WHITEPAPER

Ransomware

Incident Prevention and Response

Evandro César Vilas Boas
Vanessa Mendes Rennó
Guilherme Pedro Aquino

HUAWEI
CxSC Telecom
Centro de Segurança Cibernética
Inatel

Index

Introduction

The technological advance of digital media has made it possible to offer affordable solutions to people, increasing the number of connected individuals considerably. Consequently, for-profit organizations have begun to exploit digital communication channels as a path to redefine business and widen their customer base. Government organizations and non-profit institutions have also digitized processes to provide easy access to services. In addition, some vertical markets have benefited from the growth of connectivity to introduce disruptive digitized solutions, such as the fintech Nubank, Banco Inter, and others.

The digital migration of processes or routine activities from the physical has changed services and businesses while motivating the spread of cybercrime.

There is a substantial digital flow of business-sensitive information and personal data from work, online shopping, financial operations, and website registrations. This personal information and data have become valuable digital assets. Therefore, the digital migration of processes or routine activities from the physical has changed services and businesses while motivating the spread of cybercrime. Thus, telecommunications networks and systems are required to provide means for the secure traffic, manipulation, and storage of these assets, introducing the cyber security concept.

Cybersecurity provides means of preventing cyberattacks of any nature. It also defines response frameworks to mitigate damage under possible attacks that a company or institution may suffer. Multiple **cyberattack** techniques aim to access, capture, or damage systems and information. Occasionally, these attacks aim to extort the victim – an individual or legal entity.

Note that no organization is entirely secure, as cyberattack approaches and methodologies constantly evolve to circumvent preventive security countermeasures. However, good practices in preventing cyberattacks combined with **firewalls** and **intrusion detection/prevention systems** allow for identifying intrusion attempts or mitigating the risks caused by a possible attack.

Companies and institutions have recently faced a scenario of migration from in-person to remote work in response to prevent the spread of COVID-19. However, most organizations were unprepared for remote access to their corporate networks. Furthermore, corporations have been required to scale their cybersecurity levels to promptly adapt their networks for remote access and protect their digital assets. In Brazil, companies and institutions faced a second challenge related to the adequacy of their processes to the **General Data Protection Law**, ratified by the Federal Government and ruled since August 2021.

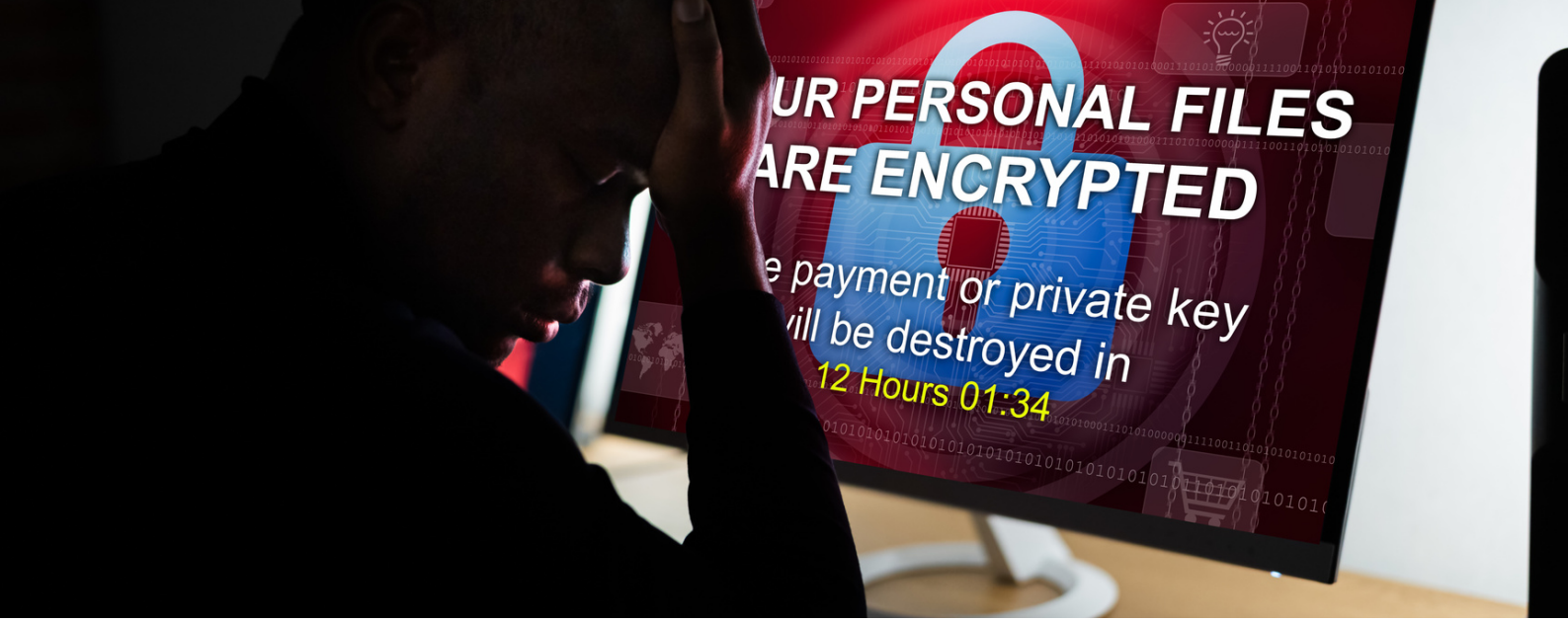
The digital world experienced major cyberattacks in **2021.** These include exploiting zero-day vulnerabilities in **Microsoft Exchange**, servers, **SolarWinds** Orion TI network monitoring program, and Apache Loggin Services Project's **Log4j** open source library that served as a gateway for malicious actors on a large number of networks.

Zero-day is a program or application vulnerability unknown to developers and users. These vulnerabilities could be exploited to gain an advantage in cyberattacks.

These attacks contributed to an increase in the number of cybercrimes recorded in 2021. According to **SonicWall** annual cyber threats report, there has been an increase in incidents involving intrusion attempts, cryptojacking attacks, ransomware attacks, and encrypted threats. Among these variants, ransomware attacks have increased by 105% this year.

On the other hand, ransomware attacks ranked as the second most prominent threat from the respondents' perspective regarding the concern level about the types of cyberattacks. Furthermore, **other studies** rated Brazil as the fourth country concerning ransomware attacks.

