Italian VIRUS Magazine

LA PRIMA RIVISTA ITALIANA DEDICATA ALLA LOTTA ANTI-VIRALE MS-DOS

Trimestrale - Anno 1, 2/95 Agosto 1995

Italian VIRUS Magazine

Italian VIRUS Magazine è una rivista elettronica dedicata alla lotta antivirale con particolare attenzione alla realtà italiana, con l'obiettivo di sensibilizzare la comunità informatica verso gli agenti patogeni che ogni giorno tentano di insidiare i nostri calcolatori e quindi il nostro prezioso lavoro.

I.V.M. (Italian VIRUS Magazine) è gratuita, quindi liberamente copiabile e distribuibile senza scopo di lucro.

Uso delle informazioni contenute in I.V.M.

Le informazioni riportate possono essere utilizzate totalmente o parzialmente solamente previa autorizzazione di TG Soft (Tel./Fax 049-631748).

Hanno collaborato: Gianfranco Tonello, Cristian Basso, Enrico Tonello.

Via Sardegna n° 5
35030 Sarmeola di Rubano (PD)
Tel./Fax 049-631748 (Fax 24h/24)

Tutti i marchi citati sono marchi registrati di proprietà delle rispettive case produttrici

NEWS

TOP TEN dei Virus più attivi nel mondo

I dieci più comuni virus segnalati negli ultimi sei mesi fino alla fine di marzo 1995 sono in ordine decrescente:

01) Form
02) Stealth Boot.B
03) AntiEXE
04) AntiCMOS
05) Monkey.B
06) B1 (NYB)
07) Parity Boot.B
08) Ripper
09) 2Kb (Jumper, French Boot)
10) Monkey.A

E' da notare che tutti i codici virali hanno in comune una caratteristica sono virus che infettano il boot sector e/o il master boot record.

I Virus segnalati attivi in Italia

In questi ultimi mesi sono stati segnalati attivi nel nostro Paese alcuni virus già noti da tempo. Tra questi citiamo Junkie.1027, Marzia.D, B1, HLLC.Crawen.8306, AntiExe, One_Half.3544 e Run_Error.504D:5658. Sono tutti virus che attaccano il Boot Sector e l'MBR (Master Boot Sector) a parte l'HLLC.Crawen.8306 che è un virus gemellare, il quale sfrutta una particolare caratteristica che lo rende fast infection (infezione veloce).
One_Half.3544, noto anche come SLOVAKIA BOMBER, ha la caratteristica di essere polimorfico e come se ciò non bastasse all'atto dell'infezione si pone in più punti del file colpito "frammentandolo".
Run_Error.504D:5658 è un virus del Boot Sector, appartenente alla famiglia degli EXTRA TRACCIA. La metodologia di infezione, sfrutta un tipico metodo utilizzato per la protezione del software, cioè la formattazione fuori standard di una o più tracce del floppy disk.

N.B. Tutti i virus citati vengono correttamente intercettati da VirIT Lite.

Cavallo di troia in PKZIP

> SUBJECT: Malicious code in counterfeit PKZip program.
>
> SUMMARY: Files falsely identified as being updates to the popular
> PKWARE Inc., PKZip utility contain malicious code. The files are
> being distributed on various network (Internet) and dial-up BBS
> systems.
>
> BACKGROUND: PKZip is a DOS shareware data compression utility.
> The counterfeit PKZip file is named either PKZ300B.ZIP or
> PKZ300B.EXE, and contains malicious code that can cause hard
> drives to be re-formatted. According to PKWARE, Inc., when the
> PKZ300B.EXE self extracting executable is run, all data on the
> hard drive is lost. The malicious code contained in the PKZ300B
> files is not a computer virus, i.e. it does not have the
> capability to automatically spread and infect other systems or
> files.
>
> IMPACT: All data on PC hard rive is lost when the corrupted
> program is executed.
>
> RECOMMENDED SOLUTIONS: Do not download and/or execute any file
> named PKZ300B.EXE/ZIP. The most current release of PKZip from
> PKWARE Inc., is PKZ204G.exe which is available via anonymous FTP
> from pkware.com (IP 198.137.186.90) in the /pub/pkware directory.

Virus dalla rete ITAX

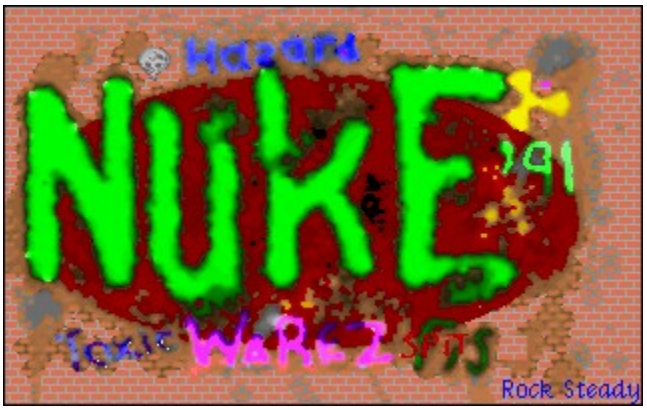
Nella rete amatoriale ITAX alla fine del mese di maggio, sono stati distribuiti 2 messaggi contenenti i seguenti codici virali: Lillith e 2Trout, sotto forma di UUENCODE. Entrambi sono di origine italiana. Il Lillith è un Dropper il quale serve per installare il virus sul Master Boot Sector dell'Hard Disk, dopo questo la diffusione avverrà attraverso il Boot Sector dei floppy disk. Il 2Trout (The Second NewBorn Trout) è il generatore, il virus è ad azione diretta ed utilizza un nuovissimo ed estremamente complesso motore polimorfico chiamato TT-PEB (Tricky Trout Plurimorphic Encryptor Builder). Questo motore sembra essere stato progettato dallo stesso autore del virus 2Trout che, dalle scritte contenute all'interno del virus, sembra essere italiano. Al tuttoggi nessun anti-virus è in grado di identificare i codici virali suddetti, per il Lillith

l'identificazione è ottenibile con le modalità usuali, mentre per il 2Trout l'identificazione è subordinata alla creazione
di un controalgoritmo che vista la complessita del virus sembra di non semplice realizzazione.

