Gli strumenti di sviluppo dei virus informatici

Alla diffusione dei virus informatici contribuiscono sicuramente la poca conoscenza e le inevitabili "mitizzazioni" che ne nascono. Già da alcuni anni si possono trovare, generalmente in ambienti "underground", dei creatori di pesti informatiche, che permettono anche agli inesperti di creare un proprio personale virus. Sebbene siano oggetti meno pericolosi di quanto sembrasse all'inizio, ne analizzeremo alcuni, da un punto di vista tecnico, illustrandone le capacità e mettendo in luce i reali pericoli derivati/derivabili dalle loro creazioni.

di Gianfranco Tonello

Molto scalpore fece, qualche anno fa, un articolo sul quotidiano La Repubblica, (dal titolo "Computer, virus fai da te - e il colletto bianco si trasforma in pirata -") nel quale si segnalava l'arrivo anche in Italia di questi programmi; era appena sbarcato da noi il VCL (Virus Creation Laboratory).
Ad onor del vero all'epoca i ricercatori anti-virus italiani (fra cui noi) erano già da qualche tempo in possesso del software e ne avevano già messo in luce i limiti nel dibattito in corso sulle varie conferenze telematiche nazionali.
Oltre al VCL, col passare del tempo sono nati altri ambienti di sviluppo; tra questi citiamo il PS-MPC del gruppo Phalcon Skism, il G2, il Generateur Virus, l'IVP (Instant Virus Production) del gruppo Youngsters Against McAfee, il VC2000 (Virus Creation 2000) ed il Virus Tutorial.
Questo solamente per citarne alcuni tra i più noti nel panorama internazionale, ma non è da escludere che in questo ultimo periodo ne siano sorti altri, o versioni "migliorate" siano state rilasciate.
Ci occuperemo nel dettaglio del funzionamento del più noto (almeno in Italia) di questi strumenti, il VCL (version 1.00), analizzeremo quello che può essere definito una sua "pezza" chiamata VCL Asm Mutator, e per concludere questo primo *excursus* sull'argomento daremo un'occhiatina al Virus Creation 2000.
Un'analisi di questi strumenti è molto interessante perché permette di capire meglio cosa sono in realtà i virus, come operano e come si propagano, sfatando così alcune leggende (virus che contagiano appena si infila il dischetto...).

Fig. 1. Il logo di NuKE, l'organizzazione di "hacker" a cui si fregia di appartenere l'autore di VCL, l'ambiente di sviluppo per i virus.

VIRUS CREATION LABORATORY VERSION 1.00 BY NOWHERE MAN

Quest'opera è "firmata" da Nowhere Man dell'organizzazione [NuKE] WaReZ. Questo software FREEWARE, ovvero di libera distribuzione (non poteva essere altrimenti...), iniziò a "circolare" dapprima negli ambienti dell'*underground* informatico italiano, fino ad essere "legalmente", almeno secondo la legislazione vigente in Italia, venduto all'interno di un CD-ROM contenente una raccolta di informazioni/programmi per l'"hackeraggio" provenienti dall'America.
Concentriamoci ora sul funzionamento del software; *in primis* non è detto che anche venendo in possesso del pacchetto si riesca ad attivarlo: infatti questo risulta essere contenuto in un file .ZIP con parola d'accesso. Una volta "trovata/scovata" la parola d'accesso si passa all'installazione del pacchetto, la quale a questo punto è molto semplice ed immediata.

All'attivazione del software appare una schermata (vedi figura 2) oltrepassata la quale si entra nel vero e proprio ambiente di "lavoro/creazione".
Questo è un ambiente IDE (Integrated Development Enviroment), con la classica struttura con menu a tendina.
Ad onor del vero la struttura del software risulta essere semplice e pulita, peraltro il programma è dotato di una guida in linea (in lingua inglese, fortunatamente, così la capiscono in meno...) che chiarisce eventuali dubbi sull'utilizzo delle varie opzioni disponibili per la creazione dei virus.
Nella parte centrale/superiore dello schermo è presente un piccolo riquadro dove è in continuo scorrimento la seguente scritta "— Virus Creation Laboratory — Written by Nowhere Man — An official [NuKE] Ware"; forse l'autore aveva il timore di non essere ricordato per il fattivo contributo dato, con questa creazione, all'intera comunità informatica.
Vedremo ora quali "prodigiose" creazioni sia capace questo generatore.

