XOPERO
Backup&Recovery

RANSOMWARE

Defense e-book

Table of contents

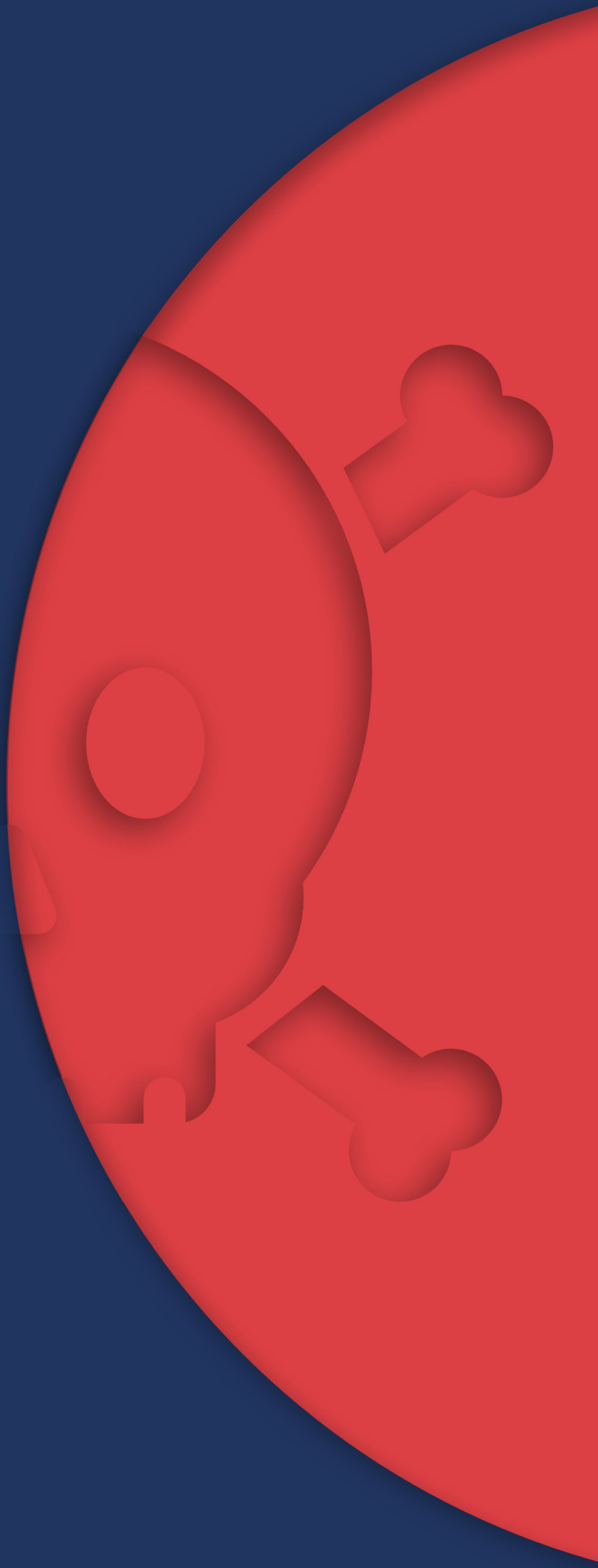
Do you know that…

every 11 seconds
there are ransomware attack attempts

92% of those
who paid ransom failed to get all their data back

1,85 mln USD
is the average cost of recovery from the ransomware attack

22 days
is the average downtime period due to a ransomware attack



How does ransomware attack occur? Why should we be wary of it?

Introduction

Let’s start with this short definition...

Ransomware is a type of software, but also a technique of attack, which blocks access to any data or the whole computer system. Ransomware’s goal is to force the person whose computer was attacked to pay ransom in exchange for unblocking or decrypting their data.

Today, it is one of the greatest threats which awaits users and businesses online. It is estimated that in 2023, a ransomware attack occurs on average every 11 seconds! Moreover, if you spend at least an hour on reading this document, criminals will have managed to attack over 327 enterprises!

Ransomware is a type of software that is constantly evolving. Hackers are modifying malicious code all the time, reaching for ever more perfect encryption mechanisms and attack methods. A (temporary) victory in dealing with hacker attacks does not mean that you can allow yourself a break in improving security systems.

98%

In the vast majority of attacks, the criminals are still demanding ransom payment in Bitcoins.

