo la distribuzione.
Driver	Sono in genere presenti driver generici, soprattutto nelle vecchie versioni di Windows. Nella maggior parte dei casi vanno installati separatamente, ma molto spesso il processo d'installazione dei driver è automatico,anche se può richiedere l'inserimento di CD o floppy e/o la connessione ad Internet	La maggior parte dei driver liberi è preinstallata nel sistema operativo. Quelli non liberi vanno scaricati, da repository o manualmente, a causa di restrizioni legali. L'installazione manuale è più complessa rispetto a quella su Windows. Alcuni driver disponibili per Windows possono essere utilizzati su Linux
Software preinstallati	Su Windows sono installati pochi programmi di uso comune: Internet Explorer come web browser, Windows Media Player come lettore multimediale, Blocco note come editor di testo, Microsoft WordPad come word processor e Paint come programma di grafica.	Le distribuzioni disponibili su CD o DVD preinstallano più di una alternativa per i programmi di uso comune. Ad esempio Konqueror e Web come browser, Totem e VLC come media player, diversi editor di testo e GIMP per la grafica. Oltre ai software comuni è possibile trovare numerosi giochi installati.

Stabilità

Per ottenere un sistema operativo soggettivamente "stabile" è necessaria la cooperazione sinergica di varie componenti. Non tutte queste componenti sono sotto il controllo del produttore del sistema operativo: se da un canto un kernel Linux o Windows può essere stabile, dall'altro applicazioni e driver mal scritti possono danneggiare seriamente la stabilità. Quindi gran parte della stabilità deriva dalla gestione del kernel in caso di comportamenti errati da parte di applicazioni e driver. In informatica, il kernel costituisce il nucleo di un sistema operativo, ovvero il software avente il compito di fornire ai processi in esecuzione sull'elaboratore un accesso sicuro e controllato all'hardware. .

Linux risulta essere più stabile di Windows, probabilmente grazie al fatto che, non dovendo scaricare numerosi programmi e potendo lavorare direttamente da server, ha meno possibilità di incappare in errori e rallentamenti. Dalla sua, Windows, ha un enorme vastità di programmi, di versioni ecc., sebbene, molti di questi, siano a pagamento contrariamente all'open source da server di Linux. Le versioni di Windows basate su kernel NT (2000, XP, Server 2003, Vista, 7 e 8) sono tecnicamente molto più stabili dei sistemi operativi Windows 9x (95, 98 e Me) basati su MS-DOS. L'installazione di driver non completamente riadattati potrebbe portare al crash del sistema. Esistono comunque diverse modalità per terminare un'applicazione che causa il blocco del sistema. I riavvii sono spesso richiesti al termine di installazioni di driver o di programmi che modificano file di sistema o in uso. Se il kernel o qualsiasi altra applicazione a livello del kernel non è in grado di consentire la sicurezza del sistema, il sistema restituisce un "bug check" (noto come Blue Screen of Death, BSOD). In questi casi viene creato un memory dump e, a seconda delle impostazioni, il computer potrebbe essere in grado di ripartire automaticamente. In certi casi può essere necessario il riavvio. La stabilità dei sistemi UNIX, invece, è basata sulla struttura modulare a livelli del kernel (famosa per la sua stabilità). Gli emulatori di terminale e i window manager sono molto stabili. Anche su Linux è possibile terminare le applicazioni su più livelli. Linux va riavviato solo dopo l'aggiornamento del kernel e il software kexec inoltre permette di utilizzare un nuovo kernel senza necessità di riavviare la

macchina. L'equivalente della BSOD nei sistemi Unix è il kernel panic. In questi casi il kernel crea un memory dump, stampa a schermo un messaggio contenente l'errore e attende il riavvio manuale.

Sicurezza

Per determinare la sicurezza di un sistema operativo è necessario conoscere cosa incoraggia i programmatori a creare malware: Il software infettato deve essere ampiamente utilizzato, per colpire il maggior numero di utenti con il minimo sforzo per riadattare il programma e le eventuali vulnerabilità che vengono sfruttate dai malware devono avere tempi di correzione molto lenti, permettendo al malware di agire più a lungo. .

Per scoraggiare la creazione di malware e ridurne l'impatto, i sistemi operativi sono multiutenti e presentano aggiornamenti regolari per neutralizzare possibili minacce ed isolare le sezioni danneggiate. Separando gli utenti comuni dall'account di root è più facile limitare i danni dei malware. Prima di Windows Vista i sistemi operativi Microsoft prevedevano la possibilità per qualunque utente di essere amministratore di sistema. Al contrario sui sistemi Linux le utenze normali sono state da sempre separate dall'amministratore. In questo modo viene resa più difficile la creazione e lo sfruttamento del malware.

Per quanto riguarda la sicurezza, Linux è intrinsecamente più sicuro di Windows sia sul server, sul desktop o in un ambiente integrato. Questo alto livello di sicurezza è dovuto in gran parte al fatto che Linux, che si basa su Unix, è stato progettato fin dall'inizio per essere un sistema operativo multiutente. Solo l'amministratore o utente root, con privilegi amministrativi, e un piccolo numero di utenti e di applicazioni hanno il permesso di accedere al kernel o tra di loro.

Questo procedimento mantiene il tutto più protetto e sicuro. Naturalmente, anche Linux viene attaccato da virus e malware, sebbene meno frequentemente, e le vulnerabilità tendono ad essere trovate e risolte in modo più rapido per le sue legioni di sviluppatori e utenti. Gli sviluppatori affermano che il kernel Linux è più sicuro poiché può essere controllato da moltissime persone e, in accordo con la legge di Linus, è più probabile che i bug vengano risolti velocemente. I bug possono essere risolti nella stessa giornata in cui vengono scoperti, sebbene in genere passino alcune settimane prima che la patch sia disponibile per tutte le distribuzioni. Windows, invece, presenta le Botnet, reti di computer infetti e controllati da remoto, che riescono a contare più di un milione di macchine. Una volta che un malware infetta un sistema operativo Microsoft in genere è difficilmente rimovibile.

Fonte: 10 consigli pratici per mettere in sicurezza un server linux

Nelle guide all'uso di Windows viene consigliato spesso di utilizzare programmi anti-malware. La Microsoft afferma che il suo sistema operativo è sicuro grazie ad un particolare ciclo di vita del software denominato "Trustworthy Computing Security Development Lifecycle". A causa della licenza proprietaria di Windows solo i programmatori hanno accesso al codice sorgente per poter correggere i bug e l'aggiornamento periodico per i bug critici avviene solamente una volta al mese. Ciò consente agli sviluppatori di malware di pianificare più facilmente gli attacchi una volta avvenuto l'aggiornamento mensile. Tuttavia, Linux concede un ambito d'azione più vasto nelle operazioni che lo stesso utente può compiere (tramite terminale con privilegi di amministratore), ciò si traduce in dei danni potenziali maggiori che l'utente inesperto può causare.

Pro e Contro

PRO

Ci sono tantissimi sistemi operativi che basano il loro Kernel su Linux, questo perché Linux è un Open Source, ma precisiamo che Open Source non vuol dire gratuito! Linux "è a codice aperto", quindi chiunque ne è capace può dare il proprio contributo migliorando il sistema operativo. Ed è proprio per questo motivo che ci sono cosi tante distribuzioni basate sul Kernel Linux, molte delle quali gratuite. La vasta scelta di sistemi Linux, rende possibile scegliere anche distro molto leggere e studiate appositamente per far funzionare al meglio anche i PC con hardware datato, donandogli di fatto nuova vita. Ma non è solo l'aspetto Open Source e le varie varianti gratuite ad essere il punto di forza di Linux, ma è un altro aspetto: la sicurezza. Le distribuzioni basate su Linux sono le più sicure in circolazione, questo perchè la community è sempre attiva e riesce a correggere bug e falle in pochissimo tempo, ed infatti esistono pochissimi virus in circolazione che sono in grado di danneggiare un sistema Linux.

CONTRO

Linux purtroppo manca di diversi programmi ed applicatavi, esistono in ogni caso delle alternative a questi software, tuttavia alcune aziende pretendono l'utilizzo di tali programmi per lavorare, e purtroppo su Linux non sono disponibili. In secondo luogo Linux non è una piattaforma studiata per il Gaming, e nonostante siano state sviluppate distro apposite per questo settore, come ad esempio SteamOS, al momento il progetto presenta circa 1900 giochi, mentre la concorrenza mette sul campo un comparto titoli ben più ampio. Infine gli accordi che le grandi aziende come Microsoft hanno preso con sviluppatori di drive video come Nvidia e AMD rendono il rilascio dei suddetti drive più "lenti" per Linux rispetto a Windows.

- *E' Open Source*
- *Vasta scelta di OS Free*
- *Supporto anche di hardware datato*
- *Sicurezza*

- *Manca la compatabilità di alcuni software*
- *Drive video arrivano in ritardo rispetto alla concorrenza*
- *Lo sviluppo nell'ambito Gaming è ancora acerbo*

PRO

Windows è il sistema proprietario di Microsoft, ed attualmente è il sistema operativo più diffuso su PC. La sua diffusione fa in modo che la disponibilità software per questo OS sia praticamente infinita, e si può trovare un programmi per qualsiasi operazione l'utente necessiti di fare. Con l'arrivo di Windows 10, l'ultima versione del sistema Microsoft, si ha la possibilità di avere un sistema modulare, dove gli aggiornamenti sono più costanti e più repentini, permettendo allo staff di Microsoft di far evolvere il sistema in qualcosa di totalmente diverso nel corso del tempo. Il supporto Driver è sempre in costante aggiornamento, questo perchè le maggiori software house in ambito viduoludico sviluppa e crea i propri titoli per questo sistema operativo, il che rende Windows un sistema perfetto per chi ama il Gaming.

CONTRO

Il sistema è a pagamento, ed il suo prezzo è davvero elevato, inoltre non essendo Open Source non dispone di un un codice aperto, e questo si traduce in scarsa possibilità di personalizzazioni da parte dell'utente o della community di programmatori indipendenti. Infine anche se negli ultimi anni la sicurezza su Windows è migliorata, ancora risulta il sistema più vulnerabile con un quantitativo di virus, trojan e malware enorme.

- *Pieno supporto dei software di notevole importanza*
- *Pieno supporto dei Driver*
- *Pieno supporto nell'ambito Gaming*
- *E' il sistema più diffuso*

- *Non è Open Source*
- *E' a pagamento*
- *E' il sistema più vulnerabile*

Curiosita'

- **Sfondo desktop Windows XP**

Bliss.
Fonte: L' incredibile storia dietro la foto dello sfondo classico di windows xp

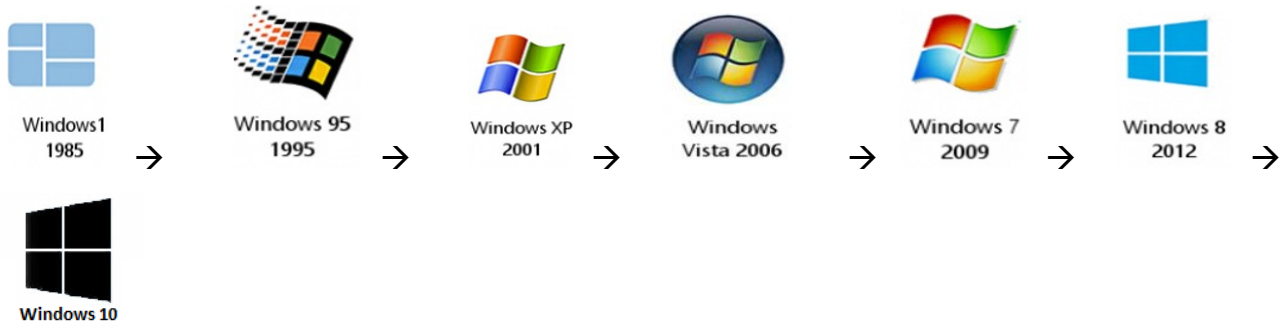
Di tutti i panorami del nostro pianeta, forse uno dei più conosciuti in assoluto, è quello usato dalla Microsoft come sfondo default del suo sistema operativo XP. Ma questa foto, anche se nessuno ci ha pensato probabilmente, non è inventata, ma è di un posto reale molto poco frequentato, completamente all'opposto della popolarità della foto. Questa singola fotografia, che non è ne ritoccata ne modificata, chiamata Bliss, cioè beatitudine, fu scattata in origine dal fotografo Charles O'Rear, nel 1996. Si trova a Sonoma County, in California, poco a sud dell'omonima Sonoma Valley. e sia stata scattata negli USA, alla Microsoft hanno pensato di fare appello all'immaginario collettivo sul posto, cercando di dare il nome che le persone avrebbero voluto vedere maggiormente.

- **Logo**

Tuz, diavolo della Tasmania.
Fonte: Tux (mascotte)

Una differenza fondamentale dei due sistemi operativi è il logo. *Linux* presenta come mascotte un pinguino paffuto dall'aria contenta conosciuto con il nome Tux. L'origine del nome è un acronimo derivato da **T**orvalds **U**ni**X** e viene anche associato al tuxedo, lo smoking a cui il pinguino assomiglia visto di profilo. Venne realizzato da Larry Edwing nel 1996 in un concorso richiesto da Tove Torvalds, moglie del creatore di Linux, Linus Torvalds, conoscendo la simpatia del marito per queste creature. Appare vestito o ritratto spesso in modo diverso, a seconda del contesto; per esempio, quando rappresenta l'algoritmo di sicurezza PaX, indossa un elmo e impugna un'ascia e uno scudo, e i suoi occhi sono rossi. Nelle distribuzioni di Linux, Tux saluta l'utente durante il boot, mentre nei sistemi multi-processore, appaiono più pinguini contemporaneamente in proporzione al numero di core o di processori. Nella versione 2.6.29 del kernel Linux è stato sostituito da un diavolo della Tasmania di nome Tuz, ma è ritornato nella versione 2.6.30.

Dopo 25 anni e centinaia di milioni di copie dei suoi programmi vendute in tutto il mondo, *Microsoft* ha cambiato il suo storico logo, quello tutto nero realizzato con il font Helvetica. Il nuovo logo ha un elemento grafico colorato – un quadrato suddiviso in 4 quadrati più piccoli – e il nome della società di colore grigio. Esso è costituito da due elementi: un logotipo e un simbolo. Per il logotipo i grafici della società hanno scelto il font Segoe, utilizzato per diversi altri prodotti di Microsoft e per le campagne di marketing dell'azienda. È più lineare ed essenziale del precedente e appare meno appesantito. Per tradizione però, i colori dei quattro quadretti che lo compongono sono tutt'ora rossi, verdi, gialli e blu.



- **La fine di Microsoft Vista**

Giunto al definitivo capolinea, per molti rappresenta una delle versioni del sistema operativo Windows meno riuscita di sempre. E' ormai ufficiale che dall'11 Aprile, Microsoft Vista non potrà più beneficiare del supporto esteso. Ciò significa che, proprio come successe a Windows XP nel 2014, verranno rilasciati gli aggiornamenti di sicurezza di Vista rendendo rischioso l'utilizzo del sistema operativo. L'interruzione del supporto esteso potrebbe rappresentare la definitiva "pietra tombale" su di una release di Windows che non passerà alla storia per la sua intrinseca qualità. Microsoft suggerisce implicitamente che è tempo di passare ad una versione di Windows più recente e al passo con i tempi.

- **Android si basa su Linux?**

Quando si scende nello specifico riguardo qualsiasi argomento inerente alla tecnologia, è semplicissimo comprendere male alcuni concetti ed incappare in errori piuttosto grossolani. Analizzando Android è possibile notare che è un sistema operativo completamente open source, proprio come Linux e molte vole vengono erroneamente associati. Con il termine "Linux" spesso si tende a generalizzare tutti i sistemi operativi delle distribuzioni GNU/Linux, mentre in realtà Android è basato su Linux inteso come kernel, non come sistema operativo in sé, in quanto il funzionamento di Android rispetto alle classiche distribuzioni GNU/Linux che siamo abituati a considerare ai giorni nostri è in buona parte differente. Il sistema operativo Android esegue la procedura d'avvio, caricando il kernel Linux, esattamente come una comune distribuzione Linux, ma non è in grado di eseguire le stesse applicazioni che troviamo sulle comuni distribuzioni desktop mentre le app Android non sono nativamente eseguibili sulle distribuzioni GNU/Linux "comuni".

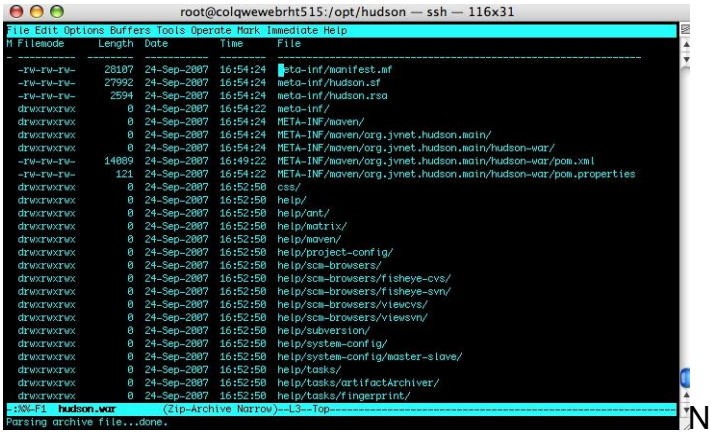
Fonti

1. Linux e Windows: due sistemi operativi a confronto
2. Comparazione tra Microsoft Wi,mndows e Linux
3. Software proprietario
4. Linux vs Windows: chi è il migliore?
5. L'incredibile storia dietro la foto dello sfondo classico di Windows XP
6. Tux (mascotte)
7. Android è basato su Linux: ma cosa significa?

I Virus

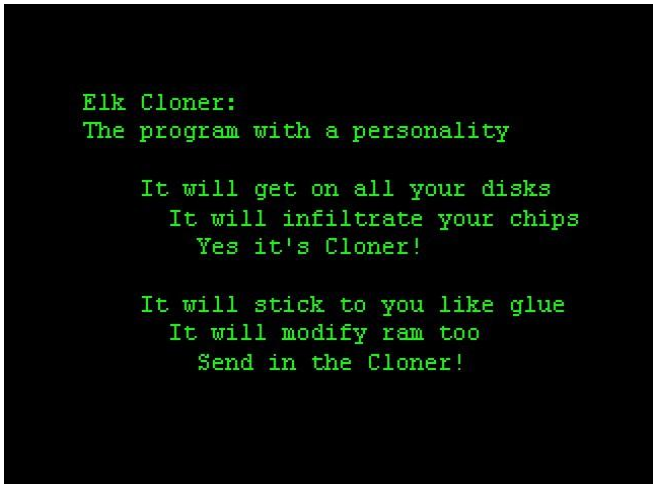
Storia

Di Caldarola Francesco e Giovanni Pisano



Nel 1949 John von Neumann dimostrò matematicamente la possibilità di costruire un programma per computer in grado di replicarsi autonomamente. Il concetto di programma auto-replicante trovò la sua evoluzione pratica nei primi anni '60 nel gioco ideato da un gruppo di programmatori dei Bell Laboratories della AT&T chiamato "Core Wars", nel quale più programmi si dovevano sconfiggere sovrascrivendosi a vicenda. Era l'inizio della storia dei virus informatici. Il termine virus è stato utilizzato per la prima volta da Len Adleman, un ricercatore dell'Università Lehigh in Pennsylvania, che ha paragonato il comportamento di un virus informatico a quello di un virus biologico, soprattutto per quanto concerne il propagarsi dell'infezione. In origine questi programmi non furono creati per provocare danni, come fanno la stragrande maggioranza dei virus di oggi, ma il principio si basava su considerazioni molto più interessanti: se era possibile creare un programma in grado di autoreplicarsi, era anche possibile fare in modo che questo si sviluppasse. Se nel processo di replicazione si verifica un errore, il codice, ovvero le informazioni codificate in bit che costituiscono il programma, risulta mutante. Così come il codice mutante

genetico determina la misura in cui un virus biologico è in grado di sopravvivere e diffondersi, il codice mutante digitale potrebbe determinare la misura in cui un virus informatico è in grado di sopravvivere nel suo ambiente. Come conseguenza logica di tale teoria, trascorso un periodo di tempo sufficiente, un virus informatico potrebbe svilupparsi in qualcosa di simile a un'intelligenza artificiale. Si ritiene che il primo virus conosciuto sia stato Creeper, che comparve nel 1970 nella rete ARPAnet facendo apparire un messaggio sui monitor dei terminali collegati; Reaper fu il programma che invece fu creato per contrastarlo. Il 27 ottobre 1980 un altro virus, denominato Arpanet Data Virus, bloccò tutte le attività della stessa rete. Questo virus fece la sua prima comparsa in una località nei pressi di Los Angeles e infettò tutti i nodi della rete fino al suo completo collasso che durò 72 ore prima che i tecnici riuscissero a ripristinare il sistema. Il programma chiamato Elk Cloner è invece accreditato come il primo virus per computer apparso al mondo. Fu creato nel 1982 da Rich Skrenta sul DOS 3.3 della Apple e l'infezione era propagata con lo scambio di floppy disk: il virus si copiava nel settore di boot del disco e veniva caricato in memoria insieme al sistema operativo all'avvio del computer. Nel corso degli anni ottanta e nei primi anni novanta fu lo scambio dei floppy la modalità prevalente del contagio da virus informatici. Dalla metà degli anni novanta, invece, con la diffusione di internet, i virus ed i cosiddetti malware in generale, iniziarono a diffondersi assai più velocemente, usando la rete e lo scambio di e-mail come fonte per nuove infezioni.



Il primo virus informatico che si guadagnò notorietà a livello mondiale venne creato nel 1986 da due fratelli pakistani proprietari di un negozio di computer per punire, secondo la loro versione, chi copiava illegalmente il loro software. Il virus si chiamava Brain, si diffuse in tutto il mondo, e fu il primo esempio di virus che infettava il settore di avvio del DOS. Nel 1988 Robert Morris, uno studente del MIT (Massachusset Institute of Technology), infettò Internet con un worm (virus che si autoreplica in memoria fino al collasso del sistema). Morris si accorse subito che il suo verme stava facendo molti danni poiché si espandeva in maniera più vertiginosa del previsto, mettendo fuori servizio molti calcolatori in tutti gli Stati Uniti, si spaventò e chiese aiuto ad un suo amico dell'università di Harvard. I due non trovarono meglio da fare che mandare un messaggio anonimo a tutti i responsabili dei sistemi in rete spiegando cosa fare per bloccare il verme, ma ormai la rete era in completo crash ed erano compromessi anche i sistemi di comunicazione, il messaggio di Morris non venne recapitato in tempo e calcolatori su calcolatori caddero sotto i colpi del virus. Nel 2000 il famoso I Love You che dà il via al periodo degli script virus, i più insidiosi tra i virus diffusi attraverso la posta elettronica perché sfruttano la possibilità, offerta da diversi programmi come Outlook e Outlook Express di eseguire istruzioni attive (dette script), contenute nei messaggi di posta elettronica scritti in HTML per svolgere azioni potenzialmente pericolose sul computer del destinatario. I virus realizzati con gli script sono i più pericolosi perché possono attivarsi da soli appena il messaggio viene aperto per la lettura. I Love You si diffuse attraverso la posta elettronica in milioni di computer di tutto il mondo, al punto che per l'arresto del suo creatore, un ragazzo delle Filippine, dovette intervenire una squadra speciale dell'FBI. Era un messaggio di posta elettronica contenente un piccolo programma che istruiva il computer a rimandare il messaggio appena arrivato a tutti gli indirizzi contenuti nella rubrica della

vittima, in questo modo generando una specie di catena di sant'Antonio automatica che saturava i server di posta.

Dal 2001 si è registrato un incremento di worm che, per diffondersi, approfittano di falle di programmi o sistemi operativi senza bisogno dell'intervento dell'utente. L'apice nel 2003 e nel 2004: SQL/Slammer, il più rapido worm della storia - in quindici minuti dopo il primo attacco, Slammer aveva già infettato metà dei server che tenevano in piedi internet mettendo fuori uso i bancomat della Bank of America, spegnendo il servizio di emergenza 911 a Seattle e provocando la cancellazione per continui inspiegabili errori nei servizi di biglietteria e check-in di alcune compagnie aeree; ed i due worm più famosi della storia: Blaster e Sasser.[7]Nel giugno 2009 è nata una nuova tipologia di virus che ha come bersaglio sistemi informatici industriali, il primo virus di questa nuova tipologia è stato Stuxnet che ha preso di mira i sistemi SCADA.

I virus informatici

Un virus informatico è simile ad un virus biologico: si tratta di un piccolo programma, che contiene una sequenza di istruzioni di cui alcune sono deputate alla replicazione dell'intero programma. Dopo la fase "riproduttiva", i virus informatici iniziano a svolgere attività di varia natura: distruttive e di ostruzionismo. I virus informatici, come quelli biologici, sono pericolosi e tendono a diffondersi tramite il trasferimento di files infetti da un computer ad un altro e, cosa ancor più grave, possono attaccare computers collegati fra loro in rete. Mentre i virus della prima generazione(1936/1956) attaccavano soltanto i file eseguibili che nel sistema operativo DOS sono riconoscibili in quanto hanno un estensione .COM o .EXE, i virus attuali sono in grado di inquinare molti altri tipi di files e sono anche in grado di cambiare le istruzioni del BIOS caricate in RAM, di diffondersi attraverso gli stessi supporti fisici contenuti nel PC e di danneggiare fisicamente, persino l'hardware.

I virus informatici della prima generazione erano in grado di diffondersi, autoreplicandosi per mezzo degli stessi programmi che essi inquinavano. Tipicamente essi svolgevano due funzioni:

- inizialmente copiavano se stessi in programmi non infettati;
- in seguito, dopo un prestabilito numero di esecuzioni, eseguivano le loro istruzioni specifiche che consistevano nella visualizzazione di messaggi, nella cancellazione o nella alterazione di files, fino alla cancellazione del contenuto dell'intero hard disk o della copiatura di quest'ultimo.

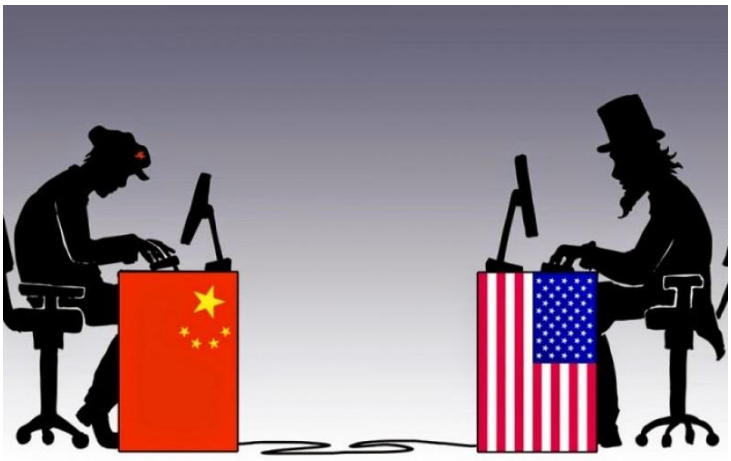
I programmi antivirus riuscirono a contrastare tale tipo di infezione definendo al loro interno delle librerie contenenti le stringhe (sequenze di caratteri) di riconoscimento per i diversi virus.
Tali stringhe si riferivano ad alcune sequenze di istruzioni caratteristiche dei vari virus che via via venivano scoperti. In questo modo gli antivirus potevano neutralizzare l'infezione, ma era necessario il loro continuo aggiornamento allo scopo di ampliare il contenuto delle librerie.

Attacchi storici

Un attacco informatico è una qualunque manovra, impiegata da individui od organizzazioni, che bersaglia sistemi informativi, infrastrutture, reti di calcolatori e/o dispositivi elettronici personali tramite atti malevoli, provenienti generalmente da una fonte anonima, finalizzati al furto, alterazione o distruzione di specifici obiettivi violando sistemi suscettibili. Tali azioni sono classificabili in cyber campaign, guerre cibernetiche o cyberterrorismo a seconda del contesto. Sono molto i virus che hanno segnato un periodo nel quale la necessità di proteggersi dagli attacchi informatici divenne una priorità, ma ovviamente all'aumentare delle misure di sicurezza aumentava in modo proporzionale la sfida per hacker e "gente del mestiere", che era ben contenta di mettere alla prova le proprie capacità di eludere i sistemi di sicurezza altrui. In questo scenario, presero vita nel corso degli anni alcuni degli attacchi informatici

più gravi che la storia ricordi. Tra gli attacchi storici che ricordiamo abbiamo la bomba logica fatta esplodere in Russia nel 1982.La CIA, una delle più famose agenzia di spionaggio degli Stati Uniti d'America, trovò il modo per intromettersi nella gestione del funzionamento di un gasdotto siberiano della Russia, senza il ricorso ad ordigni esplosivi od operazioni militari. La manomissione avvenne per mezzo di una porzione di codice informatico, che prende il nome di "bomba logica", e venne iniettato nel sistema informatico di controllo del gasdotto. La bomba logica viene vista un comune programma innocuo, e rimane nascosto nel computer della vittima per diverso tempo. Quando si verificano le condizioni per le quali è programmata, la bomba si attiva, dando vita all'esecuzione del codice malevolo. Il software mandò in tilt il sistema di gestione delle pompe, facendo schizzare in alto la pressione, e causando l'esplosione del gasdotto, creando un incendio che si racconta fosse visibile dallo spazio.

Successivamente nel 2003 gli Stati Uniti furono vittima di quello che è passato alla storia come uno dei più grandi, se non proprio il più grande, attacco informatico della storia. Gli attacchi furono estremamente coordinati ed eseguiti da diverse persone, mai identificate, ma riconducibili in un secondo momento al corpo militare cinese. Le informazioni sottratte dai computer erano finalizzati all'ottenimento di informazioni sensibili sui sistemi informatici USA, spionaggio, e portò all'accesso di molte reti informatiche quali Lockheed Martin, Sandia National Laboratories, Redstone Arsenal e della NASA.

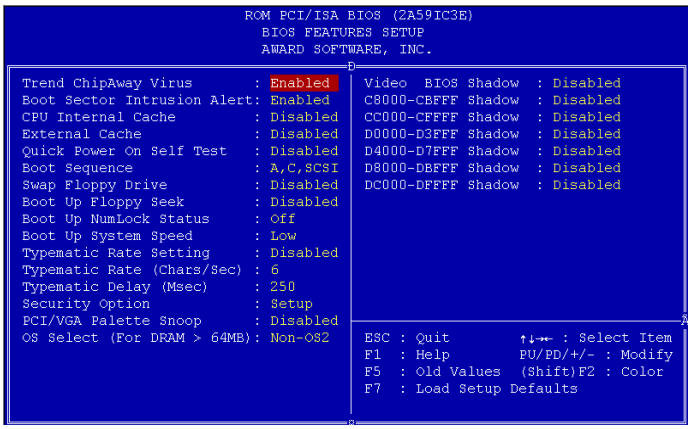


Tra tutti gli attacchi informatici subiti tuttavia quello che è noto a tutti è l'attacco informatico a Sony del 2010. Uno degli attacchi informatici più popolare, nonché perpetrato nel tempo, è quello che ancora fino a non molto tempo fa doveva fronteggiare la Sony, sul network Play Station. Nel 2011 furono ben 77 milioni gli account online del network ad essere colpiti, e fra i dati sensibili vi furono carte di credito e di debito degli ignari utenti. L'attacco fu lanciato da uno sconosciuto gruppo di hacker informatici, portando ad un danno stimato fra 1 e 2 miliardi di dollari. La cosa più incredibili è che l'attacco andò avanti per 24 giorni, nonostante gli sforzi della società per impedire la continuazione della frode. Solo dopo 24 giorni la falla era chiusa, e gli account nuovamente al sicuro, almeno per un po'. E' ormai accertato che la Corea del Nord si trovava alla base dell'attacco hacker tutto grazie all'intervento degli stessi Stati Uniti che tramite la Nsa (Nationale Security Agency) la quale si è infiltrata nel network cinese che collega la Corea del Nord al resto del mondo e, attraverso le connessioni con la Malesia utilizzate di preferenza dagli hacker nordcoreani, è riuscita a penetrare direttamente nella rete di Pyongyang, con l'aiuto della Corea del Sud e di altri alleati americani. Con un'operazione segreta, l'agenzia Usa, hanno affermato le fonti, è riuscita quindi ad inserire un malware in grado di tracciare il lavoro di molti dei computer e dei network usati dagli hacker nordcoreani, alcuni dei quali sono gestiti direttamente dal principale servizio di intelligence del Paese. Un'operazione che ha poi consentito di raccogliere le prove del coinvolgimento nordcoreano nell'attacco alla Sony.

