CCN-CERT

BP/21

Ransomware incident management

BEST PRACTICES REPORT

APRIL **2021**

ccn-cert centro criptológico nacional
CCN centro criptológico nacional

Edited by:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

centro criptológico nacional

Release Date: April de 2021

LIMITATION OF RESPONSABILITY

This document is provided in accordance with the terms set forth herein, expressly disclaiming any implied warranties of any kind that may be found to be related. In no event shall the National Cryptologic Centre be held responsible for direct, indirect, incidental or extraordinary damage derived from the use of the information and software indicated, even if advised of the possibility of such damages.

LEGAL NOTICE

Index

1. About CCN-CERT, National Governmental CERT

The CCN-CERT is the Computer Security Incident Response Team of the National Cryptologic Centre, CCN.

The **CCN-CERT** is the Computer Security Incident Response Team of the National Cryptologic Centre, CCN, assigned to the National Intelligence Centre, CNI. This service was created in 2006 as the **Spanish National Governmental CERT** and its functions are set out in Law 11/2002 regulating the CNI, RD 421/2004 regulating the CCN and in RD 3/2010, of 8 January, regulating the National Security Framework (ENS), modified by RD 951/2015 of 23 October.

Its mission, therefore, is to **contribute to the improvement of Spanish cybersecurity**, by being the national alert and response center that cooperates and helps to respond quickly and efficiently to cyber-attacks and to actively confront cyber-threats, including the coordination at state public level of the different Incident Response Capabilities or Cybersecurity Operations Centers.

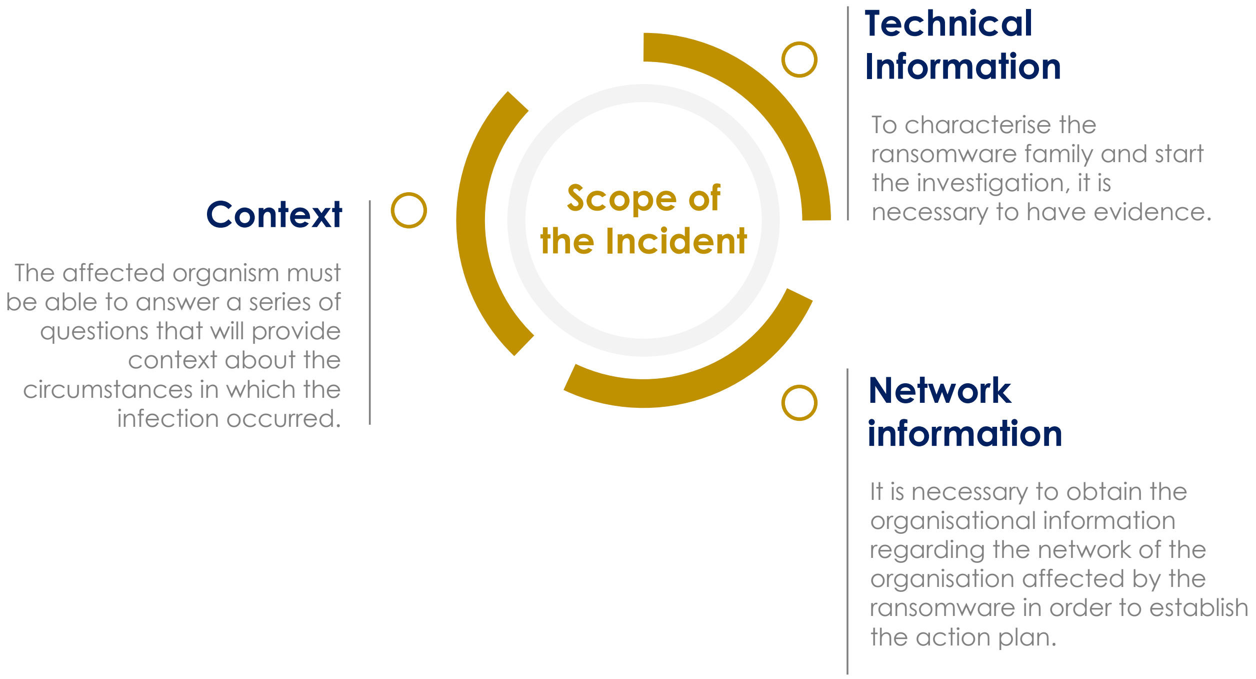
Its ultimate aim is to make **cyberspace more secure and reliable**, preserving classified information (as stated in art. 4. F of Law 11/2002) and sensitive information, defending Spain's Technological Heritage, training expert personnel, applying security policies and procedures and using and developing the most appropriate technologies for this purpose.

In accordance with these regulations and Law 40/2015 on the the Public Sector Legal System, the CCN-CERT is responsible for the management of cyber-incidents affecting any public body or company. In the case of critical public sector operators, cyber-incidents will be managed by the CCN-CERT in coordination with the CNPIC.

2. Scope of the incident

To determine the **scope of** an incident involving ransomware, it is necessary to collect:

- **Incident Background Information.**
- **Technical information about the infection.**
- **Information on the network where the infection occurred.**



Scope of the Incident

Context

The affected organism must be able to answer a series of questions that will provide context about the circumstances in which the infection occurred.

Technical Information

To characterise the ransomware family and start the investigation, it is necessary to have evidence.

