SEQURETEK

NEFILIM RANSOMWARE

OVERVIEW

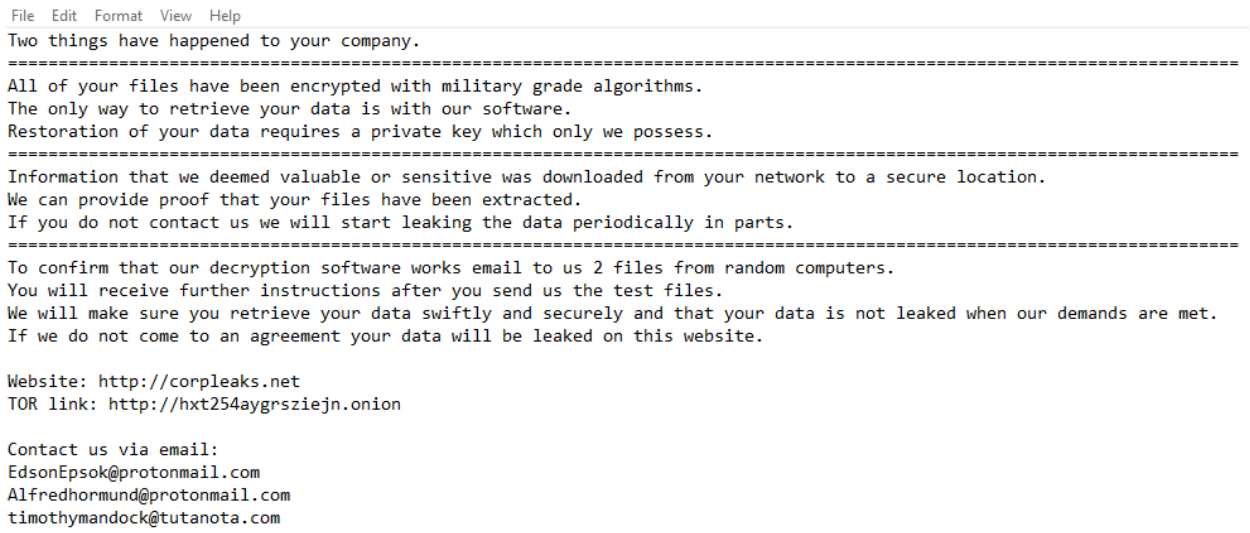
Nefilim targets victim through vulnerable RDP and threaten victims to publish data on dark web.

OVERVIEW

- Nefilim/Nephilim ransomware started spreading from the end of February 2020.
- Nefilim campaign threatens to publish victims' sensitive information on dark web if victim fails to comply to attacker's demands within seven days.
- Nefilim ransomware share similarity in code with another ransomware family Nemty 2.5 discovered in August 2019. Nemty campaign is now private, No Ransomware as a service is available now.
- The key difference between Nefilim and Nemty is, Nefilim has removed the Ransomware-as-a-Service (RaaS) component and instead of using a Tor payment site Nefilim now relies on email communications for payments.
- Nefilim attacker may have acquired code from Nemty Authors or reverse engineered.

ATTACK FLOW

- The initial entry to victim's system is through vulnerable RDP (Remote Desktop Protocol) services. After compromise RDP, attackers establish persistence and exfiltrate credentials and data, and last deliver ransomware payload for encryption.
- Nefilim encrypt files with AES-128 encryption and then AES encryption key is encrypted by RSA-2048. After infection ransomware append .Nefilim or .NEPHILIM extension to affected files.



File Edit Format View Help

Two things have happened to your company.

==========

All of your files have been encrypted with military grade algorithms.
The only way to retrieve your data is with our software.
Restoration of your data requires a private key which only we possess.

==========

Information that we deemed valuable or sensitive was downloaded from your network to a secure location.
We can provide proof that your files have been extracted.
If you do not contact us we will start leaking the data periodically in parts.

==========

To confirm that our decryption software works email to us 2 files from random computers.
You will receive further instructions after you send us the test files.
We will make sure you retrieve your data swiftly and securely and that your data is not leaked when our demands are met.
If we do not come to an agreement your data will be leaked on this website.

