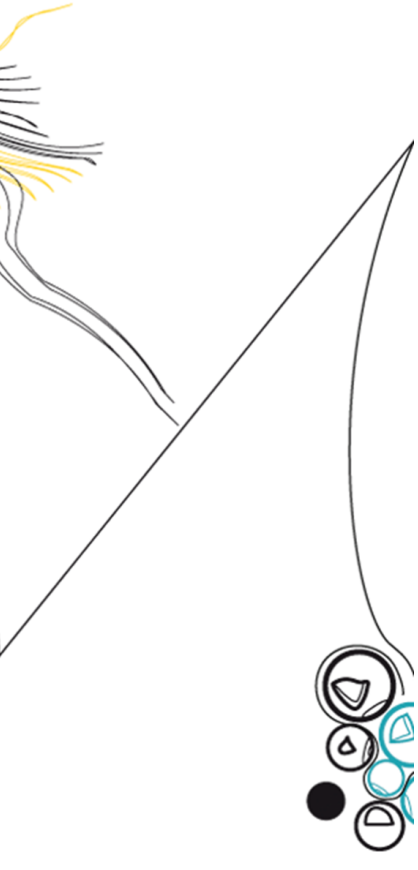
UNIVERSITY OF TWENTE.

**Faculty of Electrical Engineering,**
**Mathematics & Computer Science**

# How can the eradication phase of incident response for ransomware incidents be improved based on previous ransomware incidents?

**Romeo S. Dijkstra**

**M.Sc. Thesis**
**December 2022**



**Supervisors:**
dr. J. van der Ham
dr. ir. A. Continella

DACS and SCS
Faculty of Electrical Engineering,
Mathematics and Computer Science
University of Twente
P.O. Box 217
7500 AE Enschede
The Netherlands

# Abstract

In recent years, an increase in ransomware incidents against critical infrastructure has been observed globally [1]. Computer Emergency Response Teams (CERTs) are asked for help to recover from these ransomware incidents. Their goal is to get a victim back to business as securely and fast as possible and do this by performing incident response. During this process, they investigate the incident's root cause and try to eradicate the ransomware attack's remnants. However, the current guidelines for eradication do not provide enough guidance. For example, the NIST SP 800-61 standard does not describe the eradication process, and MITRE provides too much information, which can lead to overhead. This overhead can slows down the eradication process. This leads to the victim getting back to business slower, which is not wanted. In this research, we created a method that uses the data gathered by a CERT to improve the eradication phase of ransomware by generating mappings which will give guidance based on previous ransomware incidents. First, we use the information gathered by a CERT and store it in the open-source threat intel-sharing platform MISP [2]. Then, we map the information in MISP onto the MITRE ATT&CK framework [3], which is is a knowledge base of adversary *Tactics* and *Techniques* based on real-world observations. Next, we generate mappings with the information about the *Techniques* used during previous ransomware incidents. We used 18 reports provided by the Northwave CERT to generate mappings. Due to the limited time and data, the impact of our model could not be validated, but we think the mappings show great potential. The mappings give insight into previous ransomware incidents and can be used to make informed decisions about how to quickly and securely eradicate a ransomware incident and get a company back to business. This will be the guidance given, and we believe this will improve the eradication phase of ransomware incidents.

# Acknowledgements

First, I would like to thank my supervisors, Roland Middelweerd from the Northwave CERT, Jeroen van der Ham from the DACS group of the University of Twente and Andrea Continella from the SCS group of the University of Twente for providing me with feedback and guidance during my graduation. Your help helped me put together this research. Secondly, I would like to thank all my colleagues at Northwave for making my graduation process an enjoyable experience.

This research would not have been possible without the data provided by Northwave; therefore, I want to thank them.

Finally, I thank my family and friends for their support. Without your support, I would not have been able to do this.

# Contents

# Chapter 1

# Introduction

In 2021, the cyber security authorities of the United States, Australia and the United Kingdom observed an increase in high-impact ransomware incidents [1]. These ransomware incidents disrupt the daily operations of companies. This causes them to lose time and money. A way to recover from these incidents is to follow an incident response plan. These plans describe the steps that need to be taken during, for example, a ransomware incident to recover from it. A Computer Emergency Response Team (CERT) can help companies with incident response. A CERT usually works with an *incident response* plan and can be part of the same company or could be a commercial CERT. Guidelines for an incident response plan are described in the NIST SP 800-61 standard. The NIST standard describes all kinds of steps that need to be taken in order to recover from a cyber incident, such as ransomware. One of the steps taken is *eradication*. Eradication means *the process of getting rid of something completely or of destroying something bad*, according to the Cambridge dictionary [4]. Sadly, the NIST SP 800-61 standard states *Because eradication and recovery actions are typically OS or application-specific, detailed recommendations and advice regarding them are outside the scope of this document*.

The missing recommendations and advice regarding eradication could be solved by looking at publicly available threat intel, such as the *Software* framework from MITRE [5]. They map attack techniques used by specific types of software, like ransomware. However, this mapping consists of all the observed attack techniques used by a type of ransomware. This results in a lot of overhead eradication options and extra work for a CERT if they need to consider all the observed attack techniques. This extra work costs time and money for the victim.

The Northwave CERT is a CERT that also observed the lack of detail in the NIST SP 800-61 standard. The Northwave CERT is a commercial CERT and is part of Northwave, a Dutch cyber security company in the Netherlands, Germany, and Belgium. The Northwave CERT responds to incidents all over Europe and has assisted companies in dealing with hundreds of ransomware attacks over the last few years [6]. This means they have access to data about ransomware incidents. This research aims to use data about past ransomware incidents and determine if we can improve the *eradication* phase with it. Therefore, we came up with our main research question:

> *How can the eradication phase of incident response for ransomware incidents be improved based on previous ransomware incidents?*

The improvement is described by getting insights into what happens during ransomware attacks and using the insight to eradicate ransomware faster. As said earlier, eradication is about getting rid of something bad. In this case, the ransomware and everything it left behind. Therefore it is essential to get a good overview of which attack techniques a threat actor or ransomware strain used to determine what was left behind. The Northwave CERT gathers this information when they investigate a ransomware incident. A framework that describes the attack techniques used during an attack is the MITRE ATT&CK framework. To answer our main research question, we came up with three sub-questions:

1. *Which Techniques from the MITRE ATT&CK framework are used during a ransomware attack?*
2. *Which Techniques from the MITRE ATT&CK framework are used per ransomware strain?*
3. *What is the correlation between Techniques from the MITRE ATT&CK framework during all studied ransomware incidents?*

We are using the answers to these questions to generate mappings representing techniques used during a ransomware incident. Using these mappings, we will answer our main research question by giving more insights into what happens during ransomware attacks.

Validating if our method improves the eradication phase would take too much time. We explained this in chapter 6, where we also suggest a validation method.

# Chapter 2

# Background and Related Work

In this chapter, we will have a look at different subjects. These subjects need to be comprehended for this research. In section 2.1 ransomware, the different types of ransomware and the structure of a ransomware attack are explained. Section 2.2 explains how one can respond to a cyber attack, such as ransomware, using an incident response plan. We dive deeper into the incident response plan of NIST. In section 2.3, we discuss computer emergency response teams and look at the incident response performed by the Northwave CERT. In section 2.4, we look at the MITRE ATT&CK framework and the MITRE Software mappings. We end this chapter in section 2.5 by looking at MISP and why it is so valuable.

## 2.1 Ransomware

The term ransomware is a combination of the words malware and ransom. Malware, also known as malicious software, is designed to cause harm. This harm can be to computer systems or in the form of leaking information. The meaning of ransom is: *the redemption of a prisoner or kidnapped person, of captured goods, etc., for a price* [7]. Ransomware is a form of malware that makes a system unusable and demands money to make it usable again. It is increasingly used by criminals to generate revenue through extortion [8].

Different types of ransomware exist [9]. *Crypto ransomware* encrypts a system's files and data, making it only accessible by using the decryption key. Usually, the decryption key can be bought from the threat actors. *Lockers* completely lock your system, making it unusable. Usually, a lock screen is displayed with a ransom demand. *Scareware* or *Leakware* aims to scare the user of a system with a notification, usually about a virus being detected on the system. It asks for money to resolve the usually fake issue. Another example is threatening to spread sensitive information if a ransom is not paid. *Ransomware-as-a-service* (*RaaS*) is derived from Software-

as-a-service (*SaaS*), a business model to deliver software on a subscription basis. *RaaS* is a business model between ransomware operators and affiliates in which affiliates pay to launch ransomware attacks developed by operators [10]. It allows one that does not have the skills to develop and maintain their own ransomware to take part in the ransomware business. *RaaS* is usually a combination of *Crypto ransomware* and *Leakware*. *RaaS* is the type of ransomware mostly observed by the Northwave CERT in different, so-called ransomware strains.

### 2.1.1 Ransomware attack structure

A ransomware attack consists of three phases called *In*, *Through* and *Out* [6]. In figure 2.1, we can see the actions taken by a threat actor during ransomware attacks observed by the Northwave CERT.

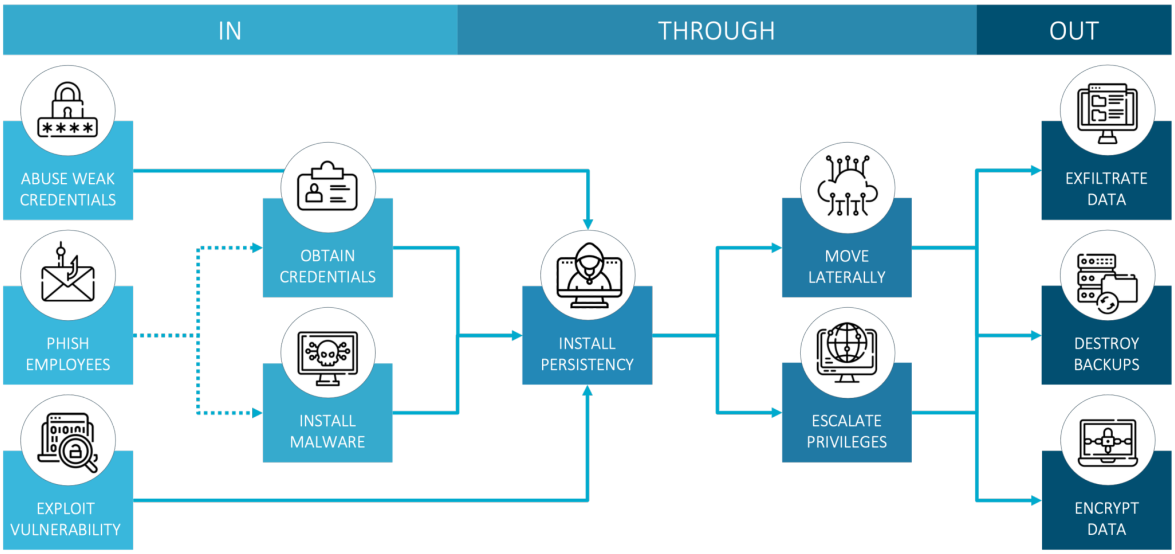



**Figure 2.1:** Phases of a ransomware attack found by Northwave [6]

The *In* phase consists of the activities taken by threat actors to gain initial access to an IT environment [6]. In the *Through* phase, the Northwave CERT observes three activities in parallel, *Install persistency*, *Move laterally* and *Escalate privileges*. With these three activities, the threat actor wants to ensure *that they do not lose their grip on the environment when their victim discovers one of their backdoors*, *to obtain an overview of the network* and to *to obtain complete control of the environment* [6]. Finally, the last phase, *Out*, is used to obtain *leverage over the victim for extortion* [6]. The Northwave CERT observed that this is usually done by exfiltrating data, destroying the backups and encrypting the data.

### 2.1.2 Ransomware role model

The activities described in section 2.1.1 are performed by different roles within a ransomware attack [11]. Northwave created a framework which shows the seven distinct roles within a ransomware attack. This framework can be seen in figure 2.2

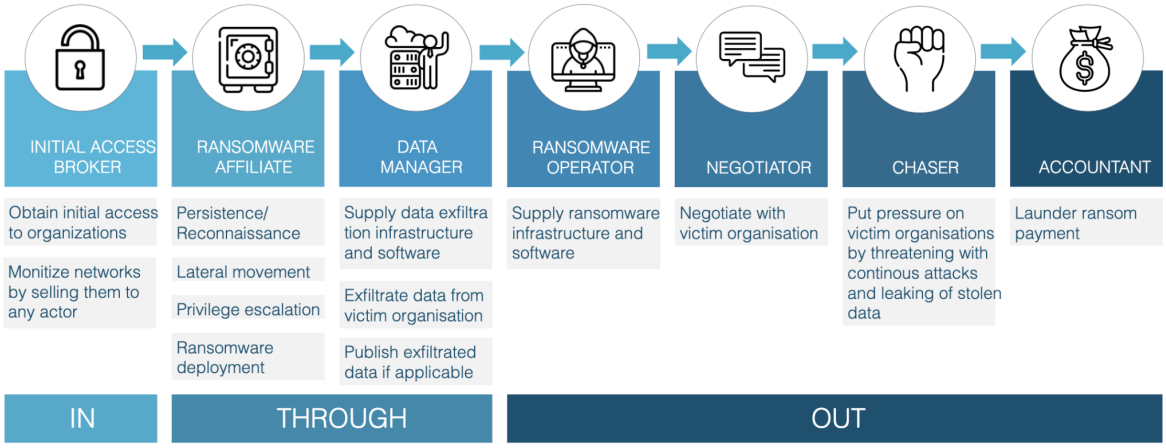



**Figure 2.2:** The ransomware role model created by Northwave [11]

Northwave observed that different threat actors frequently carry out different roles. For example, the initial access broker uses different attack techniques and often, there is a period of silence between the initial access and further activity. Northwave believes this happens because the initial access brokers are selling their access to ransomware affiliates [11].