Network information

It is necessary to obtain the organisational information regarding the network of the organisation affected by the ransomware in order to establish the action plan.

Figure 1. Scope of the incident

2.1 Context of the incident

The affected organization should be able to answer the following questions that will provide **context about the circumstances** in which the infection occurred:

1. **When did the infection occur?**
2. **How did the infection occur (email attachment, RDP, etc.)?**
3. **How many teams are affected?**
4. **Is backup of encrypted data available?**
5. **Has any mitigation action been taken?**

2.2 Technical information about the infection

In addition to answering the above questions, in order to characterize the ransomware family and start the research, the following **evidence** is needed:

- **Ransom note.**
- **Encrypted file samples (no larger than 2 megabytes).**
- **Sample of the ransomware, phishing email, office file or any evidence that allows analysis of the malicious code.**

2.3 Network information

Finally, it is necessary to obtain the following organizational information regarding the network of the organization affected by the ransomware in order to establish an action plan:

Network diagram

Diagram showing the components that make up the communication network and how they interact with each other, including routers, firewalls, servers, workstations and their connections. Examples of network diagrams are included in ANNEX I.

List of servers and main assets

Table showing IP, domain, system name and location. An example table is included in ANNEX II.

Public addressing, IP and domains

List of addresses and domains exposed to the Internet.

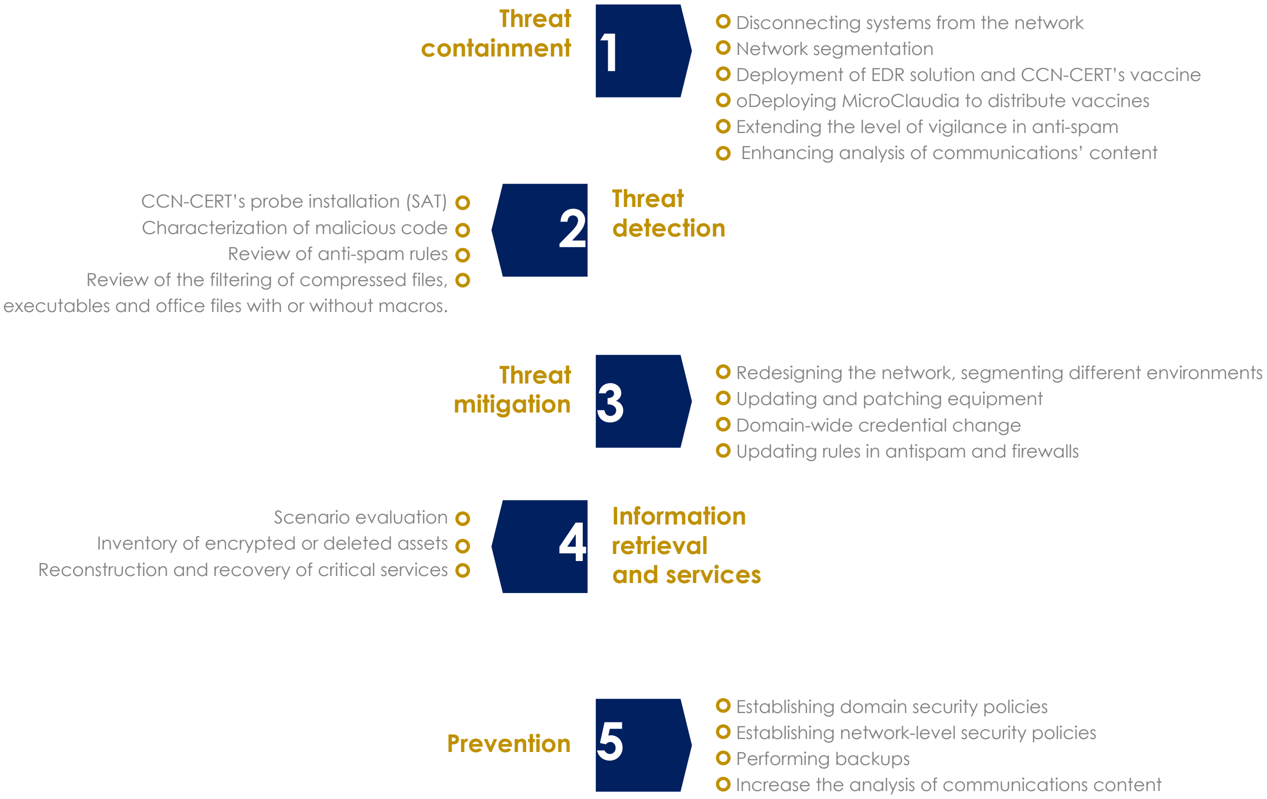
Logs

Of the security systems present in the network;

o Antivirus, EDR
o Firewall, proxy, DNS, IDS/IPS
o Antispam, quarantine email
o Remote access (VPN, SSH, Teamwiewer, etc.)
o Traffic back up

3. Guidelines

We will work on the following **lines of action**, defining a team to lead each task and designating a team leader:



Threat containment 1

- Disconnecting systems from the network
- Network segmentation
- Deployment of EDR solution and CCN-CERT's vaccine
- oDeploying MicroClaudia to distribute vaccines
- Extending the level of vigilance in anti-spam
- Enhancing analysis of communications' content

Threat detection 2

- CCN-CERT's probe installation (SAT)
- Characterization of malicious code
- Review of anti-spam rules
- Review of the filtering of compressed files, executables and office files with or without macros.

