McAfee Avert Labs
W32/Virut Family

By Jim Walter, Avert Labs Services

Contents

Finding W32/Virut

Overview

This “mini” edition of the “McAfee® Avert® Labs, Finding Suspicious Files” series covers a particular virus: W32/Virut.

The W32/Virut family is a polymorphic and parasitic file infector. W32/Virut is capable of infecting PE (executable) files, as well as HTML and ASP data files. Some variants will inject threads into running processes. Most, if not all variants, will download additional malware onto infected hosts.

The W32/Virut family also contains IRC bot–style functionality for command and control.

Eradicating W32/Virut in an actively infected environment must be approached with a high level of detail and diligence. The W32/Virut family has a number of bugs in its code, and as a result it may “misinfect” a portion of a system’s executable files. McAfee’s Scan Engine can repair those executables in which repair data is present within the virus body, but some W32/Virut infections are corrupted beyond repair.

Symptoms

Two main characteristics define the W32/Virut family. The virus is both polymorphic and parasitic. Parasitic threats append, prepend, or insert their code into data sections of files on disk. Polymorphic viruses create varied (though fully functional) copies of themselves as a way to avoid detection by anti-virus software. Some polymorphic viruses use different encryption schemes and require different decryption routines. Thus, the same virus may look completely different on different systems or even within different files.

The W32/Virut family makes use of the technique “entry point obfuscation” to evade anti-virus technologies. This technique makes it more difficult to identify the exact location of the malicious data in an infected file, thus making proper analysis, detection, and repair more challenging.

Given that this particular threat behaves similarly to a traditional IRC bot, often there will be no visible clues to indicate an infected host. Apart from executables that suddenly fail to launch properly (due to misinfection), an infected host may show no symptoms and remain unsuspected for any amount of time. There are, however, a few common indicators that may aid in confirming a suspected W32/Virut infection:

- Modified PE (executable) , ASP, or HTML files (changes in file size, behavior)

- Anomalous network activity (IRC-related traffic, DNS queries to suspect or unknown domains)
- Presence of new registry entries that allow the threat to launch upon startup
- Some variants disable Windows File Protection (WFC)
- Redirected network traffic (via HOSTS file)
- Detection of documented rootkit-like hooks via tools such as McAfee Rootkit Detective, GMER, Rootkit Revealer, or others.

Characteristics

The characteristics of W32/Virut differ across variants. The first variants were discovered in 2007, and the family has been evolving ever since. For the scope of this document we shall outline characteristics of a current variant (W32/Virut.n) and provide links to the McAfee Virus Information Library for detailed characteristics on other variants.

- W32/Virut.n
  - W32/Virut.n will first inject threads into the Winlogon.exe process. When successful, it will cause the process to download and run the following file:
    - %WINDOWS%\TEMP\VRT7.tmp
  - This file will launch a new svchost.exe process and proceed to inject threads into the process. The svchost process creates the following files in %WINDOWS\System32 folder and deletes the previous VRT7.tmp file:
    - 8.tmp (data file)
    - 9.tmp
  - The 9.tmp file will execute and can download further malware. The %WINDOWS%\System32\drivers\etc\hosts file will be modified to have the following host string prepended:
    - 127.0.0.1 ZieF.pl
  - W32/Virut.n also injects code in running processes and hooks the following functions in ntdll.dll, which transfers control to the virus every time any of these function calls are made:
    - NtCreateFile
    - NtCreateProcess
    - NtCreateProcessEx
    - NtOpenFile
    - NtQueryInformationProcess

      The detection for this hooking is currently detected as Generic.dx!rootkit

  - Registry Entries

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List
- HKEY_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UpdateHost

