Fidelity IT Department

How to Improve the IT Security Strategy & Prevent Ransomeware Infections

Corporate Guidelines

February 2019

Table of Contents

Executive Summary

In recent years, articles of the type "Company X had to pay 'ransom' for their data" or "Public Organization Y can not serve the public because their information was hacked" are increasingly common.

It seems that although organizations are prepared to face different types of physical incidents such as power outages and floods, it is still common for the whole data infrastructure to be vulnerable because someone clicked on a malicious link or opened an email attachment. Due to this many organizations fight against malware and in particular against RANSOMWARE.

Given the prevalence of Windows operating systems as the target (more than 90%) of ransomware, the guide is largely oriented towards that environment.

This document is intended to be a an in Depth guide based on a checklist, to avoid infections with ransomware and, ultimately to create adequate procedures for the retrieval of information.

Introduction

Ransomware (from the English ransom: rescue and ware: software) is a type of malware that restricts or blocks access to certain components or files of the infected system, and asks for a "rescue" to release them.

Some types of ransomware encrypt sensitive files of the operating system and others encrypt user files, office automation, databases, etc. coercing the owner to pay the ransom that will allow deciphering them. After encryption, the original files are deleted safely so that they can not be recovered by traditional methods.

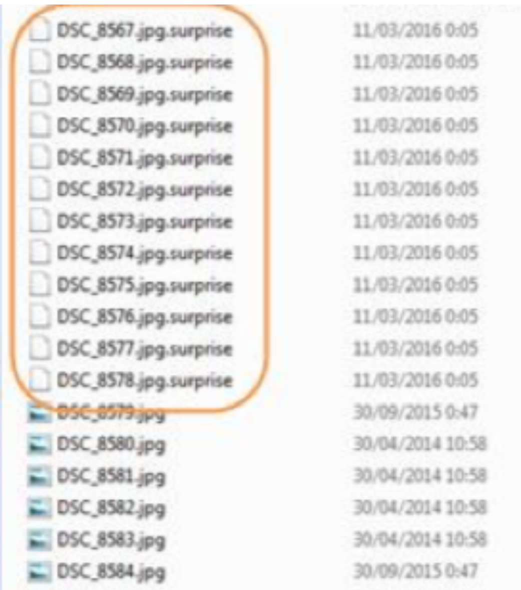
Ransomware affects businesses, governments, critical infrastructures and even domestic users, and the consequences include:

- Temporary or permanent loss of sensitive or confidential information;
- Interruption of the organisation's operations;
- Financial losses incurred to restore systems and files,

  or in the worst case, for the ransom payment;
- Potential damage to the reputation of the organisation;
- Criminal or civil liability.

This image shows an infection process, where part of the files are already encrypted and deleted.

The ransomware usually encrypts the information in all drives, both the host of the operating system and those mapped to other equipment. This includes any drive assigned to external drives, USB drives, network drives and in the cloud. This situation becomes critical when the infected computer is connected to a file server or a system responsible for backup, since the original files and the respective backup copies will be encrypted.



DSC_8567.jpg.surprise	11/03/2016 0:05
DSC_8568.jpg.surprise	11/03/2016 0:05
DSC_8569.jpg.surprise	11/03/2016 0:05
DSC_8570.jpg.surprise	11/03/2016 0:05
DSC_8571.jpg.surprise	11/03/2016 0:05
DSC_8572.jpg.surprise	11/03/2016 0:05
DSC_8573.jpg.surprise	11/03/2016 0:05
DSC_8574.jpg.surprise	11/03/2016 0:05
DSC_8575.jpg.surprise	11/03/2016 0:05
DSC_8576.jpg.surprise	11/03/2016 0:05
DSC_8577.jpg.surprise	11/03/2016 0:05
DSC_8578.jpg.surprise	11/03/2016 0:05
DSC_8579.jpg	30/09/2015 0:47
DSC_8580.jpg	30/04/2014 10:58
DSC_8581.jpg	30/04/2014 10:58
DSC_8582.jpg	30/04/2014 10:58
DSC_8583.jpg	30/04/2014 10:58
DSC_8584.jpg	30/09/2015 0:47

In general, ransomware encryption is often impossible to reverse since a combination of symmetric and asymmetric cryptography algorithms is used, and each file is encrypted with a unique key. Finally, the malware leaves a "ransom note" on the user's desktop and / or in files in different system folders (in English or in several languages), so that the victim knows the procedure to recover their hacked files.