Bisogna tuttavia prendere coscienza del fatto che dietro un attacco hacker c'è sempre un fine legato all'acquisizione di dati personali, indirizzi bancari o informazioni "top secret". E' proprio questo il caso di Gary M. il quale era molto ossessionato dall'idea di cosa potesse nascondere l'Area 51. Alieni, segreti di stato, armi del futuro, fatto sta che questo giovane hacker decise di scoprirlo da

solo, dando vita a quello che viene considerato il più grande attacco informatico indirizzato da un singolo individuo ad un sito militare. L'hacker riuscì a violare diversi server della NASA, entrando in 97 computer diversi fra Esercito, Marina, Dipartimento della Difesa, Aviazione e Pentagono. Gli Stati Uniti risalirono tutto sommato velocemente alla sua identità, e Gary McKinnon fu quindi accusato di crimini connessi all'hackin e processato il 10 maggio 2006 alla Corte dei Magistrati di Bow Street.Il 4 luglio 2006 il segretario John Reid ha deciso di concedere l'estradizione ovvero,una forma di cooperazione giudiziaria tra Stati e consiste nella consegna da parte di uno Stato di un individuo, che si sia rifugiato nel suo territorio, a un altro Stato, affinché venga sottoposto al giudizio penale. Ad un'udienza del 12 aprile 2006 l'accusa ha presentato una nota non firmata della ambasciata statunitense, pretendendo di garantire che McKinnon non sarebbe stato processato secondo la Legge marziale statunitense, tuttavia, la difesa obiettò che la nota non era firmata e quindi non vincolante. Il caso fu aggiornato al 10 maggio. Secondo la legge inglese, Extradition Act 2003, per una richiesta di estradizione americana non è richiesta la presenza di prove alle accuse. Il 30 luglio 2009 la Camera dei Lord ha dato il via libera all'estradizione negli Stati Uniti di Gary McKinnon. Tuttavia le condizioni di salute di McKinnon sembrano non essere buone. In seguito alle sue turbolente vicende giudiziarie, l'hacker ha subito nelle ultime settimane un crollo psicologico che lo avrebbe portato ad un distaccamento da sé stesso e dal mondo esterno, il che metterebbe in dubbio l'ipotesi della sua estradizione negli Stati Uniti. Il 16 ottobre 2012 Theresa May, Sottosegretario di Stato per gli Affari Interni del Regno Unito, ha respinto la richiesta di estradizione avanzata dalle autorità statunitensi circa 10 anni fa. Alla base della decisione ci sono appunto le precarie condizioni fisiche del quarantaseienne scozzese.

Tipologie di Virus



Classificazione Dei Virus:

Un sostanziale passo in avanti nello sviluppo dei virus fu rappresentato dai cosiddetti Virus TSR (Terminate and Stay Resident). Si trattava di virus che, una volta eseguiti insieme ad un programma infetto, rimanevano residenti nella memoria labile (memoria RAM) del computer e infettavano in maniera non obbligatoria altri programmi, solo qualora essi avessero particolari caratteristiche. Questo poteva poi essere richiamato o in modo automatico, ad esempio agganciandolo ad un interrupt di sistema(segnale asincrono che indica il "bisogno di attenzione" da parte di una periferica), oppure utilizzando un tasto speciale.

Il successivo passo nell'escalation dei virus fu la creazione dei Virus della Boot Area, cioè del primo settore dell'Hard Disk o dei diskette che, semplificando, è quella parte del disco che è deputata al mantenimento delle conoscenze riguardanti l'organizzazione logica del contenuto del disco stesso. Tutto il sistema di riconoscimento dei virus a mezzo di stringhe è venuto meno con la recente comparsa dei cosiddetti Virus Multipartiti o Mutanti, la cui peculiarità risiede nel fatto che possono cambiare fino a milioni di volte il loro codice eseguibile, cioè la sequenza di istruzioni contenuta nei virus stessi. In alcuni casi cambiano le istruzioni, ma il comportamento rimane lo stesso; in altri casi cambiano anche le azioni che il virus compie. A tale famiglia di virus possono essere assimilati anche i cosiddetti Virus Extra Traccia che collocano una parte del loro codice sulle tracce dei dischi che loro stessi creano.

Per contrastare tali tipi di virus sono stati creati degli antivirus che effettuano ricerche euristiche, le quali si basano sul seguente assunto: ogni virus, quando entra in funzione, usa delle specifiche sequenze di istruzioni per:

1. Nascondersi
2. Assumere il controllo del PC
3. Modificare i programmi eseguibili ecc...

Avendo a disposizione una libreria delle funzioni impiegate dai vari virus si può pensare di intercettare anche virus sconosciuti purchè per attivarsi utilizzino tali funzioni. Il problema che si pone in questo caso è che i virus possono utilizzate anche dei normali progammi.
Conseguentemente si rischia di creare degli antivirus "troppo sensibili" che riconoscono come virus anche dei programmi normali, o degli antivirus "troppo poco sensibili" che consentono ad alcuni virus di agire indisturbati. Dunque è come se tra i due, virus e antivirus ci sia una sorta di competizione che verrà vinta da chi per primo prende possesso del computer. Lo stesso tipo di problema si pone con i cosiddetti sistemi di rilevamento runtime (Trappole intelligenti) che agiscono con diverse modalità ma che, in definitiva, hanno anch'essi efficacia solo qualora prendano il controllo del PC prima dei virus.

Esistono alcuni virus estremamente sofisticati che riescono ad assumere il controllo del PC indipendentemente dal sistema operativo impiegato intervenendo a livello del BIOS come il virus CIH che blocca l'avvio di Windows e ne impedisce la formattazione o il virus Mebroni che infetta direttamente la scheda madre e per finire Chernobyl che infettò migliaia di computer sfruttando una falla degli allora S.O. Windows sovrascrivendo il BIOS delle schede madri. Da non molto tempo sono infine comparsi dei nuovi tipi di virus, i cosiddetti Virus delle Macro che si appiccicano a files documento generati per esempio con Microsoft Word per Windows, Microsoft Excel ecc...Bisogna prestare particolare attenzione a questi virus in quanto essi si possono facilmente trasmettere mediante lo scambio di files di tipo "documento" (es. posta elettronica), anche fra sistemi operativi diversi (MacOS e DOS/Windows, magari passando per Unix).

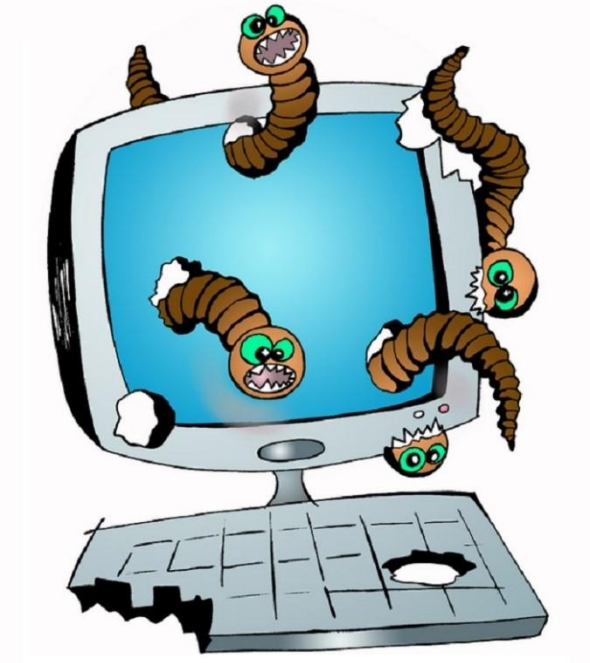
Questi virus si pongono in memoria quando viene caricato il documento infetto che li contiene e quando vengono compiute determinate operazioni (salvataggio automatico, ricerca e sostituzione di parti di testo ecc...) essi prendono il controllo del programma in questione, in barba ad eventuali antivirus che non possono/debbono interferire con le normali attività del programma. Così può capitare che al momento del salvataggio finale, sparisca dal disco fisso un'intera directory per effetto di un ordine di cancellazione (perfettamente lecito dal punto di vista funzionale) impartito dal virus stesso. Ovviamente il documento infetto trasmetterà l'infezione a qualunque altro documento dello stesso tipo aperto durante la medesima sessione di lavoro e questo, a sua volta, se aperto in un altro PC trasmetterà a sua volta l'infezione ad altri documenti presenti in un altro PC.

I virus delle macro possono manifestarsi con una molteplicità di problemi quali:

- Possibilità di salvare il documento solo in formato .txt
- Cancellazione di icone
- Occupazione eccessiva di memoria fino al blocco totale del sistema
- Cancellazione di intere directory di files dati ecc...
- Contro questi virus sono attivi solo gli antivirus più recenti.

In conclusione molto dipende dall'uso che un utente fa del proprio PC e in funzione di ciò vanno prese opportune misure.

Worm



Il termine "worm" per indicare un programma auto-replicante viene però usato per la prima volta solo nel 1975 nel romanzo di fantascienza Codice 4GH di John Brunner. La storia è ambientata in un lontano futuro in cui una gigantesca rete informatica che fa capo ad un unico supercomputer viene usata da un governo mondiale per controllare tutta l'umanità. Il personaggio principale riesce a far saltare la rete introducendo da un terminale un "worm" (nella versione italiana è tradotto con "tenia") che costringe il computer a rivelare al mondo tutte le manovre del governo globale registrate nella sua memoria. Uno dei primi worm (Creeper) di epoca moderna diffusi sulla rete fu il Morris worm, creato da Robert Morris, figlio di un alto dirigente della NSA il 2 novembre 1988, quando internet era ancora agli albori. Tale virus riuscì a colpire tra le 4000 e le 6000 macchine, si stima il 4-6% dei computer collegati a quel tempo in rete.

I worm (verme in inglese) sono quella tipologia di malware che è apparsa sulla scena mondiale con l'avvento di Internet, facendo sembrare quasi "scomparsi" i virus in senso stretto, vale a dire che per entrare all'interno di un computer hanno bisogno che l'utente svolga delle funzioni:

- eseguire un'applicazione infetta;
- avviare da un dischetto infetto;
- avviare delle macro infette,

non sono dunque malware autonomi.

Mentre per i virus in senso stretto il veicolo di diffusione è rappresentato da dischetti e programmi, i worm sfruttano per propagarsi la rete, sia locale (LAN aziendali o domestiche) che Internet: vediamo da dove possono provenire le minacce.

Posta elettronica. Essendo il principale mezzo per la trasmissione di informazioni, è anche il più utilizzato dai worm per propagarsi, generalmente in due modi: attraverso gli allegati o sfruttando vulnerabilità insite in alcuni client di posta elettronica. Gli allegati sono il metodo di propagazione più usato dai worm, anche se presenta un significativo punto debole: l'utente deve aprire l'allegato per infettare il proprio computer. A tale scopo il worm inserisce come oggetto del messaggio frasi "invitanti": ricordate ad esempio I Love You, alias Loveletter? Il messaggio di posta infetto portava l'oggetto ILOVEYOU e come allegato il file LOVE-LETTER-FOR-YOU.TXT.vbs. Poiché solitamente l'estensione dei file non viene visualizzata da parte del sistema operativo, molti utenti, credendo di avere a che fare con un file di testo, spinti dalla curiosità lo aprivano senza preoccupazioni: in realtà l'allegato era uno script che conteneva il codice dannoso. Non tutti i worm però necessitano di una "mano" per essere eseguiti: sfruttando le vulnerabilità (se non corrette tramite le opportune patch) di alcuni client di posta elettronica (due su tutti Outlook ed Outlook Express) che interpretano non correttamente alcuni tipi di comandi a cui vengono sottoposti, alcuni worm riescono ad autoeseguirsi anche nel momento in cui viene visualizzata solamente l'anteprima del messaggio, senza che ne venga effettuata l'apertura (come BugBear, Wallon e molti altri).

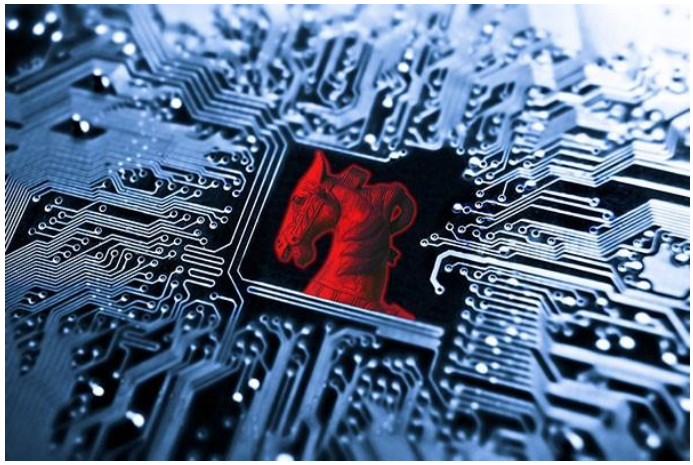
Web. I pericoli di contrarre un worm in questo caso possono provenire dai download incontrollati e dalle vulnerabilità insite nel sistema operativo (generalmente quelli Microsoft, da Windows 2000 in poi). E' risaputo ormai che aprire programmi e/o archivi scaricati dalla rete (specialmente se da siti poco raccomandabili) senza averli sottoposti preventivamente ad un adeguato controllo antivirus è un'operazione estremamente rischiosa e in alcuni casi fatale al proprio pc. Meno risaputa, a giudicare dall'incredibile numero di computer colpiti in tutto il mondo, sembra essere invece la gravità di due falle (se non adeguatamente corrette) scoperte nei sistemi operativi Microsoft, a partire da Windows 2000. Due worms che sfruttano queste falle sono Blaster e Sasser, questi due worms, per insediarsi in un computer, sfruttano due altrettante vulnerabilità del sistema operativo: il primo un bug nell'RPC (Remote Procedure Call, un protocollo usato da Windows), mentre il secondo una falla dell'Lsass (Local Security Autorithy

Subsystem Service, un servizio che si occupa della gestione delle password al login di un utente). Il payload ed il modo in cui si propagano i due worms sono simili: entrambi provvedono a mandare in crash ripetutamente ed a distanza di pochi minuti i relativi servizi vulnerabili (RPC e Lsass) causando l'arresto ed il riavvio forzato del sistema operativo. Se è attiva una connessione ad Internet, per propagarsi i due worms generano degli indirizzi IP casuali (un indirizzo IP è una stringa numerica che identifica un computer connesso alla rete), tentando quindi di sferrare l'attacco verso quegli IP: se a rispondere è una macchina vulnerabile, essa viene immediatamente infettata.

Trojans

Il Corriere della Sera del 22 maggio 1987 documentò a pagina 15 con un articolo di Mark McKain del New York Times la progressiva diffusione negli Stati Uniti di codice maligno di tipo trojan nelle BBS (Bullettin Board System). In era pre-Internet il contagio si diffondeva attraverso il caricamento e lo scaricamento di programmi infetti dalle BBS alle quali ci si collegava tramite modem. Il codice maligno celato nei programmi scaricati in genere provocava la cancellazione dei dati locali dai dischi dell'utente, talvolta con una formattazione del disco a basso livello. L'azione di diffusione dei trojan è attribuita a individui denominati "hackers". È una delle prime volte, se non la prima, che tali argomenti sono documentati sulla stampa generalista italiana.

Famoso nel 2011 il caso del "Trojan di stato" della Germania, utilizzato a fini intercettivi fin dal 2009 dietro una specifica ordinanza del tribunale che ne permetta l'uso nei confronti del soggetto finale.

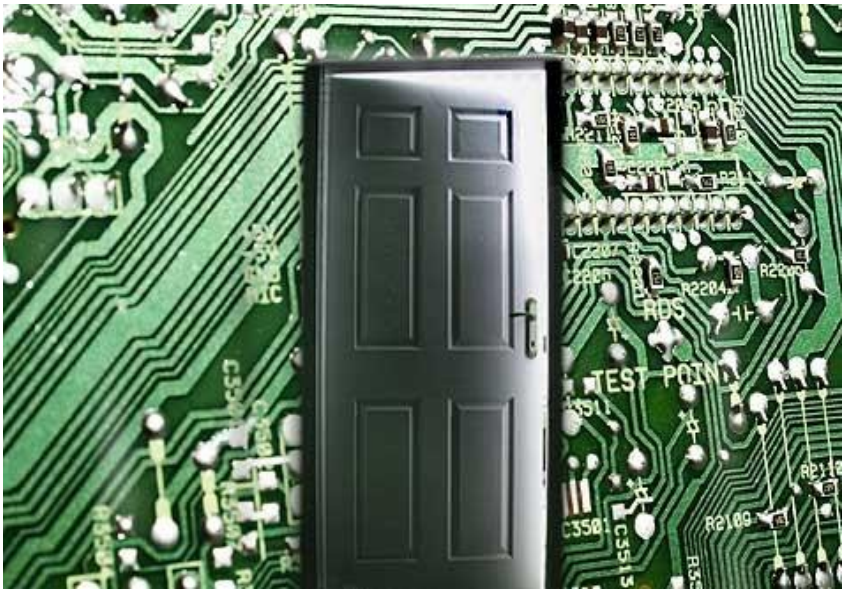


I trojans (detti anche cavalli di Troia) sono un altro tipo di malware che svolge delle funzioni diverse rispetto ai tipi descritti precedentemente. Sono subdoli e molto insidiosi: il loro nome deriva infatti dal trucco usato dagli Achei

per conquistare la città di Troia (il famoso cavallo di legno). Un trojan è solitamente un normalissimo programma, che fa credere all'utente di compiere funzioni utili. Una volta lanciato, il programma può effettivamente svolgere quelle funzioni oppure no; il punto centrale però è che esso svolge un'azione secondaria, che l'utente sicuramente non approverebbe: questa azione spesso consiste nell'installazione nel computer vittima di una backdoor, oppure nel reperire, manomettere o modificare i dati o le informazioni contenuti nell'hard disk, nonché di danneggiarli. A causa della diffusione dei programmi peer-to-peer (tipo WinMX, Kazaa, ecc.), il pericolo di venire infettati da un trojan è notevolmente aumentato, in quanto il download di file eseguibili da queste fonti spesso non sicure è un'operazione molto a rischio. A differenza degli altri malware, il Trojan non si prefigge come obiettivo principale il danneggiamento di parti del computer o l'eliminazione di file (anche se potrebbe causare disagi come l'apertura di finestre pop-up), ma il suo compito primario è permettere ai criminali informatici di accedere nel computer per rubare i dati sensibili, attaccare altri computer (soprattutto i dispositivi collegati al computer infetto) ed installare altri tipi di malware. Oggi col termine Trojan ci si riferisce ai trojan ad accesso remoto (detti anche RAT dall'inglese Remote Administration Tool), composti generalmente da 2 file: il file server, che viene installato nella macchina vittima, ed un file client, usato dall'attaccante per inviare istruzioni che il server esegue. Un trojan può contenere qualsiasi tipo di istruzione maligna. I programmi di nuova generazione hanno molteplici funzionalità, quali connessioni tramite bot IRC che permettono di formare una Botnet. Possiedono inoltre migliori funzioni e opzioni per nascondersi meglio nel sistema operativo, utilizzando tecniche di Rootkit. I Trojan sono sempre più diffusi e non tutti sono riconoscibili dagli attuali antivirus, per alcuni dei quali riescono anche a impedire l'aggiornamento. Per aumentare la loro efficacia possono nascondersi in modo tale che nemmeno l'antivirus sia in grado di eliminarli. Permettendo così di danneggiare il computer. Se questo accade, il Trojan può essere individuato e rimosso solo tramite l'eliminazione totale dei dati.

Backdoors-Corridoio segreto o porta sul retro.

Una backdoor è generalmente un programma dannoso insediato nel computer vittima e spesso nascosto o camuffato sfruttabile da chi sa che su quella macchina è installata la backdoor. E' composta da tre parti: il server, il client e lo scanner (che può anche essere integrato nel client). Il modulo server è quello che deve essere eseguito e quindi installato nel computer vittima, per aprire una determinata porta e renderlo quindi vulnerabile ad attacchi dall'esterno. Colui il quale ha intenzione di portare l'attacco usa in primo luogo lo scanner per effettuare un controllo su un determinato range (gruppo) di indirizzi IP, per ognuno dei quali viene effettuata una richiesta di accesso basata sulla porta in cui è in "ascolto" il server. Nel momento in cui un IP "risponde", significa che nella macchina associata a quell'indirizzo è in esecuzione il server. A questo punto, basta inserire nel client l'IP che ha risposto per accedere senza alcuna autorizzazione al computer vittima. Abbiamo dunque visto che per penetrare in un sistema tramite backdoor è necessario un indirizzo IP. Come molti di voi ben sanno, gli indirizzi IP nella stragrande maggioranza dei casi sono dinamici: essi variano cioè ad ogni nuova connessione alla rete. Una volta perso il collegamento client/server a causa della disconnessione da Internet della vittima sarebbe quindi necessario ricontrollare il range di IP per ritrovarla in un secondo momento. Molte tra le backdoor superano questo problema: possono essere infatti settate per notificare, ad ogni nuova connessione, il relativo indirizzo IP. Una volta stabilito il collegamento client/server, le backdoor consentono di prendere il totale controllo della macchina. Esistono infatti delle opzioni che permettono di svolgere azioni di disturbo che mandano nel panico la vittima (apertura e chiusura cassetto CD-ROM,



blocco del mouse o della tastiera, spegnimento dello schermo o rovesciamento delle immagini e molto altro), ma anche altre che consentono di recuperare informazioni personali, quali le password memorizzate (casella e-

mail, chat, ecc.) nonché di esplorare il contenuto dell'hard disk, scaricare i file in esso contenuti o offrendo anche la possibilità di formattarlo. Molte backdoor consentono inoltre di installare un ulteriore strumento maligno: un keylogger. Si tratta di una parte del server preposta a monitorare i tasti premuti tramite tastiera e di salvarli in un apposito file sul disco fisso. Questo file è consultabile attraverso il client o il suo contenuto può venire inviato dal server mediante posta elettronica nel momento in cui viene stabilita una connessione ad Internet. E' facile intuire quindi come sia semplice scovare anche in questo modo password, numeri di carte di credito, nonché altre informazioni strettamente personali della vittima. Per poter svolgere il suo compito, il server della backdoor viene generalmente eseguito ad ogni avvio del sistema operativo.

Sintomi di infezioni

Proviamo a vedere una casistica dei sintomi più comuni sofferti da un PC Windows che testimoniano la possibile o sicura presenza di virus o malware. Partiamo col dire che un computer può infettarsi anche se protetto da un antivirus che non è sempre infallibile nel bloccare il virus prima che esso possa provocare danni. E' importante notare che un virus informatico potrebbe agire in background senza provocare alcun problema inizialmente.

1) Il sintomo più visibile e fastidioso di un virus è un sensibile rallentamento del computer.
Il malware infatti potrebbe essere un processo che occupa molta potenza di elaborazione o CPU sul PC che quindi ha meno risorse da dedicare alle normali attività. Non sempre un processo che occupa troppa CPU può essere considerato un malware, ma resta sempre un problema. Analogamente anche l'avvio molto lento del computer può essere definito un sintomo che potrebbe indicare la presenza di un virus, altri casi potrebbero essere l'apertura delle finestre a fatica o l'Hard Disk in continua attività senza valide ragioni.

2) Sintomi vari che segnalano falsi problemi sul computer
Se il computer si spegne o si riavvia da solo, probabilmente c'è qualcosa di rotto ma non è da escludere l'effetto di un virus. Alcuni virus ingannano l'utente segnalando problemi inesistenti e bloccando, di fatto, ogni operazione. In genere questo tipo di malware prende il computer in ostaggio chiedendo all'utente di pagare per risolvere i problemi.

3) Problemi nelle impostazioni e funzionalità di Windows bloccate ed inaccessibili.

Ad esempio si può verificare che:

- scompaiono le icone dal desktop e dal menu Start;
- l'hard disk viene segnalato come pieno;
- viene richiesta una password di accesso mai impostata
- Non si può più accedere al task manager, Regedit o Msconfig;
- E' scomparso Internet Explorer, Il Pannello di Controllo ed altri menu di amministrazione;
- Non si è più amministratori del computer;
- La barra in basso scompare;
- Windows Update non funziona;
- Nessun programma antivirus funziona o può essere installato.
- Compaiono finestre con messaggi di errore o avvisi strani o insoliti;
- Si aprono pubblicità da sole;
- Compaiono strane icone di giochi o collegamenti a siti commerciali sul desktop;
- Il cursore del mouse si muove da solo;
- Sembrano scomparsi i file e le cartelle personali.

- L'antivirus è disattivato e non si avvia più
- Impossibilità di installare, aggiornare e avviare programmi di sicurezza

Per tutti questi sintomi, spesso macroscopici ed impossibili da ignorare o da confondere con problemi tecnici del computer, c'è sempre un modo per guarire. Se è vero che questa tipologia di virus, worm o trojan provoca problemi anche seri ed impedisce di usare il computer, è anche vero che sono immediatamente identificabili e, quindi, anche rimovibili.

3) Difficoltà nella navigazione su internet
Il computer funziona bene ma quando si apre internet non si riesce a navigare come si vorrebbe e si viene spesso indirizzati a siti web commerciali o sconvenienti, con l'apertura frequente di finestre pubblicitarie e pop-up. Il browser, soprattutto Internet Explorer, ha meno pulsanti del solito, non dà possibilità di accedere alle opzioni generali e di cambiare le impostazioni avanzate.In questo caso la diagnosi è abbastanza semplice ma la risoluzione più complicata del previsto se non si è preparati perchè diventa impossibile scaricare il tool di riparazione.

4) Anomalia nel funzionamento dei programmi che si chiudono all'improvviso o che non funzionano come dovrebbero. Questa tipologia di sintomi può essere molto difficile da individuare e da associare con la presenza di un virus. La cosa importante è sempre tenere la versione più aggiornata dei programmi e dei plugin, soprattutto se si usano programmi molto popolari come Office, Adobe, Java ecc. Ovviamente anche Windows va aggiornato sempre all'ultima versione.

5) Problemi nelle Mail

Se l'indirizzo Email è finito nelle mani sbagliate, si potrebbe notare un aumento deciso di messaggi di spam che possono comunque essere ignorati e cestinati automaticamente. Il vero problema, se si utilizza un programma come Microsoft Outlook è la comparsa di email deliranti che avvertono di messaggi di email con strani allegati e, soprattutto, l'invio automatico a tutta la rubrica del virus. Anche in questo caso i programmi di scansione anti-malware funzionano soltanto che prima possibile e come ci si accorge del problema sarebbe il caso di avvertire i contatti della rubrica di possibili messaggi infetti provenienti dal nostro indirizzo.

Virus su MS Windows e su Linux

La domanda che tutti gli utenti di Windows si pongono è perché Microsoft Windows è uno dei pochi OS (Operative System)che presenta costanti attacchi malware a causa della sua mancanza di sicurezza? C'è stato certamente un miglioramento con l'arrivo di Windows 8 infatti la differenza di performance ed utilità da Windows 7 a Windows 8 si è notata. Un ulteriore step è poi stato fatto con il miglioramento dell'interfaccia che ha apportato Windows 8.1, un sistema che organizza in modo migliore tutta la grafica dell'ambiente desktop ed

impostazioni. Tuttavia il problema "virus" non è ancora stato risolto, nonostante tutto Windows resta comunque l'OS più utilizzato al mondo. Creare virus per Windows è diventato semplicissimo e nel Web esistono tantissime guide su come si possa infettare un PC che monta il sistema operativo di Microsoft. Basta digitare i termini di ricerca su un qualsiasi motore di ricerca per poter notare quante strade ci sono per violare la privacy di utenti Windows. Si crede che Microsoft agisce in questo modo per motivi, economici. Gli antivirus sono nati proprio per proteggere Windows se pur disponibili per Ubuntu, Mac, Android, Linux sui quali non viene mai adoperato alcun anti-malware per il semplice fatto che non ne hanno bisogno. Ciò non significa che i sistemi operativi citati in precedenza siano completamente sicuri ma è necessaria una mano molto più esperta rispetto a quella necessaria per Windows per compromettere il sistema. Probabilmente Microsoft non cambia politica perché le vendite del sistema operativo non diminuiscono. Alcune ipotesi, abbastanza controverse, affermano che Microsoft crei dei virus che vanno contro il proprio software e li diffonda direttamente. Gli utenti, spaventati dalla minaccia, per proteggersi corrono ai ripari ed acquistano specifici software di protezione che, oltre ad essere abbastanza costosi (nella maggior parte dei casi) vanno anche ad appesantire il carico sull'hardware del nostro computer. Gli interessi economici sembrano quindi essere il punto focale di queste" teorie complottistiche" che vedono protagonista Microsoft a discapito della sicurezza degli utenti. Il colosso del software sembra quindi fare il doppio gioco: da un lato offre protezione agli utenti mentre dall'altro fornisce il giusto materiale alle software house produttrici di antivirus, il tutto su lauto compenso economico.

Lo stesso non si può dire dell'OS Linux il cui sistema di privilegi è di alto livello. Perciò non è possibile beccare virus a meno che non sia l'utente stesso, l'utente finale ad eseguire un software malevole. Tuttavia ciò accade anche sui sistemi operativi Windows, allora dove sta la differenza?

Su Linux a differenza di Windows sono presenti dei siti esterni dove vengono caricati tutti i vari software delle varie distribuzioni Linux. Quando scaricate un software andate direttamente sullo store del gestore della versione di Linux che voi avete scelto, così che il software che state per scaricare è prettamente

sviluppato per la vostra piattaforma. A questo punto possiamo essere sicuri di cosa stiamo installando senza installare software da internet, dove molto spesso insieme al software che state cercando scaricate anche software malevoli. Oltre a questo ci sono anche altri siti che sono gestiti da gruppi esterni, una comunità che controlla i software che vengono creati, quindi i controlli che vengono effettuati sui software prima di essere messi a disposizione sono molti. Devono passare il controllo da parte della comunità della versione di Linux che avete e devono passare anche i controlli di varie comunità libere indipendenti che per passione e lavoro fanno questo. Quindi capite che per infettare un sistema basato sul Kernel Linux è davvero difficile. Con questo non si vuole dire che Linux sia immune a qualsiasi tipo di virus perché non è così, anch'esso infatti presenta dei software che sfuggono dai controlli ma per intaccare in un virus bisognerebbe scaricarli dal sito dello stesso produttore, quindi non potete sbagliare, e poi come detto prima a causa del controllo dei privilegi d'amministrazioni elevati questo software non si potrà mai avviare senza la vostra conferma. Ovvero oltre alla conferma che dovete dare per l'installazione, ad ogni avvio il software deve avere la vostra autorizzazione, perciò seppur fosse un software malevole non potrebbe avviarsi da solo e creare danni al sistema. E' quindi praticamente impossibile contrarre un virus dati gli innumerevoli controlli che esistono dalle distribuzioni delle varie versioni di Linux e dalle comunità indipendenti che effettuano controlli sui software resi disponibili sugli store. Nel gennaio 2001 è stata diffusa una notizia destinata a sfatare il classico mito di invulnerabilità dei sistemi Unix ai virus:

Ramen: finalmente un virus per Linux; un virus con conseguenze devastanti; ecco, era solo questione di tempo e diffusione: finora nessuno si era curato di Linux, ma, ora che comincia a diffondersi, si vede come sia facile scrivere per esso dei virus estremamente maligni e dannosi e come Linux non sia affatto meglio di Windows, neanche sotto questo aspetto.

