Rewterz Threat Update - Microsoft Warns of Emerging Threat by Storm-0539 Behind Gift Card Frauds - Rewterz

Published: 2023-12-18 · Archived: 2026-04-05 14:33:20 UTC

Severity

High

Analysis Summary

Microsoft recently issued a warning of a rise in malicious activities from a new threat cluster tracked as Storm-0539 for various gift card fraud and theft campaigns using phishing via emails or SMS against retailers during the holiday shopping season. The end goal of these attacks is to distribute malicious links that redirect the targeted users to adversary-in-the-middle (AiTM) phishing pages designed to steal credentials and session tokens.

Once access to an initial session has been obtained, Storm-0539 registers a device under their control for secondary authentication prompts, gaining persistence in the environment, and bypassing multi-factor authentication (MFA) by using the compromised identity. The foothold that is obtained behaves as a conduit used for privilege escalation, lateral movement across the network, and gaining access to cloud resources to harvest sensitive information. They especially target gift card-related services for performing their fraudulent activities.

Storm-0539 is also observed collecting emails, contact lists, and network configurations to launch additional attacks against the same targeted organizations. The adversary is hence described as a financially motivated threat group that has been active since at least 2021. They are known for performing extensive reconnaissance of their victims to craft convincing phishing lures for credential and token theft and gain initial access.

The disclosure comes after Microsoft obtained a court order to seize the infrastructure of a cybercriminal group linked to Vietnam tracked as Storm-1152 that was selling access to almost 750 million compromised Microsoft accounts and identity verification bypass tools. The company also warned about several threat actors exploiting OAuth applications to perform automated cybercrimes for financial gain, like Business Email Compromise (BEC), spam campaigns, phishing, and deploying virtual machines for mining cryptocurrency illegally.

Impact

- Identity Theft
- Credential Theft
- Financial Loss

Remediation

- Always be suspicious about emails sent by unknown senders.

- Never click on links/attachments sent by unknown senders.
- Ensure that general security policies are employed including: implementing strong passwords, correct configurations, and proper administration security policies
- Enable multifactor authentication (MFA).
- Enable conditional access policies to block attacks that use stolen credentials.
- Enable antivirus and anti-malware software and update signature definitions promptly. Using multi-layered protection is necessary to secure vulnerable assets.
