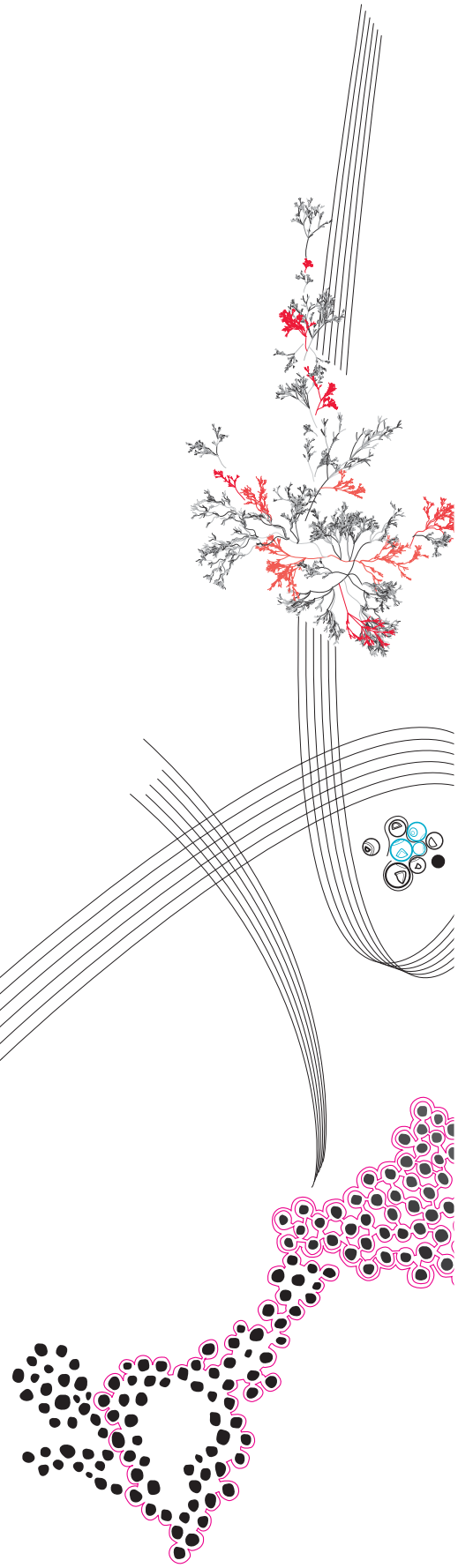


M.Sc. Faculty of Electrical Engineering, Mathematics & Computer Science Thesis Report

Ransomware as a tool for diversion and coverup. A possible modus operandi for advanced persistent threats?

Raphael Enio Hoheisel

Supervisors: dr.ing. Erik Tews, prof.dr. Marianne Junger, Rang Salih, Matthijs van Polen, Wouter van Kranenburg

October, 2022

Faculty of Electrical Engineering, Mathematics & Computer Science

UNIVERSITY OF TWENTE.

A (practical) Investigation into the Use of Ransomware as Masquerade and Distraction

Raphael Enio Hoheisel*

October, 2022

Abstract

Covering up a cyber-attack with another attack such as ransomware is rarely seen, yet a realistic and applied scenario. Especially, in times where ransomware attacks affect the majority of companies, using it as a masquerade, smokescreen or to cover up another attack seems to be the ideal moment. As a result, this thesis takes a closer look into this development. It shows that using ransomware as a cover or as a masquerade dates many years back and has been applied multiple times in the recent war in Ukraine. In addition, the thesis investigates actual ransomware cases of security company Northwave in which ransomware might have been used to cover up espionage or other malicious activities, even though, in the end, evidence suggested a purely financially motivated attack with no intention to cover up something. Besides, this study looks into the relationships between state actors such as the Russian government and its relation to ransomware gangs highlighting a sometimes close cooperation between them. *Keywords*: ransomware, wiper, cyber-espionage, apt, cover-up

*Email: raphael.hoheisel@protonmail.com

Contents

Acronyms

APT Advanced Persistent Threat.

ATM Automated Teller Machine.

C2 Command and Control.

CERT Computer Emergency Response Team.

CIA Central Intelligence Agency.

DBIR Data Breach Investigations Report.

DDoS Distributed Denial of Service.

FSB Federal Security Service.

GRU General Staff Main Intelligence Directorate.

IOC Indicator of Compromise.

IP Internet Protocol.

MBR Master Boot Record.

MICTIC Malware, Infrastructure, Control server, Telemetry, Intelligence, Cui bono.

MISP Malware Information Sharing Platform.

RaaS Ransomware as a Service.

SVR Foreign Intelligence Service.

SWIFT Society for Worldwide Interbank Financial Telecommunications.

VERIS Vocabulary for Event Recording and Incident Sharing.

Glossary

0-day vulnerability A (software) vulnerability for which there is no patch available at the time of its disclosure.

Crypto malware This type of ransomware encrypts files on a system and asks for a ransom to decrypt them again. [1].

Hacking The action Hacking is defined in VERIS as "attempts to intentionally access or harm information assets without (or exceeding) authorization by circumventing or thwarting logical security mechanisms." [2, p. 14].

Incident An incident is defined by Verizon as "A security event that compromises the integrity, confidentiality or availability of an information asset." [2, p. 4].

Leakware/Doxware Leakware or doxware is a type of ransomware that steals personal information and the threat actor uses that to blackmail the victim. [1].

Lockers This type of ransomware prevents a user from logging in until a ransom is paid. [1].

Malware The action Malware is defined in VERIS as "any malicious software, script, or code run on a device that alters its state or function without the owner's informed consent." [2, p. 14].

Ransomware as a Service (RaaS) RaaS is a service in which a group creates a ransomware build or a ransomware building tool and leases that to other actors, so-called 'affiliates', which often pay part of the ransom to the RaaS provider in return. [3, p. 15], [4, p. 4].

Scareware This type of ransomware poses as legitimate software saying it found vulnerabilities in the system and demands money to fix them. [1].

Variety A variety in the VERIS framework describes the type of an action. [2, p. 14].

Vector A vector in the VERIS framework describes through what means an action takes place. [2, p. 14].

1 Introduction

With suspenseful music and a rush of movements before the police arrive the character most carefully arranges objects and the position of the hand so that everything looks like the person committed suicide. Scenes in a similar fashion are well known in movies and series such as *A Nightmare on Elm Street* [5] (murder of Rod Lane) or *Stranger Things* (murder of Benny Hammond in season one episode two) [6]. However, masquerading the real motive of a crime such as homicide to look like suicide also happens in the real world [7]. Even states allegedly use this tactic as is suspected in the case of Boris A. Berezovsky who died of suicide. However, there are suspicions that it was in fact a homicide possibly ordered by the Russian government [8]. Since such techniques are used in offline crime, it is plausible to suggest they are also used in online crimes. This is exactly the suspicion raised by experts at Northwave[1], a Dutch cyber security company based in Utrecht. Their Computer Emergency Response Team (CERT) handled several ransomware incidents in which they suspected that the deployment of ransomware was a cover-up. Those suspicions are not unfounded. In 2016 and 2017 a destructive malware called NotPetya [9] infected thousands of computer systems worldwide masquerading itself as ransomware and in 2019 a security company named Dragos raised the suspicion that ransomware was used to cover up something during an incident at Norsk Hydro [10]. The next paragraphs will briefly introduce ransomware and thereafter explain the reasons certain ransomware incidents were considered suspicious to Northwave.

Ransomware is a generic term for different types of malware which asks the victim for a ransom to decrypt or stop malicious activity. Those types include, inter alia, Crypto malware, Lockers , Scareware, Ransomware as a Service (RaaS) and Leakware/Doxware [1]. The most prevalent today is the Crypto malware type [11, p. 1]. In the following, the name ransomware will be used to refer to Crypto malware. Ransomware is residing at position one of the top eight online threats of 2021 according to Enisa, the European Union cybersecurity agency [12, p. 6f]. In 2021 623 million ransomware incidents were reported by SonicWall and in a survey conducted by Sophos (n=5600), 66% of companies said they were attacked with such malware in 2021 [13], [14]. Given its success in the last years, ransomware attracted sophisticated actors known for other criminal activities such as espionage [15], [16]. In a press release, from November 2021, the security software company Sophos refers to the ransomware ecosystem as "Gravitational Force of Ransomware Black Hole Pulls in Other Cyber threats to Create One Massive, Interconnected Ransomware Delivery System" [17]. With that Sophos sees a further development of the ransomware ecosystem towards a more modular one where specialists for specific tasks of a ransomware attack exist, ransomware samples become more sophisticated and with an increasing market dominance of RaaS providers. Actors in the ransomware ecosystem range from criminal groups such as BlackCat [18] to state-sponsored actors from, for example, China, Iran, Russia, or North Korea [15], [19]–[21].

Six ransomware incidents had exceptional characteristics that made members of Northwave's CERT team skeptical. The two main aspects that differed greatly from the usual ransomware case the CERT handles were the type of threat actor (see Section 3.2.1 for details regarding the attribution) and the tools used. The threat actor behind the six attacks was a Chinese Advanced Persistent Threat (APT) known under the names APT 41, Barium or Wicked Panda [22]. From now on this threat actor will be referred to as APT 41. This threat actor is known for conducting financially motivated attacks as well as

[1] `https://northwave-security.com/`

espionage, but not for conducting successful ransomware attacks [23]. Recent campaigns of APT 41 targeted companies in the hospitality or aviation sector in North America and Asia [24]. Another aspect that made the ransomware attacks extraordinary was that the threat actor used legitimate tools for the encryption of data and not specially crafted ransomware which is what experts at Northwave normally observe. There are only a few other cases reported in which a threat actor used legitimate tools for the encryption (see Section 4.2).

During the initial investigations, no direct evidence was found that indicated a scenario in line with offline crime that something was covered up. Nevertheless, having the ransomware landscape in mind and the unusual techniques used in the investigated cases, it was worthwhile to take a closer look. As a result, in cooperation with Northwave and the University of Twente, more general research questions were formed to study the scenario of covering up another criminal act using ransomware. The resulting research questions are:
RQ 1: To what extent is ransomware used as a cover for other malicious activities?
The sub-question follows the main research question:
SQ1: In what way are the suspicious cases from Northwave different to ransomware cases which do not indicate an intrusion with multiple motivations? A second sub-question aims to study the relationships between states and ransomware groups further.
SQ2: To what extent do interests/operations of ransomware groups and states overlap and what could be benefits on both sides?

The questions aim to gather an insight into the use of ransomware as cover via literature review and a practical investigation into six ransomware incidents. The purpose of SQ1 is to highlight which aspects of the six ransomware cases contributed to the suspicion that ransomware was used to cover something up. Research regarding SQ2 aims to give information on cyber operations and specifically ransomware attacks conducted by non-state actors to the benefit of a state.
The thesis is structured in the following way. Firstly ransomware will be introduced in more detail, followed by background information on state and non-state actor relationships. The subsequent section covers related work followed by the introduction of the approach and methodology of this research project. After that, the results are presented and discussed in detail including their implications and limitations. In the end, a conclusion is drawn by summarising the study and mentioning future work to advance and improve the research project.

This thesis is partially based on a so-called 'research topic' written by the same author as this thesis, thus, some paragraphs have been taken over.

1.1 Ransomware - A Closer Look

The ransomware section aims to give a broader understanding of ransomware including its history, the current attack landscape, the business around it and how a ransomware attack usually works. To do this, an investigation of existing literature is presented.

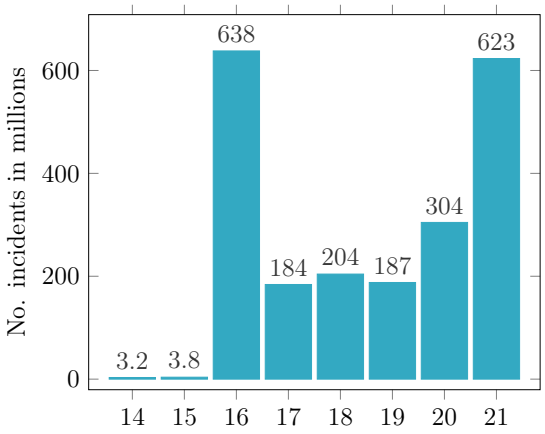
The first ransomware (known as PC Cyborg or AIDS) was created in the 1980s by Joseph L. Popp and was distributed via floppy disk. The malware used symmetrical encryption to encrypt files and asked for a ransom of US $189 to decrypt the files again [25], [26]. From there ransomware evolved into a severe threat affecting hundreds of millions of systems

worldwide each year with victims paying up to US $40 million in ransom [27] in one incident. Ransomware attacks are estimated to have caused worldwide damages of US $20 billion which represents 0.33% of the costs of all cybercrime damages in 2021 and is 57 times higher than the damages caused by ransomware in 2015 [28].

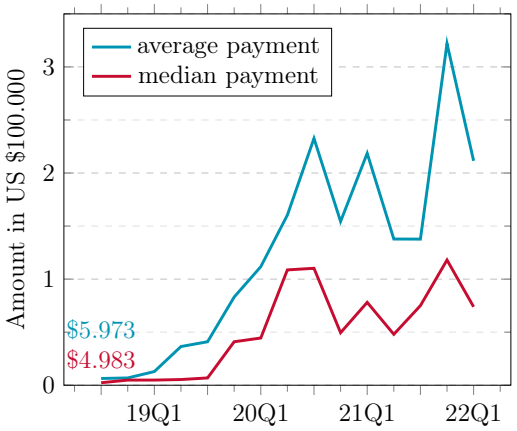
A development in the last years was the addition of the so-called 'double extortion' scheme to a typical ransomware scheme. In the double extortion scheme, attackers exfiltrate data during the attack and threaten to leak parts or all of the data if the victim does not pay the ransom. The security company CrowdStrike registered an increase in this method at the end of 2019 [29, p. 24] and according to Microsoft this method is still a threat and very lucrative for threat actors [3, p. 10]. According to a report by Corvus, double extortion changed from a share of 5 % of all ransomware cases in 2019 to 27% (2020) to 22% (beginning of Q4 2021) [30]. Another security company, Coveware, reported a considerably higher number of 84% in Q4 2021 [31]. In order to increase the pressure to pay the ransom, ransomware groups started calling employees of the affected company (observed by Northwave) or threatening to launch a Distributed Denial of Service (DDoS) attack [12, p. 37]. Furthermore, threat actors began to inform the victim's partners or customers that their data is part of the exfiltrated information and will be leaked if the ransom is not paid [12, p. 36f]. Besides reports of these multiple extortion schemes, security companies have noticed a rise in extortion cases where no data was encrypted and threat actors only exfiltrate data demanding a ransom to prevent them from publishing it. Without encryption of the data, ransomware groups save time and money, for example, there is no need to buy or develop ransomware. In addition, threat actors allegedly turn to such less disruptive extortion schemes (no business interruption due to encrypted data) to avoid the attention of law enforcement [31]–[33].

