What To Do Against Ransomware? Evaluating Law Enforcement Interventions

Tom Meurs
IEBIS
University of Twente
Enschede, Netherlands
t.w.a.meurs@utwente.nl

Raphael Hoheisel
IEBIS
University of Twente
Enschede, Netherlands
r.hoheisel@utwente.nl

Marianne Junger
IEBIS
University of Twente
Enschede, Netherlands
m.junger@utwente.nl

Abhishta Abhishta
IEBIS
University of Twente
Enschede, Netherlands
s.abhishta@utwente.nl

Damon McCoy
Department of Computer Science
New York University
New York, USA
mccoy@nyu.edu

***Abstract*—Ransomware poses an increasing challenge to society, yet there is a notable gap in research on the effectiveness of law enforcement interventions. A key insight from our study is that the presence of victims' details on leak pages following double extortion ransomware attacks offers a unique opportunity to evaluate these interventions. Analyzing a dataset containing victims published by ransomware groups, we assess the impact of five specific types of interventions: arresting group members, taking down leak page server infrastructure, freezing crypto assets, releasing decryptors, and imposing sanctions.**

From a collected list of interventions, we categorize ransomware groups' responses into three actions: ceasing operations, continuing operations, or rebranding under a new name. Initial results show that nearly half of the interventions led to ransomware groups ceasing operations. Additionally, our findings suggest minimal crime displacement, with fewer victims attacked post-intervention if the groups continued their activities. Observed rebranding among these groups is also limited.

We discuss the implications and limitations of our research and conclude with two recommendations for law enforcement: prioritize frequent small interventions over a single large intervention and diversify the set of interventions to better counter the adaptive nature of ransomware groups.

***Index Terms*—Ransomware, Intervention, Sanctions, Takedown, Arrest, Crypto, Situational Crime Prevention**

I. Introduction

In recent years, ransomware has emerged as a significant societal concern [7], [35], [43], [44]. To our knowledge, systematic empirical research towards law enforcement interventions against ransomware are lacking [56]. We have identified a useful data source to evaluate the effectiveness of law enforcement (LE) interventions: victims published on leak pages during double extortion ransomware attacks. This approach helps bridge the gap in understanding how LE interventions can disrupt or deter ransomware attacks effectively.

We examine five distinct types of law enforcement interventions: the arrest of ransomware group members, the takedown of leak page server infrastructure, the freezing of crypto assets, the release of decryptors, and the imposition of sanctions on ransomware group members. While these interventions are commonly employed, their efficacy has not been systematically evaluated [56].

To address this gap, we create metrics and identify data sources that enable an evaluation of these interventions. We measure the efficacy of LE interventions by considering the response of ransomware groups: ceasing operations, continuing operations, or rebranding under a new name. Additionally, we assess the characteristics of victims targeted by groups facing interventions compared to those who do not, as well as the changes in ransomware operations pre- and post-intervention for groups that continue their activities. These measures allow us to study the effectiveness of LE interventions against ransomware groups.

We analyse three data sources: a dataset of 12,250 ransomware victims posted by 134 ransomware groups, including characteristics of those victims such as country, number of employees, and sector; a constructed list of law enforcement interventions; and a list of rebranding occurrences. The theoretical foundation for evaluating the effectiveness of LE interventions is Situational Crime Prevention (SCP), a criminological theory that states crime occurs through favorable opportunities [30], [48], [49]. Thus, effective interventions should alter the cost-benefit trade-off of these circumstances [37].

The primary goal of this study is to assess the impact of law enforcement interventions on the operations of ransomware groups. To address our goal, we explore three sub-questions:

RQ 1: Which ransomware groups face a law enforcement intervention?

RQ 2: How do ransomware groups respond to law enforcement interventions?

RQ 3: How do ransomware operations compare prior and post-intervention for ransomware groups who continue after an intervention?

To answer these research questions, we analyzed data from 20 February 2020 till 4 March 2024 from 12,250 ransomware

victims listed on leak pages by 134 ransomware groups, alongside 29 law enforcement interventions, and identified 19 groups that rebranded. We also conducted interviews with police officers, public prosecutors, and cyber security experts to validate our findings.

Our key contributions are:

1) Ransomware groups are more likely to face an intervention if they have a large number of victims, target many large companies, or maintain long uptime of their leak pages, indicating selective LE targeting.
2) Of the 17 groups with active leak pages during intervention, 8 ransomware groups continue with their operations, 7 cease operations and 2 rebrand after an intervention. Ceasing operations was most often associated with the takedown of a leak page server.
3) Crime displacement was limited. Rebranding occured only twice (N=17) post-intervention. Furthermore, groups continuing attacks after an intervention typically have less victims post-operation compared to prior.

The outline of this paper is as follows: In §II, we combine existing literature on SCP with a small pilot of interviews with law enforcement experts to state our propositions. Subsequently, in §III, we present our data and the methodology. Afterwards, §IV presents the results of the analysis of leak page data and law enforcement interventions. To conclude, we discuss our findings, limitations and outline implications for policy makers in §V, §VI and §VII, respectively.

II. Related Works and Propositions

This section begins with an examination of double-extortion ransomware and Situational Crime Prevention (SCP) theory, first introduced by [25]. This will be combined with the results of a small pilot study. In this pilot study, we interviewed 13 experts who work in the criminal justice system, among which police officers, public prosecutors and cyber security experts. We followed the interview methodology outlined by [70]. The goal was to explore the anticipated impact of law enforcement interventions of these experts and to validate intervention and rebranding lists used later in this study. For a full description of the pilot, please contact the lead author of the study.

The present study will not use hypothesis testing due to the limited number of interventions on which information is available. Instead, we will work with propositions and assess whether the empirical findings align with these propositions.

A. Situational Crime Prevention and LE Interventions

Ransomware is a type of malware that encrypts files and demands a ransom for access [75]. Double-extortion ransomware involves both data encryption and exfiltration [70], [71], [73]. Attackers threaten to publish exfiltrated data on their 'leak pages' if the ransom is not paid. Typically, if negotiations fail, the victim's name is listed on the leak page, followed by the publication of data after a delay. Stolen data may also be sold to other malicious actors, potentially for use in subsequent attacks [65], [74].

Meurs et al. [75] found that victims are willing to pay 5.5 times larger ransom amounts when data is exfiltrated, making double extortion more lucrative than traditional ransomware [21], [35], [75]. Malicious actors, therefore, target victims who highly value their data, increasing the attack's cost [22].

In response to the global ransomware crisis, law enforcement agencies conduct various interventions, such as taking offline servers hosting leak pages to prevent data leakage. These interventions face challenges due to the international nature of ransomware crimes, information asymmetries, conflicting jurisdictions, and limited enforcement capabilities [57], [66]. Information asymmetry refers to the inconsistent enforcement of legal mandates for victims to share information about ransomware attacks. Conflicting jurisdictions occur when attackers reside in countries unlikely to prosecute them, often those not party to the Budapest Convention, which provides a unified legal framework for prosecuting cybercrime [29]. Many law enforcement agencies also suffer from a lack of personnel and technical resources, making it difficult to combat ransomware effectively. Forensic and diplomatic complications, such as difficulty attributing attacks to specific individuals, further hinder interventions [66]. While ransomware attacks can scale up easily, enhancing law enforcement responses is considerably more challenging.

Evaluating the impact of police interventions is crucial for combating ransomware. One main goal of these interventions, besides arresting attackers, is preventing subsequent attacks. Situational Crime Prevention (SCP) is an approach aimed at understanding and addressing crime prevention [25], [56], [60]. SCP focuses on the idea that malicious actors make rational choices based on favorable opportunities [30], [37], [48], [49]. Because specific types of crime differ in their modus operandi, SCP is usually 'crime specific': measures that prevent one type of crime may not prevent another [26], [36], [56].

SCP is distinguished by its focus on five general strategies: Increase the Effort, Increase the Risks, Reduce the Rewards, Reduce Provocations, and Remove Excuses [25], [28], [56], [60]. These strategies aim to deter potential offenders by making crimes more difficult or less appealing. The effectiveness of SCP strategies in combating various crimes has been studied [19], [55], [56]. For extensive elaboration of these five principles, refer to [26], [27], [36], [56], [60].

Studies evaluating SCP measures against cybercrime are scarce [56]. A notable study includes Bada et al. [4], who evaluated SCP interventions like cease and desist letters, police visits, and workshops on cybercrime, finding a general decrease in self-reported offending. Another study conducted a meta-review of cybersecurity interventions, highlighting that implementation effectiveness drives intervention success more than the mere presence of controls [108].

Other studies mainly focused on SCP in their recommendations following a crime script analysis [31], [64], [70], [84]. A crime script describes all relevant aspects of a crime's modus operandi, from preparation to aftermath [17], [26], [36], [41], [61]. Because crimes differ in their modus operandi, SCP is

usually 'crime specific'. Therefore, evaluating an intervention strategy to combat ransomware requires understanding the specific ransomware crime script.

A detailed account of the ransomware crime script involves recognizing the attack's lifecycle: infrastructure and malware development, network access, encryption, extortion through data exfiltration, ransom negotiation, data leakage for non-complying victims, and money laundering by the attackers [70], [71].

For this study, we operationalize ransomware by identifying ransomware variants typically by their file extensions post-encryption. Although multiple attackers might use the same variant, the associated leak page server is usually specific to a single group. We focus on leak pages, using 'ransomware group' to denote the group behind a leak page server of a specific ransomware strain, variant, or family.

We analyze five specific interventions targeting ransomware groups, within the control of law enforcement or other government-related agencies. For brevity, we define interventions by either law enforcement, government entities, or cybersecurity companies as law enforcement interventions. Each intervention is discussed, highlighting its importance and alignment with SCP strategies.

The five interventions used by law enforcement in this study include two that mainly increase the risks to attackers, two that decrease attackers' rewards, and one that increases the necessary effort.

The following interventions **increase the risks**:

Intervention 1: Arrests. Arrests is defined here as arrests of malicious actors associated with a specific ransomware group. This might be a 'low-level' malicious actor, like a money mule, but also a 'key player'. Obviously, when some of the attackers have been arrested, the perception of the risk of getting caught might increase for the other attackers in a ransomware group. An important point is that it is unknown for those persons how much law enforcement knows.

Intervention 2: Sanctions. Another intervention consist of asset freeze or travel restrictions to a specific individual linked to ransomware [42]. Not only does this restrict the movement of the malicious actor, but also there is a name & shame element: the name of the malicious actor becomes known in public. This might increase the perceived risk for the malicious actor to continue his/her operations, and/or other malicious actors might be hesitant to work together with that person [42]. This clearly increases the risk for an attacker, since law enforcement knows who they are.

