

KnownViruses

COLLABORATORS

	<i>TITLE :</i> KnownViruses		
<i>ACTION</i>	<i>NAME</i>	<i>DATE</i>	<i>SIGNATURE</i>
WRITTEN BY		August 22, 2024	

REVISION HISTORY

NUMBER	DATE	DESCRIPTION	NAME

Contents

1	KnownViruses	1
1.1	Main	1
1.2	File Viruses	1
1.3	Boot Viruses	2
1.4	AmixHack	7
1.5	AmixHackDOCS	7
1.6	AmixHackFILEIDDIZ	8
1.7	BootShop	9
1.8	Xtruder3.5	9
1.9	Drive Music	9
1.10	uNHaPPY NeaR NeW YeaR SuMMeR 97	9
1.11	PATCHMUIREADME	10
1.12	BEOL4Installer	10
1.13	EBOLA	10
1.14	HitchHiker411	11
1.15	HitchHiker423	11
1.16	BBSTraveller	11
1.17	ScanEbola	12
1.18	SEBOLA97DOC	12
1.19	ZIB	13

Chapter 1

KnownViruses

1.1 Main

BootBlock Viruses

File Viruses.

1.2 File Viruses

AFFE

Aram-Dol

AX-Fucker

AmixHack

BEOL4 Installer

BBS Traveller

BGS9

Biomechanic 6

BOKOR 1.01

BOKOR 1.05

BOKOR 1.06

BOKOR 1.1

BootShop Installer

Drive Music Joke

EBOLA

Happy New Year 96

Happy New Year 97

HitchHiker 2.01

HitchHiker 4.11

LiSA-Fuckup 3.0 [ScanEbola 97]

TimeBomb 0.9

Saddam 1

uNHaPPY NeaR NeW YeaR SuMMeR 97

VirusMaker1.0

Xtruder 3.5 Trojan

ZIB

1.3 Boot Viruses

AccessForbidden2

AccessForbidden

AEK

AIDSHIV

AlienNewBeat

AmigaFreak

AssProtector10

AustralianParasite

BamigaSector1

BlackFlash20

BladeRunners

BLF

Blizzard10

BlowJob

BootAIDS

Butonic11

ByteBandit1

ByteBandit2

ByteBandit3

ByteBandit4

ByteVoyager1

ByteVoyager2

ByteWarriorDASA

ByteWarriorFastLoad

CCCP

CheaterHijacker

ClaasAbraham

CLIManager

Clist

Clonk

COBRA

CodersNightMare
CopperBoot
CrackerExterminator
DAG
DAT89
DATACrime
DenizUnal
Destructor
Devils
DigitalEmotions
DigitalLife2
Disgust
DiskDoktors
DiskFurunkel
DiskGuard
DiskHerpes
DiskTerminator
DivinaExterminator1
DrMosh2
DrMosh
Eleni
Executors
Extreme
Fast1
Fast2
FastEddie
FICA
Forpib
Frity
FutureDisaster
Gadaffi
GeneStealer
GlasNost
Graffiti
Gremlin1
GXTeam
Gyros
HCS1
HCS2

Heil
Hilly
Hoden3317
ICE
Incognito
IndianaJones
Infector
Influenza
IngerIQ
INGO
Irak3
JITR
Joshua1
Joshua2
Julie
Kauki
Kefrens1
LADSVirusHunter
LamerExterminator1
LamerExterminator2
LamerExterminator3
LamerExterminator4
LamerExterminator5
LamerExterminator6
LamerExterminator7
LamerExterminatorDecoded
LameStyle
LittleSven
LoveMachine90
Loverboy
LSD
Mad2
MegaMasterMGM89
Mexx
MG
MicroSystems
MorbidAngel
MU55
MU61