1.1.1 About Ransomware Attacks and Ransom Value

In recent years, both the number of ransomware attacks and the average ransom amount were increasing. Of all the affected sectors between June 2020 and July 2021, the most targeted ones by ransomware were, according to a Microsoft report, consumer/retail with 13% followed by insurance/financial and manufacturing/agriculture both with 12% [3, p. 18]. In 2021 the number of observed ransomware incidents doubled compared to 2020 according to data collected by the cyber-security company SonicWall, with an even higher increase in the average ransom payment, as seen in Figure 1a and 1b. In 2021, the ransom payments are fluctuating but remain higher compared to 2019 and show a big increase compared to the third quarter of 2018 in which the average paid ransom amount was US $5.973 as reported by Coveware [34]. The high increase in ransomware attacks in 2016 is, according to SonicWall, caused by several factors. Access to ransomware in underground markets was getting easier accompanied by simpler options to spread and conduct a ransomware attack and a decreasing risk of being identified due to the more widespread use of Bitcoin as a payment method [35, p. 11]. SonicWall does not provide detailed information on the reasons for the high decline in ransomware attacks in 2017. The increase in the average amount of the paid ransom in 2019 is explained, by the source Coveware, by a rising amount of targeted attacks on large enterprises [36].



(A) The annual number of ransomware incidents worldwide from 2014 to 2021 as reported by SonicWall. Recreated from: [13], [35], [37]



(B) Ransom payments by quarter as reported by Coveware. Recreated from: [31], [34], [38]

1.1.2 Ransomware Ecosystem

Here, the ransomware ecosystem refers to all the actors and service providers offering services that cover one specific or many phases of a ransomware attack. The RaaS providers play a big role in the ecosystem [39]. According to the security company Trend Micro, the three ransomware groups with the highest amount of claimed ransomware attacks in the first quarter of 2022 were all RaaS providers. In total, Trend Micro reports 36 active RaaS providers in the beginning of 2022 [40]. In the case of the RaaS provider REvil, they also take care of ransom negotiation, collection and distribution as well as blackmailing of victims [41]. Leaks of internal communication of another RaaS provider, Conti, give an insight on how professionally structured such providers can be. Those leaks revealed that Conti allegedly has departments such as human resources and even seems to operate physical office(s) [42]. However, it is not known how many other groups have this high level of organisation of their criminal business. The last year RaaS providers dominated the ransomware market which is predicted to stay the same by 2022. In addition, the popularity of RaaS makes it more difficult for analysts to determine who is behind an attack since the threat actors are not so easily differentiable anymore [4, p. 4f]. Another important type of provider in the ransomware ecosystem is the so-called 'Initial Access Broker', which provides access (e.g. log-in credentials) to potential victims [4, p. 19f]. In the last years, the number of accesses via exploitation of 0-day vulnerabilities has increased which were in the past only available to highly sophisticated actors emphasising the growing expertise and monetary means in that field [12, p. 42], [39]. Figure 2 represents a more detailed model of roles in a ransomware incident. According to Northwave, their specialists have noticed in recent years that actors concentrate on one of the presented roles and tasks [43].

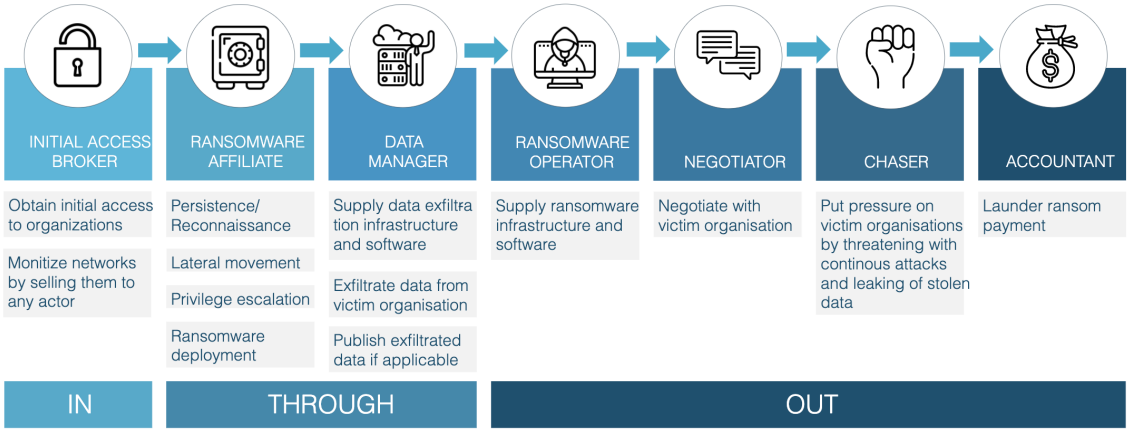


FIGURE 2: Ransomware role model derived from incident response experience of Northwave. It describes the various roles of attackers involved in a ransomware incident and the tasks a role usually executes. Image source [43].

1.1.3 Ransomware Characterization

A typical ransomware attack can be characterised in different ways, depending on the chosen framework. Prominent frameworks are the cyber kill chain [44] and the Mitre ATT&CK Framework (see Section 3.3.1). To get a good understanding of a ransomware attack we will use the so-called 'In', 'Through', 'Out' phases introduced by Northwave. During the investigation, the Mitre ATT&CK framework was chosen, since it is standardised, more detailed and thus allows for better comparisons between incidents. Using Northwave's model a ransomware incident can be mapped into three phases [45], as visualized in Figure 2:

In The 'In' phase describes how an attacker gains access into a system. This is often done via phishing, exploiting vulnerabilities, or the abuse of weak credentials.

Through The second phase, 'Through', is about how an attacker moves through a network and gains persistence (foothold), e.g., via privilege escalation.

Out The last phase, the 'Out' phase, includes how an attacker utilizes control over the network and the way the victim is extorted. This usually includes the encryption of data, exfiltration of data and the destruction of backups [45].

In practice, not all of these phases must be performed by the same threat actor, but by actors specialized in specific phases, see Section 1.1.2.

In conclusion, the current developments in ransomware show that it is an evolving, growing and financially lucrative cybercrime business model and a serious threat to companies and institutions. The popularity of double and multiple extortion schemes highlights that data exfiltration is very common in ransomware attacks and there is no guarantee the data is not further used or sold by the attackers. The RaaS business model provides a simple way to conduct ransomware attacks and makes it more difficult to find the actor behind an attack which allows them to attack without a large risk of being identified. Hacker and ransomware groups such as Evil Corp are based in Russia and even when persons belonging to that group are identified and indicted, they mostly do not get prosecuted (with exceptions in early 2022 where Russian authorities dismantled the criminal group REvil [46]), presumably because Russian authorities are hesitant to prosecute their own

citizens [47]. According to US Assistant Attorney General John C. Demers, states such as China, Iran, Russia, and North Korea provide cybercriminals with a safe haven as long as they are open to work for the benefit of the state [48]. How the relationships between states and criminal actors such as ransomware groups look is discussed in the following section.

1.2 About Ransomware Groups and Nation-States

In all incidents studied in this thesis, ransomware was deployed in the final phase of the intrusion. Ransomware is predominantly used as a means for financial gain with prominent threat actors who use or develop this malware such as BlackCat [18] or LockBit [49]. The actor behind the intrusions, APT 41, is not known to be specialised in ransomware, but in other types of financially motivated attacks and espionage [23]. In addition, APT 41 is considered a state-sponsored threat actor, which means that it has some relationship to a governing body, in this case, the Chinese state. Such a relationship fuels the suspicion that there might be another reason behind some of the ransomware attacks performed by this threat actor. To get a better understanding of different types of threat actors and their relations to a state, the following section will give some background information on such relationships in general followed by specific examples of connections between Russian intelligence agencies and criminal groups.

1.2.1 Definitions of Threat Actors

In literature discussing types of threat actors, state or state-sponsored actors are modelled as the same hacker type, 'nation States', whereas ransomware groups are defined as criminal groups, which is an association of so-called 'professionals' or 'organized crime' actors [50]. In opposition to literature, in reports from journalists or security companies there is theoretically a finer distinction between those actors. A nation-state (or state actor) is part of a governmental organisation whereas a state-sponsored actor (or state-affiliated or state-backed) is an external actor with a varying level of relationship with a governmental body. In practice, there is not always a perfect attribution which results in calling an actor state-sponsored without knowing whether it is actually a state-sponsored or a state actor at the time of publication [51, p. 23]. A ransomware group is part of the organized crime environment and normally not affiliated to any state, which does not mean that ransomware is not used by nation states or state-affiliated actors. Another important term and sub-type of threat actors is an Advanced Persistent Threat (APT). Initially a term used by the military with the purpose to be able to collaborate with civilian experts giving away just enough information so that it becomes clear that an attack is more sophisticated than those of other cyber criminals [52, p. 5]. However, APT is nowadays also a term to describe hacker groups with the means and motive for targeted sabotage and espionage contrary to cyber-criminal groups or other financially motivated actors [52, p. 5ff]. An APT is often also a state-sponsored actor. The last term that needs an introduction is cyber proxy. According to T. Maurer this term refers to a non-state "intermediary that conducts or directly contributes to an offensive action that is enabled knowingly, actively or passively, by a beneficiary" [51, p. 17]. This means that cyber proxy is a temporary classification, in contrast to an APT or state-sponsored actor. When the beneficiary is believed to be a state, authors of news articles, reports, or blog posts often refer to a cyber proxy as a state-sponsored actor.

1.2.2 About Relations Between State and Non-State Actors

Oversight and relation of the state towards non-state actors can be grouped into delegation, orchestration, or sanctioning [51, p. 20]. Delegation describes a relationship where the state is in almost full control over the other actor, whereas orchestration refers to a relationship where the state actor provides support without giving precise instructions. Sanctioning is the most passive, whereby a state actor establishes a favourable environment for a non-state actor but does not oversee its activities [51, p. 20f]. The reasons for states to seek cooperation are manifold. Some states may lack cyber-capabilities, or are not financially able to maintain them, and therefore see an opportunity in transferring such tasks to non-state actors [53, p. 10]. Cooperation can also occur from an active non-state actor, for example, the Ukrainian Cyber Forces shared intelligence with the government which in return condoned their operations [51, p. 40]. In general, countries with a liberal democratic system more often establish a relationship of delegation whereas countries non-democratic countries tend to maintain a less constrained type of relationship with non-state actors [54]. There are several benefits for states to cooperate with non-state cyber actors, those include:

Lower costs: Outsourcing such capabilities reduces spending on building up competences if they are not existing yet or not on a desired scale.

May avoid consequences and scrutiny: By using proxys for operations, states may have plausible deniability for their involvement and avoid consequences and scrutiny. This is emphasised by the observation that the general public is more concerned if the consequences of a conflict affect state personnel in contrast to employees of a private company [53, p. 10ff], [51, p. 38ff].

Profit from external expertise: By cooperating with non-state actors, a state may benefit from their expertise which otherwise might not be available to the state [51, p. 38ff].

Prevent jeopardizing of own operations: Cooperation can help to prevent activists from accidental jeopardizing intelligence operations, for example, by attacking a website the state is monitoring [51, p. 38ff]

The advantages on the side of the non-state actors range from material to ideational support from the government. While working to the benefit of the state, examples of recent history show that in return states tolerate the operations of non-state actors and do not act against them [51, p. 40ff].

The interest of ransomware groups is primarily financial gain by means of extortion. In recent years, ransomware attacks changed in different ways. They now also target big organizations and attacks can have large impacts on the organization itself and society (such as the Colonial pipeline company which transports fuel in the Unites States [55], or one of the largest meat producers JBS [56]). In addition, data exfiltration is now a common practice and some groups tend to only exfiltrate data without encrypting any data [32]. Extracting high-valued data, or disrupting the services of critical infrastructure or a prestigious company are part of the toolset of both ransomware gangs and state or state-sponsored actors [57]. This overlap makes outsourcing cyber-capabilities to non-state actors even more compelling. As an example of such outsourcing, the following section discusses the relationship between the state of Russia and criminal groups.

1.2.3 Ransomware Group Example: Russia

As a non-state actor and part of organized crime, ransomware groups are pursued in most states. However, in certain countries, such as Russia, the relationship between the state and select ransomware groups varies from sanctioning to delegation.

Investigations revealed that there are connections between states and ransomware groups in the form of persons who are both active in governmental security services and in criminal groups. In the following this will be described for the Russian Federation. The connections are reported to be on different levels:

Personal connections: A report from the cyber threat intelligence company Analyst1 revealed that hackers with ties to the threat actor EvilCorp also worked for the Federal Security Service (FSB) and still have connections to it [58]. Another report by Recorded Future identified several people which have direct or indirect connections to the criminal underground as well as to the Russian intelligence services such as the General Staff Main Intelligence Directorate (GRU), FSB or the Foreign Intelligence Service (SVR) [16].

Communication channels: Both reports from Analyst1 and Recorded Future reveal that there are well established communication channels the Russian intelligence services and cyber-criminal groups. In addition, leaks of chat messages between members of the RaaS provider Conti reveal that they have been working for or with the FSB [42].

Favorable legislation: Legislation of Russia regarding foreign intelligence gives an indication that operations of ransomware groups might fall in line with the scope of intelligence activities of the Russian state[2] (see below). Data that has been exfiltrated by ransomware groups might benefit the Russian Federation and thus fulfill one principle of foreign intelligence. This is not an argument that can be used in court and does not mean that ransomware groups act with this principle in mind. Nevertheless, this shows that the operations of both actors (intentionally or not) align to a certain degree emphasizing the incentive a state could have to work together with a ransomware group.

Legislation of foreign intelligence: Relevant legislation toward foreign intelligence can be found in the *Russian Law on Foreign Intelligence*. In Chapter 1, Article 5(3) the law mentions that the intelligence activities are performed, amongst others, under the principle of - (3) promotion of economic development, scientific and technical progress of the country and military and technical security of the Russian Federation [59][3].

Outsourcing capabilities to external actors is happening on different levels and scales. Relying partly on non-state actors for offensive actions is common practice and evidence shows that this also applies to ransomware groups even though the specific directives and agreements are not known. The extent of tasks performed by external actors for the benefit of the state varies from country to country, from attacks on critical infrastructure [20] to surveillance of citizens [60]. In a recent article, the Financial Times reported that even Chinese universities cooperate with state-sponsored actors to secretly recruit students

[2]The same might hold for other countries. A comparison between foreign intelligence goals of different countries is not part of this thesis.