Threat mitigation 3

- Redesigning the network, segmenting different environments
- Updating and patching equipment
- Domain-wide credential change
- Updating rules in antispam and firewalls

Information retrieval and services 4

- Scenario evaluation
- Inventory of encrypted or deleted assets
- Reconstruction and recovery of critical services

Prevention 5

- Establishing domain security policies
- Establishing network-level security policies
- Performing backups
- Increase the analysis of communications content

Figure 2. Guidelines

3.1 Threat containment

Containment is the first phase that is carried out to ensure that:

The malicious code does not continue to spread throughout the network (encryption of shared folders, lateral movement to computers with visibility, etc.).

In the event that an attacker gains remote access to the network, it will be immediately shut down to prevent further activity (exfiltration of information, deployment of additional backdoors, removal or destruction of evidence, etc.).

To this end, especially in security incidents in which a ransomware specimen is involved, it is necessary to proceed immediately, carrying out the actions detailed in the following sections.

3.1.1 Disconnecting systems from the network

The ransomware infection will encrypt all the files on the computer and those mapped on the connected drives, both physical devices (USBs, external hard drives, etc.) and network drives.

In the vast majority of situations, the infection is detected after the ransomware is executed and all files are encrypted. However, there is a possibility that the ransomware didn't complete its execution, allowing in the best case scenario to recover the encryption key or prevent further files from being encrypted.

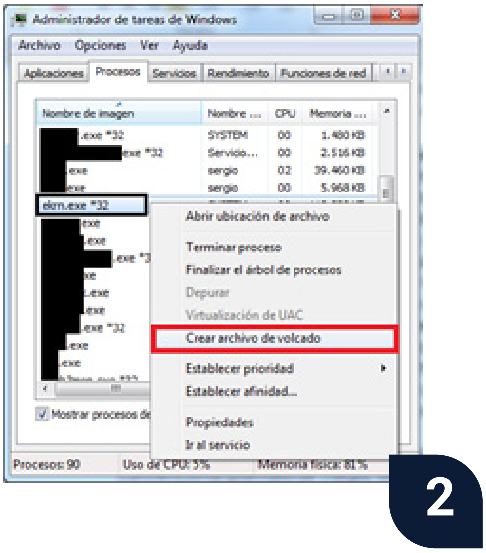
The following general steps are recommended when detecting ransomware:

1

Disconnect network drives

This means "pulling the network cable" (or disabling wireless interfaces). This may prevent the encryption of files on accessible network drives if the ransomware has not completed execution.

Check if the malicious process is still running



Nombre de imagen	Nombre ...	CPU	Memoria ...
[redacted].exe *32	SYSTEM	00	1.480 KB
[redacted]exe *32	Servicio...	00	2.516 KB
[redacted].exe	sergio	02	39.460 KB
[redacted]exe	sergio	00	5.968 KB
elkrn.exe *32			
[redacted]exe			
[redacted].exe			
[redacted].exe *3			
[redacted]xe			
[redacted].exe			
[redacted].exe			
[redacted].exe *32			
[redacted].exe			
[redacted].exe			

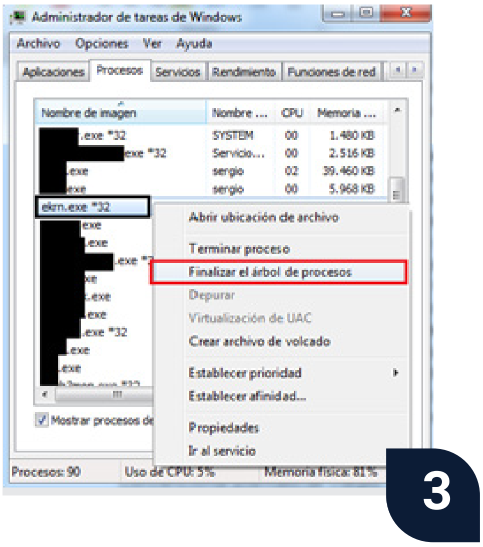
☑ Mostrar procesos de

Procesos: 90 Uso de CPU: 5% Memoria física: 81 %

This task is not easy in many cases as the malicious process might have injected itself into a legitimate process or might have simply finished running.

However, if the process in question is identified (using tools such as Sysinternals' Process Explorer), a dump of the harmful process will be performed from the Windows Task Manager. To do this, right click on the process and select the option "Create dump file" (it will be saved in %TMP%). Once the file has been dumped, it should be stored safely on an isolated system.

Terminate the execution of the harmful process



Nombre de imagen	Nombre ...	CPU	Memoria ...
[redacted].exe *32	SYSTEM	00	1.480 KB
[redacted]exe *32	Servicio...	00	2.516 KB
[redacted].exe	sergio	02	39.460 KB
[redacted]exe	sergio	00	5.968 KB
elkrn.exe *32			
[redacted]exe			
[redacted].exe			
[redacted].exe *3			
[redacted]xe			
[redacted].exe			
[redacted].exe			
[redacted].exe *32			
[redacted].exe			
[redacted].exe			

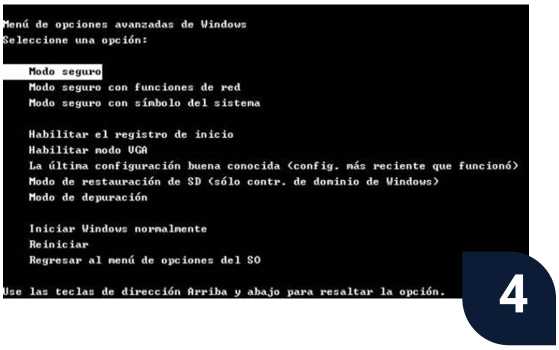
☑ Mostrar procesos de

Procesos: 90 Uso de CPU: 5% Memoria física: 81 %

There are two alternatives for this:

I. If the process has been identified, simply stop its execution from the Windows Task Manager: right click on the process and select the option "End process tree".

