GATEWATCHER

Ransomware Practical Guide_

Practical advice on how to prevent and respond to ransomware attacks.

*Summary_*

GLOSSARY_

*Ransomware_*

> Malicious software that infects connected devices. The data on the computer system is encrypted, making it inaccessible to the legitimate user. The user is typically faced with a ransom demand in exchange for the decryption key needed to restore access to their data.

*Phishing_*

> Maneuver not of hacking, but of manipulation and deceit designed to induce individuals to disclose confidential information to a third party. The tactic aims either to steal personal data or to install malicious software on a victim's device by impersonating a legitimate authority.

*Pentest_*

> Computer system security evalution with the goal of detecting and correcting potential vulnerabilities. The process involves simulating a cyber-attack to identify weaknesses and apply corrective measures to enhance protection.

*Encryption_*

> Process of securing data through cryptographic techniques that transform information into a format that is unreadable and unalterable using an algorithm. Only individuals with the decryption key can retrieve or alter this data.

*Ransomware as a Service (RaaS)_*

> Distribution model for ransomware in which cybercriminals rent or sell ready-to-use access to other attackers. This allows them to conduct more or less sophisticated attacks without needing to develop their own tools, services, or infrastructure.

*Malware-as-a-Service (MaaS)_*

> A distribution model for malicious software in which cybercriminals rent or sell ready-to-use access to other attackers. This enables them to conduct attacks of varying sophistication without having to develop their own tools, services, or infrastructure.

*Artificial Intelligence (AI)_*

> Logical and automated process generally based on an algorithm capable of performing well-defined tasks. According to the European Parliament, artificial intelligence constitutes any tool used by a machine to «reproduce human-related behaviors such as reasoning, planning, and creativity». AI specifically encompasses:

- Machine learning approaches,
- Logic-based and knowledge-based approaches,
- Statistical approaches, Bayesian estimation, and search and optimization methods.

(Source: European Union).

*External Remote Services_*

> Refers to computer services that are accessible remotely from an external network, such as cloud servers, online storage systems, or applications hosted on external servers. These services are frequently utilized by businesses to access IT resources from various geographic locations or to provide online services to their customers.

*Valid accounts_*

> Legitimate user accounts that have been compromised by cybercriminals to conduct malicious activities such as network infiltration and to carry out attacks like financial fraud or data breaches.

*Zero-Day_*

> Security flaw in software or a computer system that is discovered before the software developers have had a chance to correct it.

*Exploit Public-Facing Application_*

> Attack targeting publicly accessible software applications, such as web servers, mobile apps, or online services, by exploiting known security vulnerabilities or zero-day vulnerabilities to compromise the security of the application and gain access to sensitive information or take control.

*Drive-by compromise_*

> Attack technique used by cybercriminals to infect users' computer systems unknowingly when they visit compromised or malicious websites. This technique often exploits vulnerabilities in web browsers or plugins to install malware on the victims' computers without their consent.

*NDR_*

> Network detection and response (NDR) products detect abnormal system behaviors by applying behavioral analytics to network traffic data. They continuously analyze raw network packets or traffic metadata between internal networks (east-west) and public networks (north-south). NDR can be delivered as a combination of hardware and software appliances for sensors, and a management and orchestration console in the form of an on-premises software or SaaS.

*CTI_*

> Cyber Threat Intelligence (CTI) is the activity of collecting, analyzing, and transforming raw data into actionable intelligence to identify, understand, and mitigate threats in cyberspace. By using various sources such as open-source intelligence, social media, human and technical intelligence, as well as analysis of the deep and dark web, CTI enables defenders to make informed decisions to mitigate harmful events and protect organizational assets.

01

RANSOMWARE: the most critical cyber threat today_

Ransomware is a major concern of all business security managers. It has been the most widely observed and one of the most critical cyber threats in recent years.

Ransomware is a type of malware that aims to prevent the use of a terminal (workstation, application server, backup unit) or to render files inaccessible. Encryption is used to prevent the user from opening the files in the majority of cases. Victims, whether an individual or an organization, are asked to pay a ransom within a specified time, usually in cryptocurrency in exchange for releasing the computer or files.

Although the first security incident involving a ransomware took place in 1989, a considerable acceleration was observed from 2013 with the advent of cryptocurrency as a payment method

*The scale of the ransomware phenomenon in several figures_*

ATTACK AND INFECTION RATES_

> **75 % of organizations were affected by ransomware attacks** in 2024 *(Veeam - Data Protection Trends Report 2024).*

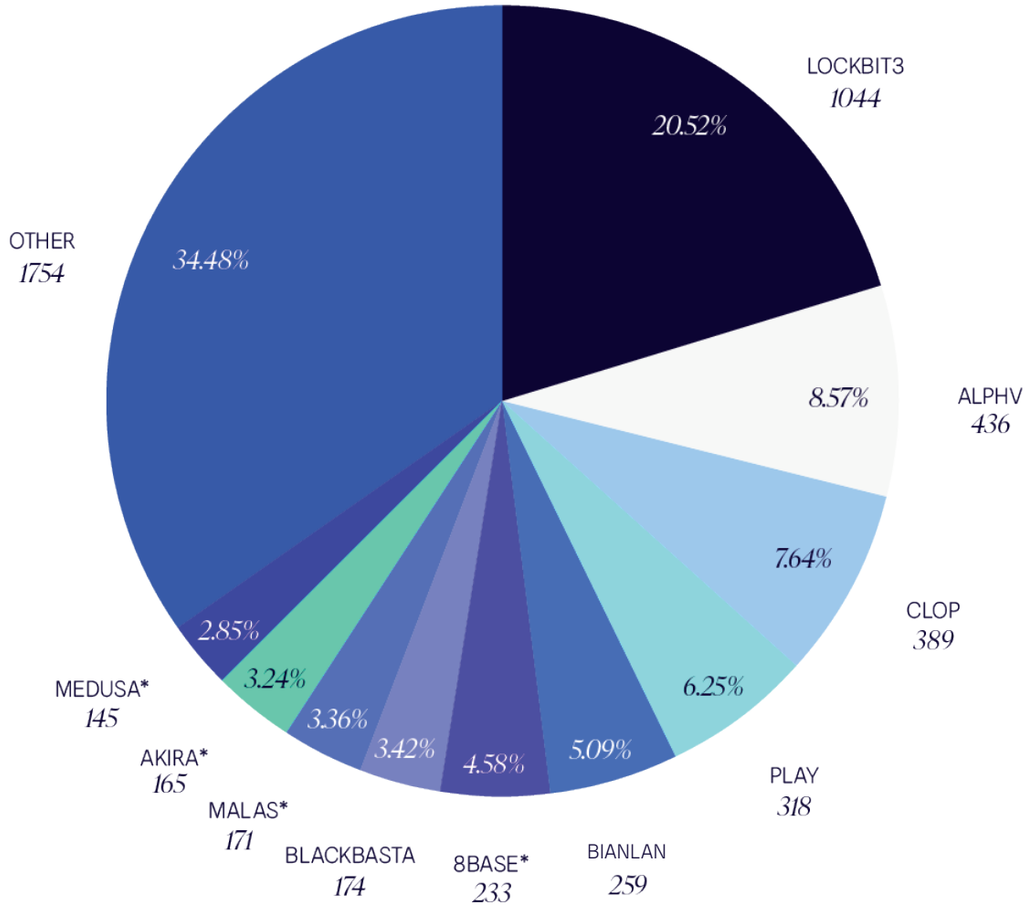
> Ransomware is involved **in 24 % of attacks** *(IBM Cost of a Data Breach 2023).*

ATTACK VICTIMS AND ATTACKERS: ID_

> At least **25 new ransomware groups emerged in 2023.** The most active groups in 2023 were Lockbit, BlackCat (ALPHV), CL0P, PLAY and Bianlian and we have identified many groups during the professionalization phase in 2024.

