CERT-PH Cybersecurity Threat Feeds

Issue Date	March 18, 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:

- China-linked Hackers Target Telcos to Steal 5g Secrets
- Cisco Plugs Security Hole in Small Business Routers
- Phishing Sites Now Detect Virtual Machines to Bypass Detection
- Microsoft Releases One-click Exchange On-premises Mitigation Tool

- ● CRITICAL
- ● URGENT
- ● INFORMATION

Description

China-linked Hackers Target Telcos to Steal 5g Secrets

2021.03.17 | Source(s): Security Affairs, Threatpost

Analysis:

Cybersecurity experts discovered that Chinese APT groups are targeting telecom companies. Collectively tracked as Operation Diànxùn, the cyberespionage campaign aims to steal sensitive data and trade secrets tied to 5G technology. Hackers are targeting people working in the telecom industry by luring them to fake websites designed to mimic tele-giant's Huawei career page. According to researchers, the tactics, techniques and procedures (TTPs) used in the campaign are compatible with the operations associated with ChineseRedDelta and Mustang Panda cyberespionage groups. Attackers used a .NET payload as a second-stage malware that was delivered tricking the victims into executing Flash-based artifacts malware and in the final stage, they deployed a backdoor to take over the victim's system.

Read more:

[https://securityaffairs[.]co/wordpress/115693/apt/chinese-hackers-5g.html]
[https://threatpost[.]com/state-sponsored-threat-groups-target-telcos-steal-5g-secrets/164841/]

Cisco Plugs Security Hole in Small Business Routers

2021.03.17 | Source(s): Bleeping Computer

Analysis:

Cisco issued fixes for security vulnerability that affects some of their routers. Tracked as CVE-2021-1287, the flaw results from an issue in the routers' web-based management interface and affects Cisco's RV132W ADSL2+ Wireless-N VPN routers and RV134W VDSL2 Wireless-AC VPN routers. Successful exploitation of the vulnerability could allow an attacker to execute arbitrary code as the root user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition on the affected device. The flaw received a CVSS score of 7.2 out of 10 making it high severity.

Read more:

[https://threatpost[.]com/cisco-security-hole-small-business-routers/164859/]

Phishing Sites Now Detect Virtual Machines to Bypass Detection

2021.03.15 | Source(s): Bleeping Computer

Analysis:

Cybersecurity experts discovered that phishing sites are now using JavaScript to evade detection by checking whether a visitor is browsing the site from a virtual machine or headless device. To bypass detection, a phishing kit utilizes JavaScript to check whether a browser is running under a virtual machine or without an attached monitor. The script checks the visitor's screen's width and height and uses the WebGLAPI to query the rendering engine used by the browser. If it discovers any signs of analysis attempts, it shows a blank page instead of displaying the phishing page.

Read more:

[https://www.bleepingcomputer[.]com/news/security/phishing-sites-now-detect-virtual-machines-to-bypass-detection/]

Microsoft Releases One-click Exchange On-premises Mitigation Tool

2021.03.16 | Source(s): Bleeping Computer, Security Affairs

Analysis:

Microsoft has released an Exchange On-premises Mitigation Tool (EOMT) tool to allow small businesses to quickly address the vulnerabilities exploited in the recent attacks. The EOMT tool is a one-click PowerShell script that allows organizations that do not have dedicated security or IT teams to apply the security updates to address the CVE-2021-26855 flaw that can be exploited for remote code execution. However, the company pointed out that the EOMT tool is not a replacement for the Exchange security update. According to experts, the Exchange On-premises Mitigation Tool runs the Microsoft Safety Scanner in a quick scan mode. The EOMT.ps1 script can be downloaded from Microsoft's GitHub repository and is capable of checking if a server is vulnerable to the ProxyLogon flaws, mitigate the Server-Side Request Forgery (SSRF) vulnerability by installing the IIS URL Rewrite module and a regular expression rule that aborts any connections containing the 'X-AnonResource-Backend' and 'X-BEResource' cookie headers and finally, downloads and runs the Microsoft Safety Scanner to remove known web shells and other malicious scripts installed via these vulnerabilities. According to experts, if administrators suspect that their installs have been compromised, the company recommends them to run the EOMT in the FULL SCAN mode.

Read more:

[https://securityaffairs[.]co/wordpress/115648/security/eomt-tool-microsoft-exchange.html]
[https://www.bleepingcomputer.com/news/microsoft/microsoft-releases-one-click-exchange-on-premises-mitigation-tool/]

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.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - **Cisco VPN Routers:**
    - **RV132W ADSL2+ Wireless-N -** version 1.0.1.15
    - **RV134W VDSL2 Wireless-AC -** version 1.0.1.21
  - **Microsoft Exchange Server -** 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.*