ASERT Threat Intelligence Report 2016-04

Flying Dragon Eye: Uyghur Themed Threat Activity TLP WHITE

Executive Summary

This paper documents attempted exploitation activity aimed at Uyghur interests outside of China. Exploitation is being attempted via the usual tactic of spear phishing containing malicious attachments to targets. The exploit code attached used for dropping the malware is older – CVE-2012-0158 – and from our vantage point, we have no indication of successful or failed exploitation. Nonetheless, we can obtain targeting information and insight into tactics from the spearphish messages used by the threat actors. Successful exploitation typically results in malware calling back to one or more Uyghur themed domain names. The malware payloads observed to be associated with the Uyghur themed C2 domains so far consist of PlugX, Gh0st RAT, and Saker/Xbox, although there may be others that are yet to be discovered.

Large-scope threat activity, malware and infrastructure described herein have been used against other targets. Those targets may benefit from the IOCs and other information provided

Concurent with this research, Palo Alto Networks released a paper found at [1] entitled “Recent MNKit Exploit Activity Reveals Some Common Threads”. This blog post was released to the public, and covers some of the same territory as the research herein. This document was therefore edited to remove material that was already discussed in the Palo Alto document, unless there was additional information to add. Researchers and defenders may benefit from viewing both documents in order to develop a more comprehesive picture, as it is rare for one security research organization to have perfect visibility into any particular campaign in every case.

ARBOR SERT
Security Engineering & Response Team
www.arbornetworks.com/asert/

Background

While this paper does not attempt to assign attribution, it is interesting to consider who might benefit most from compromising the Islamic Uyghur population and their supportive activists.

Beginning in 2012 when cyber attribution first started publically trending, numerous entities began attempting to showcase likely Chinese cyber operations targeting Uyghurs. In one case, analysts stated DDoS operations in June and July 2011 targeted the German-based World Uyghur Congress (WUC) taking down their phone servers around an important activist anniversary [2]. In 2012, Kaspersky discovered Mac OS X malware used in a spearphishing campaign specifically targeting Uyghur activists [3]. In 2013, research surfaced indicating malware dubbed 'NetTraveler' was used to target not only Chinese border country officials but pro-Tibetan/Uyghur activists too [4]. In this case, malware activity was ongoing since at least 2004.

Moving forward, news emerged likely aiding China's legitimacy in targeting Uyghurs. In March 2015, news broke claiming upwards of 300 Uyghurs left China to join the Islamic State (ISIS/IS/ISL). Chinese officials claimed the individuals were planning to return from Syria intent on carrying out terrorist operations inside Chinese borders [5].

China has a long history of leveraging cyber space capabilities to target this particular ethnic group, likely targeting Uyghurs since the inception of their cyber espionage programs. Given the decades of turmoil coupled with the more recent threat of the Islamic State supporting and being supported by Uyghurs, China seemingly has clear reasons to monitor their western Islamic populace, even if they do not publicly admit to it. For more examples of Chinese targeting of Uyghur activists, look no further than a simple internet search: https://www.google.com/search?num=100&site=&source=hp&q=china+uyghur+cyber&oq=china+uyghur+cyber&gs_l.

Uyghur Themed Malware Activity

www.yawropauyghur[.]top - PlugX

In mid to late March of 2016, ASERT became aware of an instance of the PlugX backdoor malware using an Uyghur-themed domain name we had previously documented in the Four Element Sword Engagement at https://www.arbornetworks.com/blog/asert/four-element-sword-engagement/. The malware has a compilation date of 2015-11-18 09:15:19, and uses the domain www.yawropauyghur[.]top for its Command & Control (C2). The domain was registered on 11-04-2015, resolves to 118.193.240[.]195, and the malware sample has the SHA-256 hash a351040c0da2837f19b357baea4bffe194b0cd0d86bf262f8be1126e3a9d44d8.