> The United States, the United Kingdom, Canada, Germany and France are the **top five countries affected by ransomware**.

> **The healthcare sector remains the most affected**, with 249 cases reported in 2023, followed by the education and government agency sectors (Cloudwards).



Top 10 ransom group (OSINT)

FEATURES OF ATTACKS_

> **The most common infection vectors** involve the exploitation of unpatched vulnerabilities (32 % of cases), followed by use of compromised credentials (29 % of cases) and sending emails malicious emails (23 % of cases) *(Sophos, 2023).*

> Only 47 % of victim companies found **their data and services intact** *(Cybereason, 2022)..*

FINANCIAL CONSEQUENCES_

> **The average ransom amount is USD 850,700 (Rapid 7- Coveware Report 2023)** *(Rapid 7- Coveware Report 2023).*

> Apart from the ransom, the average total cost of a ransomware attack is estimated to be $5.13 million on average, up 13% year-on-year *(IBM - Cost of a Data Breach 2022).*

BEHAVIOUR OF VICTIMS_

> **80 % of companies that paid a ransom suffered subsequent attacks, 40 % of whom ended up paying a second time** *(Cybereason, april 2022).*

> **34 % of cyber insurance claims were related to ransomware during the first half of 2022** *(Corvus Risk Insights Index).*

*The impact of a ransomware attack is often significant due to the multiple factors involved_*

> **Partial or even complete shutdown** of activities and production.

> **Direct loss of turnover or activity** in the long term.

> **Cost involved to rectify** and for disaster recovery efforts.

> **Long-lasting damage to reputation** and brand image (customers, prospects, investors).

> **Human impact** (stress and demotivation of overburdened teams)

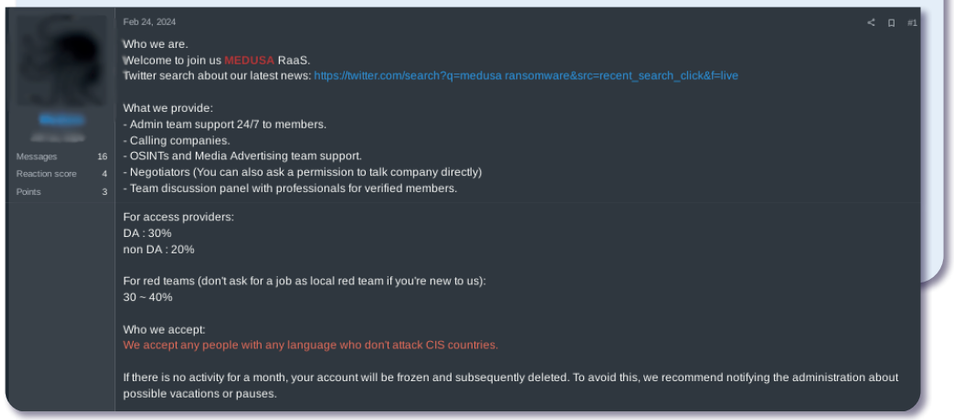
Ransomware causes an average of **18 days of service interruption** before the issue is resolved, which can lead to cash flow problems for the most fragile companies or even liquidation. Ransomware infamously contributed to the first reported death related to a cyberattack in 2020. At University Hospital in Düsseldorf, Germany, the facility was paralyzed, leading to the inability to provide any kind of treatment to patients, including performing surgeries. As a result, a woman who needed urgent care was transferred to another hospital but did not survive.

Recent developments in ransomware

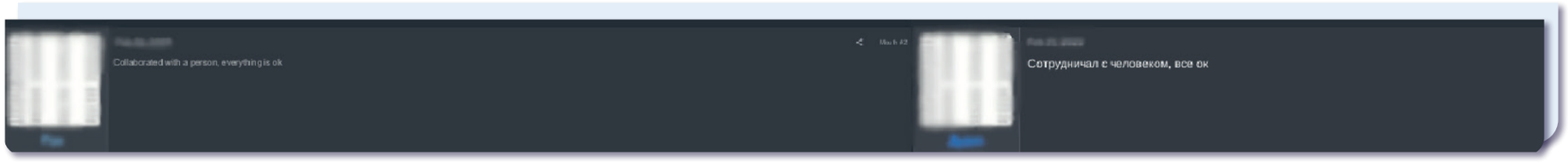
For cybercriminals, ransomware represents a quick and effective way to generate revenue. The rise of ransomware-as-a-service (RaaS) now allows hackers to rent pre-configured ransomware solutions to other criminals. This "turnkey" approach allows even individuals with little technical skills to easily access sophisticated tools and networks of potential victims, thus facilitating lucrative attacks. As highlighted in our semi-annual report on cyber threats from July to December 2023, RaaS has become a truly growing industry, particularly on the darknet. Without any complexes, it is structured by taking the example of private sector companies. From planning an attack in just a few clicks to actually carrying it out, users can benefit from customer service and check satisfaction reviews. This trend demonstrates a clear desire for organization and professionalization within cybercriminal groups.

An example with REvil Un exemple avec REvil

Also known as Sodinokibi, this group popularized ransomware as a service (RaaS). It is particularly famous for its large-scale attacks and its double extortion strategy. In 2021, REvil hit JBS USA and Kaseya Limited, disrupting JBS's operations and forcing the company to pay $11 million, while the attack on Kaseya affected more than 1,000 customers. In early 2022, the Russian Federal Security Service announced that it had dismantled REvil and indicted several of its members.



Diversity of services offered by a RaaS group to its affiliates



Feedback from a RaaS customer/affiliate

Contrary to popular belief, **ransomware attacks do not discriminate. Small and medium-sized businesses** are just as targeted as large organizations. These cybercriminals, devoid of any ethical code, attack all structures without any exception, whether small family businesses, hospitals, schools or multinationals. No one is spared from their greed.

The most high-profile attacks will often opportunistically target public services which can less afford downtime due to the number of users impacted. This partly explains the dynamics of ransomware attacks against hospitals and other health organizations, as we have seen in France particularly since 2020.

The implementation of a ransomware prevention and attack remediation strategy (PRA-PCA in French) must become a priority. In France, critical organizations (Operators of Vital Importance (OVI) and Essential Service Operators (ESO) that play a vital role in the economy or defense of the country, are legally obliged to protect against and reduce the impacts of ransomware.

Recognizing ransomware: how far does extortion go?

One of the most notorious ransomware is WannaCry. In 2017, this virus exploited a flaw in the international accounting software supply chain, resulting in the simultaneous paralysis of hundreds of thousands of computers worldwide. A real-life "pandemic" hostage situation, the attack spread in mere days to computers running Microsoft Windows.

While ransomware can be extremely lucrative for cybercriminals, it can have devastating repercussions for victims. Apart from ransom demands, some attacks aim to inflict irreparable damage on computer systems, leading to considerable operating losses and tarnishing the reputation of affected companies.