- W32/Virut.n connects to the following domains or IP addresses:
  horobl.cn
  goasi.cn
  setdoc.cn
  irc.zief.pl
  DNS2.zief.pl
  proxim.ircgalaxy.pl
  anti-captcha.com
  lorentil.cn
  thaexp.cn
  209.205.196.18
  66.232.126.195
  204.13.249.70
  58.65.232.34
  61.235.117.80
  61.235.117.81
  74.55.100.7
  124.207.41.201
  124.207.117.60
  124.236.241.91
  66.114.124.140
  64.13.232.135
  66.116.109.93
  210.51.37.106
  83.68.16.6
  211.95.79.6
  218.93.202.114
  209.205.196.18
  66.232.126.195
  69.46.16.191
  195.2.252.246
  94.247.2.38

- W32/Virut.n will connect to the following IRC servers for command and control
  - irc.zief.pl
  - proxim.ircgalaxy.pl

- Emails are harvested from the infected machine and posted to the following server:

        - 69.46.16.191
    - Additional malware are downloaded (rootkits, backdoors, etc.) from various dynamic locations.

For links to additional W32/Virut variants, see Appendix A.

Fighting W32/Virut (Prevention and Eradication)

Once active in an environment, W32/Virut will spread at a very fast rate. It is vital to isolate hosts or segments to contain the threat as quickly as possible. This can include:

Isolating specific segments

Physically disconnecting the network

Prevention

VirusScan Enterprise must be configured properly across the entire environment to effectively inhibit the further spread of the threat. Proper configuration requires the On-Access Scanner to be enabled and configured as follows:

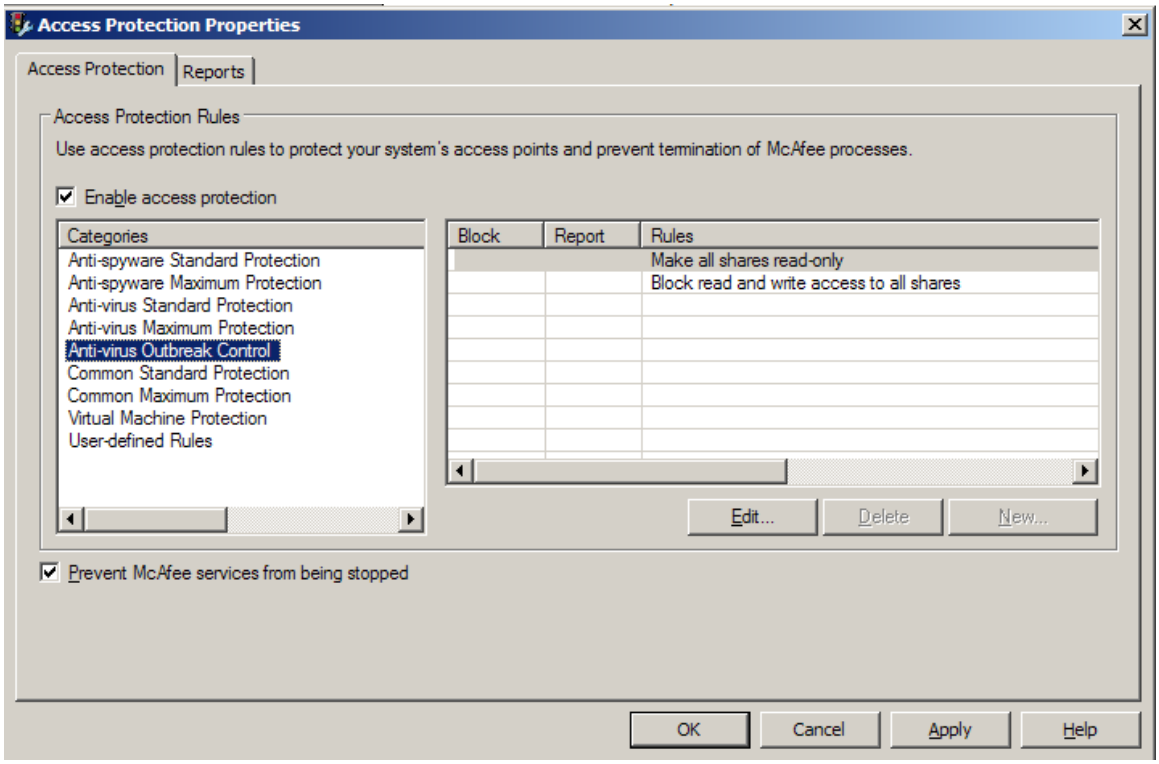
- Scan All Files
- Scan both Reads and Writes
- On-Access exclusions are at an absolute minimum (excluded directories containing executable files will allow the virus to exist free of AV scanning)

