VirIT eXplorer
Enciclopedia Virus

Referenze

# #

_184
_290
_700
_1360
10_past_3.748

_184

Azione diretta, infetta .COM, lunghezza 184 bytes. Nessuna stringa e' presente nel codice.

_290

Virus ad azione diretta, infetta file con estensione .COM, la lunghezza del codice e' di 290 bytes, ma i files infetti aumentano di una lunghezza variabile.

_700

Virus residente in memoria, infetta files con estensione .EXE. Quando un file infetto viene eseguito, il codice virale si installa in memoria, ogni file che viene eseguito (AX=4B00) o aperto (AX=3D00) nel disco fisso verra' infettato. La lunghezza del file aumentera' da 700 a 715 bytes, dovuto all'allineamento del paragrafo. Ogni file infetto sara' marcato con il valore 0505H nella chesksum word.

_1360

Virus residente in memoria, infetta files con estensione .EXE. Quando un file infetto viene eseguito, il codice virale si installa in memoria, ogni file che viene eseguito verra' infettato, la lunghezza del codice virale e' di 1360 bytes, ma il file infetto puo' aumentare da 1360 a 1376 bytes. Il virus intercetta oltre all'INT 21H anche l'INT 13H. Il codice virale contiene il seguente testo:

CHKLIST.TAV
ANTI-VIR.DAT
CHKLIST.MS

10_past_3.748

Virus residente in memoria, infetta i files con estensione .COM. I files infetti aumentano di 748 bytes. All'interno il codice virale non contiene testo.

Virus A

Abal.758
Acid.670
Ada
Akuku Family
Albania Family
Anarky.628
Andromeda.1140
Anthrax
Anticad Family
Anticmos
Antiexe
Antimon.1450
ARCV Family
Arianna Family
AT Family
Atomic_comp.425
Atomic Family
Austr_Parasite Family
Avalanche.2818

Abal.758

Virus ad azione diretta, infetta i files con estensione .COM. I files infetti aumentano di 758 bytes. All'interno il codice virale contiene il seguente testo:

ABAL - 758 (I)Virus
Thus is 758 (1) Virus ..!! Caught By Peter Ferng..!!

Acid.670

Virus residente in memoria, stealth, infetta i files .COM e .EXE quando vengono eseguiti allungandoli di 670 bytes. All'interno il codice virale contiene il seguente testo:

[Binary Acid] (c) 1994 Evil Avatar

Ada

Virus residente in memoria, infetta i files con estensione .COM allungandoli di 2600 bytes. All'interno il codice virale contiene il seguente testo:

COMMAND.COM
PCCILLIN.COM
PCCILLIN.IMG

HATI-HATI !!
ADA VIRUS DISINI !! Delete

Akuku Family

Akuku.889

Virus ad azione diretta, infetta files con estensione .COM e .EXE. I files infetti aumentano da 889 a 905 bytes. All'interno il codice virale contiene il seguente testo:

Akuku.889.A: A kuku, Nastepny komornik !!!
Akuku.889.D: (c) by Metal Thunder IVRL M

Akuku.Copmpletely

Virus ad azione diretta, infetta files con estensione .COM e .EXE. I files infetti aumentano da 1111 a 1127 bytes. All'interno il codice virale contiene il seguente testo:

Sorry, I'm copmpletely dead.

Albania Family

Virus ad azione diretta, infetta files con estensione .COM sulla corrente directory e il file COMMAND.COM. Il ceppo Albania Š composta dalle seguenti variati: Albania.429, Albania.506, Albania.575 e Albania.606.
All'interno sono visibili le seguenti stringhe:

*PATH= *.COM*

Albania.429: "ALBANIA";

Albania.506: "COMSPEC=" e "ALBANIA";

Albania.575, .606: "COMSPEC=" e "albania";

Anarky.628

Virus ad azione diretta crittografato, infetta i file .COM allungandoli di 628 bytes. All'interno il codice virale contiene il seguente testo:

-Anarky Forever- D.N.A. (C)1997

Andromeda.1140

Virus ad azione diretta, infetta i files con estensione .COM. I files infetti aumentano di 1140 bytes. All'interno il codice virale contiene il seguente testo:

-< The Andromeda Strain >-
Version 1.00 By : Crypt Keeper
Mission Complete...
Have fun with your virus(es)
*ANDROMEDA.SEC *.COM*
RUNME.COM COMMAND.COM SCAN.EXE CLEAN.EXE NAV.EXE NAV_._NO

Anthrax

Virus residente in memoria, infetta file con estensione .EXE e .COM. Quando viene eseguito un file infetto, il codice virale sovrascrive il master boot record dell'hard disk. Se eseguito dal master boot record, allora vengono infettati i files nell'hard disk. Il condice virale contiene al suo interno il seguente testo:

(c) Damage, Inc.
ANTHRAX

Anticad Family

Virus residente in memoria, infetta files con estensione .COM e .EXE, e il boot sector del disco fisso. Quando viene infettato il boot sector, il corpo del virus viene salvato dopo il master boot sector.
All'interno il codice contiene il seguente testo crittografato:

ACAD.EXE COMMAND.COM COM EXE

by Invader, Feng Chia U., Warning: Don't run ACAD.EXE!!

Anticmos

Virus residente in memoria, infetta il boot sector dei floppy disk e il master boot record dei disci fissi. Il codice virale quando Š attivo in memoria occupa 2 kb. Il virus ha la caratteristica di non preservare i boot e gli mbr originali. Casualmente altera la cmos.

Antiexe

Virus residente in memoria, stealth, infetta il boot sector dei floppy disk e il master boot record del disco fisso. Quando il calcolatore parte da un floppy infetto, il virus Antiexe infetta l'mbr dell'hard disk, si installa in memoria allocando 1 kb, ed intercetta l'int 13h. Ogni floppy disk non protetto in scrittura verra' infettato dal codice virale. Il virus Antiexe e' pericoloso quando si preme il tasto CTRL+C, viene sovrascritto il disco fisso. Il virus puo' danneggiare i file con estensione .EXE di una certa lunghezza.

Antimon.1450

Virus ad azione diretta, che infetta i files con estensione .COM. I files infetti aumentano di 1450 bytes.

ARCV Family

ARCV.255

Virus ad azione diretta, crittografato, infetta i files con estensione .COM. I files infetti aumentano di 255 bytes. All'interno il codice virale contiene il seguente testo:

Made In England

ARCV.570

Virus ad azione diretta, crittografato, infetta i files con estensione .EXE. I files infetti aumentano di 570 bytes. All'interno il codice virale contiene il seguente testo:

[X-1] ICE-9
ICE-9 Presents
In Association with The ARcV [X-1]

Michelangelo activates
-< TOMORROW >-

Esiste un'altra variante lunga 571 bytes.

ARCV.649

Virus residente in memoria, crittografato, polimorfo, infetta i files con estensione .COM. I files infetti aumentano di 649 bytes. All'interno il codice virale contiene il seguente testo:

OH NO NOT MORE ARCV
[MoRE] ICE-9

ARCV.773

Virus residente in memoria, crittografato, polimorfo, stealth, infetta i files con estensione .COM. I files infetti aumentano di 773 bytes. All'interno il codice virale contiene il seguente testo:

[Slime] By Apache Warrior, ARCV Pres

Sliming around your PC, I go make a sticky MESS over your Hard Drive!

ARCV.795

Virus residente in memoria, crittografato, stealth, infetta i files con estensione .COM. I files infetti aumentano di 795 bytes. All'interno il

codice virale contiene il seguente testo:

[SCROLL] ICE-9 ARcV
\COMMAND.COM

ARCV.916
Virus residente in memoria, crittografato, polimorfo, stealth, infetta i files con estensione .COM. I files infetti aumentano di 916 bytes. All'interno il codice virale contiene il seguente testo:

Looking Good Sliming Joanna.
Made in England by Apache Warrior, ARCV Pres.

Jo Ver. 1.11 (c) Apache Warrior 92.

I Love You Joanna, Apache..
[JO] By Apache Warrior, ARCV Pres.

ARCV.1183
Virus residente in memoria, crittografato, stealth, infetta i files con estensione .EXE. I files infetti aumentano di 1183 bytes. All'interno il codice virale contiene il seguente testo:

[BENOIT] ICE-9
Made in England
Release 5th November 1993 ICE-9
Dedicated to Benoit B. Mandelbrot

ARCV.Ice.250
Virus ad azione diretta, crittografato, infetta i files con estensione .COM. I files infetti aumentano di 250 bytes. All'interno il codice virale contiene il seguente testo:

[250] ICE-9
arCv

Arianna Family

Arianna.3375

Virus residente in memoria, crittografato, polimorfico e stealth. Infetta il master boot record e i files con estensione .EXE. Quando viene eseguito dai files, il codice virale cerca di infettare la tavola delle partizioni (MBR). Quando e' residente, la memoria libera del sistema diminuisce di 7 kb se parte dall'MBR, invece se Š eseguito dai files la memoria occupata e' di 7088 bytes. Vengono intercettati i seguenti interrupts: 21h, 2fh, 02h, 24h e 13h
Ogni programma con lunghezza compresa tra i 6000 e 458651 bytes, con struttura eseguibile (cioe' 'MZ' o 'ZM') che venga "eseguito", "chiuso" e "creato" potra' essere infettato dall'Arianna.3375, facendone aumentare la lunghezza di 3375 bytes. La data dei files non risulta venire modificata, ma il campo dell'ora nella sezione dei minuti secondi viene settato a 62.
Questa marchiatura permette al codice virale di riconoscere i files gia' infetti, e di attivare la routine stealth.
Se l'attivazione del codice virale avviene dalla tavola delle partizioni
viene incrementato un suo contatore interno per il conteggio dei Boot del calcolatore a partire dall'infezione. Quando questo contatore raggiunge il valore 400 (cioŠ sono stati eseguiti 400 boot) il virus rende visibili i suoi effetti video, visualizzando in modalita' grafica VGA/MCGA 302x200 pixel 256 colori il seguente messaggio:

Oltre questo stringa, ve ne sono altre crittate all'interno del codice:

Bcoded in BARI ThanX to DOS UNDOCUMENTED See you for a new release. Bye!

Sono conosciute altre due varianti di lunghezza rispettivamente 2864 e 3426 bytes.

AT Family

AT.149

Virus residente in memoria, infetta i files con estensione .COM. Il file infetto risulta allungato di 149 bytes, data e ora sono alterate con i valori all'atto dell'infezione. Esiste un'altra variante lunga 144 bytes.

AT_II.114

Virus residente in memoria, infetta i files con estensione .COM e .EXE. Il file infetto risulta allungato di 114 bytes, ma il suo contenuto risulta essere sovrascritto da valori casuali. Il codice virale si inserisce all'inizio del file.

AT_II.118, AT_II.122

Virus residente in memoria, infetta i files con estensione .COM.
Il file infetto risulta allungato di 118 (122) bytes.

Atomic_comp.425

Virus residente in memoria, gemellare, infetta i files con estensione .COM. I files infetti sono lunghi 425 bytes. Il codice virale contiene il seguete testo:

Atomic v1.00 by MnemoniX

Atomic Family

Atomic.371

Virus primitivo, che sovrascrive i files con estensione .COM nella corrente directory.
Il codice virale e' lungo 371 bytes, al suo interno sono visibili le seguenti stringhe:

[TAD1A] Memory Lapse -- Toronto, CANADA
The Atomic Dustbin 1A -- This is just the first step

Bad command or file name

Atomic.480

Virus primitivo, che sovrascrive i files con estensione .COM nella corrente directory.
Il codice virale e' lungo 480 bytes, al suo interno sono visibili le seguenti stringhe:

[TAD1B] Memory Lapse -- Toronto, CANADA
The Atomic Dustbin 1B -- This is almost the second step

Program execution terminated

The Atomic Dustbin - YOUR PHUCKED

Austr_Parasite Family

Austr_Parasite.338
Austr_Parasite.369
Austr_Parasite.377
Austr_Parasite.440
Austr_Parasite.482
Austr_Parasite.491
Austr_Parasite.550
Austr_Parasite.615
Austr_Parasite.635
Austr_Parasite.762
Austr_Parasite.784
Austr_Parasite.1169
Austr_Parasite.Vga_Demo

Austr_Parasite.338

Virus residente in memoria, infetta .COM aumentadoli di 338 bytes.
Contiene il seguente testo:

It is pitch black. You are likely to be eaten by a Grue

Austr_Parasite.369

Virus ad azione diretta, crittografato, infetta .COM aumentadoli di 369 bytes. Contiene il seguente testo:

[Aussie Parasite vIRUS v. 1.1]
[bLAME oTHERS]

Austr_Parasite.377

Virus residente in memoria, infetta .COM aumentadoli di 377 bytes.
Contiene il seguente testo:

Kill Dorn W. Stickle
(C) 1992 Australian Parasite

Austr_Parasite.440

Virus residente in memoria, crittografato, infetta .COM aumentadoli di 440 bytes.
Contiene il seguente testo:

Anke Huber is kicken butt on her way to be the number one womens tennis player
Arantxa Sanchez-Vicario is a steroid abuser.

Austr_Parasite.482

Virus residente in memoria, infetta .COM aumentadoli di 482 bytes. Contiene il seguente testo:

The Hitcher virus. Hitvhhiking through your system.
Didn't your mum tell you not to pick up stray viruses.
The Hitcher virus #1 by AP

Austr_Parasite.491

Virus residente in memoria, infetta .COM aumentadoli di 491 bytes. Contiene il seguente testo:

This virus was written by Jack Kenyon to test out Virus Buster.
Phone (07) 343 8866 in Australia if you have any problems

Austr_Parasite.550

Virus residente in memoria, infetta .COM aumentadoli di 550 bytes. Contiene il seguente testo:

1 Did David Gerrold have a harley when he was one?
2 Is John Brunner a shocking wave rider?
3 Is William Gibson a neurotic romantic?
4 Is the Australian Parasite the best?

1:No, 2:Yes, 3: Probably, 4: Absolutley

**.com*

Austr_Parasite.615

Virus residente in memoria, infetta .COM aumentadoli di 615 bytes. Contiene il seguente testo:

A Kevin Mitnick
U Lenny DiCcoco
S Hans Hubner
T 414's
Legion of Doom
Phiber Optik
P Dr Popp
Robert Morris
1 Shooting Shark
9 Chesire Catalyst
9 Captain Crunch
2 Ron Austin
Kevin Poulsen

Austr_Parasite.635

Virus residente in memoria, infetta .COM aumentadoli di 635 bytes. Contiene il seguente testo:

Kevin Mitnick
Lenny Dicco
Hans Hu ner
414's
Legion of Doom
Phiber Optik
Dr Popp
Robert Morris
Shooting Shark
Chesire Catalyst
Captain Crunch
Ron Austin
Kevin Poulsen
Edward Singh

are all to be congratulated

Austr_Parasite.762

Virus residente in memoria, infetta .COM aumentadoli di 762 bytes. Contiene il seguente testo:

(C) 1993 AIH; Australian Institute of Hackers.
Greets to PuKE, SCP and fellow Aussie Viral creators
You Help us to keep the Australian end of the virus underground alive.
I need to go to the Jon. More coffee anyone.
You Pat the rich huh, Hey man I Prefer the poor.
You Frigid Skilless son, of mine, won't even feel her up will ya.
Lets go to the Mall and look for Fergie's son.
Its a Cross between an icerberg and cow manure.
January, February, March April, you can't make a tapestry with a staple.
I'm Cold and Feeble.

Austr_Parasite.784

Virus residente in memoria, infetta .COM aumentadoli di 784 bytes. Contiene il seguente testo:

1. Thou shalt spread viruses
2. Thou shalt be origional
3. Thou shall not create a variant of anothers virus
4. Thou shall put witty phrases in ones codes
5. Thou shall not destroy code
6. Thou mist love Tonya Harding
7. Thou must love Anke Huber
8. Thou must condemn any virus writter brought to trial
9. All text must be in flowing English (Asians take note)
0. Its easier to write a Boot Sector virus than a resident virus

Anke Huber is the best tennis player in the world.
says the Australian Parasite

Austr_Parasite.1169

Virus residente in memoria, infetta .COM aumentadoli di 1169 bytes. Contiene il seguente testo:

SCP, What frigen lamers, Can you folks write anything else be sised
Overwriting or Vienna variant viruses.
TPE is better than MTE.
Brainnsssss, Brainnsssss,
When there is no more room in HELL,
The dead will walk the EARTH.
(C) George A. Romero
Count Zero died in the sprawl.
Ahh The joys of safe hex
Its not my fault. Its all those horror movies and death metal music.
Try to get past logging in,
Put another password in,
Bomb it out and try again.
We're Hacking, Hacking, Hacking.
Try his first wifes maiden name,
This is more than just a game.
But there again, its all the same.
Its Hacking, Hacking, Hacking.
People who use VCL, and PS-MPC are bigger lamers than SCP.

This virus was written by Jack Kenyon to test out Virus Buster.
Phone (07) 343 8866 in Australia if you have any problems.

Austr_Parasite.Vga_Demo

Virus residente in memoria, infetta .COM aumentadoli di 3896 bytes. Contiene il seguente testo:

VGA Demo dropper by AP + DV + EV

Avalanche.2818

Virus residente in memoria, stealth, crittografato, infetta i files con estensione .COM e .EXE. I files infetti aumentano di 2818 bytes. All'interno il codice virale contiene il seguente testo:

X AVALANCHE / Germany '94
Metal Junkie greets Neurobasher

B

B1
Backfont.765
Bad_Boy.1000
Bad_Brains.554
Bad_Bytes
Barrotes Family
Beethoven
BetaBoys.615
Bit_Addict.477
Blink Family
Blinky.1302
Blood.418
Bloodlust
Bloody_Warrior
Boot.388
Boot.446
BootEXE.451
Burger Family
Burglar.1150
Burma Family
Butterfly Family
BW Family
Bye
ByWay

B1

Il virus B1 è stato isolato per la prima volta nel mese di Ottobre 1994 in Italia, molto probabilmente la sua origine potrebbe anche non essere italiana, visto che è conosciuto negli Stati Uniti con il nome NYB.
Colgo l'occasione per sottolineare come sia necessario che i produttori di antivirus si uniformino ad un unico standard, questo per riuscire a capire quali e quanti siano i virus realmente circolanti. A tale proposito gli sviluppatori di anti-virus europei per la maggior parte, sono uniformati allo standard C.A.R.O. (Computer Antivirus Research Organization). Gli sviluppatori d'oltre oceano, snobbano questo standard e si affidano alla classificazione del N.C.S.A. (National Computer Security Association).
Il codice virale risulta essere residente in memoria (TSR), stealth, infetta il boot sector dei floppy disk e l'MBR (Master Boot Record) del disco fisso.
Quando il B1 si attiva dal boot dei floppy disk, si alloca in memoria nel modo consueto occupando 1 KB, la memoria libera del sistema diminuisce di un kilobyte. A questo punto viene intercettato l'interrupt 13H (Disk/Diskette Services) all'indirizzo CS:0044H e infettato il Master Boot Record (MBR) dell'hard disk. L'infezione del Master Boot Record è similare a quella addottata dal molti codici virali che infettano l'MBR. Il virus B1 quando infetta il master boot record (cilindro 0, testina 0, settore 1) del disco
fisso, salva l'MBR originale nella posizione: cilindro 0, testina 0, settore 17.
Ogni floppy disk, che verrà inserito non protetto in scrittura sarà infettato dal virus B1.
Una caratteristica del codice virale è quella di essere invisibile (stealth) quando è residente in memoria, cioè in questa situazione andando a leggere il boot sector di un floppy disk o la tavola delle partizioni (MBR) di un disco fisso infetto, il virus B1 mostrerà rispettivamente i settori originali, quelli non infetti.
Ad ogni accesso all'interrupt 13H con la funzione (AH=02 Read Disk/Diskette Sectors), il codice virale B1 legge il secondo ed il terzo bytes del Timer Ticks Counts (0040:006C) ed esegue l'operazione AND con il valore 178FH. Se questa operazione risultasse nulla, allora viene attivata la routine di payload del codice virale. Il payload del virus B1, consisterebbe nella lettura in modo alternativo del settore di coordinate cilindro=0 testina=0 settore=1 e del settore di coordinate cilindro=255 testina=0 settore=1 (in caso di floppy disk) o del settore di coordinate cilindro=1023 testina=0
settore=1 (in caso di hard disk). Nel caso di floppy disk, la lettura del cilindro 255 non è fisicamente possibile con i correnti disk drive in commercio. I valori limiti per i drive
da 1.44 Mb e 2.88 Mb nei vari formati è di 80 cilindri per testina. Quindi il tentativo di accesso al cilindro 255 produrrebbe lo sbattimento della testina del drive contro il fine corsa. Il payload del codice virale B1 potrebbe in alcuni casi danneggiare la testina del disk drive. Fino ad ora per• non è ancora stata segnalata da alcuno questa situazione, ed abbiamo evitato di riprodurre l'evento in laboratorio.

Backfont.765

Virus residente in memoria, infetta i files .EXE che vengono eseguiti. I files infetti aumentano di 765 bytes.

Bad_Boy.1000

Virus residente in memoria, infetta i files con estensione .COM allugandoli di 1000 bytes. All'interno il codice virale contiene il seguente testo crittografato:

The bad boy halt your system .....

The Bad Boy virus Copyright (C) 1991

BAD_BRAINS.554

Virus di tipo sovrascrittura, infetta file .COM, sovrascrivendo 554 bytes. Il virus risulta essere crittografato, contiene all'interno il seguente testo:

*SKISM *.COM *
Bad Brains

Bad_Bytes.109

Virus primitivo, che sovrascrive i files .COM con bytes casuali.
All'interno il codice virale contiene il seguente testo:

Bad_Bytes (C) 1998
Proprietary of TNT

Barrotes.1310

Questo codice virale è noto dalla fine del 1992 e la sua provenienza è sicuramente spagnola. Il virus è residente in memoria (TSR), non crittografato ed infetta i file con estensione .EXE e .COM.
Quando un programma infetto dal Barrotes.1310 viene eseguito il virus si installa in memoria allocando 1600 bytes ed intercetta gli interrupts 21H (funzioni DOS) e 24H (gestione degli errori critici) e il 5 gennaio anche l'interrupt 1CH (User Timer Tick) e infetta il COMMAND.COM posto in radice.
Ogni file eseguito con estensione .EXE e .COM (con lunghezza compresa tra 256 e 64002 bytes) verrà infettato, la lunghezza dei file colpiti aumenterà di 1310 bytes. I files infetti sono marcati alla fine con la stringa SO. La data e l'ora dei files infetti non vengono alterate. Il virus si attiva il 5 gennaio sovrascrivendo il master boot record (MBR) del disco fisso con i primi 512 bytes del codice virale, con la conseguenza
che non si può accedere al disco fisso. In questa data viene intercettato l'interrupt 1CH (User Timer Tick), il quale visualizza a video in alto a sinistra il seguente messaggio:

Virus BARROTES por OSoft

di colore bianco su sfondo blu, inoltre vengono visualizzate 8 colonne di vario colore, composte da 3 caratteri che prendono tutto lo schermo. Il messaggio visualizzato a video risulta essere crittografato. Il codice virale Barrotes contiene inoltre la stringa c:\command.com che risulta essere visibile, cioè non crittografata. Esistono altre due varianti del virus Barrotes, lunghe rispettivamente 1194 e 1303 bytes. Il virus Barrotes.1303 risulta essere crittografato e contiene inoltre il seguente testo:

Sta Tecla (MAD1)

Beethoven

Virus residente in memoria, crittografato, infetta i files con estensione .COM e .EXE.
All'interno il codice virale contiene il segeunte testo:

Beethoven is here....
And now. enjoy the music

BetaBoys.615

Virus residente in memoria, crittografato, infetta i files con estensione COM allungandoli di 615 bytes. All'interno il codice virale contiene il seguente testo:

DEATH RATTLE V1.00 (c) 1992 The BetaBoys Development Corp.

I BetaBoys sono un gruppo di virus-writer svedesi, esiste un'altra variante lunga 575 bytes.

Bit_Addict.477

Virus residente in memoria, infetta i files con estensione .COM allungadoli di 477 bytes. Ogni files infetto contiene all'inizio (offset 3) il seguente testo:

BIT ADDICT

Inoltre il codice virale può sovrascivere il disco fisso e visualizza a video il seguente messaggio:

The Bit Addict says:
"You have a good taste for hard disks, it was delicious !!!"

Blink Family

Blink.501

Virus residente in memoria, infetta i files con estensione .COM. I files infetti aumentano di 501 bytes. Il virus casualmente fa lampeggiare lo schermo.

Blinky.1302

Virus ad azione diretta, infetta i files con estensione .COM e il boot sector dei floppy disk. I files infetti aumentano di 1302 bytes. All'interno il codice virale contiene il seguente testo:

[Blinky Ghost]
The Pac-Man BLINKY Ghost is watching
[-Inky-]
[-Inky!-]=
[INKY Ghost] by PacMan and Associates inc.

Blood.418

Virus ad azione diretta, infetta i files con estensione .COM allungandoli di 418 bytes.
All'interno il codice virale contiene il seguente testo:

File infected by BLOOD VIRUS version 1.20

Bloodlus

Virus primitivo che sovrascrive i files con estensione .COM nella corrente directory.
Il codice virale è lungo 302 bytes, al suo interno è visibile il seguente testo:

Hi! This is the virus Blood Lust striking!
Sorry to tell tou, but your system is infected.

