Microsoft Defender for Cloud Apps Archives | Microsoft Security Blog

Published: 2026-03-04 · Archived: 2026-04-10 02:36:23 UTC

- **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.

- **New Microsoft Data Security Index report explores secure AI adoption to protect sensitive data**

  The 2026 Microsoft Data Security Index explores one of the most pressing questions facing organizations today: How can we harness the power of generative while safeguarding sensitive data?

- **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.

- **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".

- **Disrupting threats targeting Microsoft Teams**

  Threat actors seek to abuse Microsoft Teams features and capabilities across the attack chain, underscoring the importance for defenders to proactively monitor, detect, and respond effectively.

- **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).

- **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.

- **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.

- **Silk Typhoon targeting IT supply chain**

  Silk Typhoon is a Chinese state actor focused on espionage campaigns targeting a wide range of industries in the US and throughout the world.

- **Securing DeepSeek and other AI systems with Microsoft Security**

  Microsoft Security provides cyberthreat protection, posture management, data security, compliance and governance, and AI safety, to secure AI applications that you build and use.

- **Why security teams rely on Microsoft Defender Experts for XDR for managed detection and response**

  Microsoft Defender Experts for XDR is a mature and proven service that triages, investigates, and responds to incidents and hunts for threats on a customer’s behalf around the clock.

- **Chinese threat actor Storm-0940 uses credentials from password spray attacks from a covert network**

  Since August 2023, Microsoft has observed intrusion activity targeting and successfully stealing credentials from multiple Microsoft customers that is enabled by highly evasive password spray attacks.