Some steps to "harden" network-based resources are recommended. These can include:

- Disabling access to network shares
- Making network shares read only
- When access to network shares or locations is an absolute requirement (login scripts, roaming profiles, etc.), adequately secure these locations or take steps to isolate them from infected segments or hosts.

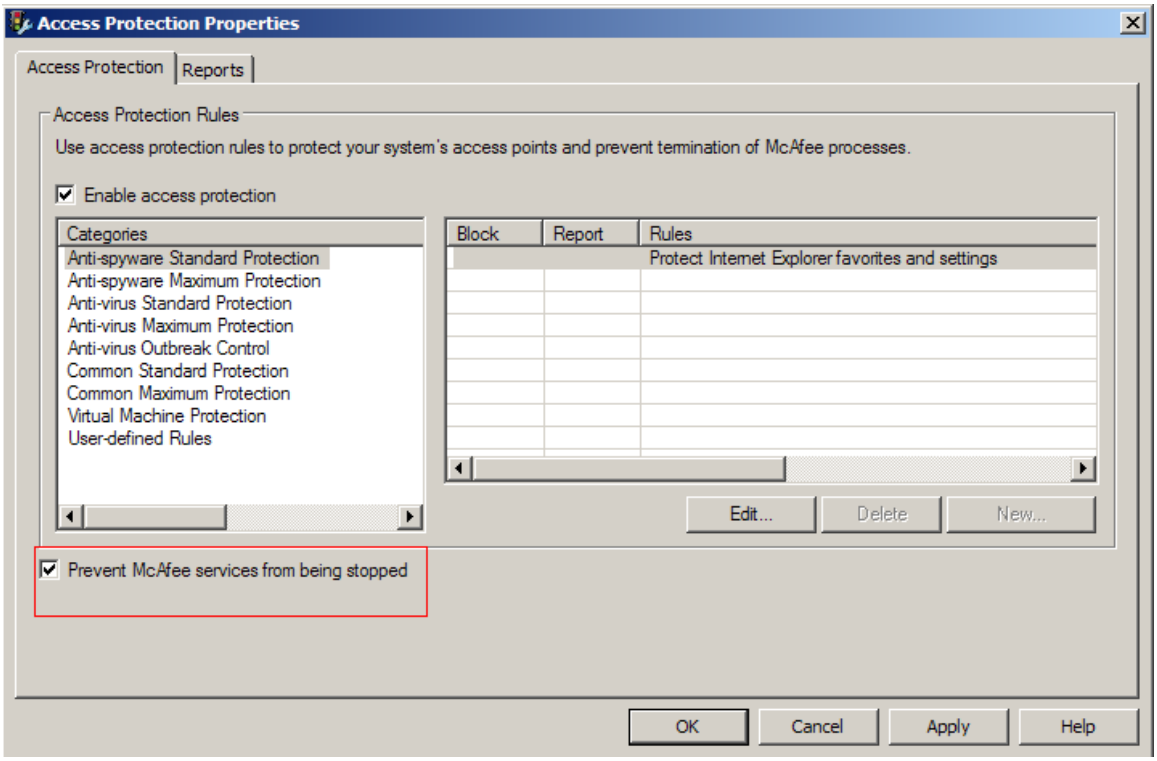
VirusScan Enterprise's Access Protection rules can effectively safeguard against the spread of W32/Virut. Some of the rules that apply:

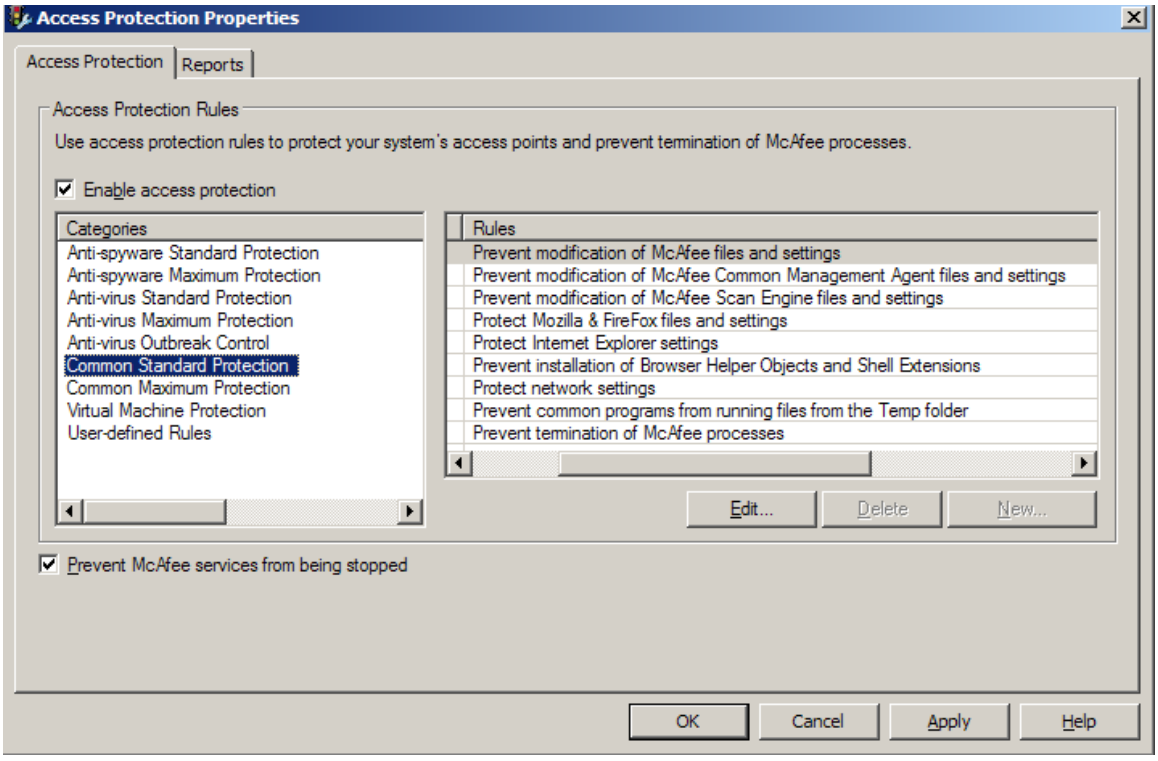
- Prevent IRC communication (Anti-virus Standard Protection)
- Prevent creation of new executable files in the Windows folder (Common Maximum Protection)
- Prevent all programs from running from the Temp folder (Anti-spyware Maximum Protection)
- Make all shares read only (Anti-virus Outbreak Control)



Some variants of the W32/Virut family will attempt to disable a variety of anti-virus products. McAfee VirusScan 8.5i and 8.7i can be configured to protect their processes from malware threats though the Access Protection policy.

- Ensure that Access Protection is enabled
- Ensure that the option to "Prevent McAfee Services from being stopped" is enabled
- Enable McAfee-specific options in the "Common Standard Protection" rule categories
  - Prevent modification of McAfee files and settings
  - Prevent modification of McAfee Common Management Agent and settings
  - Prevent modification of McAfee Scan Engine files and settings





Three articles in our Knowledgebase can assist with creating rules in the VirusScan console to protect your systems against autorun infections:

- How to use Access Protection policies in VirusScan 8.5i to prevent malware from changing folder options (KB53356)
- How to use Access Protection policies in VirusScan 8.5i to protect against viruses that can disable Regedit (KB53346)
- How to use Access Protection policies in VirusScan 8.5i to protect against viruses that can disable Task Manager (KB53355)