Ransomware evolution

AIDS - the birth of a monster

Let’s go back to year 1989. It is then, that the trojan horse AIDS was created. It differed from other threats, especially by encrypting the name of the files and changing their location on the device’s hard drive. After the 90th restart of the system, the program displayed a message about the need to connect the printer, which then printed...the ransom demand. The alleged „license renewal” was valued at 189 $. The method of spreading the virus was interesting as well - AIDS was spreading through 5,25 inch floppy disks.

Anonymous transactions

Right now, were are in the 90’s. David Chaum creates DigiCash, which revolutionizes online payments in those times. Thanks to this new technology, payment transactions have the chance to become much safer, since it’s not possible to determine the source of those operations. For the exact same reasons it became the perfect tool for anonymous exchange of ransom money for data access.

Asymmetric encryption

Public key cryptography undoubtedly played an important role in the data theft evolution. Asymmetric encryption method requires at least two keys, which are mathematically related. One of those keys is used for data encryption, while the other is used to decrypt data. In the case of AIDS trojan horse, data was encrypted with the same key which was also used to decrypt data. All that needed to be done, was to pull out the key from the virus’s files, which then enabled decryption of that data. Nowadays, decryption keys are in the hands of the criminals. Ransomware Petya used randomly generated keys. It’s also worth remembering, that the keys given by the criminals don’t guarantee that it will be possible to decrypt all data. There are cases where such keys destroyed data instead of deciphering them.

RSA keys

In 2005 ransomware started to use RSA keys -which were longer, and therefore much more difficult to crack. Gpcode.AK. used the key with as many as 1024 characters. Interesting fact: the longest RSA key which was cracked had 768 characters.

Finally home...

We are in the year 2013 - CryptoLocker demands ransom in Bitcoins. In addition it uses both symmetrical and asymmetric encryption. Despite the short time of its presence - from October to December 2013 - it generates huge profits to its creators. It is estimated that they collected as much as 27 million dollars.

Types of ransomware

Ransomware and its creators have just one goal - money. The user - the "hacker's target," is increasingly aware of the techniques used, and antivirus software producers are getting better and better at detecting threats.

Cybercriminals are therefore developing more and more new attack techniques to achieve success. Let's look at the most common types of „worms" we can get online...

Crypto-malware
Most popular type of ransomware. It encrypts the data on the infected device and displays a ransom demand. The user is still able to use the device, but he loses access to any of the data collected on that device. Crypto-malware can spread and attack data that is saved in other locations than the attacked device, such as servers or cloud storage. The average ransom payment varies in the range of $320,000.

Locker (blocking software)
This type of software completely blocks any access to the computer, even signing in to the user's account. Petya and their derivatives block computer access by encrypting the master file table on the hard drive. In some cases, general technical knowledge allows one to deal with this sort of threat and restore access.

Scareware
Scareware is known for displaying false messages - including messages which aim to intimidate users and induce them into paying the ransom. A window with the message that flash plug-in needs an update, information about detecting illegal versions of the system by the police... This is exactly how scareware works.

Leakware (Doxware)
Ransoc is just one example of doxware. Its goal, however, is not only the files but a victim's reputation. After the device is infected, it is scanned for any information which can turn out to be troublesome for the user in case this information is revealed. Doxware also searches for some information about the victim on social networks. Based on this information, the profile of the „guilty" is created, including the victim's photo and IP. Moreover, the programme blocks the victim's screen with the „personalized" ransom demand.

Ransomware + Leakware = Double Extortion
A new double extortion technique involves a combination of ransomware and leakware attacks. Criminals steal sensitive information before encrypting the victim's data and then threaten to make it public. This double extortion card increases the likelihood that the victim will comply with the demands.

"

Poland is considered to be one of the most targeted European countries by hackers. There are up to **2,000 attacks per week**.

It is estimated that by 2025. cyberattacks will cost companies annually

10 trillion dollar

Ransomware-as-a-Service, a successful business model

Software-as-a-service is undeniably one of the most popular business models of recent years. This has not escaped the notice of cyber criminals, who put their "products" up for sale on illegal forums using this very model. Hence the name Crimeware-as-a-Service - and its variations: Malware-as-a-Service, Ransomware-as-a-Service, and Phishing-as-a-Service are all services under this model which can be purchased by anyone and for less than $50!

RaaS has become increasingly popular in recent years because it allows cybercriminals to scale up their operations and target a wider range of victims. It also makes it more difficult for law enforcement to track down the perpetrators, as the RaaS provider is frequently located in a different country from the troops executing the attacks.

> **$50 - that's all it takes to become a cybercriminal.**

nearly 60%

of all attacks were carried out by RaaS.

