FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

27 MAR 2017

Alert Number

MC-000080-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact **FBI CYWATCH immediately**.

Email: **cywatch@ic.fbi.gov**

Phone: **1-855-292-3937**

*****_Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks._

In furtherance of public-private partnerships, the FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

This FLASH has been released TLP: AMBER: The recipients may only share this information with members of their own organization who need to know, and only as widely as necessary to act on that information.

Indicators Associated with Fruitfly/Quimitchin Malware

Summary

The FBI is providing the following information with HIGH confidence:

The FBI obtained indicators of compromise related to the Fruitfly/Quimitchin[i] malware based on targeting of an identified US university in early January 2017. The malware was used to access user information, log keystrokes to gather credentials, and pivot into other systems and services.

Background

According to an open source article citing a prominent security software maker, the Fruitfly/Quimitchin malware adds compatibility for antiquated code associated with Macintosh computers. The same article cited a Malwarebytes blog post, which indicated the malware communicates with command-and-control servers and can perform actions like typing, webcam and screen captures, and moving and clicking a mouse cursor.

Technical Details

The attack vector included the scanning and identification of externally facing Mac services to include the Apple Filing Protocol (AFP, port 548), RDP, VNC, SSH (port 22), and Back to My Mac (BTMM), which would be targeted with weak passwords or passwords derived from 3rd party data breaches.

[i] According to an 18 January 2017 open source report from appleinsider.com, US business Apple identifies the malware as "Fruitfly" and the Malwarebytes app identifies the code as "OSX.Backdoor.Quimitchin."

The following network indicators are attributed to the Fruitfly/Quimitchin malware (best indicators):
eidk.duckdns.org
eidk.hopto.org
tmp1.hopto.org
tmp2.hopto.org
eutq.hopto.org (historic, circa 2012)
99.153.29.240

The following Mac-based indicators are attributed to the Fruitfly.Quimitchin malware:

1. ~/Library/LaunchAgents/
2. ~/.tmp
3. ~/.client
4. ~/.cr or ~/.cr2

Context for the above indicators:

1. Denotes persistence location (plist added to autorun malware)
2. Information staging directory
3. Actual malware
4. Webcam capturing component

The following Windows-based indicators are attributed to the Fruitfly/Quimitchin malware family:

Windows malware mimics the installation paths and executables for Sophos Antivirus.

- Path of %PROGRAMFILES%\Sophos Sweep for NT\
- Custom (per infection) executables with ‘SAVCleanupService.exe’ or ‘SAVService.exe’

Windows webcam capturing executables:

File name: camrec_remote_win.exe
File size: 37376 bytes
File type: PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows, UPX compressed
MD5: daac4a2111a103ec1f32a7d76b29925e
SHA1: b0da9296995d0182916735106bc40b2cdc300e07
SHA256:
afa11134ca13de15aa31c22e188013da90d17f92011ce90eb4a1d531cc097c73

SHA512:
009723f2692a9231d0cfac08a6db2ec99cc7504f863950eeba9bd6123db9c39f1df9e4fb322f4d7a929e721051532443e3733d8c8350b58c9b210c570f7f492a
Ssdeep: 768:ZoGozb5GTuiyA7HDO29ustWzP/4xFvcKt5WLn7yKvMjzkTEjmHx:ZzBSLAXOE2CcTn7yKvSkIyHx

File name: camrec_remote_win_vfw.exe
File size: 31232 bytes
File type: PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows, UPX compressed
MD5: 1816a76e375f1fe855b2555f80e107f9
SHA1: 32f0313464ef63092811f6e48382661a3de264e6
SHA256:
1820cacfab4627f46315d9d6e5d38263266d829eaecd3fbba7dc9d4102215506
SHA512:
dfec056d5eebd9477f9aed3e51b4418a93199115c3ef5ee50c928613a518d287b67612760a62704c8875d6f766b771dcf879281257bb29e026cbba276b68333c
Ssdeep:
384:sjNDzQaMENPe60lVwn9uV5hDIe+rfgyUxFnKRJGQgQf15mSFJiSUmX1WJlIVOpnf:gNDPlx8liIIXglxFYHJbTf1W3IVOJIk

Recommended Steps for Initial Mitigation

While remediation will vary based on local environment, systems affected will at a minimum need to be imaged, malware identified and removed, and passwords changed. Additionally, credentials of any service used on the system have likely been exposed, and those credentials should be changed. Those services have likely been accessed as a result of the exposure, and a separate damage assessment should be conducted per service. In enterprise environments, base images for systems and common program installations need to be checked for re-infection vectors.

References:

Internet Blog; Thomas Reed; malwarebytes.com; “New Mac Backdoor Using Antiquated Code”; Blog.malwarebytes.com/threat-analysis/2017/01/new-mac-backdoor-using-antiquated-code/; background.

Internet site; Roger Fingas; appleinsider.com; “‘Fruitfly’ malware patched by Apple relies on ‘ancient’ Mac system calls”; 18 January 2017; Appleinsider.com/articles/17/01/18/fruitfly-malware-patched-by-apple-relies-on-ancient-mac-system-calls; 8 March 2017; background.

Reporting Notice

The FBI encourages recipients who identify the use of tool(s) or techniques discussed in this document to report information to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at 855-292-3937 or by e-mail at CyWatch@ic.fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

Your Feedback on the Value of this Product Is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here:

https://www.ic3.gov/PIFSurvey

Please note that this survey is for feedback on content and value only. Reporting of technical information regarding FLASH reports must be submitted through FBI CYWATCH.