I Tools di sviluppo dei VIRUS Informatici

di Gianfranco Tonello

Già da alcuni anni si possono ritrovare, generalmente in ambienti Underground, questi creatori di pesti informatiche, i quali permettono, anche ad utenti inesperti, di creare un loro personalissimo virus. Ne presenteremo ora alcuni, illustrandone le capacità, e mettendo in luce i reali pericoli derivati/derivabili dalle loro creazioni.



Molto scalpore fece, qualche anno fa, un articolo sul quotidiano La Repubblica il quale titolava "Computer, virus fai da te -e il colletto bianco si trasforma in pirata-" nel quale si segnalava l'arrivo anche in Italia di questi tools, era stato infatti ritrovato il VCL (Virus Creation Laboratory). Ad onor del vero all'epoca i ricercatori antivirus italiani erano già da qualche tempo in possesso del tools e ne avevano già messo in luce i limiti nelle varie conferenze telematiche nazionali, alle quali io stesso ho partecipato. Oltre al VCL, col passare del tempo sono nati altri tools 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 tools, il VCL (version 1.00), analizzeremo quello che può essere definito un suo patch chiamato VCL Asm Mutator, e per concludere questo primo escursus sull'argomento daremo un'occhiatina al Virus Creation 2000.

- V.C.L. Virus Creation Laboratory Verion 1.00 by Nowhere Man
- Virus Creation 2000 The Virus Construction Kit From Havoc The Chaos

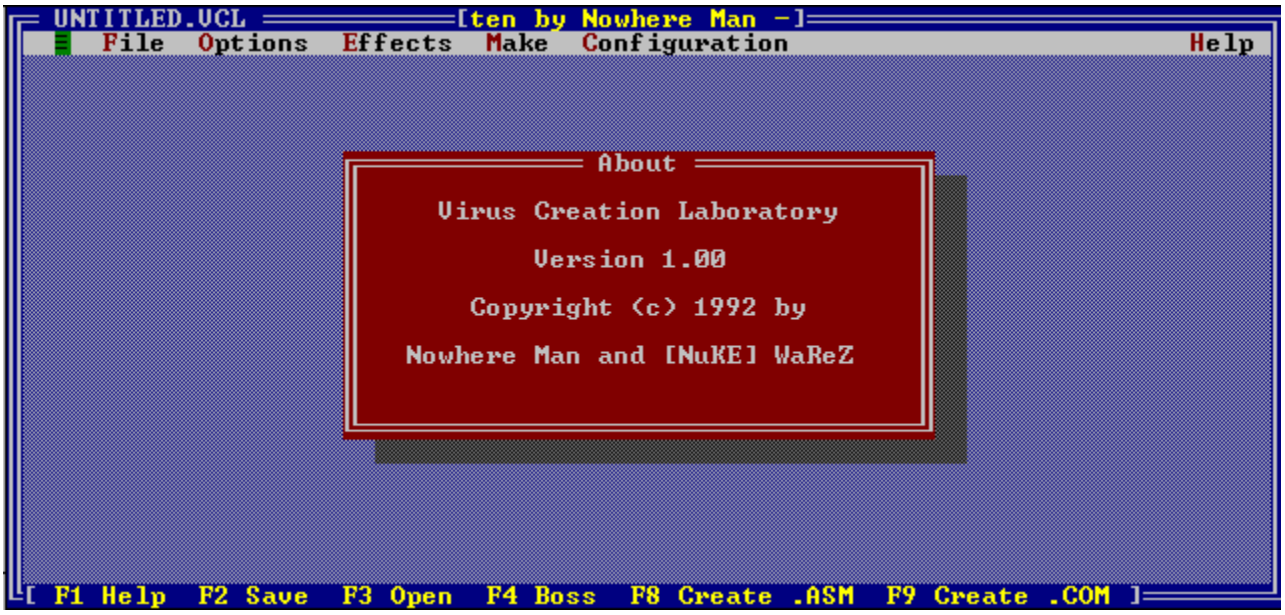
V.C.L. Virus Creation Laboratoy

Version 1.00 by Nowhere Man and [NuKe] WaReZ

La schermata di apertura del V.C.L.

Quest'opera è "firmata" da Nowhere Man dell'organizzazione [NuKE] WaReZ. Questo software FREEWARE (non poteva essere altrimenti....) di libera distribuzione 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 password. Una volta "trovata/scovata" la password si passa all'installazione del pacchetto, la quale a questo punto è molto semplice ed immediata. All'attivazione del sofware appare una schermata (vedi figura) oltrepassata la quale si entra nel vero e proprio tools di "lavoro/creazione". Questo è un ambiente IDEs (Integrated Development Enviroments), classica struttura Desk Top con menù a tendina. Ad onor del vero la struttura del software risulta essere semplice e pulita, per altro il programma è pure dotato di un Help in linea (in lingua inglese fortunatamente per noi italiani....) che chiarisce eventuali dubbi sull'utilizzo delle varie opzioni disponibili per la creazione dei virus. Nella parte

