Trojan.Volgmer | Symantec

Discovered: August 18, 2014
Updated: August 20, 2014 2:45:26 PM
Type: Trojan
Infection Length: Varies
Systems Affected: Windows

Trojan.Volgmer is a Trojan horse that opens a back door on the compromised computer.

Antivirus Protection Dates

- **Initial Rapid Release version** August 18, 2014 revision 008
- **Latest Rapid Release version** January 25, 2018 revision 019
- **Initial Daily Certified version** August 18, 2014 revision 019
- **Latest Daily Certified version** January 26, 2018 revision 002
- **Initial Weekly Certified release date** August 20, 2014

Click here for a more detailed description of Rapid Release and Daily Certified virus definitions.

Writeup By: Junnosuke Yagi

Discovered: August 18, 2014
Updated: August 20, 2014 2:45:26 PM
Type: Trojan
Infection Length: Varies
Systems Affected: Windows

Once executed, the Trojan creates the following files:

- %System%\[RANDOM FILE NAME].dll
- %Temp%\pdm.bat

It then creates a service with the following properties:

- **Display Name:** [RANDOM SERVICE NAME]
- **Image Path:** %System%\svchost.exe -k LocalSystems
- **Description:** The [RANDOM SERVICE NAME] is an essential service for management of Windows System. If the service is stopped or disabled, Windows will be able to damaged seriously.

Note: [RANDOM SERVICE NAME] may be composed of the following words:

- Application
- Background
- Control
- Desktop
- Extension
- Function
- Group
- Host
- Intelligent
- Key
- Layer
- Multimedia
- Network
- Operation
- Portable
- Quality
- Remote
- Security
- TCP/IP
- User Profile
- Volume
- Windows
- Device
- Upd
- Service
- Management
- Manager
- Enum

For example: Control Portable Volume Manager or Background Operation Windows Manager

The Trojan then creates the following registry subkey to register itself as a service:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\[RANDOM FILE NAME]

It also creates the following registry entries:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Security\"f0012345-2a9c-bdf8-345d-345d67b542a1" = "[HEXADECIMAL VALUE]"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Security\"125463f3-2a9c-bdf0-d890-5a98b08d8898" = "[HEXADECIMAL VALUE]"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_[RANDOM FILE NAME]\0000\"Service" = "[RANDOM FILE NAME]"

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_[RANDOM FILE NAME]\0000\"Legacy" = "1"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_[RANDOM FILE NAME]\0000\"DeviceDesc" = "[RANDOM SERVICE NAME]"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_[RANDOM FILE NAME]\0000\"ConfigFlags" = "0"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_[RANDOM FILE NAME]\0000\"ClassGUID" = "{8ECC055D-047F-11D1-A537-0000F8753ED1}"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_[RANDOM FILE NAME]\0000\"Class" = "LegacyDriver"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_[RANDOM FILE NAME]\"NextInstance" = "1"

Next, the Trojan connects to one or more of the following IP addresses on TCP port 8080 or 8088:

- 113.28.244.194
- 116.48.145.179
- 186.116.9.20
- 193.28.91.232
- 199.15.234.120
- 200.42.69.133
- 220.128.131.251
- 24.242.176.130
- 78.93.190.70
- 89.190.188.42

The Trojan then opens a back door on the compromised computer, allowing an attacker to perform the following actions:

- Gather system information
- Download and execute files
- Update service registry key
- Upload files

Gathered system information may include the following:

- Computer name
- IP address
- Drive name and serial number
- Locale information
- TCP connection state
- Operating system version
- Process list

Recommendations

Symantec Security Response encourages all users and administrators to adhere to the following basic security "best practices":