Bloody_Warrior

Questo codice virale è stato individuato nella prima settimana di dicembre 1993, la sua provenienza è sicuramente italiana. Il virus è residente in memoria (TSR), crittografato ed infetta i file con estensione .EXE e .COM. Quando un programma infetto dal Bloody_Warrior viene eseguito il virus si installa in memoria allocando 2768 bytes ed intercetta gli interrupts 21H (funzioni DOS) e 24H (gestione degli errori critici). Ogni file eseguito, aperto, rinominato, letto o modificato negli attributi, con estensione .EXE e .COM (con lunghezza infeziore a 60.000 bytes) verrà infettato, la lunghezza dei file colpiti aumenterà di 1344 bytes. Il virus prima di procedere all'infezione del file ne controlla il nome, verifica se la parte terminale del nome dei files .COM finisce con: "STOP" (molto probabilmente corrispondente al VIRSTOP.COM di F-Prot), invece per i file .EXE se termina con: "SCAN" (SCAN.EXE di McAfee Associates), "SHIELD" (VSHIELD.EXE di McAfee Associates), "CLEAN" (CLEAN.EXE di McAfee Associates), "CV" (CodeView Microsoft), "DEBUG" (DEBUG.EXE del DOS) e "TD" (TD.EXE Turbo Debugger della Borland), allora si disattiva dalla memoria, cioè risetta l'interrupts 21H con i vettori originali (quelli relativi a prima che si installasse in memoria).
I file .COM infetti saranno marcati all'offset 6 con la WORD 7347H, mentre i file .EXE saranno marcati all'offset 12H. Data e ora dei file infetti non vengono alterate. Il virus si attiva tutti i giorni a partire dal 4 luglio fino alla fine del mese, sovrascrivendo 256 settori partendo dal settore logico n. 1 del disco corrente con valori casuali. All'interno del codice virale, dopo la sua decrittografazione, sono visibili le seguenti stringhe, le quali non vengono mai visualizzate a video:

" FUCK YOU "
" EXECOMSCANSTOPSHIELDCLEANCVDEBUGTD "
" Hello, world ! I am the Bloody Warrior. Nice to meet you. "
" What about this virus ? Funny ? There is no hope for you. "
" This virus was released in Milan 1993. Bloody Warrior "

Boot.388

Il virus Boot.388 e' stato isolato nel mese di Maggio 1996 in Italia (Aosta), 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 del disco fisso. Quando il Boot.388 si attiva dal boot dei floppy disk, si alloca in memoria, la memoria libera del sistema diminuisce di otto kilobytes. A questo punto viene intercettato l'interrupt 13H (Disk/Diskette Services) e infettato il boot sector del disco disso. Il Boot sector originale del disco fisso viene salvato nel settore 7, testina 0 e cilindro 0.
Ogni floppy disk, che verra' inserito nel drive 0, non protetto in scrittura, sara' infettato dal virus Boot.388. Il virus Boot.388, salva il boot originale nel settore 14, cilindro 0,
testina 1, alcuni formati dei floppy hanno solo 9 settori per traccia, quindi non viene salvato il settore originale. Ad esempio nei floppy disk da 1.44Mb viene salvato il boot originale, invece nei floppy da 720Kb questa operazione fallisce.
Il codice virale Boot.388, si attiva il 20 marzo di ogni anno sovrascrivendo 5 settori alla volta, partendo dal settore 1, cilindro 0 e testina 1 con valori casuali.

Boot.446

Il virus Boot.446 e' 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 verra' inserito non protetto in scrittura sara' infettato dal virus Boot.446.
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 puo' non essere "visto" dal sistema operativo o "visto" partizionato in modo casuale.

BootEXE.451

Virus residente in memoria, infetta il boot sector dei floppy disk e del disco fisso e files con estensione .EXE. La lunghezza del codice virale e' di 451 bytes. Quando il virus e' attivo la memoria libera del sistema diminuisce di 4 KB. Il virus non preserva il boot sector originale dei floppy disk. I files .EXE vengono infettati se l'header del programma e' in grado di contenere il codice virale.

Burger Family

Virus tipo primitivo, che sovrascrive il file distruggendone il contenuto. Esisitono varianti che infettano solo files con estensione .COM, altre che infettano sia .COM e .EXE. Le varianti vanno da 382 a 560 bytes, il numero di codici virali di questa famiglia non e' precisabile, perche' l'autore Ralf Burger nel 1987 pubblic• in un libro sui virus informatci il sorgente del codice virale. Alcune varianti possono sovrascrivere il disco fisso.

Burglar.1150

Virus residente in memoria, stealth, infetta i files con estesione .EXE. I files infetti aumentano di 1150 bytes. Il codice virale all'interno contiene il seguente testo:

EAT THE GRAVE OF GRANDMA

Burglar

CLHWTBF-WVCTK

L'ultima stringa corrisponde alle iniziali di alcuni prodotto anti-virus.

Burma Family

Burma.442

Virus tipo primitivo, che sovrascrive il file distruggendo il contenuto. Il virus crea files lunghi 442 bytes. Quando viene eseguito un files infetto, viene visualizzato una spirale e il seguente testo:

[Tempest - à]

Rangon, Burma

Burma.563

Virus tipo primitivo, che sovrascrive il file distruggendo il contenuto. Il virus crea files lunghi 563 bytes. Quando viene eseguito un files infetto, viene visualizzato una spirale e il seguente testo:

Reading system configur, please wait.
S w i z z l e S t y x x !

Butterfly Family

Butterfly.Butterfly

Virus ad azione diretta, infetta files con estensione .COM. Il file infetto aumenta di una lunghezza pari a 302 bytes. All'interno il codice contiene il seguente testo:

Goddamn Butterflies

Butterfly.Crusades.COM, .EXE

Virus ad azione diretta, infetta files con estensione .COM per il virus Butterfly.Crusades.COM, invece per il Butterfly.Crusades.EXE i files con estensione .EXE. I files infetti aumentano di una lunghezza pari a 302 bytes. All'interno il codice contiene il seguente testo:

Hurray The Crusades

BW Family

BW.512

Virus ad azione diretta, crittografato, infetta i files con estensione .COM. I files infetti aumentano di 512 bytes. All'interno del codice virale sono presenti le seguenti stringhe:

[DP/1] Dementia Praecox by MnemoniX

BW.Mayberry.402

Virus ad azione diretta, infetta i files con estensione .COM. I files infetti aumentano di 402 bytes. All'interno del codice virale e' visibile la seguente stringa:

[BW] Velmalou (c) by HypoDermic!!
Part of the Mayberry Family!!!

BW.Mayberry.409

Virus residente in memoria, infetta i files con estensione .COM. I files infetti aumentano di 409 bytes. All'interno del codice virale e' visibile la seguente stringa:

[BW] OPY (c) by HypoDermic!!
Part of the Mayberry Family!!!

Bye

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 e' 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 verra' inserito non protetto in scrittura sara' infettato dal virus Bye.
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 e' quella di essere invisibile (stealth) quando e' 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.
Questa routine permetteva al codice virale di attivarsi in certi giorni (es. il 2 maggio) di ogni anno visualizzando a video il seguente messaggio:

Bye by C&C

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

ByWay

Virus residente in memoria, crittografato, polimorfico, stealth, infetta i files con estensione .COM e .EXE. Tutti i files infetti vengono ridirezionati allo stesso cluster, il quale costituisce il files CHKLIST.MS di 2048 bytes, cioe' il corpo del virus ByWay. Questa tecnica di infettaggio e' stata utilizzata in precedenza dal virus Dir_II.
Il codice virale ByWay contiene il seguente testo:

The-HndV

<by:Wai-Chan, Aug 94, UCV>

C

Carzy.9849.B
Cascade Family
Cereal
Chinese_Fish
CK.183
Clonewar Family
Coib.702
COMVIRUS
Creeper.252
Crepate.2910

Carzy.9849.B

Virus residente in memoria, infetta i files .COM e .EXE. I files infetti aumentano di 9849 bytes. Il codice virale crea un file nascosto di lunghezza zero con il nome: ABBA«º11

Cascade Family

Cascade.1701, .1701.Yap

Virus residente in memoria, crittografato, infetta i files che vengono eseguiti con estensione .COM. Il nome del codice virale deriva dal fatto che il virus fa cadere casualmente le lettere che appaiono a video. I files infetti aumentano di 1701 bytes.

Cascade.1704

Molto similare al Cascade.1701, la diversita' consiste nella lunghezza del codice virale che risulta piu' lunga di 3 bytes. Esiste una variante del Cascade.1704 che puo' formattare il disco.

Cereal

Virus ad azione diretta, crittografato, infetta i files con estensione .COM e .EXE. Il virus Cereal risulta essere compresso con LZEXE o con un programma similare, molto probabilmente il codice virale e' stato scritto con un linguaggio ad alto livello. I files .COM infetti vengono convertiti nella struttura da file .EXE. I files infetti aumentano di 5850 bytes, in alcuni casi possono essere danneggiati nella fase di infezione. Casulmente il codice virale visualizza il seguente messaggio:

I wish i had some god-damn milk! My cereal just aint the same!

Chinese_Fish

Virus residente in memoria, infetta il boot sector dei floppy disk e il master boot record dei dischi fissi. All'interno il codice virale contiene il seguente testo:

Hello! I am FISH, please don't kill me
Congratulate 80th year of the Republic of China
Building,Fish will help stone
Written by Fish in NTIT TAIWAIN 80.10.18

CK.183

Virus ad azione diretta, infetta i files con estensione .COM allungandoli di 183 bytes.
All'interno il codice virale contiene il seguente testo:

-C.K.-

Clonewar.Family

Clonewar.247

Virus tipo gemellare, che crea files nascosti con estensione .COM, con attributo HIDDEN (nascosto) lunghi 247 bytes.

Clonewar.546

Virus tipo gemellare, che crea files nascosti con estensione .COM, con attributo HIDDEN (nascosto) lunghi 546 bytes. Il codice virale contiene il seguente testo:

Beyond
The rim of the star-light
My love
Is wand'ring in star-flight
I know
He'll find in star-clustered reaches
Love
Strange love a star woman teaches.
I know
His journey ends never
His star trek
Will go on forever.
But tell him
While he wanders his starry sea
Remember, remember me.

[TrekWar]

**.EXE COM*

Clonewar.923

Virus tipo gemellare, che crea files nascosti con estensione .COM, con attributo HIDDEN (nascosto) lunghi 923 bytes. Il virus si attiva dalle ore 16 in poi, quando viene eseguito un files infetto, il cicalino del computer inizia a suonare.

Coib.702

Virus residente in memoria, infetta i files con estensione .COM. I files infetti aumentano di 702 bytes. All'interno il codice virale contiene il seguente testo:

CO
IB

COMVIRUS

Virus ad azione diretta, infetta files con estensione .COM. Il file infetto aumenta di 321 bytes. Quando viene eseguito un file infetto, il codice virale visualizza a video il seguente messaggio:

This file infected with COMVIRUS 1.0

Creeper.252

Virus residente in memoria, infetta i files con estensione .COM allungandoli di 252 bytes. Esiste un'altra variante lunga 475 bytes.

Crepate.2910

Virus residente in memoria, stealth, crittografato, multipartito: infetta files di tipo .COM e .EXE, il Master Boot Record dell' Hard Disk e il Boot Sector dei floppy disk. Il virus all'interno contiene il seguente testo:

COMcomEXEexeOV?ov?
Crepate (c)1992/93-Italy-(Pisa)
Crepa(c) bye R.T.

D

Danish_Tiny.Brenda
Dark_Avenger.2000.Traveler
DarkMan Family
Darth Family
Datalock.920
Day10.674
Deathboy.937
DelCMOS.B
Devil's_Dance
Diamond Family
Die_Hard_2
DM Family
Dream_Man
DY.278

Danish_Tiny.Brenda

Virus ad azione diretta, infetta files con estensione .COM. Quando un file viene infettato aumenta di 256 bytes. Quando viene eseguito il codice virale controlla l'ora del sistema, se e' il 5° centesimo di secondo, visualizza a video il seguente messaggio:

(C) '92, Stingray/VIPER Luv, Brenda

Dark_Avenger.2000.Traveler

Virus residente in memoria, stealth, non crittografato, infetta files con estensione .COM e .EXE. La lunghezza del codice virale e' di 2000 bytes. All'interno del codice sono presenti le seguenti stringhe:

Copy me - I want to travel

(c) 1989 by Vesselin Bontchev

Vesselin Bontchev e' uno dei maggiori ricercatori mondiali contro i virus informatici, ed e' stato responsabile del VTC (Virus Test Center) dell'Universita' di Amburgo.

DarkMan Family

DarkMan.5718

Virus ad azione diretta, infetta i files .EXE (rovinandoli). Il codice virale contiene il seguente testo:

Dark Man Virus!!
by TNT (C) 98

DarkMan.Gaia.5904

Virus Primitivo, che sovrascrive i files con estensione .EXE. Il virus e' lungo 5904 bytes. Il virus contiene il seguente testo:

Gaia By DarkMan of the NukeTeam (C) 1998

Molto probabilmemte il codice virale e' dedicato a Gaia De Laurentis.

Darth Family

Virus residenti in memoria, ma sovrascrivano all'inizio i file con estensione COM. La lunghezza in bytes di file sovrascritto dipende dal tipo di Dart: 201, 255, 344 bytes. All'interno del codice e' presente la seguente stringa:

Darth Vader

Dalla quale si puo' intuire che l'autore del codice e' un appassionato di Guerre Stellari.

Datalock.920

Virus residente in memoria, infetta files con estensione .EXE e .COM. I files con estensione .COM vengono infettati nel caso che la loro dimensione sia superiore a 22999 bytes. All'interno del codice e' presente la seguente stringa:

Datalock version 1.00

Day10.674

Virus ad azione diretta, infetta i files con estensione .COM allungandoli di 674 bytes.
Il virus si attiva nei giorni che sono divisibili per 10 sovrascrivendo il disco fisso.

Deathboy.937

Virus ad azione diretta, crittografato, infetta i files con estensione .COM e .EXE, aumentadoli di 937 bytes. All'interno del codice contiene il seguente testo:

k_CMOS / Konthark

DelCMOS.B

Il codice virale DelCMOS e' un virus residente in memoria, stealth, infetta il master boot record del disco fisso e il boot sector del floppy disk. Quando il DelCMOS.B si attiva dal boot dei floppy disk, si alloca in memoria all'indirizzo 9F80:0, la memoria libera del sistema diminuisce di due kilobyte. A questo punto viene intercettato l'interrupt 13H (Disk/Diskette Services) all'indirizzo CS:00A3H e infettato il Master Boot Record (MBR) dell'hard disk. L'infezione del Master Boot Record e' similare a quella addottata dal molti codici virali che infettano l'MBR. Il virus DelCMOS.B quando infetta il master boot record (cilindro 0, testina 0, settore 1) del disco fisso, salva l'MBR originale nella posizione: cilindro 0, testina 0, settore 2.
Ogni floppy disk, che verra' inserito non protetto in scrittura sara' infettato dal virus DelCMOS.B. Non tutti i formati dei floppy disk vengono infettati. Il settore di boot originale viene copiato in un'area non molta sicura, che puo' essere sovrascritta quando l'utente copia dei files all'interno del floppy disk.
Una caratteristica del codice virale e' quella di essere invisibile (stealth) quando e' residente in memoria, cioe' in questa situazione andando a leggere il master boot record del disco fisso, il virus mostrera' il settore originale, quello non infetto.

Devils_Dance

Virus ad azione diretta, residente, infetta files con estensione .COM. La lughenzza del codice virale e' di 941 bytes, ma il virus puo' infettare piu' volte lo stesso files. Il codice virale puo' cambiare il colore del testo a video, se si preme CTRL+ALT+DEL viene visualizzato a video il seguente messaggio:

DID YOU EVER DANCE WITH THE DEVIL IN THE WEAK MOONLIGHT ?
PRAY FOR YOUR DISKS!!

The Joker

La variante Devil's_Dance.A dopo aver premuto 5000 tasti sovrascrive un settore del disco fisso.

Diamond Family

Diamond.1024
Virus residente in memoria, stealth, infetta files con estensione .COM e EXE. I files infetti aumentano di 1024 bytes, all'interno del codice non sono visibili stringhe.

Diamond.Damage
Virus residente in memoria, stealth, infetta files con estensione .COM e EXE. I files infetti aumentano di 1063 bytes, all'interno del codice e' visibile la seguente stringa:

DAMAGE!!!!

Diamond.Lucifer
Virus residente in memoria, stealth, infetta files con estensione .COM e EXE. All'inerno del codice e' visibile la seguente stringa:

Lucifer (C) by C. J

L'autore di questa variante e' Cracker Jack, virus-writer italiano che ha firmato molti codici virali:

Die_Hard_2

Virus residente in memoria, stealth, crittografato, infetta files con estensione .COM e .EXE. La lunghezza del codice virale e' di 4000 bytes. All'interno del codice e' presente la seguente stringa:

SW DIE HARD 2

DM Family

DM.330

Virus residente in memoria, crittografato, infetta i files con estensione COM. I files infetti aumentano di 330 bytes. All'interno del codice e' visibile il seguente testo:

(C)1991 1.05 DM

DM.400

Virus residente in memoria, infetta files con estensione .COM. I files infetti aumentano di 400 bytes. All'interno del codice e' visibile il seguente testo:

(C) 1990 DM

Dream_Man

Il virus e' residente in memoria, polimorfico, infetta files con estensione COM e .EXE. L'infezione del file avviene quando si esegue il comando DOS DIR, verranno infettati un numero casuale di file, la scelta del file risulata essere anche questa casuale. I file infetti aumenteranno di una lunghezza variabile, questo e' dovuto al fatto che il virus e' polimorfico. Il corpo del codice virale e' lungo 2000 bytes. All'interno del codice
sono presenti le seguenti stringhe:

SCCLF-VIMSVSWI

[Dream Man / Doctor Revenge] 12-02-94 Italy

DY.278

Virus ad azione diretta, infetta i files con estensione .COM allungandoli di 278 bytes.
All'interno il codice virale contiene il seguente testo:

DY

E

Ear.1024.A
Elephant-2.Trojan
Eli
Enola.1864
Epbr
Estonia
Exe252.252
Excel Macro Virus
Explosion.1000

Ear.1024

Virus ad azione diretta, crittografato, infetta i files con estensione .COM e EXE, allungandoli di 1024 bytes. I files .EXE in alcuni casi sono distrutti dal codice virale. Il virus contiene il seguente testo:

[EAR-6] Dark Angel

1Auditory Canal
1Lobe
2Hammer
2Eustachian Tube
3Auditory Nerve
3Cochlea

PHALCON/SKISM 1992 [Ear-6]
Alert!
Where is the $ located?
1. External Ear
2. Middle Ear
3. Inner Ear ( )

You obviously no nothing about ears.
Try again after some study.

Wow, you know you ears!
Please resume work.

Elephant_2.Trojan

Cavallo di Troia, scritto molto probabilmente in C. Non interessante.

Eli

Virus residente in memoria, crittografato, infetta i files .COM. I files infetti aumentano di 1143 bytes, data e ora del file risulta essere alterata con i valori di quando e' stato infettato. Il codice virale contiene al suo interno il seguente testo:

SLEEP AND DANCE WITH THE DEATH...ELI IS HERE!

Oooops...I deleted your file!
Be happy and don't cry!
ELI (C) METAL MANIA

Enola.1864

Virus residente in memoria, infetta i files con estensione .COM e .EXE, I files infetti aumentano di 1864 bytes. All'interno il codice virale contiene il seguente testo:

Enola Gay
is now flying
to SoftPanorama !

command

Epbr

Virus residente in memoria, infetta il boot sector dei floppy disk e il master boot record del disco fisso. Quando il virus e' residente, la memoria libera diminuisce di 1 Kb. Il codice virale occupa 1 settore.

Estonia

Virus ad azione diretta, crittografato, infetta i files con estesione .COM. I files infetti aumentano di 400 bytes. All'interno il codice virale contiene il seguente testo:

Your drives were on the Estonia
They DIDN'T survive!!!

Exe252.252

Virus ad azione diretta, che infetta i files con estensione .EXE, se nell'header del files esiste uno spazio vuoto di almeno 252 bytes.Il codice virale non contiene stringhe.

Excel Macro Virus

Laroux

Laroux

Questo codice virale infetta i documenti di Excel, inserendovi un modulo VBA denominato Laroux. Ogni file di Excel aperto verra' infettato dal virus. Esistono molte varianti del virus Laroux, alcune funzionano solamente con Excel 5 o 7, altre con Excel 97. In Excel 5, il virus Laroux contiene le seguenti macro: Auto_Open, Check_Files, PERSONAL.XLS!auto_open e PERSONAL.XLS!check_files. Per Excel 97 esistono le seguenti varianti (che sono diffuse in Italia): PLDT e RESULTS. Il virus Laroux, quando infetta Excel, crea un file nella cartella XLSTART con il nome del modulo infettante (es. PLDT.XLS, RESULT.XLS, LAROUX.XLS). Quando si esegue Excel infetto, il foglio elettronico Microsoft non visualizza piu' il file Cartel1.XLS vuoto, ma solo il programma Excel senza il foglio vuoto. Per correggere questo incoveniente, si deve cancellare il file infettante che si trova nella cartella XLSTART.

Explosion.1000

Virus residente in memoria, infetta i files con estensione .COM e .EXE.
I files infetti aumentano di 1000 bytes.

F

Faerie.276

Virus ad azione diretta, infetta i files con estensione .COM allungandoli di 276 bytes.
All'interno il codice virale contiene il seguente testo:

Faerie

COMMANND

Fallen_Angel.335

Virus ad azione diretta, infetta i files con estensione .COM, la lunghezza del file infetto può aumentare da 335 a 351 bytes. All'interno il codice contiene il seguente testo:

**.COM*
COMMAND.COM

*FALLEN_ANGEL_*

Fax_Free Family

Fax_Free.1536.Pinniz.E

Virus residente in memoria crittografato, infetta files con estensione .EXE. Il virus all'interno contiene il seguente testo:

*Noi Otto **Pinniz** Campagna contro la Pirateria Partecipate tutti!!!*
Vettore PISello 12-2-91

VDSOFT91

Fax_Free.Joni.1536.D

Virus residente in memoria crittografato, infetta files con estensione .EXE. Il virus all'interno contiene il seguente testo:

E. ZIMUEL

Ti sentivi sicuro. Avevi lo SCAN !!! Invece lo hai preso nel culo.
Infatti il virus MECOJONI ti ha formattato l'Hard disk.
MECOJONI un virus self-modifying!
Sono state messe in circolazione 3000 varianti differenti di questo virus !!!!!
Turbo Assembler by E. Zimuel 1992

Fax_Free.Joni.1536.E

Virus residente in memoria crittografato, infetta files con estensione .EXE. Il virus all'interno contiene il seguente testo:

E. ZIMUEL

Turbo Assembler by E. Zimuel 1992

Fax_Free.Joni.1536.F

Virus residente in memoria crittografato, infetta files con estensione .EXE. Il virus all'interno contiene il seguente testo:

Ti sentivi sicuro. Avevi lo SCAN !!! Invece lo hai preso nel culo.
Infatti il virus MECOJONI ti ha formattato l'Hard disk.
MECOJONI un virus self-modifying!
Ricordati che la tua presunzione di conoscere i virus è una follia. Arrivederci.
Microsoft BASIC 7.1 (C) 1990-91

Fax_Free.Joni.1536.G

Virus residente in memoria crittografato, infetta files con estensione .EXE.
Il virus all'interno contiene il seguente testo:

Ti sentivi sicuro. Avevi lo SCAN !!! Invece lo hai preso nel culo.
Infatti il virus MECOJONI ti ha formattato l'Hard disk.
MECOJONI un virus self-modifying!
Ricordati che la tua presunzione di conoscere i virus è una follia. Arrivederci.
Microsoft BASIC 7.1 (C) 1990-91

Fax_Free.Joni.1536.H
Virus residente in memoria crittografato, infetta files con estensione .EXE.
Il virus all'interno contiene il seguente testo:

Ti sentivi sicuro. Avevi lo SCAN !!! Invece lo hai preso nel culo.
Infatti il virus MECOJONI ti ha formattato l'Hard disk.
MECOJONI un virus self-modifying!
Sono state messe in circolazione 3000 varianti differenti di questo virus !!!!!
Microsoft BASIC 7.1 (C) 1990-91

Fax_Free.Topo
Il virus Fax Free è stato isolato a Padova nel Luglio 1991, ed è di origine italiana. Questo virus è residente in memoria, utilizza meccanismo di autocrittografazione variabile ed infetta i files .EXE. Quando un programma infetto dal Fax Free viene eseguito, il virus si installa nella parte alta della memoria dei 640K, allocando 192 paragrafi, cioè 3,1 Kbytes. Il virus riesegue il programma infetto, facendo partire il programma portatore. A questo punto vengono modificati i vettori dell'interrupt 21H facendolo puntare al blocco allocato e termina l'esecuzione rimanendo residente. Dopo che Fax Free è residente, ogni programma .EXE eseguito, viene infettato dal virus, la lunghezza del file infetto aumenta da 1536 a 1552 bytes. Il virus è localizzabile alla fine del file, ma non è facile identificarlo perchè utilizza un metodo di autocrittografazione. Alla fine del file si possono notare le seguenti stringhe:

COMSPEC=C:\DOS\COMMAND.COM
PATH=C:\DOS;C:\WIN3;C:\;C:\TOPO;C:\UTILITY
PROMPT=pg TEMP=C:\WIN3\TEMP

La data e l'ora del file non vengono alterate dal virus. Il virus Fax Free modifica anche i vettori dell'interrupt 24H che gestisce gli errori critici. Il virus nei giorni 25 e 26 di ogni mese, simula un'errore sul file che si vuole far eseguire, visualizzando questa scritta:

General failure reading drive □
Abort?

oppure

General failure reading device
Abort?

Il virus all'interno contiene la seguente stringa:

FaX Free!! P 0.9 Welcome

che non è visibile essendo il virus crittografato, questo messaggio non viene mai visualizzato a video. Fax Free è ostile ai programmi debuggers, contiene una trappola per prevenire la decrittografazione, quando il virus si è accorto che si stanno usando i breakpoints esegue il reboot del sistema.

Flagyll Family

Flagyll.318

Virus primitivo, che sovrascrive il file, residente in memoria, infetta ogni file con estenzione .EXE che viene eseguito sovrascrivendo i primi 318 bytes. Il codice virale contiene il seguente testo:

-=[Crypt Newsletter 13]=-

Flagyll

Flagyll.371

Virus primitivo, che sovrascrive il file, residente in memoria, infetta ogni file con estenzione .EXE che viene eseguito, quando i secondi del calcolatore sono inferiori a 10 sovrascrivendo i primi 371 bytes. Il codice virale contiene il seguente testo:

-=[Crypt Newsletter 13]=-

Flagyll-Z

Form

Il virus Form è stato isolato per la prima volta nell'anno 1990, il codice virale è di origine Svizzera ma ha una diffusione mondiale ed è particolarmente attivo in Italia. Il codice virale risulta essere residente in memoria (TSR), infetta il boot sector dei floppy disk e quello della partizone attiva del disco fisso. Quando il Form si attiva dal boot dei floppy disk, si alloca in memoria, la memoria libera del sistema diminuisce di due kilobytes. Viene caricata in memoria la seconda parte del codice virale, e infettato il disco fisso. Il codice virale Form, copia alla fine del disco fisso la seconda parte del codice virale e il boot sector originale della partizione attiva. A questo punto viene intercettato l'interrupt 13H (Disk/Diskette Services) e il 18 di ogni mese anche l'interrupt 09H (Keyboard). Ogni floppy disk non protetto in scrittura verrà infettato dal codice virale. Il virus Form modifica la FAT (File Allocation Table) del floppy, in modo da alterare due settori marcandoli come BAD CLUSTER. In questi due settori verrano registrati la seconda parte del codice virale e il boot sector originale del floppy.
La posizione dei settori marcati BAD è variabile da floppy a floppy, dipende dalla quantità di dati registrata al suo interno. Il codice virale Form si attiva il 18 di ogni mese, intercettando l'interrupt 09H per la gestione della tastiera, l'intento dell'autore era quello di emettere un 'click' dallo speaker del calcolatore ogni qual volta si premeva un tasto. Questo effetto sembra non funzionare correttamente in alcune configurazioni di sistema. Il virus Form contiene inoltre il seguente testo:

The FORM-Virus sends greetings to every one who's reading this text.
Form doesn't destroy data! Don't panic!
Fuckings go to Corinne

Froll

Virus ad azione diretta, crittografato, infetta files con estensione .COM. Il virus si attiva dal 1996, quando il giorno della settimana (domenica=0, lunedì=1...) pi— il numero del giorno è uguale a 24, si ha video un effetto grafico e il bloccaggio del calcolatore, una data del 1996 dove si attiva il codice virale è il 24-03-1996. All'interno del codice sono presenti le seguenti stringhe:

Non sono cattivo, pero' ho piantato bene le mie radici, ora dovrai fare fatica per eliminarmi lasciando intatti tutti i FILES

Ma se sei riuscito a leggere almeno uno di questi messaggi significa che sei abbastanza in gamba

Il mio codice e':121 versione 2, sapresti dire quale e' il mio vero nome?