The following interventions **decrease the rewards**:

Intervention 3: Crypto-asset freezing. Crypto-asset freezing is the blocking of transactions of crypto-assets related to victims of a certain ransomware group. A crypto-exchange might block any transactions from a wallet, upon request from law enforcement. This means that an attacker cannot access his cryptocurrencies, thereby reduce the rewards of his malicious actor activities'.

Intervention 4: Decryptor release. Decryptor release is the release of a decryptor to victims by law enforcement. With the decryptor, the victim can regain access to files without paying the ransom. Often this is done through NoMoreRansom, an initiative to release decryptor keys safely to ransomware victims. The effect is that ransomware victims will not pay a ransom if a free decryptor is available. Subsequently, if they want to continue the attacks, ransomware groups would need to change their ransomware to make sure the victims could not recover without buying the decryption key.

The following intervention **increases the effort**:

Intervention 5: Takedown leak page server. Server takedowns relate to takedowns of leak page servers. Takedowns of other infrastructure of the malicious actors are outside the scope of this paper, since these are often not made public. While this would imply that attackers need to rebuild their infrastructure, this can also lead to an increased perceived risk. After a takedown, the group has to, which increases the effort. Furthermore, the ransomware group learns law enforcement has them in their crosshairs, increasing the perceived risks.

By comparing the interventions with the crime script, we observe that arrests and sanctions directly confront the attackers. Freezing crypto-assets disrupts the attack's monetization phase, while the release of decryptors intervenes in the file encryption process. Leak page server takedowns address the step where victims' data is exposed on leak pages. Law enforcement strategies targeting other steps of the crime script, like preventing malicious actors from gaining access to a victim's system, are outside the scope of the present study.

In addition to exploring the interventions and their effectiveness according to SCP, it is essential to determine which groups are targeted by these law enforcement interventions. This topic will be addressed in the following subsection.

B. Ransomware Groups Facing LE Interventions

Law enforcement agencies generally operate with limited resources [92] and face the challenge of more malicious actors than they can feasibly pursue. As a result, prioritization is essential in deciding which malicious actors to target [54], [92]. It seems reasonable that they will target malicious actors, according to certain selection criteria. For example, they will prioritize malicious actors who have many victims or high-value victims. As one police officer in the pilot mentioned:

> Police Officer 3: *"I think it might be smart in your study to only focus on the ransomware groups with more than, let's say, 20 victims. The smaller groups are not that interesting."*

This leads to the following proposition:

Proposition 1: *Ransomware groups targeting a greater number and more significant victims are more likely to face law enforcement interventions.*

Likewise, the same reasoning would imply that countries experiencing a high number of victims may also be more

frequently involved in interventions. Legal frameworks in most countries are built on the principles of subsidiarity and proportionality, which suggest that more aggressive interventions may be justified when the impact of ransomware crimes is relatively more significant. As one public prosecutor explains:

> Public Prosecutor: *"A takedown is not explicitly described in our legal code, so we must carefully examine the nature of the website/server, its location, and its technical aspects. Is one server sufficient, or is it a network of servers that needs to be addressed? This is then assessed within the legal framework, considering principles of proportionality and subsidiarity."*

From this, we can infer that the extent of law enforcement interventions in a country may correlate with the number of ransomware victims it has encountered.

Proposition 2: *Countries with a higher incidence of ransomware victims are more likely to undertake law enforcement interventions than those with fewer victims.*

Having examined why certain ransomware groups might face an intervention, it is now important to explore how these groups respond to such actions.

C. Ransomware Groups Responding to LE Interventions

Interestingly, participants from our pilot study were less optimistic about the impact of interventions compared to empirical evidence from studies supporting the SCP principles [25], [28], [56], [60]. Participants expressed varying opinions about the effectiveness of arresting ransomware actors. Six participants believed arrests have a significant impact, four noted the impact depends on the malicious actor's role within the organization, and three felt arrests have no effect on ransomware activities or the effect is unknown.

> Cybersecurity Expert 5: *"The position of the individual is crucial during an arrest. Otherwise, it doesn't make much sense. You really need to apprehend the key figures. If you only go after small individuals, the big ones will just keep going."*

With respect to 'increase the effort', 9 out of 13 participants believed that taking down leak page server would only have a symbolic impact.

> Police Officer 2: *"The effects of taking down leak page servers on ransomware attacks are mainly symbolic. It sparks a lot of discussion on online platforms and is considered extremely annoying for Ransomware-as-a-Service (RaaS) actors. It simply damages their reputation when their leak page is taken down."*

Only four participants were confident that a combination of LE interventions involving both arrests and takedown of leak page servers was more effective than either intervention alone.

> Police Officer 6: *"A combined approach works better because taking down a website is less complex and therefore less impactful than actually apprehending someone. This also has a greater deterrent effect. The uncertainty of what law enforcement knows will have a deterrent effect on malicious actors."*

Most participants (n=6) believed the effectiveness of an intervention depends on the role of the arrested malicious actor and whether the malicious actors have backups of the leak page server.

> SOC analyst: *"I don't expect that a combination of arrest and takedown will be significantly more effective in reducing the activity of leak page servers than just an arrest or takedown alone. People may have more difficulty regrouping and calming down after an arrest than after a takedown or a combination of both. This may lead to a temporary decrease in activity, but they often return, usually after a few months."*

Previous research similarly suggests that police officers, with respect to offline crime, generally hold more negative views about the effectiveness of police interventions [53], which is not justified considering the evidence. Based on these insights, we propose the following:

Proposition 3: *After a law enforcement intervention, a significant amount of the ransomware groups cease ransomware operations.*

An important criticism of interventions based on SCP is that they may not stop crime but merely displace it. This issue will be the focus of the following section.

D. Crime Displacement

One important consideration of crime prevention techniques is that, first, it is necessary to show, possibly in experimental research, that there is a real crime reduction and, second, there should be no crime displacement. [101] considered the effect of the takedown of a darknet forum. To assess the effects of a darknet market takedown of 220 vendors migrating to a new darknet forum. They found that although some vendors reused their PGP-key, most malicious actors started with a clean slate, which meant that they were erasing their past reputation completely. This meant they had to rebuilt their reputation of being 'a reliable' drug seller afresh. The authors concluded that a takedown is costly for malicious actors, even if there is some crime displacement [101].

Proposition 4: *Ransomware groups that continue after an intervention will target fewer and less significant victims than before the intervention.*

Rebranding is an important phenomenon in the ransomware ecosystem, where one strain disappears and another emerges, typically using the same infrastructure, part of the malware code, and operated by the same actors [24], [105]. It is believed that rebranding occurs for two main reasons: to obscure activities from law enforcement and/or to establish a new, more intimidating reputation [105]. According to [24], in 2022, the average lifespan of a ransomware strain was only 70 days, a significant decrease from 153 days in 2021 and 265 days in 2020. It could be argued that not all rebranding efforts

are publicly acknowledged. However, there is an incentive for malicious actors to make their rebranding known publicly to avoid having to rebuild their reputation from scratch, which could lead to lower ransoms from victims who are unsure if the group will return the decryption key after payment or might demand additional payments [20].

LE experts interviewed in our pilot study believe that there is a lot of rebranding.

> Cyber security expert 1: *"Yes, there is often a connection between takedowns and the rebranding of ransomware groups. This can happen depending on the circumstances and the motives of the group. A takedown operation can prompt a group to rebrand, especially if sanctions have been imposed on the group due to alleged ties with a certain entity. "*

Consequently, it is assumed that following a law enforcement intervention, malicious actors are more likely to publicly disclose their rebranding efforts. This publicly disclosed rebranding is done to maintain their reputation as a 'reliable' ransomware group, one that returns the decryption key after receiving payment.

Proposition 5: *Following a law enforcement intervention, ransomware groups are more likely to rebrand compared to continuing or ceasing operations.*

Our dataset could reveal different forms of rebranding among ransomware groups. For example, groups aiming to build a more fierce reputation might maintain their old brand for a period to smoothly transition infrastructure and affiliates to the new group. This mitigation could result in overlapping active periods for both the old and new leak pages. Conversely, rebranding following law enforcement intervention might be more abrupt, potentially leading to no overlap in the uptime of leak page servers. Such interventions could also provoke internal disputes or paranoia within the group. This could result in a groups splitting up is two or more different ransomware groups. These observations suggest a distinction between normal rebranding processes and those triggered by law enforcement actions. Therefore, we propose the following:

Proposition 6: *Rebranding following an intervention is more likely to be combined with a split-up and no overlapping time periods of leak pages, compared to rebranding without intervention.*

The next section will outline the data, operationalization of variables, and methods utilized in this study.

III. Data and Methodology

Three datasets form the basis of our analysis:

- **Dataset 1: Leak page data.** The main dataset is a nested dataset in which 134 ransomware groups, publish the names of the organisations that were a victim of ransomware: the victim's information is nested within the ransomware group. Besides the names of the victims, groups publish smaller or larger parts of the data if they managed to exfiltrated those from the victim's system. If parts of the data are published on the leak page, we assume that that specific victim did not pay. Additional information on the organizations were manually added by ecrime.ch and provided to the researchers [38]. The dataset also indicates victim's first and last seen dates, with the initial 21 observations considered outliers until bulk observations started on December 4, 2020. The dataset spanned from December 20, 2019, to March 4, 2024. It includes ransomware group names (categorical), country of victim (categorical), sector of victim (categorical), data leakage status (binary), and employee count of victim (categorical). The dataset contained 12,250 unique victims.
- **Dataset 2: Intervention list.** The second dataset comprises 36 LE interventions, with some combined into single events, resulting in 29 unique interventions. After excluding groups that stopped or rebranded before the intervention, we identified 17 unique interventions. The complete list is provided in Appendix A (Table V). To systematically explore the impact of interventions on ransomware groups' operations, we focused on groups that maintained leak pages from December 20, 2019, to March 4, 2024. Initially, we searched for relevant scientific articles using academic databases like Scopus and Web-of-Science, but this yielded no results. Consequently, we shifted our focus to cybersecurity company blogs. Using Google, we performed targeted searches with queries combining 'intervention type' and 'ransomware group name' for each intervention type and group, resulting in 670 queries (5 interventions x 134 groups). We restricted our search to the first three pages of Google results, assuming high-quality information is ranked highest. Each search result was reviewed for articles, reports, and mentions discussing the impact of interventions on ransomware groups or potential rebranding. Acknowledging potential limitations associated with using the Google Search Engine [58], we adopted four measures to mitigate the possibility of having missed interventions.
  1) Cross-referencing our interventions with the ransomware cartography developed by CERT Orange Cyberdefense [85].
  2) Conducting pilot study interviews, which identified two missing arrests.
  3) Querying the Wayback Machine of NoMoreRansom to find decryptors and their availability dates [80], which did not yield additional decryptors.
  4) Checking EU and USA sanctions websites for additional sanctions, with no new sanctions found [42], [100].

