CERT-PH Cybersecurity Threat Feeds

Issue Date	March 01, 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:

- North Korea-linked Lazarus APT Targets Defense Industry with ThreatNeedle Backdoor
- China-linked TA413 Group Target Tibetan Organizations
- New Ryuk Ransomware Implements Self-spreading Capabilities
- Cisco Fixes Three Critical Bugs in ACI Multi-Site Orchestrator, Application Services Engine, and NX-OS

- CRITICAL
- URGENT
- INFORMATION

Description

North Korea-linked Lazarus APT Targets Defense Industry with ThreatNeedle Backdoor

2021.02.25 | Source(s): Security Affairs, Threatpost

Analysis:

Dubbed as Lazarus APT, the North Korea-linked group was observed targeting the defense industry with the custom-backdoor dubbed ThreatNeedle since 2020. The attack chain starts with COVID19-themed spear-phishing messages that contain either a malicious Word attachment or a link to one hosted on company servers. ThreatNeedle attempts to exfiltrate sensitive data from the infected networks through SSH tunnels to a remote server located in South Korea. Attackers employed a custom tunneling tool to achieve this, it forwards client traffic to the server, the malware encrypts the traffic using trivial binary encryption. The backdoor is able to bypass network segmentation and access restricted networks.

Read more:

[https://securityaffairs[.]co/wordpress/115013/apt/lazarus-apt-threatneedle.html]
[https://threatpost[.]com/lazarus-targets-defense-threatneedle-malware/164321/]

China-linked TA413 Group Target Tibetan Organizations

2021.02.26 | Source(s): Security Affairs

Analysis:

Tracked as TA413, the Chinese hacking group used a malicious Firefox add-on in a cyberespionage campaign aimed at Tibetan organizations. Dubbed as FriarFox, the malicious Firefox add-on allows the threat actors to steal Gmail and Firefox browser data and deliver malware on infected systems. The attack chain begins with spear-phishing email messages that attempt to trick victims into visiting websites that ask them to install a Flash update to view the site's content. Once the FriarFox browser extension is installed, attackers gain access to the user's Gmail account and FireFox browser data. The FriarFox add-on also contacts the C2 server to retrieve the PHP and JS-based payload Scanbox frameworks.

Read more:

[https://securityaffairs[.]co/wordpress/115030/apt/china-ta413-targets-tibet.html]
[https://www.bleepingcomputer[.]com/news/security/malicious-firefox-extension-allowed-hackers-to-hijack-gmail-accounts/]

New Ryuk Ransomware Implements Self-spreading Capabilities

2021.02.25 | Source(s): Security Affairs, Bleeping Computer

Analysis:

Cybersecurity experts spotted a new Ryuk ransomware variant that implements self-spreading capabilities to infect other devices on victims' local networks. This Ryuk ransomware variant doesn't include any mechanism for blocking the execution of the ransomware (MUTEX like or else), it copies itself with a rep.exe or lan.exe suffix. The ransomware generates every possible IP address on local networks and sends them an ICMP ping. It lists the IP addresses of the local ARP cache and sends them a packet, then it lists all the

sharing resources opened on the found IPs, mounts each of them, and attempts to encrypt their content. This variant is also able to remotely create a scheduled task to execute itself on this host.

Read more:

[https://securityaffairs[.]co/wordpress/115064/reports/ryuk-ransomware-self-spreading-capabilities.html]
[https://www.bleepingcomputer[.]com/news/security/ryuk-ransomware-now-self-spreads-to-other-windows-lan-devices/]

Cisco Fixes Three Critical Bugs in ACI Multi-Site Orchestrator, Application Services Engine, and NX-OS

2021.02.25 | Source(s): Security Affairs, Threatpost

Analysis:

Cisco released security updates to address over a dozen vulnerabilities affecting multiple products, including three critical flaws impacting its ACI Multi-Site Orchestrator, Application Services Engine, and NX-OS software. The most severe vulnerability, tracked as CVE-2021-1388, is a remote bypass authentication issue that affects an API endpoint of the ACI Multi-Site Orchestrator (MSO) and received a CVSS score of 10. The flaw is caused by the improper token validation of tokens. An attacker could trigger the issue by sending crafted requests to receive a token with administrator-level privileges that they could be used to authenticate to the API on affected MSO devices. Cisco also addressed two unauthorized access vulnerabilities, tracked as CVE-2021-1393 and CVE-2021-1396, that affect the Application Services Engine. Successful exploitation of these vulnerabilities could allow an unauthenticated, remote attacker to gain privileged access to host-level operations or to learn device-specific information, create diagnostic files, and make limited configuration changes. Another critical flaw fixed by Cisco is the CVE-2021-1361 flaw that affects the NX-OS running on Nexus 3000 and Nexus 9000 series switches. The flaw received a CVSS score of 9.8, it could be exploited remotely to manipulate arbitrary files with root privileges, without authentication.

Read more:

[https://securityaffairs[.]co/wordpress/115023/security/cisco-critical-flaw.html]
[https://threatpost[.]com/cisco-critical-security-flaw/164255/]

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 ACI Multi-Site Orchestrator** - latest version
  - **Cisco Application Services Engine -** latest version
  - **Cisco NX-OS Software** - 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.*