Se mi chiami FROLL non hai un briciolo di fantasia

Fumble.867

Virus ad azione diretta, residente in memoria, infetta files con estensione COM allungandoli di 867 bytes. Il virus infetta i files nei giorni pari.

G

Garibaldi.1845
Gdynia
Genesis Family
Gergana.182
Gippo.Stunning_Blow
Giprov
Goldbug
Golgi.385
Grog Family
Grunt Family
Gullich

Garibaldi.1845

Virus residente in memoria, stelth, infetta .COM, lunghezza 1845 bytes. Il virus si attiva il 12 settembre riscrivendo un numero casuale di settori. Al suo interno sono presenti le seguenti stringhe:

Garibaldi 1.0 - Developed in IVR Laboratories 1992 (c) by C.J.

!! W GARIBALDI !!

Gdynia

Virus di origine polacca, molto probabilmente è stato scritto nella città di Gdynia che si affaccia sul Mar Baltico. Il codice virale è arrivato in Italia attraverso un messaggio di posta elettronica della rete packet radio-amatoriale agganciato ad un file uuencodato che contiene il programma TXT2COM.COM. Il file in questione è stato infettato dal virus Gdynia e dopo compressato con il programma PKLite. Il codice virale è ad azione diretta, infetta i files con estensione .COM. I files infetti aumentano di 680 bytes. Il virus infetta i files a partire dal mese di Febbraio in poi. Ogni programma infetto, se eseguito, visualizza a video il seguente messaggio:

Windows 95 may be dangerous.
OS/2 is the best operating system!
I'll prove it soon...

Queste stringhe non sono visibili perchè risultano essere crittografate. All'interno il codice virale contiene inoltre la seguente stringa:

*Gdynia 1996 *v1.0**

Genesis Family

Genesis.217

Virus ad azione diretta, infetts i files con estensione .COM. I files infetti aumentano di 217 bytes. All'interno il codice virale contiene il seguente testo:

[Genesis 1.0]Thor.COM*

Genesis.226

Virus ad azione diretta, infetts i files con estensione .COM. I files infetti aumentano di 226 bytes. All'interno il codice virale contiene il seguente testo:

[Genesis 2.0]Thor.COM*

Gergana.182

Virus ad azione diretta, infetta i files con estensione .COM. I files infetti aumentano di 182 bytes. All'interno il codice virale contiene il seguente testo:

Gergana

Gippo.Stunning_Blow

Questo codice virale è stato individuato nel mese di Febbraio 1994 in Italia. Il virus risulta essere residente in memoria (TSR) ed infetta i files con estensione .EXE, nei files risulta essere crittografato. Ogni files eseguito verrà contagiato se il nome non inizia con:

- TB -----> probabilmente TBSCAN;
- F- -----> probabilmente F-PROT;
- CP -----> probabilmente CPAV (Central Point Anti Virus);
- NA -----> probabilmente NAV (Norton Anti Virus);
- SC -----> probabilmente SCAN (McAfee);
- CL -----> probabilmente CLEAN (McAfee);
- V -----> probabilmente VSHIELD (McAfee);

Ogni file colpito aumenterà di 1234 bytes più un numero variabile tra 0 e 15, dovuto all'allineamento di paragrafo. Stunning_Blow cerca tutti i files con estensione *.CPS (file di CHKLST.CPS generati da Central Point Anti Virus), se questi sono presenti verranno cancellati. L'ora dei files colpiti viene settata con il valore 1 nel campo dei secondi, valore utilizzato dal codice virale per riconoscere se il file è già infetto, mentre la data non viene alterata. Nei seguenti giorni: 4, 8, 12, 16, 20, 24, 28 di tutti i mesi dell'anno escluso dicembre, il codice virale entra in funzione dopo 1 ora dalla sua
installazione in memoria opera uno scrolling in Y dello schermo con sottofondo musicale. All'interno del codice virale è presente la seguente stringa che viene visualizzata a video con modalita' casuale:

Stunning Blow (R) Ghost Player Italy

Giprov

Ad azione diretta, infetta .COM, lunghezza 504. Il virus contiene al suo interno il seguente testo:

*VE3.3 *.EXE -= G.I.Pro.V.=-*

Goldbug

Virus residente in memoria, polimorfico, stealth, gemellare, infetta il Master Boot Sector dei dischi fissi, i boot sector dei floppy disk da 5 1/4 e i files con estensione .EXE creando il file gemello con estensione vuota e attributo di sistema settato ON. Il virus si installa in memoria solo in HMA, se è presente tale memoria infetterà il computer. Accedendo con un floppy pulito l'unità C: non viene vista dal DOS, quindi
l'utilizzo del programma FDISK /MBR per l'eliminazione del codice virale porterebbe alla completa perdita del disco fisso. Il codice virale contiene il seguente testo:

CHKLIST????

1O7=0SLMTAU

Esiste un'altra variante che non contiene il testo "CHKLIST????".

Golgi.385

Virus residente in memoria, infetta i files con estensione .COM. I files infetti aumentano di 385 bytes. All'interno il codice virale contiene il seguente testo:

[Chromosome Glitch] v.3.0
Copyright (c) 1993 Memory Lapse

Grog Family

Grog.4_0
Grog.304
Grog.377
Grog.480
Grog.660
Grog.1089:GPE
Grog.Aver_Torto
Grog.Bog.233
Grog.Crackers.Inc
Grog.Dewy:MtE.0_90
Grog.Dream
Grog.E-Riluttanza
Grog.IlCuoco
Grog.Joe_Anthro
Grog.Lor
Grog.MiAmi:GPE
Grog.Nocciola
Grog.NTA
Grog.Outwit_C
Grog.Public
Grog.Razor
Grog.Wildcard

Grog.4_0

Residente in memoria, stealth, crittografato, infetta .COM e .EXE, lunghezza 2075 bytes. Il virus si attiva il giorno 17 di ogni mese

Grog.304

Virus ad azione diretta, infetta file .COM, in paticolare il file COMMAND.COM viene infettato sovrascrivendo lo stack del file come il virus Lehigh. Contiene il seguente testo:

DELIRIOUS (C) '93 by GROG - Italy

Grog.377

Virus ad azione diretta è molto pericoloso, infetta il settore che inizia con E9H o E8H sovrascrivendolo, lunghezza 377 bytes. Ad ogni infezione visualizza a video:

"Il nostro amore durera' per sempre", disse lui.
"Oh, si, si, si!, esclamo' lei.
"Intendo 'sempre' in senso relativo, pero'", disse lui.
Lei lo colpi' con una racchetta da sci.

Grog.480

Virus ad azione diretta, infetta .COM, lunghezza 480 bytes. All'interno contiene il seguente testo:

HopHopHop (c) '93 By GROG - Italy

Guida alla Corsa
Capitolo primo
Come correre al modo dei conigli
Hop Hop Hop Hop Hop Hop

Grog.660

Virus ad azione diretta, infetta file con estensione .COM sovrascrivendo gli ultimi 330 bytes del file. La lunghezza del virus è di 660 bytes, i files infetti aumentano di 330 bytes. Contiene il seguente testo:

Il Mostro e i Coniglietti
Storia di terrore e di ansia
Boo!, disse il Mostro

-=< Il Mostro (C) '93 by Grog - Italy >=-

Grog.1089.GPE

Virus ad azione diretta, crittografato, polimorfico, infetta files con estensione .COM. I files infetti aumentano di 1089 bytes. All'interno il codice virale contiene il seguente messaggio:

_/^_ Joe LEsquimese (C) '93 by GROG - Italy _/^_

Ã-[Grog]Ä´

L'inverno era gia' tornato un'altra volta ed era tempo per Joe l'Esquimese di ritirare le sue mucche polari.
Mentre usciva a cavallo dalla stalla, cominciavano a cadere i primi fiocchi di neve. Egli alzo' gli occhi al cielo grigio ardesia e rabbrividi'.
Ben presto fu una tormenta. Un vento ululante sbatteva la neve attraverso la prateria desolata.
Joe l'Esquimese si piego' in avanti sulla sella e sollecito' la sua cavalcatura a procedere fra i turbini di neve e l'urlo del vento.

Grog.Aver_Torto

Virus ad azione diretta, infetta .Com, lunghezza 589 bytes. Contiene il seguente testo:

Vi E' Mai Venuto In Mente Che Potreste Aver Torto ?

-=[Aver Torto (C) '93 by Grog - Italy]=-

Grog.Bog.233

Virus ad azione diretta, infetta .EXE formato Windows sovrascrivendo la parte iniziale del file, lunghezza 233 bytes. Contiene il seguente testo:

BOG (C) '93 by GROG - Italy

Grog.Crackers.Inc

Virus ad azione diretta, infetta .COM (non correttamente), lunghezza 774 bytes.
All'interno contiene il seguente testo:

G r o g 4 E v e r
Grog.Crackers.INC (c) 1993 by Grog

Grog.Dewy.MtE.0_90

Virus ad azione diretta, polimorfico, crittografato, infetta files con estensione .COM. Il motore che viene utilizzato dal virus per rendersi mutante è l'{MtE:MtE} del bulgaro Dark Avenger. All'interno il codice virale contiene il seguente testo:

-= DEWY (C) '93 by GROG - Italy =-

GROG4EVER

MtE 0.90

Grog.Dream

Virus ad azione diretta, infetta files con estensione .COM aumentandoli di 757 bytes. All'interno il codice virale contiene il seguente testo:

Grog 4 Ever

Grog.Crackers.The_Dream_Team (c) 1993 by GROG

Il codice visualizza al centro dello schermo la frase The Dream Team multicolore con la scritta Grog 4 Ever in movimento.

Grog.E-Riluttanza

Virus ad azione diretta, infetta .Com, lunghezza 689 bytes. Se il programma infetto inizia con due istruzioni NOP (90H), il virus visualizza a video il seguente testo:

Sebbene suo marito andasse spesso in viaggio per affari,
ella odiava star sola.
"Ho risolto il nostro problema", disse egli.
"Ti ho comprato un San Bernardo. Si chiama Estrema Riluttanza."
"Adesso, quando vado via sai che ti lascio con Estrema Riluttanza!"
Ella lo colpi' con un mestolo.

All'interno del codice e' visibile anche la seguente stringa:

E-RILUTTANZA (C) '92 by GROG - Italy

Grog.IlCuoco

Residente in memoria, infetta .EXE, lunghezza 1007 bytes. Il virus all'interno contiene le seguenti stringhe:

```
          IlCuoco
+---   | Il cuoco, vedendosi scoperto, impallidi'. |
        "Siete in arrosto", intimo' il poliziotto.
         "Ho un mandato di cottora!"
+-------
```

Il virus si attiva il giorno 31 di ogni mese, visualizzando all'esecuzione di ogni programma infetto la seguente stringa:

IlCuoco (C) '93 by GROG

Grog.Joe_Anthro

Virus ad azione diretta, infetta .Com, lunghezza 647 bytes. Contiene il seguente testo:

Joe Anthro (C) '93 by GROG - Italy

Joe Anthro era un'autorita' sulla cultura egiziana e babilonese. Il suo massimo risultato, tuttavia, era la sua famosa opera sulla suinicultura.

Grog.Lor

Residente in memoria, stealth, infetta .EXE e .COM, lunghezza 666 bytes. Il 26 novembre di ogni anno visualizza a video la seguente stringa:

LOR (C) '93 by GROG Italy

>>1/93<< GROG 4 EVER

Grog.MiAmi.GPE

Virus ad azione diretta, crittografato, polimorfico, infetta files con estensione .COM. I files infetti aumentano di 926 bytes. All'interno contiene il seguente testo:

Mi Ami (C) '93 by GROG - Italy

"Mi ami?" chiese lei.
"Ma certo", rispose lui.
"Mi ami davvero?" chiese lei.
"Ma certo", rispose lui.
"Mi ami davvero davvero?" chiese lei.
"No", rispose lui.
"Mi Ami?" chiese lei.
"Ma certo", rispose lui.
Lei non chiese piu' altro.

Grog.Nocciola

Virus ad azione diretta, infetta .Com, lunghezza 283 bytes. Contiene il seguente testo:

Nocciola Vildibranda Crapomena
NOCCIOLA (C) '93 by Grog - Italy

Grog.NTA

Virus ad azione diretta, infetta files con estensione .COM aumentandoli di 1016 bytes. All'interno il codice virale contiene il seguente testo:

BR

The Nokturnal Trading Alliance

NTA Grog 4 Ever

Grog.Crackers.NTA (c) 1993 by GROG

Il codice visualizza al centro dello schermo il marchio NTA multicolore con la scritta Grog 4 Ever in movimento.

Grog.Outwit_C

Virus ad azione diretta, crittografato, infetta .COM, lunghezza 518 bytes. Il virus si attiva nei seguenti giorni: 3, 7, 11, 15, 19, 23, 27, 31 di ogni mese, se a queste date corrisponde il giorno del Lunedi', scrivendo valori casuali nella pagina grafica 0A000H.
Il virus contiene le seguenti stringhe:

G.COM hehe-=> hihi-=>*

OUTWIT-C (C) '93 by GROG - Italy

Grog.Public

Virus ad azione diretta, infetta files con estensione .COM aumentandoli di 800 bytes. All'interno il codice virale contiene il seguente testo:

Grog 4 Ever

Grog.Crackers.Public_Enemy (c) 1993 by GROG

Il codice visualizza al centro dello schermo la frase Public Enemy multicolore con la scritta Grog 4 Ever in movimento.

Grog.Razor

Virus ad azione diretta, infetta files con estensione .COM aumentandoli di 801 bytes. All'interno il codice virale contiene il seguente testo:

Grog 4 Ever

Grog.Crackers.Razor (c) 1993 by GROG

Il codice visualizza al centro dello schermo la frase Razor multicolore con la scritta Grog 4 Ever in movimento.

Grog.Wildcard

Virus ad azione diretta, infetta files con estensione .COM aumentandoli di 798 bytes. All'interno il codice virale contiene il seguente testo:

[WE ARE BACK!] [o1/o3]

Grog 4 Ever

Grog.Crackers.Wildcard (c) 1993 by GROG

Il codice visualizza al centro dello schermo la frase Wild Card multicolore con la scritta Grog 4 Ever in movimento.

Grunt Family

Grunt.346

Virus ad azione diretta, infetta i files con estensione .COM se l'anno è inferiore al 1993. Il codice virale allunga i files di 346 bytes. All'interno il virus contiene il seguente testo:

[GRUNT-1] -=> Agent Orange '92 <=-

Grunt.427

Virus ad azione diretta, infetta i files con estensione .COM allungandoli di 427 bytes. All'interno il virus contiene il seguente testo:

[GRUNT-2] -=> Agent Orange '92 <=-

Rock of the Marne, Sir!

USER???? BBS

Gullich

Virus residente in memoria, stealth, infetta il boot sector dei floppy disk e del disco fisso. Il codice virale dal 1995 in poi visualizza a video il seguente messaggio:

Wolfgang Gullich

Ad ogni accesso al disco vienne emesso un suono dal cicalino. Il codice virale contiene il seguente testo:

In memory di Wolfgang Gullich Milan Italy 94

H

Happy99
HDKiller
HideNowt
HLLO Family
Howard.967

Happy99

Happy99 e' un cavallo di troia/worm, un programma in formato Win32. Quando il programma viene eseguito, visualizza alcuni fireworks ed esegue alcune operazioni in background. Happy99 crea 2 files SKA.EXE e SKA.DLL. Dopo di che altera WSOCK32.DLL e il file originale viene salvato come WSOCK32.SKA. La dimensione del cavallo di troia e' 10000 bytes.

Il file WSOCK32.DLL modificato, contiene delle routines che intercettano i messaggio della posta elettronica e dei newsgroup. Esso inviera' una copia del file SKA.EXE rinominato in HAPPY99.EXE ad ogni utente che gli e' stato inviato un messaggio di posta elettronica. Happy99 non invia il messaggio con il file in allegato HAPPY99.EXE due volte allo stesso utente, perche' mantiene aggiornato il file LISTE.SKA, contenente la lista degli indirizzi email e dei newsgroup ai quali questo file e' stato inviato. L'obiettivo di HAPPY99 e' quello di "viaggiare" (diffondersi) attraverso la posta elettronica. La prima apparizione di Happy99 e' datata Gennaio 99.

Happy99 e' conosciuto come Win32.Ska.a, Ska, Wsock32.ska e Ska.exe.

HDKiller

Virus residente in memoria, infetta boot sector dei floppy disk e master boot record (mbr) dell'hard disk. Quando viene eseguito il boot da un floppy infetto da HDKiller, il codice virale infetta il master boot record dell'hard disk e viene eseguito il boot da disco fisso. Il codice virale si è installato in memoria occupando 1 Kb, ed intercettando l'interrupt 13H e 1CH, successivamente ogni floppy disk verrà infettato.
Il codice virale non preserva il boot e master boot record precedenti, per questo motivo il clean non è realizzabile venendo a mancare i dati originali. Il virus scrive nella tavola delle partizioni il giorno che ha infettato il PC decrementato di uno. Il valore del giorno viene restituito dal sistema in formato BCD (Binary Decimal Code), quando viene decrementato dal virus, questo valore può perdere riferimento nel formato BCD, il quale utilizza solo le prime 10 cifre del binario puro ed assegnandole alle corrispondenti decimali.

Cifra decimale	b 3	b 2	b 1	b 0
0	0	0	0	0
1	0	0	0	1
2	0	0	1	0
3	0	0	1	1
4	0	1	0	0
5	0	1	0	1
6	0	1	1	0
7	0	1	1	1
8	1	0	0	0
9	1	0	0	1

Quando il codice virale parte da master boot record, esegue la comparazione del giorno (BCD) con quello decrementato, se sono uguali allora viene sovrascritto il disco fisso. All'interno del codice è presenta la seguente stringa:

HDKiller By Rasek.0UT Meilàn!

HideNowt

Virus residente in memoria, stealth, crittografato, infetta i files con estensione .COM e .EXE. Il virus HideNowt dopo che è attivo in memoria, ad ogni esecuzione del comando DIR del DOS infetterà un file (non ancora infetto) della corrente directory. La lunghezza del file colpito aumenterà da 1741 a 1757 bytes, l'allungamento del file non visibile quando il codice virale è residente in memoria, essendo l'HideNowt stealth (invisibile). Il virus risulta essere ostile ai programmi debuggers.

HLLO Family

HLLO.4032

Il codice virale è stato scritto con un linguaggio ad alto livello, sovrascrive i files con estensione .EXE sulla corrente directory. La lunghezza del codice virale è di 4032 bytes. Il virus non contiene testo.

HLLO.PU

Il codice virale è stato scritto con un linguaggio ad alto livello, sovrascrive i files con estensione .COM sulla corrente directory. La lunghezza del codice virale è di 12032 bytes. Contiene il seguente testo:

Infected with radioactive Pu !
Beware for radiation

Howard.967

Virus ad azione diretta, infetta i files con estensione .COM, aumentandoli di 967 bytes. Se un file infetto viene eseguito ad un'ora inferiore alle 12:00, il codice virale visualizza a video la seguente frase:

I'm not working until Howard Stern is done @ 11:00 am !

con bloccaggio del calcolatore. All'interno del codice sono presenti le seguenti frasi:

Bow down before the King
Smile ... [NuKE] loves you
I'm not working until Howard Stern is done @ 11:00 am !

(c) Ba Ba Stupid... Remember Studderin' John Robin, I love You!
Long Live [NuKE] Georgia needs Howard Stern

I

Icelandic.1618.A
ILOVEYOU
Intruder Family
Invisible_Man
Italian_Boy
Italy
IVP.Walky_Replico.462
I-WORM.BadTrans.B
I-WORM.Frethem.E
I-WORM.HiGuy
I-WORM.Opasoft
I-WORM.Tanatos
I-WORM.Yaha.E

Icelandic.1618.A

Virus residente in memoria, infetta files con estensione .EXE quando vengono eseguiti. I files infetti aumentano di 1618 bytes.

ILOVEYOU (VBS/LoveLetter)

Si tratta precisamente di un WORM (verme) dell'e-mail chiamato VBS/LoveLetter. Questo "verme" si trasmette attraverso i messaggi di posta elettronica annidandovi all'interno di un file chiamato LOVE-LETTER-FOR-YOU.TXT.vbs, è utile precisare che se il file non viene aperto (letto) non si corre alcun pericolo.
Queste tipologie di virus si diffondono rapidamente e in questo caso producono danni sui computer dove il file LOVE-LETTER-FOR-YOU.TXT.vbs viene eseguito. Il messaggio che accompagna il file invita subdolamente il destinatario ad eseguire "leggere" il file. E' bene precisare che le estensioni .VBS non sono visibili di default dai sistemi Windows e il file viene confuso come un normalissimo ed ignaro file .TXT.

L'effetto primario che produce il virus è quello che può inviare messaggi di posta elettronica a qualunque indirizzo e-mail contenuto nell'address book della macchina infetta.

Il messaggio di posta elettronica contenente il virus è il seguente:

From: Nome dell'utente infetto
To: Nome casuale contenuto nell'address-book
Subject: ILOVEYOU

kindly check the attached LOVELETTER coming from me.

Attachment: LOVE-LETTER-FOR-YOU.TXT.vbs

Un address books contiene generalmente gruppi di indirizzi, conseguentemente il risultato dell'esecuzione del verme VBS/LoveLetter che dovesse colpire una organizzazione è che il primo utente infetto invierà il messaggio di posta elettronica ILOVEYOU a ognuno degli indirizzi di posta elettronica presente nell'address book. Altri utenti apriranno il file e contribuiranno alla diffusione.

Unitamente a questo il virus "I love you" è in grado di creare dei nuovi script .VBS immagine di file con estensioni .JPG e MP3 e inoltre sovrascrivere gli script presente nel computer e file .HTML che dovessero contenere questo codice.

Il virus contiene il seguente testo:

barok -loveletter(vbe)
by: spyder / ispyder@mail.com / @GRAMMERSoft
Group / Manila,Philippines

VBS/LoveLetter è stato scritto con il linguaggio VBScript. Di default i programmi scritti in VBScript operano solamente sotto Windows 98 and Windows 2000.

Comunque Windows 95 and NT 4 sono anch'essi vulnerabili se hanno installato Microsoft Explorer ver. 5. Questo Worm virus sembra aver avuto la sua diffusione dalle Filippine. Le prime segnalazioni della diffusione di questo verme sono giunte giovedì 4 maggio 2000.

Very Funny

Very Funny e' una variante del VBS/LoveLetter, il quale invia un messaggio di posta elttronica con subject: JOKE.

Intruder Family

Virus ad azione diretta, infetta files con estensione .EXE. Il file infettato aumenta di numero di bytes che dipende dal tipo di virus. Sono conosciute le seguenti varianti: .1317, .1319, .1440, .1988. All'interno il codice contiene le seguenti stringhe:

/.EXE /*.**

Invisible_Man

Il codice virale Invisible_Man è stato isolato nel mese di marzo 1993 in Italia, probabilmente è stato sviluppato a Salerno. Il virus è una variante miglorata del Flip. Il codice virale è residente in memoria, polimorfico, crittografato, infetta il master boot record del disco fisso e i files con estensione .COM e .EXE. Quando il codice virale è attivo in memoria, ogni files che viene eseguito, aperto, rinominato o modificato negli attributi, viene infettato dall'Invisible_Man. I files colpiti risultano aumentati di 2926 bytes. All'interno il codice virale contiene il seguente testo:

The Invisible Man - Written in SALERNO (ITALY), October 1992.
Dedicated to Ester: I don't know either how or when
but I will hold you in my arms again

Quando viene eseguito un file infetto avente giorno e mese uguale a quello del calcolatore ma anno diverso, visualizza a video il seguente messaggio con sottofondo musicale:

I'm the invisble man.
I'm the invisble man.
Incredible how you can
See right through me.

I'm the invisble man.
I'm the invisble man.
It's criminal how I can
See right through me.

Il testo visualizzato non è altro che la prima e la terza strofa di The Invisible Man dei Queen. Il files colpito viene sovrascritto con il codice che visualizza il testo della canzone con il sottofondo musicale.

Italian_Boy

Residente in memoria, infetta .COM, lunghezza 578 bytes. Dal 3 al 30 aprile di ogni anno, visualizza a tutto schermo la bandiera italiana con al centro la seguente stringa:

ITALY IS THE BEST COUNTRY IN THE WORLD

All'interno del codice e' visibile anche un'altra stringa:

Fucks to Italian Virus Killers

Italy

Il virus Italy è stato isolato per la prima volta nell'ottobre 94 in Italia, ma la sua origine è sconosciuta. Il virus è noto anche con i nomi di Roma e PG.3.
Il codice virale risulta essere residente in memoria (TSR), infetta il boot sector dei floppy disk e quello della partizione attiva del disco fisso. Quando l'Italy si attiva dal boot dei floppy disk, si alloca in memoria, la memoria libera del sistema diminuisce di un kilobyte. A questo punto viene intercettato l'interrupt 13H (Disk/Diskette Services) all'indirizzo CS:00F1h. Il codice virale Italy infetta il boot sector del disco fisso solo in casi particolari. Il virus Italy genera un numero casuale ogni qualvolta si accede alla funzione Ah=02 (Read Sector) dell'interrupt 13H, se questo numero risulta essere minore di 36H allora il codice virale non infetterà il disco. Ogni disco infetto (disco fisso e floppy disk) contiene un contatore d'infezione. Da una macchina infetta, ogni floppy disk colpito dal virus Italy conterrà un numero progressivo ad indicare il numero d'ordine del floppy colpito in quella sessione di lavoro. Supponendo che un floppy infetto dal virus Italy abbia contatore d'infezione con valore X, se tale disco infetterà un calcolatore questo avra il valore di contatore X+1 che nel proseguo chiameremo Y. Da questo i floppy infettati in successione in una stessa sessione di lavoro avranno valore del contatore Y+1, Y+2, Y+3..... Y+n. Nelle successive sessioni di lavoro il valore del contatore inserito nei floppy infettati in successione ripartirà ancora da Y+1.
Il codice virale Italy non contiene stringhe visibili.

