Le caratteristiche dei codici virali

Nel precedente articolo abbiamo visto come si suddividono le varie tipologie virali, in questo numero analizzeremo alcune caratteristiche che possono assumere i virus informatici, come il divenire invisibile (stealth), il crittografismo e il polimorfismo

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

Virus stealth: essere invisibili

I virus stealth hanno lo scopo di non rendersi visibili all'utente, cioè di mostrare la situazione antecedente all'infezione o di nascondere le alterazioni che hanno eseguito sulle macchine colpite. Questa caratteristica può variare dalla tipologia virale, in particolare i virus residenti in memoria (TSR) sono maggiormente portati ad avere questa particolarità rispetto a quelli che non si installano in memoria. I virus stealth che infettano il boot sector e/o il master boot record (MBR) hanno la caratteristica di visualizzare il boot sector o l'MBR originale nel caso si tenti di analizzare/visualizzare il settore infettato dal codice virale. In questa situazione l'utente non è in grado di accorgersi della modifica eseguita, sulla macchina, dal codice virale. Questa capacità dei virus stealth infettanti il boot sector è dovuta al fatto che risulta essere residente in memoria prima di ogni altro software, perché l'installazione avviene ad ogni accensione della macchina quanto viene eseguito l'MBR. In questo modo, come è facile intuire, il virus può controllare a suo piacimento il calcolatore. Un modo per bypassare il codice virale è quello di far partire la macchina da un disco di boot pulito, in questo modo il virus non sarà attivo in memoria e la lettura del boot sector e/o master boot record infetto mostrerà il settore infettato dal codice virale. Il primo virus segnalato circolante, che ha implementato la caratteristica dell'invisibilità è stato il Pakistan Brain. Questo codice virale, ormai entrato nella "storia" dei virus informatici, infetta il boot sector del floppy disk, e la caratteristica di invisibilità è legata al monitoraggio delle chiamate I/O del disco, le quali vengono reindirizzate ad ogni lettura del boot sector infetto al settore che conteneva il boot sector originale. Oltre al Pakistan Brain (ormai estinto), non è raro incontrare nel nostro Paese alcuni virus aventi la caratteristica descritta, tra questi citiamo: GoldBug, Parity_Boot, AntiExe, Kampana, Ripper, Run_Error_504D:5658 e altri meno noti al grande pubblico.

I virus stealth che infettano i files hanno la capacità di mostrare la lunghezza originale e/o il corpo integro dei files infetti. In questo modo l'utente non si accorge che i files si sono allungati di una certa quantità (fissa o variabile) di bytes rispetto alla sua originaria lunghezza. Questa tecnica può essere implementata dal codice virale in vari modi. Quella maggiormente utilizzata è di marcare nel campo dell'ora, la sezione dei secondi con il valore 62 (valore anomalo tenuto conto che la sezione dei secondi può avere un valore normale, per l'uomo, tra 0 e 59) ogni files infetto. In questo modo il codice virale, che è residente in memoria (TSR), all'esecuzione del comando DIR, funge da filtro togliendo da tutti i files marcati con il valore 62 nella sezione dei secondi (quindi infetti) la propria lunghezza. In questo modo all'utente verrà visualizzata la lunghezza originale del files e non quella allungata dal virus.

Alcuni codici virali hanno implementato altre funzioni di invisibiltà, come quella di mostrare il corpo del programma originale all'apertura del file, tra questi citiamo il Grog.Lor.

Gli antivirus per intercettare questi codici virali utilizzano tecniche particolari per aprire i files in modo da bypassare il possibile virus o individuano il virus quando è attivo in memoria. In questo ultimo caso procedendo attraverso un disco di boot pulito, si può intercettare il codice virale nel files essendo questo non attivo in memoria.