Chasers are usually not part of the ransomware affiliates group and often do not know the status of negotiations [11]. Instead, their goal is to pressure the victim and threaten to leak stolen data, so the ransomware affiliates get paid.

### 2.1.3 Double extortion

Next to encrypting systems, data stealing is a method observed in recent years called *double extortion*. For example, suppose the victim does not want to pay because they have backups of the data that is encrypted. In that case, the threat actor threatens to leak sensitive company data, such as employee records or intellectual property. Microsoft states in their digital defence report of 2022 that double extortion has become standard practice [12] and show in their digital defence report of 2021 a chat with threat actor Conti stating leaking of data which can be seen in figure 2.3.

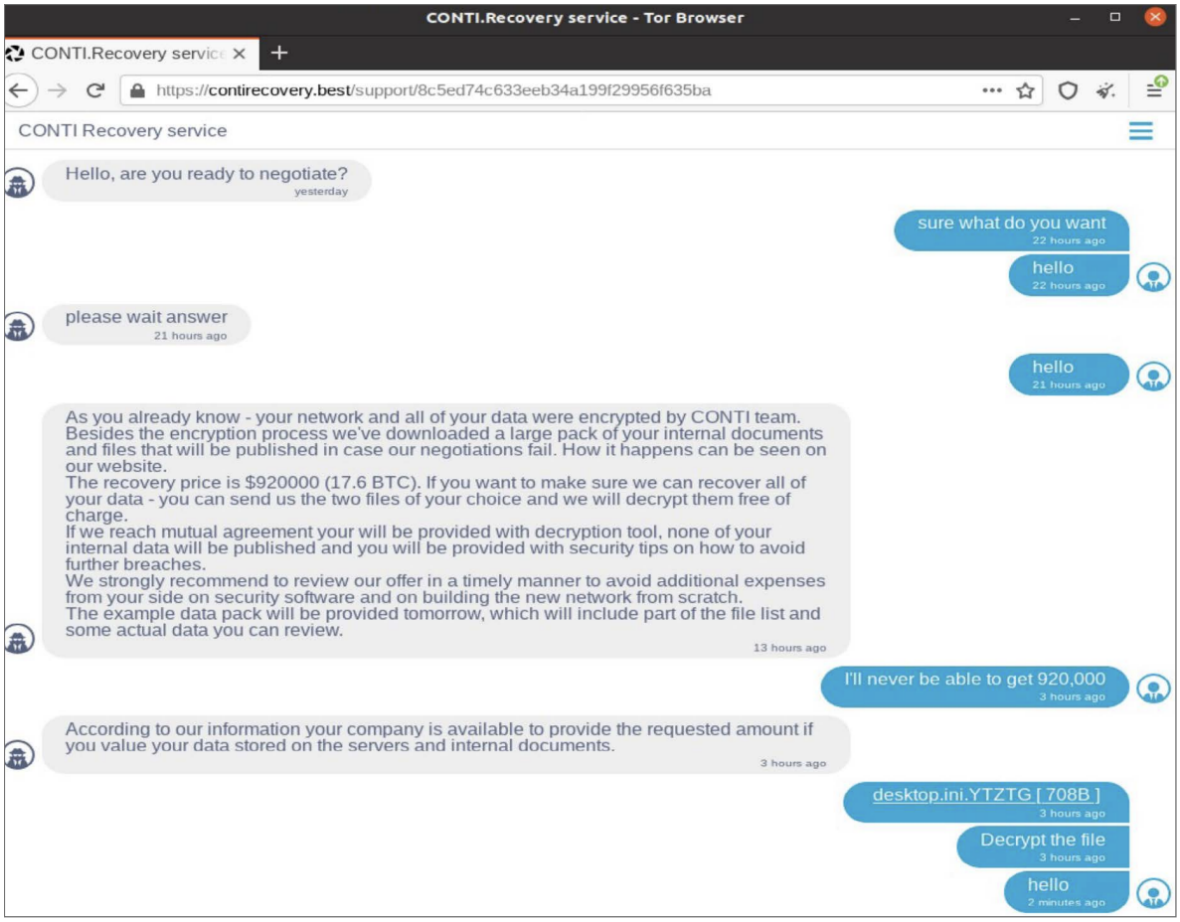



**Figure 2.3:** Chat session following ransom note upload with Conti [13]

## 2.2 Incident Response

An incident is an event that is either unpleasant or unusual [14]. An incident for a company can disrupt daily operations. An incident can happen physically, like a fire, or virtually, such as a ransomware attack. Both types of incidents can significantly impact the daily operations of a company and could lead to reputation damage or loss of money. *Incident response* is a term used to describe how one responds to an incident. In this research, we will focus on the *incident response* process for a ransomware incident. Multiple standards describe the incident response process for cyber incidents, such as the NIST SP 800-61 standard [15] and the ISO/IEC 27035 [16]. However, we will focus on the NIST SP 800-61 standard. The NIST standard is freely accessible, defines what they think a response should look like and is more technical [17]. The NIST SP 800-61 is also used by the Northwave CERT.

### 2.2.1 NIST SP 800-61

NIST describes an incident response process for computer security incidents in the NIST SP 800-61 standard, *Computer Security Incident Handling Guide*. NIST stands for National Institute of Standards and Technology and is part of the government of the United States. NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems [15]. The guide describes three parts. First, *Organising a Computer Security Incident Response Capability* discusses the need for a clear definition of an incident, what services the incident response team should provide and the importance of the right plans, policies and procedures. Second, *Handling an Incident* focuses on the several phases of incident response. Finally, the chapter *Coordination and Information Sharing* discusses the importance of information sharing and how it can *strengthen the organisation's ability to respond to IT incidents effectively* [15].

### Handling an Incident

*Handling an Incident* focuses on the several phases of incident response, or as they call it, the *Incident Response Life cycle* [15]. The *Incident Response Life cycle* can be seen in figure 2.4.

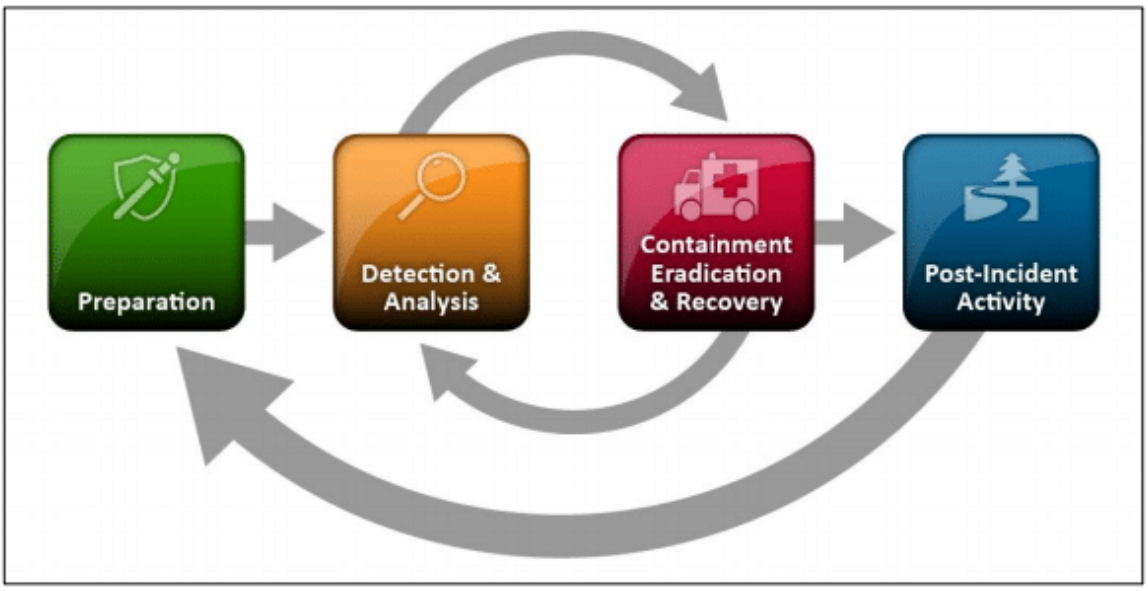



**Figure 2.4:** Incident Response Life Cycle [15]

The *Preparation* phase provides basic advice on preparing to handle cyber incidents and preventing them [15]. It discusses the need for *incident handler communications and facilities*, *incident analysis hardware and software*, *incident analysis resources* and *incident mitigation software*. Examples are the need for a secure storage facility, digital forensic workstations to save relevant incident data such as logs or disk images, network diagrams, a list of critical assets and access to clean operating system images for recovery purposes. It also states the importance of preventing a cyber incident using, for example, risk assessments and user awareness and training [15].

The *Detection & analysis* phase explains the importance of being generally prepared to handle any incident, but the focus should rely on common attack vectors [15]. It discusses how the most challenging part of the incident response process is accurately detecting an incident and how it can be detected.

During this research, we will focus on the *Containment, eradication & recovery* phase because we are looking into the eradication phase. *Containment* is the actions required to prevent the incident from spreading across the network. NIST says *eradication* may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and

mitigating all exploited vulnerabilities. During eradication, it is important to identify all affected hosts within the organisation so they can be remediated [15].

In the *Post-incident activity* phase, NIST describes a lessons learned section with questions such as *what happened exactly?* and *what information was needed sooner?*. They also suggest collecting data about the incident and a checklist. This checklist can be found in the *Computer Security Incident Handling Guide* [15].

For this research, we will be looking primarily at the *eradication* phase of the *Containment, eradication and recovery* section of the *Handling an incident* section. NIST describes eradication as the phase where it may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited [18]. However, it ends the *Eradication and Recovery* section by saying *Because eradication and recovery actions are typically OS or application-specific, detailed recommendations and advice regarding them are outside the scope of this document* [18].

## 2.3 Computer Emergency Response Team

A Computer Emergency Response Team (CERT) is a group of people who work on computer-related incidents and help to recover from these incidents. These incidents can be Distributed-Denial-of-Service (DDoS) attacks, data breaches or ransomware attacks. A CERT can best be described by the analogy of a fire department [19]. They respond quickly to cyber incidents, just like the fire department responds quickly to fires. They help a victim by minimising damage and removing the threat, just like the fire department trying to minimise the spread of fire and put out the fire. A CERT tries to minimise the impact of ransomware by performing *incident response* steps explained in section 2.2.

There are different types of CERTs. A CERT can be a team within a company, only working for that company. An example of this could be the CERT of the University of Twente [20]. A CERT could also be nationwide. For example, the National Cyber Security Centre (NCSC) fulfils that role within the Netherlands [21]. There is also a type of CERT that helps a specific sector. For example, Z-CERT [22] helps hospitals and other healthcare institutions in the Netherlands. Finally, there are also commercial CERTs. Its primary purpose is to be deployed to help other companies with their cyber security incidents. An example of this could be the Northwave CERT [23].

### 2.3.1 Incident response by Northwave CERT

The incident response process performed by the Northwave CERT is based on the NIST SP 800-61 standard, but they also added steps to help organisations to better respond to a cyber incident. Their mission is to help organisations to *get back to business as usual, as quickly and securely as possible*. The current eradication phase of the Northwave CERT is a tailored process where an extensive scope is used to achieve the *securely as possible* part of their mission. They prefer to check more than may be necessary to ensure no remnants of the ransomware are left behind. However, it is unclear if this process is *as quickly as possible* and can be improved. They use the *Indicators of Compromise* (IoCs) found during the Root Cause Analysis to decide the eradication steps. Root cause analysis (RCA) is a problem-solving method used to identify the root causes of faults or problems [24].

In the Northwave CERT's last phase of the incident response process, they implement their Endpoint Detection & Response Service (EDRS) and add IoCs found during the Root Cause analysis. The Northwave CERT also deploys behaviour-based detection, which triggers on suspicious activities. This gets monitored 24 hours a day, seven days per week by their Security Operations Centre (SOC). The SOC could help in the exceptional case when an IoC is missed during the eradication phase. This ensures that the eradication phase is performed as securely as possible.

## 2.4 MITRE

In this section, we will describe two parts of MITRE ATT&CK relevant to this research. MITRE is an American non-profit organisation which does research and development for the American government for the past 60 years. MITRE is also the founder of the Common Vulnerabilities and Exposures (CVE) system [25].

### 2.4.1 MITRE ATT&CK Framework

ATT&CK is a framework designed by MITRE. It was created out of a need to document adversary behaviours for use within a MITRE research project [3].

The framework is a knowledge base of adversary *Tactics* and *Techniques* based on real-world observations. *Tactics* represent the *why* of an ATT&CK *Technique* or sub-*Technique*, the reason for performing an action. For example, an adversary may want to achieve credential access. *Techniques* represent *how* an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access [26].

The framework lists 14 *Tactics* and 193 *Techniques* with 401 sub-*Techniques*. Each *Techniques* contains a detailed description, examples, mitigation and detection methods. A small snippet of the framework can be seen in figure 2.5.

During this research, we will map threat actor behaviour onto the MITRE ATT&CK framework. This allows us to document the threat actor's behaviour and analyse it further.

