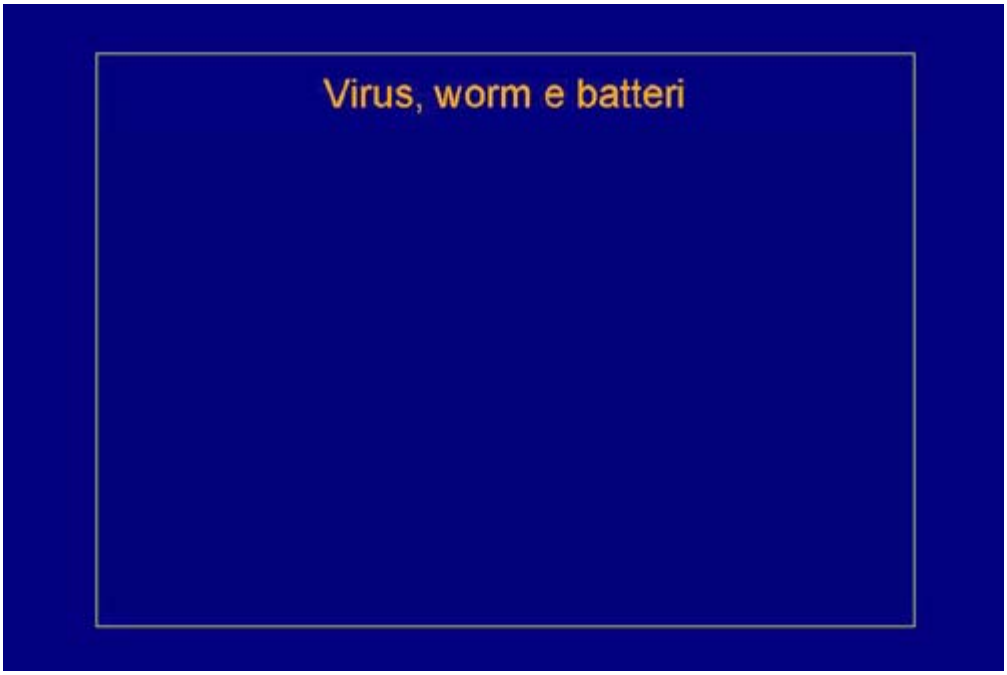
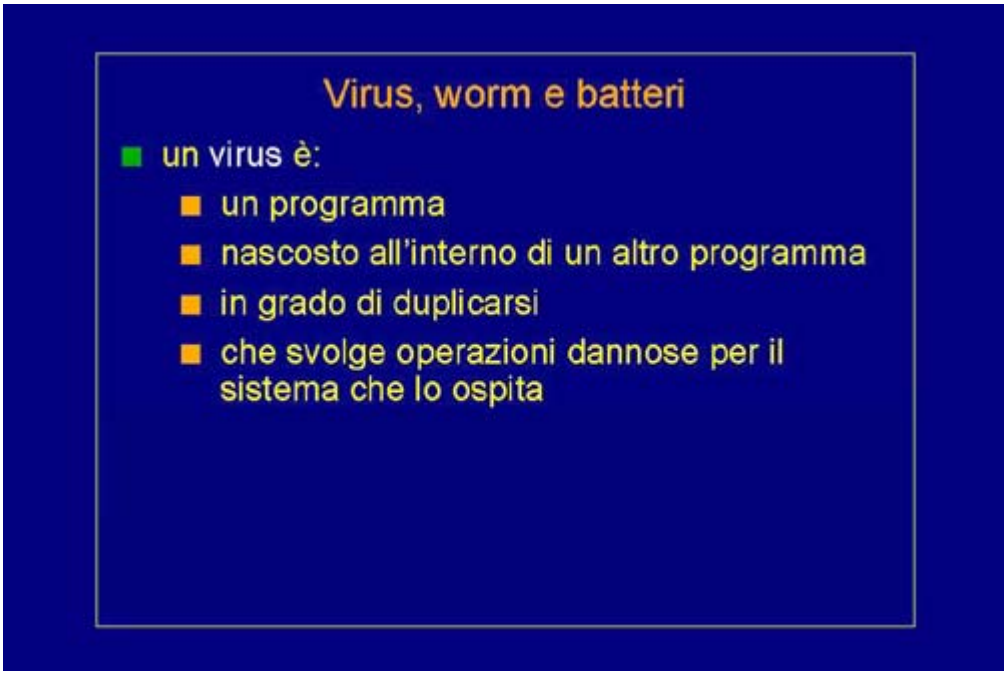
Antivirus
Virus, worm e batteri



In questa lezione tratteremo della problematica di come proteggere i nostri sistemi informativi dai virus. I virus costituiscono oggigiorno una grossa minaccia perché continuano a diffondersi grazie alla complicità degli utenti, che si scambiano facilmente dati, sia tramite Internet sia tramite dischetti, senza controllare la loro reale provenienza. In particolare i virus sono soltanto uno degli elementi di un insieme di minacce che possono arrivarci: le altre minacce sono chiamate worm (vermi) o batteri. Vediamo quali sono le cose che contraddistinguono questi tre tipi di attacchi.

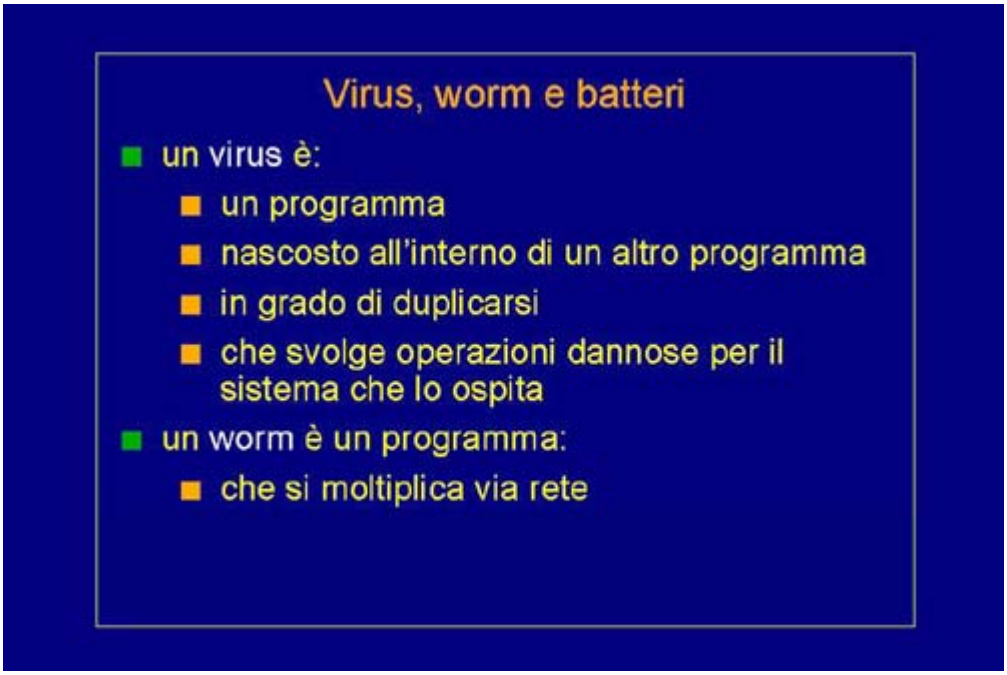
I virus



In particolare cominciamo dai virus. Il virus è un programma quindi è concettualmente del codice eseguibile che viene nascosto all'interno di un altro programma. Questo è il modo detto di infezione, ossia il virus si fa trasportare all'interno di un altro programma. In più, una delle caratteristiche di