The PlugX configuration file includes the following elements of interest:

Sample Properties:

[plugx] cnc:	www.yawropauyghur.top:445
[plugx] cnc:	www.yawropauyghur.top:53
[plugx] cnc1:	www.yawropauyghur.top:53 (TCP / HTTP)
[plugx] cnc2:	www.yawropauyghur.top:53 (UDP)
[plugx] cnc3:	www.yawropauyghur.top:53 (HTTP / UDP)
[plugx] cnc4:	www.yawropauyghur.top:445 (TCP / HTTP)
[plugx] cnc5:	www.yawropauyghur.top:445 (UDP)
[plugx] cnc6:	www.yawropauyghur.top:445 (HTTP / UDP)
[plugx] cnc_auth_str:	22222
[plugx] enable_icmp_p2p:	1
[plugx] enable_ipproto_p2p:	1
[plugx] enable_p2p_scan:	1
[plugx] enable_tcp_p2p:	1
[plugx] enable_udp_p2p:	1
[plugx] flags1:	4294967295
[plugx] flags2:	0
[plugx] hide_dll:	-1
[plugx] icmp_p2p_port:	1357

Some interesting elements from the configuration include the C2 domain name (further analysis below), the auth string (which appears to be unique to this sample, based on all of the PlugX samples that ASERT has collected) and the enabling of the Peer to Peer functionality of PlugX, which is observed in 55% of the PlugX configurations that Arbor has extracted from PlugX samples.

www.amerikauyghur[.]top - Gh0stRAT LURK0 malware

As mentioned in the Palo Alto Networks report, a Gh0stRAT LURK0 malware sample connects back to this domain (IP address 118.193.240[.]195) on TCP port 666. The sample was analyzed by ASERT on 2/28/2016. The SHA-256 hash is b625e605932196efbc6c80a18f61a71d27d82935209a1abde2ec591973fed31e and the MD5 hash is 4edda0e2a8a415272f475f3af4d17dc1.

During analysis, the following network signatures were triggered:

ET TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 101
ETPRO TROJAN Backdoor family PCRat/Gh0st CnC Response
ET TROJAN Backdoor family PCRat/Gh0st CnC traffic

The Gh0st RAT LURK0 variant has been used in a variety of threat activity against Tibetans and others [6] for some years and will not be documented further herein.

www.amerikauyghur[.]top - Saker/Xbox malware

Another sample SHA-256 c39e0fc30c2604b3eb9694591789a8e3d4cee7bcc4f9b03349e10c45304aef59 with MD5 hash 86088922528b4d0a5493046527b29822 (imphash:e9145e0c8dc228638e05f159c6a6d2b0) connects to the same domain using the following HTTP syntax:

http://www.amerikauyghur.top:993/301000000000F0FD0100363232363636364432383735323237310000000
00000000000000000000000000000000000054455155494C41424F4F4D424F4F4D0000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000001000007006A616E65
747465646F650000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000

Interestingly, the sample is observed to connect to the C2 using a crafted User-Agent value that contains an apparent typo ("Wis" instead of "Win"):

User-Agent: Mozilla/6.0 (compatible; MSIE 9.0; Wis NT 8.1; .NET CLR 2.13431)

This particular sample was also covered in the PAN report, however a search of over 110 million HTTP request headers collected by Arbor Networks from various vantage points around the world indicates that this User-Agent has yet to be observed in legitimate traffic, making this User-Agent a reasonable method to detect threat activity. A similar User-Agent value was documented by FireEye in the past.

Spear Phish Targets Nineteen Individuals

As a sample of exploitation activity targeting Uyghur interests, we examine a spearphish sent on March 3 of 2016. This was sent to nineteen distinct targets, and contained a malicious RTF attachment named uqturush.doc.

Word document metadata can be changed, however the May 2012 datestamp on the attachment suggests that the attached document is several years old. The exploit code for this particular sample appears to be (based on prominent anti-malware detection capabilities) CVE-2012-0158, an old vulnerability but one that is still being used. Due to poor update and poor patching processes, some of the targets may potentially be vulnerable, or the question of their vulnerability was enough for threat actors to attempt a targeted exploitation. Palo Alto Networks indicates that these attachments are generated by a variant of the MNKit

malware. MNKit has been in use for some years, although indicators suggest it is not a widespread threat.

