RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

RANSOMWARE ATTACKS, ALL CONCERNED

HOW TO PREVENT THEM AND RESPOND TO AN INCIDENT

CONTENTS

FOREWORD

All organisations, whether public and private, small or large, in France and elsewhere, now see their future in the light of digitalisation. Because the advantages of digital developments are considerable, companies and administrations ought to be able to rely on trustworthy and safe digital environments.

However, as digitalisation brings about new opportunities, the digital realm is also rife with risks. Indeed, the digital environment is a real playground for many malevolent actors, whose motivations are as varied as their profiles. A particular effort must be made with regard to one of the numerous threats: cyber crime.

Why? First of all, because such cyber attacks systematically have a dramatic impact on the victims; secondly, because it is often possible to reduce this risk to a residual level by raising awareness and implementing good practice.

At present, ransomware attacks are the most severe threat. They can have serious consequences on business continuity or even endanger the survival of the targeted organisation. Their scale, their frequency, and their sophistication are significantly increasing. France has organised itself to develop the appropriate responses to these new forms of cyber crime. A dedicated cyber unit has been established in the Paris Public Prosecutor's office to prosecute the perpetrators of cyber crime. Moreover, the responses go beyond specific cases themselves: France is striving to break the economic model of ransomware attacks, and drastically reduce the attackers' sense of impunity. This guide, aimed at businesses, but also local authorities, sets out the foundations of this policy.

This effort will only be meaningful if each organisation - from management to employees - takes up these issues and renews its vigilance, its cyber security investment priorities and its risk management, before it is too late.

Rather than seeking to create fear, the right way ahead is to inform, demystify, and empower, in order to positively influence decision-making.

Ransomware attacks are a current and growing trend, not only in France, but also worldwide. Because they are a serious threat, this guide translated into English aims at making our expertise and our recommendations available to a wider audience – we hope that you find it useful.

Guillaume Poupard, Director-General of the
French National Cyber Security Agency (ANSSI)

Catherine Pignon, Director for Criminal Affairs
and Pardons (DACG), Ministry of Justice

WHAT IS RANSOMWARE?

Ransomware is a type of malware designed to obtain payment of a ransom. Ransomware is one of the tools used by cyber criminals motivated by financial gain.

In a ransomware attack, the attacker reversibly renders the victim's computer or information system inoperable. In practice, most ransomware encrypts computer or system data using cryptographic mechanisms, making it impossible to view or use. The attacker then sends an unencrypted message to the victim offering to provide them with the means to decrypt their data, in exchange for the payment of a ransom.

TRENDS

The vast majority of ransomware attacks are opportunistic and take advantage of the low level of maturity of their victims' digital security. However, since 2018, there has been an increase in the number of such attacks by cyber crime groups who, after targeting individuals, are now attacking organisations with significant financial resources or particularly critical activities.

This trend brings ransomware into the category of so-called "Big Game Hunting" attacks due to the size of its targets. To extend its reach, attackers sometimes associate one or more other malicious programs (cryptominer, Trojan, etc.) with the ransomware. It then becomes possible to illegally use the hardware resources of the compromised equipment or to seize the data present on the information system. In a relatively recent phenomenon, some criminal groups now also combine the use of ransomware with threats to publish sensitive data. This increases the pressure on their victims to pay the ransom.

The attackers behind these operations usually have significant financial resources and technical expertise. Indeed, the level of sophistication achieved is sometimes equivalent to espionage operations conducted by states. Although the ransom amounts are usually hundreds or thousands of euros, those demanded during "Big Game Hunting" operations are consistent with the financial means of the victim entity, and can run into millions of euros. In addition, recent ransomware attacks have highlighted the danger of a systemic impact on an activity sector which, by targeting subcontracting or key companies in the ▶

sector, could lead to its destabilisation. These are known as indirect attacks, and they currently represent another notable trend.

The damage then goes far beyond the loss of data or the payment of a ransom, as victim organisations face many other consequences: production stoppage, drop in sales, legal risks (relating for example to the GDPR[1] if personal data is no longer accessible), damage to reputation, loss of customer trust, etc. The victim's activity is often disrupted or deteriorated as a result of these attacks. In the case of businesses, the survival of the company may even be at stake. Ransomware is a serious threat with potentially long-lasting consequences for both organisations and individuals, offering cyber criminals a highly profitable business model. It is essential to state and keep in mind that paying ransoms maintains this criminal activity and offers no guarantee of recovering the victim's data.

