Trojan, Virus, Worm and Backdoor Exploit

MTX – A Combinational Malware

By
Hamid pirooz

2/26/01
Level Two GCIH Practical Assignment

Exploit Details:

Name:
MATRIX (MTX)

Variants:
Troj_MTX.A, I-Worm.MTX, MTX_.exe, PE_MTX, W32/Apology , W95.Oisdbo, W32/Apology-B, W32/MTX@mm, W95.MTX, MTX.A, Win95.MTX, W32/MTX
There are many other names it will use with the following extensions: (.txt, .pif, .txt.pif, .scr, .jpg, .jpg.pif, .mp3, .mp3.pif, .exe, .doc, .doc.pif, .avi, .avi.pif, .html, .html.pif). It uses *.pif extension to hide itself.

Operating System:
Windows 95/98/ME/NT/2000

Protocols/Services:
SMTP, TCP/IP / Trojan, Backdoor, Virus, Worm

Brief Description:
This is a Trojan-virus-worm-backdoor spreading under Win32 systems. The virus infects Win32 executable files, attempts to send e-mail messages with infected attached files, as well as installs a backdoor component to download and spawn "plugins" on an affected system. The worm caused a global epidemic from September--October 2000.
The malicious code has an unusual structure. It consists of three different components that are run as stand-alone programs (Virus, e-mail Worm and Backdoor). The virus is the main component, and it keeps the worm and backdoor programs in its code in compressed form. While infecting the system, the virus extracts and spawns them.

Protocol Description:
This PE Trojan is sent as an email attachment from systems infected with TROJ_MTX.A. PE_MTX.A creates a modified copy of WSOCK32.DLL in order to allow it access to all internet traffic and intercept SMTP.

Windows Sockets, or **Winsock**, is a .DLL which allows applications to talk over a network, usually the Internet. The .DLL is usually called WINSOCK.DLL. Most

Winsocks speak TCP/IP. WSOCK32.DLL is a thunk to let Win32s programs use WINSOCK.DLL and it comes with Win32s. You need this if you are running a 32 bit program with Trumpet or other 16 bit Winsock. It doesn't do anything except let Win32s programs call Winsock. If you are running NT or Win95, you want to use the built-in networking, not a second TCP/IP stack.

Then the the registry is modified so that MTX_.EXE is executed in the next boot up and acts as a Client application (backdoor). The Trojan creates a copy of the WSOCK32.DLL as WSOCK32.MTX and modifies this to intercept SMTP. The Trojan patches the functions SELECT(), SEND() and SENDTO() in order to do this.

In addition, the replacement Wsock32.dll monitors the location of HTTP requests (web-browsing), and the address of e-mail recipients. The program will crash if it detects that the user is attempting to either access an anti-virus site or send e-mail to an anti-virus company.

Description of Variants:

Win95. MTX is a 32-bit virus that has worm-like behavior and drops a trojan. This PE Trojan is sent as an email attachment from systems infected with **TROJ_MTX.A**. **PE_MTX.A** creates a modified copy of WSOCK32.DLL in order to intercept SMTP. When virus is run it directly infects PE files in the windows and system directory. These files may have the extension EXE, SCR and DLL. The W95.MTX virus has not been widely spread in the Untited States; most of the infections have been in Europe and Asia. This virus, however, does have the potential to spread quickly. It infects Windows program files, such as Explorer.exe. When this happens, Windows might stop running. This virus also has the capability of blocking the Internet connections to Web sites of antivirus vendors.

Happy99 is a Win32 based Trojan program. When this program is executed it will display some fireworks. Apart from the fireworks display this program will do some other activity in the background without the user's permission. Happy99.exe copies itself into the Windows system directory as SKA.EXE and puts another file, SKA.DLL in the same directory. It then backs up WSOCK32.DLL (the system library that provides Internet connectivity to Windows) as WSOCK32.SKA and modifies the original WSOCK32.DLL to use SKA.DLL when sending email or posting news.

Happy99 does not have the virus and backdoor capabilities of the I-Worm.MTX.
For information contact :as/virus/e-mail/happy99/

W95.Hybris.gen worm

W95.Hybris.gen is worm that spreads as an attachment to outgoing email messages. When the worm is executed, the Wsock32.dll file is modified or replaced. This enables the worm to attach itself to all outbound email.