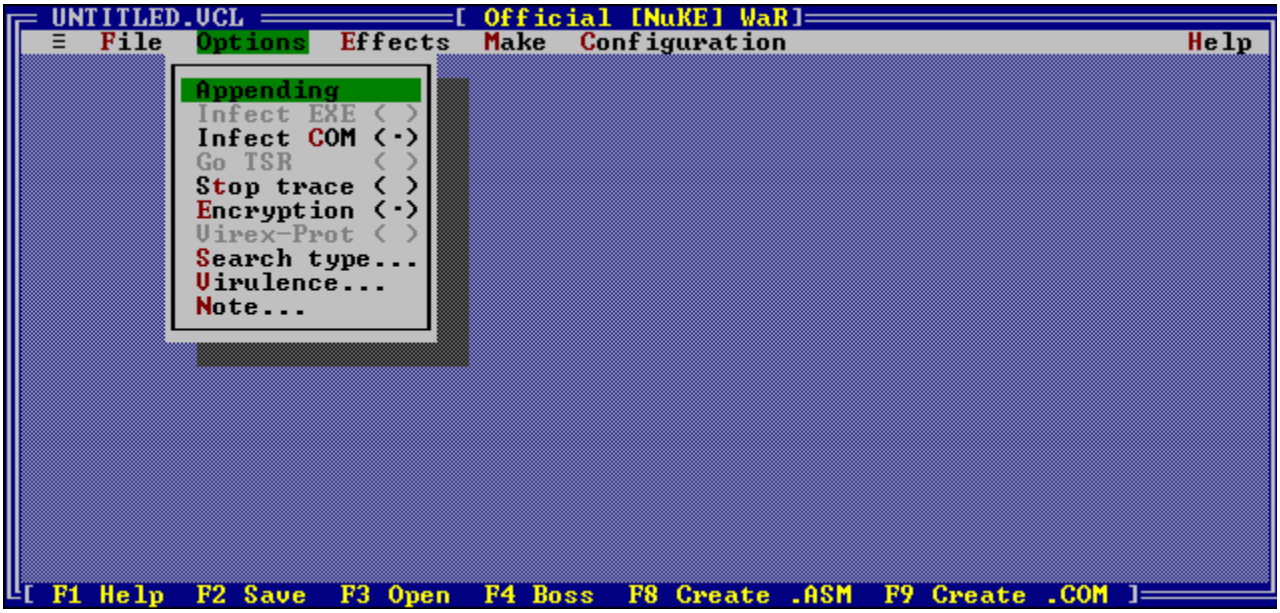
centrale/superiore dello schermo è presente un piccolo Box dove è in continuo scorrimento la seguente scritta "-- Virus Creation Laboratory -- Written by Nowhere Man -- An official [NuKE] Ware", forse l'autore aveva il timore di non essere ricordato per il fattivo contributo dato, con questa creazione, all'intera comunità informatica. Vedremo ora quali "prodigiose" creazioni sia capace questo generatore.



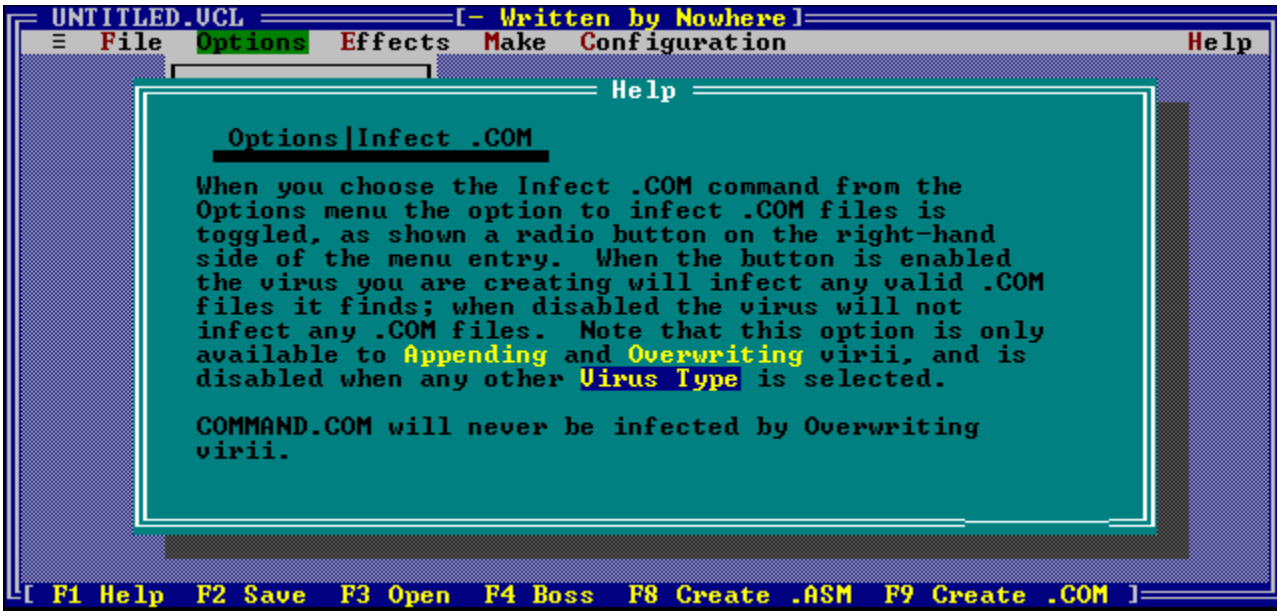
About del Virus Creation Laboratory

- Menu OPTIONS
- Menu EFFECTS
- REALI PERICOLI

Menu OPTIONS



Dal menù 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 files 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 files, ad esempio ad ogni attivazione del file infetto l'infezione può propagarsi nei files della correnti directory etc.).

Vi è poi la possibilità attraverso l'opzione Virulence di definire il numero di files 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 sono dei codici virali che sovrascrivono il file infettato (rendendolo così inutilizzabile ed irrecuperabile), rispetto agli Appending possono trasmettersi anche attraverso i files .EXE ed hanno le stesse peculiarità già descritte.

I Virus di tipo Spawning, chiamati anche Companion, hanno la caratteristica di non attaccare i files, ma di creare un file con estensione .COM con lo stesso nome dei files eseguibili (.EXE) presenti. Questa metodologia virale, sfrutta la caratteristica del Sistema Operativo MS-DOS, il quale manda prima in esecuzione i files 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.

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, sono similari ai Cavalli di Troia, possono venire linkate 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 menù EFFECTS si può naturalmente scegliere l'effetto da includere nel codice virale in fase di creazione. La scelta può essere fatta su una quantita ampia di effetti, distinguibili in due categorie distruttivi e non. I classici effetti distruttivi riguardano la formattazione, la sovrascrittura o la cancellazione dei files. Gli effetti "innocui" rigurdano la possibilità di visualizzare messaggi a video o su stampante, emettere suoni dal PC speaker 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 menù 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 virus-writer avrà a sua disposizione (TASM o MASM) definito nel menù 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 preso atto di questo, ne hanno inserito le FIRME caratteristiche, riuscendo in questo 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-writers dopo essersi "allenati" con il VCL inizieranno a modificare i codici generati così da bypassare gli antivirus. E' quindi l'aspetto formativo dei generatori di virus che, a mio 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 crati con il tool descritto.
Come abbiamo detto gli Antivirus sono in grado di intecettare preventivamente la gran parte dei virus generati con il VCL. L'organizzazione NuKE, preso atto di ciò ha quindi "ben pensato" di rilasciare il VCL MUTATOR, il quale permette di sostituire le vecchie routine dei virus generati con il VCL con delle nuove routine che rendono il virus equivalente nel funzionamento ma non più identificabile dagli Antivirus.

