FOX IT
part of nccgroup

TLP: AMBER

Classification
RESTRICTED

Express Attack Brief 026

Supply Chain Compromise Leads to Rhysida Ransomware Attack

Version:	**1.0**
Publication date:	**2023-06-19**
Prepared for:	**Fox-IT**

Table of contents

Document information

Document purpose

This document has been prepared for Fox-IT.

This document describes the attack path observed during a recent cyber security incident. It presents the steps taken by the threat actor, including associated Tactic, Technique, and Procedure (TTP) details. Where possible the TTPs are expressed in MITRE ATT&CK terminology to aid in correlation and cross-referencing with other threat intelligence sources.

This document is aimed at helping readers learn from the incident and prepare to defend against possible future attacks. Its attack path structure is designed to show how the latest cyber attacks actually happen in the real world. The inclusion of TTP details allows readers to map the attack steps to their own organization, validating their security posture, and feeding into their risk management process.

Document structure

Chapter 1 describes the overall attack and gives a summary of the steps taken by the threat actor.

Chapter 2 describes the attack steps in detail, including possible prevention and detection opportunities where appropriate.

Chapter 3 lists the MITRE ATT&CK TTPs observed in the attack in a convenient table format.

Document classification

This document is shared with Fox-IT as **TLP:AMBER** according to the Traffic Light Protocol (TLP). Recipients may only share this document with members of their own organization. Recipients may additionally share this document with their IT service providers for the sole purpose of validating or improving the security delivered to the recipients.

This document is classified as **RESTRICTED**. Any information published in this document is intended exclusively for Fox-IT. Any use by a party other than Fox-IT is prohibited unless explicitly granted by Fox-IT. The information contained in this document may be **RESTRICTED** in nature and fall under a pledge of secrecy.

Misuse of this document or any of its information is prohibited and will be prosecuted to the maximum penalty possible. Fox-IT cannot be held responsible for any misconduct or malicious use of this document by a third party or damage caused by its contained information.

1. Attack overview

1.1. Attack description

Timeframe	2023 Q2
Threat type	Ransomware
Sector relevance	All
Geographic relevance	

This EAB describes a cyber incident where an adversary gained initial access to the victim's network by abusing VPN credentials most likely stolen in a separate attack on a supplier. After gaining access in this relatively unusual way the adversary continued the relatively well-known ransomware playbook. They performed reconnaissance, disabled Microsoft Defender, created a scheduled task for a persistent 'Portstarter' backdoor, exfiltrated data using MegaSync and finally deployed Rhysida ransomware on the victim's virtualization infrastructure.

While the observed playbook is relatively standard the means of inital access and the use of the 'Portstarter' backdoor make this incident notable. This backdoor has previously been observed in ransomware attacks carried out by the threat actor ViceSociety. However, the use of this backdoor is not enough to establish overlap between these two groups. Information about the group behind the Rhysida ransomware is limited as of now. The group seems to be relatively new and is in the early stages of its operations, as the first attacks were only observed this May.

1.2. Attack path summary

Time	Tactic	Action	Target tech
Day 1, 06:05	Initial Access	Gain Inital Access using VPN credentials	
Day 1, 06:21	Reconnaissance	Perform reconnaissance from domain controller	
Day 2, 04:50	Defense Evasion	Disabling Microsoft Defender	
Day 2, 04:51	Persistence	Create a scheduled task for a persistent backdoor	
Day 4, 00:16	Exfiltration	Use MegaSync to exfiltrate data	
Day 8, 02:46	Impact	Deploy Rhysida ransomware	

Times of day are expressed in the primary timezone of the victim organization where our incident response activities took place.

2. Attack path

This chapter describes the attack steps in detail, including possible prevention and detection opportunities where appropriate.

2.1. Gain Inital Access using VPN credentials

Timestamp	Day 1, 06:05
Techniques	**T1199** Trusted Relationship to achieve **TA0001** Initial Access
Tools	RDP

The Adversary most likely abused VPN credentials of a supplier to gain access to the network.