See also the references section for sites containing information on these codes.

How the exploit works:
This is a Trojan with virus-worm-backdoor functionalities spreading under Win32 systems (Windows 95/98/ME/NT/2000). This PE Trojan is sent as an email attachment from systems infected with TROJ_MTX.A. The virus infects Win32 executable files, attempts to send e-mail messages with infected attached files, as well as installs a backdoor component to download and spawn "plugins" on an affected system. The virus has an unusual structure. It consists of three different components that are run as stand-alone programs (Virus, e-mail Worm and Backdoor). The virus is the main component, and it keeps the worm and backdoor programs in its code in compressed form. While infecting the system, the virus extracts and spawns them.

When the virus is run, it infects files in the Windows directory. Win95.Mtx then unpacks and drops its worm component twice in the Windows directory as files with the following names:

"Ie_pack.exe"
and "Win32.dll"

A trojan file named "Mtx_.exe" is also dropped in the Windows directory, and the following registry key (which runs the trojan each time Windows reboots) is created:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\SystemBackup = \MTX_.EXE

The trojan attempts to download and run files from a website which may contain other malicious programs. Next, the worm part (PE_MTX.A) is launched and creates a modified version of Wsock32.dll. It then overwrites the wininit.ini file with its own copy. (The wininit.ini file is only present on the system when required. When the system starts, commands in this file will be carried out and the file will be deleted). The virus' wininit.ini file contains commands to replace the original version of Wsock32.dll file with its own when Windows reboots. Once the original version is replaced, the new Wsock32.dll intercepts information being sent (by the send() function) from the computer to the network. The Trojan creates a copy of the WSOCK32.DLL as WSOCK32.MTX and modifies this to intercept SMTP. The Trojan patches the functions SELECT(), SEND() and SENDTO() in order to do this.

If it detects that an e-mail is being sent, it will immediately send a second e-mail to the same recipient. The second e-mail has no subject and no body; merely an attachment which is randomly picked from a list of names within the code.

In addition, the replacement Wsock32.dll monitors the location of HTTP requests (web-browsing), and the address of e-mail recipients. The program will crash if it detects that the user is attempting to either access an anti-virus site or send e-mail to an anti-virus company. It detects this communication by searching for substrings and strings in the domain name from the a list it contains.

The worm code does not contain all the necessary routines to infect the system, being sent as attachment in an infected e-mail message (see below). The worm needs "help" from the virus component, and is sent as being infected by the virus (the worm file is infected by the virus as an ordinary file and then sent). The reason for such a method is unclear, but probably the components were written by different people.

When the attachment is double clicked, the virus is executed. It drops three files, IE_PACK.EXE, WIN32.DLL (which are just a copies of itself) and MTX_.EXE (which is the PE virus) in the windows directory. These files are hidden.

Then the virus modifies the registry so that MTX_.EXE is executed in the next boot up and acts as a Client application (backdoor). The Trojan creates a copy of the WSOCK32.DLL as WSOCK32.MTX and modifies this to intercept SMTP. The Trojan patches the functions SELECT(), SEND() and SENDTO() in order to do this.

It also creates the following registry entries:

HKEY_LOCAL_MACHINE\Software\(MATRIX)
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\Run\ SytemBackup “c:\windows\mtx_.exe”

It modifies WININIT.INI to call WSOCK32.MTX instead whenever the original WSOCK32.DLL is called. It infects Win95 and 98 PE files (EXE and SCR) as well as DLLs. It does not have a destructive payload.

The Virus component contains the text strings:
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

The worm component contains the text strings:
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

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

The Virus Component:
The virus uses "Entry Point Obscuring" technology while infecting a file. That means the virus does not affect the file at its entry code, but places a "Jump Virus" instruction somewhere in the middle of the file code section to make detection and disinfection

procedures more complex. As a result, the virus is activated only in case a corresponding affected program's branch receives control.

The virus is also encrypted, so first of all, it decrypts itself when its code gains control. The virus then looks for the necessary Win32 API functions by scanning the Win32 kernel. To do this, the virus tries the Win9x, WinNT and Win2000 addresses.

