CERT-PH Cybersecurity Threat Feeds

Issue Date	March 17, 2021
TLP: White	

s

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:

- DuckDuckGo Browser Extension Vulnerability Leaves Edge Users Open to Potential Cyber-snooping
- Twitter Users Can Now Secure Accounts with Multiple Security Keys
- Hackers Hide Credit Card Data from Compromised Stores in JPG File
- ZHtrap Botnet Deploys Honeypots to Trap&Steal Bots From Rivals

- CRITICAL
- URGENT
- INFORMATION

Description

DuckDuckGo Browser Extension Vulnerability Leaves Edge Users Open to Potential Cyber-snooping

2021.03.16 | Source(s): The Daily Swig

Analysis:

DuckDuckGo fixed a universal cross-site scripting (uXSS) flaw in a popular browser extension for Chrome and Firefox. The vulnerability resides in the DuckDuckGO Privacy Essentials which blocks hidden trackers and offers private browsing features. The flaw could allow threat actors to spy on all websites that the user is visiting, leaving sensitive information and data accessible. It also allows attackers to manipulate displayed information, take over accounts and impersonate the user.

Read more:

[https://portswigger[.]net/daily-swig/duckduckgo-browser-extension-vulnerability-leaves-edge-users-open-to-potential-cyber-snooping]

Twitter Users Can Now Secure Accounts with Multiple Security Keys

2021.03.16 | Source(s): Security Week

Analysis:

The social media platform Twitter announced that users with two-factor authentication (2FA) enabled can now use multiple security keys on both mobile devices and desktop to protect their accounts. In addition, the latest version of a supported browser such as Chrome, Edge, Firefox, Opera and Safari, is needed to add or log in to a Twitter account with a security key.

Read more:

[https://www.securityweek[.]com/twitter-users-can-now-secure-accounts-multiple-security-keys]

Hackers Hide Credit Card Data from Compromised Stores in JPG File

2021.03.16 | Source(s): Bleeping Computer

Analysis:

Cybersecurity experts discovered that hackers come up with a sneaky method to steal payment card data from compromised online stores that reduces the suspicious traffic footprint and helps them evade detection. Instead of sending the card details to a server that they control, hackers conceal it in a JPG image and store it on the infected website. Dubbed as Magecart, these attacks begin when cybercriminals gaining access to an online store through a vulnerability or weakness plant malicious code designed to steal customer card data at checkout. The malicious PHP file crafted by these cybercriminals allows them to load additional malicious code by creating and calling the getAuthenticates function. It then creates a JPG image that would be used to store payment card data from customers in encoded form which can easily be downloaded by the attackers as a JPG file without triggering any alarms in the process.

Read more:

[https://www.bleepingcomputer[.]com/news/security/hackers-hide-credit-card-data-from-compromised-stores-in-jpg-file]
[https://securityaffairs[.]co/wordpress/115600/security/google-chrome-0-day.html]
[https://threatpost[.]com/google-mac-windows-chrome-zero-day/164759/]

ZHtrap Botnet Deploys Honeypots to Trap&Steal Bots from Rivals

2021.03.15 | Source(s): TheRecord

Analysis:

Cybersecurity experts discovered a new IoT botnet that deploys honeypots to capture attacks from rival botnets and then uses that information to hijack its rivals' infrastructure. Dubbed as ZHtrap, the new botnet was built on an improved version of Mirai IoT malware that was used to turn networked devices into remotely controlled bots that can be used as part of a botnet in large-scale network attacks such as DDoS. The botnet works by exploiting vulnerabilities to infect DVRs, CCTV cameras, Netgear routers and Realtek-based devices. According to researchers, on some infected devices, ZHtrap installed honeypots to collect the IP addresses belonging to the scan&exploit bots operated by rival botnet gangs. Moreover, the botnet will also install a reverse web shell on all infected devices, perform Telnet scans and even download and execute other payloads, which implies that the botnet could pivot to an access-as-a-service system and allow third-parties to launch attacks on enterprise networks via the infected devices.

Read more:
[https://therecord.media/zhtrap-botnet-deploys-honeypots-to-trapsteal-bots-from-rivals]

CERT-PH Recommendations:

- Website administrators are highly advised to facilitate integrity control checks to monitor websites and detect changes such as code modifications or new files being added to their sites.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **Google Chrome** - version 2021.2.3 or later
  - **DuckDuckGo Privacy Essentials** - latest version
- 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.*