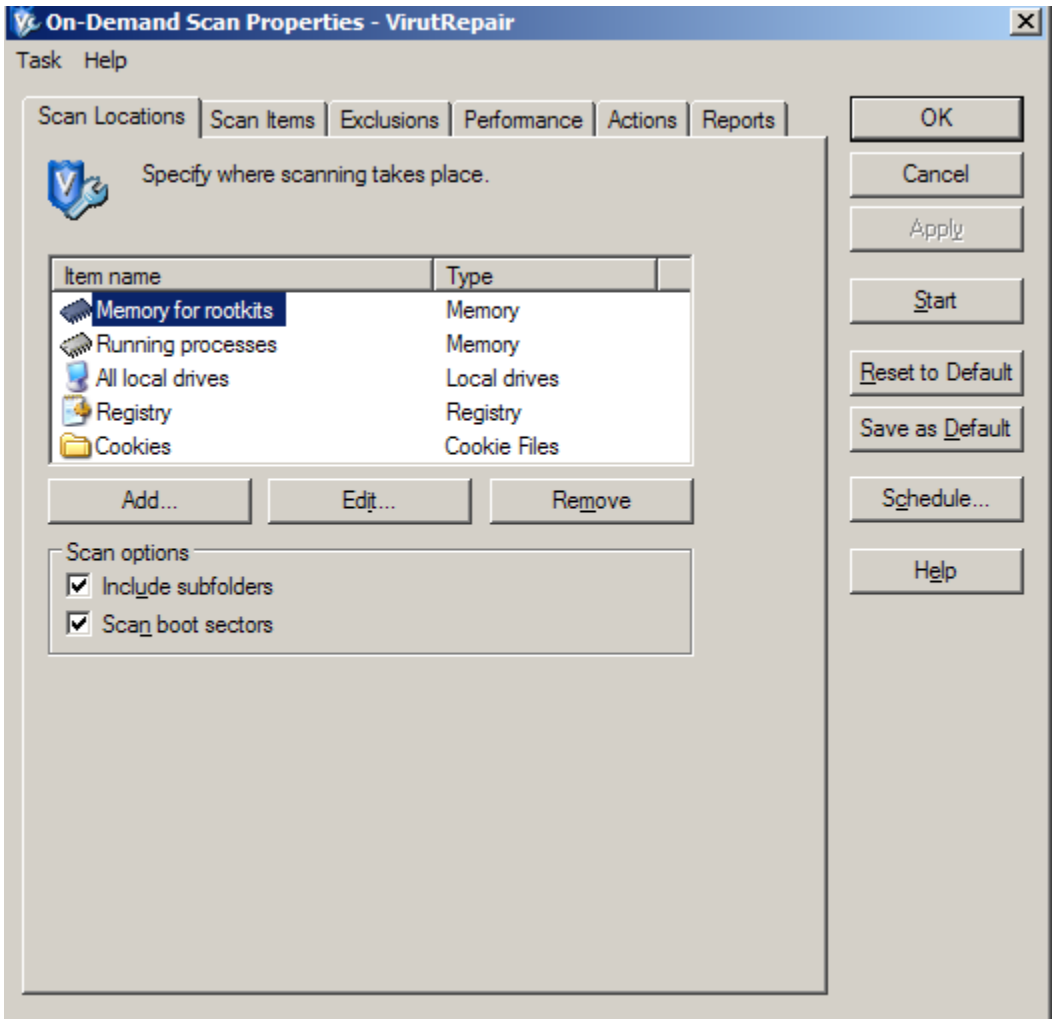
Eradication

You must run a full On-Demand Scan to clean an infected host. In some cases, it may also be necessary to run the On-Demand Scan in Safe Mode, as well as run a second scan with a reboot in-between. It is also critical that the On-Demand Scan be configured properly. Scan:

- All Local Drives
- Memory for Rootkits
- Running Processes
- Registry
- First “Action” set to “Clean”

