Threat intelligence | Microsoft Security Blog

Published: 2026-04-01 · Archived: 2026-04-05 22:59:02 UTC

The Microsoft Threat Intelligence community is made up of world-class experts, security researchers, analysts, and threat hunters who analyze 100 trillion signals daily to discover threats and deliver timely and timely, relevant insight to protect customers. See our latest findings, insights, and guidance.

Filtered by

Clear All

- Threat intelligence

Refine results

- **Mitigating the Axios npm supply chain compromise**

On March 31, 2026, the popular HTTP client Axios experienced a supply chain attack, causing two newly published npm packages for version updates to download from command and control (C2) that Microsoft Threat Intelligence has attributed to the North Korean state actor Sapphire Sleet.

- **When tax season becomes cyberattack season: Phishing and malware campaigns using tax-related lures**

  During tax season, threat actors reliably take advantage of the urgency and familiarity of time-sensitive emails, including refund notices, payroll forms, filing reminders, and requests from tax professionals, to push malicious attachments, links, or QR codes.

- **Storm-2561 uses SEO poisoning to distribute fake VPN clients for credential theft**

  Storm-2561 uses SEO poisoning to push fake VPN downloads that install signed trojans and steal VPN credentials.

- **AI as tradecraft: How threat actors operationalize AI**

  Threat actors are operationalizing AI to scale and sustain malicious activity, accelerating tradecraft and increasing risk for defenders, as illustrated by recent activity from North Korean groups such as Jasper Sleet and Coral Sleet (formerly Storm-1877).

- **Inside Tycoon2FA: How a leading AiTM phishing kit operated at scale**

  Tycoon2FA has become a leading phishing-as-a-service (PhaaS) platforms, enabling campaigns that reach over 500,000 organizations monthly, prompting Microsoft's Digital Crimes Unit (DCU) to work with Europol and industry partners to facilitate a disruption of Tycoon2FA's infrastructure and operations.

- **Inside RedVDS: How a single virtual desktop provider fueled worldwide cybercriminal operations**

  Microsoft's investigation into RedVDS services and infrastructure uncovered a global network of disparate cybercriminals purchasing and using to target multiple sectors.

- **Phishing actors exploit complex routing and misconfigurations to spoof domains**

  Threat actors are exploiting complex routing scenarios and misconfigured spoof protections to send spoofed phishing emails, crafted to appear as internally sent messages.

- **Defending against the CVE-2025-55182 (React2Shell) vulnerability in React Server Components**

  CVE-2025-55182 (also referred to as React2Shell and includes CVE-2025-66478, which was merged into it) is a critical pre-authentication remote code execution (RCE) vulnerability affecting React Server Components and related frameworks.

- **Shai-Hulud 2.0: Guidance for detecting, investigating, and defending against the supply chain attack**

  The Shai-Hulud 2.0 supply chain attack represents one of the most significant cloud-native ecosystem compromises observed recently.

- **SesameOp: Novel backdoor uses OpenAI Assistants API for command and control**

  Microsoft Incident Response – Detection and Response Team (DART) researchers uncovered a new backdoor that is notable for its novel use of the OpenAI Assistants Application Programming Interface (API) as a mechanism for command-and-control (C2) communications.

- **Inside the attack chain: Threat activity targeting Azure Blob Storage**

  Azure Blob Storage is a high-value target for threat actors due to its critical role in storing and managing massive amounts of unstructured data at scale across diverse workloads and is increasingly targeted through sophisticated attack chains that exploit misconfigurations, exposed credentials, and evolving cloud tactics.

- **Investigating targeted “payroll pirate” attacks affecting US universities**

  Microsoft Threat Intelligence has identified a financially motivated threat actor that we track as Storm-2657 compromising employee accounts to gain unauthorized access to employee profiles and divert salary payments to attacker-controlled accounts, attacks that have been dubbed “payroll pirate”.
