PE_MOFKSYS.A

trendmicro.com/vinfo/us/threat-encyclopedia/malware/PE_MOFKSYS.A/

Modified by: Sabrina Lei Sioting

OVERVIEW

Infection Channel: Downloaded from the Internet, Dropped by other malware, Infects files

This file infector arrives on a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites.

It uses Windows Task Scheduler to create a scheduled task that executes the dropped copy.

It modifies registry entries to disable various system services. This action prevents most of the system functions to be used.

It prepends its codes to target files.

It executes commands from a remote malicious user, effectively compromising the affected system.

It steals certain information from the system and/or the user.

TECHNICAL DETAILS

Arrival Details

This file infector arrives on a system as a file dropped by other malware or as a file downloaded unknowingly by users when visiting malicious sites.

Installation

This file infector drops the following non-malicious files:

- %System%\cmsys.cmn
- %User Profile%\Application Data\icsys.icn

(Note: *%System%* is the Windows system folder, which is usually C:\Windows\System32.. *%User Profile%* is the current user's profile folder, which is usually C:\Documents and Settings\{user name} on Windows 2000, XP, and Server 2003, or C:\Users\{user name} on Windows Vista and 7.)

It uses Windows Task Scheduler to create a scheduled task that executes the dropped copy.

Autostart Technique

This file infector adds the following registry entries to enable its automatic execution at every system startup:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\RunOnce
Svchost = "%Windows%\svchost.exe RO"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Active Setup\Installed Components\{Random CLSID}
StubPath = "%Application Data%\mrsys.exe MR"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\RunOnce
Explorer = "%System%\explorer.exe RO"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\Run
Explorer = "%System%\explorer.exe RU"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\Run
Svchost = "%Windows%\svchost.exe RU"

It modifies the following registry entries to ensure it automatic execution at every system startup:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows NT\CurrentVersion\Winlogon
Shell = "%Windows%\explorer.exe, %System%\explorer.exe"

(Note: The default value data of the said registry entry is *Explorer.exe*.)

The scheduled task executes the malware at the following period:

> Everyday at malware's first execution time

Other System Modifications

This file infector adds the following registry entries as part of its installation routine:

HKEY_CURRENT_USER\Software\VB and VBA Program Settings\
Explorer\Process
LO = "1"

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\Schedule
AtTaskMaxHours = "48"

It adds the following registry keys as part of its installation routine:

HKEY_CURRENT_USER\Software\VB and VBA Program Settings

HKEY_CURRENT_USER\Software\VB and VBA Program Settings\
Explorer

HKEY_CURRENT_USER\Software\VB and VBA Program Settings\
Explorer\Process

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Active Setup\Installed Components\{Random CLSID}

It modifies registry entries to disable the following system services:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\SharedAccess
Start = "4"

(Note: The default value data of the said registry entry is *2*.)

It modifies the following registry entries to hide files with Hidden attributes:

HKEY_CURRENT_USER\Software\Microsoft\
Windows\CurrentVersion\Explorer\
Advanced
ShowSuperHidden = "0"

(Note: The default value data of the said registry entry is *1*.)

File Infection

This file infector infects the following file types:

- .EXE

It prepends its codes to target files.

This is the Trend Micro detection for files infected by:

- PE_MOFKSYS.A-O

Backdoor Routine

This file infector executes the following commands from a remote malicious user:

- Update itself
- Download other files
- Capture screen
- Log Keystrokes
- Monitor mouse clicks
- Monitor window titles

It connects to the following URL(s) to send and receive commands from a remote malicious user:

- {BLOCKED}.t35.com
- {BLOCKED}.atspace.com
- {BLOCKED}.zxq.net

Dropping Routine

This file infector drops the following files:

- %Application Data%\mrsys.exe - detected as PE_MOFKSYS.A-O
- %Windows%\spoolsv.exe - detected as PE_MOFKSYS.A-O
- %Windows%\svchost.exe - detected as PE_MOFKSYS.A-O
- %System%\explorer.exe - detected as PE_MOFKSYS.A-O
- %User Profile%\Application Data\icsys.icn.exe - detected as PE_MOFKSYS.A-O
- %System Root%\Documents and Settings\All Users\Application Data\stsys.exe - detected as PE_MOFKSYS.A-O