[1] General Data Protection Regulation.

THEY EXPERIENCED IT.
THIS IS THEIR STORY.

On 15th November 2019, on the eve of the weekend, an emergency services intern reported a problem with access privileges to a business application. Shortly afterwards, the internal IT services noticed that a large number of the CHU's workstations and servers were encrypted. The diagnosis came very quickly: it was ransomware.

Cédric Hamelin,
Deputy chief of information security officer (CISO),
Rouen University Hospital Centre (CHU)

During the night of 11th-12th October 2019, the group was the target of a violent ransomware attack. After waking up too early for a Saturday, I arrived to find a very busy news day, with the radio newsroom under maximum pressure, no longer having Internet access. "What can I do without a computer?" was the question on everyone's mind. In barely two hours, all hands were on deck!

Jérôme Lefébure,
Chief financial officer (CFO), member of the management board
in charge of support functions, M6 Group, media company

On 10th April 2019, on Wednesday night/Thursday morning, a ransomware attack forced the company to cut all Internet connections and application packages. As a direct consequence of the attack, activity ceased entirely for three days, while operation proceeded in degraded mode for a fortnight.

Laurent Babin,
CISO, Fleury Michon, food industry company

REDUCE THE RISK OF ATTACK

The following measures, taken from the French National Cyber Security Agency's Guideline for a healthy information system, *will prevent a ransomware attack from affecting the organisation or reduce the losses linked to such an attack.*

The main role of ransomware is to prevent the victim from accessing their data, usually by encrypting it. In the face of this threat, regular data backups are the priority measure to mitigate the losses associated with a ransomware attack.

Measures to significantly reduce the risk of infection and the propagation of ransomware throughout the information system include: patching and updating software and operating systems; updating anti-virus signatures; implementing a filtering policy on workstations; and disabling administrator privileges for users of these workstations.

Furthermore, the application of the principle of defence in depth to the various elements of the information system will reduce the risk of total unavailability. This principle involves, in particular, segmentation of the network by zones of sensitivity and exposure of the various elements of the information system, by limiting the privileges granted to users or by controlling Internet access.

Finally, raising users' awareness of the risks, assessing the possibility of taking out cyber insurance, preparing a response plan to cyber attacks and the associated communication strategy remain important actions to be carried out.

BACKING UP DATA

Regular backups of all data, including data on file, infrastructure and critical business application servers, must be made. Keep in mind that these backups can also be affected by ransomware. Indeed, more and more cyber criminals are looking to attack backups in order to reduce the victim's ability to retrieve their data, thereby maximising the chances that they will pay the ransom.

These backups, at least for the most critical ones, must be disconnected from the information system to prevent them from being encrypted like other files. The use of cold storage solutions, such as external hard drives or magnetic tapes, protects backups from a system infection and retains critical data for disaster recovery. In this respect, it is important to note that backup-less architectures[2] effectively protect against the destruction of isolated data, when this is due to a hardware failure. However, they do not protect against targeted ransomware attacks, since attackers attempt to encrypt the data on all servers.

[2] Method of using system photography (snapshots) to protect data without using traditional backup software.

KEEPING SOFTWARE AND SYSTEMS UP TO DATE

Unpatched vulnerabilities in OS and software can be exploited to compromise the information system or to facilitate the propagation of a malware. Updates including security patches are regularly made available by the solution providers. It is crucial to install them as soon as possible, following a clear process. Should this prove impossible, for business reasons for example, isolation measures will need to be implemented for the systems concerned.

Special attention must be given to the software installed on user workstations (web browsers, office suites, PDF readers, multimedia players, etc.). It is therefore important to anticipate hardware and software life cycles in order to keep them up to date.

Similarly, resources exposed on the Internet that are not updated (e-mail services, web hosting, extranet, etc.) are regularly exploited by attackers. It is therefore essential to pay particular attention to applying security patches as soon as possible.

In addition, keeping a permanent watch enables you to stay informed of the discovery of software and hardware vulnerabilities in the services used in your entity and the availability of patches. The CERT-FR website (*www.cert.ssi.gouv.fr*) can help you in this process.