The virus then looks for anti-virus programs active in the system and exits in case any of them are detected. The list of anti-virus programs the virus pays attention to appears as follows:

AntiViral Toolkit Pro
AVP Monitor
Vsstat
Webscanx
Avconsol
McAfee VirusScan
Vshwin32
Central do McAfee VirusScan

Next, the virus installs its components to the system. They are decompressed installed to the Windows directory and then spawned. There are three files created, and they have a hidden attribute set and the following names:

IE_PACK.EXE - pure Worm code
WIN32.DLL - Worm code infected by the virus (as "Infected File" above)
MTX_.EXE - Backdoor code

The virus then infects Win32 executable PE EXE files in current, temporary, and Windows directories, and then exits.

The Worm component:
To send infected messages, the worm uses technology that for the first time was found in the "Happy" Internet worm (a.k.a. Happy99, a.k.a. SKA).

The worm affects the WSOCK32.DLL file in the Windows system directory by appending a component of its code to the end of the file and hooking the "send" WSOCK32.DLL routine. As a result, the worm then monitors all data that are sent from an affected computer to the Internet.

Usually the WSOCK32.DLL file is in use at the moment the worm starts, and it is locked for writing. To avoid this, the worm uses a standard method: it creates a copy of the original WSOCK32.DLL with a WSOCK32.MTX name, affects that copy and then writes "replace original file with infected" to the WININIT.INI file:

```
NUL=C:\WINDOWS\SYSTEM\WSOCK32.DLL
C:\WINDOWS\SYSTEM\WSOCK32.DLL=
D:\WINDOWS\SYSTEM\WSOCK32.MTX
```

where "C:\WINDOWS\SYSTEM" is the name of the Windows system directory and may differ depending on the name of the Windows directory installed.

Upon the next reboot, the infected WSOCK32 replaces the original one, and the worm gains access to data that are sent from the infected machine. The worm pays attention to Internet sites (Web, ftp) that are visited as well as to e-mail messages that are sent from a computer.

The virus prevents the ability of visiting several Internet sites, as well as disables sending messages to the same domains (they are anti-virus domain names). The virus detects them by four-letter combinations that appear as follows:

nii.
nai.
avp.
f-se
mapl
pand
soph
ndmi
afee
yenn
lywa
tbav
yman

The worm also does not allow sending e-mail messages to these domains:
wildlist.o*
il.esafe.c*
perfectsup*
complex.is*
HiServ.com*
hiserv.com*
metro.ch*
beyond.com*
mcafee.com*
pandasoftw*
earthlink.*
inexar.com*
comkom.co.*
meditrade.*
mabex.com *
cellco.com*
symantec.c*
successful*
inforamp.n*
newell.com*
singnet.co*
bmcd.com.a*
bca.com.nz*
trendmicro*
sophos.com*
maple.com.*
netsales.n*
f-secure.c*

The worm also intercepts e-mail messages that are sent and attempts to send a duplicate message with an infected attachment to the same address (the same as "Happy" worm does). As a result, a victim address should receive two messages: first, is the original message, written by a sender; second, comes a message with an empty subject and text and an attached file that has one of the names that are selected by the worm depending on the current date:

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

As an attached file, the worm uses the WIN32.DLL file that has been dropped by the virus component.

Note: the worm does not drop the WIN32.DLL file, but uses that file to attach it to messages that are sent. So the "pure worm" is not able to spread more than once: being run on a victim machine, the worm will infect WSOCK32.DLL, but will not be able to send its copies further. To "fix this problem," the worm sends its infected copy (WIN32.DLL is a worm component infected by a virus component, see above).

The known worm modification has a bug in its spreading routine and email server in many cases fails to receive affected messages from infected machine. Despite on that if the system has Dial-up connection, or mail server is fast enough, the worm sends its copies with no problems.

The Backdoor component:
Being run, a Backdoor component creates a new key in the system registry that indicates the machine is already infected:

```
HKLM\Software\[MATRIX]
```

