# Aiuken Solutions

| | |
|---|---|
| **Classification:** | **Confidential** |
| **Area:** | |
| **Author:** | **Aiuken Solutions** |
| **Creation date:** | |

*DISTRIBUTION LIST*

This document has been published (issued) to the following:

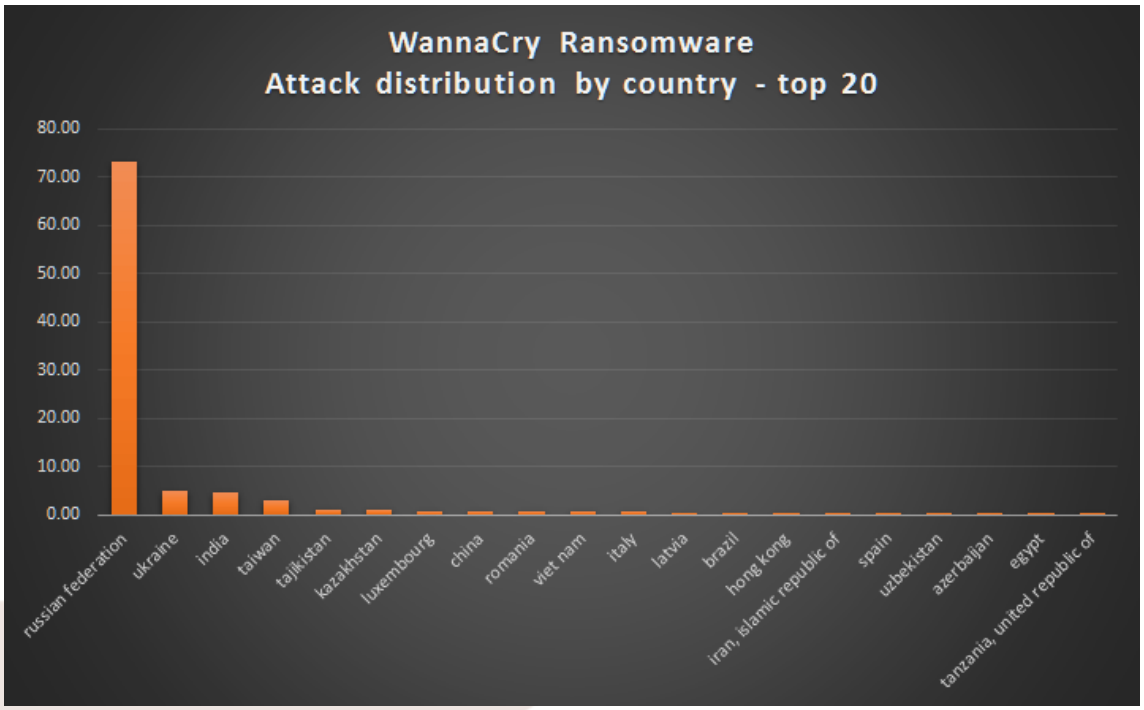
| Name | Area |
|---|---|

*COPYRIGHT*

## Content

## Introduction

About the attack of Ransomware detected initially in Spain (Telephone Company), with massive involvement on Windows computers of multiple versions, which uses a version of the malware WannaCry, which is added the following information.




There have been attacks in 74 countries around the world, with Russia the main affected

# High-level mitigations Recommended

## Reactive measures

• Disconnect computer on the network.

• Apply Current Anti-Ransomware tools (if available) released for strains already known, such as for example: HidraCrypt, Petya, etc.

• report to the brigade of cybercrime this type of crime to send the signal that this type of incidents if they are crimes and should be prosecuted criminal responsibilities of those involved, to be affected public faith, institutional systems and the privacy of citizens.

If the identification of the Ransomware occurs while you are encrypting the disk, remove the disk, and look for possible the encryption key to reverse the process.

## Preventive Measures

• Check if the computers of the company have installed the update patch ms17_010 of Microsoft.

• Stop the SMB service through policies GPO

Detection of new computers on the internal network

• Review the Firewall Rules on communications to the internet or non-secure networks on port 445 (SMB). Lock in case of suspicion.

• Enable the snort rules, IDS and IPS on indicators of the document

## Behavior of the Cyber Attack

It is believed that the malware may have infected companies for a vulnerability in the Windows SMB services (port 445) which when exploited allows you to take complete control of the computer remotely, and in this case, download and run the Ransomware. This information is based on the statement by the CCN-CERT of Spain.

This vulnerability was parched By Microsoft on 14 March 2017 under the code ms17_010, from the hand of the filtration of the tools of the CIA by the Shadowbrokers team of hackers. This filtration contained the exploits needed to exploit this vulnerability, even with a graphical interface for ease of use. There are many guides on the internet that explained step by step with photos and videos) on how to exploit this.