USING ANTI-VIRUS SOFTWARE AND KEEPING IT UPDATED

The use of anti-virus software to protect against ransomware remains necessary today on exposed resources (e.g. workstations, file servers, etc.). These tools are no guarantee of protecting your entity from as yet unknown ransomware, but they can in most cases prevent compromise and avoid the encryption of your files. However, for these tools to be effective, it is important to update the signatures and the software engine frequently and to regularly check the entity's file storage spaces for known malware.

SEGMENTING THE INFORMATION SYSTEM

Without protective measures and from a single infected machine, the ransomware can propagate through your entire information system and infect most accessible machines. On a computer network without segmentation, attackers are likely to take control of a large number of resources and thus amplify the consequences of the attack. For example, they could have access to administrative functions or equipment reserved for administrators.

To limit the risk of propagation, one or more filtering devices should be put in place to allow segmentation between the network zones of the information system with varying levels of criticality (e.g. internal server zone, server zone exposed to the Internet, user workstation zone, administration zone, etc.).

Administration level segmentation can also be put in place to ensure that the highest levels of administration are difficult for attackers to reach.

In addition, connections between user workstations must be prohibited by default. An *ad hoc* configuration of the software firewall of workstations will prevent the flow of data between these workstations and reduce the risk of ransomware propagation.

> When the diagnosis confirmed the attack, things were very tense and our first decisions were 100% operational. Our on-call teams first cut the link between the attacker and our network by implementing isolation and segmentation measures.
>
> Jérôme Lefébure

LIMITING USER PRIVILEGES AND APPLICATION PERMISSIONS

A first good practice is to check that users are not administrators of their workstation. The installation of software and the unintentional execution of malicious code will then be impossible by default.

Another good practice consists of dedicating and limiting administration accounts on information system resources and setting up workstations dedicated to administration, without Internet access. In compromise scenarios, the attackers often try to access these privileged accounts. Actions to propagate ransomware within the information system are generally carried out using administration accounts, especially during "Big Game Hunting"-type attacks. The number of such accounts should therefore be limited to the strict minimum, and particular attention paid to the use made of them. These restrictions will prevent the ransomware from running or limit its ability to encrypt files.

To further reduce the risk of a ransomware attack, it is recommended to harden[3] the configuration of the following equipment: workstations, servers and the most common applications, especially those exposed on the Internet or processing data from the Internet. Among the additional security rules that apply, software execution restriction strategies (Windows Defender ATP and Applocker on Windows) can be used to limit the execution of malware.

[3] Consists of improving the security of a system, network or application by fortifying its configuration or structure, reducing the number of objects (users, services, libraries, applications, etc.) present on the system, keeping only those that are necessary for the correct operation of the equipment and the service it provides.

CONTROLLING INTERNET ACCESS

Ransomware often uses entities' Internet access to communicate with an infrastructure hosted online by cyber criminals. Furthermore, by browsing a compromised website, employees may unknowingly download and cause the malware to be automatically installed on their workstation.

The implementation of a secure Internet gateway to block illegitimate flows with unavoidable application relays implementing security functions (e.g. proxy server for web access, DNS resolver for public domain name requests) will therefore reduce the risks relating to ransomware. In particular, this relay can be used to filter connection attempts according to the categorisation or reputation of the sites your employees are trying to visit and to identify abnormal activity (e.g. sending of a large volume of data from the information system to a server outside of the structure and its service providers).

> From a purely technical point of view, the first actions taken were to cut off all Internet access and interrupt the applications. We immediately attempted to identify the precise scope concerned by the attack, and organised communication to inform the teams of the incident and its impact on their activity.
>
> Laurent Babin

IMPLEMENTING LOG SUPERVISION

The supervision of IT security incidents requires the implementation of a logging policy on the various information system resources. It includes system infrastructure servers, administration and user workstations, business servers and network and security equipment located on the periphery or at the heart of the information system (in particular Active Directory servers, DNS servers, messaging and web proxies).

This policy must enable registration on the events generated by the various hosted services. In addition, it must be able to register events relating to authentication, account and privilege management (paying particular attention to objects with strong privileges), access to resources, changes in security strategies, and the activity of the processes and the underlying system.

A system for the supervision of logged events must be put in place. It will enable the detection of a possible compromise and the earliest possible reaction to avoid the encryption of data by the attacker. Furthermore, should an incident occur, these events will help to save time in understanding the incident.

