

# Ransomware attacks on organizations and companies in the Netherlands

Management summary (EN)

dr. Tessel Blom, ir. Wazir Sahebali, Kimberly Deppe MSc,  
ing. Peter Romijn, Floris Donath, ir. ing. Reg Brennenraedts MBA

**Commisioned by:**  
Wetenschappelijk Onderzoek-  
en Documentatiecentrum  
(WODC)

**Publicationnumber:**  
2022.173-2319-MSEN

**Date:**  
Utrecht, 1-8-2023





# Management summary

## Introduction

Commissioned by the Research and Documentation Centre (in Dutch: Wetenschappelijk Onderzoek- en Documentatiecentrum - WODC), Dialogic conducted a study on ransomware attacks on organizations and companies in the Netherlands. The WODC is looking for indicators that can give insight into the extent and nature of ransomware attacks. Based on these indicators, an image must be formed of ransomware attacks in the years 2020, 2021 and 2022. In addition the limitations of these indicators and data sources should be examined. The study answers the following research questions:

1. Which **indicators** can be used to gain insight into the extent to which ransomware attacks on organizations and companies in the Netherlands occur and the nature and consequences of these attacks with regard to the characteristics of the affected organizations and companies, the response to the attacks, the damage suffered and other consequences?
2. Do **existing data sources** contain information that provide insight into the relevant indicators?
3. Based on existing data sources, **what image can be formed for the years 2020, 2021 and 2022** about the extent to which ransomware attacks on organizations and companies in the Netherlands occur and the nature and consequences of these attacks in terms of the characteristics of the organizations and companies involved, the response to the attacks, the damage suffered and other consequences?
4. What **limitations** do existing data sources have with regard to the availability, completeness and quality of information and to what extent are there other limitations?
5. How can these limitations be **reduced or removed**?

Various methods were used to conduct this research: literature review, interviews, analysis of police report data<sup>1</sup> and web scraping.

## Part 1: Theoretical background

### The indicators of ransomware

In many cases, data sources will only be able to provide insight into a certain aspect of a ransomware attack. The indicators, which were chosen based on literature research and interviews, are:

- **Generic characteristics of a ransomware attack.** This indicator covers the attacker, the target, the initial access and the actions used to pressure the victim.
- **Victim characteristics.** This indicator specifically covers the characteristics of the victim, such as the sector, the size or the location of the organization.
- **Impact of a ransomware attack.** This indicator provides insight into the consequences of a ransomware attack for the individual organization and for society.

---

<sup>1</sup> Data obtained within Tom Meurs' PhD research on the nature and extent of ransomware in the Netherlands.

- **Frequency of ransomware attacks.** This indicator states how often certain ransomware attacks on certain victims with a certain impact occur.

## The steps in a ransomware attack

Most data sources only give insight into a particular step of a ransomware attack. With that they only contain information about a certain group of victims. With each successive step in a ransomware attack, this group of victims becomes smaller. In this study, we refer to different groups of victims as *subsets*.

## Part 2: Data sources

In this study the data sources below were analyzed. Each data source has information about a subset of victims and a limited number of indicators:

1. **Antivirus providers** often have detection mechanisms for ransomware and have information about the number of ransomware attempts.
2. **IT service providers** have information about suspicious activities of the cybercriminal once it has penetrated the IT system(s).
3. **Incident response companies** can be hired by the victim to coordinate the response to the ransomware attack.
4. **Cybersecurity insurers** are informed of a ransomware attack by the victim (if it is insured for ransomware) and are involved in the aftermath.
5. **Police reports.** Victims of ransomware can report this to the police but are not obliged to do so.
6. As part of the **CBS Cybersecuritymonitor** CBS sends a survey to a sample of Dutch organization asking whether they have had a ransomware attack in the last year and what the impact of that attack has been.
7. The **media** report on certain ransomware attacks. In doing so they also have an influence on the impact of ransomware on society. On top of that the media play an important role when it comes to raising awareness of ransomware.
8. On the **websites of ransomware groups** they threaten to publish stolen data and publish this data if the requested ransom is not paid.
9. The **Dutch Data Protection Authority (Autoriteit Persoonsgegevens - AP)** has information about reported data leaks. Victims of ransomware must report to the AP if they suspect a data breach.
10. The **cryptocurrency payment traffic** contains ransom payments to ransomware groups.
11. **No More Ransom** offers decryptors for certain ransomware software that can decrypt encrypted files.

## The ransomware image for 2020, 2021 and 2022

Existing data sources do not provide a uniform image of ransomware attacks on Dutch organizations and institutions for the years 2020, 2021 and 2022. Many data sources are too generic, which makes it for example impossible to extract specific information about the Netherlands, or they do not contain information about the full period 2020, 2021 and 2022. In addition, certain parties have commercial interests or limit the amount of information that they make public. Nevertheless we try to form an image for each indicator below.