The cybersecurity company BLACKFOG assesses the state of ransomware attacks for 2022, listing the attacks for each month on its **website**. Companies such as Toyota, Samsung, Panasonic, and Vodafone are among others that have reported ransomware attack incidents.



Ransomware

Ransomware is **malware** – malicious software – among others, such as spyware, adware, and botnets. Generally, malware is a program intentionally designed to cause damage to systems and devices on which it is installed or to provide an advantage to third parties over those devices. The nature of the malware defines the attack level and potential for damage. Notably, ransomware is considered to be the most offensive among malware variants.

Ransomware is malicious code that invades systems or devices to hijack them by blocking access or capturing and encrypting data, whose recovery demands a ransom payment to the attacker.

This malicious code invades a system or device to block access or capture and encrypt stored data. Afterward, it announces a financial request for the system, device, or information ransom. The ransom appeal may include threats to disclose the information in the public domain when information is exfiltrated. Additionally, **criptocurrency** payments are demanded to make tracking difficult, such as Bitcoin.

Financial Impacts

Ransomware attacks are ranked as extortion crimes and trigger several **factors that impact a company financially**. Initially, there is the financial ransom demand, whose numbers are usually high. Payment is not recommended since the organization cannot guarantee that the attack will end, resulting in further extortion attempts. In addition, there is a case of the data being damaged.

The attack can make the company's business process unavailable, causing losses from the interruption. On the other hand, the time required by the IT team to recover systems and data may hinder employee activities reestablishing, affecting results.

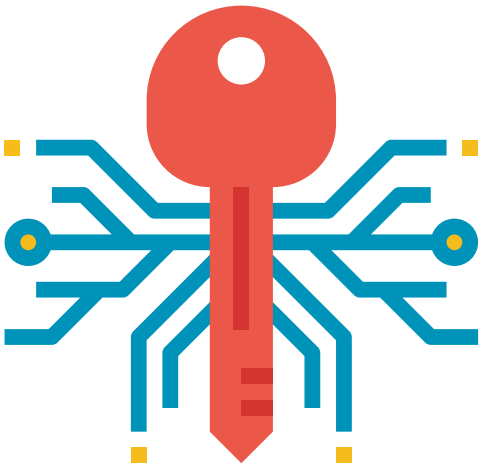
Ransomware attacks are ranked as extortion crimes and trigger several factors that impact a company financially.

The cyber incident must be reported to the local authority responsible for managing the country's data protection regulations. The incident assessment may result in a financial penalty with amounts stipulated by the legislation. For instance, the Brazilian authority is the National Data Protection Authority (**ANPD**).

More than 30 countries recognized the economic exploitation potential of ransomware attacks in 2020 at a virtual meeting. As a result, Brazil and other countries, led by the U.S. government, have initiated the International Initiative to combat ransomware.

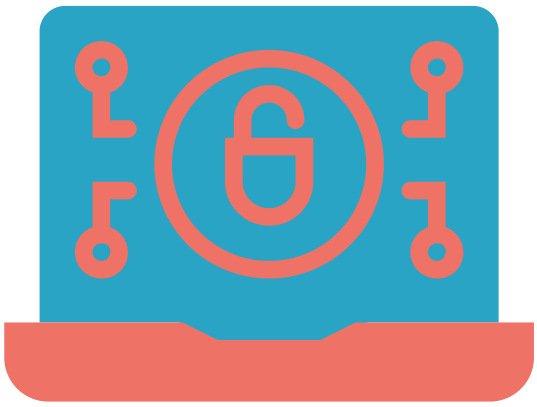
Types and methods of extortion

Several types of ransomware can be classified broadly based on the process of hijacking the system, device, or information. For example, those that employ encryption are referred to as crypto-ransomware, while others that block access are defined as locker ransomware.



Crypto ransomware **uses algorithms to encrypt important files and information, driving them unavailable for user access. The decryption process requires a ransom payment to recover the information.**

Locker ransomware **acts differently than crypto-ransomware, employing mechanisms that capture the victim's device. Consequently, the recovery of access also demands a ransom payment.**



Regarding the extortion process, recent techniques involve **double** and also **triple** extortion. The double extortion includes the ransom demand for the data and the threat of leaking victims' data and information if a second amount is not paid. This approach has been lucrative for exploiting ransomware attacks. In early 2021, triple extortion rose as a new technique to profit from ransom requests. This strategy involves extorting customers from the affected organization or using an additional attack as motivation, such as denial of service.

Recently, the malware business model has evolved to provide ransomware as a service – **RaaS**. Therefore, some hackers dedicate themselves to programming ransomware codes and making them available through a dark web repository. As a result, access is possible for cybercriminals other than the programming hacker through a subscription contract, similar to the Software as a Service (SaaS) business model. The subscription allows the criminal to profit by exploiting the ransomware to execute multiple attacks. As outlined in the contract, the ransomware owner receives a part of the profit when the attack succeeds.

Evolution of ransomware in one click

The first malware, classified as ransomware, came up in 1989. The biologist Joseph Popp created the ransomware, known as **AIDS Trojan**, and disseminated it via diskette at the World Health Organization's AIDS Conference. After installing on a machine, the ransomware would count the number of times the computer restarted, encrypting the directories or blocking access to the file names on the drive (C:) behind ninety boots. In addition, the victims were coerced to pay U$189.00 to an account identified as PC Cyborg Corporation to get access back.

In 2004, the **GPCode** ransomware was spread via spam emails cloaked as a job application form. This ransomware is a Trojan encrypts user data with the RSA algorithm, followed by a ransom request. GPCode has undergone rapid mutations, employing sophisticated encryption methods such as asymmetric encryption.

Another Trojan-type ransomware emerged in 2006, named **Archievus**. This ransomware was the first to use advanced RSA encryption, difficulting the file decryption process. The malware spread using website links and spam emails.