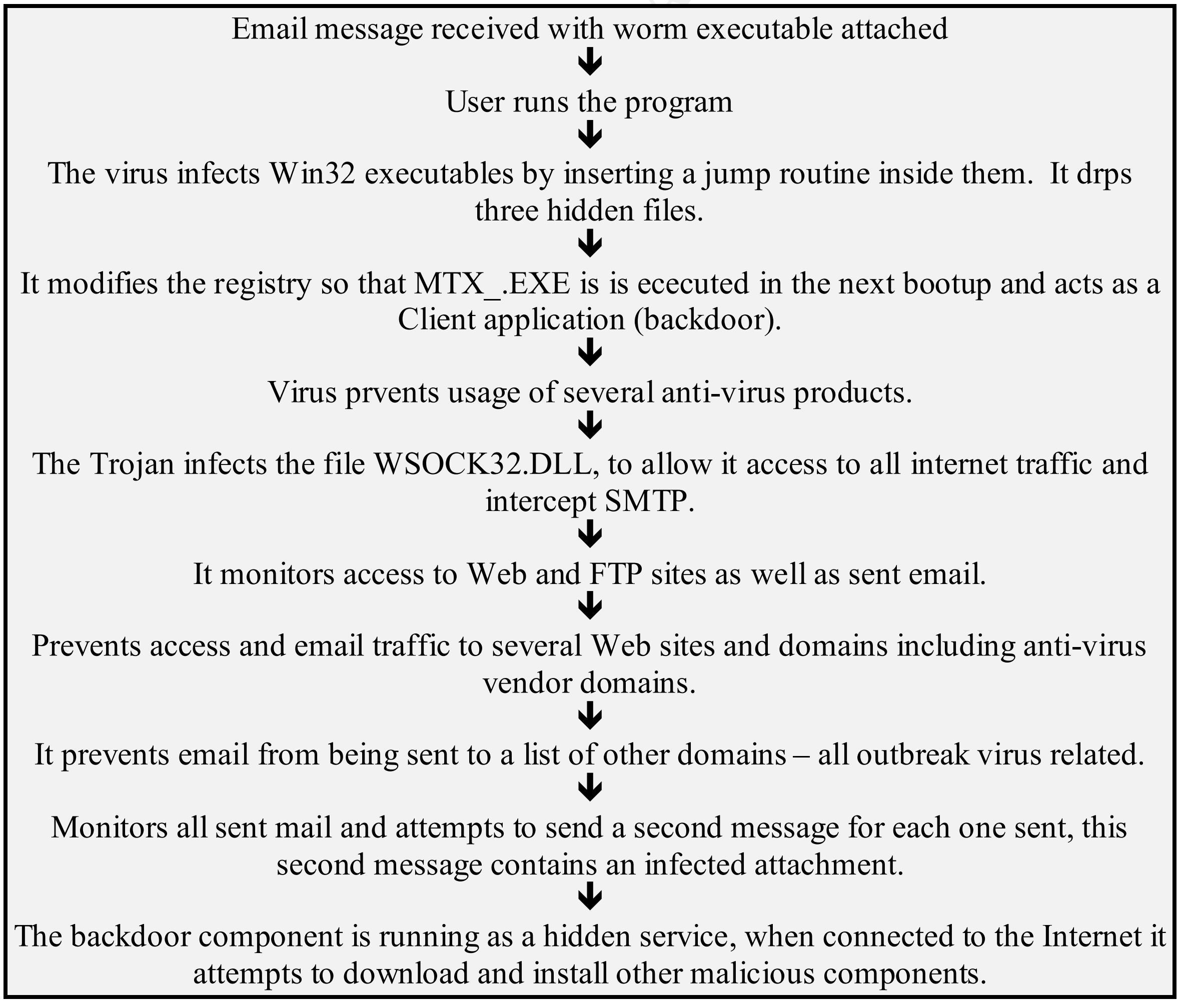
In case this key exists, the Backdoor skips the installation procedure. Otherwise, it registers itself in the auto-run section:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
SystemBackup=%WinDir%\MTX_.EXE
```

where %WinDir% is Windows directory.

The Backdoor then stays active in Windows as a hidden application (service) and runs a routine that connects to some Internet server, obtains files from there and spawns them in the system. So, the Backdoor can infect the system with other viruses or install Trojan programs or more functional backdoors.

Diagram:



Email message received with worm executable attached

↓

User runs the program

↓

The virus infects Win32 executables by inserting a jump routine inside them. It drps three hidden files.

↓

It modifies the registry so that MTX_.EXE is is ececuted in the next bootup and acts as a Client application (backdoor).

↓

Virus prvents usage of several anti-virus products.

↓

The Trojan infects the file WSOCK32.DLL, to allow it access to all internet traffic and intercept SMTP.

↓

It monitors access to Web and FTP sites as well as sent email.

↓

Prevents access and email traffic to several Web sites and domains including anti-virus vendor domains.

↓

It prevents email from being sent to a list of other domains – all outbreak virus related.

↓

Monitors all sent mail and attempts to send a second message for each one sent, this second message contains an infected attachment.

↓

The backdoor component is running as a hidden service, when connected to the Internet it attempts to download and install other malicious components.

Figure 1. Sequence of events beginning with Worm arrival

Virus structure

