K logix

BE CONFIDENT.

APRIL 2023 | THREAT INTEL NEWSLETTER |

Play Ransomware and DEV-1101

C-Suite level threat review by applicable business area addressing active threats.

Microsoft products are ubiquitous in digital environments, which makes them targets for threat actors. Both adversaries in this report capitalized on this to conduct their nefarious activities. Play ransomware exploited Microsoft Exchange flaws to gain initial access into organization's environments. DEV-1101 built phishing kits that mimic the sign-in pages of Microsoft Office and Outlook.

Play Ransomware:

Play ransomware, first observed in June of 2022, does not appear to target specific industries or geographical locations. Its most recent attacks included victims in government, retail, hospitality, and cloud technology. Victims are in the United States, Europe, Latin America, and Asia. Notably, Play is exploiting Microsoft Exchange flaws in a novel way to compromise organizations.

DEV-1101:

DEV-1101 is a threat actor Microsoft tracks who has been selling adversary-in-the-middle (AiTM) phishing kits since May 2022. The kits automate the process of launching a phishing campaign. Capabilities include detection evasion and mimicking the landing pages of popular services like Microsoft Office and Outlook. These AiTM kits are linked to several widespread phishing campaigns.

Play Ransomware

Threat Level: Medium

Attack:

By leveraging two Microsoft Exchange flaws, CVE-2022-41080 with one of the ProxyNotShell vulnerabilities, CVE-2022-41082, Play achieves remote code execution through Outlook Web Access. Post-initial access, Play utilizes a variety of tools including PsExec for execution, SystemBC Remote Access Trojan for persistence, Mimikatz for privilege escalation and Cobalt Strike for post-exploitation. The threat actor will also make use of standard system tools and packages, which is known as living-off-the-land. Examples include PsExec, WinSCP for data exfiltration (MITRE T1048.003) and the Windows Task manager for credential dumping (MITRE T1048.003). Play employs the double extortion technique.

Remediation:

- Organizations should apply the patch named KB5019758 for Exchange systems to prevent exploitation. More information can be found here. If an organization is unable to apply this patch, it is recommended to disable Outlook Web Access.
- Consider blocking or restricting the use of PsExec within your environment.
- Consider disabling or restricting command-line and scripting tools to make it more difficult for adversaries to escalate privileges and move laterally.

DEV-1101

Threat Level: Medium

Attack:

The way DEV-1101's AiTM phishing kits are used will depend on the threat actor. One notable capability is CAPTCHA checks to evade detection by a security tool. AiTM phishing enables adversaries to bypass many forms of multi-factor authentication (MFA). To do this, the adversary employs a proxy server between the user and the sign-in service. If a user falls for the phish, they are directed to a phishing site that is almost identical to the anticipated sign-in site except for the URL. As the user completes sign-in, the adversary captures the information via a session cookie and steals the user's credentials.

Remediation:

- Implement conditional access policies that examine properties of the sign-in request beyond the accuracy of MFA and the password such as the user's location, device status and sign-in time.
- Consider phishing resistant MFA methods. A widely available option is FIDO/WebAuthn Authentication. An additional option is Public Key Infrastructure (PKI)-based. More information on phishing resistant MFA methods can be found here.
- For high-risk action, consider adding additional authentication methods via a privilege access management (PAM) tool.

Play Ransomware Details:

- **An overview of the new exploit method of Microsoft Exchange flaws:** https://www.crowdstrike.com/blog/owassrf-exploit-analysis-and-recommendations/
- **An overview of Play ransomware's tactics and techniques:** https://explore.avertium.com/resource/an-in-depth-look-at-play-ransomware

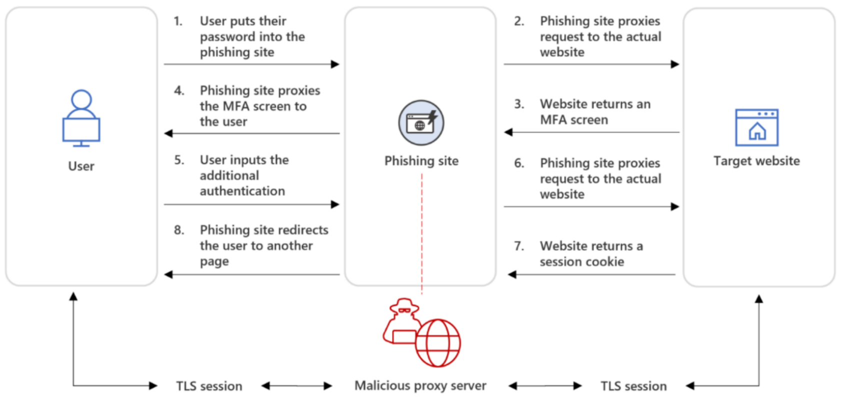
DEV-1101 Details:

- **An explanation of DEV-1101's AiTM phishing kits and its capabilities:** https://www.microsoft.com/en-us/security/blog/2023/03/13/dev-1101-enables-high-volume-aitm-campaigns-with-open-source-phishing-kit/
- **Additional information on the AiTM phishing method:** https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

How K logix Can Help

- Technology Advisory
  - Email Security
  - Endpoint Detection and Protection (EDR)
  - Identity and Access Management (IAM)
  - Managed Security Service Provider (MSSP)
  - Security Information and Event Management (SIEM)
- Programmatic Advisory
  - Advanced Risk Assessment (i.e., HIPAA, NIST, PCI, etc.)
  - Identity and Access Management Program Maturity
  - Penetration testing
  - Tabletop exercises
  - Threat Intelligence Program Maturity

AiTM Phishing Attack Diagram


User
1. User puts their password into the phishing site
4. Phishing site proxies the MFA screen to the user
5. User inputs the additional authentication
8. Phishing site redirects the user to another page
Phishing site
2. Phishing site proxies request to the actual website
3. Website returns an MFA screen
6. Phishing site proxies request to the actual website
7. Website returns a session cookie
Target website
TLS session
Malicious proxy server
TLS session

Source: https://www.microsoft.com/en-us/security/blog/2023/03/13/dev-1101-enables-high-volume-aitm-campaigns-with-open-source-phishing-kit/

ABOUT K LOGIX
Cybersecurity Advisory and Consulting Services
Our white-glove approach empowers leaders to advance their security programs to strategically align with the business to reduce risk.