Questo violentissimo "virus" non è altro che un programmino che esplora una rete per cercare macchine che usano Red Hat Linux 6.2 o 7.0 e attacca quelle che trova, utilizzando exploit(falle nell'OS che causa il lancio di un codice malevolo) noti che sfruttano problemi di sicurezza di vecchie versioni di alcuni pacchetti

server. Una volta che l'attacco ha avuto successo, il sistema può essere gestito a distanza. Per malware come "Ramen" per "Adore", che agisce in maniera del tutto analoga il termine rootkit (insieme di sofware malevoli che permettono il controllo e il mantenimento dei privilegi) non è corretto. Infatti, Ramen e Adore non fanno altro che appoggiarsi a problemi di sicurezza noti e muoversi sulla rete per automatizzare l'utilizzo di exploit noti sui sistemi attaccati. Per dirlo più chiaramente: quando è stato annunciato Ramen, già da tempo la Red Hat Inc. aveva pubblicamente rilasciato i pacchetti di correzione che risolvevano il problema di sicurezza in questione. Tali pacchetti di correzione erano e sono tuttora reperibili su una ben nota pagina web linkata perfino sul desktop di Red Hat Linux; su tale pagina si trovano tutti i pacchetti di aggiornamento e correzione che risolvono il problema. Si può dunque definire con certezza che i rootkit sono molto meno efficaci su Linux che non su Windows.

Come difendersi dai virus

- Per proteggersi dai malware è necessario un buon antivirus: meglio se a pagamento, bisogna anche controllare poi frequentemente le statistiche di eccellenza degli Antivirus per sapere come si sta comportando il vostro Antivirus nei confronti dei concorrenti ed eventualmente passare ad un prodotto migliore che deve essere costantemente aggiornato (almeno un paio di volte al mese). Ogni giorno infatti "nascono" decine e decine di nuovi virus. Essenziale è la sua presenza nel caso dei virus in senso stretto, poiché esso è in grado di ripulire i files infetti (anche se è sempre preferibile reinstallare gli originali).

- Unitamente all'antivirus è di estrema importanza dotarsi anche di un software firewall, preposto al controllo del traffico Internet in entrata ed in uscita dal proprio pc, nonché alla respinta di eventuali attacchi provenienti

dall'esterno. Il firewall infatti avvisa immediatamente l'utente circa le applicazioni che tentano di accedere alla rete, offrendo la possibilità di permettere o bloccare il tentativo; inoltre rende invisibili (stealth) le porte aperte dal proprio sistema durante la connessione, rendendo così invisibile anche il computer sulla rete. L'esempio più pratico è dato proprio dal worm Blaster, di cui abbiamo parlato in precedenza. Per infettare un computer esso infatti effettua l'attacco sulla porta 135, quella utilizzata dal protocollo RPC: se nel sistema è presente un firewall, anche se si è sprovvisti della relativa patch il worm non riuscirà a penetrare nel computer in quanto non riceverà alcuna risposta dalla porta (resa stealth dal firewall). Ad ogni modo, l'installazione di un firewall non deve sostituire la presenza delle patch risolutive delle vulnerabilità del sistema operativo.

- Oltre ad antivirus e firewall, ci sono altri modi per difendersi dalle minacce provenienti dalla rete. Quando si riceve un messaggio e-mail "strano" (con ad esempio l'oggetto in inglese ed allegati) proveniente da un mittente sconosciuto, è bene cancellarlo, poiché nella stragrande maggioranza dei casi si tratta di un worm. Va comunque prestata la massima attenzione al mittente del messaggio poiché i worms più recenti inseriscono come oggetto anche parole in italiano. In generale comunque è bene diffidare dalle e-mail che invitano espressamente ad aprire gli allegati. Nel caso si riceva un'e-mail da un mittente conosciuto, è buona norma accertarsi che questa persona l'abbia effettivamente spedita; inoltre è sempre bene controllare che nel testo del messaggio si parli espressamente di eventuali allegati e che ne venga fornita una sommaria descrizione. Per evitare di venire in qualche modo imbrogliati dalle doppie estensioni dei files (vedi Loveletter), il consiglio è quello di settare il sistema operativo in modo che visualizzi le estensioni per i tipi di file conosciuti. Ciò in genere si effettua aprendo una qualsiasi cartella, cliccando su Strumenti, Opzioni e disabilitando l'opzione che nasconde le estensioni.

- Ultima, ma non meno importante, è la raccomandazione di effettuare periodicamente il WindowsUpdate per mantenere sempre aggiornato il proprio sistema con le relative patch di sicurezza.

- purtroppo i malware sono in continuo aggiornamento e non sempre gli Antivirus sono in grado di riconoscerli ed eliminarli tempestivamente. In caso di malware di ultima generazione per cui l'unica soluzione per ripristinare il computer è la formattazione, è consigliabile (se non obbligatorio!) aver effettuato Backup periodici e dischi di ripristino, per riuscire a recuperare i dati, il sistema operativo e i programmi. Il Backup inoltre protegge anche da altre minacce non legate ai Virus, come guasti ai componenti del PC, possibili furti o eventi catastrofici naturali.

Capire quando essere diffidenti

Per evitare l'infezione del computer bisogna capire quando si deve essere diffidenti, vale a dire navigare in sicurezza sul Web evitando di selezionare tutti i link senza pensarci (lo stesso vale per i pop-up o i messaggi pubblicitari). Nel web esistono centinaia di banner pubblicitari e popup che sono stati progettati appositamente per richiamare la tua attenzione e convincerti a selezionarli con il mouse. A causa del modo in cui funzionano la maggior parte dei browser internet moderni, esistono pochissimi modi di essere infettati da qualcosa che si trova nel web, a meno che non sia proprio tu a selezionare l'oggetto contenente il virus. Questo significa che non dovresti selezionare i banner pubblicitari che pubblicizzano qualcosa che sia troppo bello per essere vero. Qualvolta clicchi un popup inoltre i file vanno a memorizzarsi nella cache quindi è sempre bene svuotarla. Inoltre è essenziale cambiare il browser nel caso in cui si utilizza Internet Explorer con altri come Google Chrome, Firefox o Opera che sono più aggiornati e sicuri. Oltre alla gestione dei siti che si visitano c'è anche bisogno di una gestione dei file che scarichiamo, ovviamente dobbiamo bisogno di essere selettivi quando scarichiamo un file controllando accuratamente lo sviluppatore evitando di scaricare software maligni. Diffidare dai software scaricabili online o da siti illegali in quanto non si è certi dell'integrità del file controllando in

aggiunta l'estensione del file che potrebbe contenere una seconda estensione nascosta a causa di un settaggio predefinito da Windows. Infine scansionare il software scaricato e leggere attentamente le licenze. Per concludere parliamo della gestione dell'e-Mail infatti gli allegati di una e-mail sono il primo veicolo utilizzato per la diffusione di virus e altri malware. Non dovresti mai aprire un allegato o un link contenuto in un e-mail proveniente da un mittente a te sconosciuto. Se non sei sicuro del mittente di un e-mail, cerca la conferma del fatto che il file allegato sia legittimo prima di procedere al download. Evitare di scaricare allegati inaspettati perché può capitare che molte volte gli utenti contraggono un virus che invia e-mail a loro insaputa. Questo significa che potresti ricevere un e-mail infetta da una fonte sicura. Se il testo dell'e-mail è strano oppure l'allegato appare erroneo evitare di aprirlo. Potrebbe anche capitare di ricevere e-Mail da associazioni con le quali sei a contatto, questa tecnica è conosciuta con il nome di phishing e prevede di creare e-mail che copino lo stile della società a cui fanno riferimento includendo link molto simili agli URL originali, ma che invece puntano a siti completamente fasulli (sono noti i casi relativi a Poste Italiane e a varie banche online). Lo scopo di questi siti consiste nel memorizzare le informazioni personali di accesso degli utenti, dato che quest'ultimi pensano di trovarsi sul sito reale.

Utilizzare Antivirus

Questo tipo di software è in grado di proteggere attivamente il computer da possibili virus, monitorando il funzionamento dei programmi attivi e pianificando la scansione completa del sistema. Esistono antivirus gratuiti che forniscono una protezione di base dai virus, come ad esempio AVG, Bitdefender e Avast. Mentre altri programmi a pagamento forniscono una protezione completa attraverso firewall e sistemi anti-phishing. I programmi a pagamento più diffusi

includono Norton, Kaspersky e le versioni a pagamento dei software antivirus gratuiti.

- Dovresti avere un solo antivirus installato sul computer, per evitare possibili conflitti.
- Assicurati di aggiornare il programma antivirus almeno una volta alla settimana.
- Esegui una scansione completa del computer almeno una volta alla settimana, o più frequentemente se sei un utente che fa un ampio utilizzo delle risorse di internet.
- Un programma antivirus non è un sistema infallibile e non è studiato per sostituire le buone regole di navigazione e il buon senso.

Un antivirus da solo, per quanto affidabile ed efficiente, non è una protezione totale contro la totalità dei virus informatici esistenti al mondo. Inoltre, un antivirus si basa su determinate regole e algoritmi scritti da esseri umani, e pertanto queste possono portare a errori o a decisioni sbagliate. Dal punto di vista tecnico ci sono svariati metodi che si possono utilizzare per prevenire e individuare malware. Un'ulteriore limitazione è dovuta al fatto che un virus potrebbe essere ancora non abbastanza diffuso, e quindi non essere ancora stato studiato da tutti i produttori di antivirus. In generale, questi metodi possono essere suddivisi in tecniche di analisi statica, che si basano esclusivamente sull'analisi di codice e dati dei file binari, e analisi dinamica , che si basano sull'esecuzione dinamica di un file per capire se è maligno o benigno. Tuttavia, queste ultime tecniche sono raramente utilizzate nei prodotti antivirus destinati agli utenti finali, ma sono generalmente utilizzate solamente all'interno dei laboratori delle aziende produttrici di software antivirus, al

fine di aiutare i ricercatori a studiare i campioni malware. Tuttavia, esistono alcuni prodotti antivirus che effettivamente implementano queste tecniche.

Tipologie di Antivirus

Storia

A cavallo della metà degli anni ’80, il fenomeno dei Virus informatici comincia a diventare una minaccia concreta per gli utenti di personal computer (non solo IBM Compatibili). Il primo virus per personal computer, realizzato a scopo didattico, viene realizzato e presentato l’11 novembre del 1983 dal prof. Fred Cohen (Università della California del Sud). Il virus è in grado di prendere il controllo dei personal computer, in meno di un’ora e di propagarsi tramite floppy disk. In realtà il lavoro di Cohen ha origine dallo studio di un progetto di ricerca di un’altra università americana che, sulla carta, era riuscita a definire un algoritmo autoreplicante in grado di cedere il controllo del sistema ad un malintenzionato: era nato il primo Trojan.

A tal proposito Cohen racconta:

“I was sitting in class with my students and I realized that if the Trojan will copy into other programs, then all that will be infected and that everyone that will run it will lead to the proliferation of malicious program”

[Ero seduto in classe con i miei studenti e mi resi conto che se il Trojan si fosse copiato (nascosto) in altri programmi, allora tutto sarebbe stato infettato e che chiunque eseguirà uno di essi sarà involontariamente responsabile della proliferazione del programma maligno]

Ma l'interesse di Cohen è rivolto soprattutto alle strategie di rilevamento dei codici maligni e i suoi studi lo portano nel 1987 a pubblicare la tesi secondo cui non esiste nessun algoritmo in grado di individuare tutti i possibili virus.

Il 1986 è decisamente l'anno della svolta: da un lato viene scoperto Brain, ufficialmente il primo virus "di massa" per il DOS , dall'altro G-Data presenta il primo concept di antivirus per l'Atari ST, commercializzato poi nel 1987 come G-Data Antivirus Kit. Sempre nel 1987 arriva VK 2000, ma a fare notizia è l'esperto di sicurezza informatica Bernt Fix (conosciuto anche come Bernd) che sviluppa un tool per contrastare le infezioni generate dal virus Vienna. Sempre nel 1987 il programmatore polacco Marek Sell crea MkS_Vir, con una UI text based completamente in polacco.

MkS_Vir

Nell'autunno del 1988 arriva il Dr. Solomon's Anti-Virus Toolkit scritto da Briton Alan Solomon, in contemporanea con AIDSTEST e AntiVir. In Europa, inoltre, nasce la mailing list VIRUS-L (basata sulla rete BITNET/EARN) pensata per alimentare discussioni sui nuovi virus e sulle relative tecniche di rilevamento e cancellazione.

Tra i membri suoi membri importanti troviamo John McAfee, già fondatore di McAfee Associates, e Eugene Kaspersky che fonderà Kaspersky Lab nel 1997.

Eugene Kaspersky

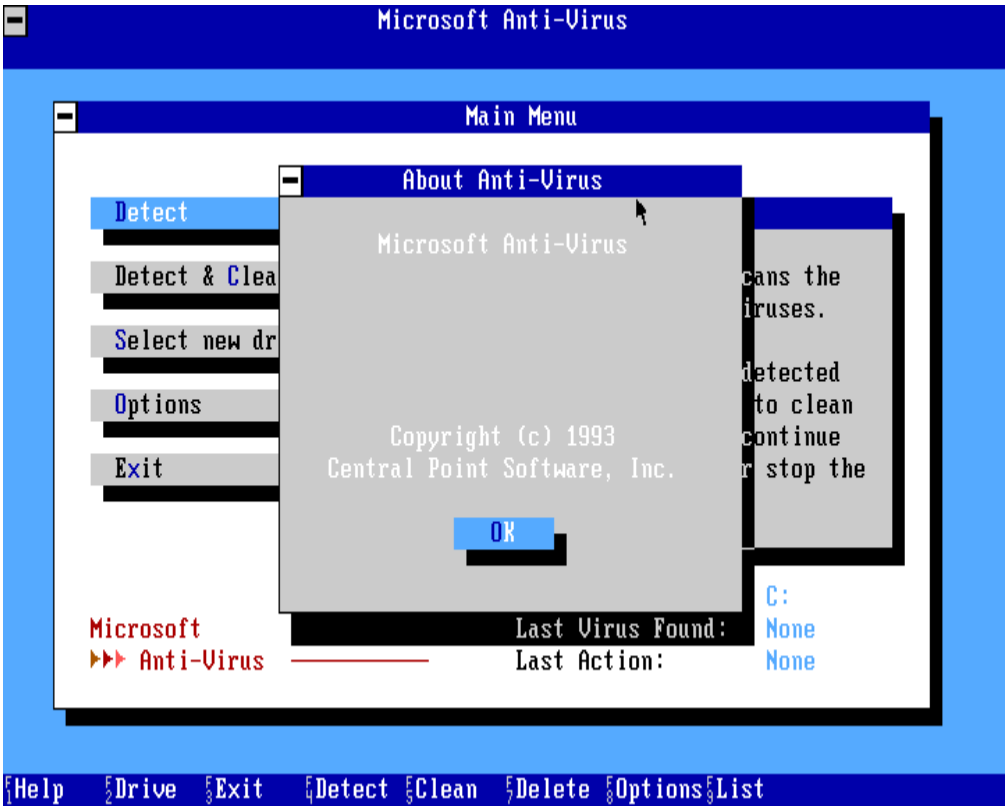
L'espansione del mercato dei PC e la necessità di proteggersi da nuovi virus che cominciano ad essere rilasciati con frequenza sempre maggiore, inaugura il nuovo decennio ('90) con circa 19 prodotti antivirus, tra cui troviamo: Central Point Anti-Virus, McAfee VirusScan, Trend Micro (PC Cillin e Virus Buster), Norton AntiVirus e altri. In particolare, Norton Antivirus (diventato di proprietà di Symantec Corp. nel 1990) si evolve in modo fondamentale nel 1992 quando Symantec acquisisce la Certus International Corp. e fa del suo fondatore, Peter Tippett, uno degli uomini chiave del proprio prodotto.

Tippett, dottore in medicina, è un uomo chiave in quanto autore di alcuni dei più importanti studi nel campo del rilevamento dei virus informatici, grazie all'intuizione della possibile similitudine tra virus biologici e virus informatici.

L'idea di cercare tali affinità nasce leggendo un articolo sul virus "Lehigh" e i suoi approfondimenti lo portano ad identificare come i virus attaccano i sistemi dal punto di vista epidemiologico (propagazione): Brain infetta il boot-sector, Leight i file .com e

Jerusalem sia i file.com che .exe. Il lavoro di Tippett si concretizza nello sviluppo di Vaccine, anch'esso divenuto di proprietà Symantec all'atto dell'acquisizione.

Chiaramente, fino all'avvento di Internet, lo strumento principe per la diffusione dei virus è il floppy disk e gli antivirus si concertano sull'analisi delle vie di infezione individuate da Tippett. Inoltre i più diffusi sistemi operativi della prima metà degli anni '90 (DOS in primis) integrarono un Antivirus minimale, spesso derivato proprio dai principali pacchetti dei succitati produttori.



Anche in Europa il mercato degli antivirus conosce dei protagonisti interessanti: dalla spagnola Panda Software di Mikel Urizarbarrena al già citato Kaspersky Lab, passando per l'AVAST Software di Praga e l'islandese FRISK Software International (F-Prot).

Nel 1998 Dr. Solomon's Group P.L.C viene acquisito da McAfee e contribuisce a rafforzare l'engine antivirus della società. Il 19 agosto del 2010 la società fondata da John McAfee verrà acquistata da Intel per ben 7,8miliardi di dollari al fine di rafforzare le politiche di security della società di Santa Clara, dopo aver investito, 5 anni prima, nella Ceca AVG Technologies facendo proprio il 65% del pacchetto azionario.

Con la diffusione delle e-mail, di Internet e dei linguaggi di sviluppo per l'estensione degli applicativi (VBA), lo scenario è completamente mutato e i nuovi antivirus sono diventati molto più complessi e solo lontanamente parenti con i primi sistemi di fine anni '80. Infatti, nonostante negli anni il nome, almeno quello ufficioso, negli anni non sia cambiato, questa tipologia di software oggi è in grado di contrastare una serie eterogenea di agenti malevoli: virus, trojan, worm, rootkits, ecc.

Antivirus di Base/Microsoft Security Essencials

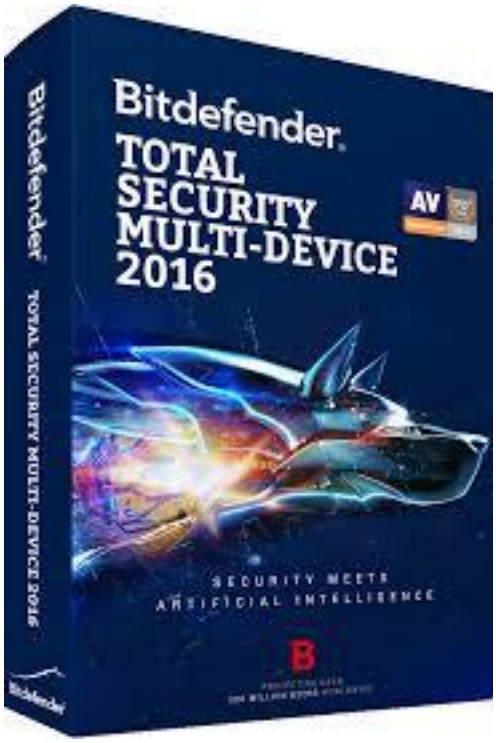
Oggi molte case produttrici di antivirus offrono software gratis ed a pagamento, ma quando scegliere il gratuito e quando pagare per un antivirus? Avendo un po' di pazienza e facendo un po' di ricerche in rete è possibile trovare alcuni antivirus gratis in grado di soddisfare le esigenze di un normale utente. Meglio sarebbe scaricarne più di uno e testarli singolarmente. Attenzione a non installare più di un antivirus sullo stesso computer. Andrebbero in conflitto e non funzionerebbero a dovere. Se invece avete un'attività con un ufficio e più computer collegati alla rete, allora è consigliabile acquistare un antivirus a pagamento. Microsoft Security Essentials (nome in codice Morro) è un antivirus freeware creato da Microsoft che difende il computer da virus, spyware, rootkit e trojan. Il programma è disponibile per Windows Xp, Vista e 7. Il software è uscito dalla fase beta il 29 settembre 2009. Microsoft Security Essentials sostituisce Windows Live OneCare e Windows Defender, il primo un servizio a pagamento mentre il secondo utile solo contro spyware; licenza gratuita per privati ed aziende con meno di 10 computer. Da Windows 8 esso è integrato con Windows ed ha preso il nome di Windows Defender che in precedenza rappresentava un semplice anti-spyware in

Windows Vista e 7. Comunque, a parte il nome, Security Essentials e Windows Defender sono molto simili.

Funzionamento: Prima dell'installazione Microsoft Security Essentials controlla se il sistema operativo è una copia valida o pirata. Se in questo caso Windows non è una copia originale, quindi pirata Microsoft Security Essentials cesserà di funzionare dopo un po' di tempo. Non è richiesto alcun dato personale. Il programma non funziona con altri sistemi di protezione attivi e li disattiverà. Gli aggiornamenti avvengono tramite Windows Update, oppure manualmente. Secondo le impostazioni predefinite i file archiviati, i download e le e-mail vengono scansionati (la posta però, a differenza di altri prodotti, non è monitorata in tempo reale-ovvero nell'istante in cui si riceve e/o invia un messaggio-ma solo quando si manipola un allegato o si apre un collegamento ad una pagina web, quindi è un controllo indiretto). I file ritenuti pericolosi vengono messi in quarantena e l'utente può scegliere se eliminarli definitivamente. Permette scansioni veloci (solo le aree critiche), complete e personalizzate (le aree selezionate dall'utente). Anche le memorie di massa connesse via USB possono essere comprese nelle scansioni.

Rispetto ai classici sistemi anti-malware, Microsoft Security Essentials è, appunto, essenziale non disponendo di tante funzioni e tecniche di scansione. D'altra parte l'anti-malware Microsoft presenza diversi vantaggi: è integrato nel sistema operativo (a differenze di prodotti di terze parti), è leggero (impegna poche risorse, se confrontato con i principali concorrenti) e molto semplice nell'utilizzo. A parte le definizioni antimalware che sono rinnovate pressoché giornalmente, anche il motore (client) è sottoposto a periodici aggiornamenti.

Internet Pro Security/Total Care



Partiamo dicendo che nessun antivirus è invincibile, nessuno rileva il 100% dei virus a volte può capitare anche che all'antivirus più blasonato sfuggano virus che invece vengono rilevati dall'ultimo degli antivirus free. È una suite completa fatta di programmi che contengono tutta una gamma di features molto utili fra cui pulizia del sistema e il sistema di backup, molto utili alle società, soprattutto quelle molto attive che hanno bisogno di una protezione alta perchè utilizzano molto il web. Sempre a tua disposizione il servizio di assistenza clienti di G DATA è disponibile 24 ore su 24, 7 giorni su 7 e 365 giorni l'anno, con i team di assistenza e il SecurityLab che lavorano fianco a fianco nella stessa sede che le soluzioni per la sicurezza informatica di G DATA forniscono i migliori tassi di rilevazione virus per combattere trojan, malware e persino virus sconosciuti. G DATA ha sviluppato il primo software antivirus al mondo ed è tuttora pioniera nell'innovazione della sicurezza informatica. Nel 2014 G DATA ha vinto il premio IPACSO dell'Istituto di ricerche UE come "società per la sicurezza cyber più innovativa". Un team dedicato di esperti di sicurezza informatica monitora le nuove minacce cyber a livello internazionale e sviluppa costantemente soluzioni per combatterle in modo efficace. Ovviamente i prezzi di queste soluzioni non sono mai bassi, anzi crescono quanto più crescono le esigenze delle aziende. Il prezzo di una suite completa non è mai inferiore al centinaio d'euro, spesso sfiora i 150 euro. Si può risparmiare qualcosina se la licenza viene acquistata con tutto il PC.

Fonti

1.wikipedia

L’evoluzione dei sistemi operativi

Linux

Di Nicola Ferrarelli

Introduzione

Linux è un sistema operativo, ovvero quell'insieme di programmi essenziali per far funzionare il computer. E' una alternativa a Windows e a MacOS, e può essere installato al loro posto (o insieme, sullo stesso computer).

Più in generale Linux è il primo rappresentante del software cosiddetto "open source, ovvero quel software che viene distribuito con una licenza che ne permette non solo l'utilizzo da parte di chiunque ed in qualsiasi circostanza ma anche la modifica, la copia e l'analisi. Linux è tipicamente usato come termine generico per indicare un sistema operativo con determinate qualità, nel concreto esistono le distribuzioni. Queste sono raccolte di software (software libero, si intende!) selezionato e predisposto per essere installato ed utilizzato nel modo più semplice possibile da parte degli utenti, fornendo una serie di strumenti essenziali per iniziare fin dall'inizio a usare il proprio PC nel pieno del potenziale.

Linux è una famiglia di sistemi operativi di tipo Unix-like, rilasciati sotto varie possibili distribuzioni, aventi la caratteristica comune di utilizzare come nucleo il kernel Linux.

Oggi molte società importanti nel campo ell'informatica come Google, IBM, Oracle Corporation, Hewlett-Packard, Red Hat, Canonical e Novell hanno infatti sviluppato e pubblicato, e continuano a farlo, sistemi Linux.

La nascita

Il kernel Linux vide la luce nell'agosto 1991 grazie al giovane studente finlandese Linus Torvalds che, appassionato di programmazione, era insoddisfatto del sistema operativo Minix (sistema operativo unix-like destinato alla didattica, scritto da Andrew Tanenbaum, professore ordinario di Sistemi di rete all'università di Amsterdam), poiché supportava male la nuova architettura i386 a 32 bit, all'epoca tanto economica e popolare. Così Torvalds decise di creare un kernel

unix con lo scopo di divertirsi e studiare il funzionamento del suo nuovo computer, che era appunto uno 80386.

Inizialmente, Linux (il sistema operativo basato sul kernel programmato da Torvalds) per girare utilizzava, oltre al kernel di Torvalds, l'userspace di Minix. Successivamente, Linus decise di rendere il sistema indipendente da Minix, anche perché non ne gradiva la licenza che lo rendeva liberamente utilizzabile solo a fini didattici, e decise, quindi, di sostituire quella parte del sistema operativo col software del progetto GNU. Per fare ciò, Torvalds cambiò la licenza e adottò la GPL, che tra l'altro considerava buona per il suo sistema operativo a prescindere dal software GNU stesso.

Linux, all'inizio, era un semplice emulatore di terminale scritto in C e assembly, e non aveva bisogno di appoggiarsi a un sistema operativo. L'emulatore di terminale avviava e gestiva due thread: uno per mandare segnali alla porta seriale, uno per riceverli; quando poi Linus ebbe bisogno di leggere e scrivere file su disco, questo emulatore fu esteso in modo che potesse gestire un file system. Lentamente, questo programma si trasformò in un intero kernel in grado di gestire un sistema operativo e Linus iniziò a documentarsi sulle specifiche POSIX, chiedendo assistenza sul newsgroup. La prima versione del kernel Linux, la 0.01, fu pubblicata su Internet il 17 settembre 1991 e la seconda nell'ottobre dello stesso anno.

Torvalds preferiva chiamare Freax il kernel a cui stava lavorando, ma Ari Lemmke, assistente alla Helsinki University of Technology che gli aveva offerto lo spazio FTP per il progetto (ftp.funet.fi), preferì assegnare alla subdirectory dedicata il nome alternativo di lavorazione Linux.

Sin dalla versione 0.01 si poteva compilare e far partire la shell GNU Bash. Fino alla versione 0.10 era richiesto un computer con Minix per configurare, compilare e installare Linux perché quest'ultimo usava il filesystem del sistema sul quale si appoggiava; dalla versione 0.11 poteva essere compilato da Linux stesso. Presto i sistemi Linux superarono Minix in termini di funzionalità: Torvalds ed altri sviluppatori della prima ora di Linux adattarono il loro kernel perché funzionasse con i componenti GNU ed i programmi in user-space per creare un sistema operativo completo, pienamente funzionante e libero.

Il rapporto con la *rete*

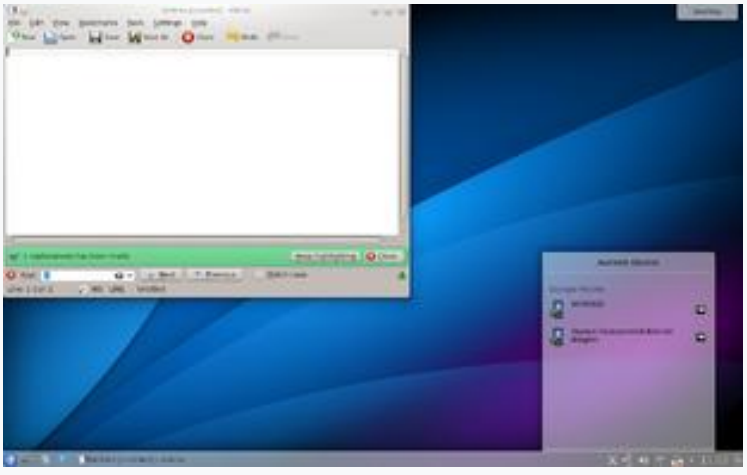
Nella primavera del 1992 l'hacker Orest Zborowski riuscì a rendere eseguibile il server X sulla versione 0.12 di Linux. Per far ciò, Orest dovette implementare tutta la struttura degli Unix Domain Socket indispensabili a X Window e quindi un primo livello socket sul quale venne poi costruita tutta l'infrastruttura di rete di Linux.

In realtà, il tutto era imbastito in maniera un po' caotica e non era ben integrato all'interno del kernel, ma Linus accettò comunque la patch perché con essa era possibile sia utilizzare X, sia utilizzare tale infrastruttura per dotare Linux di uno stack di rete.

Entusiasta della novità, Linus rilasciò, dopo la versione 0.13, la versione 0.95, senza pensare a tutti i problemi di sicurezza che la rete avrebbe comportato. Per rimediare alla leggerezza, nei due anni che trascorsero dalla 0.95 alla 1.0, Linus dovette utilizzare sia un ulteriore numero per indicare il livello di patch sia le lettere dell'alfabeto (sino alla versione 0.99.15Z, 0.99 15° livello di patch, revisione Z).

Il 12 marzo 1994 il 16° livello di patch del kernel 0.99 divenne Linux 1.0. Fu lo stesso Linus Torvalds a presentare la prima versione stabile all'Università di Helsinki.