In some cases, programming errors introduced in the malware allow developing an application to find the password, decrypt and recover the files, without paying. But, with the exception of those types of malware that have errors in their development, the only way to decipher them is by paying the ransom to obtain the corresponding passwords.

When paying the “ransome", usually in the cryptocurrency Bitcoin or Monero, the offender sends (or not) / s password / s so that the victim can decrypt the files.

“We strongly advise not to pay the ransom, as it simply encourages the scammers to continue with their profitable business model”

Yet there is no guarantee that you will ever receive the data back and if you do, it might be damaged. “Funding cyber criminals also funds larger cyber-attacks, so it must be reiterated that paying won't always get make the issue go away,”

Some known and widely spread ransomware are: Alphacrypt, Cerber, Chimera, CryptorBit, CryptoDefense, CryptoLocker, CryptoWall, GandGrab, Locky, LowLevel0, OphionLocker, Petya.

Here (https://docs.google.com/spreadsheets/d/1TWS238xacAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml) you can find an updated list of know ransomware variations together with their main characteristics and in some cases known decryption tools.

Currently, ransomware can be found on desktop operating systems such as Windows, Linux and Mac OS, as well as mobile operating systems such as Android, iOS and Windows Mobile. IoT (Internet of Thing) devices are also being hit by this threat, which will lead to infections in televisions, refrigerators and even cars.

The purpose of this guide is to disclose different countermeasures that can be used to reduce the risk of potential ransomware infections or, if necessary, try to reduce their impact by recovering the affected files.

How to avoid getting infected

None of the following measures is effective on its own and should be used as a whole as part of a layered and tiered security strategy, so that each of them contributes to making the system and the network more robust and secure.

1. Make periodic backups

Backup is a reactive measure, it does not help to prevent becoming infected, but it is so important that we have decided to include it first in the list. The only and most important tool against ransomware are backup copies.

If a malware encrypts or damages the files, recovering the last backup is the best alternative. In this way, you avoid losing information or having to pay the ransom for the data.

The backup copies must be made off-site, and the units used to perform the backup must not be mapped on the network to prevent the backup files from being reached by the ransomware.

The backup and recovery processes must be tested periodically and must be properly documented.

2. Raise awareness and train users

One of the main entry doors for ransomware are users with negligent habits and behaviours, mainly due to lack of information about current threats.

For this reason, it is recommended to carry out users training within the scope of a process of threat awareness. The goal is to learn and understand the risks associated with the use of computer resources and the Internet, and develop habits and behaviours that allow them to make responsible and safe use of them.

3. Apply the Principle of Least Privilege

If all the processes necessary to perform users tasks run with the lower possible security privilege, it will be more difficult for malicious software to run in that user's environment, either infecting the computer or spreading to others.

The use of administrative permissions facilitates the execution of harmful applications and the installation of malware. An "administrator" (or "root") user should only be used when it is necessary to perform a task that requires it, authorized by senior staff and audited on a regular basis.

Therefore, to reduce the risk of a ransomware infection, each user must be able to access only the information and resources that are necessary to perform their authorized tasks.

Each user should also access the systems using unique user credential and password. If you login this way and the model of the minimum privilege is met, you will only have access to the information and data you need, within your profile and to no sensitive directory of the operating system, which minimizes the impact of a possible infection.

For simplicity, this concept is summarized in saying that the number of "administrator / root" users should be minimal within an organization.

4. Segment the Network

The segmentation of the network through VLAN2 and ACL3 allows controlling traffic between networks of different relevance (for example, the user LAN and the servers LAN).

Segmenting a network does not prevent a ransomware attack from having access to the systems, but it will be very helpful to limit the infection and ensure that the malware remains isolated only in the network segment that has been compromised, and thus does not spread throughout the entire network.

This is particularly important for organizations that maintain legacy systems, which can no longer receive security updates.

5. *Review shared resources and external devices*

Periodic revisions of shared resources (disk drives, printers, folders, etc.) and external units (pendrives, memory cards, hard drives, etc.) connected to the equipment should be made, in order to determine if it is necessary to remain shared or not and, if necessary, establish the minimum permissions for correct performance.

6. *Use antivirus solutions*

It is advisable to use (at least) two antivirus programs: one in devices located at the perimeter of the network -firewall and corporate mail- and another one for internal clients and workstations. To avoid paying for additional licenses, you can use a paid product and a free or Open Source product.

Note: Only one antivirus should be installed on workstations.

Due to the dynamism of malware, it is normal for the antivirus software to "take" an average of 48 hours to react to a new type of threat as is the current ransomware. The longer since the appearance of a new type of malware, the greater the possibility of detection by the product.