```
ã===============¬
 ¦ The virus     ¦ --> installs Worm and Backdoor to the system,
 ¦ installation  ¦     then finds and infects Win32 executable files
 ¦ and infection ¦
 ¦ routines      ¦
 ¦---------------¦
 ¦ Worm code     ¦ --> is extracted to file and run as stand-alone
program
 ¦ (compressed)  ¦
 ¦---------------¦
 ¦ Backdoor code ¦ --> is extracted to file and run as stand-alone
program
 ¦ (compresses)  ¦
 L===============-
```

Infected EXE file

```
 ã===============¬
 ¦ File code     ¦
 ¦ and data      ¦
 ¦               ¦
 ¦===============¦
 ¦ Virus code:   ¦
 ¦--------------¬¦
 ¦¦ Installation¦¦
 ¦¦and infection¦¦
 ¦+-------------+¦
 ¦¦ Worm        ¦¦
 ¦+-------------+¦
 ¦¦ Backdoor    ¦¦
 ¦L--------------¦
 L===============-
```

How to use the exploit:

WSOCK32.DLL is a thunk to let Win32s programs use WINSOCK.DLL. It comes with Win32s, I believe. You need this if you are running a 32 bit program with Trumpet or other 16 bit Winsock. It doesn't do anything except let Win32s programs call Winsock. If you are running NT or Win95, you want to use the built-in networking, not a second TCP/IP stack.

Signature of the attack:

This component in the known virus version also has a bug that causes standard a Windows message about an error in application when a backdoor tries to access an Internet site.

The very visible behavior of the virus is due to the fact that it prevents the ability of visiting several Internet sites, as well as disables sending messages to the same domains (they are anti-virus domain names).

Browse to the following registry key would show:
HKEY_LOCAL_MACHINESOFTWARE(**MATRIX**)

How to protect against it:
Do not execute the file " **win95.mtx** " and do not open any email attachments mentioned above. Do not open any suspicious/unknown attachments and delete them immediately. Regularly update the virus definition file of your antivirus software and run a virus scan on the computer. This is to ensure that the software is able to detect the presence of a new virus. The list of known antivirus vendor can be found at:
http://www.mycert.mimos.my/anti-virus.htm
Always run a virus scan on any downloadable files before executing it. It is advisable that your antivirus software is running in "Auto Protect Mode" at all time.

Download Microsoft's Outlook Security Patch. If you haven't already installed it, download the Outlook 98 Security Patch or the Outlook 2000 Security Patch (which requires the Office 2000 Service Release 1a). Please note that this patch does not include Outlook Express. Get the Outlook Express Patch here. You can also download virus protection software from ZDNet India Downloads.

"Don't open attachments!" One of the best ways to prevent virus infections is not to open attachments, especially when viruses such as MTX are being actively circulated. Even if the e-mail is from a known source, be careful. Always scan the attached files first for viruses. Unless it's a file or an image you are expecting, delete it.

Stay informed and get protected by installing virus protection software on your machine. If you're not sure if your existing anti-virus software is up-to-date, scan your system for free to find out.

Scan your system regularly. If you're just loading anti-virus software for the first time, it's a good idea to let it scan your entire system. It's better to start your PC clean and free of virus problems. Often the anti-virus program can be set to scan each time the computer is rebooted or on a periodic schedule. Some will scan in the background while you are connected to the Internet. Make it a regular habit to scan for viruses

Detection
To detect the virus, run a latest antivirus scan on any email attachments and any downloadable files that you receive.

Removal
1) REINSTALL OS
This is since it is difficult to remove the virus.
This will be the fastest way.
1.1) Backup all the important data into virus free PC.

Make sure that the virus-free PC running the latest virus signature before do the backup.

1.2) Reinstall the OS.

2) TRY TO CLEAN UP THE VIRUS

2.1) Uninstall the anti virus software.
2.2) Reinstall the anti virus software.
2.3) Update the anti virus signature.
2.4) Run the anti virus.

All the process must be done OFFLINE to prevent from the virus to spread. You may put the latest virus signature on removeable medium (floppy disk, zip drive).

