OS X Malware Samples Analyzed

1. AT&T Cybersecurity
2. Blog

March 21, 2016 | AT&T Alien Labs
By Eddie Lee and Krishna Kona

A couple of months ago, as we rang in 2016, we thought it would be interesting to take a quick look back at some OSX malware from 2015 and 2014. As reported by the team at Bit9+Carbon Black [1], 2015 marked “the most prolific year in history for OS X malware”. We collected a few samples of malware named in that report, along with some samples of other notable OSX malware, with the intention of learning more about them and fill in any gaps in our detection mechanisms (NIDS and Correlation rules). Although our primary objective was to capture network traffic from the malware samples, we were also interested in other aspects of the malware like persistence mechanisms (if any) that they utilized, so we documented that activity as well.

To start off with, we reviewed Flashback, one of the most infamous pieces of OS X malware that reminded everyone to the fact that OS X is not immune to malware. After that, we played with KitM, which is spyware, and LaoShu, a RAT. Then we analyzed Mask, a sophisticated malware that was used for cyber espionage. We also looked into CoinThief malware that steals bitcoins from the infected machine and the WireLurker malware that is capable of infecting iPhone devices connected to the compromised machine. Finally, we analyzed OceanLotus that was discovered May last year and found to be attacking Chinese government infrastructure. Below is a summary of our findings from analyzing the samples in a sandbox – the findings include links to fully executable samples, IDS signatures, persistence mechanisms and C&C details.

OS X Malware Details

Flashback

Description: Flashback masquerades as Adobe Flash player update or a signed-java applet. Downloads/installs Web Traffic Interception component to inject ads into HTTP/HTTPS streams http://go.eset.com/us/resources/white-papers/osx_flashback.pdf [no longer available].

Sample:
https://www.virustotal.com/en/file/58029f84c3826a0bd2757d2fe7405611b75ffc2094a80606662919dae68f946e/analysis/

Persistence mechanism: Installs a malicious file in user's home directory with the filename starting with a ‘dot' to hide itself and installs a LaunchAgent in ~/Library/LaunchAgents to refer to the created malicious file.

C&C communication: Uses DGA for CnC domain names and twitter hashtags to decode the address of CnC server.

AlienVault Detections:

- IDS
  Existing SIDs: 2014596, 2014597, 2014598, 2014599, 2014534, 2014522, 2014523, 2014524, 2014525
- System Compromise, Trojan infection, Flashback

Kumar in the Mac (KitM)

Description: KitM is a signed malware that can take screenshots, download and install programs, and steal data [5].

Sample:
https://www.virustotal.com/en/file/07062d9ecb16bd3a4ea00d434f469fe63d5c1c95d1b4903705de31353e9c92ce/analysis/

Persistence mechanism: Adds a Login Item at ~/Library/Preferences/com.apple.loginitems.plist

C&C server: liveapple[dot]eu (down)

AlienVault Detections:

- IDS rules: https://github.com/AlienVault-Labs/AlienVaultLabs/blob/master/malware_analysis/OSX_Malware/snort_kitm.rules
- System Compromise, Trojan infection, KitM

LaoShu

Description: LaoShu is a data stealing RAT. It has functionality to search for files, ex-filtrate files, download new file, and execute arbitrary commands [6].

Sample:
https://www.virustotal.com/en/file/5443ad1db119b599232b91bbf0ac3d0e1e4f4894f7f4ba191e7b9f7a27acea0d/analysis/

Persistence mechanism: None

C&C server: floracrunch[dot]com (down)

AlienVault Detections:

- IDS rules: https://github.com/AlienVault-Labs/AlienVaultLabs/blob/master/malware_analysis/OSX_Malware/snort_laoshu.rules
- System Compromise, Trojan infection, LaoShu

Appetite/Mask-Careto

Description: This is a state-of-the-art malware with Windows, Mac OS and Linux variants. The OS X variant uses a backdoor based on the open source Shadowinteger's Backdoor (SBD) [7].