No antivirus is infallible, but having two or more products at different levels within the organization multiplies the possibility of detection.

Most current antivirus programs allow you to analyze the inside of compressed files in search of malware. These files will be analyzed as long as the file does not have a password.

In the case of Windows 10 (editions 2018 onwards), you can use the protection of specific folders against ransomware, configuring this option within the Security Center of Windows Defender.

7. Use antispam, firewall and content filtering

Various tools and filter recommendations are mentioned to protect the infrastructure and prevent the threat from reaching users.

Content filtering can be done manually from the mail client or from the corporate mail server, firewall, proxy or UTM, depending on what the organization decides.

Filtering at the firewall level: Generally, the ransomware must communicate with a Command and Control Center (C & C) via the Internet, to send the encryption passwords and receive instructions. The use of a firewall is fundamental (although it is not an infallible tool) in blocking this communication channel between the malware and its Command and Control Center.

8. Show file extensions

When using Windows operating system, it must be taken into account that, by default, it hides extensions for known file types (.EXE, .TXT, .SCR, etc.). This is a problem because, a traditional method of spreading malware is to use double extensions to trick the user. For example, if the file is called file.pdf.exe or file.docx.scr, Windows will display file.pdf or file.docx.

9. Filter files with dangerous extensions

The content filter can be done from the mail client or from the corporate mail server, the firewall, the proxy or the UTM, depending on what the organization decides.

Organizations that have the administration of their mail server could filter attachments with dangerous extensions (executables and scripts) through blacklists. Depending on the size of the organization, white lists can be implemented.

In case it is necessary to exchange compressed files, a temporary quarantine can be used. For example, an administrator should authorize the entry of the received files or they can be "parked" 24/48 hours to allow time for the antivirus to update its database of signatures.

Initially, at least the following types of files should be blocked: BAT, CMD, COM, CPL, DLL, EXE, JAR, JS / JSE, LNK, MSI, PIF, PS1, SCR, VBE / VBS, ZIP / RAR

10. Install operating system and application updates

The exploitation of vulnerabilities and exploits is a common factor in most malware. Criminals take advantage of bugs and lack of updates to the operating system and traditional applications such as browsers (Internet Explorer, Edge, Firefox, Chrome and Safari), Java, Flash Player and Adobe Reader, among the most popular.

All installed applications should be updated as soon as possible, either through an automatic configuration / tool or manually through the official site of the manufacturer.

It should be noted that certain browsers started to block Java and Flash Player by default since 2017 and, due to the large number of vulnerabilities that have been found, Java, Flash Player and Adobe Reader should be uninstalled whenever possible. In the case of the first two, in general they are not necessary and the last one could be replaced by an equivalent, such as Foxit Reader.

11. Disable execution of temporary files

By avoiding the use of administrative permissions, the files downloaded by the user are stored in local and temporary folders of their profile. In Windows, some of them are:

●% AppData% \

●% LocalAppData% \

●% LocalAppData% \ Temp \ ●% ProgramData% \

●% Temp% \

●% userprofile% \

●% WinDir% \ temp \

●% WinDir% \ SysWow \

The malware usually runs almost always in one of these directories. Therefore, the execution permissions on them must be blocked so that the harmful files can not be executed. To block access to these directories, you can use local software restriction policies or Active Directory GPOs ("secpol.msc").

12. Disable remote desktop

In remote desktop applications such as RDP (native Windows), VNC or TeamViewer, infection is common through the use of vulnerabilities and the use of weak passwords. When possible, these applications should be disabled and, if remote access is required, the implementation of a VPN is recommended, and its configuration should be limited only to the necessary equipment within the corporate network.

Within the framework of an in-depth defense model, it is proposed to strengthen the RDP connections with the encryption of communications through digital certificates based on PKI (X.509), preferably issued by a certifying entity (CA.) external trust (Symantec, Comodo, Goddady, etc). Another possibility is to use Remote Desktop Web Client or Remote Desktop Service (RDS).

Additionally, it is recommended to apply the following controls over remote desktop connections:

● Establish a robust password;

● enable double authentication factor (2FA) (when possible);

● use the latest versions available with all updates and patches.

13. System Restore

Windows operating systems have the functionality "System Restore", which allows restoring the operating system to a state prior to an incident. Whoever manages a domain, through a GPO, will be able to enable / disable the Volume Shadow Copy service ("vssvc.exe" - "Volume Shadow Copy") on the network equipment that is considered appropriate to protect.