The full, recommended process is to:

- Launch a full On-Demand Scan with the prior-documented configuration
- Allow the scan to run to completion
- Reboot
- Launch a second scan and allow it to run to completion to verify that the system has been cleaned



Appendix A: Additional W32/Virut Variants

W32/Virut—http://vil.nai.com/vil/content/v_141339.htm
W32/Virut!htm—http://vil.nai.com/vil/content/v_143831.htm
W32/Virut!mem—http://vil.nai.com/vil/content/v_147991.htm
W32/Virut!rtf—http://vil.nai.com/vil/content/v_154193.htm
W32/Virut.a—http://vil.nai.com/vil/content/v_139473.htm
W32/Virut.a!9BFCFE19—http://vil.nai.com/vil/content/v_146503.htm
W32/Virut.b—http://vil.nai.com/vil/content/v_139898.htm
W32/Virut.c—http://vil.nai.com/vil/content/v_141430.htm
W32/Virut.d—http://vil.nai.com/vil/content/v_141751.htm
W32/Virut.dr—http://vil.nai.com/vil/content/v_141969.htm
W32/Virut.e—http://vil.nai.com/vil/content/v_141927.htm
W32/Virut.f—http://vil.nai.com/vil/content/v_141957.htm
W32/Virut.g—http://vil.nai.com/vil/content/v_142563.htm
W32/Virut.gen—http://vil.nai.com/vil/content/v_142592.htm
W32/Virut.gen!BB215D78—http://vil.nai.com/vil/content/v_150582.htm
W32/Virut.gen!C33F18E0—http://vil.nai.com/vil/content/v_146499.htm
W32/Virut.gen.a—http://vil.nai.com/vil/content/v_143432.htm
W32/Virut.h—http://vil.nai.com/vil/content/v_143034.htm
W32/Virut.i—http://vil.nai.com/vil/content/v_143033.htm
W32/Virut.j—http://vil.nai.com/vil/content/v_143054.htm
W32/Virut.j!3C0367A2—http://vil.nai.com/vil/content/v_150634.htm
W32/Virut.j!82322FB0—http://vil.nai.com/vil/content/v_150653.htm
W32/Virut.j!C1CE762F—http://vil.nai.com/vil/content/v_150641.htm
W32/Virut.k—http://vil.nai.com/vil/content/v_143058.htm
W32/Virut.m—http://vil.nai.com/vil/content/v_153860.htm
W32/Virut.n—http://vil.nai.com/vil/content/v_154029.htm
W32/Virut.n!htm—http://vil.nai.com/vil/content/v_154039.htm
W32/Virut.n!inf—http://vil.nai.com/vil/content/v_154028.htm
W32/Virut.n!mem—http://vil.nai.com/vil/content/v_154030.htm
W32/Virut.n.gen—http://vil.nai.com/vil/content/v_154055.htm
W32/Virut.o—http://vil.nai.com/vil/content/v_154084.htm

Note on Heuristic Detections

New variants of W32/Virut are often detected heuristically under the following detection names:

- New Win32.g4
- New Win32.g3
- New Win32.g2
- New Win32.s-b

These heuristically detected samples should be submitted to Avert Labs via Webimmune.

Appendix B: Additional Tools

McAfee Avert Labs Stinger—http://vil.nai.com/vil/averttools.aspx

Stinger is a stand-alone scanning tool that can be used to scan and repair many high-profile threats, including W32/Virut. Stinger is updated approximately every four months. The signatures in the publicly posted Stinger tool may not be the latest available. However, custom Stinger builds are available through McAfee support channels. If you wish to request a custom Stinger build, please direct that request through your McAfee Support representative.

WinPE, BartPE (bootable clean environments)

These tools are handy for repairing systems that are too unstable for scanning and cleaning. The boot disk can be configured to include McAfee scanning tools and other utilities required to clean and repair a W32/Virut infection.

BartPE—http://nu2.nu/pebuilder/
WinPE—http://technet.microsoft.com/en-us/library/cc507857.aspx