Le tipologie virali

Iniziamo da questo mese una serie di articoli sulla problematica dei virus informatici, uno dei problemi più diffusi, spesso sottovalutato, tra gli utenti di PC

di **Gianfranco Tonello** (tge@maya.dei.unipd.it)

I virus informatici hanno rappresentato e rappresentano un pericolo per i dati e le informazioni dei calcolatori. Iniziamo, in questo numero, a conoscere le varie tipologie virali, per poi analizzare nel proseguo, la struttura dei cosiddetti codici virali e osservare il mondo dell'underground informatico dove "bazzicano" i virus-writer.

Prima d'iniziare, vogliamo chiarire le idee su che cosa sia un virus e quale sia la differenza con i cosiddetti "Cavalli di Troia".

Un virus informatico chiamato anche codice virale, è un programma in grado di autoreplicarsi. Considereremo appartenenti a questa famiglia tutti i programmi che hanno la capacità di eseguire una copia di se stessi in modo autonomo. I cavalli di troia, o "trojan horses", sono dei programmi che all'apparenza si presentano invitanti, ma gli scopi e gli effetti sono diversi da quelli previsti dall'ignaro utente, come la sovrascrittura o formattazione del disco fisso o la cancellazione di file. Un cavallo di troia differisce da un virus per la mancanza delle routine di autoreplicazione, ma non per gli effetti. Al contrario, un virus può avere gli effetti di un cavallo di troia ma possiede la capacità di replicarsi cioè di rendere "maligni" anche altri file.

Le tipologie virali si possono classificare in due distinte categorie. Alla prima appartengono i codici virali che infettano il boot sector e/o il master boot record (MBR), alla seconda appartengono i codici virali che colpiscono i file. Alcuni virus, poi, sfruttano entrambe le peculiarità delle due tipologie citate, nel qual caso prendono il nome di "virus multipartiti". Alcuni esempi di codici multipartiti con cui ci possiamo scontrare con una certa frequenza sono i virus della famiglia Arianna (il più attivo segnalato risulta essere la variante lunga 3375 bytes), della famiglia Marzia (il più attivo risulta essere la variante .D) e buon ultimo, ma non certo per diffusione, l'INVISIBLE_MAN.2926. Le famiglie virali citate sono di origine italiana, sviluppato sembra nel barese la prima e nel pisano la seconda, mentre l'INVISIBLE_MAN sembra essere stato sviluppato nel salernitano. Nel nostro Paese però risulta essere "vivace" la presenza di un virus multipartito svedese, chiamato Junkie.1027, scoperto in Italia nel settembre 1994.

I virus che infettano il boot sector

I virus del boot sector hanno la caratteristica di infettare il settore di bootstrap dei floppy disk, essendo questo l'unico settore che può essere eseguito durante la fase di boot di un calcolatore. Il codice virale per propagarsi da un floppy disk infetto deve essere "dimenticato" all'interno del disk drive durante la fase di partenza del calcolatore, in modo che venga eseguito il boot sector, dopodiché comparirà a video il consueto messaggio: "Non-System disk or disk error. Replace and press any key when ready". A questo punto il codice virale sarà attivo in memoria pronto a diffondere la propria infezione. Normalmente verrà infettato o il Master Boot Record (MBR) del disco fisso o il settore di boot della partizione attiva dell'hard disk e ogni floppy disk non protetto in scrittura che verrà utilizzato quando il codice virale è attivo in memoria.

Il codice virale, infettando il Master Boot Record o il boot sector della partizione attiva del disco fisso, ha la facoltà di essere attivo in memoria nel caso il calcolatore parta da disco fisso. Appartengono a questa classe l'endemico Form di origine svizzera, l'RPS2 molto attivo a Brescia e in Lombardia, il Parity_Boot, il Bye e l'AntiExe, per citarne alcuni tra i più diffusi nel nostro Paese.

Purtroppo, ogni qual volta i ricercatori analizzano e classificano i virus per tipologia in qualche sperduto angolo del globo terreste, vi è qualche buontempone che pensa bene di creare qualche nuovo agente patogeno sfruttando metodologie d'infezione di nuova concezione, a tale proposito citiamo il virus 3APA3A, il primo codice virale che infetta il kernel. Questo codice virale è stato scoperto nell'Ottobre del 1994 in Russia dal ricercatore Igor G. Muttik del dipartimento di Fisica dell'Università di Mosca. Il virus infetta il boot sector dei floppy disk nel modo "consueto", mentre nel disco fisso infetta i file kernel del DOS: IO.SYS e IBM-BIO.COM ecc., viste le sue peculiarità potrebbe costituire una tipologia virale che potremo chiamare "kernel infectors".

I virus che infettano i file

È composta dai codici virali che attaccano i file contenenti codici eseguibili o informazioni che possono essere eseguite, questi file normalmente hanno estensione tipo .COM, .EXE, .OVL ma possono avere anche estensioni .DOC o .PIF eccetera.