> On arriving, the ANSSI, together with our internal IT services and technical teams, worked on understanding the attack with a view to rebuilding differently. The systems were then restarted in stages: messaging after a week, business applications in order of priority…
>
> Jérôme Lefébure

RAISING AWARENESS AMONG EMPLOYEES

Ransomware attacks normally begin when a booby-trapped attachment is opened or viewing a malicious web page is visited. Training users in good digital security practices is therefore a fundamental step in the fight against this threat, even if it does not provide a complete barrier. The aim is also to instil or reinforce certain reflexes in users by encouraging them to report any suspicious event to the organisation's IT department (e.g. suspicious attachments or e-mails, USB key offered, unusual requests, etc.).

Depending on the characteristics of the organisation (size and workforce, sensitivity of the activity and issues at stake, level of knowledge of the employees, available means of communication, etc.), various kinds of awareness-raising operations can be envisaged: information meetings, quizzes, poster campaigns or the distribution of good practice guides. To support organisations in implementing such initiatives, several public entities, including ANSSI or cybermalveillance.gouv.fr (see useful resources), provide a number of educational resources tailored to each audience.

Experience has shown that IT teams should also be given reminders concerning their specific use of administration tools. Administrators have higher privileges on the information system. As such, they are a prime target for a well-informed attacker. It is therefore important to train this population on the cyber hygiene measures to be implemented in terms of administration in order to avoid the entire system rapidly becoming compromised.

> In these moments [when an attack occurs], one realises how such an event both traumatises and brings people closer together...
>
> Jérôme Lefébure

ASSESSING THE OPPORTUNITY TO TAKE OUT CYBER INSURANCE

Today, cyber insurance policies make it possible to support entities that fall victim to cyber attacks by providing them with legal assistance as well as financial coverage for the damage (tangible, intangible, etc.) suffered in the event of a claim. However, the market is still in its infancy and needs to continue to develop, particularly in terms of case law concerning whether or not exclusion clauses are activated.

> After these "first aid actions", we contacted our insurance company, which put us in touch with ISS experts to support us through the crisis, as well as legal experts. We were then able to identify the origin of the attack and secure the environment.
>
> Laurent Babin

IMPLEMENTING AN INCIDENT RESPONSE PLAN

The specific factor in ransomware attacks is their potential destabilising effect on organisations. Support functions such as telephony, messaging and business applications can be taken out of operation. This means switching to degraded operation and, in some cases, reverting to paper and pencil. The attack generally causes a partial interruption of activity and, in the most serious cases, a total interruption.

> New internal communication channels were set up to warn employees and maintain contact over the coming days. This ranged from instant messaging to paper and pencil and visits from office to office.
>
> Jérôme Lefébure

It is therefore crucial for organisations to define an incident response plan associated with the crisis management system - where one exists - to ensure business continuity and then a return to a nominal state. The implementation of an IT continuity plan must enable your organisation to continue to operate when an alteration to the information system occurs, regardless of its severity. Backup communication resources specific to the IT continuity plan must be seriously considered. The IT recovery plan aims to restore the information systems that have malfunctioned. In particular, it must include how systems and data are to be restored.

▶

> At the time of the attack, we already had a security incident management procedure that had been updated a few months earlier. We were therefore able to implement it very quickly by successively triggering three levels of on-call duty and setting up the crisis unit.
>
> Cédric Hamelin

The entire response plan must be regularly updated and tested through exercises. Plan preparation and exercises must involve all stakeholders in the organisation, functional areas, technical areas and management.

> Throughout the crisis, the responsiveness and commitment of many employees is to be commended. When it happened, the group already had a crisis unit, but it had never anticipated the occurrence of a cyber attack among its crisis scenarios.
>
> Laurent Babin

THINKING ABOUT THE CYBER CRISIS COMMUNICATION STRATEGY

In order to deal with a ransomware attack, it is essential to define the organisation's global communication strategy, which should be adopted from the outset to limit the impact of the crisis on the image and reputation of the entity, both internally and externally.

> External communication at group level and internal communication have been mastered, although efforts still need to be made in terms of the language used. Training is essential in order to explain how things are done and why.
>
> Laurent Babin

The development of an appropriate crisis communication strategy is based on prior contact between the "business" teams (production chain, finance, legal, communication, logistics, etc.) and the people in charge of digital security. Together, they will define an action plan and appropriate messages to be presented to the entity's management. For example, a communicator will have a detailed knowledge of the entity's audience (both internal and external) and the available means of communication. The IT manager will be able to report in real time on the situation and its possible developments. Providing information and reassurance, adopting a transparent position, must lie at the heart of the crisis communication strategy.