Website: http://corpleaks.net
TOR link: http://hxt254aygrsziejn.onion

Contact us via email:
EdsonEpsok@protonmail.com
Alfredhormund@protonmail.com
timothymandock@tutanota.com

Figure 1: Ransom Note (Source: Twitter)

- Nefilim attackers steal victim's data and share it on website if victim fails to pay ransom.
- Nefilim share data on dark web after attacking following companies.
  - ❖ Aban Offshore (India's largest offshore drilling services provider)
  - ❖ Aliansce Sonae (Management company for shopping centers in Brazil)
  - ❖ Arteris SA (Infrastructure sector in Brazil)
  - ❖ Cosan (Brazilian conglomerate producer of bioethanol, sugar and energy)
  - ❖ Fisher & Paykel (New Zealand)
  - ❖ MAS Holdings (South Asia's largest manufacturer of apparel)
  - ❖ Stadler Rail (Swiss manufacturer of railway rolling stock)
  - ❖ TOLL GROUP (Australian transportation and logistics company)
  - ❖ W&T Offshore (Gulf of Mexico)

Figure 2: Example of leaked data

INDICATORS OF COMPROMISE

File Hashes (MD5)

- 004F67C79B428DA67938DADEC0A1E1A4
- 053EC539C138AFB99054BD362BB3ED71

- 0790A7E0A842E1DE70DE194054FA11B3
- 26C35850483C877EE23F476B38D58DEB
- 3BEB3D466BCC0977EC2DD66D72AB6BB3
- 5FF20E2B723EDB2D0FB27DF4FC2C4468
- 659C4B68F2027905DEF1AF9249FEEBB3
- 70E4B9B7A83473687E5784489D556C87
- 7354E71D9C28E0C150CEA3377E5F70D9
- 80CFDA61942EB4E71F286297A1158F48
- 86E048D2EAE96A817B272A2A7258271C
- 8F90539C405672016C0DEC7AC3574EEA
- AD25B6AF563156765025BF92C32DF090
- C7D73FF9743FD8ABCDA7466F70AA3085
- CE3CD1DAB67814F5F153BCCDAF502F4C
- DC88265C361D73540A31C19583271FB0
- DDC50D4AE0674D854A845B3EB32508C3
- DFD4DBFD7CBD6179FC371E5F887F189C

Contact Email Addresses

- Derekvirgil[at]protonmail[.]com
- Samanthareflock[at]mail[.]com
- Gerardbroncks[at]tutanota[.]com

PREVENTIVE AND CORRECTIVE ACTIONS

- **For Organizations**
  - **Preventive Actions**
    - Block the IoCs in the corresponding security devices.
    - All these IoCs are combined in our Threat Intelligence Feed that is integrated with our SOC to provide proactive threat protection to our clients.
    - Employ content scanning and filtering on the organization mail servers. Inbound e-mails should be scanned for known threats and should block any attachment types that could pose a threat.

- In order to protect the systems from ransomware in general, it is important that users use good computing habits and security software. First and foremost, always have a reliable and tested backup of the data that can be restored in the case of an emergency, such as a ransomware attack.
- Make sure that all systems and software are up-to-date with relevant security patches.
- Turn off file sharing if not needed. If file sharing is required, use ACLs and password protection to limit access. Disable anonymous access to shared folders. Grant access only to user accounts with strong passwords to folders that must be shared.
- Limit the number of third-party vendors and employees that have access to RDP connections, create a user group that will be allowed remote access.
- Use strong passwords and multi-factor authentication on Remote Desktop connection especially on administrator accounts.
- Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted.
- Do not pay the ransom. It only encourages and funds these attackers. Even if the ransom is paid, there is no guarantee that one will be able to regain access to files.

- **Corrective Actions**
  - If infected, disconnect the affected system from the Network.
  - Inform the Information Security Team.
  - Use antivirus or anti-malware software to clean the ransomware.

- **For Individuals**
  - **Preventive Actions**
    - Do not open mails and mail attachments from unknown people.
    - Do not download or use software cracks and illegal software.
    - Use strong password and multi-factor authentication for your RDP (Remote Desktop Protocol) connection.
    - Make sure your RDP connection is not open to the internet.

- If not using RDP, close TCP Port 3389 on the computers.
- Enable network level authentication for RDP.
- Avoid installing free programs found on the Internet, many of them include viruses.
- Be careful of the external devices you connect to your computer.
- Update your antivirus regularly.
- Take regular backups of your data.

- **Corrective Actions**
  - If infected, disconnect your system from the Network.
  - Perform a full system scan in safe mode to remove any infections.