CIRT.GY Guyana National Computer Incident Response Team

AL2023_63 New phishing campaign utilizes EvilProxy to target Microsoft 365 users (August 22, 2023)

Description

A recent phishing campaign was observed utilizing the EvilProxy phishing tool to hijack Microsoft 365 accounts of high-level personnels at leading companies around the world.

Details

This research was carried out by Proofpoint researchers, who observed a dramatic surge in cloud account takeovers from high-level employees. According to the report, approximately 100 leading organizations were targeted worldwide and affected approximately 1.5 million employees between March and June 2023. The campaign involved threat actors utilizing sophisticated adversary-in-the-middle phishing methods in order to gain access to high-level Microsoft 365 accounts.

The threat actors employed EvilProxy, which is a phishing tool kit that allows attackers to steal multi-factor authentication (MFA) protected credentials and session cookies. This attack framework has been developed and marketed as a MFA Phishing as a Service (PhaaS). It provides attackers with low talent and experience to simply pay for pre-configured kits that can target a variety of online services (such as Gmail, Microsoft, Dropbox, Facebook, Twitter, etc.).

The campaign started with an abundance of phishing emails targeting high-level employees in organizations. The threat actors impersonated trusted services and companies such as Concur Solution, DocuSign and Adobe, sending emails that claimed to be from one of these services. The emails, however, contain a malicious link that redirects to a Microsoft 365 phishing website. Clicking on the malicious link in the email initiates the following multi-stage infection chain:

1. First, user traffic is redirected via an open, legitimate redirector (such as youtube.com or bs.serving-sys.com). The user’s email is encoded in the URL to mask it from automatic scanning tools.

2. Next, user traffic may undergo several more redirections steps, which involve malicious cookies and 404 redirects. This is done to disperse the traffic in an unpredictable way, lowering the likelihood of discovery. Also at this stage, one of the redirections that takes place leads to a legitimate hacked website that contains PHP code from the threat actors that decodes the user email from the URL for the final phishing website.

3. Eventually, user traffic is directed to an EvilProxy phishing framework (in this case the phishing Microsoft 365 login page). The landing page functions as a reverse proxy, mimicking Microsoft 365's branding and attempting to handle third-party identity providers. If needed or enabled, the page may request MFA credentials to facilitate a real, successful authentication on behalf of the victim, thus also validating the gathered credentials as legitimate. The threat actors aim to capture the valid session cookie of this authentication phase.

Once the user provides their credentials on the phishing website, the threat actors can retrieve this and use it along with the stolen session cookie to log in to the now hijacked Microsoft 365 account. The threat actors proceed to secure their foothold on the hijacked account by utilizing 'My Sign-Ins' to add their own multi-factor authentication method, with their preferred method as 'Authenticator App with Notification and Code'.

After successful hijacking of accounts, the threat actors employ various techniques, including lateral movement and malware proliferation. They would study their target organizations' culture, hierarchy, and processes, to prepare their attacks and improve success rates. To monetize their access, the threat actors were seen executing financial fraud, performing data exfiltration or partaking in Hacking-as-a-Service (HaaS) transactions by selling access to compromised user accounts.

Indicators of Compromise

Please see the link for a list of IOCs including domains, IP addresses and email addresses associated with this campaign: https://www.proofpoint.com/us/blog/email-and-cloud-threats/cloud-account-takeover-campaign-leveraging-evilproxy-targets-top-level#:~:text=365%20cloud%20environments.-,IOCs,-Indicator

Remediation

To protect yourself against this campaign, it is recommended to practice proper cyber security hygiene when navigating the internet. Here are some tips to consider:

1. Email Security: Block and monitor malicious email threats targeting your users. Effective BEC-prevention solutions can greatly minimize practical attack surfaces.

2. Cloud Security: Identify account takeover (ATO) and unauthorized access to sensitive resources within your cloud environment. These solutions should provide accurate and timely detection of both the initial account compromise and post-compromise activities, including visibility into abused services and applications. It is also important to have auto-remediation capabilities to reduce attackers’ dwell time and potential damages.
3. Web Security: Isolate potentially malicious sessions initiated by links embedded in email messages.
4. Security Awareness: Educate users to be aware of these risks when using Microsoft 365 and on general phishing and social engineering techniques.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Toulas, B (2023, August 9). *EvilProxy phishing campaign targets 120,000 Microsoft 365 users*. Retrieved from the BleepingComputer. https://www.bleepingcomputer.com/news/security/evilproxy-phishing-campaign-targets-120-000-microsoft-365-users/
- Gritzman, S., Avrham, M., Kromphardt, T., Gionet, Jake., and Bendet, E. (2023, August 9). *Cloud Account Takeover Campaign Leveraging EvilProxy Targets Top-Level Executives at over 100 Global Organizations*. Retrieved from Proofpoint. https://www.proofpoint.com/us/blog/email-and-cloud-threats/cloud-account-takeover-campaign-leveraging-evilproxy-targets-top-level