When detonated in a vulnerable environment (Windows XP, Office 2007 in this case), the following files were created and executed:

Filename	MD5	SHA-256
Msdis.dll	9de14f249afc4e6979d8f2106e405b21	69c2da4061890050dc0ca28db6f240c8ed6c4897f4174bcd5d1bca00ade537d5
Msexc.exe	2f981ac92284f1c710e53a5a2d41257a	be7a14927ff11536a5bfd6c21d3f4a304659001f1f13b6d90ce0e031522817e5

While this is an older operating environment, it is possible that there are still vulnerable installations among the target population due to the dynamics of cost and the use of pirated software.

The exact spearphish and targeting details have been removed from the public version of this report. If you need the private version of the report that contains these details, please contact your Arbor Networks representative.

We observe that the targeting is worldwide, focused on individuals and organizations that typically have had some relationship with Uyghur issues. It is not known how targeting is performed, however if claims of e-mail monitoring among the Uyghur population are true, it is possible that these addresses were harvested and targeted as part of ongoing operations. The UNPO indicates that Uyghur "email communication are heavily monitored" [7].

Malware Operations and Malicious or Likely Malicious Domain Names

From the attachment exploitation, two files are dropped. One is a DLL and the other is an EXE. The sample connects to IP address 118.193.240[.]195 on TCP/993. This IP address was mentioned in "The Four Element Sword Engagement" Threat Intelligence Report from Arbor ASERT and overlaps with other threat activity against Tibetans, Hong Kong and Taiwan booksellers and media, and Chinese Human rights workers.

A passive DNS query on the 118.193 address shows us that turkiyeuyghur[.]com resolved in 2015 to another IP address 210.209.118[.]87. This IP has hosted a variety of other domains (some were mentioned in the Four Element Sword paper and others in Palo Alto documents), to include eight Uyghur themed domains and various others. As several of these domains have already been used maliciously, it is likely that all of these have the potential for malicious use. The domains, including closely associated domain names are:

www.turkistanuyghur[.]top	**www.amerikauyghur[.]top**
www.yawropauyghur[.]top	**www.japanuyghur[.]top**
www.whitewall[.]top	**www.hotansft[.]top**
dtsx.uygurinfo[.]com	**turkiyeuyghur[.]com**
ks.uygurinfo[.]com	**www.tibetimes[.]com**

uygurinfo[.]com	**freetibet[.]top**
tibettimes[.]top	

Analysis of domain registration activity reveals a variety of other domains of interest through a common pivot on the email address 2732115454[@]qq.com. We can discover new domains registered by the same email such as russiauyghur[.]top. Our passive DNS resources reveal no activity yet for russiauyghur[.]top, but it may be used in the future, based on threat activity trends.

Further pivots reveal additional domains associated with the registrant name "Wang QiongWang Qiong" such as freetibet[.]top and tibetantimes[.]top.

All of these domains have been or are currently associated with the following IP addresses:

59.188.83[.]144	118.193.240[.]218
118.193.225[.]133	118.193.240[.]195

turkiyeuyghur[.]top, tibettimes[.]top, russiauyghur[.]top, japanuyghur[.]top, freetibet[.]top, hotansft[.]top, and amerikauyghur[.]top are all associated domains. Note that turkiyeuyghur[.]com and .top are both registered.

