

Hacking group POLONIUM uses 'Creepy' malware against Israel

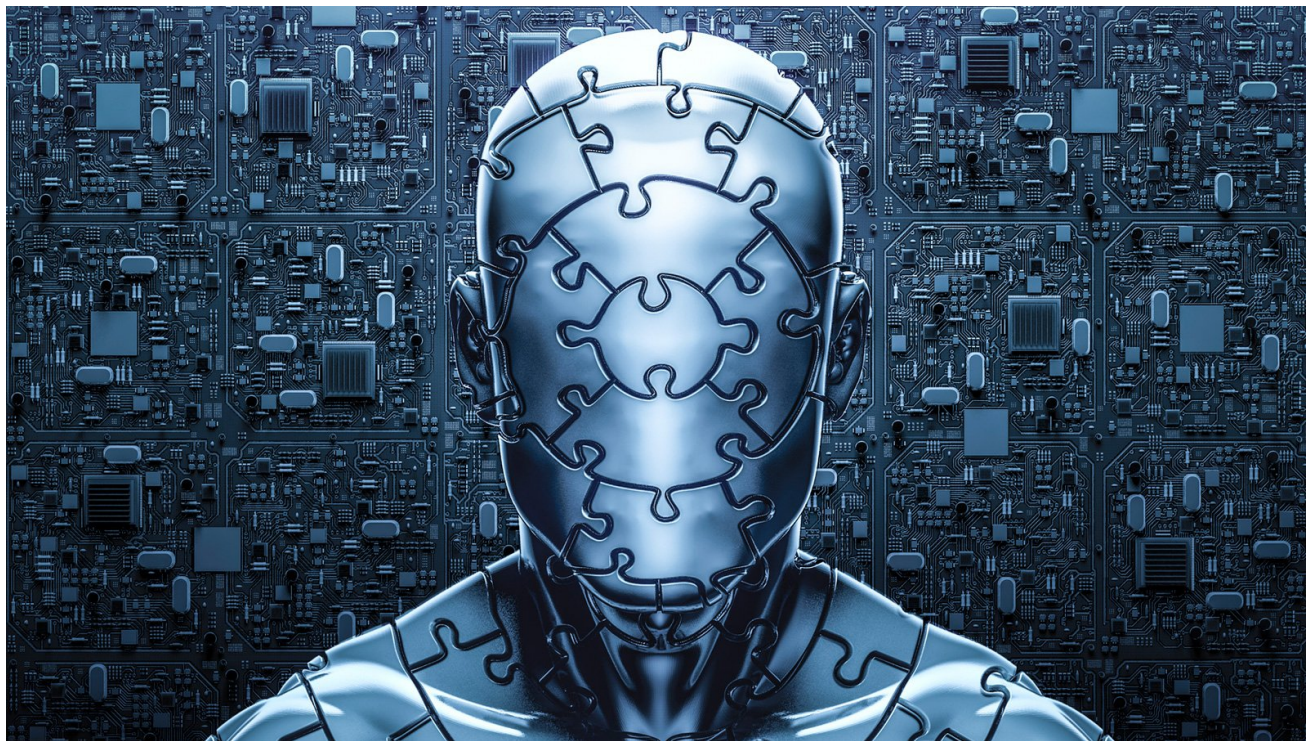
bleepingcomputer.com/news/security/hacking-group-polonium-uses-creepy-malware-against-israel/

Bill Toulas

By

[Bill Toulas](#)

- October 11, 2022
- 05:30 AM
- [0](#)