IVP.Walky_Replico.462

Virus ad azione diretta, crittografato, infetta i files con estensione .COM allungandoli di 462 bytes. All'interno contiene il seguente testo:

Walky Virus Replico E Edition
Italian Viral Labs [IVP]

BadTrans.B

Il worm BadTrans.B è una nuova variante della versione A. Il BadTrans arriva attraverso i messaggi della posta elettronica con allegato un file. Il worm sfruttando alcuni bug di Outlook Express vers. 5 e di Outlook, si esegue automaticamente selezionando solamente un messaggio infetto. Il file allegato possono avere i segunti nome:

docs, info, Me_nude,
Card, Humor, Sorry_about_yesterday
YOU_are_FAT!, stuff, news_doc
README, images, HAMSTER

I file allegati possono avere due estensione, la prima è del tipo: *.doc oppure *.zip oppure *.MP3. La seconda estensione può essere: *.scr or *.pif.
Quando viene eseguito il worm badTrans, questo crea due files KERNEL32.DLL e KDLL.DLL. Il Kernel32.DLL viene messo in esecuzione automatica, e il secondo è una backdoor che viene eseguita in automatica dal KERNEL32.DLL.

I-Worm.Frethem.E

E' un virus-worm che sta circolando via e-mail. Il virus arriva con un messaggio di posta elettronica con oggetto "Your Password!", contenente il seguente testo:

ATTENTION!

You can access very important information by this password
DO NOT SAVE password to disk use your mind

now press cancel

Il virus allega due file:
decrypt-password.exe contenente il worm
password.txt contenente il seguente testo: Your password is W8dqwq8q918213

Il virus si esegue automaticamente in Outlook Express 5, sfruttando le vulnerabiltà messe in luce da altri virus (Klez, Nimda). Si consiglia caldamente di aggiornare Internet Explorer alla vers. 6.

I-Worm.HiGuy

Si tratta di un altro virus italiano, scritto dallo stesso autore del virus Win32.Porkis. Questo worm si diffonde attraverso la posta elettronica inviando messaggi infetti allegando un file eseguibile. Il messaggio infetto puo' avevre i seguenti oggetti:

Incredible..
Incredibile..
Urgente! (vedi allegato)
Qualsiasi cosa fai,falla al meglio.

con i segeunti corpi:

see this interesting file.
okkio all'allegato ;-)
devi assolutamente vedere il file che ti ho allegato.
apri subito l'allegato,e' MOLTO interessante.

Il virus allega uno dei seguenti file infetti:

tettona.exe
euro.exe
tattoo.exe

Quando l'utente esegue il file infetto, il virus visualizza le seguenti dialog box di quiz (domande e risposte):

Error
VBRUN49.DLL not found!

Il virus contiene anche un backdooe nella porta 5001.
Il 12 gennaio visualizza il seguente messaggio

Ciao,
il tuo computer è infettato dal virus Fralì.
Certo che devi essere proprio un pirlone,
per esserti fatto fregare dal mio stupidissimo worm.
Va bè,và,non ti preoccupare,oggi non sono in vena di cattiverie,
ed è anche un giorno festivo per me.

Buona giornata..
by 4nt4R35

I-Worm.Opasoft

Il worm Opasoft arriva quando l'utente si collega in Internet ed è in grado di replicarsi attraverso la rete locale LAN. Il worm si installa nella macchina creando il file ScrSvr.EXE e modificando il file WIN.INI e il file di registro. Per infettare le macchine della rete, il worm si attiva inserendovi nella riga di RUN del file WIN.INI. Il worm è in grado di autoaggiornarsi attraverso internet collegandosi al sito www.opasoft.com.

I-Worm.Tanatos

Il worm Tanatos arriva con la posta elettronica e si esegue automaticamente come il virus Klez, nelle versioni precedenti alla 6 di Outlook Express. Il worm puo' arrivare con un file allegato con nome casuale (es. lettera.doc.pif, nome.xls.scr). Il corpo del messaggio e' casuale, invece l'oggetto del messaggio e' prelevato dal seguente insieme:

Greets!
Get 8 FREE issues - no risk!
Hi!
Your News Alert
$150 FREE Bonus!
Re:
Your Gift
New bonus in your cash account
Tools For Your Online Business
Daily Email Reminder
News
free shipping!
its easy
Warning!
SCAM alert!!!
Sponsors needed
new reading
CALL FOR INFORMATION!
25 merchants and rising
Cows
My eBay ads
empty account
Market Update Report
click on this!
fantastic
wow!
bad news
Lost & Found
New Contests
Today Only
Get a FREE gift!
Membership Confirmation
Report
Please Help...
Stats
I need help about script!!!
Interesting...
Introduction
various

Announcement
history screen
Correction of errors
Just a reminder
Payment notices
hmm..
update
Hello!

Il worm si attiva nella macchina crando un file dal nome casuale nella directory di Windows, e rilasciando una DLL virale, anche questa dal nome casuale. Il worm si attiva ad ogni avvio del pc modificando il file di registro di Windows ed inserendo un file infetto nella cartella dei programmi in esecuzione automatica. Il Worm e' in grado di infettare la rete locale LAN.

I-Worm.Yaha.E

Si tratta di un virus-worm di origine indiana. Questo worm si diffonde attraverso la posta elettronica inviando messaggi infetti allegando un file eseguibile con estensione .SCR oppure con una doppia estensione. Il file allegato è lungo circa 28 Kb. Il messaggio infetto può avere molteplici oggetti. Delle volte il virus compone l'oggetto con una o più parti:

Screensaver, Friendship, Love, relations, stuff, to ur friends, to ur lovers, for you to see, to check, to watch, to enjoy, to share, :-), !, !!

Il corpo del messaggio è composto da una o piu' delle seguenti frasi:

Check the attachment, See the attachement, Enjoy the attachement, More details attached,
Hi
Check the Attachement ..
See u

Hi
Check the Attachement ..
Attached one Gift for u..
wOW CHECK THIS

Delle volte il virus utilizza il seguente corpo:

This e-mail is never sent unsolicited. If you need to unsubscribe, follow the instructions at the bottom of the message.

Il virus allega una copia di se stesso, con un file avente estensione .SCR con uno dei seguenti nomi:

*screensaver, screensaver4u, screensaver4u, screensaverforu, freescreensaver, love, lovers, lovescr, loverscreensaver, loversgang, loveshore, love4u, lovers, enjoylove, sharelove, shareit, checkfriends, urfriend, friendscircle, friendship, friends, friendscr, friends, friends4u, friendship4u, friendshipbird, friendshipforu, friendsworld, werfriends, passion, bullshitscr, shakeit, shakescr, shakinglove, shakingfriendship, passionup, rishtha, greetings, lovegreetings, friendsgreetings, friendsearch, lovefinder, truefriends, truelovers, f*cker.*

Delle volte allega file con doppia estensione (es. doc.pif, jpg.exe).
Il virus ha la capacita' di infettare la rete locale, ri cercando le cartelle del sistema operativo (es. WINXP, WINNT, WINDOWS, etc.). Il codice virale, di solito, copia se stesso nella cartella del cestiono (Recycled), e si attiva quando l'utente apre un file eseguibile (.EXE)

J

Jerusalem Family
Jumper
Junkie.1027

Jerusalem Family

Jerusalem.998
Jerusalem.1244
Jerusalem.1588
Jerusalem.1808.Apocalypse
Jerusalem.1808.CT.Subzero
Jerusalem.1808.Frere
Jerusalem.1808.Phenomen
Jerusalem.1808.Standard, .3503, .A, .Critical, .Flag_EE, .Payday
Jerusalem.1808.sUMsDos.AR
Jerusalem.Barcelona
Jerusalem.Sunday
Jerusalem.Sunday_II
Jerusalem.sURIV_3

Jerusalem.998

Virus residente in memoria, infetta qualsiasi files che venga eseguito. I files infetti tipo COM aumentano di 998 bytes, invece files tipo EXE aumentano di 1088 bytes. Il file infetto viene marcato con la word 004Bh all'offset 12h. Il virus alloca in memoria 1280 bytes, ed intercetta l'interrupt 21h e 24h. All'interno del codice virale non sono visibile
stringhe.

Jerusalem.1244

Il virus "1244" è stato isolato a Padova nel mese di Settembre 1992, ma la prima segnalazione della sua comparsa risale al mese di Gennaio 1992, la sua provenienza è sconosciuta. Questo virus è residente in memoria ed infetta i files .EXE e .COM, ma non il COMMAND.COM. Quando un programma infetto dal "1244" viene eseguito, il virus si installa nella parte bassa della memoria dei 640K, allocando 90 paragrafi, cioè 1440 bytes. Una volta che il virus si è installato in memoria, ogni programma .EXE o .COM eseguito viene infettato. Il file infetto aumenta di dimensione per i .COM di 1244 bytes, mentre per i files .EXE va da 1244 a 1260 bytes. Il virus è localizzabile alla fine del file infetto se questo è eseguibile, invece per i files .COM lo si trova all'inizio. La data e l'ora del file non vengono alterate. Il virus "1244" intercetta l'interrupt 21h e 08h (timer).

Jerusalem.1588

Questo codice virale e' stato individuato nella prima settimana di novembre 1993, la sua provenienza e' sicuramente italiana. Il virus e' residente in memoria (TSR) ed infetta i file con estensione .EXE e .COM. Questo codice virale, dall'analisi del disassemblato, risulta essere una nuova variante reingegnerizzata dell'oramai vetusto Jerusalem.

Quando un programma infetto dal Jerusalem.1588 viene eseguito il virus si installa in memoria allocando 3424 bytes ed intercettando gli interrupts 21H (funzioni DOS), 08H (TIMER) e 24H (gestione degli errori critici). Ogni file infetto all'offset 12H sara' marcato con la WORD 3D76H, utilizzata dal codice virale per riconoscere i file gia' infetti. Se il file infetto ha estensione .COM la sua lunghezza aumentera' di 1588 bytes, mentre se l'estensione e' .EXE la sua lunghezza aumentera' da 1588 a 1604 bytes.

Il virus prima di procedere all'infezione del file ne controlla il nome. Non vengono infettati tutti i file che hanno come somma dei caratteri in codice ascii 030CH (780), 0373H (883), 0367H (871), 02D6H (726) e 01FBH (507). Si e' verificato che il file COMMAND.COM non viene infettato dal virus, infatti la somma dei codici ascii del nome e' proprio pari a 030CH (780). La data e l'ora dei file colpiti, non vengono alterate. Il virus si attiva tutti i giorni a partire dal 4 novembre fino alla fine del mese, dopo circa 25 minuti dalla sua installazione in memoria. L'attivazione del virus si esplica formattando tracce casuali partendo dall'HARD Disk 80H, e proseguendo con l'81H etc. etc. fino a formattare i drive "A" e "B". Dopo cio' vengono disattivati i LED della tastiera, relativi ai tasti Num Lock, Caps Lock e Scroll Lock. A questo punto viene visualizzata nell'undicesima riga del video la seguente stringa:

******* *Ora il tuo PC e' DISTRUTTO!!!* *******

Jerusalem.1808.Apocalypse

Molto simile al Jerusalem.1808.Standard, contiene il seguente testo:

C.J
Apocalypse!!!

Jerusalem.1808.CT.Subzero

Molto simile al Jerusalem.1808.Standard, ma il 6 giugno formatta il disco fisso.
All'interno il codice contiene il seguente testo:

LORD SKISM
Sub-Zero NYHC

Jerusalem.1808.Frere

Virus residente in memoria, infetta file con estensione .COM e .EXE. La lunghezza del codice è di 1808 bytes, ed i files aumentano di una qunatità da 1808 a 1823 bytes. Casualmente il codice suona un motivo musicale, all'interno contiene le seguenti stringhe:

NOSCROLL

Jerusalem.1808.Phenomen

Molto simile al Jerusalem.1808.Standard, contiene il seguente testo:

--*-*

PHENOME.COM

--*-*

Jerusalem.1808.Standard, .3503, .Critical, .Flag_EE, .Payday

Virus residente in memoria, infetta file con estensione .COM e .EXE. La lunghezza del codice è di 1808 bytes, ed i files aumentano di una qunatità da 1808 a 1823 bytes. Ogni Venerd 13 il virus cancella il file che si vuole eseguire. Dopo 30 minuti dalla sua installazione in memoria si ha un rallentamento del sistema. All'interno contiene le seguenti stringhe:

sUMsDos

Esistono altre varianti del Jerusalem.1808.Standard, dove è stata solo modificata la stringa sUMsDos, queste varianti vengono sempre riconosciute da VirIT come 1808.Standard. Questa stringa è stata modificata ad esempio in: UMsDos.

Jerusalem.1808.sUMsDos.AR

Molto simile al Jerusalem.1808.Standard, ma ogni Lunedì il virus sovrascrive i primi 8 settori dell'hard disk, con la perdita del master boot record.

Jerusalem.Barcelona

Virus residente in memoria, infetta i files con estensione .COM allungandoli di 1792 bytes. All'interno il codice virale contiene il seguente testo:

CATALUNYA

CATALUNYA LLIURE
FORA LES FORCES D'OCUPACIO
MORT ALS TERRORISTES TRICORNUTS

Jerusalem.Sunday

Il virus si attiva ogni domenica visualizzando a video il seguente messaggio:

Today is SunDay! Why do you work so hard?
All work and no play make you a dull boy!
Come on! Let's go out and have some fun!

Jerusalem.Sunday_II

Virus residente in memoria, infetta filestipo .COM e .EXE. La lunghezza del codice virale è di 1728 bytes. I files infetti aumentano da 1728 a 1744 bytes. All'interno il codice virale contiene il seguente testo:

Today is SunDay! Why do you work so hard?
All work and no play make you a dull boy!
Come on! Let's go out and have some fun!

P L A Y

Jerusalem.sURIV_3

Virus residente in memoria, infetta files con estensione .COM e .EXE. La lunghezza del virus è di 1808 bytes. All'interno il codice virale contiene il seguente testo:

sURIV 3.00

Jumper

Virus residente in memoria, infetta il boot sector dei floppy disk e il master boot record del disco fisso. Quando il virus è residente, la memoria libera del sistema diminuisce di 2 kilobytes. Ogni floppy disk inserito verrà infettato dal virus Jumper, il boot sector
originale è posto nell'area denominata ROOT. Il codice virale può visualizzare a video il carattere "î" codice ASCII 238=0EEH.
Il virus Jumper è conosciuto anche con i seguenti nomi: French Boot, EE, 2KB.

Junkie.1027

Il Virus Junkie.1027 è stato individuato in Italia nel mese di settembre 1994, ma il codice virale è di origine svedese. Il virus risulta essere residente in memoria (TSR), infetta il boot sector dei floppy disk e la tabella delle partizioni (Master Boot Record) e i files con estensione .COM. Quando il virus si attiva dal files con estensione COM il codice virale cerca di infettare il Master Boot Record dell'hard disk. Il codice virale crittato è localizzabile nel settore 4, testina 0 e cilindro 0, ed occupa 2 settori.
Se il virus si attiva da un floppy disk o dal Master Boot Record dell'hard disk, vengono settati gli interrupts 13H, 1CH, 21H e 24H. Dopo che il virus è residente, la memoria libera del sistema diminuisce di 3 kilobytes. Verranno infettati i seguenti floppy disk:

- 3 1/2" 2 sided 18 sector, media descriptor F0H
  Nel caso che il "media state" del disk drive sia pari a 97H il virus si pone nel settore 8, cilindro 79, testina 1.
  Altrimenti il virus si pone nel settore 17, cilindro 79, testina 1.

- 3 1/2" 2 sided 9 sector, media descriptor F9H
  In questo caso il codice virale si pone nel settore 8, cilindro 79, testina 1.

- 5 1/4" 2 sided 15 sector, media descriptor F9H
  In questa caso il codice virale si pone nel settore 8, cilindro 79, testina 1.

La routine di gestione dell'interrupt 21H controlla le seguenti funzioni:
AX = 4B00H Load and/or execute program
AH = 3DH open existing file
AH = 6CH extended open/create file
Quando vengono eseguite le chiamate sopra elencate, se l'estensione à del files e' .COM e la lunghezza del files è compresa tra 4.096 e 60.000 bytes, il files risulterà infettato dallo Junkie.1027 e la sua lunghezza risultera incrementata di 1027 bytes. Questo del codice virale è in grado di disattivare VSAFE e VWATCH della Central Point Anti-Virus. All'interno del codice virale sono presenti e visibili (quando il codice è attivo in memoria, quindi decrittografato) le seguenti stringhe:

Dr White - Sweden 1994
Junkie Virus - Written in Malmo...M01D

K

Kampana
Knight_Errant

Kampana

Questo codice virale è residente in memoria, stealth, infetta il boot sector dei floppy disk e il master boot record (MBR) dell'hard disk. Quando il codice virale è attivo, la dimensione della memoria libera del sistema diminuisce di 1 kb, dopo aver infettato il master boot record viene intercettato l'interrupt 13H a CS:029F.
Il Kampana.B salva il corpo del codice virale nel cilindro 0, testina 0 e settore 4.
Dopo 400 boot da dischi infetti, il Kampana sovrascrive parte del disco e visualizza a video il seguente messaggio:

Campana Anti-TELEFONICA (Barcelona)

Knight_Errant

Virus residente in memoria, crittografato, infetta i files con estensione .COM, allungandoli di 1273 bytes. Il codice virale non funziona correttamente, facendo impiantare la macchina. Contiene il seguente testo:

--- Knight Errant --- No (C) !
Attack th planet...
ThanKs to aLl virUs wriTers!
Arf Arf we gotcha !
I'm hungry, can I eat you floppy? Yes?!
Thanks!

KNIGHT

L

Laroux
Leprosy Family
Lilith
Lithium
Lordzero
Lost_Diskette

Leprosy Family

Leprosy.Bad_Brains.570

Virus primitivo, crittografato, che sovrascrive i files con estensione .COM sulla corrente directory. Il codice virale sovrascrive i primi 570 bytes del files. All'interno il codice virale contiene il seguente testo:

SKISM.*.COM*

Bad Brains

Leprosy.Seneca

Virus primitivo, che sovrascrive i files con estensione .EXE. All'interno sono contenute le seguenti stringhe:

HEY EVERYONE!!!

Its Seneca's B-day! Let's Party! You shouldn't use your computer so much, its bad for you and your computer.

Lilith

Virus residente in memoria, infetta il Master Boot Record del disco fisso e i boot sector dei floppy disk. Il codice virale contiene il seguente testo:

L I L I T H

Tu del creato prima donna
del sesso Maestra infernale
accogli le Nostre dannate Carni
nel Tuo satanico Ventre

Milan Italy 95

Lithium

Virus residenten in memoria, crittografato, polimorfico, infetta il boot sector dei floppy disk, il master boot record del disco fisso e files tipo COM e EXE. Il virus Lithium è di origine italiana, la sua prima presenza è stata segnalata in provincia di Padova. Il codice virale contiene il seguente testo:

Lithi

Lithium

Nuotando nel miele
Accecati dalla luce
Oppressi dalla liberta'
Nauseati dai falsi e facili sorrisi
Lottiamo per trovare qualcosa in cui credere
le note della rabbia e dell'instabilita'
sono il detonatore della voglia di proseguire...
...'CAUSE WE'RE ALIVE!
You'llKnowWhatNITROMeans!
by ATP

GENOCIDEYouthEnergy

Lordzero

Virus residente in memoria, infetta i files con estensione .COM quando vengono eseguiti. I files infetti aumentano di 372 bytes. Al suo interno è presente il seguente testo:

Swedish Warrior v1.0 by Lord Zer0

Lost_Diskette

Questo virus infetta i files .COM ed e' ad azione diretta. Quando un programma infetto dal Lost Diskette viene eseguito il virus cerca nella corrente directory un file .COM non infetto di lunghezza superiore a 2835 bytes (cioe' che non inizi con due istruzioni NOP), e quindi lo attacca incrementando un contatore di infezione. Giunto alla dodicesima infezione il virus formatta un numero di settori corrispondenti alla lettera del corrente drive (es. drive A --> 65 settori formattati (tenta)) della traccia zero e della testina zero, dopo cio' viene visualizzata a video la seguente stringa:

I'm sorry, you have lost your diskette

Questa stringa non e' visibile all'interno del file perche' crittografata. I files infetti aumentano di una lunghezza pari a 2875 bytes, data e ora non vengono alterate.

M

Maaike
Major.1644
Maltese_Amoeba
Marauder.860
Mary
Marzia Family
Milan Family
mIRC_Worm.JeepWarz
Moloch
Mombasa
Mr_Virus
MtE Family
MTZ Family
Murphy Family
Mururoa

Maaike

Questo codice virale è stato individuato nella seconda settimana di maggio 1994, la sua provenienza non è conosciuta. Il virus è residente in memoria, polimorfico, stealth, infetta .EXE creando un file con lo stesso nome, ma con estensione .COM e con attributo nascosto (H=hidden). La lunghezza del file .COM (contenente il VIRUS) è di 250 bytes. Quando si esegue un programma con estensione .EXE, se nella directory è
presente un file con identico nome ma con estensione .COM, il DOS manda in esecuzione quest'ultimo. In questo modo viene eseguito il Virus Maaike, il quale si installerà in memoria allocando 507 bytes ed intercettando l'interrupt 21H del Dos. Dopo l'allocazione in memoria, ogni file eseguito, anche con estensione .COM, sarà modificato nell'estensione, che verrà tramutata in .EXE, e successivamente eseguito.
Questa tecnica, oltre a permettere l'esecuzione del vero e proprio programma, consente di implementare una particolare tecnica stealth. Infatti cercando di debuggare un file virato con il programma DEBUG, ad esempio DEBUG PIPPO.COM,
il Virus modifica l'estensione del file in .EXE eseguendo il comando DEBUG PIPPO.EXE che visualizzerà il programma e non il codice virale. Dopo l'esecuzione del programma, il virus Maaike preleva un valore casuale dal system clock interrupt (irq 0/int 08), confronta la parte bassa di tale valore con 0EH, se si verifica l'uguaglianza, viene scritto nella pagina testo B800H il seguente testo lampeggiante:

Maaike I Love You !

in verde su sfondo rosso per un totale di 105 volte. Altrimenti il codice si crittografa e viene creato un file di 250 bytes con il nome del programma eseguito precedentemente, ma con estensione .COM e con attributo nascosto. Il Virus Maaike risulta essere anche polimorfico, polimorfismo ottenuto invertendo solamente l'ordine dei registri, il metodo di crittografazione rimane invariato.

Major.1644

Virus residente in memoria, crittografato, infetta files con estensione .EXE. Il codice virale e' lungo 1644 bytes. Il virus contiene le seguenti stringhe:

The Major BBS Virus created by Major tomTugger

Puppet, Image, Gnat, Minion, Cindy e F'nor

\BBSV6\BBSUSR.DAT
\BBSV6\BBSAUDIT.DAT

Maltese_Amoeba

Virus residente in memoria, crittografato, polimorfico, infetta files con estensione .COM e .EXE. I files aumentano di una lunghezza variabile circa 2500 bytes. All'interno del codice virale è presente il seguente messaggio:

AMOEBA virus by the Hackers Twins (C) 1991
This is nothing, wait for the release of AMOEBA-II
The universal infector, hidden to any eye but ours!
Dedicated to the University of Malta- the worst
educational system in the universe, and the
destroyer of 5X2 years of human life

Marauder.860

Virus ad azione diretta, crittografato, polimorfico, infetta files con estensione .COM.
Il file infetto aumenta di 860 bytes. All'interno il codice non contiene testo visibile.

Mary

Residente in memoria, infetta .COM, lunghezza 463 bytes. Quando viene eseguito un programma infetto compreso fra le 10:00 e 10:59, il codice visualizza a video a suon di beep il seguente testo:

Mary..... ti AMO!

<CHRIS of S.i.t.> inf

Marzia Family

Marzia.B

Residente in memoria, stealth, infetta la tabella delle partizioni, file EXE e .COM, lunghezza 2048 bytes. Il virus si attiva da Maggio a Dicembre nei giorni 30 e 31, riscrivendo i primi 7 settori di tutte le tracce della testina 0 dell'hard disk 80H con valori casuali.

Marzia.D.

Residente in memoria, stealth, infetta la tabella delle partizioni, file EXE e .COM, lunghezza 2048 bytes. Contiene il seguente testo crittografato:

PISello tenere fuori dalla portata dei bambini.

PaxTibiQuiLegis.FaxFree!! WW20V3

Marzia.M

Residente in memoria, stealth, infetta la tabella delle partizioni, file EXE e .COM, lunghezza 2048 bytes. Contiene il seguente testo crittografato:

WW PASIPHAE(c)932Knosso
CX=5757-BX=CX-AX=3031-INT21H

Marzia.O

Residente in memoria, stealth, infetta la tabella delle partizioni, file EXE e .COM, lunghezza 2048 bytes. Contiene il seguente testo:

GDA VIRUS

Milan Family

Milan.BadGuy

Virus primitivo, che sovrascrive i files con estensione .COM nella corrente directory. Il virus sovrascrive i primi 265 bytes del file. All'interno il codice virale contiene il seguente testo:

BadGuy Virus (c) by Cracker Jack 1991 (IVRL)
Italian Virus Research Laboratory (C) 1990, 1991
IVRL Head Quarter, Milan Italy

Milan.New_BadGuy

Virus primitivo, che sovrascrive i files con estensione .COM nella corrente directory. Il virus sovrascrive i primi 208 bytes del file. Ogni lunedì visualizza a video il seguente messaggio:

New BadGuy Virus - (c) by Cracker Jack 1991
IVRL Head Quarter Milan, Italy

mIRC_Worm.JeepWarz

E' un Worm, che si diffonde attraverso i programmi di IRC. Il worm JeepWarz, si basa sul file SCRIPT.INI, il quale contiene il codice per "viaggiare".
Il file SCRIPT.INI e' lungo 3160 bytes e contiene il seguente testo:

JeepWarz HI

Esiste un'altra variante che contiene il seguente testo:

Whacked HI

Moloch

Virus residente in memoria, stealth, polimorfico, crittografato, infetta il Master Boot Record del disco fisso e il boot sector dei floppy. Il polimorfismo utilizzato dal virus Moloch è similare a quello generato dal codice virale {Lilith:Lilith}. Il virus Moloch contiene al suo interno il seguente testo:

OH-MY GOD!
Moloch (tm) is here!
Moloch is a trademark of SquiBoyz

Mombasa

Virus residente in memoria, crittografato polimorfico, stealth, infetta i files con estensione .COM. Il codice del virus è lungo 3568 bytes. Il virus è estramamente veloce nel diffodersi. All'interno contiene il seguente testo:

I'M GONNA DIE...
ATTACK RADICAL!
MOMBASA VIRUS (MM 92')

Mr_Virus

Il virus Mr. Virus è stato isolato nel mese di Ottobre 1992, la sua provenienza non è conosciuta. Questo virus non è residente in memoria, ma ad azione diretta ed infetta i files .COM e il COMMAND.COM. Quando un programma infetto dal Mr. Virus è eseguito, viene infettato un file .COM nella corrente unità. La scelta del file da infettare è di tipo sequenziale, infatti il programma virulento individua il primo file non infetto partendo dalla radice e proseguendo in ordine di directory in directory. I programmi infetti aumentano di 508 bytes, il virus può essere localizzato alla fine del file. La data e l'ora del file non viene alterata. All'interno il virus contiene la seguente stringa:

Mr.Virus Ver. 1.10

MtE Family

CryPtLAB:MtE.0_90

Virus ad azione diretta, polimorfico, crittografato, infetta i files con estensione .COM. La lunghezza del codice virale è variabile. All'interno contiene il seguente testo:

CryPtLAB: THE SELECT CHOICE FOR ALL VIRUS AND TROJANRESEARCH NEEDS!