On the same day that the victim was hit by ransomware one of its Suppliers was also hit by a ransomware attack. Since it was known that the supplier had VPN access to the victim's infrastructure it was hypothesized that these attacks could be related. Investigation the VPN and RDP logs confirmed that an account of the supplier was used to setup a connection with the victim's infrastructure.

How the Adversary gained access to these credentials is not known, only that multi-factor authentication (MFA) was not enforced. This made it fairly easy for the adversary to abuse them.

We are not able to provide extra insights on how the breach of the supplier took place, as we were not involved with this investigation.

Prevention

Multi-factor Authentication

Source: ATT&CK mitigation M1032 in the context of technique T1199
Use two or more pieces of evidence to authenticate to a system; such as username and password in addition to a token from a physical smart card or token generator.

Require MFA for all delegated administrator accounts. (Microsoft Threat Intelligence Center: NOBELIUM targeting delegated administrative privileges to facilitate broader attacks, 2021-10-25)

Network Segmentation

Source: ATT&CK mitigation M1030 in the context of technique T1199
Architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to contain any internet-facing services that should not be exposed from the internal network. Configure separate virtual private cloud (VPC) instances to isolate critical cloud systems.

Network segmentation can be used to isolate infrastructure components that do not require broad network access.

User Account Management

Source: ATT&CK mitigation M1018 in the context of technique T1199
Manage the creation, modification, use, and permissions associated to user accounts.

Properly manage accounts and permissions used by parties in trusted relationships to minimize potential abuse by the party and if the party is compromised by an adversary. In Office 365 environments, partner relationships and roles can be viewed under the “Partner Relationships” page. (Microsoft: Manage partner relationships, 2022-03-04)

Detection

Hard to detect

In this stage the adversary is acting no different than the user that the access was intended for. Therefore it is difficult to detect an attacker in this stage.

2.2. Perform reconnaissance from domain controller

Timestamp	Day 1, 06:21
Techniques	**T1595.001** Scanning IP Blocks to achieve **TA0043** Reconnaissance
Tools	Advanced port scanner

The Adversary performed a port scan from one of the domain controllers

Right after the VPN connection the adversary started a second RDP session using the supplier’s account. This session was setup toward one of the DC. Traces were found that during this session the following file was executed:

```
C:/Users/*REDACTED*/Downloads/Advanced_Port_Scanner_2.5.3869.exe
```

From this it was concluded that the adversary had performed network reconnaissance from a domain controller.

Prevention

Pre-compromise

Source: ATT&CK mitigation M1056 in the context of technique T1595.001
This category is used for any applicable mitigation activities that apply to techniques occurring before an adversary gains Initial Access, such as Reconnaissance and Resource Development techniques.

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.

Unrestricted program retrieval and execution

Advanced Port Scanner was not present on the DC before this incident. From this it can be concluded that the adversary retrieved this programs themselves. This should not be possible, especially on a high profile system such as a domain controller. Therefore it is recommended restrict user behaviour on systems like these.

Detection

Monitor Network Traffic Flow

Source: ATT&CK data component Network Traffic Flow in the context of technique T1595.001
Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.

2.3. Disabling Microsoft Defender

Timestamp	Day 2, 04:50
Techniques	**T1562.001** Disable or Modify Tools to achieve **TA0005** Defense Evasion
Tools	ToggleDefender

The adversary used ToggleDefender to disable Microsoft Defender

Traces where found of the execution of ToggleDefender [1]. As the name suggests this tool can be used to disable Windows Defender. The Windows Defender logs showed that a couple of minutes before this an alert was generated. This alert had the name `Trojan:Script/Wacatac.B!ml`. This was triggered because the task `C:\Windows\System32\Tasks\System` had the process `C:\Windows\System32\rundll32.exe` executing the dll `C:\Users\Public\main.dll`. Because of this Windows Defender quarantined main.dll (more information about this in the persistence section).