Ransomware can be classified into two main categories: Crypto ransomware (encryptors) and Locker ransomware (blockers). Apart from these main categories, there are other closely related and intrinsically functional subcategories, such as scareware and leakware, which, like insidious little brothers, increase the pressure on victims and the success rate of attacks.

Main categories

« CRYPTO » RANSOMWARE

Crypto ransomware encrypts victim data, rendering it unreadable without a decryption key. This data is released by the cybercriminals holding it after the ransom has been paid. This type of ransomware aims to make data inaccessible while allowing the system to continue functioning, creating pressure on the victim to pay in order to regain access to their essential files.

Example:

CryptoLocker is often considered as marking the start of the modern era of ransomware. Distributed via a botnet, this malware was one of the first to use strong encryption to lock users' files, demanding a ransom for their decryption. CryptoLocker extorted approximately $3 million before being taken down by international law enforcement in 2014. Its success inspired many subsequent variations, such as WannaCry, Ryuk and Petya

« LOCKER » RANSOMWARE

Locker ransomware, or blockers, completely paralyzes access to the victim's device, rendering it inoperable, leaving the victim no choice but to pay the ransom to regain access.

Example:

BlackCat (or ALPHV, 2023) – Renders critical systems unusable until the ransom is paid.

Derived categories

SCAREWARE

Scareware warns users that a virus or malware has infected their device, tricking them into paying to fix an often-nonexistent issue. This technique plays on users' fear, pushing them to pay to eliminate an imaginary threat.

LEAKWARE (DOXWARE)

Leakware, or doxware, threatens to release sensitive information if the ransom is not paid. This method exploits fear around shame or legal consequences, pressurizing victims to pay to prevent their private data being made public.

However, certain groups started to deviate from this approach in the second half of 2023, opting either for a return to so-called "simple" or "encryption-less" extortion, or for even more aggressive triple or quadruple extortion tactics.

*Detecting ransomware: the cat and mouse game_*

While recognizing ransomware is straightforward once action is taken, detecting it beforehand is much more difficult. Hackers systematically camouflage the different components of their attack in order to circumvent the defenses in place.

Two factors underlie the challenge associated with ransomware:

> The silence that precedes file encryption,

> and the multiple entry points that they can use to be installed on the victim's equipment.

An effective defense system must be able to simultaneously monitor several entry points (email servers, etc.), as well as be able to detect exploits that attackers use to download the malware on to the victim's device that will execute the encryption. The exploits, the software and its attempts to communicate with the outside world are all elements that indicate the presence of the ransomware before its malicious phase.

Security researchers and organizations such as the CISA are always on the lookout for flaws in attackers' methods, working tirelessly to develop decryption solutions. Possibly the best-known initiative is ***No More Ransomware***, supported by Europol, the Dutch police and other actors. This platform offers more than a hundred decryption tools, such as the one developed by Avast for Akira ransomware, which came out during the summer of 2023.

Certain cybercriminal groups have revised their strategies in response to these efforts. Rather than risk being detected by trying to encrypt as much data as possible, they are now opting for a faster method involving the mass exfiltration of information followed by threats of disclosure. This so-called ***double extortion*** approach maximizes the pressure on victims while minimizing the risk of interception.

And the attackers are extremely intrepid. They like thinking outside of the box and playing with their victims. The latest iteration, triple extortion ransomware, is a real win for cybercriminals, who encrypt data, exfiltrate it to expose it, and add a third threat. This third threat can take the form of a DDoS attack or intimidation of the victim's customers, employees and stakeholders to obtain additional ransoms. By diversifying attack vectors, hackers strive to startle, panic, and make their victims pay up.

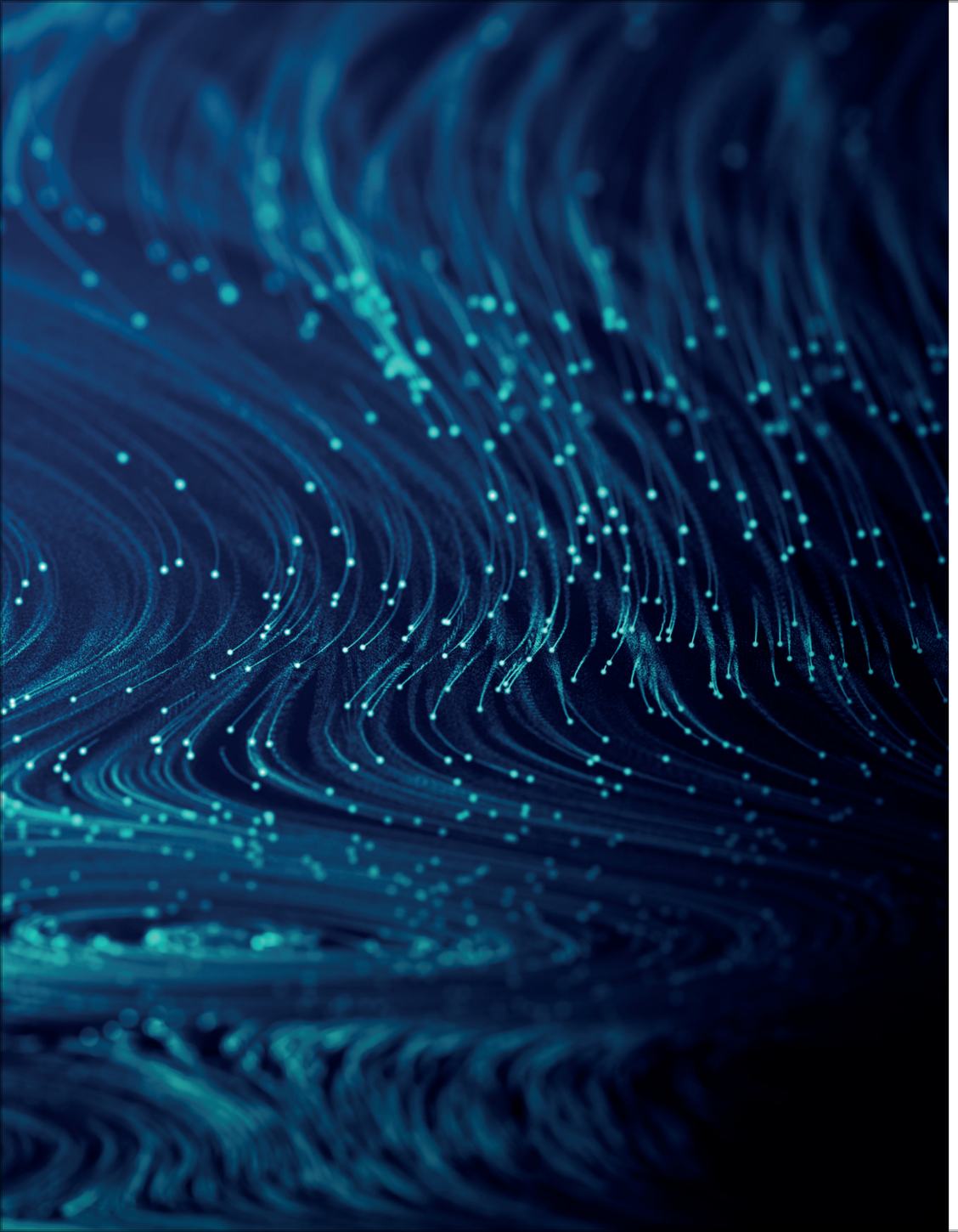
Take the case of Hunters International, a group of cybercriminals that took over after the dismantling of the Hive group. During the attack targeting the Fred Hutchinson Cancer Research Center, hackers directly contacted patients affected by the data theft, offering to erase their personal information in exchange for payment in the event of public disclosure. However, they didn't stop there: they threatened these patients with swatting, a dangerous practice which consists of involving the police under false pretenses in a private home.

