UpdateAgent Adapts Again

Jamf Blog

May 16, 2022 by Jamf Threat Labs

Security

The Jamf Threat Labs team has recently identified changes to the UpdateAgent malware dropper. These changes primarily focus on new executables written in Swift that reach out to a registration server to pull down a new set of instructions in the form of a bash script. Perhaps one of the most identifiable features of the malware is that it relies on the AWS infrastructure to host its various payloads and perform its infection status updates to the server. The continued development of this malware shows that its authors continue to remain active, trying to reach as many users as possible.

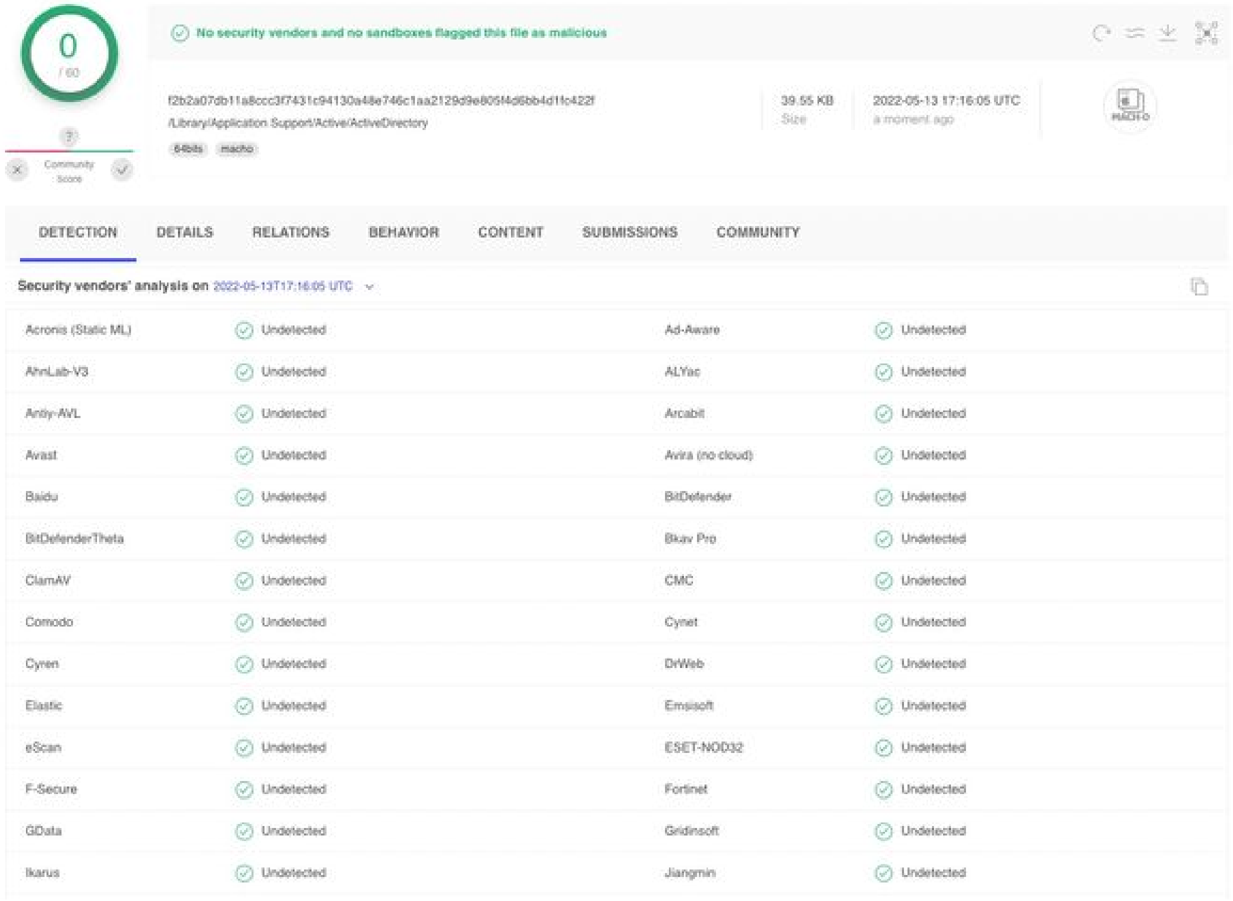
Authors: Jaron Bradley, Stuart Ashenbrenner and Matt Benyo

Dropper and Initial Instructions

The newly discovered Swift-based dropper exhibits many of the characteristics of typical dropper malware, including some minor system fingerprinting, endpoint registration and persistence. The second stage download and execute the functionality of droppers, in general, represent a risky class of malware that support a number of second-stage attacks — from malware to spyware, to adware.