After the execution of ToggleDefender the Master File Table of this system showed the creation of the files: `C:\Users\Public\main.dll` and `C:\Windows\System32\Tasks\System`. Meaning that a new task was created and that main.dll was recreated. This time however no Windows Defender alerts were triggerd.

From this it can be concluded that the adversary first tried to execute something but was stopped by Windows Defender. After which the adversary disabled Windows Defender and retried their previous steps, which succeeded.

[1] https://github.com/AveYo/LeanAndMean/blob/main/ToggleDefender.bat

Prevention

Restrict Registry Permissions

Source: ATT&CK mitigation M1024 in the context of technique T1562.001
Restrict the ability to modify certain hives or keys in the Windows Registry.

Ensure proper Registry permissions are in place to prevent adversaries from disabling or interfering with security services.

Execution Prevention

Source: ATT&CK mitigation M1038 in the context of technique T1562.001
Block execution of code on a system through application control, and/or script blocking.

Use application control where appropriate, especially regarding the execution of tools outside of the organization's security policies (such as rootkit removal tools) that have been abused to impair system defenses. Ensure that only approved security applications are used and running on enterprise systems.

Detection

Monitor Command Execution

Source: ATT&CK data component Command Execution in the context of technique T1562.001
Monitor for the execution of commands and arguments associated with disabling or modification of security software processes or services such as `Set-MpPreference-DisableScriptScanning 1` in Windows,`sudo spctl --master-disable` in macOS, and `setenforce 0` in Linux. Furthermore, on Windows monitor for the execution of taskkill.exe or Net Stop commands which may deactivate antivirus software and other security systems.

Monitor Service Metadata

Source: ATT&CK data component Service Metadata in the context of technique T1562.001
Monitor for telemetry that provides context of security software services being disabled or modified. In cloud environments, monitor virtual machine logs for the status of cloud security agents.

Monitor Windows Registry Key Deletion

Source: ATT&CK data component Windows Registry Key Deletion in the context of technique T1562.001
Monitor for deletion of Windows Registry keys and/or values related to services and startup programs that correspond to security tools such as HKLM:\SOFTWARE\Microsoft\AMSI\Providers.

Monitor Windows Registry Key Modification

Source: ATT&CK data component Windows Registry Key Modification in the context of technique T1562.001
Monitor for changes made to Windows Registry keys and/or values related to services and startup programs that correspond to security tools such as HKLM:\SOFTWARE\Policies\Microsoft\Windows Defender.

2.4. Create a scheduled task for a persistent backdoor

Timestamp	Day 2, 04:51
Techniques	**T1053.005** Scheduled Task to achieve **TA0003** Persistence
Tools	Windows scheduled task

The adversary created a new scheduled task to execute their backdoor.

The file `ConsoleHost_history.txt` contains the Powershell command history entered per user. This file contained the following for one user:

```
schtasks /delete /tn System

schtasks /create /sc ONSTART /tn System /tr "rundll32 C:\Users\Public\main.dll Test" /ru
system

schtasks /run /tn System
```

These lines represent three commands that were executed. The first one deletes a scheduled task called “System”.

Secondly, a new task gets created that runs on start-up and runs `C:\Users\Public\main.dll` with rundll32. This behaviour is similar to that described in the defense evasion step.

The third one runs this newly created task. The successful creation of the task “System” is confirmed by the creation of `C:\Windows\System32\Tasks\System`. This is the location in which scheduled tasks are stored.

It appeared that the adversary was invested in this main.dll file. VirusTotal marked this file as PortStarter[2]. Portstarter is a backdoor which written in GO. Our internal malware analysts verified this and identified that this backdoor tries to setup a connection towards an external IP address. Therefore it was concluded that the adversary successfully gained persistence using the Portstarter backdoor with a scheduled task.