Traditional

Double extortion

Triple extortion

Functional evolution of *Ransomware attack_*



02

PREVENTING RANSOMWARE: Improving your security hygiene _

Nine out of ten ransomware attacks are preventable yet despite the rise in threats, many organizations continue to ignore essential security measures. While clever and inventive in their approaches, cybercriminals often rely on proven techniques. Understanding and recognizing these patterns can allow businesses to not only prevent attacks, but also detect them quickly and limit damage. Adopting thorough digital security practices is crucial to building resilience against these pervasive threats.

*Employee awareness_*

The majority of ransomware attacks are triggered by employees opening an attachment or visiting a compromised website. Cybercriminals have become more professional over time, where these attacks were easily recognizable just a few years ago, such as sentences containing poor syntax, obvious malicious email subjects or suspicious URLs. Today, this is no longer the case.

Artificial intelligence (AI) now plays a crucial role for both attackers and defenders and has become an essential and mighty ally. Cybercriminals use generative AI in particular to automate and refine their attacks, such as for making phishing emails more sophisticated and difficult to detect. AI algorithms can analyze large amounts of data to identify exploitable vulnerabilities, making attacks more targeted and effective. Hyper-connectivity, which is supposed to simplify our daily lives, paradoxically increases our vulnerability to attacks, particularly ransomware. Generative artificial intelligence can enhance these threats by identifying vulnerabilities in target systems and adjusting attack strategies in real time to bypass defenses, making attacks even more formidable.

Defenders must constantly adapt their methods during this dynamic game of cat and mouse faced with ever more ingenious attackers. Each new connection represents a potential point of attack, further complicating the security systems task.

HOWEVER, CERTAIN BASIC HYGIENE RULES REMAIN EFFECTIVE TO ENSURE PREVENTION

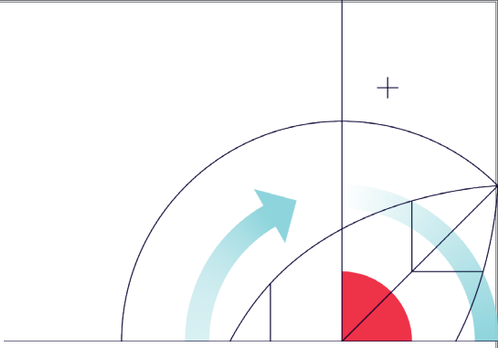
> **Not opening any attachments** from emails received from unknown senders.

> **Being aware that even known senders can send corrupted files by accident.** Therefore, taking a cautious approach to any attachments received by email.

> **Examining a link carefully before clicking on it.** A URL may sometimes seem correct at first glance. When it is checked more carefully, it may contain one or more syntactic or domain name errors that tell you that this is not a legitimate website and should raise red flags.

> **Never sharing your passwords** by email, chat or phone.

With proper training, employees can become vigilant scouts, helping to detect attacks early. Despite being often considered the weak link in the face of ransomware, effective awareness can turn individuals into valuable assets in the strategy to combat these cyber threats. Proper preparation not only allows staff to identify the warning signs of an attack, but also respond appropriately to minimize risks and impacts.



*Improving your backup and disaster recovery strategy_*

If your data is encrypted by a ransomware attack, backing it up in advance is your best strategy, but only when you host your backup externally.

SEVERAL THINGS ARE KEY WHEN IT COMES TO BACKUP:E

> Determining the frequency of backups

IT operations and information security teams should work together to define the regularity of backups. This decision will determine the amount of data potentially lost in the event of an attack. Performing backups every four hours, for example, means that any data lost will be limited to four hours.

> Testing backups regularly

It is essential to regularly check your backups to ensure that you can restore your files without problems or data loss. These tests also allow you to evaluate the time needed to become operational again following a cyberattack

> Preparing for double extortion

Cybercriminals are increasingly using double extortion tactics, where they not only encrypt your files, but also steal your data by threatening to publish it online. Within this context, having an external backup is not enough, as data can still be exposed.

> Protecting the backup administration console

Ensuring that your backup administration console is properly protected. Hackers can have a complete view of your data organization and easily locate sensitive information if they manage to access this. An unsecured console can give hackers direct access to your most valuable data.

> Physically disconnecting storage media

Physically disconnect your storage media from the network after each backup. If backups remain permanently connected, they risk being encrypted by the ransomware along with the rest of your data.

Securing remote access_

The most common entry points for attackers are **BYOD** (Bring Your Own Device) **laptops, VPN misconfigurations and vulnerabilities, and Remote Desktop Protocol** (RDP). The global shift toward remote working due to COVID-19 has only increased this risk. More and more people are working from home on devices that are not always properly protected. Remote desktop applications are one of the favorite attack vectors for hackers and are an ideal way to introduce ransomware into an organization. Hackers attempt to steal username/password combinations or perform brute force attacks to crack weak passwords. Protection against these attacks consists of forcing users to generate strong passwords (and changing them regularly), or of implementing multi-factor authentication (MFA) mechanisms. Other best practices include blocking IP addresses that fail after multiple login attempts (usually a sign of a brute force attack), restricting remote access when possible, or using a firewall to limit RDP access to a range of IP addresses or specific IP addresses.

Keeping your software up to date and patched_

As soon as any vulnerability is made public, hackers are on stand-by, ready to take pounce on it. Ransomware creators love unpatched software, showing how important it is to always update all software. As soon as a patch is available, ensure that it is installed on all devices connected to the network, whether they are your employees' computers, or the cloud services you use.

It is crucial to uninstall any software that is no longer supported by its vendor or plan its migration to more modern solutions. Unmaintained software represents an easy target for cyberattackers because no new vulnerabilities will be patched by the publisher. Switching to supported and regularly updated software will better protect you against threats.

Maintaining an updated inventory of your application fleet is essential for keeping all software up to date: knowing what software is installed on servers, terminals, communications infrastructure, etc. This inventory should also include the operating systems running on the devices.

*Some additional measures_*

As previously noted, hackers are going after known patterns. A certain number of preventive measures can therefore be implemented to slow down an attack, or to detect it at an early stage.

TO DO SO, TRY OUTSMARTING THE HACKER

> **Setting up fake administrative accounts,**

means you will likely know someone is compromising your systems if anyone tries to use these accounts.

> **Placing decoy files in strategic locations in the information system.**

An alarm should be raised if a hacker writes or reads these files.

> **Creating a “sacrificial network share” involving the use of old, slow storage media containing thousands of small files as a honeypot for hackers.**

Ransomware typically progresses through network shares in alphabetical order. Placing the sacrificial network share on an A drive allows you to save threat response time by delaying the encryption of your business data and detect malicious activity more quickly.

“Protection against ransomware is a matter of life and death in hospitals and healthcare facilities.”