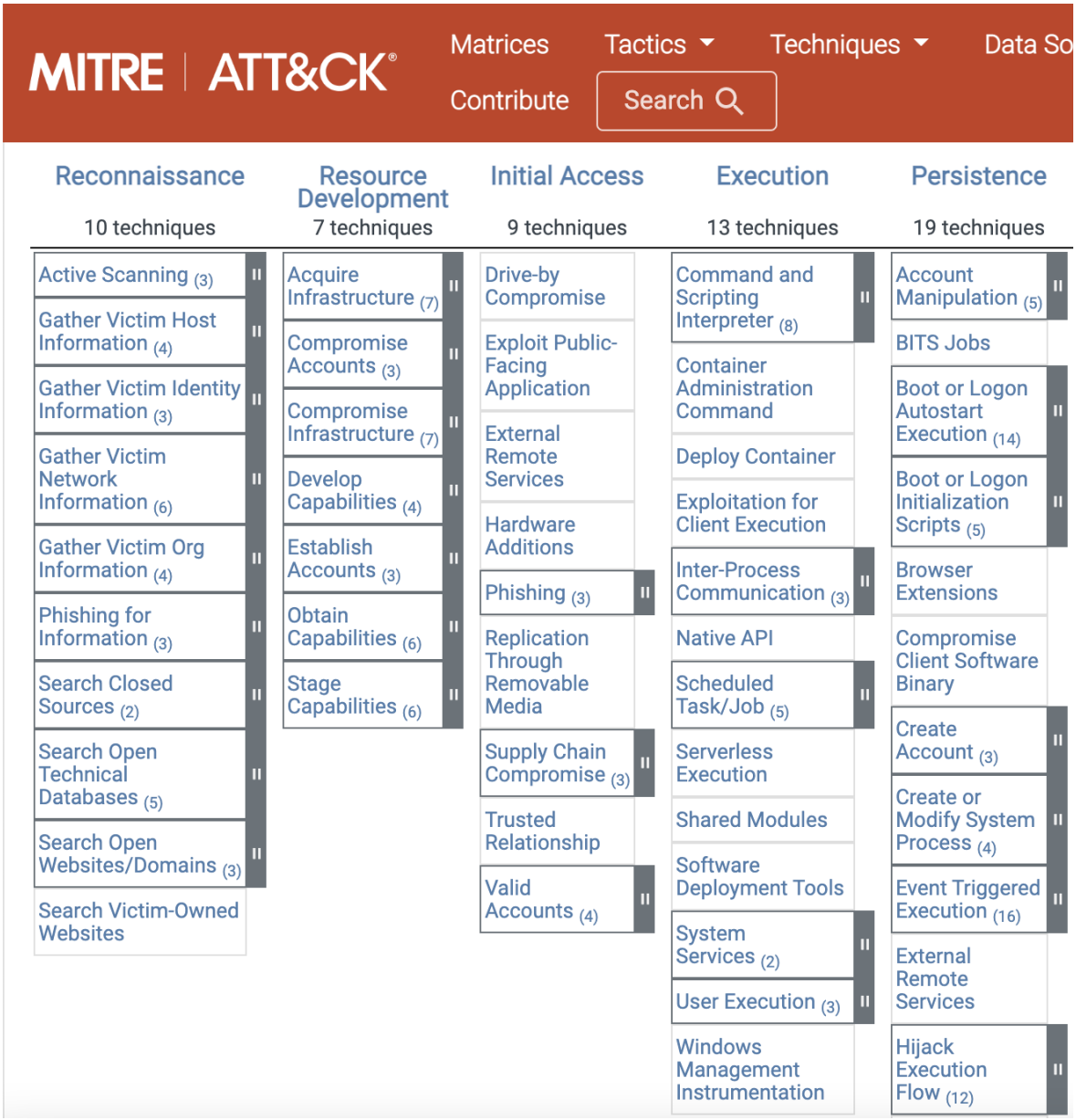



**Figure 2.5:** Part of the MITRE ATT&CK framework

### 2.4.2 MITRE ATT&CK Software

MITRE also developed *Software*, a term used to describe code or tools whose behaviour is modelled by the MITRE ATT&CK framework [5]. *Software* by MITRE is a list that shows all the *Techniques* used by a specific type of software without indicating how often a *Technique* is used. Indicating how often a *Technique* is used is needed to prevent overhead, better understand what happens and prevent time loss during the eradication phase. *RaaS* from threat actors such as Conti is described [27]. Conti is a *RaaS* and has not been observed since June 2022 [28] [29]. More recently, active threat actors, such as BlackCat [30], are not yet described.

## 2.5 MISP

MISP is an open-source threat intel-sharing platform. It can collect, store, distribute and share cyber security indicators and threats about cyber security incidents analysis and malware analysis. MISP is designed by and for incident analysts, security and ICT professionals or malware reversers to support their day-to-day operations to share structured information efficiently [2] [31].

In this research, MISP will be used for organising the data of previous ransomware incidents provided by the Northwave CERT. All the information about past ransomware incidents handled by the Northwave CERT is written down in PDF reports. This makes the data hard to analyse and find connections between cases. MISP will be used to structure this data and make it more manageable to analyse.

Information about an incident will be put in a MISP *event*. An example event can be seen in figure 2.6. All the IoCs can be added to an event and connected to a *galaxy*. A galaxy is a collection of data. In this research, two galaxy types will be used, MITRE ATT&CK and a *galaxy* describing the different ransomware strains. This information can later be used to group information about ransomware strains.

MISP also has An application programming interface (API) which will be used during this research to retrieve the information from MISP and process the data set. Other functions of MISP are information sharing between companies where one can precisely manage which IoCs will be shared and with how much detail. Correlations can also be generated in MISP. However, no overview of all *Techniques* is given and filtering on Events to be shown is not possible.

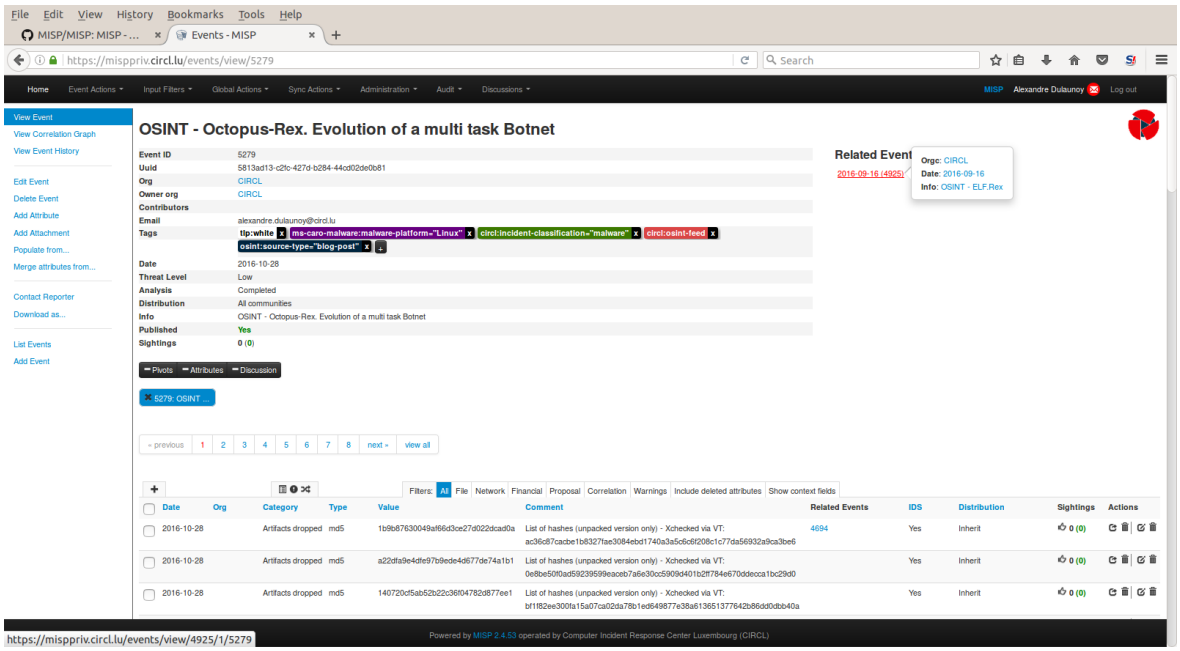



**Figure 2.6:** Example of an event in MISP [2]

# Chapter 3

# Approach

In this chapter, we will discuss the current problem, the research question we will use to try to solve this problem and the methodology to tackle the research question. This research is performed during an internship at the Northwave CERT. This means we have access to the data of previous ransomware incidents handled by the Northwave CERT.

## 3.1 Problem statement

The NIST 800-61 standard describes the eradication phase abstractly. The standard only provides guidelines and states that specific eradication steps are out of scope. Therefore, it is unclear how the eradication phase for ransomware incidents can be performed. The MITRE ATT&CK Software framework tries to tackle this problem by listing *Techniques* used by certain ransomware strains. However, no indication of the likeliness of a *Technique* is given. This limits its usefulness for the eradication phase because it can result in an overhead of *Techniques* that must be eradicated. Performing too much eradication will cost more time and money for the victim company. When too little eradication is performed, the threat actor could come back and perform another attack. With this research, we will develop a method which gives more structure and guidance to the eradication phase.

## 3.2 Research question

Based on the problem statement, we came up with the main research question we want to answer during this research:

> *How can the eradication phase of incident response for ransomware incidents be improved based on previous ransomware incidents?*

To answer this question, we also need to answer three sub-questions:

1. *Which Techniques from the MITRE ATT&CK framework are used during a ransomware attack?*
2. *Which Techniques from the MITRE ATT&CK framework are used per ransomware strain?*
3. *What is the correlation between Techniques from the MITRE ATT&CK framework during all studied ransomware incidents?*

## 3.3 Methodology

This section will describe the steps taken during this research to answer the main research question and the three sub-questions.

### 3.3.1 Research question 1 - MITRE ATT&CK Techniques

To answer the first question, we need to perform multiple steps. These steps are described in this section.

#### Collecting data

For this research question, a data set is used containing ransomware cases. We especially need information about the ransomware attack's root cause and cleaning process. This information is required to answer the sub-questions.

The data set consists of reports from ransomware incidents handled by Northwave CERT. These reports contain information about the incident, such as the root cause analysis and how Northwave responded to that incident. The response is described in a way derived from the NIST 800-61 standard.

We will need to check whether a report is suitable for the research. To determine if a report is suitable, we will be looking at three criteria:

- Does the report describe a ransomware attack?
- Does the report describe the root cause analysis (RCA)?
- Does the report describe a documented eradication process?

If these three criteria are met, the report will be added to the data used to create the data set. If a report does not meet all requirements, it will not be used for this research. For example, the reports that are not added could be about other incidents, such as Business Email Compromise (BEC).

#### Creating the data set

Once we have a list of all the data used to create the data set, we will manually add the information from the reports to MISP to build the data set. MISP will be used to create the data set because it offers a structured way to register information about incidents.

The data set in MISP will consist of basic incident information, such as the country and sector of the victim and the attack patterns used by the threat actors during the ransomware attack, which correspond to the MITRE ATT&CK framework.

#### Processing the data set

In the previous step, we structured the selected reports. Based on this data, we can generate the mapping based on our data set. The outcome will be a mapping showing the number of times a MITRE ATT&CK *Technique* is used during the ransomware attacks based on our data set.

### 3.3.2 Research question 2 - MITRE ATT&CK Techniques per strain

Once all the selected data is in MISP, we must extract each ransomware strain. Then, for each available strain, we will generate a mapping of the MITRE ATT&CK framework to show the *Techniques* used. These mapping will show the number of times a ransomware strain uses a *Technique* based on our selected reports.

### 3.3.3 Research question 3 - MITRE ATT&CK Techniques correlation

Once all the selected data is in MISP, we need to list the *Techniques* and determine the likelihood of another *Technique* being used together. We will generate a correlation matrix from this information to show the correlations.

### 3.3.4 Main research question - Improving the eradication phase

With the mappings generated from each sub-question, we will show how much information is gathered during a ransomware incident and how much insight can be created from previous ransomware incidents. Finally, we will use this information to create a method that explains how these insights can be generated and how they can be used to improve the eradication phase.

# Chapter 4

# Hypothesis

We hypothesize that we can improve the eradication phase of incident response for ransomware incidents by keeping track of information about a ransomware incident, such as ransomware strain and the IoCs. We map the IoCs onto the *Techniques* of the MITRE ATT&CK framework. From this, we can generate different types of mappings which show information about the *Techniques* used, usage per ransomware strain and the correlation between *Techniques*. These mappings give an overview which can be used during the eradication phase, which can be used to get more structure and guidance instead of eradicating everything or based on feeling, which is not very reliable.

The information found during the incident needs to be put in MISP to improve the mappings further. A Security Operation Center (SOC) can also help improve the mappings. If a part was missed during the eradication phase, it could still be detected by the SOC, and thus the mappings can be updated again if the new information is stored in MISP. One remark has to be made about the addition of the SOC. It must be determined if the current or a new incident causes the alarm. Since this has never happened before, this must be decided per alarm.

We hypothesize that the method we propose is cyclical and can be repeated each incident, thus further improving the mappings. However, we suspect it will not be easy to measure improvement because many variables come into play. Furthermore, the improvement of our method needs to be assessed by applying it to an extensive set of ransomware incidents because every ransomware case is different. However, we think that our method will improve eradication because it will give insight into what has happened during previous ransomware incidents. Therefore we think it will give more guidance and structure during the eradication phase.

# Chapter 5

# Results

In this chapter, we will present the results of each sub-question and finish with the results for our main research question.