Fig. 2 . La schermata di apertura di VCL.

MENU OPTIONS

Dal menu OPTIONS si può scegliere il tipo di virus: Appending, Overwriting, Spawning, Trojan Horse e Logic Bomb.
I Virus di tipo "Appending" sono dei codici virali che si appendono al programma ospitante.
Questa versione del VCL (la 1.0) supporta "solamente" l'infezione di file con estensione .COM.
Le peculiarità possibili dei virus così creati sono: Stop Trace (rende il virus ostile ai programmi debuggers), Encryption (permette di crittografare il codice virale), Search Type (schema adottato nell'infezione dei file, ad esempio ad ogni attivazione del file infetto l'infezione può propagarsi nei file della corrente directory etc.).
Vi è poi la possibilità attraverso l'opzione Virulence di definire il numero di file da infettare ad ogni attivazione di un programma portatore, cioè infetto; inoltre con l'opzione Note è possibile inserire all'interno del codice virale del testo a piacere.
I virus di tipo "overwriting" (sovrascriventi) sono dei codici virali che sovrascrivono il file infettato, rendendolo così inutilizzabile ed irrecuperabile, rispetto agli "appending" (accodanti) possono trasmettersi anche attraverso i file .EXE ed hanno le stesse peculiarità già descritte.
I Virus di tipo "Spawning", chiamati anche Companion, hanno la caratteristica di non attaccare i file, ma di creare un file con estensione .COM con lo stesso nome dei file eseguibili (.EXE) presenti. Questa metodologia virale sfrutta la caratteristica del Sistema Operativo MS-DOS, il quale per mandarli in esecuzione cerca prima i file con estensione .COM e poi quelli con estensione .EXE.
Così facendo, prima viene eseguito il corpo del virus e successivamente (da questo) viene mandato in esecuzione il programma attivato dall'utente.
Si tratta quindi di un'infezione abbastanza rozza, e facilmente rilevabile ed eliminabile dall'utente.
I "Trojan Horse" (Cavalli di Troia) non sono dei Virus, ma programmi che celano sotto un aspetto innocuo ed a volte "invitante", effetti distruttivi come la formattazione o la sovrascrittura dei dati contenuti all'interno del PC.
Le "Logic Bomb" (bombe logiche), sono simili ai Cavalli di Troia, possono venire incorporate in un programma, ed al verificarsi di un preciso evento (data fatidica, ora o altro...), portano a distruzioni e/o effetti collaterali nelle macchine utilizzate.

MENU EFFECTS

Nel menu EFFECTS si può naturalmente scegliere l'effetto da includere nel codice virale in fase di creazione.
La scelta può essere fatta su una quantità ampia di effetti, distinguibili in due categorie: distruttivi e non. I classici effetti distruttivi riguardano la formattazione, la sovrascrittura o la cancellazione dei file.
Gli effetti "innocui" riguardano la possibilità di visualizzare messaggi a video o su stampante, emettere suoni dall'altoparlante PC o disabilitare porte (tipo LPT e COM). Scelto l'effetto non ci resta che decidere il momento in cui questi effetti vengano a manifestarsi.
Nel menu MAKE si dà inizio alla creazione del file sorgente .ASM del codice virale.
A questo punto è possibile compilare in formato .COM il codice virale (questo codice, dal quale hanno inizio le replicazioni, viene denominato "generatore").
La compilazione del file .ASM avviene tramite l'assemblatore esterno che il novello scrittore di virus avrà a sua disposizione (TASM o MASM) definito nel menu CONFIGURATION alla voce Assembler.
All'interno del pacchetto sono inclusi degli esempi di virus già creati chiamati: Viral Messiah, Code Zero, Kinison, Pearl Harbor, Yankee][, Earth Day, Donatello e Richard Simmons Trojan.

