Medici, Computers e Virus... telematici

Data 26 ottobre 2001
Categoria scienze_varie

(di Massimiliano "Max" Vassura)

Premessa:
In seguito a diverse richieste mi son deciso a mettere giù queste semplici righe. Premetto che queste note non sono di alcuna utilità pratica per chi i PC li usa con una certa disinvoltura da anni: sono state scritte per medici assai poco pratici del mezzo telematico. Preciso inoltre che non ho alcun tipo di relazione commerciale con le società che vado a citare e che le mie sono semplici impressioni di un utente più che decennale di Personal Computers.
Da cosa dobbiamo difenderci?
La nostra macchina informatica, il nostro computer, può essere oggetto di diversi attacchi o tentativi di intrusione. Possiamo essere attaccati sia quando siamo collegati alla rete, sia quando siamo scollegati dalla rete. Sia quando navighiamo sia quando scarichiamo posta. Alcuni attacchi sono più diretti e ci siamo preparati, altri sono subdoli, o maliziosi come viene tradotto semplicemente dall'inglese.
In ordine sparso abbiamo i famigerati virus, gli script, gli ActiveX, i tentativi di intrusione, i programmi Back Orifice ed io aggiungo anche i programmi gratuiti secondo la formula AdWare. Per ognuno di questi daremo una sommaria descrizione:

· Virus: i virus nacquero qualche tempo fa, ancora prima della posta elettronica. Il sospetto è che siano nati dalle frustrazioni di progettisti software frustrati perché, a loro dire e forse con ragione, erano sottopagati ed il loro lavoro non era adeguatamente riconosciuto. Io stesso ho assistito ormai dieci anni fa alla costruzione di uno di questi software con codice virale incluso ed attivazione in una certa data. Devo dire che il progettista software qualche ragione (anzi, molte ragioni) le aveva. Anche se io cercai di dissuaderlo ed ottenni che lo presentasse come un bug del software e non come virus distruttivo. Nella maggior parte dei casi i produttori di virus li iniettavano in un programma di giochi famoso, copiavano il programma su centinaia di floppy e poi vendevano il floppy col programma ai gonzi che credevano che così avevano avuto il programma pagandolo dieci volte meno e senza "pagare dazio". In breve tempo questi gonzi si ritrovavano la macchina inservibile e dovevano riformattare il disco fisso con la perdita di dati magari molto preziosi per loro o per l'azienda per la quale lavoravano. Questa tecnica di sfruttamento dei gonzi è ancora usata: moltissimi programmino crack o warez che servono per proteggere le copie legali demo o shareware dei programmi, contengono del codice virale! Quindi è bene non fidarsi dallo scaricare dalla rete crack o warez, ma, nei limiti del possibile, comprarsi la copia regolare del software che si intende usare. Oggi la maggior parte dei virus arriva sotto forma di allegati di posta elettronica, anche se è ancora abbastanza usata la forma di infettare un gioco e renderlo disponibile sulla rete.

· Gli Script: sono come i virus, con l'unica differenza che mentre per fare un virus occorre un compilatore per trasformare il virus in un eseguibile, con lo script basta la conoscenza di un qualsiasi linguaggio di script (di solito il Visual Basic Script) ed il Notepad di Windows. Gli script sono delle piccole istruzioni che sono molto utili per scrivere delle righe di codice "al volo" per far fare qualcosa di utile alla macchina che le manda in esecuzione. Per esempio: le macro di word o di excel sono delle righe di script in visual basic. Oppure sulle pagine internet gli script sono quelle linee di codice che ci consentono di raggiungere un altro documento cliccando su un bottone, o che fanno eseguire piccole animazioni sulla pagine web. Il linguaggio script può quindi essere usato per commettere azioni illecite sulla macchina dell'utente. Classicamente i worm allegati alla posta sono degli script che vanno a leggere tutti gli indirizzi nella rubrica della posta elettronica e mandano una copia di sé stessi a tutti gli indirizzi che trovano nella rubrica. Alcuni si limitano a far questo, altri fanno anche danni sulla macchina sulla quale sono in esecuzione.

· Gli ActiveX sono una tecnologia nata per scopi di utilità, come il linguaggio script del quale sono una evoluzione, utilizzata per scopi dolosi. In realtà gli activeX consentono di utilizzare uno script molto complesso e quindi reso una specie di eseguibile per renderlo più veloce in esecuzione, e fare in modo che venga reso disponibile come risorsa per tutte le applicazioni che intendano usarlo. Uno dei più famosi activeX è il lettore di Macromedia Flash per le animazioni delle pagine web, oppure alcuni lettori per file multimediali Real Player o streaming audio vari. Quando andando su una pagina compare una finestra grigia che vi chiede di installare sul vostro PC un ActiveX, date il consenso solo se siete sicuri di ciò che state facendo..

· I tentativi di intrusione sono tentativi fatti da alcuni Hacker i quali, avendo del tempo da buttare, lo passano a scandagliare la rete ed i computer ad essa collegati per cercare di violarli e di entrare in rete. Bisogna dire che violare un pc senza che un programma in esecuzione su quel pc consenta l'intrusione è veramente difficile (anzi .. Credo impossibile). Il fatto è che molti programmi, e delle volte lo stesso Sistema Operativo, hanno degli errori di programmazione che inavvertitamente consentono l'intrusione da parte di Hacker sul nostro PC. Tutti, ripeto TUTTI i sistemi operativi hanno errori di questo tipo, probabilmente Microsoft Windows è quello che ne ha più di tutti, mentre quello che ne ha di meno è, in base alla mia esperienza, BSD.