Gli ambienti desktop e gli anni 2000



Desktop KDE SC 4.10

Nel 1996 fu scelto come logo ufficiale di Linux un pinguino disegnato da Larry Ewing, chiamato Tux come abbreviazione di Torvalds Unix.

Il compito di fornire un sistema integrato, che combini tutte le componenti di base con le interfacce grafiche (come per esempio GNOME o KDE, basate a loro volta sulla presenza dell'X Window System) e con il software applicativo, è svolto dalle distribuzioni GNU/Linux.

Per quanto riguarda il kernel vero e proprio, Torvalds già nel settembre 2009 dichiarò che esso è diventato "gonfio e grosso", non così veloce e scattante come quando l'aveva progettato. Riconosce, però, che questo "ingrassamento" non va visto solo come una cosa negativa, perché significa che Linux ha molta più compatibilità rispetto al passato. Nel luglio del 2011, per festeggiare il 20º anniversario della nascita di Linux, Torvalds decise di rilasciare il kernel Linux, passando ad un sistema di numerazione a 2 cifre, pubblicando la versione 3.0 del kernel. L'ultima release della serie 2.6 è stata la 2.6.39. Il 12 aprile 2015 è stata pubblicata la versione 4.0 che oltre a risoluzioni di bug aggiunge supporto a nuovo hardware (come intel quark) e le live patching, ovvero la possibilità di aggiornare il kernel e aggiornare punti critici del sistema senza riavviare, questa feature è dovuta anche alla collaborazione di RedHat e SUSE. L'ultima versione del kernel Linux è la 4.9 ed è stata resa disponibile al pubblico l'11 dicembre 2016. L'ultima versione attualmente in sviluppo del kernel Linux è la 4.10; il suo sviluppo è sostenuto dalla Linux Foundation, un'associazione senza fini di lucro nata nel 2007 dalla fusione di Free Standards Group e Open Source Development Labs.

Caratteristiche

Grazie alla portabilità del kernel Linux sono stati sviluppati sistemi operativi Linux per un'ampia gamma di dispositivi:

- personal computer
- cellulari
- tablet computer e console
- mainframe
- supercomputer

Esistono inoltre sistemi Linux installabili anche come server, router e sistemi embedded.

Attualmente Linux è molto usato, soprattutto come sistema operativo su server, in ambienti di produzione o in dispositivi embedded (PVR, telefoni ecc.), e ha una discreta diffusione in ambiente desktop (circa il 3% dei PC). Anche l'iniziale ampia diffusione sui netbook ha lasciato il passo a Windows, pur mantenendo una quota di penetrazione significativamente superiore a quella dei pc desktop/notebook.

Il kernel

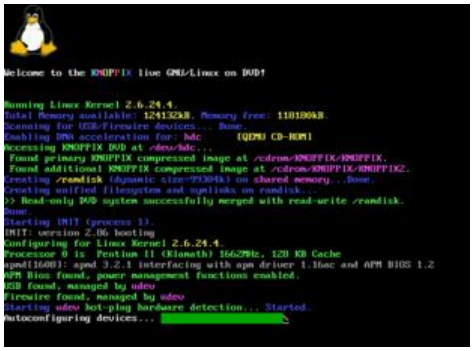
Il kernel Linux, uno dei più riusciti esempi di software open source, costituisce il nucleo dei sistemi operativi della famiglia di Linux. Fu inizialmente creato nel 1991 da alcuni studenti di informatica finlandesi tra cui Linus Torvalds, il capogruppo. Successivamente aumentarono in modo repentino i suoi sviluppatori e i suoi utilizzatori che aderivano al progetto del software libero e contribuivano allo sviluppo del nuovo sistema operativo.

Rilasciato, liberamente scaricabile e modificabile sotto la licenza libera GNU GPL (insieme ad alcuni firmware con varie licenze), è continuamente e liberamente sviluppato da collaboratori di tutto il mondo attraverso la relativa community, con lo sviluppo che ogni giorno avviene sfruttando la relativa mailing list, in modo del tutto analogo in cui sono sviluppati i protocolli di Internet.

Il ramo di sviluppo principale del kernel Linux prevede che esso contenga anche alcune parti non-libere, offuscate od oscurate come ad esempio alcuni driver. Il progetto Linux-libre si propone come variante completamente libera di Linux, da cui sono nate diverse distribuzioni completamente libere.

Il file system utilizzato dai sistemi Linux fa riferimento al Filesystem Hierarchy Standard, uno standard per file system per sistemi Unix e Unix-like di tipo ad albero gerarchizzato.

Installazione



Un sistema Linux può essere installato stand-alone su disco rigido oppure su partizione primaria e logica per un hard-disk precedentemente partizionato. Alternativamente

può essere installato su chiavetta USB o CD ed avviato opportunamente in fase di boot del computer. Tipicamente distribuzioni Live CD e Live USB una volta avviate dal loro supporto di memorizzazione forniscono supporto all'utente per l'installazione permanente su disco fisso nelle modalità di cui sopra. Opzionalmente, i sistemi Linux utilizzano anche di una partizione di swap per la memoria virtuale utile per situazioni dove la memoria RAM non è sufficiente o anche per l'ibernazione. Altra modalità tipica di installazione comune anche agli altri sistemi operativi è il ricorso alla virtualizzazione.

Utilizzo ed applicazioni pratiche

Il kernel Linux gira su svariate architetture: dai cellulari ai PC, ai supercomputer. Speciali distribuzioni esistono per piccole architetture per mainstream. Il fork del kernel ELKS può girare su un Intel 8086 o su un Intel 80286 con microprocessore a 16-bit, mentre il fork del kernel µClinux può girare su sistemi senza MMU. Il kernel gira anche su architetture che erano state progettate per utilizzare il proprio sistema operativo, come i computer Macintosh della Apple (con
architetture PowerPC e Intel), PDA, console, lettori MP3 e telefoni cellulari. Oltre che su postazioni host ovvero desktop computer, Linux è ampiamente utilizzato su postazioni server tramite apposite distribuzioni ottimizzate per la destinazione d'uso, potendo gestire facilmente un gran numero di accessi contemporanei sia lato intranet sia lato internet (server pubblici) e dove i vantaggi in termini di stabilità e affidabilità sono ancor più apprezzati.

Amministrazione

L'amministrazione, da parte di un utente o un sistemista, di un sistema Linux può avvenire per via grafica attraverso un pannello di controllo dell'interfaccia grafica del distribuzioni lato desktop oppure direttamente da riga di comando o terminale virtuale tramite ricorso ad un serie di comandi. Quest'ultima modalità è tipica delle distribuzioni server che per motivi di semplicità e di carico non presentano interfaccia grafica (per l'elenco e descrizione dei comandi vedi fondo voce).

Vantaggi e svantaggi

Numerose distribuzioni sono completamente gratuite, per l'utente privato e per le aziende. Esistono società (Red Hat, Canonical, SUSE e altre) che, dietro compenso, forniscono supporto tecnico e altri servizi per le proprie distribuzioni commerciali.

A questo si aggiunge la possibilità di modificare il sistema migliorando in proprio il codice sorgente, fornito con la licenza GPL, e di distribuirlo liberamente e legalmente, sotto forma di nuove versioni.

Il dibattito sui vantaggi e svantaggi di Linux è spesso ricompreso all'interno della comparazione tra Microsoft Windows e Linux, molto nota agli addetti ai lavori; perché alcune software house, come ad esempio Adobe, non vogliono fare il porting su varie distribuzioni.

Le distribuzioni

Non esiste un'unica versione di Linux, ma esistono diverse distribuzioni (chiamate anche *distro*), solitamente create da comunità di sviluppatori o società, che scelgono, preparano e compilano i pacchetti da includere. Tutte le distribuzioni sono sviluppate in maniera indipendente a partire dal kernel Linux comune (sia pur in versioni diverse e spesso personalizzate), e si differenziano tra loro per il cosiddetto "parco software", cioè i pacchetti preparati e selezionati dagli sviluppatori per la distribuzione stessa, per il sistema di gestione del software, i repository e per i servizi di assistenza e manutenzione offerti.

Esistono distribuzioni eseguibili direttamente da CD o pennetta USB: sono chiamate distribuzioni *live* o *desktop CD*. Una distribuzione live su CD o USB consente di provare la distribuzione ed eventualmente procedere all'installazione del sistema sul proprio computer.

Distribuzioni più diffuse

In ordine alfabetico, segue la lista delle distribuzioni più diffuse e conosciute che utilizzano il kernel linux:

- Android - È una distribuzione per dispositivi mobili (principalmente touch screen) inizialmente sviluppata dalla Startup Android Inc. e poi nel 2005 acquistata dalla Google Inc. che la supporta tuttora.

- Arch Linux - È leggera, veloce, estremamente scalabile e adattabile alle proprie esigenze. Ottimizzata per i686 e X86-64.
- Backtrack - Offre tools per fare test di penetrazione. Fino alla versione 3.0 derivava dalla distro WHAX, dalla versione 4.0 è invece basata su Ubuntu. Dopo l'ultima versione, pubblicata nell'agosto 2012, il progetto viene fermato a causa della sua architettura ormai datata e il progetto continua nella nuova distribuzione Kali Linux, più performante, più intuitiva e inoltre basata su Debian.
- CentOS - È una distribuzione basata sui sorgenti di Red Hat Enterprise Linux, quindi uguale ad essa in tutto e per tutto se non per i loghi e il nome che vengono cambiati in quanto marchi registrati. È usata per lo più in ambito server.
- Debian - Offre un ottimo sistema di gestione dei pacchetti software (in formato deb), compilati per 11 architetture differenti: Alpha, AMD64, ARM, HP PA-RISC, Intel x86, Intel IA-64, MIPS (big endian), MIPS (little endian), PowerPC, IBM S/390, SPARC. Viene definita per questo "il sistema operativo universale". Ha un'installazione disponibile sia in modalità testuale che grafica. I repository di Debian generalmente contengono solo software libero, ma è possibile attivare repository per installare software proprietario.
- Fedora - Distribuzione non commerciale sponsorizzata da Red Hat. Piuttosto curata nell'aspetto, viene aggiornata frequentemente con le ultime novità. Il sistema di pacchettizzazione è basato su RPM Package Manager e l'installazione è disponibile sia in modalità testuale che grafica.
- Gentoo Linux - Distribuzione non commerciale basata sui sorgenti che permette di ottimizzare e rendere estremamente flessibile il sistema. Implementa un sistema di porting derivato da BSD. L'installazione avviene manualmente, seguendo l'apposito manuale. Ulteriori punti di forza della distribuzione sono l'ottima documentazione e la comunità molto disponibile.
- Knoppix - La distribuzione live CD più famosa. Nata per uso forense, deriva da Debian. Molto indicata per i principianti, permette di avere un sistema completo avviabile direttamente da CD-ROM o DVD che permette, tra i vari usi, l'utilizzo dimostrativo, come tool di diagnostica, come test di compatibilità hardware, ecc. Presenta alcune varianti come Eduknoppix.

- Linspire - Era una distribuzione commerciale derivata da Debian che puntava alla facilità d'installazione e d'utilizzo anche da parte di principianti.
- Linux Mint - Derivata da Ubuntu, comprende alcuni software personalizzati per installazione e gestione, un menù principale che richiama quello di Microsoft Windows, e comprende codec multimediali preinstallati per DVD, MP3 ecc.
- Mandriva - Conosciuta come Mandrake fino al 2005, anno in cui la Mandrakesoft ha acquisito Conectiva. È una tra le distribuzioni più diffuse e maggiormente orientate all'utente desktop. È distribuita sia in forma gratuita che come prodotto commerciale (in questo caso include alcuni pacchetti proprietari), con nuove release a cadenza approssimativamente annuale. Ha un sistema di pacchettizzazione basato su RPM.
- Manjaro Linux - È una distribuzione basata su Arch Linux ed utilizza gli ambienti desktop Xfce o KDE.
- OpenSUSE - È una distribuzione non commerciale nata dall'apertura allo sviluppo comunitario di SUSE.
- Puppy - Distribuzione molto leggera, è disponibile in versione Live CD. Occupa poche risorse e spazio su disco ed è adatta a PC poco potenti o datati. Se la quantità di RAM è sufficiente (256 MB o più), può girare integralmente in memoria.
- Red Hat Linux Enterprise - È la distribuzione commerciale più diffusa. Leggera, non viene aggiornata alle ultime novità ma predilige versioni di kernel e componenti stabili e collaudate. Gli sviluppatori di Red Hat hanno realizzato il diffuso sistema di pacchetti RPM.
- Sabayon - Sabayon è una distro basata su Gentoo che si caratterizza per la compresenza di due package manager (binario e sorgente). È disponibile in diverse versioni con KDE, GNOME, XFCE, LXDE, Enlightenment, Fluxbox.
- Slackware - Creata nel 1993, viene spesso considerata la distribuzione più vicina a Unix e agli standard Linux. È molto stabile, versatile e mira alla semplicità: gli interventi sul codice sono minimi, nel rispetto delle intenzioni degli autori originali. Il sistema di gestione dei pacchetti affida all'utente la risoluzione delle dipendenze, mentre il software non incluso va compilato dai sorgenti.

- SLAX - Deriva direttamente da Slackware e ne conserva le caratteristiche di velocità, stabilità, leggerezza e ampia configurabilità in base alle varie esigenze del singolo utente. Adotta un approccio modulare avanzato.
- SUSE - Celebre distribuzione europea, molto usata a livello aziendale ma rivolta anche all'utente Desktop. Anch'essa basata su RPM, è un prodotto commerciale. È basata sul lavoro del progetto OpenSUSE.
- Ubuntu - Distribuzione derivata da Debian, è salita alla ribalta per la facilità d'installazione e d'utilizzo e per la disponibilità di frequenti aggiornamenti della versione stabile. Utilizza il gestore pacchetti APT, come Debian, e i desktop Unity e GNOME. Ne esistono numerose varianti ufficiali, tra cui Kubuntu, Xubuntu, Lubuntu, Edubuntu e Ubuntu MATE.
- Zorin OS - Distribuzione multingua basata su Ubuntu, è caratterizzata da un'interfaccia grafica molto simile a quella di Microsoft Windows.

Distribuzioni completamente libere

La maggioranza delle distribuzioni Linux non contiene esclusivamente software libero ma anche, in misura ridotta, software proprietario (ad esempio driver, codec, tool e applicazioni), spesso per mancanza di software libero ugualmente funzionale. Tuttavia alcune distribuzioni hanno scelto di non includere software proprietario e di utilizzare Linux-libre, una versione del kernel Linux completamente libera. Infatti Linux contiene parti di codice oscurate e sotto licenze non libere.

La Free Software Foundation (FSF), sulla base delle Guidelines for Free System Distributions, ha stilato una lista di distribuzioni Linux che contengono esclusivamente software libero.

Lista in ordine alfabetico:

- gNewSense - Distribuzione basata su Debian e Ubuntu e supportata dalla FSF.
- BLAG (le Brixton Linux Action Group) - Distribuzione Linux basata su Fedora.
- Dragora- Distribuzione indipendente basata sul concetto di semplicità.
- Dynebolic - Distribuzione specializzata nell'editing di audio e video.
- Kongoni - Distribuzione africana.
- Musix - Distribuzione basata su Knoppix, rivolta alla produzione audio.

- Parabola GNU/Linux-libre - Distribuzione basata su Arch che cura particolarmente la semplicità della gestione dei pacchetti e del sistema.
- Trisquel - Distribuzione orientata alle piccole imprese, agli usi domestici e ai centri educativi. Basata sui rilasci LTS di Ubuntu, è facile da usare, installare e configurare.
- Ututo - Distribuzione basata su Gentoo, è stato il primo sistema Linux completamente libero riconosciuto dal Progetto GNU.
- Venenux - Distribuzione rivolta principalmente ad utenti latinoamericani.

Distribuzioni per bambini

La scrivania della versione 4.00 della distribuzione Trisquel, completamente libera

Si tratta di distribuzioni che forniscono raccolte preinstallate di giochi educativi in ambienti adatti a bambini a partire dall'età prescolare (in alcuni casi a partire dai due anni) fino agli inizi dell'adolescenza. Tutte le distribuzioni di questo tipo adattano l'ambiente da un punto di vista grafico, ed alcune semplificano anche in maniera consistente le modalità di utilizzo dell'ambiente. Normalmente vengono fornite anche delle raccolte di giochi di esclusivo divertimento, ma a volte vengono preinstallati anche dei programmi per sviluppare la creatività.

Non di rado vengono integrati dei filtri famiglia per proteggere i bambini dall'ottenimento di pagine inappropriate durante la navigazione in Internet. I giochi educativi inclusi non differiscono molto tra una distribuzione e l'altra, e comprendono giochi per l'apprendimento dell'uso del mouse e della tastiera, dell'alfabeto e delle sillabe, dei numeri e delle operazioni, di abilità di

memorizzazione e ragionamento, fino ad attività più complesse come lo studio della geografia e delle scienze.

Ecco alcune delle distribuzioni per bambini attualmente esistenti:

- DoudouLinux - Distribuzione basata su Debian e multilingue, fa della semplicità d'uso e della adattabilità all'età del bambino i suoi punti di forza. Le attività più semplici sono utilizzabili a partire dai due anni, mentre i bambini più grandi troveranno tra le altre cose semplici programmi per lo sviluppo della creatività e navigheranno in internet protetti da un filtro famiglia. In arrivo anche uno strumento per la limitazione da parte dei genitori del tempo di uso del PC. Non richiede l'installazione, potendo essere usata da CD o da chiave USB.
- Edubuntu - Distribuzione basata su Ubuntu e supportata da Canonical.
- Edupup - Distribuzione basata su Puppy Linux.
- Foresight kids - Distribuzione basata su Foresight Linux.
- Linux KidX - Distribuzione basata su Slackware, disponibile in portoghese ed inglese.
- PaiX - Distribuzione basata su Mandriva, è in fase sperimentale.
- Qiko Junior - Distribuzione basata su QiLinux (trasformatasi in Tuga). La casa madre che la rilasciava (non scaricabile gratuitamente e provvista anche di un manuale d'uso cartaceo) è fallita.
- Qimo 4 kids - Distribuzione basata su Ubuntu e multilingue, è una distribuzione completa ed in avanzato stadio di sviluppo, che può essere anche installata come desktop environment aggiuntivo su una distribuzione Ubuntu preesistente. Non avendo sviluppato consistenti semplificazioni dell'interfaccia e delle modalità d'uso potrebbe però risultare un po' ostica per i bambini più piccoli.
- Trisquel EDU[32] - Versione di Trisquel GNU/Linux progettata per essere usata in qualsiasi scuola.
- Trisquel TOAST - TOAST, o "Trisquel On A Sugar Toast", è un'edizione del sistema operativo completamente libero Trisquel GNU/Linux che usa l'ambiente didattico Sugar. Sugar è l'interfaccia utente sviluppata da SugarLabs per i laptop di "One Laptop per Child XO" e progettata sui concetti di

apprendimento interattivo attraverso l'esplorazione. È stata impiegata con successo in molti paesi e contiene al suo interno un vasto catalogo di attività didattiche.

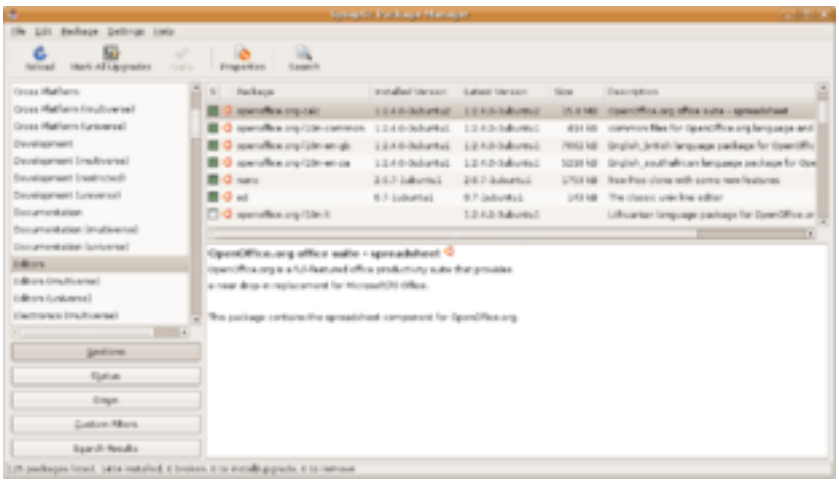
- UKnowforkids - Distribuzione basata su Arch Linux, disponibile solo in inglese ma con requisiti minimi hardware bassi.

Anche pensate per i bambini sono le distribuzioni appositamente concepite per le scuole, ma esse non sono espressamente concepite per l'uso sul singolo calcolatore domestico, ma piuttosto su reti scolastiche di calcolatori ed inoltre si rivolgono a bambini in età scolare. A tal proposito si veda la pagina Edutainment, dove si troverà anche una lista delle distribuzioni ad uso scolastico.

Distribuzioni per PC datati

- Puppy Linux
- Tiny Core Linux
- SliTaz
- Debian LXDE
- Lubuntu
- LXLE Linux
- Arch Linux

Gestori di pacchetti



La finestra del sistema di gestione dei pacchetti di Ubuntu e Trisquel

Le distribuzioni Linux sono normalmente composte da pacchetti (*packages*), ed ognuno di essi contiene una specifica applicazione o componente: ad esempio, ci possono essere pacchetti contenenti una libreria per la gestione di un formato di immagini, oppure una serie di font, oppure un browser web così come un qualsiasi altro programma. Un pacchetto è fornito normalmente come codice compilato, e la sua installazione o rimozione è gestita in maniera più sofisticata rispetto ad un semplice programma di archiviazione come tar.

Il programma preposto a queste funzioni è detto il sistema di gestione dei pacchetti (*package management system* o PMS) della distribuzione. Ogni pacchetto dedicato ad un PMS contiene delle meta-informazioni come descrizione, versione, dipendenze, ecc. Il sistema di gestione dei pacchetti tiene in considerazione queste meta-informazioni per permettere ricerche, aggiornamenti automatici a versioni più aggiornate, per controllare che tutte le dipendenze di un pacchetto siano soddisfatte e/o soddisfarle automaticamente.

Distribuzioni diverse hanno gestori di pacchetti diversi, ed i principali sono:

- rpm, adesso *RPM Package Manager* ma in origine *Red Hat Package Manager*, originariamente introdotto da Red Hat ma adesso usato in molte distribuzioni.
- deb, *Debian package*, originariamente introdotto da Debian, usato anche dalle sue distribuzioni derivate.
- .txz (sostituisce il precedente .tgz o tar.gz), standard tar + xz, a volte con ulteriori file di controllo, usato da Slackware ed altri, o a volte per la distribuzione di pacchetti molto semplici "fatti in casa".
- ebuild, file contenente informazioni su come ottenere, compilare ed installare un pacchetto nel sistema Portage di Gentoo Linux attraverso il comando emerge. Tipicamente queste sono installazioni basate sulla compilazione di sorgenti, nonostante anche alcuni pacchetti binari possano essere installati in questo modo.
- recipe, file contenente informazioni su come ottenere, decomprimere, compilare ed installare un pacchetto nella distribuzione Gobo Linux. Questo sistema è simile a quello di Gentoo.
- Autopackage, un gestore per creare un sistema di installazione indipendente ed uguale per tutte le distribuzioni Linux.

È presente inoltre la possibilità di compilare in proprio le applicazioni direttamente dai sorgenti disponibili, qualora non siano disponibili i binari precompilati. Sebbene la compilazione possa comportare alcune difficoltà, l'applicazione sarà sicuramente ottimizzata per il sistema sulla quale viene eseguita. Seguendo questa logica alcune distribuzioni (es. Gentoo) offrono la possibilità di compilare l'intero sistema operativo.

Versioni embedded

La classica schermata iniziale di un sistema operativo Android

La possibilità di intervenire sul kernel Linux e la comparsa di molti appassionati ne hanno suggerito l'utilizzo nell'elettronica dei dispositivi integrati. Infatti a partire dal 2009, è possibile reperire apparecchiature commerciali (quali router, smartphone o tablet) dotate di sistemi Linux fortemente ridotti. Esistono anche distribuzioni Linux pensate per essere utilizzate su tali sistemi embedded, ad esempio OpenWRT, FreeWRT, Android (sviluppato da Google), MeeGo o Ångström.

Sviluppo e promozione

La Linux Foundation è un'organizzazione formata dai maggiori produttori di software ed hardware il cui obiettivo è di migliorare l'interoperabilità tra le diverse distribuzioni.

Allo scopo, essa ha proposto una standard aperto e gratuito, chiamato Linux Standard Base (ufficializzato con lo standard ISO/IEC 23360) che definisce una comune ABI (Interfaccia Binaria per le Applicazioni), un unico sistema di pacchettizzazione ed una struttura per il file system che preveda le stesse convenzioni sui nomi e le stesse directory basilari in ogni sistema Linux. Molte aziende famose sono entrate nella Linux Foundation tra le quali: Cisco, Huawei, Microsoft, HP, IBM, intel, NEC, Fujitsu, Qualcomm e Samsung.

Esso al momento costituisce lo standard con maggiore *appeal*, al quale tutte le maggiori distribuzioni si stanno adeguando.

Le distribuzioni possono essere specializzate per differenti utilizzi: supporto a particolari architetture, sistemi embedded, stabilità, sicurezza, localizzazione per una particolare regione o lingua o il supporto per le applicazioni in real-time. In più, alcune distribuzioni includono solamente software libero. Attualmente, oltre trecento distribuzioni sono sviluppate attivamente, con circa una dozzina di esse che sono più famose per l'utilizzo giornaliero.

I LUG

Un Linux User Group (LUG), o anche "*Linux Users Group*" e "*Linux Users' Group*" è un gruppo formato da sostenitori e promotori del sistema operativo GNU/Linux.

I LUG sono spesso organizzati come associazioni senza scopo di lucro e la loro principale missione è contribuire alla diffusione del software libero e in particolare dei sistemi operativi basati sul kernel Linux.

Il Linux Day

I LUG italiani ogni anno promuovono e organizzano il Linux Day, una manifestazione che ha lo scopo di promuovere il sistema operativo Linux e il software libero, e avvicinare e aiutare i nuovi utenti, con un insieme di eventi contemporanei organizzati in diverse città d'Italia.

La Italian Linux Society (ILS) stabilisce la data del Linux Day e, a volte, fornisce proprio materiale pubblicitario. La responsabilità dei singoli eventi locali è lasciata ai rispettivi gruppi organizzatori, che hanno libertà di scelta per quanto riguarda i dettagli delle iniziative locali, nel rispetto delle linee guida generali definite da ILS. Giornate tematiche sul software libero e l'open source erano già state sperimentate in Italia sin dal 1999, grazie alle iniziative del gruppo ErLug (Emilia-Romagna Linux User Group). Fu grazie a queste esperienze, e i dibattiti che ne seguirono, che vennero definite le linee guida dei LinuxDay, successivamente gestite da ILS sul territorio nazionale. Le prime manifestazioni in questa nuova veste vennero proposte a partire dal 2001, per iniziativa di Davide Cerri di ILS, con lo scopo di valorizzare la rete dei LUG italiani organizzando una manifestazione di portata nazionale ma allo stesso tempo delocalizzata sul territorio. Il ruolo di ILS, tuttavia, è stato sempre secondario rispetto allo sforzo profuso dai LUG, veri artefici della manifestazione.

La prima edizione del Linux Day si è tenuta il 1º dicembre 2001 in circa quaranta città sparse su tutto il territorio.

Macintosh

Di Manuel Febbraro e Danilo Corea

La nascita del Macintosh

Mac OS è stato il primo sistema operativo di successo ad incorporare un'interfaccia grafica. Ma, a differenza di quanto si è portati a credere, l'OS della Mela non è stato il primo in senso assoluto, ispirandosi direttamente ad ALTO, nato nei laboratori dello XEROX PARC (Palo Alto Research Center), e ufficialmente riconosciuto come il primo vero computer dotato di OS grafico.

Nel 1979 Jobs visita lo XEROX PARC, restando fortemente impressionato dalle innovazioni tecnologiche sviluppate, e torna alla sede di Apple con un chiodo fisso: dotare i propri calcolatori di un sistema operativo con Interfaccia Grafica. Comincia così ad assume parte del team Xerox e da vita al progetto **Lisa**, velocemente soppiantato dal **Macintosh** che diventa un successo senza precedenti.Ma perché il Mac ha avuto successo dove ALTO e STAR, il suo diretto successore, hanno fallito? Le ragioni sono da ricercarsi principalmente nell'ambito economico/commerciale: Xerox ALTO costava circa 32.000$, lo Xerox START circa 16.600$. Inoltre la stessa Xerox non sapeva come presentare il proprio prodotto sul mercato, poiché era abituata a offrire principalmente fotocopiatrici.Il 24 gennaio 1984 Apple presenta il Macintosh (128K), al costo di 2.500$, e ne accompagna il lancio con un'ottima campagna pubblicitaria, che riesce ad ottenere un'ampia penetrazione del prodotto sul mercato e far dimenticare ad Apple l'insuccesso di LISA, rimasto nei magazzini a causa del costo proibitivo di circa 10.000$. Il sistema operativo fornito con il calcolatore della Mela viene indicato con il nome, poco fantasioso, di **System 1** e basato sul File System MFS (Macintosh File System).

Lisa

Macintosh

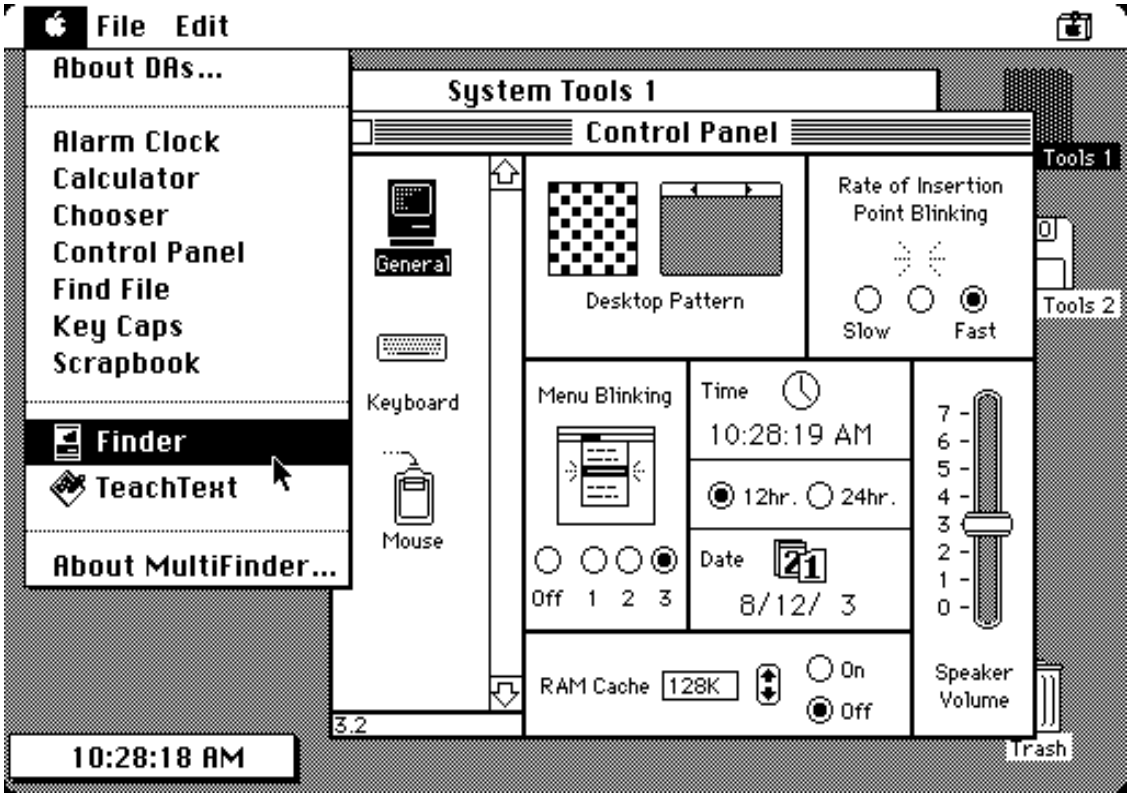
L'evoluzione di Macintosh

Ad aprile del 1985 arriva il Macintosh 512K con il System 2, praticamente identico al precedente, che, però, non risolve il limite di poter eseguire una sola applicazione per volta.

