ZDNET

Home / Tech / Security

Arid Viper hackers strike Palestine with political lures and Trojans

The threat group is suspected of being located in Gaza.

Written by **Charlie Osborne,** Contributing Writer

Feb. 2, 2022 at 5:00 a.m. PT

The Arid Viper cyberattack group is back with a new campaign targeting Palestinian organizations and activists.

Some of the world's most effective organizations are putting the latest AI

The advanced persistent threat (APT) group, believed to be located in Gaza -- an area of conflict and hotbed of tension between Israel and Palestine -- attacks organizations worldwide but now currently appears to be focused on entities related to Palestine's politics.

Arid Viper, also known as Desert Falcon, Two-tailed Scorpion, or APT C-23, has been around since at least 2015. In the past, the group has been responsible for spear phishing attacks against Palestinian law enforcement, the military, educational establishments, and the Israel Security Agency (ISA).

Windows and Android malware have been utilized previously, the latter of which is spread through fake app stores. Delphi malware, however, has featured heavily in ns and still seems to be the weapon of choice for Arid Viper.

On Wednesday, researchers from Cisco Talos said the ongoing campaign uses a Delphi-based Micropsia implant to strike activists.

"The most recent samples found by Talos lead us to believe this is a campaign linked to the previous campaign we reported on in 2017," the researchers say, adding that the main focus of Arid Viper is on cyberespionage -- and targets are selected by the operators based on the political motivation of the "liberation of Palestine."

The initial attack vector is phishing emails, with included content linked to the Palestinian political situation and usually stolen from news agencies. For example, one decoy document was related to Palestinian family reunification, published in 2021, whereas another contained a record of activist questions.

If an intended victim opens one of these documents, the implant triggers, extracting a range of Remote Access Trojan (RAT) capabilities. The malware will collect operating system and antivirus data, exfiltrate it to the operator's command-and-control (C2) server, steal content on the machine, take screenshots, and conduct further surveillance activities.

A timer contained in the implant will also establish persistence on the target machine through the Startup folder.

"The continued use of the same TTPs over the past four years indicates that the group doesn't feel affected by the public exposure of its campaigns and implants [illegible] operate business as usual," Talos says. "This complete lack of [illegible] them a dangerous group on [illegible] hey decide to target an [illegible] individual."

In related news this week, Talos and Cybereason disclosed three separate APT campaigns believed to be the work of state-backed Iranian cybercriminals. MuddyWater, Phosphorus, and Moses Staff are targeting entities in Turkey, the US, Israel, Europe, and the Middle East.

See also

- Chinese APT deploys MoonBounce implant in UEFI firmware
- Donot Team APT will strike gov't, military targets for years - until they succeed
- New advanced hacking group targets governments, engineers worldwide

Have a tip? Get in touch securely via WhatsApp | Signal at +447713 025 499, or over at Keybase: charlie0

/ security

8 habits of highly secure remote workers

How to find and remove spyware from your phone

The b comp

Editorial standards

show comments

Some of the world's most effective organizations are putting the latest AI

we equip you to harness the power of disruptive innovation, at work and at home.

Some of the world's most effective organizations are putting the latest AI

Some of the world's most effective organizations are putting the latest AI