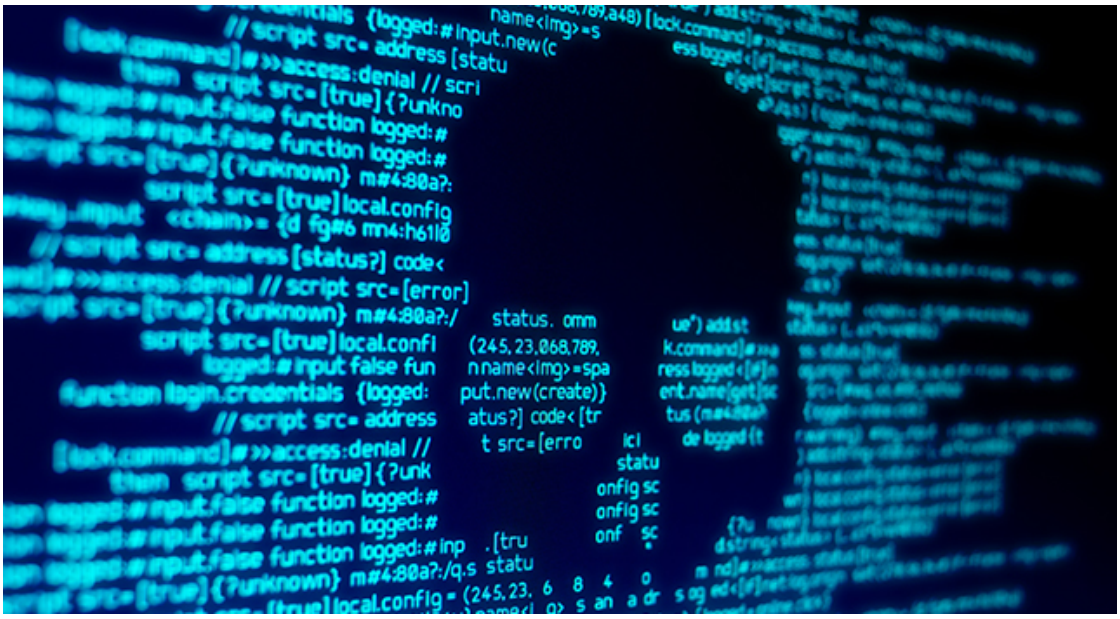
Nefilim Ransomware Attack Through a MITRE Att&ck Lens

trendmicro.com/en_us/research/21/f/nefilim-modern-ransomware-attack-story.html

June 28, 2021



Follow the story of Company X as they suffer an attack from the notorious modern ransomware family, Nefilim, and their affiliates, to learn how you can better mitigate against the common tactic and techniques used in these attacks.

By: Trend Micro June 28, 2021 Read time: (words)

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 2020, 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 extortion 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 family to demonstrate how their typical attack process occurs. The story leverages the MITRE ATT&CK Framework 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-2019-19781). 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-2017-0213). 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 Policies. 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.

```
C:\Users\User\Downloads>a2.exe
[+] Getting all settings...
[+] Creating mutex...
[+] Importing public key...
[+] Getting argument list...
[+] Starting all threads...
C:\$WinREAgent\
C:\$WinREAgent\Scratch\
C:\Documents and Settings\
```

Before starting to encrypt the files, Nefilim checks if they match its exclusion list of files and directory names. With this confirmed, Nefilim encrypts the file contents (T1486), and then replaces the original content with the encrypted version. After which it erases the encryption keys from memory and removes itself 3 seconds after, deleting its path.

```
[+] All files have been successfully encrypted!
```

Company X's CISO returns to work after a relaxing weekend to find her worst nightmare. She has been the victim of a Nefilim ransomware attack.

NEFILIM-DECRYPT.txt

```
1  All of your files have been encrypted with military grade algorithms.
2
3  We ensure that the only way to retrieve your data is with our software.
4  We will make sure you retrieve your data swiftly and securely when our demands are met.
5  Restoration of your data requires a private key which only we possess.
6  A large amount of your private files have been extracted and is kept in a secure location.
7  If you do not contact us in seven working days of the breach we will start leaking the data.
8  After you contact us we will provide you proof that your files have been extracted.
9
10 To confirm that our decryption software works email to us 2 files from random computers.
11 You will receive further instructions after you send us the test files.
12
13 jamesgonzaleswork1972@protonmail.com
14 pretty_hardjob2881@mail.com
15 dprworkjessiaeye1955@tutanota.com
```

After verifying the attack, she receives the ransom specifically tailored to her company for maximum extortion. She must now make the toughest decision of her career; does she pay the ransom? Or risk all of Company X's sensitive data being leaked and the lawsuit that will follow that?

How Could This Have Been Prevented?

When evaluating your protection against ransomware, you should start with auditing your ability to detect the impact techniques. This tactic is used to attempt to inhibit an organization's recovery ability and the techniques used are the best indicators of a potential ransomware attack. Nefilim ransomware binaries are straightforward, so general ransomware mitigation techniques would protect against this ransomware family.