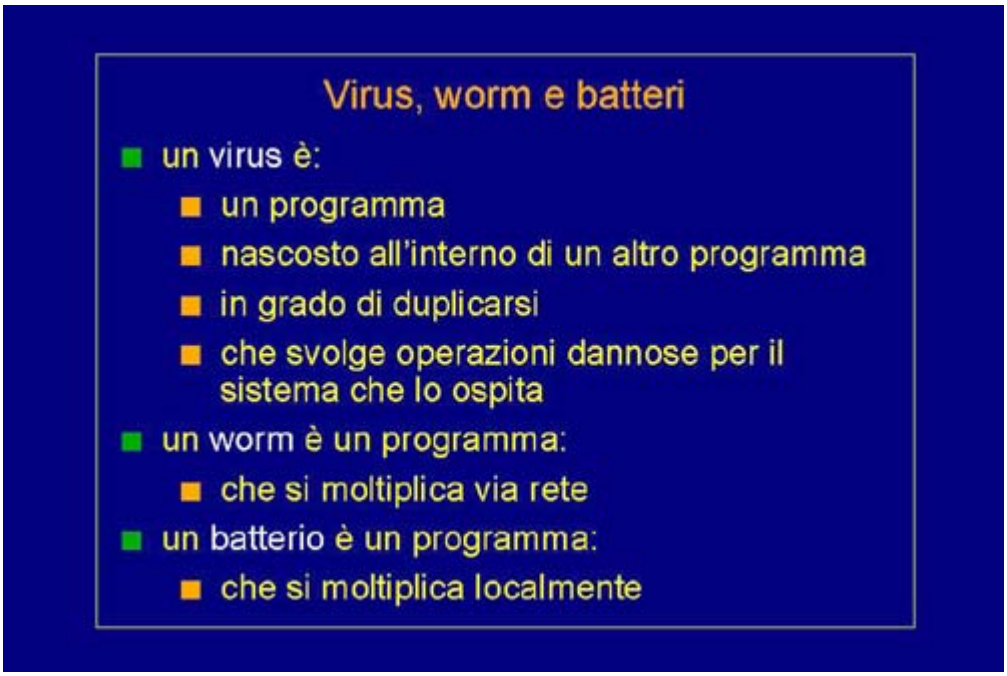
questo codice virale è quella di essere in grado di duplicarsi: ossia significa che il virus, nel momento in cui va in esecuzione, è in grado di vedere se esistono altri file che possono essere utilmente infettati. Inoltre, il virus è stato di solito sviluppato per compiere delle operazioni dannose nei confronti del sistema che lo ospita. Quindi il virus è un programma di attacco che viene inserito all'interno di altri programmi per compiere le azioni criminose e per moltiplicarsi e attaccare altri sistemi.

I worm



Un worm, invece, è un tipo di virus molto più semplice. Un worm non è nient'altro che un programma che attacca i sistemi indirettamente, generando molte copie di se stesso, tramite la rete. Ossia, in generale, un worm tende ad avere una copia di se stesso in esecuzione su tutte le macchine collegate a una rete. È ovvio che deve trovare un meccanismo di trasmissione via rete. Quindi, i worm, non si possono propagare se i due calcolatori non sono collegati in rete e non si possono propagare se i due calcolatori sono adeguatamente protetti contro le intrusioni via rete.

I batteri



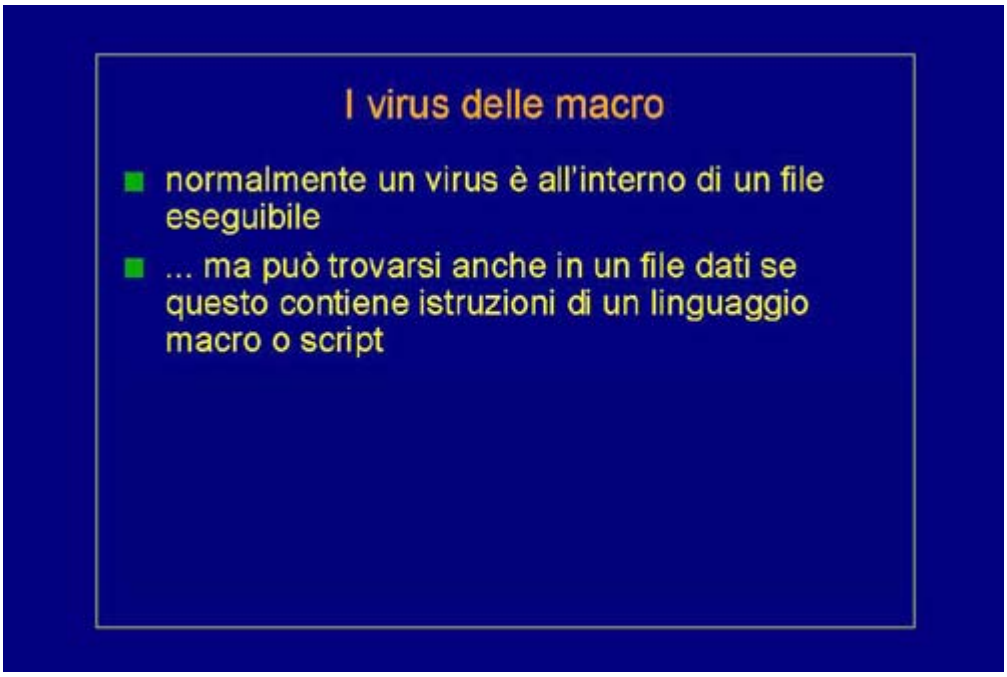
Si parla, infine, di batteri nel caso di programmi che tendono ad attaccare il sistema semplicemente generando infinite copie di se stessi, saturando quindi le risorse di calcolo. Un batterio è l'analogo di un worm però, al posto di propagarsi via rete, si limita ad effettuare le proprie copie all'interno del sistema stesso, fino a saturarne completamente la memoria, il tempo di calcolo o i dischi. In questa lezione noi ci concentreremo in particolare sui virus, perché oggigiorno costituiscono la maggior minaccia.

Anatomia di un virus

Vediamo com'è fatto: il virus è costituito da una parte di codice che serve ad inizializzare le proprie funzioni. Questa parte di codice cede ben presto il posto alla funzione di propagazione. Questo significa che il virus, durante la sua vita, controlla continuamente se esiste la possibilità di fare una copia di se stesso all'interno di altri file e all'interno di altri dischi, in modo da assicurarsi la propria moltiplicazione e la propria sopravvivenza. Inoltre, all'interno del virus è presente una sezione di codice che è il cosiddetto trigger, o grilletto, ossia una parte di codice che controlla se si è verificato

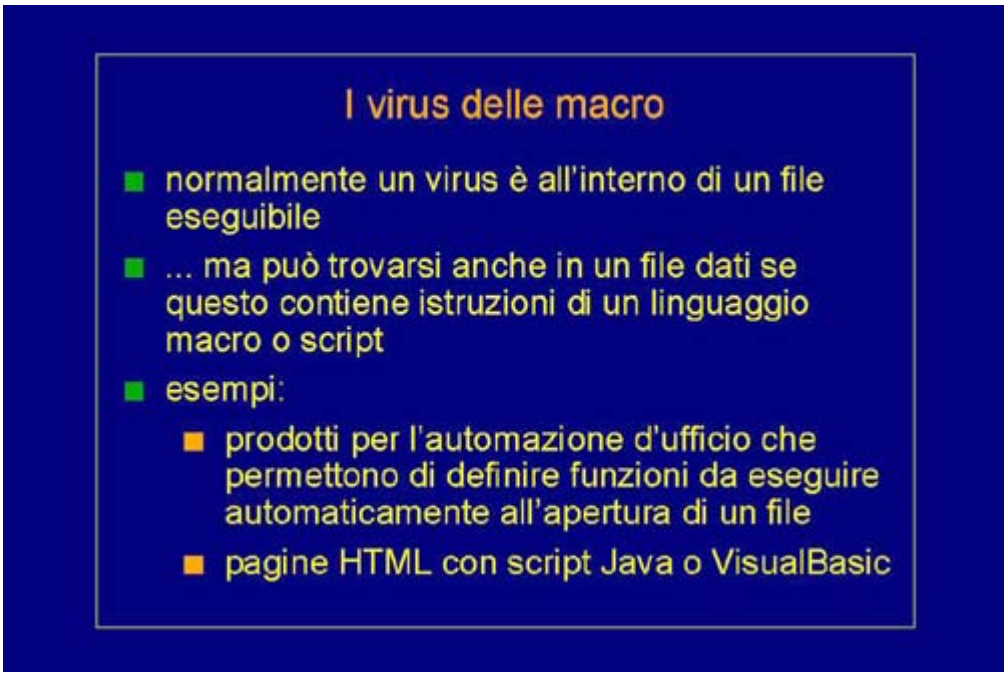
un certo evento. Ad esempio, ci sono dei virus burloni che controllano se la data del sistema coincide con il primo di aprile: se è il primo di aprile allora compiono una qualche azione, che si spera non troppo dannosa vista la particolare data scelta. In altri casi potrebbe trattarsi di operazioni molto distruttive. In ogni caso, la parte di trigger è quella che scatena il comportamento cattivo del nostro virus, quindi il virus deve contenere un'ultima sezione che è quella relativa all'azione criminosa che intende intraprendere. Quindi, tutte e quattro queste parti sono quelle che noi troviamo all'interno di quasi ogni tipo di virus e corrispondono a concetti diversi, tutti egualmente necessari alla funzionalità del nostro virus.