· I programmi Back Orifice sono collegati ai tentativi di intrusione. Loro direttamente non creano alcun danno al PC sul quale sono in esecuzione, ma, come chiaramente detto dal loro nome .. Lasciano aperta una "porta posteriore", ed

in molti casi addirittura avvertono il loro creatore che la porta è aperta sul vostro computer. In un caso come questo chi vi ha mandato il BO prende possesso del vostro pc e può fare ogni cosa. Di solito è un burlone che si diverte a farvi aprire e chiudere in continuazione il cassettino del cd rom, oppure fa stampare alla vostra stampante frasi del tipo 'Scemo che sei!'. In casi meno giocosi, può copiare la vostra cartella dei documenti, per leggerseli con calma e vedere se può trovarvi qualcosa di interessante (numeri di Carte di Credito, di Conti correnti od altre amenità simili). Ho conosciuto persone che si son ritrovate una cartella dell'hd piena di foto porno di minori: in pratica hanno appoggiato queste foto sul pc dell'ignaro utente per condividerle con altri degenerati mandando in giro per la rete l'i.p. della vittima ogni volta che questa si collegava.

· I programmi AdWare come per esempio GetRight o Mozilla installano sul vostro pc un programma legal della Aureate, di cui vi si informa durante l'installazione: questo programma dovrebbe raccogliere informazioni sui siti che visitate e sulle vostre abitudini di navigazione e poi mandare tutte queste belle informazioni a non si sa chi per farci non si sa bene cosa. Personalmente NON uso questo tipo di programmi e come FTP uso il freeware LeechFTP. Se dovessi usare GetRight mi registrerei per non dover avere il programma spione.

Perché ci dobbiamo difendere e da chi?
Ci dobbiamo difendere perché anche se è vero che molti di questi attacchi non danneggiano il nostro sistema, è anche vero che molti di questi worm mandano in giro per la rete pezzi di documenti privati pescati nei nostri HD, mandano virus a persone che sono presenti nella nostra rubrica di posta elettronica e così via. Quindi, anche se è una ipotesi remota, qualcuno che ricevesse un virus potrebbe anche denunciarci. Inoltre molti di noi sono medici e non è sicuramente piacevole che qualche autorità venga informata che pezzi di nostri documenti, magari riguardanti pazienti e dati sensibili, stanno vagando per la rete. E ci dobbiamo anche difendere da tutti coloro che potrebbero fare un uso non corretto delle informazioni presenti sul nostro PC.
Come ci possiamo difendere?
Tengo a precisare che queste sono opinioni personali, e quindi spiegherò come mi difendo io, ma questo non vuol dire né che altri sistemi di difesa siano peggiori o che non possano esistere alternative valide. Personalmente uso una soluzione integrata che è composta da tre programmi in una unica suite: Ez-Arrmor della Computer Associated (http://my-etrust.com/products/info/Armor/1)
Questa suite contiene tre programmi di protezione da intrusioni virus script maliziosi e protezione da programmi scaricati da internet. In particolar modo il punto di forza è l'antivirus che è il discendente del popolarissimo e gratuito Inoculate It Personal Editino, a mio parere uno dei migliori antivirus in circolazione per di più con un servizio di assistenza assolutamente pronto, efficiente e preparato. Il firewall è un po' scarsino e non è facilmente intuitivo, ha il vantaggio di essere basato su tecnologia in grado di autoapprendere, ma i messaggi che da sono un po' troppo criptici per l'utente medio e medio basso, per di più non è molto configurabile. Un punto a favore di questa suite è desk Shield che fornisce una protezione a livello di desktop, identificando alcuni script maliziosi od alcuni comportamenti al limite della legalità di alcuni programmi e di alcune pagine internet. Desk Shield vi avverte e voi decidete cosa fare ..
Un altro punto a favore questa suite è che costa assai poco, non richiede di essere superesperti per funzionare e per essere configurata. Insomma: un ottimo prodotto per chi non è esperto o per chi essendo esperto non ha voglia di perder tempo a configurare i vari programmi. Per di più l'antivirus è veramente buono con aggiornamenti anche bi o trigiornalieri!!! E se non ci si aggiorna, dai server americani ci mandano una mail per informarci che dobbiamo aggiornarci.
Per chi non amasse le suite, allora consiglio due prodotti:
Zone Alarm: firewall gratuito che è per me il meglio che c'è sul mercato attualmente. Ha solo l'inconveniente di considerare quasi tutti gli allegati della suite office dei virus e di segargli l'estensione. Se avessero lasciato che facesse solo il firewall forse sarebbe stato meglio. La versione PRO a pagamento è ancora più versatile e potente.
(http://www.zonelabs.com/)
Come Antivirus consiglio invece AVP del Kaspersky Lab russo che è acquistabile in italia sul sito di Paolo Monti della Future Time. AVP, per i .. Micragnosi dalle braccine corte J, viene regalato mese per mese sulla rivista CHIP acquistabile in edicola. (http://www.avp.it/)
Spero di essere stato abbastanza chiaro, ma se avete domande da fare scrivetemi pure a vassura@libero.it