Taking Action Against Hackers in China

about.fb.com/news/2021/03/taking-action-against-hackers-in-china/

April 7, 2022

Facebook threat intelligence analysts and security experts work to find and stop a wide range of threats including cyber espionage campaigns, influence operations and hacking of our platform by nation-state actors and other groups. As part of these efforts, our teams routinely disrupt adversary operations by disabling them, notifying users if they should take steps to protect their accounts, sharing our findings publicly and continuing to improve the security of our products.

Today, we’re sharing actions we took against a group of hackers in China known in the security industry as Earth Empusa or Evil Eye — to disrupt their ability to use their infrastructure to abuse our platform, distribute malware and hack people’s accounts across the internet. They targeted activists, journalists and dissidents predominantly among Uyghurs from Xinjiang in China primarily living abroad in Turkey, Kazakhstan, the United

States, Syria, Australia, Canada and other countries. This group used various cyber espionage tactics to identify its targets and infect their devices with malware to enable surveillance.

This activity had the hallmarks of a well-resourced and persistent operation while obfuscating who's behind it. On our platform, this cyber espionage campaign manifested primarily in sending links to malicious websites rather than direct sharing of the malware itself. We saw this activity slow down at various times, likely in response to our and other companies' actions to disrupt their activity.

We identified the following tactics, techniques and procedures (TTPs) used by this threat actor across the internet:

- **Selective targeting and exploit protection:** This group took steps to conceal their activity and protect malicious tools by only infecting people with iOS malware when they passed certain technical checks, including IP address, operating system, browser and country and language settings.
- **Compromising and impersonating news websites:** This group set up malicious websites that used look-alike domains for popular Uyghur and Turkish news sites. They also appeared to have compromised legitimate websites frequently visited by their targets as part of watering hole attacks. A watering hole attack is when hackers infect websites frequently visited by intended targets to compromise their devices. Some of these web pages contained malicious javascript code that resembled previously reported exploits, which installed iOS malware known as INSOMNIA on people's devices once they were compromised.
- **Social engineering:** This group used fake accounts on Facebook to create fictitious personas posing as journalists, students, human rights advocates or members of the Uyghur community to build trust with people they targeted and trick them into clicking on malicious links.
- **Using fake third party app stores:** We found websites set up by this group that mimic third-party Android app stores where they published Uyghur-themed applications, including a keyboard app, prayer app, and dictionary app. These apps were trojanized (contained malware that misled people of its true intent) with two Android malware strains — ActionSpy or PluginPhantom.
- **Outsourcing malware development:** We've observed this group use several distinct Android malware families. Specifically, our investigation and malware analysis found that Beijing Best United Technology Co., Ltd. (Best Lh) and Dalian 9Rush Technology Co., Ltd. (9Rush), two Chinese companies, are the developers behind some of the Android tooling deployed by this group. Our assessment of one of them benefited from research by FireEye, a cybersecurity company. These China-based firms are likely part of a sprawling network of vendors, with varying degrees of operational security.

- **Industry tracking:** Our industry peers have been tracking parts of this activity as being driven by a single threat actor broadly known as Earth Empusa, or Evil Eye, or PoisonCarp. Our investigation confirmed that the activity we are disrupting today closely aligns with the first two — Earth Empusa or Evil Eye. While PoisonCarp shares some TTPs including targeting and use of some of the same vendor-developed malware, our on-platform analysis suggests that it is a separate cluster of activity.

We shared our findings and threat indicators with industry peers so they too can detect and stop this activity. To disrupt this operation, we blocked malicious domains from being shared on our platform, took down the group's accounts and notified people who we believe were targeted by this threat actor.

Threat Indicators:

Hashes

MD5 Hash	Description	Malware Family
10c1f38305792a0f925e8a2cf9482ce3	Keyboard	Plugin Phantom
3c0a20f0726032ad816e670971509b2d	قۇرئان كەرىم (The Holy Quran)	Plugin Phantom
01fe88068e43c2276f7d8bbf54824f0f	系统服务 (System Service)	Plugin Phantom
fd8da30dd9e45bd31af79a9652d50ece	地球 (Earth)	Plugin Phantom
10748ca7648d26316b4857b6139ca93d	AwazlikKitap	Plugin Phantom
a5199e6f1904f5a532a562fbb9d5abc6	Uighur Keyboard	Plugin Phantom

670a389a93b82ccf198dd7789a865096	Ekran	Action Spy
9bc5fec740bdb4d93f2da9b2db75dc3f	Uyghurs History	Action Spy

Domains

Domain	Description
misran[.]org	Hosting PluginPhantom malware
apkprue[.]info	Hosting PluginPhantom malware
www.apkpure[.]bz	Hosting PluginPhantom malware
gotossl[.]ml	Hosting ActionSpy malware
geo2ipapi[.]org	Hosting ActionSpy malware
anayurt[.]net	Hosting ActionSpy malware
preservtyg[.]com	Watering hole with malicious iframe
uhtpuerdfbnm[.]com	Watering hole with malicious iframe
uyghurhaber[.]com	Watering hole with malicious iframe

newyorkingsite[.]com	Watering hole with malicious iframe
istiqlaihaber[.]com	Watering hole with malicious iframe
uyghur-news[.]com	Watering hole with malicious iframe
strunhvgpk[.]com	Contained malicious javascript resembling previously reported exploit code which installed INSOMNIA
sslportservices[.]com	Connected to infrastructure hosting malicious javascript
playgoog1e[.]com	Believed to be used to host Android malware
www.apkhl[.]pw	Believed to be used to host Android malware
uyghur-soft-market[.]com	Believed to be used to host Android malware
icptime[.]com	Believed to be used to host Android malware