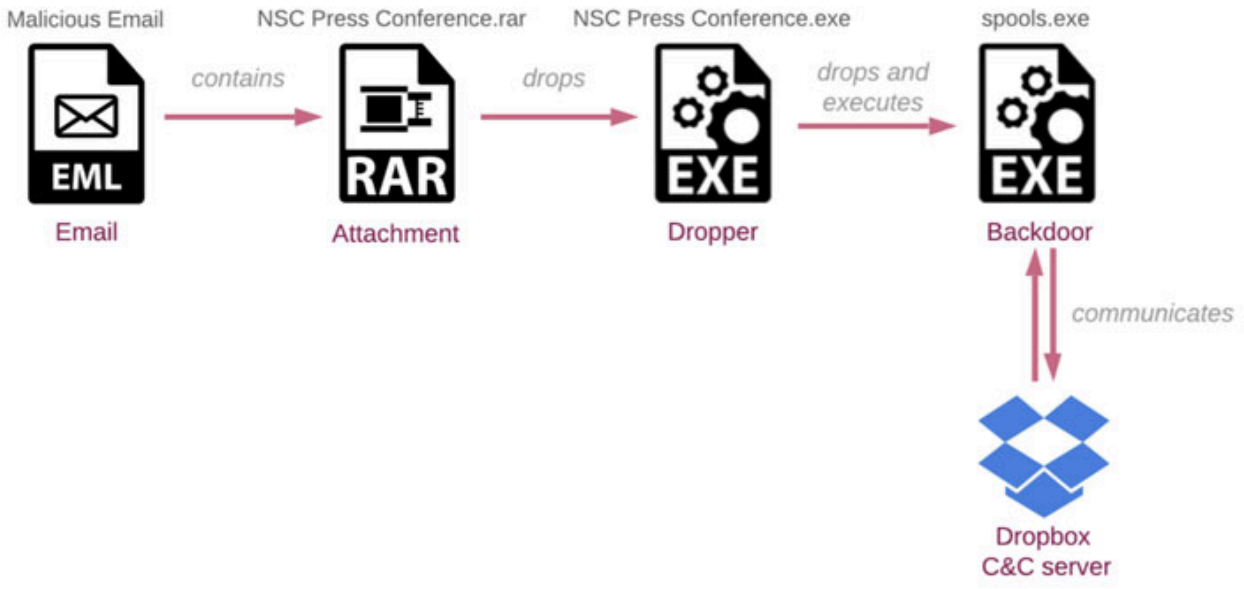
IndigoZebra APT Hacking Campaign Targets the Afghan Government

By The Hacker News

Published: 2021-07-01 · Archived: 2026-04-05 15:27:24 UTC



Cybersecurity researchers are warning of ongoing attacks coordinated by a suspected Chinese-speaking threat actor targeting the Afghanistan government as part of an espionage campaign that may have had its provenance as far back as 2014.

Israeli cybersecurity firm Check Point Research attributed the intrusions to a hacking group tracked under the moniker "IndigoZebra," with past activity aimed at other central-Asian countries, including Kyrgyzstan and Uzbekistan.

"The threat actors behind the espionage leveraged Dropbox, the popular cloud-storage service, to infiltrate the Afghan National Security Council (NSC)," the researchers said in a technical write-up shared with The Hacker News, adding they "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."

IndigoZebra first came to light in August 2017 when Kaspersky detailed a covert operation that singled out former Soviet Republics with a wide swath of malware such as Meterpreter, Poison Ivy RAT, xDown, and a previously undocumented piece of malware called xCaon.

Check Point's investigation into the attacks commenced in April when NSC officials began receiving lure emails allegedly claiming to be from the Administrative Office of the President of Afghanistan.

While the message urged the recipients to review modifications in an attached document related to a pending NSC press conference, opening the decoy file — a password-protected RAR archive ("NSC Press conference.rar") — was found to trigger an infection chain that culminated in the installation of a backdoor ("spools.exe") on the targeted system.

Additionally, the attacks funneled malicious commands into the victim machine that were camouflaged using the Dropbox API, with the implant creating a unique folder for every compromised host in an attacker-controlled Dropbox account.

The backdoor, dubbed "BoxCaon," is capable of stealing confidential data stored on the device, running arbitrary commands, and exfiltrating the results back to the Dropbox folder. The commands ("c.txt") themselves are placed in a separate sub-folder named "d" in the victim's Dropbox folder, which is retrieved by the malware prior to execution.

BoxCaon's connection to IndigoZebra stems from similarities shared by the malware with xCaon. Check Point said it identified about 30 different samples of xCaon — the earliest dating back to 2014 — all of which rely on HTTP protocol for command-and-control communications.

Telemetry data analyzed by the researchers also found that the HTTP variants primarily set their sights on political entities located in Kyrgyzstan and Uzbekistan, suggesting a shift in targeting in recent years along with a revamped toolset.

"What is remarkable here is how the threat actors utilized the tactic of ministry-to-ministry deception," said Lotem Finkelsteen, head of threat intelligence at Check Point.

"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."

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.

Source: https://thehackernews.com/2021/07/indigozebra-apt-hacking-campaign.html