CYBERFORCE

January 17, 2024

DECEMBER 2023 MONTHLY BULLETIN

CyberForceIQ continues to work diligently to detect the latest threats of the cyber landscape. Our monthly bulletin covers the most prominent security incidents of the past month and provides insights into emerging trends and tactics used by threat actors, so you can stay informed.

Key Takeaways

Takeaway 1

Watch for typo-squatting. Typo-squatting is a technique where malicious actors register domain names that are similar to popular websites or brands but contain deliberate typos.

Takeaway 2

APT28 performs lateral movement and changes Outlook mailbox permissions to perform targeted email theft. Perform necessary security updates.

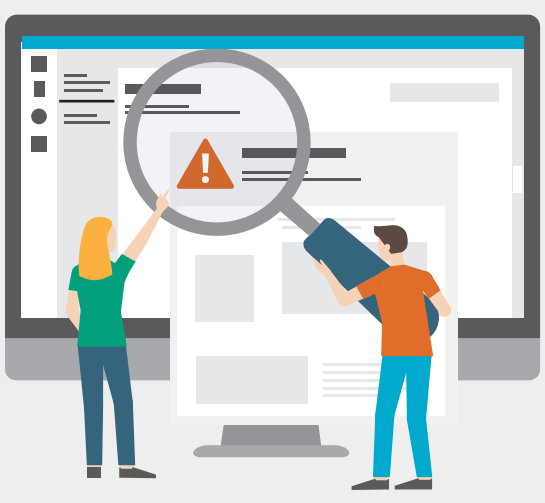
Takeaway 3

Using Web or DNS filtering solutions to block access to known typo-squatted domains can prevent inadvertently visiting fraudulent websites.

Case Study

Growing Trend of Typo-Squatting in Phishing Emails Targets Users for Login Credentials

During December, our team observed a growing trend in the use of typo-squatting in phishing emails. Typo-squatting is a technique where malicious actors register domain names that are similar to popular websites or brands but contain deliberate typos. The goal is to deceive users into visiting these fraudulent websites and providing their login credentials for business services like Microsoft Office 365. Registered domain names can be modified by adding or removing letters, adding hyphens, or using subdomains and top-level domains (TLDs), among other options.



For example, below are typo-squatted domains closely resembling Wells Fargo and Chase Bank:

- wellc-fargo[.]com
- Secure[.]chase-onilne-us[.]com
- secure[.]chase-bakn[.]com

Typically, the emails will prompt the recipient to click a link to view a document related to banking. However, the sender, domain, and domain's server have no affiliation with the actual company. The document, in many cases, serves as a lure to trick the recipient into logging in through a fake login portal. Additionally, the sender may use a service account, such as Google Shares, to send the email. This is done to make the email appear more legitimate and trustworthy to the recipient, while also bypassing standard email security filters.

Steps To Mitigate

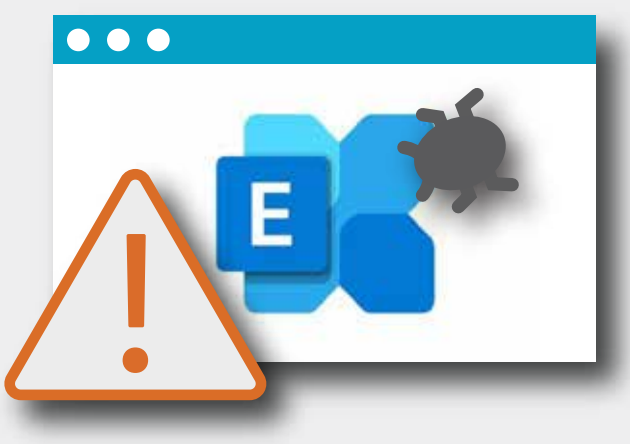
Employee Education: Provide regular training and awareness programs to educate employees about the dangers of typo-squatting and how to identify suspicious domain names.

Domain Blocking: Use web filtering or DNS filtering solutions to block access to known typo-squatted domains. This can prevent employees from inadvertently visiting fraudulent websites.

Two-Factor Authentication (2FA): Enable 2FA for all business services, such as Microsoft Office 365, to add an extra layer of security. Even if employees unknowingly provide their login credentials on a typo-squatted website, 2FA can help reduce the likelihood of unauthorized access.

External Trend

APT28 Exploiting Critical Outlook Flaw to Hijack Microsoft Exchange Accounts



Microsoft's Threat Intelligence team has issued a warning about APT28, a Russian state-sponsored actor, actively exploiting the CVE-2023-23397 Outlook flaw. This vulnerability allows APT28 to hijack Microsoft Exchange accounts and steal sensitive information. The targeted entities include government, energy, transportation, and other key organizations in the United States, Europe, and the Middle East.

CVE-2023-23397 is a critical elevation of privilege (EoP) vulnerability in Outlook on Windows. It was fixed by Microsoft in the March 2023 Patch Tuesday. APT28 has been exploiting this flaw since April 2022 using specially crafted Outlook notes to steal NTLM hashes. By elevating their privileges on the system, APT28 performs lateral movement and changes Outlook mailbox permissions to perform targeted email theft. Despite security updates and mitigation recommendations, the attack surface remains significant, and a subsequent fix (CVE-2023-29324) in May has worsened the situation.

Steps To Mitigate

Apply the available security updates for CVE-2023-23397 and its bypass CVE-2023-29324.

Limit SMB traffic by blocking connections to ports 135 and 445 from all inbound IP addresses.

Disable NTLM in your environment.

Reset passwords of compromised users and enable MFA (multi-factor authentication) for all users.

How CyberForceIQ Can Help

For over 27 years, CyberForceIQ has been a trusted name in advancing cybersecurity programs. Our expertise lies in designing and executing measurable cybersecurity strategies tailored to organizations of all sizes. With a track record of proven results, we offer services such as customized security assessments, robust security operations centers, and comprehensive strategic guidance. Let us assist your organization in prioritizing its goals, elevating your cybersecurity capabilities, and providing meaningful measurements of progress. Our participants are innovative leaders who share optimal strategies to implement and advance a proven cybersecurity program. Together, we are protecting the cyber realm.

Contact Us For More Information

248-837-1400 • solutions@cyberforceq.com

CYBERFORCE