[3]The translation was done with an online translator and can therefore differ slightly from the meaning of the original document.

for espionage [61]. Given the benefits of relying on the capabilities of non-state actors and the evidence of existing cooperation, it seems likely that some ransomware attacks performed by ransomware groups and especially state-sponsored threat actors have a state as beneficiary.
Before introducing the research approach of this thesis, the following section will briefly describe works related to it.

2 Related Works

The related works section covers studies or work by others which is similar to aspects of this thesis such as the use of malware as cover, determining the motives behind an intrusion, and the (forensic) investigation of an incident.

2.1 Malware as Cover

The modus operandi of using malware as a cover for other malicious activities does not appear often in threat or incident reports, meaning that it is either not often applied or difficult to identify. However, threat actors have used such methods and are still using them. The following paragraph will give examples for such a modus operandi. In arguably the most prominent campaign of this kind, a wiper with worm-like behaviour was masqueraded as ransomware created by hackers linked to Unit 74455 of the GRU [62]. This malware is known as NotPetya and was targeting Ukraine in particular but spread to the whole world, causing damage of around US $10 billion [9], [63]. Characteristics malware mimics to appear as ransomware are e.g.:

- Files appear to be encrypted
- Ransom note was dropped
- Custom file endings were added to (encrypted) files

Those characteristics exist in different combinations in reported incidents, e.g., Bleeping Computer reported that malware destroyed files on a system except those necessary for the system's basic functionality while dropping a ransom note [64].
Reports of attackers using such an approach date back to 2016, however, it is possible that such tactics have been used earlier. The latest examples of wider use of wipers masquerading themselves as ransomware are from early 2022 when such malware was used against Ukrainian companies, presumably before and as part of the Russian invasion [65]–[68]. It is not clear why threat actors choose such an approach, especially because often the masquerading is revealed quickly by security specialists. Most likely it serves the purpose of hiding the real objective (for example disruption) of the attack and the functionality of the malware at first sight. Other possible explanations are that threat actors try to mislead CERTs in their investigations and countermeasures or that it is a simply different type of ransomware business model, demanding money even though there is no way to decrypt the data again [69]. The appendix contains a table of reports on different incidents where malware was masqueraded as ransomware (Table 2). Besides using ransomware as a cover, other types of malware or more precisely other types of attacks are used to cover up other malicious activities such as bank robbery, credential theft, or espionage. For example, in 2018 attackers used destructive malware on the Banco di Chile to hide malicious Society for Worldwide Interbank Financial Telecommunications (SWIFT) transactions worth US $10 million [70]. In the same year, the security company Positive Technologies reported

that threat actors used malware to damage the boot record of Automated Teller Machines (ATMs) in order to cover the tracks of cash theft attacks [71]. To distract from credential theft, a threat actor deployed a cryptocurrency miner, as reported by Microsoft [72]. A different modus operandi is reported by Neustar based on a survey the company did in 2014 in which they assessed that DDoS attacks are used to distract, for example the security team of a company, from the actual attack, e.g., stealing money or installing malware on the system [73]. A similar approach was reported about the so-called 'IT ARMY of Ukraine' which used a DDoS attack to cover up the exfiltration of private data [74]. In a survey done by Kaspersky in 2016, 56% of the around 4000 interviewed company representatives were confident that DDoS attacks against their company were used as a smokescreen or decoy operation [75]. In 2020, Bleeping Computer reported on ransomware that was probably used to draw away the focus from the installation of information stealing malware on the victim's system [76]. In a report from June 2022, Secureworks assessed with high certainty that Chinese threat actors used ransomware to cover up their espionage activities [77].

2.2 Assessment of Goals and Motives

There are different approaches introduced to study the motivations and goals of cyber criminals and other types of hackers. In their work, Bada et al. provide a systematic review of research from the years 2006-2020 regarding profiling cyber criminals highlighting that there is not a common definition of such profiling. The methods that are regularly used, according to Bada et al., for profiling are "a) interviews; b) case studies; c) psycholinguistic analysis of digital communications; d) crime script analysis; e) behavioural analysis; f) deductive or inductive methodology to analyse the information; g) FBI's criminal profiling framework; h) mathematical framework, constructing typologies for organised cyber-criminal networks; and i) geographic-mathematical framework analysis." [78, p. 6]. Doynikova et al. introduce an ontology to determine the goal of a cyber attack with the help of neuro-fuzzy networks [79]. The authors name four main objectives of attackers, damage, financial gain, political gain and challenge, thrill or status besides different types of attackers [80, p. 16]. Furnell defines a total of seven motivations which are namely, challenge, ego, espionage, ideology, mischief, money, and revenge [81, p. 35]. Meyers et al. come up with more specific motivations for different types of attackers, e.g. by adding disgruntlement as a possible motivation for an insider attack [82]. Chng et al. provide an overview of attacker types and motivations resulting in seven motivations such as curiosity, financial, notoriety, revenge, recreation, ideology, and sexual impulses where espionage is split into ideology and financial [50]. Verizon investigates yearly thousands of incidents and amongst others publishes the results of their analysis of the motives of actors. In their 2022 Data Breach Investigations Report (DBIR), the authors determined eight different motivations for external actors. In over 95% of the incidents the motivation is financial or espionage, whereas other motivations such as ideology or grudge are barely associated with incidents according to Verizon [2, p. 13]. The research presented in this thesis uses some of the findings of Verizon, as it provides information extracted from a high number of incidents over the last years. More details on the data used are provided in Section 3.2.

2.3 Investigation/Attribution

There are frameworks designed for investigations into threat actors and attribution of attacks to a specific group or individual. The most commonly used one is the so-called 'Diamond model' [83], which takes four categories of an attack into account, *victim*, *attacker*, *infrastructure*, and *capability*. Creating a diamond model for different events in

attacks or for attacks themselves can help to find similar attacks and eventually attribute that to an existing cluster or threat actor or identify it as a new campaign/cluster/threat actor. In the book 'Attribution of advanced persistent threats' the author Timo Steffens introduces the Malware, Infrastructure, Control server, Telemetry, Intelligence, Cui bono (MICTIC) Framework [52, p. 46]. It is designed for the technical attribution of an attack from an APT and according to the author is a more detailed version of the diamond model. Another model is the so-called 'Q model' which was introduced by Thomas Rid and Ben Buchanan in 2015 [84]. The goal was to provide a model to guide and explain an investigation to help improve the quality of attribution of cyber attacks and consists of several questions regarding the technical, operational, strategic and communication aspects of an attack/attacker.
In practice, investigations are based on various Indicators of Compromise (IOCs), malware samples, or other artefacts. For example, the security company Arctic Wolf was able to find with a high certainty multiple threat actors working together (Karakurt, the Conti and Diavol ransomware group) [85]. They achieved this (in cooperation with other companies), by finding connections and similarities in cryptocurrency transactions and wallets used by the groups, aspects of the attacks such as tools and malware, and contents of leaked internal chats of the Conti ransomware group [85]. The analysis of the malware deployed during an attack, can give information on what the malware is capable of and help in the attribution of the threat actor and connections to other threat actors by e.g. identifying similarities to other malware. For example, researchers found very similar code in the ransomware of Lockbit 3.0 and the older BlackMatter ransomware, followed by the hypothesis that Lockbit may have hired former BlackMatter developers [86].

Regarding the use of malware as cover or ransomware as masquerade, other work has covered such intrusion individually up to great detail, however, not in a broader collection. The table presented in the appendix of this thesis (Table 2) is therefore a novel contribution. There are different ways of investigating intrusion and assessing the motivation behind the attack. The reason why in this thesis a new approach is chosen and not one presented in this section is explained in the subsequent paragraphs.

3 Approach and Methodology

This section aims to introduce the data gathering, processing and analysis methods used to study the research questions.

3.1 Approach

The methodology chosen for this research is influenced by the research questions. Similar significance for the choice is the availability and type of data at Northwave (see Section 3.2). Another relevant aspect is that the attribution of the attacks to a threat actor (APT 41) was already done. Finding direct evidence that a threat actor used ransomware as a cover for other malicious activity is rarely possible. This also applies to the studied incidents, however, experts of Northwave's CERT observed characteristics which could indicate such a modus operandi even though it is not apparent at first sight. Those cases are described in more detail in Section 3.2.1.

Initially, the approach was based on an intrusion analysis supported by the diamond mode, the Mitre ATT&CK Framework, and Malware Information Sharing Platform (MISP) as a data platform (see Section 3.3.1 and Section 3.3.2). The aim was to compare the intrusion

analysis with other ransomware incidents and draw conclusions from that on whether other malicious activities took place during the ransomware attack. However, while preparing the incidents for the intrusion analysis it became clear that there was not enough data available in each of the suspicious incidents and that only comparing the intrusion analysis will not lead to results from which any conclusion could have been drawn regarding the hypothesis. Missing was data such as clear information on the initial access vector, indicators that could reveal the infrastructure used by the threat actors, and malicious binaries. Since the threat actors made use of only publicly available tools in the attack, a forensic investigation of these tools would be less insightful (e.g., no insights into code similarity with other malware). Surely, an intrusion analysis could provide a good overview of an incident and would make it possible to understand how the attacker proceeded. However, with no direct evidence, it would have been difficult to interpret the findings towards the possibility that the threat actor tried to exfiltrate data or sabotaged the victim's computer network.

The main aspect that contributed to the change to a different methodology was the uncertainty and difficulty in finding direct evidence. Therefore, the new approach did not focus on finding direct evidence of other malicious activities but rather to assess the goal/motive of the attacks. The premise of the new approach is that assessing (with remaining uncertainty) the motivation/goal of an attack helps to determine whether the threat actor tried to cover up other malicious activities. The assumption therefore is that if the actions of the threat actor point towards a financial goal of a ransomware attack then it was likely only a ransomware attack. In contrast, when the actions point towards an espionage motivation of a ransomware attack then there is a high chance that the threat actor not only deployed ransomware but likely performed additional malicious actions. The incidents described in Section 3.2.1 will be compared to three different threat profiles, financial gain, espionage, and sabotage/destruction.

Besides the chosen three there are, generally speaking, the motives Challenge, Ego, Mischief, Revenge, or Ideology [81, p. 35]. However, according to Verizon most of these motivations play a negligible role in the motivation behind an incident. In their DBIR of 2022, Verizon reports that the motive behind incidents[4] was in over 90% financial gain followed by espionage with around 5% [2, p. 13]. The threat intelligence company Intel471 states in a blog post that usually cyber attacks can either be attributed to nation-states or actors with the goal of financial gain [87]. In addition, the actor to which six of the incidents in this study are attributed is known to act out of the motive of espionage and financial gain [23]. As a result, out of all possible motives, espionage and financial gain are chosen for this research as possible motives behind the six incidents. A third profile was added as a consequence of reports that there have been campaigns in which destructive malware, disguised as ransomware, was used to destroy data on the victim's computer network [9], [69]. The incidents of Northwave all involve ransomware so this third profile also covers the destructive goal a ransomware attack might have. These three profiles are further defined in Section 3.4 and the underlying data in Section 3.2. For the representation of incidents Northwave uses MISP and in order to compare actions of attackers used during an intrusion, those are mapped to Mitre ATT&CK. The actual comparison of techniques is done in Jupyter Notebooks [88].

[4]This refers to 2209 investigated incidents in which data was revealed to an illegitimate party and the attack was performed by an external party.

With the newly designed approach, it will not be possible to get a definite answer on whether the activities performed during the intrusion were all needed and part of a successful ransomware attack. What it provides though, is a founded baseline and expectations which help to interpret the existing evidence resulting in a better outcome as a basis for the evaluation of the research question.

3.2 Data

This section entails the description of the available data for the research. The data on incidents will be explained in more detail.

The study is based on data gathered from two main sources, Northwave's internal data and online sources. The Northwave internal sources can be described as the knowledge of Northwave employees and data of handled incidents. Online sources refer to all reports, scientific references, blog posts, and other material obtained from the internet.

3.2.1 Incident Data

The CERT of Northwave handles cyber incidents of companies in various European countries. Part of the incident response service of Northwave is a forensic investigation of the intrusion to find out how the attacker got into the network, how the attacker moved through the network and how the attacker exploit the access to the network. The investigation is based on server images, and log files of different services, such as the Firewall. However, the available data sources vary from incident to incident, this is due to the fact that companies have different logging policies or attackers successfully covered their tracks by, for example, deleting log files. Besides general information about the victim and the attack, the incident reports from Northwave include detailed information on the actions performed by the attacker, tools used, commands, scripts and conversations. In addition, technical information such as Internet Protocol (IP) addresses and hashes of binaries are provided. That information varies greatly between events and depends on what the analyst was able to find and how many tracks were covered by the attacker(s), for instance, by deleting binaries or log files. As a result, often reports do not entail binaries of the malware, hashes of binaries, specific commands executed, complete initial access vectors, and detailed information on the infrastructure of the attackers.

