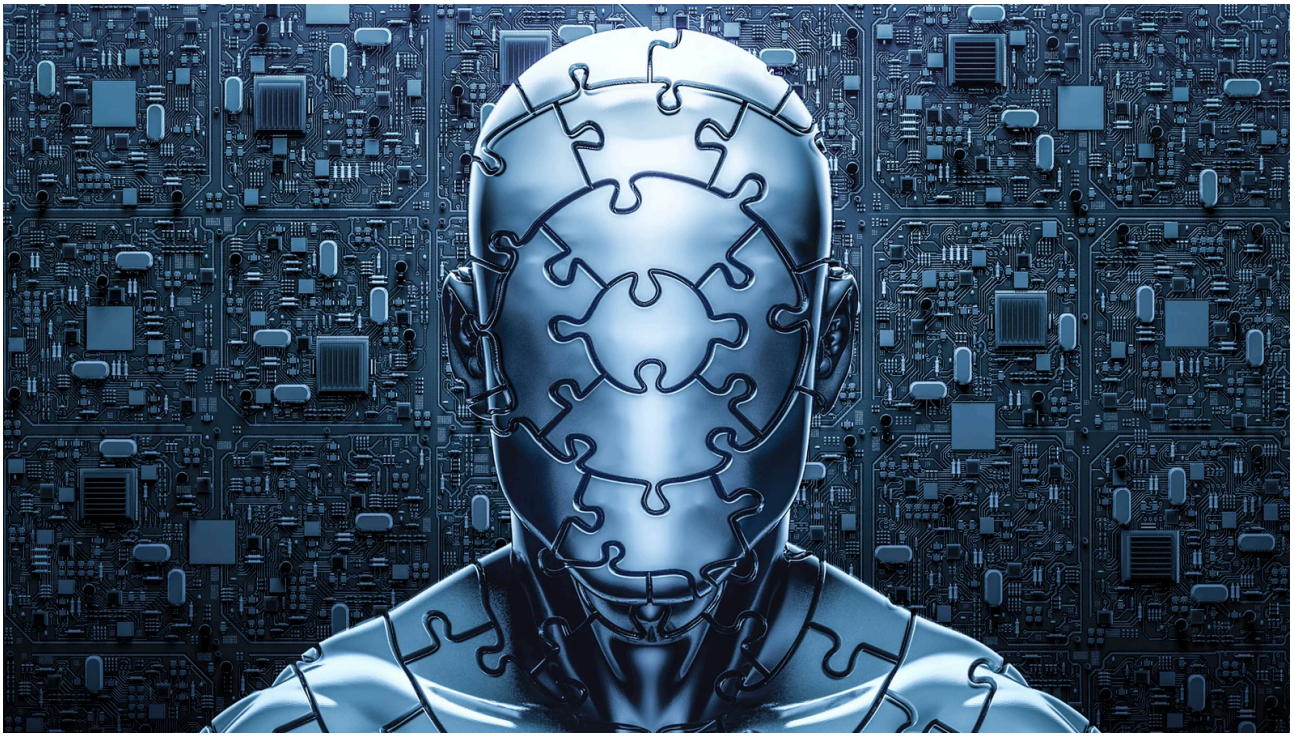
Hacking group POLONIUM uses ‘Creepy’ malware against Israel

By Bill Toulas

Published: 2022-10-11 · Archived: 2026-04-10 02:44:11 UTC



Security researchers reveal previously unknown malware used by the cyber espionage hacking group 'POLONIUM,' threat actors who appear to target Israeli organizations exclusively.

