CYBERFORCE

May 17, 2023

TLP: Clear - Unlimited disclosure, this information can be shared publicly with everyone.

APRIL 2023 MONTHLY BULLETIN

CyberForce|Q continues to work diligently to detect the latest threats of the cyber landscape. Cyber criminals work around the clock to steal your personal information. At CyberForce|Q we work to stay ahead of the cyber criminals. 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.

01 Executive Summary

Our collaborative and information sharing efforts have grown stronger, despite the threat landscape remaining consistent. This is beneficial for our participants as it allows them to access a wider range of expertise and resources, which can enhance their ability to detect and respond to potential cyber incidents, thereby improving their overall security posture.

By staying informed, we help our participants stay ahead of threats and keep their sensitive information and systems secure. In these monthly bulletins, we cover the most prominent security incidents of the past month and provide insights into emerging trends and tactics used by threat actors.

02 Case Study

Office 365 - Most Abused Branding in Phishing and Credential Harvesting Emails

Microsoft Office 365 is a subscription-based online suite of services offered by Microsoft, designed for enterprise organizations. It includes Office applications (Word, Excel, PowerPoint, etc.), email services with Exchange Online, online storage with OneDrive for business, and collaboration tools with SharePoint and Teams. However, Office 365 brand impersonation is also attractive to cyber criminals because it is a widely used platform and many people are familiar with it. This makes it easier to create realistic-looking phishing emails and websites that trick users into giving away their login credentials or other sensitive information. Additionaly, because Office 365 is often used business purposes, successful phishing attacks can result in access to sensitive company data, financial information, and more.

While our SOC receives a variety of suspicious email submissions from users for analysis, Office 365 is the most commonly impersonated brand in emails attempting to steal a user's domain login information. The risk associated with a threat actor gaining initial access into a domain network is significant, as it allows for extensive opportunities for internal information gathering, data theft, and other unwanted activities that could additionally be used as a precursor to operational disruption.

Steps to Mitigate Risk

- Educate employees on how to identify and avoid phishing attempts.
- Implement phish-resistant multi-factor authentication (MFA) on all employee accounts.
- Use an up-to-date endpoint detection and response (EDR) solution and our 24/7 monitoring service to promptly identify and stop suspicious user device activity.
- Have a thorough incident response plan in place to minimize the impact of a successful compromise.

03 External Trend Spotlight

Tax-themed Phishing and Malware Attacks Targeting Organizations and Individuals During Tax Filing Season

Cybercriminals are targeting victims during tax season with a variety of phishing and malware attacks. Various campaigns include scammers sending emails claiming to be from the IRS to deliver the Emotet trojan, a hacker group known as TACTICAL#OCTOPUS relying on valid employee W-2 tax documents, I-9 forms, and real estate purchase contracts to download malware onto victims' systems among others.

The IRS issued an advisory urging taxpayers to be cautious and vigilant of new tax-related scams. The agency emphasizes that it never requests personal details from users via email or phone. Additionally, it recommends using strong passwords and forwarding suspicious emials to the IRS to stay safe from phishing attacks.

Contact Us for More Info: 248-837-1400 solutions@cyberforceq.com