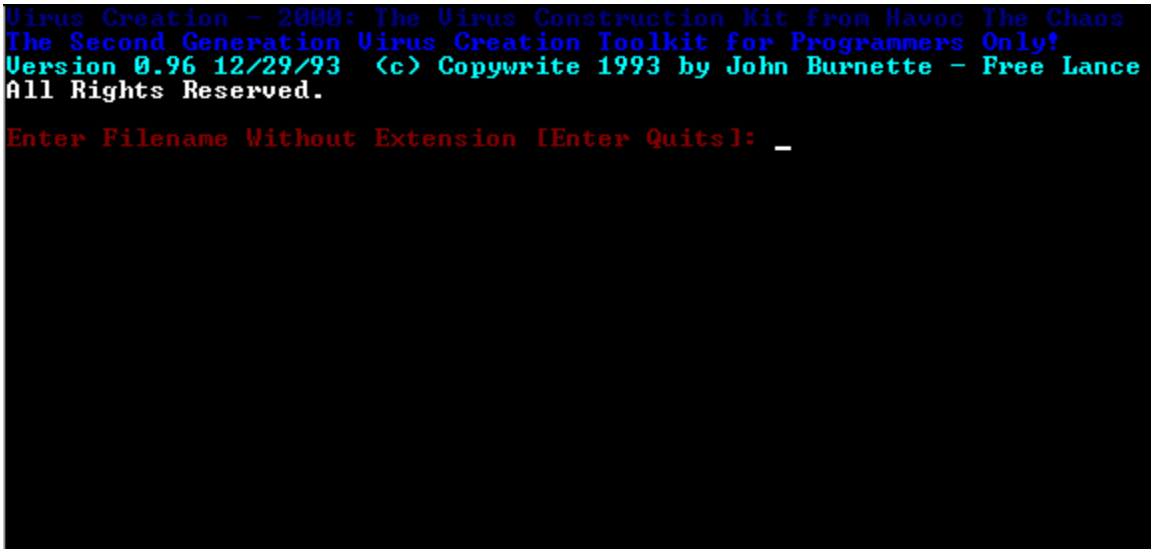
 VCL Mutator V.99b by Firecracker [NuKe]

VCL MUTATOR v.99b

By FireCracker, [NuKe]

Il funzionamento di questo tool 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 routines, 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. Questo file è editabile, quindi può essere modificato da qualsiasi persona che abbia adeguate conoscenza del linguaggio assembly e soprattutto condivida le "ideologie" dei virus-writers. Ogni novello virus-writer può quindi generarsi una propria libreria per rendere i virus generati dal VCL non identificabile dai maggiori AV.

VIRUS CREATION 2000



Questo tools per la crazioni di virus informatici che presenteremo in questo breve escursus 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 caratterizzata da un'interfaccia estremamente spartana costituita da una serie di domande/risposte del tipo Yes or No. Per l'attivazione dell'editore di virus è necessario conoscere una password "segreta" (comunemente nota a qualsiasi programmatore medio/scarso). Oltepassato 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 files da infettare ad ogni attivazione di un files infetto, se ripristinare data e ora del file, controllare se il file era già infetto, è inoltre possibile scegliere quali siano i tipi di files da infettare tra .EXE, .COM, .BIN, Overlay files, .SYS, .BAT, .VXD (Windows Virtual Driver), .DLL (OS/2), 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 bypassare 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 fundus l'ultimo dilemma posto al novello 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.

Analisi Virus

coordinatore Gianfranco Tonello

- New_ExeBug
- Bye
- Satyricon.338
- Boot.446

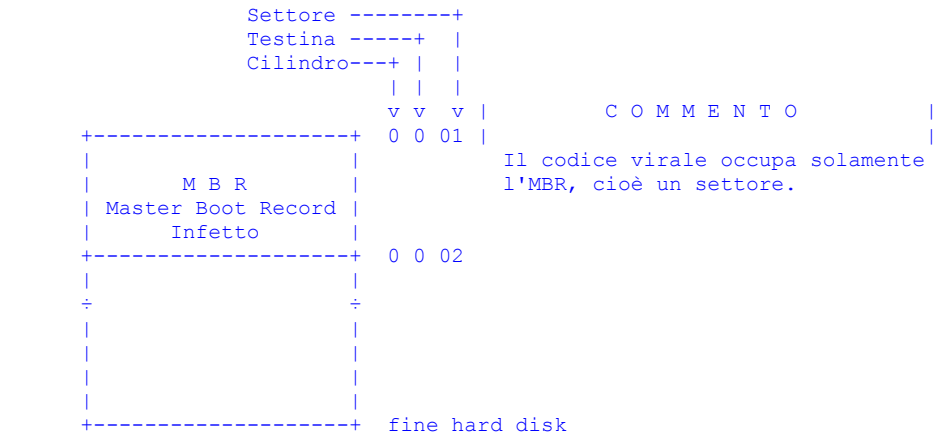
New_Exebug

di Gianfranco Tonello

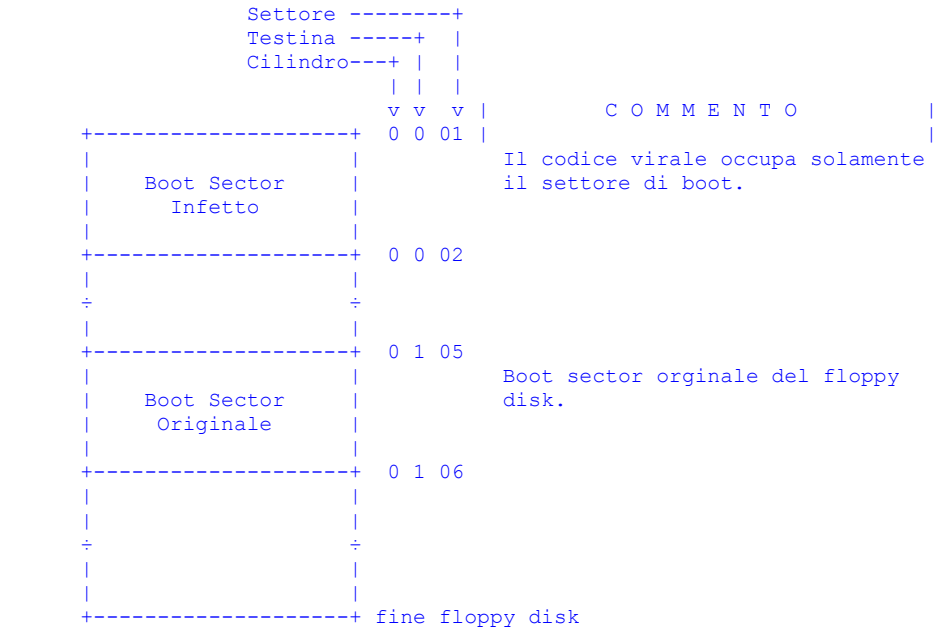
Nome virus:	New_ExeBug
Aliases:	
Variante:	Possibile variante del virus EXEBUG
Stato:	Nuovo
Isolato:	16 Maggio 1995 (Italia)
Sintomi:	diminuzione della memoria libera del sistema
Origine:	Sconosciuta
Dimensione:	512 bytes (1 settore)
Tipo:	Residente in memoria, infetta boot sector (floppy disk), Master Boot Record (Hard disk).
Analisi a cura di:	Gianfranco Tonello Tel/Fax 049-631748