Exploitation of the vulnerability is quite simple and is carried out via the SMB protocol (Port 445) of Windows machines using the technique of Double click Eternal blue with. Once exploited the vulnerability and installed the Backdoor is to download the ransomware and to make their infection.

According to the NCC-CERT of Spain ransomware used is the WannaCry, which once infected the computer encrypts all files on your hard disk drive and request a reward for that which must be paid through Bitcoins and the Tor network.

***Note:*** *To be an attack in progress, there is no complete certainty of how it develops, however what is described in this section is the product of the analysis and the sharing of information between centers of cyber-security. Once mitigated the cyber-attack will be carried out all the forensic analysis to detect the origin and exploited.*

## Affected Systems

The following Windows versions that have the SMB service enabled may be affected:

- Microsoft Windows Vista SP2
- Windows Server 2008 SP2 and R2 SP1
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2012 and R2
- Windows 10
- Windows Server 2016

# Technical Context

Then, we'll describe the various technical aspects of the attack, as vectors, vulnerabilities exploited, hashes, snort rules, etc.

## Hashes of Malware

The following table includes the signatures of the different versions of the Malware used

| Type | Hash |
|---|---|
| FileHash Hash-SHA256 | Ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa |
| FileHash Hash-SHA256 | B9c5d4339809e0ad9a00d4d3dd26fdf44a846a54abf32819bb9b560d81391c25 |
| FileHash Hash-SHA256 | 2584e1521065e45ec3c17767c091097fc6291c065429038ea8b22c8a502c41dd |
| FileHash Hash-SHA256 | Ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa |
| FileHash Hash-SHA256 | 09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa |
| FileHash Hash-SHA256 | 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c |
| FileHash Hash-SHA256 | F8812f1deb8001f3b85640b6fc7672ECB123bc2304b563728e6235ccbe782d85 |
| FileHash Hash-MD5 | 509c41ec97bb81b0567b059aa2f50fe8 |
| FileHash Hash-MD5 | 7bf2b57f2a205768755c07f238fb32cc |
| FileHash Hash-MD5 | 7f7ccaa16fb15eb1c7399d422f8363e8 |
| FileHash Hash-MD5 | 84c82835a5d21bbcf75a61706d8ab549 |
| FileHash Hash-MD5 | Db349b97c37d22f5ea1d1841e3c89eb4 |
| FileHash Hash-MD5 | F107a717f76f4f910ae9cb4dc5290594 |
| FileHash Hash-SHA1 | 51e4307093f8ca8854359c0ac882ddca427a813c |
| FileHash Hash-SHA1 | 87420a2791d18dad3f18be436045280a4cc16fc4 |
| FileHash Hash-SHA1 | Aff889544e85ffaf8b0d0da705105dee7c97fe26 |
| FileHash Hash-SHA1 | 45356a9dd616ed7161a3b9192e2f318d0ab5ad10 |

| Type | Hash |
| --- | --- |
| FileHash Hash-SHA1 | Bd44d0ab543bf814d93b719c24e90d8dd7111234 |
| FileHash Hash-SHA256 | 2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d |
| FileHash Hash-SHA256 | 4a468603fdcb5770705898A2eb7cf9ef37AADE532a7964642ecd705a74794b79 |

## Security Patches

The following table lists the different patches to mitigate the vulnerabilities exploited by this malware:

| Name | Vulnerability | Patch |
|---|---|---|
| EternalChampion EternalBlue EternalRomance EternalSynergy | MS17-010 | Msft-CVE-2017-0143 msft-CVE-2017-0144 msft-CVE-2017-0145 msft-CVE-2017-0146 msft-CVE-2017-0147 msft-CVE-2017-0148 |
| EmeraldThread | MS10-061 | WINDOWS-hotfix-MS10-061 |
| EducatedScholar | MS09-050 | WINDOWS-hotfix-MS09-050 |
| EclipsedWing | MS08-067 | WINDOWS-hotfix-MS08-067 |