## 5.1 Research question 1 - MITRE ATT&CK Techniques

In this chapter, we are describing the results we found for our first research questions,

> *Which Techniques from the MITRE ATT&CK framework are used during a ransomware attack?*

We divided this question into three steps, collecting data, creating the data set, and processing the data set.

### 5.1.1 Collecting data

We started with creating an overview of all the cases handled by the Northwave CERT. For each criterion we specified in section 3.3.1, we needed to make requirements to test if a report matched the criteria. We made a script to classify each report on the requirements. Through iteration, we refined the requirements, which resulted in a list of reports we could use for our research. However, the script could not determine the usability of the reports. It can only check if specific requirements of criteria are present. It resulted in too many reports for this research due to time constraints. Together with experts from Northwave, we made a more critical selection. In this selection process, we looked at the level of detail of the root cause. When the initial access and the steps taken by the threat actor could be determined and were clearly described, we added the report to the list. If a root cause analysis contains more details and is more complete, we would better understand the *Techniques* used. This process resulted in 18 reports that we used during this research.

### 5.1.2 Creating the data set

After the previous step, we have the data to create the data set. First, however, we need an effective way to use the data because it is still in PDF reports. As described in section 2.5, MISP is a tool that can structure an incident's findings. In MISP, we stored all the IoCs found during the root cause analysis of a given incident. Then, we manually mapped each IoC onto the MITRE ATT&CK framework. The result was 18 structured reports in MISP, which enabled us to process the reports in the next step.

### 5.1.3 Processing the data set

In the previous step, we structured the selected reports. This allows us to process the data to answer our first research question. Using the MISP API, PyMISP [32]

and Jupyter Notebook [33], we made a script that gathers the data from MISP [34]. For the first question, we want to know all the *Techniques* used during the ransomware incidents from the selected reports. We gathered all *universally unique identifier*s (UUID)s of each incident in MISP. MISP has a feature where the MITRE ATT&CK *Techniques* of an incident can be mapped onto the MITRE ATT&CK framework based on the provided UUIDs. The result can be seen in figure 5.1. This result gives a clear overview of *Techniques* used by the threat actors in our data set. It also gives a small insight into which *Techniques* we have not seen. This could result from the *Technique* not being in the data set, threat actors not using the *Technique* or the Northwave CERT unable to detect the *Technique*.

### 5.1.4 Mapping

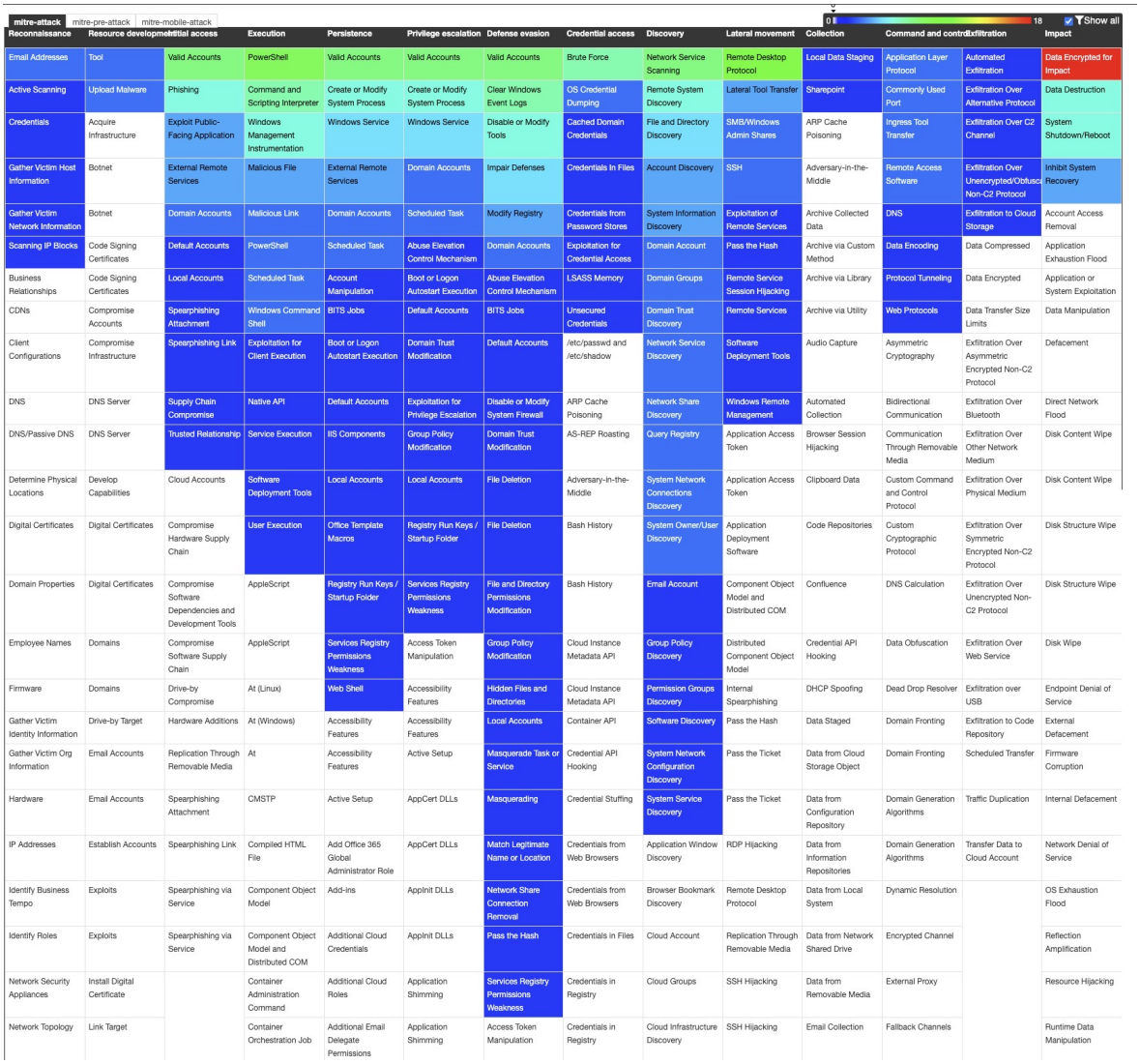
Figure 5.1 shows a screenshot of the interactive mapping based on our data set. The actual version is an interactive page within MISP showing the occurrence of each *Technique* and its explanation. Each column title shows a different *Tactic* of the MITRE ATT&CK framework [35]. In addition, each column contains MITRE ATT&CK *Techniques* linked to the *Tactic*. The scale goes from white, purple, blue, green, and yellow to red. White being never used, purple being once and towards yellow means used more, with red being used the most. Also, the higher a *Techniques* is within a column, the more it is used. We first observe the variety of *Techniques* used during different ransomware incidents.

The column with the most MITRE ATT&CK *Techniques* used is *Defense evasion*. This means it is something to look out for during the eradication phase. That *Defense evasion* is seen often can happen because of multiple reasons. First, the *Defense evasion Tactic* contains the most *Techniques*, including *sub-Techniques*. Because of the wide variety of *Techniques*, it could be the most seen. Secondly, the Northwave CERT could be good at finding *Defense evasion Techniques* during the Root Cause Analysis. Alternatively, the threat actors could be bad at hiding their *Defense evasion Techniques*. Based on the mapping of our data set, it is something to look out for and eradicate because it occurs a lot.

The column with the least amount of items is *Collection*. This can happen because of multiple reasons. First, the Northwave CERT could be less good at finding *Collection Techniques* during the Root Cause Analysis. Alternatively, the threat actors could be good at hiding their *Collection Techniques*. Based on this result, we cannot say, *the eradication of Collection can have less priority because it occurs less*. Less occurrence does not make it less critical to eradicate when it occurs. With these mappings, we show occurrences to give guidance based on what has happened before.

It can be observed *Data Encryption for Impact* is red, meaning it happens the most. In this case, it happened in all 18 cases in our data set. This is a result we expect because we are looking at ransomware, which core component is encrypting data for impact. In contrast with our previous paragraph, this result means eradicating the ransomware executable remnants should have high priority. Again, this is because it has always happened, based on our data set.

All the information shown in figure 5.1 can be used to make more informed decisions about eradicating ransomware. This is the guidance given for the eradication phase of ransomware attacks based on previous ransomware attacks.



mitre-attack | mitre-pre-attack | mitre-mobile-attack

0 — 18 — Show all

| Reconnaissance | Resource development | Initial access | Execution | Persistence | Privilege escalation | Defense evasion | Credential access | Discovery | Lateral movement | Collection | Command and control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Email Addresses | Tool | Valid Accounts | PowerShell | Valid Accounts | Valid Accounts | Valid Accounts | Brute Force | Network Service Scanning | Remote Desktop Protocol | Local Data Staging | Application Layer Protocol | Automated Exfiltration | Data Encrypted for Impact |
| Active Scanning | Upload Malware | Phishing | Command and Scripting Interpreter | Create or Modify System Process | Create or Modify System Process | Clear Windows Event Logs | OS Credential Dumping | Remote System Discovery | Lateral Tool Transfer | Sharepoint | Commonly Used Port | Exfiltration Over Alternative Protocol | Data Destruction |
| Credentials | Acquire Infrastructure | Exploit Public-Facing Application | Windows Management Instrumentation | Windows Service | Windows Service | Disable or Modify Tools | Cached Domain Credentials | File and Directory Discovery | SMB/Windows Admin Shares | ARP Cache Poisoning | Ingress Tool Transfer | Exfiltration Over C2 Channel | System Shutdown/Reboot |
| Gather Victim Host Information | Botnet | External Remote Services | Malicious File | External Remote Services | Domain Accounts | Impair Defenses | Credentials In Files | Account Discovery | SSH | Adversary-in-the-Middle | Remote Access Software | Exfiltration Over Unencrypted/Obfusc Non-C2 Protocol | Inhibit System Recovery |
| Gather Victim Network Information | Botnet | Domain Accounts | Malicious Link | Domain Accounts | Scheduled Task | Modify Registry | Credentials from Password Stores | System Information Discovery | Exploitation of Remote Services | Archive Collected Data | DNS | Exfiltration to Cloud Storage | Account Access Removal |
| Scanning IP Blocks | Code Signing Certificates | Default Accounts | PowerShell | Scheduled Task | Abuse Elevation Control Mechanism | Domain Accounts | Exploitation for Credential Access | Domain Account | Pass the Hash | Archive via Custom Method | Data Encoding | Data Compressed | Application Exhaustion Flood |
| Business Relationships | Code Signing Certificates | Local Accounts | Scheduled Task | Account Manipulation | Boot or Logon Autostart Execution | Abuse Elevation Control Mechanism | LSASS Memory | Domain Groups | Remote Service Session Hijacking | Archive via Library | Protocol Tunneling | Data Encrypted | Application or System Exploitation |
| CDNs | Compromise Accounts | Spearphishing Attachment | Windows Command Shell | BITS Jobs | Default Accounts | BITS Jobs | Unsecured Credentials | Domain Trust Discovery | Remote Services | Archive via Utility | Web Protocols | Data Transfer Size Limits | Data Manipulation |
| Client Configurations | Compromise Infrastructure | Spearphishing Link | Exploitation for Client Execution | Boot or Logon Autostart Execution | Domain Trust Modification | Default Accounts | /etc/passwd and /etc/shadow | Network Service Discovery | Software Deployment Tools | Audio Capture | Asymmetric Cryptography | Exfiltration Over Asymmetric Encrypted Non-C2 Protocol | Defacement |
| DNS | DNS Server | Supply Chain Compromise | Native API | Default Accounts | Exploitation for Privilege Escalation | Disable or Modify System Firewall | ARP Cache Poisoning | Network Share Discovery | Windows Remote Management | Automated Collection | Bidirectional Communication | Exfiltration Over Bluetooth | Direct Network Flood |
| DNS/Passive DNS | DNS Server | Trusted Relationship | Service Execution | IIS Components | Group Policy Modification | Domain Trust Modification | AS-REP Roasting | Query Registry | Application Access Token | Browser Session Hijacking | Communication Through Removable Media | Exfiltration Over Other Network Medium | Disk Content Wipe |
| Determine Physical Locations | Develop Capabilities | Cloud Accounts | Software Deployment Tools | Local Accounts | Local Accounts | File Deletion | Adversary-in-the-Middle | System Network Connections Discovery | Application Access Token | Clipboard Data | Custom Command and Control Protocol | Exfiltration Over Physical Medium | Disk Content Wipe |
| Digital Certificates | Digital Certificates | Compromise Hardware Supply Chain | User Execution | Office Template Macros | Registry Run Keys / Startup Folder | File Deletion | Bash History | System Owner/User Discovery | Application Deployment Software | Code Repositories | Custom Cryptographic Protocol | Exfiltration Over Symmetric Encrypted Non-C2 Protocol | Disk Structure Wipe |
| Domain Properties | Digital Certificates | Compromise Software Dependencies and Development Tools | AppleScript | Registry Run Keys / Startup Folder | Services Registry Permissions Weakness | File and Directory Permissions Modification | Bash History | Email Account | Component Object Model and Distributed COM | Confluence | DNS Calculation | Exfiltration Over Unencrypted Non-C2 Protocol | Disk Structure Wipe |
| Employee Names | Domains | Compromise Software Supply Chain | AppleScript | Services Registry Permissions Weakness | Access Token Manipulation | Group Policy Modification | Cloud Instance Metadata API | Group Policy Discovery | Distributed Component Object Model | Credential API Hooking | Data Obfuscation | Exfiltration Over Web Service | Disk Wipe |
| Firmware | Domains | Drive-by Compromise | At (Linux) | Web Shell | Accessibility Features | Hidden Files and Directories | Cloud Instance Metadata API | Permission Groups Discovery | Internal Spearphishing | DHCP Spoofing | Dead Drop Resolver | Exfiltration over USB | Endpoint Denial of Service |
| Gather Victim Identity Information | Drive-by Target | Hardware Additions | At (Windows) | Accessibility Features | Accessibility Features | Local Accounts | Container API | Software Discovery | Pass the Hash | Data Staged | Domain Fronting | Exfiltration to Code Repository | External Defacement |
| Gather Victim Org Information | Email Accounts | Replication Through Removable Media | At | Accessibility Features | Active Setup | Masquerade Task or Service | Credential API Hooking | System Network Configuration Discovery | Pass the Ticket | Data from Cloud Storage Object | Domain Fronting | Scheduled Transfer | Firmware Corruption |
| Hardware | Email Accounts | Spearphishing Attachment | CMSTP | Active Setup | AppCert DLLs | Masquerading | Credential Stuffing | System Service Discovery | Pass the Ticket | Data from Configuration Repository | Domain Generation Algorithms | Traffic Duplication | Internal Defacement |
| IP Addresses | Establish Accounts | Spearphishing Link | Compiled HTML File | Add Office 365 Global Administrator Role | AppCert DLLs | Match Legitimate Name or Location | Credentials from Web Browsers | Application Window Discovery | RDP Hijacking | Data from Information Repositories | Domain Generation Algorithms | Transfer Data to Cloud Account | Network Denial of Service |
| Identify Business Tempo | Exploits | Spearphishing via Service | Component Object Model | Add-ins | AppInit DLLs | Network Share Connection Removal | Credentials from Web Browsers | Browser Bookmark Discovery | Remote Desktop Protocol | Data from Local System | Dynamic Resolution | | OS Exhaustion Flood |
| Identify Roles | Exploits | Spearphishing via Service | Component Object Model and Distributed COM | Additional Cloud Credentials | AppInit DLLs | Pass the Hash | Credentials in Files | Cloud Account | Replication Through Removable Media | Data from Network Shared Drive | Encrypted Channel | | Reflection Amplification |
| Network Security Appliances | Install Digital Certificate | | Container Administration Command | Additional Cloud Roles | Application Shimming | Services Registry Permissions Weakness | Credentials in Registry | Cloud Groups | SSH Hijacking | Data from Removable Media | External Proxy | | Resource Hijacking |
| Network Topology | Link Target | | Container Orchestration Job | Additional Email Delegate Permissions | Application Shimming | Access Token Manipulation | Credentials in Registry | Cloud Infrastructure Discovery | SSH Hijacking | Email Collection | Fallback Channels | | Runtime Data Manipulation |