[2]https://www.virustotal.com/gui/file/4e73b21941b9ec81a1298f8bdd177ac8d8db0491a4f41d56c449dcb632c821fc/detection

Prevention

Difficult to prevent

Deleting, creating and running scheduled tasks is a core part of Windows. They are not inherently malicious and have a lot of legitimate use-cases. It's the implementation in which this mechanism gets abused. Therefore it is hard to prevent a scheduled task from being created. What could have prevented this was a swift and proper response into the generated alert from Windows Defender about the main.dll file.

Detection

Monitor Command Execution

Source: ATT&CK data component Command Execution in the context of technique T1053.005
Monitor executed commands and arguments for actions that could be taken to gather tasks may also be created through Windows system management tools such as Windows Management Instrumentation and PowerShell, so additional logging may need to be configured to gather the appropriate data.

Implementation 1 : New processes whose command line includes commands that create or modify scheduled tasks with a suspicious script, extension or user writable path

Detection Pseudocode

```
suspicious_processes = filter ProcessId, ProcessFilePath, command_line,
ProcessParentFilePath,ProcessParentCommandLine where (EventId == "1" OR EventId ==
"4688") AND command_line LIKE '%SCHTASKS%' AND (command_line LIKE '%/CREATE%' OR
command_line LIKE '%/CHANGE%') AND (command_line LIKE '%.cmd%' OR command_line LIKE
'%.ps1%' OR command_line LIKE '%.vbs%' OR command_line LIKE '%.py%' OR command_line LIKE
'%.js%' OR command_line LIKE '%.exe%' OR command_line LIKE '%.bat%' OR command_line LIKE
'%javascript%' OR command_line LIKE '%powershell%' OR command_line LIKE '%rundll32%' OR
command_line LIKE '%wmic%' OR command_line LIKE '%cmd%' OR command_line LIKE '%cscript%'
OR command_line LIKE '%wscript%' OR command_line LIKE '%regsvr32%' OR command_line LIKE
'%mshta%' OR command_line LIKE '%bitsadmin%' OR command_line LIKE '%certutil%' OR
command_line LIKE '%msiexec%' OR command_line LIKE '%javaw%' OR command_line LIKE '%
[%]APPDATA[%]%' OR command_line LIKE '%\\AppData\\Roaming%' OR command_line LIKE '%
[%]PUBLIC[%]%' OR command_line LIKE '%C:\\Users\\Public%' OR command_line LIKE '%
[%]ProgramData[%]%' OR command_line LIKE '%C:\\ProgramData%' OR command_line LIKE '%
[%]TEMP[%]%' OR command_line LIKE '%\\AppData\\Local\\Temp%' OR command_line LIKE '%\
\Windows\\PLA\\System%' OR command_line LIKE '%\\tasks%' OR command_line LIKE '%\
\Registration\\CRMLog%' OR command_line LIKE '%\\FxsTmp%' OR command_line LIKE '%\\spool\
\drivers\\color%' OR command_line LIKE '%\\tracing%' OR)
```

Monitor Scheduled Job Creation

Source: ATT&CK data component Scheduled Job Creation in the context of technique T1053.005
Monitor for newly constructed scheduled jobs by enabling the "Microsoft-Windows-TaskScheduler/Operational" setting within the event logging service. (Satyajit321: Scheduled Tasks History Retention settings, 2015-11-03) Several events will then be logged on scheduled task activity, including: Event ID 106 on Windows 7, Server 2008 R2 - Scheduled task registered; Event ID 4698 on Windows 10,

Server 2016 - Scheduled task created; Event ID 4700 on Windows 10, Server 2016 - Scheduled task enabled; Event ID 4701 on Windows 10, Server 2016 - Scheduled task disabled

Implementation 1 : New schedule tasks whose content includes suspicious scripts, extensions or user writable path

