Russia-Linked Hackers Target Diplomatic Entities in Central Asia

By Eduard Kovacs

Published: 2018-10-16 · Archived: 2026-04-05 19:56:51 UTC

Cybersecurity companies have been monitoring the activities of a threat group that focuses on espionage campaigns aimed at diplomatic entities in Central Asia.

Earlier this month, ESET detailed the threat actor's operations, which it tracks as Nomadic Octopus, at the Virus Bulletin conference. On Monday, Kaspersky also published a blog post covering some of the group's attacks and tools.

According to Kaspersky, which tracks the group as **DustSquad**, the hackers appear to speak Russian.

Anton Cherepanov, the ESET senior malware researcher who detailed Nomadic Octopus at Virus Bulletin, confirmed for *SecurityWeek* that the hackers may speak Russian based on the spear-phishing emails they send out and the use of Russian malware filenames.

ESET, which says the threat actor is very persistent, has identified only one type of malware used by Nomadic Octopus and has found evidence that the group has been active since at least 2015.

Kaspersky, however, has discovered both Windows and Android malware, and identified a campaign that dates as far back as 2014. The cyberspies appear to be focusing on private individuals and diplomatic entities in Central Asia, mostly former Soviet Union countries and Afghanistan.

In April 2018, researchers at Kaspersky discovered a new sample of DustSquad's Windows malware, which they are tracking as Octopus. The malware had been disguised as the Telegram messaging application, specifically a Russian version that appeared to have been used by the Democratic Choice (DVK) opposition party in Kazakhstan. The fake app emerged just as Kazakhstan had threatened to block Telegram over its use by the DVK.

DustSquad uses the Delphi programming language to develop its Octopus Trojan, the same as Sofacy's Zebrocy malware. While both DustSquad and Sofacy have been linked to Russia and malware from both groups was found on compromised machines, Kaspersky believes the threat actors are not related.

An analysis of the Octopus malware's different components revealed some apparently unfinished functionality. However, experts believe that the malware was actually created in a hurry and its developers decided not to implement certain capabilities.

Once it infects a system, the malware gives attackers remote access to the targeted machine, including the ability to execute commands, upload and download files, take screenshots, and search for RAR archives.

"Political entities in Central Asia have been targeted throughout 2018 by different actors, including IndigoZebra, Sofacy (with Zebrocy malware) and most recently by DustSquad (with Octopus malware)," Kaspersky researchers said. "Interestingly, we observed some victims who are 'threat magnets' targeted by all of them. From our experience we can say that the interest shown by threat actors in this region is now high, and the traditional 'players' have been joined by relative newcomers like DustSquad that have sprung up locally."

Related: Russian Cyberspies Shift Focus From NATO Countries to Asia

Related: Chinese Cyberspies Target National Data Center in Asia

Related: RANCOR Cyber Espionage Group Uncovered

Source: https://www.securityweek.com/russia-linked-hackers-target-diplomatic-entities-central-asia