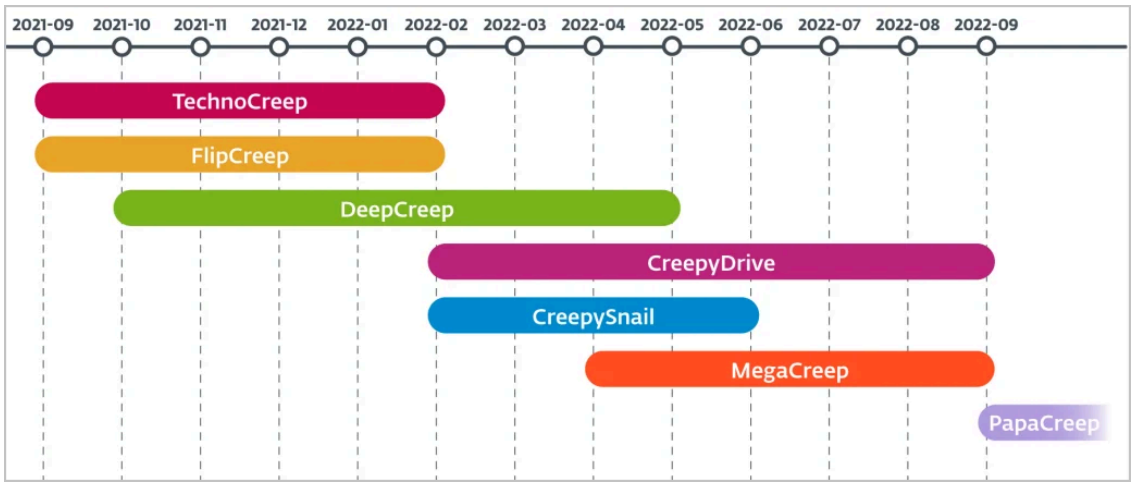
According to ESET, POLONIUM uses a broad range of custom malware against engineering, IT, law, communications, marketing, and insurance firms in Israel. The group's campaigns are still active at the time of writing.

Microsoft's Threat Intelligence team first documented the group's malicious activities in June 2022, linking POLONIUM threat actors in Lebanon with ties to Iran's Ministry of Intelligence and Security (MOIS).

The POLONIUM toolset

ESET reports that POLONIUM is solely interested in cyberespionage and does not deploy data wipers, ransomware, or other file-damaging tools.

Since September 2021, the hackers have used at least seven variants of custom backdoors, including four new undocumented backdoors known as 'TechnoCreep', 'FlipCreep', 'MegaCreep',, and 'PapaCreep.'