Detection Pseudocode

```
suspicious_scheduled_jobs = filter UserName, JobName, JobContent where EventId == "4698" AND (JobContent LIKE '%.cmd%' OR JobContent LIKE '%.ps1%' OR JobContent LIKE '%.vbs%' OR JobContent LIKE '%.py%' OR JobContent LIKE '%.js%' OR JobContent LIKE '%.exe%' OR JobContent LIKE '%.bat%' OR JobContent LIKE '%javascript%' OR JobContent LIKE '%powershell%' OR JobContent LIKE '%wmic%' OR JobContent LIKE '%rundll32%' OR JobContent LIKE '%cmd%' OR JobContent LIKE '%cscript%' OR JobContent LIKE '%wscript%' OR JobContent LIKE '%regsvr32%' OR JobContent LIKE '%mshta%' OR JobContent LIKE '%bitsadmin%' OR JobContent LIKE '%certutil%' OR JobContent LIKE '%msiexec%' OR JobContent LIKE '%javaw%' OR JobContent LIKE '%[%]APPDATA[%]%' OR JobContent LIKE '%\\AppData\\Roaming%' OR JobContent LIKE '%[%]PUBLIC[%]%' OR JobContent LIKE '%C:\\Users\\Public%' OR JobContent LIKE '%[%]ProgramData[%]%' OR JobContent LIKE '%C:\\ProgramData%' OR JobContent LIKE '%[%]TEMP[%]%' OR JobContent LIKE '%\\AppData\\Local\\Temp%' OR JobContent LIKE '%\\Windows\\PLA\\System%' OR JobContent LIKE '%\\tasks%' OR JobContent LIKE '%\\Registration\\CRMLog%' OR JobContent LIKE '%\\FxsTmp%' OR JobContent LIKE '%\\spool\\drivers\\color%' OR JobContent LIKE '%\\tracing%')
```

Detection Notes

- Detection of the creation or modification of Scheduled Tasks with a suspicious script, extension or user writable path. Attackers may create or modify Scheduled Tasks for the persistent execution of malicious code. This detection focuses at the same time on EventIDs 4688 and 1 with process creation (SCHTASKS) and EventID 4698, 4702 for Scheduled Task creation/modification event log.

2.5. Use MegaSync to exfiltrate data

Timestamp	Day 4, 00:16
Techniques	**T1567.002** Exfiltration to Cloud Storage to achieve **TA0010** Exfiltration
Tools	MegaSync

The Adversary used MegaSync to exfiltrate data

It was concluded that the adversary installed MegaSync because the folder ``C:\Users*REDACTED*\AppData\Local\Mega Limitedwas created during a session in which the adversary was active. According to theActionCenterCache``` function in Windows, MegaSync was started a couple of minutes after the folder was created and ran for 50 hours.

Adding to this are the entries in the shellbag artifact on the affected machine. This artifact contains the history of the Windows explorer. This gave the investigators insight into which locations were viewed by the adversary. In this case it appeared that the adversary was interested in at least two file servers during the time MegaSync was active.

Taking all this into account Fox-IT concluded that it is highly likely that the adversary exfiltrated data from two file servers.

Prevention

Restrict Web-Based Content

Source: ATT&CK mitigation M1021 in the context of technique T1567.002
Restrict use of certain websites, block downloads/attachments, block Javascript, restrict browser extensions, etc.

Web proxies can be used to enforce an external network communication policy that prevents use of unauthorized external services.

Detection

Monitor Network Connection Creation

Source: ATT&CK data component Network Connection Creation in the context of technique T1567.002
Monitor for newly constructed network connections to cloud services associated with abnormal or non-browser processes.

Monitor Network Traffic Flow

Source: ATT&CK data component Network Traffic Flow in the context of technique T1567.002
Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.