For NAI, this is the URL:
http://service1.symantec.com/SUPPORT/nav.nsf/docid/199811293832

3) FOLLOW STEPS GIVEN BY NAI

http://www.norton.com/avcenter/venc/data/w95.mtx.html
Look under Removal: How to repair

4) USE THE STEPS GIVEN BY F-SECURE ON HOW TO REMOVE THE VIRUS MANUALLY
http://www.europe.F-Secure.com/v-descs/mtx.htm

"If the F-Secure Anti-Virus is not able to remove one of the dropped MTX components (in the case that the files are locked by Windows), please download and run the following REG file, restart your system and scan your hard drives again:
ftp://ftp.Europe.F-Secure.com/anti-virus/tools/mtxdisin.reg

You can delete the 3 components from your Windows directory manually from DOS:
IE_PACK.EXE
WIN32.DLL
MTX_.EXE

The Windows WinSock library WSOCK32.DLL that is patched by MTX should be restored from backups as the virus does not preserve the original file."

Source code/Psuedo code:
I was unable to find either the source code or the executable itself. So I have attached the Happy99 code which is similar. The following virus community sites were also visited, including the MTX official site (Cordez): (Screen prints of the official MTX site are also attached to this paper as attachment 1.

http://www.oninet.es/usuarios/darknode/

http://dmoz.org/Computers/Hacking/Viruses/Groups/

No Title
http://www.resonantcoderz.com/

Coderz.NET NetWork Virus Exchange
http://www.virusexchange.org/

Coderz Home Page coderz
http://www.coderz.com/

Additional Information:

Network Associates
http://vil.nai.com/vil/virusMethodOfInfection.asp?virus_k=98797
Symantec Antivirus Research Center
http://www.norton.com/avcenter/venc/data/w95.mtx.html
F-secure
http://www.europe.F-Secure.com/v-descs/mtx.htm

Command Software Systems, Inc.
http://www.commandcom.com/virus/vbsvwg.html
Computer Associates
http://ca.com/virusinfo/virusalert.htm#vbs_sstworm
F-Secure
http://www.f-secure.com/v-descs/onthefly.shtml
Finjan Software, Ltd.
http://www.finjan.com/attack_release_detail.cfm?attack_release_id=47
McAfee
http://www.mcafee.com/anti-virus/viruses/vbssst/default.asp
Dr. Solomon, NAI
http://vil.nai.com/vil/virusSummary.asp?virus_k=99011
Sophos
http://www.sophos.com/virusinfo/analyses/vbsssta.html
Symantec
http://www.symantec.com/avcenter/venc/data/vbs.sst@mm.html
Trend Micro
http://www.antivirus.com/pc-cillin/vinfo/virusencyclo/default5.asp?VName=VBS_KALAMAR.A

CERT/CC's Computer Virus Resources Page located at:
http://www.cert.org/other_sources/viruses.html

Attachement 1

Print screens of the official MTX site.
Coderz Home Page coderz
http://www.coderz.com/

The Matrix Manifesto

(In other words: who I am and what do I think about this virus)

Who I am and the state of this domain

Hello, my name is Fran. I apologize that this site pretty much sucks, but I wanted to get some information up as soon as possible. I registered this domain a couple years ago with the intention of creating a site for people who write code (hence the name coderz). I really dig programming, so I thought it would be a natural extension to come up with a site about the stupid programs and games I write. Unfortunately, I've come to realize that it means a little bit more than just programming computers. Apparently, it has meaning to the hacker community. Although, I don't know the exact definition, I'm going to go out on a limb and assume it means "hacker-warm-fuzzy-good". In other words, it would refer to writing software cracks, trojan horses and probably viruses - among other things. Its this meaning thats caused some confusion and misunderstanding lately.

The virus

This is where it gets a little fuzzy for me. To my knowledge, a group that used the name "Coderz", wrote a virus. From what different people have told me it appears that any of the following may or may not be true of the virus:

- It is passed through e-mail
- It is the MTX or Matrix virus.
- It is really nasty once it get on a PC. One guy told me that he couldn't get it off his computer even after a reformat (although I'm a little puzzled by this).
- It has a string of text in it which seems to imply it came from my domain, coderz.com.

