McAfee Labs Threat Advisory

Trojan-Wiper

December 4, 2014

McAfee Labs periodically publishes Threat Advisories to provide customers with a detailed analysis of prevalent malware. This Threat Advisory contains behavioral information, characteristics, and symptoms that may be used to mitigate or discover this threat, and suggestions for mitigation in addition to the coverage provided by the DATs.

To receive a notification when a Threat Advisory is published by McAfee Labs, select to receive "Malware and Threat Reports" at the following URL**:** https://sns.snssecure.mcafee.com/content/signup_login.

Summary

McAfee Labs was made aware of a destructive malware capable of wiping files and disk sectors of affected machines. The malware is composed of several modules that performed different functions, including spreading over network utilizing a hard coded list of addresses.

The infection consists of modules that depict the following:

- Dropper/network spread module
- Ransom/reporting module
- Anti-AV module
- Web Server module

The samples utilized hard coded IP addresses and other information in order to spread. The malware does not have the ability to spread to an unrestricted list of IP addresses, but only to those hardcoded in its body, which is an indication that this attack is well organized and prior reconnaissance had been done on affected victims.

The known samples are covered by below generic McAfee detection:

- Trojan-Wiper

The list of filenames used by the known samples are listed below:

- COMON32.EXE
- DISKPARTMG16.EXE
- DPNSVR16.EXE
- EXPANDMN32.EXE
- HWRCOMPSVC64.EXE
- IGFXTRAYEX.EXE
- MOBSYNCLM64.EXE
- RDPSHELLEX32.EXE
- RECDISCM32.EXE
- TASKCHG16.EXE
- TASKHOSTS64.EXE
- ISSSRV.EXE
- USBDRV3.SYS

Detailed information about the threat, its propagation, characteristics and mitigation are in the following sections:

- Infection and Propagation Vectors
- Mitigation
- Characteristics and Symptoms
- Restart Mechanism
- Indicators of Compromise (IOC)
- McAfee Foundstone Services

The minimum DAT versions required for file detection are:

Detection Name	DAT Version	Date
Trojan-Wiper	7641	2014/12/03

Infection and Propagation Vectors

At the time of authoring, the initial delivery vector for this threat is not known. Post infection, the malware spreads laterally on the network via NetBIOS shares, to hardcoded IP addresses, using stolen usernames and passwords.

The spread mechanism used by the malware is NetBIOS over TCP/IP. The malware attempts to access the *$IPC* and *$ADMIN* shares on a list of machines hardcoded in the malware body.

The malware will attempt to save a copy of itself to either *$IPC* or *$ADMIN* shares on remote machines, using one of the names present in the summary section.

After saving the file to the remote machine, the malware will attempt to start a new service on the remote machine using Windows WMIC tool as shown below:

- wmic.exe /node:[123.123.123.123] /user:[username] /password:[password] PROCESS CALL CREATE "\\[123.123.123.123]\admin$\system32\taskchg16.exe"

This feature uses the remote admin capabilities in NetBIOS to create and start a new service on the remote machine. The IP address, username and passwords above are examples. These are stored within the malware body.

Mitigation

Mitigating the threat at multiple levels such as file, registry, and URL could be achieved at various layers of McAfee products. Browse the product guidelines available here (click Knowledge Center, and select Product Documentation from the Content Source list) to mitigate the threats based on the behavior described below in the "Characteristics and symptoms" section.

