Nefilim Ransomware Threatens to Expose Stolen Data

trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/nefilim-ransomware-threatens-to-expose-stolen-data

A new ransomware named Nefilim 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), as shared by SentinelLabs' Vitali Krimez and ID Ransomware's Michael Gillespie via Bleeping Computer.

Nefilim's code shares many notable similarities with Nemty 2.5 ransomware; the main difference is the fact that Nefilim has done away with the Ransomware-as-a-Service (RaaS) component. It also manages payments via email communication rather than through a Tor payment site. There is nothing that indicates that the same threat actors are behind Nemty and Netfilim. The new ransomware is most likely spread through RDP, like other ransomware such as Nemty, Crysis, and SAMSAM.

Netfilim uses AES-128 encryption to encrypt victim's files. An RSA-2048 embedded in the ransomware executable will then encrypt the AES encryption key. The encrypted AES key will then be added to every encrypted key. The ransomware also adds a "NEFILIM" string as a file marker to all encrypted files. The encrypted files will have .NEFILIM appended to their file names (for example, a file called 1.doc would be named 1.doc.NEFILIM).

To decrypt these files, victims need to get the RSA private key from the ransomware developers. Details of the ransom have not been released yet.

Race against ransomware

Ransomware continues to expand its reach as threat actors continue to come up with new ransomware variants and families. The healthcare, government, and education sectors were on the receiving end of many such attacks last year, as revealed in the Trend Micro 2019 Annual Security Roundup. Unfortunately, many feel pressured to pay the ransom to prevent the paralysis of operations and the loss of valuable data.

Like Nefilim, many of these ransomware attacks abuse exposed RDP ports. Enterprises can take the following steps to defend against RDP abuse:

- Close unused RDP ports. If closing them is not possible, limit the source addresses that can access the ports.
- Configure settings to ensure that only authorized users can gain RDP network admin access.
- Monitor the network to spot signs of attacks.
- Limit the number of failed login attempts to keep unauthorized logins at bay.

[Read: InfoSec Guide: Remote Desktop Protocol (RDP)]

Companies should also establish firm protocols and rules in dealing with unverified emails; employees should avoid opening these emails or attachments. To prevent data loss, employees should also regularly backup files. Finally, regularly updating software and applications can ensure that the system is protected against both old and recent vulnerabilities.

Enterprises can also further improve security against ransomware through the combination of behavioral analysis and high-fidelity machine learning across email, endpoints, servers, and networks.

Enterprises that are dealing with a ransomware attack can try the Trend Micro Ransomware File Decryptor (available in Windows and macOS) for free.

Indicators of compromise

SHA-256	Trend Micro Pattern Detection	Trend Micro Machine Learning Detection
5ab834f599c6ad35fcd0a168d93c52c399c6de7d1c20f33e25cb1fdb25aec9c6	Ransom.Win32.NEFILIM.B	Troj.Win32.TRX.XXPE50FFF034

HIDE

Like it? Add this infographic to your site:
1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

Posted in Cybercrime & Digital Threats, Ransomware