Guilhèm Savel - CISO, Bordeaux University Hospital

Healthcare institutions are particularly vulnerable to cyberattacks. Not only do they store a multitude of sensitive personal data, their equipment also increasingly relies on computer processing and is permanently connected to the internet. HCA Healthcare, Regal Medical Group & NHS are only a small number of public and private health institutions, regardless of size, targeted by cyberattacks in recent years. The health and medico-social sector represented 42 % of cybersecurity incidents in Europe between 2021 and 2023. This is explained by the combination of two factors: a certain delay in terms of cyber security of its activities and high-value sensitive data. In fact, at a time when technology and automation have colonized many parts of the “health trail” such as electronic patient records (EHR), medical administrative management, economic and financial management, connected medical devices (CMD) and telemedicine systems, cybersecurity has become an essential pillar guaranteeing the security and confidentiality of critical data. Considered the “new black gold” of the 21st century, they pose significant dangers due to their frenetic exploitation and have become prime targets for cybercriminals.

« In case of infection, hospitals and other healthcare facilities are currently facing a double crisis as all staff are already strained due to COVID-19, and the last thing they need is ransomware attacks. It is essential to be prepared and have a crisis plan in place», says Guilhem Savèl, CISO from Bordeaux University Hospital, in the podcast «In the eye of cyber» conducted by Gatewatcher. This observation has pushed the sector to work on several fronts:

THIS OBSERVATION HAS PUSHED THE SECTOR TO WORK ON SEVERAL FRONTS:

> **Educating all staff to be careful not to open email attachments** or click on suspicious links. End users are the first level of defense against cybercrime. Apart from training new staff members and the regular distribution of awareness-raising letters and videos, the major media attention on cybercrime constitutes a good reminder for all staff.

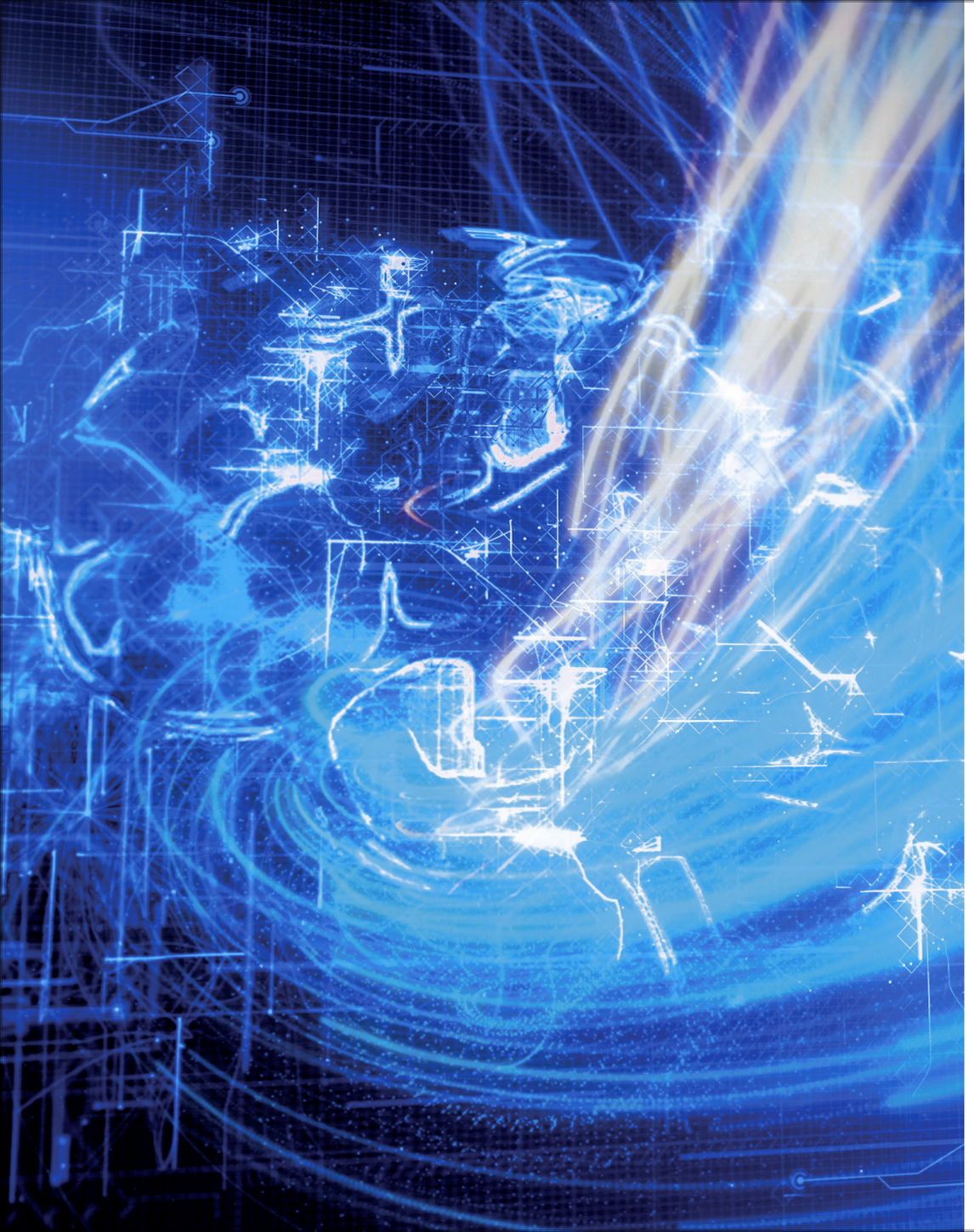
> **Establishing crisis plans:** patient care must continue even if a hospital is hit by a cyberattack. This is why hospitals have implemented procedures that allow doctors and nursing staff to work in degraded mode with as little IT support as possible. With syringes, paper and a pen, vaccinations, blood tests, infusions, and a significant number of treatments can still continue. Specific measures must be taken regarding biomedical equipment connected to the internet for the analysis of test results. The crisis plan must also include a Disaster Recovery Plan (DRP) once the cyberattack has been warded off and the network is restored.

> **Investing to better defend yourself:** not only by making the most of the capabilities of existing firewalls and antiviruses, but also by migrating to the latest generation technologies that allow early detection and remediation of cyberattacks.

Health action on the front line: an inspiration for all areas of activites

Many hospitals, underinvested in IT and cybersecurity, have realized the issue and are catching up. 110 of them now work in close collaboration with the French Cybersecurity Agency (ANSSI) and the Digital Health Agency, which helps them with customized audits to detect vulnerabilities, for example in messaging systems and Internet access. The fact that French authorities prohibit hospitals from paying ransomware perpetrators could also make cybercriminals realize they are attacking the wrong target.

In a constantly evolving legislative landscape, as with the imminent implementation of the European directive NIS2, all Operators of Vital Importance (OVI) and Essential Service Operators (ESO), ultimately Essential Entities (EE), are now also required to implement cyber crisis management. The extension of the criteria of the NIS2 directive to include these essential (EE) and important (IE) entities meets both cyclical and structural needs, particularly in the health sector. This European regulatory framework strengthens the level of security by imposing common rules, which is beneficial for combating cyberattacks. Certain solutions make it possible to combine obligation and opportunity, thus offering increased protection. Olivier Pedurand, CISO of SIB (leading cooperative player in digital technology serving the health and public sectors in France) recognizes within the context of success story feedback with Gatewatcher that “the regulatory framework makes it possible to positively evolve the level of security. Having a European constraint makes it possible to protect the resources allocated to the ISS”.



03

8 URGENT ACTIONS to be taken following an attack _

The preventive measures detailed in the previous chapter are essential to protect against ransomware. We are going to discover the tools and solutions that complement this basic protection in the following chapter. Neglecting these measures or use inappropriate tools puts you at risk of becoming a victim of ransomware.

