CERT-PH Cybersecurity Threat Feeds

Issue Date	May 19, 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:

- Bizarro Banking Trojan Targets Banks
- Decryptor Released for NoCry and Judge Ransomware
- PoC Exploit Code for Windows CVE-2021-31166 Bug Released
- Conti Ransomware Hit Ireland Health Service Executive

- CRITICAL
- URGENT
- INFORMATION

Description

Bizarro Banking Trojan Targets Banks

2021.05.18 | Source(s): Security Affairs, The Hacker News

Analysis:

A new banking trojan was recently detected targeting banks in Europe and South America that uses sophisticated means in compromising victim's account. Dubbed Bizarro, the banking Trojan allows threat actors to capture online banking credentials and hijack Bitcoin wallets from the victims devices. Bizarro has contains malicious code that tries to trick victims into entering their two-factor authentication codes in fake pop-ups. According to security researchers, the application was distributed via social engineering, Microsoft Installer packages, and bundled with trojanized applications. The ZIP archive contains a malicious DLL written in Delphi, a legitimate executable that is an AutoHotkey script runner, and a small script that calls an exported function from the malicious DLL. Upon execution, the malware kills all running browser processes to terminate any existing sessions with online banking websites. Once the victim attempts to access the banking services, they will be forced to re-enter their credentials, which will be captured by the malware. In order to force the victims into re-entering their credentials the malware disables the autocomplete feature in a browser. Bizarro gathers system info, including computer name, OS version, default browser name, installed antivirus software.

Read more:

[https://securityaffairs[.]co/wordpress/118032/cyber-crime/bizarro-banking-trojan.html]
[https://thehackernews[.]com/2021/05/70-european-and-south-american-banks.html]

Decryptor Released for NoCry and Judge Ransomware

2021.05.18 | Source(s): Security Affairs

Analysis:

A decryptor for Judge ransomware that can help in recovering victim's files for free. The Judge ransomware is written in a .NET that has the ability to determine whether it runs in a sandbox environment. The malware has also the ability to kill blacklisted processes and deletes system restore points before encrypting the victim's files. Security researchers also detected another ransomware that has the same encryption with the Judge malware, dubbed as NoCry. It was determined that the same decryptor can be used to retrieve encrypted files.

Read more:

[https://securityaffairs[.]co/wordpress/118054/malware/nocry-ransomware-analysis.html]

PoC Exploit Code for Windows CVE-2021-31166 Bug Released

2021.05.17 | Source(s): Security Affairs

Analysis:

Security researcher published a working proof-of-concept exploit code for a wormable Windows IIS server vulnerability. Tracked as CVE-2021-31166, the flaw is a critical HTTP Protocol Stack Remote Code Execution that could be exploited by an unauthenticated attacker by sending a specially crafted packet to a targeted server utilizing the HTTP Protocol Stack (http.sys) to process packets. This stack is used by the Windows built-in IIS server, which means that it could be easily exploited if the server is enabled. The flaw is wormable and affects different versions of Windows 10, Windows Server 2004 and Windows Server 20H2.

Read more:
[https://securityaffairs[.]co/wordpress/118015/hacking/poc-windows-iis-cve-2021-31166.html]

Conti Ransomware Hit Ireland Health Service Executive

2021.05.17 | Source(s): Security Affairs

Analysis:

Ireland Health Service Executive (HSE) refuses to pay a $20 million ransom demand after its systems were hit by the Conti ransomware gang. The Health Service Executive opted to shut down its infrastructure as a precaution to avoid the threat from spreading. Conti further stated that they would provide a decryptor and delete the stolen data if a ransom of $19,999,000 is paid to the threat actors. The Conti ransomware gang claims to have stolen 700 GB of sensitive data from the HSE over two weeks. Stolen info includes patient documents, contracts, financial statements, and payroll. Conti ransomware operators run a private Ransomware-as-a-Service (RaaS), the malware appeared in the threat landscape at the end of December 2019 and was distributed through TrickBot infections.

Read more:
[https://securityaffairs[.]co/wordpress/118001/cyber-crime/ireland-health-service-executive-conti-ransomware.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 unsecured 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.
- Avoid installing unknown or unverified applications, especially from third-party distribution platforms.
- For users who have been hit with a ransomware, immediately contact and report the incident to your IT/Cybersecurity for their checking and remediations.
- Update any vulnerable system/applications/devices to their latest and patched versions:
  - Microsoft May 2021 security update
- 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.*