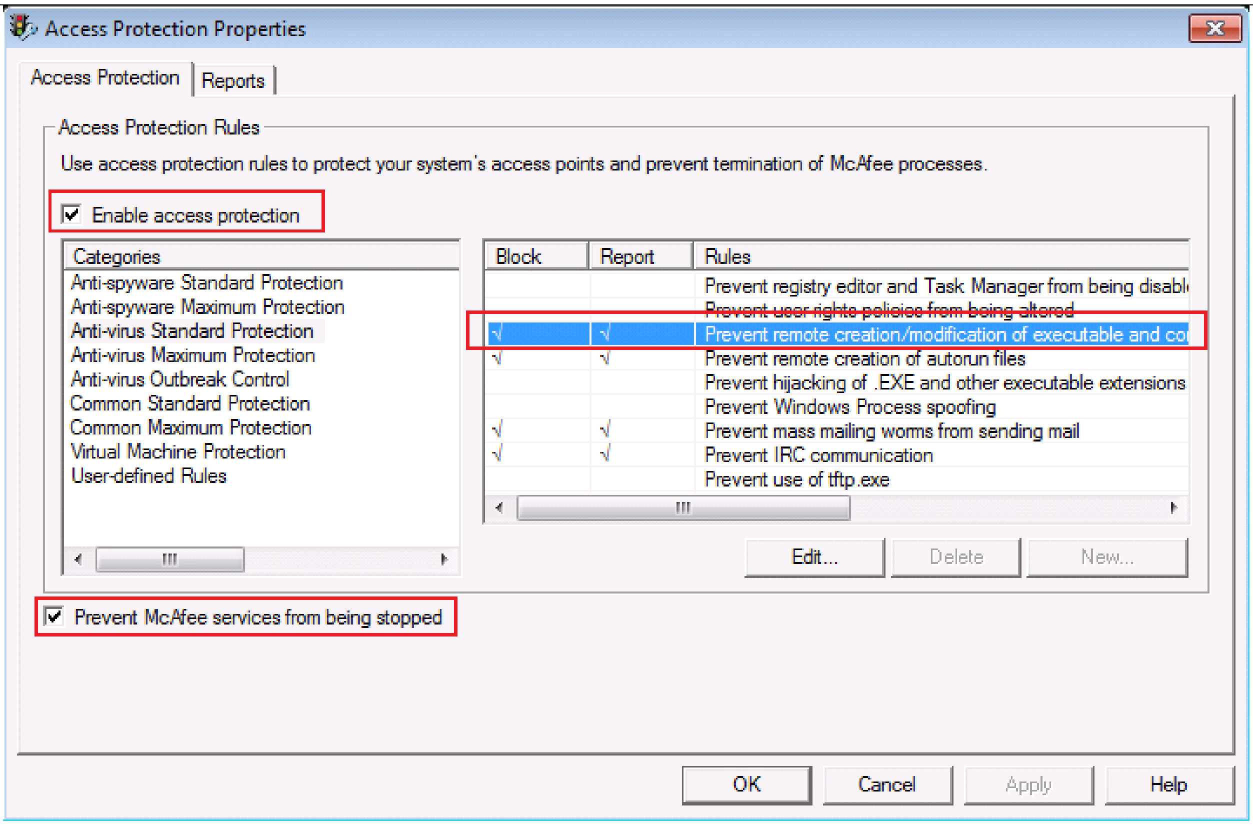
VSE (Virus Scan Enterprise)

Refer the following KB articles to configure Access Protection rules in VirusScan Enterprise:

- KB81095 - How to create a user-defined Access Protection Rule from a VSE 8.x or ePO 5.x console
- KB54812 - How to use wildcards when creating exclusions in VirusScan Enterprise 8.x

Users can configure and test Access Protection Rules to restrict the creation of new registry keys, files and folders when there are no other legitimate uses.

A quick way to block the spread mechanism of the Trojans described here is to enable the Access Protection rule to block the creation of remote executables. In the Access Protection configuration, click on Anti-virus Standard Protection then enable the blocking for the rule as shown as follows:



Access Protection Properties

Access Protection Rules

Use access protection rules to protect your system's access points and prevent termination of McAfee processes.