I virus nelle macro



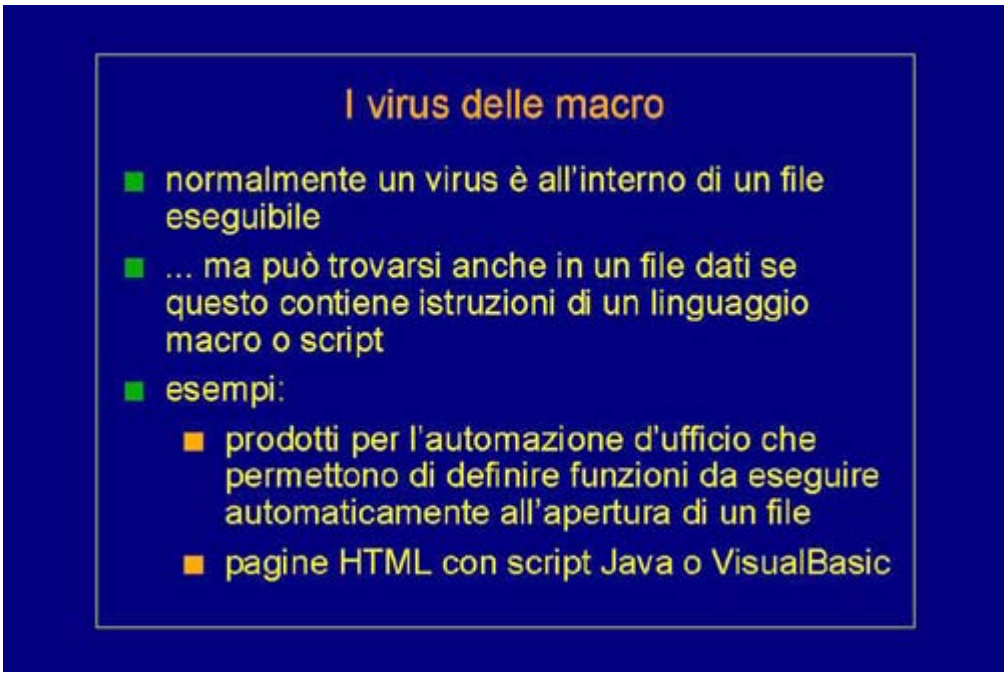
In particolare abbiamo detto che, in generale, un virus è situato all'interno di un file eseguibile. Che cos'è un file eseguibile? Un file eseguibile può essere di diverso tipo. In generale, non è detto che un file eseguibile sia un vero e proprio file binario, perché oggigiorno si sta diffondendo sempre di più l'abitudine, per chi sviluppa applicazioni, di nascondere pezzi di programmi, quindi pezzi di applicazioni, anche all'interno di file dati. In particolare notiamo che esistono dei linguaggi macro, o dei linguaggi di script, che vengono allegati all'interno di file dati.

I virus nelle macro - esempi



Ad esempio, questo è tipico nei prodotti per l'automazione d'ufficio. Ci sono molti word processor, spread sheet e sistemi di presentazione grafica che permettono di definire funzioni da eseguire automaticamente all'apertura del file. Allora, i cosiddetti macrovirus sono quelli che si annidano non all'interno di un file eseguibile binario, ma all'interno della macro, quindi di quel pezzo di codice scritto con un opportuno linguaggio di script e che servirebbe teoricamente a completare le funzionalità di uno di questi prodotti per l'automazione d'ufficio.

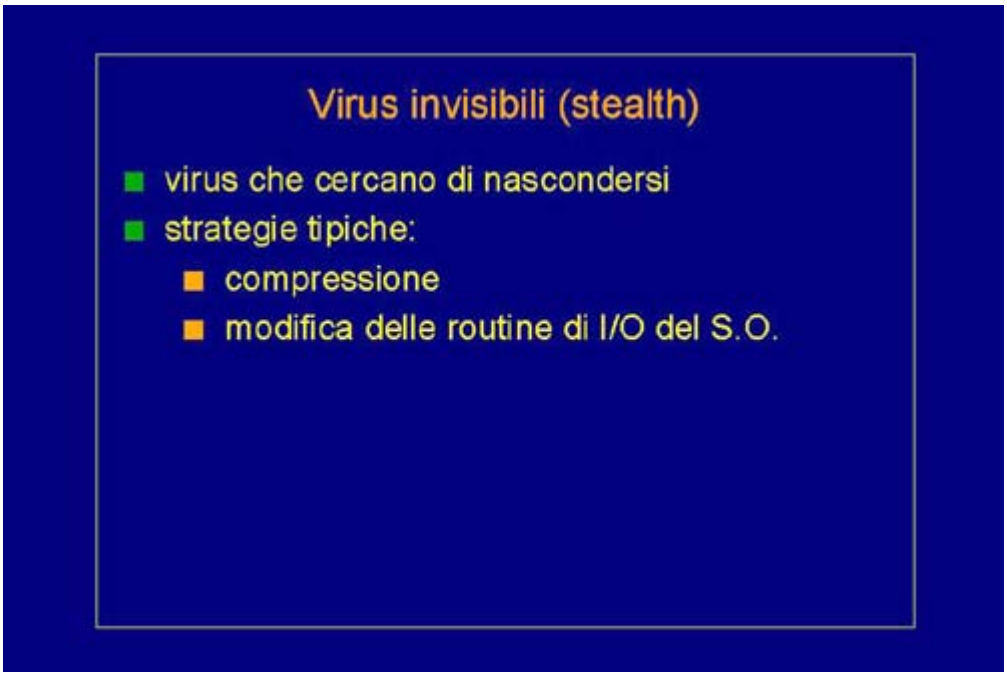
I virus nelle macro - esempi - HTML



In modo analogo cominciano a diffondersi virus anche attraverso le pagine HTML. Di per sé una pagina HTML non dovrebbe essere nient'altro che una pagina che presenta del testo, della grafica, eventualmente dei filmati o dei suoni. Ma, recentemente, è stato possibile inserire all'interno delle pagine HTML anche dei brevi script, quindi diciamo delle funzioni, scritti con degli appositi linguaggi, ad esempio: Java Script e Visual Basic Script. Allora, a questo punto, diventa pericoloso anche semplicemente navigare via Web. Perché, navigando via Web, posso visualizzare una pagina

