Threat actors | Latest Threats | Microsoft Security Blog

Published: 2026-04-01 · Archived: 2026-04-06 00:48:20 UTC

Microsoft actively discovers and tracks threat actors across observed state-sponsored, ransomware, and criminal activities. Get insights from the 60 nation-state actors, 50 ransomware groups, and hundreds of other attackers we've tracked.

Filtered by

Clear All

- threat-actors

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.

- **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.

- **Investigating active exploitation of CVE-2025-10035 GoAnywhere Managed File Transfer vulnerability**

  Storm-1175, a financially motivated actor known for deploying Medusa ransomware and exploiting public-facing applications for initial access, was observed exploiting the deserialization vulnerability in GoAnywhere MFT's License Servlet, tracked as CVE-2025-10035.

- **Frozen in transit: Secret Blizzard's AiTM campaign against diplomats**

  Microsoft Threat Intelligence has uncovered a cyberespionage campaign by the Russian state actor we track as Secret Blizzard that has been ongoing since at least 2024, targeting embassies in Moscow using an adversary-in-the-middle (AiTM) position to deploy their custom ApolloShadow malware.

- **Disrupting active exploitation of on-premises SharePoint vulnerabilities**

  Microsoft has observed two named Chinese nation-state actors, Linen Typhoon and Violet Typhoon, exploiting vulnerabilities targeting internet-facing SharePoint servers.

- **Protecting customers from Octo Tempest attacks across multiple industries**

  To help protect and inform customers, Microsoft highlights protection coverage across the Microsoft Defender security ecosystem to protect against threat actors like Octo Tempest.

- **Jasper Sleet: North Korean remote IT workers' evolving tactics to infiltrate organizations**

Since 2024, Microsoft Threat Intelligence has observed remote IT workers deployed by North Korea leveraging AI to improve the scale and sophistication of their operations, steal data, and generate revenue for the North Korean government.

- **Defending against evolving identity attack techniques**

  Threat actors continue to develop and leverage various techniques that aim to compromise cloud identities.

- **New Russia-affiliated actor Void Blizzard targets critical sectors for espionage**

  Microsoft Threat Intelligence has discovered a cluster of worldwide cloud abuse activity conducted by a threat actor we track as Void Blizzard, who we assess with high confidence is Russia-affiliated and has been active since at least April 2024.

- **Marbled Dust leverages zero-day in Output Messenger for regional espionage**

  Since April 2024, the threat actor that Microsoft Threat Intelligence tracks as Marbled Dust has been observed exploiting user accounts that have not applied fixes to a zero-day vulnerability (CVE-2025-27920) in the messaging app Output Messenger, a multiplatform chat software.
