cyber espionage
hacktivism

attributed to Moses Staff have involved RATs and ransomware with no indications of
responsibility for attacks on entities located outside of Israel but with geopolitical
two groups are likely part of a single cluster (also referred to as Cobalt Sapling) and

Lebanese Cedar is a lesser-reported APT with a history of successful intrusions
CreepyDrive malware uses Cloud services for command and control purposes, likely
consists of a wide range of well-maintained custom tooling exemplified by the Creepy

Plaid Rain is a threat actor rst documented in 2022 with a primary focus on targeting

Gaza Cybergang is a threat actor that has been active since at least 2012. The group
Their attacks, showing a notable preference for

Arvid Viper. This includes pre-selected
campaign targeting soldiers stationed near the Gaza border, which is suspected to be

Based primarily on the geopolitical context of its activities, Arid Viper is suspected to

operations since at least 2017, predominantly against targets in the Middle East.

Taking Action Against Arid Viper – Meta

The Desert Falcons targeted attacks – GReAT

Mantis: New Tooling Used in Attacks Against Palestinian Targets –

Arid Viper Disguising Mobile Spyware as Updates for Non-Malicious

Mole Rat targets Palestine with new wave of politically themed

Gaza Cybergang

The overall objectives of Gaza Cybergang appear to be primarily intelligence

access. They have been known to use malicious documents and email attachments to

their attacks, showing a notable preference for

scripting languages, such as Delphi, Go, Python, and C++.

In recent years, Gaza Cybergang has targeted the Israeli military, with a particular focus on soldiers stationed near the Gaza border. Their tactics include the use of targeted attacks involving the compromise of computer systems and networks, with a notable preference for using malicious documents and email attachments to deliver implants and maintain access.

Potential collaboration between MOIS and Plaid Rain positions this threat group in

the attacks from Hamas on October 7th, social media became a hotbed of

By Tom Hegel and Aleksandar Milenkoski

State-Sponsored Activity of Interest

The Israel-Hamas War | Cyber Domain

Tom Hegel is a Senior Threat Researcher with SentinelOne. He

©2023 SentinelOne, All Rights Reserved.