  Consequently, we believe we have a reasonably complete overview of LE interventions against the ransomware groups included in our study.
- **Dataset 3: Rebranding list.** The third dataset consists of a list of ransomware group rebrandings, which we compiled using the same search strategy as for identifying interventions. This resulted in 19 instances of

TABLE I
VARIABLES IN THE LEAK PAGE DATASET AND MISSING VALUES

Variables	Unit / Categories	Missing Values	%
Ransomware Group	Categorical (134 Groups)	0/12,250	0%
Country	Categorical (156 Countries)	137/12,250	1.1%
Sector	Categorical (309 Sectors)	1,010/12,250	8.2%
Data Leaked	Binary (Yes = 1 / No = 0)	6,098/12,250	49.8%
Number of Employees	Categorical (Small, medium, large)	1,767/12,250	14.4%
Victim First Seen	Date (YYYY-MM-DD)	0/12,250	0%
Victim Last Seen	Date (YYYY-MM-DD)	0/12,250	0%

rebranding, with the list provided in Appendix B. Using Google, we searched for 'rebranding' AND 'ransomware group name', generating 134 queries aimed at uncovering rebranding events in cybersecurity blogs. We cross-referenced our rebranding list with the ransomware cartography developed by CERT Orange Cyberdefense [85]. Further validation was conducted through interviews from our pilot study, which added one more rebranding event to our list. Given the clandestine nature of rebranding, we acknowledge that our list may not be exhaustive. However, we believe it provides valuable exploratory insights to understand displacement within the scope of this study.

Overall, our findings yielded a list of 36 interventions, with some combined interventions treated as single events, resulting in 29 unique interventions. Groups stopping or rebranding before the intervention were excluded from the study, resulting in 17 unique interventions. The complete list is provided in Appendix A, with Table V presenting interventions alongside corresponding malicious actor actions after the intervention. Similarly, we identified 19 instances of ransomware group rebranding, with a list available in Appendix B.

Next, we describe the variables used in this study. The two **dependent variables** in our study are (see Table I):

1a. *Law Enforcement Intervention:* This categorical variable addresses propositions 1 and 6 by indicating whether the ransomware group experienced an intervention within our dataset. For propositions 2-5, it is also important to know the type of intervention. Therefore, we categorize the interventions as follows: 'arrest', 'sanction', 'crypto', 'decryptor', 'takedown', 'takedown+arrest', 'takedown+decryptor', and 'takedown+decryptor+arrest'. These interventions are described in Section II-A.

1b. *Response to Intervention:* This categorical variable addresses propositions 3 and 5 by indicating the different responses of ransomware groups to an intervention. Timing is crucial for this variable since some groups might have stopped publishing victims before a law enforcement intervention, making it impossible to measure the intervention's effect. If the ransomware group stopped publishing victims before the intervention, we denote the response as 'BEFORE'. If no victims were published on leak pages after an intervention, we assume the group stopped all ransomware operations, denoted as 'STOP'. If new victims were published after an intervention, we assume ransomware operations continued, denoted as 'CONTINUE'. If the groups rebranded after the intervention, they are categorized as 'REBRAND'.

The **independent variables** in this study are (See Table I):

2a. *Ransomware Group:* Names of the ransomware groups involved (categorical). In total 134 groups were found online and were included in the leak page dataset.

2b. *Country of Victim:* The country where the victim is located (categorical). There were 156 countries in the leak page dataset. Due to the prevalence of single or infrequent observations in countries and sectors, aggregation was performed. The top 10 most frequent countries were used, other countries were aggregated to category 'Other'.

2c. *Economic sector of Victim:* The economic sector in which the victim operates (categorical). The victims represented in the leak page dataset were active in 309 sectors. Due to the prevalence of single or infrequent observations aggregation was performed. Sectors were manually categorized as important or critical according to EU NIS2 legislation [82]. After aggregation 3,356 victims were considered critical, 2,415 victims were considered important and 5,463 victims were considered none of these. Additionally, sectors were aggregated based on technical intensity, measured through sector-level R&D expenditure [52]. After aggregation 2,391 victims were considered from sectors with high technological intensity, 3,187 victims with medium technological intensity, and 2,391 victims with low technological intensity. For an overview see Table I. See Table I.

2d. *Data Leakage Status:* Victims who were listed on the leak pages did not always have data exfiltrated. Data leakage status indicates whether data from the victim was or was not leaked, that is, data were published on the leak page (data leaked, binary: yes = 1 / no = 0).

2e. *Employee Count of Victim:* The number of employees working for the victim (categorical). Employee counts were aggregated into small (1-50 employees), medium (51-500 employees), and large (501+ employees) companies, following definitions by [23].

The analyses were conducted using RStudio and R version

4.3.1, employing packages *ggplot*, and *dplyr*. Listwise deletion was applied to handle missing observations. This research has received approval by the Ethics Committee at the University of Twente, registered under number 240026. We aim to collect empirical evidence which might align with the propositions as stated in Section II.

- **Proposition 1:** Logistic regression was used to determine if ransomware groups targeting a larger number of significant victims were more likely to face law enforcement interventions . In this context, "significant" refers to companies that are either critical according to the NIS directive, technologically intensive, based in the USA or elsewhere, or are large enterprises.
- **Proposition 2:** Due to many countries having a small number of attacks, or have victims listed by ransomware groups who faced an interventio n, a non-parametric Spearman's correlation test tested if countries with a many ransomware are more likely to conduct law enforcement interventions.
- **Propositions 3 and 5:** A binomial regression model tested to what extent ransomware groups cease operations, continue operations or rebrand after a LE intervention, compared to a baseline of zero.
- **Proposition 4:** A paired t-test and the non-parametric Wilcoxon signed-rank test were employed to compare the scale of operations—measured by the number and significance of victims—before and after interventions for groups that continued operations. Here, significance is defined as victims from high technological sectors and/or critical infrastructure according to NIS2.
- **Proposition 6:** A multinomial logistic regression will assess the relationship between an intervention, uptime of a leakpage, the number of victims and possible rebranding either with or without split-up and with or without overlapping uptime of leak page servers of the original group and the rebranded group.

A p-value of 0.05 or lower indicates that the variable significantly predicts the dependent variable at a significance level of $\alpha = 0.05$. Given the limited number of observed interventions, the statistical power of these tests is likely to be low. While conducting these tests could provide explorative insights regarding our propositions, the results should be interpreted cautiously due to the increased risk of Type I errors (false positives) and Type II errors (false negatives).

IV. Results of Analysis

In this section, we explore the group characteristics influencing the likelihood of a LE intervention. Subsequently, we outline the nature of the interventions carried out against the ransomware groups. Finally, we will conclude the section with an analysis of the reaction of the groups on the LE intervention.

A. Ransomware Groups Facing an LE Intervention

An overview of the descriptive statistics can be found in Table XI. Victims were reported across 156 countries and 309 sectors. Top sectors included Construction (662 observations), Law Practice (384 cases), and Hospitals and Health Care (378 victims). Most victims were from the United States, with 5,783 victims (47,7%). After normalizing for GDP [109], most countries appear to be relatively evenly affected, except for Canada (30.6%) and India (5.3%). Although the number of victims from critical (NIS) and technologically intensive (Tech) sectors is comparable to that of other countries, the percentage of data leaked on leak pages in the U.S. is lower at 37.2%, compared to 40-45% in other countries. This would suggests that the companies from the U.S. are more willing to pay, assuming that their data is less frequently published.

A summary of the results of the logistic regression analysis to address **Proposition 1** is shown in Table III. The analysis revealed several key findings regarding the impact of various factors on the probability of a ransomware group being targeted by a LE intervention. Firstly, groups that attack a large number of victims and mainly target large companies among have a much higher likelihood of facing a LE intervention then groups that make fewer victims and focus on smaller companies. Conversely, groups that attacked organisations belonging to Network Information Systems (NIS), to the technology sector, (Tech), whether or not they data was leaked and published on the leak page, and the amount of victims from the USA were not experiencing more LE interventions. Moreover, the total amount of time a group was active decreased the probability of intervention. Taken together, the evidence suggests support for **Proposition 1**, as a ransomware group's likelihood of facing intervention seems to rise with the number of victims, especially when those victims are substantial in size.

Although ransomware groups with many victims in the USA might not have a higher probability of facing interventions, US law enforcement could be more frequently involved with interventions compared to other countries. Table XI shows that the USA is involved in 20 out of 29 interventions. Similarly, LE in other top 10 most frequently attacked countries, such as France, Germany, Canada, Spain, and the UK, is also very active against ransomware groups (Table XI). While Ukraine is not among the top 10 most targeted countries, it might be involved in many interventions since any arrests in Ukraine

TABLE II
Descriptive Statistics of Leak Page Dataset: Frequency of Attacks, Frequency over GDP, Sector Importance (NIS and Tech), Company Size, and Data Leaked.

Country	Freq	Freq/GDP $\times 10^5$	% NIS	% Tech	% Large Companies	% Data Leaked
USA	5783 (47.7%)	24.7	47.3	44.2	26.7	37.2
UK	696 (5.7%)	24.5	48.3	40.9	26.9	43.5
Canada	608 (5.0%)	30.6	42.3	42.9	26.6	37.3
Germany	508 (4.2%)	13.5	46.7	51.0	43.9	40.6
France	494 (4.1%)	19.3	41.9	42.1	36.1	40.9
Italy	416 (3.4%)	22.1	50.7	46.9	25.8	35.6
Spain	260 (2.1%)	19.9	48.1	49.2	29.1	45.4
Australia	255 (2.1%)	16.4	46.7	40.0	20.1	44.3
Brazil	224 (1.8%)	12.7	46.0	44.2	53.6	46.0
India	168 (1.4%)	5.3	67.3	64.9	67.1	42.3
Other	2701 (22.3%)	X	48.9	50.6	47.1	41.8

TABLE III
LOGISTIC REGRESSION ANALYSIS OF THE LIKELIHOOD OF 134 RANSOMWARE GROUPS FACING AN INTERVENTION.

Variable	Estimate	Std. Error	z-value	Pr($>|z|$)
Intercept	-1.57	0.50	-3.13	0.002*
Total victims	0.19	0.09	2.12	0.034*
NIS count	-0.26	0.21	-1.22	0.224
Tech count	-0.22	0.19	-1.17	0.244
Uptime leakpage mean	-0.01	0.01	-2.44	0.015*
Data leak count	-0.13	0.07	-1.84	0.066
Large company count	0.45	0.20	2.27	0.023*
USA	-0.04	0.09	-0.43	0.667

TABLE IV
SUMMARY OF 29 INTERVENTIONS BY COUNTRY, WITH MULTIPLE COUNTRIES INVOLVED IN SOME INTERVENTIONS. TOP 10 COUNTRIES ARE SHOWN; OTHERS ARE GROUPED AS 'OTHER'.