REALI PERICOLI

I virus generati grazie al VCL, risultano essere un assemblaggio di routine predefinite (prefabbricate), e quindi tutti i maggiori antivirus in circolazione, prendendo atto di questo, ne hanno inserito le *firme* caratteristiche, riuscendo in que-

sto modo ad intercettare preventivamente i codici virali creati.
Il reale pericolo deve essere visto non tanto nell'immediato, ma in futuro, quando gli aspiranti *virus-writer* dopo essersi "allenati" con il VCL inizieranno a modificare i codici generati così da aggirare gli anti-virus.
È quindi l'aspetto formativo dei generatori di virus che, a nostro parere, deve essere sottolineato, e non tanto i pericoli derivanti dall'immediato.
In Italia infatti il VCL ha una certa diffusione (sono relativamente numerose le persone ad esserne in possesso), però ad onor del vero, non sono a noi note segnalazioni significative, derivanti dalla diffusione nel nostro paese, di codici virali creati con lo strumento descritto.
Come abbiamo detto gli Anti-Virus sono in grado di intecettare preventivamente la gran parte dei virus generati con il VCL.
La controrisposta dell'organizzazione NuKE è il rilascio del VCL MUTATOR, il quale permette di sostituire le vecchie routine dei virus generati con il VCL con delle nuove che rendono il virus equivalente nel funzionamento ma non più identificabile dagli Anti-Virus.

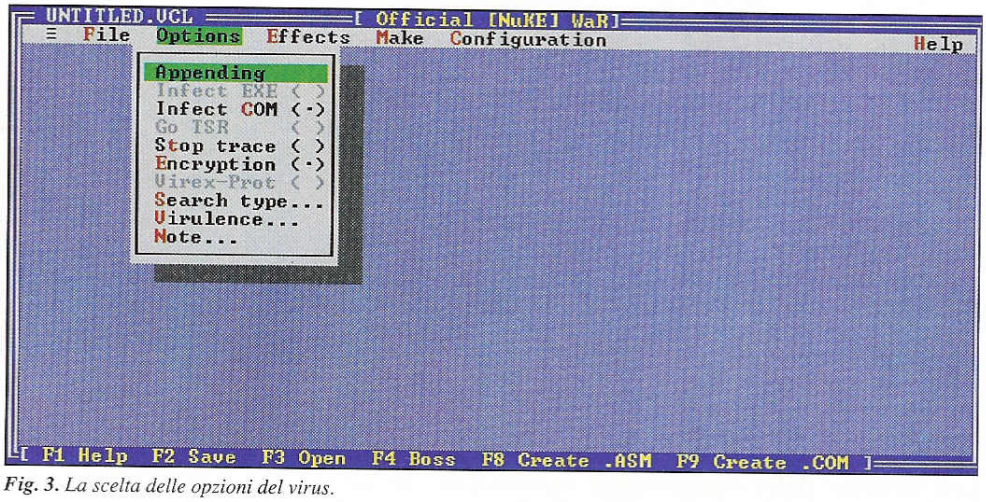

Fig. 3. La scelta delle opzioni del virus.

Andremo ora ad analizzare questo strumento con maggiore dettaglio.

VCL MUTATOR V.99B BY FIRECRACKER, [NUKE]

Il funzionamento di questa "pezza" è molto semplice: dopo aver generato il sorgente del virus sottoforma di file .ASM, il VCL Mutator ricompila il codice sostituendo, come detto, le vecchie routine, rendendo così il virus non rintracciabile dagli Scanner AV.
La libreria che viene utilizzata per la sostituzione del vecchio codice è contenuta in un file PATTERN di configurazione.

Gianfranco Tonello è ricercatore anti-virus ed autore del software anti-virus VirIT, disponibile anche nella versione "Lite", gratuita, anche presso il BBS M&P Connect (LIB virus), e presso il nostro servizio Distribuzione Shareware (12/94), oltre che in svariati nodi della rete Fidonet.
È da anni apprezzato consulente in materia di sicurezza informatica nell'ambito anti-virale in ambito aziendale e bancario. È possibile contattare Gianfranco Tonello in FidoNet: Gianfranco Tonello 2:333/316.4; in Internet all'indirizzo E-Mail tge@maya.dei.unipd.it.
I lettori che lo desiderano potranno, possibilmente tramite il modulo di segnalazione delle infezioni in atto e l'invio di materiale sospetto, dare un fattivo contributo all'analisi ed alla comprensione del fenomeno, ed essere consigliati per la soluzione, il più indolore possibile, dei loro problemi informatici.

Questo file è modificabile, quindi può essere modificato da qualsiasi persona che abbia adeguate conoscenze del linguaggio assembly, e soprattutto condivida le "ideologie" dei *virus-writer*. Ogni novello *virus-writer* può quindi generarsi una propria libreria per rendere i virus generati dal VCL non identificabili dai maggiori AV. Siamo ben lontani, comunque, dalla possibilità "anche per gli inesperti di generare virus non identificabili da nessun antivirus".