NastyNasty
NoBanditAnymore
NorthStar1
NorthStar2
NorthStarChecker
Nuked007
Obelisk1
Obelisk2
ObeliskFormat
Opapa
Paradox1
Paradox2
Paramount
Paratax1
Paratax2
ParataxIII
PayDay
PentagonCircle1
PentagonCircle2
PentagonCircle3
PerverseI
Plastique
PowerBomb
RedGhost
Rene
Revenge12G
RevengeBootLoader
Riska
Sachsen1
SaddamHussein
SaoPaulo
Scarface
SCA
Sendarian
SherLock2
SHI
SinisterSyndicate2
SinisterSyndicate
Sonja

SS
StarLight2
StarLightWarhawk
SuicideMachine
Suntronic
SuperBoy
SupplyTeam
SwitchOff
SystemZ30
SystemZ40
SystemZ50
SystemZ51
SystemZ53
SystemZ54
SystemZ61
SystemZ64
SystemZ65
TaiPanChaos
TaiPanLameBlame
Target
Telstar
Termigator
TFCRevenge
TimeBomb10
TNK
TomatesGentechnic20
TomatesGentechnic
Traveller10
Triplex
TTS
Turk
TwinzSantaClaus
ULDV8
UltraFox
Unknown1
Vermin
VIPHS
VirKill2
Virus42

VirusFighter
VirusHunter
VirusSlayer10
VirusV1
VKill10
WarHawk1
WarsawAvenger
ZAccess10
ZAccess20
ZAccess30
_16BitCrew
_2001

1.4 AmixHack

Creation Date : 14th June 1995

Distribution : DEC-SCPLZX (9645 bytes)

AmixHack.DOC (1721 bytes)

AmixHack0.Exe (8348 bytes)

AmixHack1.Exe (8348 bytes)

AmixHack2.Exe (8348 bytes)

AmixHack3.Exe (8348 bytes)

AmixHack4.Exe (8348 bytes)

DEC-SCP.FILEID.DIZ (884 bytes)

A simple BBS trojan attacking the Ami-Express system, which appears to be written in AMOS Basic. The 5 generations are intended to be run on a specific nodes. Ie, AmixHack2.Exe hacks node 2.

1.5 AmixHackDOCS

sCOOP v1.0 aMIeX hACKER bY dECODER/wSD/rAN^cDV/sQH^eXC^7LL

Ok...i have incuded this files in this archive:

+++++

AmixHack0.Exe

AmixHack1.Exe

AmixHack2.Exe

AmixHack3.Exe

AmixHack4.Exe

AmixHack.Doc

File_ID.DIZ

Well...you wonder how to use it and how it works?..well...ok...first
of all you gotta be nice to the sysop..blah...lets see.....

AmixHack0.Exe Is for Hacking If Serial Node is On Node 0

AmixHack1.Exe Is for Hacking If Serial Node is On Node 1

AmixHack2.Exe Is for Hacking If Serial Node is On Node 2

AmixHack3.Exe Is for Hacking If Serial Node is On Node 3

AmixHack4.Exe Is for Hacking If Serial Node is On Node 4

Ok...you gotta fool the sysop to run the file on his machine.....;(

So you ask if he has a library named "TTA.LIBRARY" ...if he does say
that you want it.....but why?...hehe...

what Scoop does:

1. Deletes Caller Log so that sysop won't see that you have uploaded
the file.

2. Copies User.Data to Libs:TTA.Library

3. hmm...nothing more!

Hehe..that wassn't much he?..well...

What you gotta do:

1. Rename one of the files (for right node) and get sysop to run it.

(Nothing happens when he runs it...say that is broken then..he!)

2. Call back within a week....ask if he has a library called

TTA.Library...(it should be in he's libs:)...you get it...but

thats he's User.Data!!!...Well...now you gotta use a /X user data

password hacker....;(....next time login as the sysop!

If you got some questions contact me on a Norwegian Elite Board.

1.6 AmixHackFILEIDDIZ

.....

. _____ .

.J||||.

.|_|_|O|O|O|.

.|_|_|_|_|.

.|_|_|_|_|_|_|_|....

.....

.....sCOOP V1.0 - /X hACKER.....

.....

.....mADE bY dECODER.....

.....

.....

.....DO NOT RUN ON YOUR HD!.....