☑ Enable access protection

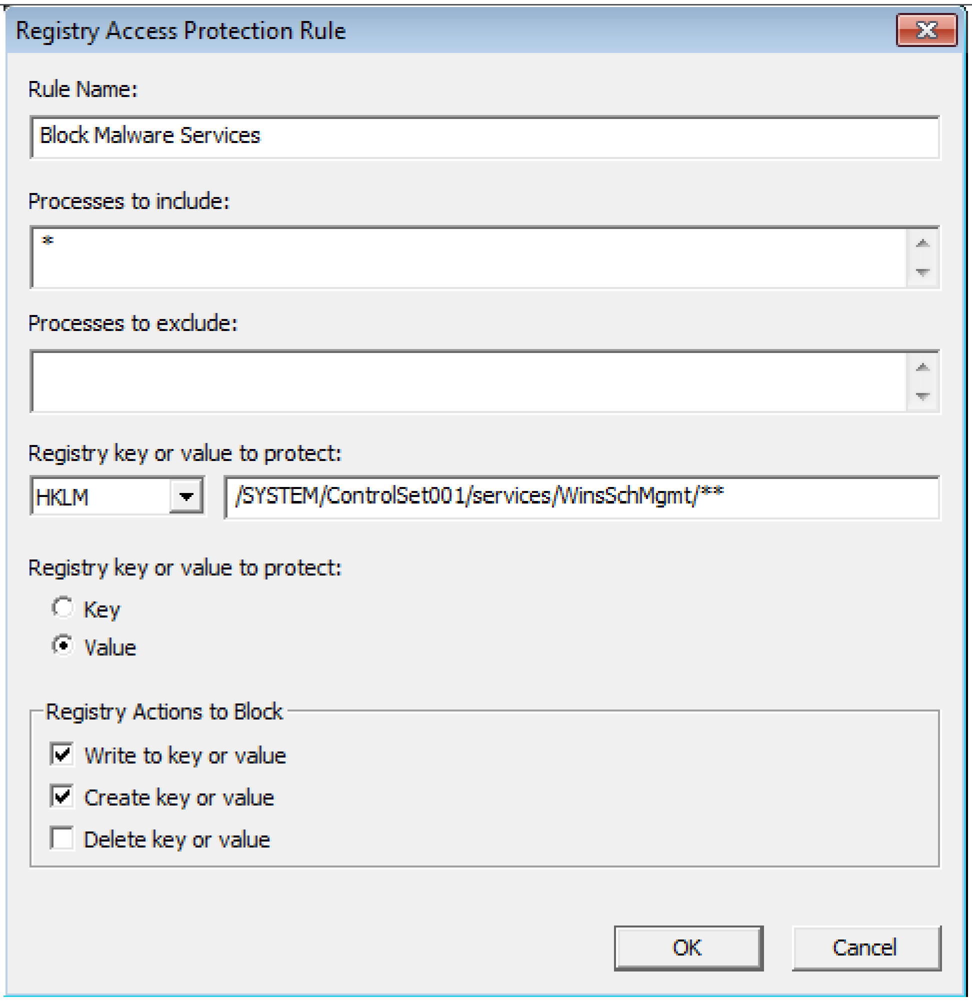
Categories
Anti-spyware Standard Protection
Anti-spyware Maximum Protection
Anti-virus Standard Protection
Anti-virus Maximum Protection
Anti-virus Outbreak Control
Common Standard Protection
Common Maximum Protection
Virtual Machine Protection
User-defined Rules

Block	Report	Rules
		Prevent registry editor and Task Manager from being disabl
		Prevent user rights policies from being altered
√	√	Prevent remote creation/modification of executable and co
√	√	Prevent remote creation of autorun files
		Prevent hijacking of .EXE and other executable extensions
		Prevent Windows Process spoofing
√	√	Prevent mass mailing worms from sending mail
√	√	Prevent IRC communication
		Prevent use of tftp.exe

☑ Prevent McAfee services from being stopped

Alternatively a user can create custom rules blocking the creation of the malware services (described in the next section). In order to do that, create a new User-defined rule and choose Registry Blocking Rule. Add the following information in Registry key or value to protect:

- HKLM/SYSTEM/ControlSet001/services/WinsSchMgmt/**



Registry Access Protection Rule

Rule Name: Block Malware Services

Processes to include: *

Processes to exclude:

Registry key or value to protect: HKLM /SYSTEM/ControlSet001/services/WinsSchMgmt/**

Registry key or value to protect:

○ Key

● Value

Registry Actions to Block

☑ Write to key or value

☑ Create key or value

□ Delete key or value

In “Process to Include” put an asterisk “*” and mark the options “Key” in Registry or Value to Protect, and mark the two checkboxes for “Write Key or Value” and “Create key or value”. Proceed the same way for other service you would like to block.

HIPS (Host Intrusion Prevention System)

- To blacklist applications using a Host Intrusion Prevention custom signature, refer to KB71329.
- To create an application blocking rules policies to prevent the binary from running, refer to KB71794.
- To create an application blocking rules policies that prevents a specific executable from hooking any other executable, refer to KB71794.
- To block attacks from a specific IP address through McAfee Nitrosecurity IPS, refer to KB74650.

