Global Information Assurance Certification Paper

Windows 2000 Streaming Virus
Ruth Parish
November 20, 2000

A new virus is taking advantage of a currently little-used programming technology and could provide major headaches to security and system administrators. In addition, future use of the technology may possibly embarrass some anti-virus software vendors who discount the ingenuity of virus authors.

The new virus is variously referred to as: W2K.Stream by Kaspersky Lab and also by Symantec Corporation, (Norton anti-virus software) W2K/Streams by John Leyden of www.vnunet.com, WNT/Stream by Network Associates, Inc, (McAfee anti-virus software) and PE_STREAM.A by Trend Micro, Inc (PC-Cillin and Office Scan anti-virus software). The virus takes advantage of a programming technology and methodology called the Stream Companion. This technology allows more than one stream to be assigned to files and folders. Unfortunately, most and possibly all anti-virus software examine only the main program stream for viruses.

This type of virus has not been seen thus far on personal computers running Microsoft operating systems because the technology hasn't been available until it was introduced in later editions of Microsoft Windows NT including Microsoft Windows 2000. The Stream Companion technology is only available on NTFS disks.

The first virus to take advantage of this technology is the W2K.Stream virus. It appears to have been written by two people working under the names of Benny and Ratter. Symantec Corporation indicates that these two are from the "29A" virus group. A search of Symantec Corporation Antivirus Research Center web site virus articles lists a number of viruses written by the "29A" group. This virus was discovered by Kaspersky Lab, the largest Russian developer of anti-virus provider programs, and was announced by them on September 4, 2000. Eugene Kaspersky, director of anti-virus research said in his article, "Certainly, this virus begins a new era in computer virus creation."

Stream Technology

As indicated above, Microsoft introduced the Stream Companion technology into their operating systems with the advent of NTFS and Windows NT 3.1. This type of technology, which is also referred to as Alternative Data Streams (ADS), is unavailable on FAT disks and cannot run on earlier versions of Microsoft Windows operating systems. Since anti-virus software checks only the main programming stream, viruses can be written to run in the additional alternative streams. In this way the virus can perform its dirty work out of site of the user and the anti-virus software.

Files and directories can have associated multiple streams, which can be a service stream or autonomous program. All but the main stream is normally invisible to the user. When files with associated streams are copied to a FAT device, such as a floppy or FAT disk, everything but the main stream is lost. Additionally it is important what type of application is used to transfer or run stream-based files. If the software can't handle streams, only the main stream is transferred or used.

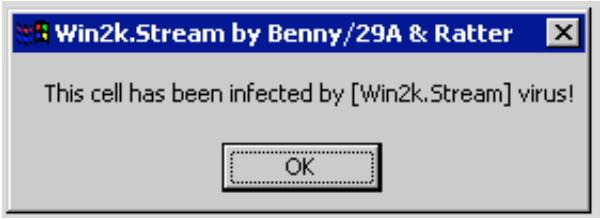
Oddly enough, Symantec Corporation indicates that a client with a non-NT operating system "can access streams on an NTFS share, independent of their file system" as long as they are using a "stream aware client."

The Virus

The W2K.Stream virus is the first virus to take advantage of the Stream Companion method of programming. Kaspersky Lab indicates in their article, "A new Generation of Windows 2000 Viruses is Streaming" that the authors are from the Czech Republic and assembled the virus sometime in late August of 2000.

According to Kaspersky Lab, "… the virus creates an alternative data stream name "STR" and moves the original content of the host program there. Then, it replaces the main data stream with the virus code. As a result, when the infected program is run, the virus takes control, completes the replicating procedure and then passes control to the host program."

The virus is only activated on personal computers running Microsoft Windows 2000. This is due to a misconception by the W2K.Stream virus authors, in that they believed that streaming wasn't available on PCs running Microsoft Windows NT. One of the virus' initial tasks is to check the operating system, if it isn't Windows 2000 it displays:



Screen capture provided by Symantec Corporation.

Once it has confirmed a Windows 2000 operating system it infects any file in the host directory. The virus infects other files (only executables, via the extension type) by replacing the host application with itself, which is 3628 bytes in length. Because of this, all infected files become 3628 bytes in size. It hides the fact that it is using additional disk space by adding the compression flag to each infected file. The virus ignores any read-only attribute. According to Symantec, "the virus uses temporary files to copy the data streams." The authors used the Portable Executable file compressor called Petite to reduce the size of the virus.

It hides its actions from the user, by writing the host program to a secondary stream, called

"host-application-name.exe.STR." If the STR stream is not available it will also display the message window, shown above. As an example, Microsoft WordPad would be written to WORDPAD.EXE.STR. This process allows the host application to continuing running in the secondary stream and the virus in the main stream. Neither Microsoft Windows NT nor Microsoft Windows 2000 standard commands or applications display alternative data streams assigned to files, making it difficult for the user to identify these types of files.

