CPR analyzes A 7-year mobile surveillance campaign targeting largest minority in China

By etal

Published: 2022-09-22 · Archived: 2026-04-06 00:17:58 UTC

Highlights:

- Check Point Research (CPR) examines a long running mobile surveillance campaign, targeting the largest minority in China- the Uyghurs.
- The campaign is attributed to the ***Scarlet Mimic hacking group***, which has used more than 20 different variations of its Android malware, disguised in multiple Uyghur related baits such as books, pictures, and even an audio version of the Quran.
- The malware capabilities allow the attackers to easily steal sensitive data from the infected device, as well as perform calls or send an SMS on the victim's behalf and track their location in real-time

Background

CPR researchers have recently observed a new wave of a long-standing campaign targeting the Uyghur community, a Turkic ethnic group originating from Central Asia, one of the largest minority ethnic groups in China. This malicious activity, that we have attributed to the actor called **Scarlet Mimic,** was first brought to light in 2016 with a campaign that targeted the Uyghur and Tibetan minority rights activists. Past reports have suggested it could be linked to China, which has previously been accused of hacking and surveillance toward the Uyghurs.

Since then, CPR has observed the group using more than 20 different variations of their Android malware, disguised in multiple Uyghur related baits such as books, pictures, and even an audio version of the Quran. The malware is relatively unsophisticated from a technical standpoint. However, its capabilities allow the attackers to easily steal sensitive data from the infected devices, even perform calls or send an SMS and track their location in real-time. This makes it a powerful and dangerous surveillance tool. This tool also allows audio recording of incoming and outgoing calls, as well as surround recording.

In this report, we present a technical analysis and describe the evolution of the campaign in the last seven years. Although a small part of this campaign was briefly discussed in Cyble's publication as an isolated and unattributed incident, in this article we put the whole campaign in perspective and outline almost a decade's worth of persistent efforts in phone surveillance of the Uyghur community.

Overview of the campaign

Since first discovered back in 2015, we have identified more than 20 samples of Android spyware called **MobileOrder**, with the latest variant dated mid-August 2022. As there are no indications that any of them were

distributed from the Google Store, we can assume the malware is distributed by other means, most likely by targeted social engineering campaigns. In most cases, the malicious applications masquerade as PDF documents, photos, or audio. When the victim opens the decoy content, the malware begins to perform extensive surveillance actions in the background. These include stealing sensitive data such as the device information, SMS messages, the device location, and files stored on the device. The malware is also capable of actively executing commands to run a remote shell, take photos, perform calls, manipulate the SMS, call logs and local files, and record the surround sound.

The MobileOrder malware, despite being actively used and updated, still does not support some modern Android OS features, such as runtime permissions or new intent for APK installation, and does not use techniques common to most modern malware such as accessibility usage, avoiding battery optimization, etc.
CPR researchers are not able to identify whether the attacks have been successful, yet the fact that the group has continued to develop and deploy the malware for so many years suggests that they have been successful, at least, in some of their operations.

Victimology and lures

Most of the malicious applications we observed have names in the Uyghur language, in its Arabic or Latin scripts. They contain different decoys (documents, pictures, or audio samples) with content related to the ethnic geopolitical conflict centered on Uyghurs in China's far-northwest region of Xinjiang, or with the religious content referencing the Uyghurs' Muslim identification. We can therefore conclude that this campaign is likely intended to target the Uyghur minority or organizations and individuals supporting them, which is consistent with the Scarlet Mimic group's previously reported activity.

A few interesting examples of decoys used by the actor over the years include:

- The sample with the original name "photo" (md5:a4f09ccb185d73df1dec4a0b16bf6e2c) contains the picture of Elqut Alim, the "New Chief Media Officer" of the Norwegian Youth Union who call themselves "a group of Uyghur youth who live in Norway with a common understanding and a common goal, which is to stand up against China's invasion of East Turkestan." The malware was uploaded to VT with the name in Uyghur Latin and a fake ".jpg" extension.

Decoy image from the sample a4f09ccb185d73df1dec4a0b16bf6e2c.

- The application named پارتىزانلىق ئۇرۇشى" which translates from Uyghur to "Guerrilla Warfare" (md5: b5fb0fb9488e1b8aa032d7788282005f) contains the PDF version of the short version of the military course by Yusuf al-Ayeri, the now deceased first leader of Al-Qaeda in Saudi Arabia, which outlines the tactical methods of guerrilla warfare.

The lure PDF containing the materials by the military wing of Al-Qaeda.

- The sample called "The China Freedom Trap" (md5: a38e8d70855412b7ece6de603b35ad63) masquerades as a partial PDF of the book with the same name written by Dolkun Isa, politician and activist from the region of Xinjiang and the current president of the World Uyghur Congress:

The cover of the lure PDF.

- The sample called “quran kerim” which translates as “Noble Quran” (md5: f10c5efe7eea3c5b7ebb7f3bf7624073) uses as a decoy an mp3 file of a recorded speech in what seems to be a Turkic language.

How To Protect Against Android Malware

Cyber criminals and governments target mobile devices because users do not always secure their devices or practice safe habits. Mobile Device Security is a combination of strategies and tools that secure mobile devices against security threats.
Common best practices of preventing against mobile threats will include securing email communications on mobile devices, for instance, use software that warns people not to click on suspicious links, enforcing their organization’s security policies and requiring mobile users to use a virtual private network (VPN).
Although mobile security components vary based on each organization’s needs, mobile security always involves authenticating users and restricting network access. This is accomplished best with mobile security software.
Harmony Mobile leverages Check Point’s ThreatCloud and award-winning file protection capabilities to block the download of malicious files to mobile devices and prevent file-based cyber-attacks on organizations.
If you need a mobile security solution, Request a free demo of Check Point Harmony Mobile to see how we can protect your mobile devices from cyber-attacks.

Conclusion

Scarlet Mimic seems to be a politically motivated group. In the past, there have been reports from other researchers that it could be linked to China. If true, it would make these surveillance operations part of a much wider issue, as this minority group has reportedly been on the receiving end of attacks for many years.
What we do know is that Scarlet Mimic has been carrying out its espionage operations for the last eight years

against the Uyghur community using Android malware. The persistence of the campaign, the evolution of the malware and the focus on targeting specific populations indicate that the group's operations over the years are successful to some extent. This threat group's shift in attack vector into the mobile sector provides evidence of a growing tendency of extensive surveillance operations executed on mobile devices as the most sensitive and private assets.
