Iranian Hackers Using New Marlin Backdoor in 'Out to Sea' Espionage Campaign

thehackernews.com/2022/02/iranian-hackers-using-new-marlin.html

February 9, 2022

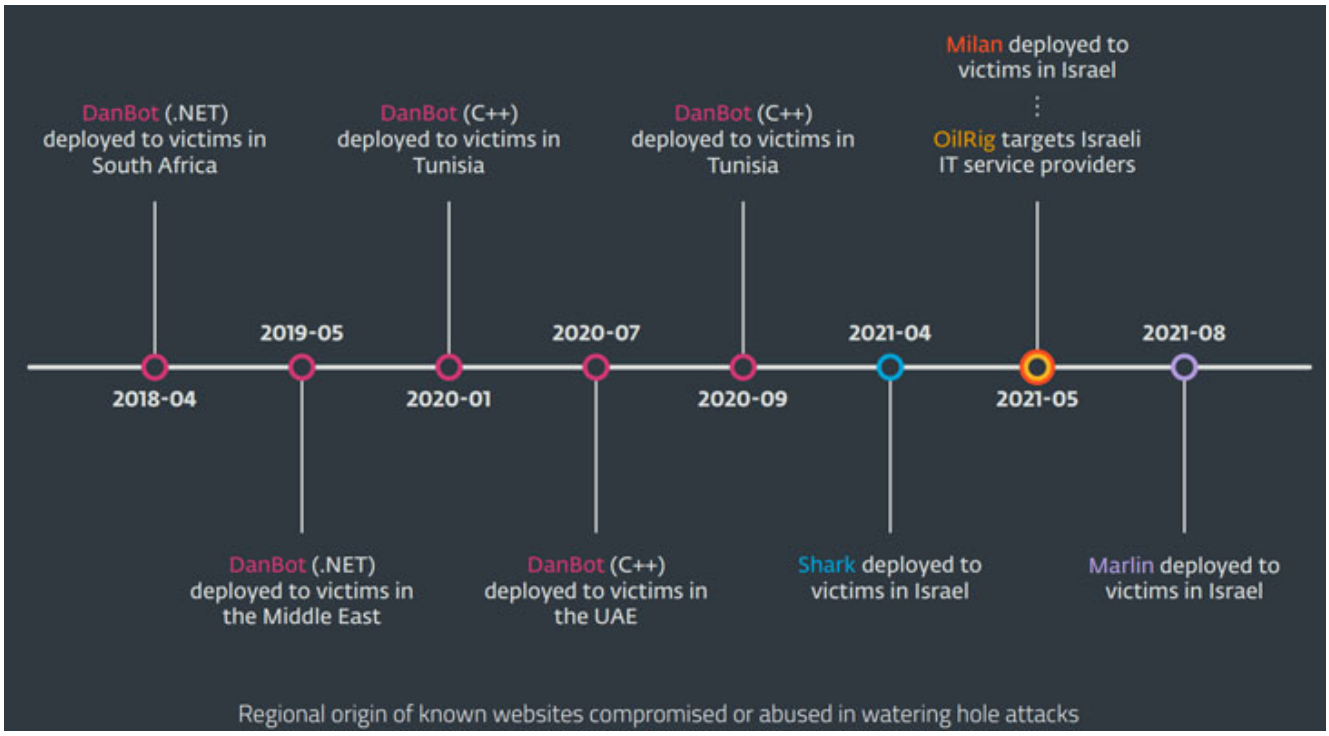
An advanced persistent threat (APT) group with ties to Iran has refreshed its malware toolset to include a new backdoor dubbed **Marlin** as part of a long-running espionage campaign that started in April 2018.

Slovak cybersecurity company ESET attributed the attacks — codenamed **"Out to Sea"** — to a threat actor called OilRig (aka APT34), while also conclusively connecting its activities to a second Iranian group tracked under the name Lyceum (Hexane aka SiameseKitten).

"Victims of the campaign include diplomatic organizations, technology companies, and medical organizations in Israel, Tunisia, and the United Arab Emirates," ESET noted in its T3 2021 Threat Report shared with The Hacker News.

