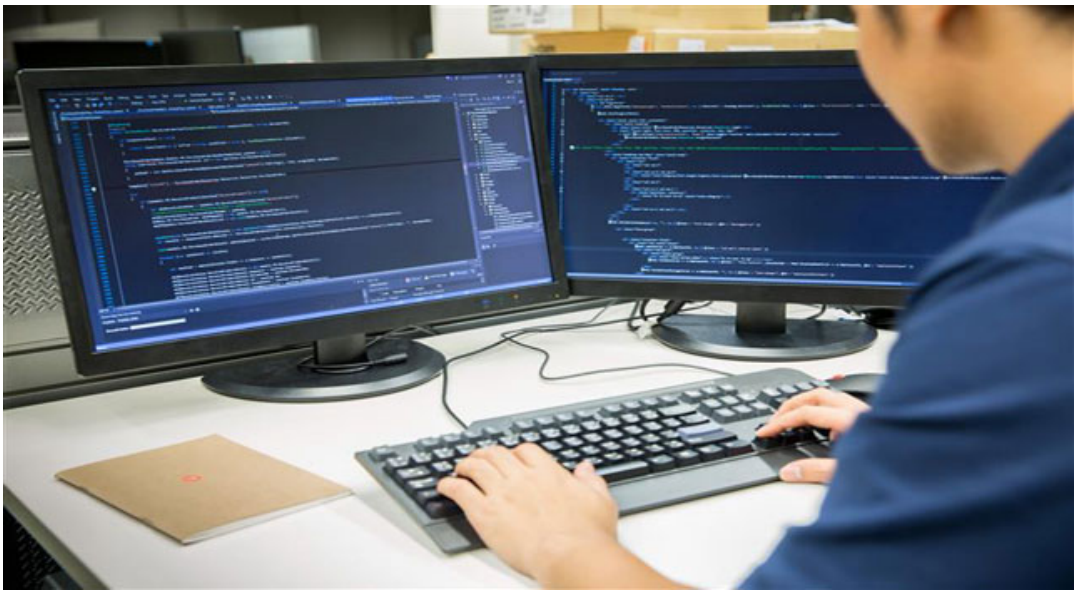
An Analysis of the Nefilim Ransomware

trendmicro.com/en_us/research/21/b/nefilim-ransomware.html

February 23, 2021



Ransomware

Nefilim is known for its double extortion capabilities and notable attacks in 2020. We give an overview of its techniques and tools in this entry.

By: Janus Agcaoili, Byron Gelera February 23, 2021 Read time: (words)

Nefilim is among the notable ransomware variants that use double extortion tactics in their campaigns. First discovered in March 2020, Nefilim threatens to release victims' stolen data to coerce them into paying the ransom. Aside from its use of this tactic, another notable characteristic of Nefilim is its similarity to Nemty; in fact, it is believed to be an evolved version of the older ransomware.

We provide a brief analysis of this active ransomware and how to defend systems against it.

Technical Details

Initial access

For its initial access, threat actors behind Nefilim make use of various affiliates to spread their malware. These affiliates use various methods. Based on previous attacks, Nefilim has been largely known to reach systems via exposed RDPs. Some affiliates also use other known vulnerabilities for initial access. This is supported by various reports, from which we found the use of the Citrix vulnerability (CVE-2019-19781), an unsecure and brute-force RDP, to enter a system.

Nefilim has also been seen using party tools to gather credentials that include Mimikatz, LaZagne, and NirSoft's NetPass. The stolen credentials are used to reach high-value machines like servers.

Once inside a victim system, the ransomware begins to drop and execute its components such as anti-antivirus, exfiltration tools, and finally Nefilim itself.

Lateral movement on the network

The attackers make use of several legitimate tools for lateral movement. For example, it uses PsExec or Windows Management Instrumentation (WMI) for lateral movement, dropping and executing other components including the ransomware itself. Nefilim has been observed to use a batch file for terminating certain processes and services. It even uses third-party tools like PC Hunter, Process Hacker, and Revo Uninstaller to terminate antivirus-related processes, services, and applications. It also uses AdFind, BloodHound, or SMBTool to identify active directories and/or machines that are connected to the domain.

Data exfiltration

A notable aspect of recent ransomware variants are their data exfiltration capabilities. As for Nefilim, it has been observed to copy data from servers or shared directories to a local directory and to archive these using 7-Zip. It then uses MEGAsync to exfiltrate this data.

Defending systems against ransomware

Campaigns that are similar to Nefilim spend a lot of time between the initial breach and the start of serious lateral movement. However, as soon as lateral movement begins, threat actors work quickly. They prioritize moving between hosts and exfiltrating data. Therefore, organizations can consider limiting the number of computers that can be leveraged during a lateral movement phase. This involves solutions such as utilizing two-factor authentication (2FA) wherever they can, implementing application safelisting, and practicing least privilege security.

With regard to defending systems against the threat of Nefilim, best practices still apply. It is best to work on defenses that prevent the lateral movement of similar attacks. Organizations should consider the use of canary file-based monitoring, encryption monitoring, and process killing. Other best practices to review include the following:

- Avoid opening unverified emails or clicking on their embedded links, as these can start the ransomware installation process.
- Back up your important files using the 3-2-1 rule: Create three backup copies on two different file formats, with one of the backups in a separate location.
- Regularly update software, programs, and applications to ensure that your apps are current, with the latest protections from new vulnerabilities.

If you believe that your organization has been affected by this campaign, visit this page for the available Trend Micro solutions that can help detect and mitigate any risks from this campaign.

Indicators of Compromise (IOCs)

SHA256	Detection name
08c7dfde13ade4b13350ae290616d7c2f4a87cbeac9a3886e90a175ee40fb641	Ransom.Win32.NEFILIM.A
205ddcd3469193139e4b93c8f76ed6bdbbf5108e7bcd51b48753c22ee6202765	Ransom.Win32.NEFILIM.D
5da71f76b9caea411658b43370af339ca20d419670c755b9c1bfc263b78f07f1	Ransom.Win32.NEFILIM.D
7a73032ece59af3316c4a64490344ee111e4cb06aaf00b4a96c10adfdd655599	Ransom.Win32.NEFILIM.C
eacbf729bb96cf2eddac62806a555309d08a705f6084dd98c7cf93503927c34f	Ransom.Win32.NEFILIM.G
ee9ea85d37aa3a6bdc49a6edf39403d041f2155d724bd0659e6884746ea3a250	Trojan.Win64.NEFILIM.A
f51f128bca4dc6b0aa2355907998758a2e3ac808f14c30eb0b0902f71b04e3d5	Ransom.Win32.NEFILIM.D
fdaefa45c8679a161c6590b8f5bb735c12c9768172f81c930bb68c93a53002f7	Ransom.Win32.NEFILIM.D