Northwave Cases

The investigation is based on the reports of six ransomware incidents which are attributed to the threat actor APT 41. The attacks happened between April 2020 and August 2021 and targeted companies in central Europe. The companies are located in various market sectors, including but not limited to, research, manufacturing, construction and retail. In all cases, Northwave was able to help the affected clients to recover and continue with their businesses. Besides the encryption tools, the incidents shared other tools, scripts and binaries. For example a script called `copys.bat`, as seen in Figure 3. In the earliest of the six attacks parts of the content of the script were executed manually step by step. There were minor changes to the script in some incidents, but overall the script is designed to place the ransom note, turn on Bitlocker and restart the system. The usage of this script is also reported by a different security company (Further_eye) in a similar attack [89], with its content shown in Figure 4 (the Bitlocker related commands are are not included in this case).

```
copy "c:\Readme.txt" "c:\Documents and Settings\All Users\desktop\Readme 1.txt" /y
copy "c:\Readme.txt" "c:\Documents and Settings\All Users\desktop\Readme 2.txt" /y
copy "c:\Readme.txt" "c:\Documents and Settings\All Users\desktop\Readme 3.txt" /y
copy "c:\Readme.txt" "c:\Documents and Settings\All Users\desktop\Readme 4.txt" /y
copy "c:\Readme.txt" "c:\Documents and Settings\All Users\desktop\Readme 5.txt" /y
copy "c:\Readme.txt" "c:\Documents and Settings\All Users\desktop\Readme 6.txt" /y
copy "c:\Readme.txt" "c:\Documents and Settings\All Users\desktop\Readme 7.txt" /y
copy "c:\Readme.txt" "c:\Documents and Settings\All Users\desktop\Readme 8.txt" /y
copy "c:\Readme.txt" "c:\Documents and Settings\All Users\desktop\Readme 9.txt" /y
copy "c:\Readme.txt" "c:\Documents and Settings\All Users\Start Menu\Programs\Startup\Readme.txt" /y
copy "c:\Readme.txt" "c:\users\public\desktop\Readme 1.txt" /y
copy "c:\Readme.txt" "c:\users\public\desktop\Readme 2.txt" /y
copy "c:\Readme.txt" "c:\users\public\desktop\Readme 3.txt" /y
copy "c:\Readme.txt" "c:\users\public\desktop\Readme 4.txt" /y
copy "c:\Readme.txt" "c:\users\public\desktop\Readme 5.txt" /y
copy "c:\Readme.txt" "c:\users\public\desktop\Readme 6.txt" /y
copy "c:\Readme.txt" "c:\users\public\desktop\Readme 7.txt" /y
copy "c:\Readme.txt" "c:\users\public\desktop\Readme 8.txt" /y
copy "c:\Readme.txt" "c:\users\public\desktop\Readme 9.txt" /y
copy "c:\Readme.txt" "c:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\Readme.txt" /y
reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE" /f 33
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE" /v EnableBDEWithNoTPM /t REG_DWORD /d "0x1" /f
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE" /v UseAdvancedStartup /t REG_DWORD /d "0x1" /f
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE" /v RecoveryKeyMessage /t REG_SZ /d ^
"□□□□□n□ □□▲□□ ق□□□ö▲□□ □Ł₹▲₹ □□□, □□ö□ ق ا □○□□ □□ admin@google.com." /f
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE" /v RecoveryKeyMessageSource /t REG_DWORD /d "0x2" /f
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE" /v RecoveryKeyUrl /t REG_SZ /d " " /f
powershell -command install-windowsfeature bitlocker -restart
ServerManagerCmd -install BitLocker -restart
shutdown -r -t 0 -f
```

FIGURE 3: Content of one of the `copys.bat` scripts found in all of the six APT 41 incidents at Northwave. The script places the ransom note, configures and installs Bitlocker and forces the system to reboot immediately.

```
copy "c:\Readme_unlock.txt" "c:\Documents and Settings\All Users\desktop\Readme unlock 1.txt" /y
copy "c:\Readme unlock.txt" "c:\Documents and Settings\All Users\desktop\Readme unlock 2.txt" /y
copy "c:\Readme unlock.txt" "c:\Documents and Settings\All Users\desktop Readme unlock 3.txt" /y
copy "c:\Readme unlock.txt" "c:\Documents and Settings\All Users\desktop\Readme unlock 4.txt" /y
copy "c:\Readme unlock.txt" "c:\Documents and Settings\All Users\desktop Readme unlock 5.txt" /y
copy "c:\Readme unlock.txt" "c:\Documents and Settings\All Users\desktop\Readme unlock 6.txt" /y
copy "c:\Readme unlock.txt" "c:\Documents and Settings\All Users\desktop Readme unlock 7.txt" /y
copy "c:\Readme unlock.txt" "c:\Documents and Settings\All Users\desktop\Readme unlock 8.txt" /y
copy "c:\Readme_unlock.txt" "c:\Documents and Settings\All Users\desktop\Readme unlock 9.txt" /y
copy "c:\Readme unlock.txt" "c:\Documents and Settings\All Users\Start Menu\Programs\Startup\Readme unlock.txt" /y
copy "c:\Readme unlock.txt" "c:\users\public\desktop\Readme unlock 1.txt" /y
copy "c:\Readme unlock.txt" "c:\users\public\desktop\Readme unlock 2.txt" /y
copy "c:\Readme unlock.txt" "c:\users\public\desktop\Readme unlock 3.txt" /y
copy "c:\Readme unlock.txt" "c:\users\public\desktop\Readme unlock 4.txt" /y
copy "c:\Readme unlock.txt" "c:\users\public\desktop\Readme unlock 5.txt" /y
copy "c:\Readme unlock.txt" "c:\users\public\desktop\Readme unlock 6.txt" /y
copy "c:\Readme unlock.txt" "c:\users\public\desktop\Readme unlock 7.txt" /y
copy "c:\Readme unlock.txt" "c:\users\public\desktop\Readme unlock 8.txt" /y
copy "c:\Readme unlock.txt" "c:\users\public\desktop\Readme unlock 9.txt" /y
copy "c:\Readme unlock.txt" "c:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\readme unlock.txt" /y
shutdown -r -t 0 -f
```

FIGURE 4: Content of the `copys.bat` script from Further_eye which places the ransom note and forces the system to reboot immediately. Source: [89].

An additional incident shares the use of Bitlocker for encryption with the other six cases. However, other characteristics are quite different, for example, the initial access vector and deployed web shells overlapped with those of the Hades ransomware group and the Hafnium threat actor [90], [91]. The Hafnium threat actors are, same as APT 41, known for espionage and could therefore also be of interest to this study. However, this incident includes many uncertainties and as a result is not included in this research. Those uncertainties

arise from the fact that there was very little forensic evidence available for investigation, leaving too much room open for speculation on the threat actor and other aspects of the attack. Other companies, such as Lifars, Synacktiv, Further_eye, and Varonis, reported cases which are very similar [15], [89], [92], [93]. Taking the other reports into account, the attacks were carried out in a time frame from March 2020 to the last quarter of 2021 (the exact date of the last occurring attack was not published).
In all incidents, those seen by Northwave and other companies, there were no indications of data exfiltration and neither did the threat actor threaten to leak data, as is typically done in multiple extortion schemes (see Section 1.1). The reports of the other companies did not suggest that other malicious activities besides ransomware were carried out by the threat actor.

The attribution to APT 41 was done with the help of two publicly available reports by Lifars [15] and Mandiant [94]. In their report, Mandiant attributed several intrusions to APT 41 providing, amongst others, IPs, domains, and files used by the threat actor. Lifars, seeing multiple overlaps in a ransomware incident with the APT 41 IOCs from Mandiant, attributed the ransomware attack to APT 41. As a result of similarities in files and tools of the Northwave ransomware cases to the one of Lifars, Northwave attributed, with sufficient certainty, the cases also to APT 41. The overlaps between the Northwave cases and the report by Lifars include (amount of overlap changes between cases):

- IP address: 176.123.3[.]104
- File hash (md5): 88ef5955f8fa58e141da85580006b284
- File: 'o.txt'
- Tools: Bitlocker, BestCrypt, NATBypass, PsExec
- Ransom note

3.2.2 Verizon Data

The data of Verizon which is published in their annual report [95], [96] is an ideal source for the analysis of actions performed by the attacker(s) during an incident and the possible motive of the attacker. In these reports, Verizon provides data about how often which actions are used by attackers with different motives such as financial gain or espionage. The motive of sabotage or disruption is not present in that data and therefore is not part of that threat profile (see Section 3.4). Their findings are based on their analysis of 29,207 incidents (2021) [95, p. 6] and 23,896 Incidents (2022) [2, p. 6]. Verizon distinguishes between actions performed by an attacking entity such as *Hacking*, *Malware* or *Misuse*. In addition, there is a distinction between types of action in *Variety* and *Vector*. The present research solely makes use of the actions *Hacking* and *Malware* for the reason that they fit best to the studied incidents. Additionally, *Variety* and *Vector* are merged since this differentiation does not exist in incident reports of Northwave. The data on attacker actions is based on the Vocabulary for Event Recording and Incident Sharing (VERIS) framework. In this work, however, the Mitre ATT&CK framework is used and therefore, a mapping from VERIS to Mitre ATT&CK is applied which is based on the mapping that is provided by Verizon itself [97]. Due to its incomplete and outdated content, the mapping was partially completed and renewed. This refers to the fact that not all mappings were relevant for the analysis and thus omitted. In addition, an action was removed called "Backdoor or C2" which occurs often in the data of Verizon. However, it is vaguely defined since it leaves open whether an artefact is a backdoor or Command and Control (C2).

3.3 Frameworks and Tools

This section is dedicated to brief introductions to the tool and framework used in this thesis. These include the MITRE ATT&CK Framework and the MISP platform.

3.3.1 Mitre ATT&CK

The Mitre ATT&CK framework is a public framework that can be used to characterize attacks. The framework consists of a matrix structure which represents the techniques and tactics of an adversary. Each of the 14 matrix columns represents a tactic in the overall workflow of an adversary, such as *Reconnaissance*, *Resource Development*, *Initial Access*, and, *Execution Persistence*. The rows represent different techniques of a tactic, such as *Exploit Public-Facing Application* or *Data Encoding* and existing mitigation [98]. Table 1 shows the parts of the matrix. For every entry exists a detailed description, a unique id, and mitigation and detection technique(s). Using the different techniques and tactics it is possible to characterise an incident by assigning a tactic and if possible a technique to each action an attacker performs. It depends on the knowledge about the attackers' actions whether it is possible to identify a specific technique of an attacker and assign an ATT&CK technique to it.

Reconnaissance 10 techniques	**Resource Development** 7 techniques	**Initial Access** 9 techniques	**...** ...
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	...
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	...
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	...
...	...	...	

TABLE 1: First three entries of the Mitre ATT&CK matrix. The number in brackets represents the number of sub-techniques.

3.3.2 Malware Information Sharing Platform

MISP [99] is a platform to store, visualize, and share information about malware or general security incidents. Northwave feeds its incident reports into the platform to share details with clients and partners as well as generate intelligence from all of those incidents. MISP makes it possible to easily find common attack patterns, infrastructure or other aspects of attacks between incidents. The Mitre ATT&CK framework is fully integrated into MISP which allows tagging observed actions performed by the attacker with ATT&CK techniques.

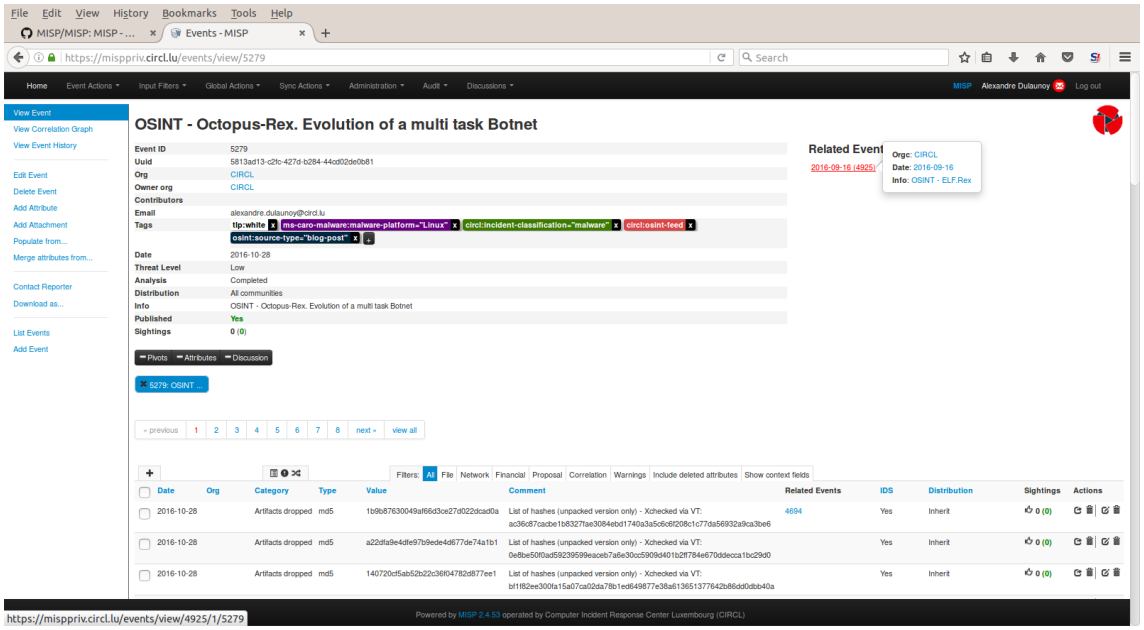


FIGURE 5: Example of an event in MISP. Image source: [100]

3.4 Threat Profiles

In the following, the threat profiles are defined, which will be used to get a better understanding of what the motivation/goal of the attacks observed by Northwave could be. The profiles consist of questions based on assumptions and expected behaviour which aim to help the analyst to decide which profile fits best to one or a group of incidents.

Financial Gain

The threat profile for actors or campaigns with the main goal of financial gain consists of the following characteristics:

- *Actor History.* Is the actor known for conducting financially motivated attacks?
- *Demanded Ransom.* Is the demanded ransom of a similar amount as reported by Coveware in the same time period? Is the demanded ransom around 2% of the victim's annual revenue? Does the amount of the ransom correspond with the number of affected systems in the victim's network?
- *Techniques.* Do the used techniques match with the ones reported by Verizon as being used in incidents with the goal of financial gain?

Espionage

- *Actor History.* Is the actor known for conducting cyber espionage?
- *Position Victim.* Does the victim produce goods or services of potential interest to foreign countries or does it operate in a sector of interest?
- *Techniques.* Do the used techniques match with the ones reported by Verizon as being used in incidents with the goal of espionage?

Sabotage/Disruption/Damage

- *Actor History.* Is the actor known for conducting such attacks?
- *Recovery.* Was there evidence of any steps taken by the attacker to hinder data recovery (for example, corrupted data, unsuccessful data recovery with the paid decryptor, no contact details of the attackers)?
- *Position Victim.* Is the victim a crucial company for a country's economy or infrastructure?
- *Announcement.* Did a threat actor announce or claim this attack?
- *Worm.* Did the malware show signs of worm-like behaviour?

3.4.1 Profiles Elaboration

The profile characteristics were chosen based on observations and experience by Northwave or by studying reports on cyber-attacks and threat actor behaviour.
The *Actor History* plays a role in every profile following the reasoning that when a threat actor is reported to only conduct financially motivated attacks, then a different attack by the same actor is probably also financially motivated. Some actors, however, are known for having attacked out of different motives/goals, such as financial gain and espionage in the case of APT 41 [23]. The details of the *Demanded Ransom* characteristic are based on observations and insight gained by Northwave in the last years. The assumption is that if the demand is much lower than the expected value, the likelihood increases that the financial gain through the ransom was not the main goal of the attack. The *Position Victim* characteristic accounts for the changes in the likelihood of an impending attack motivated by financial gain, espionage or sabotage depending on the type of company and the goods or services it produces. When a nation-state is involved in espionage, the goal can be to improve its knowledge about certain technologies [101, p.39]. The *Recovery* aspect of the *Sabotage/Disruption/Damage* profile is based on the reported behaviour of wipers which were masqueraded as ransomware and had for example, no contact details in their ransom notes or the data was not encrypted but overwritten with random bytes [66], [102]. One threat actor officially claimed responsibility for destructive ransomware attacks and revealed the political motivation behind the goal of these attacks [103]. As a result, this behaviour is included in the profile (*Announcement* characteristic). Certain destructive malware showed worm-like behaviour such as NotPetya [69].

