CERT-EU

Memo

19/09/2019 - TLP:WHITE

Large scale and powerful cyber surveillance by China

Reference: Memo [190919-1] – Version: 1.0

Keywords: China, Uyghurs, dissidents, smart devices, espionage, surveillance, monitoring

Sources: Publicly available information

Key Points

- According to researchers, Chinese authorities are purportedly monitoring Uyghurs, both locally and internationally, through cyber means
- The threat actors reportedly leveraged several techniques including multiple exploit chains against Android and iOS, several strategic web compromises, as well as bypassing the two-factor authentication of Google services
- The wide range of leveraged methods demonstrates the threat actors' significant capabilities, funds and technical expertise

Summary

Chinese authorities are attempting to contain dissent on several fronts including among the Uyghur Muslim population, who mainly reside in the Xinjiang region in the west of the country. Since at least 2013, China is active in the monitoring of the Uyghur population according to several trustworthy sources, both domestically and abroad, in order to exercise stronger control. A recent analysis[1] indicates that the surveillance activities combine several infiltration and control techniques as summarised below.

Strategic web compromise - At least 11 websites of interest for the Uyghur population have been infiltrated and offensive malicious code has been installed in order to capture and relay information on visitors and possibly infiltrate their systems. Such operations have highly likely been active since at least 2015 and researchers believe that at least two Chinese APT groups were likely involved in the large-scale infiltration. It should be noted that the campaign has almost certainly been targeting the Uyghur diaspora, as the compromised websites were blacklisted by the Great Firewall of China (GFW).

- In several of the websites, *Scanbox*, an analysis tool, is installed on visitors' systems via hidden iframes. Coded in JavaScript and embedded in the compromised website, *Scanbox* is executed by the victim's browser. It can fingerprint both the browser and the system on which it runs. Additionally, it can operate as a keylogger and, if needed, can additionally push extra payloads to the victim.
- Also, if a mobile device is used to access compromised sites, an Android OS malware/loader called *Evil Eye* is installed. *Evil Eye* is an information exfiltration tool. Researchers believe a specific threat group known by the same name and almost certainly of Chinese origin is behind this activity. This malware has also been used in the past to monitor Tibetan dissidents.

Android and iOS exploits - The attacks against Android devices have reportedly[2] [3] been performed in parallel with the exploitation of several iOS (iPhone/iPad) vulnerabilities. According to Google Project Zero, some of the compromised websites took advantage of 14 vulnerabilities across 5 distinct exploit chains affecting iOS. According to Apple, they have been patched in February 2019. They were, however, associated with a number of compromised websites of Uyghur interest for at least two years before that. It should be noted that the offensive code was operating indiscriminately against the site visitors (Uyghurs or otherwise). Apple, while denying any widespread exploitation of the vulnerabilities leading to a massive breach of iOS devices, acknowledged the targeting of devices used by the Uyghur community by way of the infected websites.

Compromise of the two-factor authentication of Google services - Another method employed for surveillance was the effort to compromise the two-factor authentication of Google services, thus allowing the threat actors to gain complete access to emails and other data on the platform. Visitors of compromised websites were redirected to locations that asked for permanent access to Gmail accounts and Google services via OAuth. Possibly, deceived users may have been misled into granting such authorisations.

Comments

The targeted entities, the persistence of the campaign, the cost associated with the numerous employed techniques and multiple zero-day vulnerabilities, along with the development of exploits for them, indicate the almost certain involvement of state-sponsored actors.

It is also a display of ability to summon talent and funds at a substantial scale and determination to use them to achieve their objectives. It should also be noted that, although focused on a particular group, the operation has likely, and collaterally, gained access to systems of other individuals.

[1] https://www.volexity.com/blog/2019/09/02/digital-crackdown-large-scale-surveillance-and-exploitation-of-uyghurs/

[2] https://www.forbes.com/sites/thomasbrewster/2019/09/01/iphone-hackers-caught-by-google-also-targeted-android-and-microsoft-windows-say-sources

[3] https://www.wired.com/story/ios-hacks-apple-response