Together, they can develop a strategy taking into account:

- The mapping of audiences and the associated communication objectives: internal audience, clients, partners, authorities, general public/media.

▶

- The mapping of communication stakeholders with whom it will be necessary to coordinate: service providers, subsidiaries, authorities, etc.
- The actions to be taken in the short, medium and long term, both externally (press relations, web communication, etc.) and with employees.

In the case of a ransomware, traditional means of communication may be unavailable, which contributes to the destabilisation of the teams. IT should be noted that crisis communication can be tested during exercises to manage a crisis of cyber origin in order to check the coherence and relevance of the communication strategy defined in advance.

> Once things had been resolved, we tried to find out how it was viewed by those involved. At the industrial site, the employees viewed it as a crisis overcome professionally. For the support and subsidiary functions, however, the impressions were more nuanced. Some rued the lack of communication and coordination, and the fact that the applications were recovered too late.
>
> Laurent Babin

REACT IN THE EVENT OF AN ATTACK

The aim of the following measures is to help victim organisations respond to a ransomware attack. The first technical actions proposed, when implemented quickly, make it possible to reduce the losses linked to such an attack.

ADOPTING APPROPRIATE RESPONSES

The first response is to open a log to trace the actions and events related to the incident. Each entry in this document must contain, as a minimum:

- The time and date of the action or event.
- The name of the person who initiated the action or who reported the event.
- The description of the action or event.

This document should make it possible at all times to inform decision-makers on the progress of the actions undertaken.

> Maintaining a regularly updated log throughout the incident made it considerably easier to track the actions at each stage. Subsequently, this log was a precious help to us in producing feedback and identifying areas for improvement.
>
> Cédric Hamelin

In order to prevent the propagation of ransomware to other IT equipment in the entity, it is important to disconnect your backup media as soon as possible after making sure that it is not infected and isolating the infected equipment from the IS by disconnecting it from the network. It may be useful to check whether or not there is a wireless connection on this equipment and, if necessary, deactivate it.

In order to cut off the access to your information system for the attackers acting from the Internet, it is important to isolate it by blocking all communication to and from the Internet. The attackers will then no longer be able to control their ransomware or trigger a new wave of encryption. This will also prevent possible data exfiltration. This measure may have significant consequences on the entity's activity (loss of access to certain outsourced applications, freezing of e-mails sent externally, etc.), which should be managed in parallel.

One of the first actions implemented was to cut off access to the Internet and the internal network, then isolate all unaffected components, starting with backups, databases and storage bays.

Cédric Hamelin

Once the malicious programs causing the infection have been identified, it will be possible to search the logs of the information system for any identifying features (for example: URLs used to communicate with the attacker's infrastructure, file name, hash, subject of the e-mail, etc.). These elements can be used on application gateways or network filtering equipment to prevent new infections. In particular, if an IP address is identified as malicious, it will be possible to set up a firewall rule.

If all the files in a machine have been encrypted, turning off the power of the machine may reduce the chances of finding elements in the device's memory allowing the recovery of encrypted files. Therefore, if the infected machine allows it, it is recommended to enable hibernation to stop the activity of the malicious program while preserving the memory for later analysis.

In order to limit the propagation of the ransomware and data encryption on new machines, it is preferable to leave unbooted equipment switched off (e.g. when an employee returns from holiday or starting up a machine at the beginning of the day) and to prohibit the use of removable storage media (USB key, external hard drive, etc.).

Even though the data is encrypted by the ransomware, it is possible that an encryption solution may be discovered and made public later. It is therefore important to keep the encrypted data. The ***No More Ransom*** project by Europol, the National High Tech Crime Unit of the Dutch police and McAfee identifies decryption methods for a large number of ransomware programs.

COORDINATING MANAGEMENT OF THE CYBER CRISIS

The issues involved in such an attack go far beyond the loss of data or the payment of a ransom. Indeed, victim organisations face many other consequences, which is why it is recommended to set up a crisis unit at the highest level of the organisation, independent of the operational working groups which will have responsibility for coordination and execution.