Virus crittografati

I virus crittografati hanno la caratteristica di non mostrare il proprio aspetto, cioè il proprio codice. Sono costituiti da una routine di decrittografazione, che è l'unica parte del codice visibile, la quale serve a decifrare il corpo del codice virale. La routine di decifrazione può utilizzare una o più chiavi per decrittografare il codice virale, nella maggior parte dei casi la chiave di decrittografazione è variabile come nel caso del virus Cascade (noto anche come 170X), ma può esssere costante come nel caso del virus November_17th.900.C, molto attivo in Italia nel 1995.

Nella maggior parte dei casi, la routine di decrittografazione è costante ed a chiave variabile, cioè ad ogni infezione la procedura o la funzione di decifrazione è sempre la stessa. Se la funzione è mutante o variabile, il codice virale viene detto polimorfico o mutante. La procedura di decifrazione è costituita da un ciclo (loop) avente una funzione che

va a scrivere in memoria le funzioni maggiormente utilizzate. Queste generalmente coinvolgono gli operatori di addizione (ADD), sottrazione (SUB) ed OR esclusivo (XOR).

Virus polimorfici: l'arte di saper mutare

Un virus polimorfico ha la caratteristica di mutare il proprio aspetto ad ogni infezione, rendendo in questo modo complessa la sua individuazione. Un codice virale può anche non essere crittografato per essere polimorfico, anche se la crittografazione ne può facilitare il polimorfismo. Mutare il proprio aspetto ad ogni infezione, cioè il proprio codice, così da ottenere il medesima funzionalità, permette al virus di propagarsi rendendo maggiormente difficoltaso l'opera di intercettazione prima e rimozione poi da parte dei software antivirus. La maggior parte dei codici virali polimorfici sono crittografati, hanno la capacità di mutare (riscrivere) in vari modi diversi il proprio codice grazie ad una routine di decrittografazione che permette di ottenere un codice sempre diverso ma in grado di compiere le medesime operazioni.

I virus polimorfici si possono suddividere in cinque gruppi: virus oligomorfici; virus che utilizzano un decrittatore costante con opcode/registri variabili; virus altamente polimorfici; virus permutati; e virus che si basano su motori polimorfici. I virus oligomorfici hanno la caratteristica di avere una quantità predefinita di mutazioni. Questi codici virali utilizzano una o più routine di decrittografazione, ad ogni infezioni viene scelta la routine da utilizzare. Ad esempio il codice virale Screaming_Fist.II utilizza 2 decrittatori, invece il Whale ne utilizza ben 30.

I virus polimorfici che utilizzano un decrittatore costante con opcode/registri variabili, costruiscono una routine di decrittografazione con una funzione costante (ad esempio ADD) e fanno variare i registri di indice (SI, DI, BP e BX) utilizzato dalla funzione per rendersi polimorfico. I codici virali che appartengono alla famiglia Flip utilizzano questa tecnica per mutare il proprio codice. I virus altamente polimorfici hanno la caratteristica di mutare complentamente il proprio codice, cioè la routine di decrittografazione, sia nella forma che in lunghezza. Questi codici virali sono in grado di generare mutazioni totalmente diverse l'una dall'altra. Appartengono a questa famiglia i seguenti codici virali: Invisible_Man, Sat-Bug, V2Px.

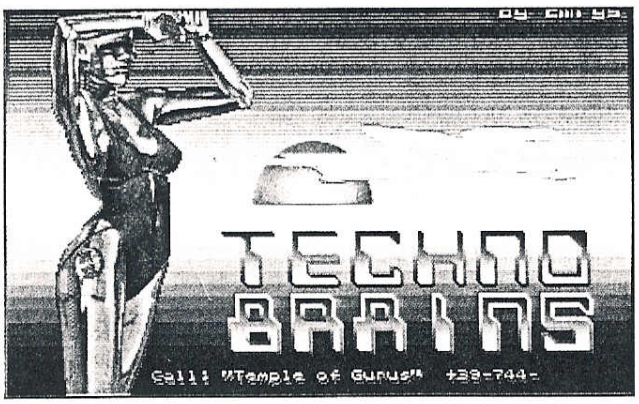
I codici virali permutati hanno la particolarità di non essere crittografati, ma il loro polimorfismo è dovuto ad una inversione di posizione di alcuni codici operativi nella parte iniziale del virus. Questa inversione, naturalmente non altera il risultato/prestazione del codice virale. Appartengono a questa famiglia i virus Leech e Bad_Boy.