Challenges regarding the available data and the topic to study led to the creation of a special research approach. The new approach allows the assessment of the motive and goal of an attack even when not every detail of the intrusion is known. During the assessment every characteristic in each profile/motive is evaluated regarding six Northwave cases and the profile with the most positively answered characteristics is assumed to be the most likely profile/motive. The results of this approach are shown in the following section.

4 Results

In this section the results of the study are presented. These cover the investigation of the suspicious cases as well as provide a closer look into the use of legitimate software for the encryption of data during a ransomware attack.

4.1 Profile Comparison

At first, the results of the six APT 41 cases are presented. The cases were evaluated regarding the created threat profiles with the aim to assess the motivation of the attack.

Actor History: This characteristic is present in all three profiles and since all six cases have been attributed with sufficient certainty to the threat actor APT 41, thus, evaluation is possible. According to reports, APT 41 has been conducting attacks with the goal of espionage and financial gain [23]. However, disruptive attacks have not been reported to the knowledge of the authors.
As a result, the likelihood is higher for the goal of these six attacks to be either espionage or financial gain.

ATT&CK Techniques: A baseline for such techniques is only available for espionage and financially motivated actors and therefore only present on those profiles. Figure 6 shows the comparison between the techniques observed in Northwave cases and the Verizon cases. The graphs are based on the six APT 41 cases from Northwave and around 2500 incidents for espionage and around 5800 for the financial motive for the Verizon data.

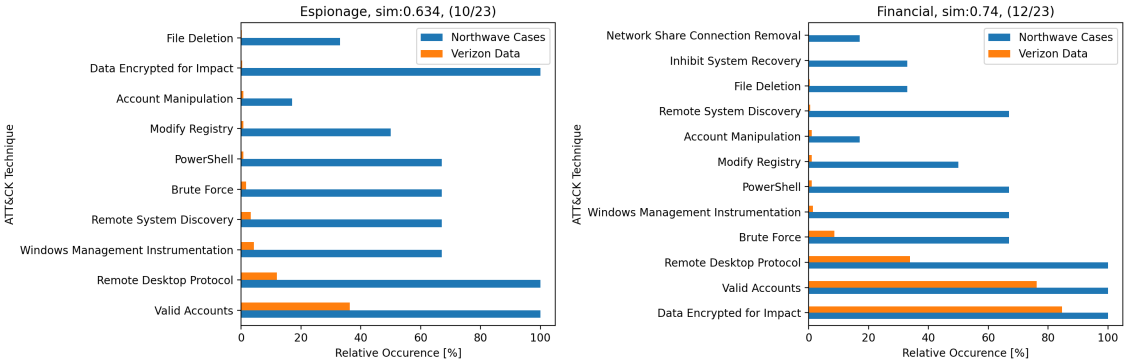


FIGURE 6: Comparison of Mitre ATT&CK techniques between the Northwave APT 41 cases and Verizon data (Hacking and Malware combined). Left: Comparison to ATT&CK Techniques used in attacks with espionage as motive. Right: Comparison to attacks with financial gain as motive.

The similarity value, seen in the title of Figure 6, refers to the cosine similarity between the blue (Northwave) and orange (Verizon) bars. The type of similarity value is arbitrary, this measure is simply used to quantify the difference between the blue and orange bars. The fraction in the title refers to how many techniques that are present in the Verizon data (16 and 19) match with the 29 different techniques observed in all six Northwave cases. The comparison shows that the Mitre ATT&CK techniques observed at the six Northwave incidents are more similar to those used in financially motivated incidents (Verizon data).

The results of this comparison should not be interpreted as exact numbers and as a clear indication of what the motivation of the actors behind the attacks was. There are various uncertainties and limitations associated with this analysis. Nevertheless, it gives an indication that the motive was more likely financial gain than espionage.

Demanded Ransom: The paid ransom is in five out of the six cases either in between (three cases) the median and average value reported by Coveware [104]–[108] or above (two cases). In the incident where the paid ransom was lower than the average and median values of Coveware, the demanded ransom was also much lower than 2% of the annual revenue. This could be an indication that the financial gain of this attack was not the primary goal. However, when looking at the number of encrypted servers or workstations, it shows that this incident was also the incident out of the six where the least amount of servers was encrypted. The incident in which the attackers could encrypt the highest number of servers was also the one with the highest ransom.

Characteristics Attacked Entity: The profiles of espionage and sabotage/disruption include a characteristic that is related to the sector it is operating in and the company itself. The companies that have been attacked operate in various sectors. However, they are neither seen as part of critical infrastructure nor exceptionally essential to the economy, which reduces the likelihood of a sabotage/disruptive attack. Two of the victims produce special goods which are market leading or at least specialized goods with only a few companies who can produce those. This would make these companies potential targets for espionage. However, the goods produced by a company or its intellectual property alone is not a significant indicator of the motivation of an attack. Northwave has helped multiple companies which fall into this category where the attack did not give any indication that it was motivated by anything other than financial gain.

Recovery: The communication with the attackers and the recovery using the keys that the attackers provided after paying the ransom showed no signs of any plans to hinder the recovery process. A communication channel could be established and with the received keys, decryption was possible.

Announcement: There was no publication or announcement of any kind regarding the observed attacks. Without public announcements it can be assumed that the goal of the attackers was not to attract attention, for example, to amplify the implications of sabotage and destructive attacks.

Worm: None of the malware had indications of worm-like behaviour. Meaning that its goal was not to spread itself to cause as much damage as possible, for example as seen in the NotPetya or WannaCry malware [63].

Paragraphs **Recovery**, **Announcement**, and **Worm** contribute to the proposition that the goal of the attacks was not the sabotage, damage or disruption of the victims operations. By examining all partial results and fusing them together, the profile that fits best to the seen observed attacks is the financial goal profile. There are aspects such as the actor's history or the use of unusual tools for the encryption that rise the suspicion towards another goal than financial gain. However, by taking all the aspects of the profiles into account financial gain is the most likely motive, meaning that certain aspects of the attacks are unusual but overall not unusual enough to provide sufficient ground to suspect the existence of other malicious activities during the incident. As the threat actor is known to conduct both financially motivated attacks and espionage [23], it is possible that in the six studied

cases the goal was financial gain. In a recent blog post (July 2022) by threat intelligence analysts 'The intrusion group', the authors come to the conclusion, that APT 41 is probably more of a network of individual Chinese threat actors instead of an actual group. Actors in this network share tools and knowledge and appear to have a high level of autonomy regarding their operations, according to the blog post [109]. Given this information, there is a chance that the intrusions investigated in this thesis were a side project of a threat actor of the APT 41 network.

4.2 On Off-the-shelf Encryption Software

The tools used for the encryption of the data have not been seen before by the CERT team members of Northwave and therefore, this section will take a closer look at those tools. The attackers used Bitlocker [110] and BestCrypt [111] for the encryption, which are publicly available tools. The use of publicly available open source or proprietary legitimate tools in hacking operations is very common. Almost every attack includes tools that are freely available such as Mimikatz [112] or proprietary tools such as Cobalt Strike [113]. In addition, cyber-criminals often use software which is already on the victim's system for their malicious activities, which is referred to as 'living-off-the-land' techniques [114]. However, those tools are usually used for privilege escalation, execution, or lateral movement and not for encryption. For the encryption threat, actors mostly use their 'own' malware, which makes the observed cases by Northwave outstanding in that regard. Nevertheless, those cases are not the only ones where threat actors used legitimate tools for encryption. There are reports about other threat actors using such tools as mentioned in the following:

1. Qwerty used GnuPG (2018) [115]
2. Moses Staff used DiskCryptor (2021) [116]
3. Mamba used DiskCryptor (2021) [117]
4. Phosphorus and/or a sub group of it, DEV-0270, used Bitlocker and DiskCryptor (2021, 2022) [118], [119]
5. Hades used Bitlocker (2021, attribution not clear, Northwave)
6. APT 41 used Bitlocker and BestCrypt (2020) [15]
7. THT used BestCrypt (and Bitlocker) (2020) [120]
8. DeepBlueMagic used Bitlocker and BestCrypt (2021) [93]

There is a big overlap between the incidents reported in bullet points 6-8 such as the tooling and the ransom note, which leads to the speculation that there is a connection between them. This connection could mean that the actors worked together, imitated each other, or one actor intentionally tried to give the impression that these attacks have been conducted by various actors. The reason why specific actors use legitimate software for encryption in certain campaigns and not special malware is not clear, but there are some speculations and possible explanations. On the one hand, using existing tools is cheap and if applied correctly works without errors. On the other hand, such tools might not come with all the needed features and support for various platforms. The authors of a report about APT 35 believe that the use of open source tools reflects the insufficient coding skills of the attackers [121]. Another research team comments the reason for the way Moses Staff used pen source encryption tools as probably having poor coding skills, little experience with ransomware and maybe not financial gain as the primary goal (encryption possibly

reversible, no ransom demand and no decryption option) [116]. The reason for the use of Bitlocker in connection with another encryption tool might be that Bitlocker is not supported on all systems [118].
Taking those aspects into account and looking again at the Northwave cases of APT 41 it is possible to see some connections. APT 41 is not known to be an established ransomware group, so the use of Bitlocker and BestCrypt might be the result of lacking knowledge about ransomware. In all six cases, Bitlocker was used on systems with only a single volume and BestCrypt on systems with multiple volumes. Why exactly this setup was chosen is not clear. Most likely some technical aspects of Bitlocker and BestCrypt led to this decision.

The results show that the goal of the threat actor, APT 41, was most likely financial gain. Coming back to the assumption of the research approach that would mean that deploying ransomware was likely not to cover up other malicious activities. The use of legitimate software for the encryption of data is an unusual, but not unique approach and might show that the threat actor is not experienced in ransomware operations. The following section discussed the research questions and results in more details and provides limitations to the results presented here.

5 Discussion

The aim of the discussion section is to revisit the research by summarizing the relevant aspects of each of the questions. In addition, conflicting interpretations are discussed and limitations of the study are presented. In addition, the section includes open questions that came up during the research but were beyond the scope of this thesis and as such remain unanswered.

5.1 Revisiting Research Questions

The main hypothesis of this thesis is **To what extent is ransomware used as cover for other malicious activities?** The known extent of such an approach is limited given that there are barely any reports on it in contrast to reports of 'normal' ransomware incidents. The intent of a cover-up to not be discovered contributes to the lack of knowledge on the total extent on the use of ransomware as cover. In many of the reported cases ransomware is used as cover for politically motivated attacks be it espionage or destruction or sabotage in which wiper malware is masqueraded as ransomware.

The profile comparison in Section 4.1 aims to gain additional insights on whether the intention of using ransomware in the six Northwave cases was to cover up other activities such as sabotage or espionage. The assessment resulted in the assumption that the actors were purely financially motivated and therefore, the use of ransomware was likely not a cover-up. However, the evaluation of the individual profile characteristics (see Section 4.1) is not unequivocal proof that the threat actor was financially motivated and that ransomware did not serve as a cover for other malicious activities. The following presents a few conflicting explanations.

Ransom Amount: The threat actor (APT 41) could have chosen a ransom amount in line with or higher than the numbers reported by Coveware, on purpose, to make it seem that the focus is the monetary gain. The choice of demanding a very low ransom does not necessarily mean that the goal is not financial gain, instead, it could imply that a threat actor is more interested in staying under the radar of law enforcement to improve business continuity, or with the hope that the chances for receiving the

ransom is higher (quantity over quality). In the end, the real reason for the value of the ransom is not known.

Multiple Motivations: There is the possibility that the threat actor had two motivations and that the assessment revealed only the financial motivation. Since there was insufficient data to get a complete picture of the whole intrusion, it may be that the threat actor successfully hid actions which would have revealed an additional motivation. This is a possibility which should not be disregarded, however, in such investigations it rarely occurs that all possible data is available and therefore it is necessary to work with the available data and base the assessment on that.

Initial Assumption: Besides challenging the evaluation one can also challenge the initial assumption that when an attack is financially motivated and the threat actor used ransomware, then there is a high chance that the goal of the whole attack was to earn money via the ransom. Examples of financially motivated ransomware groups which take political stances show that attacking a company with ransomware can also serve a political goal, e.g., by showing power or disrupting services while making money [122]. The threat profile *sabotage* evaluates this scenario and in this case, did not result in any indication of such a scenario.

This section aims to summarise the relevant insights to answer the research question **Secondary 1: In what way are the suspicious cases from Northwave different to ransomware cases which have no indication of an intrusion with multiple motivations?**

These three aspects define the biggest differences between the suspicious cases and the average ransomware case at Northwave. The average case refers to what is usually observed and found during investigations such as that mostly the motivation behind a ransomware case is financial gain or at least there are mostly no indications for a contrary assessment.

Threat Actor: In all ransomware cases at Northwave where the actor or ransomware type was known, the suspicious cases are the only ones where the threat actor is an APT. This is based on the knowledge and finding of the CERT team of Northwave.

Legitimate Software for Encryption: In no other incident investigated by Northwave, except for the one mentioned in Section 3.2.1, legitimate tools such as Bitlocker and BestCrypt were used for the encryption of data. For more details see Section 4.2.

Tools: Certain scripts or tools were only observed in those cases and have not been seen used in other incidents.

The last aspect is merely a new aspect of the six APT 41 attacks but comes in combination with the fact that the attacks were performed by the same threat actor, meaning that the tactics, techniques and procedures are almost the same in each attack.
In summary, the biggest differences and the reason for the initial suspicion are the threat actor APT 41 and the use of legitimate encryption tools Bitlocker and BestCrypt.
The findings could be interpreted differently, for example regarding the threat actor. It is possible that the attribution of the cases to APT 41 is not correct. Even though there is overlap with incidents which have been attributed to APT 41, it does not mean that it was indeed the same threat actor. In addition, it could be that the attribution from security companies Northwave relied on was already inaccurate.

The introduction presented arguments why ransomware could be a good cover-up for other malicious activities. There are, however, also some unanswered questions why ransomware

is not a good cover or may even be contra-productive. If an attacker is undetected in a computer system, deploying ransomware results in the complete opposite and the victim detects the intrusion shortly after. Why would a threat actor not try to stay undetected? The correct answer to these questions is not known, nevertheless, there are possible explanations. Threat actors could deploy ransomware trying to get additional money out of the attack. Moreover, analysts suggest that ransomware is used as a security measure to destroy evidence and cover tracks [19], [77]. A ransomware incident disrupts the business operations of the affected company (on average it takes one month to recover according to Sophos[14]), the goal of incident response is to get the company back to business as fast and as securely possible (according to Northwave). As a result, deploying ransomware takes the focus to business recovery and away from a thorough investing in malicious activities other than ransomware as it is suggested by experts at Secureworks and Dragos [10], [77]. Thus, deploying ransomware can be effective for hiding other activities and therefore, might be chosen in favour of an intrusion which focuses on staying completely undetected.

