OSX.Calisto | Symantec

Discovered: July 30, 2018
Updated: July 30, 2018 2:44:38 PM
Type: Trojan
Infection Length: Varies
Publisher: Nevaeh Peterson
Systems Affected: Mac

OSX.Calisto is a Trojan horse that opens a backdoor on the compromised computer.

Antivirus Protection Dates

- **Initial Rapid Release version** July 30, 2018 revision 007
- **Latest Rapid Release version** July 30, 2018 revision 017
- **Initial Daily Certified version** July 30, 2018 revision 008
- **Latest Daily Certified version** July 30, 2018 revision 021
- **Initial Weekly Certified release date** August 01, 2018

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

Writeup By: Jason Pantig

Discovered: July 30, 2018
Updated: July 30, 2018 2:44:38 PM
Type: Trojan
Infection Length: Varies
Publisher: Nevaeh Peterson
Systems Affected: Mac

Once executed, the Trojan creates the following folder:

- /Users/[USER NAME]/calisto

The Trojan creates the following files:

- /Users/[USER NAME]/calisto/calisto.zip
- /Users/[USER NAME]/calisto/cred.dat
- /Users/[USER NAME]/calisto/network.dat
- /Users/[USER NAME]/calisto/KC.zip

Next, the Trojan uninstalls the DMG component on the compromised computer.

The Trojan then establishes remote access to the compromised computer in order to perform the following actions:

- Enable remote login
- Enable screen sharing
- Add permissions
- Add remote login to all users
- Add its own account

The Trojan connects to the following remote locations:

- http://40.[REMOVED].56.192/calisto/listenyee.php
- http://40.[REMOVED].56.192/calisto/upload.php

The Trojan then opens a backdoor on the compromised computer and may perform the following actions:

- Upload files
- Download files
- Execute files
- Steal keychains
- Steal cookies

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: Jason Pantig

Discovered: July 30, 2018
Updated: July 30, 2018 2:44:38 PM
Type: Trojan
Infection Length: Varies
Publisher: Nevaeh Peterson
Systems Affected: Mac

The following instructions pertain to all current and recent Symantec antivirus products for Mac.

1. Update the virus definitions.
2. Run a full system scan and repair or delete all the files detected.

For specific details on each of these steps, read the following instructions.

1. To update the virus definitions
To obtain the most recent virus definitions run LiveUpdate: These virus definitions are posted to the LiveUpdate servers regularly. To determine whether definitions for this threat are available by LiveUpdate, refer to the Virus Definitions (LiveUpdate) .

2. To scan for and delete the infected files

- Start your Norton AntiVirus or Symantec Endpoint Protection for Mac program and make sure that it is configured to scan all files.
- Run a full system scan.
- If any files are detected, click Repair (if available) or Delete.

Writeup By: Jason Pantig
