

Virus, questi sconosciuti ... ossia Nozioni di sicurezza informatica per tutti

Inizia qui quella che, spero, sia una lunga e proficua collaborazione con questa rivista. Innanzitutto due parole di presentazione: mi occupo da oltre venti anni di informatica e, precisamente, di formazione e di divulgazione ... come dire, cerco di insegnare e di rendere chiaro a tutti l'uso degli elaboratori elettronici e dei programmi che li fanno funzionare: una vitaccia ma, in fondo, lavorare in miniera è peggio.

Nel fare questo cercherò di limitare al massimo l'uso di termini tecnici, a costo di apparire banale, ma devo adattarmi anche ai lettori meno addentro la materia. Nel caso debba usare una "parolaccia" ne darò immediatamente la spiegazione.

Bene, abbiamo rotto il ghiaccio e, quindi, possiamo iniziare ad entrare nel vivo dell'argomento: chiunque usi, per lavoro o per diporto, un elaboratore elettronico sa, o dovrebbe sapere, che è esposto al rischio di essere "infettato" da programmi ostili, comunemente detti "virus". Vedremo in seguito che la categoria, in realtà, è molto composita e variegata e che il termine "virus" è, spesso, usato in modo generico anche per indicare programmi ostili che, a rigore, virus non sono.

In molti lettori, a questo punto, può sorgere spontanea una domanda: ma chi può avere interesse a creare i virus, e perché? Le risposte in merito sono diverse: un programma ostile può essere creato per scopi illeciti, come nel caso dei cavalli di Troia (più noti come trojan), per studio, oppure, anche se sembra incredibile, per vanità.



Nel 2000 si diffuse via Internet, e fece grandi danni, un virus, o meglio un worm, dal romantico nome di "I love you": le indagini appurarono che a realizzarlo e a diffonderlo erano stati dei ragazzini di Manila e che lo avevano creato per far parlare di loro. C'è un illustre precedente in proposito: il pastore Eratostrato che, nel 356 a.C., incendiò il tempio di Artemide a Efeso, considerato una delle sette meraviglie del mondo, solo perché desiderava diventare famoso ... come si vede, niente di nuovo sotto il sole.

Quanto ai virus diffusi per scopi illeciti, a parte i già citati trojan, che servono ad assicurare ad un estraneo il controllo del nostro elaboratore, si stanno diffondendo, anche se per ora in modo piuttosto limitato, altri componenti nocivi, i cosiddetti "ransomware", che, insediatisi nel sistema, bloccano i file personali dell'utente, rendendoli di fatto inutilizzabili. Per tornare ad avere la piena padronanza dei propri file l'utente attaccato deve mettere mano al portafoglio e pagare un riscatto. In letteratura è citato un caso piuttosto recente (la notizia è del 21 maggio scorso) di un programma, chiamato CryZip, che crea un archivio compresso protetto da password all'interno del quale "blinda" file dell'utente: per ottenere la password e sbloccare i propri dati occorre provvedere al versamento di 300 dollari.

Un altro esempio di file ostile creato per scopi illeciti? Eccovi accontentati: un'azienda che si occupa di sicurezza informatica ha scoperto, nello scorso mese di aprile, un trojan, denominato Trojan-Phisher-Rebery, distribuito attraverso un sito web dai contenuti pornografici: questo programma contiene funzionalità che permettono il furto dei dati inseriti nei moduli online, e di catturare screenshot (cioè un'istantanea di ciò che appare sul monitor del computer), raccogliendo, quindi, informazioni riservate anche per questa via.

I virus, comunque, già da tempo hanno iniziato a comparire anche sui quotidiani e sugli altri mezzi di informazione anche se, a dire il vero, non sempre le notizie date sono precisissime anche per superficialità e incompetenza di chi le dà.

Cerchiamo adesso di sfatare alcune false percezioni che si possono essere formate negli anni, anche per carenze informative. Innanzitutto ricordate che la sicurezza informatica non è un problema occasionale, da rammentare quando il telegiornale informa su una nuova infestazione (come nel febbraio scorso con il virus denominato Kamasutra): dobbiamo fare i conti tutti i giorni con virus e affini. Per un programma ostile che conquista gli onori delle cronache, perché particolarmente virulento o per la sua larghissima diffusione, ce ne sono migliaia di altri che restano esclusi da tale ribalta.

