dialogic
innovatie • interactie

Radically Open Security

Exploratory study on risk factors for ransomware attacks

Management summary (EN)

Reg Brennenraedts MSc MBA, Tommy van der Vorst MSc, Jessica Kats MSc, Melanie Rieback PhD, Anouk Vos MSc, Nick Jelicic MSc, Roos Jansen MSc, Tessel Blom MSc, Nino van Sambeek

Commisioned by:
WODC

Publication number:
2021.148-2222-MSEN

Date:
Utrecht, 5 augustus 2022

Management summary

Introduction

Commissioned by the Research and Documentation Centre (in Dutch: Wetenschappelijk Onderzoek- en Documentatiecentrum - WODC), Dialogic conducted an exploratory study on risk factors for ransomware attacks. The objective of this research is to identify and quantify factors that influence ransomware attacks. A second objective is to provide insight into the potential for awareness among managers of medium-sized and small organizations, both in the public and private sectors. The study answers the following research questions:

1. What risks do ransomware attacks pose?
2. What do ransomware attacks look like today and what tools are used in the process?
3. What types of parties participate in these attacks?
4. What internal and external factors contribute to ransomware risk for an organization?
5. To what extent are these factors quantifiable?
6. What tool can be used to raise awareness of ransomware risks among decision makers in medium and small organizations?
7. What are key factors for companies and organizations to get started with the tool?

Various methods were used to conduct this research: literature review, exploration of existing risk assessment models, exploration of cybersecurity insurance, interviews, case studies affected organizations in the Netherlands and validation sessions. This study attempts to outline the most current situation of the issues at hand.

Impact of ransomware attacks

The first research question is: *What risks do ransomware attacks pose?*

The risk of a cyber attack is high and growing. Ransomware is a specific cyber attack. In it, criminals usually focus on encrypting the victim's data and, to a lesser extent, preventing the victim from accessing their own systems. The core of ransomware is that the victim is pressured by the perpetrator (typically: because of the encryption of data) to do something against his or her will. Usually this is paying a ransom (ransom). There are four forms of attack. With single extortion, files are encrypted, and victims are extorted by the threat of losing access to these files. In the case of double extortion, in addition to encryption, the data is stolen and there is a threat to make it public. In triple extortion, other cyber attacks, such as DDoS attacks, are additionally performed on the systems of the victim to make the recovery process more complex. Finally, in quadruple extortion, the victim's associates are also extorted into disclosing their data.

The impact that such attacks can have on organizations consists of the following aspects: (1) Additional costs for response capacity, (2) Costs due to loss of data, (3) Costs due to disclosure of data. This third point breaks down into costs due to reputational damage, fines, for example because of the General Data Protection Regulation and damages. (4) Ransom payment, (5) Costs due to disruption of business continuity and (6) Systems recovery costs. The average ransom payment is difficult to determine exactly but is between $50,000 and $500,000. Estimating the cost of business continuity disruption is even trickier but often appears to be a multiple of the ransom payments. Of the other items, it is difficult to interpret this quantitatively and varies from case to case.

Finally, there are also social effects of ransomware attacks. Because of dependencies between organizations, the disruption of the business continuity of an attacked organization can have a major impact on other actors in the value chain, such as customers and suppliers. The superlative of this is, of course, attacks on vital sectors, because of which large parts of the economy will be indirectly affected. Moreover, because there are links between the ICT systems of different organizations, perpetrators can also jump between organizations. A final social effect is a decrease in trust in the democratic rule of law because criminals are not (or cannot be) prosecuted.

Design of ransomware attacks

The second research question reads: *What do ransomware attacks look like today and which tools are used in the process?*

A ransomware attack consists of various steps in which different tools are used for each step.

1. **Initial access**. The attacker gains initial access ("foothold") with the victim, often an account of an employee of an organization within a specific application or on a specific server. This is done by using tools that automatically scan for weaknesses in systems. (Spear) phishing is also widely used.
2. **Consolidate access and position**. Once the attacker has an entry point, it will try to expand access to the victim's systems. For example, the attacker will look for systems with valuable information and try to gain access to accounts with more rights on these systems. This step requires a large amount of (non-automated) 'manual work' and involves the use of various tools and software.
3. **Data exfiltration**. In some ransomware attacks, data is stolen from the victim, after which the attacker uses the threat of reselling or publishing the data as a means of extortion. Exfiltration involves not only looking at files located on an organization's own server, but, but often using cloud services (such as Dropbox and OneDrive), web-based services (such as Mega and WeTransfer) and even systems deployed by the victim to make their own backups.
4. **Ransomware deployment**. The first two steps were generic steps used in many different cyber attacks. In this step, the attacker makes the choice to deploy ransomware to quickly monetize their position in victims' systems. The ransomware software performs the actual "holding hostage" of files. The goal of this step is to encrypt a large amount of an organization's (preferably valuable) files with a key that only the attacker has access to.
5. **Extortion and cash out**. In this phase, the attacker communicates with the victim and communicates what the victim must do to stop the attack and recover the data or stop it from being published.

