How to Beat Nefilim Ransomware Attacks

By Suleyman Ozarslan, PhD

Published: 2020-12-03 · Archived: 2026-04-05 14:12:29 UTC

A Detailed Walkthrough of Nefilim Ransomware TTPs

Over the course of 2020, the number of ransomware attacks has increased enormously. As an emerging ransomware family, Nefilim has caused dozens of high profile breaches since March 2020. In this blog post, we provide tactics, techniques and procedures (TTPs) utilized by the Nefilim threat actors, since detecting and blocking TTPs used by a threat is the most effective method to prevent that threat. TTPs allow us to detect potential intrusions and analyze the behavior of those attempting to intrude.

Our analysis uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) version 8 framework. See the ATT&CK for Enterprise version 8.1 for all referenced threat actor tactics and techniques.

This blog describes:

- TTPs used by the Nefilim ransomware, categorized under MITRE ATT&CK tactics and techniques.
- An example threat in the **Picus Threat Library** that can be used to simulate the TTP.
- An example mitigation rule in the **Picus Mitigation Library** that can be used to prevent/detect the given TTP.

---

1. **Initial Access**

Adversaries use Initial Access techniques to gain a foothold in the target network.

1.1 MITRE ATT&CK T1190 Exploit Public-Facing Application

Nefilim operators exploit public-facing applications for initial access. They mainly use the `CVE-2019-19781` Remote Code Execution vulnerability affecting Citrix ADC/Gateway. Picus Threat Library includes 600+ vulnerability exploitation threats associated with the relevant CVE (Common Vulnerabilities and Exposures) identification number.

Following threats in the Picus Threat Library can be used to simulate this TTP:

Threat ID	Threat Name
321318	Citrix Application Delivery Controller (ADC) and Gateway Path Traversal Vulnerability Variant-1
311195	Citrix Application Delivery Controller (ADC) and Gateway Path Traversal Vulnerability Variant-2

Following mitigation signatures can be used to prevent CVE-2019-19781 exploitation:

Security Product	Signature ID	Signature Name
Check Point NGFW	asm_dynamic_prop_CVE_2019_19781	Citrix Multiple Products Directory Traversal (CVE-2019-19781)
Cisco Firepower NGFW	1.52512.2, 1.52603.1	SERVER-WEBAPP Citrix ADC and Gateway arbitrary code execution attempt
F5 BIG-IP	200004998	Citrix NetScaler NSC_USER Remote Code Execution
Forcepoint NGFW		HTTP_CRL-Citrix-Path-Traversal-CVE-2019-19781
FortiGate IPS	48653	Citrix.Application.Delivery.Controller.VPNs.Directory.Traversal
FortiWeb WAF	090501033	Known Exploits
McAfee NSP	0x45272800	HTTP: Citrix ADC Arbitrary Code Execution Vulnerability (CVE-2019-19781)
Palo Alto Networks NGFW	57497	Citrix Application Delivery Controller And Gateway Directory Traversal Vulnerability
TippingPoint TPS	36876	HTTP: Citrix Application Delivery Controller (ADC) Directory Traversal Vulnerability

---

2. **Execution**

2.1 MITRE ATT&CK T1106 Native API

Nefilim directly interacts with the native OS application programming interface (`API`) to execute behaviors.

Picus Threat Library - Threat	Picus Mitigation Library - Detection Rule
338852 Execution through API Attack Scenario	8418 New Process Creation via CreateProcess API Call

---

3. **Defense Evasion**

3.1 MITRE ATT&CK T1055 Process Injection

The Nefilim ransomware creates a new `wermgr.exe` (the Windows error reporting manager) process and injects its payload to evade process-based defenses. You can read our process injection blog post for a detailed description of this method.

Picus Threat Library - Threat	Picus Mitigation Library - Detection Rule
481103 Process Injection Attack Scenario	6443 Reflective Portable Executable Injection

3.2 MITRE ATT&CK T1574.002 Hijack Execution Flow: DLL Side-Loading

Nefilim uses `WerFault.exe` and `wermgr.exe` for DLL Side Loading, a defense evasion technique used by adversaries to execute malicious payloads by hijacking the library manifest used to load DLLs. `Werfault.exe` is the Windows Error Reporting binary used by many different programs to report errors.

