Republic of the Philippines
National Police Commission
NATIONAL HEADQUARTERS, PHILIPPINE NATIONAL POLICE
ANTI-CYBERCRIME GROUP
Camp BGen Rafael T Crame, Quezon City
E-mail: acg@pnp.gov.ph

ACG-CYBER SECURITY BULLETIN NR 197

ACG-CSB 092320197

Reference Number ACG-CSB 092320197

Beware of and Nemty and Nefilim 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

The two primary differences between Nefilim and NEMTY are the payment model, and the lack of a RaaS operation. Nefilim instructs victims to contact the attackers via email, as opposed to directing them to a TOR-based payment portal. To add even more confusion to the family tree, Nefilim appears to have evolved into ‘Nephilim’, and the two are technically similar, differentiated primarily by extension and artifacts in encrypted files.

Nefilim and nemty has been discovered, threatening to release its victims’ data to the public if they fail to pay the ransom. It is most likely distributed through exposed Remote Desktop Protocol (RDP),

Nefilim and nefilim and typically proliferates via trojans, spam campaigns, illegal activation tools and fake updaters and untrusted download sources. Trojans are malicious programs that have many dangerous capabilities, which can include download or installation of additional malware The term "spam campaign" describes large scale operations, during which thousands of deceptive/scam emails are sent. These messages can have infectious files attached to or linked inside. Infectious files can be in various formats When they are opened, the infection process is triggered. Rather than activating licensed products, illegal activation like cracking tools can cause infections. Fake updaters infect systems by exploiting outdated products and/or simply installing malware rather than the promised updates. Malicious software can be unintentionally downloaded from untrusted sources such as unofficial and free file-hosting sites, P2P sharing networks and other third party downloaders.

Nefilim is a malicious program categorized as ransomware. It operates by encrypting the files of infected systems in order to demand payment for decryption tools/software. During the encryption process, all compromised files are appended with the ".NEFILIM" extension. For example, a file originally named something like

"1.jpg" would appear as "1.jpg.NEFILIM" following encryption. Once this process is complete, a ransom message within "NEFILIM-DECRYPT.txt" is created on the victims' desktops.

Nemty is a high-risk ransomware-type infection. The purpose of this ransomware is to encrypt data stored on the system so that developers can make ransom demands by offering paid recovery of files. NEMTY PROJECT also appends each filename with the ".nemty" extension (e.g., "sample.jpg" becomes "sample.jpg.nemty"). Additionally, NEMTY PROJECT stores a text file named "NEMTY-DECRYPT.txt" in most existing folders. An updated variant of NEMTY Project ransomware appends filenames with the "._NEMTY_[random_characters]_" extension (e.g., "1.jpg" -> "1.jpg._NEMTY_huWhN62_") and creates another text file "_NEMTY_[random_characters]_-DECRYPT.txt" (e.g., "_NEMTY_huWhN62_-DECRYPT.txt") containing an identical message.

Nefilim and nemty ransomware have designed it to encrypt data with cryptographic algorithms that cannot be broken with third party software. Decryption is impossible without the unique decryption key, which is held by the cyber criminals behind the infection. These criminals promise to quickly and safely recover the affected data, if their demands are met. Additionally, they claim to have exfiltrated a large amount of users' data, and if they do not establish contact within seven working days, these files will be leaked (publicized) online. After contact is made via email, victims are informed that they will be provided with 'proof' that this threat is not a hoax and some files have indeed been stolen. To ensure that decryption is possible, users can send two encrypted files to test it. Unfortunately, in many cases of ransomware infections, decryption is impossible without the involvement of the cyber criminals responsible, unless the malware is still in development or has bugs/flaws

opening suspicious or irrelevant emails, especially those received from unknown senders. Any attachments or links present in dubious messages must not be opened, as doing so can result in high-risk infection. Use only official and verified download channels. It is also important to activate and update products with tools/functions provided by legitimate developers. Do not use illegal activation tools or third party updaters, as they are often employed to proliferate malware.

RECOMMENDATION

All PNP personnel as well as the public are advised to follow the tips in order to avoid the dangers of Nefilim Ransomware, to wit:

- Never click on unverified links
- Do not open untrusted email attachments
- Only download from sites you trust
- Keep your software and operating system updated
- Keep security software updated
- Backup your data
- Isolate your computer
- Never pay the ransom

For additional information, please refer to the following websites:

- https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/nefilim-ransomware-threatens-to-expose-stolen-data
- https://cisomag.eccouncil.org/nefilim-ransomware-the-gennext-of-nemty-ransomware/
- https://www.safe-t.com/nefilim-ransomware-uses-rdp-to-expose-sensitive-data/
- https://www.pcrisk.com/removal-guides/17305-nefilim-ransomware
- https://labs.sentinelone.com/meet-nemty-successor-nefilim-nephilim-ransomware/
- https://labs.sentinelone.com/meet-nemty-successor-nefilim-nephilim-ransomware/
- https://www.trendmicro.com/vinfo/se/security/news/cybercrime-and-digital-threats/nemty-ransomware-ceases-public-operations-focuses-on-private-schemes#:~:text=Nemty%20ransomware%20was%20discovered%20in,information%20from%20the%20infected%20device.

POINT OF CONTACT

Please contact PMAJ JOSEPH ARVIL L VILLARAN, Police Communication Relation officer 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.