Attack vectors

But the hacker does not live on ransomware alone...

Cybercriminals have a lot more tools at their disposal. Let's take a look at the next few.

Backdoor

The Backdoor is a loophole in the building of the operating system, which weakens the defense mechanism. Created intentionally, usually with the help of another loophole or an installed trojan horse. It provides almost unlimited access to the victim’s computer.

Botnet

That’s what we call a network consisting of infected computers. The devices are used to send out spam and viruses for stealing data or executing DDoS attacks.

by 2031

a ransomware attack will probably occur every 2 seconds.

Downloader

This is a programme that is used for downloading other harmful programmes. After the device is taken over by a hacker, it is usually the first one to get on the hard drive of the victim.

Keylogger

This programme registers everything, that the user writes on his keyboard. That means that the keylogger will save the sequence of pressed buttons while logging in to Internet banking services.

Launcher

That is nothing else than an extra programme, which masks the actions of malware. The programme is able to not only mislead the user but also the operating system.

Rootkit

It allows the hacker to gain administrator access to the infected system. Rootkits are not able to spread on their own. They are components of other malicious software. If the antivirus finds such programmes in the system, it means that other dangerous apps has already infected the computer.

Worms

Those programs are able to replicate and spread on their own by using a computer network. What gives them away? They use a lot of memory, and overload network bandwidth, and the device as well. Your computer doesn’t follow your commands? Perhaps it's high time to scan it for viruses!

Trojan

It's a type of virus that pretends to be a useful programme, while in reality, it steals data and damages the computer. Trojan horses are usually concealed in free games, apps, as well as pirate movies. After being infected, the computer starts working slower - mostly because the processor is overloaded.

Virus

Software, or just a piece of malicious code which imperceptibly infects the victim's computer. Viruses are quite often concealed in games, PDF readers, or in attachments. What can reveal their presence in the system? Is your internet connection incredibly slow or doesn’t work at all? Has your antivirus stopped working? It's time to delete all temporary files and start an antivirus scan.

Phishing
the most popular attack vector

Phishing is one of the simplest attack vectors, yet still the most effective. Why? Hackers attack the weakest link in the security system, which is invariably humans. Lack of suspicion about the sender, clicking on links, opening attachments - but that's not allt. Cybercriminals are using more sophisticated social engineering techniques. For example, they can take control of legal sites and distribute malicious content through them, or entice users to provide information - such as credit card numbers.

64% of organizations

have experienced a phishing attack in the past year.

Most common email phishing attacks...

Spear phishing

The attacker uses already-acquired information about the victim, such as name, job title, or email address, to create a more credible phishing message that looks like it's coming from a trusted source.

Whaling phishing

This attack is similar to a spear phishing attack, though, in this case, the attacker targets high-profile individuals in the organization. The goal of this attack is to gain access to sensitive and business-critical data.

Clone phishing

The attacker creates copies of real e-mails and inserts malware or links. Recipients can easily fall victim to such an attack if they do not pay attention to small differences in the e-mail.

You receive 5 phishing messages a week

That's 20 emails every month and as many as 240 during the whole year

30% of emails

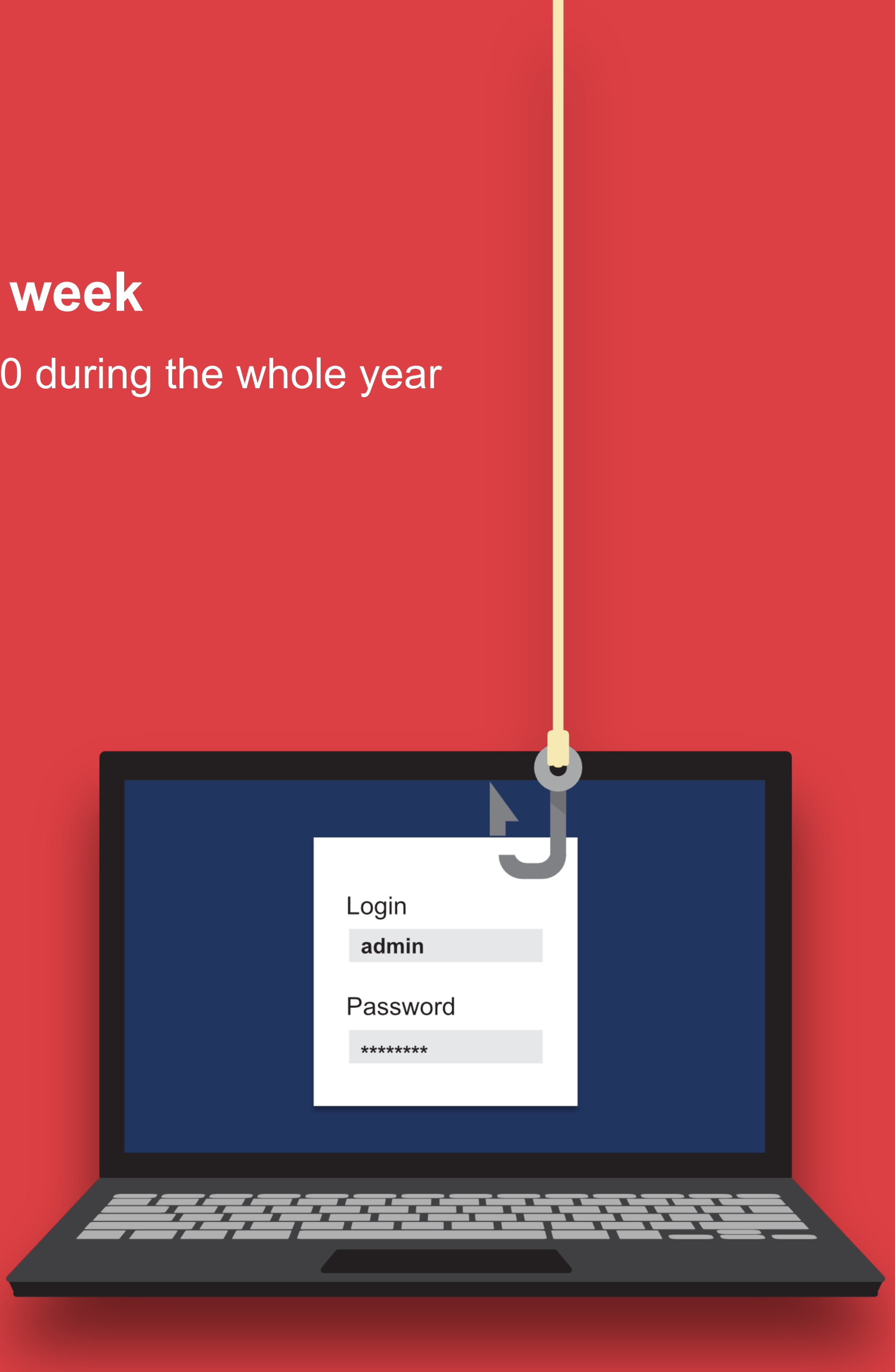
are passed through spam filters

2/3 of messages

contain malicious links

50% of emails

contain some form of malware



Three lines of defence

1

Prevention

It's important to realize what potential threats await us online and what steps should be taken to prevent them. Above all, we should be conscious when we receive to any unexpected messages with links and attachments which have unknown sources and treat them as a potential threat. You haven't bought anything online? Then the link to trace the package is probably fake. Take a look at the email address of the sender more precisely, the footer, title, and the content of the message. Compare this email with other real emails you have received from the courier or the store. Can you see the difference between them? Exactly. It would be better to delete this message. Obviously, any attachments you received via social media, online messengers, or SMS should also be deleted.

It is also essential to properly assign permissions to resources in a company's network. Granting full access to all managers in a company is a common mistake. Statistics show that it is mostly the management that falls prey pray to personalized attacks.

2

Antivirus

A moment of inattention can happen to anyone - that's true. That is why it is so important to have trusty antivirus software. This way, dangerous files can be eliminated before making any damage to the system.

However, if the antivirus fails and the attack will happen, turning off the computer should be a priority. In some cases, malicious software displays the information about infecting the computer first and begins data encryption later. Ransomware is also not able to download encryption keys and additional components such as cryptominer from the C&C server.

3

Backup

The most effective way to regain control over the infected computer is to format the hard drive and use the third line of defense against ransomware... And the one we had in mind is obviously a backup solution and disaster recovery.

It allows fast data recovery from any moment, which prevents downtime and ensures business continuity. According to studies, every single dollar spent by a company on a backup system saves them $4 when the company experiences a cyberattack or data loss. What is more, about 93% of the companies which backed up their data are able to restore their data within a short period of time.

Backup allows the company not only to restore data from before the attack in a fast and swift manner but also gives a 100% guarantee that the data will be recovered. If you decide to pay a ransom, the only guarantee is a word of... criminals.

"

> **We do not know a way which would give us a 100% guarantee that we are safe from ransomware, mostly because ransomware is constantly evolving. For that reason, a good backup serves as a lifeline in case we lose our data.**
>
> - Grzegorz Bąk, Chief of R&D, Xopero Software S.A.

TOP 10 SECURITY TIPS for ransomware prevention

1. Do not pay the ransom. You don't have any guarantee that you will get your data back.
2. Back up your data regularly. It's best to set up automatic backups.
3. Create an HDD image backup - then you can launch the image as a virtual machine and get back to work fast.
4. Choose a reliable anti-virus and/or anti-malware solution.
5. Regularly update the operating system. Hackers love unpatched and vulnerable OS.
6. Be careful with emails and don't click on suspicious links or attachments.
7. Use the user's account on a daily basis (instead of the administrator’s account).
8. Assign permissions to resources on your corporate network with caution.
9. Disable remote desktop protocol. Unsecured RDP is one of the most favorite access points.
10. Do you suspect a ransomware attack? Disconnect your computer from the network immediately.

A backup plan
with XUP and Xopero ONE

Instant recovery for business continuity

93% of companies without a disaster recovery plan fail one year after data loss! Disaster recovery features allow you to quickly restore data from any point in time, avoiding downtime and ensuring business continuity. Backup not only allows you to quickly and efficiently get back to the moment before the attack but gives you a 100% guarantee of data recovery.

Avoidance of legal consequences

Having a backup is a requirement based on major regulations (including SOC 2 Type II and ISO 27001). Data loss can incur high costs due to RODO (especially if customer data is involved), and it can also damage companies reputation in the market, which will directly affect its customer trust.

Cost reduction

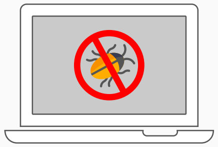
Even a relatively short outage can result in gigantic financial losses that will sink your business. Meanwhile, every $1 spent on a disaster recovery system saves companies $4 when a cyber attack occurs.

Monitoring

An advanced reporting system will allow you to ensure compliance with regulations, security standards, and the organization's internal processes - which will take some responsibility off your team in case of audits and inspections.

Do you know that

93% of business which don't have a DR plan
fails within the year since losing the data.



96% of companies which backed up their data,
restores it efficiently after the ransomware attack.

> 50% of companies after a failure
experience a downtime longer than 1 day.

Ransomware Protection with XUP and Xopero ONE

Immutable storage

Take advantage of WORM-compliant storage technology that writes each file only once and reads it many times. It prevents data from being modified or erased and makes it ransomware-proof.

Non-executable data in the copy

Xopero ONE compresses and encrypts the data and stores it in non-executable form in the storage. It means that even if ransomware will hit your files on the backup source, it will be impossible to execute these data in the storage.

Limited access to storage credentials

Authentication data of the backup storage is sent to the agent only while performing backup so there is no way for ransomware to access your storage even if the source machine is infected.

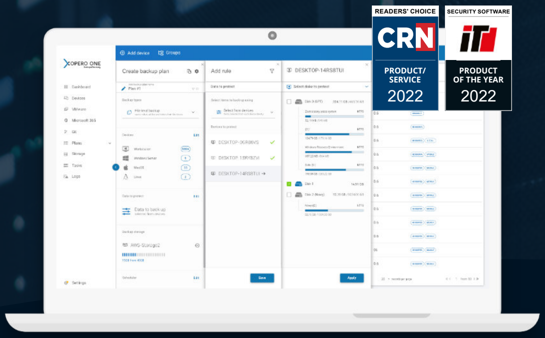
Multi-storage system and replication

In Xopero ONE you can add an unlimited number of data storages - cloud or local, and thanks to replication plans create native copies in different locations. Now you can easily implement the 3-2-1 backup rule, and in the event of a failure or attack on one of the storages, you can restore the copy from the next one.

$11.6k

that's the cost of downtime for Business per minute.

Choose a cutting-edge solution customized to your infrastructure



Xopero ONE Backup&Recovery

A comprehensive backup and recovery software designed for your compliance needs

Try for free

Xopero Unified Protection

ALL-in-ONE backup appliance - backup software, disk array, archiver, deduplication device

Find out more

Xopero protects all your data

Windows | LINUX | vmware | Microsoft Hyper-V | Red Hat | ORACLE

Microsoft SQL | MySQL | PostgreSQL | Microsoft 365 | iOS | and more!

XOPERO
Backup&Recovery