The long organizational name "Shen Chou Shi Xing Le Hui Can Yin Guan Li You Xian Gong Si" is only associated with xinglehui[.]top. This domain resolves to 59.188.83[.]144, which hosts approximately 75 other domains at this time of writing. As those domains aren't clearly associated with obvious threat activity other than via a registrant, organizations are encouraged to be aware of the lower confidence, indirect threat assessment.

www.turkiyeuyghur.com - Saker/Xbox Malware

Malware sample SHA-256 3714058d90b214916918841877316 5b620abd1481b47d1551d79679bfe21d28c (MD5: e490174855b8548161613fd5d9955e7a) connects to turkiyeuyghur[.]com on TCP port 666. It is worth noting that we have previously observed a Gh0stRAT LURK0 variant using TCP 666 that may be associated with the same threat actors. However in this case, the sample appears to be from the Saker/Xbox malware family.
This domain was sinkholed by Arbor ASERT.
A URL generated from sandboxing this sample appears as such:

http://turkiyeuyghur.com:666/301000000000F0FD01003632323636363644323837353232373100000000000
000000000000000000000000000054455155494C41424F4F4D424F4F4D000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000001000007006A616E6574746
5646F6500000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000

The domain resolved to the aforementioned IP address 210.209.118[.]87 (prior to ASERT sinkholing).

A list of created files is as follows:

- C:\Documents and Settings\Admin\Application Data\mntat
- C:\Documents and Settings\Admin\Application Data\mntat\msexc.exe
- C:\Documents and Settings\Admin\Start Menu\Programs\Startup\msexw.lnk
- C:\Documents and Settings\Admin\Application Data\mntat\msexw.zip

The binary also creates a .LNK file in the Startup folder containing the Target of C:\Users\admin\AppData\Roaming\mntat\msexc.exe.

A ZIP file is embedded as an overlay inside the binary. It is password protected, and the output file is msdis.dll. The timestamp on the ZIP file is 2015-09-02 08:13:00.

The malware creates a mutex pcdebug.1, which appears in a small amount of other malware samples. The hashes of other samples that create the same mutex name (and match the import hash value of dd96a7da43b3853dc38e219abc6cac25) are as follows:

SHA-256	MD5
f15840fbade7a5611391193a4a53f63ef465ab451f7783da21cad7303ea3b68c	e49e235b301a4316ef58753c093279f0
97ec795227818fedc70fad9f2df8cb839d9fb75b502f3598614610d4e8e1be78	0ea68dd9463626082bb96ad373bd84e0

The PEHash value of these two samples is 59781db8be6bb162f5c8ee8cf950fe191417baa4. Pivoting from this hash, we discover four other samples that have the following hash values:

SHA-256	MD5
444c6589ed030da41ba49d20ac38029e5213978fadef2ee94408e4f91395b488	1a169a7e52879bad47e2834abfe50361
ef3e7b1c37aef1d8359169cca9409db4709632b9aa8bf44febe0d91e93ab537e	731a9761626e39bb84b34343bdae67b0
62a033fc586c6220ee0c0ea8ff207ab038776455505fa2137e9591433ada26e1	1dc2e57dbf63051608cff83d8b88d352
087e45f63ce00c4df07f81837eceb0b322773822feee01cfc005e5fc14e50f5e	de07dc9e83bfd445ad7cc58baab671f2

Many of these samples are only tagged by antimalware as a downloader and some as the Zeus trojan. The compilation dates on the malware are from September of 2015, and are all exactly 2015-09-02@01:59:21. While compilation dates can be modified, the cluster of samples around this date suggests a similar actor or some aspect of a campaign at play.

Additional Uyghur Themed Targeting Documents – CVE-2012-0158

More documents targeted at the Uyghur and Uyghur associated communities are as follows:

Document hash (SHA-256)	Attachment filename
3f3d0a5aa2799d6afe74c5cb6e077e375078b173263c5ca887ffe2e22164b10f	Google aqsakla Rabiye isming.doc
7b587b104219784e9fd3dc9c13a0f652e73baed01e8c3b24828a92f151f3c698	agahlandurushname.doc
4ab388b1310918144ad95e418ebe12251a97cb69fbed3f0dd9f04d780ddd132d	chaqiriq.doc
940d0770e644c152d60a13f9d40015a1089419361de33fe127e032f4bb446c69	chaqiriq.doc
0c35a508ece0c9269e176b6b278a96f7ca29e04a2ca2319a91b585f27abfe2f6	chqiriq.doc