**Figure 5.1:** The MITRE ATT&CK *Techniques* used by the ransomware threat actors in the data set TEMPLATE

## 5.2 Research question 2 - MITRE ATT&CK Techniques per strains

In this chapter, we describe the results we found for our second research question,

> *Which Techniques from the MITRE ATT&CK framework are used per ransomware strain?*

Using the steps taken for answering the first sub-question in section 5.1, the data of the reports is available in MISP. We made a script in Jupyter Notebook to identify all the unique ransomware strains in our data set [34]. This resulted in the following list.

- APT41
- Black Basta Ransomware
- BlackCat Ransomware
- Conti / Conti Group / Conti Ransomware
- Lockbit Ransomware / LockBit
- Phobos Ransomware
- Sodinokibi Ransomware
- Suncrypt
- Zeppelin Ransomware

In the next step, the script gathered all the UUIDs of each MISP event and grouped them per ransomware strain. Then, we used the MISP feature to generate the mappings.

Three of the mappings generated can be seen in figure 5.2, 5.3 and 5.4. Like in section 5.1.4, the figures show a screenshot of an interactive mapping. The mappings of the other ransomware strains can be found in Appendix A. Based on our data set, the result is an overview of the likeliness of each of the MITRE ATT&CK *Techniques* from occurring per ransomware strain.

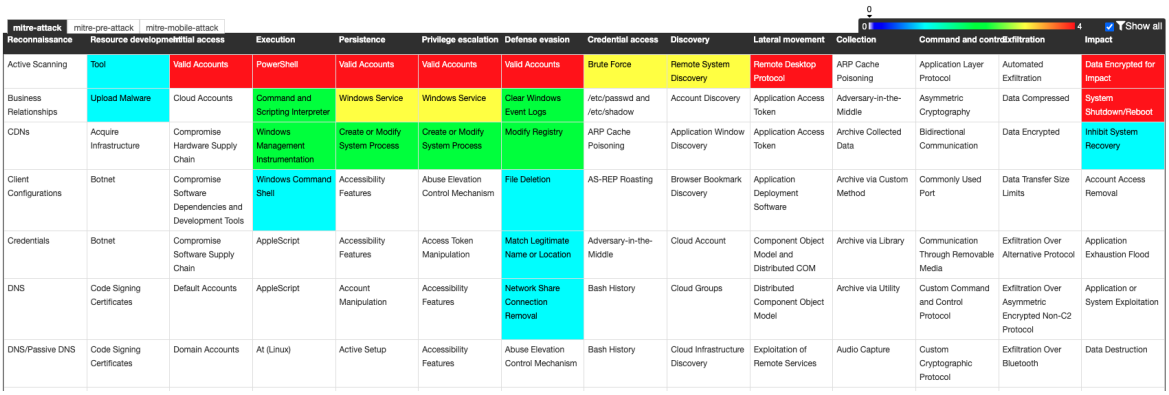
The level of detail and, therefore, the usefulness of each mapping varies. For example, as we can observe with the mappings of Conti in figure 5.3, it contains a lot more detail with 4 cases than the Lockbit mapping shown in figure 5.4 with 2 cases. This highlights why it is essential to keep updating the information in MISP and mappings as more data is gathered. Otherwise, the mapping result provides less certainty, and the result becomes less helpful during the eradication phase.

Every mapping contains the *Technique Data Encryption for Impact*. Like in section 5.1, this is a result we expect because we are looking at ransomware, which core component is encrypting data for impact.

It can be seen with which strain the Northwave CERT observed data exfiltration, which is most likely used for double extortion. As described in section 2.1.3, Conti is known for using double extortion, which can also be seen in our mapping in figure 5.3.

Next to showing available information, the mappings give an overview of all the *Techniques* used by a ransomware strain. This information helps to improve the eradication phase for ransomware because it gives guidance and can be used to make informed decisions on what to eradicate.

These mappings are generated based on our data set of 18 reports. These are example observations based on the data used to create the mappings.



| mitre-attack | mitre-pre-attack | mitre-mobile-attack | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Reconnaissance | Resource development | Initial access | Execution | Persistence | Privilege escalation | Defense evasion | Credential access | Discovery | Lateral movement | Collection | Command and control | Exfiltration | Impact |
| Active Scanning | Tool | Valid Accounts | PowerShell | Valid Accounts | Valid Accounts | Valid Accounts | Brute Force | Remote System Discovery | Remote Desktop Protocol | ARP Cache Poisoning | Application Layer Protocol | Automated Exfiltration | Data Encrypted for Impact |
| Business Relationships | Upload Malware | Cloud Accounts | Command and Scripting Interpreter | Windows Service | Windows Service | Clear Windows Event Logs | /etc/passwd and /etc/shadow | Account Discovery | Application Access Token | Adversary-in-the-Middle | Asymmetric Cryptography | Data Compressed | System Shutdown/Reboot |
| CDNs | Acquire Infrastructure | Compromise Hardware Supply Chain | Windows Management Instrumentation | Create or Modify System Process | Create or Modify System Process | Modify Registry | ARP Cache Poisoning | Application Window Discovery | Application Access Token | Archive Collected Data | Bidirectional Communication | Data Encrypted | Inhibit System Recovery |
| Client Configurations | Botnet | Compromise Software Dependencies and Development Tools | Windows Command Shell | Accessibility Features | Abuse Elevation Control Mechanism | File Deletion | AS-REP Roasting | Browser Bookmark Discovery | Application Deployment Software | Archive via Custom Method | Commonly Used Port | Data Transfer Size Limits | Account Access Removal |
| Credentials | Botnet | Compromise Software Supply Chain | AppleScript | Accessibility Features | Access Token Manipulation | Match Legitimate Name or Location | Adversary-in-the-Middle | Cloud Account | Component Object Model and Distributed COM | Archive via Library | Communication Through Removable Media | Exfiltration Over Alternative Protocol | Application Exhaustion Flood |
| DNS | Code Signing Certificates | Default Accounts | AppleScript | Account Manipulation | Accessibility Features | Network Share Connection Removal | Bash History | Cloud Groups | Distributed Component Object Model | Archive via Utility | Custom Command and Control Protocol | Exfiltration Over Asymmetric Encrypted Non-C2 Protocol | Application or System Exploitation |
| DNS/Passive DNS | Code Signing Certificates | Domain Accounts | At (Linux) | Active Setup | Accessibility Features | Abuse Elevation Control Mechanism | Bash History | Cloud Infrastructure Discovery | Exploitation of Remote Services | Audio Capture | Custom Cryptographic Protocol | Exfiltration Over Bluetooth | Data Destruction |

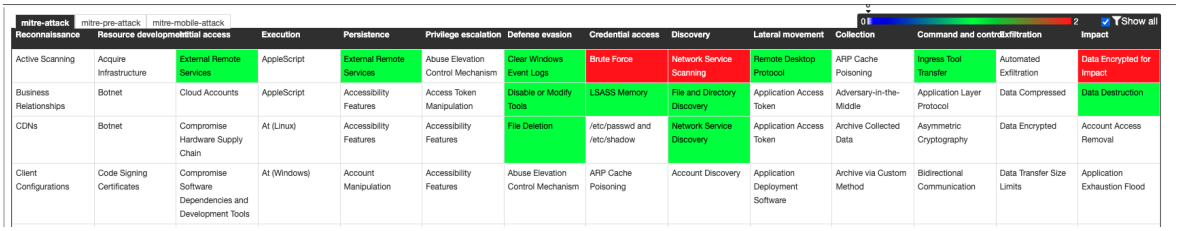
**Figure 5.2:** MITRE ATT&CK *Techniques* used by APT41 ransomware strain based on 4 cases

mitre-attack | mitre-pre-attack | mitre-mobile-attack

0 4 Show all

| Reconnaissance | Resource development | Initial access | Execution | Persistence | Privilege escalation | Defense evasion | Credential access | Discovery | Lateral movement | Collection | Command and control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Email Addresses | Upload Malware | Phishing | Malicious File | Valid Accounts | Valid Accounts | Disable or Modify Tools | Cached Domain Credentials | Account Discovery | SMB/Windows Admin Shares | ARP Cache Poisoning | Commonly Used Port | Exfiltration Over Alternative Protocol | Data Encrypted for Impact |
| Scanning IP Blocks | Acquire Infrastructure | Valid Accounts | Malicious Link | BITS Jobs | Abuse Elevation Control Mechanism | Valid Accounts | Credentials from Password Stores | Domain Account | Exploitation of Remote Services | Adversary-in-the-Middle | DNS | Exfiltration Over Unencrypted/Obfusc Non-C2 Protocol | Data Destruction |
| Active Scanning | Botnet | Domain Accounts | Command and Scripting Interpreter | Create or Modify System Process | Create or Modify System Process | Abuse Elevation Control Mechanism | Unsecured Credentials | Domain Groups | Lateral Tool Transfer | Archive Collected Data | Ingress Tool Transfer | Automated Exfiltration | Inhibit System Recovery |
| Business Relationships | Botnet | Spearphishing Link | Native API | Domain Accounts | Domain Accounts | BITS Jobs | /etc/passwd and /etc/shadow | Domain Trust Discovery | Pass the Hash | Archive via Custom Method | Application Layer Protocol | Data Compressed | Account Access Removal |
| CDNs | Code Signing Certificates | Trusted Relationship | PowerShell | Office Template Macros | Domain Trust Modification | Domain Accounts | ARP Cache Poisoning | Network Service Scanning | Remote Service Session Hijacking | Archive via Library | Asymmetric Cryptography | Data Encrypted | Application Exhaustion Flood |
| Client Configurations | Code Signing Certificates | Cloud Accounts | PowerShell | Registry Run Keys / Startup Folder | Exploitation for Privilege Escalation | Domain Trust Modification | AS-REP Roasting | System Owner/User Discovery | Software Deployment Tools | Archive via Utility | Bidirectional Communication | Data Transfer Size Limits | Application or System Exploitation |
| Credentials | Compromise Accounts | Compromise Hardware Supply Chain | Scheduled Task | Scheduled Task | Group Policy Modification | File and Directory Permissions Modification | Adversary-in-the-Middle | Email Account | Windows Remote Management | Audio Capture | Communication Through Removable Media | Exfiltration Over Asymmetric Encrypted Non-C2 Protocol | Data Manipulation |
| DNS | Compromise Infrastructure | Compromise Software Dependencies and Development Tools | Software Deployment Tools | Services Registry Permissions Weakness | Registry Run Keys / Startup Folder | Group Policy Modification | Bash History | File and Directory Discovery | Application Access Token | Automated Collection | Custom Command and Control Protocol | Exfiltration Over Bluetooth | Defacement |
| DNS/Passive DNS | DNS Server | Compromise Software Supply Chain | User Execution | Accessibility Features | Scheduled Task | Impair Defenses | Bash History | Group Policy Discovery | Application Access Token | Browser Session Hijacking | Custom Cryptographic Protocol | Exfiltration Over C2 Channel | Direct Network Flood |
| Determine Physical Locations | DNS Server | Default Accounts | Windows Command Shell | Accessibility Features | Services Registry Permissions Weakness | Modify Registry | Brute Force | Network Share Discovery | Application Deployment Software | Clipboard Data | DNS Calculation | Exfiltration Over Other Network Medium | Disk Content Wipe |
| Digital Certificates | Develop Capabilities | Drive-by Compromise | AppleScript | Account Manipulation | Access Token Manipulation | Pass the Hash | Cloud Instance Metadata API | Permission Groups Discovery | Component Object Model and Distributed COM | Code Repositories | Data Encoding | Exfiltration Over Physical Medium | Disk Content Wipe |
| Domain Properties | Digital Certificates | Exploit Public-Facing Application | AppleScript | Active Setup | Accessibility Features | Services Registry Permissions Weakness | Cloud Instance Metadata API | Query Registry | Distributed Component Object Model | Confluence | Data Obfuscation | Exfiltration Over Symmetric Encrypted Non-C2 Protocol | Disk Structure Wipe |
| Employee Names | Digital Certificates | External Remote Services | At (Linux) | Add Office 365 Global Administrator Role | Accessibility Features | Access Token Manipulation | Container API | Remote System Discovery | Internal Spearphishing | Credential API Hooking | Dead Drop Resolver | Exfiltration Over Unencrypted Non-C2 Protocol | Disk Structure Wipe |
| Firmware | Domains | Hardware Additions | At (Windows) | Add-ins | Active Setup | Application Access Token | Credential API Hooking | System Information Discovery | Pass the Hash | DHCP Spoofing | Domain Fronting | Exfiltration Over Web Service | Disk Wipe |
| Gather Victim Host Information | Domains | Local Accounts | At | Additional Cloud Credentials | AppCert DLLs | Application Access Token | Credential Stuffing | System Network Configuration Discovery | Pass the Ticket | Data Staged | Domain Fronting | Exfiltration over USB | Endpoint Denial of Service |
| Gather Victim Identity Information | Drive-by Target | Replication Through Removable Media | CMSTP | Additional Cloud Roles | AppCert DLLs | Asynchronous Procedure Call | Credentials In Files | System Network Connections Discovery | Pass the Ticket | Data from Cloud Storage Object | Domain Generation Algorithms | Exfiltration to Cloud Storage | External Defacement |
| Gather Victim Network Information | Email Accounts | Spearphishing Attachment | Compiled HTML File | Additional Email Delegate Permissions | AppInit DLLs | Binary Padding | Credentials from Web Browsers | Application Window Discovery | RDP Hijacking | Data from Configuration Repository | Domain Generation Algorithms | Exfiltration to Code Repository | Firmware Corruption |