Ad un anno di distanza, gennaio del 1986, Apple presenta System 3 che, grazie al nuovo *HFS* (*Hierarchical File System*), permette una reale gestione gerarchica dei file e delle cartelle, a differenza dei suoi predecessori che simulavano tale funzionalità attraverso speciali tabelle indicizzate. Il passo successivo è System 4.0 (System 3.2, Finder 5.3) che fa la sua comparsa nel Marzo del 1987, a corredo del *Mac Plus,* e aggiunge il supporto per lo SCSI e il tool AppleTalk in bundle.

Continuando lungo la nostra timeline entriamo nel regno della confusione, grazie a System 5.0, che in realtà non è mai esistito.

Infatti, normalmente, con tale numero di versione si indica System 4.2 (Finder 6.0), rilasciato nell'ottobre del 1987, che introduce il *Multifinder* per lo scambio di informazioni tra l'unica applicazione attiva ammessa e le altre dormienti.



System 4.2

Nel 1988 è la volta di **System 6** che aggiunge l'agognato supporto ai monitor a colori ed introduce la nuova tecnologia QuickDraw al fine di estenderne le capacità grafiche. Il MultiFinder viene notevolmente migliorato con l'introduzione del *multitasking cooperativo*, apprestandosi a divenire l'unico Finder disponibile.

Bisogna attendere due anni (1990) per il rilascio di **System 7** che va a consolidare la precedente versioni e rende Mac OS un sistema stabile e completo, soprattutto grazie alle numerose ottimizzazioni del kernel, tra cui: *una nuova architettura di comunicazione tra i processi di sistema*, tra i *processi a livello utente* e una *migliore gestione dei driver delle periferiche*. Ciò porta ad un indirizzamento della memoria *full 32-bit* e non più a *24bit* come accadeva in precedenza a causa delle limitazioni dell'hardware dei primi Mac. Il *MultiFinder*, ormai maturo, diventa l'unico *Finder* disponibile ed opera in modalità *multitasking cooperative*.

Negli anni a seguire le cose per Apple si complicano notevolmente.

Windows 95 è ormai leader del mercato ed i vari tentativi di Apple di realizzare un OS per contrastare l'avanzata di Microsoft si rivelano un disastro. Da *Pink OS*, frutto di una joint venture tra IBM ed APPLE, abortito nel 1995, a Copland, sviluppato interamente da APPLE, che a due anni dall'annuncio (1996) viene abbandonato come progetto in se. Parte dei componenti di quest'ultimo vengono integrati nei vari aggiornamenti di System 7, che raggiunge velocemente la release **System 7.6**.

Per risalire la china, APPLE tenta allora una strada completamente diversa: acquisire *Be Inc*, produttrice del popolare BeBox e, soprattutto, del **BeOS**. L'accordo di acquisizione raggiunge lo stadio finale ma si blocca per questioni economiche: APPLE offre 120 milioni di dollari mentre Be ne chiede 200, nonostante i "soli" 20 milioni di dollari totali degli investimenti sostenuti dalla società. La lunghezza della trattativa, anche se non del tutto naufragata, spinge la casa di Cupertino a considerare l'adozione di sistemi operativi terzi come Solaris e, addirittura, Windows NT.

In questa fase di incertezza e di panico, rispunta Jobs, precedentemente uscito da Apple, che chiama il CEO Amelio e gli offre il proprio OPENSTEP e la piattaforma tecnologia di NeXT, società fondata dallo stesso Jobs dopo il divorzio dalla "sua" Apple il 31 maggio del 1985. Le due società raggiungono un accordo di

acquisizione ed il 20 dicembre del 1996 APPLE acquista NeXT per 427 milioni di dollari.Sul divorzio tra Jobs ed Apple a predominare è quasi sempre stata la versione secondo cui Apple abbia licenziato il proprio fondatore, ma nel 2011 **Jay Elliot** (vice presidente esecutivo Apple**)**, nel suo libro "Steve Jobs – L'uomo che ha inventato il futuro", racconta la verità in quanto spettatore dell'episodio.

Accadde che Steve Jobs, anni prima, si innamorò di un prototipo nato nei centri di ricerca di Apple e diede vita alla divisione Macintosh. L'Apple II, il computer che aveva reso Apple molto ricca, si trovò in competizione con un nuovo modello. Jobs creò di proposito avversità tra la divisione Apple II e la divisione Macintosh, tanto da chiamare "pirati" chi lavorava al Mac e "marina" chi sottostava alle regole ufficiali di Apple.

Al lancio del Mac le vendite decollarono, ma si fermarono pochi mesi dopo per le scarse prestazioni hardware del computer e per l'esigua presenza di software. Sculley chiese a Jobs di cambiare il prodotto per renderlo più commerciale, ma quest'ultimo proseguì per la sua strada con l'idea di creare il computer perfetto ideale per tutti. Tutta l'operazione, però, stava diventando dannosa per l'economia di Apple, così Sculley sollevò Jobs dalla divisione Mac per promuoverlo a CTO di Apple.

Il capriccioso Jobs non accettò l'offesa e uscì dagli uffici della società. Poco dopo vendette tutte le sue azioni, eccetto una, e si diede a una serie di viaggi, tra l'altro iniziando dall'Italia. Qualche anno dopo Steve Jobs chiese ad Apple di collaborare per una nuova startup e Apple gli diede alcuni dipendenti, portando la nascita di NeXT. Quindi in realtà Steve Jobs non fu mai licenziato da Apple, ma si allontanò di sua volontà e NeXT, acquistata negli anni '90 da Apple, nacque proprio da una costola della società.

Subito dopo l'acquisizione di NeXT, APPLE comincia lo sviluppo di *Rhapsody*, il suo nuovo OS NeXT-based, la cui roadmap porta al veloce rilascio di due *developer release*, la prima a settembre del 1997 e la seconda a maggio dell'anno successivo.

Nel frattempo, sempre nel 1997, viene rilasciato **Mac Os 8** (non *System 8*) che fa proprio il File System HFS+ e aggiorna la GUI, permettendone una più ampia personalizzazione. Miglioramenti importanti si riscontrano anche nella gestione delle reti, nella condivisione delle risorse e dei driver delle periferiche.

Il 16 settembre del 1997 Steve Jobs viene nominato CEO ad interim di APPLE e pochi mesi dopo, al WWDC del 1998, annuncia che APPLE è pronta a rilasciare il nuovo Mac OS X, che comunque garantirà la compatibilità con il precedente Mac OS grazie ad una sorta di sand-box. Da questo momento in poi il vecchio sistema Apple sarà indicato come “Classic”. Anche se con leggero ritardo i tempi vengono rispettati ed il 16 marzo del 1999 APPLE presenta Mac OS X Server 1.0 e una *developer preview* della Desktop edition denominata *Darwin 0.1*. Nel contempo Mac OS 8 viene aggiornato alla release **8.5** (1998) eseguibile solo su architettura power pc e accompagnato dal nuovo sistema di ricerca *Sherlock*.

I tempi di rilascio della versione definitiva del nuovo OS sono però ancora lunghi e la società di Cupertino decide di aggiornare ulteriormente Mac OS, rilasciando prima la versione **8.6**, che introduce un "*nanokernel*" per il multi tasking e il supporto al multiprocessing, e poi **Mac OS 9**, pensato per guidare la transizione a MacOS X e, nel contempo, garantire una migliore integrazione nel nuovo OS in ottica retrocompatibilità. Mac OS 9 contiene fondamentalmente una serie di

tecnologie pensate per preparare gli utenti, ma soprattutto gli sviluppatori, alla rivoluzione X, tra cui l'API **Carbon,** fondamentale per lo sviluppo di applicazioni compatibili anche con Mac OS X. Nelle successive minor release Apple ne rende, addirittura, obbligatorio l'utilizzo.

L'attesa termina il 24 Marzo del 2001: nasce **Mac OS X**.

Ad oggi sono state rilasciate 11 major release di Mac OS X.

Dal 2001 a Oggi

Nel 2001 il Macintosh fece un secondo fondamentale cambiamento, questa volta nel suo sistema operativo, passando dal vecchio macOS al nuovo macOS il cui kernel è basato su Unix.

Durante il Keynote del WWDC 2005, Steve Jobs annunciò il passaggio dai processori PowerPC alle CPU Intel.

Con sei mesi di anticipo rispetto alle previsioni, il 10 gennaio 2006, durante il tradizionale Keynote del Macworld Expo, Steve Jobs presentò i nuovi iMac e il nuovo MacBook Pro con CPU Core Duo di Intel. Il giorno 7 agosto 2006, dopo soli 210 giorni e ben prima delle aspettative, la transizione ai processori Intel fu completata. Da quel giorno non sono più in commercio sistemi Macintosh con processori PowerPC.

Un Power Mac G4 "Quicksilver" (2003) vs MacBook Air (2016)

Fonti

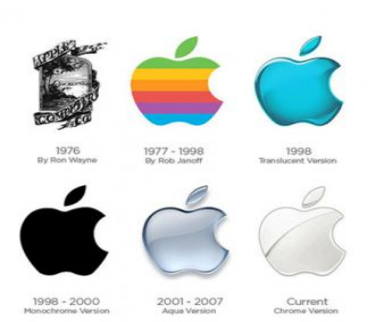
1. www.storiainformatica.it/mac
2. www.wikipedia.it

IOS

Di Domenico Cosentino e Fotino Mattia

Introduzione

La Apple Computer ha cambiato la storia dell'informatica. È stata fondata inizialmente da tre soci, il 1° aprile 1976 in un garage: le principali menti sono Stephen Wozniak e Steve Paul Jobs.Adesso che avevano deciso di mettersi in affari,avevano bisogno di un nome. Jobs aveva fatto un'altra capatina all'All One Farm,dove stava portando i meli di Gravenstein, e Wozniak era andato a prendere all'aeroporto. Durante il viaggio fino a Los Altos,discussero delle possibili opzioni. Presero in considerazione alcune tipiche parole tecniche,come Matrix,e alcuni neologismi, come Executek. Alla fine lui propose Apple computer.<<Stavo seguendo in quel momento una delle diete a base di frutta ed ero appena tornato dal meleto>>spiega. Mi sembrava un nome simpatico,vivace,che non metteva in soggezione. "Apple",mela ammorbidiva la parola "computer",Apple fu una scelta brillante il nome comunicava subito un idea di simpatia e semplicità. Il primo logo della Apple Computer rappresentava Isaac Newton seduto sotto a un albero di mele e fu disegnato nel 1976 da un ex socio di Steve Jobs Il disegno in questione, dalla grafica particolareggiata e poco accattivante, non soddisfò mai Jobs, che nel 1977 commissionò al grafico Rob Janoff una nuova immagine. Questi ideò allora il logo della mela morsicata. Tra l'altro, la parola morso - in inglese *bite* - bene si abbinava ai *bit* e ai *byte* del linguaggio informatico, e la stessa mela mordicchiata alludeva al peccato originale, a sottolineare l'anticonformismo della Apple. All'inizio Janoff tratteggiò una mela monocromatica, ma Jobs la volle colorata, poiché il modello che proponeva in quel momento, l'Apple II, si presentava con una innovativa interfaccia a colori. Il designer arricchì quindi il logo con una serie multicromatica di bande orizzontali, come un arcobaleno, e tale immagine rimase immutata fino al 1998, quando si tornò al colore unico.



Storia

Il sistema operativo è stato presentato il 9 gennaio 2007 al Macworld di San Francisco e la versione 1.0, ancora priva di nome, è entrata in commercio con il primo iPhone il 29 giugno dello stesso anno[2]. Il 6 marzo 2008, in concomitanza con la pubblicazione della prima beta del SDK, il sistema operativo è stato denominato ufficialmente come "iPhone OS" (che sta per "iPhone Operating System").

L'11 luglio 2008 viene pubblicato, in concomitanza della vendita di iPhone 3G, l'aggiornamento a iPhone OS 2 che aggiunge, tra le altre funzioni, il molto atteso App Store e la possibilità di installare applicazioni di terze parti tramite quest'ultimo.

iPhone OS 3, pubblicato con l'iPhone 3GS il 17 giugno 2009, ha aggiunto molte funzioni che furono richieste dagli utenti, alcuni dei quali il copia e incolla e gli MMS. Tutti i dispositivi erano aggiornabili a iPhone OS 3, ma con delle limitazioni per la prima generazione di iPhone e iPod touch. Il primo iPad, entrato in commercio nell'aprile 2010, ha avuto inizialmente un "ramo" separato di iPhone OS 3, fino all'unificazione con gli altri dispositivi con la versione 4.2.1 del software.

Il quarto aggiornamento del sistema operativo, pubblicato con iPhone 4 il 21 giugno 2010, ha aggiunto numerose funzioni quali il multitasking per le applicazioni di terze parti, FaceTime e iBooks. L'ora rinominato "iOS", ha unificato i vari dispositivi (iPhone, iPod touch e iPad) con una versione comune, la 4.2.1.

Il 6 giugno 2011 è stata presentata alla WWDC la quinta versione di iOS, con numerose nuove funzioni, tra cui la sincronizzazione wireless, l'integrazione con il servizio iCloud di Apple e un rinnovato sistema di notifiche. Nel giorno stesso è stata pubblicata la prima beta del sistema operativo. iOS 5 è stato distribuito ufficialmente il 12 ottobre 2011.

L'11 giugno 2012 è stata presentata alla WWDC la sesta versione di iOS, con l'applicazione Mappe completamente rinnovata, nuovissime funzioni e lingue per l'assistente vocale Siri, tra cui l'attesa inclusione della lingua italiana,

l'integrazione con Facebook, nuove funzioni di risposta alle chiamate e novità grafiche. iOS 6 è stato reso disponibile per il download dal 19 settembre 2012.

Il 10 giugno 2013 è stata presentata alla WWDC la settima versione di iOS, con uno stile grafico completamente rinnovato in chiave minimale, che presenta icone molto più semplici e colorate, meno reminiscenti di elementi del mondo reale. Altro importante punto di rottura col precedente iOS è la rimozione della barra di sblocco presente fin dalla prima release di iOS, sostituendola con una schermata di sblocco più semplice e minimalista. Altro rinnovamento sostanziale è la totale revisione del multitasking, modificandone il look e le funzionalità, rendendolo più attuale e al pari dei sistemi concorrenti. Sono state presentate molte altre novità, fra le quali l'introduzione di nuove 1500 API in dotazione agli sviluppatori. La data di pubblicazione, che è stata comunicata al keynote tenutosi a Cupertino il 10 settembre 2013, è il 18 settembre dello stesso anno. Il 2 giugno 2014 è stata presentata alla WWDC l'ottava versione di iOS, che mantiene la stessa grafica di iOS 7, ma con nuove funzionalità come ad esempio la possibilità di inviare messaggi vocali con iMessage, la funzione di Quick Reply per poter rispondere velocemente a un messaggio semplicemente tirando verso il basso una notifica. Attraverso Spotlight si può anche cercare in iTunes/App Store, cercare su Mappe o avere risultati di ricerca da Bing. Aggiunta una nuova funzione di iCloud, "In famiglia", così da poter condividere ogni acquisto tra tutti i membri della famiglia. È stata aggiunta su iPhone e iPod touch l'applicazione Salute. , iOS 9 è stato rilasciato nella versione finale mercoledì 16 settembre. Le novità grafiche consistono in una Siri rinnovata, in grado di interagire maggiormente dando suggerimenti nella pagina di Spotligh, rinominata "Proactive" (con i vari suggerimenti dell'assistente vocale). Sono state introdotte diverse novità nell'applicazione Note e alcune migliorie per l'applicazione Mappe, che ora offre anche i dati e le linee dei mezzi di trasporto pubblici delle principali città del mondo. Su iPad arriva la funzione *Split-View* che consente di visualizzare due applicazioni contemporaneamente e il Multitasking ora si trova a sinistra della schermata home e presenta un grafica molto più scorrevole, "a pagine". Con iOS9, è stata introdotta la modalità di *Risparmio Energetico* che riduce il consumo della batteria. Il 13 giugno 2016 è stata presentata alla la decima versione, che porta molteplici novità, tra le quali più apertura del sistema a sviluppatori terzi.

L'applicazione Foto ora riconosce i volti e gli oggetti. L'applicazione musica è stata completamente ridisegnata, Anche l'applicazione Messaggi ha ricevuto un enorme aggiornamento, ora è possibile inviare messaggi con effetti visivi, sticker, GIF e le emoji sono 3 volte più grandi.

Tecnologia

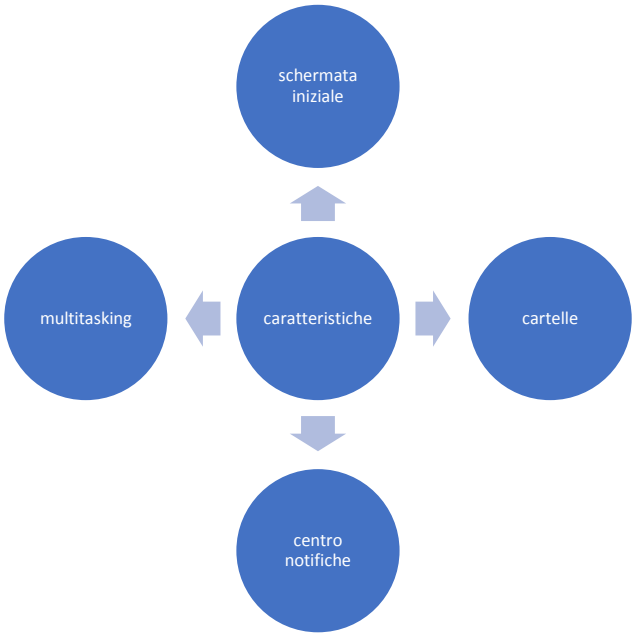
Il processore di iPhone e iPod Touch è un RISC ARM, come il SoC usato nell'iPad è allo stesso modo di architettura ARM Cortex, a differenza del processore x86 (e prima PowerPC o MC680x0) che viene comunemente usato nella linea Macintosh; le soluzioni ARM sfruttano OpenGL ES 1.1 e OpenGL ES 2.0 renderizzate da un processore video PowerVR.

Le applicazioni per macOS non possono essere ufficialmente copiate e lanciate in dispositivi con iOS ma necessitano di essere personalizzate e compilate specificatamente per iOS e per l'architettura ARM.

Tuttavia, il web browser integrato Safari supporta le web applications

Caratteristiche

Come macOS, è una derivazione di UNIX (famiglia BSD) e usa un microkernel XNU Mach basato su Darwin OS. iOS ha quattro livelli di astrazione: il Core OS layer, il Core Services layer, il Media layer e il Cocoa Touch layer. Il sistema operativo occupa meno di mezzo Gigabyte della memoria interna del dispositivo. Il sistema operativo non aveva un nome ufficiale fino all'uscita della prima beta dell'iPhone SDK il 6 marzo 2008; prima di allora, il marketing Apple affermava che "iPhone usa OS X". Molti fanno utilizzo del termine iDevice per riferirsi ai dispositivi che usano iOS. Ogni App del mondo Apple ha bisogno del sistema operativo iOS per andare in esecuzione; tuttavia gli sviluppatori possono simulare le proprie applicazioni tramite il programma Xcode, disponibile solamente per il sistema operativo macOS.



Schermata iniziale

La schermata iniziale (Home) viene visualizzata quando viene sbloccato il dispositivo (tramite la schermata di sblocco) oppure cliccando sul tasto home sotto il display. In alto, un barra mostra l'ora, il segnale telefonico, lo stato della batteria, l'attivazione o meno del 3G, 4G, LTE, Edge, Wi-Fi, Bluetooth, localizzazione e sveglia. La schermata iniziale permette inoltre di visualizzare tutte le applicazioni presenti sul dispositivo e in basso le applicazioni usate più frequentemente (di default su iPhone: telefono, safari, messaggi e musica; su iPod touch e iPad: messaggi, safari, mail e musica), che possono essere spostate e modificate a proprio piacimento.

A partire dalla versione 3.0 viene anche integrata la funzione Spotlight, che ricerca nel dispositivo contatti, messaggi, e-mail, canzoni, video, podcast, applicazioni, promemoria, eventi, applicazioni di terze parti oppure cercare su Internet ciò che si è digitato. Vi si può accedere scorrendo verso il basso dalla schermata home oppure dalla versione 10 anche scorrendo verso destra sempre dalla schermata home. Dalla versione 3.2 è inoltre possibile modificare lo sfondo.

Cartelle

A partire da iOS 4.0 è possibile raggruppare in cartelle le applicazioni della schermata principale, semplicemente trascinando l'icona di un'applicazione su di un'altra. Ciascuna cartella può essere rinominata a piacimento. Se si ricevono delle

notifiche dalle applicazioni poste all'interno di una cartella, esse vengono segnalate con un badge sulla cartella stessa. Ciascuna cartella può contenere fino a 12 applicazioni su iPhone 4S e iPod Touch quarta generazione e precedenti, 16 su iPhone 5 e iPod Touch quinta generazione, 20 su iPad.

Da iOS 7 in poi il numero di applicazioni inseribili in ciacuna cartella non è più limitato: le app all'interno di una cartella sono infatti organizzate in pagine, come nella schermata principale.

Centro notifiche

Dalla versione 5.0 trascinando verso il basso partendo dall'alto dello schermo, viene mostrata una "tendina" con il meteo, la borsa, l'integrazione con Facebook e Twittere le varie notifiche, tra cui anche promemoria ed eventi. Con la versione 7.0, il centro notifiche è stato separato in tre sezioni: Oggi (con il riepilogo degli eventi, meteo, promemoria e borsa), Tutti (dove verranno visualizzate tutte le notifiche ricevute) e Perse (dove verranno visualizzare le ultime notifiche perse). In iOS 8 è stata rimossa la sezione Perse e sono stati aggiunti i widget. Con iOS 10 il centro notifiche è stato completamente ridisegnato. Trascinandolo dalla parte superiore dello schermo verranno mostrate le notifiche e scorrendo da sinistra verso destra (dal centro notifiche) tutti i widget. È ora possibile scorrere da sinistra a destra dalla schermata principale per accedere ai widget.

Multitasking

Le funzioni multitasking sono state introdotte nella versione 4.0, perché Apple dubitava della durata della batteria con l'esecuzione di più applicazioni di terze parti contemporaneamente, rendendo disponibile questa funzionalità solo a partire da iOS 4 tramite le sue specifiche API

Aggiornamenti software

Apple ogni anno fornisce un aggiornamento di iOS su iTunes e, dalla versione 5.0, anche sul dispositivo stesso tramite aggiornamenti over-the-air. Fino all'uscita di iOS 4.0 tutti i possessori di iPod touch dovevano pagare per poterlo installare.

iOS SDK

Il 17 ottobre 2007, in una lettera aperta scritta nel blog *How News* di Apple, Steve Jobs ha annunciato che un SDK (software development kit) sarebbe stato disponibile agli sviluppatori di terze parti in febbraio 2008. L'SDK è stato distribuito il 6 marzo 2008 e permette agli sviluppatori di creare applicazioni per iPhone e iPod touch, e testarle in un simulatore di iPhone. Tuttavia il caricamento di una applicazione nei dispositivi è possibile solamente dopo aver pagato una tassa di iscrizione all'iOS Developer Program. L'ambiente di sviluppo per iOS SDK è Xcode.

Gli sviluppatori sono liberi di scegliere qualsiasi prezzo per le loro applicazioni che sono distribuite tramite App Store, per le quali riceveranno il 70% del ricavo. Essi possono anche optare per pubblicare gratuitamente l'applicazione non pagando nessun costo di pubblicazione o distribuzione, eccetto la tassa di sottoscrizione al programma developer.

Contenuto SDK

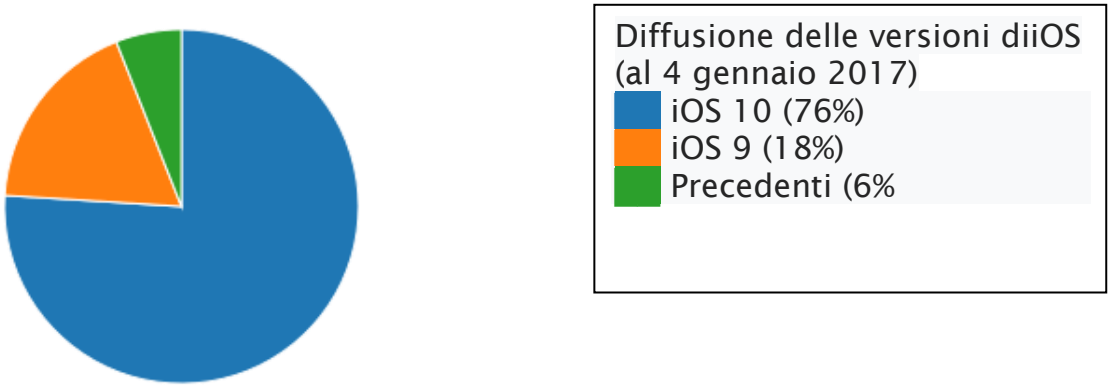
Dato che l'iPhone è basato su una variante dello stesso kernel XNU usato da macOS, gli strumenti usati per lo sviluppo sono basati su Xcode.

L'SDK è diviso nei seguenti set:

- Cocoa touch
  - eventi e controlli
  - Supporto
  - View gerarchica
  - Localizzazione
  - Camera supporto
- Media
  - OpenAL
  - Audio mixing e recording
  - Video playback
  - Image file formats
  - Quartz
  - Core animation
  - OpenGL ES
- Core Service
  - Networking
  - Embedded SQLite database
  - Geolocation
  - Threads
- OS X Kernel
  - TCP/IP
  - Sockets
  - Power managment
  - File system
  - Security

All'interno dell'SDK è contenuto l'iPhone Simulator, un programma usato per emulare il "look and feel" dell'iPhone nel desktop dello sviluppatore. Originariamente chiamato Aspen Simulator, è stato rinominato con la beta 2 dell'SDK. Da notare che l'iPhone Simulator non è un emulatore ed esegue codice generato per un target x86.L'SDK richiede un Mac Intel con Mac OS X Leopard. Altri sistemi operativi, inclusi Microsoft e vecchie versioni di macOS, non sono supportati, ma vi sono applicazioni non ufficiali che permettono ciò.

Diffusione



ll 6 giugno 2011 al WWDC viene annunciato che il numero di dispositivi iOS venduti ha raggiunto quota 200 milioni, il 18 febbraio 2012 viene comunicato il superamento di quota 316 milioni.

Secondo StatCounter, a settembre 2013 Apple iOS è il secondo sistema operativo mobile con il 23% del mercato. A settembre 2015 l'87% dei dispositivi Apple utilizza l'ultima versione disponibile del sistema operativo.

Pregi e critiche

Il sistema Apple ha delle peculiarità di funzionamento che ne determinano una diversa fruizione delle applicazioni e dei dispositivi. Uno studio della Symantec evidenzia come questo sistema operativo sia più sicuro del maggiore avversario Android grazie alle sue peculiarità, anche se ha evidenziato che è in realtà più sicuro soprattutto per via dei minori tentativi di attacco da parte degli hacker, che concentrano gli sforzi su Android in quanto maggiormente diffuso a livello mondiale rispetto a iOS. Con l'aggiornamento del sistema alla versione 4.3, si è evidenziato come questi aggiornamenti non fossero abilitati per le applicazioni web il problema è stato risolto però con la versione 5 del sistema operativo. La particolarità di questo sistema è data anche dal blocco di alcuna funzionalità, come ad esempio il bluetooth che può essere usato solo per connettere dispositivi ausiliari, come ad esempio cuffiette auricolari, ecc. Apple tramite il suo store evita l'installazione di applicazioni non approvate, perché prima di essere approvate vengono vagliate e viene testato la loro sicurezza e un eventuale problema nel loro uso, così come la loro qualità. Questo rende più difficile l'installazione di applicazioni malevole ma al contempo limita la libertà dell'utente. I rappresentanti del movimento opensource criticano questo approccio ritenendolo troppo limitante per l'utente e ritengono che di dispositivi così limitati non possano essere equiparati a dei computer. Tuttavia, è possibile evitare questo limitazione di attività attraverso un procedura ormai frequente e dichiarata legale dal Tribunale Federale USA chiamata jailbreak o in italiano "sblocco", la quale permette l'uso di applicazioni non approvate da Apple, presenti su Cydia. Nel 2012 è emerso di come le applicazioni potrebbero estrapolare le foto personali dell'utente dal proprio dispositivo, inoltre altre applicazioni come Path, memorizzano tutti i contatti, con i rispettivi nomi e cognomi registrati sul

cellulare su cui è installata l'applicazione. Problemi del genere vennero poi sistemati, all'uscita di iOS 6, con l'introduzione di appositi avvisi e impostazioni che permettono all'utente di consentire o negare alle singole applicazioni l'accesso a contatti, calendari, promemoria e immagini in modo del tutto simile a come già avveniva per la localizzazione.

Nel 2013, all'uscita di iOS 6.1, è stata individuata un falla di sicurezza che consentiva a chiunque effettuasse una precisa procedura di accedere all'applicazione telefono bypassando il codice di sblocco. In questo modo qualsiasi malintenzionato poteva effettuare telefonate, visualizzare contatti, ecc. Tali problematiche si erano già verificate in passato con le versioni 2.0 e 4.1 dell'OS e sono state corrette con gli aggiornamenti successivi.

Fonti

1. Andreucci Giacomo, *Applicazioni iOS e Android con Google Maps*, Edizioni FAG, Milano, 2011, pp. 348
2. Iacubino Angelo, *Creare applicazioni di successo per iPhone e iPad*, Edizioni Hoepli, 2010, pp. 312
3. Stark Jonathan, *Sviluppare applicazioni per iPhone*, Ed. Tecniche Nuove, 2010, pp. 161
4. Walter Isaacson, *Steve Jobs*, Mondadori, 2011.

Mobile

Di Ivan elia

Evoluzione dei sistemi operativi mobile

Un sistema operativo per dispositivi mobili, in inglese "mobile OS", è un sistema operativo che controlla un dispositivo mobile, con lo stesso principio con il quale viene controllato un computer. L'unica differenza tra i due OS è l'hardware: il mobile OS deve lavorare con CPU e ram limitate, nuovi metodi di immissione (touchscreen e mini tastiere) e ridotte dimensioni del display.

Oggigiorno i leader mondiali sul mercato "mobile OS" sono Android e iOS, mentre altri OS come Windows Phone, RIM (Blackberry) o Symbian seguono a ruota.