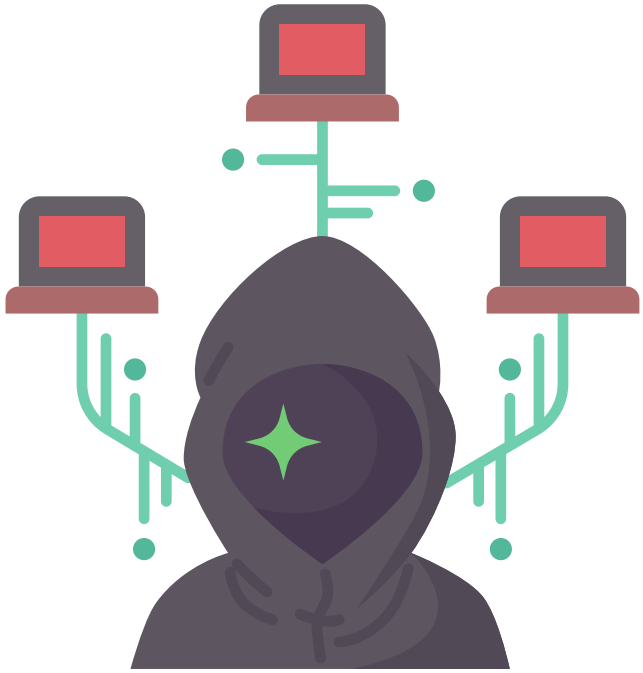
In 2013, the original **CryptoLocker** Trojan extorted about U$3 million from its victims. Therefore, it has become a ransomware model for many hackers, resulting in successful variants over the years. This ransomware also employed asymmetric RSA encryption with 2048 bits key length.

The **WannaCry** ransomware attack reached a global scale with estimated losses of U$4 billion in 2017. This ransomware exploited a vulnerability in Microsoft Windows using a hack called EternalBlue. Although Microsoft released an update to fix the vulnerability, the lack of awareness about the importance of updating programs and systems became a loophole for WannaCry to contaminate about 230 thousand computers. At this point, the criminals started requesting cryptocurrency payments with values around U$300 in Bitcoins.

The WannaCry ransomware attack reached a global scale with estimated losses of $4 billion in 2017. This ransomware exploited a vulnerability in Microsoft Windows using a hack called EternalBlue.

The **Petya** ransomware has emerged concurrently with WannaCry and exploited the EternalBlue vulnerability. This malware has proven effective at infecting systems and devices, including those updated against the EternalBlue vulnerability. Petya acts on the Master Boot Record by compromising the infected operating system. In 2017, the **Bad Rabbit** ransomware spread to European countries through fake update messages from the Adobe Flash Player program. Users who accepted the update were infected by the virus, whose ransom value was U$1,000 in Bitcoin.

Recently, ransomware attacks using the RaaS approach have emerged as a means to spread malware quickly. In 2019, **REvil** ransomware was detected exploiting **Oracle** WebLogic server vulnerability. Two years later, the same ransomware exploited a vulnerability in **Kaseya** systems, striking security management providers from several client companies. The system's ransom payment request is for U$70 million. Still, this ransomware was linked to the cyberattacks suffered by the **JBS** company subsidiaries in 2021, which succumbed to extortion by paying about U$11 million in Bitcoin.



In addition, recent attacks report using a RaaS, known as **Egregor** and **Conti**. **Barnes & Nobles** is considered the primary victim of the Egregor attacks. Meanwhile, the **Conti** ransomware ranked as the second largest number of victims in 2021, using various methods to break into corporate networks.

A new type of ransomware programmed in the Rust language has claimed recent attacks, dubbed **BlackCat**. Through cross-compiling, BlackCat can target both Microsoft Windows and Linux operating systems. This ransomware is considered a successor to the **BlackMatter** and REvil variants due to its similar behavior.

Ransomware Attack

The life cycle of a ransomware attack comprises eight steps:

- Reconnaissance;
- Preparation and Delivery;
- Initial access;
- Installation;
- Discovery;
- Lateral movements;
- Data collection and exfiltration;
- Encryption, access blocking and extortion.

The three main initial access vectors exploited in ransomware attacks are: malware infection, using credentials for remote access, and scanning and exploiting vulnerabilities in server interfaces with the Internet.

Reconnaissance

The reconnaissance involves exploring **initial access vectors** to gather information about the target organization. At this stage, the hacker surveys information about the organization's employees by collecting emails or analyzing social media profiles. Another possibility is exploiting Internet-facing interfaces by scanning the corporate network.

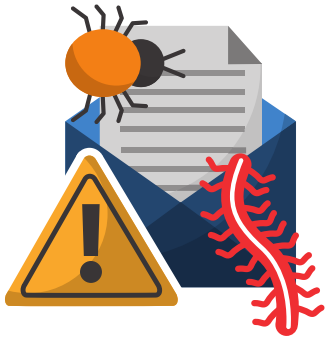
Preparation adn Delivery

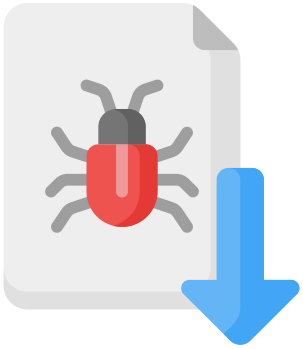
The information gathered in the reconnaissance phase is used to define strategies to insert ransomware into the corporate network. For example, regarding **Social Engineering**, the attacker uses phishing emails to spread the ransomware by attaching it to download files – pdf, word, excel – or insert the malware on compromised websites. On the other hand, the attacker can exploit vulnerabilities in the reconnaissance step to map out the tools needed to execute the intrusion.

Initial access

Initial access to the target network or device begins with executing the approach defined in the Preparation and Delivery stage. Next, the delivery requires an action – downloading suspicious programs or phishing email files – by the victim to release the ransomware onto the network or successfully exploit a vulnerability.

This phase is a crucial point to be assessed by organizations, mainly when the delivery is through social engineering techniques. Social engineering practices are considered adequate for spreading ransomware and easy intrusion methods.





These approaches use phishing emails with attached files or downloads and installing programs from suspicious websites. In addition, phishing attack surfaces are evolving for text messaging and chat applications.

Spear phishing is also targeted at high-level hierarchical collaborators to obtain confidential information by posing as legitimate collaborators of the organization.

On the other hand, the remote work scenario has increased the number of **Remote Desktop Protocol** – RDP – servers to provide corporate connection to employees. Shortly, attackers began using brute force attacks against RDP services, virtual private networks, and user accounts. Other input vectors consider exploiting vulnerabilities in outdated operating systems, programs, or applications.

