Arid Viper Hacking Group Using Upgraded Malware in Middle East Cyber Attacks

Apr 04, 2023 Ravie Lakshmanan

The threat actor known as **Arid Viper** has been observed using refreshed variants of its malware toolkit in its attacks targeting Palestinian entities since September 2022.

Symantec, which is tracking the group under its insect-themed moniker Mantis, said the adversary is "going to great lengths to maintain a persistent presence on targeted networks."

Also known by the names APT-C-23 and Desert Falcon, the hacking group has been linked to attacks aimed at Palestine and the Middle East at least since 2014.

Mantis has used an arsenal of homemade malware tools such as ViperRat, FrozenCell (aka VolatileVenom), and Micropsia to execute and conceal its campaigns across Windows, Android, and iOS platforms.

The threat actors are believed to be native Arabic speakers and based in Palestine, Egypt, and Turkey, according to a report published by Kaspersky in February 2015. Prior public reporting has also tied the group to the cyber warfare division of Hamas.

In April 2022, high-profile Israeli individuals employed in sensitive defense, law enforcement, and emergency services organizations were observed being targeted with a novel Windows backdoor dubbed BarbWire.

Attack sequences mounted by the group typically employ spear-phishing emails and fake social credentials to lure targets into installing malware on their devices.

The most recent attacks detailed by Symantec entail the use of updated versions of its custom Micropsia and Arid Gopher implants to breach targets before engaging in credential theft and exfiltration of stolen data.

Arid Gopher, an executable coded in the Go programming language, is a variant of the Micropsia malware that was first documented by Deep Instinct in March 2022. The shift to Go is not unusual as it allows the malware to stay under the radar.

Micropsia, alongside its ability to launch secondary payloads (like Arid Gopher), is also designed to log keystrokes, take screenshots, and save Microsoft Office files within RAR archives for exfiltration using a bespoke Python-based tool.

"Arid Gopher, like its predecessor Micropsia, is an info-stealer malware, whose intent is to establish a foothold, collect sensitive system information, and send it back to a C2 (command-and-control) network," Deep Instinct said at the time.

Evidence gathered by Symantec shows that Mantis moved to deploy three distinct versions of Micropsia and Arid Gopher on three sets of workstations between December 18, 2022, and January 12, 2023, as a way of retaining access.

Arid Gopher, for its part, has received regular updates and complete code rewrites, with the attackers "aggressively mutating the logic between variants" as a detection evasion mechanism.

"Mantis appears to be a determined adversary, willing to put time and effort into maximizing its chances of success, as evidenced by extensive malware rewriting and its decision to compartmentalize attacks against single organizations into multiple separate strands to reduce the chances of the entire operation being detected," Symantec concluded.

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

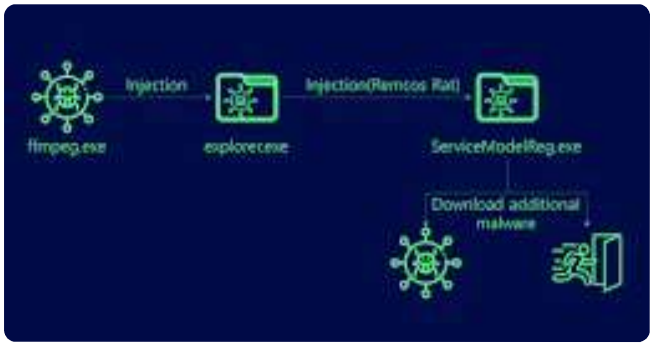
CYBERSECURITY WEBINARS

Breaking News

Zero-Day Alert: Update Chrome Now to Fix New Actively Exploited Vulnerability...

Alert: Over 178,000 SonicWall Firewalls Potentially Vulnerable to Exploits - Act Now...

Case Study: The Cookie Privacy Monster in Big Global Retail...

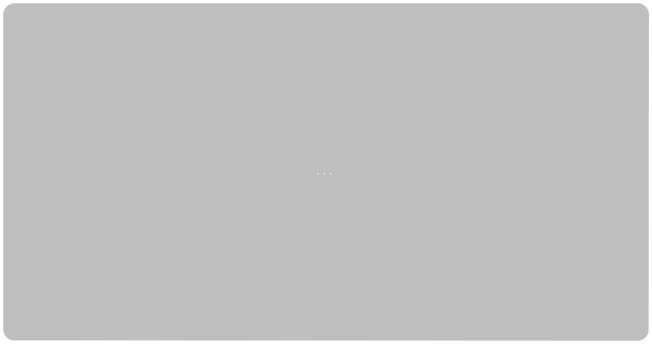


Remcos RAT Spreading Through Adult Games in New Attack Wave...

Cybersecurity Resources

MSPs & MSSPs: Start Your vCISO Journey Here

ThreatLocker® Redefines Incident Response with Zero Trust



Empower Your Defense with SMB Threat Insights

Earn a Master's in Cybersecurity Risk Management

Join 120,000+ Professionals

Sign up for free and start receiving your daily dose of cybersecurity news, insights and tips.

Your e-mail address

Connect with us!

Company

About THN
Advertise with us
Contact

Pages

Webinars
Deals Store
Privacy Policy

Contact Us