CERT-PH Cybersecurity Threat Feeds

Issue Date	May 10, 2021
TLP: White	

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:

- APT29 Group Changes Tactics Techniques and Procedures (TTPs)
- Qualcomm Chip Bug Opens Android to Eavesdropping
- Microsoft Warns of a Large-scale BEC Campaign

- ● CRITICAL
- ● URGENT
- ● INFORMATION

Description

APT29 Group Changes Tactics Techniques and Procedures (TTPs)

2021.05.07 | Source(s): Security Affairs

Analysis:

The UK and US cybersecurity agencies have published a report detailing techniques used by a Russia-linked cyberespionage group. Dubbed as APT29, the group's campaigns are aimed at organizations involved in COVID-19 vaccine development throughout 2020 using WellMess and WellMail malware. According to security experts, the group's tactics include the deployment of the open-source tool Sliver to gain persistence on the compromised infrastructure and the use of multiple vulnerabilities, including Microsoft Exchange ProxyLogon vulnerability CVE-2021-26855. APT29 targets organizations that align with Russian foreign intelligence interests. The list of targets includes governmental, think-tank, policy and energy targets, and organizations involved in the development of the COVID19 vaccine.

Read more:

[https://securityaffairs[.]co/wordpress/117667/apt/apt29-changes-ttps.html]

Qualcomm Chip Bug Opens Android to Eavesdropping

2021.05.06 | Source(s): Threatpost

Analysis:

Cybersecurity experts discovered a vulnerability in a 5G modem data service could allow mobile hackers to remotely target Android users by injecting malicious code into a phone's modem, gaining the ability to execute code, access mobile users' call histories and text messages, and eavesdrop on phone calls. Tracked as CVE-2020-11292, the flaw is a heap overflow vulnerability that exists in the Qualcomm Mobile Station Modem (MSM) Interface, also known as QMI. According to researchers, as an attack vector, attackers can exploit the bug to attack a mobile device remotely, via a malicious or trojanized Android application.

Read more:

[https://threatpost[.]com/qualcomm-chip-bug-android-eavesdropping/165934/]

Microsoft Warns of a Large-scale BEC Campaign

2021.05.08 | Source(s): Security Affairs

Analysis:

Microsoft is warning of a large-scale business email compromise (BEC) campaign that targeted hundreds of organizations leveraging typo-squatted domains registered days before the attacks. The attackers targeted organizations in multiple industries, including the consumer goods, process manufacturing and agriculture, real estate, discrete manufacturing, and professional services sectors. The threat actors leverage typo-squatted domains to trick the recipients into believing that the emails were originating from valid senders. The emails, that pretend to be sent by managers of employees working in various organizations, requesting to purchase gift cards to give to the team as an incentive for their hard work during the pandemic. Moreover, attackers show high reconnaissance skills that were used to gather intelligence on the targets and target the right employees within the organizations. Attackers are also faking the In-Reply-To and References headers to add an extra air of legitimacy to the email.

Read more:
[https://securityaffairs[.]co/wordpress/117672/cyber-crime/bec-gift-card-scam.html]

CERT-PH Recommendations:

- 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.
- 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.

Critical	*The information stated is deemed to be crucial to organizations and can significantly shift security concerns and issues based on following events.*
Urgent	*The information stated needs to be addressed timely, which may require immediate attention and/or prompt action.*
Information	*The information stated is good to know knowledge that provides awareness and understanding to the topic.*