CERT-PH Cybersecurity Threat Feeds

Issue Date	April 28, 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:

- Linux Kernel Bug Opens Door to Wider Cyberattacks
- Apple AirDrop Bug Could Leak Personal Info to Anyone Nearby
- Dridex Malware Returns In a New Global QuickBooks Malspam Campaign
- 3.2 Billion Leaked Passwords Contain 1.5 Million Records with Government Emails

- CRITICAL
- URGENT
- INFORMATION

Description

Linux Kernel Bug Opens Door to Wider Cyberattacks

2021.04.27 | Source(s): Threatpost

Analysis:

An information-disclosure security vulnerability has been discovered in the Linux kernel, which can be exploited to expose information in the kernel stack memory of vulnerable devices. Tracked as CVE-2020-28588, the flaw exists in the /proc/pid/syscall functionality of 32-bit ARM devices running Linux and is due to an improper conversion of numeric values when reading the file. According to security experts, attackers can output 24 bytes of uninitialized stack memory, which can be used to bypass kernel address space layout randomization (KASLR). KASLR is an anti-exploit technique that places various objects at random to prevent predictable patterns that are guessable by adversaries. Moreover, if utilized correctly, an attacker could leverage this information leak to successfully exploit additional unpatched Linux vulnerabilities.

Read more:

[https://threatpost[.]com/linux-kernel-bug-wider-cyberattacks/165640/]

Apple AirDrop Bug Could Leak Personal Info to Anyone Nearby

2021.04.26 | Source(s): The Hacker News, Security Affairs

Analysis:

Cybersecurity experts discovered a privacy issue in Apple's wireless file-sharing protocol Apple AirDrop that could expose user's contact information, such as email addresses and phone numbers. AirDrop is a proprietary ad hoc service present in Apple's iOS and macOS operating systems, allowing users to transfer files between devices by making use of close-range wireless communication. According to security researchers, the flaw can be exploited by attackers to learn contact identifiers, such as phone numbers and email addresses, of nearby AirDrop senders and receivers. In addition, the flaws originate from the exchange of hash values of such contact identifiers during the discovery process, which can be easily reversed by attackers via brute-force or dictionary attacks.

Read more:

[https://thehackernews[.]com/2021/04/apple-airdrop-bug-could-leak-your.html]
[https://securityaffairs[.]co/wordpress/117250/hacking/apple-airdrop-bug.html]

Dridex Malware Returns in a New Global QuickBooks Malspam Campaign

2021.04.26 | Source(s): Hot for Security

Analysis:

Security experts detected an ongoing phishing attacks masquerading as QuickBooks invoices are targeting users of the popular accounting software in an attempt to infect victim's devices with a banking trojan. According to the experts, the Intuit-themed malspam campaign reels in QuickBooks users with fake payment notifications and invoices. More than half of the spoofed emails originate

from IP addresses in Italy. The perps have forged the header ('quickbooks@xxxx.intuit.com'), making it seem like the messages are genuine. To avoid multiple detection tools, threat actors play with the subject lines and sender names. Attackers also tailored the emails' body in an attempt to sneak past anti-phishing and anti-spam mechanisms. The emails contain a seemingly harmless Microsoft Excel Spreadsheet attachment carrying a hidden threat. A malicious macro within the .xls file will launch a Trojan dropper infecting the victim's machine. Dubbed as Dridex, the banking Trojan, commonly delivered via phishing emails containing malicious Microsoft Word and Excel documents. This malicious software steals confidential information from victims, including banking credentials that threat actors can use to access bank accounts and make fraudulent transactions.

Read more:

[https://hotforsecurity.bitdefender[.]com/blog/dridex-malware-returns-in-a-new-global-quickbooks-malspam-campaign-25715.html]

3.2 Billion Leaked Passwords Contain 1.5 Million Records with Government Emails

2021.04.26 | Source(s): The Hacker News

Analysis:

Cybersecurity experts discovered a leak of 3.28 billion passwords linked to 2.18 billion unique email addresses were exposed in what's one of the largest data dumps of breached usernames and passwords.he leak includes 1,502,909 passwords associated with email addresses from government domains across the world, with the U.S. government alone taking up 625,505 of the exposed passwords, followed by the U.K (205,099), Australia (136,025), Brazil (68,535), and Canada (50,726). Dubbed as COMB21, also known as Compilation of Many Breaches, the massive 100GB data was published for free in an online cybercrime forum by putting together data from multiple leaks in different companies and organizations that occurred over the years. According to security experts, the passwords are said to have been obtained via techniques such as password hash cracking after being stolen or through phishing attacks and eavesdropping on insecure, plaintext connections.

Read more:

[https://thehackernews[.]com/2021/04/32-billion-leaked-passwords-contain-15.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.
- Apple users can protect themselves by disabling AirDrop discovery in the system settings and by refraining from opening the sharing menu.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **Linux Kernel** - versions 5.10-rc4, 5.4.66 and 5.9.8
- 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.*