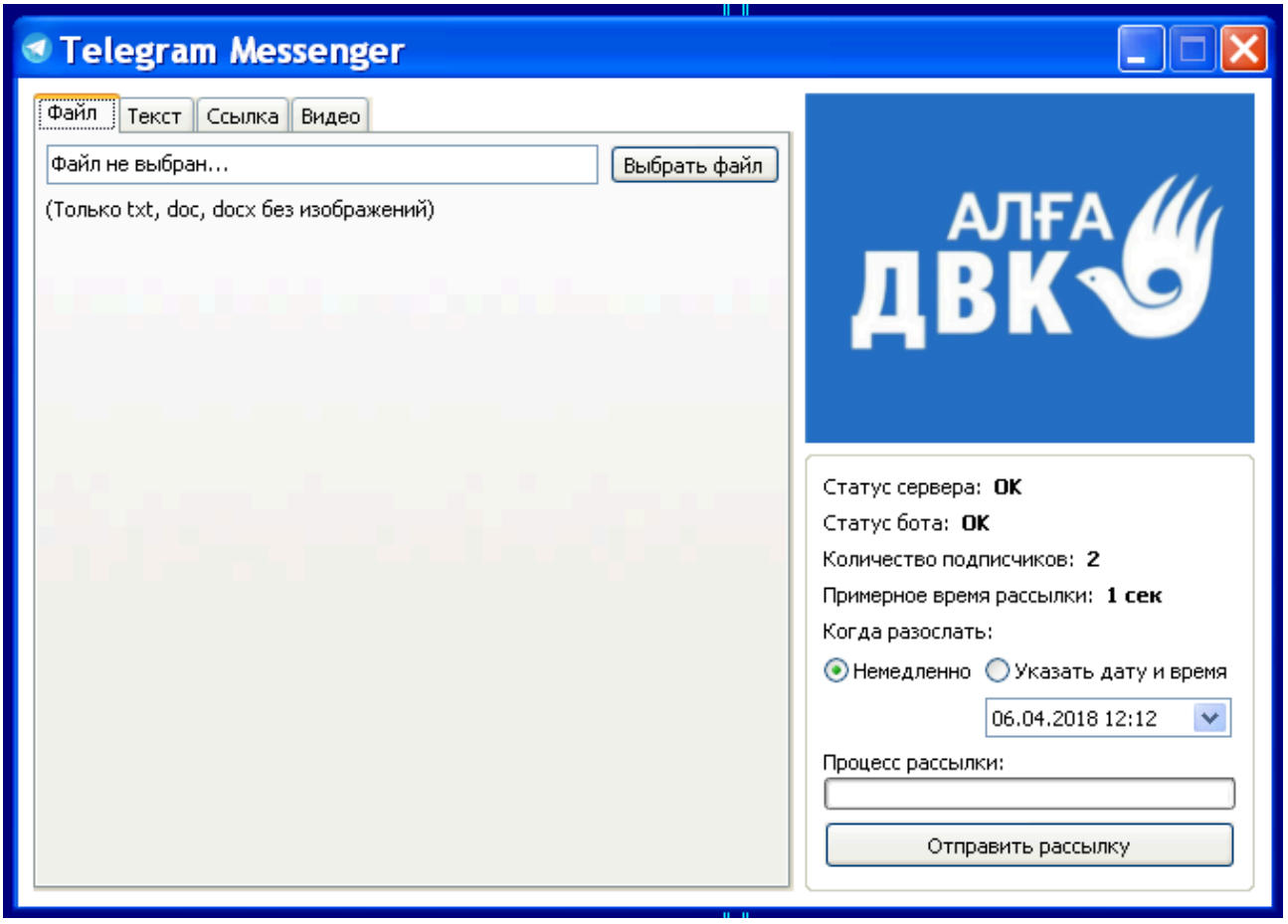
Russia-linked APT group DustSquad targets diplomatic entities in Central Asia

By Pierluigi Paganini

Published: 2018-10-16 · Archived: 2026-04-06 00:46:22 UTC



Kaspersky experts published a detailed analysis of the attacks conducted by the Russian-linked cyber espionage group DustSquad.

Earlier October, security experts from ESET shared details about the operations of a cyber espionage group tracked as Nomadic Octopus, a threat actor focused on diplomatic entities in Central Asia.

The group has been active since at least 2015, ESET researchers presented their findings at the Virus Bulletin conference.