-URNST KOUCH

MtE 0.90

L'autore Urnst Kouch è anche responsabile della rivista elettronica underground Crypt News Letter

PC_Weevil:MtE.0_90

Molto simile al codice CryPtLAB, all'interno il virus contiene il seguente testo:

PC Weevil: Still the select choice for your virus research needs

MtE 0.90

MTZ Family

MTZ.Pink_Panther.4481
Residente in memoria, polimorfo, stealth, crittografato, infetta .EXE, lunghezza 4481 bytes. All'interno contiene il seguente testo

- The Pink Panther - (c) MTZ Sept. 1993 Italy

MTZ.Pink_Panther.4510
Residente in memoria, polimorfo, stealth, crittografato, infetta .EXE, lunghezza 4510 bytes. All'interno contiene il seguente testo:

- The Pink Panther - (c) MTZ Sept. 1993 Italy

MTZ.Pink_Panther.5081
Residente in memoria, polimorfo, stealth, crittografato, infetta .EXE, lunghezza 5081 bytes. All'interno contiene il seguente testo:

*- The Pink Panther 2 (*The Last One*) - (c) MTZ '1 Jan 1994' Italy*

Dedicated to Federica!

[MTZ 1994]

MTZ.Xandu.2385
Virus residente in memoria, crittografato, polimorfico, infetta files con estensione .EXE. All'interno contiene il seguente testo:

XANDU Virus ! (C) 1993 By MTZ - Italy !

<Hit any key to continue>

Murphy Family

Murphy.Swami

Virus residente in memoria, infetta files con estensione .COM e .EXE. All'interno il codice virale contiene il seguente testo:

Bhaktivedanta Swami Prabhupada (1896-1977)

Mururoa

Il virus è stato scoperto nel mese di Marzo 1996. Il codice virale Mururoa è residente in memoria, crittografato, stealth e infetta i files con estensione .COM e .EXE. Il codice virale è lungo 2464 bytes, al suo interno sono visibili le segueti stringhe:

I have one mesage to all people on earth:

Stop all French nuclear testing in the PACIFIC
Dont forgot :Comon peolple dont like nuc. tests!
This is is a MURUROA 1.386 by Blesk

PLUTONIUM IS BETTER IN POWER-PLANT !!!!!

My greet to VYVOJAR,SVL,METABOLIS and all IRC.

N

Napoli_Trojan.6032
NetBus_Trojan
New_Exebug
November_17th Family
No_of_the_Beast
Number_1.AIDS

Napoli_Trojan.6032

Napoli_Trojan.6032 è un cavallo di troia scritto da Dark Man autore del {TPTG:TPTG}. Questa è una versione modifcata del PKTROJAN. Al suo interno sono visibile le seguenti stringhe:

And now begin damage:
deltree /y c:.* /C*
Error in EXE code'Infection by Napoly_TROJAN (c) 1998 TNT
Hard disk state: EMPTY I've erased all your file !!
C:\NAPOLI.TRJ

NetBus_Trojan

NetBus e' un programma che permette di controllare in remoto il computer di un altro utente collegato alla rete. NetBus permette di amministrare il computer remoto se questo supporta il protocollo TCP/IP.
Esistono varie versioni di NetBus alcune freeware ed altre commerciali.

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 inserito (non protetto dalla 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.

November_17th Family

November_17th.706.B
Residente in memoria, infetta .EXE e .COM, lunghezza 706 bytes. Il virus si attiva l'8 luglio di ogni anno riscrivendo 8 settori partendo dalla traccia zero dell'unita' corrente. Il giorno 8 dei mesi diversi da quello di luglio, il codice virale si inluppa, bloccando il funzionamento della macchina Contiene il seguente testo:

Italian ICEvirus

November_17th.768
Residente in memoria, infetta .EXE e .COM, lunghezza 768 bytes. Il codice virale sovrascrive i primi 8 settori partendo dalla traccia zero dell'unità corrente, la data di attivazione dipende dalla variante:

November_17th.768.B: si attiva l'8 di luglio;
November_17th.768.C: si attiva dal 17 al 30 novembre:

Contiene il seguente testo: SCAN.CLEAN.COMEXE

November_17th.800.B
Residente in memoria, infetta .EXE e .COM, lunghezza 800 bytes. Il virus si attiva dal 17 al 30 novembre di ogni anno riscrivendo 8 settori partendo dalla traccia zero dell'unita' corrente. Contiene il seguente testo:

SCAN.CLEAN.COMEXE

No_of_the_Beast

Virus residente in memoria, stealth, non crittografato, infetta files con estensione .COM. Il codice virale utilizza una nuova tecnica per rendersi invisibile quando infetta il files. Il virus No_of_the_Beast copia il primo settore del file nella parte rimanente dell'ultimo cluster del file, a questo punto viene sovrascritto il primo settore con il codice del virus, che è solo di 512 bytes. All'interno del codice è presente la seguente stringa:

666

Il codice virale No_of_the_Beast dovrebbe essere opera di Dark Avenger.

Number_1.AIDS

Virus primitivo, che sovrascrive i files con estensione .COM. Il codice virale è stato scritto in Turbo Pascal ed è lungo circa 13K. All'interno contiene il seguente testo:

```
                              ATTENTION:
I have been elected to inform you that throughout your process of
collecting and executing files, you have accidentally  Hš›Kä
yourself over; again, that''s PHUCKED yourself over. No, it cannot
be; YES, it CAN be, a û□ç-s has infected your system. Now what do
you have to say about that? HAHAHAHA. Have  Hš¥ with this one and
                  remember, there is NO cure for

   ÛÛÛÛÛÛÛÛÛÛ     ÛÛÛÛÛÛÛÛÛÛÛÛ    ÛÛÛÛÛÛÛÛÛÛÛ      ÛÛÛÛÛÛÛÛÛÛ
  ÛÛÛ±±±±±±ÛÛÛ     ±±±±ÛÛ±±±±±±   ÛÛ±±±±±±±ÛÛÛ    ÛÛÛ±±±±±±±ÛÛ
  ÛÛ±±      ÛÛ±        ÛÛ±         ÛÛ±       ÛÛ±   ÛÛ±±       ±±
  ÛÛ±       ÛÛ±        ÛÛ±         ÛÛ±       ÛÛ±   ÛÛ±
  ÛÛÛÛÛÛÛÛÛÛÛÛÛ±        ÛÛ±         ÛÛ±       ÛÛ±   ÛÛÛÛÛÛÛÛÛÛÛÛ
  ÛÛ±±±±±±±±ÛÛ±        ÛÛ±         ÛÛ±       ÛÛ±    ±±±±±±±±ÛÛ±
  ÛÛ±       ÛÛ±        ÛÛ±         ÛÛ±       ÛÛ±             ÛÛ±
  ÛÛ±       ÛÛ±        ÛÛ±         ÛÛ±      ÛÛÛ±   ÛÛ       ÛÛÛ±
  ÛÛ±       ÛÛ±   ÛÛÛÛÛÛÛÛÛÛÛÛ    ÛÛÛÛÛÛÛÛÛÛÛ±±    ÛÛÛÛÛÛÛÛÛÛ±±
   ±±        ±±    ±±±±±±±±±±±    ±±±±±±±±±±      ±±±±±±±±±
```

O

Old_Yankee.Enigma
One_Half.3544
Ooops.368
Orion Family

Old_Yankee.Enigma

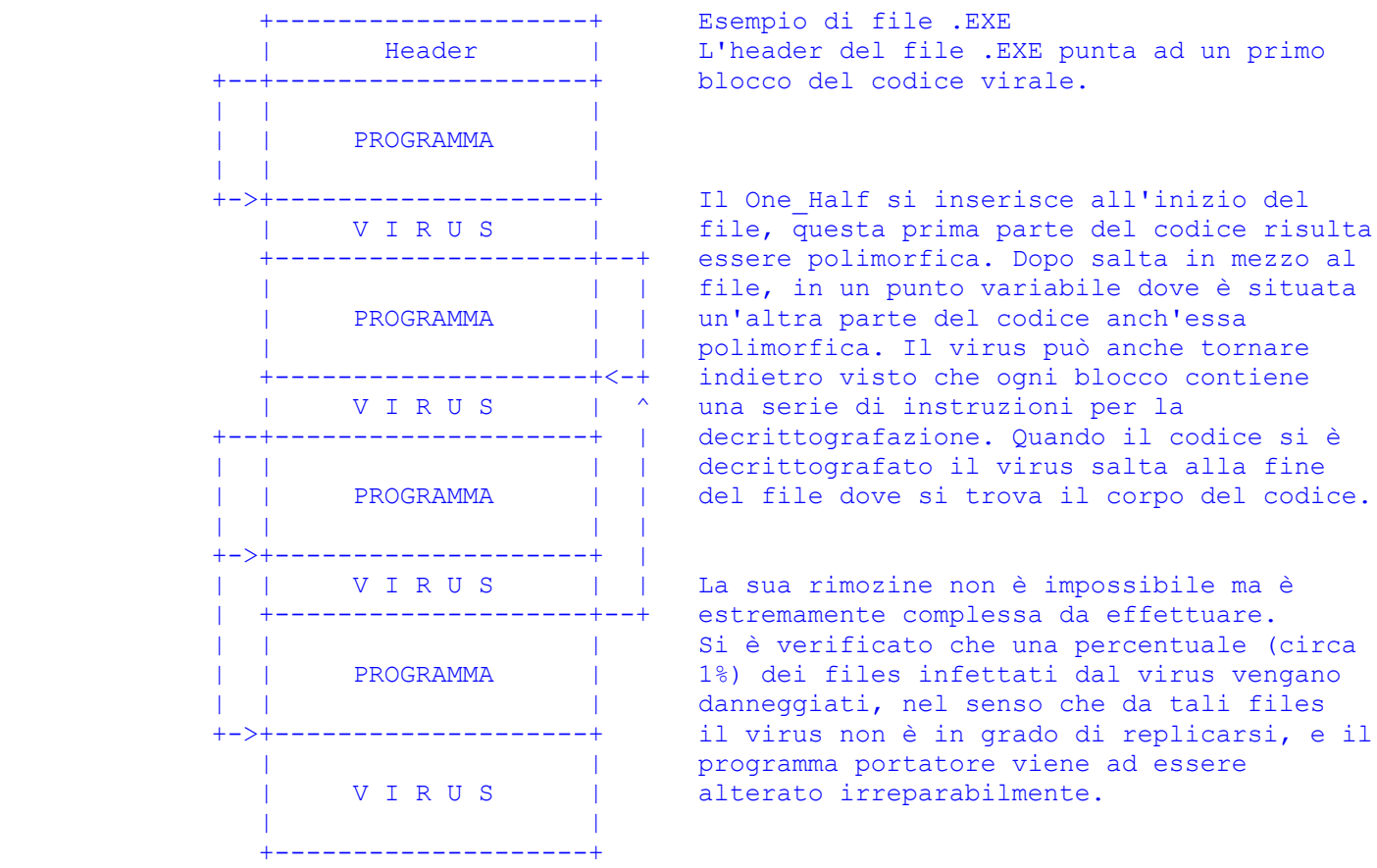
Virus ad azione diretta, infetta files con estensione .EXE aumentandoli di 1755 bytes. Contiene il seguente testo:

This is the voice of the Enigma virus.....the spirits of the hell are coming back!

*(C) 1991 by Cracker Jack * Italy **

One_Half.3544

Il virus residente in memoria, polimorfo, stealth, crittografato, infetta files con estensione .EXE e .COM e il master boot record (mbr). Ogni files che sarà eseguito, aperto, creato verrà infettato dal codice virale, la lunghezza del files aumenterà di 3544 bytes, l'aumento non è visibile quando il virus è attivo in memoria. Il virus One_Half è estremamente polimorfo, il quale si inserisce in più parti all'interno del file colpito come nel seguente modo:



All'interno del codice sono presenti le seguenti stringhe:

Dis is one half
Press any key to continue ...

COM EXE SCAN CLEAN FINDVIRU GUARD NOD VSAFE MSAV CHKDSK

Did you leave the room ?

Ooops.368

Codice primitivo, che sovrascrive i files con estensione .COM sulla corrente directory. La lunghezza del codice virale è di 368 bytes. Questo virus è pericoloso perchè casualmente sovrascrive il contenuto del disco visualizzando il seguente testo:

Ooops.. I've managed to erase your File Allocation Tables...
Good thing I made a copy of them... now where did I put those damn things?"

Orion Family

Orion.262
Virus residente in memoria, infetta i files .COM allungandoli di 262 bytes.

Orion.365
Virus residente in memoria, infetta i files .COM allungandoli di 365 bytes.

P

Parity_Boot
Peace_Keeper
Peach
Phalcon.Cloud.1117
Pieck.4444
Pixel Family
Pizelun
PKTROJAN
Polifemo Family
Prague.Backtime
Pretty_Park
Protipus
PS-MPC Family
Pulce.1840

Parity_Boot

Virus residente in memoria, stealth, infetta il boot sector dei floppy disk e il master boot record dell'hard disk. Quando il virus è attivo, la memoria libera del sistema diminuisce di 1 Kb. La lunghezza del codice virale è di 512 bytes (un settore). Casualmente visualizza a video il seguente messaggio:

PARITY CHECK

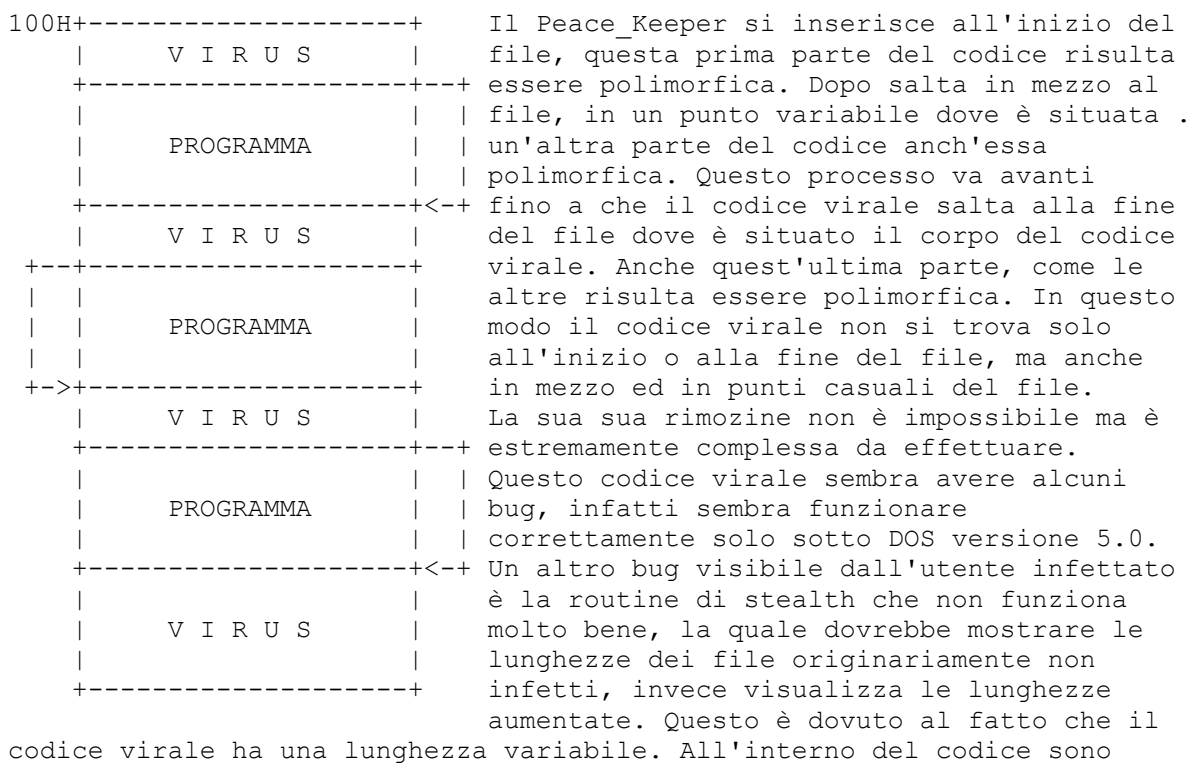
Il virus simula questo errore con il bloccaggio (crash) del calcolatore.

Peace_Keeper:MCG.0_31

Il virus è polimorfo, stealth, residente in memoria, crittografato, infetta files con estensione .EXE e .COM. All'interno è presente la seguente stringa:

[MCG v0.31]

Potrebbe essere la sigla del motore che il codice virale utilizza per diventare polimorfo, questa sigla attualmente è nuova al mondo dei ricercatori. Il polimorfismo dipende dal tipo di file infettato, se il file ha estensione .EXE la mutazione è semplice, invece il file è tipo .COM il codice virale è estremamente polimorfico. Nei file .COM infetti il Peace_Keeper risulta inserito nel file nel seguente modo:



Il Peace_Keeper si inserisce all'inizio del file, questa prima parte del codice risulta essere polimorfica. Dopo salta in mezzo al file, in un punto variabile dove è situata . un'altra parte del codice anch'essa polimorfica. Questo processo va avanti fino a che il codice virale salta alla fine del file dove è situato il corpo del codice virale. Anche quest'ultima parte, come le altre risulta essere polimorfica. In questo modo il codice virale non si trova solo all'inizio o alla fine del file, ma anche in mezzo ed in punti casuali del file. La sua sua rimozine non è impossibile ma è estremamente complessa da effettuare. Questo codice virale sembra avere alcuni bug, infatti sembra funzionare correttamente solo sotto DOS versione 5.0. Un altro bug visibile dall'utente infettato è la routine di stealth che non funziona molto bene, la quale dovrebbe mostrare le lunghezze dei file originariamente non infetti, invece visualizza le lunghezze aumentate. Questo è dovuto al fatto che il codice virale ha una lunghezza variabile. All'interno del codice sono presenti anche le seguenti stringhe:

Peace-Keeper Virus V2.10 Written by Doctor Revenge 18-May-1994 , Italy

EXECOMSCCLVIVSMSCPF-IMVHTH

Peach

Il virus è residente in memoria, infetta ogni file che viene eseguito con estensione .COM e .EXE. La lunghezza del codice virale è di 887 bytes, ma l'aumento del file può essere anche di una quntità maggiore. Il codice virale cancella i files della Central Point chklist.cps. All'interno del codice sono presenti le seguenti stringhe:

Roy CuatroNo 2
Peach GardenMayer Rd. Spore 1543

chklist.cps

Phalcon.Cloud.1117

Virus ad azione diretta, crittografato, infetta i files con estensione .COM allungandoli di 1117 bytes. All'interno il codice virale contiene il seguente testo:

Bob Ross lives!
Bob Ross is watching!
Maybe he lives here...
What a happy little cloud!&
Maybe he has a neighbour right here...
(You can make up stories as you go along.

Pieck.4444

Virus multipartito, residente in memoria, crittografato, polimorfico, stealth, infetta il master boot record e i file tipo EXE. Il codice virale e' polimorfico anche in memoria. contiene il seguente testo:

Zrobione
Wersja
Kodowanie
Licznik HD

k a c z o r t e s t

Pixel Family

Pixel.847

Virus ad azione diretta, infetta files com estensione .COM. Il file infetto aumenta di 847 bytes. All'interno il codice virale contiene il seguente testo:

*IV *.COM*

Le seguenti varianti differiscono dal messaggio che contengono:

Pixel.847.Advert

Buy AMSTRAD it is THE CHEAPEST COMPUTER that you can buy

Pixel.847.Hello

Hello, John Mcafee,please up rade me.Beast regards,Jean Luz

Pixel.847.Pixel:

Program sick error:Call doctor or buy PIXEL for cure description

Pixel.847.Near_End

THE END IS NEAR!! THE SIGNS OF THE BEAST ARE EVERYWHERE

Pixel.847.RV1:

En tu PC hay un virus RV1, y sta es su quinta generaci

Pixel.852

Virus ad azione diretta, infetta files .COM, aumentandoli di 852 bytes. All'interno contiene il seguente testo:

*SS *.COM*

Pixel.Hydra.403

Virus ad azione diretta, infetta i files con estensione .COM allungandoli di 403 bytes. All'interno il codice virale contiene il seguente testo:

YD HyDra-1 Beta - Not For Release.

Copyright (c) 1991 by C.A.V.E. HYDRA

Pixel.Hydra.736
Virus ad azione diretta, infetta i files con estensione .COM allungandoli di 736 bytes.
All'interno il codice virale contiene il seguente testo:

YD HyDra Beta - Not For Release.

Copyright (c) 1991 by C.A.V.E. HYDRA
Watch for the many heads.

The first eight are easy to find and kill.

Their replacements will be more sophisticated.

1991 - C. A. V. E.

Coalition of American Virus Engineers
Dedicated to supporting the anti-virus industry without recognition or reward.

Pixel.Self.550
Virus ad azione diretta, infetta i files con estensione .COM allungandoli di 550 bytes.

Pizelun

Virus residente in memoria, crittografato, stealth, infetta files con estensione .EXE e .COM. Il codice virale è lungo 3599 bytes, ma quando il virus è attivo, la lunghezza del file infetto rimane inalterata. Il Pizelun si attiva nel mese di Maggio 1995, visualizzando a video il seguente messaggio:

Pizelun attivato, attivatissimo!
Premere un tasto per continuare .

Se vengono premuti i tasti CTRL+ALT+DEL viene visualizzato una serie di righe in movimento. All'interno il codice virale contiene il seguente testo:

**.COM *.EXE*

PIZELUN

PKTROJAN

PKTROJAN è un cavallo di troia scritto da Dark Man autore del {TPTG:TPTG}. il quale ha messo in circolazione una versione fasulla di PKZIP 4.0 datata 19-02-97. Se il programma trojano viene eseguito senza opzioni, il PKTROJAN visualizza a video le schermate di info di PKZIP. Se invece viene eseguito con un opzione, PKTROJAN cancellerà i files del disco C: con il comando:

DELTREE /y c:.**

e viene visualizzato a video il seguente messaggio:

PKTROJAN 4.00v
A new trojan virus by DarkMan
Written in Italy
Copyright(c) 1997

What do you think about me...

PKTROJAN oltre a questo messaggio contiene il seguente testo:

DarkMan lives... Somewhere in time !!
Freddy Mercury lives...
Somewhere in time !!
VIRUS !!
I love this game
God save Duke Nukem
I am a corrupted file
Playing DOOM][
Long life to Jerusalem virus
According to PKWARE

Alla lunga lista non mancano i nomi delle seguenti ragazze:

Daniela
Sara
Roberta
Manuela
Serena
Sara

Esistono le seguenti varianti del PKTROJAN lunghe 33696, 41920 e 45680 bytes.

Polifemo Family

Polifemo.736

Virus ad azione diretta, infetta files con estensione nella corrente directory, o nelle seguenti: \dos, \windows, \qemm, \dv. Il codice virale altera data e ora del file e la lunghezza è aumentata di 736 bytes. Il codice virale contiene il seguente testo:

***** Polifemo *****

Il codice virale è scritto molto male, in alcuni casi può portare al bloccaggio del sistema.

Prague.Backtime

Virus residente in memoria, infetta files con estensione .COM quando vengono eseguiti. Il file .COM verrà infettato se la lunghezza è inferiore a 60000 bytes. La lunghezza del codice virale è di 528 bytes. All'interno del virus si può vedere la seguente stringa:

BackTime

Pretty_Park

Il codice virale Pretty_Park è un cavallo di troia/worm, un programma in formato Win32. Quando il programma viene eseguito, modifica il file di registro di Windows, in modo che ad ogni esecuzione di un programma, venga eseguito il file FILES32.VXD. La dimensione del cavallo di troia è 37376 bytes. Esso invierà una copia del file Pretty Park.exe ad ogni utente elencato nel Windows address book della posta elettronica.

Pretty Park

Protipus

Il virus Protipus è stato isolato nel mese di Novembre 1992, la sua provenienza è italiana. Questo virus è ad azione diretta ed usa una tecnica di diffusione di tipo gemellare, molto probabilmente è stato scritto in un linguaggio ad alto livello (es. Pascal). Quando un programma infetto dal Protipus viene eseguito (es. PLUTO.EXE) il virus rinomina il file da infettare sostituendo all'ultimo carattere del nome la lettera "V" e setta l'attributo del file come nascosto (es. PIPPO.EXE .... diventa PIPPV.EXE H...
dove H=hidden cioè nascosto). A questo punto il virus crea un file con lo stesso nome del file rinominato (cioè PIPPO.EXE) il quale contiene però solamente il codice virale, che avrà lunghezza 5472 bytes. Dopo ciò viene eseguito il file originario cioè quello nascosto (nel nostro caso PLUTV.EXE), che va in esecuzione. Il virus contiene al suo interno la seguente stringa, che viene visualizzata a video:

Sei stato contagiato dal Protipus Virex!!!!
Conficius said: 'Arrangietes'.

PS-MPC Family

PS-MPC.331

Virus ad azione diretta, infetta i files con estensione .COM allungandoli di 331 bytes. Contiene al suo interno il seguente testo:

[MPC]

PS-MPC.Abraxas

Virus ad azione diretta, infetta files con estensione .COM e .EXE. I files infetti aumentano di 546 bytes. All'interno il codice virale contiene il seguente testo:

[Z10] Abraxas

Pulce.1840

Virus residente in memoria, polimorfico, crittografato, stealth, infetta i files con estensione .COM e .EXE. I files infetti aumentano di 1840 bytes. Il codice virale si attiva ogni mercoledi dalle 13 in poi. All'interno il codice Pulce contiene il seguente testo:

**.EXE *.COM COMMAND SCAN CLEAN F-PROT*
KRLN286 KRLN386 QBASIC VPIC

Hey! C'e' una PULCE nella CPU!!!
PULCE! v2.1 24/4/94 by AL

Ingegneri d'Ancona succhiate il ..... e fatemi usare il PC!
Adesso e' ora di fare festa!

BERLUSCONI ....!

PULCE! Libera di andare dove vuole.

Q

Quox

Quox

Virus residente in memoria, stealth, infetta il boot sector dei floppy disk e il Master Boot Sector del disco fisso. Quando il virus è residente la memoria libera del sistema diminuisce di 1 kilobytes. Il virus può danneggiare l'accesso a floppy disk ad alta densità 1.44 Mb. Il boot sector originale dei floppy è salvato nell'ultimo settore, invece il Master Boot Sector dell'HD viene salvato in una posizione che dipende dalle dimensione del disco fisso. Il virus al suo interno non contiene nessuna stringa.

