ARMY CRIMINAL INVESTIGATION DIVISION

10 June 2024

Cybercrime Prevention Flyer

Adversary-In-The-Middle

More internet accessible accounts are using a process known as multifactor authentication (MFA), two-step verification, or dual-factor authentication, making it more difficult for nefarious actors to gain unauthorized access. MFA, providing an added security layer in the authentication process, requires users to verify themselves in more than one way to gain access to an account or system. If a victim's password is compromised, MFA is another mechanism to ensure account access is authentic. Examples of MFA include the use of onetime passwords, QR codes, or authenticator applications.

As organizations increase their reliance on MFA, cybercriminals are implementing more sophisticated techniques to try and gain unauthorized access to victim accounts. The Microsoft Detection and Response Team reported an increase in token theft to circumvent MFA. Token theft involves criminals compromising and replaying security tokens to gain authenticated access to a secure account. An emerging trend to accomplish this is through Adversary-In-The-Middle (AiTM) phishing attacks.

AiTM typically involves a phishing email or text message pretending to be from a trusted source (i.e. a bank, Google, Microsoft). The email or text includes a link to a fictitious webpage mimicking the trusted source webpage (i.e. Microsoft O365 login page). Once a victim provides their username and password, the account credentials are then forwarded to the cybercriminal and automatically used to log in to the legitimate website. If the victim has Multi-Factor Authentication (MFA) enabled, the MFA is also forwarded to the victim as normal. Once the victim completes the MFA, they are logged in to the trusted website as normal. However, the session cookie is provided to the cybercriminal and can be used later to access the legitimate service by impersonating the victim without alerting them via MFA. In these instances, the cybercriminal is acting as a proxy between the victim and legitimate webpage.

Despite these attempts, MFA is recommended as it does increase account security.

Techniques to defend against AiTM:

- Use strong and unique passwords.
- Enable MFA.
- Use biometric logins if available.
- Encrypt your data.
- Be cautious of public Wi-Fi networks.
- Verify the website's authenticity and security by looking for the padlock symbol in the address bar.
- Be aware of phishing attempts and methodologies and report them.
- Keep software and devices up to date.

Department of the Army Criminal Investigation Division: Report a Crime

FBI Internet Crime Complaint Center (IC3): File a Complaint

Federal Trade Commission: Report Fraud

Authorized for widest release, without restrictions.

To receive Cyber Field Office Cybercrime Prevention Flyers, send an email to: CYDIntel@army.mil

CPF 0048-2024-CID221

Cyber Field Office
Russell Knox Building
27130 Telegraph Road
Quantico, VA 22134