“ESET researchers recently discovered an interesting cyber espionage campaign active in several countries of Central Asia. We attribute these attacks to a previously undocumented APT group that we have named Nomadic Octopus.” states the blog post published by Virus Bulletin.

"Our findings suggest that this APT group has been active since at least 2015. The main goal of Nomadic Octopus appears to be cyber espionage against high-value targets, including diplomatic missions in the region"

The experts presented their findings at the Virus Bulletin conference.

Now Kaspersky experts published a detailed analysis of the attacks conducted by the group, tracked by the Russian firm as **DustSquad,** and the tools they used.

Kaspersky is monitoring the activity of the group for the last two years, DustSquad is a Russian-language cyberespionage group particularly active in Central Asian.

"For the last two years *we have been monitoring a Russian-language cyberespionage actor that focuses on Central Asian users and diplomatic entities. We named the actor DustSquad and have provided private intelligence reports to our customers on four of their campaigns involving custom Android and Windows malware." states the [analysis](#) published by Kaspersky Lab.*

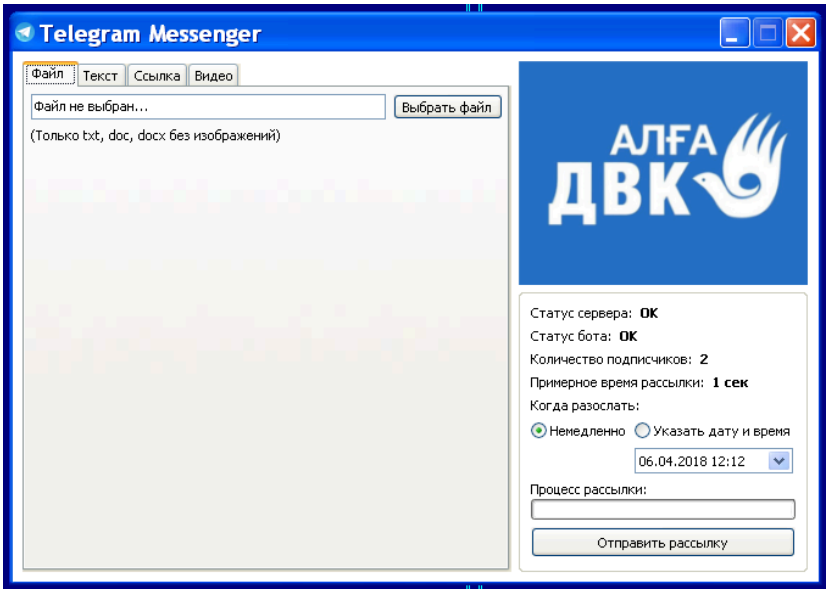
"The name was originally coined by ESET in 2017 after the 0ct0pus3.php script used by the actor on their old C2 servers. We also started monitoring the malware and, using Kaspersky Attribution Engine based on similarity algorithms, discovered that Octopus is related to DustSquad, something we reported in April 2018. "

The group targeted the victims with spear-phishing emails, the threat actors use Russian malware filenames.

Kaspersky tracked a campaign conducted by the group back to 2014 when hackers targeted entities in the former Soviet republics of Central Asia, plus Afghanistan.

In April 2018, the researchers discovered a new Octopus sample developed to target Windows systems, the malicious code had been disguised as a Russian version of the Telegram app used by the Democratic Choice (DVK) opposition party in Kazakhstan.

Attackers attempted to exploit the threaten of the Kazakhstan government to block Telegram over its use by the DVK.



The Octopus Trojan is written in Delphi, the same programming language used by Russian-linked APT group Sofacy for the development of the Zebrocy backdoor.

The malicious code backdoor features, including the ability to execute commands, upload and download files, take screenshots, and finding *.rar archives on the host.

Experts noticed that even if they found malware used by both DustSquad and Sofacy APT on the compromised machines, the two cyber espionage groups are not linked.

Kaspersky pointed out that many components of the Octopus malware are still unfinished, likely attackers created the malicious code in a hurry and not implemented certain features such as communication functionalities.

"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)," continues the Kaspersky report.

"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."*

Additional technical details are reported in the analysis, including IoCs.

[adrotate banner="9"]	**[adrotate banner="12"]**

Pierluigi Paganini

(Security Affairs – DustSquad, Russia)

[adrotate banner="5"]

[adrotate banner="13"]

Source: https://securityaffairs.co/wordpress/77165/apt/russia-linked-apt-dustsquad.html