Characteristics and Symptoms

As we have mentioned in the summary, this attack contains the following modules:

- Dropper/network spread module
- Ransom/communication module
- Anti-AV Module
- Web Server module

Dropper/network spread module

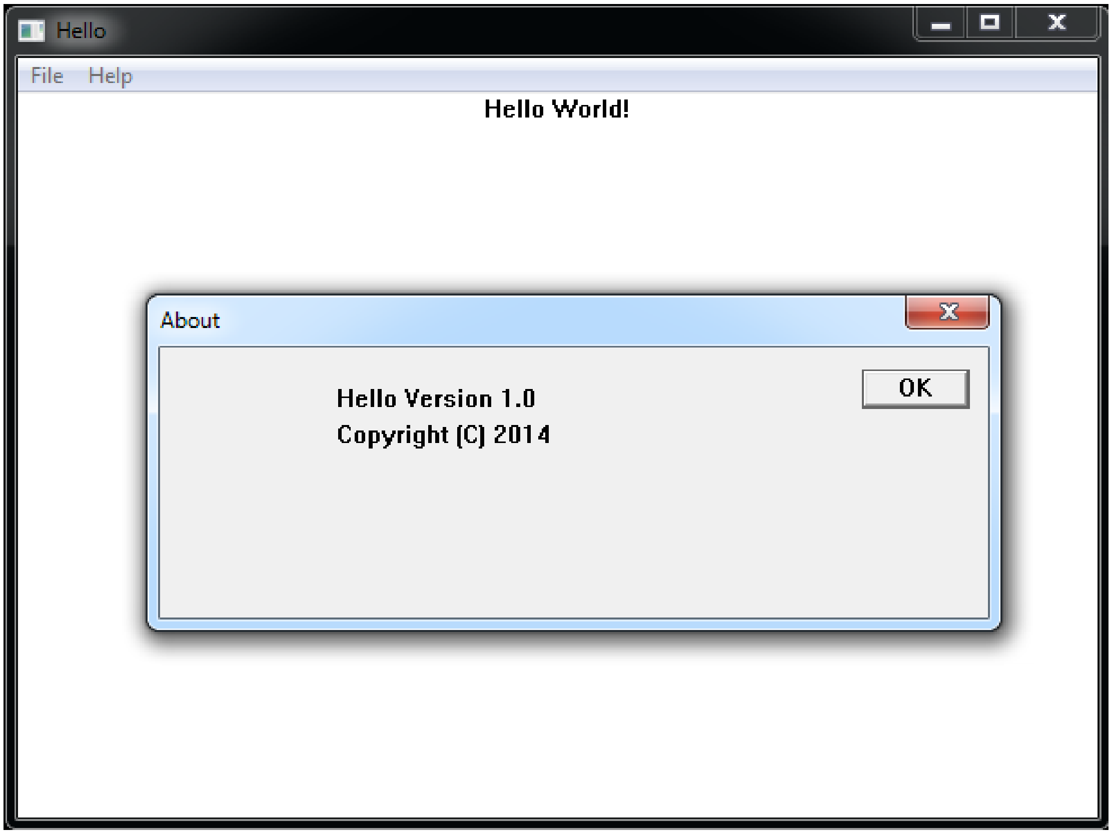
The dropper module is responsible for starting the infection on the target machines. The original delivery mechanism for this sample is not known, but once it is executed in a machine internal to victim’s network, it will attempt to spread to a list of hardcoded machine names and IP addresses using specific usernames and passwords, also hardcoded into the malware.

Once the malware is executed, it will install itself as a service under the following name:

- "WinsSchMgmt" with description "Windows Schedule Management Service"

After installing itself, the malware will decompress the Ransom module and install it as a service. The Ransom module is stored as a ZLIB packed blob of data at the end of the Dropper module. After installing and running the Ransom service, the dropper module will start its infection spreading mechanism in order to infect other machines in the network as described in the Infection and Propagation section.

The malware will execute the above actions if it is executed with **–i** parameter as well as no parameter passed. If any other parameter is used, the malware will show a default template windows for *Hello World* and with an *About windows available too, as shown below:*



Hello World!