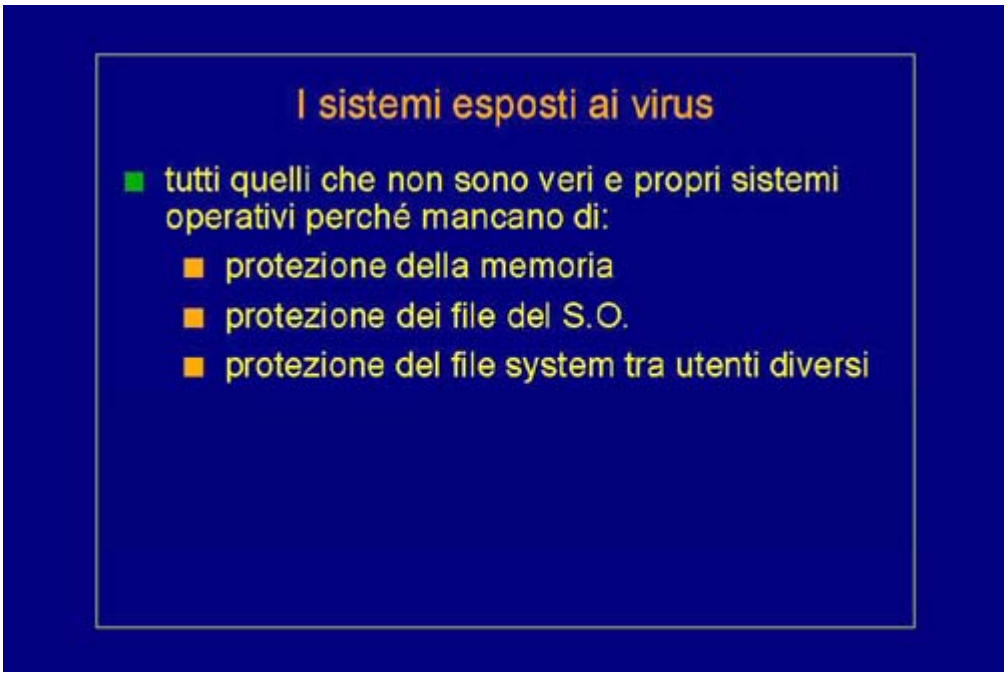
HTML che contiene questo codice eseguibile e, nel momento in cui la visualizzo, questo codice può essere eseguito automaticamente sul mio calcolatore. Se il codice allegato all'interno della pagina HTML è un codice cattivo, è un codice virale, ecco che questo può condurre degli attacchi. Quindi sarebbe consigliabile, per chi scrive le pagine HTML, cercare di limitare o meglio ancora non utilizzare queste capacità di scripting, per chi naviga via Web sarebbe fortemente consigliabile, soprattutto quando visita pagine di siti non fidati, di disabilitare l'esecuzione degli script annidati all'interno delle pagine HTML.

Virus invisibili



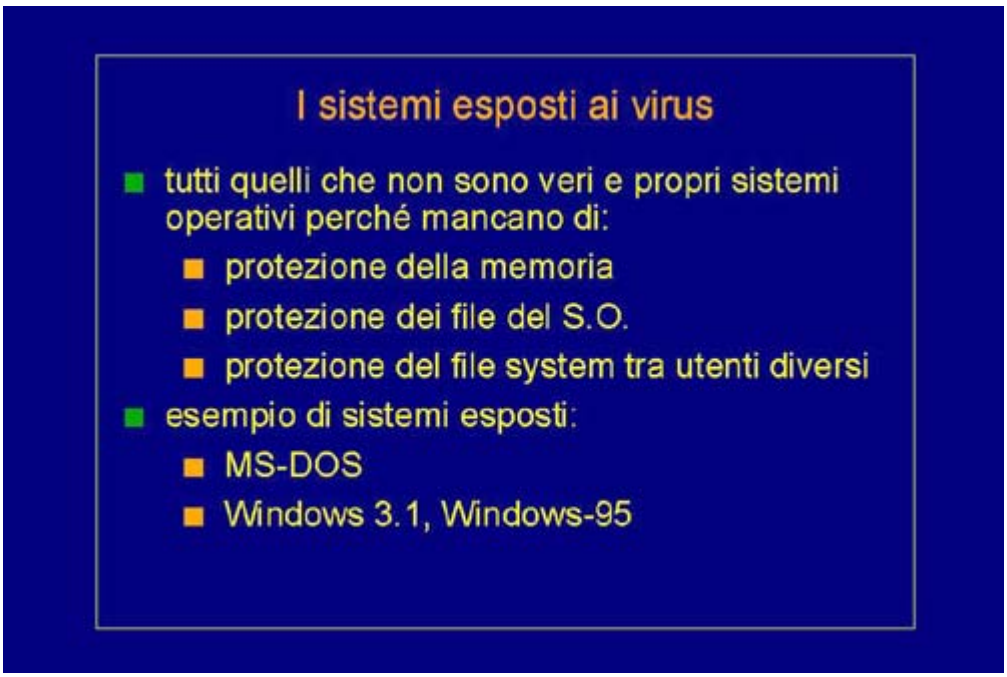
Esiste una continua battaglia tra chi sviluppa il software antivirus e gli hacker che scrivono il codice dei virus. In particolare, chi scrive il codice dei virus cerca di non rivelare la propria presenza, cerca di far sì che il virus possa passare inosservato. Si parla quindi di virus invisibili, o col termine inglese stealth virus, per tutti quanti quei casi in cui i virus cercano di nascondere la propria presenza all'interno del sistema. Esistono due strategie tipiche con cui gli scrittori di virus tendono a nascondere il proprio codice. La prima strategia tipica è quella di comprimere il codice. Il codice compresso non assomiglia più in nessun modo alle tipiche istruzioni assembler di un calcolatore, assomiglia piuttosto a dei normalissimi dati e quindi questo potrebbe trarre in inganno i software antivirus. È ovvio che il virus, prima di entrare in esecuzione, dovrà decomprimere le proprie istruzioni, proprio perché altrimenti queste non potrebbero essere mandate in esecuzione. Una seconda possibilità che alcuni virus mettono in atto, è quella di andare a modificare le routine di input/output del sistema operativo al cui interno loro operano. In questo modo, quando il software antivirus cerca di leggere i dati relativi al virus, loro al posto di fornire i veri e propri dati e quindi farsi rivelare, forniscono dei dati fasulli che non permettono la rivelazione. È chiaro che un sistema in cui sono stati manipolati addirittura le routine di input/output del sistema operativo è un sistema fortemente compromesso.

Virus polimorfici e cifrati



Altre due categorie di virus molto aggressivi e molto diffusi sono i virus polimorfici e cifrati. Sono quei virus che per evitare di essere rivelati cambiano il proprio codice ad ogni infezione. Questi sono i cosiddetti virus polimorfici: ossia, poiché la medesima operazione può essere in genere compiuta in diverse sequenze di istruzioni assembler, ci potrebbero essere dei virus che cambiano il modo con cui svolgono le proprie azioni ogni volta che si duplicano. Questo fa si che i virus assumano ogni volta una forma diversa e quindi sono più difficili da rivelare da parte dei software antivirus. Ancora meglio sono i virus che cifrano una parte del proprio codice tramite un algoritmo di crittografia. Questi sono i cosiddetti virus cifrati ed ovviamente sono ancora più difficili dei precedenti da visualizzare. In un certo senso sono simili a quelli che comprimono una parte del proprio codice, con l'aggiunta che, mentre noi potremmo provare a decomprimere i virus compressi, nel caso di virus cifrati è praticamente impossibile decifrare il virus se non si conosce la chiave di crittografia che è stata utilizzata. Quindi i virus cifrati sono ancora più difficili da rivelare, sia dei virus compressi, sia dei virus polimorfici.

