

Infostealer.Catchamas | Symantec

Archived: 2026-04-06 02:00:46 UTC

The Wayback Machine - <https://web.archive.org/web/20190508165711/https://www-west.symantec.com/content/symantec/english/en/security-center/writeup.html/2018-040209-1742-99>

Discovered: March 14, 2018

Updated: April 02, 2018 10:17:05 AM

Type: Trojan

Infection Length: Varies

Systems Affected: Windows

Infostealer.Catchamas is a Trojan horse that steals information from the compromised computer.

Antivirus Protection Dates

- **Initial Rapid Release version** March 14, 2018 revision 020
- **Latest Rapid Release version** November 06, 2018 revision 032
- **Initial Daily Certified version** March 14, 2018 revision 038
- **Latest Daily Certified version** November 07, 2018 revision 002
- **Initial Weekly Certified release date** March 21, 2018

Click [here](#) for a more detailed description of Rapid Release and Daily Certified virus definitions.

Writeup By: Mark Anthony Balanza

Discovered: March 14, 2018

Updated: April 02, 2018 10:17:05 AM

Type: Trojan

Infection Length: Varies

Systems Affected: Windows

When this Trojan is executed, it creates the following files:

- %UserProfile%\Local Settings\Microsoft\Windows\Caches\caches_version.db
- %System%\wbem\tmf\caches_version.db
- [PATH TO MALWARE]\info.config

The Trojan then creates the following registry entries:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\NetAdapter\ "Description" = "Study the net adapters to which the computer has connected, collects and stores properties for these net adapters, and notifies applications when these properties change."

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\NetAdapter\ "DisplayName" = "NetAdapter"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\NetAdapter\ "ImagePath" = "[PATH TO MALWARE][MALWARE FILE NAME] /ins"

Next, the Trojan steals the following information from the compromised computer:

- Keystrokes
- Clipboard data
- Screenshot based on specified keywords in the window title
- Network adapter information such as Mac address, IP address, adapter name, adapter description, etc.

The Trojan then saves the stolen information in the following locations:

- %UserProfile%\Local Settings\Microsoft\Windows\Caches\caches_version.db
- %System%\wbem\tmf\caches_version.db
- %UserProfile%\Local Settings\Microsoft\Windows\Burn\[KEYWORD]_[NUMBER].bmp
- %System%\wbem\xml\[KEYWORD]_[NUMBER].bmp

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: Mark Anthony Balanza

Discovered: March 14, 2018

Updated: April 02, 2018 10:17:05 AM

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

- [Download SymDiag to detect Symantec product issues](#)
- [About the Threat Analysis Scan in SymDiag](#)
- [About Symantec Power Eraser](#)
- [What you should know before you run Power Eraser](#)

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: Mark Anthony Balanza