Here is what you need to do after an incident to limit the damage and restore your systems.

1 Knowing your enemy

As soon as you notice that an attack is in progress, try to identify the ransomware variant that has infected you as quickly as possible. Each ransomware has a unique way of infecting your files. Understanding its specific capabilities will help you solve the issue. For some encryption tools, decryption software are available, enabling you to avoid paying a ransom or losing files. Additionally, online tools like ID Ransomware can assist you in identifying the specific strain of ransomware that has attacked you.

2 Isolating infected IS elements

If you notice that a device, server, desktop or laptop PC has been infected, disconnect it from the network immediately. This stops the virus from continuing to spread from that specific device. It is also essential to isolate the network segment where the infected system is hosted from the rest of your fleet.

3 Identifying damage

Time is of the essence whenever the ransomware is running. Try to find out the scale of the attack, the amount and value of the data compromised as quickly as possible. Determine which device was infected first, and which shared drives or network segments it is connected to. Check which external hard drives or cloud storage systems are connected to the infected device. This will help you determine how the ransomware is spreading in your network.

4 Communicating

If containing the damage is the most important task to accomplish, internal communication is just as crucial. If your organization has implemented a crisis communication plan for security incidents, follow this plan closely. Ensure that all concerned employees are well-informed and coordinate your actions within the crisis management. A strong and united internal communication is the core of the crisis response; if it is not coherent, the external communication will suffer.

5 Contacting the authorities

In the event of a ransomware attack, immediately contact the relevant authorities such as NCSC, your CERT, CISA,... Their expertise is crucial for assessing, containing the attack, and recovering the data. Reporting the incident and filing a complaint helps prevent future attacks and contributes to the fight against cybercrime. Also, remember to notify your cyber insurance provider. Finally, be prepared to communicate transparently and organized externally as needed.

6 Scanning infected machines and eradicate ransomware

Once you are sure that you have contained the ransomware attack, you can begin removing the infection. The priority objective is to find patient zero. Also ensure that no malicious residual files are still active in the system, as they could trigger a new attack

7 Checking and restoring your backup

As backups are also often the target of a ransomware attack, simply installing the most recent backup is not enough. You need to ensure that the backup itself is not compromised. Check if your backup is stored on is readable and correct. You should only restore backups if these conditions are met.

8 Monitoring and mastering your resumption of activity

Once all of the ransomware is removed and all files and drives have been restored, it is time to find out how the ransomware infected your system. What was the first entry point? How did the malware get in? Was it due to human error or did your protection fail due to software vulnerabilities that were not resolved? Once the root cause has been determined, take the necessary steps to close the security gaps. It may also be time to educate your employees about security.

WHAT IF SURRENDERING TO BLACKMAIL MADE THE PROBLEM WORSE?

It is advisable to never pay the ransom demanded (recommendation issued by the OFFICIAL CYBERSECURITY AGENCIES). In fact, while it may be tempting, this is a never a good idea as there is no guarantee that the situation will be resolved even if you do pay! In many cases, the money is collected but the server, responsible for distributing the decryption key, is ultimately no longer reachable, down or simply no longer exists. There are a number of considerations to take into account. Even if you pay, you are also not safe from a new attack by the same cybercriminal network a few weeks later. Furthermore, in a double extortion scheme, hackers may keep your data and ask you for money later, threatening to publish your data online if you do not continue to pay. Cybercriminals may also decide to sell the attack method or stolen data to other malicious actors. If you have purchased cyber insurance, ensure that all conditions are met before paying.

Typically, **paying a ransom is really the last action you should resort to.** Exhaust all other options first.

Besides the loss of personal income, **paying a ransom involves other lesser-known risks and consequence**s. First, giving in means encouraging cybercriminals to continue their activities. Every ransom paid funds more cyberattacks, creating a perpetual cycle of crime. By financially supporting these attacks, you indirectly contribute towards them increasing and becoming more sophisticated.

Secondly, **Paying a ransom may also attract other attacks**. Organizations that give in to ransom demands may be seen as easy targets and be attacked again, sometimes even by the same criminals.

Finally, **it helps fight terrorism and money laundering.** By refusing to pay, you are supporting global efforts to reduce the effectiveness and financial attractiveness of ransomware.

In short, **it is crucial not to surrender to the attemps at extortion** by cybercriminals and to instead focus on prevention measures, particularly any that developed here, to protect your data and your organization.

04

THE 5 MAIN QUESTIONS to ask yourself before choosing your protection_

There are many products available that can be used to prevent ransomware attacks or mitigate the consequences of an attack, making it important to ask the right questions in order to choose the right vendor to work with. We have listed several questions here that are a good starting point for building a list of vendors you are considering working with.

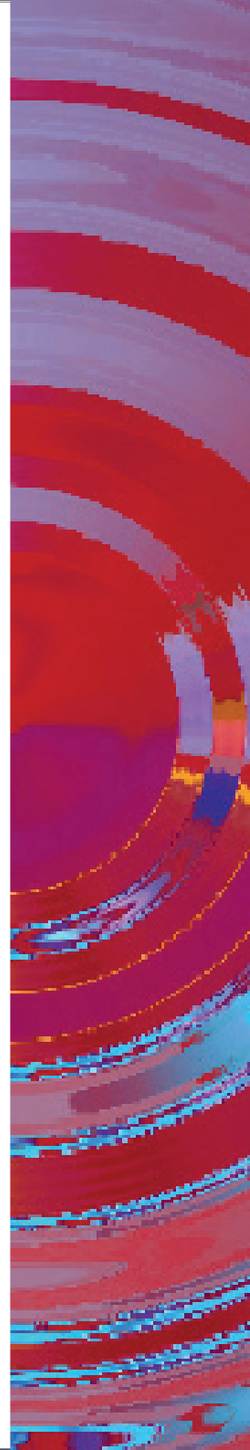
1 *Is your future protection modular?*

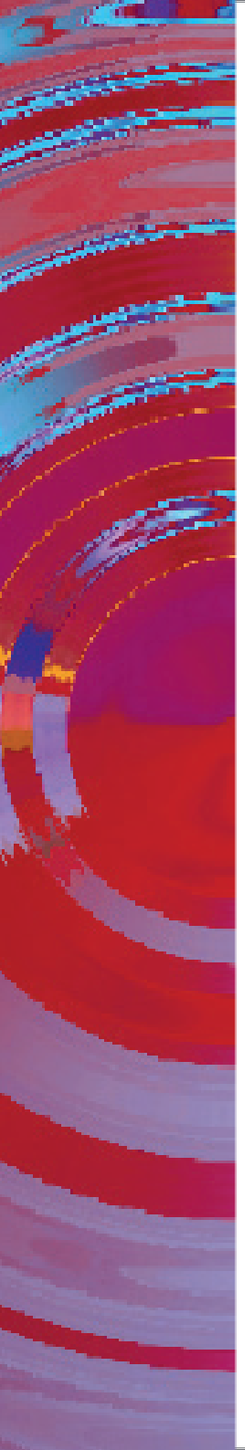
Cyber threats are constantly evolving. As cybersecurity solution providers improve their intrusion detection techniques, cybercriminals are also upgrading their tools. They are creative in finding new attack vectors, exploiting new vulnerabilities and learning from experience.

A ransomware attack consists of different phases, each of which evolves at its own pace. It is therefore important to check whether your cyber detection solution provider has modular products that can keep pace with these distinct developments.

2 *Do your security solutions share a common architecture?*

Vendors sometimes offer different products to address distinct issues in your security environment. Technology is evolving so quickly that vendors are sometimes slow to integrate their products and make them work together seamlessly. While these vendors have a modular approach, it can be difficult to integrate their products into your overall security strategy. If you encounter vendors that offer multiple products, ask them if their products are based on a common architecture. If this is not the case, be aware that the integration effort may be greater.





3 *Is your protection model technologically state-of-the-art?*

New threats emerge and existing threats evolve into new variants all the time. It is therefore extremely important for your ransomware tool provider to always use the most up-to-date defenses against these new attacks. Artificial intelligence and machine learning can adapt to new attack methods implemented by cybercriminals. Ask your potential supplier how they use them to improve their products.

4 *Do you have the right focus?*

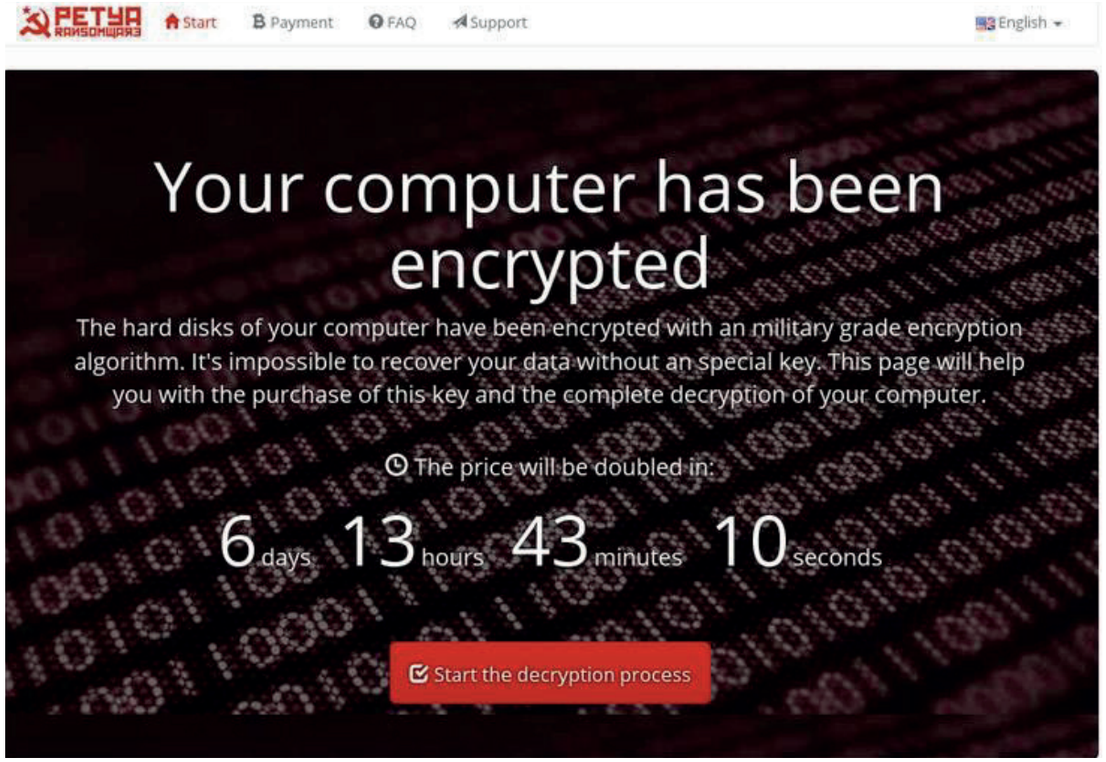
Ransomware is a very specific threat but generally carries a large arsenal composed of infostealers, cryptominers, etc. Effective detection and remediation therefore require specific knowledge. Test your potential suppliers against their specific objectives. Is ransomware their main concern or are they just putting an anti-ransomware label on an existing product? Only a true ransomware specialist is up to date with all developments in this specific area and can provide the right answers to meet this challenge.

Do you have partners experienced in this issue for its implementation?

5

Developing ransomware protection products is one thing, implementing them in your business is quite another. The provider who will implement the selected intrusion detection solution, should be familiar with your specific architecture, your data strategy, how you perform backups, etc. This is why it is important to check in advance whether they can implement and integrate this into your environment efficiently and on time. Do they have the right skills for its implementation? Are they familiar with your industry and its specific business requirements? Is it technically (and commercially) accredited by the software provider?

Choosing the right implementation partner is just as important as choosing the solution that will protect you against ransomware.



05

DETECTING RANSOMWARE BEFORE ITS EXECUTION?

The benefits of a proactive NDR

Machine learning coupled with threat awareness helps you stay ahead of ransomware. An NDR (Network Detection & Response) solution can autonomously identify new attack scenarios by automatically collecting and analyzing the presence of certain markers using algorithms. While ransomware attacks generally follow the same basic steps, the techniques used by the latest generations of ransomware cannot be detected by traditional static detection technologies.

How does NDR solution work?

An NDR type solution consists of a series of sensors positioned within an IT infrastructure in such a way as to provide visibility into all of the most critical communications, both internal and to or from the public network to an asset such as a laptop or a server. Positioned in bypass (mirroring), the sensors are invisible to cybercriminals and a ransomware attack will not be able to detect their presence.

These sensors are connected to a supervision server which in turn provides advanced analysis features while also supporting major operational activities such as keeping security policies up to date

Each sensor therefore sends the results in real time of a first level of analysis, particularly of a static nature supplemented with all communication metadata to the management server, which performs a detailed analysis by combining a set of engines based on different machine learning technologies.

In the event of an alert or suspicion, the management server immediately interacts with the customer's SIEM/SOAR or other security equipment such as an EDR solution, a firewall, a proxy, etc. This allows its rectification as early as possible but especially of a global nature, protecting the entire infrastructure as best as possible according to existing solutions.

AIONIQ: a proactive NDR response against ransomware and other cyber threats

In response to the rise of ransomware, Gatewatcher offers an NDR solution guaranteeing immediate improvements to the protection of its customers' infrastructures. AIONIQ offers robust and comprehensive protection for business information systems.

The modules within AIONIQ® are capable of detecting the elements specific to ransomware attacks before their execution: exploiting an initial access established on infected patient 0, network discovery attempts and possible exploitations towards critical servers (lateral movements), attempts to exfiltrate data taking place before the actual encryption. The platform's fine detection capabilities offers you the benefit of being able to react as early as possible, both on the purely preparatory aspect of these attacks as well as the detection of malware and therefore its execution.

> Ransomware Detection Engine

AIONIQ has a built-in detection engine specifically designed to track ransomware. Based on the analysis of SMB protocol, Ransomware Detect monitors all malicious uses likely to impact the different types of data available in your information system, particularly their encryption. This proactive monitoring allows for the rapid detection of ransomware attempts and enables intervention before significant damage occurs.

> Visibility and multi-vector detection

AIONIQ provides complete visibility into information system assets and users. This capability facilitates investigations and makes it possible to detect intrusions as soon as the first weak signals emerge thanks to intelligent contextual analysis. This proactive approach is essential for identifying and blocking intrusion attempts before they cause significant damage.

> Seamless Integration

The solution easily integrates with the company's existing ecosystem, maximizing the efficiency of operational security centers (SOC) without disrupting day-to-day operations. AIONIQ works seamlessly with security tools such as EDR, XDR, SIEM and SOAR, making it a flexible solution adaptable to various security environments.