I sistemi esposti ai virus

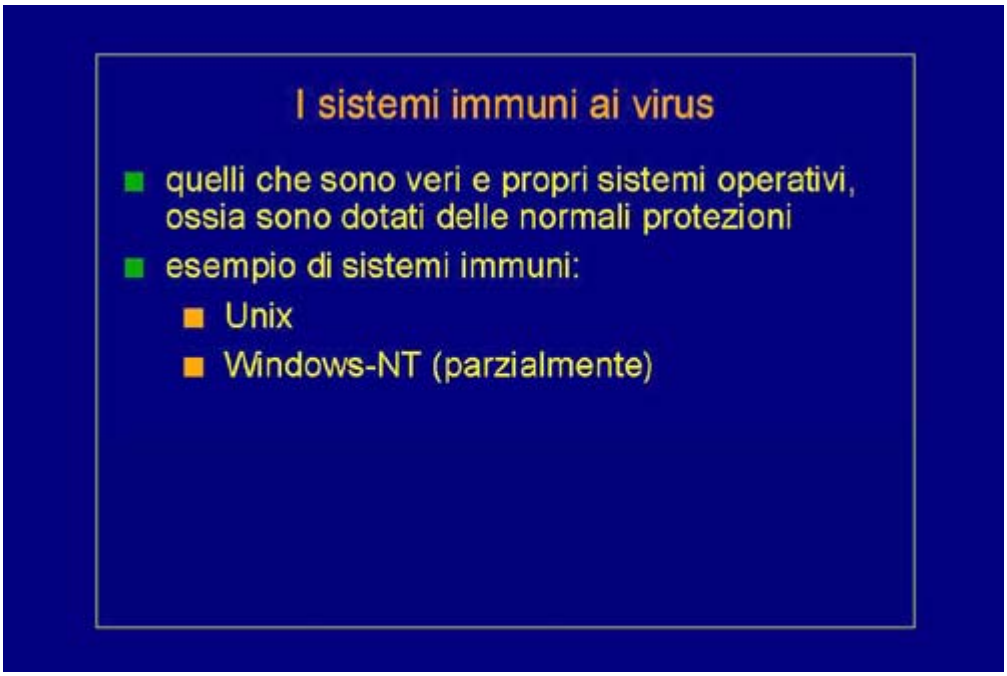


In generale, quali sono i sistemi esposti ai virus? Bisogna che qualunque persona in possesso di un calcolatore elettronico sia preoccupato dell'esistenza dei virus? La risposta è: no. Esistono certe categorie di computer che sono soggette ai virus e certe categorie di computer che sono invece immuni ai virus. In particolare, i sistemi esposti ai virus sono tutti quelli che non sono dotati di un vero e proprio sistema operativo. Ovverosia, sono dotati di pseudo-sistemi operativi che mancano delle tipiche caratteristiche di protezione. Ossia tutti quei sistemi che non proteggono la memoria fisica presente all'interno del sistema, ma permettono ad un qualunque programma di scrivere in una qualunque locazione di memoria. Sono quei sistemi che non impediscono ai programmi di modificare i file stessi del sistema operativo. Sono tutti quei sistemi che non hanno un file system che protegge i dati di utenti diversi e quindi permette ad un programma di manipolare i dati anche di un altro utente.

I sistemi esposti ai virus - esempi

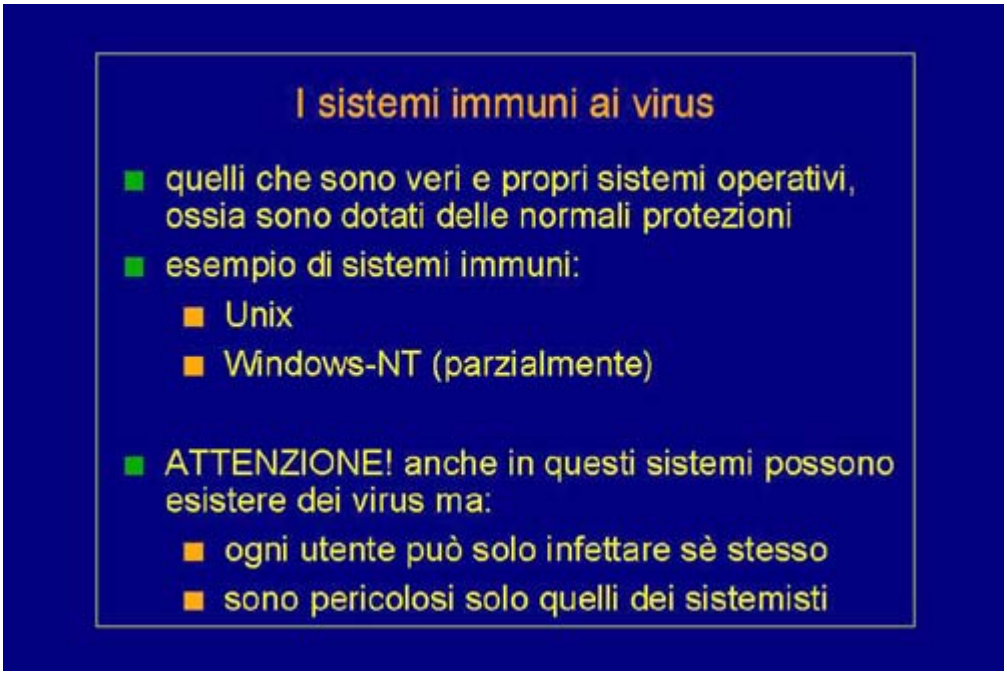
Esempi sono i primi sistemi di uso personale: il sistema operativo MS-DOS, il sistema operativo Windows 3.1 e Windows 95. Sono sistemi operativi particolarmente semplici da utilizzare, ma questa loro semplicità è stata ottenuta a scapito della protezione e del grado di sicurezza. E quindi questi, in generale, sono i sistemi operativi più esposti agli attacchi dei virus, proprio perché permettono al virus di andare a scrivere in qualunque locazione di memoria, su qualunque file, di qualunque utente e addirittura di andare a modificare i dati del sistema operativo stesso. Questi sono i tipici ambienti in cui i virus nascono, si sviluppano, crescono e si moltiplicano.

Sistemi immuni ai virus 1/2



Quali sono invece i sistemi immuni ai virus? Sono ovviamente l'insieme complementare. Sono tutti quanti quei sistemi dotati di un vero e proprio sistema operativo, ossia dotati di tutte le normali protezioni che abbiamo visto mancare invece nella prima categoria di sistemi. Esempi di sistemi immuni, allora, sono Unix e Windows NT, ossia tutti quei sistemi che implementano delle forti politiche di protezione. Nel caso di Windows NT bisogna fare attenzione, perché al suo interno esiste un sottoinsieme di esecuzione che fornisce compatibilità con i Windows di tipo precedente. Come tale, questo ambiente, offrendo la compatibilità con le applicazioni Windows di tipo a 16 bit o a 32 bit, offre anche la compatibilità con i virus sviluppati per DOS, per Windows a 16 bit e per Windows a 32 bit. Quindi, Windows NT è insensibile ai virus, ma sono ed esclusivamente per la parte che riguarda le applicazione native NT e non per le applicazioni invece in modalità di compatibilità Dos o Windows di tipo più vecchio.