II. If the process could not be identified, it is recommended to shut down the system manually and immediately.



```
Menú de opciones avanzadas de Windows
Seleccione una opción:

    Modo seguro
    Modo seguro con funciones de red
    Modo seguro con símbolo del sistema

    Habilitar el registro de inicio
    Habilitar modo VGA
    La última configuración buena conocida (config. más reciente que funcionó)
    Modo de restauración de SD (sólo contr. de dominio de Windows)
    Modo de depuración

    Iniciar Windows normalmente
    Reiniciar
    Regresar al menú de opciones del SO

Use las teclas de dirección Arriba y abajo para resaltar la opción.
```

4

Start the computer in Safe Mode

Before Windows gets started in the conventional way (loading screen), press F8 key to access the advanced boot menu, from which you can select “Safe Mode”. This will prevent the ransomware from restarting again in case it is persistent.

5

Back up your computer

This backup will contain all encrypted and unencrypted files, and should be made on an external storage device isolated from the network. I**n the event that the files cannot be decrypted, it is important to keep them**, as encryption may be broken or the C&C keys may be released in the future.

3.1.2 Network segmentation

This is probably a key step.

This is probably a key step. Typically, ransomware is able to spread across the network through shared drives in the domain. However, trends indicate that in recent campaigns involving ransomware there may also be **additional malicious code** with greater capabilities and complexity. It has been observed that in some cases the threat can escalate privileges, move laterally across the network using compromised credentials, turn on shut down computers using WoL (*Wake on Lan*), and exfiltrate information.

Systems managers have to redesign the network and establish the ideal point to locate the Firewall. The firewall will allow visibility of all network traffic passing through it, this will be especially useful in case of having IOC (indicators of compromise) to locate those computers on the network that try to establish communications with known command and control servers (C2).

> **Trends indicate that in recent campaigns involving ransomware there may also be additional malicious code with greater capabilities and complexity**

3.1.3 Deployment of EDR solution and CCN-CERT vaccine

To conclude the containment phase, it is recommended to deploy an EDR (*Endpoint Detection and Response*) solution on endpoints, client systems and servers, to improve detection and isolation capabilities.

For its part, the CCN-CERT distributes specific vaccines for each case of ransomware through its **MicroClaudia** tool. MicroClaudia generates actions that allow **the immediate blocking of any malware** related to **Emotet**, **Trickbot**, **Bitpaymer**, **Ryuk** and **Sodinokibi** so that their execution can be stopped in case the computers are infected or the harmful code tries to spread.

3.2 Threat detection

After the containment phase, we proceed to d**etect which computers have been affected** by the malicious code, either because the attacker has used them to pivot through the network or to encrypt and/or delete their content.

During this phase, the following tasks are carried out.

3.2.1 Installation of CCN-CERT probe (EAS)

The CCN-CERT has a probe, Early Alert System, which performs the functions of IDS (*Intrusion Detection System*) and can be deployed at an interconnection point of the network where there is visibility of all incoming and outgoing traffic.

This probe allows to detect, based on the patterns known by the CCN-CERT, the traffic categorized as harmful in the network, so that it allows to act in a timely manner to locate and neutralize the threat.

</sat>

3.2.2 MicroClaudia installation

The CCN-CERT makes available its tool to distribute specific vaccines for each ransomware and thus prevent their execution.

The tool is installed in end computers and contains action detectors based on research on different ransomwares.

The **MicroClaudia** team **adds new vaccines based on the analysis of emerging samples**.

3.2.3 Characterisation of the malicious code

The CCN-CERT has reports on malicious code (ID) on its portal (https://ccn-cert.cni.es) related to different families of ransomware.

These reports compile the threats' characterization, including **characteristics**, **functionality**, **connectivity**, **persistence** and **indicators that allow detection**.

There are several websites that can help identify the ransomware family involved in an incident using a sample file, the most effective and recommended are:

nomoreransom.org

Link: https://www.nomoreransom.or/crypto-sheriff.php

IDRansomware

Link: https://id-ransomware.malwarehunterteam.com

Encrypted files and **ransom notes** can be uploaded to these pages. This way, based on the type of encryption and ransomware method, it is possible to find out which type of family is responsible for the infection.

3.3 Threat mitigation

The mitigation phase can be carried out in parallel to the containment and detection of the threat, consisting of effectively neutralizing the malware deployed by the attacker. To do so, the following steps can be followed:

3.3.1 Redesigning the network by segmenting the different environments

In an unsegmented network, it is trivial for an attacker to have visibility of all assets, despite having different routings.

Once the attacker obtains domain credentials, previously compromising a computer on the network, he could start moving laterally, looking for the most interesting computers to steal, encrypt or delete content.

Taking into account the nature of computers and servers (DMZ, LAN, DC and servers, etc.), if the network is properly segmented using network elements such as Firewalls and separating environments and routings, the potential impact that could result from a ransomware infection would be lower than in the case of a flat network. In fact, segmentation would allow to isolate the affected computers during a security incident, preventing the malicious code from spreading through the network and ultimately taking control of it after the Domain Controller (DC) is compromised.

Ideally, firewall policies should be adjusted on the basis of a ***whitelist***-approach, that is, enabling only those connectivities that are essential in each case for the correct functioning and operation of systems.

Ideally, firewall policies should be adjusted on the basis of a *whitelist*- approach, that is, enabling only those connectivities that are essential in each case for the correct functioning and operation of systems.

3.3.2 Systems' updating and patching

There is often a very heterogeneous set of versions of the devices and operating systems in the equipment pool.

This means that, in some cases, the patching level is not uniform or that support for security updates is no longer available.

It is **essential** to keep providing **support and maintenance** in the form of patches and updates periodically.

It is essential to keep providing support and maintenance in the form of patches and updates periodically.

3.3.3 Domain-wide credentials reset

When a network is breached, usually by exploiting a vulnerability in one of the services exposed to the Internet in the DMZ area or by *spear-phishing* one of the workers via email, the attacker will try to **escalate privileges** on the compromised machine to get the **credentials** of the computer and the domain.

Then, after reconnaissance of the network, the attacker will try to move and pivot to new computers on the network until he manages to gain access to the Domain Controller (DC), from which he will have full control of the network.

The solution is to **reset the domain credentials**, once the DC has been rebuilt together with the Active Directory (AD). Also, all administrator users must be detected, in order to identify possible privileged users created by the attacker.

The solution is to reset the domain credentials, once the DC has been rebuilt together with the Active Directory (AD).

3.4 Retrieval of information and services

This line of action can also be carried out in parallel to the rest. After a security incident involving the encryption and deletion of assets, it is essential to establish the extent of the impact suffered, assessing what information can be recovered and what services have been affected.

3.4.1 Scenario evaluation

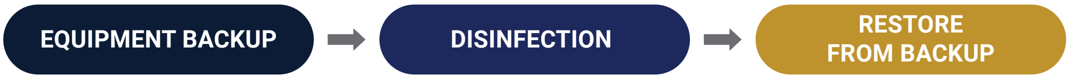
It is necessary to **perform an assessment of the ransomware** impact to try and recover the encrypted files.

Possible scenarios are listed below, starting from the most favorable to the most unfavorable:

SCENARIO {1}

Full backup of the affected computer is available

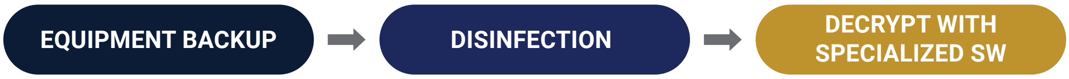
In this scenario, the affected computer would be disinfected and restored from backup.


EQUIPMENT BACKUP → DISINFECTION → RESTORE FROM BACKUP

SCENARIO {2}

There is a tool that allows decryption

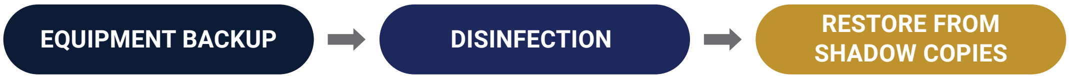
If public tools are available to restore the files encrypted by a particular ransomware specimen, they will be used. Unfortunately, only a few ransomware variants are decryptable, either because all the encryption keys have been obtained after the intervention of the C&C server, or because there is a known vulnerability in the malicious code that allows the files to be decrypted. See seventh section, "Decrypting ransomware".


EQUIPMENT BACKUP → DISINFECTION → DECRYPT WITH SPECIALIZED SW

SCENARIO {3}

Shadow Volume Copy is available

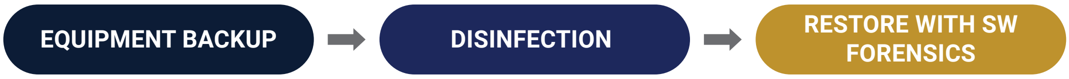
It would be enough to restore Windows' automatic backup of files, using Shadow Explorer, for example. In many cases the ransomware makes this action impossible.


EQUIPMENT BACKUP → DISINFECTION → RESTORE FROM SHADOW COPIES

SCENARIO {4}

Files can be recovered with SW forensics

Sometimes certain forensic programs are able to recover some of the original files deleted by the ransomware.


EQUIPMENT BACKUP → DISINFECTION → RESTORE WITH SW FORENSICS

SCENARIO {5}

Keeping encrypted files safe and sound

It is possible that the affected files could be decrypted in the future with a specific tool.

EQUIPMENT BACKUP → DISINFECTION

Paying the ransom does not guarantee that the attackers will send the decryption utility and/or password, it only rewards their campaign and motivates them to continue mass-distributing this type of malicious code.

3.4.2 Inventory of encrypted or deleted assets

To determine the scope of the infection and the impact of the incident, it is necessary to **list the affected services** based on the information that was encrypted or deleted.

Attached below is an example of a table that can be used to list the assets affected, including the impact:

SERVER	DATA	IMPACT	RESULTS
XXXXXXXXX	Corporate Mail Documentary databases	No impact on the virtual server Deleted or encrypted backups Encrypted backup	**Complete recovery**

3.4.3 Reconstruction and recovery of critical services

Some recommendations for information retrieval are described below.

Windows' Shadow Copy service, also known as **Volume Snapshot Service (VSS)**, allows to make periodic automatic backups of data stored on shared resources, as well as computer drives (on NTFS file systems). For this purpose, VSS creates hidden copies of the changes made to data blocks in the file system, allowing to recover individual information (e.g. files) in case of loss or accidental deletion. For further technical information about this system we recommend reading "*Volume Shadow Copy*" from Microsoft's website.

Unlike the system implemented in Windows XP[1] (system restore), the VSS maintains *snapshots* of system volumes; for example, the entire C drive. In this way, not only system files but all data contained on that drive, including user documents, program files, etc., will be protected.

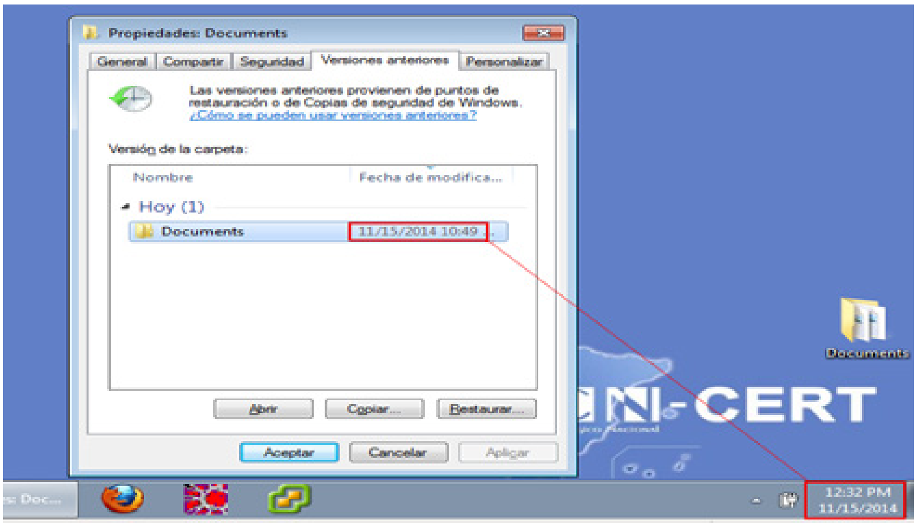
If you use Windows Vista[2] or a higher operating system, in case of falling victim to a ransomware attack from which it is practically impossible to recover the original files –for example, due to the encryption system used–, it is advisable to consider using VSS to try and recover a previous backup of the affected files (as long as the VSS drive is not affected).

**The VSS maintains *snapshots* of system volumes; for example, the entire C drive.
In this way, not only system files but all data contained on that drive.**

[1] Sistema operativo de Microsoft Windows, lanzado en el año 2002, cuyo soporte técnico finalizó en 2014.
[2] Sistema operativo de Microsoft Windows, lanzado en el año 2007, cuyo soporte técnico finalizó een 2017.

To restore the files of a certain directory open its properties and select the tab “**Previous Versions**”.

From this tab it will be possible to view and restore each of the copies created by VSS on that directory. Keep in mind that the most recent *backup* may not match (since it is an older version) with the last version of the original file before being affected by the ransomware.



Propiedades: Documents

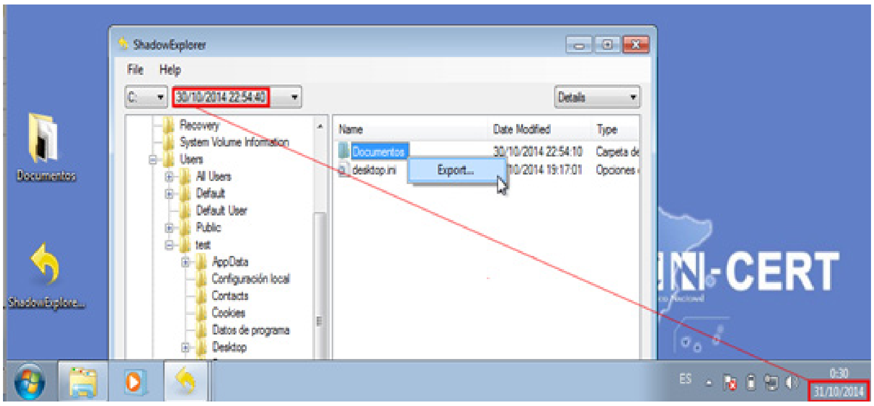
Las versiones anteriores provienen de puntos de restauración o de Copias de seguridad de Windows.
¿Cómo se pueden usar versiones anteriores?

Versión de la carpeta:

Nombre	Fecha de modifica...
Hoy (1)	
Documents	11/15/2014 10:49 ...

12:32 PM
11/15/2014

Another alternative to restore the documents of the backup created by VSS is to use the software **Shadow Explorer**. This program has a very simple interface from which you can view and restore each of the copies created by VSS. In the following screenshot, the most recent backup, prior to the infection of a certain ransomware, has been selected. Then, after right-clicking on the selected directory, the “**Export**” option has been selected.



It is worth noting that the most recent *ransomwares*, aware of this mechanism to restore files, implement functionalities to disable VSS and delete restore points.

In certain cases, it is possible to decrypt files encrypted by a particular ransomware specimen. Tools that allow decryption and restoration of files can take advantage of:

- **Weaknesses in the encryption algorithm used by the ransomware.**
- **Key recovery through the information contained or generated by the binary (temporary files, registry keys, etc.).**
- **Sometimes, through police and international collaboration, it is possible to take control of C&C servers, from which keys used in encryption processes can be extracted.**

Listed below are some of the existing **online tools** and **utilities** which allow decryption of certain ransomware specimens sorted by family:

Ransonware	Tool	Web
AlcatrazLocker	Avast Tool	https://files.avast.com/files/decryptor/avast_decryptor_alcatrazlocker.exe
Apocalypse	Avast Tool	https://files.avast.com/files/decryptor/avast_decryptor_apocalypse.exe
Bad Block	Avast Tool	https://files.avast.com/files/decryptor/avast_decryptor_badblock.exe
Bandarchor	Kaspersky Tool	https://support.kaspersky.com/sp/viruses/disinfection/10556
Bart	Avast Tool	https://files.avast.com/files/decryptor/avast_decryptor_bart.exe
Cryptodefense	Emsisoft Tool	https://decrypter.emsisoft.com/cryptodefense
Cryptolocker	-	http://www.decryptcryptolocker.com
CryptXXX v3	Kaspersky Tool	https://support.kaspersky.com/mx/8547
Crysis	-	https://files.avast.com/files/decryptor/avast_decryptor_crysis.exe
DMAlocker	Emsisoft Tool	https://decrypter.emsisoft.com/dmalocker
Globe	Avast Tool	https://files.avast.com/files/decryptor/avast_decryptor_globe.exe
JigSaw	Avast Tool	https://files.avast.com/files/decryptor/avast_decryptor_jigsaw.exe
Legion	AVG Tool	http://files-download.avg.com/util/avgrem/avg_decryptor_Legion.exe
Locky	Emsisoft Tool	https://decrypter.emsisoft.com/autolocky
Petya	Bleepingcomputer Tool	http://download.bleepingcomputer.com/fabian-wosar/Petyaextractor.zip
SFZLocker	-	https://www.avg.com/es-es/ransomware-decryption-tools#szflocker
Teslacrypt	Eset Tool	https://download.eset.com/special/ESETTeslaCryptDecryptor.exe
Torrentlocker	Bleepingcomputer Tool	http://download.bleepingcomputer.com/Nathan/TorrentUnlocker.exe
Zerolocker	Vinsula Tool	http://vinsula.com/security-tools/unlock-zerolocker/

In addition to these links, you can consult:

Link to **Trendmicro's solution**, to combat a wide range of **ransomware** strains (including some that are not so well known)

Link: https://success.trendmicro.com/solution/1114221-downloading-and-using-the-trend-micro-ransomware-file-decryptor

A tool by **Emsisoft**, which **fights the infection of several Ransomware families**, also less known and some of them not included in the previous tools list.

Link: https://decrypter.emsisoft.com/

In case the variant that has infected the computer is not listed in any of the above tools, try the search engine offered by **Barkly**.

Link: https://www.barkly.com/ransomware-recovery-decryption-tools-search

3.5 Prevention

The above lines of work are meaningless without the appropriate security policies and mechanisms to ensure the prevention of a new infection that follows patterns similar to those exhibited in this intrusion.

To prevent future infections with a similar *modus operandi*, the following guidelines should be established:

3.5.1 Setting security policies in the domain

Once all the disinfection and mitigation tasks described in the previous points have been carried out, it is necessary to:

Deploy policies for the entire domain, **disabling the execution of PowerShell** on all computers and allowing it only on those systems that strictly need it. This prevents the execution of post-exploitation tools used by the attacker to obtain information and move around the network.

It is also necessary to **disable the execution of macros** in office documents, which is typically the infection vector commonly used to enter a network.

For further information on how to do this check the following C**CN-CERT's Threat Report** which explains the procedure in detail:

Link: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/4171-ccn-cert-ia-52-19-implementacion-segura-de-microsoft-windows-office-frente-a-la-campana-emotet/file.html

Force the **use of strong passwords** that expire periodically. Ideally, for those services exposed to the Internet, require a **second authentication factor**, using SMS, email, Google Authenticator, or any other solution deemed appropriate.

Periodically review users with administrator privileges in the domain, checking that all of them are under control and reducing to the minimum the level of access from users. This will prevent the attacker from easily obtaining domain administration credentials and colonizing the network after an infection.

3.5.2 Setting security policies at the network level

It is necessary to establish policies at the network level that allow granular control of the connections that can be established between the different points and computers on the network. To this end, it is advisable to follow these recommendations:

- **Blocking at the Firewall level**, preferably layer 7, all those connections that are not strictly necessary. To do this, it is recommended to follow a ***whitelisting*** approach, enabling only essential connections and denying the rest of the traffic.

- **All activity** of the Firewall, proxy, DNS and any security element or service on the network **should be recorded** to analyze and monitor anomalous patterns:

    - **Client's computers that attempt to access other systems** in the organization, such as servers, computers in other segments, etc. that they should not have access to.

    - **Connectivity to and from the Internet by computers on the network using non-standard ports** (other than 53/UDP, 80/TCP, 443/TCP) and outside the whitelist set in the proxy.

    - Ideally, all logs and traces should be centralized in a **SIEM** in order to **monitor all logs from a single point** in an integral way.

For those users, companies or clients that require external access to the Intranet through VPN, the source IP from where the communication is to be established should always be requested, whenever possible, in order to reduce the exposure surface as much as possible. These accesses should be checked periodically to confirm their legitimacy.

In this way the security team can have **visibility** and **traceability** of all events generated in the network, detecting in a timely manner **anomalous activity** that could denote malfunctioning or possible intrusions in the network.

3.5.3 Anti-spam performance

The main route of entry are emails with malicious content, so special emphasis should be placed on detection rules in antispam. Also, the use of sandbox for attachments should be considered.

Files can contain malware, whether they are office files or files encrypted with a password through popular tools such as ZIP and RAR. As the files are encrypted, they may be allowed to pass without proper analysis, so you should take extreme precautions with these or try to always use PGP encryption as it would be a personal encryption.

3.5.4 Backups

Backing up is probably the most important point when managing an incident involving ransomware. It is important that these backups are performed according to the following recommendations:

At least daily and incremental **backups** of the organization's priority information systems.

Isolation of the backup servers, or cabinets, with respect to the rest of the network, so that after the infection of a computer the malware cannot jump directly to that server (solutions that implement NAC, *Network Access Control*, can be used for this purpose).

Having enough storage to **keep more than one copy of the same asset**, since in the event that the information is encrypted through the attack and is introduced in the backup, a previous copy that is not encrypted could be available.

Ideally, **a backup** that is physically isolated and disconnected from the network **should be made periodically**, every month, for example.

Annex I

Examples of a NETWORK diagram:

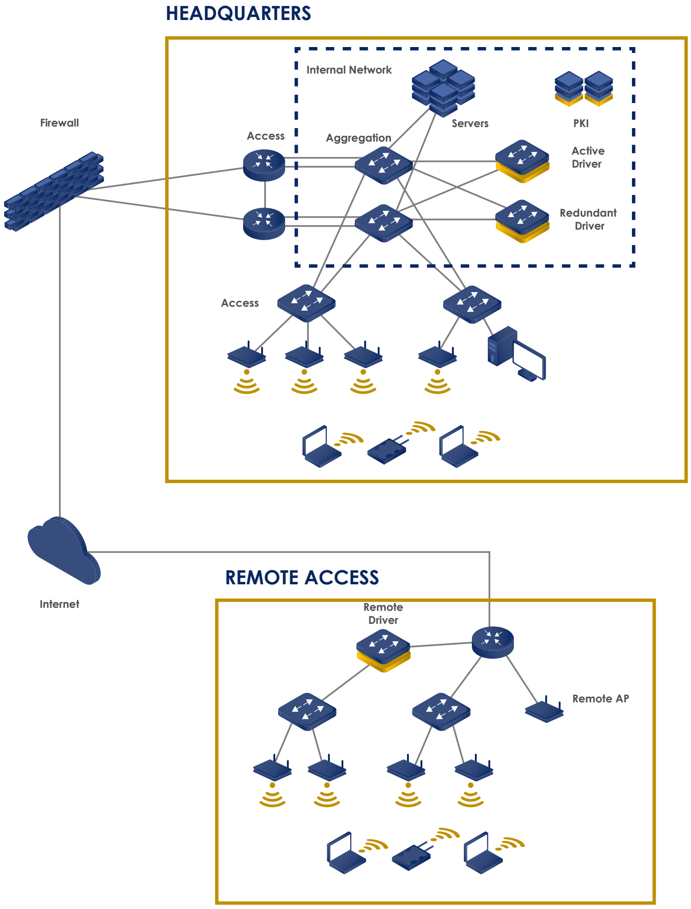


Figure 3. Network diagram

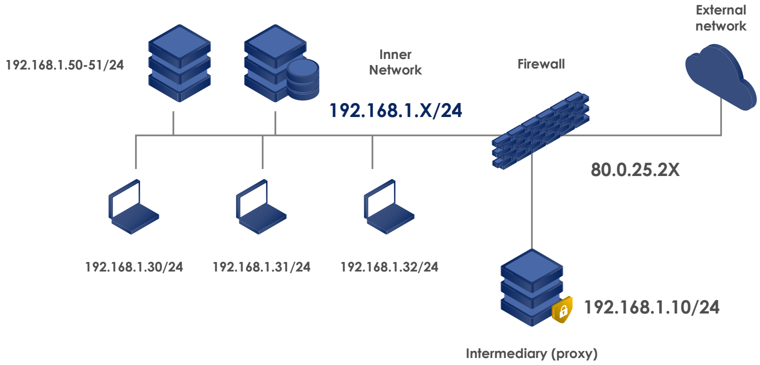


Figure 4. Network diagram

Annex II

Sample List of servers and core assets:

Device	IP	Type	Location	Observations
RADIUS Server	192.168.1.6/24	W2012	North Headquarters	Isolated in the MANAGEMENT VLAN.
Activity Directory Server	192.168.1.10	W2008R2	ISOLATED DPC	Pending upgrade to W2016
DHCP Server	192.168.1.101	W2008R2	South Headquarters	Rango de IP 192.168.50 - 99
Virtualization Server	192.168.102	VMWare 6.5	North Headquarters	No Backup

CCN
centro criptológico nacional

ccn-cert
centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es