Hello Version 1.0
Copyright (C) 2014

Ransom/communication module

The Ransom module, upon execution in the victim's system will stay in the memory for some time; it then starts to wipe the non-critical folders from the windows disk as well as files in remote shares mounted locally. The amount of time can vary, going from a few minutes to more than 1 hour before the disk wiping routines start.

The ransom module can be executed with many parameters which will change the behavior of the code. The description of these parameters are below:

-i : When executed with this parameter the malware will install itself as a service named as one of the examples below:
"**PMSvc**" with description " **Performance Manager**"
"**brmgmtsvc**" with description "**Backup and Restore Management Service**"

-k : With this parameter the malware will remove the service above leaving no traces of the installation

-d : This parameter will start the file wipe module immediately. All files in the local disk that are not in Program Files or Windows folder will be deleted, as well as any file in locally mounted remote shares.

-s : this parameter will cause the malware to attempt to mount specific remote shares using a hardcoded username and password. The files in the remote shares will then be enumerated and deleted.

-m : Drops a file named **usbdrv3.sys** in %TEMP% folder and created a service named “**usbdrv3**” with description “**USB 3.0 Host Controller**” pointing to it. This module is part of *Eldos Software RawDisk* kernel driver. See below for description. It will wipe the MBR of the disk rendering it unusable.

-a : When executed on Windows 7, this parameter will start the Anti-AV module in some variants of the malware. It will drop both anti-AV modules AMS.EXE and KPH.SYS in %TEMP% folder and start the process.

-w : In some variants of the malware, this parameter will drop and execute the Web Server used to display the malware ransom message.

The malware has some IP addresses hardcoded in it. These IP addresses are used as a beacon to report successful executions of the malware.

The hardcoded IPs are mentioned below:

AS	IP	CC	AS Name
37992	203.131.222.102	TH	THAMMASAT-BORDER-AS Thammasat University in thailand,TH
5617	217.96.33.164	PL	TPNET Orange Polska Spolka Akcyjna,PL
3269	88.53.215.64	IT	ASN-IBSNAZ Telecom Italia S.p.a.,IT
6866	212.31.102.100	CY	CYTA-NETWORK Cyprus Telecommunications Authority,CY
3758	58.185.154.99	SG	ERX-SINGNET SingNet,SG
6568	200.87.126.116	BO	Ag para el Desarrollo de la Sociedad de la Inf en Bolivia

Besides the IPs addresses mentioned above, the malware has hundreds of hardcoded user names, passwords, machine names and IP addresses hardcoded in its body. The usernames are used to map internal network shares and wipe files which indicate that the users used in this module have privileged access to some important resources.

The malware uses the following format to map the shares:

- net use \\<machinename> "<password>" /u:"<username>"
- cmd.exe /q /c net share shared$=%SystemRoot% /GRANT:everyone,FULL

The hardcoded user name and password in the malware indicates that the credentials were stolen before the malware was created.

The binaries have another interesting characteristic. All of them have a hidden Dialog window set as below:

- Hello Version 1.0
- Copyright (C) 2014
- Hello
- Hello World!

This seems to indicate the use of a template project.

As seen above, the malware makes use of a kernel driver to wipe de MBR of the disk rendering it unusable. This driver allows physical access to the disk from inside Windows. *Eldos Software RawDisk* is a commercial product used by many applications to enable raw access to the hard disk from within Windows. The kernel driver is user-locked, which means it only works if a user key is passed as parameter during the execution. Since such a key was present in the malware, it appears that this key may have been compromised and used as a part of this attack.

The Ransom component removes all files in the system and remote shares, leaving behind only Program Files and Windows folder.

Once the disk wiping is finished, the malware will contact one of the IP addresses above to report the successful operation. The traffic is not HTTP even though they use normal HTTP ports. This is done to avoid network filters to block the communication. The only information sent in the packet is the name of the machine that was wiped.

Finally, the ransom module also is capable of dropping either the Anti-AV or the Web Server modules, depending on which variant of the malware is used. The files are stored in its resource section as stated above.

Anti-AV Module

The second module is an anti-AV module which targets McAfee products.

