Cyber Espionage on Afghanistan, Kyrgyzstan and Uzbekistan by Chinese-speaking Hacker Group

By gmcdouga

Published: 2021-07-01 · Archived: 2026-04-24 02:16:02 UTC

Check Point Research (CPR) detects an ongoing cyber espionage operation targeting the Afghan government. Attributed to a Chinese-speaking hacker group, the threat actors impersonated the Office of the President of Afghanistan to infiltrate the Afghan National Security Council (NSC) and used Dropbox to mask their activities. CPR believes that this is the latest in a longer-running operation that dates as far back as 2014, where Kyrgyzstan and Uzbekistan are also victims.

- Threat actors send a dupe email urging action on an upcoming press conference hosted by the NSC
- Threat actors use Dropbox to go undetected, leveraging the API as their command and control center
- CPR spots malicious actions taken by threat actors, including access of victims' desktop files, deployment of scanner tool, and execution of Windows built-in networking utility tools

Check Point Research (CPR) has observed an ongoing cyber espionage operation targeting the Afghan government. Believed to be the Chinese-speaking hacker group known as "IndigoZebra", the threat actors behind the espionage leveraged Dropbox, the popular cloud storage service, to infiltrate the Afghan National Security Council (NSC). Further investigation by CPR revealed that this is the latest in longer-running activity targeting other Central Asian countries, Kyrgyzstan and Uzbekistan, since at least 2014.

"From the Office of the President of Afghanistan"

CPR's investigation began in April, when an official at the Afghanistan National Security Council received an email allegedly from the Administrative Office of the President of Afghanistan. The email urged the recipient to review the modifications in the document related to an upcoming press conference by the NSC.

Figure 1. Malicious email sent to the Afghan government employees

Infection Chain Begins with Ministry-to-Ministry Deception

CPR summarized the methodology of the cyber espionage in the following steps:

1. **Send email under guise of high-profile entity.** The threat actors orchestrated a ministry-to-ministry style deception, where an email is sent to a high-profile target from the mailboxes of another high-profile victim.
2. **Lace malicious attachment.** The threat actors add an archive file that contains malware, but pretends to be a legitimate attachment. In this case, the email contained a password-protected RAR archive named NSC Press conference.rar.
3. **Open the first document.** The extracted file, NSC Press conference.exe, acts as a dropper. The content of the lure email suggests that the attached file is the document, hence, to reduce the suspicion of the victim running the executable, the attackers use the simple trick: the first document on the victim's desktop is opened for the user upon the dropper execution. Whether the dropper found a document to open or not, it will proceed to the next stage – drop the backdoor.
4. **Utilize Dropbox as a command and control center.** The backdoor communicates with a preconfigured and unique to-every-victim folder on Dropbox. This serves as the address where the backdoor pulls further commands and stores the information it steals.

Figure 2: Diagram of Infection Chain

Mask and Persist with Dropbox

The threat actors use the Dropbox API to mask their malicious activities, as no communication to abnormal websites takes place. The backdoor crafted by the threat actors creates a unique folder for the victim in an attacker-controlled Dropbox account. When the threat actors need to send a file or command to the victim machine, the threat actors place them in the folder named “d” in the victim’s Dropbox folder. The malware retrieves this folder and downloads all its contents to the working folder. The backdoor establishes persistence by setting a registry key designed to run anytime a user logs on.

Cyber Espionage Actions Spotted by CPR

In this attack, some of the actions that CPR spotted included:

- Download and execution of a scanner tool widely used by multiple APT actors, including the prolific Chinese group APT10
- Execution of Windows built-in networking utility tools
- Access to the victim’s files, especially documents located on the Desktop

Targets: Afghanistan, Kyrgyzstan and Uzbekistan

While CPR saw the Dropbox variant targeting Afghan government officials, the variants are focused on political entities in two particular Central Asian countries, Kyrgyzstan and Uzbekistan. CPR provides specific indicators of the victimology in its technical report.

Figure 3. Targeted Region

The detection of cyber espionage continues to be a top priority for us. This time, we've detected an ongoing spear-phishing campaign targeting the Afghan government. We have grounds to believe that Uzbekistan and Kyrgyzstan have also been victims. We've attributed our findings to a Chinese-speaking threat actor. What is remarkable here is how the threat actors utilized the tactic of ministry-to-ministry deception. This tactic is vicious and effective in making anyone do anything for you; and in this case, the malicious activity was seen at the highest levels of sovereignty. Furthermore, it's noteworthy how the threat actors utilize Dropbox to mask themselves from detection, a technique that I believe we should all be aware of, and that we should all watch out for. It's possible that other countries have also been targeted by this hacker group, though we don't know how many or which countries. Hence, we're sharing a list of other possible domains used in the attack at this time, in hope that their names can be leveraged by other cyber researchers for contribution to our own findings.
