# Windows News and Insights | Microsoft Security Blog

Published: 2026-04-01 · Archived: 2026-04-05 23:39:25 UTC

- **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.

- **WhatsApp malware campaign delivers VBScript and MSI backdoors**

  A malware campaign uses WhatsApp messages to deliver VBS scripts that initiate a multi-stage infection chain.

- **Unveiling RIFT: Enhancing Rust malware analysis through pattern matching**

  As threat actors are adopting Rust for malware development, RIFT, an open-source tool, helps reverse engineers analyze Rust malware, solving challenges in the security industry.

- **Cyber Signals Issue 9 | AI-powered deception: Emerging fraud threats and countermeasures**

  Microsoft maintains a continuous effort to protect its platforms and customers from fraud and abuse.

- **Threat actors misuse Node.js to deliver malware and other malicious payloads**

  Since October 2024, Microsoft Defender Experts has observed and helped multiple customers address campaigns leveraging Node.

- **Analyzing open-source bootloaders: Finding vulnerabilities faster with AI**

  Using Microsoft Security Copilot to expedite the discovery process, Microsoft has uncovered several vulnerabilities in multiple open-source bootloaders impacting all operating systems relying on Unified Extensible Firmware Interface (UEFI) Secure Boot.

- **Malvertising campaign leads to info stealers hosted on GitHub**

  Microsoft detected a large-scale malvertising campaign in early December 2024 that impacted nearly one million devices globally.

- **Microsoft’s guidance to help mitigate Kerberoasting _**

  Kerberoasting, a well-known Active Directory (AD) attack vector, enables threat actors to steal credentials and navigate through devices and networks.

- **Chained for attack: OpenVPN vulnerabilities discovered leading to RCE and LPE**

  Microsoft researchers found multiple vulnerabilities in OpenVPN that could lead to an attack chain allowing remote code execution and local privilege escalation.

- **New Windows 11 features strengthen security to address evolving cyberthreat landscape**

  Today, ahead of the Microsoft Build 2024 conference, we announced a new class of Windows computers, Copilot+ PC.

- **New Microsoft Incident Response guide helps simplify cyberthreat investigations**

  Discover how to fortify your organization’s cybersecurity defense with this practical guide on digital forensics from Microsoft’s Incident Response team.

- **Analyzing Forest Blizzard’s custom post-compromise tool for exploiting CVE-2022-38028 to obtain credentials**

  Since 2019, Forest Blizzard has used a custom post-compromise tool to exploit a vulnerability in the Windows Print Spooler service that allows elevated permissions.

---