Global Information Assurance Certification Paper

MTX: The Super-Virus You've Probably Never Heard Of

By Jason Bruce

October 19, 2000

The W95.MTX super-virus was first discovered on August 17, 2000 and has been termed a super-virus because of its three-component structure. It is composed of a worm, virus and backdoor. These components run as stand-alone programs and spread under WIN32 systems. The virus component infects WIN32 executable files, attempts to send e-mail messages with infected attachments and installs the backdoor component to download and spawn "plug-ins" on an infected system.

Now lets take a closer look at how the super-virus operates.

The virus component uses a method known as Entry Point Obscuring (EPO), in which it places a jump to the virus file code somewhere inside an infected file, thus making detection of the virus more complex. It is important to note that the virus will not be "set in motion" until that file code section is given control. Once the virus code has been given control it decrypts itself and looks for necessary WIN32 API functions by scanning the WIN32 Kernel. The virus then attempts to determine if any of the following anti-virus programs are running through the use of four-letter combinations:

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

If none of the above anti-virus programs are found to be on the system, the virus installs itself and the following files are created with the hidden attribute set:

- IE_PACK.EXE - pure Worm code
- WIN32.DLL - Worm code infected by the virus
- MTX_.EXE - Backdoor code

The Worm component uses technology that was first introduced by the Happy99/Ska Internet worm to send infected messages. The Worm makes a copy of WSOCK32.DLL and names it WSOCK32.MTX. The Worm then makes an entry in the WININIT.INI with

the following code to overwrite its WSOCK32.MTX upon the next reboot.

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

The virus is allowed to propagate itself by intercepting e-mail messages that are sent from the infected computer. It then sends both the original message and a second message with an empty subject and text, but with an infected attachment selected by the worm (the attachment name is dependent on the current date).

The worm also blocks the user from sending e-mail messages to the following domains:

wildlist.o*	mabex.com *
il.esafe.c*	cellco.com*
perfectsup*	symantec.c*
complex.is*	successful*
HiServ.com*	inforamp.n*
hiserv.com*	newell.com*
metro.ch*	singnet.co*
beyond.com*	bmcd.com.a*
mcafee.com*	bca.com.nz*
pandasoftw*	trendmicro*
earthlink.*	sophos.com*
inexar.com*	maple.com.*
comkom.co.*	netsales.n*
meditrade.*	f-secure.c*

It should be noted that the current worm modification has a flaw in its spreading routine that prevents the e-mail server from receiving the affected messages from the infected machine.

The backdoor component of the super-virus creates a new key in the systems registry that indicates that the machine is already infected. The registry key will look like this:

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

If the key already exists, the installation procedure is skipped, and the Backdoor registers itself in the auto-run section:

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

The %WinDir% is where the Windows directory is located. The backdoor then stays active in Windows as a hidden application (service) and runs a routine that connects to some Internet server, gets files from there and spawns them to the system. This enables the Backdoor to infect the system with other viruses or install Trojan programs or more functional backdoors.

The backdoor in the known virus version has a bug that causes a standard error message

when the backdoor tries to access the Internet site.

In its present state, the MTX Super-Virus has several flaws, but it is important to see that with a few adjustments to the code this could prove to be a very destructive virus indeed. That is why the following basic steps should be taken to nullify the propagation of viruses such as the MTX Super-Virus:

1) Ensure that you have downloaded the latest security patch for your e-mail client.

2) Don't open attachments from an unknown source. It is also wise to be weary of attachments from known sources, because as the above virus shows, your friends/colleagues can propagate these types of viruses unbeknownst. If you do find it necessary to open these e-mail attachments, ensure that you use an updated anti-virus program to scan for destructive attachments. This leads us to the next step in our computers protection.

3) Update your anti-virus software regularly. Several anti-virus software vendors allow the program to automatically remind you when your virus protection is getting out of date. It is generally a good idea to have these reminders enabled.

4) Stay informed of the latest virus advisories. There are many places that keep you up to date on the latest viruses propagating throughout the Internet.

5) Scan your system regularly for viruses. Some anti-virus programs can be set to scan each time you reboot your system, although this might be a nuisance to some, it can prevent a lot of time and heartache. If this is still to much to try to bear set your anti-virus program up for periodic scans of your computer.

References:

Vamosi, Stephen. "MTX Supervirus Outsmarts Itself" September 20, 2000. URL: http://www.zdnet.com/zdhelp/stories/main/0,5594,2630479-1,00.html (October 21, 2000).

Vamosi, Stephen. "MTX Supervirus Outsmarts Itself" September 20, 2000. URL: http://www.zdnet.com/zdhelp/stories/main/0,5594,2630479-3,00.html (October 21, 2000).

"W95.MTX" October 16, 2000. URL: http://www.symantec.com/avcenter/venc/data/w95.mtx.html (October 22, 2000).

Kaspersky, Eugene. Podrezov, Alexey. "F-Secure Virus Descriptions: MTX" September 2000. URL: http://www.data-fellows.com/v-descs/mtx.htm (October 23, 2000).