L'alterazione del file colpito è dipendente dalla struttura del file e dalle caratteristiche del codice virale. Ad esempio un file con struttura .COM può essere alterato in almeno cinque modi diversi:

1) il codice virale si inserisce all'inizio del file (tecnica utilizzata dal virus Jerusalem);
2) il codice virale si accoda alla fine del file ed inserisce un jump (un salto) all'inizio del file che punta alla coda virale (tecnica utilizzata dalla maggior parte dei codici virali);
3) il codice virale si inserisce in più punti in mezzo al file. Questa metodologia è poco utilizzata perché estremamente complessa (tecnica utilizzata dal virus OneHalf di origine Slovacca e dal virus Peace_Keeper dell'italiano Doctor Revenge);
4) il codice virale sovrascrive l'inizio del file, in questo caso il file colpito non risulta allungato e la tipologia virale è definita overwriting (tecnica utilizzata dal virus Burger);
5) il codice virale cerca all'interno del file una zona continua di byte costanti, ad esempio di zeri, poi questa viene sovrascritta con il codice virale e inserito un jump all'inizio del file per puntare al corpo del virus, il file colpito non risulta allungato (tecnica utilizzata dal virus Lehigh);

Categorie di base

I virus che colpiscono i file, si possono suddividere in due categorie in base alla metodologia d'infezione adottata: azione diretta e residenti in memoria. I virus ad azione diretta utilizzano un proprio schema o tattica d'infezione, all'esecuzione di un programma infetto il virus cerca un altro file da infettare all'interno del disco. La scelta della vittima è dipendente dal tipo di virus, alcuni codici virali infettano i file solo all'interno della corrente directory, altri cercano nell'albero delle directory in base ad uno schema predefinito o pseudocasuale. Un virus molto diffuso in passato nel nostro Paese, che utilizza la metodologia ad azione diretta, è lo Stardot del quale sono note numerose varianti Stardot.600, Stardot_789.A, Stardot_789.B tanto per citarne alcune.

Virus TSR

I virus residenti in memoria sfruttano la capacità di essere programmi TSR (terminate stay resident). Quando viene eseguito un file infetto, il codice virale si installa in memoria rimanendo in attesa che l'utente compia delle operazioni tali da permettergli di infettare i file. La strategia di attivazione d'infezione è legata al tipo di virus, le più usate sono l'esecuzione, l'apertura e la rinominazione di file da parte dell'uten-

Glossario

Boot Sector: Il primo settore di una partizione o di un floppy disk, contiene le informazioni del formato, cioè il numero di byte per settore, il numero di settori per traccia eccetera.

CMOS: Acronimo di "Complementary Metal Oxide Semiconductor". Indica un'area di memoria utilizzata nei sistemi AT e PC per il salvataggio delle informazioni di sistema, generalmente utilizzata per mantenere le informazioni della data e ora mentre il PC è spento. La memoria CMOS non è un normale indirizzo di memoria per la CPU, in questa area non può essere eseguito codice. Un virus può sovrascriverla o corromperla con il proprio codice, ma non potrà mai essere eseguito.

Device Driver: Sono programmi overlay per il kernel, che vengono caricati dal DOS in memoria, i quali implementano delle funzioni per il supporto di hardware extra. Il device driver può essere visto come un'estensione del sistema operativo.

Kernel: Il sistema operativo DOS risiede principalmente in due file, uno di questi è MSDOS.SYS, che contiene il kernel del DOS. Il DOS kernel non è altro che il gestore dei servizi delle applicazioni (programmi) attraverso l'interfaccia dell'interrupt 21H, che consiste in un set di funzioni del sistema.

MBR: Acronimo di "Master Boot Record", indica il primo settore assoluto del disco fisso di un PC (traccia 0, testina 0, settore 1), che usualmente contiene la tabella delle partizioni, cioè le informazioni della ripartizione del disco fisso.

TSR: Acronimo di "Terminate and Stay Resident", sono programmi PC che rimangono attivi in memoria mentre il calcolatore può essere utilizzato per altri scopi. Normalmente i programmi TSR sono utility, software di rete e purtroppo buona parte dei codici virali attualmente circolanti nel nostro Paese.

te. L'apertura dei file è una delle "strategie" che possono addirittura sfruttare l'utilizzo degli antivirus per propagare l'infezione. Infatti nell'ipotesi di utilizzo di software antivirus datati che non riconoscano il virus in oggetto, attivando la scansione (che comporta l'apertura dei file), essendo il virus in memoria l'utente con questa operazione contribuisce a propagare l'infezione su parte e/o tutti i file scanditi (cioè aperti dallo scansore per verificare la presenza di virus noti).

