Minority report: Fake human rights documents and websites used in cyberattacks targeting Uyghurs, a Turkic ...

By gmcdouga

Published: 2021-05-27 · Archived: 2026-04-06 01:04:58 UTC

Highlights

- Check Point Research (CPR), in collaboration with Kaspersky's Global Research & Analysis Team (GReAT), have been tracking an ongoing attack targeting a small minority group of Uyghur individuals in Xinjiang and Pakistan
- Attackers use fake United Nations (UN) documents and human rights websites to spread malware that has the ability to exfiltrate information and take control of victims' PCs
- The Uyghurs are a Turkic ethnic group, culturally affiliated with Central and East Asia, and considered one of China's 55 officially recognized ethnic minorities

Background

In the past year, Check Point Research (CPR), in collaboration with Kaspersky's Global Research & Analysis Team (GReAT), have been tracking an ongoing attack targeting a small group of Uyghur individuals located in Xinjiang, China and Pakistan.

Malicious actors disguised their attacks in the following ways:

- They created documents that appear to be from the UN, using real UN information to ensure these looked authentic.
- Set up websites for non-existent organizations claiming to fund charity groups

This blog details the investigation of the decoy methods this group used.

Fake UN documents as a tool for initial infections

The researchers' investigations began with a malicious document found on the free malware scanning service VirusTotal named "**UgyhurApplicationList.docx**" which carried the logo of the United Nations Human Rights Council (UNHRC), and contained content from a UN general assembly discussing human rights violations that made the document seem genuine.

After the user opens the document by clicking on “enable editing”, a malicious external template containing a macro code is downloaded, and this macro code proceeds to decode an embedded backdoor. After the backdoor is decoded, it is then named “OfficeUpdate.exe” and saved under the %TEMP% directory.

In the two “OfficeUpdate.exe” examples the researchers located, the payload was a shellcode loader that utilizes basic evasion and anti-debugging techniques by using functions such as sleep and QueryPerformanceCounter.

Delivery Websites – Impersonating the UN’s Commission for Human Rights

The domain observed in the malicious document (officemodel[.]org) led to the same IP address as unohcr[.]org – a domain impersonating the Office of the High Commissioner for Human Rights (OHCHR).

Investigating this method of fake domains and websites revealed a tactic of distributing malware through fake websites that host malicious executables targeting Windows users.

Another IP address that unohcr[.]org led to was a domain named tcahf[.]org, which hosted a website claiming to represent the Turkic Culture and Heritage Foundation (TCAHF).

TCAHF claims to be a private organization that funds and supports groups working for Turkic culture and human rights, when in fact it is a made up entity, with most of its website’s content having been copied from the legitimate “*opensocietyfoundations.org*”.

Figure 2: Fake website (top) compared to the legitimate one (bottom)

The malicious functionality of the TCAHF website is well disguised and will only appear when the victim attempts to apply for a grant (see the added “Application” menu button in Fig. 5). The website then claims it must make sure that the operating system of the victim’s PC is safe before they enter sensitive information for the transaction, and asks them to download a program to scan their PC environment. The website offers two download options, one for MacOS and one for Windows, but when the team analyzed the website, only the download for Windows was available, while the MacOS version link served an empty file.

Figure 3: Links to download a fake security scanner

Uyghur minority as a target

Based on the nature of the malicious websites and the decoy content used in the delivery document, the researchers assessed that this campaign is intended to target the Uyghur minority or the organizations supporting them. The Uyghurs are a Turkic ethnic group, culturally affiliated with Central and East Asia, and considered one of China's 55 officially recognized ethnic minorities.

The research team's telemetry supports this assessment, as it has identified a handful of victims in Pakistan and China. In both cases, the victims were located in regions mostly populated by the Uyghur minority.

Attribution

Although the researchers were unable to find code or infrastructure similarities to a known threat group, they attribute this activity, with low to medium confidence, to a Chinese-speaking threat actor. When examining the malicious macros in the delivery document, the research team noticed that some excerpts of the code were identical to VBA code that have appeared in multiple Chinese forums, and might have been copied from there directly.

Figure 4: Similar macro code in Chinese forum

Impact of attacks and conclusion

While most of the activity described above happened in 2020, it appears the attackers behind this campaign are still active, and working with newly registered domains. The findings of this research indicate these attacks are ongoing, and new infrastructure is being created for what looks like future attacks.

Most recently, one of the domains appeared to be impersonating the Turkic Ministry of the Interior, but this and another domain redirected to the website of a Malaysian government body called the “Terengganu Islamic Foundation”. This suggests that they are pursuing additional targets in countries such as Malaysia and Turkey. However, the malicious group might still be developing those resources, since researchers have yet to find any malicious artifacts associated with those domains.

The malicious executables created by the attackers exfiltrate basic information about the infected system but can also download a second-stage payload, or in the case of the documents, fetch additional commands from the command and control server. This means that the researchers have not yet seen all the capabilities of this malware, or the full course of action taken by the attackers following a successful infection.

The motivation behind these cyberattacks seem to indicate a campaign of espionage, with the end game of the operation being the installation of a backdoor into the computers of high-profile targets in the Uyghur community. The attacks are designed to fingerprint infected devices, including all of its running programs. CPR and Kaspersky GReAT researchers will continue investigating this issue and report any new relevant findings.