Country	Arrest	Sanction	Crypto	Decryptor	Takedown	Multiple Interventions	Total
USA	6	5	1	1	2	5	20
UK	1	3	0	0	0	4	8
France	2	0	0	0	1	4	7
Germany	3	0	0	0	0	4	7
Netherlands	2	0	1	0	0	3	6
Ukraine	4	0	0	0	1	1	6
Sweden	1	0	0	0	0	3	4
Canada	1	0	0	0	0	2	3
Australia	1	1	0	0	0	1	3
Spain	0	0	0	0	0	3	3
Other	10	4	2	3	5	24	48

require the assistance of Ukrainian LE.

To address **Proposition 2**, we conducted a Spearman's correlation test, which was also significant. The test reveals a moderate, positive correlation ($\rho = 0.437, p < 0.001$) between the number of victims and the number of interventions, supporting **Proposition 2** that countries that suffer a relatively high level of victimization correlates are also involved in more LE interventions.

B. Actions Of Ransomware Groups After Intervention

We begin this section by examining the interventions we identified during the data collection process and providing examples of exactly what happened. We refer to ransomware groups by their name, for example 'Cl0p', 'Doppelpaymer', etc.

Intervention 1: Arrests. The ransomware group 'Cl0p' faced arrest of six persons and equipment seized on June 1, 2021, allegedly involving the part of the group responsible for money laundering [96]. They continued operations until the end of our data collection period. The arrests begin when Cl0p breached four South Korean companies in 2019. The 'Doppelpaymer' group faced an arrest on February 28, 2023. The last victim that they put online on their leak page was in September 2021; the group allegedly rebranded before [98]. LE in Germany arrested one person, together with the Ukrainian police. Both police forces also seized equipment. In addition, arrest warrants for three important figures in the group were issued. The same with 'Grief' ransomware group, which faced an arrest on February 28, 2023, whereas the last victim appeared on their leak page on March 2022. They probably rebranded before to 'NoEscape' [98]. Finally, 'REvil' faced arrests twice, on November 4, 2021, and January 14, 2022, and also apparently rebranded (at least partially) before to 'Blogxx', 'Spectre', and 'Ransom Cartel' [10], [47], [85]. The last victim of REvil was in October 2021 after LE intervention. 'Egregor' stopped after affiliates were arrested on February 10, 2021, in a collaborative operation of Ukraine and France LE [13]. France LE started the investigation apparently after complaints from the public over the ransomware gang. Finally, Lockbit faced an arrest of an affiliate on June 15, 2023, but continued its activities until the end of our dataset period [83].

Intervention 2: Sanctions. Sanctions typically involve travel restrictions, asset freezes, and/or arrest warrants [42], [100]. It is important to note that these actions were all initiated by LE. However, they are often implemented with considerable delays, frequently occurring after the targeted ransomware group has already ceased operations or undergone rebranding. For instance, sanctions against 'BlogXX' and 'Babuk' were imposed well after these groups had ceased publishing victims on leak pages, with more than a year passing before the individuals behind these operations were sanctioned [16], [97]. The imposition of sanctions against 'Babuk' may be linked to the public interview conducted with Babuk [97]. Similarly, sanctions against 'Conti' and 'REvil' were implemented after these groups had rebranded. In the case of 'Conti', sanctions were imposed half a year to one year after the group ceased operations [78], [79], while sanctions against REvil were enacted one month after the group stopped [111].

Intervention 3: Crypto-asset freezing. The freeze of crypto of the group 'DarkSide' occurred in the aftermath of the Colonial Pipeline attack, and after the group had already rebranded to 'BlackMatter' and/or 'BlackCat' [113]. Another crypto freeze involved the seizure of Cl0p assets in connection with the attack on Maastricht University [81]. It is worth mentioning that as a result of the freeze, Maastricht University received a refund of the ransom they had paid, and generated a significant profit due to the increased value of Bitcoin. 'Cl0p', however, continued their activities after this intervention.

Intervention 4: Decryptor release. 'Egregor' discontinued its ransomware operations before its creators distributed a decryptor, attributing the decision to the arrests of REvil members [114]. 'Avaddon' continued for 5 months after the decryptor became publicly available [110]. The 'BlackBasta' decryptor was known by December 30, 2023, but the group continued operations afterwards. Possibly, groups continuing operations after a decryptor becomes available change their ransomware malware [15]. After the 'REvil' decryptor became known on September

16, 2021, the USA assisted in its release [77]. A month later, on October 16, 2021, they released their last victim and rebranded [85]. While Bitdefender could not share details about how they obtained the master decryption key or the law enforcement agency involved, they informed BleepingComputer that it works for all 'REvil' victims encrypted before July 13th 2021. The Maze decryptor was released on February 9, 2022, while their latest victim was mentioned on the group's leak page on December 15, 2020. Allegedly, they published the decryptor released by their own makers, indicating a link to the 'REvil' arrests [114]. The Prometheus decryptor became known on August 1, 2021. A month later, on September 14, 2021, the last victim of the group was mentioned in the leak page data. The malware has a weak random number generator, which made a decryptor possible. Initially the Prometheus malware was based on Thanos ransomware, it later evolved into Spook, but they ceased operations on October 26, 2021 [14].

Intervention 5: Takedown of the leak page infrastructure. DarkSide experienced a takedown of their leak page infrastructure on May 13, 2021, although it remains unclear whether law enforcement was involved or if the group self-initiated the takedown to rebrand and mitigate the risk of law enforcement action [8]. Egregor was taken down on February 16, 2021, by the combined efforts of LE in the USA, France, and Ukraine. Following the takedown, the site remained offline, and associates deactivated their forum profiles [90]. Similarly, REvil was taken down on October 21, 2021. However, given that their last victim appeared on the group's leak page on October 16, this suggests that they already ceased their operations before the takedown. This takedown was initiated by the United States LE in response to REvil's significant Kaseya attack. Additionally, REvil's servers were reportedly hacked by the United States LE earlier in the same year [88]. Lastly, the takedown of Trigona was not conducted by LE but by the Ukrainian Cyber Alliance, an activist group targeting Russian hacker groups due to the Russian-Ukraine war [2].

6. Multiple interventions. There are five LE interventions that consisted of multiple actions . For instance, a takedown was combined with an arrest, decryptor, or both. AlphVM/Blackcat, which was the target of a joint operation involving LE of the USA, Germany, Denmark, Australia, UK, Spain, Switzerland, and Austria, underwent a takedown, followed by the subsequent release of a decryptor. Despite some fluctuations in website availability, the group continued its operations, with the last victim recorded on March 4, 2023 [3]. Similarly, Lockbit3.0 faced a takedown and decryptor release through coordinated efforts by LE of multiple countries including France, Germany, the Netherlands, Sweden, Australia, Canada, Japan, the UK, USA, and Switzerland [46]. Despite these actions, Lockbit3.0 persisted in publishing victims on their leak pages, remaining active throughout our observation period. The takedown and arrest of Netwalker and Ragnar Locker on January 27, 2021, and October 11, 2023, respectively, were successful, meaning that no further victims were reported on the groups leak page or on other security blogs post-intervention [9], [45]. Likewise, Hive, targeted on January 26, 2023, experienced a takedown, a decryptor release, and arrests through coordinated actions involving the LE of 13 countries [89]. Subsequently, there was no further activity from Hive on the leak page.

It is important to note that we encountered several events occurring across multiple groups, which could have potentially impacted a groups' decisions to cease operations or undergo rebranding. These events included internal disputes, self-shutdowns, and public interviews. We describe these events below.

Two groups experienced an internal dispute that resulted in leaks of private communications. These leaks became known as the Conti leaks and the Yanluowang Leaks [40], [112]. The Conti leaks ensued after a conflict over a public statement indicating Conti's support for Russia in the Russia-Ukraine war [51]. Yanluowang, consisting of 18 members, of which 5 were active, and had chats that were exposed by a group member, revealing plans to target critical infrastructure, excluding those from the Soviet Union [40].

Some groups publicly announced they ceased operations, sometimes combined with the release of decryption keys. This is also labelled as 'self-shutdowns'. Sometimes this self-shutdown is combined with an 'exit scam', in which ransomware groups state they have been arrested by LE, with the hidden aim to keep the profit share of affiliates to themselves [95]. We observed self-shutdowns of File Leaks, AstroLocker, Ragnarok, BlackMatter, and Avaddon. Two groups, File Leaks and AstroLocker, underwent rebranding after a self-shutdown [12], [14]. Avaddon possibly rebranded after 2.5 years to NoEscape [10].

Furthermore, some ransomware actors grant interviews [62], [97], possibly driven by a desire to establish a reputation or a perception of invincibility against arrest [39], [62]. Typically, these interviews are conducted anonymously. One notable exception is the interview with Wazawaka, who provided insights into ransomware attacks of Babuk ransomware that only the perpetrator could possess [97]. This interview revealed the identity of Wazawaka and might therefore have an impact on the continuation of ransomware operations of Babuk.

There are several considerations regarding the labeling of interventions. Firstly, it's important to highlight that two groups, Hive and Netwalker, potentially underwent rebranding some time after the intervention, with Hive rebranding after nine months. According to the Hive operators, they sold their ransomware malware to Hunters International, but they kept operating independently as two separate groups. We decided that this incident is no rebranding event because there appear to be two different groups.

Secondly, the arrest of an actor associated with Doppelpaymer/Grief/Entropy is treated as a single intervention due

TABLE V
THE ACTIONS OF RANSOMWARE GROUPS IN RESPONSE TO VARIOUS INTERVENTIONS, WHICH INCLUDES INTERVENTIONS OCCURRING PRIOR TO GROUP STOPPING (STOP BEFORE) OR REBRANDING (REBRAND BEFORE).

Intervention	STOP BEFORE	REBRAND BEFORE	CONTINUE	STOP	REBRAND	Total
Arrest	0	4	2	1	0	7
Crypto Freeze	1	0	1	0	0	2
Decryptor	2	0	2	0	2	6
Sanction	1	3	0	1	0	5
Takedown	0	1	1	2	0	4
Takedown, Arrest	0	0	0	2	0	2
Takedown, Decryptor	0	0	1	0	0	1
Takedown, Decryptor, Arrest	0	0	1	1	0	2
Total	**4**	**8**	**8**	**7**	**2**	**29**

to the multiple rebrandings preceding the arrests, indicating a complex scenario where all three groups were linked to the same attack.