Installation

Successful ransomware delivery allows the attacker first access the network and installs the malicious code to start the infection process. Then, the ransomware is installed as a binary, opening a **backdoor** to communicate with a command and control server and uploading files necessary for the subsequent phases.

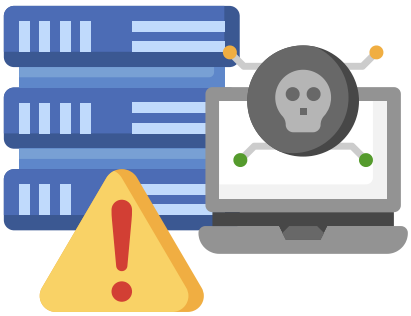
This step also includes procedures to avoid intrusion detection, ensure the reinfection of the device and protect it from attacks by other ransomware.

Discovery

Upon completing the procedures inherent in the Installation step, the attacker initiates awareness of the environment through scanning and enumeration to discover information and collect credentials and data.

The credential collection employs specific tools to enumerate and select users with local or domain administrator privileges. Network architecture mapping through scanning and enumeration lets the attacker perform lateral movements. Data collection is the first stage in searching for valuable information that can be used in the negotiation process.

Lateral movements



Mapping the network through scanning and enumeration tools allows the attacker to perform lateral movements. This step aims to expand access beyond the initially compromised device or application based on network awareness to other machines and services.

Lateral movement provides a means for the attacker to search for sensitive data and other valuable digital assets while avoiding detection and ensuring network access. However, detecting lateral movements is difficult because traffic analysis interprets the actions as usual.

Data collection and exfiltration

The double or triple extortion techniques introduce the phase of data collection and **exfiltration**.The attacker aims to transfer data to their backups while performing actions that could compromise the victim's restoration process. Some approaches consider changing backup routines and rigging the process. As well as introduce flaws in the backup program to compromise the restoration process. Data exfiltration is usually performed through the same communication channel established in the installation process.

Encryption, access blocking and extortion

The last step in implementing a ransomware attack involves releasing the encryption processes and/or blocking access to the systems and data repositories exploited in the previous steps. Then, the announcement of the attack and the ransom demand occurs in the face of the threat of impairing the systems and devices, exposing the data to the public domain, or destroying them.

Ransomware Risk Management

Cybersecurity risk management is a set of practices dedicated to providing security solutions for digital assets. Therefore, some security frameworks guide companies or institutions to prevent or mitigate the damage against cyberattacks while using digital means to develop their business.

There are frameworks dedicated to comprehensively mapping the network infrastructure, including best practices focused on incident prevention. Meanwhile, other actions allow the detection of events that pose a risk or violate cybersecurity. Finally, some approaches are dedicated solutions to mitigate errors and guide the organization in recovery.

Herein, we focus on establishing a set of activities for ransomware risk management. Note that some approaches can be generalized to broader management. The set of actions under discussion is organized following the Ransomware Risk Management framework proposed by the National Institute of Standards and Technology – **NIST**, which groups them in:

- Identify;
- Prevention;
- Detection;
- Incident response;
- Recovery.

Identification

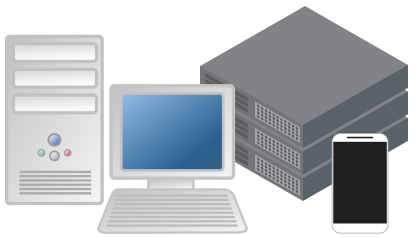
The identification is the initial phase for implementing measures in ransomware risk management. Since this malware aims to exploit vulnerabilities in the network infrastructure and access critical digital assets, it is necessary to map the network and service architecture. This action provides an overview of the organization's infrastructure and helps identify and fix potential vulnerabilities.

Identification provides an overview of the organization's infrastructure and helps identify and fix potential vulnerabilities.

Under incidents, documented information supports the investigation, enabling quick and accurate determination of potential gaps in security implementation and the damage caused by the incident. In general, actions aimed at identification are organized into:

- Hardware documentation;
- Programs, services, and applications documentation;
- Data and information documentation;
- External services documentation;
- Roles and responsibilities documentation.

Hardware documentation



The organization must prepare documentation about all equipment used to offer the necessary services and applications for its business development. The documentation must contain the equipment's functionality, its application in the context of the infrastructure, and its location. This information helps the IT team implement incident response procedures, such as isolating affected domains. This information assists the IT team in implementing incident response procedures, such as isolating affected domains.

Programs, services, and applications documentation

Similarly, programs, services, and applications must be mapped. The survey should include basic information such as version, last update, host device, and documented and unpatched vulnerabilities. In the case of scheduled updates, information must be added to the documentation contemplating the improvements and corrections indicated by the provider. This information allows the strategic action of the IT team to manage mass attack alarms by exploiting vulnerabilities in a given program. In addition, compromised programs, services, or applications can be identified during incident response and support digital forensics investigation.

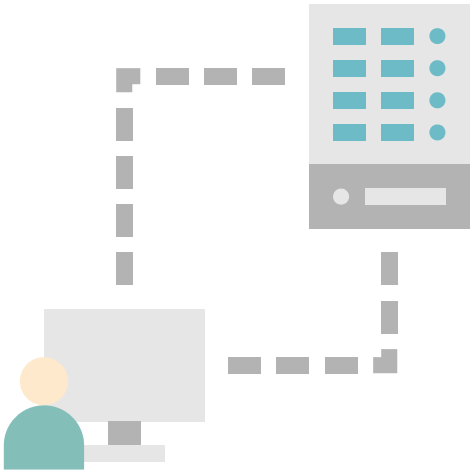
Data and information documentation

The organization must prepare a detailed document about the collected, manipulated, and stored data types and the development of business line information. The documentation must set out the collection means, handling procedures, and storage form and place, including possible backups.

The survey allows the organization to map the data and information criticality level for the business, supporting the implementation of adequate security levels. Again, the information is helpful in incident response periods, allowing the scope of the attack to be defined.

External services documentation

To carry out routine activities, an organization needs to access services that support its business development. This approach requires the company's network to establish external connections with other networks or servers.



Therefore, it is essential to map the external connection types, implement adequate security layers, and, most importantly, the external service provider security level. Some ransomware attacks start by exploiting security holes in external connections and/or the service **provider's infrastructure**.