R

Rape.747

Virus residente in memoria, stealth, non crittografato, infetta i files con estensione .COM. I files infetti aumentano di 747 bytes, ma quando è attivo in memoria il codice virale l'allungamento non è visibile. Se un file viene infettato al 19-esimo centesimo di secondo, il codice cirale sovrascrive il disco con valori casuali e visualizza a video il seguente messaggio:

DataRape! v1.1
(c)1991 Zodiac
RABID, USA

RebelBase

Il virus RebelBase è stato isolato nel mese di Novembre 1994 in Italia e la sua origine è italiana. Questo virus è residente in memoria ed infetta i files con estensione .EXE.
Quando un programma infetto dal RebelBase viene eseguito, il virus controlla se è gia attivo in memoria eseguendo una chiamata all'int 21H con AX=DDEEH, se viene restituito il registro BX=9797H allora è gia attivo altrimenti si pone residente in memoria. Il virus alloca 95 paragrafi cioè 1520 bytes e intecetta l'interrupt 21H (funzioni DOS) facendolo puntare a CS:0422H. Ogni programma che viene eseguito (AH=4BH) o aperto (AH=3DH), viene rinominato cambiando l'ultimo bytes dell'estensione con il valore 0E2H, cioè da PIPPO.EXE in PIPPO.EX? dove il ? corrisponde al valore esa 0E2H. Vengono risettati gli attributi del file, il codice virale infetta il file rinominato, la dimensione aumenterà da 1509 a 1524 dovuto all'allineamento del paragrafo. Viene settato l'attributo originale del file e rinominato con l'estensione appropriata. Il virus è localizzabile alla fine del file infetto e sono visibile le seguenti stringhe:

chklist.ms chklist.cps smartchk.cps

Se sono presenti questi files, durante la fase di infettaggio il codice virale li cancellerà.
La data e l'ora del file non vengono alterate. Il RebelBase si attiva il 16 Aprile di ogni anno visualizzando a video il seguente messaggio:

Happy Birthday KAORI!
Dedicato a tutte le meravigliose ragazze giapponesi
(C) BitLabs (The RebelBase) 1993, N. Italy.

Questo testo non è visibile, perchè risulta crittografato e si decrittografa solo quando viene visualizzato a video. La chiave di decrittografazione avviene con l'istruzione XOR con il valore 45H.

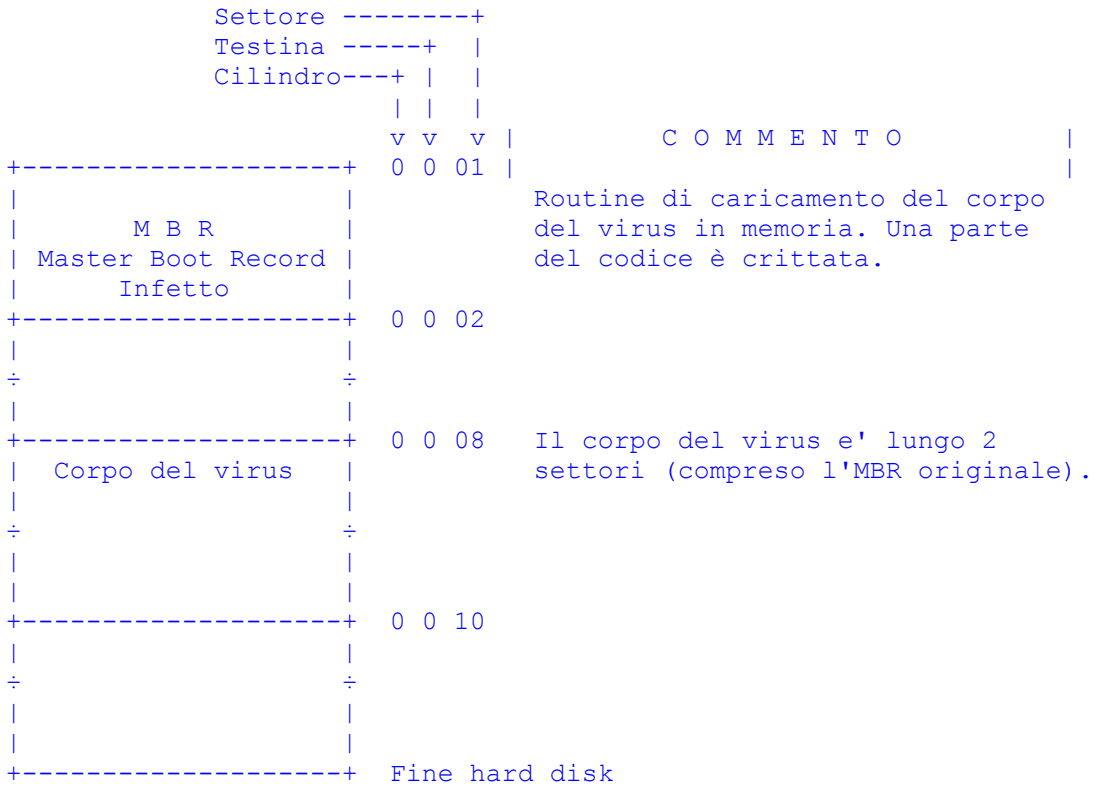
Riot.426

Virus ad azione diretta, infetta .COM, lunghezza 426 bytes. Contiene il seguente testo:

ARBEIT MACHT FREIT!
The Unforgiven / Immortal Riot Sweden 01/10/93

Ripper

Virus residente in memoria, stealth, infetta il master boot record del disco fisso e il boot sector dei floppy disk. Quando è residente, la memoria libera del sistema diminuisce di 2 kilobytes. Il disco fisso risulta infetto in questo modo:



Il virus ha una parte di codice crittografata e contiene il seguente testo:

FUCK 'EM UP !

(C)1992 Jack Ripper

Il codice virale casualmente può corrompere i dischi.

RPS2

Virus residente in memoria, infetta il boot sector dei floppy disk e la tabella delle partizioni (mbr) del disco fisso. Il codice virale quando infetta non salva il boot o il master boot record originali, ma ci scrive sopra, per questo motivo la rimozione del codice non è possibile per la strada standard. Il virus RPS2 è stato scritto utilizzando instruzione che sono presenti nei processori dall'186 in su, quindi nei vecchi 8086/8088 il codice virale non funziona. Il virus quando si installa in memoria, sovrascrive la tabella dei vettori degli interrupt, questo può portare al crash del sistema in alcuni programmi. Il codice virale utilizza un contatore interno, quando questo è a zero, alla lettura del mbr, vengono riscritti alcuni settori dell'hard disk. Il codice virale al suo interno contiene il seguente testo:

RPS2

Il virus RPS2 contiene molti bug, ad esempio i floppy infetti possono non funzionare correttamente. Questo codice virale risulta essere molto attivo nella provincia di Brescia.

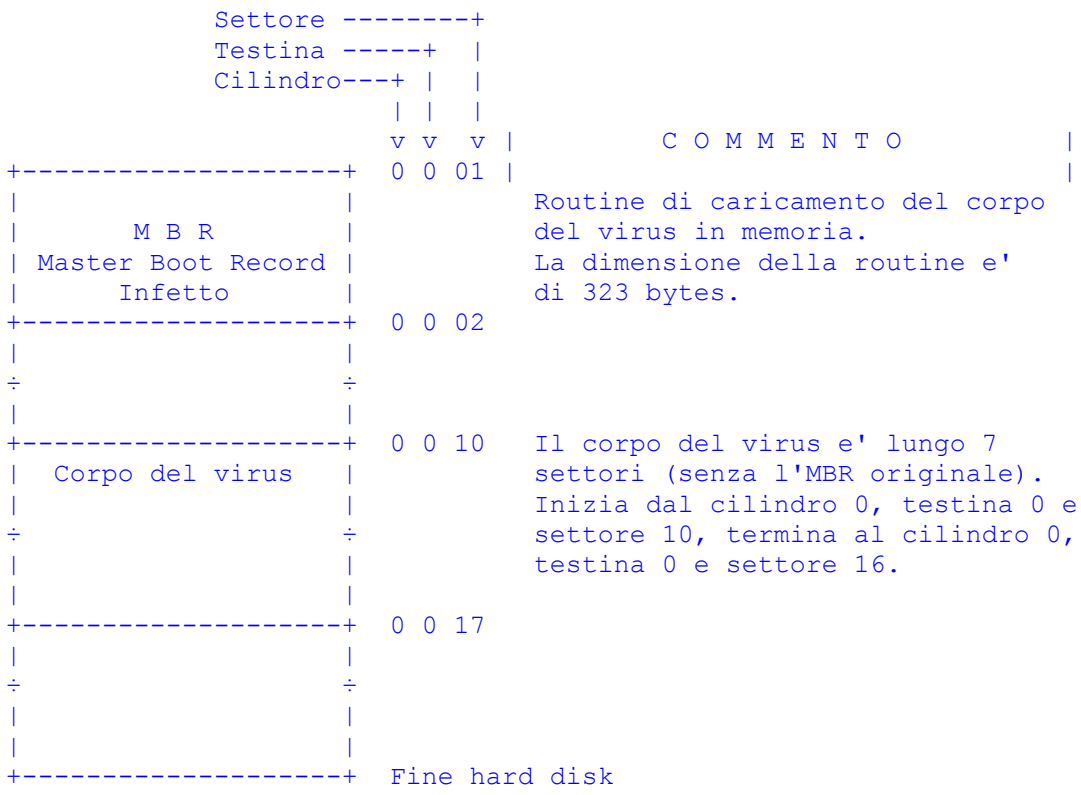
Run_error_504D:5658

Questo codice virale e' stato individuato nel mese di Luglio 1994 in Italia. Il virus risulta essere residente in memoria (TSR), stealth ed infetta il boot sector dei floppy disk e la tabella delle partizioni (Master Boot Record).
Per verificare la sua eventuale attivazione in memoria, il codice virale, chiama l'interrupt 13H con AX=DEF0H, se viene restituito AX=9ABCH significa che è già attivo in memoria. Nel caso contrario il virus si alloca in memoria all'indirizzo 9E00:0000 sottraendo 8 Kb di memoria. Dopo ciò vengono intercettati gli interrupts 13H all'indirizzo 9E00:0B03, l'interrupt 05H all'indirizzo 9E00:0B09, l'interrupt 08H all'indirizzo 9E00:0B06. Dell'interrupt 13H vengono controllate le seguenti funzioni:

AH = 08 Get Drive parameter: quando viene chiamata questa funzione il virus somma al contenuto della locazione 0:413H gli 8 Kb di memoria tolta per allocarsi. Questa tecnica vuole camuffare l'allocamento in memoria. La tecnica non sembra essere molto efficace visto che con il programma DOS MEM.EXE viene visualizzata la mancanza di 8 Kb in memoria!!!

AH = 02 (Read sector), 03 (Write sector): con queste due funzioni il virus attiva la routine di stealth (invisibilita') e si propaga.

L'infezione si trasmette al floppy o all'hard disk accedendo a questi con le consuete modalità. Nell'hard disk non vengono formattate tracce non standard, il corpo del codice virale risulta avere una lunghezza pari a 8 settori ed è localizzabile dal cilindro 0, tesina 0 e settore 10, l'infezione risulta come segue:



Nei Floppy Disk vengono formattate tracce non standard, il corpo del codice virale risulta avere una lunghezza pari a 8 settori e la sua localizzazione è dipendente dal tipo di disco.
All'interno del codice virale sono presenti le seguenti stringhe:

Invalid Partition Table. Error Loading Operating System.
Missing Operating System

Le stringhe sopra sono utilizzate per camuffare l'MBR (Master Boot Record), infatti alcune di queste possono essere anche visualizzate a video se si verificano eventuali errori, ad esempio la stringa "Missing Operating System" verrà visualizzata se l'MBR nella locazione all'offset 1FEH è diversa da 55AAH.

Nel caso in cui si verifichino delle "strane" situazioni per il virus, viene visualizzata la seguente stringa, dalla quale si è deciso di desumere il nome del virus stesso:

Run time error 504D:5658

Le routine che gestiscono l'interrupt 08 e 05 non sono di particolare interesse, per l'interrupt 08 la routine incrementa la locazione 9E00:0B60 ed al raggiungimento del valore 4000H viene riportata a 0 (zero). Per l'interrupt 05, ad ogni chiamata, viene settata la locazione 9E00:0B8CH alternativamente a 0 e 1.

S

S_E_K
Sampo
Satan.612
Satirycon Family
Screaming_Fist.Stranger
Serena
Slam_Tilt.703
SMEG Family
Snow.297
Spirit
Star_Dot Family
Stealth_Boot.C
Stoned Family
Suomi
Susan
Swedish_Disaster.I
Swiss_Boot
Sylvia.1332

S_E_K

Resedente in memoria, crittografato, infetta .COM, lunghezza 1491 bytes. Il virus scatta il 13 luglio di ogni anno visualizzando a video il seguente testo:

IL SISTEMA è FOTTUTO!!
S.E.K. VIRUS Made in Italy RM
5iD G.Ferraris 90/91 (c)

a questo punto vengono riscritti 9 settori dell'hard disk partendo del settore 1 traccia 0 testina 1.

Sampo

Virus residente in memoria, stealth, infetta il Master Boot Record del disco fisso e il Boot Sector del floppy disk. Questo virus e' di origine Filippine e contiene il seguente testo:

SAMPO
"Project X"
Copyright(c) 1991 by the SAMPO X-Team
All rights reserved
University of The East Manila

Satan.612

Virus ad azione diretta, infetta i files con estensione .COM. I files infetti aumentano di 612 bytes. Il codice virale si attiva il 1ø di aprile e il 25 dicembre, cancellando i files.

Satirycon Family

Satirycon.355

Virus ad azione diretta, infetta .COM, lunghezza 355 bytes.
Contiene il seguente testo:

**.COM C:\DOS\FORMAT.COM*
DEMON

Satyricon.360

Questo codice virale è stato individuato nella seconda settimana di settembre 1993, la sua provenienza è quasi sicuramente italiana. Il virus è ad azione diretta ed infetta i files .COM della corrente directory. Quando un programma infetto dal Satyricon viene eseguito, il virus legge la data del sistema, se corrisponde al giorno 13 si inluppa, altrimenti infetterà tutti i file con estensione .COM nella corrente directory con il penultimo byte diverso da 0AFH. Dopo di che infetterà il file FORMAT.COM presente nella directory C:\DOS.
La lunghezza dei files aumenterà dai 360 ai 375 bytes, questa variazione è dovuta all'allineamento di paragrofo eseguito dal codice virale prima dell'infezione, data e ora dei files colpiti non vengono modificate. All'interno del codice sono presenti le seguenti stringhe:

.COM C:\DOS\FORMAT.COM

SATYRICON

Quest'ultima stringa non viene mai visualizzata a video. Il virus oltre alla sua propagazione con le modalità già viste non risulta procurare danni di sorta, si può facilmente desumere dalla "qualità" e "funzionalità" del codice, che questo non può che essere un virus di sperimentazione.

Screaming_Fist.Stranger

Virus residente in memoria, crittografato, infetta files con estensione COM e .EXE.
All'interno del codice sono presenti le seguenti stringhe:

I am a stranger in a strange land

C:\COMMAND.COM

Serena

Il virus Serena è stato isolato nel mese di Novembre 1992, la sua provenienza è italiana. Questo virus è residente in memoria (TSR), ed utilizza una routine di crittografazione onde evitare di essere scoperto all'interno dei files .COM infettati. Quando un programma infetto dal virus Serena viene eseguito, questo si installa in memoria allocandosi nell'area del COMMAND.COM la quale aumenterà di 1056 bytes. Il virus modifica i vettori dell'interrupt 21H e a volte l'interrupt di gestione del CTRL-BREAK e quello degli errori critici (int. 24). Dopo che il virus è residente in memoria ogni files .COM eseguito viene infettato. La sua lunghezza aumenta di 792 bytes. Il virus è localizzabile alla fine del file, la sua individuazione non è immediata essendo il virus crittografato. La data e l'ora del file non vengono alterate dal virus. Lanciando un file infetto nel giorno di Venerd□ 17 il virus riscriverà, nella corrente unità 200 settori partendo dal settore zero se questa è il disco rigido, oppure 35 settori se il drive è A: o B:. Dopo la riscrittura comparirà a video la seguente stringa:

psSerena ti ho ama

dopo ciò il virus si "inluppa". La stringa che doveva comparire a video era " Serena ti ho amata ", questo non accade essendo presente un errore di puntatore. L'istruzione corretta doveva essere:

MOV DL,[BX+0120] e non MOV DL,[BX+0122]

La stringa non è visibile in memoria rimanendo quest'ultima crittografata. Il virus è attivo ogni Venerd□ anche se la data è diversa da 17, in tali giorni viene inizializzata la tabella dei parametri del disco. Ogni 17 del mese il virus modifica i vettori dell'interrupt della gestione del CTRL-BREAK e degli errori critici.

Slam_Tilt.703

Virus ad azione diretta, crittografato, infetta .Com, lunghezza 703 bytes. Contiene il seguente testo:

<<SLAM TILT>>

SMEG

Pathogen

Il virus è polimorfico, residente in memoria, crittografato, infetta files con estensione .EXE e .COM. Secondo l'autore, questo codice virale utilizza il motore polimorfico SMEG (Simulated Metamorphic Encryption Generator) versione 0.1. Il virus si attiva ogni Luned□ dalle 17:00 alle 18:00 sovrascrivendo l'hard disk e visualizza:

Your hard-disk is being corrupted, courtesy of PATHOGEN!
Programmed in the U.K. (Yes, NOT Bulgaria!) [C] The Black Baron 1993-4.
Featuring SMEG v0.1: Simulated Metamorphic Encryption Generator!
'Smoke me a kipper, I'll be back for brakfast.....'
Unfortunately some of your data won't!!!!!

All'interno del codice sono presenti anche le seguenti stringhe:

EXECOM
SMEG v0.1

Snow.297

Data scoperta: Ottobre 2000

Origine: Italia

Autore: DiAm0nD

Descrizione:

Virus ad azione diretta, che infetta tutti i files con estensione .COM nella stessa directory. I file si allungano di 297 bytes. Alla fine dell'infezione visualizza un effetto grafico. Il virus contiene il seguente testo:

Happy_Christmas By DiAm0nD

Spirit

Virus residente in memoria, stealth, extratraccia, infetta il boot sector dei floppy disk e il master boot record del disco fisso. Il codice virale infetta i floppy disk formattando una nuova traccia alla fine del dischetto. Invece il master boot record viene infettato nel modo standard. Il codice virale contiene il seguente testo:

SPIRIT (c) MW

Star_Dot Family

Star_Dot.600

La sua provenienza non è conosciuta, ma quasi sicuramente è di origini italiana. Questo virus non è residente in memoria, ma ad azione diretta ed infetta i files .EXE. Quando un programma infetto dallo Star_Dot.600 è eseguito, il virus infetta un file .EXE nella corrente unità, la scelta del file da infettare è casuale. I programmi infetti aumentano in lunghezza da 600 a 615 byte, il virus può essere localizzato alla fine del file infetto. Il virus Star Dot può infettare in alcuni casi più volte lo stesso file. La data e l'ora del file non viene alterata dal virus.

Star_Dot.789

La sua provenienza non è conosciuta, ma quasi sicuramente è di origini italina. Questo virus non è residente in memoria, ma ad azione diretta ed infetta i files .EXE, .COM e COMMAND.COM. Quando un programma infetto dallo Star_Dot è eseguito, il virus infetta il file COMMAND.COM contenuto in root se non è infetto, altrimenti un file .EXE nella corrente unità o un file .COM se gli eseguibili sono infetti, la scelta del file da infettare è casuale. I programmi infetti aumentano in lunghezza da 789 a 805 bytes, il virus può essere localizzato alla fine del file infetto. Lo Star_Dot può infettare in
alcuni casi più volte lo stesso file (soprattutto se i files sono molto corti!). La data e l'ora del file non viene alterata dal virus. Il virus Star_Dot.789 entra in funzione il 24 Settembre di ogni anno dalle ore 7 in poi riscrivendo tutti i dischi presenti dall'unità Z all'unità A.Questa riscrittura comporta la distruzione del Boot Sector e della FAT.

Star_Dot.801

La sua provenienza non è conosciuta, ma quasi sicuramente è di origini italiana. Questo virus non è residente in memoria, ma ad azione diretta ed infetta i files .EXE, .COM e COMMAND.COM. Quando un programma infetto dal virus Star_Dot.801 è eseguito, il virus infetta il file COMMAND.COM contenuto in root se non è infetto, altrimenti un file .EXE nella corrente unità o un file .COM se gli eseguibili sono infetti, la scelta del file da infettare è casuale.
I programmi infetti aumentano in lunghezza da 801 a 817 bytes, il virus può essere localizzato alla fine del file infetto. Può infettare in alcuni casi più volte lo stesso file. La data e l'ora del file non viene alterata dal virus. Il virus Star_Dot.801 entra in funzione il 13 Febbraio di ogni anno dalle ore 13 in poi riscrivendo il disco corrente.

Stealth_Boot.C

Virus residente in memoria, stealth, infetta il boot sector dei floppy disk e il master boot record (mbr) dell'hard disk. Quando il virus è residente la dimensione della memoria libera del sistema è diminuita di 4 kbytes. Il codice virale infetta i floppy disk da 3 1/2" da 1.44 Mb e 720 Kb, e i floppy da 5 1/4" da 1.2 Mb e 360 Kb ogni qualvolta
viene letto/scritto un settore del floppy.

Stoned Family

Stoned.Angelina
Questo codice virale è di origine polacca, risulta essere residente in memoria, stealth, infetta il boot sector dei floppy disk e il master boot record (mbr) dell'hard disk. Quando il virus è residente la dimensione della memoria libera del sistema è diminuita di 1 kbytes. Il virus contiene al suo interno il seguente testo in forma crittata:

Greetings for ANGELINA !!!/by Garfield/Zielona Gora

Zielona Gora è la città dove è stato sviluppato il codice virale.

Stoned.Dinamo
Questo codice virale è di origine ucraina o ex-sovietica, risulta essere residente in memoria, infetta il boot sector dei floppy disk e il master boot record (mbr) dell'hard disk. Quando il virus è residente la dimensione della memoria libera del sistema è diminuita di 2 kbytes. Il virus contiene al suo interno il seguente testo in forma crittata:

Dinamo(Kiev)-champion !!!

Kiev è la capitale dell'Ucraina, dove è stato sviluppato il codice virale e la Dinamo Kiev è la squadra di calcio molto famosa negli anni 1986-1990 con i giocatori Belanov e Zavarov, quest'ultimo è stato il primo calciatore sovietico a passare ad una squadra italiana, la Juventus.

Stoned.Empire.Monkey
Virus residente in memoria, stealth, infetta il boot sector dei floppy disk e il Master Boot Sector del disco fisso. Quando il virus è residente la memoria libera del sistema diminuisce di 1 kilobytes. Il virus crittografa il boot sector originale dei floppy e l'MBR originale del disco fisso, il quale è posto nel settore 3, testina 0 e cilindro 0. Accedendo con un floppy pulito l'unità C: non viene vista dal DOS, quindi l'utilizzo del programma FDISK /MBR per l'eliminazione del codice virale porterebbe alla completa
perdita del disco fisso. Per la rimozione del codice virale contattare il supporto tecnico TG Soft.

Stoned.HiDos
Virus residente in memoria, stealth, infetta il boot sector dei floppy disk e il master

boot record (mbr) dell'hard disk. Quando il virus è residente la dimensione della memoria libera del sistema è diminuita di 2 kbytes. I floppy disk da 1.44 Mb infetti dallo Stoned.HiDos sono resi inaccessibili al DOS. Il codice virale contiene all'interno il seguente testo:

[HiDos] By Apache

Stoned.LZR
Virus residente in memoria, infetta il boot sector dei floppy disk e il master boot record (mbr) dell'hard disk. Quando il virus è residente la dimensione della memoria libera del sistema è diminuita di 2 kbytes. I floppy disk da 1.44 Mb non sono infettati correttamente dallo Stoned.LZR, il quale salva il boot originale nell'area dati del floppy disk. Il codice virale è pericoloso perchè casualmente può sovrascrivere il contenuto del disco.

Stoned.NoInt
Virus residente in memoria, stealth, infetta il boot sector dei floppy disk e il master boot record (mbr) dell'hard disk. Quando il virus è residente la dimensione della memoria libera del sistema è diminuita di 2 kbytes. La routine per la gestione dello stealth, blocca l'accesso alla lettura del master boot record.

Suomi

Virus ad azione diretta, non residente in memoria, crittografato, infetta files con estensione .COM. La lunghezza del codice virale è di 1008 bytes. Quando viene eseguito un file infetto, il codice virale si toglie dal file e infetta il COMMAND.COM. All'interno del codice è presente la seguente stringa:

Oulu

Il virus è di origine finlandese.

Susan

Virus residente in memoria, ma di tipo primitivo che sovrascrive il file. Il codice virale sovrascrive i primi 571 bytes, quando viene eseguito un file infetto viene visualizzato a video il seguente messaggio:

Bad command or file name

All'interno del codice è presente la stringa:

Susan

Swedish_Disaster.I

Virus residente in memoria, infetta il boot sector dei floppy disk e il master boot record (mbr) dell'hard disk. Quando il virus è residente la dimensione della memoria libera del sistema è diminuita di 2 kbytes. I floppy disk da 1.44 Mb infetti dallo Swedish_Disaster.I sono resi inaccessibili al DOS. Il codice virale contiene all'interno il seguente testo:

The Swedish Disaster I

Swiss_Boot

Virus residente in memoria, infetta il boot sector dei floppy disk e del disco fisso.
Quando il virus rimane residente, la memoria libera del sistema diminuisce di 3 KB.
Il codice virale si attiva il 7 febbraio di ogni anno, visualizzando a video il seguente messaggio:

Schafft die Schweizer Armee ab !

e sovrascrivendo il disco fisso.
La stringa risulta essere crittografata, quindi non visibile.

Sylvia.1332

Virus ad azione diretta, infetta files con estensione .COM allungandoli di 1332 bytes. All'interno il codice virale contiene il seguente testo:

```
This
    program
           is
             infected
                    by
                      a
                       HARMLESS
                               Text-Virus V2.1

Send a FUNNY postcard to : Sylvia Verkade,
                           Duinzoom 36b,
                           3235 CD Rockanje
                           The Netherlands

You might get ANTIVIRUS program.....
```

T

Taiwan.743.A

Virus ad azione diretta, infetta i files con estensione .COM. Ad ogni esecuzione di un file infetto, il codice virale infetta 3 file non infetti, aumentandoli di 743 bytes. Il giorno 8 di ogni mese sovrascrive con valori casuali il disco.

Tenbytes.1554

Virus residente in memoria, infetta files con estensione .COM e .EXE. La lunghezza del codice virale è di 1554 bytes. All'interno del codice non sono presenti stringhe.

Tequila

Virus residente in memoria, polimorfico, crittografato, infetta il Master Boot Sector del disco fisso e files con estensione .EXE. I files infetti aumentano di 2468 bytes. All'interno il codice virale contiene il seguente messaggio:

Welcome to T.TEQUILA's late/t production
Contact T.TEQUILA/P.o.Box 543/6312 St'hausen/Swi(zerland.
Loving thoughts to L.I.N.D.A.
*Beer and Tequila for e*er!*

Execute: mov ax, FE03 / int 21. Key to go on!

