CERT-PH Cybersecurity Threat Feeds

Issue Date	January 04, 2021
TLP: GREEN	

Summary

The latest cyber threat topics gathered from the web and analyzed by the CERT-PH research team over the last 24 hours that may impact the Philippine government and cyberspace:

- Hackers Phish 615,000 Login Credentials by using Facebook Ads
- CISA Releases Azure, Microsoft 365 Malicious Activity Detection Tool

- CRITICAL
- URGENT
- IMPORTANT

Description

Hackers Phish 615,000 Login Credentials by using Facebook Ads

2020.12.28 | Source(s): HackRead

Analysis:

A phishing campaign was discovered that uses Facebook ads and redirecting users to Github, where the actual phishing pages resided. The phishing campaign is executed via Facebook ads posted from pages that impersonates legitimate companies in order to avoid user suspicion. Once clicked, users are directed to GitHub page that masquerade as a legitimate Facebook login page. Facebook users from a number of countries including Egypt, the Philippines, Pakistan, and Nepal are targeted by the campaign.

Read more:

[https://www.hackread.com/hackers-phish-login-credentials-with-facebook-ads/?web_view=true]

CISA Releases Azure, Microsoft 365 Malicious Activity Detection Tool

2020.12.28 | Source(s): Bleeping Computer

Analysis:

The Cybersecurity and Infrastructure Security Agency (CISA) has released a PowerShell-based tool that helps detect potentially compromised applications and accounts in Azure/Microsoft 365 environments. Dubbed as Sparrow, the PowerShell-based tool can be used to narrow down larger sets of investigation modules and telemetry to those specific to recent attacks on federated identity sources and applications. checks the unified Azure/M365 audit log for indicators of compromise (IoCs), lists Azure AD domains, and checks Azure service principals and their Microsoft Graph API permissions to discover potential malicious activity.

Read more:

[https://www.bleepingcomputer.com/news/security/cisa-releases-azure-microsoft-365-malicious-activity-detection-tool/?&web_view=true]

CERT-PH Recommendations:

o Users are advised to be cautious and always check the authenticity of the website before giving any private information or login credentials. Phishing attacks often use multiple redirects and unsecure connections before landing on the attacker's controlled website. If unsure of the website visited and causes to raise red flags, immediately put the website in your browser's list of locked webpages.

o Agencies must protect their assets and perimeter by minimizing the point of entry that an unwanted attacker might take. Thus, actions must be taken such as:

- Closing misconfigured and/or unused ports that are accessible in the public internet.
- Regularly monitoring and patching of systems, software application, and devices.
- Educating employees regarding cyber hygiene and cybersecurity best practices.