COMMENTO GENERALE

Questo codice virale potrebbe essere una variante del virus EXEBUG ed è stato catalogato provvisoriamente col nome di New_ExeBug.
Il codice virale risulta essere residente in memoria (TSR), infetta il boot sector dei floppy disk e l'MBR (Master Boot Sector) del disco fisso. Quando il New_ExeBug si attiva dal boot dei floppy disk, si alloca in memoria intercettando l'interrupt 13H (Disk/Diskette Services), la memoria libera del sistema diminuisce di un kilobytes e viene infettato il master boot sector dell'hard disk.



Ogni floppy disk verrà infettato dal virus New_Exebug nel modo seguente:



Ogni floppy disk non protetto in scrittura verrà infettato dal virus New_Exebug. Per i floppy disk da 720Kb, 1.2Mb e 1.44Mb non ci sono problemi, perchè il
codice virale salva il Boot Sector originale nella sezione denominata "ROOT DIRECTORY" con la sovrascrittura di un settore della root. Per i floppy disk da 360Kb, il virus sovrascrive un settore della sezione denominata "DATA SECTOR", con la perdita del funzionamento del file che occupava quel settore.
Quando il virus New_ExeBug parte da disco fisso, controlla la data del calcolatore, nel caso sia inferiore al 1993 non viene intercettato l'interrupt 0BH (IRQ3, porta seriale, segmento non presente). L'int 0BH gestito dal codice

virale ha lo scopo di emettere il comando EOI (End Of Interrupt). All'interno il codice virale non presenta stringhe visibili.