2.6. Deploy Rhysida ransomware

Timestamp	Day 8, 02:46
Techniques	**T1486** Data Encrypted for Impact to achieve **TA0040** Impact
Tools	Linux CLI

The adversary deployed the ransomware on the ESXi server

The investigators found a file named `123` on multiple compromised systems. This file appeared to be a Linux executable (ELF). Using SFTP the adversary was able to transfer the file `123` to the ESXi virtualization servers. Using the following commands the file was executed:

```
[root]: cd usr/share/

[root]: chmod +x 123

[root]: ./123 -d /vmfs/volumes/
```

The `/vmfs/volumes/` is the location where the storage volumes were mounted that contain the virtual machine files such as configuration files and virtual disks. This verified the investigator's suspicions that `123` is the ransomware. The malware analysis concluded that this ransomware was related to Rhysida. This was also confirmed by the ransom note that was left on the affected systems.

Ransom note:

```
Critical Breach Detected

Immediate Response Required

Dear company,
This is an automated alert from cybersecurity team Rhysida. An unfortunate situation has arisen
your digital ecosystem has been compromised, and a substantial amount of confidential data has
been exfiltrated from your network. The potential ramifications of this could be dire, including
the sale, publication, or distribution of your data to competitors or media outlets. This could
inflict significant reputational and financial damage.

However, this situation is not without a remedy. Our team has developed a unique key, specifically
designed to restore your digital security. This key represents the first and most crucial step in
recovering from this situation. To utilize this key, visit our secure portal: *REDACTED* with your
secret key *REDACTED* or write email: *REDACTED* \ *REDACTED*

It's vital to note that any attempts to decrypt the encrypted files independently could lead to
permanent data loss. We strongly advise against such actions. Time is a critical factor in mitigating
the impact of this breach. With each passing moment, the potential damage escalates. Your immediate
action and full cooperation are required to navigate this scenario effectively.

Rest assured, our team is committed to guiding you through this process. The journey to resolution
begins with the use of the unique key. Together, we can restore the security of your digital
environment.

Best regards
```

Prevention

Data Backup

Source: ATT&CK mitigation M1053 in the context of technique T1486
Take and store data backups from end user systems and critical servers. Ensure backup and storage systems are hardened and kept separate from the corporate network to prevent compromise.

Consider implementing IT disaster recovery plans that contain procedures for regularly taking and testing data backups that can be used to restore organizational data. (Ready.gov: IT Disaster Recovery Plan, 2019-03-15) 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. (Gietzen, S: S3 Ransomware Part 2: Prevention and Defense, 2021-04-14)

Detection

Monitor File Creation

Source: ATT&CK data component File Creation in the context of technique T1486
Monitor for newly constructed files in user directories.

Monitor File Modification

Source: ATT&CK data component File Modification in the context of technique T1486
Monitor for changes made to files in user directories.

Monitor Network Share Access

Source: ATT&CK data component Network Share Access in the context of technique T1486
Monitor for unexpected network shares being accessed on target systems or on large numbers of systems.

3. MITRE ATT&CK TTPs

This chapter lists the MITRE ATT&CK Tactics, Techniques, and Procedures (TTPs) of the attack described in this report. The TTPs are listed in the order they were observed in the attack. They are formatted in a table to facilitate ingestion of this data into other tools, such as Threat Intelligence Platforms (TIPs).

Note that each tactic-technique-procedure combination is listed here, which can lead to apparent duplication. For example, if a procedure is linked to more than one technique, it will be listed repeatedly for each technique.

Tactic	Technique	Procedure
TA0001 Initial Access	**T1199** Trusted Relationship	The Adversary most likely abused VPN credentials of a supplier to gain access to the network.
TA0043 Reconnaissance	**T1595.001** Scanning IP Blocks	The Adversary performed a port scan from one of the domain controllers
TA0005 Defense Evasion	**T1562.001** Disable or Modify Tools	The adversary used ToggleDefender to disable Microsoft Defender
TA0003 Persistence	**T1053.005** Scheduled Task	The adversary created a new scheduled task to execute their backdoor.
TA0010 Exfiltration	**T1567.002** Exfiltration to Cloud Storage	The Adversary used MegaSync to exfiltrate data
TA0040 Impact	**T1486** Data Encrypted for Impact	The adversary deployed the ransomware on the ESXi server