It attempts to disable AV detection by disabling **MCSHIELD** service but is unsuccessful in doing so if AP is enabled (default product setting). To achieve this, it uses Process Hacker (a Process Explorer clone) kernel module **KPH.SYS**. The kernel module is used by process hacker to read information from all processes but in the malware case it is using it to have access to McAfee product's process memory.

Strings found in the Anti-AV binary module indicate that the malware targets McAfee services.

```
\Device\KProcessHacker2
SecurityLevel
System\CurrentControlSet\Services\%s\Parameters
KProcessHacker2
ImagePath
SYSTEM\CurrentControlSet\services\McShield
McShield
Open " goto Loop del " if exist " :Loop del "
\kph.sys
zawq.bat
mcshield.exe
\kph.sys
\mcshield.exe
UdaterUI.exe
McTray.exe
shstat.exe
FrameworkService.exe
VsTskMgr.exe
mfeann.exe
naPrdMgr.exe
```

Upon execution, the malware creates a service named "**KProcessHacker2**" pointing to file **KPH.SYS** and start it in order to attempt to kill McAfee process. It will enter a loop trying to remove the registry keys associated with the McAfee product and attempt to kill **MCSHIELD.EXE** from memory.

Web Server Module

The web server module does not contain any backdoor or remote communication capability, and seems to be used just to deliver the ransom message after the disk wiping is done. The module is dropped and executed by the wiping module if the parameter **–w** is passed, which is done after the wiper module finishes working.

Once executed, the malware tries to stop the following services:

- W3SVC
- WMServer
- SSIS
- SSRS
- MSDEPSVC

After that it will start a listener on port 80 and wait for connections to it. Once a connection is made, the malware does a few simple checks:

1. If the URI requested contain the string ".wav" the malware will extract the resource named RSRC_WAV, decrypt it and serve the file to the client
2. If the URI requested contain the string ".jpg" the malware will extract the resource named RSRC_JPG, decrypt it and serve the file to the client
3. If any other request is made, the malware extracts the resource named RSRC_HTML, decrypt is and serve

to the client.

The HTML file contains a ransom message.

Restart Mechanism

The malware installs itself as the services described in the IOC section below. The restart mechanism is useless since the malware wipes the system and will not boot again.

Indicators of Compromise (IOC)

The following indicators can be used to identify potentially infected machines in an automated way.
Presence of the following files and/or folders:

- COMON32.EXE
- DISKPARTMG16.EXE
- DPNSVR16.EXE
- EXPANDMN32.EXE
- HWRCOMPSVC64.EXE
- IGFXTRAYEX.EXE
- MOBSYNCLM64.EXE
- RDPSHELLEX32.EXE
- RECDISCM32.EXE
- TASKCHG16.EXE
- TASKHOSTS64.EXE
- AMS.EXE
- KPH.SYS
- Usbdrv3.sys

Presence of the following Services:

- "PMSvc" with description "Performance Manager"
- "brmgmtsvc" with description "Backup and Restore Management Service"
- "WinsSchMgmt" with description "Windows Schedule Management Service"
- "Usbdrv3" with description "USB 3.0 Host Controller" pointing to a file in %TEMP% folder
- "KProcessHacker2" with description "KProcessHacker2" pointing to file "KPH.sys"

Network communication to any of the IP addresses below at the network gateway/IPS level:

- 212.31.102.100
- 58.185.154.99
- 200.87.126.116
- 203.131.222.102
- 217.96.33.164
- 88.53.215.64

The ports used by the malware can be one of the following:

- 80
- 8080
- 8000

Presence of network communication over NetBIOS attempting to save EXE files on *$IPC* and *$ADMIN* shares.

Presence of unexpected network shares mounted on the machine. The malware seems to use the drive **U:** and above to mount them.

Getting Help from the McAfee Foundstone Services team

This document is intended to provide a summary of current intelligence and best practices to ensure the highest level of protection from your McAfee security solution. The McAfee Foundstone Services team offers a full range of strategic and technical consulting services that can further help to ensure you identify security risk and build effective solutions to remediate security vulnerabilities.

You can reach them here: https://secure.mcafee.com/apps/services/services-contact.aspx

This Advisory is for the education and convenience of McAfee customers. We try to ensure the accuracy, relevance, and timeliness of the information and events described; they are subject to change without notice.