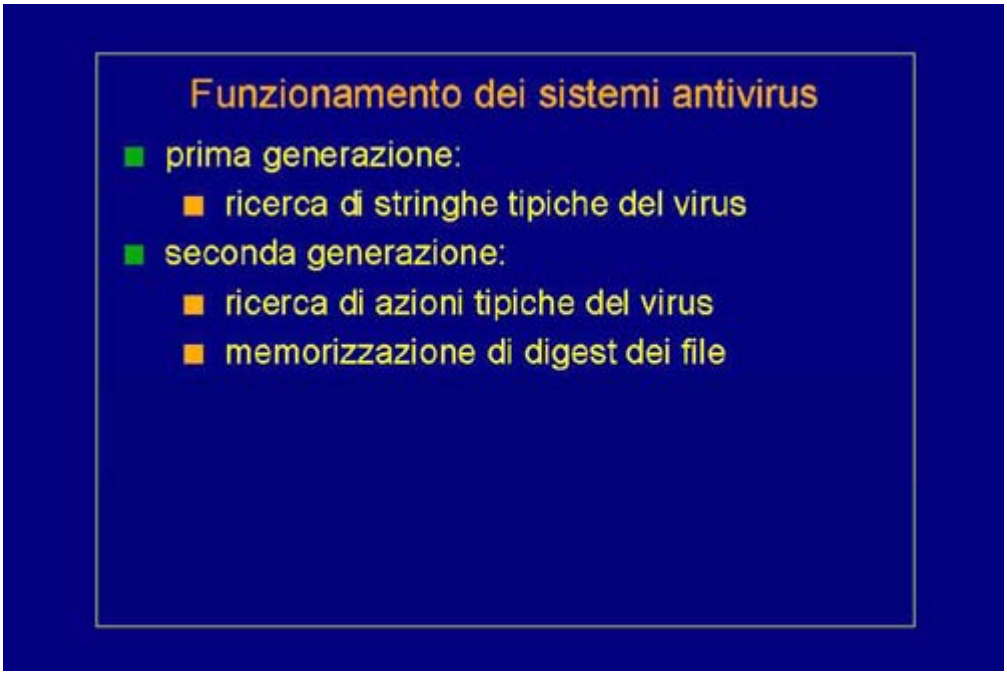
Sistemi immuni ai virus 2/2



Bisogna però fare attenzione ad una cosa. Questi sistemi offrono protezione nei confronti dei virus

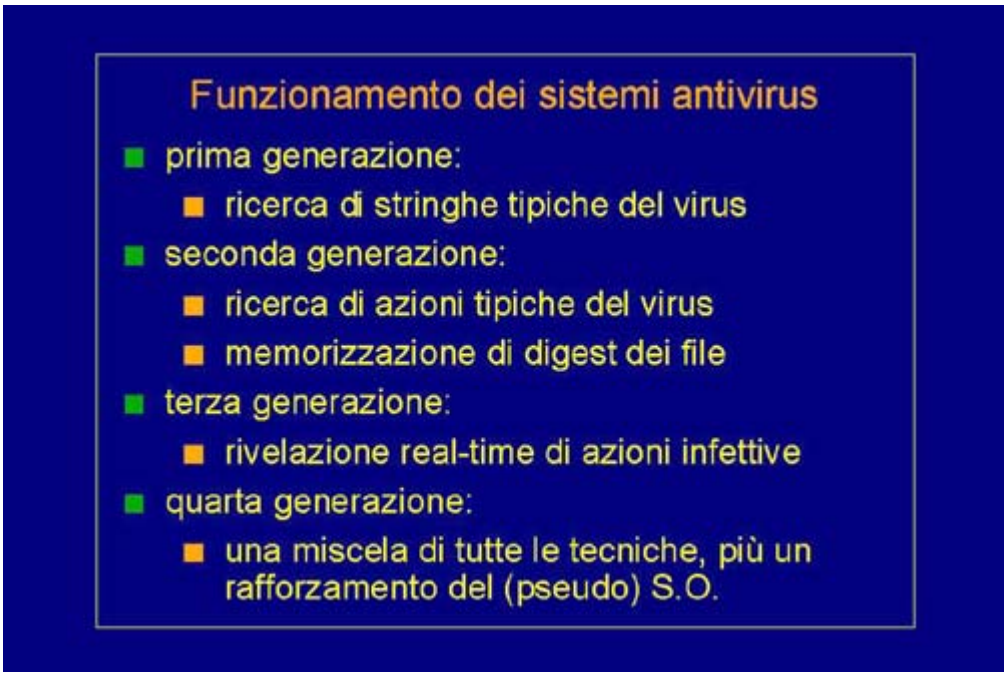
che cercano di alterare i dati di altri utenti o i dati del sistema. Questo non significa che i virus non possano esistere mai all'interno di questi sistemi, ma significa piuttosto che un singolo utente può introdurre un virus nel sistema ma, questo virus, sarà in grado di svilupparsi, moltiplicarsi e colpire solo ed esclusivamente l'utente stesso. Il virus non potrà propagarsi, proprio per i vincoli che il sistema operativo pone. Quindi, in particolare, bisogna fare molta attenzione a quali sono i file introdotti dai sistemisti, perché i sistemisti hanno il permesso di andare a modificare i dati di qualunque utente e anche i dati del sistema operativo stesso. Ovviamente, se un sistemista introducesse per sbaglio un virus all'interno del sistema, allora questi sarebbero dei problemi molto grossi, perché questo potrebbe infettare tutti i dati di tutti quanti gli utenti.

Funzionamento dei sistemi antivirus 1/2



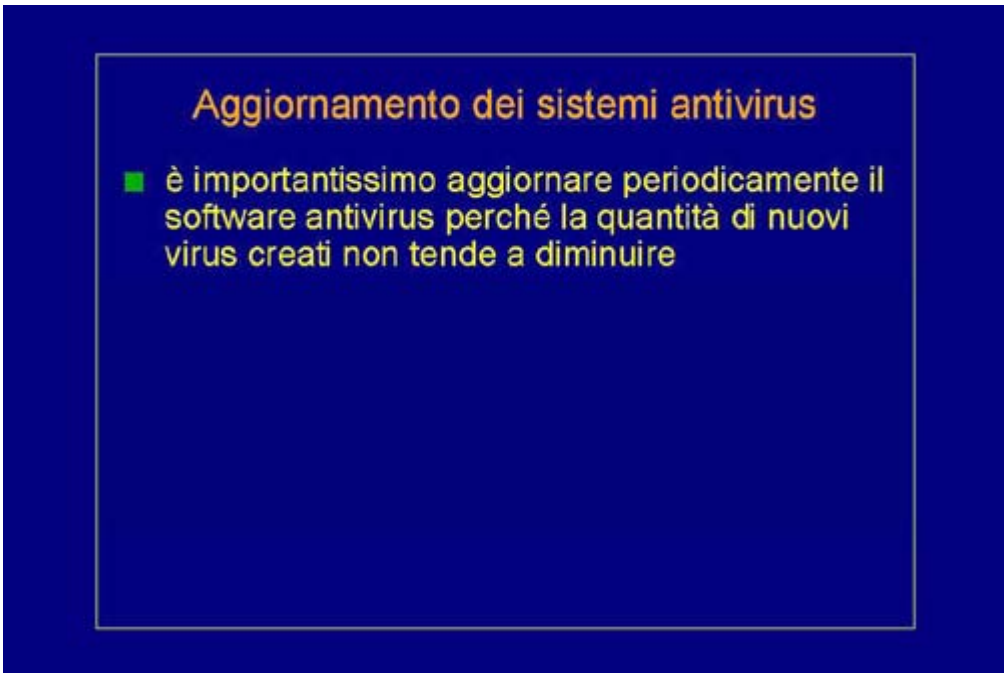
Come funziona, in generale, un sistema antivirus? Esistono varie strategie, alcune più efficaci, alcune meno efficaci; in particolare le strategie sono state affinate nel corso degli anni per rispondere ai nuovi tipi di virus che venivano sviluppati. I sistemi antivirus di prima generazione erano dei sistemi monto semplici, che non facevano nient'altro che ricercare quelle sequenze di istruzioni tipiche di un certo virus. Per ogni virus, veniva definita quella che è la sua signature: ossia le istruzioni tipiche che si trovano solo in quel virus. Il nostro software antivirus non faceva nient'altro che cercare quella sequenza di istruzioni all'interno di tutti i file presenti nel sistema. Gli antivirus di seconda generazione, invece, sono diventati un po' più sofisticati e, oltre a fare la ricerca delle stringhe tipiche dei virus, vanno anche a considerare il codice assembler generico, andando a vedere quali sono le tipiche modalità di operazione dei virus. Ad esempio: quando trovano all'interno di un file delle istruzioni che cercano di copiare un pezzo di questo file all'interno di un altro file, questo potrebbe essere un indizio della presenza di un virus. Oppure, ci sono software antivirus che calcolano il digest (il numero che permette di controllare l'integrità dei file) e vanno a verificare se il file è stato modificato dopo che questo digest è stato calcolato. Questo può essere indicazione di un'infezione virale in corso.