Roles and responsibilities documentation

The workforce and the relationship with the company/institution's functions and processes must be documented in terms of policies and good practices related to data handling and access to confidential information.

Therefore, the employee must have access to the security policies related to his organizational occupation, being assured by the IT team. In addition, the document supports prevention methods related to employee education through targeted actions.

Prevention and Detection

Several actions can be used within a company or institution to prevent ransomware attacks, ranging from the cybersecurity education of employees to implementing technological solutions. These actions create protection stages at different levels of attempted intrusion of a ransomware attack.

Preventing ransomware attacks includes both employee education and the implementation of technological solutions.

Also, there are dedicated tools for detecting possible cybersecurity incidents, which consider factors such as traffic analysis. This section presents these actions to provide valuable insights for sound management of the IT team.

Employees education

Regarding cybersecurity, the human is the weakest and easiest link to break. Therefore, attackers employ different social engineering forms to invade and install themselves on a network. For example, as discussed earlier, phishing emails with attached files that appear trustworthy induce the recipient to open them and download the attachment.

On the other hand, the employees' lack of knowledge can lead them to compromised or malicious sites when they practice their craft looking for necessary information or tools. Inappropriate program downloads raise the opportunity for ransomware to install itself on the company's device and contaminating the network.

Therefore, employee education on cybersecurity best practices is essential to prevent ransomware attacks. Thus, employees are aware of the effects of ransomware attacks and how they can facilitate agents for cybercriminals. This process is accomplished through cybersecurity educational content dissemination or short courses.

Furthermore, it is crucial to keep employees on alert, reinforcing the risks of exposure when browsing the web. In this way, the IT team must develop social engineering campaigns and apply them to employees. In addition, the results should be compiled and used to demonstrate the importance of cybersecurity education. Finally, the IT team must discuss the results with employees to demonstrate how to identify suspicious emails and, mainly, how to report them.

Apply web traffic filters

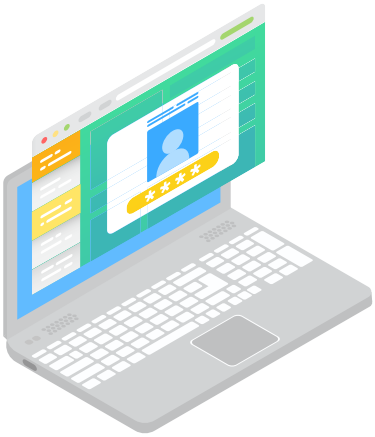
Applying **web traffic filtering technologies** to computers and devices can create a barrier to ransomware entry. URLs and websites are evaluated and filtered, preventing the user from accessing those defined as suspicious or categorized as malicious.

Web traffic filters operate in two ways to check a URL or website and determine blocking content access. Factors such as the site's quality and verifying in well-known lists that categorize web pages according to genre and content can be used.

The tool can also perform a web page content evaluation to distinguish between blocking or not, according to the configured parameters. These tools generally use databases that list URLs from different domains and the possible association with malware, phishing, and other types of attacks.

Reduce access privileges

When performing tasks related to the job, a concise mapping must be carried out on which employees demand administrator privileges on computers and devices connected to the corporate network. In addition, credentials with administrator privileges should be reduced to the lowest possible number to limit the attacker's ability to perform lateral movements, encrypt files, or block access to equipment.

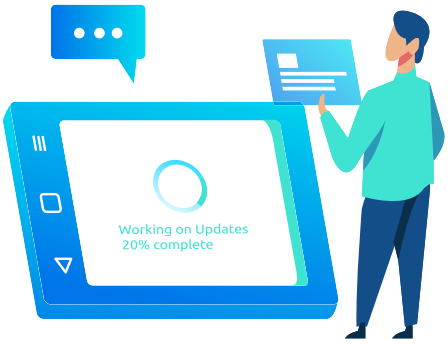


Providing unnecessary administrator privileges to employees poses a risk to the company or institution's cybersecurity. Because when web browsing with such privilege, the employee can expose himself to social engineering attacks, delivering valuable information to a potential invader. Also, it can download and install malicious programs and applications that set up gateways for ransomware.

Therefore, it is recommended to limit the employee's privileges access when performing routine tasks such as web browsing, and opening documents and applications, among others. In this way, compromised employees' access credentials used for an invasion by a ransomware attack limit access to the local computer or device.

Update operating systems, programs, and applications

Exploiting vulnerabilities in operating systems, programs, and applications represents a critical ransomware entry vector on a network.



As we discussed earlier, some ransomware attacks exploit these vulnerabilities to speed up and scale the malware spread process, compromising many machines.

Therefore, the IT team must follow the updated recommendations requested by the operating systems, programs, and applications used for the organization's business development. The IT team should perform the updates remotely when verifying an update request. Alternatively, inform and ask employees to execute them immediately, ensuring that possible vulnerabilities are corrected.

This practice eliminates the computer or device's possible contamination under the prerogative that all machines on the network are updated in terms of the operating systems, programs, or hosted applications.

Network monitoring

Using network monitoring programs integrated with a firewall is a means to prevent ransomware or other attacks. Generally, the first step in cyberattacks involves network scanning.

Then, the monitoring system can automatically identify and isolate the device from an attacker's scrutiny, disconnect it from the Internet and report the activity to the company's IT team for review. This practice can end a potential attack by preventing the identified device from infecting other machines.

Enforce password policies and reduce remote access

Strict password-writing policies should be implemented to prevent intrusions via brute force attacks. Force employees to periodically change passwords and implement policies that prevent them from reusing passwords from previous periods.

Corporate network remote access must be periodically evaluated according to the employee's activity. For instance, considering the partial return of some employees to the offices, remote access should be removed immediately, reducing possible VPN intrusion.

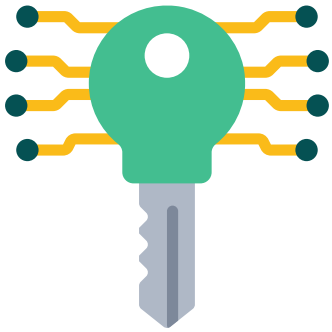
Implement backup routines

Performing periodic systems, data, and infrastructure backups and running test restore procedures from time to time is effective against ransomware attacks. This practice allows the organization to restore alternatives to the affected parties during the attack, eliminating the need to pay the ransom.