**Figure 5.3:** MITRE ATT&CK *Techniques* used by Conti ransomware strain based on 4 cases



mitre-attack | mitre-pre-attack | mitre-mobile-attack

0 2 Show all

| Reconnaissance | Resource development | Initial access | Execution | Persistence | Privilege escalation | Defense evasion | Credential access | Discovery | Lateral movement | Collection | Command and control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Active Scanning | Acquire Infrastructure | External Remote Services | AppleScript | External Remote Services | Abuse Elevation Control Mechanism | Clear Windows Event Logs | Brute Force | Network Service Scanning | Remote Desktop Protocol | ARP Cache Poisoning | Ingress Tool Transfer | Automated Exfiltration | Data Encrypted for Impact |
| Business Relationships | Botnet | Cloud Accounts | AppleScript | Accessibility Features | Access Token Manipulation | Disable or Modify Tools | LSASS Memory | File and Directory Discovery | Application Access Token | Adversary-in-the-Middle | Application Layer Protocol | Data Compressed | Data Destruction |
| CDNs | Botnet | Compromise Hardware Supply Chain | At (Linux) | Accessibility Features | Accessibility Features | File Deletion | /etc/passwd and /etc/shadow | Network Service Discovery | Application Access Token | Archive Collected Data | Asymmetric Cryptography | Data Encrypted | Account Access Removal |
| Client Configurations | Code Signing Certificates | Compromise Software Dependencies and Development Tools | At (Windows) | Account Manipulation | Accessibility Features | Abuse Elevation Control Mechanism | ARP Cache Poisoning | Account Discovery | Application Deployment Software | Archive via Custom Method | Bidirectional Communication | Data Transfer Size Limits | Application Exhaustion Flood |

**Figure 5.4:** MITRE ATT&CK *Techniques* used by Lockbit ransomware strain based on 2 cases

## 5.3 Research question 3 - MITRE ATT&CK Techniques correlation

In this chapter, we describe the results we found for our third research question,

> *What is the correlation between Techniques from the MITRE ATT&CK framework during all studied ransomware incidents?*

Using the steps taken in the first sub-question in section 5.1, the data needed is available in MISP. First, we selected and compared all the MITRE ATT&CK *Techniques* used per event. Next, we stored the information in a table, from which we generated a correlation heatmap. This was done by making a script using Jupyter Notebook [34].

The final result can be seen in figure 5.5. It shows the correlation between the *Techniques* without causation. The heatmap needs to be read from the vertical axis to the horizontal axis. For example, if *T1486 (Data Encrypted for Impact)* [36] is seen on the vertical axis, you see in *0.56* of the cases the use of *sub-Technique T1021.001 (Remote Services: Remote Desktop Protocol)*. This means that in 0.56 of the cases where *T1486 (Data Encrypted for Impact)* was seen, *T1021.001 (Remote Services: Remote Desktop Protocol)* is also seen. This exciting result shows the potential of using these mappings if the input data increases. A zoomed-in version can be seen in figure 5.6.

Two things that stand out in figure 5.5 are the dark red diagonal and vertical lines. The diagonal line happens because every *Technique* is always seen with itself. The red vertical line is because *T1486 (Data Encrypted for Impact)* is seen with every *Technique*. After all, it is used in all the cases in our data set, as expected for ransomware.

Also, some patterns can be observed in the mappings. These patterns occur because the *Techniques* has only been seen used together. The limited amount of data in our data set causes this. When more data is added, the patterns could disappear if *Techniques* are seen independently. Alternatively, the patterns could stay if they are only seen together.

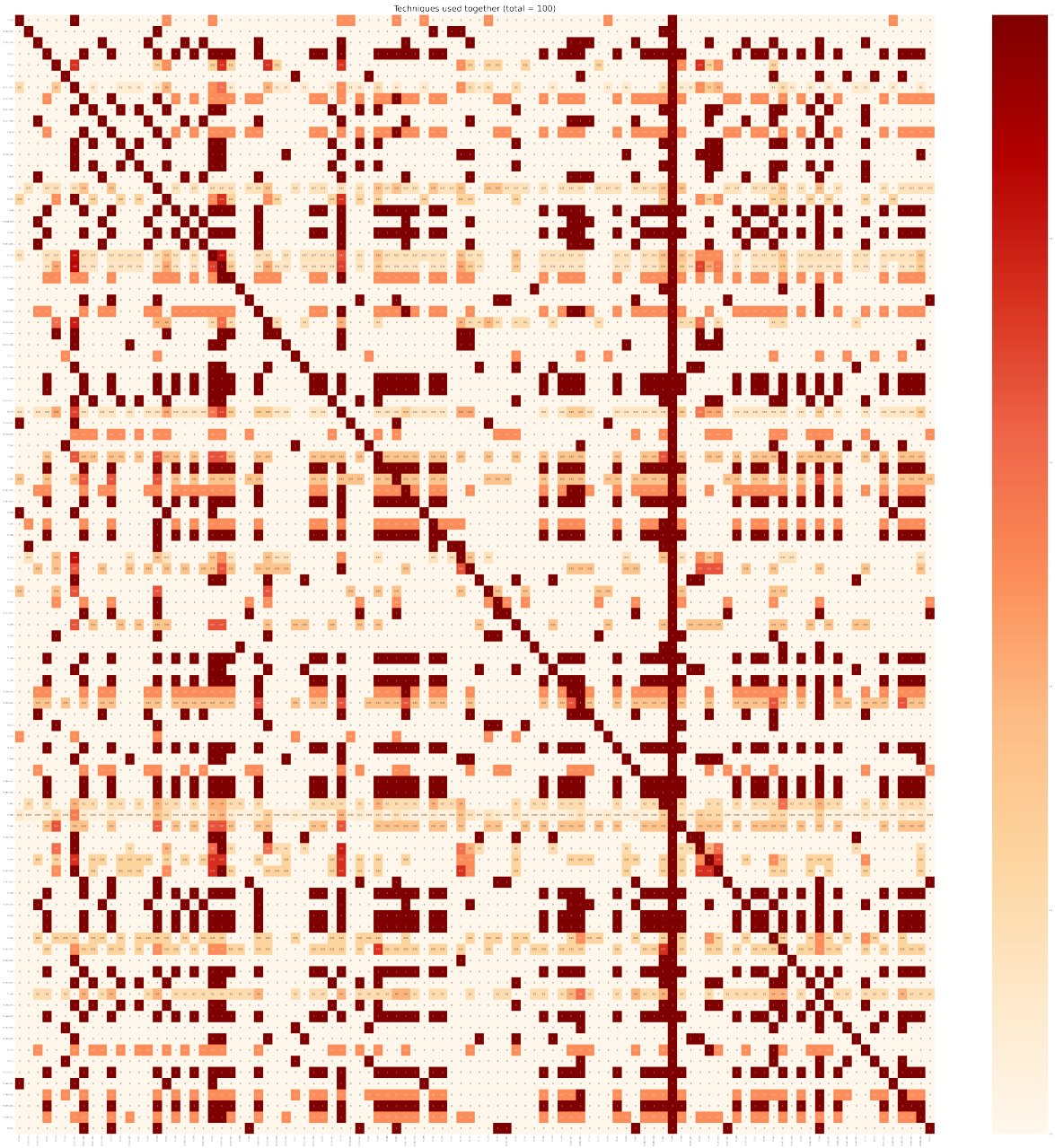



**Figure 5.5:** Correlation heatmap of MITRE ATT&CK *Techniques* based on the 18 ransomware incidents in our data set

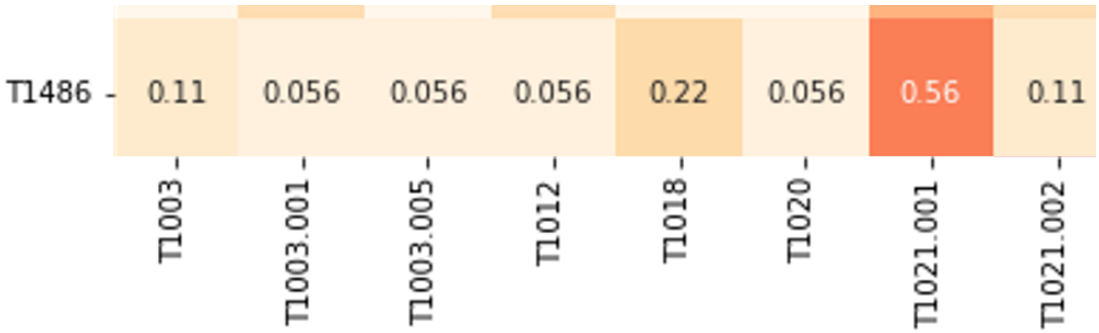



**Figure 5.6:** Zoom-in of the correlation heatmap of MITRE ATT&CK *Techniques* to show the correlation between T1486 and T1021.001

## 5.4 Main research question - Improvement

In this chapter, we describe the results we found for our main research questions,

> *How can the eradication phase of incident response for ransomware incidents be improved based on previous ransomware incidents?*

As described in section 2.3.1, the current eradication phase of the Northwave CERT is a tailored process where an extensive scope is used to achieve the *securely as possible* part of their mission. They prefer to eradicate more than may be necessary to ensure no remnants of the ransomware are left behind. However, it is unclear if this process is *as quickly as possible* and can be improved.

To answer our main research question, we created a method which uses the data already gathered by a CERT to generate mappings to show the MITRE ATT&CK *Techniques* used in previous ransomware incidents. Our method starts with storing ransomware incident data, such as IoCs, in MISP per incident. The next step is to map this data onto the MITRE ATT&CK framework by adding the *Techniques* used during the incident. After that, our scripts can be used to gather this data from MISP and create the type of mappings shown in this research. We created a mapping that gives a clear overview of all the *Techniques* used by different ransomware strains, we created mappings for the *Techniques* used by each ransomware strain, and we created a heatmap for the correlation between *Techniques* of all the ransomware strains. In sections 5.1, 5.2 and 5.3, we showed what can be seen on the mappings. The mappings give insight into previous ransomware incidents and can be used to make informed decisions about how to quickly and securely eradicate a ransomware incident and get a company back to business. This will be the guidance given, and we believe this will improve the eradication phase of ransomware incidents.

# Chapter 6

# Validation

This research suggests a validation process that can be used to validate our created method. To validate if our method improves the eradication phase, we suggest measuring the time spent on eradication with and without the mappings generated with our method. For this, multiple ransomware incidents are needed. One incident cannot be used to validate if the mappings created with our method improve the eradication phase. This is because many variables can influence the time spent on the eradication phase for ransomware, such as the size of the IT infrastructure.

Next to needing multiple incidents to validate our method, more data is needed to fill the mappings. If more data is available to generate mappings, the result will be more complete mappings. If the mappings are more complete, they can be better applied during the eradication phase of ransomware. If they can be applied better, they can also be validated better, and it can be determined if they improve the eradication phase or not. The 18 reports we used to demonstrate our method did not produce complete enough mappings. This makes it hard to validate if our method improves the eradication phase.