I codice virali che si basano su motori polimorfici, sono virus che integrano delle librerie esterne (files .OBJ) che servono a generare le mutazioni. Queste librerie vengono identificate con il nome del motore. Il primo motore polimorfico è stato il Mutating Engine (MtE) del bulgaro Dark Avenger, il quale ha rilasciato la propria libreria in formato .OBJ, quindi utilizzabile da qualsiasi virus-writer. Secondo Dark Avenger, il motore MtE può generare fino a 4,6 bilioni di mutazioni diverse, da un test eseguito si è riscontrato che il 5% delle mutazioni non risultano essere crittografate. Le mutazioni generate dall'MtE sono molto diverse l'una dall'altra, visto che l'algoritmo di decrittografazione differisce anche in lunghezza. Alcuni codici virali che utilizzano questo motore sono: CoffeShop:MtE.0_90, Dedicated:MtE.0_90, Pogue:MtE.0_90 e molti altri. Un altro motore polimorfico è il Trident Polimorphic Engine (TPE) scritto dal virus-writer olandese Masud Khafir.

Masud Khafir è un nome composto, Masud deriva da Masud Barzani (leader della ribellione Kurda) e da Masud

Esempio di routine di crittografazione:

1036:04E8 BFF804	MOV	DI,04F8
1036:04EB B03C	MOV	AL,3C
1036:04ED 3005	XOR	[DI],AL
1036:04EF 47	INC	DI
1036:04F0 FEC0	INC	AL
1036:04F2 81FFA307	CMP	DI,07A3
1036:04F6 75F5	JNZ	04ED
1036:04F8 D43D	AAM	3D



Logo di una BBS di virus exchange, dove oltre allo scambio di virus si possono trovare sorgenti, librerie e tools per sviluppare virus informatici.

Rajavi (leader degli Iranian Mujahedin) e da altri leader della ribellione afghana che hanno tutti nome Masud. Khafir non è un nome di persona, ma è una parola, che prende vari significati da paese a paese, in Olanda signifca IDIOTA (quindi se in Olanda vi definiscono un "khafir" avete ben inteso cosa vogliono dire). Questo motore è stato ispirato dall'MtE di Dark Avenger, ed è in grado di generare tutte le mutazioni crittografate rispetto all'MtE, ed il numero di mutazioni differenti non è quantificabile. Del motore TPE esistono varie versioni, l'ultima in circolazione è la 1.4, anche questa viene rilasciata sotto forma di libreria (files .OBJ) con la possibilità di linkarla nei propri codici virali. Questo motore venne utilizzato anche in Italia da un gruppo di virus-writer italiani che si fanno chiamare Electronic SheepsTeam, rilasciarono il codice virale Lamers_Exterminator il quale implementare come polimorfismo quello generato dal TPE 1.4. Il virus venne distribuito su varie BBS della rete FIDO Net in formato .ZIP che conteneva: la libreria del TPE, il virus citato, e alcuni file di documentazione in lingua inglese sul TPE, e in lingua italiana che presentavano all'opinione pubblica il loro gruppo, la loro creazione e i loro intenti. Una piccola curiosità riguarda il termine LAMERS, che nel gergo dei virus-writers (scrittori di virus) intende identificare tutti quei programmatori, che si cimentano nella scrittura di virus informatici scopiazzondo le tecniche di infezione, creando quindi codici di nessuna originalità.

Oltre al TPE.Lamer_Exterminator, il motore TPE viene utilizzato anche dai seguenti virus: Bosnia:TPE.1_4, Girafe:TPE.1_0, Civil_War:TPE.1_3, YB-1:TPE.1_4 e altri..