W2K.Stream is a "proof of concept" virus and has not been seen "in-the-wild" (in circulation) as yet (9/7/00) per Symantec AntiVirus Research Center.

The Virus Controversy

At present there is a quite a controversy about whether a virus using the Stream Companion process to hide its actions presents any kind of real danger to the users protected by anti-virus software. Eugene Kaspersky states, "By default, anti-virus programs check only the main data stream. There will be no problems protecting users from this particular virus," Continuing he says, "However, the viruses can move to the additional data streams. In this case, many anti-virus products will become obsolete, and their vendors will be forced to urgently redesign their anti-virus engines."

The Bob Sullivan article on the www.msnbc.com web site indicates "The SANS Institute, a group of security researchers, issued an "alert" criticizing antivirus companies for not updating their products to scan the contents of any file stream earlier."

In McAfee's web site article on the virus, Network Associates, Inc states "The detection issue raised by SANS can become a problem IF a virus writer was able to hide the virus in the alternative data stream completely. This is not possible, as there will need to be some function of the virus in the main body of the file, it has infected, that calls the virus to infect. Because of this Antivirus scanners will be able to detect these types of viruses now and in the future."

The WWW.ISP-Planet.com article on the virus quotes Eric Chen, chief researcher at Symantec's Antivirus Research Centre, as saying "Antivirus packages offer protection from this kind of infection. But if virus writers make more use of stream technologies we will have to develop new parsing engines to specifically look in alternative data streams."

The article further quotes Jack Clark, European anti-virus product manager at Network Associates (makers of McAfee) as saying "Virus writers are not standing still. This is another example of them using the methods made available by modern operating systems."

Graham Cluley of Sophos reiterates McAfee's theory "To execute code in an ADS you have to call the code from a non-ADS stream. So far we have not seen evidence that the code can be executed directly."

Conclusion

Fortunately, the W2K.Stream virus itself is easily preventable. All one has to do is load any reputable anti-virus software on their computer(s). What about future viruses using the same methodology, do we need worry about them?

Some well-respected groups say files using the Stream Companion methodology may cause serious problems in the future and others, as respected, say not to worry, that the current anti-virus software can handle any virus hidden in files using Streams. It all boils down to the ingenuity of our ever-present virus authors. Will they figure out a way to hide the virus in alternative streams without ever making a suspicious call in the main stream? Regrettably, to use that well-worn phrase only "time will tell."

References

Lemos, Robert. "New Virus Hides Behind Old Technology." ZDNet News. 5 September 2000. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2624500,00.html (13 September 2000)

Townley, John. "Killer Virus Streaming Near You." InternetNews – Streaming Media News Archive. 5 September 2000. URL: http://www.internetnews.com/streaming-news/article/0,,8161_452391,00.html (17 September 2000)

Leyden, John. "Windows 2000 Virus Hides from Scanners." vnunet.com. 6 September 2000. URL: http://be.internet.com/html/print.asp?ln=0&R=1472 (17 September 2000)

Sullivan, Bob. "New trick can hide computer viruses." Technology Goofs and Glitches. MSNBC. 6 September 2000. URL: http://www.msnbc.com/news/455905.asp?0nm=N22h (13 September 2000)

Greene, Thomas C. "Malicious code exploits unique Win2k function." The Register. 5 September 2000. URL: http://www.theregister.co.uk/content/1/13046.html (6 September 2000)

VIRUSLIST.COM. "A New Generation of Windows 2000 Viruses is Streaming." VL-New Viruses!... 4 September 2000. URL: http://www.viruslist.com/eng/default.asp?tnews=2&nview=1&id=657 (23 September 2000)

AntiVirus Research Center. "NTFS Streams." SYMANTEC.UNITED STATES. URL: http://www.symantec.com/ns-search/sarc/avcenter/reference/ntfs.streams.html?NS-search-set=/39ccf/aaajgXz7_ccfdab&NS-doc-offset=0& (23 September 2000)

AntiVirus Research Center. "W2K.Stream." SYMANTEC.UNITED STATES. 7 September 2000. URL: http://www.symantec.com/avcenter/venc/data/w2k.stream.html (13 September 2000)

Virus Information Center, Virus Encyclopedia. "PE_STREAM.A." Trend Micro. URL: http://www.antivirus.com/vinfo/virusencyclo/default5.asp?aspVName=PE_STREAM.A (21 September 2000)

Virus Information Library "Virus Name: WNT/STREAM." McAfee – Avert. URL: http://vil.nai.com/vil/virusChar.asp?virus_k=98803 (13

Last Updated: May 26th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event