Android

Android è un sistema operativo sviluppato da Google e basato sul kernel Linux. Esso è il sistema operativo per sistemi mobili più usato al mondo, con ben il 61% di vendite sul mercato. Lo sviluppo di Android, oltre ai diversi firmware prodotti da Google, è basato sulle Google Apps programmate da esterni, mediante l'Android Open Source Project, software libero. Nell'ottobre 2003 Andy Rubin (cofondatore di Danger), Rich Miner (cofondatore di Danger e di Wildfire Communications), Nick Sears (vicepresidente di T-Mobile) e Chris White (principale autore dell'interfaccia grafica di Web TV), fondarono una società, la Android Inc. per lo sviluppo di quello che Rubin definì «...dispositivi cellulari più consapevoli della posizione e delle preferenze del loro proprietario». Inizialmente la società operò in segreto, rivelando solo di progettare software per dispositivi mobili. Durante lo stesso anno il budget iniziale si esaurì, motivo per cui fu fondamentale un finanziamento di 10 000 dollari da parte di Steve Perlman (amico intimo di Rubin) per poter continuare lo sviluppo. Steve Perlman consegnò a Rubin il denaro in una busta ma rifiutò ogni proposta di partecipazione al progetto. Il 17 agosto 2005 Google ha acquisito l'azienda, in vista del fatto che la società di Mountain View desiderava entrare nel mercato della telefonia mobile. È in questi anni che il team di Rubin comincia a sviluppare un sistema operativo per dispositivi mobili basato sul kernel Linux. La presentazione ufficiale del "robottino verde" avvenne il 5 novembre 2007 dalla neonata OHA (Open Handset Alliance), un consorzio di aziende del settore Hi Tech che include Google, produttori di smartphone come

HTC e Samsung, operatori di telefonia mobile come Sprint Nextel e T-Mobile, e produttori di microprocessori come Qualcomm e Texas Instruments Incorporated. Il primo dispositivo equipaggiato con Android che venne lanciato sul mercato fu l'HTC Dream, il 22 ottobre del 2008. Dal 2008 gli aggiornamenti di Android per migliorarne le prestazioni e per eliminare eventuali problemi di sicurezza delle precedenti versioni sono stati molti. Una caratteristica degli aggiornamenti di Android sono i nomi: ognuno di essi, ad eccezione del 1.0 e 1.1, ha per nome un dolce; il primo fu il Cupcake (1.5) mentre l'ultimo, tutt'ora in beta, è il Nougat (7.0). Dalla versione 1.5 ogni aggiornamento o release, similmente a quanto accade per molte versioni di Linux, segue una precisa convenzione alfabetica per i nomi, che in questo caso sono quelli di dolci: la versione 1.0 e 1.1 non hanno un nome di dolce e sono identificate col solo numero di versione (tuttavia la seconda, durante lo sviluppo, fu nominata in via ufficiosa Petit Four), la 1.5 venne chiamata Cupcake, la 1.6 Donut, la 2.1 Eclair, la 2.2 Froyo, la 2.3 Gingerbread, la 3.0 Honeycomb, la 4.0 Ice Cream Sandwich, la 4.1 Jelly Bean, la 4.4 Kit Kat in seguito ad un accordo con la Nestlé poi la 5.0 Lollipop. Il 5 ottobre 2015, tocca alla 6.0, col nome Marshmallow. Google lancia la possibilità di far scegliere agli utenti il nome della prossima versione. Molti italiani votano per Android nutella ma non sarà poi quello il nome. Il 30 giugno 2016 viene annunciato ufficialmente il nome della versione successiva e il 22 agosto è pronta ad apparire sugli smartphone android con il nome di 7.0 nougat (torrone). Nell'immagine sottostante sono messe a confronto alcune delle versioni di Android.

iOS

iOS è il sistema operativo sviluppato da Apple per iPhone, iPod touch e iPad. È il secondo sistema operativo mobile più venduto, con ben il 32% di vendite sul mercato, secondo solo ad Android.

Il sistema operativo è stato presentato il 9 gennaio 2007 al Macworld Conference & Expo di San Francisco e la versione 1.0, ancora priva di nome, è entrata in commercio con il primo iPhone il 29 giugno dello stesso anno. Il 6 marzo 2008, in concomitanza con la pubblicazione della prima beta del SDK, il sistema operativo è stato denominato ufficialmente come "iPhone OS" (che sta per "iPhone Operating System"). L'11 luglio 2008 viene pubblicato, in concomitanza della vendita di iPhone 3G, l'aggiornamento a iPhone OS 2 che aggiunge, tra le altre funzioni, il molto atteso App Store e la possibilità di installare applicazioni di terze parti tramite quest'ultimo. Come macOS, è una derivazione di UNIX (famiglia BSD) e usa un microkernel XNU Mach basato su Darwin OS. iOS ha quattro livelli di astrazione: il Core OS layer, il Core Services layer, il Media layer e il Cocoa Touch layer. Il sistema operativo occupa meno di mezzo Gigabyte della memoria interna del dispositivo. Il sistema operativo non aveva un nome ufficiale fino all'uscita della prima beta dell'iPhone SDK il 6 marzo 2008; prima di allora, il marketing Apple affermava che "iPhone usa OS X". Molti fanno utilizzo del termine iDevice per riferirsi ai dispositivi che usano iOS. Ogni App del mondo Apple ha bisogno del sistema operativo iOS per andare in esecuzione. La schermata iniziale (Home) viene visualizzata quando viene sbloccato il dispositivo (tramite la schermata di sblocco) oppure cliccando sul tasto home sotto il display. In alto, un barra mostra l'ora, il segnale telefonico, lo stato della batteria, l'attivazione o meno del 3G, 4G, LTE, Edge, Wi-Fi, Bluetooth, localizzazione e sveglia. La schermata iniziale permette inoltre di visualizzare tutte le applicazioni presenti sul dispositivo e in basso le applicazioni usate più frequentemente (di default su iPhone: telefono, safari, messaggi e musica; su iPod touch e iPad: messaggi, safari, mail e musica), che possono essere spostate e modificate a proprio piacimento. A partire dalla versione 3.0 viene anche integrata la funzione Spotlight, che ricerca nel dispositivo contatti, messaggi, e-mail, canzoni, video, podcast, applicazioni, promemoria, eventi, applicazioni di terze parti oppure cercare su Internet ciò che si è digitato. Vi si può accedere scorrendo verso il basso dalla schermata home oppure dalla versione 10 anche scorrendo verso destra sempre dalla schermata home. Dalla versione 3.2 è inoltre possibile modificare lo sfondo.

Le funzioni multitasking sono state introdotte nella versione 4.0, perché Apple dubitava della durata della batteria con l'esecuzione di più applicazioni di terze

parti contemporaneamente, rendendo disponibile questa funzionalità solo a partire da iOS 4 tramite le sue specifiche API.

Dalla versione 5.0 trascinando verso il basso partendo dall'alto dello schermo, viene mostrata una "tendina" con il meteo, la borsa, l'integrazione con Facebook e Twitter e le varie notifiche, tra cui anche promemoria ed eventi. Con la versione 7.0, il centro notifiche è stato separato in tre sezioni: Oggi (con il riepilogo degli eventi, meteo, promemoria e borsa), Tutti (dove verranno visualizzate tutte le notifiche ricevute) e Perse (dove verranno visualizzare le ultime notifiche perse). In iOS 8 è stata rimossa la sezione Perse e sono stati aggiunti i widget. Con iOS 10 il centro notifiche è stato completamente ridisegnato. Trascinandolo dalla parte superiore dello schermo verranno mostrate le notifiche e scorrendo da sinistra verso destra (dal centro notifiche) tutti i widget. È ora possibile scorrere da sinistra a destra dalla schermata principale per accedere ai widget.

Nell'immagine sottostante sono messe a confronto alcune delle versioni di iOS.

Classifica mobile OS sul mercato

1. **Android** è al primo posto con il 60,99% di smartphone e tablet. Addirittura il sistema operativo del robottino verde è più utilizzato di tutti gli altri **sistemi operativi** messi insieme, e detiene la maggior parte del mercato. Nello specifico, la versione Android 5 Lollipop è la più attiva

2. **iOS** di Apple iPhone e iPad è al secondo posto con il 31,7%. Se escludiamo Android, questo sistema operativo è più utilizzato dei restanti sommati

3. **Windows Phone** è al terzo posto unito con Windows 10 Mobile. E' vero, ma ha solamente il 2,54% di share. Nonostante gli smartphone con il sistema operativo Microsoft siano molto all'avanguardia (si veda ad esempio Microsoft Lumia 950 e 950 XL con Continuum), non sta facendo le vendite sperate e non riesce a concorrere con Android e iOS

4. **Java ME:** il sistema operativo presente nella stragrande maggioranza dei vecchi cellulari GSM, viene al quarto posto con il 2,07%

5. **Synbian** era il sistema operativo più avanzato all'epoca dei vecchi cellulari, ed era presente sui dispositivi Nokia. Adesso è installato sull'1,4% dei cellulari ancora attivi. Una volta era Synbian il sistema operativo migliore, ma gli smartphone hanno causato letteralmente la sua morte

6. **BlackBerry OS**, che come suggerisce il nome è installato sugli smartphone della casa produttrice canadese (eccetto Priv) si attesta con l'1,17%

7. Al settimo posto il vecchio sistema operativo **Samsung Bada** con lo 0,04%

8. Infine tutti gli altri **sistemi operativi** hanno complessivamente lo 0,03%

I mobile OS dal 2000 a oggi

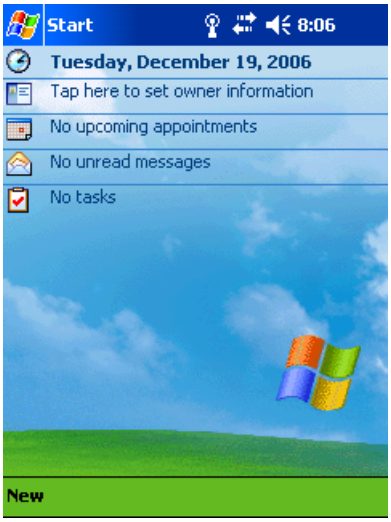
I primi mobile OS nascono nei primi anni del 2000:

· Microsoft, il 19 aprile 2000, lancia Pocket PC 2000, un vero e proprio computer palmare, con sistema operativo il nuovo Windows CE (Windows Embedded Compact). Esso è un sistema operativo real time sviluppato da Microsoft, a partire dal 1996, per dispositivi portatili (PDA, Palmari, Pocket PC), Smartphone e sistemi embedded. Come si intuisce dal nome, è un derivato della famiglia di sistemi operativi Windows, ma ha un kernel differente e non è quindi una semplice "riduzione". Le API e l'aspetto grafico sono comunque molto simili. Il termine "Windows CE" è in realtà il nome "tecnico" con il quale viene indicata la piattaforma generale di sviluppo di questo sistema operativo. Essendo "Windows CE" sufficientemente modulare e flessibile, sono state sviluppate delle specifiche versioni per dispositivi differenti. Tali specifiche versioni prendono il nome "commerciale" di "MS Handheld 3.0" (e 3.1), "MS Handheld 2000", "Microsoft Pocket PC 2000" (e 2002), "MS Smartphone 2002", tutta la serie Windows Mobile e Windows Phone 7.x. Tali varianti fanno tutte riferimento a specifiche evoluzioni della piattaforma di riferimento "Windows CE". Data la moltitudine di nomi non è raro che generi ambiguità, impiegando erroneamente in modo ambivalente i termini "Windows Mobile" o "Windows CE" e simili. Questo sistema operativo funziona anche con un netbook di nome Minimind (della Mindtech).

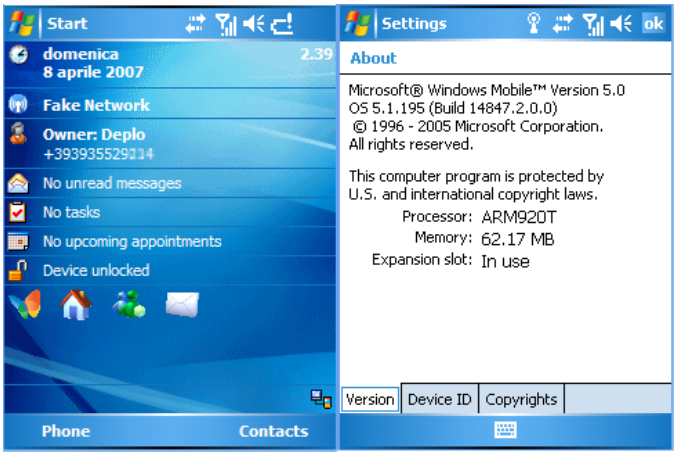
Questo sistema operativo viene anche utilizzato per i nuovi Salvatempo, e per alcune casse automatiche, dei supermercati e ipermercati Coop.

È utilizzato anche in alcuni navigatori GPS.

- Microsoft, il 23 giugno 2003, presenta Windows Mobile 2003, un sistema operativo basato sulle Application programming interface (Windows API). È molto simile al predecessore, però porta aggiornamenti notevoli: interfaccia di comunicazione sono state migliorate con la gestione del dispositivo Bluetooth. Che ha consentito di file Bluetooth raggiante, supporto auricolare Bluetooth e il supporto per Bluetooth aggiuntivo alle tastiere. Un'applicazione immagini con la visualizzazione, il ritaglio, e-mail, e il supporto è stato aggiunto raggiante. Miglioramenti multimediali incluso il supporto MIDI file come suonerie Phone Edition e Windows Media Player 9.0 con ottimizzazione streaming. Un gioco di puzzle con il titolo Jawbreaker è tra i programmi preinstallati.



- Microsoft, il 12 maggio 2005, rilascia Windows Mobile 5, un sistema operativo molto simile ai precedenti, ma anch'esso con alcuni aggiornamenti: nuova versione di Office era in bundle chiamato " Microsoft Office Mobile "con include PowerPoint Mobile, Excel Mobile con capacità grafica e Word Mobile con la possibilità di inserire tabelle e immagini. Gestione dei media e la riproduzione è stata potenziata con l'immagine e il pacchetto video, che convergevano la gestione di video e immagini e di Windows Media Player 10 Mobile. Tra le nuove caratteristiche hardware sono state migliorate Bluetooth di sostegno, di default QWERTY tastiera supporto e un'interfaccia di gestione per il Global Positioning System (GPS). I miglioramenti sono stati fatti per ActiveSync 4.2 con 15% di aumento della velocità di sincronizzazione. I clienti commerciali hanno beneficiato di un nuovo impianto di segnalazione di errore simile a quello presente nel desktop e server di Windows sistemi. Caller ID supporta ora le foto in modo che un utente può applicare un'immagine a ogni contatto per

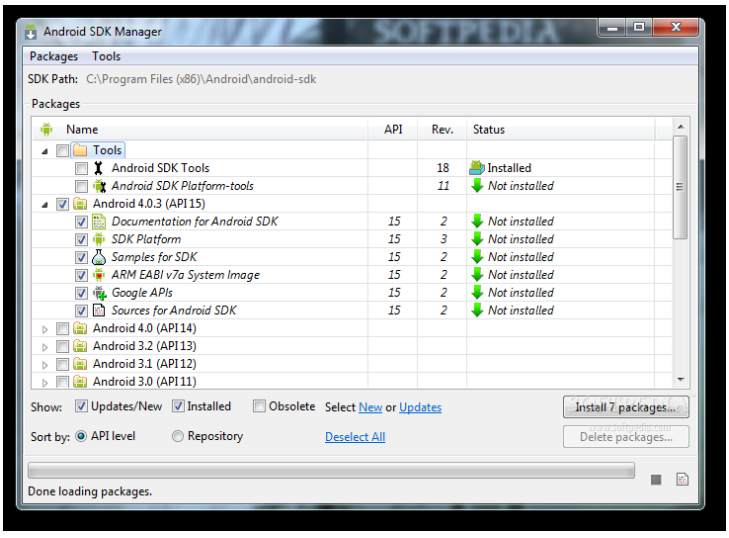


mostrare quando si riceve una chiamata. DirectShow è stata aggiunta in modo nativo.

Nel 2007 l'era del mobile cambia: entrano in gioco Google ed Apple con idee rivoluzionarie. Le novità sono le applicazioni, scaricabili da uno Store/Market, cosa già presente sui sistemi Linux per computer:

- Apple, il 29 giugno 2007, lancia la prima versione di iOS, inizialmente chiamato iPhone OS, con il primo iPhone EDGE. Non è mai stato dato un nome officiale alla prima versione; il settore marketing di Apple ha semplicemente dichiarato che l'iPhone installava una versione del sistema operativo desktop di Apple, macOS.

- Google, il 12 novembre 2007, rilascia un'anteprima dell'SDK (software development kit), ovvero un kit di sviluppo per software disponibili a tutti. Le app sono in genere sviluppate in linguaggio Java, nonostante siano disponibili altri ambienti di sviluppo.



- Google, il 9 febbraio 2009, lancia le prime versioni di Android, la 1.0 e la 1.1. Erano versioni non commerciali, infatti erano considerate come alpha e beta. Esse comprendevano il market, il browser, la gestione delle cartelle (creazione, cancellazione e ridenominazione), accesso ai servizi di posta elettronica e il supporto di reti wi-fi, fotocamere e le prime Google Apps per smartphone Android. Le prime release non avevano nomi specifici, ma venivano indicati in maniera più generale come Astro Boy e Bender, per poi essere sostituita da nomi di dolci.

Il 2009 ed il 2010 sono gli anni in cui Apple è il leader, sia per le innovazioni sia per le vendite. Android, però, segue con le stesse quote di mercato seppur leggermente inferiori:

- Apple, il 21 giugno 2010, lancia iOS 4.0 è la quarta versione del sistema operativo per dispositivi mobili iOS, sviluppato dalla Apple Inc. e successore di iPhone OS 3. È stato il primo aggiornamento a essere rinominato in "iOS", invece che "iPhone OS". Con la quarta versione di iOS, alcuni dispositivi non vengono più supportati ed è stato anche il primo aggiornamento gratis per iPod touch.

- Google, il 20 maggio 2010, rilascia la versione 2.2 di Android, anche conosciuta come Froyo. Con esso sono stati resi disponibili importanti aggiornamenti: nuovo kernel linux 2.6.32, nuovo compilatore JIT, V8 Engine per il JavaScript, Tethering Wi-fi Nativo per utilizzare il terminale come Hotspot Wireless, nuove Icone per la Home, Telefono (Sinistra) e Browser (Destra). Adobe Flash Player 10.1 e Adobe AIR Integrato. Possibilità di installare le apps sulla memoria SD, feature molto attesa dalla community mondiale. Aggiornamento automatico Over-the-Air delle Applicazioni. Nuove Api per gli sviluppatori, tra cui le OpenGL ES 2.0.

- Microsoft, il 21 ottobre 2010, lancia Windows Phone 7 a livello globale. Esso Si rivolgeva al mercato consumer invece che al mercato enterprise come il suo predecessore, abbandonando alcune caratteristiche in dotazione a Windows Mobile.[3] Era radicalmente diverso da tutte le precedenti versioni di Windows Mobile con le quali era incompatibile, ma supportava il multitouch, gli schermi capacitivi, aveva una nuova interfaccia grafica molto simile a quella di Zune HD e confermata nel successore Windows Phone 8, e riuniva in una sola piattaforma i contenuti di Xbox Live e Zune. Inoltre gestiva gli account di social network quali

Facebook e Twitter, e possedeva una nuova versione di Internet Explorer basata su Windows Internet Explorer 9.[4] Questa versione di Windows Phone conteneva un'edizione di Microsoft Office dalle funzionalità limitate e ottimizzata per gli schermi tattili, con Word, Excel, Powerpoint, OneNote e Sharepoint.

Dal 2010 fino ad oggi, i sistemi operativi mobile hanno subito diversi aggiornamenti: quasi tutti i nuovi smartphone hanno la possibilità di leggere le impronte digitali, alcuni addirittura la retina. L'unica differenza tra i precedenti smartphone e quelli odierni è l'hardware, che a sua volta riesce a reggere sistemi operativi più pesanti e complessi.

I migliori smartphone degli scorsi anni sono:

- iPhone 7 e iPhone 7 Plus, presentati il 7 settembre 2016. È il primo modello di iPhone in cui il tasto Home fisico non è più presente ma è stato sostituito con un "tasto virtuale" capace di offrire una risposta tattile grazie al nuovo Taptic Engine. iPhone 7 è stato rilasciato con la decima versione del sistema operativo di Apple, iOS 10. Esso porta alcune modifiche nella UI e aggiunge nuove funzioni.

- Samsung Galaxy S7 e Samsung Galaxy S7 Edge, presentati il 21 febbraio 2016 durante una conferenza stampa Samsung al Mobile World Congress 2016 ed è stato messo in commercio l'11 marzo in Europa e Nord America. Il Galaxy S7 monta Android 6.0.1 Marshmallow con personalizzazione dell'interfaccia Android di Samsung chiamata TouchWiz. Una nuova funzionalità è quella di mostrare l'orologio o altre informazioni come la data e il calendario a schermo spento chiamato "Always-On". Con l'introduzione di Android Marshmallow già dal momento del lancio e l'aumento della capacità della batteria, l'autonomia del telefono è incrementata rispetto al predecessore Samsung Galaxy S6 il quale aveva mostrato numerosi problemi in questo senso.

- Huawei P9 (Standard, Lite e Plus), distribuito agli inizi di aprile 2016. È il successore dello smartphone Huawei P8 ed ha un design simile al predecessore. Nella parte posteriore è presente un sensore di impronte digitali e una doppia fotocamera co-progettata con la nota azienda tedesca di materiale fotografico Leica, di cui una è esclusivamente "bianco e nero" e utilizzata parallelamente con la fotocamera RGB permette un'elevata resa cromatica e nei dettagli. Integra la versione Android 6.0 Marshmallow.

Cosa aspettarci dagli smartphone nel 2017

Dai rumors apparsi negli ultimi mesi, il 2017 potrebbe essere un anno veramente importante per gli smartphone. Dopo alcuni modelli abbastanza simili sotto il punto del design, Apple è decisa a rivoluzionare il proprio smartphone: l'iPhone 8 dovrebbe essere realizzato con un schermo OLED che coprirà la gran parte del device e con il tasto home che scomparirà per far posto a un lettore di impronte digitali nascosto nel display. Anche in casa Samsung si sta lavorando per presentare durante il Mobile World Congress il nuovo top di gamma dell'azienda coreana. Le uniche certezze riguardano il nuovo assistente personale che dovrà far concorrenza a Siri e, inoltre, il jack audio da 3,5mm sarà sostituito dalla porta USB type-C, la stessa utilizzata per ricaricare lo smartphone.

Ma Samsung e Apple non saranno le uniche ad avere le luci dei riflettori puntati addosso. Tra gli smartphone più attesi del 2017 ci sarà sicuramente il Huawei P10, chiamato a confermare quanto di buono fatto vedere negli ultimi anni, e il OnePlus 5 (secondo i bene informati, il numero quattro sarà saltato perché porterebbe sfortuna) pronto a stupire ancora una volta il mondo con un rapporto qualità-prezzo davvero imbattibile.

Fonti

1. Wikipedia
2. Ridble
3. Tech4d

DATABASE

Storia

Di Costantino Lorenza e Amelio Emanuele

Introduzione

Il termine base di dati o banca dati, indica un insieme di dati, omogeneo per contenuti e per formato, memorizzati in un elaborato elettronico e interrogabili via terminale utilizzando le chiavi di accesso previste.

Le informazioni contenute in database sono strutturate e collegate tra loro secondo un particolare modello logico scelto dal progettista . Gli utenti si interfacciano con le base dati attraverso i cosiddetti query language e grazie a particolari applicazioni software dedicati (DBMS).

I database non sono nati con l'avvento dei personal computer e neppure con i grossi mainframe loro predecessori, ma sono stati inventati molto tempo prima, in quanto un database è fondamentalmente una collezione di dati organizzati.

Essi sono strettamente associati ai computer poichè nella maggior parte delle situazioni i computer sono il sistema più veloce ed efficiente per gestire i dati, ed è per questo che il termine "database" è entrato a far parte del mondo informatico a partire dai primi anni '60.

Nel 1964 viene coniato il termine “data base”, l’idea di questo nuovo strumento nasce all’interno degli ambienti militari statunitensi e denota una collezione di dati condivisa dagli utilizzatori finali dei terminali. Nella seconda metà degli anni

’60, alcune società di prim’ordine avviano lo sviluppo di proprie soluzioni basate sul modello a rete (network).

In particolare è Charles Bachmann, ritenuto uno dei pionieri dei database, a progettare e guidare lo sviluppo di IDS (Integrated Data Store, network model), il primo DBMS.

Nel 1966 IBM avvia lo sviluppo dell’IMS (Information Management System), pensato specificamente per supportare il programma spaziale APOLLO e sviluppato per il mitico System/360. Nel 1981 sono apparsi sul mercato i primi sistemi commerciali e sono nati con lo scopo di superare le limitazioni dei modelli di database allora esistenti.

Il modello relazionale è stato introdotto alla fine degli anni'60 ed è diventato il più diffuso modello di database al mondo. L'inventore di questo modello è stato Edgar F, Codd, un ricercatore all IBM, e fece questa"scoperta" mentre stava cercando un modo per applicare alla teoria dei database regole matematiche per risolvere i problemi. Essendo egli stesso un matematico, credeva che dovesse esistere una branca della matematica in grado di risolvere i problemi di duplicazione dei dati, integrità e struttura delle informazioni che affliggevano i modelli gerarchico e reticolare cosi tanto in voga a quei tempi. Dopo anni di studi, nel 1970 presentò il suo nuovo modello di gestione relazionale dei dati, basandolo su due nuovi settori della matematica: la teoria degli insiemi e la logica dei predicati del primo ordine.

L'aggettivo "relazionale" deriva, dalla parola "relazione" che è un termine proprio della teoria degli insiemi.

Nel 1980 nasce Ashton-Tate uno sviluppatore di database, concorrente di Oracle.

Nel 1984 nasce Sybase considerato, insieme a Oracle e ad Ashton-Tate, uno dei tre grandi database relazionale.

Fonti

1. Wikipedia
2. Teoria e pratica dei database, Mondadori Informatica

Tipologia di Database

Di Costantino Lorenza e Amelio Emanuele

Database basati su mainframe

Prima dell'avvento dei mini e poi the personal computer, tutti i database del mondo erano ospitati nei primi "grandi" computer della storia, i mainframe, prevalentemente di IBM.

Database basati su file

Hanno fatto anche la loro comparsa i sistemi di database basati su file. Tali sistemi utilizzano file diversi per mantenere le diverse informazioni che costituiscono il database e vengono gestiti mediante il sistema ISAM (Index Sequential Access Method), sigla che spiega il meccanismo mediante il quale i dati vengono scritti e letti effettivamente sul rapporto fisico. Ancora utilizzati, rientrano in tale categoria prodotti come dBase, FoxPro, Paradox e Access.

DBMS

I DBMS (DataBase Management System), sistemi per la gestione delle basi di dati , rappresentano quanto di meglio offre la tecnologia per l'archiviazione di grosse quantità di dati. Un DBMS non è solo un sistema per archiviare o recuperare informazioni, ma fornisce anche meccanismi per conservare l'integrità dei dati, al contrario dei sistemi che utilizzano tecnologie come VSAM o ISAM, che hanno invece il difetto di non aver nessun controllo su come i dati vengono gestiti all'interno del database.
Le funzioni fornite da un DBMS sono:

- **Definizione della base di dati:** un DBMS deve permettere all'utente di definire le caratteristiche delle informazioni che costituiscono la base di dati e delle relazioni tra queste informazioni.
- **Interrogazione aggiornamento di dati:** un DBMS deve permettere

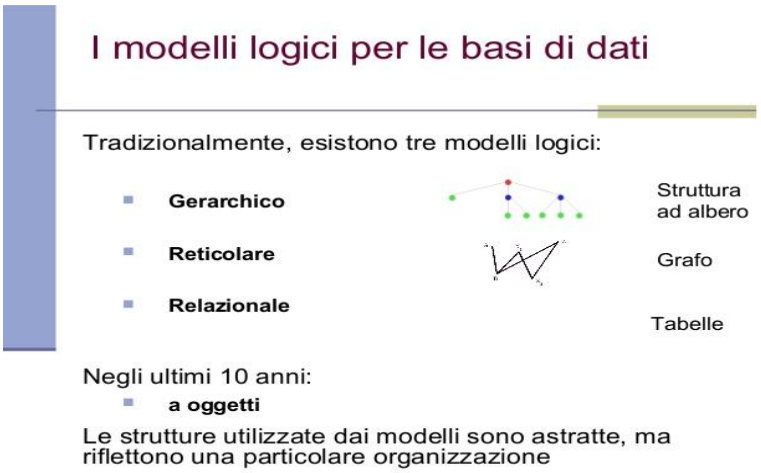
all'utente di selezionare le informazioni che vuole conoscere, tra tutte quelle memorizzate nel database, e consentirgli di aggiornarle, con inserimenti, modifiche e cancellazioni.

- **Indipendenza dei dati**: un DBMS deve poter presentare i dati in termini astratti, ossia, l'utente non deve necessariamente sapere come e dove i dati sono memorizzati nel laboratorio.
- **Sicurezza dei dati:** il sistema deve controllare che l'utente, che richiede una certa informazione, abbia l'autorizzazione e sia abilitato a farlo. Deve pertanto concedere l'accesso alle informazioni solamente agli utenti autorizzati e al contrario negarla a quelli non autorizzati.
- **Integrità dei dati**: il DBMS deve garantire l'integrità dei dati. Il sistema dovrà consentire di inserire e gestire i vincoli di consistenza, ossia le proprietà che devono essere soddisfatte dai dati del database, ed essere in grado di controllare se i dati memorizzati soddisfino detti vincoli.
- **Sincronizzazione dei dati:** due o più applicazioni possono accedere simultaneamente ai dati perciò, magari per un aggiornamento, potrebbe accadere che i dati non siano consistenti a causa della scrittura quasi contemporanea da parte di più utenti. Il DBMS deve garantire la corretta esecuzione delle operazioni di aggiornamento che possono avvenire simultaneamente e fornire la protezione contro problematiche di questo tipo.
- **Protezione dei guasti e ripristino delle informazioni:** se durante l'utilizzo di un DBMS si verificano errori dovuti a malfunzionamenti dell'hardware o del software il DBMS deve fornire la possibilità di fare copie e di ricostruire il database dopo il verificarsi dell'errore.

I tipi di database

Nello sviluppo della teoria dei database, i modelli che si sono avvicendati nello scenario mondiale sono: quello gerarchico, reticolare, relazionale e a oggetti.

La storia di ogni modello è legata alle caratteristiche della macchina su cui il database doveva funzionare e quindi ogni modello è ottimizzato per certe specifiche esigenze.



Il modello gerarchico

Il modello gerarchico è il primo che si afferma nella storia del mercato dell'informatica.

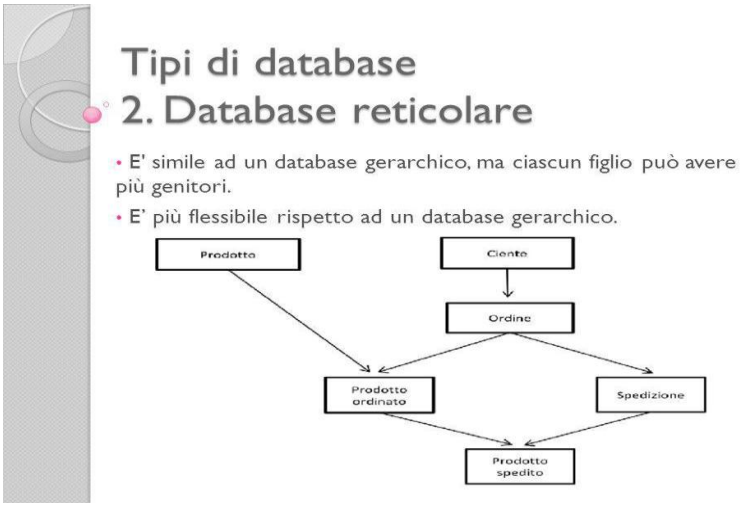
Esso è indicato nelle situazioni in cui i dati sono rappresentati secondo uno schema ad albero, infatti una struttura dati gerarchica è composta da un insieme ordinato di istanze dello stesso albero.