This unit will be responsible for responding to the strategic level issues of the crisis by establishing, for example, internal and external communication strategies and the elements to be provided for legal action or regulatory notification, in particular for the French Data Protection Authority (CNIL) in the event of a personal data breach. In the latter case, with the support of the Data Protection Officer (DPO), this unit will have to identify the level of risk generated for the persons whose data is affected by the breach and warn them accordingly (employees, customers, members, etc.). More generally, this unit will also be responsible for identifying the impacts of these malfunctions on the organisation's activities and organising the response in these fields.

> To ensure patient safety, non-vital emergencies were moved to other facilities while the critical applications were rebuilt. And to preserve staff activity, the internal IT services crisis unit was led by four people to absorb the pressure resulting from the incident and interface with the various stakeholders involved.
>
> Cédric Hamelin

FINDING TECHNICAL ASSISTANCE

Some entities have neither the resources nor the expertise required to deal with a security incident. In these circumstances, they may call on service providers who specialise in responding to security incidents.

For private individuals and small businesses, the French government has set up the cybermalveillance.gouv.fr platform, which enables contact with local service providers.[4]

> On site, several service providers were involved. While some suppliers and solution providers supported us within the framework of the maintenance contract we have with them, other companies, particularly local ones, spontaneously offered their help.
>
> Cédric Hamelin

> We were quickly joined by service providers for the reconstruction phase. They have shown a strong commitment to us.
>
> Laurent Babin

> It is obvious that we could not face the situation alone. On the morning of 12th October, we therefore called on the ANSSI, a FORENSIC firm to begin the analysis, and the French digital crime-fighting centre (C3N) to file a complaint, as well as reporting the claim to the CNIL and our insurer.
>
> Jérôme Lefébure

[4] https://ssi.gouv.fr/en-cas-dincident/

COMMUNICATING AT THE APPROPRIATE LEVEL

In the event of a proven attack, the communication strategy defined in advance, or even tested upstream by the "business" and technical teams, can be deployed in conjunction with management.

To define the stances and actions to be taken, it is important to take into account the context in which the attack takes place: the technical, media (cyber specialised press) and social (internal perception) situation at the time of the attack, evolution scenarios, etc.

It is also necessary to think very quickly about providing support to employees through appropriate internal communication. The presence of the ransomware is often manifested by the display of a ransom note or even a countdown on the screens. This modus operandi is very often a source of stress and anxiety in the victim entity.

It is prudent to ask employees to apply the confidentiality clause in their employment contract concerning the various media requests and publications (media, social networks, etc.). In all cases, it must be ensured that employees pass on all external requests to the entity's communication department or, failing that, to the manager responsible.

Throughout the crisis, there was a genuine effort for transparency and communication from the internal IT services towards the most critical personnel and services (emergencies, Urgent Medical Aid Services, etc.) which was appreciated. We also informed the CISO of the Ministry of Health and the CERT-FR of the situation, with whom we have been in contact on the advice of the ANSSI delegate for our region.

Cédric Hamelin

DO NOT PAY THE RANSOM

It is recommended never to pay the ransom. Paying is no guarantee of receiving the means for decryption, encourages cyber criminals to continue their activities and therefore maintains this fraudulent system. Furthermore, paying the ransom will not prevent your entity from being targeted by cyber criminals again.

In addition, experience shows that obtaining the decryption key does not always allow all encrypted files to be reconstructed. In particular, files modified by an application and encrypted at the same time by the ransomware are very likely to be corrupted (e.g. a database file).

FILING A COMPLAINT

It is strongly recommended to file a complaint with the police or gendarmerie in the event of a ransomware attack. Firstly, filing a complaint makes it possible to carry out an investigation followed by a "key hunt", at the end of which it may be possible to decrypt the altered data. Secondly, filing a complaint is generally a prerequisite for repairing the damage and can make it possible to identify, arrest and bring to justice the perpetrators of the attack.

The following elements may be requested or may be searched for as part of the investigation (depending on the profile of your entity, these elements may differ):

- A detailed timeline of events relating to the incident (the log), in particular the date of the ransom note and the facts observed.
- The location of each potentially infected device.
- The security logs associated with the incident.
- The technical analysis of the attack.
- The collection of samples of encrypted files.
- The preservation of the media or machines (where possible) on which the ransomware was executed (system disk).
- The e-mail and cryptocurrency addresses provided by the cyber criminals.
- The text of the ransom note.
- The contact details of witnesses to the incident.

The complaint must be filed in the name of the entity. If this action is entrusted to an employee, a delegation of authority must be prepared for this person, signed by a legal representative of the legal entity, in order to allow them to file the complaint.

