Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

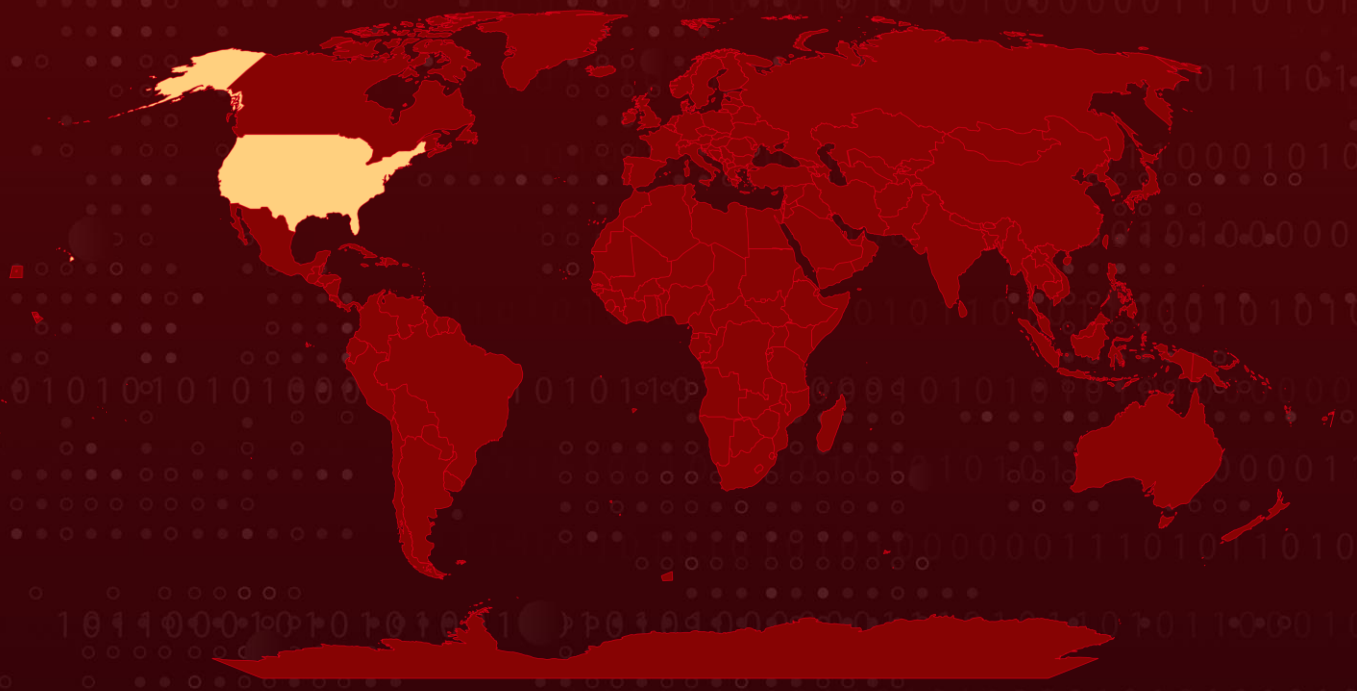
EvilProxy Phishing Attack Targets Indeed Job Platform

Date of Publication	Admiralty Code	TA Number
October 4, 2023	A1	TA2023395

Summary

Attack Began: July 2023
Attack Region: United States
Affected Industries: Banking, Financial services, Insurance providers, Property Management, Real Estate, Manufacturing, Software, Electronic Components Manufacturing, Business Consulting, Accounting, Pharmaceuticals, Healthcare, Construction, Supply Chain Management and Logistics and Insurance Providers
Attack: A new phishing campaign has emerged, specifically targeting high-profile US executives. This campaign takes advantage of open redirects from the jobs platform Indeed and employs EvilProxy to pilfer session cookies. Stolen session cookies bypass all authentication mechanisms, including multi-factor authentication (MFA), potentially granting unauthorized access to attackers.

Attack Regions



Attack Details

#1 In July 2023, a new phishing attack was identified that made use of an open redirection vulnerability in the 'indeed.com' website. This vulnerability redirected victims to a phishing page that impersonated Microsoft. The threat actors behind this attack were observed using a phishing-as-a-service platform called 'EvilProxy' to deploy the phishing pages.

#2 This campaign is specifically aimed at C-suite employees and other key executives within U.S.-based organisations across different industries. The attack began with a phishing email containing a link designed to appear as if it originated from a reputable source, in this case, 'indeed.com.' When the recipient clicked on the link, they were redirected to a counterfeit Microsoft Online login page.

#3 The phishing page used in this campaign is created and managed through the EvilProxy phishing framework. It dynamically fetches all its content from the legitimate Microsoft login site, making it appear convincing to victims. Essentially, the phishing site functions as a reverse proxy, forwarding the victim's login requests to the real Microsoft website while simultaneously capturing their login credentials for malicious purposes.