- Use a firewall to block all incoming connections from the Internet to services that should not be publicly available. By default, you should deny all incoming connections and only allow services you explicitly want to offer to the outside world.
- Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers. This helps to prevent or limit damage when a computer is compromised.
- Ensure that programs and users of the computer use the lowest level of privileges necessary to complete a task. When prompted for a root or UAC password, ensure that the program asking for administration-level access is a legitimate application.
- Disable AutoPlay to prevent the automatic launching of executable files on network and removable drives, and disconnect the drives when not required. If write access is not required, enable read-only mode if the option is available.
- Turn off file sharing if not needed. If file sharing is required, use ACLs and password protection to limit access. Disable anonymous access to shared folders. Grant access only to user accounts with strong passwords to folders that must be shared.
- Turn off and remove unnecessary services. By default, many operating systems install auxiliary services that are not critical. These services are avenues of attack. If they are removed, threats have less avenues of attack.
- If a threat exploits one or more network services, disable, or block access to, those services until a patch is applied.
- Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services.
- Configure your email server to block or remove email that contains file attachments that are commonly used to spread threats, such as .vbs, .bat, .exe, .pif and .scr files.
- Isolate compromised computers quickly to prevent threats from spreading further. Perform a forensic analysis and restore the computers using trusted media.
- Train employees not to open attachments unless they are expecting them. Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.
- If Bluetooth is not required for mobile devices, it should be turned off. If you require its use, ensure that the device's visibility is set to "Hidden" so that it cannot be scanned by other Bluetooth devices. If device pairing must be used, ensure that all devices are set to "Unauthorized", requiring authorization for each connection request. Do not accept applications that are unsigned or sent from unknown sources.
- For further information on the terms used in this document, please refer to the Security Response glossary.

Writeup By: Junnosuke Yagi

Discovered: August 18, 2014
Updated: August 20, 2014 2:45:26 PM
Type: Trojan

Infection Length: Varies
Systems Affected: Windows

You may have arrived at this page either because you have been alerted by your Symantec product about this risk, or you are concerned that your computer has been affected by this risk.

Before proceeding further we recommend that you run a full system scan . If that does not resolve the problem you can try one of the options available below.

FOR NORTON USERS
If you are a Norton product user, we recommend you try the following resources to remove this risk.

Removal Tool

- Run Norton Power Eraser (NPE)
- Norton Power Eraser did not remove this risk

If you have an infected Windows system file, you may need to replace it using the Windows installation CD .

How to reduce the risk of infection
The following resources provide further information and best practices to help reduce the risk of infection.

- Operating system updates to fix vulnerabilities
- File sharing protection
- Disable Autorun (CD/USB)
- Best practices for instant messaging
- Best practices for browsing the Web
- Best practices for email

FOR BUSINESS USERS
If you are a Symantec business product user, we recommend you try the following resources to remove this risk.

Identifying and submitting suspect files
Submitting suspicious files to Symantec allows us to ensure that our protection capabilities keep up with the ever-changing threat landscape. Submitted files are analyzed by Symantec Security Response and, where necessary, updated definitions are immediately distributed through LiveUpdate™ to all Symantec end points. This ensures that other computers nearby are protected from attack. The following resources may help in identifying suspicious files for submission to Symantec.

- Locate a sample of a threat
- Submit a suspicious file to Symantec

Removal Tool

- Run Symantec Power Eraser in Symantec Help (SymHelp)
- About Symantec Power Eraser
- Symantec Power Eraser User Guide

If you have an infected Windows system file, you may need to replace it using the Windows installation CD .

How to reduce the risk of infection

The following resource provides further information and best practices to help reduce the risk of infection.
Protecting your business network

MANUAL REMOVAL

The following instructions pertain to all current Symantec antivirus products.

1. Performing a full system scan

How to run a full system scan using your Symantec product

2. Restoring settings in the registry

Many risks make modifications to the registry, which could impact the functionality or performance of the compromised computer. While many of these modifications can be restored through various Windows components, it may be necessary to edit the registry. See in the Technical Details of this writeup for information about which registry keys were created or modified. Delete registry subkeys and entries created by the risk and return all modified registry entries to their previous values.

Writeup By: Junnosuke Yagi