Gathering data from additional ransomware incidents would take more time than is available for this research. That is why we propose to perform validation for future work. However, we do suggest how to validate our method.

Start with storing available information about previous ransomware incidents in MISP and map the MITRE ATT&CK *Techniques* onto this data. Use this information to generate a base for the suggested mappings, all seen *Techniques*, *Techniques* per ransomware strain and a correlation matrix of all *Techniques*. When the next ransomware incident occurs, fill in the findings from the Root Cause Analysis in MISP and update the mappings. Keep repeating this process as long as the mappings keep changing. Also, keep track of the amount of time spent on the eradication phase for ransomware. After multiple incidents with this new method, it should become apparent that the mappings do not change much anymore. At that point, it can be assumed that the mappings are complete enough to be validated. Start us-

ing the mappings during the eradication phase and keep track of the time spent on the eradication phase. Compare the time spent on eradication without mappings and with mappings. Based on this comparison, it can be determined if our created method improves the eradication phase, does not influence the eradication phase, or worsens the eradication phase for ransomware.

# Chapter 7

# Discussion and future work

In this chapter, we will discuss our research and future work related to this research.

## 7.1 Mappings

The mappings suggested in this research are limited to the information in MISP. If the ransomware incident information is not correctly stored in MISP, the mappings will fail to guide the eradication phase. Also, the mappings shown in this research are biased because they are generated using data provided by Northwave. The ideal solution would be a MISP instance in which more data is gathered from multiple sources. However, the proposed method is independent of the input data set.

## 7.2 Validation

Due to the complicated verification method and limited time, we did not validate our method in this research. However, we suggested a validation method in chapter 6. Validation should be done, and we highly suggest it be done in future work.

## 7.3 Time as measurement

Time is not the best measurement to measure improvement for the created method. The time the eradication phase for ransomware takes can vary depending on the state and the size of the digital infrastructure of the victim. To tackle this problem during validation, we suggested applying our method to multiple ransomware incidents in chapter 6. Next to validating based on multiple ransomware incidents, we suggest creating a method to classify the effectiveness of a performed eradication. Time could be part of a more extensive formula that defines improvement, but we

think the state and the size of the digital infrastructure of the victim should be taken into account.

## 7.4 The next step

In this research, we created a method that can be used to gain more insight into *Techniques* used with ransomware which can be used as guidance during the eradication phase of ransomware. The next step is researching the most effective ways to eradicate the found *Techniques*. We suggest research to classify which MITRE ATT&CK *Techniques* can be eradicated by which tools or methods.

## 7.5 Root cause analysis

With this research, we showed the MITRE ATT&CK *Techniques* used during a ransomware attack to improve the eradication of ransomware. However, we suspect this information could also be used to help during the Root Cause Analysis because Eradication and Root Cause Analysis are related. Therefore, we suggest researching how information on previous ransomware incidents can help the Root Cause Analysis of a ransomware attack.

# Chapter 8

# Conclusions

We started this research because there needed to be better guidelines for performing the eradication phase for ransomware incidents. These missing guidelines make it difficult for a CERT to know how to perform the eradication phase for ransomware as securely and fast as possible. We created a method that uses the data already gathered by a CERT to create mappings of the MITRE ATT&CK *Techniques* used during a ransomware incident. These mappings showed all the *Techniques* used, the *Techniques* per ransomware strain and a correlation between *Techniques*. This gives insight into what has happened during previous ransomware attacks and can be used as guidance during the eradication phase of ransomware. For example, based on our data set, we saw in 0.56 of the cases *Data encryption for impact* was seen, *Remote Services: Remote Desktop Protocol* was also seen. Due to time and data constraints, we could not validate and measure the improvement of our method. However, we suggested a validation method. The mappings give insight into previous ransomware incidents and can be used to make informed decisions about how to quickly and securely eradicate a ransomware incident and get a company back to business. This will be the guidance given, and we believe this will improve the eradication phase of ransomware incidents.

# Bibliography


[1] FBI, CISA, NSA, ACSC, and NCSC UK, "2021 Trends Show Increased Globalized Threat of Ransomware," Tech. Rep., 2 2022.

[2] "GitHub - MISP/MISP: MISP (core software) - Open Source Threat Intelligence and Sharing Platform." [Online]. Available: https://github.com/MISP/MISP

[3] A. Pennington, A. Applebaum, K. Nickels, T. Schulz, B. Strom, and J. Wunder, "GETTING STARTED WITH ATT&CK."

[4] "ERADICATION — English meaning - Cambridge Dictionary." [Online]. Available: https://dictionary.cambridge.org/dictionary/english/eradication

[5] "Software — MITRE ATT&CK®." [Online]. Available: https://attack.mitre.org/software/

[6] N. Keijzer, "Inside the world of ransomware, Part 1/3: dissecting the attack - Northwave." [Online]. Available: https://northwave-security.com/en/inside-the-world-of-ransomware-dissecting-the-attack/

[7] "Ransom Definition & Meaning — Dictionary.com." [Online]. Available: https://www.dictionary.com/browse/ransom

[8] P. O'Kane, S. Sezer, and D. Carlin, "Evolution of ransomware," *IET Networks*, vol. 7, no. 5, pp. 321–327, 9 2018. [Online]. Available: https://onlinelibrary-wiley-com.tudelft.idm.oclc.org/doi/full/10.1049/iet-net.2017.0207https://onlinelibrary-wiley-com.tudelft.idm.oclc.org/doi/abs/10.1049/iet-net.2017.0207https://ietresearch-onlinelibrary-wiley-com.tudelft.idm.oclc.org/doi/10.1049/iet-net.2017.0207

[9] "Most Common Types of Ransomware — CrowdStrike," 2022. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/ransomware/types-of-ransomware/

[10] "Ransomware as a Service (RaaS) Explained — CrowdStrike," 2022. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

[11] N. Keijzer, “Inside the world of ransomware part 2/3: Different roles within a ransomware attack - Northwave.” [Online]. Available: https://northwave-security.com/inside-the-world-of-ransomware-part-2-3-different-roles-within-a-ransomware-attack/

[12] “Microsoft digital defense report 2022.” [Online]. Available: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

[13] “Microsoft Digital Defense Report OCTOBER 2021 2 TOC INTRODUCTION THE STATE OF CYBERCRIME NATION STATE THREATS SUPPLY CHAIN, IOT, AND OT SECURITY HYBRID WORKFORCE SECURITY DISINFORMATION ACTIONABLE INSIGHTS TEAMS.”

[14] “INCIDENT — English meaning - Cambridge Dictionary.” [Online]. Available: https://dictionary.cambridge.org/dictionary/english/incident

[15] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, “Computer Security Incident Handling Guide Recommendations of the National Institute of Standards and Technology,” 2012. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-61r2

[16] “ISO - ISO/IEC 27035-3:2020 - Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations,” 2020. [Online]. Available: https://www.iso.org/standard/74033.html

[17] “NIST SP 800-61 and ISO/IEC 27035 - Attempt of Short Comparison — Rapid7 Blog,” 2017. [Online]. Available: https://www.rapid7.com/blog/post/2017/05/31/nist-sp-800-61-and-isoiec-27035-attempt-of-short-comparison/

[18] “NIST General Information — NIST.” [Online]. Available: https://www.nist.gov/director/pao/nist-general-information

[19] M. J. West-Brown, D. Stikvoort, K.-P. Kossakowski, G. Killcrece, R. Ruefle, and M. Zajicek, “Carnegie Mellon Handbook for Computer Security Incident Response Teams (CSIRTs),” 2003.

[20] “Report an incident — Cyber Safety.” [Online]. Available: https://www.utwente.nl/en/cyber-safety/reportincident/

[21] “Incidentrespons — Nationaal Cyber Security Centrum.” [Online]. Available: https://www.ncsc.nl/onderwerpen/incidentrespons

[22] “Home - Z-CERT.” [Online]. Available: https://www.z-cert.nl/

[23] “Home - Northwave.” [Online]. Available: https://northwave-security.com/

[24] P. F. Wilson, L. D. Dell, and G. F. Anderson, “Root Cause Analysis: A Tool for Total Quality Management,” *Journal For Healthcare Quality*, vol. 18, no. 1, p. 40, 1 1996.

[25] “CVE - CVE.” [Online]. Available: https://cve.mitre.org/

[26] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, “MITRE ATT&CK: Design and Philosophy.”

[27] “Conti, Software S0575 — MITRE ATT&CK®.” [Online]. Available: https://attack.mitre.org/software/S0575/

[28] “Conti Ransomware — CISA.” [Online]. Available: https://www.cisa.gov/uscert/ncas/alerts/aa21-265a

[29] “Conti ransomware group’s pulse stops, but did it fake its own death?” [Online]. Available: https://www.malwarebytes.com/blog/news/2022/06/conti-ransomware-disappears-did-it-fake-its-own-death

[30] “The many lives of BlackCat ransomware - Microsoft Security Blog.” [Online]. Available: https://www.microsoft.com/en-us/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/

[31] C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody, “MISP - The design and implementation of a collaborative threat intelligence sharing platform,” *WISCS 2016 - Proceedings of the 2016 ACM Workshop on Information Sharing and Collaborative Security, co-located with CCS 2016*, pp. 49–56, 10 2016.

[32] “MISP/PyMISP: Python library using the MISP Rest API.” [Online]. Available: https://github.com/MISP/PyMISP

[33] “Project Jupyter — Home.” [Online]. Available: https://jupyter.org/

[34] S. Dijkstra, R, “Thesis scripts.” [Online]. Available: https://gitlab.utwente.nl/s2214075/thesis-scripts

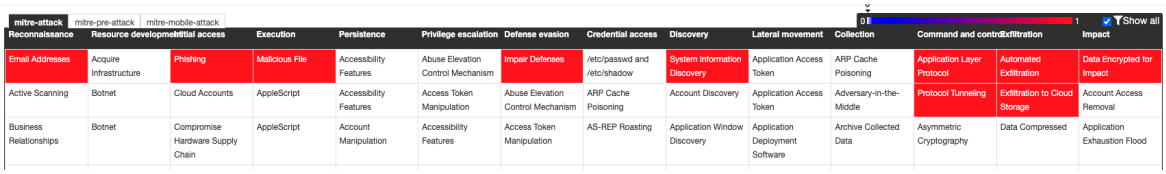
[35] “Tactics - Enterprise — MITRE ATT&CK®.” [Online]. Available: https://attack.mitre.org/tactics/enterprise/

[36] “Data Encrypted for Impact, Technique T1486 - Enterprise — MITRE ATT&CK®.” [Online]. Available: https://attack.mitre.org/techniques/T1486/

# Appendix A

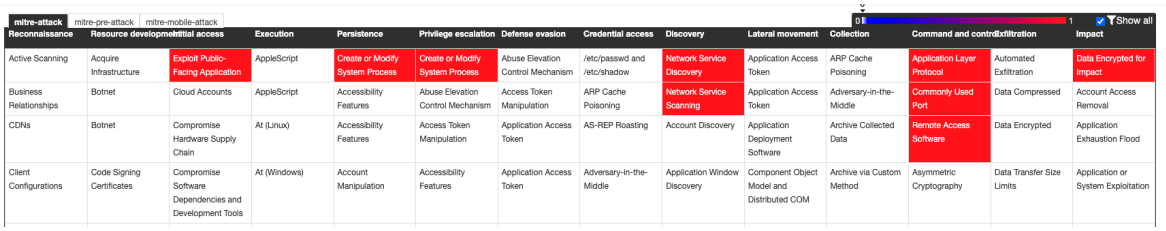
# Mappings per strain

In this Appendix we show the other mappings per ransomware strain, we generated using our method.



