

CCN-CERT BP/04



Ransomware

GOOD PRACTICE REPORT

MAY 2021

ccn-cert
centro criptológico nacional

CCN
centro criptológico nacional

Edit



Centro Criptológico Nacional, 2018

Date of edition: May 2021

LIMITATION OF RESPONSABILITY

This document is provided in accordance with the terms compiled in it, expressly rejecting any type of implicit guarantee that might be related to it. In no case can the National Cryptologic Centre be considered liable for direct, indirect, accidental or extraordinary damage derived from using information and software that are indicated even when warning is provided concerning this damage.

LEGAL NOTICE

Without written authorisation from the National Cryptologic Centre, it is strictly forbidden, incurring penalties set by law, to partially or totally reproduce this document by any means or procedure, including photocopying and computer processing, or distribute copies of it by means of rental or public lending.

Index

1. About CCN-CERT, National Governmental Cert	5
2. Introduction	6
3. Vectors of infection	9
3.1 Phishing via e-mail	9
3.2 Via web link	10
3.3 By attachment	11
3.4 Web browsing. Web exploit kits	11
3.5 Attacks by RDP	13
3.6 Attacks without user interaction	14
3.7 By means of other malware	15
4. Disinfection	16
4.1 First steps	16
4.2 Identifying ransomware	18
4.3 Aspects to be taken into account	19
4.1.1 Time	19
4.1.2 Removal of harmful code	19
4.1.3 File recovery	19
4.4 Mitigate the effects of infection	21
5. Good practices	22
6. Awareness	24



Index

7. Shadow copies	25
7.1 Windows operating systems prior to Windows 8	25
7.2 Windows 8 or later operating systems	27
7.3 Generic backup	28
7.4 Macro locking	30
7.5 Correct configuration of user accounts and their permissions	32
7.6 Honeypots or trap systems	33
7.7 Safe navigation	34
7.8 Known file extensions	36
7.9 Applocker	37
7.10 BYOD policies	38
7.11 Secure passwords	40
7.12 File retrieval via cloud storage	41
7.13 When all seems lost	42
8. Conclusion	43
9. Basic security decalogue	44

1. About CCN-CERT, National Governmental Cert

**The CCN-CERT is the
Information Security
Incident Response
Capability of the
National Cryptologic
Centre, CCN**

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

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

All of this, with the ultimate aim of achieving a safer and more reliable cyberspace, 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 Legal Regime of the **Public Sector**, 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-incident management will be carried out by the CCN-CERT in coordination with the CNPIC.

2. Introduction

The family of harmful code known as ransomware has been the most prevalent and damaging threat, with a great deal of evolution in recent years.

Around 2012, the first variants were found whose main purpose was to lock the infected computer. Years later, ransomware evolved into what are known today as file encryptors. The scenario worsened in 2015-2016 with the proliferation of RaaS (Ransomware as a Service), services offered by cybercriminals to allow them to easily design this type of malware in exchange for a percentage of the campaign's potential profits.

The period from 2019 to 2020 saw a clear increase in cyber-attacks, as the pandemic began to spread around the world and governments in several countries enacted containments.

According to Emsisoft¹, in 2020 the total number of ransomware attacks grew by 12.39 % compared to the previous year. In January 2020, ransomware-related incidents grew by 59.84% compared to the same month last year. In February, ransomware attacks grew by 137.17%. But it was not until April that the record growth was recorded: 156.55%. From May onwards, the growth slowed down. That month saw growth of 64.36% compared to the same month of May of the previous year, and in summer the difference oscillated around 30%. The second half of 2020 recorded fewer incidents than during the same period in 2019.

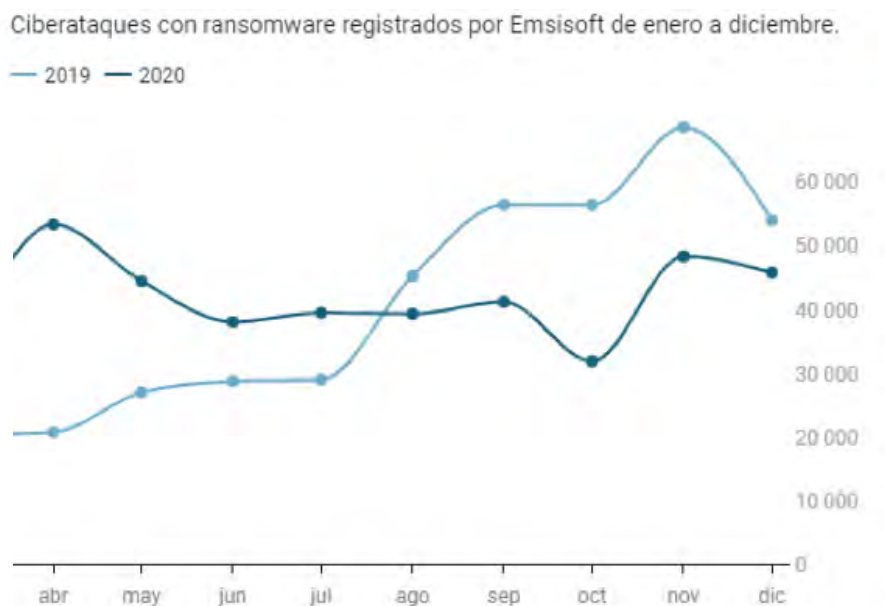
In November 2020, approximately 25 different ransomware groups were reported to be active.

The total number of ransomware attacks grew by 12.39 % compared to the previous year

1. <https://www.businessinsider.es/grafico-ensena-como-pandemia-ha-disparado-ciberataques-834287>.

2. Introduction

[Figure 1]
Ransomware
cyber-attacks
recorded by
Emsisoft



Reports such as the one by Cognyte² claim that the three most active ransomware families globally in 2020 were Ryuk, Maze and REvil/Sodinokibi. Moreover, according to another report by Palo Alto Networks³ cybercriminals operating ransomware attacks collected more money than ever before in the same year.

In ransomware cyberattacks, cybercriminals⁴ attack using harmful code that encrypts data and computer systems, and then demand a ransom from their victims if they want to get back to normal. Importantly, criminals are increasingly targeting vulnerable targets, such as healthcare organisations, and have developed more aggressive strategies that force the payment of ransoms.

**In ransomware
cyberattacks,
cybercriminals attack
using harmful code
that encrypts data and
computer systems,
and then demand a
ransom from their victims
if they want to get back
to normal**

2. See: <https://www.cognyte.com/blog/what-you-need-to-know-about-the-top-4-global-ransomware-vulnerabilities-and-how-to-stay-protected/>

3. See: <https://unit42.paloaltonetworks.com/ransomware-threat-report-highlights/>

4. See: <https://www.businessinsider.es/pagos-rescate-ransomware-triplicaron-durante-pandemia-833859>

2. Introduction

The method of payment has remained unchanged over the years, with cryptocurrencies (in most cases Bitcoin) being used because of their anonymous nature.

In a world where most cyber-security sources expect cyber-threats to continue to increase, it is important to know how to defend yourself.

This guide will set out measures that are applicable to these phases.

**Face of cyber attacks, action is needed
in at least four distinct phases:**

- ① **Prevention**
- ② **Detection**
- ③ **Response**
- ④ **Remediation of the attack**



3. Vectors of infection

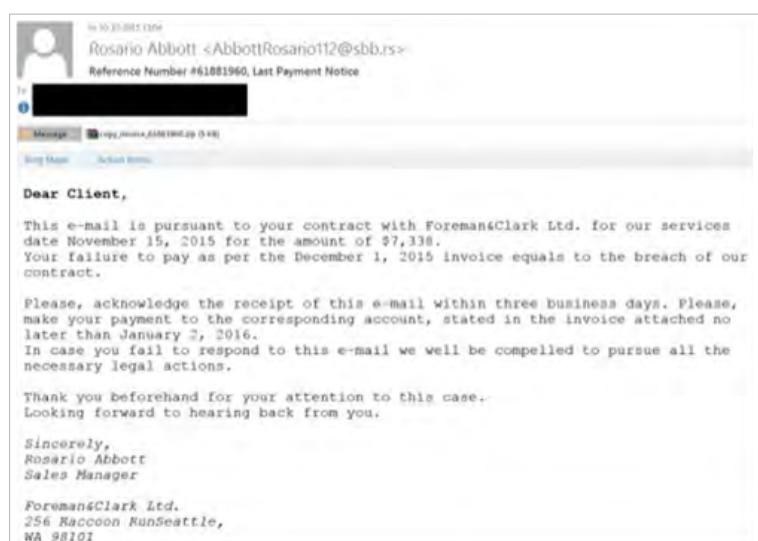
In order to prevent infections, it is best to know the means of entry of the threat, as well as its propagation mechanisms. However, after an infection, it is not always possible to determine the exact origin or causes.

The mechanisms and possibilities for infection are varied, and it is important to know the most common vectors. In some cases, the harmful code may remain latent in the system for some time and manifest itself following a specific action or determination of a specific date, making it difficult to pinpoint the exact time of infection.

3.1 Phishing via e-mail

Although decreasing (in the case of ransomware), the use of fraudulent e-mails (phishing) is still very present in everyday life.

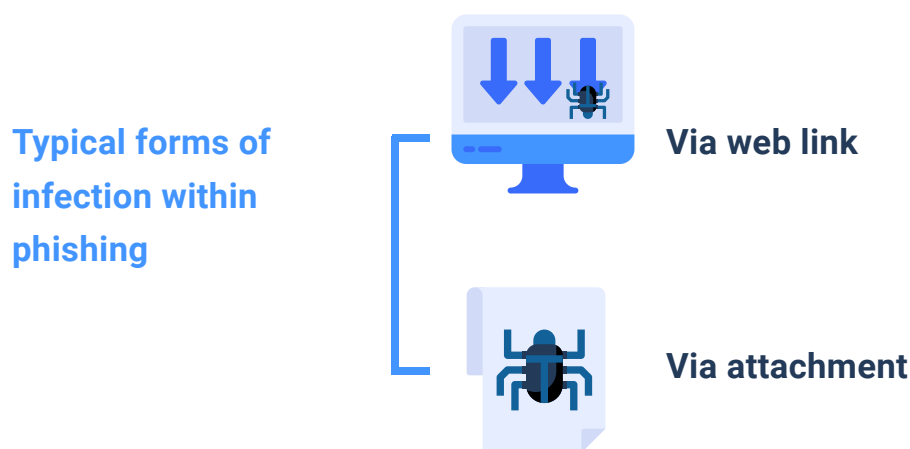
[Figure 2] Fraudulent mail used by TeslaCrypt



3. Vectors of infection

This type of mail relies on so-called social engineering (the manipulation of people in order to get them to perform a series of tasks to the manipulator's liking) to get the user to execute a seemingly harmless file.

There are two typical forms of infection within phishing, either via a link to a fraudulent page, which hides the harmful code in an apparently legitimate application, or via a specially manipulated file attached to the e-mail message.



3.2 Via web link

This type of infection consists of directing the victim to a website that may be legitimate, but which the cybercriminals have altered beforehand, or it may be a virtually identical copy that is indistinguishable from the legitimate version.

In both cases, the victim downloads or executes (consciously or unconsciously) an application that, although it does not seem suspicious at first glance, hides the harmful code.

3.3 By attachment

In this case, the e-mail message itself carries a file semantically related to the text of the message and, under some excuse (fake bank report, forms, images, curriculum vitae, etc.), invites and gets the victim to open it, which triggers the execution of the malicious code.

For more information on how to prevent these forms of infection, it is advisable to consult the report BP-02-16 Good Practices in Electronic Mail.



3.4 Web browsing. Web exploit kits

There are also what are known as Web Exploit Kits: a more subtle and transparent way of infection that exploits a known vulnerability in the browser or an installed plugin to execute harmful code.

The transparency of this method lies in the fact that ransomware campaigners first take control of legitimate servers to compromise the pages they offer, including harmful content that exploits browser weaknesses. In this way, they cause the user's browser to download binary code that is immediately executed, initiating the infection process.

Web Exploit Kits: a more subtle and transparent way of infection that takes advantage of a known vulnerability in the browser or an installed plugin in order to execute malicious code

3. Vectors of infection

To avoid this type of infection, the only thing you can do is to use the most up-to-date version of the browser and its extensions. In principle, it is advisable to block all components that are not strictly necessary. Some of the most commonly used plugins are Flash Player, Java and Silverlight.

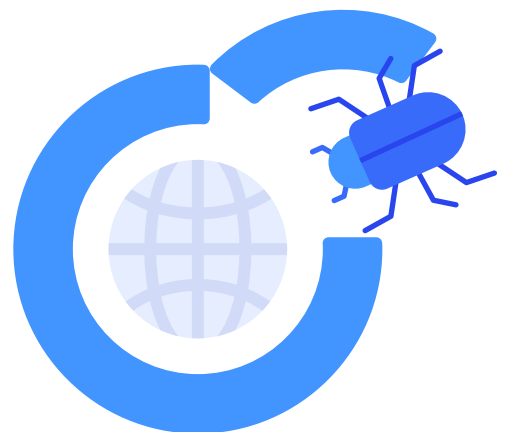
One of the main problems with plugins is that they significantly increase the exposure to certain types of attacks during web browsing. Some of these plugins contain a large number of critical vulnerabilities that allow attackers to execute code on the victim's computer.

It only takes a user to click or browse to a malicious page for their computer to be compromised (without even downloading or interacting with the page in question). Most browsers allow you to enable or disable installed components. Enabling plugins, such as Flash and Java, temporarily and in a user-controlled manner can be a good option.

It is also advisable to use specific plug-ins to block the opening of pop-ups⁵, *iframes*, execution of JavaScript code and advertisements (Ads). All of these mechanisms can be used to force the browser to load pages, which may be compromised, or to execute harmful code.

For more information on how to prevent these forms of infection, it is advisable to consult BP-06-16 Good Practice in Web Browsers.

To avoid this type of infection, the only thing you can do is to use the most up-to-date version of the browser and its extensions



5. See: <http://es.ccm.net/faq/9996-bloquear-ventanas-emergentes-de-publicidad-pop-ups>

3.5 Attacks by RDP

Aware of the changed scenario due to the COVID 19 pandemic, which has forced employees to do much of their work through remote access, cybercriminals - especially ransomware operators - are trying to exploit the new opportunities to increase their profits⁶.

RDP has become a popular attack vector in recent years, especially among ransomware operators, who use this protocol to gain access to infrastructure machines and then propagate.

Attackers, using automated tools, search for computers that have this service exposed to the Internet. Then, using a brute-force attack (i.e. trying all possible alphanumeric combinations) or dictionary attacks (large files composed of the most common users and passwords used on the Internet), they try to gain access to the computer.

For this reason, it is vital to ensure that the username and password combinations used to access services are robust.

RDP has become a popular attack vector in recent years, especially among ransomware



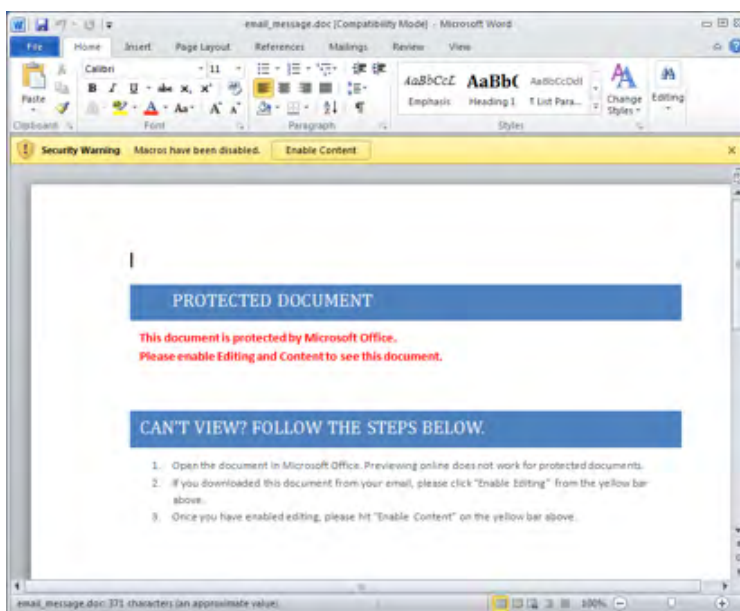
6. <https://www.welivesecurity.com/la-es/2020/06/29/crecieron-ataques-fuerza-bruta-dirigidos-rdp-durante-pandemia/>

3.6 Attacks without user interaction

Faced with a scenario where more and more users are educated about computer attacks and the most frequent methods of infection (in short, more aware of computer security), malware writers (across the board) adapt their methods in order to spread their malicious executables as much as possible.

This development has been seen in the distribution of malicious office documents, the content of which at first glance appears unreadable or protected. It is noted that in order to be able to read the document, macros need to be activated, after which the harmful code is executed.

However, since the end of 2017, methods have started to be used where social engineering is no longer necessary, as user interaction is eliminated. One example is the use of exploits (programmes that take advantage of an insecurity to execute arbitrary code) in office documents themselves, which are executed by simply opening the document, without the need to activate macros. This type of attack is very dangerous because there is no need for interaction, as no alert or window is usually displayed, which makes it difficult to determine when the infection took place.



[Figure 3]
Example of a harmful document
supposedly protected

3.7 By means of other malware

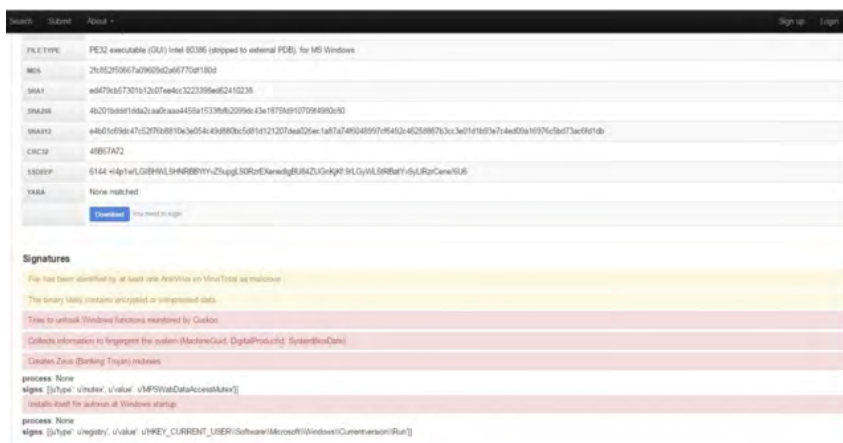
It is quite common for malware to enter the computer via other malware that has been previously installed

Such cases can occur, for example, with the family of viruses known as Trojans, which give full control of the system to the attacker, downloaders whose sole purpose is to download more malware or backdoors, i.e. backdoors that are left open on the infected computer with the aim of gaining direct entry in the future.

In turn, it is very common for programs intended for *pirating* commercial software to be infected. At first, it may appear that such programmes perform their function correctly, but it is in these cases that the attached malware may not be detected, as the software actually manages to run and infect the system at the same time.

For such cases, a more thorough analysis of the file is needed. There are web services that will scan a suspicious document with various antivirus software free of charge, such as <http://www.novirusthanks.org/>.

Similarly, for an even more in-depth examination, it is possible to use the service of <https://malwr.com/> whose technology implements a Sandbox with Cuckoo (virtual machine) where the sample is executed and analysed in detail (files created, logs modified, connections, system calls, screenshots...), to offer much more complete and thorough results.



[Figure 4]
Example of analysis carried
out by "malwr"

4. Disinfection

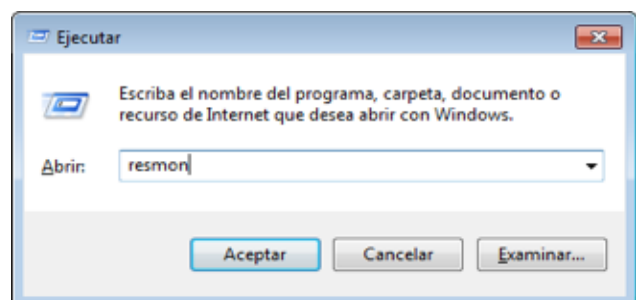
4.1 First steps

The first thing to do if an infection is detected is to disconnect the computer from the network, since encryption usually requires the computing power of the infected computer to work. This procedure serves several purposes:

- ▶ **Prevent the encryption action from reaching the content hosted on network drives accessible from the infected computer.**
- ▶ **Prevent harmful code from contacting your command and control server.**

Analysing which processes are running on the computer does not usually help much in diagnosing what is going on, as in most cases ransomware is often disguised under the guise of a legitimate process such as "explorer.exe". If you identify the process that is massively accessing the disk, you should act on it by terminating it⁷.

To help identify the harmful process, the Windows Resource Monitor tool can be used. To access it, simply run "resmon" (Windows key + r).



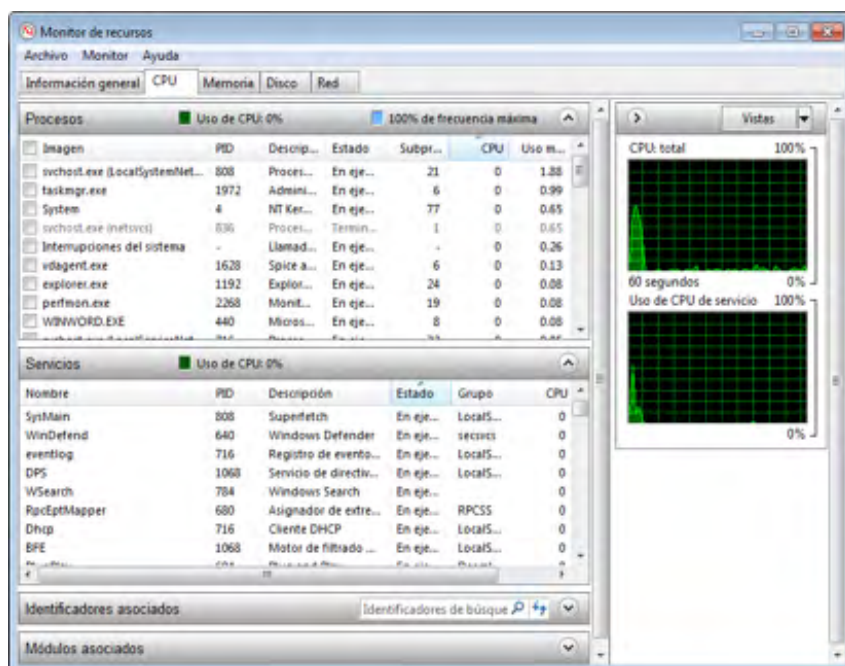
[Figure 5]
"execute" command window

7. Close processes with Task Manager, see <https://support.microsoft.com/es-es/kb/2499971>.

4. Disinfection

Because the file encryption operation requires CPU time and disk access, these characteristics can be used to identify the process or application that is performing the attack. For this purpose, attention should be paid to the following:

- ▶ **Application processes that are not actually running:** If you notice that a process with the name of an application such as "notepad.exe" or "calc.exe" appears in the process list, and this application is not actually open, it is very likely to be a harmful process disguised as a harmless application.
- ▶ **Identify repeated processes with different PIDs⁸:** if processes with the same name appear several times, they can be identified by their PID. All these processes must depend on the original one and be part of its process tree. If there is one outside the process tree, it is -probably a harmful process.
- ▶ **Processes with a large number of open files or with excessive CPU or disk usage:** the encryption process is expensive in terms of resource consumption, so the attacking process will use a large amount of resources, especially CPU and disk access.



[Figure 6]
Image of the resource monitor
in Windows 7

8. PID, "Process ID": is a unique identification number that represents each running process. See <https://www.computerhope.com/jargon/p/pid.htm>

4.2 Identifying ransomware

It is important to know which ransomware variant has infected the affected computers, which can be done using one of these services:

NoMoreRansom or **IDRansomware**.

On these web pages, the files can be uploaded and the family of the harmful code that has infected the computer and encrypted its files can be identified. In this case, the attacker can be identified by providing an encrypted file or by sending the file containing the ransom instructions. Both elements are sufficiently illuminating to know if it is a known attacker.

Knowing which family has attacked the systems allows a search to be carried out on the details and behaviour of the harmful code, and valuable information can be obtained (such as whether or not a decryption and file recovery tool exists).



4.3 Aspects to be taken into account

4.3.1 The time



Some varieties of ransomware use the time elapsed after infection as a pressure factor to force the victim to pay the ransom.

It is best to use this time to contact cybersecurity experts and authorities to get as much information as possible about similar infections and advice on how to deal with them.

4.3.2 Removal of harmful code



The main goal of ransomware is usually not to persist on the infected computer, as the ransom demand itself reveals its presence.

For this reason, in most cases, removal can be straightforward and specially developed disinfection tools are often available for victims to remove the harmful code from the attacked device.

4.3.3 File recovery



Once the ransomware that has infected the computer has been identified, Internet sites can be consulted which indicate whether or not recovery (decryption) of the hijacked files is possible at that time.

If such a recovery is possible, it is due to tools developed by organisations as varied as Kaspersky⁹, Intel Security, McAfee, Panda Security, Sophos, HitMan, anti-malware companies, various response centres known as CERT¹⁰, research teams such as NoMoreRansom¹¹, national and international law enforcement agencies, specialised forums such as bleepingcomputer¹² and researchers and security analysts, who release master keys publicly and altruistically, among many others.

9. See: <http://www.kaspersky.es/>

10. See: <https://searchdatacenter.techtarget.com/es/consejo/CERT-vs-CSIRT-vs-SOC-Cual-es-la-diferencia#>

11. See: <https://www.nomoreransom.org/index.html>

12. See: <http://www.bleepingcomputer.com/>

4. Disinfection

There is a frequently updated utility that compiles information on all known ransomware families (recovery tools, dates of occurrence, etc.). It is recommended to consult it if you have been a victim of an infection, so that you can find out what information is available about the attack and, if necessary, obtain a recovery tool. This tool can be found at the following link:

<https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml>

In addition, it is essential to review the document entitled "CCN-CERT IA-11-18 Ransomware Security Measures", which lists many more resources to facilitate file recovery, among others:

- ▶ http://files-download.avg.com/util/avgrem/avg_decryptor_Legion.exe
- ▶ <https://success.trendmicro.com/solution/1114221-downloading-and-using-the-trend-micro-ransomware-file-decryptor>
- ▶ <https://www.mcafee.com/us/downloads/free-tools/index.aspx>
- ▶ <https://decrypter.emsisoft.com/>

It is important to mention that in the absence of decryption tools, payment is not advisable, as this only serves as an incentive for cyber-criminals to continue creating ransomware campaigns.

Also, paying the ransom does not ensure the recovery of the files. There are campaigns that not only offer real decryption tools, but also store the credit card details used. Fraudulent TOR pages (anonymous links where ransom payments are usually made) have also been detected. According to Symantec 2017, one in five businesses failed to recover their files after making the payment.

Paying the ransom does not ensure the recovery of the files



4.4 Mitigate the effects of infection

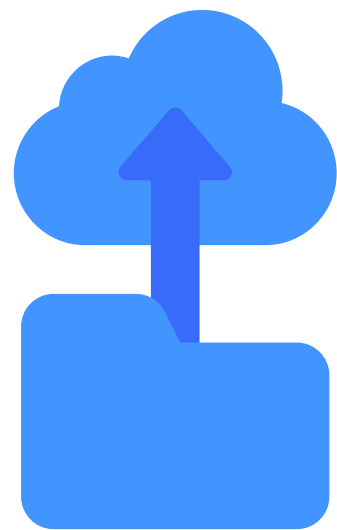
Mitigating the effects of the infection should be understood as those actions that allow the victim to reduce the effects of the infection, in this case in the number of encrypted files, or that enable full or partial recovery from the infection.

Once an infection has occurred and the files have been encrypted, they can be recovered by various means:

- ▶ By means of a specific decryption tool (Section 4.3.3).
- ▶ Through system restore, which allows encrypted files to be recovered.

There are several solutions for such restoration:

- ▶ If the infected computer is running Windows 7 or earlier, the preventive option of activating and using so-called Shadow Copies is available.¹³
- ▶ On Windows systems after version 7 it is possible to use the File History option.¹⁴
- ▶ For any type of operating system and infrastructure it is always possible to use backup tools.



13. See: <https://www.welivesecurity.com/la-es/2017/09/26/shadow-copies-backup-windows-ransomware/>

14. See: <https://support.microsoft.com/en-us/help/17128/windows-8-file-history>

5. Good practices

The following are the main measures to prevent, detect or partially mitigate the action of ransomware:

- 1 **Maintain regular backups** of all important data. It is necessary to keep such copies isolated and without connectivity to other systems, thus preventing access from infected computers.
- 2 **Keep the system up to date** with the latest security patches, both for the operating system and any software installed.
- 3 **BYOD (Bring Your Own Device) policies.** It is becoming increasingly common for companies to adopt this type of policy, which allows workers to use their electronic devices as a means of working within the organisation. These devices are a potential vector of infection, which is why it is essential to define security rules.
- 4 **Secure passwords.** As mentioned above, attacking services visible from the Internet with weak access credentials (insecure passwords) is a procedure that is becoming more and more common.
- 5 **Maintain a first line of defence with the latest signatures for harmful code** (antivirus), as well as having the **correct configuration of firewalls** at application level (based on whitelisting of allowed applications).
- 6 **Have anti-spam systems in place at the e-mail level** and set a high level of filtering. This reduces the chances of infection through mass e-mail ransomware campaigns.

5. Bonnes pratiques

- 7 **Establish security policies on the system** to prevent the execution of files from directories commonly used by ransomware (App Data, Local App Data, etc.). Tools such as AppLocker, Cryptoprevent or CryptoLocker Prevention Kit make it easy to create such policies.
- 8 **Block traffic related to domains and C2 servers** by means of an IDS/IPS, thus preventing communication between the harmful code and the command and control server.
- 9 **Do not use accounts with administrator privileges**, thus reducing the potential impact of ransomware.
- 10 **Maintain access control lists** for network mapped drives. In case of infection, encryption will occur on all mapped network drives on the victim machine. Restricting network write privileges will partially mitigate the impact.
- 11 We recommend the **use of Javascript blockers** for the browser, such as "Privacy Manager", which prevents the execution of all scripts that could damage your computer. This reduces the chances of infection from the web (Web Exploit Kits).
- 12 **Display extensions for known file types**, in order to identify possible executable files that could masquerade as another file type.
- 13 Additionally, it is recommended to **install the "Anti Ransom" tool**, which will try to block the encryption process of a ransomware (by monitoring "honey files"). In addition, this application will perform a memory dump of the harmful code at the time of its execution, in which hopefully the encryption key that was being used can be found.
- 14 Finally, the **use of virtual machines** will prevent ransomware infection in a high percentage of cases. Due to the anti-debug and anti-virtualisation techniques commonly present in this type of harmful code, it has been demonstrated that in a virtualised environment its action does not materialise.



6. Awareness

The security of an organisation relies, to a large extent and in one way or another, on its users. Making them aware of the threats in the digital world is an essential task to be undertaken.

It is of utmost importance that people working with computers are aware of the different techniques used by cyber criminals to hack into computer systems, and are able to detect and avoid them in order to reduce the number of infections.

As detailed above, many of the strategies used by attackers require the human factor, in particular the use of social engineering, for example in the case of phishing e-mails or when activating macros in an infected office document. User awareness therefore greatly reduces the risk of attacks.

It has also been observed that human interaction is not necessary.

This is a sign that the world of IT security is always on the move, and for this reason it is necessary that the training of a corporation's staff is continuous over time and with some frequency in order to keep up with the new threats that emerge on a daily basis.

Awareness of the human component can greatly reduce the risk associated with incoming mail, documents and other downloads into the system. Describing the ease with which many of these attacks are carried out is one of the best ways to make the user aware of the consequences of misusing system resources.

Describing the ease with which many of these attacks are carried out is one of the best ways to make the user aware of the consequences of misusing system resources

7. Shadow copies

7.1 Windows operating systems prior to Windows 8

In operating systems ranging from Windows XP to Windows 7 inclusive, a technology called **Shadow Copies** is available, which allows the user to make, manually or automatically, copies of the files stored on the computer, even if they are in use. These copies are made in order to be able to restore them later if any mishap makes it necessary.

This is an easy-to-implement preventive measure and does not require additional software. However, it is not a valid solution against all types of ransomware; for example, "CryLocker" and "CryptoWall" explicitly delete these restore files. However, it can be useful in the case of a ransomware infection that does not alter the **Shadow Copies**. They are activated as follows:

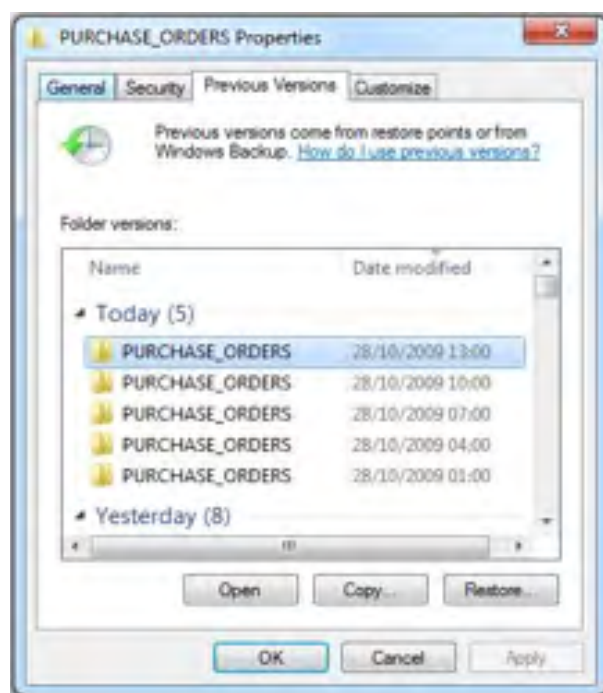
Shadow Copies technology allows the user to manually or automatically make copies of files stored on the computer, even when they are in use



7. Shadow copies

1. From **Start**, open the **Control Panel**.
2. **System** is accessed.
3. Under System, go to the **System Protection** section.
4. In the **Protection Settings** section, you select the drives for which you want to make **Shadow Copies**.
5. Finally, select **Create**.

[Figure 7] Shadow Copies in Windows 7



In cases where the infection has not affected the Shadow Copies, the effect of the infection can be combated by restoring these copies to a previously disinfected computer without traces of the harmful code. To do this, follow the instructions below:

- ▶ From the **System Protection** menu (following steps 1, 2 and 3 of its creation), choose the **System Restore** option.
- ▶ Then select the **restore point** to which you want to **return**.
- ▶ It is **confirmed** and awaits completion of the **restoration process**.

For more information on the use of **Shadow Copies**, please refer to Microsoft's article ¹⁵ on this service.

15. [https://technet.microsoft.com/en-us/library/ee923636\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/ee923636(v=ws.10).aspx)

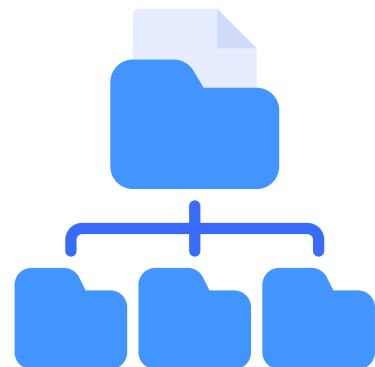
7.2 Windows 8 or later operating systems

From Windows 8 onwards, the functionality that allows different copies of files to be made is called **File History** and consists of storing backups **on removable media**¹⁶, which is a big difference compared to the same functionality in previous versions of Windows operating systems. In addition, it is also possible to enable the **Shadow Copies** mentioned above.

Before using **File History**, it is necessary to choose where the backups are to be made. To do this, you can select a **removable medium** such as an external disk or a USB memory stick connected to the computer, or even a disk accessible on the same local network to which the computer is connected.

Note that **File History only copies** files stored in the Documents, Music, Pictures, Videos and Desktop folders, as well as files stored on OneDrive for off-line access on the computer.

File History allows to make different copies of the files, storing the backups on a removable media



16. See: <http://www.howtogeek.com/74623/how-to-use-the-new-file-history-feature-in-windows-8/>

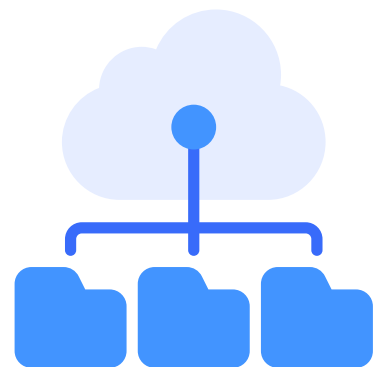
7.3 Generic backup

The most effective measure against ransomware is to always have several backup copies of all important files. In fact, extortion only occurs when the ransomware attacker has managed to encrypt **files that are unique and unrecoverable** and there is no choice but to pay the ransom if they are to be recovered. It is essential to have at least one **backup copy** of all important files, so that you can fall back on that backup copy when you need to recover them.

Backup policies recommend always having three up-to-date, complete copies, deposited in three different and geographically distant locations, stored on two different types of media and, above all, **all of them outside the network**. For example, one possibility, although not the best, would be to simultaneously use your own computer, a cloud storage service and a removable medium.

Backups need to protect both the **integrity** and **confidentiality of the** backups, so it is recommended to **encrypt and cryptographically sign them**, especially if they are to be stored in the cloud.

The most effective measure against ransomware is to always have several backup copies of all important files



7. Shadow copies

The following are a number of open source applications that allow for efficient backup/backup.

- ▶ **Amanda**¹⁷. It is a cross-platform tool (Windows, Linux, macOS) that allows you to make copies on magnetic disks, tapes, optical devices (DVD) and cloud storage systems.



- ▶ **BackupPC**¹⁸. It is a tool available for Windows and Linux that allows you to make backup copies of large amounts of data, using file compression to reduce the size of the information to be saved, thus reducing costs.



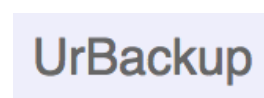
- ▶ **Bacula**¹⁹. It is one of the most widely used backup suites in the business world. It is available for Windows, Linux and macOS environments.



- ▶ **FreeFileSync**²⁰. It is a folder synchronisation tool that allows you to make backup copies of both local computers and network drives. Its most useful features include task automation, detailed error reports and the possibility of using long path names. It is available for Linux, Windows and macOS.



- ▶ **UrBackup**²¹. This tool allows backups to be made in the background, while working, so that it does not interfere with the user's work. It is a fast and efficient tool, as well as allowing backups to be made over the Internet. Available for Windows and Linux.



17. See: <http://www.amanda.org/>

18. See: <https://backuppc.github.io/backuppc/>

19. See: <http://blog.bacula.org/>

20. See: <http://www.freefilesync.org/>

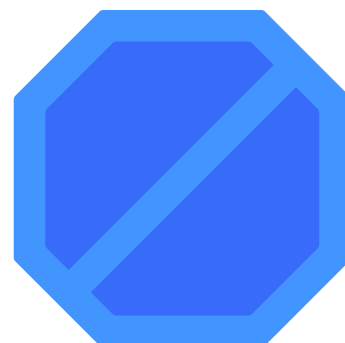
21. See: <http://www.urbackup.org/>

7.4 Macro locking

Since the arrival of the MS Office 2007 suite, documents ending in *.docx*, *.xlsx* and *.pptx* do not contain macros²², only those ending in *.m*. In MS Office 2016 versions²³, macros are disabled by default. It is best to work in an environment where macros are not required.

To ensure that macros are disabled²⁴, you can proceed as follows:

1. Select from the **File tab** (MS Office 2013-2010) or the **Microsoft Office button** (MS Office 2007).
2. Select **Options** (MS Office 2013-2010), **Excel/Word/... Options** (MS Office 2007).
3. Select **Trust Centre** and then select **Trust Centre Settings**.
4. Select **Macro Settings**.
5. Select **"Disable all macros without notification"**.
6. **Accept**.
7. **Exit** the program and **restart** to verify the chosen configuration.



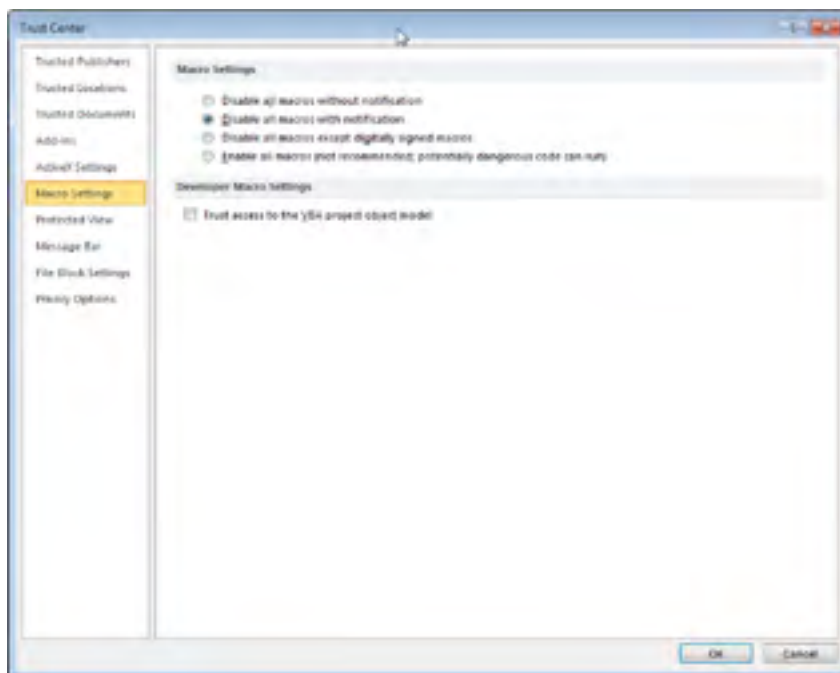
22. See: <https://support.microsoft.com/es-es/office/inicio-r%C3%A1pido-crear-una-macro-741130ca-080d-49f5-9471-1e5fb3d581a8>

23. See: <https://blogs.technet.microsoft.com/mmmpc/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/>

24. See: <https://support.office.com/es-es/article/Habilitar-o-deshabilitar-macros-en-documentos-de-Office-7b4fdd2e-174f-47e2-9611-9efe4f860b12>

7. Shadow copies

[Figure 8]
Blocking Macros in Microsoft Office



If the execution of VBA code (macros) is required, it is recommended to choose the option **"Disable all macros with notification"**, in order to be able to examine their behaviour a priori using tools such as Office-MalScanner. If macros are required, the best option is **"Disable all macros except digitally signed macros"**.

On the Internet there are services that allow you to analyse the content of any file²⁵, but there are also others that specialise in analysing harmful macros included in PDF, Word, Excel and PowerPoint documents. In any case, it should be borne in mind that when the file is analysed, exclusive control of it is lost, so it should be taken into consideration that it **has been made public**.

Some of these services include the following:

- ▶ **General** (<http://www.document-analyzer.net/>).
- ▶ **Doc** (<https://malwaretracker.com/doc.php>).
- ▶ **PDF** (<https://malwaretracker.com/pdf.php>).

25. For example, see <https://www.virustotal.com/es/>

7.5 Correct configuration of user accounts and their permissions

Any multi-user operating system (Windows is one of them) has to follow a permissions policy that is as restrictive as possible, so that users have access only to those resources and functionalities that are necessary for their work.

This is known as "**least privilege**" and should be applied in all scenarios. Proper implementation of the permissions policy can prevent one user from being able to infect an entire network if ransomware spreads.

Below is a series of addresses with instructions on how to correctly manage user permissions on machines with different versions of the Windows operating system:

- ▶ **Windows 7:** <http://www.welivesecurity.com/la-es/2015/05/22/como-administrar-permisos-usuarios-grupos-usuarios-windows-7/>
- ▶ **Windows 10:** <https://channel9.msdn.com/Blogs/MVP-LATAM/Administra-tus-cuentas-de-usuario-en-Windows-10>



7.6 Honey pots or trap systems

One of the phases of any defensive process against an attack is the detection of the attack. In general, the sooner it is known that the system is under attack, the sooner it can react by stopping it or mitigating its effects.

One of the ways to detect ransomware infections is to install a honeypot²⁶, system on the machine, which acts as a decoy that reveals the presence of the harmful code.

The measure consists of creating a folder with various files that are attractive to the harmful code, but which are not those used by the users of that machine. Actions on that folder are monitored in real time so that when the ransomware accesses them to encrypt them, its presence is detected and it is stopped.

A limitation of this measure is that it does not detect the actions of the harmful code until it accesses the decoy files and encrypts part of the system. Since the contents of the folder will not represent a significant percentage of the totality of the files, its sensitivity in detecting the attack may not be high. An example of such a tool can be found at:

http://www.security-projects.com/?Anti_Ransom

If an infection is detected, the programme displays an alert indicating which process is modifying one of the bait files and will offer the option to terminate that process or let it continue..



[Figure 9] Anti-Ransomware

26. See: <https://www.redeszone.net/tutoriales/seguridad/que-es-honey-pot/>

7.7 Safe navigation

One of the most common methods of infection used by ransomware is the exploitation of vulnerabilities in web browsers. This is done by **exploit kits**²⁷, which are programmes designed to exploit known vulnerabilities in applications in order to gain full control over the attacked system.

However, this is not the only method of infection that is related to web browsers, but also phishing or any other method that results in the execution of harmful code on the victim's computer (advertising USB sticks, given or found USB sticks, to trendy pps, web services, etc.).

To protect against this type of attack, the basic recommendation is to keep both the web browser and the extensions or add-ons installed on it up to date. In this way, all known fixes will have been applied to the browser, thereby reducing the number and extent of weaknesses that the attacker can use (**exposure surface**).

In addition, it is recommended to make use of web browser extensions or add-ons aimed at increasing the security of web browsers. The recommended extensions are those that block the opening of pop-up windows, such as **AdBlock**²⁸ (Google Chrome and Mozilla Firefox), which prevents the loading of pages that are not requested by the user or that are known to be harmful. As a complement, the **PopUp Blocker** plugin can be added to prevent pop-up windows from appearing.

It is also recommended to use extensions to protect against phishing (which are included in all major browsers) and other threats, such as the **Avast Online Security** extension for Google Chrome.

One of the most common methods of infection used by ransomware is the exploitation of vulnerabilities in web browsers, using exploit kits

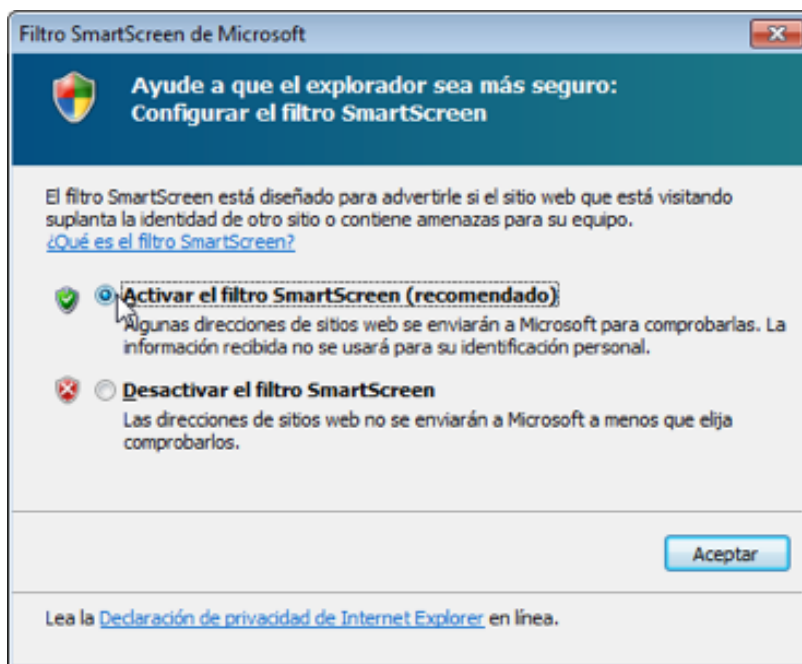
27. See: <https://www.eset.com/bo/empresas/compania/kit-de-exploits-que-son-y-como-protegerse-de-ellos/>

28. See: <https://getadblock.com/>

7. Shadow copies

If you use other browsers that do not allow this type of extension, such as Internet Explorer, you can use tools such as the **SmartScreen** filter, which indicates whether the page you are accessing is legitimate or whether it is trying to impersonate another. To activate this filter, select the **Security** tab **SmartScreen Filter Activate filter**.

[Figure 10]
Blocking Macros in
Microsoft Office



A more drastic, but very effective, measure is to disable the execution of **JavaScript**²⁹, allowing it to be activated only on trusted websites. Executing this type of code is dangerous because it can allow the automatic activation of harmful code that downloads and executes ransomware on the machine.

Disabling JavaScript can be achieved in the settings of the web browser itself or by using extensions such as **NoScript** (FireFox) and **ScriptSafe** (Chrome). This measure, effective in preventing the execution of harmful code, is the most intrusive for the user and can cause problems with some of your usual websites, causing them not to display as they should or eliminating some functionalities.

Among these functionalities are some *plugins*, data visualisation, web presentations, search engines and graphic elements in general. The deactivation of JavaScript, therefore, gives a much flatter appearance to the website.



29. See: https://developer.mozilla.org/es/docs/Learn/JavaScript/First_steps/What_is_JavaScript

7.8 Known file extensions

Cloaking is a deception technique widely used by malware in general and byphishing in particular. The idea is to hide an executable file under the guise of a non-executable and seemingly innocuous one.

For the convenience of the user, in current operating systems, the most common file extensions are omitted from the file name and their icon is chosen to be the most representative for that file type.

This behaviour can be used to trick the user into thinking that a file is something other than what it really is; for example, an executable process could pretend to be an image by having a name ending in ".jpg", but actually be a file with the ending ".jpg.exe" which is something completely different. By having the option to hide known extensions enabled, the user will not see that it is an executable and not an image.

To show hidden extensions, you need to access the folder options in Windows Explorer. The easiest way is from the toolbar of any Explorer window, by choosing the **Folder Options** option under the **View** menu. Once in the folder options, in the View section, the **Hide extensions for known files** option must be deactivated.

Another way of abusing this behaviour is the creation of shortcuts whose icon is modified to make the user believe that it is a known file type. The way to distinguish a file from a shortcut is as simple as looking at the bottom left corner of the icon, which, if it is a shortcut, will show an arrow indicator and should not be used unless you are confident of its provenance.

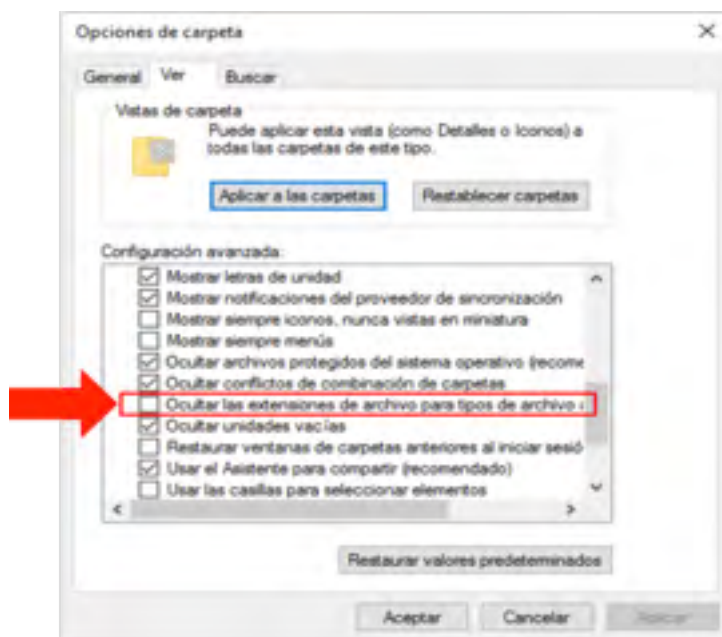
Cloaking is a deception technique widely used by malware in general and byphishing in particular



7. Shadow copies

[Figure 11]

Option not to hide known extensions



7.9 Applocker

AppLocker³⁰ is an application introduced in Windows Server 2008 R2 and Windows 7 that extends its application control features and execution policies.

This tool is used to create rules based on file attributes (name, digital signature, etc.) in order to control access to the software installed on the computer. This control allows, among many options, to block access to a particular program or service. Detailed information on AppLocker can be found at the following link:

[https://technet.microsoft.com/es-es/library/mt431725\(v=vs.85\).aspx](https://technet.microsoft.com/es-es/library/mt431725(v=vs.85).aspx)



30. See: [https://msdn.microsoft.com/es-es/library/ee424367\(v=ws.11\).aspx](https://msdn.microsoft.com/es-es/library/ee424367(v=ws.11).aspx)

7.10 BYOD policies

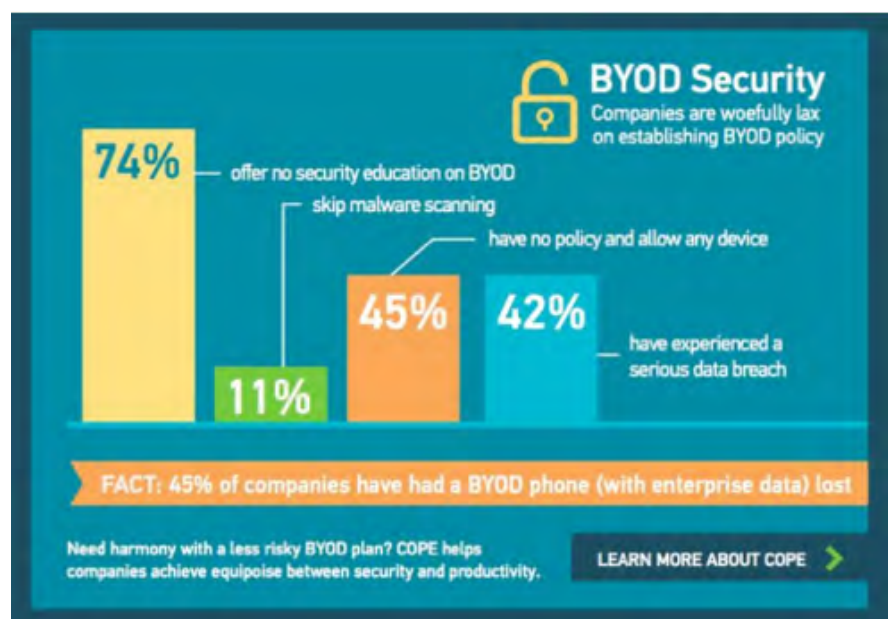
As BYOD expands (as many as 74% of organisations have such policies in place or plan to introduce them in the future), employers or managers of organisations must ensure that both their employees and the company itself are adequately protected against the new risks they are exposed to.

Such risks may involve:

- ▶ Loss of customer or company information.
- ▶ Unauthorised access to the company's network.
- ▶ Malware infections.

As BYOD expands, employers or managers of organisations must ensure that both their employees and the company itself are adequately protected against the new risks they expose themselves to

[Figure 12]
Statistics on
policies derived
from BYOD
implementation



Here are some recommendations to mitigate risks as much as possible:

- 1** Ensure that devices are not unlocked without entering a PIN, pattern or password. It seems obvious, but more than 30% of users do not set up any access protection on their device because it is more cumbersome.
- 2** Monitor the connections being made, especially at Wi-Fi access points, which should be properly configured and always password protected. Other controls can also be implemented, such as whitelisting access control or MAC filtering.
- 3** Regular backups.
- 4** It is interesting to have "Find my device" type services available, as implemented by many Android smartphones, which can be located (even without GPS enabled) via the associated Google account, even allowing the information to be deleted if necessary.
- 5** Business-related data should never be stored on devices that are to be used outside the company.
- 6** Have specific antivirus for mobile devices or tablets.
- 7** There are many commercial applications that scan the system for harmful code, as well as providing an extra layer of protection against the most common threats. While having such software does not guarantee freedom from attack, it is an indispensable measure.
- 8** As mentioned above, software offering MDM, such as Docker or Sandbox, should be used. The IT team should evaluate the different possibilities and examine them thoroughly in order to make the best choice.

For more information, please consult the CCN guide on Android security, CCN-STIC Guide 453C.

7.11 Secure passwords

As mentioned, it is important to have robust access credentials to the services deployed by the organisation. It is also essential to ensure that users and passwords that are already configured by default are never used; they need to be reset. Here are some tips on how to choose a secure password:

- ▶ **Use a combination of alphanumeric characters: it is imperative that passwords are not limited to a sequence of letters or numbers only.**
- ▶ **Use different passwords for each service.**
- ▶ **Length not less than 12 characters.**
- ▶ **Use of symbols to make brute force more difficult, as well as alternating upper and lower case.**

Ideally, the password should be **random**. The robustness of the chosen sequence can be tested on web services such as <http://password-checker.online-domain-tools.com/> where it will be estimated how difficult it would be for an attacker to guess it by brute force or dictionary attacks (it is recommended to use a similar password and not the final one).

Following these steps can significantly mitigate attacks against services such as the aforementioned RDP.

It is important to have robust access credentials to the services deployed by the organisation



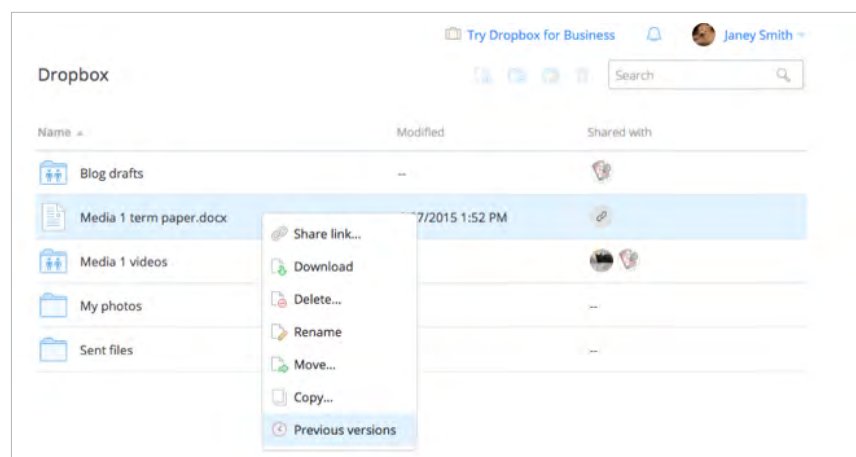
7.12 File retrieval via cloud storage

For some time now, the use of **file synchronisation**³¹ or cloud storage **services has been** very common³² ou de stockage en nuage.

When the content of a local folder is synchronised with another in the cloud, both locations have the same files. If a local computer is attacked by a ransomware agent, the local copies will be encrypted and then the synchronisation system will copy those same files to the cloud, deleting the previous ones, so that the cloud copies will also be encrypted.

However, file deletion is an apparent action in many of these cloud storage services, as it is really a version-controlled file system³³.

[Figure 13]
Version control in Dropbox



31. See: <https://support.microsoft.com/es-es/office/v%C3%ADdeo-%C2%BFqu%C3%A9-es-la-sincronizaci%C3%B3n-de-archivos-7b265f0e-2e36-478a-8857-7026b9ec831c>

32. See: <https://azure.microsoft.com/es-es/overview/what-is-cloud-storage/>

33. See: <https://www.techopedia.com/definition/1861/versioning-file-system>

7. Shadow copies

In these systems, deleted files are not actually deleted, but are stored as a previous version that remains accessible to the administrator of the cloud service.

In such cases, and depending on the service provider's policy, it is sometimes possible to remove encrypted (hijacked) versions from the cloud and recover older versions of the same files.

Both **Dropbox**³⁴ and **Google Drive**³⁵ offer possibilities in this regard, so you should always consider restoring what you had synchronised in the cloud. Obviously, the restore operation should be done after the affected computer has been completely wiped clean.

7.13 When all seems lost

Once the system has been infected and the ransomware has managed to encrypt the entire accessible file system, it may be the case that by consulting specialised forums there is no antidote that allows the information to be recovered. In this case, **it is not advisable to delete the affected files**.

The fact that a tool for decrypting the hijacked files does not exist at the moment does not mean that it may not exist in the near future. In that case, it is better not to destroy the only existing copy of the files, even if it is encrypted with a key that is not available at the time.

The most advisable is:

- 1 **Copy all encrypted files to an empty external drive.**
- 2 **Clean and disinfect infected equipment.**
- 3 **Secure a backup copy of the encrypted files until some way of recovering the files is known.**

34. See: <https://www.dropbox.com/help/11>

35. See: <https://support.google.com/docs/answer/190843?hl=es>

8. Conclusion

When securing a computer system, it is necessary to apply all available measures and, if possible, to organise them in layers to make it more difficult for any attack to succeed.

In addition, rapid detection of the infection can stop it, limiting the number of files affected. The computer is then completely cleaned and attempts are made to recover the files that have been affected.

Since the real risk of ransomware is that it hijacks **the only available copy of a file**, the entire resilience of the system depends on keeping properly **updated, encrypted** and **signed backups** out of reach (**off-line**) of your computer. Having a proper backup of important files makes a ransomware attack a nuisance, rather than a disaster. Finally, to keep up to date with security measures against ransomware, we recommend reading the CCN-CERT Threat Report IA-11/18.

When securing a computer system, it is necessary to apply all available measures and, if possible, to organise them in layers to make it more difficult for any attack to succeed



9. Basic security decalogue

This Decalogue of Best Practices aims to lay the groundwork for security measures against ransomware.

- 1 inform and raise awareness among all users of the risks and threats posed by ransomware, so that their awareness, alertness and education will reduce the likelihood of infection.
- 2 Maintain an up-to-date backup/backup system of both local systems and remote locations. If possible, at least two backups should be kept in different locations and disconnected from the system.
- 3 Disable macros in microsoft office documents and other similar applications.
- 4 Disable windows script host to prevent the execution of scripts on the system. to do this you can follow the steps described in the following microsoft link:
<https://technet.microsoft.com/es-es/library/ee198684.aspx>
- 5 Follow the published recommendations on e-mail protection. (see ccn-cert guide bp-02/16).
- 6 Complement your personal antivirus and firewall with programs such as applocker (program execution blocking) and emet (detection and blocking of exploit techniques).
- 7 Maintain secure browsing behaviour, using fully updated web browser tools and extensions that help prevent unauthorised code execution in the web browser.
(see ccn-cert guide bp-06/16)
- 8 Enable the display of file extensions to prevent the execution of harmful code disguised as a legitimate non-executable file.
- 9 Configure windows uac (user access control) as restrictively as possible, always asking for confirmation for the execution of those processes that require high privileges.
- 10 Keep the operating system and all security solutions up to date, as well as the personal firewall enabled. do not use default users and passwords.