The Section 1.2 covered the background to the research question (SQ2) **To what extent do interests/operations of ransomware groups and states overlap and what could be the benefits for both sides?**. The interests and operations of non-state actors such as ransomware groups and state actors overlap on different levels. Reports show that there is overlapping in tools and techniques, often with the aim to hide their identities [123], [124]. On the victim level, ransomware groups target, amongst others, high-value companies and even those important to critical infrastructure. In addition, objectives such as the extraction of information with great value are shared between the two types of actors. In 2022 the Conti ransomware group caused Costa Rica to declare a state emergency and even addressed the citizens of Costa Rica urging them to overthrow the government [125]. Such operation were not known to be executed by ransomware groups but by foreign intelligence agencies such as the the Central Intelligence Agency (CIA) [126]. Besides the operational level, there is also an overlap in personnel, as shown in the example of Russia where well-established relationships exist between criminal organizations and the FSB. The benefits for the state are the cost efficiency of the possibility of denying any involvement and responsibility if an attack gets investigated for potentially being 'ordered' by the state. Additionally, it theoretically provides a better cover for intelligence operations. As an example, by letting a ransomware group extract important information from a victim masquerading it as a usual ransomware attack with multiple extortions (there is no direct evidence available for the existence of such a scenario). For the criminal group, the benefits range from protection from prosecution to support in ideation and tools or financial means. Even though it is not part of the research question, it is worth mentioning that there are also certain risks involved within the various types of state-non-state actor relationships resulting from the principle-agent problem [54], [127]. As an example, a non-state actor may not be satisfied with its compensation and starts to perform other attacks to earn additional money. By doing so the actor draws attention to its operations which may give investigators enough information to create a profile for this actor and attribute other attacks to it. As a result, previous state sponsored attacks could be exposed and attributed to this actor, against the interested of the state who coordinated those attacks. In summary, the interests/operations of ransomware groups and states overlap on different levels and there is evidence that shows cooperation between them. However, more research is required into such relationships, in terms of the level of relationship and to widen the scope to include more countries. Moreover, there are a few questions that came up during the research which still remain unanswered. The following paragraph will present these open questions.

5.1.1 Open Questions

The thesis mentioned reports of threat actors conducting destructive attacks by masquerading wiper malware as ransomware. But why are they not using normal ransomware and just do not hand over the decryption key? The data would be lost as well, but it would be more difficult to prove that the attack was indented to destroy data and could be the result of an inexperienced ransomware operator accidentally losing the key. Or if there was no intention to hide the motivation behind the attack, why would they even masquerade the wiper malware? And why are the wipers masqueraded so that can be easily identified as masquerade? Is there a particular reason for that or is it a sign of a lack of skill or carelessness? Another open question is regarding the use of exfiltrated data as part of a ransomware attack. To what extent is exfiltrated data given or sold to a third party such as a state? It would be interesting to know whether ransomware groups give exfiltrated data to foreign intelligence agencies and whether some ransomware attacks are only serving that purpose.

5.2 Limitations

The limitations of this study can be summarised into

1. *Availability of data.* The data available for this study was limited, which restricted the investigations.
2. *Results of investigations.* The analysis is based on the results of the forensic investigations. This means that some aspects of the attack might have been unnoticed by the experts at Northwave.
3. *Motive coverage.* The analysis covers three motives and evaluates which motive the attacks fit best by looking at the characteristics of the attacks. The assumption is that a ransomware attack is by default financially motivated, and if the characteristics do fit a different motive, then there is a chance that some other malicious activities were carried out during the intrusions. This, however, does not cover all the possible scenarios. It is theoretically possible that a threat actor conducts a purely financially motivated and typical ransomware attack with double extortion (exfiltration of data). However, the threat actor additionally sells this data to a third party also purely financially motivated. In the end, the attack would have been a financially motivated ransomware and espionage attack, without being able to detect it with the approach used in this study.
4. *Scope of the investigation.* The results are based on a limited number of cases (six). An investigation into more cases could result in more insights.
5. *Uncertainty - Interpretation.* The study tried to be as objective as possible and tried to prevent bias when interpreting the result. The assumptions and interpretations that were made in this study could turn out to be wrong or stated differently by other researchers.
6. *Mitre ATT&CK mapping.* The mapping of threat actor actions to Mitre ATT&CK and their comparison is an important part of the threat profiles. Such a mapping is done by hand and even though the individual techniques are well described in the ATT&CK framework, the final mapping varies from person to person. The differences are influenced by, the interpretations of what the best ATT&CK technique is for an observed action by the threat actor, how precisely to map, and what data is

available on the actions of the attacker. The incidents of Northwave were mapped by the same person and by uncertainties checked by other experts at Northwave, which resulted in a precise and consistent mapping. For the Version data, it is not known how the mapping was done and which considerations influenced it. In addition, the mapping from the VERIS framework to Mitre ATT&CK takes away some precision. An action in the VERIS framework can map to several techniques in the Mitre ATT&CK framework and in the end, it is not clear which of the techniques were actually used by the threat actor. Despite possible inconsistencies and different levels of precision, comparing the data from Northwave and Verizon still results in a satisfying outcome as seen in the Section 4.1. Since the goal is to compare the occurrence of every mapped technique and not the total number of techniques it is not problematic if one set is less precise and contains more techniques.

7. *External resources.* The data used in this study that provides insight in, amongst others, the number of ransomware attacks or the average ransom payments is taken from private security companies. These numbers cannot be verified independently and it is not perfectly clear how they have been determined. As a result, numbers and graphs presented in this study only represent what private companies see and publish which might not be representative regarding the actual events and actions.

The discussion of the conducted research highlighted the challenges entailed within the research question. Investigations into the activities of threat actors without having or finding definitive proof leaves room for uncertainties and conflicting interpretations. However, the methodology used throughout this study made it possible to get a better understanding of the intrusions and motives behind them. Even though, the result still carries some uncertainty, it was possible to find a well-founded answer to the initial suspicions and the posed research questions. A final conclusion to this thesis is drawn in the upcoming chapter combined with suggestions for future work.

6 Conclusion

This thesis investigated to what extent ransomware is used as a cover for other malicious activities. It started with giving background information on ransomware showing that it is an ongoing and severe threat to companies. The related works section covered other contributions to the topics partly covered in this research. The subsequent section introduced the research approach, including the threat profiles, data, and tools for conducting this study. In the following, the results were presented, showing that the investigated cases did not show evident signs that ransomware was used to cover up other malicious activities even though they seemed suspicious. The result section was followed by a discussion and mentioning of the limitations of this research.

This research showed that even though no evidence of a cover-up was found in the cases of Northwave, ransomware is used to cover up activities such as espionage and destructive attacks. In addition, it highlights that states and non-state actors are working together and that ransomware might pose as a good cover for foreign intelligence. These results contribute to a better understanding and overview of smoke-screen and cover-up attacks. In addition, the chosen methodology might help other researchers to develop a better approach to studying such scenarios. The insights could encourage security engineers to take a closer look at ransomware attacks when there are indications that fit the introduced threat profiles. The possibility of ransomware being used as cover could also mean for law enforcement to observe such attacks in more detail as an additional attack vector of

nation-states. Already or in the future exfiltrated data could be used to make money or just as information to please the government of a state. Only looking for APTs and nation-states when it comes to espionage might be dangerous since ransomware actors also exfiltrate data and work together and might be used as proxies for espionage purposes. A focus on this issue could help to create better policies for companies and may even help to encourage better political actions and laws.

In the future, it would be beneficial to widen the scope and look at more cases with the focus on assessing whether ransomware might have been used as a cover-up. For example, intrusions of the RaaS provider Conti could be interesting to investigate, due to indications that they work with or for the FSB and therefore their ransomware attacks could pursue multiple goals. The methodology of this thesis could also be improved and research conducted into the use of frameworks and tools such as Mitre ATT&CK and MISP to better understand motivations behind attacks, even when there is data missing on all actions performed by the threat actor. Additionally, it would help to talk to attackers to understand their motivations better behind such attacks, especially in the attacks where wipers were 'poorly' masqueraded as ransomware, even though it might be difficult to reach them. Another focus in future work could be to work together on this with different security companies as well as international law enforcement to get a better overview and to assess the threat level to companies and society.

References

[1] A. Singh, A. R. Ikuesan, and H. S. Venter, "Digital forensic readiness framework for ransomware investigation," in *International conference on digital forensics and cyber crime*, Springer, pp. 91–105.

[2] Verizon, "2022 data breach investigations report," Report. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/.

[3] Microsoft, "Digital defense report," Microsoft, Report, 2021. [Online]. Available: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi.

[4] Sophos, "Interrelated threats target an interdependent world," Sophos, Report, 2021-11. [Online]. Available: https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2022-threat-report.pdf.

[5] W. Craven. "A Nightmare on Elm Street." (1985-08), [Online]. Available: https://www.imdb.com/title/tt0087800/.

[6] "The Weirdo on Maple Street." (), [Online]. Available: https://strangerthings.fandom.com/wiki/The_Weirdo_on_Maple_Street (visited on 07/27/2022).

[7] P. Leth and A. Vesterby, "Homicidal hanging masquerading as suicide," *Forensic Science International*, vol. 85, no. 1, pp. 68–70, 1997, ISSN: 0379-0738. DOI: https://doi.org/10.1016/S0379-0738(96)02082-8. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0379073896020828.

[8] I. Cobain, "Boris Berezovsky inquest returns open verdict on death," en-GB, *The Guardian*, 2014-03, ISSN: 0261-3077. [Online]. Available: https://www.theguardian.com/world/2014/mar/27/boris-berezovsky-inquest-open-verdict-death (visited on 07/15/2022).

[9] J. Fruhlinger. "Petya ransomware and notpetya malware: What you need to know now." (2017-10-17), [Online]. Available: https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html (visited on 03/09/2022).

[10] J. Slowik, "Spyware stealer locker wiper: Lockergoga revisited," Dragos, Report, 2020-03. [Online]. Available: https://www.dragos.com/resource/spyware-stealer-locker-wiper-lockergoga-revisited/.

[11] L. Y. Connolly and D. S. Wall, "The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures," *Computers & Security*, vol. 87, p. 101 568, 2019, ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2019.101568. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404819301336.

[12] Enisa, "Enisa threat landscape 2021," European Union Agency for Cybersecurity, Report, 2021-10. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

[13] SonicWall, "2022 sonicwall cyber threat report," 2022. [Online]. Available: https://www.sonicwall.com/2022-cyber-threat-report/.

[14] Sophos, "The state of ransomware 2022," Report, 2022-04. [Online]. Available: https://www.sophos.com/en-us/whitepaper/state-of-ransomware.

[15] Lifars, "Apt41 the spy who encrypted me," Lifars, Report, 2020. [Online]. Available: https://lifars.com/wp-content/uploads/2020/04/APT41-the-spy-who-encrypted-me-case-study.pdf.

[16] R. Future, "Dark covenant: Connections between the russian state and criminal actors," Recorded Future, Report, 2021. [Online]. Available: https://go.recordedfuture.com/hubfs/reports/cta-2021-0909.pdf.

[17] Sophos. "Sophos 2022 threat report: Gravitational force of ransomware black hole pulls in other cyberthreats to create one massive, interconnected ransomware delivery system." (2021-11-09), [Online]. Available: https://www.sophos.com/en-us/press-office/press-releases/2021/11/sophos-2022-threat-report.aspx (visited on 11/25/2021).

[18] A. H. Amanda Tanner and D. Santos. "Threat assessment: Blackcat ransomware." (2022-01-27), [Online]. Available: https://unit42.paloaltonetworks.com/blackcat-ransomware/ (visited on 07/15/2022).

[19] C. Nocturnus. "Strifewater rat: Iranian apt moses staff adds new trojan to ransomware operations." (2022-02-01), [Online]. Available: https://www.cybereason.com/blog/research/strifewater-rat-iranian-apt-moses-staff-adds-new-trojan-to-ransomware-operations (visited on 05/11/2022).

[20] CISA. "Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure | CISA." (2022-01-11), [Online]. Available: https://www.cisa.gov/uscert/ncas/alerts/aa22-011a (visited on 07/22/2022).

[21] CISA. "North korean state-sponsored cyber actors use maui ransomware to target the healthcare and public health sector." (2022-07-07), [Online]. Available: https://www.cisa.gov/uscert/ncas/alerts/aa22-187a (visited on 07/15/2022).

[22] Malpedia. "Axiom (actor)." (2022), [Online]. Available: https://malpedia.caad.fkie.fraunhofer.de/actor/axiom (visited on 03/22/2022).

[23] FireEye, "Double dragon: Apt41, a dual espionage and cyber crime operation," FireEye™, Report, 2019. [Online]. Available: https://content.fireeye.com/apt-41/rpt-apt41.

[24] N. Rostovtsev. "APT41 World Tour 2021 on a tight schedule." (2022-08-18), [Online]. Available: https://blog.group-ib.com/apt41-world-tour-2021 (visited on 08/24/2022).

[25] R. Richardson and M. M. North, "Ransomware: Evolution, mitigation and prevention," *International Management Review*, vol. 13, no. 1, p. 10, 2017. [Online]. Available: https://digitalcommons.kennesaw.edu/facpubs/4276.

[26] CrowdStrike. "History of ransomware." (2021-06-21), [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/ (visited on 10/12/2021).

[27] K. Mehrotra and W. Turton. "Cna financial paid $40 million in ransom after march cyberattack." (2021-05-20), [Online]. Available: https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack (visited on 02/21/2022).

[28] "Cybercrime To Cost The World $10.5 Trillion Annually By 2025." (2020-11-13), [Online]. Available: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (visited on 08/02/2022).

[29] CrowdStrike, "2020 global threat report," CrowdStrike, Report, 2020. [Online]. Available: https://www.crowdstrike.com/resources/reports/2020-crowdstrike-global-threat-report/.

[30] Corvus, "Corvus cyber risk insights index," Corvus, Report, 2021. [Online]. Available: https://info.corvusinsurance.com/2021-corvus-risk-insights-index.

[31] Coveware. "Ransomware threat actors pivot from big game to big shame hunting." (2022-05-03), [Online]. Available: https://www.coveware.com/blog/2022/5/3/ransomware-threat-actors-pivot-from-big-game-to-big-shame-hunting (visited on 05/17/2022).

