CERT-PH Cybersecurity Threat Feeds

Issue Date	March 02, 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:

- Beware: AOL Phishing Email States your Account will be Closed
- Gootkit Delivery Platform Gootloader Used to Deliver Additional Payloads
- Critical Authentication Bypass Flaw Found in Rockwell Automation Software
- T-Mobile Customers Were Hit with SIM Swapping Attacks

- CRITICAL
- URGENT
- INFORMATION

Description

Beware: AOL Phishing Email States your Account will be Closed

2021.02.28 | Source(s): Bleeping Computer

Analysis:

Cybersecurity experts observed an AOL mail phishing campaign that steals users' login name and password by warning recipients that their account is about to be closed. The email stated that they need to login and verify their account within 72 hours, or AOL will deactivate their account. Enclosed in the email was a link to a poorly constructed AOL phishing landing page that asked visitors to log in to AOL. Once AOL credentials are submitted on the form, the stolen credentials are sent to the attackers, and the user is redirected to the standard AOL login page.

Read more:

[https://www.bleepingcomputer[.]com/news/security/beware-aol-phishing-email-states-your-account-will-be-closed/]

Gootkit Delivery Platform Gootloader Used to Deliver Additional Payloads

2021.02.28 | Source(s): Bleeping Computer

Analysis:

Cybersecurity researchers discovered that the Javascript-based infection framework for the Gootkit RAT was enhanced to deliver a wider variety of malware, including ransomware. The Gootkit delivery platform was used by multiple threat actors to deliver ransomware and other malware, including the REvil ransomware, the Kronos trojan, and Cobalt Strike. Recently Gootloader attempted to evade detection and has started using "fileless" methodology. The framework uses black search engine optimization (SEO) techniques to poison Google search results and spread links pointing to the malware. When the visitor clicks on the link provided by the search engine, they are redirected to landing pages that answer their exact questions, using the same wording as the search query. Gootloader infection process is multi-stage, it begins with a .NET loader, which comprises a Delphi-based loader malware, which, in turn, contains the final payload in encrypted form.

Read more:

[https://securityaffairs[.]co/wordpress/115144/cyber-crime/gootkit-gootloader-evolution.html]

Critical Authentication Bypass Flaw Found in Rockwell Automation Software

2021.02.27 | Source(s): Security Affairs

Analysis:

Tracked as CVE-2021-22681, is a critical authentication bypass vulnerability that can be exploited by remote attackers to compromise programmable logic controllers (PLCs) manufactured by Rockwell Automation. The flaw received a CVSS score of 10 and affects multiple Rockwell Logix controllers. The vulnerability exists in the Logix Designer software that uses a poorly protected private cryptographic key to verify communications with controllers. The secret keys are used to digitally sign all communication

with the Rockwell PLCs, then PLCs verify the signature and authenticate the company engineering software. An attacker that obtained the key impersonates the engineering software and controls the PLC.
Read more:
[https://securityaffairs[.]co/wordpress/115085/ics-scada/rockwell-automation-software-flaw.html]

T-Mobile Customers Were Hit with SIM Swapping Attacks

2021.02.27 | Source(s): Security Affairs

Analysis:

The telecommunications provider T-Mobile has disclosed a data breach after it became aware that some of its customers were allegedly victims of SIM swap attacks. Crooks conduct SIM swapping attacks to take control of victims' phone numbers tricking the mobile operator employees into porting them to SIMs under the control of the fraudsters. Once hijacked a SIM, the attackers can steal money, cryptocurrencies and personal information, including contacts synced with online accounts. The criminals could hijack social media accounts and bypass 2FA services based on SMS used by online services, including financial ones. An unknown attacker gained access to customers' account information, including personal info and personal identification numbers (PINs), T-Mobile already notified the impacted customers.
Read more:
[https://securityaffairs[.]co/wordpress/115068/data-breach/t-mobile-sim-swapping.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.
- Impacted T-Mobile customers are recommended to change their password, PIN, and security questions.
- 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.*