Nefilim Ransomware Attack Through a MITRE Att&ck Lens

By By: Trend Micro Jun 28, 2021 Read time: 14 min (3807 words)

Published: 2021-06-28 · Archived: 2026-04-05 19:12:01 UTC

Nefilim is among a new breed of ransomware families that use advanced techniques for a more targeted and virulent attack. It is operated by a group that we track under the intrusion set "Water Roc". This group combines advanced techniques with legitimate tools to make them significantly harder to detect and respond before it is too late.

This allows them to remain undetected in the system for weeks, navigating across the environment to maximize their damage. Before the attack is even initiated, deep victim profiling is done, allowing them to use victim-specific extortion pricing to tailor the ransom.

Nefilim is a Ransomware as a Service(RaaS) operation first discovered in March 2020open on a new tab, and believed to have evolved from the earlier Nemty ransomware family. They target multi-billion dollar companies, primarily based in North or South America, in the financial, manufacturing or transportation industries. They operate under a profit share model, where Nefilim earns 30% for their ransomware service, and the remaining 70% goes to the affiliates who provide the network access and implements the active phase of the attack.

Like all ransomware, recovery is dependent on an external backup drive or paying for the encryption key, as Nefilim ransomware replaces the original files with encrypted versions.

Along with a new wave of double extortionopen on a new tab ransomware families, Nefilim affiliates are particularly vicious when victims don't immediately pay the ransom, leaking their sensitive data over an extended period of time. They are one of few groups that host leaked victim data long-term, for months to years, using it to deliver a chilling message to future victims.

The following is a fictional use case built using an in-depth case study of the Nefilim ransomware familyopen on a new tab to demonstrate how their typical attack process occurs. The story leverages the MITRE ATT&CK Frameworkopen on a new tab to define each tactic and technique used, with a detailed table below for further technical information.

Victim Use Case of Nefilim

Meet Company X, a fictional company serving the purpose of being the victim of a typical Nefilim ransomware attack. Company X is a global manufacturing organization with a yearly revenue of US$1 Billion and headquartered in North America, making them an ideal target of Nefilim.

Infiltrating the Environment

During their active vulnerability scanning (T1595.002) of Company X's internet facing hosts, the adversaries find that X has not patched a Citrix Application Delivery Controller vulnerability (CVE-2019-19781open on a new

tab). This is a vulnerability they can exploit to gain initial access (T1133) through the exposed Remote Desktop Protocol (RDP), and so the attack begins!

X's security team should have maintained an inventory of their exposed services across their environment, periodically scanning for vulnerabilities so they can proactively mitigate any potential inroads to their network. Internet-facing systems such as Citrix should always be a patching priority and managed with strong access controls. Access can be limited with a least-privileged administrative model and a strong multifactor authentication system (M1032) to strengthen account security and prevent credential access. If the RDP is unnecessary, which may be why it was left unpatched, then it should be disabled or blocked (M1042). Network proxies, gateways, and firewalls can also be leveraged to deny direct remote access to the internal system, blocking the inroad by which the adversaries are entering.

Intrusion Prevention Systems (IPS) can provide an additional layer of protection in advance of patch availability or patch deployment, which is particularly important with preventing targeted ransomware attacks, such as this one. IPS logs also provide relevant information for detecting initial access activities.

Once the actors have successfully infiltrated X's network, they begin downloading the additional tools they will need to further their plot (T1608). They download a Cobalt Strike beacon to establish a backdoor and persistent access to the environment so they can remotely execute commands, and later exfiltrate the data. This beacon is connected back to one of their pre-established shell companies that hosts their Cobalt Strike Command and Control (C&C) server. They also download Process Hacker to stop endpoint security agents (T1489), and Mimikatz to dump credentials (T1003.001), along with other tools they will need throughout their attack.

The adversaries need elevated permissions to run certain tools as administrators. They take advantage of another unpatched vulnerability in X's system (T1068), a Windows COM Elevation of Privilege Vulnerability (CVE-2017-0213open on a new tab). Armed with elevated permissions and credentials courtesy of Mimikatz, they are ready to continue their invasion.

The use of multiple vulnerabilities that were disclosed several years ago is a reminder of the importance of timely software updating (M1051) and patch management. A threat intelligence program can be developed to help identify what software exploits and N-day vulnerabilities may have the most impact on an organization (M1019). Virtual patching programs can enhance existing patch management processes to further defend against known and unknown vulnerabilities. Application isolation and sandboxing can also be used to mitigate the impact of advisories taking advantage of unpatched vulnerabilities (M1048). Ultimately, an organization needs good application security that looks for and detects exploitation behavior.

Mimikatz is a popular tool used for credential dumping of plaintext passwords, hashes, Kerberos tickets and other sensitive data from memory. It can also be used to gain access to other systems within the network through a pass-the-hash attack (T1550). However, Mimikatz has no major legitimate use that would explain admins having it on their system, so this tool should be treated as suspicious in most cases.

Mitigations can be established through strict account management and Active Directory Audit Policiesopen on a new tab. Enforcing the least-privileged administrative Model (M1018) and limiting credential overlap (M1026) across systems helps to further prevent compromised credential enabling lateral movement.

Completing the Invasion

The attackers take advantage of tools that already exist in the system to move laterally and expand their invasion (T1570). They use PsExec to launch taskkill to stop services that could alert X's security team, and to stop backup services (T1489). AdFind gives them vital information about the active directory setup which they use to map out X's infrastructure and find other targets of interest (T1018). Over time, they move throughout X's entire environment, including peripheral devices (T1120) and shared drives (T1135), identifying all the valuable data (T1083), and then using PowerShell commands, they strategically drop Cobalt Strike beacons in specific systems important to their attack as they go.

Network intrusion detection and prevention systems (M1031) are critical to mitigate adversary activity after initial access at the network level. These systems can help security teams see that they've been breached and track the attacker's activities with sensors at the network, cloud, and endpoint/server layers. Network segmentation and micro segmentation can help to inhibit lateral movement and support security monitoring.

Exfiltration for Encryption

The attackers use automated exfiltration (T1020) with their existing C&C channels established with the Cobalt Strike beacons set up across X's environment (T1041). The sensitive data is stolen using file transfer protocols (FTP) in fixed size chucks to avoid triggering network data transfer threshold alerts (T1030). For any large files, they use mega.nz to callback the data over the legitimate web service (T1567).

To prevent the exfiltration of data, web-based content can be restricted (M1021) and network traffic can be filtered (M1037). Any suspicious DNS, HTTP and HTTPS connections should be monitored or blocked entirely. AV software should also be kept up-to-date with machine learning plug-ins. As a rule of thumb, it is important to block any traffic to a Cobalt Strike C&C server, however since Cobalt Strike is designed to evade security measures, a multilayer approach is needed for this to be effective.

Execution of Ransomware

After a few weeks, the attackers are satisfied that they have identified all valuable data within X's environment. They wait until a weekend to help ensure they remain undetected, and then they deploy the Nefilim ransomware on X's network. The ransom note is prepared for decryption, then Nefilim imports an RSA-2048 public key and leaves it ready to use for encryption. The Nefilim payload is executed with a command-line argument (T1059) containing the full path of directory with the files identified to be encrypted. All of X's logical drives are encrypted, and a decrypted ransom note named "NEFILIM-DECRYPT.txt" is written for each one.