Just to go on the record, **I DID NOT WRITE THIS VIRUS.** I know that the people who were infected seemed to think there was a connection to me, but I didn't have anything to do with it. If I had, you can bet I wouldn't have signed it with my own name. In the interest of not pointing fingers at possibly innocent people, I'm won't provide any information on who I think might have been involved with this. I don't know any names, but I have a couple ideas about where someone could start looking if they were inclined to do so. I'm empathetic with people that might have been infected, but accusing me in e-mail or by phone isn't going to help you because I don't have any information other that what little I described above.

My proposal

Here's what I propose. Since, I'm sure that there will be those who won't take my pleas of innocence seriously, I'm willing help document the virus so that you can remove it. Obviously, it doesn't look to cool if everone thinks I wrote it. If you've been infected, please e-mail me and describe all the symptoms which occur and why you think it came from my domain. If you figure out how to remove it, tell me about that as well. I'll take all the information I get and try to organize it right here on this site. The only thing I won't post here are accusations of who you think wrote it. So don't bother telling me that you read on some newsgroup that so-and-so wrote the virus. It won't make it on this site. Because I can't be 100% sure that the information would be true, I don't want to ruin someone's reputation for nothing.

Alternatively, you can just contact the authorities. I'm sure that they would love to know about new computer viruses out there. They have a pretty extensive branch that deals with computer crime, so this may apply.

Good Luck.

Fran

How to remove the Matrix virus

Intro

Here are a number of sources you can use to figure out how to remove the Matrix (MTX) virus. I haven't been infected personally, so I can't be sure that they work at all or are safe to perform on your computer. If you're in doubt, contact the customer support people for your computer or use one of the commercial pieces of virus software.

Cure #1

Leprechaun Software has an antivirus tool that is actually free on their site as a trial download.

Cure #2

These instructions were sent to me from a site that apparently knows how to perform this removal. I couldn't tell where it was sent from, so I can't give credit to the original author.

W32/MTX@MM - Manual Removal Steps

Boot to Safe Mode Command Prompt Only

1. **Turn the computer off. Wait a few seconds.**
2. **Turn on the computer. Immediately after you turn the computer on, press the F8 key repeatedly until you see the Microsoft Startup Menu.**
3. **Using the arrow keys, select "Safe Mode Command Prompt Only", and press ENTER.**
4. **You will come to a black screen where you will see a C:\>**

Delete Infected Files

1. **At the C:\> prompt type CD \Windows and then press enter.**
2. **Then type in ATTRIB -h -r -s IE_PACK.EXE and then press enter.**
3. **Type in ATTRIB -h -r -s MTX_.EXE and then press enter.**
4. **Type in ATTRIB -h -r -s WIN32.DLL and then press enter.**
5. **Type in DEL IE_PACK.EXE and then press enter.**
6. **Type in DEL MTX_.EXE and then press enter.**
7. **Type in DEL WIN32.DLL and then press enter.**
8. **Next type in CD SYSTEM and then press enter.**
9. **Then type in DEL WSOCK32.DLL and then press enter.**

Recover WSOCK32.DLL

1. **From a clean computer, with the same Browser, copy the file C:\WINDOWS\SYSTEM\WSOCK32.DLL to a floppy disk**
2. **Put the floppy in the drive of the infected computer.**
3. **Type in COPY A:\WSOCK32.DLL . and press enter.**
   NOTE: There is a space after the filename, and a period.
4. **Restart the Computer.**

Edit Registry Entries

1. **Click on Start, then click on Run.**
2. **In the open field, type in REGEDIT and click OK.**
3. **Click the plus (+) next to HKEY_LOCAL_MACHINE.**
4. **Click the plus (+) next to Software.**
5. **Click the plus (+) next to Microsoft.**

6. **Click the plus (+) next to Windows.**
7. **Click the plus (+) next to CurrentVersion.**
8. **Click the plus (+) next to Run.**
9. **Single click on SystemBackup "C:\windows\MTX_.EXE" and press the delete key on the keyboard.**
10. **Scroll to the top of the registry. Click the minus (-) next to Microsoft.**
11. **Single click on [MATRiX] and press the delete key on the keyboard.**
12. **Close the Registry Editor.**