In this case, Jamf Threat Labs was tipped by an increase in adware/malware threat preventions that appeared to be a part of the same family. Additionally, each instance was traced to an executable named PDFCreator. This executable was unsigned and running from the “/Library/Application Support” directory. Upon further inspection, the executable was determined to be written in Swift, containing suspiciously obfuscated (base64) strings.

At the time of discovery, this binary had zero hits from antivirus vendors in VirusTotal.



No security vendors and no sandboxes flagged this file as malicious

f2b2a07db11a8ccc3f7431c94130a48e746c1aa2129d9e805f4d6bb4d1fc422f
/Library/Application Support/Active/ActiveDirectory
64bits macho

39.55 KB
Size

2022-05-13 17:16:05 UTC
a moment ago

Security vendors' analysis on 2022-05-13T17:16:05 UTC

Acronis (Static ML)	Undetected	Ad-Aware	Undetected
AhnLab-V3	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected
BitDefenderTheta	Undetected	Bkav Pro	Undetected
ClamAV	Undetected	CMC	Undetected
Comodo	Undetected	Cynet	Undetected
Cyren	Undetected	DrWeb	Undetected
Elastic	Undetected	Emsisoft	Undetected
eScan	Undetected	ESET-NOD32	Undetected
F-Secure	Undetected	Fortinet	Undetected
GData	Undetected	Gridinsoft	Undetected
Ikarus	Undetected	Jiangmin	Undetected

When executed, this binary is responsible for reaching out to a registration server and setting up persistence on the system on which it runs.

When this executable runs, the following command is run to gather the machine hardware id in order to use it as a unique identifier moving forward.

The executable then uses the following curl command to reach out to a server to register the device and acquire a bash script to be executed.

The execution of this bash script is the mach-O executable’s primary task. After pulling it from the URL, it runs directly from the Swift dropper without hitting the hard drive. During our analysis, the script contents were uploaded to VirusTotal and can be seen here.

Based on the results we are seeing, we suspect this bash script is likely built dynamically as machines are registered. This script performs a large number of actions. Below are just some of the interesting variables that are used which we’ve labeled with comments.

Additionally, another variable titled “URL” was set. However, it was obvious that at the time of investigation the link meant to provide this URL value was currently down or unattainable as the $URL variable was set to a “File not found” type error.

However, other samples of this malicious script can be found on VT that appear to have URLs pointing to AWS S3 buckets. AWS has been made aware of the specifics.

Dropped Malware

When the URL variable is accurately set by the server, it gets used to download a stage-2 disk image (DMG) to the endpoint. Below, we’ve again commented on the code to describe what's happening.

In cases where the $URL is active, the downloaded DMG contained an application. The application file name held within the DMG appears to have been created by combining a few random words together. This application is then copied to the /tmp directory. A handful of the ones we’ve seen are as follows:

The path to the newly created application is then stored within the $TMPFILE variable created earlier.

One interesting trick that this malware uses is that it modifies the /etc/sudoers file with the following command:

This command makes it so that the basic user can execute the script ($TMPFILE) as root without requiring a password. This modification to the sudoers file is only possible if UpdateAgent is already running as root.

The malware then creates a user-level LaunchAgent by running a series of PlistBuddy commands. Here’s an example of a resulting launch agent:

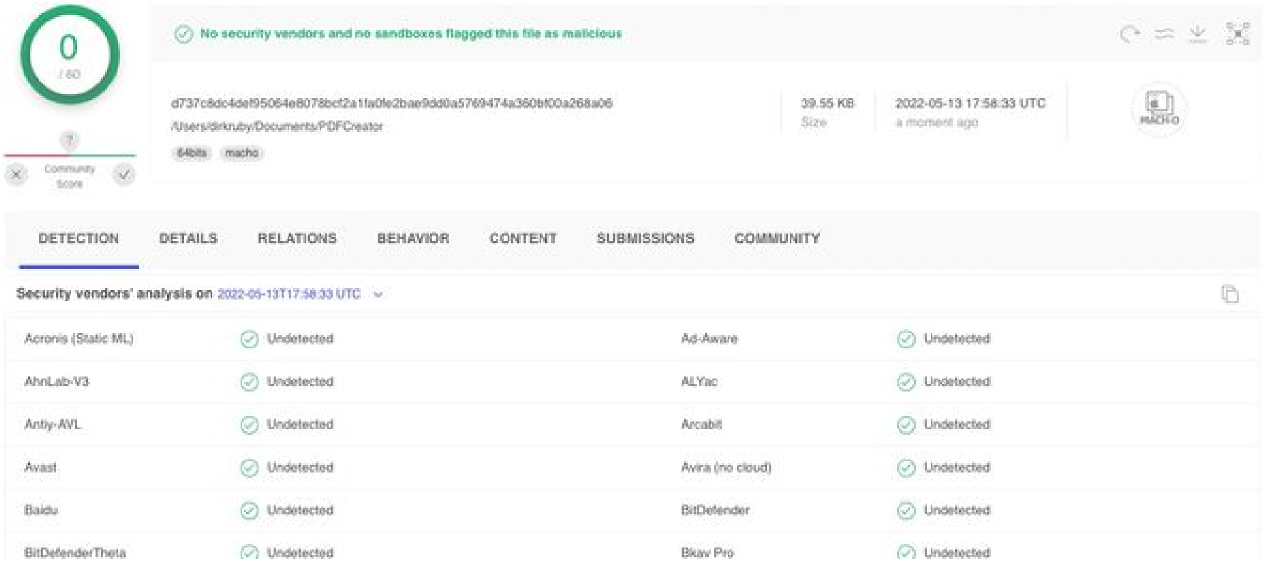
Both the editing of the sudoers file and the creation of persistence using the PlistBuddy command align with past workflows done by UpdateAgent according to previous findings from Microsoft.

When this plist loads at runtime, it will execute the temporary application. Even though it runs as a user LaunchAgent it is able to escalate to root without a password due to the previously mentioned modification made to the /etc/sudoers file.

After the LaunchAgent is loaded, the malicious bash script sleeps for a short period of time and then performs cleanup by unmounting the DMG file and removing the changes it made to the sudoers file.

Other Executables

In many circumstances, we see yet another plist and binary combination being dropped by PDFCreator called“ActiveDirectory”.



No security vendors and no sandboxes flagged this file as malicious

d737c8dc4def95064e8078bcf2a1fa0fe2bae9dd0a5769474a360bf00a268a06
/Users/dirkruby/Documents/PDFCreator
64bits macho

39.55 KB
Size

2022-05-13 17:58:33 UTC
a moment ago

Security vendors' analysis on 2022-05-13T17:58:33 UTC

Acronis (Static ML)	✓ Undetected	Ad-Aware	✓ Undetected
AhnLab-V3	✓ Undetected	ALYac	✓ Undetected
Antiy-AVL	✓ Undetected	Arcabit	✓ Undetected
Avast	✓ Undetected	Avira (no cloud)	✓ Undetected
Baidu	✓ Undetected	BitDefender	✓ Undetected
BitDefenderTheta	✓ Undetected	Bkav Pro	✓ Undetected

Once again, in the VirusTotal screenshot above, this binary is seen as clean.

After close examination, we noted that this executable is almost identical to the PDFCreator executable. The primary difference is that it reaches out to a different URL from which it should load a bash script.

In the cases that we observed, this downloaded bash script would send a simple check-in event to the cloud. If the contents of this URL change, the victim computer can perform any given instructions when it checks in next.

Conclusion

The authors of the UpdateAgent malware remain vigilant in keeping it up to date. It is known for having a well-built backend that allows itself to be easily updated, and although we’ve only seen adware families dropped by it, security experts are concerned that there might be other malicious plans for the future with such a well-built infrastructure.

Jamf Protect users are covered against the known, existing families of this malware, including various different detection surrounding suspicious behaviors and potentially unwanted applications, thanks to the frequently updated behavioral analytics.

IoC's

Threat actors and malware authors are savvy to updating their toolsets to continue compromising endpoints.

So, why not rely on a solution, like Jamf Protect, that is consistently updated and has the strength of the Jamf Threat Labs behind it to prevent the latest threats?

Request Trial

Jamf Threat Labs
Jamf

Jamf's internal research team comprised of Jaron Bradley, Stuart Ashenbrenner, Ferdous Saljooki and Matt Benyo.