Picus Threat Library - Threat	Picus Mitigation Library - Detection Rule
286264 DLL Side-Loading by using Xwizard.exe	6042 Arbitrary DLL Load

3.3 MITRE ATT&CK T1562.001 Impair Defenses: Disable or Modify Tools

The Nefilim ransomware uses a batch file to stop services and kill processes in the local host. This batch file abuses `taskill.exe` using CMD to kill predefined services and processes in the target host. Nefilim distributes this batch file to multiple hosts using two batch files. One of the batch files uses the ‘copy’ command, and the other one uses WMI with hard-coded admin credentials.

Picus Threat Library - Threat	Picus Mitigation Library - Detection Rule
650331 Stop Service Attack Scenario	8863 Critical Services Termination with TaskKill Tool

3.4 MITRE ATT&CK T1070.004 Indicator Removal on Host: File Deletion

Nefilim removes itself from the target systems after infection with the following code:

del "C:\Users\admin\AppData\Local\Temp\<ransomware_file_name>.exe" /s /f /q	
Picus Threat Library - Threat	**Picus Mitigation Library - Detection Rule**
681453 Indicator Removal on Host Attack Scenario	6467 Defense Evasion by Windows Security Event Log Deletion

3.5 MITRE ATT&CK T1497.003 Virtualization/Sandbox Evasion: Time Based Evasion

Nefilim uses the following ‘timeout’ command to delay the execution of the ‘del’ command. Adversaries use this command also to evade sandbox analysis.

"C:\Windows\System32\cmd.exe" /c timeout /t 3 /nobreak	
Picus Threat Library - Threat	**Picus Mitigation Library - Detection Rule**
744943 Virtualization/Sandbox Evasion by using Timeout Command in Command-Line Tool	2313 Sandbox Evasion by Pausing The Command Processor via Timeout Command

---

4. **Credential Access**

Nefilim threat actor uses hard-coded admin credentials to utilize PsExec and WMI to execute commands and binaries in remote hosts (lateral movement). Since these credentials are hard-coded in the batch files, it must be stolen before the attack with some credential access techniques.

4.1. MITRE ATT&CK T1056.001 Input Capture: Keylogging

The Nefilim ransomware creates a `DirectInput` object using the `DirectDrawCreateEx` function to capture keystrokes.

Picus Threat Library - Threat	**Picus Mitigation Library - Detection Rule**
431235 Input Capture Attack Scenario	5924 User Input Capture via PowerShell Script

4.2 MITRE ATT&CK T1003 OS Credential Dumping

Nefilim uses the Mimikatz tool to obtain username and password information useful in gaining access to additional systems in the target network.

Picus Threat Library - Threat	**Picus Mitigation Library - Detection Rule**

393510 Credential Dumping using Mimikatz Tool	4920 Password and Hash Dump via Mimikatz

5. **Discovery**

Interestingly, the batch files used by Nefilim include hard-coded Internal IP addresses, admin credentials, services, and processes. This means that Nefilim attacks are highly targeted attacks as the hard-coded information requires an intensive discovery operation prior to attacks. Dynamic analysis of the Nefilim ransomware samples shows that the following techniques are used by Nefilim to discover the required information.

5.1 MITRE ATT&CK T1518.001 Software Discovery: Security Software Discovery

The Nefilim ransomware uses `IsDebuggerPresent`, `CheckRemoteDebuggerPresent`, and `NtQueryInformationProcess` API functions to check if a user-mode debugger is running. Debuggers are used by security analysts to inspect malware's behavior at the run-time. In the presence of a debugger, malware samples exhibited less malicious behavior. Moreover, Nefilim uses the `NtSetInformationThread` API function to evade debugging.

Picus Threat Library - Threat	**Picus Mitigation Library - Detection Rule**
112771 Security Software Discovery Attack Scenario	3379 Security Software Discovery

5.2 MITRE ATT&CK T1018 Remote System Discovery

Nefilim reads the hosts file (`C:\Windows\System32\drivers\etc\hosts`) to get a listing of other systems by IP addresses and hostnames on the network that may be used for Lateral Movement from the current system.

Picus Threat Library - Threat	**Picus Mitigation Library - Detection Rule**
101233 Gather Windows Host File	6813 Remote System Discovery by Obtaining Mappings of IP Addresses to Host Names

5.3 MITRE ATT&CK T1082 System Information Discovery

The Nefilim ransomware queries volume information (disk volume name and serial number) and Cryptographic Machine GUID. Ransomware families use Cryptographic Machine GUID and volume serial number to generate a unique identifier for the host for encryption/decryption processes.

