VIRUS ANALYSIS

NOT WORTHY

Peter Ferrie
Symantec Security Response, USA

The members of the RRLF virus-writing group were very proud when they released the first viruses for *Microsoft Shell* (see *VB*, November 2005, p.4), believing that these were the first viruses on the *Vista* platform. Of course, they were wrong: those are *Microsoft Shell* viruses, not *Vista* viruses. Then *Microsoft* announced that it would no longer be shipping *Microsoft Shell* with the first release of *Vista* in any case.

So what did the group do? They tried again. The second attempt at the 'first' *Vista* virus is called Idonus. However, this is not a *Vista* virus either – it's an *MSIL* virus. Give it up, guys.

IT GETS BETA AND BETA

MSIL/Idonus runs only on the *.NET* framework version 2.0, which has just been released. It is freely available from *Microsoft*, and can be installed on *Windows 98* (yes, indeed!), *Windows ME*, *Windows 2000, Windows XP* (if SP2 is installed), *Windows 2003* (if SP1 is installed) and, of course, *Vista* (which is currently at the Beta 1 stage).

The virus also requires the *WinFX Runtime Components Core* 3.0 to be installed (this includes the *Windows Presentation Foundation*, which is used to display the payload of the virus). *WinFX* is currently at the Beta 2 stage, is also freely available from *Microsoft*, and can be installed on *Windows XP* and *Windows 2003*.

The virus author wanted to call the virus 'Idoneus', from the Latin meaning 'suitable' or 'worthy'. If any virus were worthy of anything at all, this isn't it. The code looks awful, it was built in debug mode, which makes it look even worse, and it appears to be unfinished. Perhaps it is in the beta stage, too.

REGISTER HERE

Whenever the virus is executed, it creates a list in memory of all subdirectories under C:\. Then it attempts to open the registry key 'HKCU\Software\Retro'. If the registry key does not exist, the virus will create that key, then create the registry value 'Idoneus' within it. The virus sets the registry value data to 'c:\', followed by a directory name chosen randomly from the list it created. This is followed by the filename of the currently running program. The virus will also copy itself to the same randomly chosen directory, maintaining the name of the currently running program.

If the registry value 'Idoneus' exists, the virus reads it and deletes the file to which the registry value points, then copies itself to another randomly chosen directory, and rewrites the registry value with the newly chosen directory name. Thus, the virus moves around the drive each time it is executed.

The virus also creates the registry value 'Idoneus' under the registry key 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run', and sets the registry value data to 'c:\', followed by the randomly chosen directory name and the filename of the currently running program. This ensures that the virus is executed each time the machine starts.

START HERE

The virus searches only in the current directory for files to infect, and only for those files whose suffix is '.exe'. For each file that the virus finds to infect, the virus reads its own code entirely into memory, then reads the victim's code entirely into memory, but then writes out only the virus code. Thus, the virus overwrites the host file.

It appears that the virus was intended to be a prepender (by writing out the host code afterwards, and including code to extract the host and run it), but perhaps the virus author was under pressure to release sooner.

GET THE MESSAGE

After the infection process has completed, the virus displays a message containing the virus name, the group's website and the text 'GeNeTiX is EVIL!'. It is not clear if the virus author is targeting a particular molecular biology industry company of that name, or the group that is campaigning against genetically-modified foods, or another group entirely.

CONCLUSION

The expression of controversial opinions in viruses is nothing new. We have seen, for example, anti-Israel comments in W32/Simile (see *VB*, May 2002, p.4), and other political messages in viruses such as W32/Maldal. However, using a virus to get the message across is not a good way to do it, especially when that virus destroys user data. Now that's evil.

MSIL/Idonus	
Size:	16,384 bytes.
Type:	Direct-action overwriter.
Payload:	Displays message box.
Removal:	Delete infected files and restore them from backup.