However, it is important to note that, the ransomware, also uses this service to eliminate backup copies, therefore, it will be useful only in case the malware has not eliminated them. In any case, the best recommendation is to have it enabled, to increase the chances of recovering the affected system.

14. *Deactivate macros and ActiveX in office automation tools*

One of the propagation techniques used by the ransomware, are the malicious attachments of office automation (DOCX, XLSX, ODT, etc.) sent as attachments through emails. These documents contain macros that are automatically executed when the document is opened.

Subsequently, the macro downloads and executes an EXE file, which is the real Trojan / ransomware that infects the system.

15. *Disable scripting services and consoles*

Spam campaigns containing compressed attachments such as ZIP and RAR with VBS (VisualBasicScript) or JS (JavaScript) files have become popular. If the user executes the attached script, then the malware (.EXE) that is usually a ransomware is downloaded and executed.

Windows operating systems, by default, open scripts with the Windows Based Script Host (WSH) application. Therefore, the recommendation is to disable the service in question through a group policy (GPO) or locally. In the same way it is recommended to disable or uninstall Windows Power Shell and CMD since most of the users do not require these tools.

16. *Block advertising and pop-ups*

It is common to find malware embedded in website advertisements, as these outsource their spaces to display advertisements related to the content of the website. This technique is called Malvertising (Malware + Advertising) and, therefore, just by visiting a site with these characteristics, you can infect the victim's system automatically.

The measure of protection to apply, is to install an add-on in the browser to block pop-ups and advertising. Two free and effective blockers are Adblock and Adblock Plus, which work in any browser and can be installed through a GPO.

17. Deactivate Autorun / Autoplay

Since the launch of Windows Vista (year 2006), the "Autorun / Autoplay" service of external storage media, such as USB and CD, is disabled by default, but in previous versions it is activated. In some occasions (still), it is possible to find malware that spreads through USB devices using this function and therefore, it must be deactivated.

Through the use of GPO or manually in a local computer, this service can be deactivated, in such a way that the autorun file does not run automatically when an external device is inserted.

18. Turn off wireless connections

On mobile devices, over which there is generally no adequate control (phones, tablets and notebooks), the use of wireless networks (bluetooth, infrared and Wi-Fi) should be disabled whenever possible, because of the risk of malware spreading through automatically.

19. Disable or remove obsolete protocols

Obsolete protocols are usually left activated (eg FTP, TELNET, etc.) although the organization does not use them and because nobody has noticed this situation.

These protocols should be replaced by updated versions to address security vulnerabilities, or directly removed because they are not required in normal business processes.

An example of this situation is the implementation of the SMBv1 protocol in Windows environments. It should be remembered that SMBv1 is one of the infection vectors used by Wannacry ransomware to spread through the network. Maintaining this version of the protocol is justified in very few cases:

- When there are still computers with Windows XP or Server 2003, under a customized support agreement;

- there is old management software or legacy programs that require users to navigate through a master list of "network neighborhood";

- there are multifunction printers with old firmware, used in order to "scan to share".

None of these things should affect the end user or the business. Unless the administrators allow it or do not manage the corresponding mitigations.

20.Manage obsolete operating systems

Any software without the manufacturer's support or whose life cycle is about to expire is considered "obsolete".

The primary idea is to analyze the risks arising from maintaining obsolete operating systems on computers connected to the corporate network (eg Windows XP or Server 2003) and the resulting possibilities, if they exist. When an operating platform reaches the end of its "useful life" it is highly likely that it will stop receiving updates from the manufacturer. With the passage of time new vulnerabilities appear, which are not always evaluated or patched, increasing the attack surface of the entire network of the organization.

In some cases, such as ATMs, industrial environments or embedded applications, it is not possible to replace the hardware and / or the "old" operating system, so migrating to a more current version of the platform is not usually an immediate option. Therefore, these cases should be monitored in a timely manner and subject to possible changes, such as preventing them from connecting to the Internet, enabling a local firewall, disabling ports or idle services, etc.

Conclusion

Ransomware, has been the protagonist threat for the last 3 years and probably, will remain to be in 2019.

It is necessary to implement a progressive security strategy in layers so that the impact for the normal functioning of an organization is as tenuous as possible.

We want to contribute and help prevent infections, in order to reduce the number of cases and combat all ransomware.

The present guidelines have been developed with the aim of providing the IT community with a simple guide to follow when dealing with the ransomware problem.

All the points of this guide have been summarized and written in a language as simple as possible, so that it can be read fluently and with a minimum reading time.