Thirdly, out of the 25 groups targeted by interventions, seven experienced multiple interventions over time, with REvil facing the highest number of interventions (five in total) before rebranding. It's noteworthy that law enforcement's decryptor capabilities, as claimed in some cases like Lockbit3.0, appear to be relatively limited.

Reviewing the outcomes of various interventions (see Table V), we observe that prior to any intervention, 4 groups stopped victim publication (STOP BEFORE), while 8 groups rebranded before an intervention (REBRAND BEFORE). 8 ransomware groups continued their activities post-intervention (CONTINUE). Additionally, 7 groups ceased operations post-intervention (STOP), and 2 groups rebranded after the intervention.

To address **Proposition 3**, a binomial test was conducted to evaluate the effectiveness of interventions on ransomware groups ceasing operations. With 7 cases where groups ceased operations out of 17 total interventions where groups did not already stop or rebrand before the intervention. The test was significant ($p < 0.001$). However, rebranding was with 2 out of 17 cases not significantly different from 0 ($p = 0.2078$), which implies groups do not rebrand after an intervention, contradicting **Proposition 5**.

In addition to examining post-intervention behaviors of ransomware groups, it is interesting to better understand the dynamic between ransomware group characteristics and type of interventions. Table VI offers an overview of statistics of intervention type and ransomware group characteristics. Notably, the analysis helps improve our understanding of intervention strategies and ransomware group actions. For example, sanctions (such as travel restrictions and/or assets freeze) and arrests typically occur after a group has ceased operations, reflecting the time it takes for law enforcement to identify suspects.Ransomware groups facing arrests and sanctions tend to have the largest average amount of victims, as observed among those subjected to multiple interventions. Taken together, these results imply that arrests and sanctions take more effort from law enforcement, and are used against ransomware groups that claim large of victims. Additionally, the decryptor intervention yields minimal differences between uptime and intervention time, suggesting that many ransomware groups rebrand or cease operations if a decryptor is available. Here, intervention time is the time between a group published there first victim and the LE intervention. Finally, takedowns is associated with an intervention time of approximately 197 days, despite groups continuing operations for roughly another 200 days thereafter, implying a relatively straightforward intervention process for law enforcement.

TABLE VI
SUMMARY OF RANSOMWARE GROUP STATISTICS BY INTERVENTION TYPE.

Intervention Type	Freq	Mean Victims	Mean Intervention Time	Mean Uptime Leak Page	Δ Uptime - Intervention Time
Arrest	7	468	399	636	237
Sanction	5	425	727	505	-222
Crypto	2	316	379	671	292
Decryptor	6	243	316	348	32
Takedown	4	171	197	399	202
Multiple interventions	5	540	604	622	18
Interview, Dispute, Shutdown	10	373	442	551	109

C. Crime Displacement After Intervention

In this subsection we will first compare the scale of the operations of ransomware groups, before and after a LE intervention. Subsequently, we will examine the relationship between law enforcement interventions and specific types of rebranding.

Firstly, ransomware groups may alter their targeting strategy following an intervention, potentially opting to target fewer victims or shifting focus away from critical infrastructure to mitigate the risk of further interventions or Law Enforcement attention. See Table VII for overview of groups who continue after an LE intervention.

To evaluate **Proposition 4**, we conducted a paired t-test, revealing no significant differences in the mean values of the number of victims ($p = 0.143$), % of large companies ($p = 0.378$), % NIS ($p = 0.856$), and % USA ($p = 0.492$). However, only for % tech companies, the paired t-test yielded a

TABLE VII
COMPARISON OF VICTIM CHARACTERISTICS OF RANSOMWARE GROUPS WHO CONTINUE BEFORE AND AFTER INTERVENTIONS

Ransomware Group	Intervention	Victims Before Intervention	Victims After Intervention	% Large companies before Intervention	% Large companies after Intervention	% NIS before Intervention	% NIS after Intervention	% Tech before Intervention	% Tech after Intervention	% USA before Intervention	% USA after Intervention
AlphVM	Takedown, Decryptor	687	64	38.7	33.9	50.5	58.1	20.4	25.8	50.1	57.8
Avaddon	Decryptor	23	173	22.2	23.8	33.3	54.3	16.7	21.0	69.6	36.0
BlackBasta	Decryptor	382	42	34.5	22.5	43.0	40.0	20.7	15.0	57.5	53.7
CL0P	Crypto	131	399	40.3	63.7	60.5	64.5	24.8	31.4	62.6	61.0
CL0P	Arrest	66	464	66.7	56.8	70.8	62.5	26.2	30.3	50.0	63.0
LockBit 3.0	Takedown, Decryptor, Arrest	1574	19	28.1	47.4	50.0	47.4	20.4	21.1	35.9	63.2
LockBit 3.0	Arrest	902	691	29.4	27.2	49.2	50.9	20.9	19.9	33.2	40.2
REvil	Decryptor	312	5	33.9	40.0	45.1	20.0	17.5	20.0	60.5	20.0
Trigona	Takedown	35	13	18.2	18.2	42.4	50.0	15.2	25.0	45.7	33.3

significant result ($p = 0.039$), meaning that percentage of tech companies before is larger than amount of tech companies after intervention. Additionally, to assess the robustness of these findings, we employed a non-parametric Wilcoxon signed-rank test. The results of this test resembled those of the paired t-test, indicating no significant differences, before and after the LE intervention in the number of victims ($p = 0.160$), % large companies ($p = 0.441$), % NIS ($p = 0.695$), and % USA ($p = 0.625$). Yet, for % tech companies, the Wilcoxon test is on the verge of statistical significance with p= ($p = 0.064$) with $\alpha = 0.05$. We conclude that, besides a decrease of tech companies after intervention, we do not have sufficient statistical evidence to support **Proposition 4**.

The second issue is rebranding. Ransomware groups may choose to rebrand and adopt a different strain, which could represent a form of crime displacement. We identify four types or groups of rebranding in our dataset, see Table VIII.

To address **Proposition 6**, a multinomial logistic regression was performed to assess the relationship between interventions, leak page uptime, and the number of victims in relation to different types of rebranding: with or without split-up and with or without overlapping uptime. Despite the limited number of observations in the different groups (see Table VIII), the model revealed a significant relationship between intervention and Group 1 (no split-up and no overlap) ($p < 0.001$). The other variables were not significant. This result is not congruent with **Proposition 6**, as Group 1 has no split-up. However, given that only two ransomware groups split up after rebranding, these findings may be attributed to the limited number of observations.

TABLE VIII
NAMES OF RANSOMWARE GROUPS WHO REBRANDED CATEGORIZED BY OVERLAP AND SPLIT-UP

Overlap	No split-up	Split-up
No Overlap	**Group 1** Avaddon, Cuba, Babuk, Darkside, Hive, RansomHouse, Nefilim, Prometheus	**Group 2** Conti
Overlap	**Group 3** DoppelPaymer, Haron, Lockbit1.0, Lockbit2.0, Vice Society	**Group 4** Maze

V. DISCUSSION AND CONCLUSION

In this study, our primary objective was to investigate the response of ransomware groups to law enforcement interventions. To achieve this, we formulated three research questions.

RQ1 aimed to understand the factors influencing the probability of a law enforcement intervention. We found that ransomware group characteristics such as total amount of victims, uptime of the leakpage, and the presence of large companies significantly impacted intervention probability. Additionally, law enforcement was more active in countries heavily affected by ransomware attacks. However, other factors like victim count of critical infrastructure, technological intensive sectors and data leakage did not affect the likelihood of ransomware groups being targeted by law enforcement.

RQ2 aimed to understand how ransomware actors respond to various law enforcement interventions, including arrests, sanctions, crypto-asset freezes, decryptors, and takedowns. Post-intervention, 8 out of 17 groups continued operations, 7 groups ceased operations, and 2 groups rebranded. We conclude that law enforcement interventions significantly impact ransomware operations, aligning with Situational Crime Prevention theory, where interventions increase efforts and risks while decreasing profits for ransomware groups.

RQ3 aimed to understand crime displacement. We found that ransomware groups typically do not rebrand after an intervention. However, there was limited evidence suggesting that groups continuing operations post-intervention change the type or number of victims they target, including a decreased number of victims from technological intensive sector. Additionally, interventions were linked to rebranding characterized by no overlap between the old and new group's leak page uptime and no split-up into multiple new groups.

Our exploratory analysis suggests that arrests and sanctions may correlate with ransomware groups having a high victim count, with law enforcement taking longer to intervene from the time the first victim is published. Different kinds of interventions appeared to have specific consequences. The presence of a decryptor was linked to shorter leak page uptimes post-intervention. Takedowns of leak pages were associated with fewer victims and quicker intervention times. Considering that 2 out of 4 ransomware groups ceased activity following

takedowns, this approach could be seen as a cost-effective intervention strategy against ransomware.

VI. Limitations and Further Work

There are different limitations of this study:

1. **Causality.** Drawing causal conclusions from observational data presents challenges [63], [106], [108]. Ransomware groups may differ in various ways beyond facing interventions. Nonetheless, as emphasized by [108], an overly strict focus on the 'causation versus correlation distinction' can be limiting, as even randomized control experiments do not always provide watertight evidence. Furthermore, there are legal and ethical challenges conducting randomized trials with law enforcement interventions. Therefore, we argue this paper is a best effort of understanding the relationship between interventions and action of ransomware groups.
2. **Low sample size.** Due to low sample size of interventions, it is hard to draw definitive conclusions because the statistical tests that were used do not have that much statistical power. Furthermore, it makes an analysis more prone to measurement errors, to the volatility or special circumstances of specific groups.
3. **Biased intervention list.** Our list of interventions may be biased due to the 'searchlight effect' [108], wherein interventions are more likely to be found in areas that are actively searched, potentially overlooking others. For example, the absence of Chinese or Japanese-speaking authors may hinder the identification of interventions from these regions. Additionally, some law enforcement interventions may not be publicly disclosed. To mitigate this bias, future research could explore alternative search engines from different countries and continents.

Further research could explore the costs associated with different types of law enforcement and government agency interventions, both material and immaterial [68]. This would enable cost-benefit analyses to evaluate the effectiveness and efficiency of various intervention strategies and compare them with preventive interventions, which might be more cost-effective [19], [55], [56], [86]. Additionally, investigating the impact of perceived attacker reputation on ransomware groups' decisions to rebrand or cease operations could provide valuable insights. Attacker reputation usually refers to the perceived likelihood of receiving a decryption key after payment [20]. Examining how law enforcement interventions affect attacker reputation from both the victim's and affiliate's perspectives could offer a broader understanding of intervention effectiveness.

In conclusion, this study is the first to evaluate ransomware interventions using data from victims published on leak pages after double-extortion ransomware attacks. Despite its limitations, we believe this study represents a step in the right direction for policymakers and law enforcement agencies worldwide to make more evidence-based decisions regarding law enforcement interventions.