Il tipico albero che forma il database è composto da un unico record che rappresenta la radice e tanti sottoalberi di livello inferiore. Ogni sottoalbero è a sua volta formato da un singolo record radice, da altri sottoalberi e via dicendo.

Il modello gerarchico è molto adatto e utilizzato in tutti gli scenari in cui sono presenti relazioni uno a molti tra i vari record, ed è altrettanto evidente che questo modello ha importanti limiti sia di carattere strutturale sia di altra natura.

Il modello reticolare

Il modello reticolare permette la rappresentazione di relazioni molti a molti in modo più semplice rispetto al modello gerarchico.



La struttura che utilizzata non è più un albero ma un grafo, che rende molto più complicata la realizzazione sia della parte di gestione dei dati sia di quella di programmazione per l'accesso agli stessi.

Modello relazionale

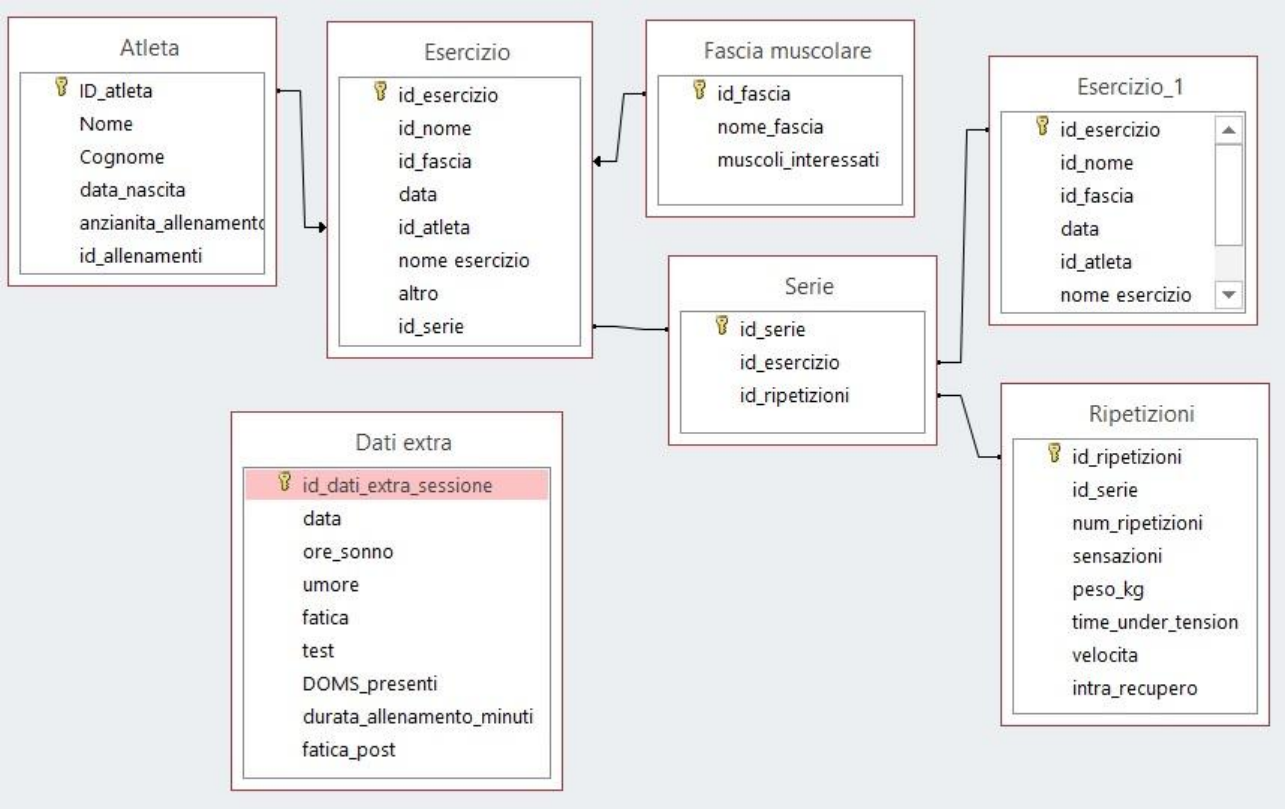
Un database relazionale è un insieme direlazioni di grado diverso, variabil nel tempo, che godono delle seguenti proprietà:

- Ogni riga rappresenta un elemento distinto della relazione e tutte le righe devono essere diverse tra loro.
- Ogni colonna, individuata da un nome di attributo, deve contenere dati omogenei.
- Non esiste nessun tipo di precedenza e di ordinamento né tra le righe né tra le colonne.

Un database relazionale memorizza i dati in relazioni che l'utente percepisce come tabelle, e ogni relazione è composta da tuple(record) e attributi (campi).

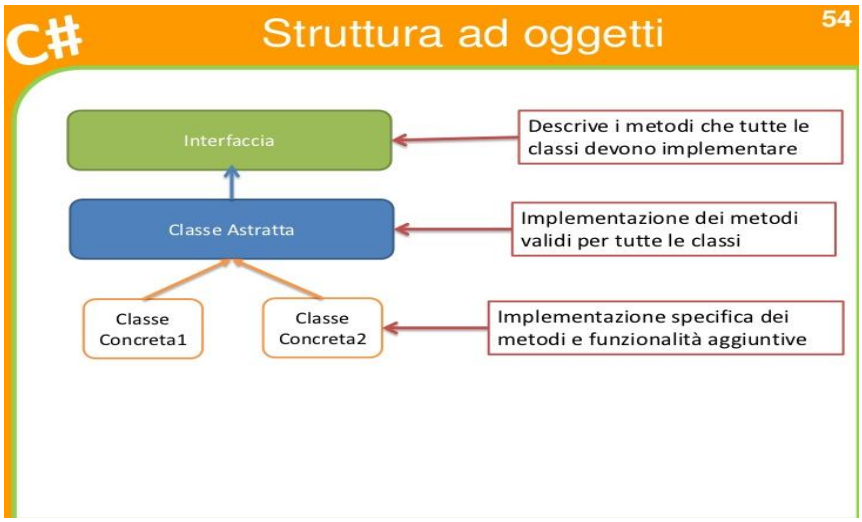
Altre due caratteristiche sono che l'ordine fisico di memorizzazione dei record non è importante e che ogni record è identificato da un campo che contiene un valore univoco. Queste due caratteristiche permettono che i dati possano esistere indipendentemente da come vengano memorizzati fisicamente al'interno del computer. L'utente non deve necessariamente conoscere la loro posizione fisica, al contrario di quanto avviene con il modello gerarchico e quello reticolare. Inoltre, il modello relazionale offre dei vantaggi rispetto agli altri modelli tra cui:

- **Integrità:** è incorporata nel database a vari livelli. A livello di campo per garantire l'accuratezza dei dati; a livello di tabella, per assicurare che non esistano record duplicati o privi di chiave univoca; a livello di relazione, per garantire che le relazioni tra due tabelle siano valide.
- **Indipendenza logica e fisica dei dati dall'applicazione:** questo garantisce che nessuna modifica a livello fisico o logico del database possa ripercuotersi sull'applicazione che utilizza quel database.
- **Facilità di estrazione dei dati:** i dati possono essere recuperati o da una tabella o da più tabelle all'interno di un database in numerosi modi.



Modello a oggetti

Un modello di Base di dati a oggetti o *base di dati orientata agli oggetti o* megio conosciuto come database a oggetti **ODBMS (***Object Database Management System*) è un modello di base di dati in cui l'informazione è rappresentata in forma di oggetti come nei linguaggi di programmazione ad oggetti.



Gli oggetti che compongono i database

Un Database (SQL server, Oracle, DB2 ecc) contiene molti oggetti tra cui:

- l'istanza del server;
- Il Database
- Le tabelle
- Gli indici
- I vincoli

L'istanza del server è: il gestore di sistema del Database, un programa in esecuzione nella macchina server ed è in grado di fornire utti i servizi che possono essere utilizzati all'interno del database.

Il database è l'entità per eccellenza che si può trovare in un'istanza. In alcune implementazioni possono esistere più database all'interno di una singola istanza del server, mentre in altri, ogni istanza ammette l'uso di un singolo database.

Le tabelle sono l'oggetto più importante presente all'interno del database e tutti i dati sono memorizzati in esse. Ogni tabella è composta da dati del dominio (colonna) e dati dell'entità (righe).

Gli indici sono altri oggetti che compongono l'interno di una tabella e sono composti da una chiave che può essere ordinata in senso crescente o decrescente. Gli indici servono per ricercare in maniera veloce le informazioni all'interno della tabella.

Fonti

1. Wikipedia
2. Teoria e pratica dei database, Mondadori Informatica

E-Commerce

Storia

Di Pasquale Di Maio e Alfredo Costa

Cos'è un e-commerce

E-Commerce è l'acronimo di Electronic Commerce (commercio elettronico) e consiste nella presentazione, vendita e gestione di prodotti utilizzando strumenti elettronici, in particolare attraverso siti internet. Avere un sito di e-commerce, o implementare la possibilità di fare e pagare acquisti sul tuo sito tramite carta di credito, offre la possibilità di estendere a livello mondiale i potenziali clienti, facendo crescere così il proprio business.

L'evoluzione, dal 1982 ai giorni nostri

Il vero primo e-commerce nacque nel 1982 in Francia in seguito alla nascita del Minitel, una rete commerciale promossa dall'azienda di poste e telecomunicazioni dello stato che funzionava via modem utilizzando il sistema videotext. L'e-commerce come lo conosciamo noi, dal quale poi si svilupparono le transazioni commerciali online, invece, nacque con l'EDI (Electronic Data Interchange), diffuso già dal 1970 e diventato standard nel 1984. L'EDI era il primo servizio elettronico

attraverso il quale si trasferivano documenti come ordini d'acquisto o fatture in formato elettronico, utilizzato da imprese di grandi dimensioni attraverso reti di telecomunicazione private. L'integrazione del sistema EDI alla rete internet, ha portato alla nascita di un sistema flessibile e più vicino allo standard di e-commerce. Fu nel 1994 che Netscape lanciò i suoi servizi di browser di navigazione dando la possibilità di navigare in modo semplice sul web e incorporando la navigazione con gli standard di sicurezza per le transazioni online, in modo da non scoraggiare i potenziali utilizzatori. La nascita dei browser intuitivi fu la spinta decisiva verso la nascita di veri e propri siti internet dedicati all'e-commerce. Grazie a ciò, nel 1995 nacquero i primi due portali americani dedicati agli acquisti online: Amazon ed E-bay. Il loro avvio fu lento poiché gli acquisti non prevedevano ancora le aste e, soprattutto, non era ancora disponibile una connessione ad alta velocità. Verso il 1999 la diffusione della linea ADSL ad alta velocità ha dato il definitivo slancio allo shopping online. Nel 2011, in base alla ricerca di mercato di Netcomm, dei 25 milioni di italiani presenti sul web, 12,5 milioni hanno acquistato on-line almeno una volta nella vita, 8,8 milioni avevano comprato nei tre mesi precedenti all'indagine e ben 5,4 milioni sono coloro per i quali gli acquisti in rete sono diventati ormai un abitudine. Ma il dato più interessante che è stato fornito è la stima del numero di persone che si appresterebbero a comprare via internet per la prima volta: 1,3 milioni, una cifra che conferma la notevole crescita del fenomeno.

I vantaggi dell'e-commerce

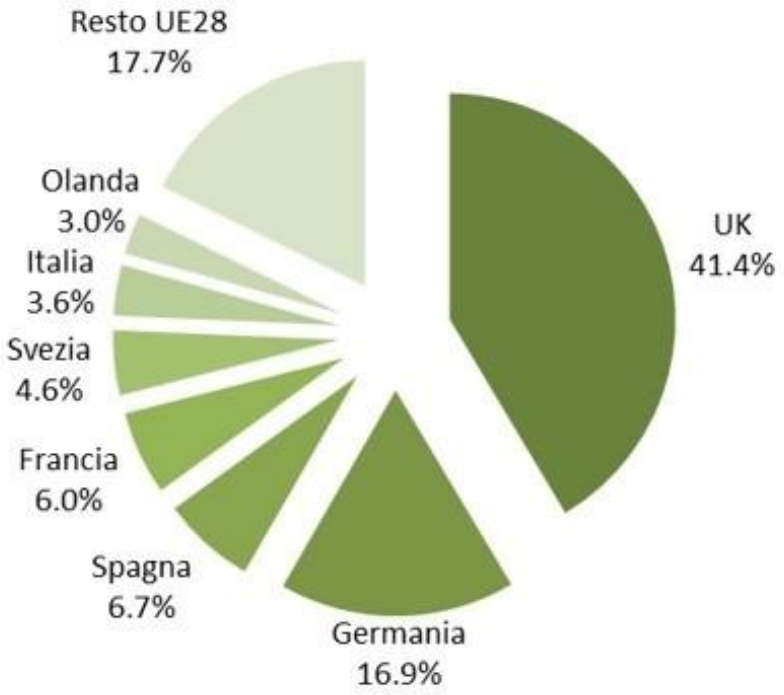
La vendita online è un contesto aziendale che sta attirando l'attenzione di molti imprenditori perché permette un rapporto diretto con il cliente, indipendenza da fornitori e non permette pagamenti post consegna per evidenti ragioni burocratiche. Le aziende oggi sono in enorme difficoltà per i pagamenti, tante volte perché proprio non arrivano e non ci sono soluzioni per riprenderli ma, non da meno, perché quelli che arrivano sono in estremo ritardo. Il mercato si sta "girando", l'offerta supera di molto la domanda, la concorrenza è ovunque e anche i grandi brand cominciano l'avventura del proporre in modo diretto i prodotti con forti sconti sul listino e con estrema convenienza proprio per il taglio degli intermediari. Il sito e-commerce diventa così una fonte di speranza, perché a tutti gli effetti non ha limiti se non umani, si vende molto, si incassa subito e si hanno

maggiori profitti. Gli aspetti da considerare e sapere di un sito e-commerce sono molti ma ci preme porre l'attenzione sullo step iniziale, quello concettuale, la fase in cui si pensa di fare un sito e-commerce perché fin da subito serve avere chiaro un passaggio: un sito e-commerce costa e deve essere funzionale. Una medio-piccola azienda in 5 anni investe almeno 40 mila euro e questa verità, per quanto scomoda, deve essere chiaramente capita prima di partire per evitare insofferenze e lavori sommari che non porteranno risultati e saranno di intralcio all'attività. Primo costo da sostenere è il tempo, che tradotto in soldi sono ore che il titolare toglie all'azienda e, se consideriamo che il lavoro di un titolare può essere fatto da almeno due dipendenti, capiamo che con estrema facilità arriviamo a spendere questi 40 mila euro anche in meno di 5 anni. Il tempo, sembra scontato, ma è indispensabile, serve studiare le descrizioni dei prodotti fianco a fianco con l'agenzia web che si occupa della stesura dei testi e serve seguire l'andamento sia in ottica vendite, ma soprattutto in ottica accessi e aspettative. Altro costo importante è l'aspetto tecnico, che deve essere fatto su misura e deve essere studiato nei minimi dettagli per agevolare le visite dei clienti**.** È importante il connubio tecnica/proiezione strategica perché il sito è un insieme di cose, non una cosa. Possiamo pensare ad un'area riservata, possiamo pensare a gestire le vendite con la registrazione o meno dei clienti, in base al numero di acquisti che supponiamo possano fare in un anno, possiamo valutare una newsletter e comunque valutare come integrare altre forme di comunicazione che fino a oggi sono state l'asse portante del nostro piano marketing.

E-Commerce in Italia

Gli acquisti online crescono in Italia a doppia cifra dal 2009, superando quota 13 miliardi a fine 2014. In tre anni il numero di acquirenti è passato da 9 a oltre 16 milioni, ma solo il 4% delle imprese italiane vende online. Il potenziale del Made in Italy è totalmente inespresso a livello internazionale, soprattutto considerando che nel mondo la popolazione che compra sulla rete è costituita da 1,2 miliardi di persone. Se acquistare e vendere beni e servizi tramite il web è divenuta oramai una pratica di uso comune in molti paesi, in Italia l'e-commerce rimane ancora su una scala molto contenuta. Come emerge dal Rapporto sull'e-commerce 2016 elaborato da BEM Research, il valore del commercio elettronico tra imprese e consumatori è stimabile in Italia, secondo i dati relativi al 2015, in circa 21

miliardi di euro. Rispetto al complesso del mercato europeo, che raggiunge una dimensione di poco meno di 600 miliardi di euro, l'e-commerce italiano è pari ad appena il 3,6%, contro una quota dei consumi delle famiglie italiane, effettuati attraverso tutti i canali di acquisto possibili, pari al 12%.



Problematiche del commercio elettronico

Anche se un fornitore di beni e servizi di Commercio Elettronico seguisse i "fattori chiave" per realizzare una strategia di vendita in linea, possono tuttavia sorgere ugualmente delle difficoltà. Tra le principali troviamo:

- Difetti di comprensione del comportamento della clientela, vale a dire come e perché acquistano un certo prodotto. Se i produttori e i venditori non sono in grado di cogliere le abitudini di acquisto dei consumatori, come pure le aspettative e le motivazioni, anche un prodotto famoso può non raggiungere i target di vendita prefissati. Il commercio elettronico, per rispondere a tale inconveniente potrebbe avviare delle ricerche di mercato più mirate.
- Mancanza di analisi dello scenario concorrenziale. È possibile disporre delle capacità tecniche per realizzare un'attività di vendita di libri in rete, ma potrebbe mancare la volontà per competere con siti specializzati nella vendita di libri online.

- Incapacità di prevedere le reazioni nell'ambiente in cui opera l'impresa. I concorrenti potrebbero introdurre marchi in concorrenza con il nostro o potrebbero realizzare dei siti web analoghi per farci concorrenza. Questo, potrebbe portare ad ampliare i servizi offerti, far scoppiare una guerra di prezzi ed il governo non rimarrà di certo a guardare. Per evitare queste conseguenze è consigliabile analizzare la concorrenza, i settori industriali e i mercati coinvolti, proprio come si farebbe nel caso di un'attività tradizionale.
- Sovrastima delle competenze aziendali. Non è possibile sapere se i dipendenti, il sistema hardware, i software e i flussi di informazione riusciranno a padroneggiare la strategia adottata; come non è possibile sapere se i negozianti sono riusciti a formare adeguatamente i propri dipendenti e a sviluppare le competenze necessarie. Queste tematiche possono rendere necessarie una pianificazione delle risorse maggiormente dettagliata e una formazione dei dipendenti più estesa.
- Mancanza di coordinazione. Se i controlli non bastano, è possibile cambiarli adottando una struttura organizzativa maggiormente affidabile e lineare, anche se non è detto che questo cambiamento permetta di raggiungere un migliore coordinamento interno.
- Incapacità nell'assicurarsi l'impegno dei vertici aziendali. Spesso la conseguenza principale si traduce nell'impossibilità di raggiungere un determinato obiettivo societario a causa delle scarse risorse. Viene consigliato di coinvolgere fin dall'inizio i vertici aziendali nella nuova avventura del commercio elettronico.
- Incapacità nell'assicurarsi l'impegno da parte dei dipendenti. Se i progettisti non traducono in modo chiaro la loro strategia ai sottoposti, oppure non riescono a delineare loro il quadro generale in cui si troveranno a operare, un possibile rimedio può essere quello di offrire un percorso di formazione dedicato, come pure di fissare uno schema di incentivi ai dipendenti.
- Sottovalutazione dei tempi richiesti per il raggiungimento degli obiettivi aziendali. La realizzazione di un'impresa di e-commerce può richiedere un considerevole dispendio di tempo e denaro, e l'incapacità di comprendere la giusta sequenza dei processi imprenditoriali e la tempistica relativa a tali

operazioni può portare a rilevanti aumenti dei costi, rispetto a quanto preventivato. La capacità di generare profitti può essere sacrificata per raggiungere una determinata quota di mercato.

- Incapacità di rispettare la pianificazione dei tempi. Una scarsa verifica del rispetto degli obiettivi fissati inizialmente, come pure un ridotto controllo della performance aziendale rispetto a quanto ipotizzato in fase di pianificazione, possono far sorgere delle difficoltà nella conduzione aziendale. È possibile risolvere questi inconvenienti con dei tipici strumenti di gestione aziendale: benchmarks (indicatori dell'attività dei concorrenti presi a riferimento), traguardi interni di performance, analisi della variazione degli indicatori aziendali, istituzione di penalizzazioni per il conseguimento di performance negativa o, viceversa, ricompense per il raggiungimento di obiettivi aziendali, e, infine, misure per riallineare l'attività aziendale.
- Mancanza di ottimizzazione. Un e-commerce ha bisogno di un monitoraggio continuo per valutare l'impatto che ha sui motori di ricerca e sui consumatori in modo da essere perfezionato costantemente. Inoltre, Internet è in continuo aggiornamento: si deve essere sempre all'avanguardia e al passo con le nuove tecniche per non fallire.

Fonti

1. https://www.easynolo.it/easynolo/ecommerce/mondo_ecommerce/cosa_e_ecommerce.jsp?p=com_00
2. http://www.themarketingfreaks.com/2014/03/la-storia-del-e-commerce-levoluzione-dal-1982-a-giorni-nostri/
3. http://amdweb.it/curiosita-e-strategie-di-un-sito-ecommerce
4. http://www.rainews.it/dl/rainews/media/evoluzione-e-commerce-in-Italia-81af0311-7a13-47a3-bfe5-b888b3cc4d70.html
5. https://it.wikipedia.org/wiki/Commercio_elettronico

Frodi online

Di Koci Alessia e Nanci Erika

Con l'avvento dell'e-commerce e del contante digitale le transazioni monetarie, oltre ad essere diventate più semplici, sono diventate meno sicure. Spesso ,quando si effettua un acquisto, non si pensa alle possibili truffe e frodi nelle quali si potrebbe incorrere. Quello delle frodi online è un tema molto caldo specialmente per il numero sempre in aumento di truffe.

Protocolli per le transazioni sicure

Per cercare di rendere più sicure le transazioni online si utilizzano i seguenti protocolli:

- SSL (Secure Sockets Layer)
  - Stabilisce un canale di comunicazione sicuro tra un browser ed un server
  - La componente fondamentale di una connessione protetta dal SSL è rappresentata dal SSL Handshake Protocol caratterizzato da una fase di negoziazione tra le parti e successivamente alla fase di trasferimento dei dati. Se il server non può essere autenticato, la connessione non può essere stabilita.
- SET (Secure Electronic Transaction)
  - Il titolare della carta di credito SET riceve dalla banca emittente un certificato criptato che permette di identificare l'utente. Il titolare registra sul suo computer il certificato e, nel momento in cui effettua un pagamento via internet, dà la possibilità alla banca di certificare al venditore se chi sta utilizzando la carta sia l'effettivo titolare della stessa.
  - La banca si sostituisce al venditore nell'onere di verificare la corrispondenza tra la firma di chi effettua il pagamento e la firma apposta sul retro della carta di credito.

- Protegge l'identità delle parti coinvolte nella transazione attraverso la firma digitale che permette di verificare il mittente ed il destinatario.

- HTTPS
  - Protocollo di livello applicativo utilizzato per aggiungere sicurezza alle pagine del WWW in modo tale da rendere possibili applicazioni quali il commercio elettronico.
  - È ottenuto abbinando SSL al normale standard HTTP.
  - Garantisce l'invio delle informazioni personali sottoforma di pacchetti criptati.
  - Gli accessi vengono effettuati sulla porta 443 e tra il protocollo TCP e HTTP si interpone un livello di crittografia/autenticazione.
  - assicura una buona protezione contro attacchi del tipo man in the middle(attacco dell'uomo in mezzo) nei quali l'attaccante è in grado di leggere, inserire o modificare a piacere, messaggi tra due parti senza che nessuna delle due sia in grado di sapere se il collegamento che li unisce reciprocamente sia stato effettivamente compromesso da una terza parte. (Esiste una tecnica molto nota, chiamata ARP poisoning che rende gli attacchi "man in the middle" facilmente fattibili ingannando i PC presenti su una LAN facendogli pensare che una certa macchina, controllata dal truffatore, funzioni da gateway locale inducendo tutti gli utenti della LAN ad inviare a loro insaputa tutto il traffico Internet).

Tecniche di attacco online

Per commettere una truffa o una frode, esistono diverse tecniche più o meno semplici da utilizzare. Tra le tecniche più diffuse abbiamo:

- Phishing (utilizzata per il furto di identità): si basa sull'utilizzo delle comunicazioni elettroniche, specie messaggi di posta elettronica falsi che hanno lo scopo di reperire credenziali dell'utente direttamente o attraverso link di siti fittizi. Suo sostituto è il Vishing che si basa sulla comunicazione vocale come mezzo per spillare info sensibili.

- Negazione del servizio (DoS):è condotto attraverso reti (botnet) formate da alcuni computer detti zombie che ad sovraccaricano un sito internet connettendosi contemporaneamente rendendolo inutilizzabile. In alcuni casi i computer attaccanti sono migliaia. (pratica utilizzata per recuperare credenziali di accesso e numero di carte di credito degli utenti che si collegano)
- Keylogging : intercetta tutto ciò che un utente digita sulla tastiera del proprio computer. I keylogger possono essere hardware (collegati al cavo di comunicazione tra la tastiera ed il computer o all'interno della tastiera) o software(programmi che controllano e salvano la sequenza di tasti che viene digitata da un utente).
- Firesheep: è un add-on per Firefox in grado di rendere estremamente facile il furto di identità. Cattura le credenziali di accesso degli utenti presenti su una stessa rete. Sfrutta alcuni bug presenti in alcuni siti web come Facebook, Amazon, Twitter.

Ingegneria sociale

L'ingegneria sociale consiste nel persuadere e convincere le persone a rivelare informazioni importanti senza che essi se ne accorgano.

Le fasi di questo tipo di truffa sono 4:

1) bisogna cercare un' obiettivo, preferibilmente un'azienda con un grande numero di dipendenti in modo che nessuno possa conoscere tutti i dipendenti;

2) gli impiegati più abbindolabili sono le segretarie e i neoassunti che farebbero qualsiasi cosa pur di soddisfare un presunto capo reparto;

3) dopo aver scelto la vittima bisogna instaurare con quest'ultima una relazione in modo tale che la richiesta di dati sensibili non desti sospetto;

4) una volta instaurata una relazione di

fiducia con la vittima si possono ottenere le informazioni desiderate.

L'ingegneria umana può essere di tre tipi:

- umana: È la tecnica migliore, ma anche la più difficile. L'attaccante deve avere doti di improvvisazione, esser loquace e riuscire ad instaurare un rapporto di fiducia con uno sconosciuto, il quale non si fiderà immediatamente. Altri metodi possono essere:
  - intercettare le comunicazioni
  - shoulder surfing (spiare la digitazione di una tastiera per ricavarne informazioni)
  - dumpster diving (cercare nella spazzatura alla ricerca di informazioni utili)

- digitale: Si basa sull'utilizzo del computer. Viene utilizzata per inviare phishing, fake mail (in cui viene chiesto di cliccare su un link e seguire alcune istruzioni) e finestre pop-up in cui si viene avvisati che si hanno vinto un milione di euro, si è il milionesimo cliente, che siamo i prescelti, etc. etc. (per evitarle basta installare un buon adblocker).
- Mobile: Negli ultimi tempi, gli smartphone sono diventati perennemente presenti nella vita di ogni persona. Con un SMS (e link in esso) è possibile installare un malware all'interno del dispositivo, con un app finta è possibile rubare tutti i dati del proprietario (es. l'app che simula i fulmini su Google Play, chiede anche l'accesso alla fotocamera, scaricata da +500.000 persone).

Casi reali di truffe

- Hack EMV

Un giovane studente dell'Università di Cambridge (Omar S. Choudary), presentando una tesi con tanto di video dimostrativo, ha mostrato come sia possibile utilizzare una carta di credito rubata sfruttando le falle presenti nella tecnologia "chip & pin" (basata sul protocollo EMV). La Smart Card Detective

fornisce in tempo reale alcune informazioni sulla transazione, permettendo al titolare della carta di controllare che la somma visualizzata sul POS di un dato esercizio commerciale sia effettivamente quella addebitatagli e che il terminale non sia stato alterato.

- Truffa su Facebook

L' applicazione che permette di giocare online a Twilight Breaking Dawn è una truffa. Iniziando a giocare, viene automaticamente deciso che il gioco "piace", esponendo al pericolo anche tutti gli amici. In più viene permesso a "terze parti" di accedere al vostro account e sarà fornito anche un sondaggio "malevolo" da compilare.

- Siti online fasulli

Un 18enne che vive in provincia di Bergamo, di nome Stefano, ha pubblicato su un sito si acquisti online un annuncio per la vendita del suo motorino e il giorno dopo essersi registrato il sito gli aveva inviato una mail che lo informava del fatto che il suo account era stato violato e che doveva fare clic sull'URL della mail per tornare all'account del sito. Stefano ha seguito le indicazioni e ha creato nuovamente l'account. Due giorni dopo Stefano ha trovato un acquirente per la sua moto e in breve tempo ha ricevuto il denaro pattuito e per questo ha rimosso l'annuncio. Ciò nonostante il sito ha inviato a Stefano una mail che lo informava del fatto che aveva un articolo in vendita. Controllando sul sito in questione Stefano ha scoperto che il suo motorino risultava ancora in vendita ma l'indirizzo e-mail per il contatto non era il suo nonostante fosse molto simile. Preoccupato, Stefano si rivolge al fratello Carlo e, insieme, hanno contattato il venditore del motorino fingendo di essere interessati all'acquisto hanno ricevuto da lui stesso tutte le indicazioni per la spedizione dei soldi, i suoi dati e l'indirizzo di residenza. I due ragazzi hanno denunciato l'accaduto a un loro parente impiegato nella polizia postale e in breve

tempo il truffatore è stato rintracciato. Stefano è stato ingannato nel momento in cui era entrato nel sito per ricreare il suo account apparentemente violato: in realtà l'URL che Stefano aveva usato portava a una copia del sito originale e da questa pagina web i truffatori hanno potuto ottenere le sue credenziali.

Ruolo della polizia postale

Come si può capire da questa storia, se si è vittima di truffe è necessario denunciare l'accaduto alla polizia postale che si occupa dei crimini informatici. È proprio sull'homepage del sito della Polizia Postale che si legge questo:

"le nuove frontiere del commercio e della circolazione di denaro impongono un puntuale monitoraggio delle risorse tecnologiche correlate con la finalità di garantirne la sicurezza."

La polizia postale, dunque, si occupa in modo attento della circolazione di denaro che avviene in rete e per farlo si avvale dell'aiuto degli Uffici di Polizia stranieri per estendere il monitoraggio anche all'estero, proprio come scritto sul sito web della Polizia Postale:

"pilastro fondamentale della divisione operativa è la sezione dedicata alle collaborazioni internazionali impegnata con omologhi Uffici di Polizia stranieri nel contrasto al Cybercrime"

Si potrebbe dunque pensare che la polizia postale si occupi in modo efficace dei suddetti crimini ma non tutti la pensano così, come si intende dal commento lasciato da un utente di una pagina web:

~~Massimo~~

Membro

In realtà questo è solo un piccolo caso: la vera sorpresa è che la Polizia se ne sia occupata. Le tentate truffe via web sono un numero enorme: solo oggi ho ricevuto una decine di false fatture di tutti i tipi, che mi invitavano ad aprire file zippati. Di questi sembra che nessuno se ne preoccupi, eppure la diffusione di virus provoca danni anche maggiori delle false vendite. Come pure innumerevoli sono le false mail di banche note.