## **Generic characteristics of ransomware attacks**

*Attacker:* The cryptocurrency payment traffic shows that the market share of various ransomware groups fluctuates strongly for the years 2020, 2021 and 2022. Arresting and dismantling a certain ransomware group often leads to the creation of new groups with new software. This diversity of ransomware groups is also apparent in reports by antivirus providers, which say that many different ransomware strains are detected. Analyses of the websites of ransomware groups show that the LockBit group is responsible for most data breaches at Dutch organizations in 2021 and 2022.

*Target:* Antivirus providers show that there is a worldwide increase of targeted ransomware attacks in 2021. These antivirus providers also show that consumers were the most affected by the rise of Ransomware-as-a-Service and that large companies and SMEs were less affected by it.

*Initial access:* Both IT service providers and incident response companies say that, for the years 2020, 2021 and 2022, email was the most used method for initial access (*phishing*), followed by desktop sharing software.

*Actions to exert pressure:* There is no data source that provides insight into the relative use of different actions that can be used to pressure ransomware victims (locking, encryption, data exfiltration). Interview respondents stated that data exfiltration is becoming more common (often even without encryption of the files), while the locking of IT-systems is happening less these days.

## **Victim characteristics**

*Location:* Analyses of the websites where ransomware groups publish their victims show that the Netherlands is 12<sup>th</sup> on the list of countries with most published organizations in 2021 and 2022. American organizations are published most frequent. IT service providers also claim that most ransomware victims are located in the United States.

*Sector:* According to incident response companies, the industrial and financial sectors are globally most affected by ransomware. The CBS Cybersecuritymonitor also shows that in the Netherlands the manufacturing and financial services sectors are targeted most by ransomware. Most police reports of ransomware come from the trade sector. These data sources categorize organizations into sectors differently, but all point towards organizations operating in the industry sector as most likely victims of ransomware. Compared to 2020 there was a 200% increase in police reports from the IT sector. This increase in attacks was also noticed by the Dutch Data Protection Authority, who specifically highlighted the attacks on IT suppliers in their report of 2021.

*Size:* The CBS Cybersecuritymonitor shows that the larger the organization is (measured by the amount of employees), the greater the chance is that the organization has had to deal with a ransomware attack. The Dutch Data Protection Authority also says that in 2020 it mainly received reports of data leaks from larger organizations that possess a lot of personal data. Members of the Dutch Association of Insurers on the other hand indicate that they in particular see smaller SMEs become victims of ransomware due to their dependence on a single system and low awareness.

## **Impact of ransomware attacks**

*Ransom:* Incident response companies indicate that the amount of attacks in which ransom is paid has been strongly decreasing relatively across the period of 2020, 2021, 2022. The cryptocurrency payment traffic also shows that there has been a turnaround in 2022, compared to 2020 and 2021, where all victims combined are paying much less ransom.

Furthermore, in the period from June 2022 to June 2023, 32% of the published organizations were removed from LockBit's website. Organizations are often removed from the website after paying a ransom. This implies that about a third of the LockBit victims that have been published still paid ransom. Among these victims that paid there was only one Dutch organization. The decrease in the willingness to pay for that period is offset by an increase in the average ransom that is paid. Police reports show that the ransom that is demanded by the criminals from Dutch victims in the trade and IT sector averages to more than one million euros. Small companies pay a larger percentage of their total turnover as ransom than larger companies (CBS Cybersecurity Monitor).

*Costs:* In addition to paying a ransom, ransomware attacks can also incur other costs, such as the disruption of business continuity, the loss of customers due to reputational damage, the recovery of the IT systems or the hiring of an incident response company. Police reports nonetheless show that the ransom demand is in many cases disproportionately high and that the financial damage suffered by a ransomware attack often ends up lower.

### **Frequency of ransomware attacks**

According to reports from the insurers (based on surveys), 26% of Dutch companies was affected by ransomware in 2022. On the other hand, in 2021 and 2022 only 107 and 110 ransomware reports were filed by the police respectively. The police suspect that only 2% to 4% of victims report a ransomware attack. A low percentage of victims that seek help from the police also appears in the CBS Cybersecuritymonitor, where only 13% of organizations that were a victim of ransomware indicate that they have sought help from the police. Of all the organizations surveyed in the CBS Cybersecuritymonitor only 1% said they had a ransomware attack in 2021. Analysis of media coverage suggests that ransomware was a major theme in 2021 in particular, but less so in 2020 and 2022.

### **Limitations**

No data source in this research report is free of limitations. A first limitation is the availability of (relevant) data. A number of data sources (such as antivirus providers, IT service providers, incident response companies and cybersecurity insurers) have commercial interests. Partly for this reason they do not publish raw data, but only publish reports they have composed. These reports often contain figures and conclusions whose origins are difficult to trace, but which tell a story that underlines the necessity of these parties. Because it is also unclear on which data or customer segment the figures are based, the results from the various data sources cannot be combined. Furthermore there are parties such as the NCSC and the Dutch Data Protection Authority that do not currently share data (the AP, however, indicates that they are working on this). A second limitation, which applies to most data sources, is that the data sources are not specifically aimed at Dutch companies and organizations. Many data sources focus on North America or cover the whole world. The only data sources that specifically focus on the Netherlands are police reports, data breaches reported to the Dutch Data Protection Authority and the results of the CBS Cybersecurity Monitor.