VII. Policy Recommendations

This study provides insights for policymakers and law enforcement on the effectiveness of ransomware interventions. The results suggest the following:

Policy Implication 1: Emphasize Frequency over Scale. Based on our findings, increasing the frequency of interventions might be disruptive. Smaller, frequent actions might significantly pressure malicious actors, contrary to the expert belief that only major takedowns or arrests are effective.

Policy Implication 2: Maintain Unpredictability. Vary and randomize interventions to counter ransomware groups' adaptive methods. Use the different types of interventions discussed in this paper as inspiration. Focusing on implementing Situational Crime Prevention principles—such as Increasing Effort, Increasing Risks, Reducing Rewards, Reducing Provocations, and Removing Excuses—can enhance effectiveness [4], [26], [27], [36], [56], [60].

While our study indicates smaller interventions can be effective, more controlled studies are needed. The discrepancy between our findings and expert opinions underscores the need for further research to refine these recommendations.

VIII. Ethics

We follow the principles from Menlo Report [5] to justify the ethical considerations made in this study:

Respect for Persons: Prioritizing privacy and confidentiality, data was aggregated at country and sector levels to safeguard the privacy of victims.

Beneficence: While there is a possibility that providing information about interventions may aid criminals in altering their actions, we believe our approach ultimately aids law enforcement in combating ransomware. We estimate that the overall impact of our study is positive.

Justice: All ransomware attacks included in the study were afforded equal opportunity, without bias towards specific entities. Selection criteria were based solely on the presence of ransomware-related keywords.

Respect for Law and Public Interest: Information pertaining to law enforcement operations and government interventions was handled discreetly. Our study aims to offer valuable insights into the effectiveness and cost-benefit of law enforcement interventions against ransomware, thereby assisting law enforcement in making well-informed decisions when planning interventions.

IX. Acknowledgments

We would like to extend our sincere gratitude to the Dutch Police. We would like to thank the Cybercrime Unit East Netherlands and the participants of the interviews for their expertise. Please note that the views expressed in this work are ours alone and do not necessarily reflect those of the Dutch Police. Finally, we would like to thank the anonymous reviewers for their suggestions to improve this paper. Funding support from the National Science Foundation (NSF) grants 1844753 and 2039693.

REFERENCES

[1] Alzahrani, S., Xiao, Y., & Sun, W. (2022). An analysis of conti ransomware leaked source codes. IEEE Access, 10, 100178-100193.

[2] Ars Technica (2023). Retrieved March 27, 2024, from https://arstechnica.com/security/2023/10/two-ransomware-gangs-knocked-out-of-commission-in-a-single-week/

[3] Ars Technica (2023). Retrieved March 27, 2024, from https://arstechnica.com/security/2023/12/alphv-ransomware-site-is-seized-by-the-fbi-then-its-unseized-and-so-on/

[4] Bada, M., Hutchings, A., Papadodimitraki, Y., & Clayton, R. (2023). An evaluation of police interventions for cybercrime prevention (No. UCAM-CL-TR-983). University of Cambridge, Computer Laboratory.

[5] Bailey, M., Dittrich, D., Kenneally, E., & Maughan, D. (2012). The menlo report. IEEE Security & Privacy, 10(2), 71-75.

[6] Berlusconi, G. (2023). Open Acess: Come at the king, you best not miss: criminal network adaptation after law enforcement targeting of key players. In The Criminology of Carlo Morselli-Part I (pp. 44-64). Routledge.

[7] Blatchly, J. (2023). The Impact of Ransomware–A Comparison of Worldwide Governmental Policies and Recommendations for Future Directives (Doctoral dissertation, Utica University).

[8] BleepingComputer (2021). Retrieved March 27, 2024, from https://www.bleepingcomputer.com/news/security/darkside-ransomware-servers-reportedly-seized-operation-shuts-down/

[9] BleepingComputer (2021). Retrieved March 27, 2024, from https://www.bleepingcomputer.com/news/security/NetWalker-ransomware-dark-web-sites-seized-by-law-enforcement/

[10] BleepingComputer (2021). Retrieved March 27, 2024, from https://www.bleepingcomputer.com/news/security/avaddon-ransomware-shuts-down-and-releases-decryption-keys/

[11] BleepingComputer (2021). Retrieved March 27, 2024, from https://www.bleepingcomputer.com/news/security/ragnarok-ransomware-releases-master-decryptor-after-shutdown/

[12] BleepingComputer (2021). Retrieved March 27, 2024, from https://www.bleepingcomputer.com/news/security/synack-ransomware-releases-decryption-keys-after-el-cometa-rebrand/

[13] BleepingComputer (2021). Retrieved March 27, 2024, from https://www.bleepingcomputer.com/news/security/egregor-ransomware-affiliates-arrested-by-ukrainian-french-police/

[14] BleepingComputer (2022). Retrieved March 27, 2024, from https://www.bleepingcomputer.com/news/security/astralocker-ransomware-shuts-down-and-releases-decryptors/

[15] BleepingComputer (2023). Retrieved March 27, 2024, from https://www.bleepingcomputer.com/news/security/new-black-basta-decryptor-exploits-ransomware-flaw-to-recover-files/

[16] BleepingComputer (2024). Retrieved March 27, 2024, from https://www.bleepingcomputer.com/news/security/us-uk-australia-sanction-revil-hacker-behind-medibank-data-breach/

[17] Borrion, H., Dehghanniri, H., & Li, Y. (2017). Comparative analysis of crime scripts: One CCTV footage—twenty-one scripts. Paper presented at the 2017 European Intelligence and Security Informatics Conference (EISIC).

[18] Branas, C., Buggs, S., Butts, J. A., Harvey, A., Kerrison, E. M., Meares, T., & Webster, D. (2020). Reducing violence without police: A review of research evidence.

[19] Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A., Maimon, D., ... & Maimon, D. (2019). Situational crime prevention. Cybercrime Prevention: Theory and Applications, 17-33.

[20] Cartwright, A., & Cartwright, E. (2019). Ransomware and reputation. Games, 10(2), 26.

[21] Cartwright, A., Cartwright, E., MacColl, J., Mott, G., Turner, S., Sullivan, J., & Nurse, J. R. (2023). How cyber insurance influences the ransomware payment decision: theory and evidence. The Geneva Papers on Risk and Insurance-Issues and Practice, 48(2), 300-331.

[22] Hernandez-Castro, J., Cartwright, A., & Cartwright, E. (2020). An economic analysis of ransomware and its welfare consequences. Royal Society open science, 7(3), 190023.

[23] Centraal Bureau voor de Statistiek. (2017, July 11). Meer bedrijven met bedrijfsopleidingen. CBS. Retrieved March 27, 2024, from https://www.cbs.nl/nl-nl/nieuws/2017/28/meer-bedrijven-met-bedrijfsopleidingen/bedrijfsgrootte

[24] Chainalysis (2024). Crypto Crime Report 2024. Retrieved March 27, 2024, from https://go.chainalysis.com/2024/crypto-crime-report.html

[25] Clarke, R. V. (1983). Situational crime prevention: Its theoretical basis and practical scope. Crime and justice, 4, 225-256.

[26] Clarke, R. V., & Eck, J. E. (2005). *Crime Analysis for Problem Solvers in 60 Small Steps*. Retrieved from Washington D.C.: http://www.popcenter.org/library/reading/PDFs/60steps.pdf

[27] Clarke, R. V. (2008). Situational crime prevention. In R. Wortley & L. Mazerolle (Eds.), Environmental Criminology and Crime Analysis (pp. 178-194). London, UK: Willan.

[28] Clarke, R. V. (2009). Situational crime prevention: Theoretical background and current practice. In Handbook on crime and deviance (pp. 259-276). New York, NY: Springer New York.

[29] Clough, J. (2014). A world of difference: the Budapest convention on cybercrime and the challenges of harmonisation. Monash University Law Review, 40(3), 698-736.

[30] Cohen, L. E., & Felson, M. (1979). Social-change and crime rate trends - routine activity approach. American Sociological Review, 44, 588-608. Retrieved from ¡Go to ISI¿://A1979HL64700005

[31] Coles-Kemp, L., & Theoharidou, M. (2010). Insider threat and information security management. In Insider threats in cyber security (pp. 45-71). Boston, MA: Springer US.

[32] Collier, B., Thomas, D. R., Clayton, R., & Hutchings, A. (2019, October). Booting the booters: Evaluating the effects of police interventions in the market for denial-of-service attacks. In Proceedings of the internet measurement conference (pp. 50-64).

[33] Collier, B., Thomas, D. R., Clayton, R., Hutchings, A., & Chua, Y. T. (2022). Influence, infrastructure, and recentering cybercrime policing: evaluating emerging approaches to online law enforcement through a market for cybercrime services. Policing and Society, 32(1), 103-124.

[34] Connolly, L. Y., Wall, D. S., Lang, M., & Oddson, B. (2020). An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability. Journal of Cybersecurity, 6(1), tyaa023.

[35] Connolly, A. Y., & Borrion, H. (2022). Reducing ransomware crime: analysis of victims' payment decisions. Computers & Security, 119, 102760.

[36] Cornish, D. B. (1994). Proceedings of the International Seminar on Environmental Criminology and Crime Analysis (pp. 30–45). Tallahassee, FL: Florida Statistical Analysis Center, Florida Criminal Justice Executive Institute and Floria Department of law enforcement.

[37] Cornish, D. B., & Clarke, R. V. (2014). The reasoning criminal: Rational choice perspectives on offending: Transaction Publishers.

[38] Cosin Camichel. 2022. Ecrime. https://ecrime.ch/. Accessed: 01-03-2023.

[39] Cyble (2021). Retrieved March 27, 2024, from https://cyble.com/blog/uncensored-interview-with-revil-sodinokibi-ransomware-operators/

[40] Darktrace (2022). Retrieved March 27, 2024, from https://darktrace.com/blog/inside-the-yanluowang-leak-organization-members-and-tactics

[41] Dehghanniri, H., & Borrion, H. (2019). Crime scripting: a systematic review. *European Journal of Criminology*.

[42] European Sanctions Map (n.d.). Retrieved March 20, 2024, from https://sanctionsmap.eu/#/main

[43] Europol (2021). Internet Organised Crime Threat Assessment (IOCTA) 2021, Publications Office of the European Union, Luxembourg, Retrieved August 31, 2022, from https://www.europol.europa.eu/publications-events/mainreports/internet-organised-crime-threat-assessment-iocta-2021

[44] Europol (2023). Internet Organised Crime Threat Assessment (IOCTA) 2023. Luxembourg: Publications Office of the European Union. Retrieved August 31, 2023, from https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-assessment-iocta-2023

[45] Europol (2023). Retrieved March 27, 2024, from https://www.europol.europa.eu/media-press/newsroom/news/ragnar-locker-ransomware-gang-taken-down-international-police-swoop

[46] Europol (2024). Retrieved March 27, 2024, from https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

[47] Europol (2021). Retrieved March 27, 2024, from https://www.europol.europa.eu/media-press/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged

[48] Felson, M. (2017). Linking criminal choices, routine activities, informal control, and criminal outcomes. In The reasoning criminal (pp. 119-128): Routledge.