Nefilim obtains Cryptographic Machine GUID by querying the value of `MachineGuid` in the following Registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography

Picus Threat Library - Threat	Picus Mitigation Library - Detection Rule
793307 Query Cryptographic Machine GUID in Registry	6886 System Information Discovery via Querying MachineGuid Key Value in Registry

5.4 MITRE ATT&CK T1083 File and Directory Discovery

Like a typical ransomware TTP, Nefilim enumerates files before encrypting them. It uses some FileAPI functions such as `FindFirstFileW`, `lstrcmpiW` and FindNextFileW to discover files.

Picus Threat Library - Threat	Picus Mitigation Library - Detection Rule
286738 File and Directory Discovery Attack Scenario	4771 Sensitive Information Discovery by Searching Filenames

---

6. **Lateral Movement**

Lateral Movement refers to a tactic that adversaries use to move through a network to access and control remote assets in the network. To accomplish Lateral Movement, adversaries may use legitimate tools with valid accounts as well as their remote access tools.

6.1. MITRE ATT&CK T1570 Lateral Tool Transfer

The Nefilim ransomware downloads the `Psexec.exe` tool, and it also abuses the Windows built-in `WMI` (Windows Management Instrumentation) utility for lateral movement. PsExec is a free Microsoft tool that can be used to execute commands and binaries on remote systems and download or upload a file over a network share. Nefilim uses PsExec and WMI with hard-coded admin credentials to remotely execute the batch files and the ransomware file in remote hosts.

Picus Threat Library - Threat	Picus Mitigation Library - Detection Rule
526471 Remote File Encryption with PsExec	3244 PsExec Tool Remote Command Execution

---

7. **Collection**

Adversaries use the techniques in the Collection tactic to gather information relevant to their objectives. Various data types such as text, audio, and video are collected from multiple sources such as local system cloud, network drive, removable media, and clipboard. The next goal after data collection is often to exfiltrate the data.

7.1 MITRE ATT&CK T1056.001 Input Capture: Keylogging

The Nefilim ransomware creates a `DirectInput` object using the `DirectDrawCreateEx` function to capture keystrokes. Keylogging is both a Credential Access and Collection tactic.

Picus Threat Library - Threat	**Picus Mitigation Library - Detection Rule**
431235 Input Capture Attack Scenario	5924 User Input Capture via PowerShell Script

---

8. **Exfiltration**

Adversaries use techniques in the Exfiltration tactic to steal data from your network. They encrypt or compress the data to be exfiltrated and use different channels and protocols to avoid detection. For example, the Nefilim ransomware compresses collected files and exfiltrates them to cloud storage.

Data loss protection is one of the top priority issues for CISOs today. Organizations utilize DLP solutions to protect and secure their data and comply with regulations. Picus simulates the exfiltration of a wide range of data over different channels to test the effectiveness of both network and endpoint-based data loss prevention (DLP) solutions. Picus Threat Library includes hundreds of data files consisting of different types of information mapped to standards and regulations, including PII, PCI DSS, PHI, GDPR, HIPAA, PIPEDA, confidential files such as password files of OSs, and Intellectual Property (IP) data.

Some examples of data exfiltration attacks in the Picus Threat Library are given in the following table:

Picus Threat Library - Threat	
107307	Italy PCI and PII Information Exfiltration including Full Credit Card Info
893939	Italy PII Info. Exfiltration including Codice Fiscale
727983	IBAN Numbers of 100 Countries Exfiltration in XLSX Format

8.1 MITRE ATT&CK T1567.002 Exfiltration Over Web Service: Exfiltration to Cloud Storage

Nefilim operators use the `MEGAsync` application to exfiltrate data to cloud storage. MEGAsync application synchronizes folders between the infected computer and an adversary-controlled MEGA Cloud Drive.

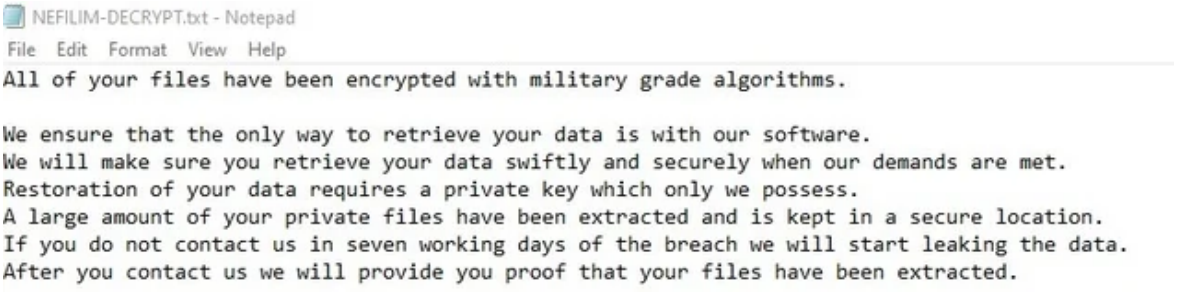
---

9. **Impact**

The Impact tactic covers techniques that manipulate, interrupt, or destroy your systems to disrupt availability, compromise integrity, or cover a confidentiality breach.

