Virus:Win32/Virut.gen!epo

Article URL
malware.php?mal_id=986950914fdc2300e50889.38552152

Author
SecurityHome.eu

Published: 16 June 2012

Aliases :

Virus:Win32/Virut.gen!epo

is also known as *W32/Virut.AL!Generic (Command), Win32/Virut (AVG), W32/Virut.gen (Avira), Win32.Virut.56 (Dr.Web), Virus.Win32.Virut.ce (Kaspersky), W32/Virut.gen.gen (McAfee), Win32.Virut.dw (Rising AV), W32/Scribble-B (Sophos), W32.Virut.CF (Symantec), PE_VIRUX.Q-1 (Trend Micro), Win32.Virut.AB.Gen (VirusBuster)*

.

Explanation :

Virus:Win32/Virut.gen!epo is a generic detection for a polymorphic and memory-resident file infecting virus that is also capable of allowing unauthorized remote access and control of your infected computer.

Installation

If a file infected with Virus:Win32/Virut.gen!epo is run, the virus injects code into system processes and certain Windows kernel APIs to infect files when they are created or opened or when processes are started.Spreads via... File infectionThe virus targets files that have either .EXE or .SCR file extension and uses a technique known as entry point obfuscation (EPO) when infecting a host file.The virus is selective in that it does not infect files that begin with the following letters:

* PSTO
* WC32
* WCUN
* WINC

During infection, the virus appends its code to the host file.

Payload

Disables Windows system file protection

Virus:Win32/Virut.gen!epo disables Windows system file protection by modifying instances of the Windows system files "SFC.DLL" and "SFC_OS.DLL" in memory.

Performs backdoor functions

Virus:Win32/Virut.gen!epo connects to a remote server to allow an unauthorized backdoor. A remote attacker could connect to your computer and issue a command to download and execute unwanted programs and malwares on your computer. We've observed this virus to connect to various remote servers such as the following, for this purpose:

* proxim.ircgalaxy.pl:65230
* ilo.brenz.pl:80
* veoccw.com:443
* irc.zief.pl:80

Additional information

In certain varaints of Virus:Win32/Virut.gen!epo, the virus carries the following strings which are never displayed:

O noon of life! O time to celebrate!
O summer garden
Relentlessly happy and expectant, standing: -
Watching all day and night, for friends I wait:
Where are you, friends? Come! It is time! Its late!)

Analysis by Jim Wang

Last update 16 June 2012