## Exploits Available

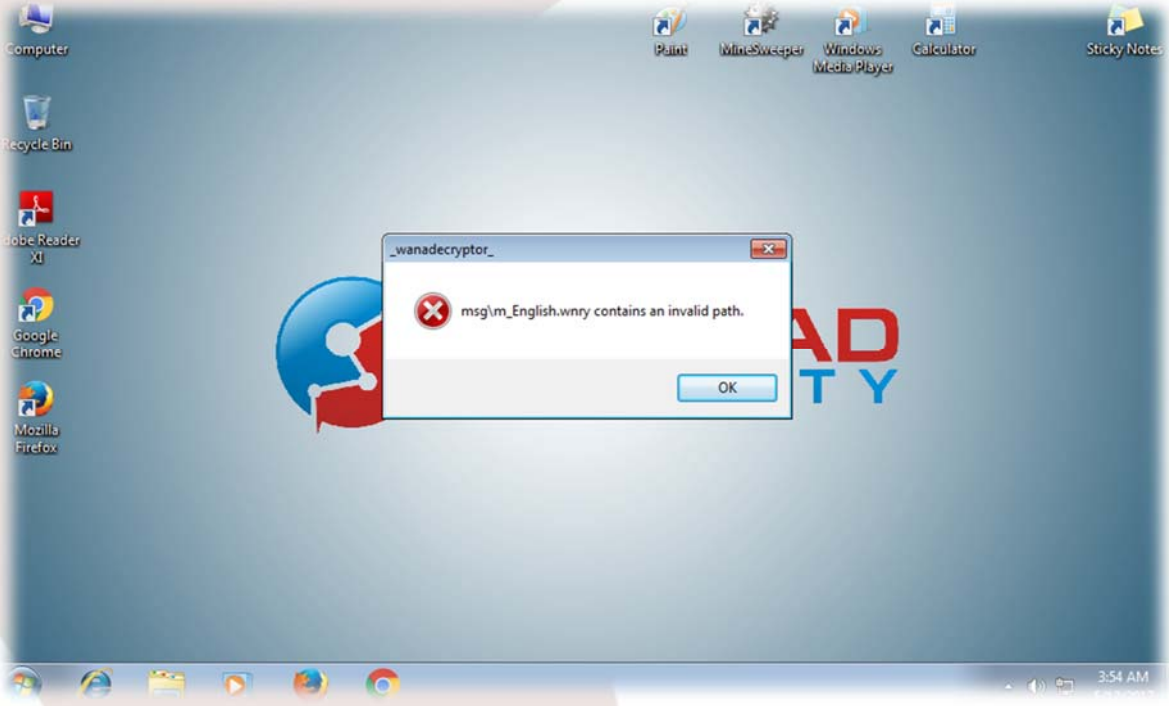
The following table lists the exploits used by malware to the exploitation of vulnerabilities:

| Name | Vulnerability | Metasploit module |
|---|---|---|
| EternalBlue | MS17-010 | Auxiliary/scanner/smb/smb_ms17_010 |
| EmeraldThread | MS10-061 | Exploit/windows/smb/PSEXEC |
| EternalChampion | MS17-010 | Auxiliary/scanner/smb/smb_ms17_010 |
| EternalRomance | MS17-010 | Auxiliary/scanner/smb/smb_ms17_010 |
| EducatedScholar | MS09-050 | Auxiliary/DOS/Windows/SMB/ms09_050_smb2_negotiate_pidhigh, auxiliary/DOS/Windows/SMB/ms09_050_smb2_session_logoff, exploits/windows/smb/ms09_050_smb2_negotiate_func_index |
| EternalSynergy | MS17-010 | Auxiliary/scanner/smb/smb_ms17_010 |
| EclipsedWing | MS08-067 | Auxiliary/scanner/smb/ms08_067_check exploits/windows/smb/ms08_067_netapi |

## IP addresses of the Malware

| | |
|---|---|
| 149.202.160.69 | 62.138.7.171 |
| 197,231,221,211 | 51,255,203,235 |
| 128.31.0.39 | 51.15.36.164 |
| 46.101.166.19 | 217.79.9001:179,177 |
| 91.121.65.179 | 128.31.0.39:9101 |
| 129.128.31.0.39 | 213.61.66,116:9003 |
| 188.166.23.127 | 212.47.9001:232,237 |
| 193.23.244.244 | 81.30.9001:158,223 |
| 2.3.69.209 | 79,172.193.32:443 |
| 146.0.32.144 | 163,172,149,155 |
| 50.7.161.218 | 167.114.35.28 |
| 192.42.113.102 | 176.9.39.218 |
| 83.169.6.12 | 193.11.114.43 |
| 158.69.92.127 | 199.254.238.52 |
| 86.59.21.38 | 89.40.71.149 |

## Images of the Ransomware


## URL used by the Malware discovered

- Hxxtp://www[.]btcfrog[.]com/qr/bitcoinpng[.]php? address
- Hxxp://www[.]rentasyventas([.])com/include/rk/images[.]html
- Hxxp://www[.]rentasyventas[.]com/include/rk/images[.]html?retention=081525418
- Hxxp://www[.]ifjaposdfjhgosurijfaewrwergwea iuqerfsodp9[.]com

## TOR Nodes Used

- 188,166.23,127:443
- 193.23.244,244:443
- 2.3.69,209:9001
- 146.0.32,144:9001
- 50.7.161,218:9001

## Indicators of Commitment

The following rules help the rapid detection of infection.