Backups allow the IT team to restore machines to prior versions of the infection process. Therefore, keeping versions of the same system at different time intervals is recommended. For example, a 30-day interval backup and a 60-day interval backup. This practice avoids restoring contaminated versions for a few weeks, triggering a long and ineffective restoration process by rework.

In addition to the option of maintaining the offline backup, a possible but unusual practice, backup storage may involve separate and distributed locations. Therefore, cloud solutions are used in different availability areas from the same provider – different Datacenters. Alternatively, a strategy is known as multi-cloud, even in clouds of several providers. This way, ransomware is prevented from quickly gaining access to all storage locations and practicing encryption or destruction of backups to eliminate restoration sources to reinforce the ransom demand.

Encrypt data

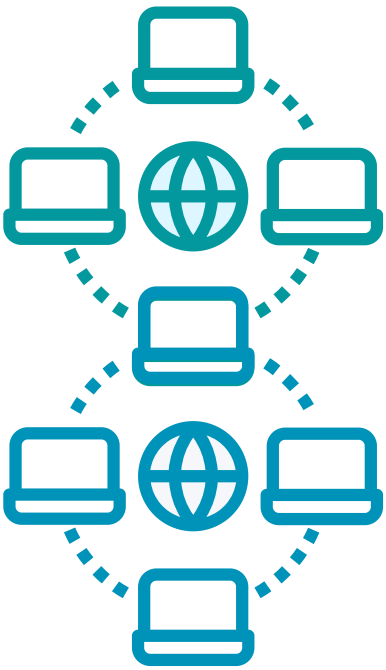


Periodic backups are essential to help the organization recover from a ransomware attack and avoid paying the ransom. However, the sensitivity of the data can be a deciding factor in paying the ransom under the threat of exposure to the public domain.

Therefore, it is crucial to carry out appropriate data and information mapping handled by the company, list its sensitivity level, and implement encryption mechanisms. It is noteworthy that the encryption keys involved in the process must be stored in restricted access places different from those where the data is held.

Segment the network

Segmenting external services is the best practice when designing a computer network. This process restricts access to/from these services. In addition, remote access must be evaluated by a network monitoring system and include two-factor authentication.



Network segments must be configured to limit information traffic to specific services and monitored by an appropriate segmentation device. These traffic policies must be designed so that a ransomware attack and infection on one segment does not affect others or the entire network. Thus, isolating critical servers using independent segments is recommended instead of grouped in a single network segment. In addition, the services' critical level can be used to delimit segments, isolating internal networks from those exposed to the Internet, for example. Finally, in workstation domains, it is recommended to configure machines to prevent data flow between each other.

Machines that require Internet connectivity must be configured to use a central server in a perimeter network – also called the Demilitarized Zone, **DMZ** – rather than acquiring a direct IP address. In addition, machines that perform web searches must be isolated from direct contact with other machines or devices that do not have this functionality, preventing their vulnerabilities from being exploited.

Explore and fix vulnerabilities

The presence of vulnerabilities in a network is innate since operating systems, programs, and applications undergo update processes. As well, network elements are configured and reconfigured according to day-to-day demands.

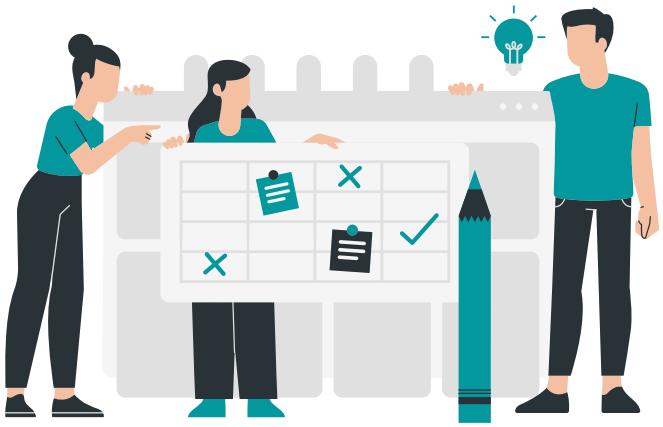
Updates have two purposes in the life cycle of an operating system, program, or application: to offer a better experience to the end user or correct possible vulnerabilities. In addition, the configuration of network elements is linked to human activity, which can unduly expose communication ports to the Internet.

Regardless of the purpose, the update process can introduce a new vulnerability, whose existence knowledge comes first from cybercriminals, resulting in "zero-day" vulnerabilities. Hence, attackers exploit them to spread ransomware attacks on networks with computers and devices running the operating system, program, or application with the identified vulnerability.

Therefore, proactive vulnerability analysis allows the IT team to identify violations of access policies or vulnerable devices. This process involves executing intrusion tests – ***Pentest*** – by experienced professionals called ***Ethical Hacker***. The test allows for identifying possible vulnerabilities and correcting them.

Plan and train the team

It is paramount to reinforce: no company or institution is immune to cyber-attacks! Technological evolution is a two-way path. On the one hand, defensive solutions improve to reduce attack surfaces. On the other hand, offensive solutions evolve by improving existing techniques and/or creating new attack approaches.



Therefore, the best prevention is developing a reasonable response and recovery incidents plan involving a ransomware attack. Additionally, a support manual accessible to those responsible for security management within the company or institution should be developed. This manual should be periodically reviewed and updated.

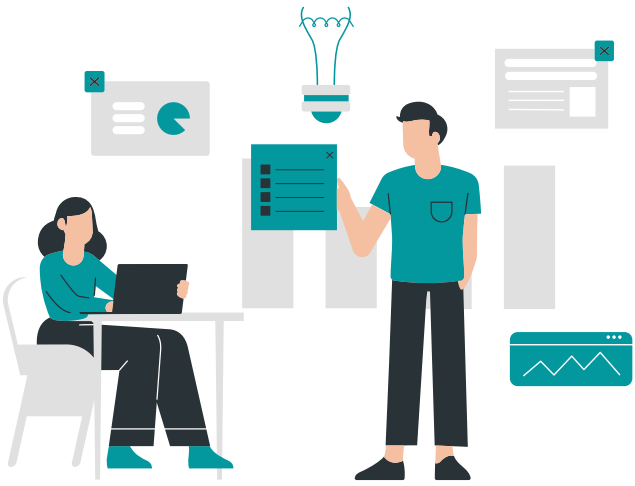
The action plan is designed to provide organization and calmness during a ransomware attack. Therefore, the plan is expected to define the activities and those responsible for executing them, avoiding confusion. In this way, the action plan must include identifying interested parties for execution and managing the incident response. The IT team, public relations, systems/applications teams, and legal assistance are included in this context.

Some important observations regarding the action plan writing process involve aspects of communication, critical data systems, and the selection of restoration methods. For example, the plan should prioritize critical data systems to provide coordinated recovery actions from the most critical to the minor priority level. Likewise, it must contain secure means of communication that are not compromised or made unavailable during the attack, such as corporate e-mail or telephone system.

This process must identify systems and critical services to the company's or institution's lines of business and map their respective interactions with other systems and services to establish tidy recovery strategies. The priority is recommended on network infrastructure services such as active directories – e.g., DNS and DHCP.

Similarly, the plan should include a concise mapping of the data handled by the company. This step allows the company to identify the data type compromised during an attack and its criticality for the business. Consequently, one can protect uninfected data and establish methods for recovering from those attacks' targets.

The strategy for recovering and restoring systems and services in an attack scenario must be included in the action plan. The plan execution should include recovery and restoration processes that best fit the purpose according to the attacks' nature. For instance, recovering machines through secure backups can result in the loss of uninfected or encrypted files or data between the date of the respective backup and the attack. Therefore, file-level or database-level recovery strategies may be a better approach. For large attacks, mass recovery is recommended. A key point in the recovery process is automation to minimize human errors and speed up the process.



Finally, a good plan requires periodic testing, evaluation, and corrections. Testing allows for identifying bottlenecks and reworking them to ensure complete execution in response to an incident. Simulations enable human resources to perform their skills and responsibilities, providing greater confidence in actual incidents. It is recommended that the test environment be as realistic as possible and planned so as not to interrupt the business of the company or institution.

Digital forensics support

In cases of incidents, the company or institution must have the support of other companies that provide services in digital forensics. Therefore, hiring a **digital forensics.** service provider is recommended for immediate support in attack or suspected attack scenarios.

This service provision allows quick response in determining the attack extent on the network and its neutralization. Hence, specialized technical support can be obtained to determine strategically safe points for the recovery processes.

Apply detection methods

Three techniques are used to detect a ransomware attack: signature tracking, behavior analysis, and deception. Signature tracing involves identifying the ransomware's signature by comparing a sample of its hash with known ones. This approach allows for quick analysis of suspicious files and the definition of their malicious nature. Generally, antivirus programs employ this technique.

The first antiviruses used a reactive analysis considering previous research by human action or autonomous programs to analyze the type of ransomware and track its signature. At this point, it is worth remembering that each ransomware has its signature. Therefore, this approach had a loophole regarding those "zero-day" ransomware that had not been previously evaluated.

This gap has led attackers to update ransomware types to adapt their signatures under different forms of encryption. In addition, antivirus programs began implementing complex tracking signatures techniques considering malware families through heuristic solutions.

Later, ransomware codes evolved tactics to circumvent antivirus systems using the polymorphism concept. The polymorphism allows ransomware to disguise its signature to avoid tracking and detection by antivirus programs. In addition, attackers use the "packing and encrypting" approach to modify ransomware at the binary level.

Polymorphism has ensured the efficiency of ransomware attacks, as shown by studies by **Webroot**, whose numbers reveal that 97% of ransomware detected on computers and devices is unique. However, despite the introduction of polymorphism, the signature track is the first line of defense and can help identify known ransomware.

Behavior analysis allows a historical basis to evaluate new activities in a network. For example, it can be used to analyze the execution of files or related tasks, identifying abnormal activities such as excessive copying of files per unit of time. Another possibility is to map the creation of files with excessive entropy, indicating the installation of ransomware in an incubation period. Traffic analysis also allows for defining suspicious network activities, such as increased traffic directed to a particular server.

A more active approach considers creating file repositories that are not accessible by company employees in general but become an easy opportunity under attack. Therefore, monitoring access to fake servers can track a possible ransomware attack.

Response and Recovery

In a ransomware attack, actions must be followed to provide adequate incident response and recovery approaches. Some of the practices discussed in this section integrate or must be previously defined in the incident response and recovery plan, recommended as a preventive methodology. In general, actions can be listed as follows:

- Attack validation
- Establish the attack scope
- Isolate infected systems and preserve evidence
- Report the attack to all stakeholders and authorities
- Assess and neutralize the attack
- Restore systems and data
- Post-recovery assessment and learning

Attack validation is the first step in a cybersecurity incident response process.

Attack validation

Attack validation is the first step in a cybersecurity incident response process. This approach is intended to define the nature of the attack so that the essential procedures are taken.

This section addresses activities for responding to and recovering from an ransomware incident. Therefore, the following steps are valid for execution if the attack is validated and identified as ransomware. Employees often report ransomware attacks when they encounter typical ransom messages or find supposedly encrypted files.

These events require the IT team's attention, which must initiate an analysis process without prompting confirmation of an attack. This is because the messages found may be fake, or the encrypted file may come from a process that took place in the past.

An infection stage assessment step should be started in case of suspected ransomware presence. Early ransomware identification allows for removing and isolating from the infected machine without requiring a comprehensive incident response. However, performing preventive analysis on all machines that share the network domain is essential. If more than one machine has been infected, proceed with the complete execution of the prepared action plan.

Establish the attack scope

Attack confirmation must be carried out by delimiting the extent of the incident on the network. This action is essential to assist the IT team in executing damage mitigation processes. On the other hand, defining the scope of the attack allows an understanding of which services, systems, and data were compromised. Hence, mapping the affected systems and working on targeted recovery processes. If the attack scope is not defined, restoring all systems and data is recommended.

This approach results in increased data loss and recovery time. Identifying the scope of the attack concerning the data handled by the company and linking the criticality level allows for determining if additional procedures need to be implemented and customers notified.

Scoping should consider evaluating shared and non-shared folders and drivers, network and cloud storage spaces, external drivers, and essential files. One way to determine the scope of the attack is to consult the logs of files generated by the ransomware, which specify which ones were encrypted. However, this approach requires knowing the type of ransomware installed during the attack. Regarding the data, it is possible to determine which ones were copied based on the ransomware ransom message. In addition, it is possible to explore the network itself to look for evidence of massive data copying.