The adversaries stopped services throughout the lifecycle of their attack over several weeks (T1489). These actions could be prevented with permission restrictions (M1022 & M1024) and network segmentation (M1030) techniques. The risk of an attacker seeing and interfering with critical response functions can be decreased by separating the networks that operate intrusion detection, analysis and response systems from the production environment. Critical services can be protected from interference or being disabled by attackers by restricting registry and directory permissions. Ultimately, secure account management (M1018) is important to ensure only authorized admins have access to critical services.

Organization's security teams can also consider developing disaster recovery plans for situations like a successful ransomware attack. These plans can also contain proactive processes such as routine data back-up (M1053) and testing the security of the back-up drives that can be used to recover from an attack.

These back-ups should be stored securely off the system and versioning enabled in cloud environments to make copies of the backups. However, this does not stop the stolen data from being leaked, so prevention is key with modern ransomware attacks.

The Answer to Modern Ransomware Prevention

With most organizations using multiple, separate security layers, threat information is siloed, with an endless amount of uncorrelated alerts. This results in a lack of visibility, making it extremely difficult to connect the traces of advanced ransomware attacks in time to prevent it. To stay ahead of modern attack techniques, a solution that can look across the entire environment, correlate suspicious activity, and detect critical threats with quality alerts is essential.

We have answered the challenge of modern ransomware with a purpose-built threat defense extended detection and response (XDR) solution, Trend Micro Vision One. It uses native sensors and protection points — coupled with XDR capabilities to stitch together threat activity across layers — enabling you to quickly identify complex attacks, like Nefilim ransomware, that bypass traditional prevention. This provides you with the ability to run root cause analysis, look at the execution profile, and identify the scope of the impact across your environment. With a broader perspective and better context to hunt, detect and contain threats with fewer, higher quality alerts so you can see more and respond faster.

Tactic	Technique	Observable	Mitigation	Prevention
Reconnaissance	Active Scanning: Vulnerability Scanning T1595.002	Attackers actively scan for internet-facing hosts that are vulnerable to recently disclosed exploits.	Pre-compromise M1056	This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.
Initial Access	T1133 : External Remote Services	Attackers gain initial access using valid accounts that have been exposed via services such as RDP, VPN, Citrix, or similar services.	M1042: Disable or Remove Feature or Program	Disable or block remotely available services that may be unnecessary.

M1035: Limit Access to Resource Over Network	Limit access to remote services through centrally managed concentrators such as VPNs and other managed remote access systems.			
M1032: Multi-factor Authentication	Use strong two-factor or multi-factor authentication for remote service accounts to mitigate an adversary's ability to leverage stolen credentials, but be aware of Two-Factor Authentication Interception techniques for some two-factor authentication implementations.			
M1030: Network Segmentation	Deny direct remote access to internal systems through the use of network proxies, gateways, and firewalls.			
Resource Development	T1608 -Stage Capabilities	Adversaries may upload, install, or otherwise set up capabilities that can be used during targeting.	Pre-compromise M1056	This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.

Privilege Escalation	T1068 : Exploitation for Privilege Escalation	Attackers exploit known vulnerabilities to elevate privileges to perform administrative actions or actions requiring elevated privileges	M1048: Application Isolation and Sandboxing	Make it difficult for adversaries to advance their operation through exploitation of undiscovered or unpatched vulnerabilities by using sandboxing. Other types of virtualization and application microsegmentation may also mitigate the impact of some types of exploitation. Risks of additional exploits and weaknesses in these systems may still exist.
M1038: Execution Prevention	Consider blocking the execution of known vulnerable drivers that adversaries may exploit to execute code in kernel mode. Validate driver block rules in audit mode to ensure stability prior to production deployment.			

M1050: Exploit Protection	Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. Many of these protections depend on the architecture and target application binary for compatibility and may not work for software components targeted for privilege escalation.
M1019: Threat Intelligence Program	Develop a robust cyber threat intelligence capability to determine what types and levels of threat may use software exploits and 0-days against a particular organization.
M1051: Update Software	Update software regularly by employing patch management for internal enterprise endpoints and servers.

Credential Access	T1003.001 : OS Credential Dumping: LSASS Memory	Attackers dump and use credentials to gain access to additional parts of the internal network after gaining initial access. It is also subsequently used for lateral movement. Look for evidence/artifacts indicating the use of such techniques.	M1043: Credential Access Protection	With Windows 10, Microsoft implemented new protections called Credential Guard to protect the LSA secrets that can be used to obtain credentials through forms of credential dumping. It is not configured by default and has hardware and firmware system requirements. It also does not protect against all forms of credential dumping.
M1028: Operating System Configuration	Consider disabling or restricting NTLM. Consider disabling WDigest authentication.			
M1027: Password Policies	Ensure that local administrator accounts have complex, unique passwords across all systems on the network.			
M1026: Privileged Account Management	Do not put user or admin domain accounts in the local administrator groups across systems unless they are tightly controlled, as this is often equivalent to having a local administrator account with the same password on all systems. Follow best practices for design and administration of an enterprise network to limit privileged account use across administrative tiers.			
M1025: Privileged Process Integrity	On Windows 8.1 and Windows Server 2012 R2, enable Protected Process Light for LSA.			