[49] Felson, M., & Clarke, R. V. (1998). Opportunity Makes the Thief. Police Research Series, Paper 98. Policing and Reducing Crime Unit, Research, Development and Statistics Directorate. London: Home Office.

[50] Fleiss, J.L., "Measuring Agreement between Two Judges on the Presence or Absence of a Trait", Biometrics, vol. 31, no. 3, pp. 651–659, 1975, ISSN: 0006341X, 15410420. Available at: http : / / www. jstor. org / stable/2529549 (visited on 09/01/2022).

[51] Gray, I. W., Cable, J., Brown, B., Cuiujuclu, V., & McCoy, D. (2022, November). Money Over Morals: A Business Analysis of Conti Ransomware. In 2022 APWG Symposium on Electronic Crime Research (eCrime) (pp. 1-12). IEEE.

[52] Galindo-Rueda, F. and F. Verger (2016) OECD Taxonomy of Economic Activities Based on R&D Intensity, OECD Science, Technology and Industry Working Papers, 2016/04, OECD Publishing, Paris. http://dx.doi.org/10.1787/5jlv73sqqp8r-en

[53] Guerette, R. T., & Bowers, K. J. (2009). Assessing the extent of crime displacement and diffusion of benefits: a review of situational crime prevention evaluations. Criminology, 47(4), 1331 - 1368

[54] Heaton, R., & Tong, S. (2016). Evidence-based policing: from effectiveness to cost-effectiveness. Policing: a journal of policy and practice, 10(1), 60-70.

[55] Hodgkinson, T., & Farrell, G. (2018). Situational crime prevention and Public Safety Canada's crime-prevention programme. Security Journal, 31, 325-342.

[56] Ho, H., Ko, R., & Mazerolle, L. (2022). Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review. Computers & Security, 115, 102611.

[57] Irwin, A. S., & Dawson, C. (2019). Following the cyber money trail: Global challenges when investigating ransomware attacks and how regulation can help. Journal of money laundering control, 22(1), 110-131.

[58] Jamali, H. R., & Asadi, S. (2010). Google and the scholar: the role of Google in scientists' information-seeking behaviour. Online information review, 34(2), 282-294.

[59] Jansen, F., & van Lenthe, J. (2016). Adaptation strategies of cybercriminals to interventions from public and private sectors. In Cybercrime Through an Interdisciplinary Lens (pp. 224-255). Routledge.

[60] Hartel, P. H., Junger, M., & Wieringa, R. J. (2010). Cyber-crime science= crime science+ information security. CTIT, University of Twente, Technical Report TR-CTIT-10-34.

[61] Keatley, D. (2018). Crime Script Analysis. In *Pathways in Crime: An Introduction to Behaviour Sequence Analysis* (pp. 125-136). Cham: Springer International Publishing.

[62] KELA (2021). Retrieved March 27, 2024, from https://www.kelacyber.com/lockbit-2-0-interview-with-russian-osint/

[63] Lanfear, C. C., Matsueda, R. L., & Beach, L. R. (2020). Broken windows, informal social control, and crime: Assessing causality in empirical studies. Annual review of criminology, 3, 97-120.

[64] Leukfeldt, R., & Kleemans, E. E. (2019). Cybercrime, money mules and situational crime prevention: Recruitment, motives and involvement mechanisms. In Criminal networks and law enforcement (pp. 75-89). Routledge.

[65] Li, Z., & Liao, Q. (2020). Ransomware 2.0: to sell, or not to sell a game-theoretical model of data-selling ransomware. In Proceedings of the 15th International Conference on Availability, Reliability and Security (pp. 1-9).

[66] Lubin, A. (2022). The Law and Politics of Ransomware. Vand. J. Transnat'l L., 55, 1177.

[67] Maimon, D. (2020). Deterrence in Cyberspace: an interdisciplinary review of the empirical literature. The Palgrave handbook of international cybercrime and cyberdeviance, 449-467.

[68] Manning, M., Wong, G. T., Graham, T., Ranbaduge, T., Christen, P., Taylor, K., & Skorich, P. (2018). Towards a 'smart'cost–benefit tool: using machine learning to predict the costs of criminal justice policy interventions. Crime Science, 7, 1-13.

[69] Marshall, J., Khodjibaev, A., Korzhevin, D., & McKay, K. (2021, February 2). Interview with a LockBit ransomware operator. Talos Intelligence Blog. Retrieved March 20, 2024, from https://blog.talosintelligence.com/interview-with-lockbit-ransomware/

[70] Matthijsse, S. R., van 't Hoff-de Goede, M. S., & Leukfeldt, E. R. (2023). Your files have been encrypted: A crime script analysis of ransomware attacks. Trends in Organized Crime, 1-27.

[71] Meurs, T., Junger, M., Tews, E., & Abhishta, A. (2022). Ransomware: How attacker's effort, victim characteristics and context influence ransom requested, payment and financial loss. In 2022 APWG Symposium on Electronic Crime Research (eCrime) (pp. 1-13). IEEE.

[72] Meurs, T., Junger, M., Tews, E., & Abhishta, A. (2022). NAS-ransomware: hoe ransomware-aanvallen tegen NAS-apparaten verschillen van reguliere ransomware-aanvallen. Tijdschrift voor Veiligheid, 21(3-4), 69-88. https://doi.org/10.5553/TvV/.000044

[73] Meurs, T., & Holterman, L. (2022). Whitepaper data-exfiltratie bij een ransomware-aanval. Cyberveilig Nederland. Retrieved March 20, 2024, from https://executivefinance.nl/wp-content/uploads/2023/01/VCNL-Whitepaper-Exfiltratie.pdf

[74] Meurs, T., Junger, M., Abhishta, A., Tews, E., & Ratia, E. (2022). CO-ORDINATE: A model to analyse the benefits and costs of coordinating cybercrime. JISIS, 12(4).

[75] Meurs, T., Cartwright, E., Cartwright, A., Junger, M., Hoheisel, R., Tews, E., & Abhishta, A. (2023, November). Ransomware economics: a two-step approach to model ransom paid. In 18th Symposium on Electronic Crime Research, eCrime 2023.

[76] Malwarebytes (2022). Retrieved March 27, 2024, from https://www.malwarebytes.com/blog/news/2022/06/rsa-2022-prometheus-ransomwares-flaws-inspired-researchers-to-try-to-build-a-near-universal-decryption-tool

[77] MSSP Alert (2021). Retrieved March 27, 2024, from https://www.msspalert.com/news/fbi-withheld-revil-ransomware-decryptor-key-as-some-msps-suffered-encryption

[78] National Crime Agency (2023). Retrieved March 27, 2024, from https://www.nationalcrimeagency.gov.uk/news/ransomware-criminals-sanctioned-in-joint-uk-us-crackdown-on-international-cyber-crime

[79] National Crime Agency (2023). Retrieved March 27, 2024, from https://www.gov.uk/government/news/uk-sanctions-members-of-russian-cybercrime-gang

[80] No More Ransom. (n.d.). Retrieved March 25, 2024, from https://web.archive.org/web/20240000000000*/www.nomoreransom.org

[81] NOS. (2022). Retrieved March 27, 2024, from https://nos.nl/artikel/2434926-universiteit-maastricht-krijgt-losgeld-voor-hack-terug-met-flinke-winst

[82] NCSC (2024). Amendment: NIS2 Directive Protects Network Information Systems. Retrieved March 27, 2024, from https://business.gov.nl/amendment/nis2-directive-protects-network-information-systems/

[83] Office of Public Affairs (2023). Retrieved March 27, 2024, from https://www.justice.gov/opa/pr/russian-national-arrested-and-charged-conspiring-commit-lockbit-ransomware-attacks-against-us

[84] Padayachee, K. (2015, August). A framework of opportunity-reducing techniques to mitigate the insider threat. In 2015 Information Security for South Africa (ISSA) (pp. 1-8). IEEE.

[85] Pichon, M. (March 2024, version 26). Global CERT Orange CyberDefense - World Watch team's ransomware ecosystem map. Retrieved from https://github.com/cert-orangecyberdefense/ransomware_map

[86] Piza, E. L. (2018). The effect of various police enforcement actions on violent crime: Evidence from a saturation foot-patrol intervention. Criminal Justice Policy Review, 29(6-7), 611-629.

[87] Plano Clark, V. L. (2017). Mixed methods research. The Journal of Positive Psychology, 12(3), 305-306.

[88] Reuters (2021). Retrieved March 27, 2024, from https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/

[89] Reuters (2023). Retrieved March 27, 2024, from https://www.reuters.com/world/us/announcement-posted-hive-ransomware-groups-site-says-it-has-been-seized-by-fbi-2023-01-26/

[90] SC Magazine (2021). Retrieved March 27, 2024, from https://www.scmagazine.com/news/the-egregor-takedown-new-tactics-to-take-down-ransomware-groups-show-promise

[91] Sekoia (2022). Retrieved March 27, 2024, from https://blog.sekoia.io/the-story-of-a-ransomware-builder-from-thanos-to-spook-and-beyond-part-2/

[92] Sherman, L. W. (2013). The rise of evidence-based policing: Targeting, testing, and tracking. Crime and justice, 42(1), 377-451.

