AL2025_04 Microsoft Advertisers Account Hacked Using Malicious Google Ads (03rd February 2025)

Description

A phishing campaign has been identified, targeting Microsoft advertisers through malicious Google Ads. Attackers are leveraging sponsored search results to impersonate Microsoft's advertising platform, aiming to steal user credentials and bypass two-factor authentication (2FA) measures.

Attack Details

In this campaign, threat actors purchase Google Ads that appear when users search for terms like "Microsoft Ads." These ads redirect users to phishing sites that closely mimic the legitimate Microsoft Ads login page. To evade detection, attackers use advanced techniques such as redirection and cloaking. When unwanted IP addresses, including those from VPNs, bots, or security scanners, attempt to access the malicious ads, they are redirected to harmless "white pages." Meanwhile, genuine users are subjected to a Cloudflare challenge to verify their authenticity before being redirected to the phishing site.

The phishing sites are designed to closely resemble Microsoft's official domain, using deceptive URLs such as ads[.]mcrosoftt[.]com. Upon attempting to log in, victims encounter fake error messages prompting them to reset their passwords. Additionally, the phishing kit is capable of attempting to bypass two-factor authentication (2FA), a common feature in modern phishing campaigns.

To further obfuscate their tactics, attackers employ a unique deception method if users navigate directly to the malicious domain instead of clicking through the ad, they are met with a "rickroll," an internet prank intended to mock visitors. This extra layer of misdirection serves to deter analysis and further disguise the true intent of the phishing campaign.

Indicators of Compromise (IOCs)

The following domains have been identified as associated with this phishing campaign:

- ads[.]mcrosoftt[.]com
- Additional domains sharing similar attributes, including specific favicon and image files, have been identified. Some of these domains were hosted in Brazil or used Brazilian top-level domains (.com.br).

Remediation

To mitigate the risks associated with this phishing campaign, users and organizations are advised to implement the following best practices:

1. **Verify URLs**: Always inspect URLs for inconsistencies or misspellings before entering credentials. Be cautious of domains that closely resemble legitimate ones but contain subtle differences.
2. **Enable Two-Factor Authentication (2FA)**: While 2FA adds an extra layer of security, remain vigilant about unexpected prompts or requests. Use authenticator apps or hardware tokens instead of SMS-based 2FA when possible.
3. **Monitor Accounts Regularly**: Regularly review your advertising and other critical accounts for suspicious activity, such as unauthorized changes or login attempts.
4. **Report Suspicious Ads**: If you encounter fraudulent ads, report them to the platform provider. This helps protect other users and improves overall platform security.
5. **Educate and Train Employees**: Conduct regular cybersecurity awareness training sessions to inform employees about the latest phishing tactics and how to recognize them.
6. **Implement Advanced Email Filtering**: Use advanced email filtering solutions to detect and block phishing emails before they reach end-users.
7. **Stay Informed**: Keep abreast of the latest cybersecurity threats and updates from reputable sources to ensure timely implementation of protective measures.

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

References

1. Kaaviya. (2025, February 3). Microsoft advertisers account hacked using malicious Google ads. Retrieved from *Cyber Security News*. https://cybersecuritynews.com/microsoft-advertisers-account-hacked/
2. Segura, J. (2025, January 30). *Microsoft advertisers phished via malicious Google ads*. Retrieved from Malwarebytes. https://www.malwarebytes.com/blog/news/2025/01/microsoft-advertisers-phished-via-malicious-google-ads