VIRUS ANALYSIS

Stream of Consciousness

Péter Ször
Symantec Corporation

In September, Benny 29A and Ratter released W2K/Stream, the first known virus to utilise NTFS streams. The virus (and the surrounding hype) generated much confusion for users worldwide. This is understandable. Currently most (all?) on-demand anti-virus software does not scan the NTFS streams for virus code. Since NTFS streams are invisible with standard *Windows NT/2000* applications the news generated panic among users, just like when NTFS streams were first discussed in public (at the time without an actual virus example).

In recent news some 'experts' went as far as claiming that systems will be 'Trojanised by current AV software'. In this short article I do not intend to comment on all the false claims. However, I would like to say that as far as the detection of the virus is concerned, it should be no problem for any current AV software.

W2K/Stream uses an NTFS feature that exists on both *Windows NT* and *Windows 2000*. The virus writers believed that this particular feature did not exist on *NT* and reduced Stream to being *Windows 2000*-specific by checking the OS version. NTFS streams are virtually hidden from the users because *NT* commands and standard *Windows 2000* applications do not display them. Any given file on an NTFS volume is basically the first, unnamed stream of a file. Any file (or even directory) can have associated, named streams. These streams can be accessed via standard file operations. Most *Windows NT/2000* applications do not use named streams. Some applications, including the *Windows 2000* shell, use streams to write file property information into a named stream of a particular file. This way, additional information can be kept together with a file object without changing the actual file content.

The W2K/Stream virus is 3,628 bytes long. The virus is compressed with *Petite*, a popular Portable Executable (PE) file compressor. The virus code inside is very short but the actual, compiled standalone file would be at least 4 KB. First the virus checks the *Windows* version of the current system. If it is not *Windows 2000* the virus displays a message box.

This is basically a new sub-class of companion virus, a stream-companion virus. When the virus infects a file it replaces the host application with itself. Basically, Stream implements the simplest possible virus infection by overwriting the host program with its own code. In other words, each infected file will be 3,628 bytes long after the infection. The trick is that Stream saves the original host application as a named stream of the host program.

For instance, when NOTEPAD.EXE gets infected, the size of the file will change to 3,628 bytes. At the same time the virus creates a 'NOTEPAD.EXE:STR' stream that will have the copy of 'NOTEPAD.EXE' content. This way, the virus can execute the host program as long as the infected file remains on an NTFS partition. (The virus uses temporary files during infections and execution of the host programs. The 'STR' stream of the host is not executed directly.)

When someone copies an infected file to a diskette, the host program will be lost, since the diskette uses FAT instead of NTFS storage format. However, the virus and the host will be copied over the network from an NTFS to an NTFS partition with a copy command. W2K/Stream is clearly a 'proof of concept' virus. Whenever the STR stream is missing the virus will display its introduction message box.

The virus uses the file compression flag as an infection marker. It sets this special NTFS file attribute via the DeviceIoControl() API. This way, the used disk space of the virus is not that obvious, although the free disk space does not calculate with the actual size of streams on the disk. The virus will infect all files in the current directory that have an .EXE extension. It does not pay attention to the actual file type.

Neither does it mind the read-only attribute. During infection operations the virus uses temporary files to copy the data streams. As self-recognition is performed via the compression flag, the already cleaned applications will not get the infection again since the AV software will not remove the compression flag. The virus will obviously re-infect itself without a host. Therefore, the actual host stream might hold virus code only. Stream passes the command-line parameters to the executed temporary file that it creates from the STR stream.

We might see special reincarnations of the DIR-II virus idea for NTFS. It is very likely that new viruses and Trojans will take advantage of the NTFS streams in various ways. The support for on-demand NTFS stream scanning is trivial and repair will be important against future trends.

W2K/Stream

Alias:	W32/Stream, WNT/Stream.
Type:	Direct action stream-companion.
Payload:	Displays message box when executed on a non-*Windows 2000* system or if 'STR' stream is missing from the file.
Self-recognition in files:	Set the NTFS compression flag for the infected file.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.