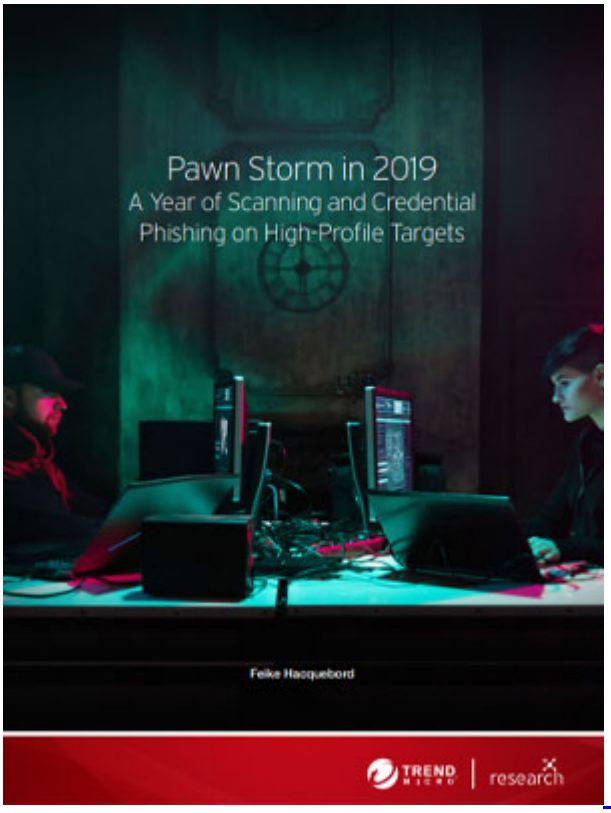
Probing Pawn Storm: Cyberespionage Campaign Through Scanning, Credential Phishing and More

By By Feike Hacquebord (Trend Micro Research)

Archived: 2026-04-05 18:26:30 UTC



open on a new tabDownload Probing Pawn Storm: Cyberespionage Campaign Through Scanning, Credential Phishing and More

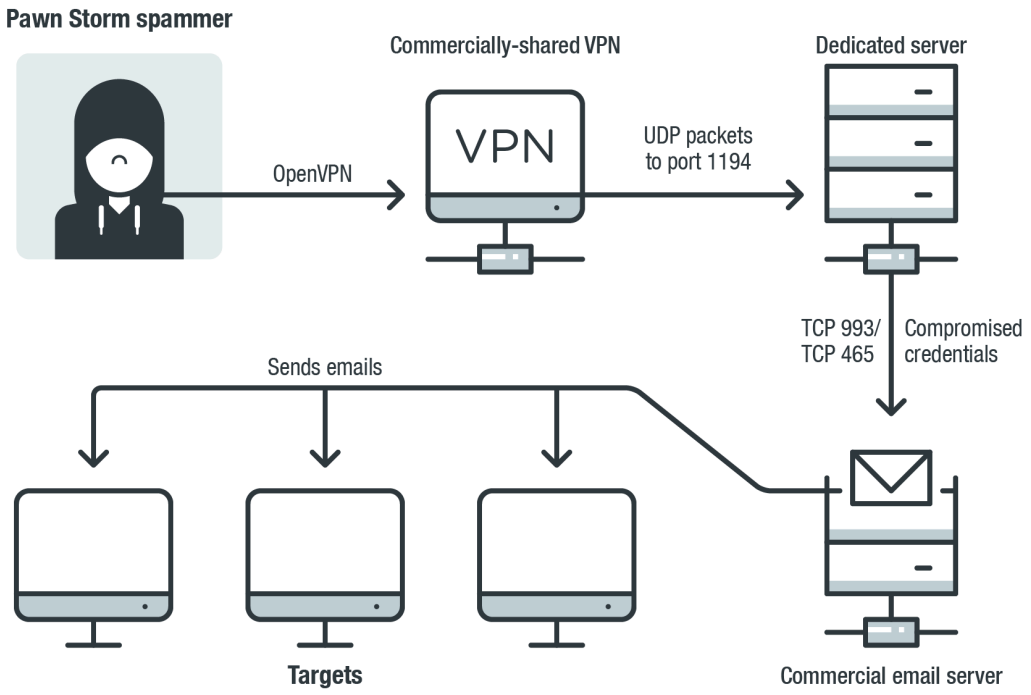
Pawn Stormopen on a new tab, an ongoing cyberespionage campaign with activities that can be traced as far back as 2004, has gained notoriety after aiming cyber-attacks at defense contractor personnel, embassies, and military forces of the United States and its allies, as well as international media and citizens across different civilian industries and sectors, among other targets.

For years, Trend Micro has been closely monitoring Pawn Storm and its various attack vectors and methodologiesopen on a new tab, which have been generally facilitated for geopolitical disruption and espionage. This newer operation has employed a number of attack methods, including the use of spear-phishing emails against high-profile targets, a staple in Pawn Storm's arsenal. Here are some of the many threats the group has wielded against its targets:

- Watering hole attacksopen on a new tab against compromised websites frequently visited by targets
- Open Authentication (OAuth) abuseopen on a new tab for compromising targets in advanced social engineering schemes

- Private exploit kitopen on a new tab that included zero-days and common vulnerabilities used to infect targets
- iOS spywareopen on a new tab specifically designed for espionage
- Tabnabbingopen on a new tab for persuading users into submitting credentials to known (impersonated) sites

We have uncovered more information on the group's current attack methods, which primarily centered on scanning for servers and credential phishingopen on a new tab among high-profile entities. Below we give an overview of our other notable findings from the past year.