Isolate infected systems and preserve evidence

Scoping the attack makes it possible to carry out an appropriate containment procedure by isolating the infected systems. Hence, ransomware is prevented from spreading to uninfected computers and devices in a domain or other network segments.

This stage requires disconnecting the equipment from a wired or wireless network at the physical level. For other networks, it is necessary to temporarily disconnect them from the Internet to guarantee total unavailability of access by the attacker.

Note that isolated systems and devices must have valid, non-expired snapshots to allow data recovery. Additionally, a network perimeter must be established after the ransomware neutralization and removal, along with the recovery process. The affected devices must also be monitored through service-level agreements based on retention policies for at least one year.

Another essential recommendation during a ransomware attack response is collecting and preserving evidence such as log files and system images. In addition, it is crucial to monitor the status of this evidence, which can change during the stages of the attack until its complete neutralization.

For ransomware attacks, encryption keys are also important as evidence for further investigation and must be captured before it is deleted by malware. In case of a ransom request, it is recommended to register the email, payment address, and message. This information is requested by the entity that will conduct the forensic investigations.

Defining the type of ransomware is relevant, as each malware has a standard of encryption, data theft, and ransom announcement. Some ransomware can compose variants of families already mapped from previous attacks, whose information helps the organization in decision-making. Additionally, cybersecurity consulting firms may maintain information about the encryption keys employed by the ransomware type, aiding in the decryption process. Other technical aspects can provide insights for the neutralization process to be effective.

Report the attack

After complying with the previous steps, everyone involved in the prevention plan must be immediately communicated to carry out the established routines. The communication must be done through the communication channel defined in the action plan. The information must be presented clearly and objectively to the entire IT team, executives, managers, and legal and public relations teams.

In the legal sphere, the figure of the DPO – Data Protection Office – is included in leading the company regarding the legal actions to be taken against the authority of each country and the customers in case the attack involves their respective data. The company must manage the internal and external impacts of the attack through the correct and real-time sharing of findings, allowing the public relations sector properly position itself to minimize financial impacts on the brand.

Assess and neutralize the attack

It is crucial to keep the assessment of the attack's current state so that recovery takes place after the attack is fully neutralized. If the attack is not neutralized, there is a high chance of reintroducing the ransomware and reinfecting systems, resulting in more significant damage and downtime for further recovery. Therefore, it is essential to establish a quarantine perimeter to start the recovery process. Restores can be validated before being returned to the production environment.

System and data restoration

The systems recovery process should only be started after the ransomware has been neutralized. Recovery before ransomware removal results in a secondary infection. If the malware cannot be isolated and neutralized, recovery should be directed to an isolated environment, so the infection does not spread.

Data recovery must involve detailed analysis to identify the best approach. Then, if the ransomware is identified, it is possible to decrypt the data to avoid loss between the last backup date and the attack's occurrence. Currently, there is an initiative called **No More Ransom** involving IT security and legal companies to provide support for recovery from ransomware attacks. However, note that the decryption must be carried out in an isolated and controlled environment.

System and data recovery through backup must be carried out in isolated environments from the one in which the ransomware is infected, avoiding secondary attacks. Furthermore, as discussed within the premises of preparing the recovery plan, the process must be triggered based on the level of priority linked to the service or system affected.

There are two approaches to restoring systems: repairs or rebuilding. Fast restoration of the parts impacted by the attack, not recommended, is a cheap and agile option. However, there is no guarantee that the malware has been completely removed, exposing the network infrastructure to a possible secondary attack. On the other hand, rebuilding each service or application on the network is a best practice, ensuring the complete elimination of ransomware. Unfortunately, it takes more time for IT teams to work and can impact the organization's production processes.

Post-recovery assessment and learning

After responding to the incident and recovering systems and data, conducting a digital forensic investigation at the data and information level is essential to identify whether only local encryption occurred in the attack process. If signs of exfiltration are detected, the competent authorities must be informed, and involved customers must be notified.

Digital forensics enables the assessment of the vulnerabilities that allowed the attack to happen in the first instance. Subsequently, implementing best cybersecurity practices must apply this knowledge in the vulnerability correction process. At this point, the prevention efforts presented in this document are valid according to the identified case.

Manage risks

The response and recovery plan for ransomware incidents must include risk management and a ransom payment policy. Thus, the partakers involved must establish solid guidelines to define whether or not the ransom payment will be executed. Note that the recommendation is to avoid paying the ransom for the following reasons:

- Payment does not guarantee that the attacker will hand over the decryption means
- Payment reinforces the criminal practice
- Experience shows that not all encrypted files are always reconstructed
- There is no guarantee that the attacker will stop the extortion process after the first payment. If data exfiltration occurs, there is the possibility of a second ransom demand
- Payment is no guarantee that the attacker will preserve the information and unpublish it.

However, the organization must map its technical capabilities and, during a ransomware incident, define the chance of recovering systems, data, and information. In addition, a tradeoff between the data and information sensitivity level in the attacker's possession and the impacts on the organization's business must be established. These factors influence the decision on whether to pay the ransom.

The possible approaches must be defined if the organization decides to pay the ransom. For example, the negotiator's figure, the value the company is willing to pay, and the means of accessing cryptocurrency for payment.

About the CxSC Telecom

The Cyber Security Center (Centro de Segurança Cibernética do Inatel, CxSC Telecom) is the cyber security research center of the National Institute of Telecommunication – Instituto Nacional de Telecomunicações, Inatel – located in Santa Rita do Sapucaí, MG, Brazil. The CxSC encompasses different areas of activity such as education, certification, training, applied research, and services related to cybersecurity and related topics. Created in 2020, the CxSC aims to develop cybersecurity in the context of Brazilian society. The center relies on research work by Inatel professors and specialists. It also has partnerships with companies such as Huawei, Sikur, and other research institutes such as IMREDD (Institut Méditerranéen du Risque, de l'Environnement et du Développement Durable).

Acknowledgment

This work was developed with information and opinions from several people and companies in the telecommunications sector. Inatel appreciates all the information received and, in particular, the support and contributions from Huawei, which always encourage the initiatives of the Inatel Cyber Security Center (CxSC Telecom).

HUAWEI

24 ANOS
NO BRASIL PARA O BRASIL

CxSC Telecom
Centro de Segurança Cibernética

Inatel