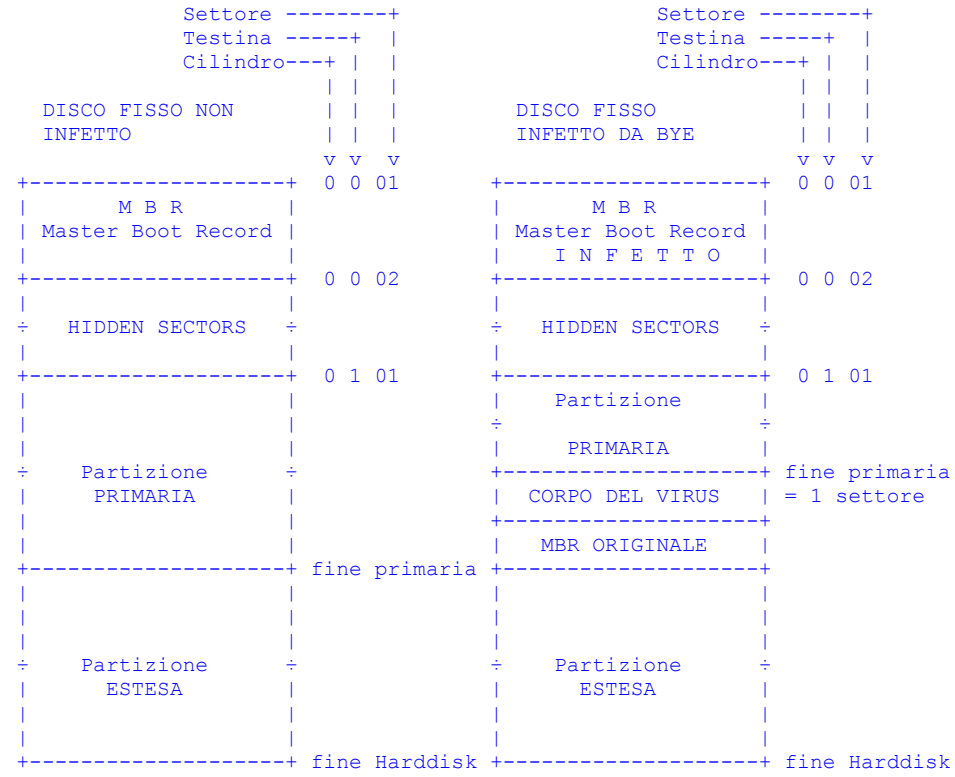
Bye

di Gianfranco Tonello

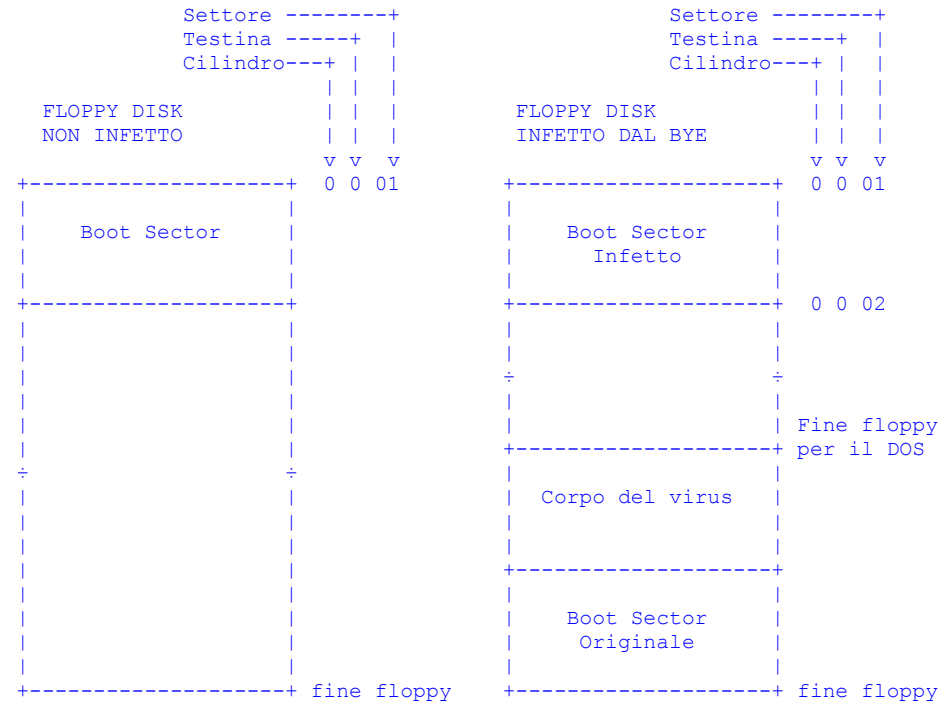
Nome virus:	Bye
Aliases:	
Variante:	
Stato:	
Isolato:	Noto dal mese di Settembre 1994
Sintomi:	diminuzione della memoria libera del sistema
Origine:	Italia (?)
Dimensione:	2 settori (compreso il boot originale)
Tipo:	Residente in memoria, stealth, infetta boot sector (floppy disk), Master Boot Record (Hard disk).
Analisi a cura di:	Gianfranco Tonello Tel/Fax 049-631748
Data:	27/05/1995

COMMENTO GENERALE

Il virus Bye è stato isolato per la prima volta nel mese di Settembre 1994 in Italia, la sua origine potrebbe anche non essere italiana.
Il codice virale risulta essere residente in memoria (TSR), stealth, infetta il boot sector dei floppy disk e l'MBR (Master Boot Sector) del disco fisso.
Quando il Bye si attiva dal boot dei floppy disk, si alloca in memoria, la memoria libera del sistema diminuisce di un kilobyte. Il virus carica nel blocco allocato gli ultimi due settori del floppy disk, rispettivamente il corpo del virus e il boot sector originale del floppy disk. A questo punto viene intercettato l'interrupt 13H (Disk/Diskette Services) e infettato il master boot sector dell'hard disk. L'infezione del Master Boot Sector è similare a quelle addottate dai virus Flip e Invisible_Man, il codice virale cerca la partizone attiva del disco fisso e copia alla fine di questa il corpo del virus e il master boot sector originale.



Ogni floppy disk, che verrà inserito non protetto in scrittura sarà infettato dal virus Bye nel modo seguente:



Il virus Bye, quando infetta il boot sector dei floppy e il master boot sector,

utilizza una routine lunga 49 bytes per caricare il corpo del codice virale, questo gli permette di bypassare alcune tecniche euristiche.
Un'altra caratteristica del codice virale è quella di essere invisibile (stealth) quando è residente in memoria.
Il codice virale Bye presenta un'anomalia, un byte del virus sembrerebbe essere stato alterato con un valore casuale, questo non gli permeterebbe di attivarsi o solo in casi particolarissimi. La parte del codice incriminata è la seguente:

```
E8 F7 00        CALL  0124
CC              INT   3
04 CD           ADD   AL,CD
1A 80 FE 05     SBB   AL,[BX+SI+05FE]
75 18           JNZ   004E
```

```
Il codice corretto doveva essere:
```

```
E8 F7 00        CALL  0124
B4 04           MOV   AH,04
CD 1A           INT   1A
80 FE 05        CMP   DH,05
75 18           JNZ   004E
```

Questa routine permetteva al codice virale di attivarsi il 2 Maggio di ogni anno visualizzando a video il seguente messaggio:

Bye by C&C

Questa stringa risulta essere non visibile perchè crittografata all'interno del codice virale.

Satyricon.338

di Cristian Basso

Nome virus: Satyricon.338
Aliases: Fallen_Angel
Variante:
Isolato: Aprile 1995
Sintomi: lunghezza dei files aumentata
Origine: Italia (?)
Dimensione: 338 bytes
Tipo: Azione diretta, infetta .COM
Analisi a cura di: Cristian Basso Tel. 049/5848335

COMMENTO GENERALE

Questo virus è una variante del virus Satyricon.360 ,ha le stesse caratteristiche e alcune parti di codice uguali.
E' stato individuato alla fine di Aprile 1995 e quasi sicuramente è di provenienza italiana. Il virus è ad azione diretta, quindi quando viene eseguito infetta tutti i files .COM della corrente directory. Questi però devono iniziare con il byte E9h, cioè devono iniziare con un JUMP diretto near .Inoltre l'ultimo byte deve essere diverso da 5Fh in modo da non infettare un file che può essere già infetto.
Dopo la ricerca e ,se possibile l'infezione dei files .COM nella corrente directory viene infettato il file 'C:\COMMAND.COM'.
La lunghezza dei files aumenterà dai 338 ai 353 bytes, questa variazione è dovuta all'allineamento di paragrafo eseguito dal codice virale prima dell'infezione.

All'interno del codice sono presenti le seguenti stringhe:

```
*.COM

COMMAND.COM

FALLEN_ANGEL_
```

Quest'ultima stringa non viene mai visualizzata a video.

Questo virus non può procurare danni ,e visto il metodo di infezione non può avere una vasta infezione (infetta solo i .COM della corrente directory che iniziano con un Jump near) ,si può quindi desumere che è un virus primitivo di sperimentazione.