5e818eeb0cffeb6f65f611a17f522560912ae19372e7f734be6df5e35ba82337	tetqiqat doklati.doc
e55912a134902ab73c52cb42f32051745214275b59a95d565cfcb7560d32f601	istepaname.doc
45e39db2a877ff2663efc4d66ed4084ffdb6ddb4926112b7c471872208b96767	jedwel.doc
f4fd8554710017caa042b52122d7985c7f510df8e2c26f1ffa6e27233bfe9b54	teklipname.doc
9feee2a3fe49fe774d414999ac393655255e7c035ffc93bbd031a2331fd89dc8	Tetqiqat doklati.doc
3bbf0f821c89ba03d30deb63eec59c8e9e76c20578ad805de9971bdbcd2855d2	uqturush.doc

ASERT would like to thank Michael Yip of Stroz Friedberg for insight into further details of spear phish activity provided in the preceeding table and also for YARA rules that provided additional visibility.

Conclusion

This is only a sampling of threat activity that is obviously targeted against a specific population of interest. Threat activity against this population is likely to continue, and others communicating with this population, or showing interest in Uyghur related human rights issues may also be swept up in the net. Threat actors involved in this targeting appear to have been active for years, based on numerous interconnections between past and present threat infrastructure and malcode.

It is possible that additional targeting well beyond CVE-2012-0158 is at play, although in this case it appears that threat actors still thought they could obtain benefit from using a four-year-old vulnerability that has been widely associated with numerous cyber-espionage operations over the years. This may be due to the weakness of defensive posture among those targeted and an attempt at higher return on investment by using exploit code that might still be adequate considering the targets. Pivots on threat infrastructure suggest that the same or related threat actors have direct or indirect access to other types of exploit code such as the "Four Element Sword" builder and the numerous types of malware delivered with it (PlugX, 9002 RAT 3102 variant, T9000, Grabber, Gh0st RAT LURK0 variant and perhaps others), profiled in previous ASERT threat intelligence products.

Mitigation is not difficult in this case since these documents are exploiting old vulnerabilities (CVE-2012-0158). Organizations with limited resources may not be up to date and thus continue the long tail of vulnerability.

References

1. http://researchcenter.paloaltonetworks.com/2016/06/unit42-recent-mnkit-exploit-activity-reveals-some-common-threads/
2. http://www.rfa.org/english/news/uyghur/hackers-09062012153043.html
3. http://www.ubergizmo.com/2012/06/new-mac-os-x-virus-discovered/
4. https://www.rt.com/news/nettraveler-malware-network-kaspersky-240/
5. http://www.independent.co.uk/news/world/asia/chinese-uighurs-join-isis-overseas-and-return-to-take-part-in-terror-plots-officials-claim-10099674.html
6. http://www.welivesecurity.com/2014/11/14/targeted-attacks-tibetan-advocates-using-g20-2014-summit-lure/
7. http://unpo.org/members/7872

About ASERT

The Arbor Security Engineering & Response Team (ASERT) at Arbor Networks delivers world-class network security research and analysis for the benefit of today's enterprise and network operators. ASERT engineers and researchers are part of an elite group of institutions that are referred to as “super remediators,” and represent the best in information security. This is a reflection of having both visibility and remediation capabilities at a majority of service provider networks globally.

ASERT shares operationally viable intelligence with hundreds of international Computer Emergency Response Teams (CERTs) and with thousands of network operators via intelligence briefs and security content feeds. ASERT also operates the world1s largest distributed honeynet, actively monitoring Internet threats around the clock and around the globe via ATLAS®, Arbor's global network of sensors: http://atlas.arbor.net. This mission and the associated resources that Arbor Networks brings to bear to the problem of global Internet security is an impetus for innovation and research.

To view the latest research, news, and trends from Arbor, ASERT and the information security community at large, visit our Threat Portal at http://www.arbornetworks.com/threats/.