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

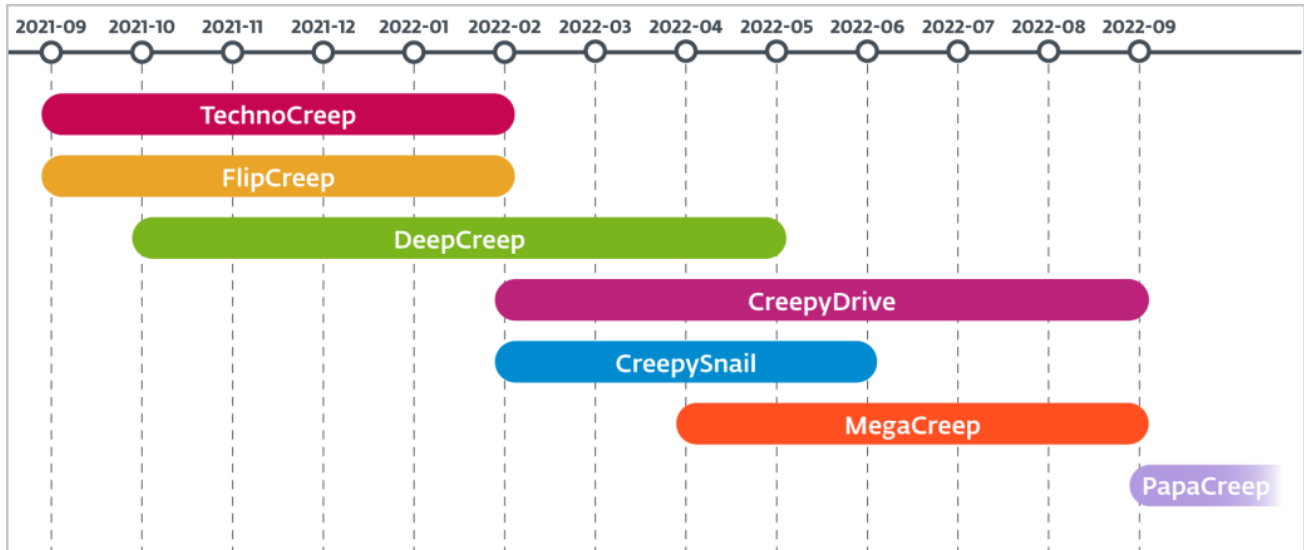
According to ESET, POLONIUM uses a broad range of custom malware against engineering, IT, law, communications, marketing, and insurance firms in Israel. The group's campaigns are still active at the time of writing.

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.

```
HTTP/1.1 200 OK
Content-length:1024
Content-Type:text/html
```

```
<html><body>code#sCmRpciBD0lwKIFZvbHVtZSBpbiBkcm12ZSBDIGhhcyBubyBsYWJlbc4KIFZvbHVt
ZSBTZXJpYWwgTnVtYmVyIGlzIDRFRUETMdc4QgoKIERpcmVjdG9yeSBvZiBD0lwKCjIwMjAtMDctMTQgID
AxOjM4IFBNCiAgIDxEsVI+ICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
Svi+ICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
4yMC05ODQzNy1nZjAyYjYxMzA3LW1zdmMtd2luZG93cy56aXAKMjAyMi0wOS0xOSAgMDc6NTMgQU0gICAg
PERJUj4gICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
AgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIC
MzYxIHRpbnlfdHJhY2VyLTlucm56aXAKMjAyMS0xMC0yNSAgMTA6MTEgQU0gICAgICAgICAgICAgICAgIC
AgdG9vbHMkMjAyMC0wNy0xNSAgMDc6NTQgQU0gICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIC
NSAgMDk6MjEgQU0gICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
kgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
IGJ5dGVzIGZyZWUKcode#f</body></html>.....:.....
```

↓ decoded output

```
dir C:\
Volume in drive C has no label.
Volume Serial Number is 4EEA-078B

Directory of C:\

2020-07-14 01:38 PM <DIR> PerfLogs
2021-07-08 04:11 PM <DIR> pin
2021-10-23 09:20 AM 32,832,198 pin-3.20-98437-gf02b61307-msvc-windows.zip
2022-09-19 07:53 AM <DIR> Program Files
2021-10-25 10:13 AM <DIR> Program Files (x86)
2021-10-23 09:30 AM 519,361 tiny_tracer-2.0.zip
2021-10-25 10:11 AM <DIR> tools
2020-07-15 07:54 AM <DIR> Users
2022-09-15 09:21 AM <DIR> Windows
                2 File(s) 33,351,559 bytes
                7 Dir(s) 16,314,044,416 bytes free
```

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.

Related Articles:

[Microsoft: Iranian hackers encrypt Windows systems using BitLocker](#)

[New Iranian hacking group APT42 deploys custom Android spyware](#)

[Hacking group updates Furball Android spyware to evade detection](#)

[Hackers target Asian casinos in lengthy cyberespionage campaign](#)

[Signal calls on users to run proxies for bypassing Iran blocks](#)

- [APT](#)
- [Hacking Group](#)
- [Iran](#)
- [Israel](#)
- [Lebanon](#)
- [Polonium](#)

[Bill Toulas](#)

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.

- [Previous Article](#)
- [Next Article](#)

Post a Comment [Community Rules](#)

You need to login in order to post a comment

Not a member yet? [Register Now](#)

You may also like:
