The Florida Bar Standing Committee on Technology

Ransomware Guide

By: John Giantsidis, JD, M.Eng.

Contents

Introduction

We are immersed in a technological evolution caused by the eruption of the Internet, the exponential growth of mobile devices, cloud services and, most recently, the Internet of Things (IoT). As expected, this evolution is not without risks, since the same advantages of immediacy, mobility, ubiquity, ease of payment, communication from which law firms, clients and users benefit, are also taken advantage of by those engaged in illegal criminal activities.

Among the malicious activities that provide cybercriminals with a quick economic benefit, a type of malware (malicious software) focused on extortion, called ransomware, stands out for its success. The objective of malware is to block access to the affected device or some of the information it contains and then ask for a ransom in exchange for unlocking it. This type of malware proliferation is related to advances in cryptography (encryption algorithms that allow access to information only to those who know the unlock key), the proliferation of devices connected to the Internet, as well as the increasingly widespread use of international payment systems with virtual currencies that allow anonymity, such as bitcoin. These circumstances allow cybercriminals to obtain a high economic return, by providing them not only with diversity and permeability of the targets for their attacks, but also a great facility to hide.

Ransomware affects any user, business, or activity by demanding the payment of a ransom in exchange for the return of access to their information. This malware is affecting home users, businesses, governments, and even critical services, such as hospitals or power plants. A ransomware attack can cause temporary or permanent loss of information and disrupt normal activity, causing economic or reputational losses and, in some cases, considerable damage to the population when attacks occur against the critical infrastructures of a country.

Ransomware affects all types of computers: desktops and laptops, web servers, file servers, other servers, and mobile devices. Currently, the take-off of the IoT and the increasing Internet connection of previously isolated industrial devices is leading to a new area of action for cybercriminals. These devices automate, for example, the lighting, heating, production chain of companies or the control of their vehicle fleet.

Cybercriminals take advantage of the vulnerabilities of these devices to, among other actions, infect them with ransomware, forcing companies and law firms to make the payment of a ransom to be able to recover access to them. In this guide I propose actions to recognize, prevent and mitigate this threat.

What is Ransomware

In general, ransomware is an evolving type of malware that prevents access to information of a device, threatening to destroy it or make it public if the victims do not agree to pay a ransom within a certain time period.

But let's have a closer look.

Ransomware spreads, like other types of malware, in multiple ways: through spam campaigns, vulnerabilities or software misconfigurations, updates of fake software, untrusted software download channels, and unofficial program activation tools (cracking). Cybercriminals try to get the user to open an infected attachment or click on a link that takes them to the attacker's website where they will be infected.

Currently, in addition to the blocking of information, cybercriminals threaten the leakage of confidential information to the public sphere (Internet) which could cause economic and reputational damages. The threat of publicity involved with more scandalous data breaches like the recent hack of OnlyFans often incentivizes these victims to pay more to cybercriminals than data breaches involving less sensitive data.

The Mechanics of a Ransomware Attack

When cybercriminals access protected data, they normally encrypt the data to make it inaccessible to the data controller. Then they send a ransom request to the victim through a message or pop-up window, performing what we would call a virtual kidnapping. This message, which is usually threatening and pressing, warns the victim that the only way by which they can decrypt their files, recover the system, or avoid an information filtering, is to make the payment of a ransom. Frequently, these ransomware demands include a time limit to pay and threaten destruction of the hijacked files, their publication, or an increase in the value of the ransom if it is not paid on time.

The ransom payment is often requested in the form of some cryptocurrency (virtual currency) such as bitcoin. Cybercriminals often involve intermediaries who transfer the ransom payments from these illegal activities to help them hide their trail. In exchange for payment, cybercriminals promise to facilitate the mechanism to unlock the computer or decrypt the files. However, there are no guarantees that once paid, the victim will be able to recover the information. So, it is strongly suggested not to pay the ransom to avoid the proliferation of these threats. Moreover, payments made to cybercriminals who have been specially designated on the US Office of Foreign Assets Control list could result in felony charges brought against the victim. Further, links provided by cybercriminals that enable victims to unlock access to the hostage data could also hold malware, cause another infection, and permit the theft of passwords and other sensitive information. For this reason, it is quite common for devices once infected by ransomware to also be infected with other types of malware.

Why do cybercriminals demand ransom payment in cryptocurrency?

Cryptocurrencies are virtual currencies that allow almost anonymous payment between individuals, these transactions difficult to track. Through the addition of mixers and tumblers that jumble otherwise traceable information attached to cryptocurrency transactions, cybercriminals can more easily hide their identity and the trail of transactions from law enforcement tools, making it easier to extort money from their victims without the police or FBI being able to immediately track them down.

How does ransomware infect devices?

As in the case of other types of malware, cybercriminals use one or more of these avenues to infect the victim:

- Malware developers have tools that allow them to recognize and take advantage of vulnerabilities (security holes) in computer software and related applications to introduce malware.
    - Some varieties of ransomware use outdated web servers as a gateway to install the ransomware.
    - They also take advantage of systems connected to the Internet without basic security measures. For example, there is more equipment for climate control, manufacturing components or other devices that were not connected to any computer network and are now connected to corporate networks or the Internet without the minimum-security measures.
- They obtain access credentials to computers with administrator privileges through deception (phishing and its variants), procedural weaknesses (i.e. failing to force changes to default usernames and passwords), software vulnerabilities or use of bad design practices such as hard-code passwords (which consists of embedding them in the source code of programs). With access to these accounts, they can install malware on these computers.
    - Many of the IoT devices that have recently connected to the Internet retain the same factory or default credentials for access and administration, are "hardcoded", or they simply lack access limits altogether.
- The most commonly used technique by cybercriminals involves social engineering. Using social engineering techniques, cybercriminals trick users into installing malware by sending a fake or phishing email with a link or an attachment that, when clicked or opened by the recipient, installs the malware. These tactics may also utilize messages sent through social media or instant messaging services.
- They use methods known as drive-by download and watering hole, directing victims to previously infected websites that install malware through browser vulnerabilities without notification to the victim. They also use malvertising techniques embed malicious ads on legitimate websites. When the user visits that ad website, which usually impersonates another legitimate one, they can be infected without needing to download any application. This technique is employed to install malware, which in turn can lead to a ransomware infection.
- They take advantage of services exposed to the Internet, such as remote desktop, which allow opening a door to an attack. If they do not have the necessary security measures deployed, these exposed services can be the origin of a security incident, such as a ransomware infection.

Types of ransomware

From minor to major importance, we can classify ransomware in general into:

- Hoax ransomware: only simulates encryption using social engineering techniques to extort money from the user, demanding payment for recovering their files or preventing them from being deleted. It is a type of simulated ransomware.
- Scareware: uses the lure of fake software or support. It appears in the form of an annoying pop-up advertisement that reports a virus infection and provides an easy and quick solution,

downloading a cleaning program that is almost always malware. The pop-up ad itself launched by the visited page does not usually pose a threat, although it is recommended not to click on its links and pay attention when closing the pop-up window, as it usually includes fake close buttons.

- Screen blockers: prevent the use of the device by showing a window that occupies the entire screen and does not allow it to be closed. In the window two types of messages can appear:
    - In some cases, the encryption of files and the procedure for recovering them is reported, but the files are intact. In this case, only one screen lock has occurred.
    - In other cases, a message from the security forces indicates that illegal activities have been detected and a penalty is requested to unlock the equipment (also known as like the police virus), but in no case does this message relate to state security forces.
- Encryption ransomware: considered the most dangerous of all. Its main goal is the encryption of information to demand a ransom. Cybercriminals make use of the latest advances in encryption information to prevent data from being decrypted. Within this variant there is a wiper call, which does not return access to the files, it simply deletes them.
- Doxware: uses a technique known as doxing, which consists of threatening the user with making the extracted personal data public. This technique causes an increase in pressure on the user, which translates into an increase in the effectiveness of the attack and the benefit for the cybercriminal.

Ransomware is a very lucrative criminal activity that affects all types of companies. Since its start, this type of malware has become increasingly sophisticated and destructive, evolving to evade detections by specialized applications. Some ransomware are associated with other types of malware that steal information (bank accounts, login credentials...), open back doors or install botnets. They are adapted even with rescue messages in the language of the victims. New variants for mobile, industrial and IoT devices also appear, and new forms of extortion, such as threats to disseminate the information obtained, previously mentioned as doxing. On the other hand, the emergence of cryptocurrencies and their "laundering" mechanisms guarantee an anonymous payment system for ransoms. Advances in the complexity of encryption algorithms allowed them to improve their extortion mechanism. Before, they only used programs that blocked the system; now, they can also encrypt the information that it found on the hard drives and other storage systems of its victims, making it more difficult to recover. This makes it possible to increase the value of the ransom. Some varieties encrypt, in addition to infected computers, attached storage devices, shared network storage devices that have partners or services in the cloud that are mapped to the infected computer.

How can you protect yourself?

To protect against ransomware, it is necessary to adopt a series of good practices and consider two main purposes: on one hand, to avoid falling victim to deception by knowing the most common social engineering techniques; and on the other hand, configure and maintain the systems avoiding that they are technically vulnerable. The following sections develop these good practices.

Awareness and training

Most ransomware infections are taking place through social engineering hoaxes, and 75% of the time they manage to successfully carry out the cyberattack. Users are tricked into performing a certain action of their interest, which will allow the cybercriminal to install malware with which they can infect the device. It is essential that we train and raise our employees' knowledge, teaching them to recognize these situations and how to act accordingly.

Users must know the company's policies on cybersecurity, such as those related to the permitted use of applications and devices, the use of public Wi-Fi, security in the workplace and mobility or the password policy.

How does a social engineering attack work?

Social engineering attacks are not much different from classic scams. The cybercriminal follows the same steps as the face-to-face scammer: recognition, establishment, contact and trust, and manipulation to obtain his goal and get away from the stage without raise suspicions.

The first step is to try to gather as much information as possible about the company that may be useful to them to know their victim, such as lists of employees and phones, departments, location, suppliers.

Cybercriminals will then select a target victim (usually an employee or some collaborator of the company) and will try to establish some relationship with the target that allows you to gain its trust, for which they will use information obtained from a service the target trusts: their bank, their computer maintenance company, a particular situation, etc.

Once they have earned their target’s trust, they manipulate the target (now victim) to get the data they need (credentials, confidential information, etc.) or get them to perform some action for the cybercriminal (install a program, send some emails, ...).

The techniques to gain trust and manipulate the victim are diverse:

- Respect for authority, when the attacker pretends to be a senior manager of the company or a member of the FBI;
- Desire to be useful, help or collaborate that is appreciated in business environments;
- Fear of losing something, as in messages asking to do an income to get a job, a reward, a prize, etc.
- Appeal to the ego of individuals by telling them that they have won a prize or have achieved something and that to obtain it they must perform an action that in another they wouldn't do it; and
- create emergency situations and achieve the objectives due to laziness, ignorance, or naivety of the victim.

Finally, after achieving their goal, cybercriminals must step aside without raising suspicion. Sometimes, they destroy the evidence that may link them to some later criminal activity that they execute with the information obtained (for example, unauthorized access if they obtain the credentials, publication of compromised information ...).

How to recognize a social engineering attack?

To avoid ransomware, or any similar type of attack carried out by social engineering, be wary of all messages received by email, SMS, instant messaging applications or social networks, in the one who is coerced or urged to act before a sanction.

As general guidelines, to avoid falling victim to ransomware-type fraud it is warned:

- Do not open emails from unknown users or that you have not requested, delete them directly. Do not reply in any case to these emails.
- Check the links before clicking even if they are from known contacts. Be wary of shortened links or use some service to expand them before visiting them.
- Be wary of attachments, even if they are from known contacts.
- Always have updated the operating system and antimalware software from official repositories. In the case of anti-malware software, also check that it is active.
- Ensure that your employees' user accounts use strong passwords and do not have more permissions than necessary to perform their work.
- Only install applications allowed and necessary for the work that comes from official sources.

Prevention

To avoid ransomware, we can adopt a series of technical measures so that our systems do not have security holes, keeping them updated and well configured.

First of all, we will have to adopt a good design of our network, for example, performing subnetting or network segmentation, to prevent us from exposing internal services to the outside and that the entire network can be compromised, so that it is more difficult for the cybercriminal to infect us in the event of an incident, display file extensions and train users in threat detection using this technique.

We must not forget either the installation and periodic update of specific software known as anti-ransomware, in addition to conventional antivirus and other antimalware tools. Finally, surveillance and audits will keep us alert to any suspicion

Backups

In case you are the object of a ransomware attack, the main security measure that will allow you to recover the activity of your law firm in a brief period, is to make a backup or backups.

Here are the basic recommendations for backups:

- Make and keep at least three up-to-date backups on different media. If you have suffered a ransomware attack you have three options: pay the ransom, recover the information from a backup or assume that you have lost your data. Of these three options, the best, without a doubt, is to recover your contents from a backup. And since backups can also fail, it is recommended to keep at least three copies up to always date, for example: specific hard drive for copies, external USB, and cloud.
- Saves backups in a different place than the file server because there are ransomware variants that encrypt information (including backup files) from hard drives or network storage systems other than the infected computer, ideally is to store them, whenever possible, on physical discs (DVD or Blu-Ray) or on external media not connected to our network).
- If you back it up and host it in the cloud (cloud backup), make sure it is synchronized continuously. Remember that some ransomware families they also encrypt and block cloud backups, so you may want to turn off persistent synchronization.
- Check regularly that the backups you have stored are working properly and you know the steps to recover them. Backups can also get corrupted. Therefore, it is necessary to periodically check that backup copy, for which you must try to restore some files from time to time. Finally, to avoid ransomware that threatens to leak your data, encrypt the most sensitive information so that, in case of theft of your files, cybercriminals cannot make the information public. Don't forget that you shouldn't save the encryption key on the same device, and if you use a certificate to decrypt it, save it to a USB stick and keep it disconnected from your computers.

Browse safely

Use virtual private networks (VPNs) whenever possible. Virtual private networks are a type of network connection in which traffic travels encrypted and in which attackers cannot view its contents. VPNs are used when you are outside the company, and we want to access any document we have on the intranet or in our corporate team. In this way, we will have access to all our documents and at the same time we will navigate safely.

Avoid also visiting websites with dubious content. As mentioned above, there are web pages that, appearing to be legitimate, hide the so-called exploit kits, which detect the vulnerabilities of our web browser and take advantage of them to install ransomware on our device. To avoid this, as always, it is advisable to keep updated web browsers, the operating system and, of course, any security solution we use, without forgetting logic and common sense in our activities online.

Updates

Cybercriminals take advantage of vulnerabilities or security holes in software, operating systems, or firmware, even in an automated way (exploit kits). Therefore, the more up to date the systems you use, the fewer vulnerabilities they will have and the more difficult it will be for them to enter or infect you.

Make sure that operating systems, apps, and devices have automatic update installation enabled.

If you use custom software, make sure that its design has considered security requirements and that it has updates. Request the aid from software audit experts to prevent vulnerabilities in this type of software.

Minimum privileges

A basic principle of security is to keep security privileges to a minimum; that is, to prevent users and groups of users from having more privileges than they need. This is possible by managing privileges to access information or to install software.

For general users, accounts with limited privileges should be used, instead of accounts with "administrator" privileges. This prevents general users from having access to services, information, or procedures that they do not need for their activity. This affords added protection by preventing distinct types of malware from being installed, by mistake or if their credentials were lost or stolen. Privileged accounts should only be used by administrators. Here are some basic tips about using user accounts:

- Use strong passwords. Attackers get a higher success rate the easier it is to crack our password. To do this, they use specific decryption tools usually based on dictionary words. For this reason, it is of vital importance to always use strong passwords and locking policies (in those systems that allow it by policies) so that, in case it is make a certain number of unsuccessful access attempts to the system, the attacker is blocked for a time that prevents him from developing a brute-force decryption attack, that is, by testing random combinations of letters, symbols and numbers. This blocking time makes the decryption time large enough to give up and try it with another victim whose safety profile is lower.
- Do not use accounts with administrator permissions. If we use this type of user and our password reaches the hands of the attacker, he will have full control over our computer. If, instead, we use user accounts with limited permissions, we make it harder for the attacker to reach critical data.
- Deletes or disables those user accounts that are not needed. Any account that has access to our equipment is a source of access to it. No need to have a "guest". If we do not use something, better remove it. We must also end the accounts that are no longer used and that of employees who do not already belong to our company.
- Do not use post-ITs to write down your company passwords, anyone outside could see them. Use password managers, specific applications so you don't have to remember more than a single password (the manager's) for everything.

A good practice is also to organize data according to its importance to the company: where in the organization it is used, by whom, and the security measures they need. This will be possible to apply measures to separate the places where the information is located and apply access controls physically and logically by profiles or groups (for example, accounting programs and data, but not others) or special protective measures (such as encryption) in cases of more sensitive or confidential information. One way to separate critical applications or systems is to use virtualized environments

We must not forget to save logs of the use of files and external access to perimeter devices (routers, firewalls, etc.) that will allow us to investigate any incident and provide data in case of complaint or to be able to demonstrate before an insurance (cyber insurance that we have indeed suffered an attack.

It is also advisable to use policies to prevent employees from installing disallowed applications and use filters to control browsing traffic in the company, authorizing reliable pages and those strictly indispensable

Minimal exposure

Another basic cybersecurity principle is that of minimum exposure; that is, to avoid exposure to the outside of the company's internal network or that information or service that does not need to be accessed from outside the company. same.

Companies need to offer some services over the Internet to their customers or workers: email, corporate website, remote applications, or file repositories. Some companies opt for the outsourcing of these services, others prefer to do it internally and assume the installation and management of servers and equipment in their own premises, so they can save costs and increase control over their information.

In this case it is necessary to separate the servers accessible from the outside from the private servers of our organization. To make those servers we want accessible from the Internet, it is necessary to open a part of our network, always avoiding that the rest of it is unprotected: this is achieved using firewalls.

A firewall or firewall is a security system capable of establishing rules to block or allow connections in or out of our network. For the firewall to "know" what is allowed and what is not, we must configure:

- What kind of connections do we allow (web, mail, chat, P2P downloads, etc.)?
- In what sense do we allow them: incoming (from the Internet) or outgoing (to the Internet).
- Which computers it affects (all teams, only one or one set) of them).
- Which IP addresses are blocked (for being on malicious IP listings)?

Currently, there are open-source firewalls, that is, supported by a community of users that are usually free and highly efficient and secure. In addition, they allow corporate use. Some of these firewalls include what is called IDS and IPS, intrusion prevention and detection systems that will help keep the internal network of our company through a passive and active control simultaneously.

In addition, a basic security measure is to disable the remote access protocol (RDP or remote desktop in Windows) to the systems if it is not being used or change the default port if it is used. Currently, direct access to the remote desktop is not considered secure, it is advisable to implement the use of VPN networks or use specific more secure systems.

Sometimes a firewall is not enough to protect our internal servers. Once we have allowed access to our network, an attacker could take advantage of a vulnerability in our server to compromise it, and from there, try to attack other servers or devices on the internal network that you do not initially have access to from outside the network. To avoid this security breach there is a configuration called a demilitarized zone (or network) or DMZ.

A DMZ network is a network isolated from the rest of the internal network, where only the servers that must be accessible from the Internet are located. This way, if one of these servers is attacked and compromised, the rest of the network will be protected.

This DMZ network, due to the fact of being exposed to attacks from the Internet, must be specially controlled and monitored, being highly recommended to install intrusion detectors, take special care when it comes to protect and configure your servers and give priority when installing critical security updates and patches.

Some examples of candidate teams to be within a DMZ would be:

- Mail and Webmail servers.
- VPN servers (virtual private networks). Before deploying this type of servers, it is advisable to carry out a study of the needs and topology of the company's network.
- DNS Servers (Domain Name Server).

If we contract technological services or outsource any of them on the facilities of suppliers, we must include in the service level agreements the clauses that allow us to verify that they take these minimum exposure measures and the rest of the technical measures in this section.

Email

Email is one of the main ways of entering phishing emails with which they will try to steal our passwords to access our services, and others with deceptions so that we install malware or visit pages where to infect us. Therefore, email servers must:

- Have spam filters to prevent phishing emails from reaching the employees' mailbox. This filter must be activated, configured, and reviewed continuously. In this way, the employee is prevented from making the decision to open attachments or clicking on links potentially dangerous for him and for the company. In some cases, the domain provider itself provides a spam filter with several levels of sensitivity, which is maintained by them and can be activated for all the email addresses of the company, thus saving us the cost and time of maintenance.
- Avoid email spoofing or email spoofing using incoming email authentication, there are different protocols that can help if implemented and configured.
- Scan incoming and outgoing emails with an up-to-date antivirus to detect threats and filter potentially malicious files. It is advisable to always look at the extensions of the received files and see if they are consistent with the name, for example: "invoice.pdf.exe" is not a legitimate file, but everything opposite. This type of practice is quite common in emails that contain malware. To be able to view file extensions, this option must be enabled specifically on some systems
- Disable the macros of the Office files or any other office suite or use a document preview (there are online alternatives) instead of opening the files directly with the office programs.

- Disable the display in HTML format in critical email accounts or publicly available to contact the company. This format allows you to include a programming language called JavaScript, widely used for functionalities offered by email. this functionality can make spammers verify that the email address is valid or redirect the user's web browser to a malicious page that ends up infecting our computer. In this way, it would not be possible to view attractive emails, but it would be much safer.
- Use virtual environments to open suspicious files. Do not open them directly on a company computer with sensitive information. Recently, in some versions of Windows 10, there is the option "Sandbox", a virtual environment of fast execution designed for these cases. If your system does not have this option, you can use third-party tools such as Cuckoo Sandbox compatible with most platforms.

Incident Response Plan

Another preventive action is to have an action plan or response to incidents. In the preparation phase will have to consider:

- carry out the management of incidents within the enterprise;
- Documentation necessary on the systems and networks that are used in the organization. It will be necessary to define what is the normal activity that allows us to detect suspicious activities that are indications of incidents. For example, in the case of outsourced services, the provider is responsible. It is also useful, in case of suffering an incident, contact an incident response center, in which they will indicate how we can recover our files if there is already a successful mechanism.

In the detection and analysis phase, the incident must be classified to determine what a ransomware is, its origin, the criticality of the affected systems, etc. Also, in this phase we must escalate the incident, if we do not have our own resources to solve it, or we need to have external experts for its resolution. In the containment, resolution and recovery phase, the steps to retrieve the activity and data. Once the incident is closed, we must record all the necessary data about it: affected users, equipment, what actions have been taken, results, etc. With this, improvements can be detected to act in case a similar incident is repeated.

Audits

A basic good practice is to scan computers with anti-malware software and schedule it to run periodically. This software must be up-to-date and active.

It is also advisable to periodically carry out an audit of our systems, both to test our security mechanisms and to check our defense ability against attacks. Currently, this task is simple, as there are products and services to automate it. However, it is still necessary for them to be carried out by specialized personnel of the company or, in case of not having such personnel, an outsourced service. These are the aspects that should be considered, for ransomware prevention, when we request an audit:

- anti-virus, anti-spam, and content filtering protection;
- administration of user permissions and access to services;
- security of mobile devices;
- automated management of updates and patches;

- vulnerability detection;
- monitoring of the use of computer and network resources; and
- real-time security event monitoring and analysis (SIEM).

These are the several types of tests you can request:

- Penetration test: it is a type of technical audit that consists of a set of tests to which an application, service or system is subjected, with the aim of to find gaps or failures through which it would be possible to gain unauthorized access to company information.
- Network audit: allows to analyze the company's network in search of open ports, shared resources, services, or network electronics (router, switch, etc.). In addition, this audit uses tools that allow cataloging the infrastructures connected to the network or even detecting versions of insecure devices, software versions or the need to install updates or patches.
- Perimeter security audit: this is a process aimed at determining the level of security of the barriers that protect the communications network of an organization from the risks that come from the outside and the inside. We could include it within the network audit, although it is more specialized in detecting security flaws from the outside point of view.
- Web audit: analyzes security flaws or vulnerabilities that affect the operation of a web page.
- Forensic audit: post-cybersecurity incident audit to identify the causes that produced it. Its objective is to collect and preserve the evidence or evidence of an incident to, after its subsequent analysis, know what and how it has happened, learn from it and debug the possible legal consequences.

What to do if impacted?

If you have suffered a security incident in which your data has been encrypted and you are being extorted to pay a ransom, you must know how to act. Remember that the first thing is to turn off the affected computer so that it does not spread to other devices on the internal network. In all cases you should follow these two recommendations:

- Never pay the ransom, as this does not guarantee that you can recover the information or that they will not demand a second ransom from you again.
- If you have an incident response plan, you will apply it to minimize as much as possible the damage caused and recover corporate activity as soon as possible. This response plan will set the guidelines to follow to obtain evidence that serves for a denunciation of the criminal action. If you don't have an incident response plan, use the latest backup of your information to recover lost information.

How do I recover my activity and data?

To recover the activity as soon as possible and avoid greater economic losses, we can carry out a series of actions aimed at recovering the data and continue with the normal functioning of the business activity:

- Clone the hard drive: It is recommended to perform a complete cloning of the disk. In this way, you will be able to keep the original device and thus try to recover the data about the clone. If there were no solution today, it is possible that in the future there is, so you could recover your files.
- Connect the hard drive of the affected computer to another computer isolated from the network and prepared for tests and do not boot with it, use it to check what information has been saved and make a copy. You must be careful to save only important data (documents, photos, certificates...) and not executable files or programs that can re-infect your computer. If possible, it collects and isolates samples from encrypted files or from the ransomware itself, such as the file attached to the message from which we are infected.
- Report the incident:
    - FBI
    - NSA
- Change the hard drive. You can also remove the affected hard drive and keep it as proof or keep it stored in case, later, a solution of decryption of the information appears that allows you to recover its content.
- Disinfect the cloned disk: it would be the next step to try later to recover it. To do this, an up-to-date antivirus or antimalware tool must be used. It is particularly important to remove the malicious software and its remnants before recovering the data, because if it is not done, it could be encrypted again.
    - Recovers and restores the equipment to continue with the activity. If possible, reinstall the computer with the original software or boot into safe mode and recover a previous backup if you have one.
        - Try to recover the data: with the disinfected disk we can start the process to try to recover the data. It is recommended to use the website www.nomoreransom.org, which is a collaborative project endorsed by

EUROPOL and has a database of attacks by this type, as well as solutions. You will need two encrypted files or the ransom note. Remember to read the rules for sending data before.

- If there is a solution, the page will offer you the tool to decrypt the files and an explanatory manual that contains detailed information on how to use it. Read it in detail before putting it into practice and contact your computer support.
- If there is no solution, keep the disk encrypted in case a solution appears in the future.
- If you have an antivirus in your company, contact their software provider in case they have developed a specific tool.

- Restore the backup. Check if the operating system's file system has shadow copy or snapshot, which maintain copies of previous versions of files. Locate a pre-infection copy and restore it. You will have lost data, but you will be able to continue with your activity.
  - Finally, it uses a new or formatted disk, in addition to a clean installation of the operating system, and restores the most recent backup prior to the infection. If you have decrypted the information, you can transfer it to your installation on the new media.

Why don't you have to pay the ransom?

If an incident has happened to you, you will have many doubts about whether to agree to pay the ransom or not. Our recommendation is that you do not pay the ransom demanded by cybercriminals for the following reasons:

- Paying does not guarantee that you will have access to the data again, remember that these are criminals.
- If you pay, you may be subject to subsequent attacks, as they already know you are willing to pay.
- They may request a higher amount once you have paid.
- Payment promotes the business of cybercriminals.