Oltre all'MtE e TPE, ci sono altri motori polimorfici come il Dark Slayr's Mutating Engine (DSME), il Dark Slayer's Confusion Engine (DSCE), il Dark Angel's Mutating Engine (DAME), il Mark Ludwig's Visible Mutating Engine (VME) e il Mutagen.

Negli ultimi mesi, alcuni virus-writer italiani stanno rilasciando le loro creature con spiccate attitudini al polimorfismo, come il codice virale Minosse di Willi Wonka che sfrutta il Camaleo Code 4.1, il virus Dream_Man e Peace_Keeper di Doctor Revenge e il The Second NewBorn Trout di The Tricky Trout che sfrutta il Tricky Trout Plurimorphic Encryptor Builder versione 2.01 (TT-PEB).

** 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.*

Esempio di due mutazioni del codice virale Dedicated:MtE.0_90 che utilizza il motore MtE.

```
1036:0610 PUSH   AX
1036:0611 MOV    BP,F4CC
1036:0614 MOV    AX,73B7
1036:0617 MOV    CX,BP
1036:0619 AND    CL,1F
1036:061C SHR    AX,CL
1036:061E XCHG   SI,AX
1036:061F MOV    AX,4F9F
1036:0622 ADD    AX,BP
1036:0624 MOV    CL,03
1036:0626 ROL    AX,CL
1036:0628 XCHG   CX,AX
1036:0629 MOV    AX,[BP+11AF]
1036:062D MOV    DX,E9B7
1036:0630 MUL    DX
1036:0632 XCHG   DI,AX
1036:0633 MOV    AX,1E12
1036:0636 SUB    AX,DI
1036:0638 ADD    AX,120A
1036:063B ROR    AX,CL
1036:063D ADD    AX,SI
1036:063F MOV    CL,03
1036:0641 ROL    AX,CL
1036:0643 MOV    [BP+11AF],AX
1036:0647 MOV    DI,BP
1036:0649 MOV    BX,DI
1036:064B MOV    CL,07
1036:064D ROR    BX,CL
1036:064F ADD    BX,63CF
1036:0653 ROL    BX,1
1036:0655 MOV    SI,BX
1036:0657 MOV    BX,SI
1036:0659 ROR    BX,1
1036:065B SUB    BX,63CF
1036:065F MOV    CL,07
1036:0661 ROL    BX,CL
1036:0663 MOV    BP,BX
1036:0665 INC    BP
1036:0666 INC    BP
1036:0667 JNZ    0614
1036:0669 < virus crittografato >
1036:0610 PUSH   AX
1036:0611 MOV    DI,A667
1036:0614 MOV    CL,03
1036:0616 ROR    DI,CL
1036:0618 MOV    BX,DI
1036:061A MOV    AX,[BX+1196]
1036:061E MOV    DX,7397
1036:0621 MUL    DX
1036:0623 XCHG   AX,[BX+1196]
1036:0627 MOV    DI,BX
1036:0629 MOV    SI,1BA8
1036:062C AND    SI,9B6D
1036:0630 MOV    BP,SI
1036:0632 MOV    SI,DI
1036:0634 MOV    CX,BP
1036:0636 ROR    SI,CL
1036:0638 ROR    SI,1
1036:063A ROR    SI,1
1036:063C MOV    BP,SI
1036:063E MOV    DI,1BA8
1036:0641 AND    DI,9B6D
1036:0645 MOV    SI,DI
1036:0647 MOV    DI,BP
1036:0649 ROL    DI,1
1036:064B ROL    DI,1
1036:064D MOV    CX,SI
1036:064F ROL    DI,CL
1036:0651 MOV    BX,DI
1036:0653 INC    BX
1036:0654 INC    BX
1036:0655 JNZ    061A
1036:0657 < virus crittografato >
```