1.7 BootShop

This old program will allow users to select custom bootblocks, and install them onto disks. It also has a collection of viruses which can be installed if you get some questions correct. These questions are not too difficult, and any idiot could get access to some viruses.

1.8 Xtruder3.5

In version 3.5 of this virus killer is a routine which when a cracked keyfile is found, will delete some files. This routine could possibly also get triggered if the file got corrupted. Such routines should never belong in a viruskiller, and this is classed as a trojan.

1.9 Drive Music

Not intended as a malicious program, but this could panic some users into doing something stupid, like resetting while they have unsaved data or something. I don't like 'Joke' programs like this, so this is added to the brain.

1.10 uNHaPPY NeaR NeW YeaR SuMMeR 97

Creation Date : 19th August 1997

Distribution : MUI020.lha (2709 bytes)

filecomment `from 193.212.237.22'

[This seems to be some shareware site]

File Sizes : MUI_Patch (Executable) 2696 bytes.

ReadMe.txt 555 bytes.

Stealth : Aborts if Snoopdos is running.

This is supposed to be a program which patches muimaster.library to use 68020 instructions. And allegedly, it was written by me. Of course, I did not write this, and the program does not do what it describes. The executable is a REXXMasher compiled AREXX script, which seems to create a muimaster.library in the T: assign, which is the main virus. On all my systems, the virus crashed after making this file.

The muimaster.library file is also as bug ridden as it's dropper. It patches the LoadSeg() vector, with a routine which loads the file, and then adds itself to the end of the first code hunk. However this patch is so

buggy it never even managed to reopen the file to infect it on my systems.
This seems to be a reprogramming of a 'Happy New Year' link-virus, as the self-identification and infection preconditions match, it also has a bugged LoadSeg() patch.
Evidently, this is the work of a lamer.
Now if only I could get my hands on the fool who made this rubbish...

1.11 PATCHMUIREADME

```
=====
Patch MUI 020+ version 1.1 by DJ (you know who!)
=====
*****

Usage:
*****

Simply unpack the archive into a directory and run the MUI_Patch program
which will then try to locate MUI:muimaster.library and make the necessary
modifications/optimizations to the libraries internals for an increase in
performance of some routines upto 35%

...Now when is Stefan going to release a truely written 020+ MUI???
```

1.12 BEOL4Installer

I couldn't get this to run on my system, as the executable was damaged.
There was also an Aztec-C source code distributed with it, which could be compiled, but I'll add recognition for any others in the wild as and when I see them.

1.13 EBOLA

Yawn, Yet another lame link-virus.
Adds code to the first code hunk, and changes a \$4EAE to a \$4EBA to jump into it's own code when the infected program is run.
Infects LoadSeg() vector, and contains a routine to remove itself cleanly from memory, which FVK exploits.

1.14 HitchHiker411

Tries to look like a decruncher with the string `CopyCat Decruncher 1.01` in the beginning of the code. Don't be fooled, this is something more sinister. The strings `FLK!` and `-TRSi=` can also be found, obviously trying to make out that it was written by Markus Schmall (Author of Virus Workshop) This is of course complete bullshit.

It infects the `exec.library PutMsg()` vector by writing a random Trap #n opcode over the first word of the Jump-table, and writing the address of a trap-handler into the appropriate entry of the vectorbase.

A process will be created, with a random name created from scanning the `exec/liblist`, so it depends on what is currently loaded. It skips the trailing `.library` off the name. This process simply continually reinstalls the patches.

The file infection is unlike most Link-viruses, in that this one includes the original file in it's own datahunk.

Doing a directory of infected files returns the length of the uninfected files.

1.15 HitchHiker423

Pretty much the same as [HitchHiker 4.11](#) In that it still patches `PutMsg()` in the same way, and still infects files the same way. The only main difference is that this one also patches `LIB_OPEN()` from `bsdsocket.library` as an extra way to infect files. This library will be created in memory if you run the MIAMI TCP/IP program, and maybe AmiTCP.