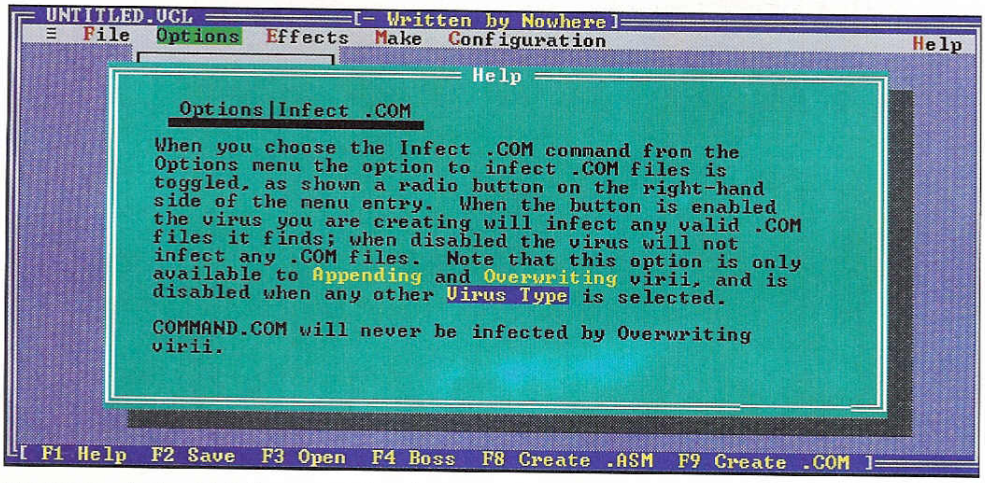

Fig. 4. C'è anche la guida in linea; notare la scritta scorrevole con cui l'autore si immortala.

VIRUS CREATION 2000 V. 0.96 BY JOHN BURNETTE

L'ultimo ambiente per la creazione di virus informatici che presenteremo in questa carrellata sull'argomento è il Virus Creation 2000. Rispetto al VCL, il quale presenta per la creazione un'interfaccia utente in Turbo Vision, quest'ultimo "creatore" è caratterizzato da un'interfaccia estremamente

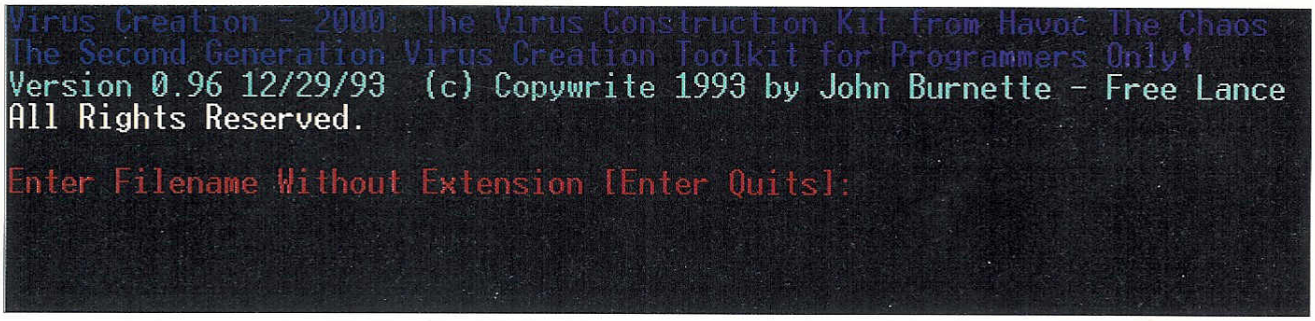

Fig. 5. Un altro creatore di virus più spartano: il Virus Creation 2000.

