Republic of the Philippines
NATIONAL POLICE COMMISSION
**PHILIPPINE NATIONAL POLICE**
**ANTI-CYBERCRIME GROUP**
Camp BGen Rafael T Crame, Quezon City

# ACG-CYBER SECURITY BULLETIN NR 198

## ACG-CSB 110520198

Reference Number ACG-CSB 110520198

## BEWARE OF RAGNAR LOCKER RANSOMWARE

The following information was obtained from different cyber security sources for notification to all parties concerned pursuant to the mandate of the Philippine National Police Anti-Cybercrime Group (PNP ACG) and classified as **"Restricted"** pursuant to the PNP Regulation 200-012 on Document Security and Impact Rating as high based on PNP Information Communication Technology (ICT) Security Manual s.2010-01 p. 22 and p.129.

## SUMMARY

Ragnar Locker is ransomware-type software designed not only to encrypt data but also to terminate installed programs, which are commonly used by managed service providers and various Windows services. This ransomware renames encrypted files by appending an extension, which contains "ragnar" and a string of random characters. For example, it will rename a file named "1.jpg" to "1.jpg.ragnar_0DE48AAB", and so on. It also creates a ransom message with a text file, the name of which contains the same string of random characters as the appointed extension. In this case, the ransom message would be named "RGNR_0DE48AAB.txt"

cyber criminals proliferate ransomware via spam campaigns, fake software updaters, untrusted software download channels, Trojans and unofficial software activation ('cracking') tools. They proliferate malware via spam campaigns by sending emails with malicious attachments or web links that download malicious files. Typically, they attach files such as Microsoft Office, PDF documents, archive files such as ZIP, RAR, executable files (.exe) or JavaScript files. Their main goal is to trick recipients into opening the attachments or downloaded files.

The ransom message states that this ransomware encrypts all files, and that the only way to decrypt them is using tools purchased from Ragnar Locker's developers. The initial cost of these tools is 25 Bitcoins, however, it is mentioned that unless the cyber criminals behind Ragnar Locker are contacted within 14 days of encryption, the cost of decryption tools is doubled, and after 21 days, decryption keys are deleted permanently. Victims are also warned that if they do not contact Ragnar Locker's developers at all, some of their personal/sensitive data will be uploaded to a public server and/or sold to third parties. To contact these cyber criminals, victims must supposedly use the qTox messenger and look for the provided contact or via the hello_psecu@protonmail.com email address. As mentioned, Ragnar Locker terminates certain services (relating to managed service providers) so that its attack cannot be detected and terminated. Furthermore, it does takes this approach with various Windows security services. Typically, victims of ransomware cannot decrypt compromised files without the correct tools held only by the cyber criminals who

designed the program. Unfortunately, this is the case with Ragnar Locker ransomware.

## RECOMMENDATION

All PNP personnel as well as the public are advised to follow the tips in order to avoid the risk of Ragnar Locker ransomware:

- Never Click unverified Links
- Do not open untrusted email attachments
- Only download from sites you trust
- Avoid giving out personal data
- Use security software
- Backup your data
- Keep security software updated

For additional information, please refer to the following websites:

- https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/
- https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ragnarlocker-ransomware-threatens-to-release-confidential-information/
- https://www.pcrisk.com/removal-guides/17018-ragnar-locker-ransomware
- https://www.kaspersky.com/resource-center/threats/how-to-prevent-ransomware

## POINT OF CONTACT

Please contact **PMAJ JOSEPH ARVIN L VILLARAN**, Police Communication Relation thru e-mail address acg@pnp.gov.ph or contact us on telephone number (632) 7230401 local 3562 for any inquiries related to this CYBER SECURITY BULLETIN.