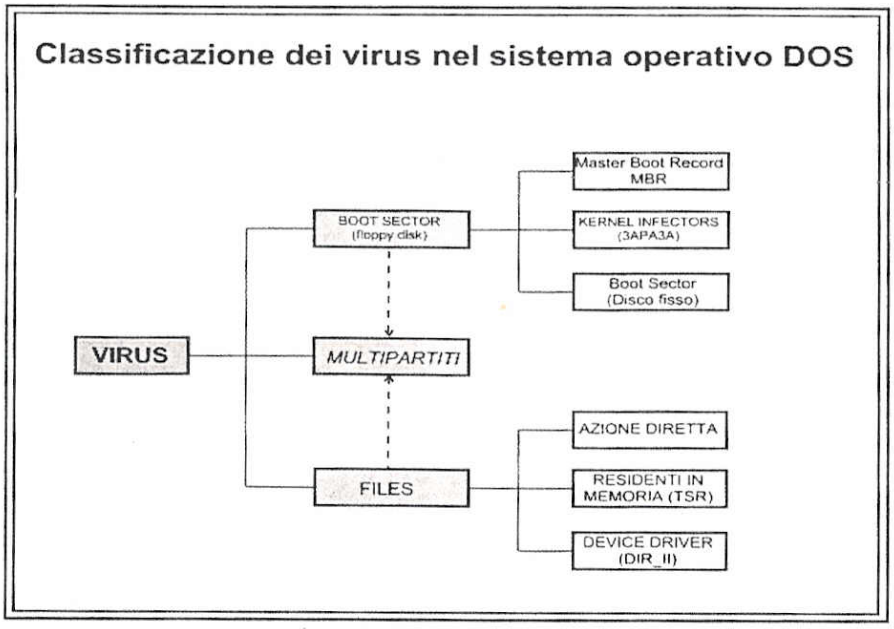
Un codice virale TSR che utilizza queste tecniche è considerato un virus ad infezione veloce (fast infection), un esempio è il virus Dark Avenger di origine bulgara dell'omonimo autore.

Virus gemellari

Una metodologia d'infezione che può essere utilizzata sia dai virus ad azione diretta sia dai virus residenti in memoria è quella dei codici virali gemellari. Questi virus sfruttano una peculiarità del sistema operativo DOS che conferisce priorità di esecuzione a file con estensione .COM rispetto ai file con estensione .EXE. Questa caratteristica permette di non modificare file esistenti, creando però nuovi programmi che possono essere eseguiti dalla linea di comando. Normalmente il programma generato ha estensione .COM e attributo nascosto e porta il nome di un file esistente .EXE. Quando l'utente esegue un programma, il sistema operativo DOS manda in esecuzione il programma con estensione .COM, invece di quello .EXE. In questa situazione viene eseguito il programma generato dal virus, da questo verrà mandato in esecuzione il programma .EXE che l'utente aveva l'intenzione di eseguire. Questa tecnica è utilizzata dal virus HL-LC.Crawen.8306 molto attivo nel triveneto.

Device Driver virus

Tra i virus "atipici" infettanti i file, citiamo il codice virale Dir_II, il quale potrebbe costituire una classe a parte dei Device Driver Virus. Il codice virale ha le peculiarità di non infettare il boot sector o i file nei modi citati, ma di infettare le "directory". Il virus Dir_II è un device driver, con lo scopo di alterare lo Starting Cluster (posto nel settore delle directory) dei file con estensione .COM e .EXE, facendolo puntare al corpo del virus. Gli autori del Dir_II (secondo le notizie riportate nel documento The Bulgarian and Soviet Virus Factories redatto da Vesselin V. Bontchev ex V.T.C. dell'Università di Amburgo) sono due ragazzi della Mathematical High School di Varna (città che si affaccia sul Mar Nero in Bulgaria).



Classificazione dei virus.

Conclusioni

Esiste una leggenda metropolitana che circola tra i negozianti e rivenditori di computer. Si dice che i codici virali infettino con insistenza la CMOS. Se un codice virale sovrascrivesse tale area di memoria, non potrebbe replicarsi, in quanto non verrebbe più eseguito. Un virus per replicarsi deve essere eseguito e la CMOS non è un'area attivabile. Le aree generalmente colpite sono il boot sector e/o master boot record e i file. Sono da evitare comportamenti a rischio quali l'utilizzare di floppy di incerta provenienza, ma soprattutto evitare di dimenticarli all'interno del drive all'atto dell'accensione. Per i floppy di sistema o bootabili, consigliamo di proteggerli dalla scrittura, ricordiamo inoltre, per chi ha la fortuna di possedere i dischetti originali del DOS, che il primo di questi è di tipo "bootable" e che è buona norma conservarlo protetto dalla scrittura (finestrella aperta), così da preservarlo da infezioni. L'utilizzo legale del software è il primo passo verso la sicurezza dei nostri programmi e dei nostri dati.

Gianfranco Tonello è ricercatore antivirus e sviluppatore del pacchetto antivirus VirITPro, disponibile anche in versione freeware chiamata VirIT Lite.
Può essere contattato inviando un e-mail all'indirizzo: tge@maya.dei.unipd.it.