[32] J. L. Hardcastle. "Ransomware gangs move into pure extortion without encryption." en. (2022-05-25), [Online]. Available: https://www.theregister.com/2022/06/25/ransomware_gangs_extortion_feature/ (visited on 07/21/2022).

[33] M. J. Schwartz. "Conti ransomware group explores post-encryption future." (2022-06-16), [Online]. Available: https://www.databreachtoday.com/conti-ransomware-group-explores-post-encryption-future-a-19359 (visited on 07/21/2022).

[34] Coveware. "Coveware's 2018 q4 ransomware marketplace report." (2019-01-22), [Online]. Available: https://www.coveware.com/blog/2019/1/21/covewares-2018-q4-ransomware-marketplace-report (visited on 04/04/2022).

[35] SonicWall, "2017 annual threat report," Report, 2017. [Online]. Available: https://bluekarmasecurity.net/wp-content/uploads/2017/06/SonicWall-2017-Annual-Threat-Report.pdf.

[36] Coveware. "Ransomware Payments Up 33% in Q1 2020." (2020-04-29), [Online]. Available: https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report (visited on 04/05/2022).

[37] J. Joseph. "Annual number of ransomware attacks worldwide from 2016 to 2020." (2021-07-22), [Online]. Available: https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/ (visited on 10/27/2021).

[38] Coveware. "Law enforcement pressure forces ransomware groups to refine tactics in q4 2021." (2022-02-03), [Online]. Available: https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021 (visited on 03/24/2022).

[39] S. Ranger. "Ransomware is now a giant black hole that is sucking in all other forms of cybercrime." (2021-11-19), [Online]. Available: https://www.zdnet.com/article/ransomware-is-now-a-giant-black-hole-that-is-sucking-in-all-other-forms-of-cybercrime/ (visited on 11/22/2021).

[40] Trend Micro. "Lockbit, conti, and blackcat lead pack amid rise in active raas and extortion groups." (2022-05-23), [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-conti-and-blackcat-lead-pack-amid-rise-in-active-raas-and-extortion-groups-ransomware-in-q1-2022 (visited on 10/28/2022).

[41] Intel471. "Ransomware-as-a-service: The pandemic within a pandemic." (2020-11-16), [Online]. Available: https://intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer (visited on 11/30/2021).

[42] J. T. John Fokker. "Conti leaks: Examining the panama papers of ransomware | trellix." (2022-03-31), [Online]. Available: https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/conti-leaks-examining-the-panama-papers-of-ransomware.html (visited on 04/05/2022).

[43] N. Keijzer. "Inside the world of ransomware part 2/3: Different roles within a ransomware attack." (2022-03-01), [Online]. Available: https://northwave-security.com/inside-the-world-of-ransomware-part-2-3-different-roles-within-a-ransomware-attack/ (visited on 03/21/2022).

[44] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues in Information Warfare & Security Research*, vol. 1, no. 1, p. 80, 2011.

[45] N. Keijzer, *Inside the world of ransomware, Part 1/3: Dissecting the attack*, en-US, 2021-11-02. [Online]. Available: https://northwave-security.com/en/inside-the-world-of-ransomware-dissecting-the-attack/ (visited on 01/03/2022).

[46] T. Balmforth and M. Tsvetkova. "Russia takes down revil hacking group at u.s. request - fsb." (2022-01-14), [Online]. Available: https://www.reuters.com/technology/russia-arrests-dismantles-revil-hacking-group-us-request-report-2022-01-14/ (visited on 03/29/2022).

[47] J. Tidy. "Evil corp: 'my hunt for the world's most wanted hackers'." (2021-11-17), [Online]. Available: https://www.bbc.com/news/technology-59297187 (visited on 11/30/2021).

[48] J. C. Demers. "Assistant attorney general john c. demers remarks for press conference on united states v li, et al. (edwa)." (2020-07-21), [Online]. Available: https://www.justice.gov/opa/speech/assistant-attorney-general-john-c-demers-remarks-press-conference-united-states-v-li-et (visited on 12/03/2021).

[49] J. Walter. "LockBit 3.0 Update | Unpicking the Ransomware's Latest Anti-Analysis and Evasion Techniques." (2022-07-21), [Online]. Available: https://www.sentinelone.com/labs/lockbit-3-0-update-unpicking-the-ransomwares-latest-anti-analysis-and-evasion-techniques/ (visited on 08/24/2022).

[50] S. Chng, H. Y. Lu, A. Kumar, and D. Yau, "Hacker types, motivations and strategies: A comprehensive framework," *Computers in Human Behavior Reports*, vol. 5, p. 100 167, 2022, ISSN: 24519588. DOI: 10.1016/j.chbr.2022.100167. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S245195882200001X.

[51] T. Maurer, *Cyber mercenaries : the state, hackers, and power*. Cambridge, United Kingdom; Cambridge University Press, 2018, ISBN: 978-1-107-12760-9. DOI: 10.1017/9781316422724. [Online]. Available: https://doi.org/10.1017/9781316422724.

[52] T. Steffens, *Attribution of advanced persistent threats*. Berlin, Germany: Springer Vieweg Berlin, Heidelberg, 2020, ISBN: 978-3-662-61313-9. DOI: 10.1007/978-3-662-61313-9. [Online]. Available: http://link.springer.com/10.1007/978-3-662-61313-9, ebook.

[53] W. G. o. t. u. o. mercenaries, "Use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination," Report, 2021-07. [Online]. Available: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/192/08/PDF/N2119208.pdf?OpenElement.

[54] T. Maurer, "Cyber proxies and their implications for liberal democracies," *The Washington Quarterly*, vol. 41, no. 2, pp. 171–188, 2018, ISSN: 0163-660X, 1530-9177. DOI: 10.1080/0163660X.2018.1485332. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/0163660X.2018.1485332.

[55] Office of Cybersecurity, Energy Security, and Emergency Response. "Colonial pipeline cyber incident." (), [Online]. Available: https://www.energy.gov/ceser/colonial-pipeline-cyber-incident (visited on 11/25/2021).

[56] A. Lawrence. "Jbs paid $11 million to revil ransomware, $22.5m first demanded." (2021-06-10), [Online]. Available: https://www.bleepingcomputer.com/news/security/jbs-paid-11-million-to-revil-ransomware-225m-first-demanded/ (visited on 11/25/2021).

[57] R. J. Harknett and M. Smeets, "Cyber campaigns and strategic outcomes," *Journal of Strategic Studies*, vol. 45, no. 4, pp. 534–567, 2022. DOI: 10.1080/01402390.2020.1732354. eprint: https://doi.org/10.1080/01402390.2020.1732354. [Online]. Available: https://doi.org/10.1080/01402390.2020.1732354.

[58] J. DiMaggio, "Nation state ransomware," Report, 2021-08. [Online]. Available: https://analyst1.com/file-assets/Nationstate_ransomware_with_consecutive_endnotes.pdf.

[59] Legal Rule or Regulation, 2020. [Online]. Available: https://cis-legislation.com/document.fwx?rgn=1537.

[60] I. Truth. "Apt41: A case sudy." (2022-07-20), [Online]. Available: https://intrusiontruth.wordpress.com/2022/07/20/apt41/ (visited on 07/21/2022).

[61] E. Olcott and H. Warrell. "China lured graduate jobseekers into digital espionage." (2022-06-30), [Online]. Available: https://www.ft.com/content/2e4359e4-c0ca-4428-bc7e-456bf3060f45 (visited on 07/01/2022).

[62] "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace." en. (2020-10), [Online]. Available: https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and (visited on 06/20/2022).

[63] A. Greenberg. "The untold story of notpetya, the most devastating cyberattack in history." (2018-08-22), [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (visited on 06/21/2022).

[64] C. Cimpanu. "Killdisk fake ransomware hits financial firms in latin america." (2018-01-16), [Online]. Available: https://www.bleepingcomputer.com/news/security/killdisk-fake-ransomware-hits-financial-firms-in-latin-america/ (visited on 03/09/2022).

[65] L. Abrams. "Microsoft: Fake ransomware targets ukraine in data-wiping attacks." (2022-01-16), [Online]. Available: https://www.bleepingcomputer.com/news/security/microsoft-fake-ransomware-targets-ukraine-in-data-wiping-attacks/ (visited on 03/09/2022).

[66] K. Zetter. "What we know and don't know about the cyberattacks against ukraine - (updated)." (2022-01-18), [Online]. Available: https://zetter.substack.com/p/what-we-know-and-dont-know-about.

[67] Microsoft. "Destructive malware targeting ukrainian organizations." (2022-01-16), [Online]. Available: https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/.

[68] T. H. Team. "Ukraine: Disk-wiping attacks precede russian invasion." (2022-02-25), [Online]. Available: http://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia (visited on 03/09/2022).

[69] G. Revay. "An overview of the increasing wiper malware threat | fortiguard labs." (2022-04-28), [Online]. Available: https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat (visited on 05/10/2022).

[70] "Timeline of Cyber Incidents Involving Financial Institutions." (), [Online]. Available: https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline#BancoDeChile2018 (visited on 06/20/2022).

[71] P. Technologies. "Positive technologies: Hackers using malware to cover their tracks, motives." (2018-02-12), [Online]. Available: https://www.ptsecurity.com/ww-en/about/news/hackers-using-malware-to-cover-their-tracks-motives/ (visited on 08/15/2022).

[72] M. D. T. I. Team. "Threat actor leverages coin miner techniques to stay under the radar – here's how to spot them." (2020-11-30), [Online]. Available: https://www.microsoft.com/security/blog/2020/11/30/threat-actor-leverages-coin-miner-techniques-to-stay-under-the-radar-heres-how-to-spot-them/ (visited on 08/15/2022).

[73] Neustar, "2014 ddos attacks and impact report," Report, 2014. [Online]. Available: https://web.archive.org/web/20141030203055/https://www.neustar.biz/resources/whitepapers/ddos-protection/2014-annual-ddos-attacks-and-impact-report.pdf.

[74] S. Soesanto, *Yesterday, the it army acknowleged for the first time that it used a ddos campaign to run cover for a data exfiltration op. target: Russia's e-procurement resource platform roseltorg.* 2022-07-01. [Online]. Available: https://twitter.com/iiyonite/status/1542771007529918471?cxt=HHwWjoC9mdaDg-kqAAAA (visited on 07/01/2022), https://twitter.com/iiyonite.

[75] Kaspersky. "Research reveals hacker tactics: Cybercriminals use ddos as smokescreen for other attacks on business." (2016-11-22), [Online]. Available: https://www.kaspersky.com/about/press-releases/2016_research-reveals-hacker-tactics-cybercriminals-use-ddos-as-smokescreen-for-other-attacks-on-business.

[76] L. Abrams. "New coronavirus ransomware acts as cover for kpot infostealer." (2020-03-12), [Online]. Available: https://www.bleepingcomputer.com/news/security/new-coronavirus-ransomware-acts-as-cover-for-kpot-infostealer/ (visited on 08/15/2022).

[77] C. T. U. R. Team. "Bronze starlight ransomware operations use hui loader." (2022-06-23), [Online]. Available: https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader (visited on 06/24/2022).

[78] M. Bada and J. R. C. Nurse, "Profiling the cybercriminal: A systematic review of research," in *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, pp. 1–8. DOI: 10.1109/CyberSA52016.2021.9478246.

[79] E. Doynikova and I. Kotenko, "Approach for determination of cyber-attack goals based on the ontology of security metrics," *IOP Conference Series: Materials Science and Engineering*, vol. 450, p. 052 006, 2018, ISSN: 1757-899X. DOI: 10.1088/1757-899X/450/5/052006. [Online]. Available: https://iopscience.iop.org/article/10.1088/1757-899X/450/5/052006.

[80] D. H. John and A. L. Thomas, "A common language for computer security incidents," Report SAND98-8667, 751004, 1998. DOI: 10.2172/751004. [Online]. Available: http://www.osti.gov/servlets/purl/751004-JhkwDA/webviewable/.

[81] S. Furnell, "The problem of categorising cybercrime and cybercriminals," in *2nd Australian information warfare and security conference*, M. Warren and J. Burn, Eds., Churchlands, Western Australia: School of Management Information Systems, Edith Cowan University. [Online]. Available: https://ro.ecu.edu.au/ecuworks/6758/.

[82] C. Meyers, S. Powers, and D. Faissol, "Taxonomies of cyber adversaries and attacks: A survey of incidents and approaches," Report LLNL-TR-419041, 967712, 2009-10. [Online]. Available: https://www.osti.gov/servlets/purl/967712/.

[83] S. Caltagirone, A. Pendergast, and C. Betz, "The diamond model of intrusion analysis," Center For Cyber Intelligence Analysis and Threat Research Hanover Md, Report, 2013.

[84] T. Rid and B. Buchanan, "Attributing cyber attacks," *Journal of Strategic Studies*, vol. 38, no. 1-2, pp. 4–37, 2015, ISSN: 0140-2390. DOI: 10.1080/01402390.2014.977382. [Online]. Available: https://doi.org/10.1080/01402390.2014.977382.

[85] A. Wolf. "The karakurt web: Threat intel and blockchain analysis reveals extension of conti business model." (2022-04-15), [Online]. Available: https://arcticwolf.com/resources/blog/karakurt-web (visited on 06/28/2022).

[86] F. Wosar, *There was an unconfirmed rumour that after we pwned blackmatter for 8 weeks [...]* 2022-07-03. [Online]. Available: https://twitter.com/fwosar/status/1543705282194411527?cxt=HHwWjsC88c7xq-wqAAAA (visited on 07/11/2022), https://twitter.com/fwosar.

[87] Intel471. "The blurry boundaries between nation-state actors and..." (2021-06-08), [Online]. Available: https://intel471.com/blog/the-blurry-boundaries-between-nation-state-actors-and-the-cybercrime-underground (visited on 05/05/2022).

[88] Jupyter. "Project jupyter." (2022), [Online]. Available: https://jupyter.org (visited on 06/24/2022).

[89] Further_eye. "合法件勒索工具，深信服edr提供防御方案." (2020-06-12), [Online]. Available: https://www.secpulse.com/archives/133410.html (visited on 05/17/2022).

[90] T. Seals. "Hades ransomware gang exhibits connections to hafnium." (2021-03-29), [Online]. Available: https://threatpost.com/hades-ransomware-connections-hafnium/165069/ (visited on 07/01/2022).

[91] J. White. "Analyzing attacks against microsoft exchange server with china chopper webshells." (2021-03-08), [Online]. Available: https://unit42.paloaltonetworks.com/china-chopper-webshell/ (visited on 07/05/2022).

[92] A. Palhière and R. Jullian. "Unransomware." (2022-01-31), [Online]. Available: https://www.synacktiv.com/en/publications/unransomware.html (visited on 05/17/2022).