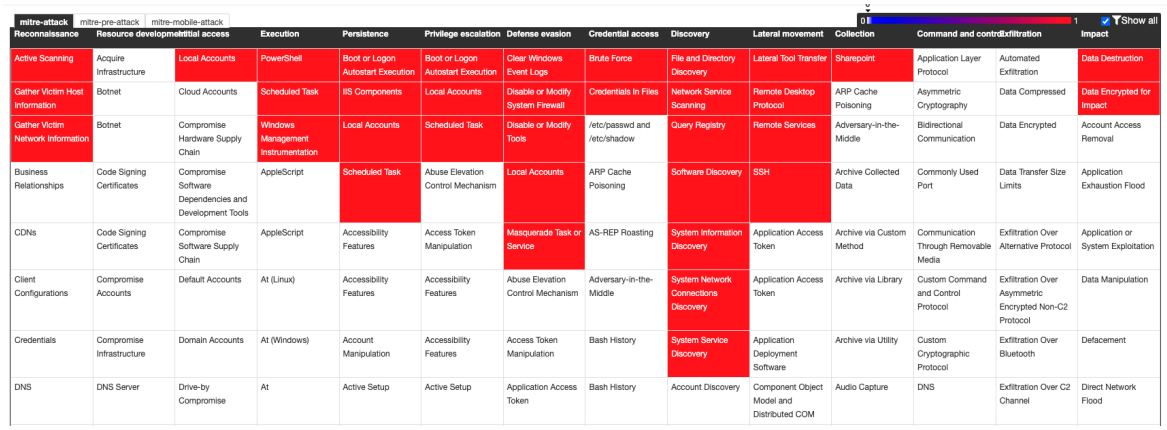
| Reconnaissance | Resource development | Initial access | Execution | Persistence | Privilege escalation | Defense evasion | Credential access | Discovery | Lateral movement | Collection | Command and control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Email Addresses | Acquire Infrastructure | Phishing | Malicious File | Accessibility Features | Abuse Elevation Control Mechanism | Impair Defenses | /etc/passwd and /etc/shadow | System Information Discovery | Application Access Token | ARP Cache Poisoning | Application Layer Protocol | Automated Exfiltration | Data Encrypted for Impact |
| Active Scanning | Botnet | Cloud Accounts | AppleScript | Accessibility Features | Access Token Manipulation | Abuse Elevation Control Mechanism | ARP Cache Poisoning | Account Discovery | Application Access Token | Adversary-in-the-Middle | Protocol Tunneling | Exfiltration to Cloud Storage | Account Access Removal |
| Business Relationships | Botnet | Compromise Hardware Supply Chain | AppleScript | Account Manipulation | Accessibility Features | Access Token Manipulation | AS-REP Roasting | Application Window Discovery | Application Deployment Software | Archive Collected Data | Asymmetric Cryptography | Data Compressed | Application Exhaustion Flood |

**Figure A.1:** MITRE ATT&CK *Techniques* used by Black Basta ransomware strain based on 1 case



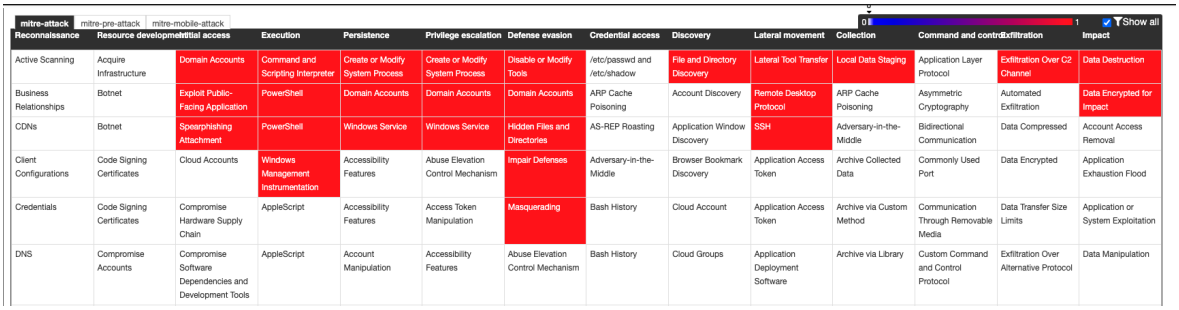
| Reconnaissance | Resource development | Initial access | Execution | Persistence | Privilege escalation | Defense evasion | Credential access | Discovery | Lateral movement | Collection | Command and control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Active Scanning | Acquire Infrastructure | Exploit Public-Facing Application | AppleScript | Create or Modify System Process | Create or Modify System Process | Abuse Elevation Control Mechanism | /etc/passwd and /etc/shadow | Network Service Discovery | Application Access Token | ARP Cache Poisoning | Application Layer Protocol | Automated Exfiltration | Data Encrypted for Impact |
| Business Relationships | Botnet | Cloud Accounts | AppleScript | Accessibility Features | Abuse Elevation Control Mechanism | Access Token Manipulation | ARP Cache Poisoning | Network Service Scanning | Application Access Token | Adversary-in-the-Middle | Commonly Used Port | Data Compressed | Account Access Removal |
| CDNs | Botnet | Compromise Hardware Supply Chain | At (Linux) | Accessibility Features | Access Token Manipulation | Application Access Token | AS-REP Roasting | Account Discovery | Application Deployment Software | Archive Collected Data | Remote Access Software | Data Encrypted | Application Exhaustion Flood |
| Client Configurations | Code Signing Certificates | Compromise Software Dependencies and Development Tools | At (Windows) | Account Manipulation | Accessibility Features | Application Access Token | Adversary-in-the-Middle | Application Window Discovery | Component Object Model and Distributed COM | Archive via Custom Method | Asymmetric Cryptography | Data Transfer Size Limits | Application or System Exploitation |

**Figure A.2:** MITRE ATT&CK *Techniques* used by Blackcat ransomware strain based on 1 case



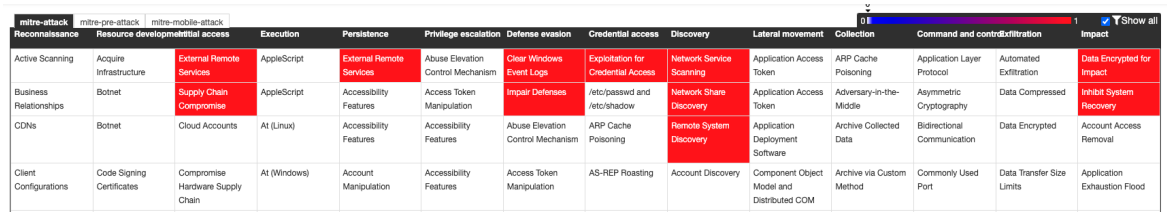
| Reconnaissance | Resource development | Initial access | Execution | Persistence | Privilege escalation | Defense evasion | Credential access | Discovery | Lateral movement | Collection | Command and control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Active Scanning | Acquire Infrastructure | Local Accounts | PowerShell | Boot or Logon Autostart Execution | Boot or Logon Autostart Execution | Clear Windows Event Logs | Brute Force | File and Directory Discovery | Lateral Tool Transfer | Sharepoint | Application Layer Protocol | Automated Exfiltration | Data Destruction |
| Gather Victim Host Information | Botnet | Cloud Accounts | Scheduled Task | IIS Components | Local Accounts | Disable or Modify System Firewall | Credentials In Files | Network Service Scanning | Remote Desktop Protocol | ARP Cache Poisoning | Asymmetric Cryptography | Data Compressed | Data Encrypted for Impact |
| Gather Victim Network Information | Botnet | Compromise Hardware Supply Chain | Windows Management Instrumentation | Local Accounts | Scheduled Task | Disable or Modify Tools | /etc/passwd and /etc/shadow | Query Registry | Remote Services | Adversary-in-the-Middle | Bidirectional Communication | Data Encrypted | Account Access Removal |
| Business Relationships | Code Signing Certificates | Compromise Software Dependencies and Development Tools | AppleScript | Scheduled Task | Abuse Elevation Control Mechanism | Local Accounts | ARP Cache Poisoning | Software Discovery | SSH | Archive Collected Data | Commonly Used Port | Data Transfer Size Limits | Application Exhaustion Flood |
| CDNs | Code Signing Certificates | Compromise Software Supply Chain | AppleScript | Accessibility Features | Access Token Manipulation | Masquerade Task or Service | AS-REP Roasting | System Information Discovery | Application Access Token | Archive via Custom Method | Communication Through Removable Media | Exfiltration Over Alternative Protocol | Application or System Exploitation |
| Client Configurations | Compromise Accounts | Default Accounts | At (Linux) | Accessibility Features | Accessibility Features | Abuse Elevation Control Mechanism | Adversary-in-the-Middle | System Network Connections Discovery | Application Access Token | Archive via Library | Custom Command and Control Protocol | Exfiltration Over Asymmetric Encrypted Non-C2 Protocol | Data Manipulation |
| Credentials | Compromise Infrastructure | Domain Accounts | At (Windows) | Account Manipulation | Accessibility Features | Access Token Manipulation | Bash History | System Service Discovery | Application Deployment Software | Archive via Utility | Custom Cryptographic Protocol | Exfiltration Over Bluetooth | Defacement |
| DNS | DNS Server | Drive-by Compromise | At | Active Setup | Active Setup | Application Access Token | Bash History | Account Discovery | Component Object Model and Distributed COM | Audio Capture | DNS | Exfiltration Over C2 Channel | Direct Network Flood |

**Figure A.3:** MITRE ATT&CK *Techniques* used by Phobos ransomware strain based on 1 case



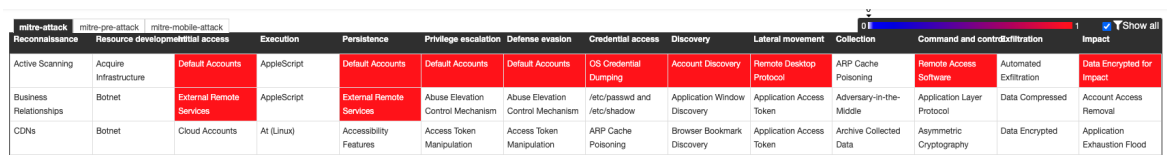
| Reconnaissance | Resource development | Initial access | Execution | Persistence | Privilege escalation | Defense evasion | Credential access | Discovery | Lateral movement | Collection | Command and control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Active Scanning | Acquire Infrastructure | Domain Accounts | Command and Scripting Interpreter | Create or Modify System Process | Create or Modify System Process | Disable or Modify Tools | /etc/passwd and /etc/shadow | File and Directory Discovery | Lateral Tool Transfer | Local Data Staging | Application Layer Protocol | Exfiltration Over C2 Channel | Data Destruction |
| Business Relationships | Botnet | Exploit Public-Facing Application | PowerShell | Domain Accounts | Domain Accounts | Domain Accounts | ARP Cache Poisoning | Account Discovery | Remote Desktop Protocol | ARP Cache Poisoning | Asymmetric Cryptography | Automated Exfiltration | Data Encrypted for Impact |
| CDNs | Botnet | Spearphishing Attachment | PowerShell | Windows Service | Windows Service | Hidden Files and Directories | AS-REP Roasting | Application Window Discovery | SSH | Adversary-in-the-Middle | Bidirectional Communication | Data Compressed | Account Access Removal |
| Client Configurations | Code Signing Certificates | Cloud Accounts | Windows Management Instrumentation | Accessibility Features | Abuse Elevation Control Mechanism | Impair Defenses | Adversary-in-the-Middle | Browser Bookmark Discovery | Application Access Token | Archive Collected Data | Commonly Used Port | Data Encrypted | Application Exhaustion Flood |
| Credentials | Code Signing Certificates | Compromise Hardware Supply Chain | AppleScript | Accessibility Features | Access Token Manipulation | Masquerading | Bash History | Cloud Account | Application Access Token | Archive via Custom Method | Communication Through Removable Media | Data Transfer Size Limits | Application or System Exploitation |
| DNS | Compromise Accounts | Compromise Software Dependencies and Development Tools | AppleScript | Account Manipulation | Accessibility Features | Abuse Elevation Control Mechanism | Bash History | Cloud Groups | Application Deployment Software | Archive via Library | Custom Command and Control Protocol | Exfiltration Over Alternative Protocol | Data Manipulation |

**Figure A.4:** MITRE ATT&CK *Techniques* used by Sodinokibi ransomware strain based on 1 case



| Reconnaissance | Resource development | Initial access | Execution | Persistence | Privilege escalation | Defense evasion | Credential access | Discovery | Lateral movement | Collection | Command and control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Active Scanning | Acquire Infrastructure | External Remote Services | AppleScript | External Remote Services | Abuse Elevation Control Mechanism | Clear Windows Event Logs | Exploitation for Credential Access | Network Service Scanning | Application Access Token | ARP Cache Poisoning | Application Layer Protocol | Automated Exfiltration | Data Encrypted for Impact |
| Business Relationships | Botnet | Supply Chain Compromise | AppleScript | Accessibility Features | Access Token Manipulation | Impair Defenses | /etc/passwd and /etc/shadow | Network Share Discovery | Application Access Token | Adversary-in-the-Middle | Asymmetric Cryptography | Data Compressed | Inhibit System Recovery |
| CDNs | Botnet | Cloud Accounts | At (Linux) | Accessibility Features | Accessibility Features | Abuse Elevation Control Mechanism | ARP Cache Poisoning | Remote System Discovery | Application Deployment Software | Archive Collected Data | Bidirectional Communication | Data Encrypted | Account Access Removal |
| Client Configurations | Code Signing Certificates | Compromise Hardware Supply Chain | At (Windows) | Account Manipulation | Accessibility Features | Access Token Manipulation | AS-REP Roasting | Account Discovery | Component Object Model and Distributed COM | Archive via Custom Method | Commonly Used Port | Data Transfer Size Limits | Application Exhaustion Flood |

**Figure A.5:** MITRE ATT&CK *Techniques* used by Suncrypt ransomware strain based on 1 case



| Reconnaissance | Resource development | Initial access | Execution | Persistence | Privilege escalation | Defense evasion | Credential access | Discovery | Lateral movement | Collection | Command and control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Active Scanning | Acquire Infrastructure | Default Accounts | AppleScript | Default Accounts | Default Accounts | Default Accounts | OS Credential Dumping | Account Discovery | Remote Desktop Protocol | ARP Cache Poisoning | Remote Access Software | Automated Exfiltration | Data Encrypted for Impact |
| Business Relationships | Botnet | External Remote Services | AppleScript | External Remote Services | Abuse Elevation Control Mechanism | Abuse Elevation Control Mechanism | /etc/passwd and /etc/shadow | Application Window Discovery | Application Access Token | Adversary-in-the-Middle | Application Layer Protocol | Data Compressed | Account Access Removal |
| CDNs | Botnet | Cloud Accounts | At (Linux) | Accessibility Features | Access Token Manipulation | Access Token Manipulation | ARP Cache Poisoning | Browser Bookmark Discovery | Application Access Token | Archive Collected Data | Asymmetric Cryptography | Data Encrypted | Application Exhaustion Flood |

**Figure A.6:** MITRE ATT&CK *Techniques* used by Zeppelin ransomware strain based on 1 case