Sample:
https://www.virustotal.com/en/file/0710be16ba8a36712c3cac21776c8846e29897300271f09ba0a41983e370e1a0/analysis/ (Verified executability: tries to connect to itunes212[dot]appleupdt[dot]com)

Persistence mechanism: Installs a LaunchAgent at Library/LaunchAgents/com.apple.launchport.plist and references a malicious binary in /Applications/.DS_Store.app

C&C servers:

- itunes212[dot]appleupdt[dot]com
- itunes214[dot]appleupdt[dot]com
- itunes311[dot]appleupdt[dot]com

(As of Feb 6, 2014, the above C&C domains have been suspended by Apple.)

AlienVault Detections:

- IDS
  - Existing SIDs: 2021712, 2021714, 2021715
  - New rules: https://github.com/AlienVault-Labs/AlienVaultLabs/blob/master/malware_analysis/OSX_Malware/snort_careto.rules
- System Compromise, Targeted Malware, Careto

CoinThief

Description: CoinThief installs browser extensions to steal credentials to popular Bitcoin wallet sites [8].

Sample:
https://www.virustotal.com/en/file/7d5eff5f83ab79e5f75acb9b84138561c8fd63ba00c050699c9f5be29d342f6e/analysis/

Persistence mechanism: Installs a LaunchAgent and browser extensions.

The LaunchAgent is installed at ~/Library/LaunchAgents/com.google.softwareUpdateAgent.plist and references a malicious binary at ~/Library/Application Support/.com.google.softwareUpdateAgent/com.google.softwareUpdateAgent.

A Safari extensions is installed at ~/Library/Safari/Extensions/Pop-Up Blocker.safariextz.

A Chrome extensions is installed at ~/Library/Application Support/Google/Chrome/Default/DefaultApps/noehjlabkmejilomimnebjkdjaoomabh/1.0.0_0.

C&C server: www[dot]media02-cloudfront[dot]com (down)

AlienVault Detections:

- IDS rules: https://github.com/AlienVault-Labs/AlienVaultLabs/blob/master/malware_analysis/OSX_Malware/snort_cointhief.rules
- System Compromise, Trojan infection, CoinThief

WireLurker

Description: WireLurker monitors an infected system for a USB connection to an iOS device and installs malicious applications on the device [9].

Sample:
https://www.virustotal.com/en/file/5d4f4fb2a663f1f79fb96edcd832374304af877938747b5844daacf4beba2427/analysis/

Persistence mechanism:

- Installs LaunchDaemons
- /System/Library/LaunchDaemons/com.apple.MailServiceAgentHelper.plist
- /System/Library/LaunchDaemons/com.apple.appstore.plughelper.plist
- /System/Library/LaunchDaemons/com.apple.periodic-dd-mm-yy.plist
- /System/Library/LaunchDaemons/com.apple.systemkeychain-helper.plist

C&C servers: www[dot]comeinbaby[dot]com (down)

AlienVault Detections:

IDS

Existing SIDs: 2019660, 2019661, 2019662, 2019663, 2019664, 2019665, 2019666, 2019667, 2019731, 2019718

- System Compromise, Malware infection, WireLurker
- System Compromise, Mobile trojan infection, WireLurker

OceanLotus

Description: OceanLotus is malware that has been used against Chinese targets and essentially gives attackers full control over a compromised machine [10] [11].