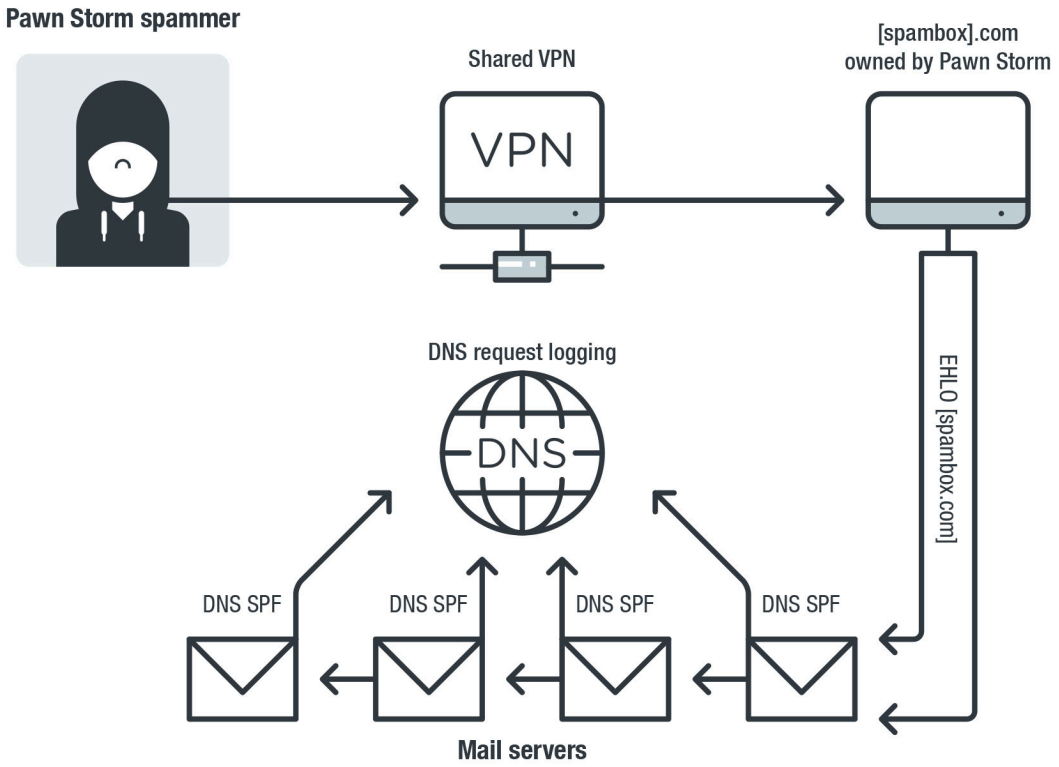


open on a new tab

The setup Pawn Storm frequently used to send out credential phishing spam in 2019

Since May 2019, Pawn Storm has been abusing compromised email addresses to send credential phishing spam. The majority of the compromised systems were from defense companies in the Middle East. Other targets included organizations in the transportation, utilities, and government sectors.

Pawn Storm also regularly probed many email and Microsoft Exchange Autodiscover servers across the world. The group looked for vulnerable systems in an attempt to brute force credentials, exfiltrate email data, and send out waves of spam.



open on a new tab

The setup we used to monitor Pawn Storm's email campaigns for more than two years

Our more than two-year-long monitoring of all DNS requests for Pawn Storm's domains also enabled us to monitor and detect credential phishing campaigns that the group has facilitated from their servers from 2017 to 2019. The campaigns included spam waves against webmail providers in the United States, Russia, and Iran.

Our research, "Pawn Storm in 2019: A Year of Scanning and Credential Phishing on High-Profile Targetsopen on a new tab," covers these developments and the group's other noteworthy activities, what organizations can best do to minimize the risk of compromise across all layers, and indicators of compromise.

Trend Micro Solutions

Organizations and governments can benefit from advanced Trend Micro solutions that can proactively keep IT environments protected from a wide range of cybersecurity threats. The Trend Micro™ XDRopen on a new tab solution effectively protects connected emails, endpoints, servers, cloud workloads, and networks. Trend Micro XDR uses powerful AI and expert security analytics to correlate data, as well as deliver fewer yet higher-fidelity alerts for early threat detection. In a single console, it provides a broader perspective of enterprise systems while at the same time giving a more focused and optimized set of alerts. This allows IT security teams to have better context for identifying threats more quickly and therefore to understand and remediate impact much more effectively.

Meanwhile, Trend Micro Managed XDRopen on a new tab provides expert threat monitoring, correlation, and analysis from skilled and seasoned Managed Detection and Response analysts. Managed XDR is a flexible, 24/7 service that allows organizations to have one single source of detection, analysis, and response. Analyst expertise

is enhanced by Trend Micro solutions that are optimized by AI and enriched by global threat intelligence. The Managed XDR service allows organizations to expand with the cloud without sacrificing security or overburdening IT teams.

HIDE

Like it? Add this infographic to your site:

1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.