The Ministry of the Interior will open an online complaint platform for Internet scams called "THESEE". The objectives of this platform will be:

- To improve the service provided to victims of Internet scams.
- To avoid the regional services receiving large numbers of complaints.
- To improve the fight against these scams by centralising, analysing and grouping these complaints or reports.

Offences committed on the Internet against a private individual, including ransomware attacks, can be reported on this platform.

RESTORING SYSTEMS FROM HEALTHY SOURCES

In the case of infected equipment, it is preferable to reinstall the system on a known media and restore the data from backups made, preferably, prior to the date the system was compromised. This is to verify that the restored data is not infected by the ransomware. The effectiveness or safety of alternative cleaning methods is difficult to qualify. The following safety rules must be applied to the restoration media and all healthy machines:

- The vulnerability initially exploited by the attacker must be corrected in order to avoid further infection (example: software update, modification of the network filtering policy).
- If research has identified the ransomware, check that there are no changes made by the malicious program to maintain itself after restarting a previously infected machine (example: registry values and malicious files).
- Change passwords.
- Apply the preventive measures presented in this guide.

THEIR ADVICE TO YOU

Today, it is important to remind organisations in the healthcare sector as well as others that we are not alone in dealing with this type of situation. Do not hesitate to seek outside assistance and advice.

Cédric Hamelin,
Deputy CISO, Rouen CHU

I have not one but three pieces of advice to share. 1) Managing a cyber crisis involves both implementing a plan and playing it by ear. For these two aspects, nothing is done alone! 2) Stay calm (only works if you are not alone). 3) Finally, from a more organisational point of view, this experience has confirmed my belief that a CISO must have direct and easy access to all parties involved in crisis management - including senior management and managers - to prepare the organisation for these events and to react to them if necessary.

Jérôme Lefébure,
CFO, member of the management board in charge of
support functions, M6 Group, media company

My last piece of advice would be to be prepared! You can't get through it alone.

Laurent Babin,
CISO, Fleury Michon, food industry company

RESOURCES

ANSSI

▶ ***Guideline for a healthy information system:***
www.ssi.gouv.fr/en/guide/40-essential-measures-for-a-healthy-network/

▶ ***Controlling the digital risk: the trust advantage:***
www.ssi.gouv.fr/en/guide/controlling-the-digital-risk-the-trust-advantage/

▶ ***EBIOS Risk Manager:***
www.ssi.gouv.fr/guide/ebios-risk-manager-the-method/

COLLECTIVE

▶ **NoMoreRansom:** www.nomoreransom.org

ACKNOWLEDGEMENTS

We warmly thank the Criminal Affairs and Pardons Office for having encouraged this close partnership between our two institutions in order to protect French organisations and citizens from ransomware.

Because this rapidly growing form of cyber crime can only be fully understood with the help of insight from various sources, we would like to thank the Public Interest Group for Action against Cyber Crime (GIP Acyma), the Information Technology Fraud Investigation Brigade (Befti), the French Data Protection Authority (CNIL) and the Central Directorate of the Judicial Police (DCPJ) for their valuable contributions.

Last but not least, since the originality and strength of this document lies in their contributions: thanks to Laurent Babin, Cédric Hamelin and Jérôme Lefébure for their accounts of their experience. All of them were on the front line when, without warning, their organisations saw their daily lives turned upside down following a ransomware attack. Your testimonials are rare, invaluable, and contribute immeasurably to increasing awareness of the risks!

"During the night of 11th-12th October 2019, the group was the target of a violent ransomware-type cyber attack. [...] 'What can I do without a computer?' was the question on everyone's mind. In barely two hours, all hands were on deck!"

Jérôme Lefébure, M6 Group, media company

Industry, media, hospitals, etc. Regardless of the activity sector, cyber attacks spare no one. In this respect, the rise in ransomware is a cause for concern and for action at the highest state levels. By calling for the perpetrators not to go unpunished and by combining testimonies from victims with good digital security practices, this guide shines a powerful spotlight on this threat and invites organisations - from the executive committee to employees - to take up these issues.

Version 1.0 – August 2021 – **ANSSI-GP-077-EN**
Licence Ouverte/Open Licence (Etalab — V1)
ISBN : 978-2-11-167101-0
Dépôt légal : septembre 2021

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.ssi.gouv.fr — communication@ssi.gouv.fr