Thanksgiven

Virus residente in memoria, infetta files con estensione .COM, boot sector dei floppy disk e la tavola delle partizioni (mbr) del disco fisso. Il codice virale occupa in memoria 2 kb, ed intercetta interrupt 8, 13H, 21H. Ogni file .COM eseguito, la lunghezza del file aumenterà di 1253 bytes. Quando infetta il disco fisso, il codice virale si pone al seguente indirizzo: cilindro=0, testina=0, settore=4. Il codice virale si attiva dal 24 novembre 1990 in poi, riscrivendo i settori dei floppy e del disco fisso con valori casuali. All'interno del codice è presente la seguente stringa:

V-1

Tic.109

Virus ad azione diretta, infetta tutti i files con estensione .COM nella corrente directory. I files infetti aumentano di 109 bytes, il codice virale è localizzabile all'inizio del file. Il virus non ha effetti oltre alla sua replicazione.

TOPA Family

Topa.2476

Virus residente in memoria, crittografato, infetta i files con estensione COM e EXE. I files infetti aumentano di 2476 bytes. Il virus contiene al suo interno i nomi della maggior parte degli anti-virus, in modo da non infettare i suddetti files. Esistono altre due varianti del codice virale lunghe 2456 e 2520 bytes.

Torpino

Virus residente in memoria, polimorfico, crittografato, infetta i files .COM e .EXE. In particolar modo infetta il file KEYB.COM nella directory del DOS o in WINDOWS\ COMMAND.
Il codice virale contiene il seguente testo:

Your keyboard has exipired its evaluation period!
Please, register to Microsoft(c) Corporation.

Found hardware error on video card (code 23001):
Please, move your monitor and reboot the PC.

Found error: ah ah ah ah... eh eh eh eh... uh uh uh uh...
Dr.SCSI & Mr.IDE

Your Hard Disk is boring to live...
Youthanasia will start now... (formating C:)

Found Boot error: replace the TORPINO card
and reboot the system immediately !

This message is a property of F-PROT Antivirus:
Please, contact fridrick for more info...

C O N G R A T U L A T I O N S !
Your PC is my new house !
I'm not a destroyer...
I'm the incredible Virus . . .
--> T O R P I N O (c) <--
Turn on Sound Blaster Speakers !

You are a Torpiner

Thank Very Much the F-PROT Antivirus For The
Contribution To The Spread of This Virus...
Have A Good Time!
By The Virus TORPINO (C) Ver. 2.0, Copyright(C) 1997
By DR.SCSI And Mr. IDE.
Total Rows Code: 3474,
Coded In ITALY, Around MATERA, In July-December 1997.
Direrct Support: Our Heads; Dave Mustaine; Billy (A Programmer Dog!).
Indirect Support: The Great Dark Avenger; N.R.L.G. Team;
Peter Norton (smack!); Our Workstation: Two 486;
The Obscure Author of Tentacle.

TPE Family

Il TPE non è un virus, ma un motore per rendere i virus i polimorfici. Il TPE è similare al motore MtE del bulgaro Dark Avenger, TPE sta per TridenT Polimorphic Engine è firmato dal gruppo di virus-writers olandesi TridenT, l'autore del TPE è Masud Khafir. Masud Khafir è un nome composto, Masud deriva da Masud Barzani (leader della ribellione kurda) e da Masud Rajavi (leader degli Iranian Mujahedin) e da altri leader della ribellione afghana. Khafir è una parola che prende vari significati da Paese a Paese, in Olanda è usata per definire un'idiota.

YB-1:TPE.1_4

Virus ad azione diretta, infetta i files con estensione .COM, utilizza per rendersi polimorfico il motore TPE versione 1.4. Il codice virale al suo interno contiene il seguente testo:

YB-1 / Konthark
**.COM*

[MK / TridenT]
[TPE 1.4]

TPTG.0_02

Il TPTG.0_02 è un generatore di trojan horse, cioè cavalli di troia, scritto da un autore italiano che si fa chiamare DarkMan. Il codice generato dal TPTG è in linguaggio PASCAL.

Big_Bug:TPTG.0_02
E' un cavallo di troia che sovrascrive il file CONFIG.SYS con il seguente messaggio:

Virus created by TPTG

Visualizza a video la seguente frase:

CONFIG.SYS destroied ! I am BIG_BUG. FUCK THE SYSTEN !!

WinKill:TPTG.0_02
E' un cavallo di troia che sovrascrive il file C:\WINDOWS\WIN.COM con il seguente messaggio:

I am the WIN_Kill !! You have found a new trojan virus !!

Visualizza a video la seguente frase:

Bye bye Windows !

Nel caso non sia in grado di sovrascrivere il file visualizza a video il messaggio: This program requied Microsoft Windows.

WinKill2:TPTG.0_02
E' un cavallo di troia che sovrascrive il file C:\WINDOWS\PROGMAN.EXE con il seguente messaggio:

GAIA DE LAURENTIIS LIVES... SOMEWHERE IN TIME
I am the Win_Kill_2 !! You have found a new varian of WIN_Kill virus

Visualizza a video la seguente frase:

Bye bye Windows !

Nel caso non sia in grado di sovrascrivere il file visualizza a video il messaggio: This program requied Microsoft Windows.

Gaia De Laurentis è la presentatrice del programma televisivo TARGET.

Triplicate

E' un macro virus di Excel 97. Il virus Triplicate, crea un file denominato BOOK1 nella directory XLSTART. Ogni documento di Excel che verra' chiuso, sara' infettato dal macro virus Triplicate.
Questo virus contiene le seguenti macro: Document_Close, Workbook_Deactivate e Actionhook(Tristate).
Contiente il seguente testo:

TRIPLICATE

Trivial Family

Trivial.42, .45

Virus tipo primitivo, che sovrascrive files con estensione .COM sulla corrente directory. All'interni è presente la seguente stringa:

*.COM

Trivial.Explode

Virus tipo primitivo, che sovrascrive files con estensione .COM sulla corrente directory. Quando viene eseguito un programma infetto, viene visualizzato a video il seguente messaggio:

Program too big to fit in memory.

Contiene anche il seguente testo:

Your hard drive is about explode!

Trojan.MBR

Data scoperta: Ottobre 2000

Origine: Italia

Autore: DiAm0nD

Descrizione:

Cavallo di troia contenuto nel file mbr.com, quando eseguito sovrascivere il master boot record del disco fisso. Contiene il seguente testo:

Inserimento dati in corso...

Impossibile leggere da MBR.COM!

MBR By DiAm0nD

Trojector.1561

Virus residente in memoria, stealth, crittografato, infetta i files con estensione .COM e .EXE allungandoli di 1561 bytes. Il codice virale contiene il seguente testo:

TROJECTOR]I[, (c) Armagedon Utilities,
Athens 1992, Greetings to Vesselin.

U

Unashamed
UVR

Unashamed

Virus residente in memoria, stealth, infetta il boot sector dei floppy disk e il master boot record del disco fisso. Il codice virale casualmente visualizza a video il seguente messaggio:

the UNashamed Naked!

UVR

Virus residente in memoria, infetta files con estensione .COM. Ogni files che verrà infettato dal codice virale aumenterà di 3919 bytes. All'interno il codice virale contiene il seguente testo:

UVR Already installed.

Questo testo è visibile all'interno del virus, ma un'altra stringa è presente all'interno di UVR, quest'ultima risulta essere crittografata (non visibile):

Vietato FUMARE!

V

V-Sign
V2Px Family
Varcella.749
VBS/HappyTime
VBS/LoveLetter
VBS/OnTheFly
VCL Family
Viaggio
Vienna Family
Virdem.1542
Vota_DC

V-Sign

Virus residente in memoria, infetta il master boot record del disco fisso e il boot sector dei floppy disk. Il codice virale non preserva l'MBR e i boot originali. Dopo aver infettato 64 dischetti visualizza a video una grande V.

V2Px Family

V2Px.1260

Virus ad azione diretta, polimorfico, crittografato, infetta files con estensione .COM. Ogni file infetto aumenta di 1260 bytes. All'interno del codice è visibile solo la stringa:

*.COM

Il virus risulta essere una rielaborazione del Vienna.

V2Px.1840, .1993

Virus ad azione diretta, polimorfico, crittografato, infetta files con estensione .COM. Ogni file infetto aumenta di 1840 (1993) bytes. All'interno del codice è visibile solo la stringa:

**.COM PATH=*

Varcella.749

Virus ad azione diretta, infetta i files tipo EXE e COM allungandoli di 749 bytes. Il virus manda in crash il calcolatore.

VBS/HappyTime

Questo virus e' uno script virale che viaggia attraverso la posta elettronica, inserendovi il suo codice nei messaggi html. Il messaggio che arriva non contiene allegati, ma uno script. Il virus si attiva nel momento che si visualizza il messaggio, anche solo in anteprima. Quando il virus e' attivo, crea i seguenti files: HELP.HTM, HELP.VBS e UNTITLED.HTM, ed infetta i files con estensione .htm, .html, htt. Ogni messaggio di posta elettronica inviato, sara' infettato dal virus inserendovi lo script virale nei messaggi in formato html.

VBS/OnTheFly

E' un VBscript worm, che viaggia attraverso la posta elettronica. Il worm si trasmette inviando il seguente messaggio ai destinatari presenti nell'address book.

Subject: Here you have, ;o)

Hi:
Check This!

Con allegato il file AnnaKournikova.jpg.vbs.

L'ignaro utente pensa di aver ricevuto un'immagine della tennista russa Anna Kournikova, eseguendo il file, il worm si attiva e invia il messagio sopra citato agli utenti presenti nell'address book. Il worm si attiva il 26 Gennaio collegandosi al sito http://www.dynabyte.nl.

Il worm risulta essere crittografato.

VCL Family

VCL.BEv.516
Virus ad azione diretta, crittografato, infetta i files con estensione .COM allungandoli di 516 bytes. All'interno il codice virale contiene il seguente testo:

Happy 4th!
Hope you enjoy your messed up computer!
-=BEv#A96=-

VCL.Diarrhea.1221
Virus ad azione diretta, crittografato, infetta files con estensione .COM. I files infetti aumentano di 1221 bytes. Il codice virale visualizza a video il seguente messaggio:

EAT MY DIARRHEA!

-GG Allin & The Texas Nazis

All'interno il codice virale contiene la stringa: [VCL]. Esiste un'altra variante lunga 931 bytes.

VCL.Divide.433
Virus gemellare che crea un file con estensione .COM di lunghezza 433 bytes con attivi tutti gli attributi: nascosto, di sistema, etc. Contiene il seguente testo:

**.EXE*
Divide overflow [VCL]

VCL.Divide.546, .554
Virus overwriting, che sovrascrive i files con estensione .COM e .EXE. Esistono due varianti di lunghezza 546 e 554 bytes. All'interno il codice virale contiene il segeuente testo:

Divide Overflow [VCL]

**.com *.exe*

La variante VCL.Divide.546 contiene la parola DOME, invece la variante lunga 554 bytes contiene la parola DOME2. Quando ha infettato tutti i files, il codice virale sovrascriverà ogni files con valori casuali.

VCL.Elena
Virus ad azione diretta, infetta .COM, lunghezza 730 bytes. Contiene all'interno il seguente testo:

Elena M. Tnx2NMan

Hey Jack! please contact me, I'm in your city! What? This is a simple virus? Don't worry.. it's only a demo!

VCL.Heevahava.514
Virus gemellare che crea un file con estensione .COM di lunghezza 514 bytes con attivi tutti gli attributi: nascosto, di sistema, etc. Contiene il seguente testo:

**.EXE*
Only heeva-hava's get stuck with THE HEEVAHAVA VIRUS!
HEEVA[VCL]

VCL.YoungBlood
Virus ad azione diretta, crittografato, infetta .COM, lunghezza 914 bytes. Contiene all'interno il seguente testo:

C:\DOS.EXE C:\DOS*.COM C:*.**

>>YoungBlood<< Productions

*[****** TECHNOCLASH *****]*
[Blast Your System Off !]
[xxx] [Hello!]

Viaggio

Virus residente in memoria, crittografato, infetta i files con estensione .COM. I files infetti aumentano di 1051 bytes, data e ora del file risultano alterate. Il virus contiene il seguente testo visibile:

UN VIAGGIO

IL VIAGGIO

Inoltre contiene il seguente testo in forma crittata:

OLLELE OLLALA FACCELA VEDE FACCELA TOCCA

Questo sistema e' totalmente impestato da un virus, buon anno!

Quando si è installato in memoria, se è presente il file C:\^^___#@.$$$ termina la propria esecuzione.

Vienna Family

Vienna.353
Virus ad azione diretta, infetta files con estensione .COM. I files infetti aumentano di una lughezza di 353 bytes. Il codice virale contiene la seguente stringa:

*.COM

Esiste un'altra variante lunga 435 bytes.

Vienna.621
Virus ad azione diretta, infetta files con estensione .COM. I files infetti aumentano di una lughezza di 621 bytes. Il codice virale contiene la seguente stringa:

*.COM
PATH= nome del file infetto

In alcuni casi può corrompere (distruggere) files con estensione .COM.

Vienna.645, .648
Virus ad azione diretta, infetta files con estensione .COM. I files infetti aumentano di una lughezza di 645 (648) bytes. Il codice virale contiene la seguente stringa:

*.COM

PATH= nome del file infetto

Esistono moltissime sotto-varianti del virus Vienna.648, alcune di queste contengono all'interno del testo:

Vienna.648.Lisbon: "@AIDS"

Vienna.BNB
Virus ad azione diretta, infetta i files con estensione .COM allungandoli di 429 bytes. All'interno il codice virale contiene il seguente testo:

Beware the Beast-N-Black

Vienna.W-13.534
Virus ad azione diretta, infetta files con estensione .COM. I files infetti aumentano di una lughezza di 534 bytes. Il codice virale setta la data del file infettato col il valore del mese uguale a 13. Esistono altre 2 varianti di questo codice virale lunghe rispettivamente 377 e 507 bytes.

Virdem.1542

Virus ad azione diretta, infetta files con estensione .COM. I file infettati aumentano di una lunghezza pari a 1542 bytes. I files colpiti risultano rovinati dal codice virale, il quale sovrascrive erroneamente una parte del file. Questo porta al malfunzionamento del file, e all'impossibilità della rimozione del codice virale. Quando ha infettato tutti i files, il codice virale visualizza un'immagine grafica. All'interno il codice non contiene
stringhe visibili.

Vota_DC

Residente in memoria, infetta i file .COM, lunghezza 591 bytes. Visualizza nel mese di Aprile la seguente frase:

Messaggio promozionale: Vota DC!

W

WelcomeB
Win32.Cih
Win32.Kriz
Win32.Magistr
Win32.MTX
Win95.Marburg
Win32.Navidad
Win32.Nimda
Win32.Porkis
Win95.Roma
Winword Macro virus
Worm.Fix2001

WelcomeB

Virus residente in memoria, infetta il boot sector dei floppy disk e il master boot record del disco fisso. Il codice virale contiene il seguente testo:

Welcome to BUPT 9146, Beijing!

Win32.Cih

Virus residente in memoria, infetta i files formato Windows 95/98 (PE), ogni files aperto o eseguito sara' infettato dal virus. Contiene il seguente testo:

CIH v1.2 TTIT

Il virus sovrascrive il disco ogni 26 Aprile. Esistono altre varianti che entrano in funzione il 26 di ogni mese.

Win32.Kriz

Il virus Kriz e' residente in memoria, polimorfico, infetta file .EXE e .SCR.
Il codice virale quando eseguito, va ad infettare il file KERNEL32.DLL, permettendo al virus di rimanere sempre residente. Per infettare questo file, il virus crea come copia di Kernel32.Dll il file KRIZED.TT6 ed infetta quest'ultimo, dopo modificando il file WININIT.INI al successivo boot sostituisce il KERNERL32.DLL con il file KRIZED.TT6. Il virus si aggancia a 16 funzioni del Kernel32.
Il virus si attiva il 25 Dicembre sovrascrivendo il disco fisso e cancellando la memoria CMOS e i FLASH BIOS come il virus Win32.CIH (Chernobyl).

Win32.Magistr

Il virus Win32.Magistr e' costituito da due componenti virus e worm. la componente worm è in grado di viaggiare attraverso la posta elettronica, invece quella virus infetta i files locali della macchina e quelli locali della rete (LAN).
Il virus e' estremamente pericoloso, dopo un mese dall'infezione il Magistr sovrascrive il disco fisso e il contenuto della memoria CMOS e Flash Bios come il virus Win32.CIH (Chernobyl).
Il codice virale Magistr e' polimorfico, e la sua riomozione e' molto complessa. Il virus e' lungo circa 30Kb, scritto interamente in assembler.
Quando viene eseguito un files infetto, il virus si carica in memoria agganciadosi ai processi di Explorer.exe. Dopo 3 minuti il virus entra in funzione infettando files di tipo eseguibile (.EXE) e screen saver (.SCR). Il virus per rendersi attivo al succesivo boot, aggiunge una nuova esecuzione nel registro RUN di HKLM. Invece nelle macchine remote, modifica il file WIN.INI nella riga RUN=.
La componente Worm preleva gli indirizzi di posta elettronica dal vostro Address Book, ed invia un email con allegati un file eseguibile infetto e un altro file con estensione .DOC oppure.TXT. L'oggetto e il corpo del messaggio sono casuali, il testo e' prelevato da file .TXT a caso.
Il virus contiene il seguente testo:

Another haughty bloodsucker....
YOU THINK YOU ARE GOD, BUT YOU ARE ONLY A CHUNK OF SHIT

ARF! ARF! I GOT YOU! v1rus: Judges Disemboweler. by: The Judges Disemboweler. written in Malmo (Sweden)

YOUARESHIT

Win32.MTX

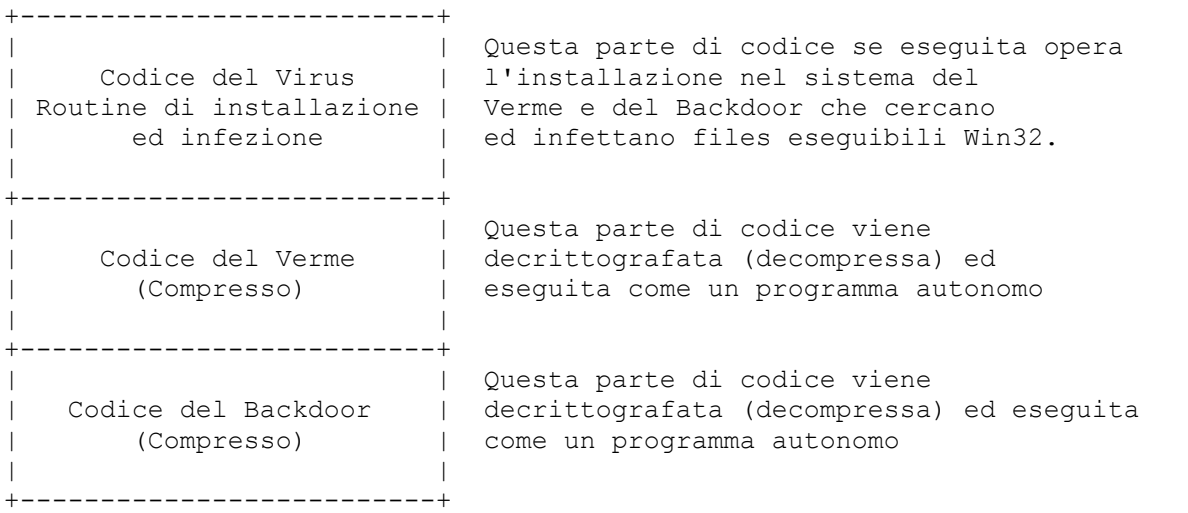
Data scoperta: Settembre 2000

Origine:

Autore: MATRIX

Descrizione:

Win32.MTX è un virus da alta infettività costituito da 3 componenti, il "verme", il "virus" e il "backdoor". Il codice virale infetta i file eseguibili Win32 e si diffonde grazie all'invio di un file attach, contenente il codice infettivo, ai messaggi di posta elettronica. Questa operazione viene effettuata dalla parte del codice denominata worm. Le 3 componenti di Win32.MTX vengono mandate in esecuzione come programma autonomi dalla parte principale cioè dal "virus" che risulta essere in forma non compressa, mentre il "verme" e il "backdoor" risultano essere in formato compresso così da poter sfuggire ai controlli per il rilevamento dei virus di nuova generazione. La struttura di Win32.MTX è simile a quella che riportiamo di seguito:



Il codice del Verme non contiene necessariamente tutte le routine per infettare il sistema durante l'invio come un file attach quando "infetta" un messaggio e-mail. Il file "Verme" è infettato dal virus come un file ordinario quando viene inviato.
Il codice del Virus contiene il seguente testo:

SABIÁ.b ViRuS
Software provide by [MATRiX] VX TeAm: Ultras, Mort, Nbk, LOrd DArk, Del_Armg0, Anaktos
Greetz: All VX guy in #virus and Vecna for help us
Visit us at:
http://www.coderz.net/matrix

Il codice del Verme contiene il seguente testo:

Software provide by [MATRiX] VX team:
Ultras, Mort, Nbk, LOrd DArk, Del_Armg0, Anaktos
Greetz:
All VX guy on #virus channel and Vecna
Visit us: www.coderz.net/matrix

Il codice del Backdoor contiene il seguente testo:

Software provide by [MATRiX] team:
Ultras, Mort, Nbk, LOrd DArk, Del_Armg0, Anaktos
Greetz:
Vecna 4 source codes and ideas

Tecnologie utilizzate nel codice del Virus

Le routine che costituiscono il Virus utilizzano la tecnologia EPO (Entry Point Obscuring) per infettare i files. Questo significa che il virus non modifica l'entry code (l'inizio del codice), ma inserisce un salto alle istruzioni del virus in qualunque punto in mezzo al file infetto. Questo rende le procedure di identificazione e rimozione molto complesse. In questo modo il virus può attivarsi solamente quando il programma infetto va ad eseguire l'istruzione che il codice virale ha modificato (inserito).
Win32.MTX risulta anche essere anche crittografato.
Successivamente il virus installa le sue componenti nella directory di Windows:

IE_PACK.EXE: Codice del verme per modificare il file WSOCK32.DLL
WIN32.DLL: Codice del verme infetto dal virus Win32.MTX
MTX_.EXE: Backdoor

Tecnologie utilizzate nel codice del Verme

Per inviare messaggi "infetti" la componente Verme utilizza la stesse tecnologia che venne utilizzata per la prima volta dal virus Happy99/Ska (Virus/Verme diffuso anche in Italia). Il Verme modifica il file WSOCK32.DLL nella directory Windows\ System appendendo delle componenti del suo codice alla fine del file che permettono di monitorare le routine di invio. Il risultato è che il Verme in questo modo è in grado di controllare tutti i dati inviati da un computer infetto in Internet.
Il Verme, controllato i dati inviati in Internet non permette l'invio di messaggi ad alcuni domini, inoltre intercetta i messaggi inviati duplicandoli ed inserendovi l'attach infetto ed inviandoli ad alcuni indirizzi e-mail. In questo modo, all'indirizzo vittima verranno inviati due messaggi, il primo è il messaggio originale scritto dal mittente, il secondo è un messaggio con soggetto e contenuto vuoti, ma con un attach che ha come nome uno dei file dell'elenco. Il nome del file inviato viene selezionato dal Verme in relazione alla data corrente.

README.TXT.pif
I_wanna_see_YOU.TXT.pif
MATRiX_Screen_Saver.SCR
LOVE_LETTER_FOR_YOU.TXT.pif
NEW_playboy_Screen_saver.SCR
BILL_GATES_PIECE.JPG.pif
TIAZINHA.JPG.pif
FEITICEIRA_NUA.JPG.pif
Geocities_Free_sites.TXT.pif
NEW_NAPSTER_site.TXT.pif
METALLICA_SONG.MP3.pif
ANTI_CIH.EXE
INTERNET_SECURITY_FORUM.DOC.pif
ALANIS_Screen_Saver.SCR
READER_DIGEST_LETTER.TXT.pif
WIN_$100_NOW.DOC.pif
IS_LINUX_GOOD_ENOUGH!.TXT.pif
QI_TEST.EXE
AVP_Updates.EXE
SEICHO-NO-IE.EXE
YOU_are_FAT!.TXT.pif
FREE_xxx_sites.TXT.pif
I_am_sorry.DOC.pif
Me_nude.AVI.pif
Sorry_about_yesterday.DOC.pif
Protect_your_credit.HTML.pif
JIMI_HMNDRIX.MP3.pif
HANSON.SCR
FUCKING_WITH_DOGS.SCR
MATRiX_2_is_OUT.SCR
zipped_files.EXE
BLINK_182.MP3.pif

Tecnologie utilizzate nel codice del Backdoor

Durante l'esecuzione del codice di Backdoor questo crea una nuova chiave del registro di sistema che permette al virus di riconoscere che la macchina è già infetta. Nel caso che la chiave già esista, quindi che la macchina sia già infetta, viene saltata la procedura di installazione. Comunque il codice di backdoor si aggiunge alla lista dei programmi in esecuzione automatica.
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
SystemBackup=%WinDir%\MTX_.EXE

Win95.Marburg

Virus ad azione diretta, polimorfico, crittografato, che infetta i files Win32 .EXE e Screen Saver di Windows 95/98. Il virus infetta in particolar modo i file contenuti nella sua stessa directory e quelli contenuti in C:\Windows e C:\Windows\System. Il codice virale contiene il seguente testo:

Marburg Virus BioCoded By Griyo

Il virus visualizza casualmente sul desktop l'icona di errore di Windows.

Win32.Navidad

Win32.Navidad e' un worm che viaggia attraverso la posta elettronica, allegando ai messaggi il file NAVIDAD.EXE. Quando l'utente esegue il file NAVIDAD.EXE, il worm si attiva, visualizzando un occhio vicino all'orologio e alcuni messagi scritti in spagnolo. Il virus modifica il file di registro di Windows, rendendo impossibile l'esecuzione dei programmi. Il virus per infettare la posta elettronica usa la libreria MAPI, inviando il messaggio infetto a tutti i destinatari presenti.

Win32.Nimda

Win32.Nimda e' un virus/worm win32 che è in grado di viaggiare atraverso la posta elettronica, la rete locale LAN, i web server e attraverso i files .EXE.
Il virus sovrascrive la dll RICHED20.DLL con il proprio codice virale,e crea files con estensione .EML e .NWS contenenti messaggi e news infetti dal virus. Questa dll infetta viene copiata nelle cartelle dove vi sono documenti Word. Quando viene aperto un documento Word, si attiva la RICHED20.DLL attivando il virus.
Il codice virale sfrutta alcuni bachi dei sistemi Microsoft Internet Explorer e IIS. E' consigliabile aggiornare questi software con le relative patch.
Questi buchi pemettono al virus di eseguirsi in modo automatico senza eseguire il file infetto. Il codice virale contiene il seguente testo:

Concept Virus(CV) V. 5, Copyright(C)2001 R.P.China

Win32.Porkis

Si tratta di un virus italiano, che si diffonde attraverso la posta elettronica inviando messaggi infetti allegando un file eseguibile. Il messaggio infetto puo' avevre i seguenti oggetti:

"Storielle.."
"Divertimento assicurato.."
"Leggete urgentemente questa e-mail!! (se avete tempo da perdere)"

con i segeunti corpi:

"dai un' occhiata all' allegato e ti farai due risate ;-)"
"devi assolutamente vedere il file che ti ho allegato."
"guarda l' allegato... ti potrebbe interessare."