Moreover, no data source is complete. Earlier we discussed that data sources can only provide insight into a subset of victims, but they are often incomplete in that respect as well. For example, not all victims report a ransomware attack to the police nor do all victims of data exfiltration end up on the websites of ransomware groups.

Finally the quality of the data is in some cases insufficient for creating an image of ransomware attacks on Dutch companies and organizations. Surveying a sample of Dutch organizations about their experiences with ransomware should provide a good picture of the problem. However, the percentage varies greatly between the different surveys. Surveys by

banks and insurers seem to overestimate the frequency of ransomware, while the CBS Cybersecuritymonitor seems to underestimate it. The problem with the banks and insurers probably lies in the chosen sample (which contains a disproportionate number of victims), while the problem with the CBS Cybersecuritymonitor may lie in the way the questions are asked. Most results from the reports of commercial parties also do not meet the standards of reproducibility, so that the quality of the results cannot be determined.

## Recommendations

A central point of contact where various institutions can report their data (anonymized and/or aggregated), could remove some of the limitations of certain data sources (that currently only issue reports and do not share data). Incident response companies that have been approached and operate in the Netherlands say they report incidents to the NCSC. In addition, the Dutch Data Protection Authority has reports of data breaches and victims can indicate in the reporting process that it concerns a ransomware attack. Both the NCSC and the AP do not currently share this data (not even with each other). This central point could also request data about Dutch customers specifically from, for example, the antivirus companies and monitor the websites of ransomware groups for Dutch victims.

A preliminary study has already shown that the CBS Act provides the basis for mandatory data supply by government organizations to CBS. CBS could, at least for government organizations, act as a central point for depositing data about ransomware. This obligation does not apply to commercial parties, such as insurers, antivirus providers or IT service providers. The government should investigate under what conditions these parties are willing to share data about attacks on Dutch organizations.

Victims should also be encouraged to report the crime to the police. The information that comes from police reports is very rich, but unfortunately only a small percentage of victims file a report. Insurers could possibly play a role here by making a police report a condition for the payment of the damage (as is for example also the case for theft).

The CBS Cybersecuritymonitor could finally also be expanded and adapted. The questions, and in particular the examples given, are now very restrictive. They focus for example exclusively on locker ransomware (while that is rare at the moment) and do not ask about encryption of documents or data exfiltration. Some results also imply that the questionnaire was not completed by the right person within an organization. Asking about the knowledge level of the respondent would allow for a better interpretation of the results. A larger sample would also be desirable, so that all subcategories (different forms of ransomware, ransom amounts, whether or not the ransom was paid, costs incurred, but also the sector and size of the organization) are large enough. Ransomware victims may be more inclined to participate in a survey about ransomware, so it will not give a fully representative image of the frequency of ransomware in Dutch institutions, but it could give better insights into the proportions within the group of ransomware victims.

To form a reliable image based on existing data sources we make four concrete recommendations:

1. Investigate how barriers for sharing data about ransomware victims, such as privacy laws, can be removed (e.g. through anonymization or aggregation). Subsequently encourage data sharing by government organizations such as the NCSC, the Dutch Data Protection Authority and the police with a central point of contact such as the CBS. Article 33 of the CBS Act provides the legal basis for mandatory data sharing by government organizations to CBS. Combining (and if possible linking) data about

ransomware from (at least) the government organizations is an important first step towards forming an image of the ransomware problem.

2. The government should investigate under which conditions commercial parties such as antivirus providers, IT service providers and insurers are prepared to share data about attacks on Dutch organizations. Ideally this is done with the same central point of contact government organizations communicate with. These commercial parties possess information that government organizations cannot collect, but do not share this data and barely report on it. In addition, the reports are written with the interest of these commercial parties in mind and often tell a one-sided story that is aimed at attracting more customers.
3. Investigate how the willingness of victims to report a ransomware attack to the police can be increased. It could for example be investigated whether insurers can play a role in this by making a police report a condition for paying out the damage (as is also the case in for example theft). Police reports are a very rich source of information when it comes to the characteristics of the victim and the impact of the ransomware attack, but currently only a fraction of victims file a report. Overarching trends from the reports on the characteristics of attacks are furthermore used by the ransomware task force to detect and dismantle the criminal organizations.
4. Make better use of national surveys and monitors, such as the CBS Cybersecuritymonitor, by increasing the sample size and expanding and improving the questions related to ransomware. Surveying organizations nationwide is a good method for getting insight into the frequency of ransomware attacks, the characteristics of the attacks and victims, and the impact of ransomware attacks. The current results however suggest that the number of surveyed organizations that were actually victims of ransomware in the past year was very small. As a result it is not possible to form a reliable image of ransomware attacks on Dutch companies based on these results. When an organization is approached to complete the survey, and indicates that it has experienced a ransomware attack, the characteristics of the attack, the characteristics of the victim and the impact of the ransomware attack should be asked about in detail.