#4 When a user accesses their account through the phishing server, which convincingly mimics the authentic login page, the threat actor seizes the opportunity to capture the authentication cookies. As users have already completed the necessary multi-factor authentication (MFA) steps during their initial login, the cookies obtained by cybercriminals grant them full access to the victim's account.

#5 The increased adoption of EvilProxy can be attributed to several compelling reasons. It is known for its user-friendly interface, accompanied by easily accessible tutorials and documentation on the dark web. EvilProxy has the significant capability to bypass multi-factor authentication (MFA), which enhances its effectiveness as a valuable tool for cybercriminals. These factors combined make EvilProxy a powerful and attractive asset in the toolkit of malicious actors.

Recommendations

Remain vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Email Security: Enhance email security measures and educate users on recognizing social engineering tactics to mitigate the risk of falling prey to phishing attacks leveraging deceptive file attachments.

Implementing FIDO-based MFA: This approach entails the adoption of FIDO (Fast Identity Online) standards for authentication. It leverages PKI for MFA, significantly raising the difficulty for attackers to intercept authentication credentials.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0006 Credential Access	T1566 Phishing
T1036 Masquerading	T1204 User Execution	T1557 Adversary-in-the-Middle	T1539 Steal Web Session Cookie
T1566.002 Spearphishing Link	T1078 Valid Accounts	T1556 Modify Authentication Process	T1556.006 Multi-Factor Authentication
T1189 Drive-by Compromise	T1090 Proxy		

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	lmo[.]roxylvfuco[.]com[.]au, lmo[.]bartmfil[.]com, lmo[.]triperlid[.]com, roxylvfuco[.]com[.]au, earthscigrovp[.]com[.]au, mscr.earthscigrovp[.]com[.]au, vfuco.com[.]au, catalogsumut[.]com, ivonnesart[.]com, sheridanwyolibrary[.]org
IPv4	199.204.248[.]121, 193.239.85[.]29, 212.224.107[.]74, 206.189.190[.]128, 116.90.49[.]27, 85.187.128[.]19, 202.139.238[.]230

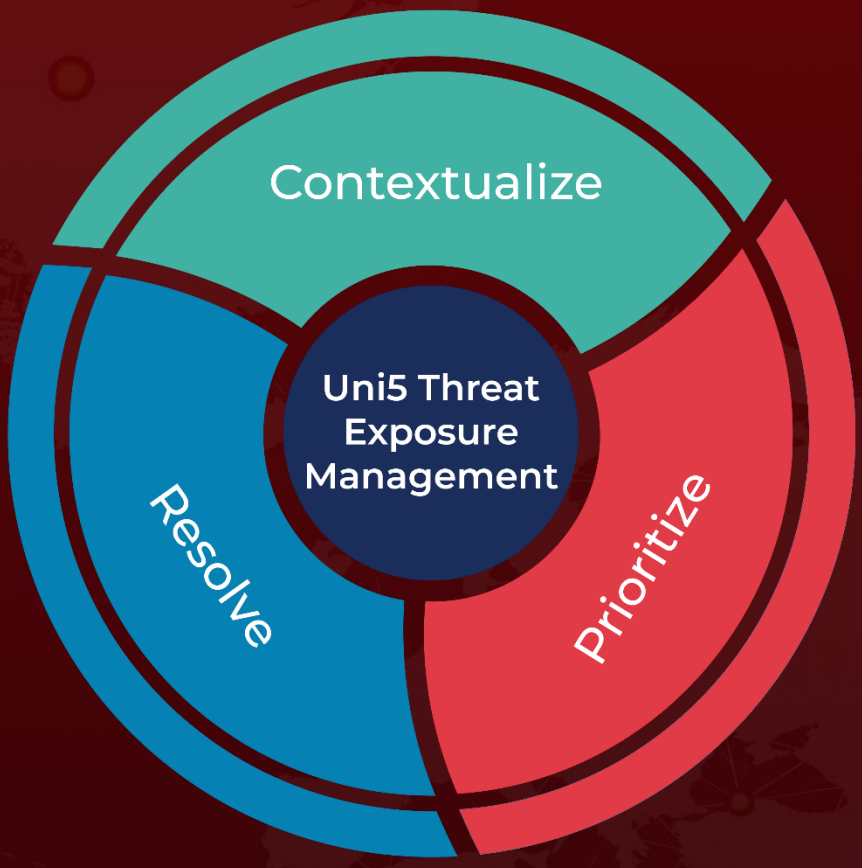
References

https://www.menlosecurity.com/blog/evilproxy-phishing-attack-strikes-indeed/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 4, 2023 . 8:25 AM

More at www.hivepro.com