Il virus allega uno dei seguenti file infetti:

"bar.exe"
"pippo.exe"
"porkis.exe"

Quando l'utente esegue il file infetto, il virus visualizza le seguenti dialog box di quiz (domande e risposte):

D: "Cosa dice un vettore ad un altro?"
R: "...Scusa, hai un momento?..."

D: "Sai chi è il fratello di Giorgio Armani?"
R: "...Emporio!"

D: "Ti trovi al volante della tua auto e circoli ad una velocità costante.
Alla tua sinistra c'è un precipizio.
Alla tua destra un camion dei pompieri che viaggia esattamente alla tua stessa velocità.
Davanti a te cavalca un maiale visibilmente più grande della tua macchina.
Dietro di te ti segue un elicottero che vola raso terra.
Gli ultimi due, anch'essi alla tua stessa velocità.
Che fai per fermarti?"
R: "...scendi dalla giostra, imbecille!!!"

D: "Gesù ai discepoli: 'In verità, in verità vi dico: y=x^2-4x+7'.
I discepoli commentano un po' fra di loro, poi Pietro si avvicina mestamente a Gesù, dicendogli:
'Maestro, perdonaci, ma non comprendiamo il tuo insegnamento...'
E Gesù, arrabbiato: 'Sciocchi, è una parabola!' "

A questo punto il virus ha infettato il vostro computer creando nella directory di Windows il file DLLMGR.EXE

Il virus Win32.Porkis contiene anche il segeunte testo:

"Oggi non e' mica un giorno fesso come gli altri:
spegnete il computer e uscite,godetevi la vita,abbracciate e baciate la persona a voi piu' cara.

Viva l'amore.
;-) Accadde il 6 settembre "

"Don't Worry: ItsNotDangerous. IloveTheWorldAndThePeople.Bye"

"MARTA VirII by 4nt4R35 (March2002)"

Win95.Roma

Virus Win32 che infetta i files .EXE di Windows, il codice virale non funziona in ambiente Win98. All'interno il codice contiene il seguente testo:

The Roma Virus by Renegade 1999
all Right reserved
Roma a Capitale der monno
This virus is dedicated to Rome

Word Macro Virus

WM/Alliance
WM/Atom
WM/Bandung
WM/Birthday.A:De
WM/Botschaft
WM/CAP
WM/Colors
WM/Concept
WM/Divina
WM/Date
WM/Eva_Herzigova
WM/Gangsterz
WM/HellGate
WM/Italian
WM/MVDK2
WM/Niki
WM/NJ-WMLDK1.D
WM/Rats
WM/ShowOff
WM/Wazzu
W97M/Akuma
W97M/Antismyser
W97M/Arbind2000
W97M/Blaster
W97M/ColdApe
W97M/Ethan.A
W97M/IIS-Modul1
W97M/Kursk
W97M/Machiavelli
W97M/Marker
W97M/Model
W97M/Nono
W97M/Not_a_virus
W97M/Onex
W97M/Smac
W97M/Story
W97M/Thus

WM/Alliance

Contiene 1 macro: AutoOpen, e il seguente testo:

You Have Been Infected by the Alliance

WM/Atom

Questo virus infetta i files di Word 6,7. Il 13 dicembre cancella tutti i files.

Atom.C: Contiene 4 macro: Atom, AutoOpen, FileSaveAs, FileOpen
Atom.E: Contiene 7 macro: Spiff, Citation, AutoClose, Atom, AutoOpen, FileOpen, FileSaveAs.

WM/Bandung

Contiene 6 macro: AutoExec, AutoOpen, FileSave, FileSaveAs, ToolsMacro e ToolsCustomize.

WM/Birthday.A:De

Contiene 2 macro: AutoOpen, Dateispeichernunter. Virus di origine tedesca.

WM/Botschaft

Questo codice virale contiene 3 macro: AutoOpen, Virenlist1 e Virenlist2.
All'interno c'e' il seguente testo:

Ich bin das Super Macro Botschaft f r Deutschland
Ich habe KEINE Schadensfunktion, ich bin als Liebesbotschafter
und bingegen RECHTS gedacht!BITTE last mich am leben
j s NR: 0516047684070397-3
Das S hemein Adolf Hitler wurde am 20.04.1889 in Braunau
(Osterreich) geborenj Das Schmein wurde geboren Hitler,
die feige sar, hay am 30.04.1945 in Berlin Selbstmord begannen,
er wolke Seich der strafe de volkes etziech...

WM/CAP

Questo codice virale contiene 15 macro: Autoexec, CAP, AutoOpen, FileApri, FileOpen, FileSave, AutoClose, FileClose, FileSalva, FileSaveAs, ToolsMacro, FileModelli, FilesTemplates, FileSalvaConNome, FileChiudiOChiudiTutto.
Nella macro CAP Š contenuto il seguente testo:

C.A.P: Un virus social.. y ahora digital
(jqw3rty@hotmail.com)
Venezuela, Maracay, Dic 1996
P.D. Que haces gochito? Nuncaseras Simon Bolivar.. Bolsa!

WM/Colors

Questo codice virale contiene 9 macro: macros, FileNew, AutoExec, AutoOpen, FileExit, FileSave, AutoClose, FileSaveAs, ToolsMacro.

WM/Concept

Questo codice virale contiene 4 macro: AAAZAO, AAAZFS, PayLoad e FileSaveAs.

WM/Divina

Questo codice virale contiene la macro AUTOCLOSE, con il seguente testo:

DIVINA IS THE BEST!
zio Massimo
Oggi e' il compleanno di Divina: devi far festa!
Non continuare o verra' formattato il disco rigido...
Virus 'DIVINA' in esecuzione
ROBERTA TI AMO! . . . Massimo
Hard Disk damaged. Start antivirus ?
Virus 'ROBERTA' is running
Exit from system and low level format are recommended.
Virus Stopped

WM Date

Questo codice virale contiene 1 macro: AutoOpen, e il seguente testo:

Infezione

WM/Eva_Herzigova

Questo codice virale contiene 5 macro: AutoClose, EvaHzg, FileTemplates, TCloseAN e ToolsMacro. Il codice virale crea nel disco fisso il file EVAH.BMP e lo assegna
come desktop di default di Windows. Il file e' una fotografia della top model Eva Herzigova. Il codice virale contiene il seguente testo:

EvaHzg by NAENBGOURSG
231074 - GREECE
Thaks to NEURO
VRD 19-4-1997 VRP A.U.A.

WM/Gangsterz

Contiene 2 macro: Gangsterz, Paradise.

Molto probabilmente dedicato alla canzone Gangster Paradise di Coolio.

WM/HellGate

Questo codice virale contiene 10 macro, e il seguente testo:

Written by Bill_HellGate

WM/Italian

Questo codice virale contiene 3 macro, e il seguente testo:

Word.Macro.Italian VIRUS Written Jan, 1996

WM MVDK2

Questo codice virale contiene 5 macro: Bilbo1, AutoExec, AutoOpen, FileExit, FileSave e il seguente testo:

Anarchy
This macro was generated by MVDK v1.0

WM/Niki

Questo codice virale di origine italiana, contiene 7 macro: AutoExec, AutoOpen, FileApri, FileSalvaConNome, Niki, NNNIIIKKK, StrumMacro, e il seguente testo:

Niki

Il codice virale Niki puo' cancellare files DOC e DLL.

WM/NJ-WMLDK1.D

Contiene 5 Macro: AutoOpen, AutoExex, Archie, AutoNew, AutoClose e il seguente testo:

A Virus from Nightmare Joker's Demolition Kit!
Translated into English by Dark Night.

WM/Rats

Contiene 3 Macro e il seguente testo:

Presence of AVP for winword
AVP for winword is a nice tutorial
(C) 2 Rats Soft.

Rats.A: Contiene le macro: AutoOP, WWUpdated e FileOpen
Rats.B: Contiene le macro: AutoOpen, WWUpdated e DaniloffMuDaK

WM/ShowOff

Contiene 1 Macro (AutoOpen) la quale crea ed esegue il file: C:\RUNME.EXE.

WM/Wazzu

Questo codice virale contiene la macro AutoOpen, con il seguente testo:

Wazzu

W97M/Akuma

Macro virus che infetta i documenti di Word. Il virus casualmente puo' visualizzare dei messagi a video oppure creare il file KILL.BAT che cancella tutti i files dei dischi dissi C:, D:, E:. Il virus crea il file autoexec.kil.

W97M/Thus

Macro virus di Word 97, contiene la macro Document_Open. Il virus si attiva ogni 13 Dicembre cancellando i files del disco C:\.

W97M/Antismyser

Questo virus è una variante del macro virus Thus. Contiene il seguente testo:

This virus is an alteration of a virus wich was designed to delete all files from one's c: drive on DEC 13th.
This code is completely benign.

W97M/Arbind2000

Macro virus che infetta i documenti di Word. Il virus contiene il seguente testo:

arbind2000
An experiment in Macro Programming ;)
Minimun Stealth, No encryption, No payload, No mail replicaton
If you had looked you colud have found and deleted it but....
You probably never knew it was here!

W97M/Blaster

Macro virus di Word, molto probabilmente scritto in Italia, da un virus-writer che si fa chiamare Dream Blaster. Il virus infetta ogni documento di Word che viene aperto/chiuso. Il virus si attiva ogni 17 del mese, inserendo nel file AUTOEXEC.BAT il comando DELTREE per la cancellazione di file e directory dei dischi fissi C:, D: E: e F:. Il virus contiene il seguente testo:

Macro Carrier
Dream Blaster
Minny

Created by Dream Blaster
Minny, you are simply a bitch

W97M/ColdApe

Monkey

E' un macro virus che contiene la macro AutoOpen, infetta ogni documento che viene aperto di Word.
Il virus genera i seguenti files VBScript: happy.vbs, A4.vbs e AVM.vbs. Questi files vengono eseguiti per far viaggiare il virus attraverso la posta elettronica. Il virus contiene il seguente testo:

AVM
Nick "The Love Monkey" Virus Package by ALT-F4 and ALT-F11 for the Alternative Virus Mafia

Dog

Questa e' una variante del virus Monkey modificata in Italia. Contiene il segeunte testo:

cane
Dog

W97M/Ethan.A

Il virus Ethan infetta i documenti di Word 97, contiene la macro Document Close. Quando un documento viene chiuso, il virus lo infetta. Il codice virale oltre a propagarsi, cancella il file C:\CLASS.SYS e crea in radice il file ETHAN.___ (con attributo nascosto e di sistema) dove viene copiato il codice della macro virale. Il virus casualmente visualizza una dialog box con titolo Ethan Frome e con autore: EW/LW/CB.

W97M/IIS-Modul1

Macro virus di Word 97, polimorfico, stealth, infetta tutti i documentii di Word. Il codice virale crea i seguenti file nel disco fisso:

troop.dat
lo.sys
flitnic.drv

W97M/Kursk

Data scoperta: Settembre 2000

Origine: Italia

Autore: 444543A & 4D41434B (DECJ & MACK)

Descrizione:

Macro virus di Word, utilizza un modulo visual basic denominato KURSK, con le seguenti macro: AUTOOPEN e AUTONEW. Questo codice virale è stato scritto in Italia da persone che si fanno chiamare 444543A & 4D41434B (DECJ & MACK). Il virus cancella i programmi degli antivirus e i relativi file di registro degli scudi, creando un file di testo NOME-ANTIVIRUS.txt con all'interno il seguente testo:

"THE KURSK IS DEATH IN THE SEA, BUT ITS GHOST IS IN YOUR COMPUTER".

Il virus si attiva casualmente, cancellando il contenuto del disco A: e creando il file KURSK.TXT con il seguente testo:

```
'*************************************************************************
'*                                        THE KURSK
'*************************************************************************
'* THE KURSK IS A NUCLEAR POWERED SUBMARINE, IT IS DEATH IN THE BARENT SEA

'* WE DEDICATE IT AT YOU FOR REMENBER THE CAPTAIN AND ITS SEAMAN THAT NOW
'* THEY'RE DEATH WHIT THE SUBMARINE
'* THE KURSK IS NOW A MACRO VIRUS WRITTEN BY 4445434A & 4D41434B
'* THIS NEW MACRO VIRUS INFECT THE NORMAL TEMPLATE AND THE WORD'S DOCUMENT

'* THE KURSK DELETE ALL KNOW ANTIVIRUS (NORTON, MCAFEE, PANDA, AVP
'* AND PC-CILLIN).
'*************************************************************************
'*                                     AND MANY MORE ++
'*************************************************************************
```

Analisi eseguita da: Tonello Gianfranco (TG Soft S.a.s.).

W97M/Machiavelli

Questo codice virale e' un macro virus di Word, molto probabilmente scritto in Italia. Il codice virale infetta tutti i documenti di Word. Il virus si attiva nel mese di dicembre, visualizzando il seguente messaggio:

In december of 1513, Niccolo' Machiavelli wrote:
Virtu' contro furore
Prendera' l'arme, e fia el combatter corto;
che' l'antico valore
Nell'italici cor non e' ancor morto

--==<<ITALIAN PoWeR >>==--

MAD T0Y is here!

Machiavelli Word 97 Virus Version 0.1B

W97M/Marker

Il virus Marker infetta i documenti di Word 97, contiene la macro Document Close. Quando un documento viene chiuso, il virus lo infetta. Il codice virale oltre a propagarsi, crea 2 file: NETLDX.VXD e HSF5442.SYS dove viene copiato il log dell'infezione (cioe' chi e' stato colpito).

W97M/Marker.O

L'autore di questo virus si firma con la sigla LSK. Questa variante contiene il seguente testo:

Happy Birthday Shankar-25th July. The World may Forget but we.
Did you wish shankar on his birthday?
Thank you! I Love you. You are wonderfull
You are heart less. You will be punished for this.

Are you suprised

:-D You are marked!

Questi msg sono visualizzati in dialog box di word

I documenti infetti riportano come Autore: LSK, come Oggetto: Birthday e come Commento: Shankar's Birthday falls on 25th July. Don't Forget to wish him.

W97M/Model

Macro virus di Word 97, che contiene il modulo VBA Code con le seguenti macro: AutoNew, AutoOpen, CopyVirCodeToModel, RemoveProtection.

W97M/Nono

Macro virus di Word 97, che utilizza moduli esterni di visual basic V1.BAS in C:\. Il virus crea un ulteriore NORMAL.DOT nella cartella AVVIO di OFFICE e modifica quello contenuto nella cartella MODELLI di OFFICE.

W97M/Not_a_virus

Questo e' un macro virus per Word 97, molto probabilmente e' una nuova variante del virus CAP per Word 6. Il virus contiene 15 macro.
Per maggiori informazioni consultare la scheda del virus:

CAP

W97M/Onex.E

Macro virus di Word, che contiene la macro AutoOpen. Ogni documento aperto sara' infettato dal virus Onex. Il virus utilizza un modulo visual basic denominato HOMER. Casualmente il virus cancella il file C:\WINNT\SYSTEM32\ NTOSKRNL.EXE.

W97M/Smac

Macro virus di Word, contiene le macro AutoOpen e AutoClose. Questo virus crea il file bdoc2.txt, dover registra il codice virale e disabilita il menu Strumenti.

W97M/Story

Questo virus contiene la macro AutoClose. Sfrutta il programma mirc di chat, creando un file di script per inviare un file infetto (C:\windows\story.doc). Questo virus contiene il seguente testo:

Jack-In-The-Box

Worm.Fix2001

Fix2001 e' un verme che viaggia attraverso Internet. Il verme si installa nel sistema, ed intercetta le funzioni di accesso ad internet di Windows. Il verme appare come file Fix2001.Exe (12 Kb) allegato ai messaggi della posta elettronica con oggetto:

"Internet problem year 2000.

e corpo del messaggio:

Estimado Cliente:

Rogamos actualizar y/o verificar su Sistema Operativo para el correcto funcionamiento de Internet a partir del A o 2000. Si Ud. es usuario de Windows 95 / 98 puede hacerlo mediante el Software provisto por Microsoft (C) llamado -Fix2001- que se encuentra adjunto en este E-Mail o bien puede ser descargado del sitio WEB de Microsoft (C) HTTP://WWW.MICROSOFT.COM Si Ud. es usuario de otros Sistemas Operativos, por favor, no deje de consultar con sus respectivos soportes tecnicos.

Muchas Gracias.
Administrador.

Internet Customer:

We will be glad if you verify your Operative System(s) before Year 2000 to avoid problems with your Internet Connections. If you are a Windows 95 / 98 user, you can check your system using the Fix2001 application that is attached to this E-Mail or downloading it from Microsoft (C) WEB Site: HTTP://WWW.MICROSOFT.COM If you are using another Operative System, please don't wait until Year 2000, ask your OS Technical Support.

Thanks.
Administrator.

Il verme contiene inoltre il seguente testo:

RCPT TO:<getmodulehandle
@elrancho.com>
@hotmail.com>
@ciudad.com.ar>

Fix2001
THE REAL KEY TO LIVE A HAPPY LIFE, IS: BE A GOOD MAN.
PARA CONSEGUIR LA VERDADERA FELICIDAD, SE UN BUEN TIPO
.

Il verme, alla sua prima esecuzione, visualizza il seguente messaggio:

Y2K Ready !!
Your Internet Connection is already Y2K, you don't need to upgrade it.
[OK]

Il verme si attiva sovrascrivendo il file C:\COMMAND.COM con un programma trojano che al successivo boot cancella tutti i dati del disco fisso.

X

X97M/Barisada

Macro virus che infetta i folgli elettronici di Excel. Il virus crea il file RMC.XLS nella cartella XLSTART. Il codice virale si attiva il 24 Aprile alle ore 14 visualizzando una serie di domande. Se le risposte dell'utente sono sbagliate, il virus cancella tutte le celle selezionate dei fogli elettronici in uso.

Y

Yankee_Doodle.Login Family

Yankee_Doodle.Login.3045

Virus residente in memoria, infetta files eseguibili con formato tipo COM e EXE. I files infetti aumentano da 3045 a 3061 bytes per l'allineamento del paragrafo. All'interno il codice virale contiene il seguente testo:

LOGIN.EXE
5 and
Insufficoent memory for

Esiste una variante lunga 3052 bytes.

Z

Zero.1174

Virus residente in memoria, crittografato, infetta i files con estensione COM. I files infetti aumentano di 1174 bytes. All'interno il codice virale contiene il seguente testo:

Virus Zero 1997 II Written by D.N.A.
Stealth, AntiDebugger, Advanced Virus

Il codice virale non funziona con la versione del DOS 6, ma sembra funzionare con la 3.31.

Zero-to-0.403.A

Virus residente in memoria, infetta i files con estensione .COM. I files infetti sono sovrascritti dal codice virale, i quali sono lunghi 403 bytes. All'interno il codice virale contiene il seguente testo:

ScUD 1991!

Zipped_Files

Zipped_files e' un cavallo di troia/worm, un programma in formato Win32, che si trasmette attraverso la posta elettronica come file allegato ZIPPED_FILES.EXE lungo 210Kb. Quando il programma viene eseguito, Zipped_files si installa in memoria, ed invia dei messaggi di posta elettronica agli indirizzi di emails trovati in Inbox. Per non farsi notare visualizza a video il seguente messaggio:

Cannot open file: it does not appear to be a valid archive. If this file is part of a ZIP format backup set, insert the last disk of the backup set and try again. Please press F1 for help.

Per installarsi nel sistema di Windows, il worm copia se stesso nella directory di Windows con il nome _SETUP.EXE e nella directory di WINDOWS\SYSTEM con il nome di EXPLORE.EXE.
Per essere eseguito ogni volta che parte WINDOWS, il virus modifica il file WIN.INI. Il worm modifica la riga "run=" in uno dei seguenti modi possibili:
run=_setup.exe
run=C:\WINDOWS\SYSTEM\EXPLORE.EXE

Il worm ora è attivo in memoria, per controllare la sua presenza premere i tasti CTRL-ALT-DEL e verificare nella lista dei task la presenza di almeno uno dei seguenti nomi: Zipped_files, Explore o _setup.

I messaggi di posta elettronica infetti, avranno il seguente corpo:

Hi nome della persona !
I received your email and I shall send you a reply ASAP.
Till then, take a look at the attached zipped docs.
Sincerely.

Con in allegato il file worm Zipped_files.exe

Il worm Zipped_files è molto pericoloso, perché sovrascrive tutti i files con estensione: .C, .H, .CPP, .ASM, .DOC, .XLS, .PPT. Sovrascrive in particolar modo i documenti di Office, cancellando complentamente il loro contenuto. I files vanno recuperati dalle copie di backup.

Index

Andromeda.1140
Anthrax
Anticad Family
Anticmos
Antiexe
Antimon.1450
Appendix A
Arbind2000
ARCV Family
Arianna Family
AT Family
Atomic Family
Atomic_comp.425
Austr_Parasite Family
AustrPar1169
AustrPar338
AustrPar369
AustrPar377
AustrPar440
AustrPar482
AustrPar491
AustrPar550
AustrPar615
AustrPar635
AustrPar762
AustrPar784
AustrParVGA
Avalanche.2818

B

B
B1
Backfont.765
Bad_Boy.1000
BAD_BRAINS.554
Bad_Bytes.109
Badtransb
Barisada
Barrotes.1310
Beethoven
BetaBoys.615
Bit_Addict.477
Blaster
Blink Family

Blinky.1302
Blood.418
Bloodlus
Bloody_Warrior
Boot.388
Boot.446
BootEXE.451
Burger Family
Burglar.1150
Burma Family
Butterfly Family
BW Family
Bye
ByWay

C

C
Carzy.9849.B
Cascade Family
Cereal
Chinese_Fish
cih
CK.183
Clonewar.Family
Coib.702
ColdApe
COMVIRUS
Creeper.252

D

D
Danish_Tiny.Brenda
Dark_Avenger.2000.Traveler
DarkMan Family
Darth Family
Datalock.920
Day10.674
Deathboy.937
DelCMOS.B
Devils_Dance
Diamond Family
Die_Hard_2
DM Family
Dream_Man
DY.278

E

E
Ear.1024
Elephant_2.Trojan
Eli
Enciclopedia Virus
Enola.1864
Epbr
Ethan
ExcelMAcro
Exe252.252
Explosion.1000

F

F
Faerie.276
Fallen_Angel.335
Fax_Free Family
Fix2001
Flagyll Family
Form
Frethem
Froll
Fumble.867

G

G
Garibaldi.1845
Gdynia
Genesis Family
Gergana.182
Gippo.Stunning_Blow
Giprov
Glossary
Goldbug
Golgi.385
Grog Family
Grog.1089.GPE
Grog.304
Grog.377
Grog.4_0
Grog.480
Grog.660
Grog.Aver_Torto

Grog.Bog.233
Grog.Crackers.Inc
Grog.Dewy.MtE.0_90
Grog.Dream
Grog.ERiluttanza
Grog.IlCuoco
Grog.Joe_Anthro
Grog.Lor
Grog.MiAmi.GPE
Grog.Nocciola
Grog.NTA
Grog.Outwit_C
Grog.Public
Grog.Razor
Grog.Wildcard
Grunt Family
Gullich

H

H
Happy99
HappyTime
HDKiller
HideNowt
HiGuy
HLLO Family
Howard.967

I

I
Icelandic.1618.A
IIS_modul1
ILOVEYOU
Index
Intruder Family
Invisible_Man
Italian_Boy
Italy
IVP.Walky_Replico.462

J

J
Jeepwarz
Jerusalem Family
Jerusalem.1244

Jerusalem.1588
Jerusalem.1808.Apocalypse
Jerusalem.1808.CT.Subzero
Jerusalem.1808.Frere
Jerusalem.1808.Phenomen
Jerusalem.1808.sUMsDos.AR
Jerusalem.1808.vari
Jerusalem.998
Jerusalem.Barcelona
Jerusalem.Sunday
Jerusalem.Sunday_II
Jerusalem.sURIV_3
Jumper
Junkie.1027

K

K
Kampana
Knight_Errant
Kriz
Kursk

L

L
Laroux
Leprosy Family
Lilith
Lithium
Lordzero
Lost_Diskette

M

M
Maaike
Machiavelli
Magistr
Major.1644
Maltese_Amoeba
Marauder.860
marburg
Marker
Mary
Marzia Family
Milan Family
Model

Moloch
Mombasa
Mr_Virus
MtE Family
MTX
MTZ Family
Murphy Family
Mururoa

N

N
Napoli_Trojan.6032
Navidad
Netbus
New_ExeBug
Nimda
No_of_the_Beast
nono
Not_a_virus
November_17th Family
Number_1.AIDS

O

O
Old_Yankee.Enigma
One_Half.3544
Onex
OnTheFly
Ooops.368
Opasoft
Orion Family

P

P
Parity_Boot
Peace_Keeper.MCG.0_31
Peach
Phalcon.Cloud.1117
Pieck.4444
Pixel Family
Pizelun
PKTROJAN
Polifemo Family
Porkis
Prague.Backtime

PrettyPark
Protipus
PS_PC Family
Pulce.1840

Q

Q
Quox

R

R
Rape.747
Rebelbase
Riot.426
Ripper
Roma
RPS2
Run_error_504D_5658

S

S
S_E_K
Sampo
Satan.612
Satirycon Family
Screaming_Fist.Stranger
Serena
Slam_Tilt.703
smac
SMEG
Snow
Spirit
Star_Dot Family
Stealth_Boot.C
Stoned Family
story
Suomi
Susan
Swedish_Disaster.I
Swiss_Boot
Sylvia.1332

T

T
Taiwan.743.A
Tanatos

Tenbytes.1554
Tequila
Thanksgiven
THUS
Tic.109
TOPA Family
Topic1
Topic1
Torpino
TPE Family
TPTG.0_02
Triplicate
Trivial Family
Trojan
Trojector.1561

U

U
Unashamed
UVR

V

V
V2Px Family
Varcella.749
VCL Family
Viaggio
Vienna Family
Virdem.1542
Vota_DC
VSign

W

W
WelcomeB
WM Alliance
WM Atom
WM Bandung
WM Birthday.A De
WM Botschaft
WM CAP
WM Colors
WM Concept
WM Date
WM Divina

WM Eva_Herzigova
WM Gangsterz
WM HellGate
WM Italian
WM MVDK2
WM Niki
WM NJ WMLDK1.D
WM Rats
WM ShowOff
WM Wazzu
Word Macro
Word6

X

X

Y

Y
Yaha
Yankee_Doodle.Login.3045

Z

Z
Zero to 0.403.A
Zero.1174
Zipfiles

Glossary

Appendix A

Insert Appendix A text here