(Note: *%Application Data%* is the current user's Application Data folder, which is usually C:\Documents and Settings\{user name}\Application Data on Windows 2000, XP, and Server 2003, or C:\Users\{user name}\AppData\Roaming on Windows Vista and 7.. *%Windows%* is the Windows folder, which is usually C:\Windows.. *%System%* is the Windows system folder, which is usually C:\Windows\System32.. *%User Profile%* is the current user's profile folder, which is usually C:\Documents and Settings\{user name} on Windows 2000, XP, and Server 2003, or C:\Users\{user name} on Windows Vista and 7.. *%System Root%* is the root folder, which is usually C:\. It is also where the operating system is located.)

Information Theft

This file infector steals the following information:

- Email configurations
- - User name
- - Password
- - Authenticate status

- - Use of SSL
- - SMTP server
- - SMTP port
- - recipients
- Instant messenger credentials
- Websites visited
- Clipboard contents

Drop Points

This file infector uses its own SMTP engine to send the stolen data using the following domain server:

- {BLOCKED}1@gmail.com
- {BLOCKED}1@gmail.com
- {BLOCKED}2@gmail.com
- {BLOCKED}2@gmail.com
- {BLOCKED}6@gmail.com

NOTES:

It infects all .EXE files inside the folders that was accessed by the user in all physical and removable drives.

It also shares the following folder in the network:

> %System Root%\Documents and Settings\All User\Application Data

SOLUTION

Step 1

Before doing any scans, Windows XP, Windows Vista, and Windows 7 users must disable *System Restore* to allow full scanning of their computers.

Step 2

Remove the malware/grayware file that dropped/downloaded PE_MOFKSYS.A

> PE_MOFKSYS.A-O

Step 3

Identify and delete files detected as PE_MOFKSYS.A using the *Recovery Console*

[Learn More]

Step 4

Delete this registry key

[Learn More]

Important: Editing the *Windows Registry* incorrectly can lead to irreversible system malfunction. Please do this step only if you know how or you can ask assistance from your system administrator. Else, check this Microsoft article first before modifying your computer's registry. Before you could do this, you must restart in Safe Mode. For instructions on how to do this, you may refer to this page If the preceding step requires you to restart in safe mode, you may proceed to edit the system registry.

In *HKEY_CURRENT_USER\Software*
VB and VBA Program Settings

Step 5

Delete the random registry key/s that this malware created

[Learn More]

Important: Editing the *Windows Registry* incorrectly can lead to irreversible system malfunction. Please do this only if you know how to or you can seek your system administrator's help. You may also check out this Microsoft article first before modifying your computer's registry.

Step 6

Delete this registry value

[Learn More]

Important: Editing the *Windows Registry* incorrectly can lead to irreversible system malfunction. Please do this step only if you know how or you can ask assistance from your system administrator. Else, check this Microsoft article first before modifying your computer's registry.

- In *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce*
  Explorer = "%System%\explorer.exe RO"
- In *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce*
  Svchost = "%Windows%\svchost.exe RO"
- In *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*
  Explorer = "%System%\explorer.exe RU"

- In *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*
  Svchost = "%Windows%\svchost.exe RU"
- In *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Schedule*
  AtTaskMaxHours = "48"

Step 7

Restore this modified registry value

[Learn More]

Important: Editing the *Windows Registry* incorrectly can lead to irreversible system malfunction. Please do this step only if you know how or you can ask assistance from your system administrator. Else, check this Microsoft article first before modifying your computer's registry.

- In *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon*
  From: **Shell = "%Windows%\explorer.exe, %System%\explorer.exe"**
  To: **Shell = Explorer.exe**
- In *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess*
  From: **Start = "4"**
  To: **Start = 2**
- In *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced*
  From: **ShowSuperHidden = "0"**
  To: **ShowSuperHidden = 1**

Step 8

Scan your computer with your Trend Micro product to clean files detected as PE_MOFKSYS.A. If the detected files have already been cleaned, deleted, or quarantined by your Trend Micro product, no further step is required. You may opt to simply delete the quarantined files. Please check this Knowledge Base page for more information.

Did this description help? Tell us how we did.