M1017: User Training	Limit credential overlap across accounts and systems by training users and administrators not to use the same password for multiple accounts.			
Lateral Movement	T1550: Use Alternate Authentication Material	Attackers can use Mimikatz to dump hashes, tickets, or plain text passwords.	M1026: Privileged Account Management	Limit credential overlap across systems to prevent the damage of credential compromise and reduce the adversary's ability to perform Lateral Movement between systems.
M1018: User Account Management	Enforce the principle of least-privilege. Do not allow a domain user to be in the local administrator group on multiple systems.			
T1570: Lateral Tool Transfer	Attackers can deploy tools within systems to aid in lateral movement. This includes tools such as PsExec, Bloodhound, and AdFind.	M1037: Filter Network Traffic	Consider using the host firewall to restrict file sharing communications such as SMB.	

M1031: Network Intrusion Prevention	Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware or unusual data transfer over known tools and protocols like FTP can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions.			
Discovery	T1018 Remote System Discovery	Cybercriminals can abuse tools like AdFind to collect Active Directory information and map out the infrastructure to find more targets.		This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.
T1083 - File and Directory Discovery	Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system.		This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.	
T1120 - Peripheral Device Discovery	Adversaries may attempt to gather information about attached peripheral devices and components connected to a computer system.		This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.	

T1135 - Network Share Discovery	Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement.	M1028: Operating System Configuration	Enable Windows Group Policy "Do Not Allow Anonymous Enumeration of SAM Accounts and Shares" security setting to limit users who can enumerate network shares.[36]	
Exfiltration	T1020: Automated Exfiltration	Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during Collection.		This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.
T1041: Exfiltration Over C2 Channel	Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.	M1031: Network Intrusion Prevention	Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool command and control signatures over time or construct protocols in such a way to avoid detection by common defensive tools.	

T1030: Data Transfer Size Limits	An adversary may exfiltrate data in fixed size chunks instead of whole files or limit packet sizes below certain thresholds. This approach may be used to avoid triggering network data transfer threshold alerts.	M1031: Network Intrusion Prevention	Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware can be used to mitigate activity at the network level. Signatures are often for unique indicators within protocols and may be based on the specific obfuscation technique used by a particular adversary or tool, and will likely be different across various malware families and versions. Adversaries will likely change tool command and control signatures over time or construct protocols in such a way to avoid detection by common defensive tools.
T1567: Exfiltration Over Web Services	Adversaries may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel. Popular Web services acting as an exfiltration mechanism may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to compromise. Firewall rules may also already exist to permit traffic to these services.	M1021: Restrict Web-Based Content	Web proxies can be used to enforce an external network communication policy that prevents use of unauthorized external services.

Execution	T1059 - Command and Scripting Interpreter	Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries.	M1049: Antivirus/Antimalware	Anti-virus can be used to automatically quarantine suspicious files.

M1045: Code Signing	Where possible, only permit execution of signed scripts.
M1042: Disable or Remove Feature or Program	Disable or remove any unnecessary or unused shells or interpreters.
M1038: Execution Prevention	Use application control where appropriate.
M1026: Privileged Account Management	When PowerShell is necessary, restrict PowerShell execution policy to administrators. Be aware that there are methods of bypassing the PowerShell execution policy, depending on environment configuration.

M1021: Restrict Web-Based Content	Script blocking extensions can help prevent the execution of scripts and HTA files that may commonly be used during the exploitation process. For malicious code served up through ads, adblockers can help prevent that code from executing in the first place.			
Impact	T1486 - Data Encrypted for Impact	Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources.	M1053: Data Backup	Consider implementing IT disaster recovery plans that contain procedures for regularly taking and testing data backups that can be used to restore organizational data. Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery. Consider enabling versioning in cloud environments to maintain backup copies of storage objects.
T1489 - Service Stop	Adversaries may stop or disable services on a system to render those services unavailable to legitimate users.	M1030: Network Segmentation	Operate intrusion detection, analysis, and response systems on a separate network from the production environment to lessen the chances that an adversary can see and interfere with critical response functions.	

M1022: Restrict File and Directory Permissions	Ensure proper process and file permissions are in place to inhibit adversaries from disabling or interfering with critical services.
M1024: Restrict Registry Permissions	Ensure proper registry permissions are in place to inhibit adversaries from disabling or interfering with critical services.
M1018: User Account Management	Limit privileges of user accounts and groups so that only authorized administrators can interact with service changes and service configurations.