Avete mai provato a rivolgervi alla polizia postale? E' come un muro di gomma. Non accettano la segnalazione via telefono o mai, anche se corredata da copia della mail truffa: vi chiedono di andare presso di loro a fare la denuncia. Questo è per me un modo indiretto per dirvi di pensare ai fatti vostri. Se proprio vi mettete in testa di andare a fare la denuncia, alla fine avete perso 2 ore per sentirvi dire che i delinquenti non si possono prendere perché agiscono dall'estero: come se non si potesse sapere da dove viene la mail e fare in modo di bloccare la fonte. Evidentemente l'Interpol e la collaborazione delle polizie di vari paesi è solo una fiction cinematografica inventata da Spielberg.

Il commento di questo utente è scritto in seguito alla pubblicazione sul sito webnews.it che dice le seguenti parole:

"Importante operazione della Polizia Postale italiana che ha identificato e bloccato 49 siti di eCommerce al cui interno si nascondeva una colossale truffa"

Non è chiaro, dunque, quale sia il ruolo reale della Polizia Postale, fatto sta che ha effettivamente ottenuto dei risultati in quanto a frodi online.

Guida per acquistare in rete sicuri

Data la scarsa fiducia che gli utenti del web ripongono nella polizia postale, è necessario stare attenti a ciò che si fa e ad ogni singolo dettaglio. Per questo il sito Repubblica.it ha pensato di pubblicare una guida per tutti gli utenti con consigli e suggerimenti da seguire durante la navigazione in internet. Le regole da seguire per una navigazione sicura sono le seguenti:

- Utilizzare software e browser completi e aggiornati. Il primo passo per acquistare in sicurezza è avere sempre un buon antivirus aggiornato all'ultima versione sul proprio dispositivo informatico. Gli ultimi sistemi antivirus danno protezione anche nella scelta degli acquisti su Internet. Per una maggiore sicurezza online, inoltre, è necessario aggiornare all'ultima versione disponibile il browser utilizzato per navigare perché ogni giorno nuove minacce possono renderlo vulnerabile.

- Dare la preferenza a siti certificati o ufficiali. In rete è possibile trovare ottime occasioni ma quando un'offerta si presenta troppo conveniente rispetto all'effettivo prezzo di mercato del prodotto che si intende acquistare, allora è meglio verificare su altri siti. Potrebbe essere un falso o rivelarsi una truffa. Meglio scegliere negozi online di grandi catene già note perché oltre a offrire sicurezza in termini di pagamento sono affidabili anche per quanto riguarda l'assistenza e la garanzia sul prodotto acquistato e sulla spedizione dello stesso. In caso di siti poco conosciuti si può controllare la presenza di certificati di sicurezza che permettono di validare l'affidabilità del sito web.

- Dietro all'indirizzo di un sito deve esserci un vero negozio. Prima di completare l'acquisto verificare che il sito sia fornito di riferimenti quali un numero di partiva Iva, un numero di telefono fisso, un indirizzo fisico e ulteriori dati per contattare l'azienda. Un sito privo di tali dati probabilmente non vuole essere rintracciabile e potrebbe avere qualcosa da nascondere. I dati fiscali sono facilmente verificabili sul sito istituzionale dell'Agenzia delle Entrate.

- Leggere sempre i commenti e i feedback di altri acquirenti. Prima di passare all'acquisto del prodotto scelto è buona norma leggere i 'feedback' pubblicati dagli altri utenti del sito. Anche le informazioni sull'attendibilità

attraverso i motori di ricerca, sui forum o sui social sono utilissime. Le 'voci' su un sito truffaldino circolano velocemente online.

- Su smartphone o tablet utilizzare le app ufficiali dei negozi online. Se si sceglie di acquistare da grandi negozi online, il consiglio è quello di utilizzare le app ufficiali dei relativi negozi per completare l'acquisto. Questo semplice accorgimento permette di evitare i rischi di 'essere indirizzati' su siti truffaldini o siti clone che potrebbero catturare i dati finanziari e personali inseriti per completare l'acquisto.

- Utilizzare soprattutto carte di credito ricaricabili. Per completare una transazione d'acquisto sono indispensabili pochi dati come numero di carta, data di scadenza della carta e indirizzo per la spedizione della merce. Se un venditore chiede ulteriori dati probabilmente vuole assumere informazioni personali che, in quanto tali, dovete custodire gelosamente e non divulgare. Al momento di concludere l'acquisto, la presenza del lucchetto chiuso in fondo alla pagina o di 'https' nella barra degli indirizzi sono ulteriori conferme sulla riservatezza dei dati inseriti nel sito e della presenza di un protocollo di tutela dell'utente, ovvero i dati sono criptati e non condivisi. Attenzione: Non cadere nella rete del 'phishing' o dello 'smishing', ovvero nella rete di quei truffatori che attraverso mail o sms contraffatti, richiedono di cliccare su un link al fine di raggiungere una pagina web trappola e sfruttando meccanismi psicologici come l'urgenza o l'ottenimento di un vantaggio personale, riusciranno a rubare informazioni personali quali password e numeri di carte di credito per scopi illegali. L'indirizzo internet a cui tali link rimandano differisce sempre, anche se di poco, da quello originale.

- Assicurare gli acquisti. Oltre che controllare i dettagli della transazione e le modalità di consegna, è importante scegliere sempre una spedizione tracciabile e assicurata. Il costo potrebbe essere di poco superiore ma

permette di sapere in modo certo e tempestivo dove si trova l'oggetto acquistato fino alla sua consegna.

Nascondere l'indirizzo IP su internet

Uno dei primi passi per diventare hacker, o meglio cracker, è imparare a non lasciare tracce sul dispositivo utilizzato. È necessario, dunque, saper nascondere l'indirizzo IP.

- Il software migliore è il progetto TOR. All'interno del pacchetto vi sono 3 componenti chiamate Tor, Vidalia e Privoxy; La navigazione anonima con Tor Browser è possibile grazie ad una versione Firefox Portable che funziona in modo automatico e può essere portato su una penna USB.

- AnonymoX è un'estensione per Firefox che basta installare sul browser per navigare con IP straniero. Con AnonymoX si può scegliere il server a cui collegarsi per camuffare l'IP e permette di navigare su siti con restrizioni geografiche e non disponibili in Italia come Hulu.com. AnonymoX è la soluzione più facile ed efficiente che si può trovare e sfrutta anche i server di TOR.

- In generale il metodo più semplice per navigare anonimi è cercare su google una lista di proxy, digitando le parole "*Surf anonymous*", aggiornata e impostarlo sul proprio browser. Un sito veramente ottimo per entrare in modo anonimo su qualunque sito internet è Anonym.to.

- SafeIP serve a proteggere l'identità su internet e nascondere l'indirizzo IP reale per navigare sul web in forma anonima. Gli utenti possono scegliere la posizione geografica dell'IP falso velocemente. Con SafeIP si può simulare la connessione da paesi diversi come USA, Regno Unito, Francia, Canada, Hong Kong, Austria, Polonia, Germania, Paesi Bassi ed anche dall'Italia.

L'interfaccia di SafeIP è facile da usare e per attivare la navigazione anonima basta selezionare il paese di cui si vuole l'IP falso.

- Un modo per navigare anonimi con IP straniero diverso da quello di origine sono le VPN.
- Un metodo potente ma che non sempre funziona, è usare il programmino Toonel. Si scarica il client da questa pagina e senza installazione si lancia il programma. Bisogna poi configurare il vostro browser in modo da accedere ad Internet con indirizzo IP "127.0.0.1" e come porta "8080". Se si prova a chiudere il browser e riaprirlo in questa stessa pagina si noterà che l'indirizzo IP che si può leggere nella figura sotto, sarà cambiato.
- Un altro metodo per restare anonimi su internet senza quindi essere tracciati può essere semplicissimo usando Google o Yahoo**.** Proprio i due siti più importanti del mondo, grazie al loro servizio di traduzione dei siti web, sono dei portali a cui accedere per rimanere anonimi. Con Google**:** andare su http://translate.google.com/, segnare il sito che si vuol visitare e scegliere la traduzione da Inglese a Italiano.

Anonymous

l'inizio era soltanto una forma di protesta contro la setta di Scientology, poi Anonymous ha iniziato ad attivarsi contro ogni forma di censura e contro i dittatori, i violatori dei diritti umani, i distruttori dell'ambiente e anche contro aziende private. Non tutti gli attivisti di Anonymous perseguono questi obiettivi, anche perché nessuno può parlare a nome degli altri. Gli Anonymous non sono dei criminali infatti non si occupano di truffe e raggiri. Il gruppo di Anonymous vede se stesso come un movimento popolare che si batte per la libertà di espressione. Ma il gruppo spesso ignora le leggi e molte azioni risultano quindi illegittime. In alcuni stati, gli attivisti sono per tanto considerati come un gruppo terroristico. Anonymous ha iniziato a diventare di dominio

pubblico dal 2008, ma le origini del collettivo risalgono a molto prima. Circa 10 anni fa internet cresceva in popolarità ed iniziavano a diffondersi le prime piattaforme sulle quali venivano pubblicati testi ed immagini in forma completamente anonima. Su queste piattaforme nacque Anonymous. Il volto sorridente di plastica ha contribuito notevolmente alla reputazione di Anonymous. E' il volto di Guy Fawkes colui che cercò di fare esplodere il parlamento britannico 400 anni fa. La maschera è la caratteristica distintiva degli attivisti in internet. In manifestazioni e messaggi video i membri la usano come mimetizzazione. Anonymous ha scelto questo simbolo per una ragione poco storica: nel film *"V COME VENDETTA"* i combattenti per la libertà si travestivano con questa maschera quando agivano contro il governo totalitario. Anonymous lancia attacchi internet ed organizza dimostrazioni. Anonymous attacca in particolare le istituzioni finanziarie che aderiscono al blocco dei conti della piattaforma Wikileaks. Anonymous di solito utilizza l'applicazione "LOIC" che può essere usata da migliaia di persone, ma questa lascia tracce rivelatrici e gli attaccanti possono essere facilmente scovati. La nuova arma di Anonymous *"RefRef*" può invece far crollare un sito web sfruttando anche un solo computer e colui che utilizza questo strumento software praticamente non può essere rintracciato. Anonymous non è una sorta di club, si partecipa direttamente, migliaia di persone sono coinvolte nelle azioni del gruppo e ciascuno decide da se a cosa vuol partecipare. Ufficialmente non ci sono leader o gerarchie di sorta. Questo rende molto più difficile riconoscere se un azione o un video o una lettera siano effettivamente collegati con Anonymous. Dei membri di Anonymous sono stati arrestati in Spagna nel Regno Unito ed in USA decine e decine di sostenitori di Anonymous in attacchi a siti web sono stati registrati i loro indirizzi IP e da qui il loro indirizzo reale. Attualmente è in corso un intensa attività investigativa da parte del FBI e dell'INTERPOL sul gruppo hacker LULZSEC e suoi presunti vertici di Anonymous. Secondo gli investigatori dell'FBI lo scorso anno è caduto nella loro rete "SABU'" uno dei top hacker di Anonymous accusato di Cyber

attacchi contro grandi imprese ed istituzioni governative. Il ventottenne padre di famiglia si è pentito ed ha fornito l'identità di diversi attivisti di Anonymous, che sono stati in seguito arrestati. Gli attivisti di Anonymous si incontrano soprattutto su internet e per mantenere anonime le conversazioni i membri parlano in IRC su uno spazio protetto, qui discutono e decidono nuove azioni. Per inciso, anche se si dovessero incontrare nella vita reale, gli utenti di Anonymous si chiamerebbero solamente con il loro nomi in codice.

Le operazioni più famose di Anonymous sono:

- Operation Sony anno 2011: Anonymous lancia attacchi alla Play Station Network, dopo che Sony aveva citato in giudizio 2 hacker che si occupavano di giochi per la console. Rimane ancora da chiarire se Anonymous sia responsabile anche del furto dei dati di milioni di utenti del network Sony.
- Operation Zeta anno 2011: l'azione è rivolta contro i boss messicani della droga. Quando fu preso un attivista come ostaggio, Anonymous minacciò di pubblicare gli indirizzi dei signori della droga, l'attivista venne rilasciato. Anonymous solitamente attacca su internet mediante negazione del servizio.

Fonti

1. www.Repubblica.it
2. www.webnews.it
3. www.ragazziweb.it
4. www.Commissariatodips.it
5. www.Mondo-prestiti.it
6. www.hacktips.it
7. www.navigaweb.net
8. www.viveresulgarda.com
9. http://www.dsi.unive.it/~marek/files/seminari/Angelico%20Massimo/%5BAngelico%20-%20823903%5D%20Presentazione.pdf

PayPal

Di Koci Alessia e Nanci Erika

Introduzione generale

L'espressione commercio elettronico, in inglese *e-commerce* (anche *eCommerce*), può indicare diversi concetti: può riferirsi all'insieme delle transazioni per la commercializzazione di beni e servizi tra produttore (offerta) e consumatore (domanda), realizzate tramite Internet. Nell'industria delle telecomunicazioni, si può altresì intendere il commercio elettronico come l'insieme delle applicazioni dedicate alle transazioni commerciali. Un'ulteriore definizione descrive il commercio elettronico come l'insieme della comunicazione della gestione di attività commerciali attraverso modalità elettroniche, come l'EDI (EletronicDataInterchange) con sistemi automatizzati di raccolta dati. Alcune tipologie di prodotti o servizi appaiono maggiormente adattabili alle vendite online, mentre altri sono più indicati per il commercio tradizionale. Le imprese di commercio elettronico che hanno realizzato le migliori performance restando tuttavia un'entità totalmente virtuale (senza aprire fisicamente degli esercizi commerciali) vendono solitamente prodotti informatici come i supporti di archiviazione, il recupero dei dati e il loro trattamento, la vendita di brani musicali, i film, i corsi e i materiali didattici, i sistemi di comunicazione, il software, la fotografia e le attività di intermediazione finanziaria. Tra queste imprese si segnala a titolo di esempio: Google, eBay e PayPal.

Storia

Negli ultimi anni si sente sempre più spesso parlare di PayPal e sempre più persone utilizzano questo metodo di pagamento per i propri acquisti e vendite, sia per questioni di sicurezza che di praticità; ma che cos'è PayPal e come

funziona? PayPal è una società che dal 2002 al 2015 è stata controllata da eBay, fino alla scorporazione e alla quotazione in borsa avvenuta nel luglio 2015. Essa offre servizi di pagamento digitale e trasferimento di denaro via Internet. Il punto di forza del sistema, e ciò che lo differenzia da altri, sta nel permettere di effettuare transazioni senza che vi sia alcuna condivisione dei dati della carta di credito con il destinatario del pagamento.

Venne fondata nel 1998 da Peter Thiel e Max Levchin e ben presto si diffuse in molti paesi del mondo, soprattutto si affermò rapidamente come mezzo per effettuare pagamenti on-line, insieme alle carte di credito e prepagate, ciò spinse il gruppo eBay (eBay Inc.) ad acquistare la società nel 2002.

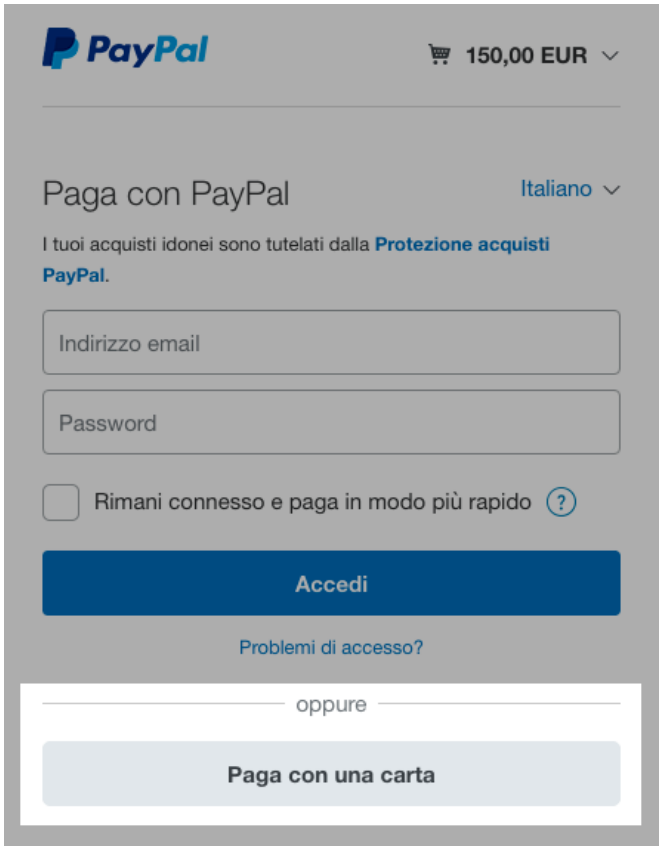
Nel 2004 il valore totale delle transazioni effettuate attraverso PayPal era di 18,9 miliardi di dollari, aumentando ulteriormente nel 2005 a 27,5 miliardi di dollari; una crescita costante, che ha portato ad arrivare nel 2009 a 71 miliardi di dollari.

Intanto nel 2007 PayPal sbarca anche in Europa: infatti riceve la licenza a operare in Europa, in particolare come istituto di credito dalla *Commission de Surveillance du Secteur Financier (CSSF)*, in Lussemburgo.

PayPal al 25 novembre 2011 ha registrato 250 milioni di conti attivi, arrivando ad essere disponibile in 190 paesi e territori.

Come funziona?

Registrandosi gratuitamente presso il sito web della società, è possibile aprire il proprio conto PayPal, che consente di effettuare pagamenti, utilizzando l'indirizzo e-mail e la relativa password. Al proprio *account* è possibile associare una carta di credito (fino ad un massimo di otto), una carta prepagata oppure il proprio conto corrente bancario. A questo punto è possibile ricaricare il proprio saldo dal proprio conto corrente bancario tramite bonifico, senza l'addebito di ulteriori tariffe da parte di PayPal. Dal conto PayPal sarà dunque possibile prelevare fondi trasferendoli o carta di credito/carta prepagata per poi effettuare acquisti on-line oppure in maniera inversa riportarli sul proprio conto bancario. PayPal mette inoltre a disposizione, agli utenti che ne facciano richiesta, una carta di credito, operante su circuito VISA, ed una carta prepagata operante su circuito MasterCard. Quindi società leader a livello mondiale per i pagamenti online, consente ad acquirenti e aziende di inviare e ricevere pagamenti online. È accettato dai commercianti di tutto il mondo, su eBay e su altri siti. L'idea di base consiste nell'effettuare transazioni senza condividere i dati della carta con il destinatario finale del pagamento: il sistema infatti non trasmette i dati sensibili delle carte collegate al conto. PayPal ti consente infatti di proteggere le informazioni della tua carta di credito grazie a innovativi sistemi di sicurezza e di prevenzione delle frodi. Quando utilizzi PayPal, le tue informazioni finanziarie non vengono mai comunicate al commerciante. Uno dei tratti distintivi e caratterizzanti dei servizi PayPal è il programma di sicurezza che la società offre; si tratta di una tutela ad acquirenti e venditori che copre l'intero importo d'acquisto in caso di mancata consegna o di consegna di un oggetto diverso da quello descritto.



PayPal garantisce ai venditori una protezione efficace contro perdite causate da reclami per pagamenti fraudolenti o oggetti non ricevuti. PayPal è supportato da una vasta gamma di shop online e di siti Internet, primo fra tutti è eBay che, come abbiamo detto, ha acquisito la proprietà del servizio e dal 2002, è inoltre il metodo di pagamento predefinito per le aste su questo.

Transizioni e prelievi

Per inviare soldi bisogna collegarsi alla home page di PayPal e selezionare il testo "Invia denaro" digitando poi l'indirizzo e-mail del destinatario. In caso di mancanza di liquidità sul conto PayPal il servizio preleverà automaticamente il denaro sulla carta di credito associata al vostro account.

Per ricevere pagamenti sul conto PayPal basterà comunicare l'indirizzo e-mail associato al conto. Ovviamente è possibile anche trasferire denaro dal conto

PayPal al proprio conto corrente bancario o sulle proprie carte associate all'account, selezionando nel menu "Preleva" le voci "Trasferisci denaro sul conto bancario" piuttosto che "Trasferisci denaro sulla carta".

Se desiderate versare denaro dal vostro conto corrente bancario al conto PayPal dovrete selezionare "Ricarica conto" ed eseguire un bonifico seguendo le istruzioni fornite dal servizio. L'invio di denaro è gratuito mentre la ricezione è soggetta a tariffe (0,35 € più una percentuale variabile sull'importo).

Per quanto riguarda il prelievo, è gratuito se la cifra è superiore o uguale a 100 euro, mentre si paga 1,00 euro nel caso sia inferiore. Il prelievo su carta PayPal (carta di credito o ricaricabile) è sempre gratuito.

Tutela dell'utente

Se si riceve inoltre un pagamento non autorizzato (ad esempio, da un account colpito dagli hacker) o se un cliente dichiara di non aver ricevuto un oggetto acquistato, PayPal tutela per l'importo complessivo della vendita, senza costi aggiuntivi, purché la vendita rispetti alcuni requisiti. Vi sono anche le vendite

protette, la protezione si applica solo in caso di articoli materiali soggetti a spedizione che sono stati pagati con PayPal. La transazione deve essere contrassegnata come idonea alla Protezione vendite nella pagina "Dettagli transazione" del conto dell'utente. In caso di reclamo per pagamento non autorizzato o oggetto non ricevuto, devi avere la prova di avvenuta spedizione, mentre in caso di chargeback (un chargeback si verifica quando un acquirente richiede alla società emittente della propria carta di credito di stornare un pagamento già eseguito) per oggetto non ricevuto, si deve avere la prova di avvenuta consegna.

Esiste inoltre un'applicazione sviluppata appositamente per PayPal che consente di effettuare transazioni dai telefoni cellulari; si chiama Send Money ed è disponibile sia per iPhone che per e Windows Phone.

Esempi di utilizzo: eBay

Proprio da eBay nasce l'equivoco sulla sicurezza di Paypal, vediamo il perchè: se un'inserzionista eBay accetta il pagamento tramite PayPal, all'interno troviamo questa situazione. "Paga con PayPal: protezione integrale" è una garanzia per l'utente che acquista, nel caso in cui il materiale non venga spedito, o non sia conforme alla descrizione, o comunque se si delinea una truffa, l'acquirente può attivare una pratica di contestazione tramite eBay e se il venditore non riesce a dimostrare di avere spedito e di aver fatto tutto in regola, l'acquirente ottiene il rimborso direttamente da PayPal. Tutto molto semplice, ma è da qui che nasce l'equivoco. PayPal va ritenuto un metodo di pagamento "anti frode" se, come nell'esempio sopra, facciamo un acquisto su eBay e procediamo al pagamento seguendo la procedura e i link forniti da eBay a fine asta, in questo modo infatti il

pagamento rimane legato all'oggetto acquistato. Tutta la transazione ha una storia dimostrabile in un clic ad eBay, ecco perchè in questo caso va ritenuto un metodo di pagamento super affidabile. Quand'è allora che non va considerato un pagamento sicuro? Beh, in tutte le altre situazioni, facciamo un esempio: trovando un oggetto su subito.it o un qualsiasi altro sito di annunci, si contatta il venditore e si fa l'acquisto pagando con PayPal, per effettuare il pagamento: in realtà non si è seguita una procedura particolare come quella presente in eBay, molto più semplicemente il venditore ha fornito il suo conto PayPal ed è stato fatto un versamento su questo conto. È chiaro quindi che in caso di truffa, diventa impossibile dimostrare che il versamento è stato fatto per acquistare un oggetto mai consegnato, molto probabilmente il truffatore sparirà dalla circolazione, ma se anche non sparisse, sarebbe la parola dell'acquirente contro la sua, di fatto lui potrebbe inventarsi qualsiasi motivo per cui l'utente avrebbe dovuto dargli quei soldi, non esiste un collegamento (come nel caso di eBay) tra oggetto acquistato e pagamento, per questo motivo PayPal non vi rimborserà assolutamente niente. In questa situazione, pagare tramite PayPal o ricaricare una PostePay(altro metodo poco affidabile) ha le stesse garanzie, cioè nessuna garanzia. Col passare del tempo è nato eBay Annunci che non è assolutamente la stessa cosa di eBay Classico(quello con le aste), nel secondo caso, come già detto, PayPal è sicuro, nel primo caso invece è un sito di annunci del tutto paragonabile a qualsiasi altro sito di annunci gratuiti, vale quindi il discorso legato all'esempio di prima, il solo PayPal non va considerato una garanzia.

La tua sicurezza al primo posto. Il tuo denaro è al sicuro in un unico portafoglio virtuale. Proteggiamo gli acquisti, le vendite e i metodi di pagamento usati. Invia e ricevi denaro in Italia e all'estero. Alla tua sicurezza pensiamo noi.

Come associare una carta di credito, di debito o prepagata a PayPal

E' davvero semplice. Basta andare nella home page del servizio e, dal menù di sinistra, scegliere "Conti correnti e carte". Dalla pagina successiva sarà possibile aggiungere un conto corrente bancario o postale, oppure una carta di ogni tipo.

Tenete presente che, nel fare questa procedura, vi verranno addebitati dal conto o dalla carta che legherete dei piccoli importi di circa 1 € / 1,50 € , che vi ritroverete

però sul conto PayPal. E' una misura di sicurezza che serve a PayPal per essere certo che la carta o il conto che state dichiarando di voler usare sia proprio vostro.

- Associare una carta

Nel caso della carta, riceverete un addebito di 1,50 € . Sull'estratto conto che riceverete o che potrete consultare online, avrete una riga con scritto "PAYPAL" o "PPP", seguito da un codice a 4 cifre. Quando questa procedura sarà fatta (potrebbe chiedere qualche giorno) dovrete tornare nel vostro conto PayPal e verificarlo inserendo le 4 cifre di cui sopra.

- Associare un conto corrente bancario o postale

Nel caso in cui vogliate invece associare un conto corrente bancario o postale, vi verranno addebitati dallo stesso due importi diversi, di solito entrambi inferiori a **1 €**.Quando vedrete tali addebiti dall'estratto conto, potete rientrare nel conto PayPal e verificarlo inserendo gli importi addebitati. Ricordatevi, in tutti e due i casi descritti sopra, che i soldi che vi saranno addebitati dalla carta o dal conto, vi saranno accreditati sul conto PayPal. Dunque, aprire un conto PayPal è gratis.

Perché PayPal è sicuro per fare acquisti online?

La sicurezza principale di PayPal come metodo di pagamento online sta nel fatto che è possibile usarlo per fare acquisti senza dover fornire il proprio numero di carta di credito, che rimane salvato nei server sicuri di PayPal stesso. Al momento del pagamento con PayPal, infatti, dal sito dove si sta facendo l'acquisto, si verrà reindirizzati su quello del metodo di pagamento PayPal, bisogna fare accesso con il proprio indirizzo email e password e dare conferma di voler procedere. Al termine della procedura si verrà rimandati sul sito originario, quello dove si è fatto l'acquisto, per visualizzare i ringraziamenti e la conferma d'ordine. Inoltre, pagando con PayPal su eBay, si è maggiormente protetti da frodi e da raggiri, secondo le norme della Protezione acquirenti.

Come ricaricare il proprio conto PayPal

Per poter versare denaro sul PayPal si possono scegliere tre metodologie:

- ricevere denaro da un familiare o un amico;
- spostare il denaro dalla carta di credito / debito / prepagata al conto PayPal;

In realtà, per fare acquisti con PayPal non c'è bisogno necessariamente di avere denaro sul conto. Se ce n'è, in automatico PayPal usa i fondi del conto come metodo di pagamento, in caso contrario va a prelevare direttamente dalla carta o dal conto corrente bancario (in questo caso il sistema PayPal diventa una specie di intermediario nel pagamento).

Come ricevere denaro su PayPal

Per farsi pagare su PayPal basta semplicemente comunicare a chi invierà il denaro il proprio indirizzo email di registrazione al servizio PayPal.

Esatto, basta dirgli "inviami i soldi al mio indirizzo e-mail", dicendogli ovviamente qual è. Tutto qui, ogni transazione viene fatta tramite indirizzo di posta elettronica, e non c'è pericolo di confusione perché solo voi potete avere, in tutto il mondo, un certo indirizzo di posta.

Come ritirare (o prelevare) soldi da PayPal

Quando siete arrivati ad avere un certo importo su PayPal, potete tranquillamente prelevare le somme che vi spettano. Per farlo, dalla home page della vostra area personale, dovete selezionare "Prelevare denaro", si trova nel menù di sinistra. A questo punto vi verrà chiesto quanto volete prelevare e dove volete che vi venga inviato il denaro (nel caso in cui avete aggiunto più di un conto o più di una carta). L'importo minimo del prelievo è di 0,02 € (2 centesimi) e non ci sono commissioni da pagare.

Quando costa ricevere soldi su PayPal?

Ricevere pagamenti su PayPal non costa nulla se il versamento viene fatto, dall'altra persona, in qualità di donazione (è il caso di un parente o un amico che ci dà dei soldi), se invece si tratta di un pagamento per aver venduto un bene (ad esempio all'asta su eBay), allora ci sono delle commissioni da pagare.

Commissioni PayPal 2016: quanto costa

Ecco l'aggiornamento delle commissioni 2016 PayPal:

Fare acquisti in euro	Gratuito

Vendere in zona euro	fino al 3,4% + 0,35€ per transazione
Vendere fuori dalla zona euro	si applicano le tariffe di conversione e quelle per la vendita internazionale
Inviare denaro in zona euro con conto Paypal	Gratis
Inviare denaro in zona euro con carta collegata	fino al 3,4% + 0,35€ per transazione
Inviare denaro fuori dalla zona euro	si paga un costo di ricezione dei pagamenti internazionali compreso tra lo 0,4% e l'1,8%. Se si usa una carta si paga anche una commissione fino al 5,2% + 0,35€ per transazione. Le tariffe definitive variano in base al Paese di destinazione.

Fonti

1. www.guidaconsumatore.com
2. www.wikipedia.com
3. www.community.ebay.it
4. www.swarro.it
5. www.mondo-prestiti.it
6. www.paypal.com

Conclusione

Terminato il lavoro, gli studenti hanno preso atto che, le ricerche e gli studi effettuati per la stesura del presente libro, hanno permesso di ampliare le conoscenze riguardanti anche tematiche precedentemente non prese in considerazione o reputate superflue. E di aumentare la consapevolezza che gli strumenti informatici, in un mondo in continua evoluzione, sono ormai indispensabili in tanti campi di applicazione. Infatti nel corso degli ultimi decenni grazie alle loro implementazioni sono stati raggiunti traguardi importanti nel mondo della ricerca medica, scientifica, aerospaziale, ed in tanti altri settori. Per tale ragione ed affinché il loro utilizzo sia finalizzato a garantire un continuo progresso a favore della società, dagli approfondimenti eseguiti è emerso che è necessario essere dotati di adeguate competenze per sfruttarne al massimo le potenzialità ed evitare un loro impiego passivo o improprio.

Di Catanese Claudia e Talarico Federica