Sample:
https://www.virustotal.com/en/file/83cd03d4190ad7dd122de96d2cc1e29642ffc34c2a836dbc0e1b03e3b3b55cff/analysis/

Persistence mechanism: Installs a LaunchAgent at ~/Library/LaunchAgents/com.google.plugins.plist and references a malicious binary at ~/Library/Logs/.Logs/corevideosd

C&C servers:

- kiifd[dot]pozon7[dot]net
- shop[dot]ownpro[dot]net
- pad[dot]werzo[dot]net

AlienVault Detections:

> IDS rules: https://github.com/AlienVault-Labs/AlienVaultLabs/blob/master/malware_analysis/OSX_Malware/snort_oceanlotus.rules

System Compromise, Targeted Malware, OceanLotus

Persistence Mechanisms

The samples we looked at used well known [2] persistence mechanisms and were not difficult to detect. Specifically, the samples that we looked at use the following persistence mechanisms: launch agents, launch daemons, login items, and browser extensions. For those that aren't familiar with how these mechanisms are used, below is a short summary.

Launch daemons: These are start-up programs that run when the system first boots up.

> Items in **/Library/LaunchDaemons** and **/System/Library/LaunchDaemons** load when OSX starts up, and run as the **root** user.

Launch agents: These are start-up programs that are executed on a per-user basis.

- Items in **/Library/LaunchAgents** and **/System/Library/LaunchAgents** load when **any** user logs in, and run as that user.

- Items in **~/Library/LaunchAgents** load only when that particular **user** logs in, and run as that user.

Login items

These programs are run at the end of the login process and can be found in **~/Library/Preferences/com.apple.loginitems.plist**. The login items can be viewed in System Preferences -> Users & Groups -> [User Name] -> Login Items

Browser extensions

These are plugins that are loaded when a user starts a web browser such as Safari, Chrome, Firefox or Opera. These plugins are often used to monitor browser activity and steal sensitive information such as login credentials. Although the samples we looked at used browser extensions, malicious plugins are not limited to browsers – malicious plugins can be added to a variety of applications that support plugins.

OTX Stats

In addition to gathering samples, we also took a look at some statistics from Open Threat Exchange (OTX). The top 3 offenders that we saw in that data were:

1. OSX/Flashback User-Agent (49.5%)
2. OSX ADWARE/Mackeeper (26.6%)
3. OSX/WireLurker (23.7%)

This represents slightly over 20k events and includes only data prior to us enhancing our detection capabilities, so it doesn't include hits for OceanLotus, LaoShu, CoinThief, or KitM.

The following pulses from Open Threat Exchange (OTX) are related to the samples we examined:

LaoShu: https://otx.alienvault.com/pulse/568da8bc4637f2624bcdc2d1/

KitM: https://otx.alienvault.com/pulse/568da7e467db8c057c6fc696/

CoinThief: https://otx.alienvault.com/pulse/568da51b67db8c057c6fc689/

WireLurker: https://otx.alienvault.com/pulse/55d4c6dc67db8c37b0a358ea/

Mask/Careto: https://otx.alienvault.com/pulse/5531bbbfb45ff53dc229c806/

Observations

We found this exercise to be quite useful as it allowed us to get better acquainted with the behavior of the above malware and we were indeed able to improve our detection capabilities. Part of the process was to obtain fully functional OSX malware samples, but we found that can sometimes be difficult since many samples on VirusTotal are stand-alone executables rather than full '.app' bundles. Hopefully, we have made it a little easier for you to perform your own analysis by including links to fully executable samples.

Although this was an interesting exercise, we noted that most of the C&C servers have been taken offline, so the risk associated with these samples is not high. However, any signs of activity from these samples could be an indication of a deeper compromise so they should not be summarily dismissed.

Looking Ahead

Apple is making strong inroads in the corporate space. Apple's rising market share is making it lucrative for malware authors to write more OSX malware. In the Silicon Valley (where we are headquartered), many startups offer Macbooks as the default laptop when onboarding new hires. Therefore, it should come as no surprise that as the adoption of OSX increases, so will the prevalence of OSX-based malware. Furthermore, 2015 has been a tremendous year for OSX-based vulnerability disclosure [3]. As the number of known vulnerabilities increase, we expect more malware will take advantage of those flaws.

References:

Share this with others

Tags: malware, osx