CERT-PH Cybersecurity Threat Feeds

Issue Date	January 15, 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:

• Telegram-based Phishing Service Classiscam • Facebook Sues Makers of Malicious Chrome Extensions for Scraping Data • Verified Twitter Accounts Hacked In $580k 'Elon Musk' Crypto Scam • Denial of Service Vulnerability in F5 BIG-IP Systems	• CRITICAL • URGENT • INFORMATION

Description

Telegram-based Phishing Service Classiscam

2021.01.14 | Source(s): Bleeping Computer

Analysis:

At least 40 cybercriminal gangs are using a scam-as-a-service that relies on Telegram bots, tracked as Classiscam, to provide pages that impersonate popular classifieds, marketplaces, and delivery services to lure interested users to fraudulent merchant sites or to phishing pages that steal payment data. Note that the scammers can pose as both sellers and buyers. When pretending to be a customer, they send a fake payment form obtained from a Telegram bot that impersonates a marketplace. The seller then gets a fake form asking for card details in order to receive the alleged payment.

Read more:

[https://securityaffairs[.]co/wordpress/113404/cyber-crime/criminal-scheme-classiscam.html]
[https://threatpost[.]com/telegram-bots-classiscam-scam/163061/]
[https://www.bleepingcomputer[.]com/news/security/telegram-based-phishing-service-classiscam-hits-european-marketplaces/]

Facebook Sues Makers of Malicious Chrome Extensions for Scraping Data

2021.01.14 | Source(s): Bleeping Computer

Analysis:

Facebook has taken legal action against the makers of malicious Chrome extensions used for scraping user-profiles and other information from Facebook's website and from users' systems without authorization. The two defendants developed and distributed the malicious browser extensions through the Chrome Web Store working under the "Oink and Stuff" business name. After being installed on the users' computers, these Chrome extensions also installed malicious code in the background which allowed the defendants to scrape user data from Facebook's site including the victims' name, user ID, gender, relationship status, and age group among others.

Read more:

[https://threatpost[.]com/facebook-malicious-chrome-extension-developers-scraped-profile-data/163079/]
[https://www.bleepingcomputer[.]com/news/security/facebook-sues-makers-of-malicious-chrome-extensions-for-scraping-data/]

Verified Twitter Accounts Hacked in $580k 'Elon Musk' Crypto Scam

2021.01.14 | Source(s): Bleeping Computer

Analysis:

Threat actors are hacking verified Twitter accounts in an Elon Musk cryptocurrency giveaway scam that has recently become widely active. The tweets will contain links that redirect to Medium article promoting the fake giveaway. The articles contain further links to the scam landing pages that state if you send bitcoins to the listed address, they will send you back twice the amount. The threat actors have earned $587,000 in Bitcoin and $2700 in Etherium.

Read more:
[https://www.bleepingcomputer[.]com/news/security/verified-twitter-accounts-hacked-in-580k-elon-musk-crypto-scam/]

Denial of Service Vulnerability in F5 BIG-IP Systems

2021.01.14 | Source(s): Security Affairs

Analysis:

Security researchers discovered a flaw in the F5 BIG-IP product that can be exploited to conduct denial-of-service (DoS) attacks. Tracked as CVE-2020-27716, is a vulnerability that resides in the Traffic Management Microkernel (TMM) component which processes all load-balanced traffic on BIG-IP devices and that affects certain versions of F5 BIG-IP Access Policy Manager (APM). An attacker could trigger the flaw by simply sending a specially crafted HTTP request to the server hosting the BIG-IP configuration utility, and that would be enough to block access to the controller for a while, until it automatically restarts.

Read more:
[https://securityaffairs[.]co/wordpress/113440/security/f5-big-ip-dos.html]

CERT-PH Recommendations:

o Trust only official websites. Before entering your login details and payment information, double check the URL and Google it to see when it was created. If the site is only a couple of months old, it is highly likely to be a scam or a phishing page.

o Whenever purchasing online, keep the conversation on the official platform that intermediates the transaction so that it can serve as evidence in case of a fraud attempt.

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 Users are urged to check their browser extensions and immediately remove the following extensions:

- **Web for Instagram plus DM**
- **Blue Messenger**
- **Emoji keyboard**
- **Green Messenger**

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.