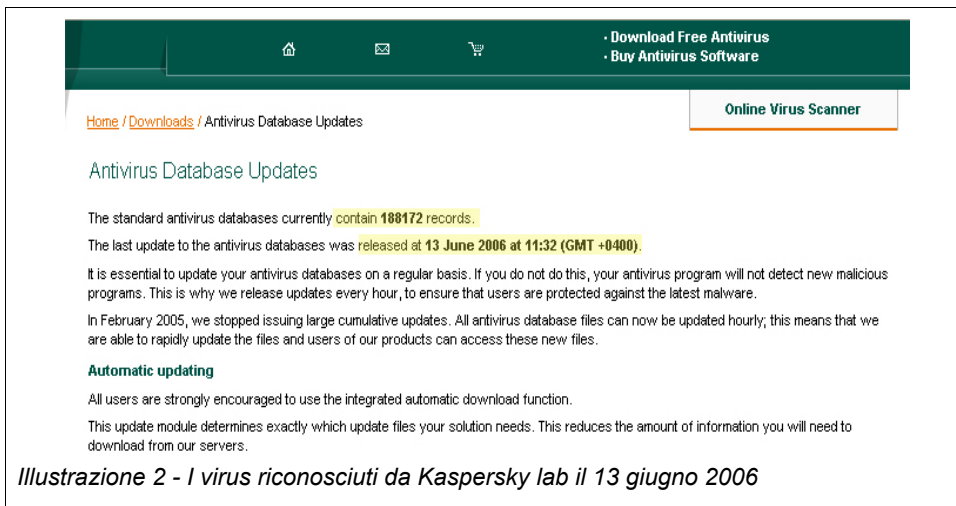


Illustrazione 2 - I virus riconosciuti da Kaspersky lab il 13 giugno 2006

Già, perché quanti sono i virus conosciuti? Cinquanta? Cento? Mille? Siete tutti fuori strada ... uno dei più noti produttori di software antivirus, Kaspersky Lab, il 13 giugno 2006, ha, in archivio, 188.172 virus.

Un altro celebre produttore di antivirus, Symantec, indica di aver scoperto 104 nuove minacce nel periodo 15 maggio – 13 giugno 2006.

Altra falsa percezione è quella di non avere nulla

da temere perché non abbiamo archivi segreti, informazioni top secret e chissà quali altre invitanti meraviglie. Nessuno è inattaccabile: sul nostro computer sicuramente abbiamo archiviato i nostri dati personali, abbiamo traccia dei movimenti eseguiti con la carta di credito e possediamo una ghiottissima rubrica di indirizzi di posta elettronica, oggetti questi che ci rendono obbiettivi potenzialmente interessanti per i malintenzionati e ci espongono ad attacchi informatici. Occorre poi considerare anche un'altra cosa: l'attacco di virus e altri

software ostili non è mirato, se non in rari casi, ma indiscriminato. In pratica colpisce nel mucchio: certi virus, diffusi un paio di anni fa, come Sasser e Blaster, attaccavano chiunque si connettesse ad Internet senza adeguata protezione ... non occorre fare nulla, semplicemente collegarsi alla rete (esperienza fatta da chi vi scrive ...).

Vediamo adesso in quali categorie si possono suddividere i programmi nocivi, quelli che, finora, abbiamo genericamente indicato come virus, ma che è sicuramente più corretto chiamare mal-



Illustrazione 3 - Le minacce virali più recenti secondo Symantec

ware o software ostili. Ecco, quindi, il nostro bestiario informatico:

- virus propriamente detti: sono programmi dotati di una certa autonomia operativa, in grado di replicarsi e di alterare il funzionamento del computer in modi che variano da una semplice manifestazione della loro presenza, a un degrado delle prestazioni dell'elaboratore, alla perdita di dati e programmi. I virus possono infettare il settore d'avvio (boot sector) dell'elaboratore, installarsi nella Ram o attaccarsi ai file eseguibili. Si tratta di programmi e quindi entrano in azione solo se eseguiamo il programma infetto;
- worm: si replicano all'interno di un sistema un numero indefinito di volte fino a saturarlo; disattivano gli antivirus e i programmi che gestiscono gli aggiornamenti, assumono il controllo del client di posta elettronica ed iniziano ad inviare messaggi infetti a tutti gli indirizzi della rubrica o ad altri generati automaticamente; possono anche stabilire connessioni con siti dai quali scaricano altri malware, come i trojan;
- trojan (o cavalli di Troia): sono programmi inizialmente non identificati come virus che, tramite la connessione a Internet, consentono ad un estraneo di entrare nell'elaboratore infettato attraverso una backdoor (porta posteriore) appositamente creata. Il proprietario del cavallo di Troia, si trova così a poter gestire una rete clandestina (botnet) costituita da numerosissimi elaboratori infetti (i cosiddetti