9.1 MITRE ATT&CK T1486 Data Encrypted for Impact

Like other ransomware threats, Nefilim encrypts files on the target system using AES-128 and adds NEFILIM, NEPHILIM, MERIN, TRAPGET, MEFILIN, TELEGRAM, SIGARETA, or OFFWHITE extension to encrypted files. It uses an RSA-2048 public key embedded in the ransomware executable to encrypt the AES encryption key. It also adds a file that includes the ransom note to the root directory, such as `C:\NEFILIM-DECRYPT.txt`.



Nefilim abuses Microsoft's Enhanced Cryptographic Provider to import cryptographic keys and encrypt data with API functions such as `CryptImportKey`, `CryptAcquireContext`, `CryptCreateHash`, `CryptHashData`, `CryptDeriveKey`, `CryptReleaseContext`, `CryptDestroyKey`, `CryptEncrypt` .This behavior is a very specific TTP of ransomware.

Picus Threat Library - Threat	**Picus Mitigation Library - Detection Rule**
767981 File Encryption with PowerShell	4737 Cryptography Encryptor and Decryptor Utilization via PowerShell

---

9.2 MITRE ATT&CK T1490 Inhibit System Recovery

Deleting volume shadow copies is very typical behavior of ransomware. The Nefilim ransomware uses `WMIC` with the following command to delete all volume shadow copies on the system to prevent recovery. WMIC is a command-line utility to access WMI.

Nefilim also uses bcdedit.exe twice to disable automatic Windows recovery features by modifying boot configuration data.

```
bcdedit /set {default} recoveryenabled No
bcdedit /set {default} bootstatuspolicy ignoreallfailures
```

Moreover, the Nefilim ransomware uses wbadmin to delete the backup catalog:

```
wbadmin delete catalog -quiet
```

Picus Threat Library - Threat	**Picus Mitigation Library - Detection Rule**
205796 Inhibit System Recovery by Deleting All Volume Shadow Copies with WMIC	7087 Shadow Copy Deletion via WMIC Tool

562990 Inhibit System Recovery by Disable Automatic Windows Recovery Features with bcdedit	3165 Disabling Windows Recovery Features via Bcdedit Tool
407822 Inhibit System Recovery by Deleting Windows Backup Catalog with Vbadmin	7067 Deleting Windows Backup Catalog via Vbadmin tool

Nefilim TTP Map

TTP Map of Nefilim that is created with TTPs detected from dozens of Nefilim ransomware samples can be found in the table below.

Although these TTPs are determined from the Nefilim samples, they are common in most ransomware families. The red techniques are very specific ransomware TTPs.

Initial Access	Execution	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
T1190 Exploit Public-Facing Application	T1106 Native API	T1574.002 Hijack Execution Flow: DLL Side-Loading	T1056.001 Input Capture: Keylogging	T1518.001 Software Discovery: Security Software Discovery	T1570 Lateral Tool Transfer	T1056.001 Input Capture: Keylogging	T1567.002 Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1486 Data Encrypted for Impact
		T1055 Process Injection	T1003 OS Credential Dumping	T1018 Remote System Discovery				T1490 Inhibit System Recovery
		T1562.001 Impair Defenses: Disable or Modify Tools		T1082 System Information Discovery				
		T1070.004 Indicator Removal on Host: File Deletion		T1083 File and Directory Discovery				
		T1497.003 Virtualization/ Sandbox Evasion: Time Based Evasion						

Conclusion

We analyzed dozens of Nefilim ransomware samples to determine tactics, techniques and procedures (TTPs) utilized by Nefilim. Continuously monitoring adversary TTPs within a company's IT system allows companies to discover adversary behaviors and stop them before they can go any further. Picus emulates adversary TTPs and gives actionable mitigation information for each TTP for building a proactive defense against adversaries and their malware.

Source: https://www.picussecurity.com/resource/blog/how-to-beat-nefilim-ransomware-attacks