### Modified Files

- C:\WINDOWS\system32\msctfime.ime
- C:\windows\win.ini
- C:\Docume~1\User\Locals~1\Temp\c.wnry
- C:\Docume~1\User\Locals~1\Temp\msg\m_English.wnry

### Registry Keys

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\IMM
- HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-1004\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\CTF
- HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\SystemShared
- HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-1004
- HKEY_LOCAL_MACHINE\Software WanaCrypt0r
- HKEY_CURRENT_USER\Software WanaCrypt0r
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-1547161642-507921405-839522115-1004
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\CTF\LangBarAddIn\
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\LangBarAddIn\

## Details of Hash Ransomware

| Field | Value |
|---|---|
| FILE NAME | *WanaDecryptor*.exe |
| FILE SIZE | 245760 bytes |
| FILE TYPE | PE32 executable (GUI) Intel 80386, for MS Windows |
| MD5 | 7bf2b57f2a205768755c07f238fb32cc |
| SHA1 | 45356a9dd616ed7161a3b9192e2f318d0ab5ad10 |
| SHA256 | B9c5d4339809e0ad9a00d4d3dd26fdf44a846a54abf32819bb9b560d81391c25 |
| SHA512 | 91to39e919296cb5c6eccba710b780519d90035175aa460ec6DBE631324e5e5753bd8d87f39 5b5481bcd7e1ad623b31a34382d81faae06bef60ec28b49c3122a9 |
| CRC32 | 4E6C168D |
| SSDEEP | 3072:eigWcR Rmrhd5U1+FLlG uiUg6p44tlL8z+mmCeHFZjoHEo3m:REd5+IZiZhLlG4AimmCo |
| YARA | None matched |
| % | 4a468603fdcb5770705898A2eb7cf9ef37AADE532a7964642ecd705a74794b79 |
| % | 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c |
| % | B9c5d4339809e0ad9a00d4d3dd26fdf44a846a54abf32819bb9b560d81391c25 |
| % | Ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa |

# High-Level mitigations recommended

## Reactive measures

- Disconnect computer on the network.
- Apply current Anti-Ransomware tools (if available) released for strains already known, such as for example: HidraCrypt, Petya, etc.
- Report to the brigade of cybercrime this type of crime to send the signal that this type of incidents if they are crimes and should be prosecuted criminal responsibilities of those involved, to be affected public faith, institutional systems and the privacy of citizens.
- If the identification of the Ransomware occurs while you are encrypting the disk, remove the disk, and look for possible the encryption key to reverse the process."

## Good General Practices

- Have an up-to-date statement of critical assets and ad hoc protection policies for the protection of the assets prioritized based on the risk (probability of realization of a threat versus impact of such materialization, for example).
- Check that the critical assets are backed up with evidence of recovery you make with a frequency according to the criticality of the assets and the optimal time windows to potential loss of data and the confidence levels of the backup tools that are implemented.
- Avoid the use of administrator accounts both the domain and local, for uses that do not require these elevated privileges. The activities must be conducted in general with the normal user profile.
- The computers that do not have the latest versions of updates in operating systems and programs such as flash, java, adobe, Internet Explorer it is recommended that are not connected to the Internet.
- In the context of management of environment of the computers of users, it is necessary to mitigate attack techniques in which are designed to hide the real extent of the data files sent to the users, to force the operating system to display it. In conjunction to this measure must educate the user to know how to recognize the extensions and which of them are potentially dangerous. To implement the control that displays the extensions, should be applied as far as possible through Policy (GPO) to all computers or in its defect for some relevant case, verifying that properties in Windows is enabled "Hide file extensions".
- If the institution is to maintain legacy applications on operating systems that are no longer supported by the manufacturer, you should consider not exposed to the Internet these teams, in attention to their high vulnerability and likely to be impacted by malware.

## Sources


- Https://otx.alienvault.com/pulse/5915db384da2585b4feaf2f6/
- Https://otx.alienvault.com/pulse/5915d8374da2585a08eaf2f6/
- Https://otx.alienvault.com/pulse/5915abfa0d3cde45e3669850/
- Https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html
- Https://malwr.com/analysis/YTllMjk1N2I0MTlmNGRlMmFhY2UyOTExMjg5ZTFiYjA/
- Https://isc.sans.edu/forums/diary/ETERNALBLUE+Windows+SMBv1+Exploit+Patched/22304/
- Https://www.euroweeklynews.com/3.0.15/news/on-euro-weekly-news/spain-news-in-english/144385-telefonica-allegedly-hacked-and-held-to-ransom
- Https://www.hybrid-analysis.com/sample/b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25?environmentId=100
- Http://www.bbc.com/news/health-39899646
- Alert Https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html CCN-CERT:
- Microsoft Security Bulletin https://technet.microsoft.com/en-us/library/security/ms17-010.aspx#ID0ERPAG:
- Information on Https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012:
- Https://support.microsoft.com/en-us/help/204279/direct-hosting-of-smb-over-tcp-ip