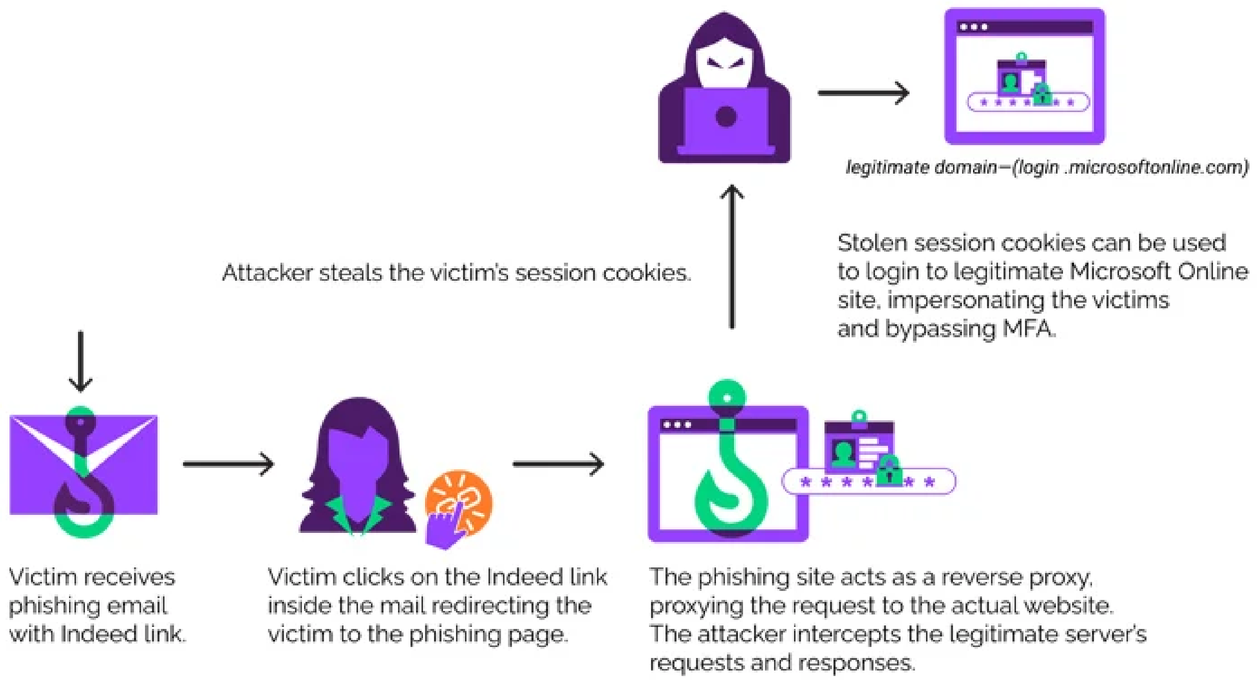
# Cyber Criminals Using EvilProxy Phishing Kit To Target Senior Executives in U.S. Firms

linkedin.com/pulse/cyber-criminals-using-evilproxy-phishing-kit-target-senior-soral/

Shubhi Soral



legitimate domain–(login .microsoftonline.com)

Attacker steals the victim's session cookies.

Stolen session cookies can be used to login to legitimate Microsoft Online site, impersonating the victims and bypassing MFA.

Victim receives phishing email with Indeed link.

Victim clicks on the Indeed link inside the mail redirecting the victim to the phishing page.

The phishing site acts as a reverse proxy, proxying the request to the actual website. The attacker intercepts the legitimate server's requests and responses.

Cybercriminals have launched a phishing campaign targeting senior executives in U.S. firms, using the EvilProxy phishing toolkit for credential harvesting and account takeover attacks. This campaign, initiated in July 2023, primarily targets sectors such as banking, financial services, insurance, property management, real estate, and manufacturing. The attackers exploit an open redirection vulnerability on the job search platform "indeed.com," redirecting victims to malicious phishing pages impersonating Microsoft. EvilProxy functions as a reverse proxy, intercepting credentials, two-factor authentication codes, and session cookies to hijack accounts. The threat actors, known as Storm-0835 by Microsoft, have hundreds of customers who pay monthly fees for their services, making attribution difficult. The attacks involve sending phishing emails with deceptive links to Indeed, redirecting victims to EvilProxy pages for credential harvesting.

How U.S. Firms Can Overcome Such Attacks:

1. Employee Training and Awareness: Conduct regular cybersecurity awareness training to educate employees, especially senior executives, about phishing threats and safe email practices.
2. Email Filtering and Security: Implement advanced email filtering solutions that can detect and block phishing emails before they reach employees' inboxes.

3. Multi-Factor Authentication (MFA): Enforce MFA for accessing sensitive accounts and systems, making it harder for attackers to compromise accounts even if they obtain credentials.
4. Vulnerability Patching: Keep software, websites, and platforms up to date to mitigate open redirection vulnerabilities.
5. Endpoint Security: Deploy robust endpoint protection tools to detect and prevent malicious activities on employees' devices.
6. Incident Response Plan: Develop and regularly update an incident response plan to quickly detect, mitigate, and recover from security incidents like phishing attacks.
7. Threat Intelligence Sharing: Collaborate with industry peers and share threat intelligence to stay informed about emerging threats and tactics used by cybercriminals.
8. Security Awareness Beyond Email: Extend security awareness efforts beyond email to include social engineering attacks like QR code-based phishing.
9. Cloud Security: Enhance cloud security measures to protect against attackers abusing cloud-based infrastructure, as mentioned in the Digital Defense Report.
10. Regular Security Audits: Conduct regular security audits and assessments to identify vulnerabilities and weaknesses in the organization's security posture.

By implementing these measures, U.S. firms can enhance their resilience against phishing attacks and protect senior executives and sensitive corporate information. To know more read this article https://thehackernews.com/2023/10/cybercriminals-using-evilproxy-phishing.html