[93] Smilyanets, D. (2022). An interview with initial access broker Wazawaka: 'There is no such money anywhere as there is in

ransomware'. The Record. Retrieved March 20, 2024, from https://therecord.media/an-interview-with-initial-access-broker-wazawaka-there-is-no-such-money-anywhere-as-there-is-in-ransomware
[94] Sutter, T., Bozkir, A. S., Gehring, B., & Berlich, P. (2022). Avoiding the hook: influential factors of phishing awareness training on click-rates and a data-driven approach to predict email difficulty perception. Ieee Access, 10, 100540-100565.
[95] The Hacker News (2024). Retrieved March 27, 2024, from https://thehackernews.com/2024/03/exit-scam-blackcat-ransomware-group.html
[96] The Record (2021). Retrieved March 27, 2024, from https://therecord.media/ukrainian-police-arrest-clop-ransomware-members-seize-server-infrastructure
[97] The Record (2022). Retrieved March 27, 2024, from https://therecord.media/an-interview-with-initial-access-broker-wazawaka-there-is-no-such-money-anywhere-as-there-is-in-ransomware
[98] The Register (2023). Retrieved March 27, 2024, from https://www.theregister.com/2023/03/06/DoppelPaymerransomwarearrests/
[99] U.S. Department of the Treasury. (2023). Retrieved March 27, 2024, from https://home.treasury.gov/news/press-releases/jy1486
[100] U.S. Department of the Treasury. (n.d.). Sanctions List Search. Retrieved March 25, 2024, from https://sanctionssearch.ofac.treas.gov/
[101] Van Wegberg, R., & Verburgh, T. (2018). Lost in the Dream? Measuring the effects of Operation Bayonet on vendors migrating to Dream Market. In WebSci'18: Evolution of the Darknet (pp. 1-5). Association for Computing Machinery (ACM).
[102] Wortley, R. (2001). A classification of techniques for controlling situational precipitators of crime. Security Journal, 14, 63-82.
[103] Wortley, R. (2016). Situational precipitators of crime. In Environmental criminology and crime analysis (pp. 81-105). Routledge.
[104] Yuste, J., & Pastrana, S. (2021). Avaddon ransomware: An in-depth analysis and decryption of infected systems. Computers & Security, 109, 102388.
[105] Wall, D. S. (2022). The transnational cybercrime extortion landscape and the pandemic: Changes in ransomware offender tactics, attack scalability and the organisation of offending. Special Issue 5 Eur. L. Enf't Rsch. Bull., 45.
[106] Winship, C., & Morgan, S. L. (1999). The estimation of causal effects from observational data. Annual review of sociology, 25(1), 659-706.
[107] Weimann, G. (2006). Virtual disputes: The use of the Internet for terrorist debates. Studies in conflict & terrorism, 29(7), 623-639.
[108] Woods, D. W., & Seymour, S. (2024). Evidence-based cybersecurity policy? A meta-review of security control effectiveness. Journal of Cyber Policy, 1-19.
[109] World Bank (2024). World Development Indicators. Retrieved from https://databank.worldbank.org/reports.aspx?source=2
[110] ZDNet (2021). Retrieved March 27, 2024, from https://www.zdnet.com/article/free-decrypter-released-for-avaddon-ransomware-victims-aaand-its-gone/
[111] ZDNet (2021). Retrieved March 27, 2024, from https://www.zdnet.com/article/doj-charges-and-sanctions-revil-leaders-behind-kaseya-attack-seizes-6-million-in-ransoms/
[112] ZDNet (2021). Retrieved March 27, 2024, from https://www.zdnet.com/article/blackmatter-ransomware-to-shut-down-affiliates-transferring-victims-to-lockbit/
[113] ZDNet (2021). Retrieved March 27, 2024, from https://www.zdnet.com/article/doj-charges-and-sanctions-revil-leaders-behind-kaseya-attack-seizes-6-million-in-ransoms/
[114] ZDNet (2022). Retrieved March 27, 2024, from https://www.zdnet.com/article/decryptor-for-maze-egregor-and-sekhmet-ransomware-strains-released/

APPENDIX A

This appendix provides detailed information about the ransomware strains, their interventions, and the frequency of ransomware incidents by country. The following tables summarize the key aspects of the dataset used in this study Table IX, X, and XI.

TABLE IX
LIST OF RANSOMWARE STRAINS AND INTERVENTIONS

ID	Strain	Event	Date intervention	Date last victim
1	AlphVM	Takedown, Decryptor	19/12/2023	01/03/2024
2	Darkside	Takedown	13/05/2021	13/05/2021
3	Egregor	Takedown	16/02/2021	10/02/2021
4	HiveLeaks	Takedown, Decryptor, Arrest	26/01/2023	26/01/2023
5	NetWalker	Takedown, Arrest	27/01/2021	27/01/2021
6	RagnarLocker	Takedown, Arrest	16/10/2023	11/10/2023
7	REvil	Takedown	21/10/2021	16/10/2021
8	Trigona	Takedown	21/10/2023	01/03/2024
9	LockBit 3.0	Takedown, Decryptor, Arrest	20/02/2024	01/03/2024
10	CL0P	Arrest	01/06/2021	26/02/2024
11	DoppelPaymer	Arrest	28/02/2023	17/09/2021
12	Egregor	Arrest	10/02/2021	10/02/2021
13	Grief	Arrest	28/02/2023	24/03/2022
14	LockBit 3.0	Arrest	15/06/2023	01/03/2024
15	REvil	Arrest	04/11/2021	16/10/2021
16	REvil	Arrest	14/01/2022	16/10/2021
17	Avaddon	Shutdown	11/06/2021	11/06/2021
18	BABUK	PublicInterview	26/08/2022	26/02/2021
19	BlackBasta	Decryptor	30/12/2023	01/03/2024
20	BlackMatter	Shutdown	01/11/2021	04/11/2021
21	Conti	InternalDispute	27/02/2022	22/06/2022
22	Darkside	Crypto	07/06/2021	13/05/2021
23	MAZE	Decryptor	09/02/2022	15/12/2020
24	Prometheus	Decryptor	01/08/2021	14/09/2021
25	Ragnarok	Shutdown	26/08/2021	26/08/2021
26	REvil	Decryptor	16/09/2021	16/10/2021
27	Avaddon	Decryptor	15/01/2021	11/06/2021
28	BABUK	Sanction	16/05/2023	26/02/2021
29	Conti	Sanction	09/02/2023	22/06/2022
30	Conti	Sanction	07/09/2023	22/06/2022
31	REvil	Sanction	08/11/2021	16/10/2021
32	Yanluowang	InternalDispute	31/10/2022	31/10/2022
33	File Leaks (SYNack)	Shutdown	15/08/2021	15/08/2021
34	AstroLocker	Shutdown	04/07/2022	09/06/2021
35	BlogXX	Sanction	23/01/2024	06/01/2023
36	Egregor	Decryptor	09/02/2022	10/02/2021
37	CL0P	Crypto	02/07/2022	01/03/2024

TABLE X
STRAIN REBRANDING

Initial Strain	**Rebrand strain 1.0**	**Rebrand strain 2.0**
Avaddon	NoEscape	
Cuba	IndustrialSpy	
Babuk	Payload.bin	
Conti	3AM, Akira, Blackbastsa, BlackByte, MountLocker, Karakurt	
	Royal	Blacksuit
	XingLocker	Quantum
Darkside	Blackmatter	Blackcat
Doppelpaymer	Grief	
Haron	Midas	
Hive	Hunters International	
Ransomhouse	8Base	
Lockbit1.0	Lockbit2.0	Lockbit3.0
Revil	LV	
Nefilim	Nokoyawa	
Prometheus	Spook	
Maze	Suncrypt, Egregor	
Vice Society	Rhysida	

TABLE XI
SUMMARY OF COUNTRY FREQUENCIES FOR RANSOMWARE VICTIMS

ID	Country	Freq	ID	Country	Freq	ID	Country	Freq
1	United States	5783	54	Hungary	14	107	Iran, Islamic Republic of	2
2	United Kingdom	696	55	Puerto Rico	14	108	Isle of Man	2
3	Canada	608	56	Venezuela	14	109	Madagascar	2
4	Germany	508	57	Dominican Republic	13	110	Maldives	2
5	France	494	58	Ecuador	13	111	Monaco	2
6	Italy	416	59	Finland	13	112	Myanmar	2
7	Spain	260	60	Guatemala	13	113	North Macedonia	2
8	Australia	255	61	Kenya	12	114	Saint Kitts and Nevis	2
9	Brazil	224	62	Angola	10	115	Seychelles	2
10	India	168	63	Jamaica	10	116	Ukraine	2
11	Switzerland	141	64	Morocco	10	117	Virgin Islands, U.S.	2
12	Unknown	137	65	Pakistan	10	118	Zimbabwe	2
13	Netherlands	130	66	Panama	10	119	Antigua and Barbuda	1
14	Mexico	117	67	Slovakia	10	120	Belize	1
15	Belgium	109	68	Bangladesh	9	121	Bermuda	1
16	Japan	104	69	Croatia	8	122	Brunei	1
17	Thailand	91	70	Cyprus	8	123	Burkina Faso	1
18	Austria	88	71	Nigeria	8	124	Cayman Islands	1
19	Taiwan	86	72	Trinidad and Tobago	8	125	Curacao	1
20	China	85	73	Uruguay	8	126	Democratic Republic of the Congo	1
21	United Arab Emirates	79	74	Iran	7	127	Ethiopia	1
22	South Africa	73	75	Oman	7	128	French Guiana	1
23	Argentina	70	76	Tunisia	7	129	Gambia	1
24	Israel	70	77	Jordan	6	130	Ghana	1
25	Sweden	69	78	Lithuania	6	131	Gibraltar	1
26	Hong Kong	65	79	Serbia	6	132	Greenland	1
27	Singapore	63	80	Sri Lanka	6	133	Guernsey	1
28	Turkey	62	81	Bahrain	5	134	Guyana	1
29	Indonesia	58	82	Namibia	5	135	Honduras	1
30	Portugal	54	83	Nicaragua	5	136	Iceland	1
31	Colombia	51	84	Senegal	5	137	Iraq	1
32	Malaysia	47	85	Bahamas	4	138	Jersey	1
33	Poland	38	86	Barbados	4	139	Kazakhstan	1
34	Philippines	37	87	Bolivia, Plurinational State of	4	140	Libya	1
35	Denmark	36	88	Bosnia and Herzegovina	4	141	Liechtenstein	1
36	Peru	35	89	Botswana	4	142	Macedonia, Republic of	1
37	Chile	33	90	Estonia	4	143	Mali	1
38	New Zealand	33	91	Slovenia	4	144	Malta	1
39	Saudi Arabia	32	92	Tanzania	4	145	Moldova	1
40	South Korea	32	93	Algeria	3	146	Mongolia	1
41	Czech Republic	31	94	Cameroon	3	147	Montenegro	1
42	Vietnam	30	95	Cuba	3	148	Palestine	1
43	Egypt	27	96	El Salvador	3	149	Papua New Guinea	1
44	Ireland	27	97	Fiji	3	150	Russia	1
45	Norway	27	98	Haiti	3	151	Sint Maarten	1
46	Romania	27	99	Ivory Coast	3	152	Syria	1
47	Bulgaria	23	100	Latvia	3	153	Tonga	1
48	Greece	23	101	Mauritius	3	154	Uzbekistan	1
49	Kuwait	18	102	Paraguay	3	155	Vanuatu	1
50	Luxembourg	18	103	Uganda	3	156	Virgin Islands, British	1
51	Costa Rica	16	104	Albania	2	157	Zambia	1
52	Lebanon	16	105	Czechia	2			
53	Qatar	16	106	Gabon	2			