The seven backdoors deployed by POLONIUM since September 2021 *(ESET)*

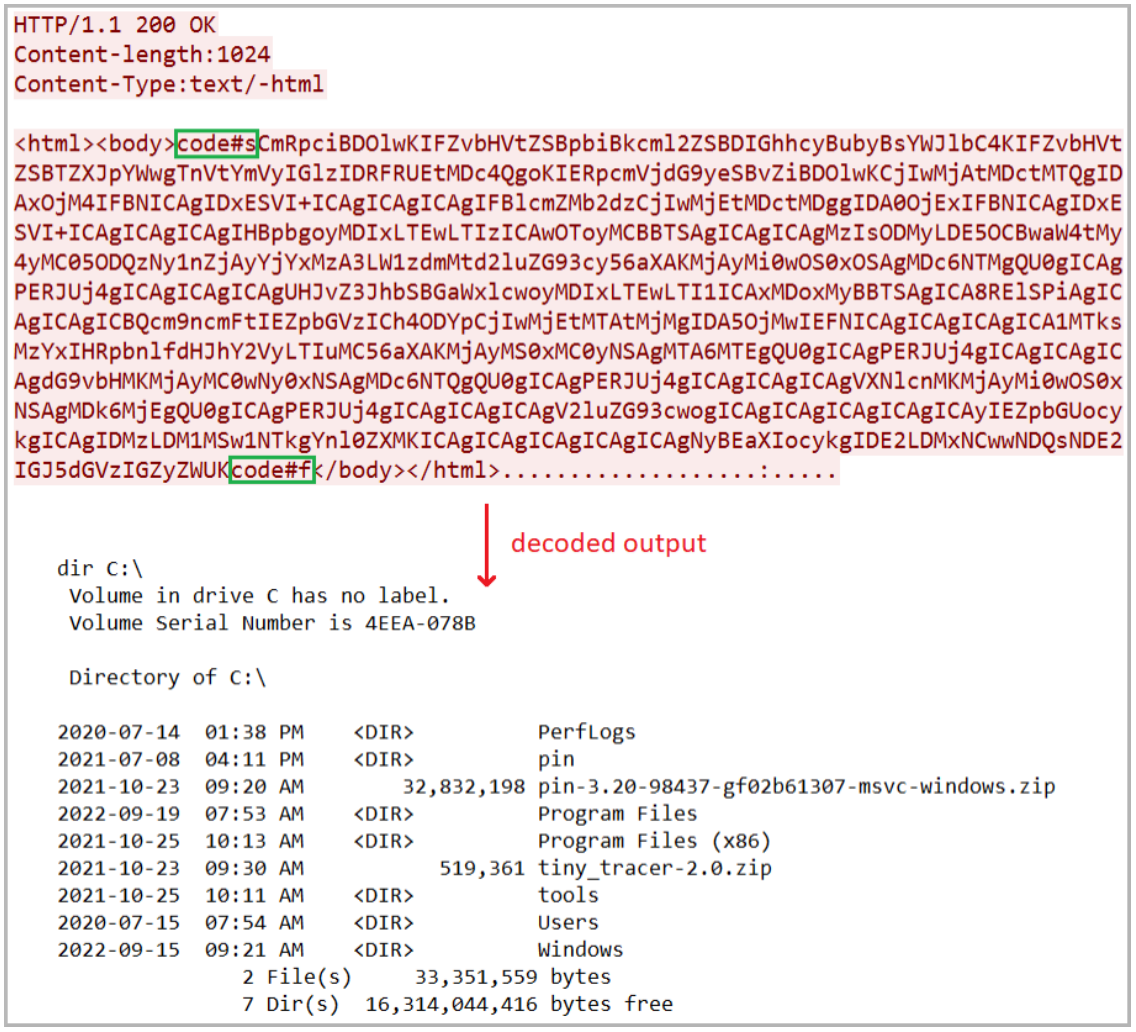
Some backdoors abuse legitimate cloud services, such as OneDrive, Dropbox, and Mega, to act as command and control (C2) servers. Other backdoors utilize standard TCP connections to remote C2 servers or get commands to execute from files hosted on FTP servers.

While not all backdoors have the same features, their malicious activity includes the ability to log keystrokes, take screenshots of the desktop, take photos with the webcam, exfiltrate files from the host, install additional malware, and execute commands on the infected device.

The most recent backdoor, PapaCreep, spotted in September 2022, is the first one in C++, whereas the hackers wrote older versions either in PowerShell or C#.

PapaCreep is also modular, breaking its command execution, C2 communication, file upload, and file download functions into small components.

The advantage is that the components can run independently, persist via separate scheduled tasks in the breached system, and make the backdoor harder to detect.



PapaCreep's encrypted request to C2 *(ESET)*

Besides the 'Creepy' variants, POLONIUM also uses various open source tools, either custom or off-the-shelf, for reverse proxying, screenshot taking, keylogging, and webcam snapping, so there's a level of redundancy in the operations.

An elusive hacking group

ESET couldn't discover POLONIUM's tactics used to initially compromise a network, but Microsoft previously reported that the group was using known VPN product flaws to breach networks.

The threat actor's private network infrastructure is hidden behind virtual private servers (VPS) and legitimate compromised websites, so mapping the group's activities remains murky.

POLONIUM is a sophisticated and highly targeted threat whose crosshairs are fixed at Israel right now, but this could change any moment if the priorities or interests change.

Source: https://www.bleepingcomputer.com/news/security/hacking-group-polonium-uses-creepy-malware-against-israel/