[93] J. Hill. "Good for evil: Deepbluemagic ransomware group abuses legit encryption tools." (2021-10-19), [Online]. Available: https://www.varonis.com/blog/deepbluemagic-ransomware (visited on 05/17/2022).

[94] C. Glyer, D. Perez, S. Jones, and S. Miller. "This is not a test: Apt41 initiates global intrusion campaign using multiple exploits." (2020-03-25), [Online]. Available: https://www.mandiant.com/resources/apt41-initiates-global-intrusion-campaign-using-multiple-exploits (visited on 10/07/2021).

[95] Verizon, "2021 data breach investigations report," Report. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/.

[96] Verizon. "Interactive verizon data breach investigations report." (), [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/interactive/ (visited on 06/02/2022).

[97] Verizon. "Mitre att&ck mapping structured as graph edges." (), [Online]. Available: https://github.com/vz-risk/veris/blob/master/bin/vcaf-rev2020-v1_0_3.csv (visited on 06/02/2022).

[98] T. M. Corporation. (), [Online]. Available: https://attack.mitre.org/ (visited on 11/18/2021).

[99] Misp. "Misp open source threat intelligence platform." (), [Online]. Available: https://www.misp-project.org/ (visited on 02/21/2022).

[100] Misp. "Misp - threat intelligence sharing platform." (), [Online]. Available: https://github.com/MISP/MISP/tree/v2.4.126 (visited on 06/15/2022).

[101] National Coordinator for Security and Counterterrorism, "Cyber security assessment netherlands 2021," NCTV, Report, 2021. [Online]. Available: https://

english.nctv.nl/binaries/nctv-en/documenten/publications/2021/08/05/cyber-security-assessment-netherlands-2021/CSBN2021_EN_02.pdf.

[102] S. Gatlan. "Hackers used billing software zero-day to deploy ransomware." (2021-10-25), [Online]. Available: https://www.bleepingcomputer.com/news/security/hackers-used-billing-software-zero-day-to-deploy-ransomware/ (visited on 11/30/2021).

[103] C. Cimpanu. "New moses staff group targets israeli organizations in destructive attacks." (2021-11-15), [Online]. Available: https://therecord.media/new-moses-staff-group-targets-israeli-organizations-in-destructive-attacks/ (visited on 05/13/2022).

[104] Coveware. "Ransomware attackers down shift to 'mid-game' hunting in q3." (2021-10-21), [Online]. Available: https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts (visited on 06/23/2022).

[105] Coveware. "Ransomware attack vectors shift as new software vulnerability exploits abound." (2021-04-26), [Online]. Available: https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound (visited on 06/23/2022).

[106] Coveware. "Ransomware payments fall as fewer companies pay data exfiltration extortion demands." (2021-02-01), [Online]. Available: https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020 (visited on 06/23/2022).

[107] Coveware. "Q3 ransomware demands rise: Maze sunsets & ryuk returns." (2020-11-04), [Online]. Available: https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report (visited on 06/23/2022).

[108] Coveware. "Ransomware attacks split between enterprise & raas." (2020-08-03), [Online]. Available: https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report (visited on 06/23/2022).

[109] I. Truth. "Chinese apts: Interlinked networks and side hustles." (2022-07-24), [Online]. Available: https://intrusiontruth.wordpress.com/2022/07/24/chinese-apts-interlinked-networks-and-side-hustles/ (visited on 07/25/2022).

[110] Microsoft. "Bitlocker - windows security." (2022-03-06), [Online]. Available: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview (visited on 06/23/2022).

[111] Jetico. "Data encryption | jetico." (), [Online]. Available: https://www.jetico.com/data-encryption (visited on 06/23/2022).

[112] CISA. "Publicly Available Tools Seen in Cyber Incidents Worldwide." (2018-10-11), [Online]. Available: https://www.cisa.gov/uscert/ncas/alerts/AA18- (visited on 07/01/2022).

[113] M. Labs. "Cobalt Strike, a penetration testing tool abused by criminals." (2021-06-01), [Online]. Available: https://blog.malwarebytes.com/researchers-corner/2021/06/cobalt-strike-a-penetration-testing-tool-popular-among-criminals/ (visited on 07/01/2022).

[114] S. Security Response. "Living off the Land: Attackers Leverage Legitimate Tools for Malicious Ends." en. (2019-12-24), [Online]. Available: http://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/living-land-legitimate-tools-malicious (visited on 07/01/2022).

[115] L. Abrams. "Qwerty Ransomware Utilizes GnuPG to Encrypt a Victims Files." (2018-03-09), [Online]. Available: https://www.bleepingcomputer.com/news/security/qwerty-ransomware-utilizes-gnupg-to-encrypt-a-victims-files/ (visited on 07/01/2022).

[116] C. Research, *Uncovering MosesStaff techniques: Ideology over Money*, Web Page, 2021-11-15. [Online]. Available: https://research.checkpoint.com/2021/mosesstaff-targeting-israeli-companies/ (visited on 07/01/2022).

[117] FBI. "Fbi flash: Mamba ransomware." (2021-03-23), [Online]. Available: https://www.cisa.gov/stopransomware/fbi-flash-mamba-ransomware.

[118] T. D. REPORT. "Exchange exploit leads to domain wide ransomware." (2021-11-15), [Online]. Available: https://thedfirreport.com/2021/11/15/exchange-exploit-leads-to-domain-wide-ransomware/ (visited on 05/13/2022).

[119] P. Oliveria. "Profiling DEV-0270: PHOSPHORUS' ransomware operations." (2022-09-07), [Online]. Available: https://www.microsoft.com/security/blog/2022/09/07/profiling-dev-0270-phosphorus-ransomware-operations/ (visited on 09/12/2022).

[120] k_hamza75. "Timisoarahackerteam (tht) ransomware support topic - ransomware help & tech support." (2020-04-14), [Online]. Available: https://www.bleepingcomputer.com/forums/t/714270/timisoarahackerteam-tht-ransomware-support-topic/.

[121] C. Nocturnus. "Powerless trojan: Iranian apt phosphorus adds new powershell backdoor for espionage." (2022-02-01), [Online]. Available: https://www.cybereason.com/blog/research/powerless-trojan-iranian-apt-phosphorus-adds-new-powershell-backdoor-for-espionage (visited on 06/29/2022).

[122] K. L. Global Research & Analysis Team. "New ransomware trends in 2022." (2022-05-11), [Online]. Available: https://securelist.com/new-ransomware-trends-in-2022/106457/ (visited on 05/13/2022).

[123] ANSSI, "Cyber threat overview 2021," Report, 2022-03. [Online]. Available: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2022-CTI-004.pdf.

[124] Enisa, "Enisa threat landscape 2020 - ransomware," Report, 2020-10. [Online]. Available: https://www.enisa.europa.eu/publications/ransomware/@@download/fullReport.

[125] M. Burgess. "Conti's attack against costa rica sparks a new ransomware era." (2022-06-12), [Online]. Available: https://www.wired.com/story/costa-rica-ransomware-conti/ (visited on 07/19/2022).

[126] M. T. Zahrani, "The coup that changed the middle east: Mossadeq v. the cia in retrospect," *World Policy Journal*, vol. 19, no. 2, pp. 93–99, 2002, ISSN: 07402775, 19360924. [Online]. Available: http://www.jstor.org/stable/40209809 (visited on 07/19/2022).

[127] S. A. Ross, "The economic theory of agency: The principal's problem," *The American Economic Review*, vol. 63, no. 2, pp. 134–139, 1973, ISSN: 00028282. [Online]. Available: http://www.jstor.org/stable/1817064 (visited on 07/25/2022).

[128] R. Lipovsky and P. Kálnai. "Killdisk now targeting linux: Demands $250k ransom, but can't decrypt." (2017-01-05), [Online]. Available: https://www.welivesecurity.com/2017/01/05/killdisk-now-targeting-linux-demands-250k-ransom-cant-decrypt/ (visited on 07/19/2022).

[129] A. Dahan. "Night of the devil: Ransomware or wiper? a look into targeted attacks in japan using mbr-oni." (2017-10-31), [Online]. Available: https://www.cybereason.com/blog/night-of-the-devil-ransomware-or-wiper-a-look-into-targeted-attacks-in-japan (visited on 03/09/2022).

[130] L. Abrams. "Oni ransomware used in month-long attacks against japanese companies." (2017-10-31), [Online]. Available: https://www.bleepingcomputer.com/

news/security/oni-ransomware-used-in-month-long-attacks-against-japanese-companies/ (visited on 03/09/2022).

[131] C. Beek. "Taiwan bank heist and the role of pseudo ransomware." (2017-10-12), [Online]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/taiwan-bank-heist-role-pseudo-ransomware/ (visited on 03/09/2022).

[132] Jareth. "Why are cybercriminals disguising wipers as ransomware?" (2019-09-26), [Online]. Available: https://blog.emsisoft.com/en/34134/why-are-cybercriminals-disguising-wipers-as-ransomware/ (visited on 03/09/2022).

[133] Malpedia. "Ordinypt(malware family)." (2019), [Online]. Available: https://malpedia.caad.fkie.fraunhofer.de/details/win.ordinypt (visited on 03/10/2022).

[134] I. Ilascu. "Germanwiper ransomware erases data, still asks for ransom." (2019-08-04), [Online]. Available: https://www.bleepingcomputer.com/news/security/germanwiper-ransomware-erases-data-still-asks-for-ransom/ (visited on 03/09/2022).

[135] ClearSky. "Operation quicksand." (2020-10-15), [Online]. Available: https://www.clearskysec.com/operation-quicksand/ (visited on 09/13/2022).

[136] M. d. Jesus and D. O. Ladores. "Chaos ransomware: A proof of concept with potentially dangerous applications." (2021-08-10), [Online]. Available: https://www.trendmicro.com/en_us/research/21/h/chaos-ransomware-a-dangerous-proof-of-concept.html (visited on 03/09/2022).

[137] A. B. S. Ehrlich. "From wiper to ransomware | the evolution of agrius - sentinellabs." (2021-05-25), [Online]. Available: https://www.sentinelone.com/labs/from-wiper-to-ransomware-the-evolution-of-agrius/.

[138] A. B. S. Ehrlich. "New version of apostle ransomware reemerges in targeted attack on higher education." (2021-09-30), [Online]. Available: https://www.sentinelone.com/labs/new-version-of-apostle-ransomware-reemerges-in-targeted-attack-on-higher-education/ (visited on 03/09/2022).

[139] eSentire. "Ransomware hackers attack a top safety testing org. using tactics and techniques borrowed from chinese espionage groups." (2021-09-21), [Online]. Available: https://www.esentire.com/security-advisories/ransomware-hackers-attack-a-top-safety-testing-org-using-tactics-and-techniques-borrowed-from-chinese-espionage-groups (visited on 03/09/2022).

[140] C. Cimpanu. "Microsoft warns of malware campaign spreading a rat masquerading as ransomware." (2021-05-20), [Online]. Available: https://therecord.media/microsoft-warns-of-malware-campaign-spreading-a-rat-masquerading-as-ransomware/.

[141] L. Abrams. "Beware: Onyx ransomware destroys files instead of encrypting them." (2022-04-27), [Online]. Available: https://www.bleepingcomputer.com/news/security/beware-onyx-ransomware-destroys-files-instead-of-encrypting-them/ (visited on 07/19/2022).

[142] B. Toulas. "Fake adult sites push data wipers disguised as ransomware." (2022-10-09), [Online]. Available: https://www.bleepingcomputer.com/news/security/fake-adult-sites-push-data-wipers-disguised-as-ransomware/ (visited on 10/11/2022).

A Reports on as Ransomware Masqueraded Malware

Masqueraded Malware	Malware Name/Description	Scheme	Date of reported activity	Source
Wiper	KillDisk	Wiper with ransomware capabilities Missing way for decryption.	2016	[128]
Wiper	KillDisk	Wipe files but leaves ransom note	2016-2018	[64]
Wiper	NotPetya (worm), related to Petya ransomware	Wiper with ransomware capabilities Missing way for decryption.	2016 - 2017	[9]
Wiper	ONI, other version is MBR-ONI which is based on DiskCryptor (legitimate tool also seen in Bad Rabbit ransomware)	Ransomware used as wiper Email used in ransom note: hyakunoonigayoru@yahoo[.]co.jp	2017	[129] [130]
Ransomware	Hermes ransomware	Ransomware deployed but no note or ransom demand. Cover up believed but not sure what (probably bank heist)	2017	[131]
Wiper	Strain from Ordinypt	Wiper masquerading as ransomware	2019	[132]
Wiper	GermanWiper (seems to be the same as Ordinypt, see [133]) Similarities with Sodinokibi ransomware campaign	Ransomware but overwrites with gibberish instead of encrypting	2019	[134] [133]
Ransomware	Destructive version of Thanos ransomware	Shows ransom note but overwrites Master Boot Record (MBR) making the system unusable	2020 (not seen in action)	[135]
Wiper	Named Chaos but related to Ryuk	Wiper looking like ransomware	Start development June 2021, last update August 2021	[136]
Wiper	Deadwood (aka Detbosit), and Apostle wiper which was turned into ransomware. Apostle allegedly written by same developer as IPsec Helper	Wiper masquerading as ransomware	Beginning 2020, still active late 2021	[137] [138]
Ransomware (Most likely)	TTP matches Hello ransomware campaigns. Modus operandi similarity to APT27	Attack stopped before ransomware was deployed. Indicators that ransomware was not primary goal	July 2021	[139]
RAT	STRRAT The resemblance to ransomware is that it appends .crimson to files, but the files are not encrypted	RAT masquerades as ransomware. Capable of stealing data. Gives full control of victim.	Spotted in June 2020 Newer version spread May 2021	[140]
Ransomware	Apparently borrows code from AutoIT-based ransomware families	Ransomware that uses an email address (pusheken91@bk[.]ru) as file ending for encrypted files. Does not drop ransom note.	May 2020	[102]
Wiper	MBRLocker plus data wiper	Malware leaving ransom note and address but no way to get decryption key, in combination with malware that overwrites data with fixed number of bytes	January 2022	[65] [66] [67]
Wiper	Trojan.Killdisk (HermeticWiper)	Wiper that leaves ransom note. Similarities to so-called 'WhisperGate' attack (see above)	February 2022	[68]
Ransomware	Onyx (Chaos variant, see above)	Ransomware that destroys data (even with leak page).	April 2022 (this version)	[141]
Wiper	Malware equipped to delete all system drives. (This functionality was not working properly in the investigated binary)	Malware renames all files, drops ransom note and deletes drives, but no way to recover files.	October 2022	[142]

Table 2: Overview of reports over malware masquerading as ransomware.