



Weekly Intelligence Briefing

27 March 2026

The Weekly Intelligence Briefing is intended to provide current intelligence on the cyber threat landscape relevant to the FS-ISAC membership. It synthesizes insights from monitoring operations and member sharing to concisely highlight key areas of concern.

Current Developments

TeamPCP Orchestrates Open-Source Supply Chain Campaign

Summary: The cybercrime group TeamPCP is reportedly responsible for a month-long open-source software supply chain campaign across five ecosystems: GitHub Actions, Docker Hub, npm, OpenVSX, and PyPI. Beginning with the compromise of the [Trivy](#) open-source security scanner on 19 March, TeamPCP leveraged downstream access to distribute a self-propagating worm named "[CanisterWorm](#)." On 22 March, the worm was identified deploying a [wiper payload](#) specifically targeting Kubernetes Clusters on systems that use the Iranian time zone or are configured with Farsi as a default language. Subsequently, on 23 March, TeamPCP compromised the application security firm [CheckMarx's](#) open-source KICS infrastructure-as-code security scanner. On 24 March, TeamPCP similarly exploited the open-source Python library [LiteLLM](#) to perpetrate extensive secret and credential collection, while establishing persistent backdoors in compromised software development pipelines. TeamPCP's recent focus on [security-adjacent tools](#) is likely intended to compromise valuable credentials and other secrets which enable broad, downstream access.

FS-ISAC Comment: [TeamPCP](#) first emerged in December 2025 compromising corporate cloud environments using a self-propagating worm that exploited exposed Docker APIs, Kubernetes clusters, Redis servers, and the React2Shell vulnerability. According to security researchers, TeamPCP commonly boasts about their exploits on Telegram, which suggests the targeting of misconfigured Iranian cloud services may be an attempt to use the ongoing conflict to garner notoriety in the cybercriminal community.

Tycoon2FA Persists Following Takedown

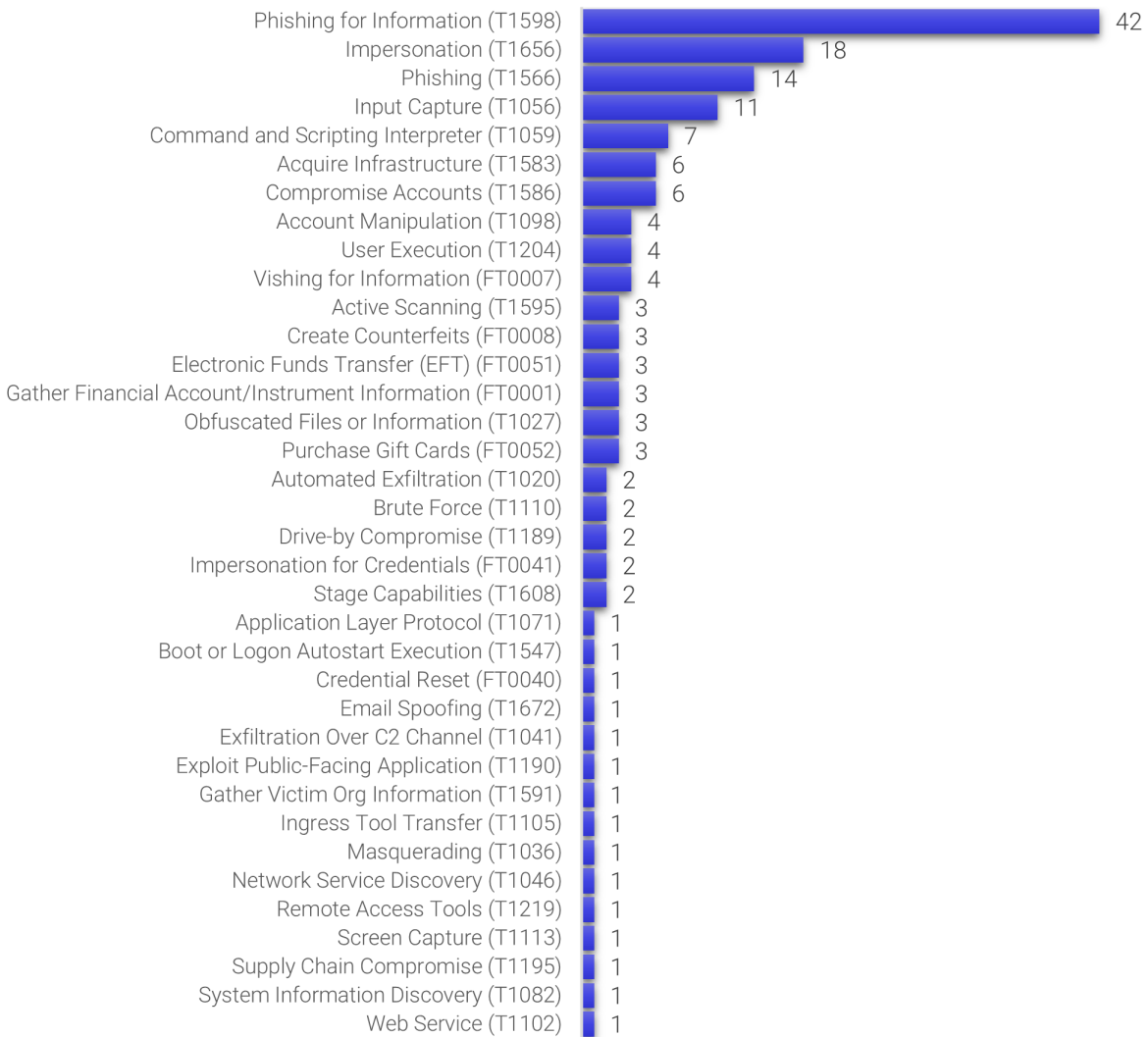
Summary: On 4 March, [Europol](#) announced the technical disruption of Tycoon2FA, a subscription-based phishing-as-a-service (PhaaS) platform that enabled cybercriminals to bypass multifactor authentication (MFA) and compromise email accounts. Law enforcement authorities from six countries worked with industry partners to seize 330 domains that formed the platform's core infrastructure. However, on 20 March, [CrowdStrike](#) reported that despite experiencing a short-term decrease in volume, Tycoon2FA campaign activity has resurged to early 2026 levels.

