Microsoft Defender for Cloud Archives | Microsoft Security Blog

Published: 2026-04-01 · Archived: 2026-04-05 22:41:48 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.

- **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).

- **How Microsoft builds privacy and security to work hand-in-hand**

  Learn how Microsoft unites privacy and security through advanced tools and global compliance to protect data and build trust.

- **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.

- **New IDC research highlights a major cloud security shift**

  New IDC research shows why CISOs must move toward AI-powered, integrated platforms like CNAPP, XDR, and SIEM to reduce risk, cut complexity, and strengthen resilience.

- **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.

- **Storm-0501's evolving techniques lead to cloud-based ransomware**

  Financially motivated threat actor Storm-0501 has continuously evolved their campaigns to achieve sharpened focus on cloud-based tactics, techniques, and procedures (TTPs).

- **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.

- **Understanding the threat landscape for Kubernetes and containerized assets**

  The dynamic nature of containers can make it challenging for security teams to detect runtime anomalies or pinpoint the source of a security incident, presenting an opportunity for attackers to stay undetected.

- **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.

- **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.