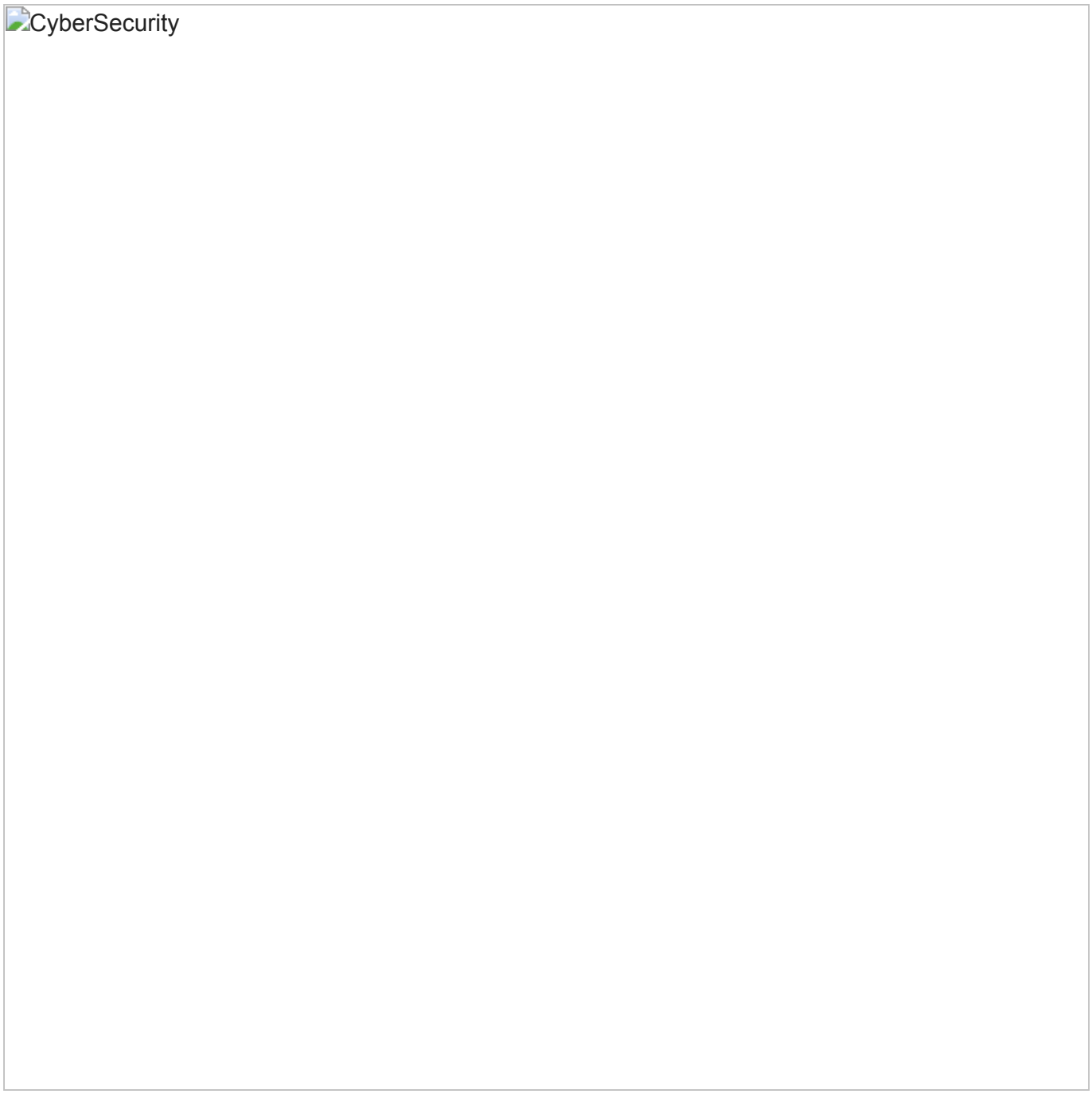
Active since at least 2014, the hacking group is known to strike Middle Eastern governments and a variety of business verticals, including chemical, energy, financial, and telecommunications. In April 2021, the actor targeted a Lebanese entity with an implant called SideTwist, while campaigns previously attributed to Lyceum have singled out IT companies in Israel, Morocco, Tunisia, and Saudi Arabia.

The Lyceum infection chains are also notable for the fact that they have evolved to drop multiple backdoors since the campaign came to light in 2018 — beginning with DanBot and transitioning to Shark and Milan in 2021 — with attacks detected in August 2021 leveraging a new data collection malware called Marlin.



The changes don't end there. In what's a significant departure from traditional OilRig TTPs, which have involved the use of DNS and HTTPS for command-and-control (C&C) communications, Marlin makes use of Microsoft's OneDrive API for its C2 operations.

ESET, noting that initial access to the network was achieved by means of spear-phishing as well as remote access and administration software like ITbrain and TeamViewer, cited similarities in tools and tactics between OilRig's backdoors and that of Lyceum as "too numerous and specific."



"The ToneDeaf backdoor primarily communicated with its C&C over HTTP/S but included a secondary method, DNS tunneling, which does not function properly," the researchers said. "Shark has similar symptoms, where its primary communication method uses DNS but has a non-functional HTTP/S secondary option."

ToneDeaf, which supports collecting system information, uploading and downloading of files, and arbitrary shell command execution, is a malware family that was deployed by the APT34 actor targeting a broad range of industries operating in the Middle East in July 2019.

Additionally, the findings also pointed out the overlapping use of DNS as a C&C communication channel, while also employing HTTP/S as a secondary communication method and the use of multiple folders in a backdoor's working directory for uploading and downloading files from the C&C server.

SHARE □ □ □ □ □

SHARE □