Funzionamento dei sistemi antivirus 2/2



I sistemi della terza generazione sono, invece, dei sistemi attivi on-line. Significa che esiste un programma attivo in continuazione sul nostro sistema, il quale controlla le azioni fatte da tutte le applicazioni e cerca di capire se le azioni che vengono svolte sono operazioni normali (lecite) di una applicazione, o sono invece azioni sintomo di un virus. Nel qual caso tende a bloccarle e a segnalare la presenza del virus. I sistemi più recenti, quelli cosiddetti della quarta generazione, ormai mischiamo insieme tutte quante queste tecniche. Anzi, fanno anche di più: molto spesso questi sistemi sono messi all'interno di un insieme di prodotti, diciamo di una suite di prodotti, che offre anche degli strumenti per elevare il livello di sicurezza, quindi anche il livello di protezione, di quei sistemi che abbiamo visto essere eccessivamente insicuri e quindi facilmente esposti ai virus.

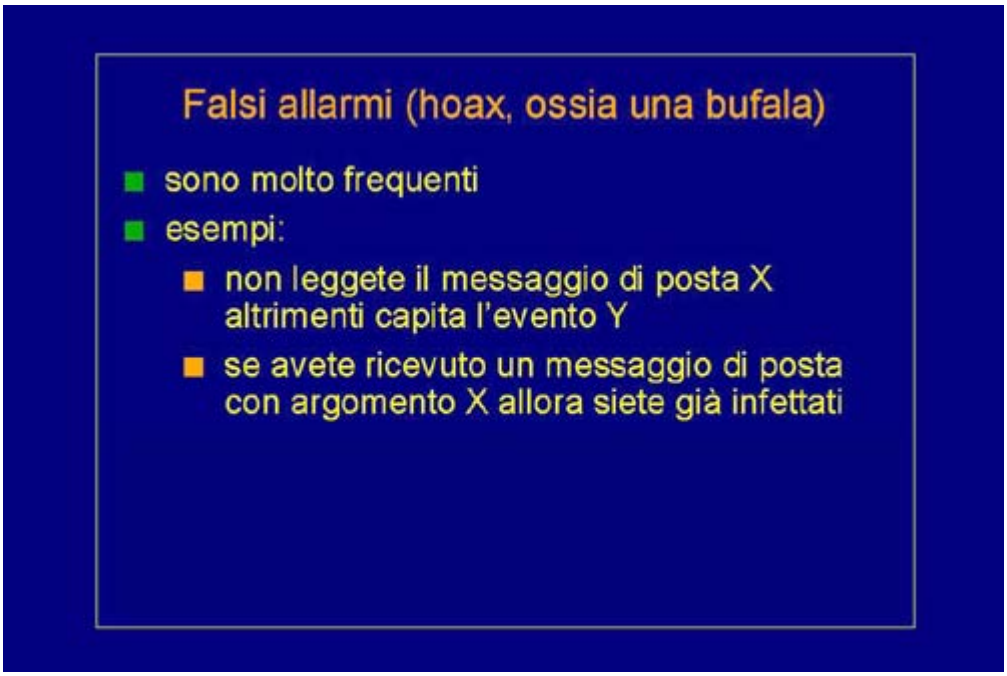
Aggiornamento dei sistemi antivirus



Bisogna ricordare che installare il software antivirus su un computer è una operazione necessaria, ma non sufficiente a garantirci la protezione da tutti i virus. Bisogna ricordarsi che, in generale, vengono sviluppati in continuazione decine e decine di virus. La stima è che ogni mese vengano introdotti in

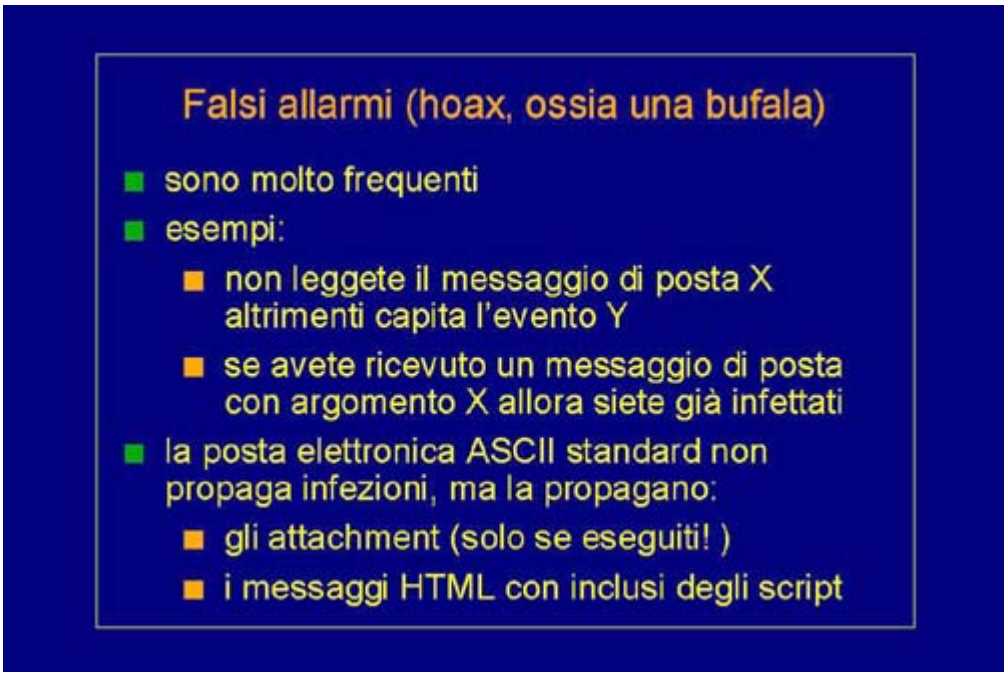
circolo alcune centinaia di virus di tipo nuovo. Questo significa che se io ho installato il software antivirus in una carta data, dopo sei mesi il mio sistema è aperto all'attacco di circa seicento nuovi virus, che non possono essere rivelati dal software esistente. È quindi importantissimo aggiornare periodicamente il software antivirus su tutte le macchine. Questo può significare due cose: la prima è aggiornare i file di informazioni, ad esempio quelli che contengono le stringhe tipiche dei virus. Ma questo può non bastare: a volte è necessario anche aggiornare il motore, ossia il programma che effettua la ricerca dei virus, proprio perché nascono in continuazione nuovi tipi di virus e nuove modalità di infezione. Quindi, anche avendo fornito nuovi dati, se l'applicazione antivirus non è stata pensata per rivelare un certo tipo di infezione, non sarà in grado, anche con nuovi dati, di rivelare i nuovi tipi di virus. Quindi: aggiornamento costante e continuo, sia dei dati che rappresentano i virus, sia del motore di ricerca dei virus.

Falsi allarmi (hoax) 1/2



Indirettamente collegata al virus c'è una tematica, che sarebbe divertente se non fosse in certi casi tragica. Molto spesso vengono diffusi via rete dei falsi allarmi: i cosiddetti hoax, o come diremmo noi italiani, delle bufale. Ossia delle cose che non stanno né in cielo né in terra, ma siccome gli utenti dei sistemi informativi non sono necessariamente degli esperti di informatica, riescono ad avere presa su molti utenti e a generare molto spesso delle azioni non appropriate. In particolare, questi falsi allarmi si stanno diffondendo con molta frequenza. Esempi: a me personalmente, e credo anche a molti di coloro che ascoltano questa lezione, è capitato di ricevere dei messaggi di posta in cui si dice: attenzione, non leggete il messaggio di posta X, perché altrimenti vi viene cancellato direttamente tutto quanto il disco. Questo è chiaramente un hoax, come vedremo tra poco. Oppure esistono degli altri avvisi che circolano in rete, che dicono: attenzione, se avete ricevuto un messaggio di posta con questo argomento, anche se non lo avete letto, siete già automaticamente infettati. Diciamo che, nell'immaginario collettivo, la posta elettronica diventa uno dei metodi di propagazione di virus più frequenti.

Falsi allarmi (hoax) 2/2



Allora voglio sottolineare che, in generale, la posta elettronica di tipo ASCII, quindi quella che contiene sono ed esclusivamente del testo, non può essere veicolo di propagazione di virus. La posta elettronica può propagare dei virus solo se contiene degli attachment, ossia dei pezzi aggiuntivi uniti al testo della posta elettronica, e se questi attachment sono di tipo eseguibile e vengono eseguiti. Quindi, è molto importante che sul proprio sistema, il programma di posta elettronica sia configurato in modo tale da non eseguire automaticamente gli attachment ricevuti. Prima di eseguire un attachment bisognerebbe sempre farlo passare al controllo di un software antivirus. Esistono anche degli antivirus che sono in grado di fare automaticamente il controllo degli attachment ancor prima che vengano letti. L'unica possibilità per cui un virus si annidi all'interno del testo di posta elettronica, è se il testo non è stato scritto in ASCII, ma in HTML. Questa è una caratteristica che gli e-mailer più recenti hanno: permettono la spedizione di messaggi di posta elettronica scritti in HTML. Questo permette di formattare, di abbellire, il nostro messaggio. Ma poiché l'HTML può contenere, al proprio interno, degli script Java o degli script Visual Basic, come abbiamo già visto poco fa, ecco allora che anche tramite un messaggio di posta elettronica ci può essere inviato un cosiddetto macrovirus (uno script virus) che ci infetta. Quindi sarebbe bene, anche in questo caso, disabilitare l'esecuzione di questi script, se presenti all'interno del testo del messaggio di posta elettronica che ci viene inviato.

La firma degli applicativi 1/2

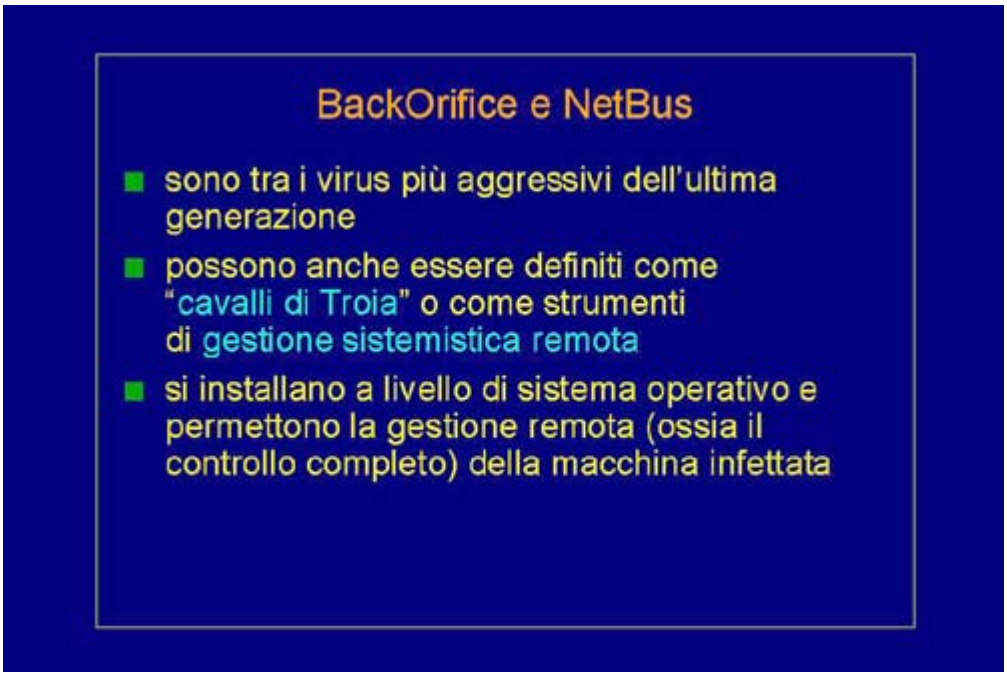
Esiste la possibilità di porre fine a questa infinita saga dei virus? Teoricamente la possibilità esiste e si basa sul concetto di firma digitale, che abbiamo già affrontato nell'ambito di questo corso, ma che vogliamo qui ribadire. La firma digitale di un insieme di dati ci permette di garantirne due cose: l'integrità e l'autenticazione. L'integrità ci permette di dire che i dati non sono stati modificati, da quando sono stati creati. L'autenticazione ci permette di identificare in modo univoco chi ha creato questi dati. È ovvio che se noi abbiamo un file, che è stato infettato da un virus, questo file non è più integro. Quindi se noi abbiamo calcolato la sua firma digitale prima dell'infezione e la ricalcoliamo dopo l'infezione, la firma digitale non sarà più la stessa. Quindi, la semplice verifica della firma digitale di un file ci permetterà di scoprire subito che è stato infettato e quindi di ripristinare il file originario, o almeno di cancellare il file infettato.

La firma degli applicativi 2/2

Questo significa che noi potremmo liberarci completamente dei virus, se all'interno dei nostri calcolatori tutto il codice eseguibile, sia quello direttamente in forma binaria (i programmi, le

applicazioni), sia quello annidato dentro ai dati (gli script), fosse firmato digitalmente. La firma digitale è un elemento necessario ma non sufficiente. Se anche noi avessimo tutti i dati firmati, questo non ci basterebbe a togliere i virus: bisogna anche che il sistema operativo che esegue il programma binario, o l'applicazione che utilizza i dati che a loro volta contengono lo script, prima di eseguire il file binario e prima di eseguire lo script, ne controllasse la firma. Se la firma indica che i dati sono stati manipolati, allora il sistema operativo e l'applicazione dovrebbero rifiutarsi di eseguirlo. Questa è una pia speranza? No, è una realtà quasi pronta per essere rilasciata. Cominciano ad esserci tracce di importanti ditte di software che stanno lavorando in questa direzione, per fornire sistemi operativi in grado di apporre e di verificare la firma digitale a tutti quanti gli eseguibili. Analogamente, ci sono ditte che stanno sviluppando applicazioni che controllano che gli script non siano stati modificati; anche in questo caso l'integrità degli script viene verificato tramite la loro firma digitale.

BackOrifice e NetBus



Concludiamo questa chiacchierata sui virus parlando di due virus che ultimamente hanno ottenuto una grande notorietà: si tratta di BackOrifice e NetBus. Questi sono due virus, particolarmente aggressivi, che sono stati sviluppati per gli ambienti di tipo Windows. Sono tra i virus più aggressivi tra quelli dell'ultima generazione e possono anche essere classificati come cavalli di Troia, o come strumenti di gestione sistemistica. Cavallo di Troia è normalmente un virus che si inserisce all'interno di un sistema, non per danneggiarlo direttamente, ma per aprirne le porte ai nemici che stanno fuori. Esattamente come il cavallo di Troia non serviva direttamente a danneggiare la città, ma serviva semplicemente ad aprire le porte della città agli attaccanti che stavano all'esterno. Di che cosa si tratta? Entrambi i sistemi, una volta installati su un sistema Windows, permettono la gestione remota di tutte le funzionalità della macchina. Allora, in senso benigno, possono essere visti come dei programmi di ausilio a un gestore di sistema che desidera gestire remotamente alcune macchine. Se però il BackOrifice o il NetBus è stato installato all'insaputa del proprietario della macchina, questo significa avere una porta aperta in cui una qualunque persona di passaggio sulla rete è in grado di controllare completamente la funzionalità del nostro sistema. E questa, ovviamente, è una cosa estremamente negativa e quindi sicuramente equiparabile a un cavallo di Troia o a un virus.