zombie) e la può usare per i suoi scopi, di solito illegali. Un cavallo di Troia, infatti, può essere impiegato per raccogliere informazioni riservate (ad esempio numeri di carte di credito e relativi codici segreti, password per l'accesso a siti riservati, file contenenti dati sensibili eccetera), oppure per fornire al gestore della botnet una formidabile potenza di fuoco da impiegare per lanciare attacchi Dos (Denial of Service) che mettono fuori uso siti e server, bombardandoli con migliaia di tentativi di accesso contemporanei o di messaggi di posta elettronica. Spesso questi attacchi si risolvono in una tentata estorsione o servono a coprire un tentativo di accesso a informazioni riservate. Una botnet, infine, può permettere al suo autore anche di compiere operazioni di spamming (invio non richiesto di messaggi pubblicitari che, spesso nascondono truffe) o di scaricare illegalmente da Internet software, film, brani musicali o altri contenuti coperti da diritto d'autore o da altri vincoli analoghi, consentendogli l'anonimato e l'impunità. Il computer infetto, infine, può essere utilizzato per ospitare contenuti illegali, quali immagini di tipo pedo pornografico, garantendo così l'impunità a chi controlla lo zombie;

- spyware (da spy, spia), o adware (da advertising, pubblicità): piccoli software che, tramite Internet, inviano a terzi (ad esempio a società commerciali), e all'insaputa dell'utente, informazioni sulle sue preferenze di navigazione, con ovvia violazione della privacy. Questi piccoli programmi possono entrare, consensualmente o di nascosto, con l'installazione d'altri programmi, dei quali, in certi casi, è concesso l'uso gratuito. Gli spyware non devono essere confusi con i cookie, file di testo che contengono informazioni sui siti visitati dall'utente: in questo caso è il server che ospita il sito che crea il cookie e lo archivia sul computer dell'utente, per andarne a verificare l'esistenza durante un successivo collegamento. I browser più evoluti avvisano della loro presenza e lasciano all'utente la possibilità di accettarli;
- dialer: sono programmi che trasformano la semplice chiamata urbana al gestore di telefonia o all'Internet Server Provider che fornisce il collegamento, in una costosissima telefonata internazionale, parte dei proventi della quale è destinata a chi ha, più o meno fraudolentemente, fornito tale software. Si possono installare cercando di accedere a siti che offrono beni o servizi di ogni genere, come ad esempio suonerie, software a basso prezzo, immagini o filmati pornografici, casinò on line.

Un discorso a parte, ma meritevole di un cenno, è quello relativo ai cosiddetti hoax, in inglese burla: con questo termine s'intendono tutte quelle false notizie, diffuse per mezzo di messaggi e-mail, relative alla diffusione di nuovi, potentissimi virus contro i quali non c'è difesa alcuna, oppure alla possibilità di ricevere gratis telefoni cellulari e simili. Un caso abbastanza recente segnalava come virus un file parte del sistema operativo Windows e consigliava tutta la procedura da seguire per cancellarlo. I danni prodotti dagli hoax sono indiretti, perché possono spingere a compiere azioni potenzialmente nocive per il corretto funzionamento dell'elaboratore (come nel caso appena descritto), oppure perché la loro diffusione crea traffico inutile su Internet.

A questo punto, come si scriveva una volta nei romanzi d'appendice, non mi resta che concludere con "il resto alla prossima puntata", nella quale esamineremo come è possibile riconoscere queste minacce e mettere in atto utili accorgimenti per proteggerci.

Articolo pubblicato per gentile concessione della rivista "Porto e Diporto" della AM editori Srl - Napoli