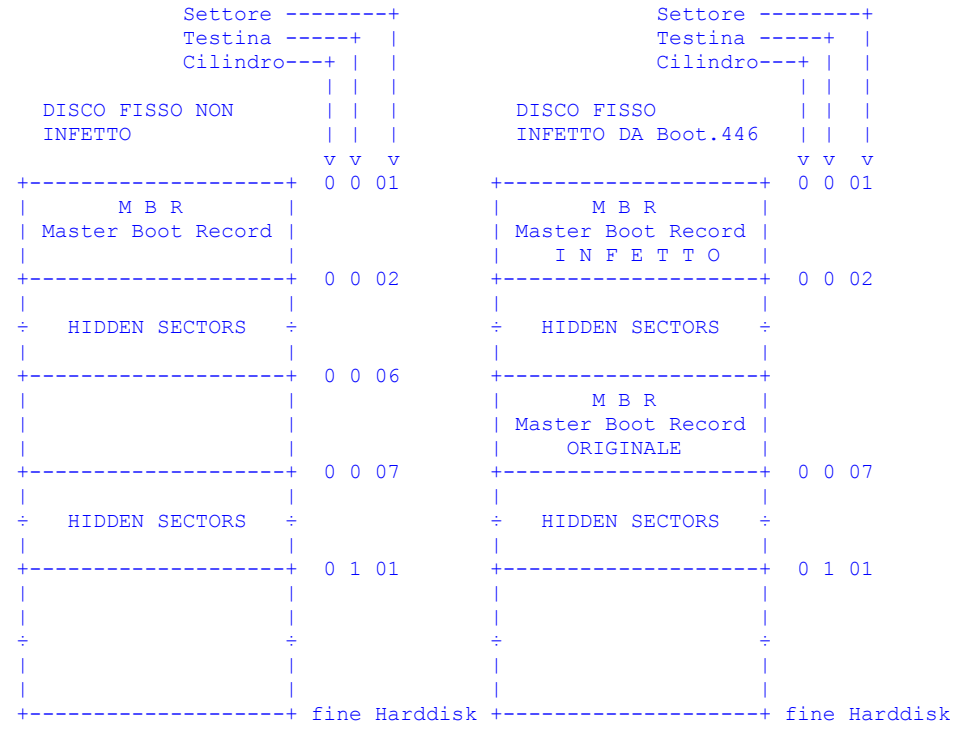
Boot.446

di Gianfranco Tonello

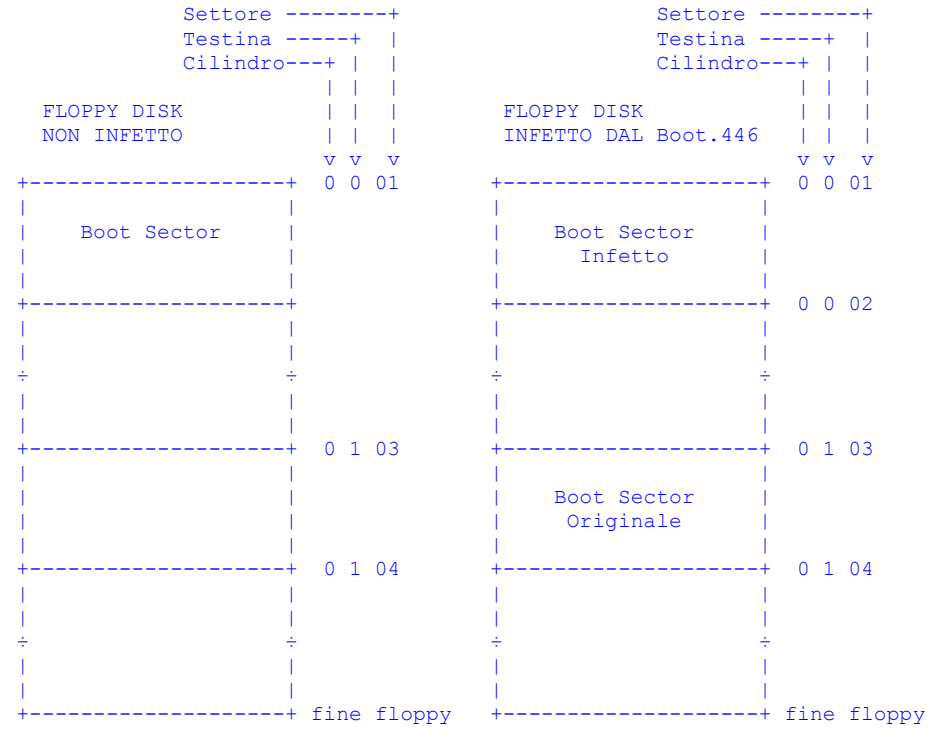
Nome virus:	Boot.446
Aliases:	
Variante:	
Stato:	Nuovo
Isolato:	Agosto 1995
Sintomi:	diminuzione della memoria libera del sistema 2kb
Origine:	Sconosciuta
Dimensione:	1 settore (la lunghezza del codice è di 446 bytes)
Tipo:	Residente in memoria, infetta boot sector (floppy disk), Master Boot Record (Hard disk).
Analisi a cura di:	Gianfranco Tonello Tel./Fax 049-631748
Data:	04/08/1995

COMMENTO GENERALE

Il virus Boot.446 è stato isolato nel mese di Agosto 1995 in Italia, la sua origine potrebbe anche non essere italiana. Il codice virale risulta essere residente in memoria (TSR), infetta il boot sector dei floppy disk e l'MBR (Master Boot Sector) del disco fisso. Quando il Boot.446 si attiva dal boot dei floppy disk, si alloca in memoria, la memoria libera del sistema diminuisce di due kilobytes. A questo punto viene intercettato l'interrupt 13H (Disk/Diskette Services) e infettato il master boot sector dell'hard disk. Il Master Boot Recors originale del disco fisso viene salvato nel settore 6, testina 0 e cilindro 0.



Ogni floppy disk, che verrà inserito non protetto in scrittura sarà infettato dal virus Boot.446 nel modo seguente:



Il codice virale Boot.446, utilizza un contatore di bootstrap dal disco fisso. Se questo risulta essere maggiore di 250, il virus sovrascrive la tabella delle

partizioni con valori casuali. Al successivo boot il disco fisso può non essere "visto" dal sistema operativo o "visto" partizionato in modo casuale.

Collabora con Italian VIRUS Magazine

Sei un ricercatore Anti-Virus, sei in grado di analizzare un codice virale, hai notizie o informazioni riguardanti i virus informatici MS-DOS, che abbiano qualche interesse per la comunità informatica italiana?
Contatta la redazione di Italian VIRUS Magazine scrivi a:

TG Soft
Via Sardegna n° 5
35030 Sarmeola di Rubano (PD)

Allega una tua presentazione e/o un tuo curriculum, nonchè una traccia del materiale in tuo possesso. Se tale materiale sarà ritenuto interessante per la pubblicazione sarai ricontattato ed invitato a scrivere un articolo.

