Enciclopedia Virus

List of virus

A

B

Referenze

Indice

Glossario

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 vodice 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
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

Index

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

A

A
Abal
Acid.670
Ada
Akuku Family
Albania Family
Anarky.628
Andromeda.1140
Anthrax
Anticad Family
Anticmos
Antiexe
Antimon.1450
Appendix A
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
E
Enciclopedia Virus
G
Glossary
I
Index

Glossary

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

Appendix A

Insert Appendix A text here