spartana costituita da una serie di domande/risposte del tipo "Yes or No". Per l'attivazione dell'editore di virus è necessario conoscere una parola chiave "segreta" (comunemente nota a qualsiasi programmatore medio/scarso). Oltrepassato questo "ostacolo" vi è la richiesta di alcune informazioni preliminari riguardanti il nome del codice virale che si intende creare, il nome dell'autore dello stesso, e alcune informazioni sul virus. Successivamente vi è la richiesta per la gestione dell'interrupt 24h (gestione degli errori), riguardante il suo utilizzo. Nella sezione successiva si definiscono le specifiche dell'infezione: può essere attivato il controllo sulla lunghezza del file da infettare, se infettare il COMMAND .COM o meno, la scelta del tipo di percorso che seguirà l'infezione, l'uso del DTA (Disk Transfer Area), se ripristinare gli attributi del file prima dell'infezione, il numero di file da infettare ad ogni attivazione di un file infetto, se ripristinare data e ora del file, controllare se il file era già infetto; è inoltre possibile scegliere quali siano i tipi di file da infettare tra .EXE, .COM, .BIN, Overlay files, .SYS, .BAT, .VXD (Windows Virtual Driver), .DLL (Windows, OS/2), e come ultima possibilità permette di includere all'interno del codice delle proprie routine esterne. Fino ad ora nulla di "strano", è a partire da questa fase che risulta essere possibile inserire particolari routine che permetteranno al codice virale di aggirare alcuni anti-virus tra i più famosi ed efficaci del panorama internazionale.
Inoltre è possibile controllare la "tracciatura" del codice (cioè il controllo passo per passo da parte dei ricercatori anti-virus., che rende questo ostile ai programmi di debugger). Nell'ultima sezione chiamata Creation Handler si opera la scelta del tipo di virus Overwriting o meno, ad azione diretta o TSR (Terminate Stay Resident); il TSR in questa versione però non è ancora stata implementata (buon per noi...).
La funzione più "interessante" riguarda la possibilità di creare un programma per il riconoscimento del nuovo virus creato, così da permettere che il suo autore non resti vittima della sua stessa creazione.
Dulcis in fundum, l'ultimo dilemma posto all'aspirante *virus-writer* riguarda il tipo di assemblatore con il quale verrà compilato il sorgente (MASM o TASM); viene così creato un file .BAT contenente le informazioni per attivare la compilazione del file .ASM generato, inoltre viene creato anche un file .DOC contenente le informazioni riguardanti il virus creato.
Comparandolo al VCL questo software generativo si differenzia per l'impossibilità di scegliere gli effetti del codice virale generato, a meno che non sia lo stesso autore a creare le routine necessarie allo scopo.

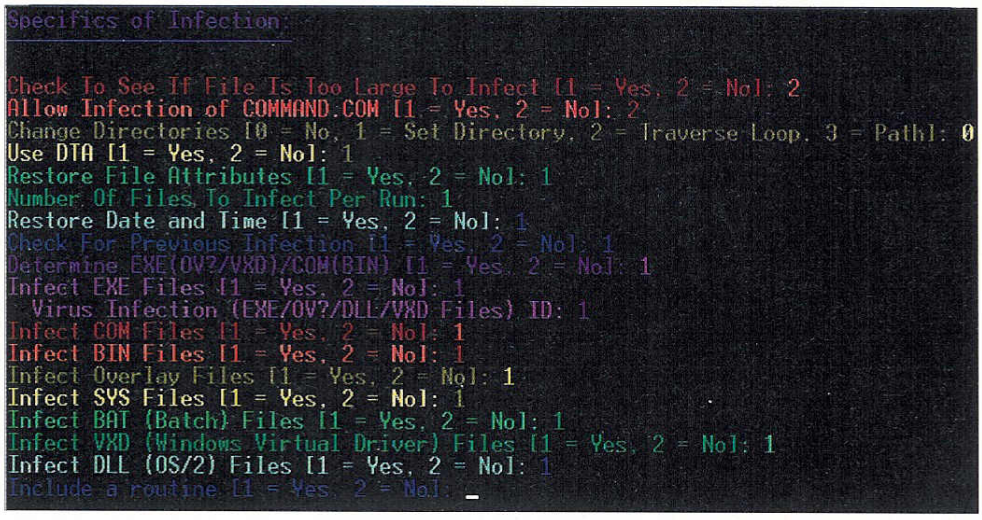

Fig. 6. Le opzioni offerte dal Virus Creation 2000. Anche i virus da esso creati possono essere pericolosi solo se utilizzati da persone abbastanza esperte.

CONCLUSIONI

Come si può notare è in atto una continua lotta tra gli autori di virus e i produttori di anti-virus: vi è un continuo "gioco" di mossa e contromossa che, per ora, non sembra tendere ad attenuarsi. Per quanto ci riguarda, non ci resta che sorvegliare l'evolversi di questa insana situazione; è proprio per questo che Micro & Personal Computer, sensibile al fenomeno, ha deciso di inaugurare questo nuovo spazio editoriale, nella speranza di diffondere nei lettori conoscenze e comportamenti che rendano più difficili e meno distruttivi possibili gli eventuali contagi.