> Prioritization and Threat Management:

AIONIQ simplifies alert management by prioritizing threats according to an evolving risk score based on the context of the information system. This allows SOC experts to quickly triage alerts and make informed decisions to remediate security incidents, reducing the workload related to false positives.

> Overall remediation capacity

AIONIQ enables comprehensive threat remediation by providing response capabilities spanning endpoints, users and perimeter protections. This includes detection of encrypted streams, a crucial feature for countering ransomware that uses encryption to hide its malicious activities.

> Flexibility in terms of implementation

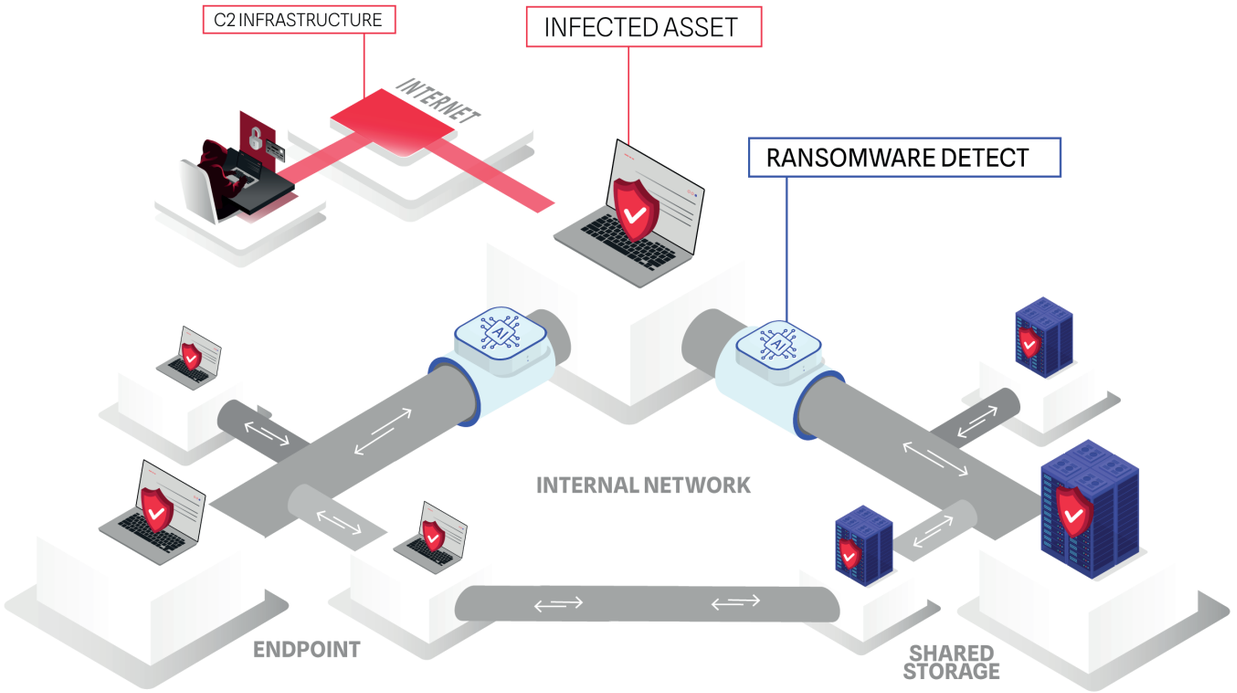
AIONIQ can be deployed on-premises or in the cloud, respecting the company's current security policies. This operating flexibility ensures constant protection adapted to the specific needs of each organization.

> By design Resilience and Security

AIONIQ strengthens resistance to corruption attempts and reduces the attack surface thanks to its hardened operating system and a «Secure by design» approach, which is crucial for preventing ransomware infections and other advanced threats.

> Reduction in Mean Time to Detection (MTTD)

AIONIQ significantly reduces the Mean Time to Detect (MTTD) threats. Swiftly detecting suspicious activity and effectively prioritizing alerts allows security teams to respond faster and more effectively, limiting the potential impacts of attacks.



Data theft and their encryption by ransomware are part of the three initial consequences that a business must deal with within the scope of a cyber attack

*In a nutshell_*

In a few words: Ransomware is not inevitable, and it is possible to protect against it. Regular and offline backups of your data are essential for a quick return to normal. In the event of an attack, the first step is to disconnect the infected machine or network segment from the internet and the computer network. Also, unplug healthy hard drives to prevent the encryption of intact files and isolate the computer to prevent spreading. Afterwards, promptly contact your IT department or cybersecurity professionals. Beyond data recovery, it is crucial to verify and secure the files before reinstalling them

There are other easy-to-implement common sense measures :

> Running software patches to keep systems up to date.

> Using anti-virus software and apply updates.

> Changing the default passwords for all access points.

> Using two-factor authentication.

> Identifying your critical data and defining a backup strategy accordingly.

> Training staff to recognize suspicious emails.

> Having a defined plan in case of attack.

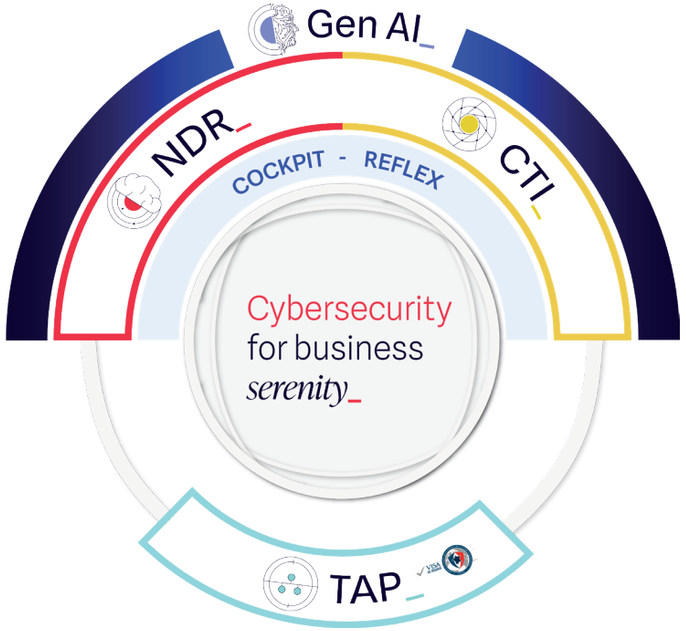
Strengthening your protection with an NDR type solution is a wise choice against ransomware and other cyber threats. NDR offers comprehensive defense against ransomware with early detection capability at a network level while integrating in a highly complementary manner with your existing endpoint protection (EPP, EDR, etc.). AIONIQ, Gatewatcher's NDR solution combines early detection, increased visibility, seamless integration, effective threat management, deployment flexibility, an advanced ransomware detection engine, and significant MTTD reduction. This solution allows businesses to immediately strengthen their security posture and minimize the risks associated with cyberattacks.

*Easy as_*

NDR_

CTI_

TAP_



ABOUT_

A leader in cyber threat detection, Gatewatcher has been protecting the critical networks of businesses and public institutions around the world since 2015. Our Network Detection and Response (NDR) and Cyber Threat Intelligence (CTI) solutions analyze vulnerabilities, detect intrusions and respond quickly to all attack techniques. Gatewatcher provides a real-time, 360° view of cyber threats across the entire network, in the cloud and on-premises thanks to the combination of AI with dynamic analysis techniques.