FS-ISAC Comment: Tycoon2FA began its operations in 2023 and provided a subscription-based toolkit that intercepted live authentication sessions using adversary-in-the-middle (AITM) techniques. In mid-2025, the platform was responsible for 62% of all phishing attempts blocked by [Microsoft](#). Although temporary, the service's disruption likely set back current customers by impeding phishing operations and damaged the long-term reputation of the PhaaS provider in the crimeware landscape.

THREAT METRICS OVERVIEW

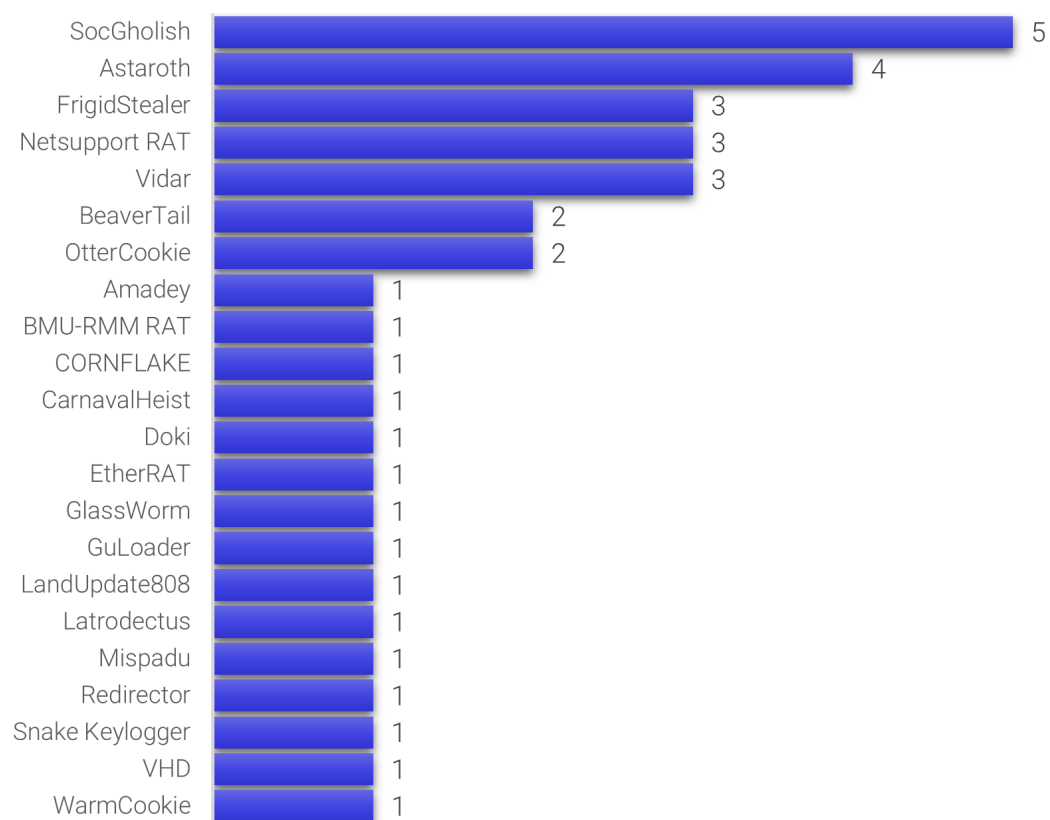
These threat metrics cover member submissions for the reporting period 18 March 2026 to 24 March 2026.

Techniques:*



*A single member submission may be associated with more than one technique.

Malware Variants:



Notable Publications & Member Submissions

- **TLP AMBER:** Trivy Supply Chain Compromise - 20 MAR 2026– Alert ID: [d5770145](#)
- **TLP AMBER:** SEO Poisoning & GitHub - EtherRat Campaign – Alert ID: [7366a23c](#)
- **TLP AMBER:** Threat Actor "UAT-9244" (Famous Sparrow/Salt Typhoon) Reconnaissance Activity – Alert ID: [0598d5e1](#)
- **TLP AMBER:** MuddyWater Malware Variants - Detection Opportunities and IOCs – Alert ID: [99d6b3b8](#)
- **TLP AMBER:** Kongtuke ClickFix Leading to VICE SPIDER CORNFLAKE Deployment – Alert ID: [2b84bf9c](#)

FOR FS-ISAC MEMBERS ONLY. Please direct feedback and questions to intelligence@fsisac.com.

TLP **GREEN** 

© FS-ISAC 2026

12120 Sunset Hills Rd, Reston
VA 20190

To manage emails you may receive, please log in to the Member Services platform of the Intelligence Exchange to [update subscription preferences](#).