A ransomware attack can be either targeted or untargeted. In an untargeted attack, the attacker does not care which organization or person becomes the victim. With a targeted attack, an attacker has a priori a specific organization in his sights. Nowadays, it is mainly "semi-directed" attacks on organizations. After the first step (initial access) it is determined which access data is interesting enough to proceed to the next step. This process repeats itself in the following steps.

Actors involved in ransomware attacks

The third research question is as follows: *What types of actors participate in these attacks?*

The first ransomware attacks were perpetrated by individual criminals, but by now there is a perfectly functioning supply chain of several types of actors with a high degree of

specialization. The ransomware ecosystem operates as if it were a legitimate, well-developed service industry. For example, initial access to networks is often sold through platforms to the highest bidder. There are several types of parties trying to gain this access in diverse ways. The buyers of the initial access in turn work this out, consolidate this position, and again sell this position to the highest bidder. The actual ransomware attack only comes in the phase after. The parties that develop and manage ransomware software are not always the parties that use it. Often affiliates are used to conduct the attack. There are also data managers who analyze, sell and/or make public stolen data. In the ultimate step (extortion and cash out), a wide range of parties are involved: negotiators, helpdesks, money launderers, et cetera.

By far the most common motive for ransomware attacks is financial gain. Activism occurs only sporadically. Ransomware criminals behave to some extent as rational actors: the costs, revenues, and chances of being caught are carefully weighed up. Perpetrators seem to come often from countries that were formerly part of the Soviet Union. In some cases, perpetrators deliberately do not attack certain types of organizations. Examples include organizations from countries in the former Soviet Union and the healthcare sector during the Corona crisis.

Risk factors for ransomware attacks.

The fourth and fifth research questions are: *What internal and external factors contribute to ransomware risk for an organization? To what extent are these factors quantifiable?*

Internal factors involve aspects over which the possible victim has control. To examine internal factors, we looked at literature, risk assessment tools, and cybersecurity insurance policies. By counting how often factors appear in these various sources, the size of this risk factor was quantified. The table below shows the ten internal factors most often named in these three sources ranked by size of risk factor. A generic internal risk factor that overlays the factors listed below is not having a complete overview of what systems are being used. The results were verified with interviews. The

1. Not having a good backup | phase: recovery
2. Inadequate training employees on phishing, scams, etc. | phase: prevention
3. Software is not up to date | phase: prevention
4. Not having an incident response plan | phase: recovery
5. Inadequate use of (up to date) anti-malware solutions | phase: prevention
6. Insufficient privileged access strategy | phase: limiting
7. Insufficiently secured accounts | phase: prevention
8. Insufficient continuous monitoring | phase: limiting
9. Insufficient network segmentation | phase: limiting
10. Insufficient email security | phase: prevention

In addition to the above list, there is a large series of other factors that are mentioned less frequently. These are mostly technical measures to prevent infections from occurring.

External factors are those over which the possible victim has no or limited control. In line with the various types of impact that attacks have on organizations, the following aspects increase the expected profit for perpetrators (and thus the risk for victims) (1) having a higher turnover, (2) the use of IT systems whose failure could disrupt business continuity, (3) the storage of personal data. There is some debate among experts if having a history of paying ransoms also increases the risks of being attacked again. The following two aspects reduce the cost to the perpetrator: the low probability of being caught and not being too much on the radar.

Policy options to reduce risk

The sixth and seven research questions are: *What tool can be used to raise awareness of the risks of ransomware among managers in medium-sized and small organizations, and (How) can the captured factors be used in this tool?*

Our analysis suggests that an awareness campaign for managers of medium-sized and small organizations is likely to be an efficient and effective tool for reducing the likelihood and impact of ransomware attacks. Currently, both the risk and impact of these attacks are underestimated by the management of these organizations. ICT practitioners are much more aware of this, but this is not sufficiently conveyed to the management of these organizations. Because large organizations often are more developed in this area (and because they have a specific context), it is logical to focus on medium-sized and small organizations. A good campaign should include the following elements:

- The campaign should include confrontational facts, such as the average harm experienced by victims.
- Managers should be encouraged to reflect on their own situation. This can be done by asking them what the impact on their organization is if (1) all data becomes public or (2) ICT cannot be used for three weeks or (3) ransom must be paid equal to 5 percent of the annual turnover.
- The campaign must include concrete actions by making it clear how and what cybersecurity level an organization must obtained to be properly protected against ransomware attacks. The internal risk factors fit in well with this.
- The content of the campaign must therefore be actively promoted, and managers must receive a personally targeted message. Various channels are possible for this, but it seems sensible to connect with known relations of the manager so that a reliable and known source is used.
- Due to the high degree of heterogeneity of this target group, a sectoral approach seems obvious. In combination with the previous point, branch and sector organizations could play a significant role.
- Finally, presenting a social norm can be a powerful tool. Managers must get the feeling that similar organizations are also taking steps to protect themselves against ransomware.

There are, of course, other ways to achieve behavior change and awareness. For example, a certain level of cybersecurity could be enforced by customers, suppliers, insurers or even the government. This could apply to both ICT service providers and mainstream organizations.