1.16 BBSTraveller

Simple link-virus, seems to be a clone of Ebola, hence most people calling it EBOLA-II, The only main difference being the addition of a routine which installs a reset-routine which changes the `exec.library DoIO()` vector to trash the first disk it boots.

The Virus refuses to install itself if it finds `VirusZ`, `Virus_Checker`, `SnoopDos SetFunktionManager`, or another killer which installs a string `TRSI` (Probably something by M. Schmall)

This virus patches a series of functions, and if certain arguments are passed to them, the virus removes itself. FVK exploits this routine in its `mem-clean`.

I couldn't get this virus to infect memory on my system, but I've written what I think to be a working `mem-clean` routine, including a cleaner for the reset-routine. Unfortunately, the damage done by the formatter cannot be repaired.

1.17 ScanEbola

Creation Date : 9th October 1997

Distribution : sebola97.lha

file_id.diz (57 bytes)

ScanEbola97.info (857 bytes)

ScanEbola97/**ScanEbola97.readme** (872 bytes)

ScanEbola97/ScanEbola97 (7004 bytes)

This showed up on a Danish BBS and it was claimed that it was a killer for the EBOLA 97 Virus. To this date (15.10.97) This virus has not showed up.

It is also claimed in the docs that a copy of the virus has been sent to Virus Help Team DK, but Jan Anderson has received no such file.

The file will delete your SYS: partition, and relabel it

`LiSA FUCKUP v3.0'

Further analysis will be performed at a later date.

FileID_Diz

ScanEbola97: Scans your hard-drive for the Ebola97-virus.

1.18 SEBOLA97DOC

ScanEbola97 is a little tool I wrote to check if your computer is infected with the new Ebola97-virus. The virus isn't detected by any VirusKiller *YET*, so use this tool meanwhile.

Start the tool in your shell without parameters and it will automatically start to scan your sys:-assign, because the Ebola97-virus will only infect the boot-disk.

When ScanEbola97 finds an infected file, you will be noticed. The virus can't be removed, so you'll have to delete the infected file by hand (ScanEbola97 will NOT do this for you...)

IMPORTANT:

If ScanEbola97 found infected files, delete them and turn the computer ****OFF****, because the Ebola97 stays resident in memory and will start infecting files again!

I have sent the Ebola97-installer with description of the Ebola97 to Virus Help Team Denmark.

MaXOZ/TLK

the original 'spatch' with the installer version. So there for, take care when ever you meet the 'spatch' in an archive, and if the size is 16716 bytes, don't use it.

Here is some info about this archive:

Archive name...: opus566p.lzx

Archive size...: 138502 bytes (LZX packed)

Infector name...: spatch

Infector size...: 16716 bytes (not packed)

Archive info...: Directory Opus 5 Magellan version 5.66 to 5.661

Upgrade Patch. (fake archive)

At ths time, no viruskiller will find this infector. But some of the anti-virus programs, will find and remove this 'ZIB' virus:

VT v3.01 - By Heiner Schneegold

FastVirusKiller v1.12 - By Dave Jones

AntiBeol v1.34a - By Gideon Zenz

Killanother1 v1.0 - By Harry Sintonen.

Thanx to Jakob Anderson for sending us this archive.

Regards....

___ VirNet...: 9:451/247.0

___ /// Jan Andersen FidoNet.: 2:237/38.100

\\// ----- AmyNet...: 39:140/127.100

\\XX/ VIRUS HELP TEAM DENMARK E-Mail...: vht-dk@post4.tele.dk

<http://home4.inet.tele.dk/vht-dk/>

.. . oo OOOOOOOO oo . .. Virus Help Team Denmark .. . oo OOOOOOOO oo . ..

~~~~~

Please support us with all the new and old virus that you find so that we can support the antivirus programmers. You are very welcome to mail to our support BBS (+45 6381 8005).

Every Amiga Virus that is uploaded to Virus Help Team Denmark's BBS, will be send directly to the anti-virus programmers all over the world.

Every PC Virus that is uploaded to Virus Help Team Denmark's BBS will be send to Virus Test Center, in Hamburg, Germany.