Segnala i VIRUS circolanti in Italia

Segnalare le infezioni derivanti da virus informatici significa dare un concreto contributo alla lotta antivirale, permettendo agli sviluppatori di antivirus di mettere a disposizione dell'utenza gli antidoti per combattere efficacemente i virus più diffusi in Italia.

Come si segnalano i virus circolanti

Le infezioni informatiche in atto sono da segnalare con le seguenti modalità:
- a mezzo telefono allo 049-631748 (TG Soft)
- a mezzo Fax allo 049-631748 (24h/24)
- telematicamente in Fido Net all'indirizzo: Gianfranco Tonello 2:333/316.4
- telematicamente in INTERNET all'indirizzo e-mail: tge@maya.dei.unipd.it

Saranno gradite le seguenti informazioni:

Nome Virus: _____ Anti-virus rilevatore: _____

N.Computer colpiti: _____ Data __-__-__ Provincia: _____

Azienda: [ ] Privato: [ ]

VirIT Lite

L'antivirus gratuito sia per i privati che per le aziende

Molti utenti sono convinti che programma shareware significhi gratuito, può sembrare superfluo ricordare che non è così. Inoltre molti programmi distribuiti come shareware, hanno questa caratteristica quando sono usati da utenza PRIVATA, mentre in ambito AZIENDALE il loro uso senza la relativa LICENZA non è autorizzato. Questa situazione è tipica per molti prodotti antivirus tra i più noti. Molti, anche in ambiti aziendali, li utilizzano indiscriminatamente per lunghi periodo credendo (a torto) di essere in FASE di VALUTAZIONE. Generalmente le istruzioni che compaiono all'attivazione del software vengono ignorate (vuoi perchè in lingua inglese, vuoi per la fretta di utilizzare il programma), queste spiegano chiaramente che l'utilizzo AZIENDALE è consentito solamente se il software è munito di regolare LICENZA d'USO.

VirIT -Il Servizio Antivirus italiano- ha pensato di risolvere questo "problema" realizzando una versione GRATUITA, sia per i PRIVATI che per le AZIENDE del software antivirus VirIT, chiamata VirIT Lite.
VirIT Lite è liberamente utilizzabile e distribuibile senza scopo di lucro, viene distribuito come file VLT-*.ZIP (es. VLT-098D.ZIP etc. etc.), ed è facilmente reperibile.***

Dove trovare VirIT Lite

- in INTERNET presso il sito FTP.DSI.UNIMI.IT del D.S.I. (Dipartimento di Scienza dell'informazione) dell'Università di Milano nella directory \.1\security\docs\TGSoft
- in tutti i nodi della rete VIRNET
- presso GREENEYES BBS Tel. 049-8800998 (24h/24 fino a 14.400)
- richiedendolo a TG Soft Tel. 049-631748 (per l'invio dovrà essere corrisposta una piccola somma come contributo spese di spedizione, imballo e supporto magnetico).

Index

N

New_Exebug

NEWS

R

REALI PERICOLI

Redazione

S

Satyricon.338

SEGNALA_INFEZIONI

T

Tools

V

VCL Mutator

VCL

VirIT Lite

VIRUS CREATION 2000

Glossary

≡
#
A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
S
T
U
V
W
X
Y
Z

C

Cavallo di troia
CODICI VIRALI
Cristian Basso

E

Enrico Tonello
EURISTICO

F

FIRME VIRALI

G

Gianfranco Tonello

S

Shareware
Stealth

T

TG Soft

TROJAN

V

virus

Cavallo di troia

Trojan horse, o cavallo di troia:Programma che nasconde sotto una facciata innocua ed invitante un programma killer che generalmente distrugge i dati dell'hard disk

CODICI VIRALI

Sinonimo di virus informatico, ossia il vero e proprio programma che é in grado di autoreplicarsi.

Cristian Basso
Ricercatore anti-virus indipendente. Può essere contattato telefonando allo 049-5848335.

Enrico Tonello
Curatore delle Pubbliche Relazioni della TG Soft. Consulente di sicurezza informatica in materia antivirale in ambito bancario ed aziendale. Ha proposto diverse metodolgie per la valutazione dell'efficacia dei prodotti antivirus, soprattutto per quanto riguarda i virus polimorfici. Può essere contattato allo 049-631748.

EURISTICO

Metodo che consente di determinare se un programma esegue operazioni sospette, ossia operazioni tipiche dei virus informatici permette pertanto di intercettare dei virus di cui non si conosce ancora la firma virale.

FIRME VIRALI

Il codice esadecidemale che permette di identificare il virus. I virus polimorfici cercano di automodificarsi per non farsi intercettare dai comuni antivirus.

Gianfranco Tonello

Esperto di sicurezza informatica in ambito bancario ed aziendale, sviluppatore del software anti-virus VirIT & VirIT Lite e coordinatore di VirIT -Il Servizio Antivirus italiano-. E' contattabile telematicamente in rete FIDO Net all'indirizzo:Gianfranco Tonello 2:333/316.4in INTERNET all'indirzzo e-mail: tge@maya.dei.unipd.it

Shareware

modalità di distribuzione, che prevede la possibilità di provare il software prima di acquistarlo (try before you buy). L'utilizzatore dopo aver provato il software (per il periodo prescritto), se lo ritiene utile per la sua attività, e quindi decide di continure ad utilizzarlo dovrebbe registarsi inviando all'autore la somma richiesta.

Stealth

viene definito in questo modo un codice virale che ha la capacità di mostrare la situazione antecedente all'infezione, quindi di non farsi individuare (invisiblità).

TG Soft

Software house specializzata in Sicurezza Informatica con particolare attenzione nel campo della lotta anti-virale in ambiente MS-DOS, realizzatrice di VirIT -Il Servizio Antivirus italiano- l'unico servizio antivirus realizzato interamente in Italia, costituito da un pacchetto software e da servizi di complemento di provata efficacia in ambito bancario ed aziendale. Per ulteriori informazione Tel./Fax 049/631748 (Fax 24h/24).

TROJAN

Trojan horse, o cavallo di troia:Programma che nasconde sotto una facciata innocua ed invitante un programma killer che generalmente distrugge i dati dell'hard disk

virus
Programma in grado di autoreplicarsi.