Universidad Nacional Autónoma de México

Facultad de Ingeniería

Ingeniería en Computación

Sistemas Operativos

Presentación: WannaCry y EternalBlue

Profesor: Gunnar Eyal Wolf Iszaevich

Alumno:

Reza Chavarria, Sergio Gabriel

Contenido

¿Qué es Malware?

Durante las épocas de desarrollo han existido múltiples casos en los que equipos computacionales son sometidas a daños ocasionados por entidades terceras con diferentes propósitos desde el ocio hasta el robo de información, interrupción de funcionamientos del sistema, alteraciones a la seguridad de diferentes sistemas de alta importancia. Estos ataques son provocados por programas maliciosos que infectan un sistema, estos denominados Malware.

El concepto de malware (contracción de "*Malicious Software"*) se da a partir de un programa o código diseñado para llevar a cabo acciones no deseadas y sin el consentimiento explícito del usuario, esto para daña a un ordenador o red, o para obtener algún tipo de benefició. Los malware son proporcionados a los ordenadores por los engaños provocados a los usuarios de estos, siendo que vienen de descargas de programas que tienen el código malicioso, engaños por medio de correos y enlaces de carácter engañoso, entre otros descuidos de los usuarios, que usualmente, no tienen en cuenta este concepto y los creadores del malware aprovechan.

Ransomware

El Ransomware (secuestro de datos) es un programa malicioso que restringe el acceso a determinadas partes de los sistemas operativos infectados a partir de dar acceso a los atacantes. Estos encriptan nuestros archivos quitándonos el control de toda la información y datos almacenados. Después de realizar el proceso el usuario es informado, a partir de un aviso emergente, para realizar un "pago de rescate" como manera de recuperación de datos.

En general existen varias maneras en las que un Ransomware utiliza para atacar el sistema operativo

- Ransomware de bloqueo: Deniega al acceso al sistema, siendo imposible darle un uso regular.

- Crypto-ransomware: Incorpora algoritmos avanzados de cifrado los cuales provocan el bloqueo de los ficheros del sistema la información almacenada en el disco de la víctima.
- Modificación del MBR (Master Boot Record): Este permite al SO arrancar con normalidad. El MBR infectado lleva un proceso de cifrado de la MFT (Master File Table) la cual contiene los punteros a directorios del sistema. Esto haciendo inaccesibles los ficheros.

A partir de esta información general y tener un panorama de lo que un Ransomware puede afectar, existen variantes derivados de este. A continuación, se hablará acerca de un derivado del Ransomware que es llamado 'WannaCry'

WannaCry

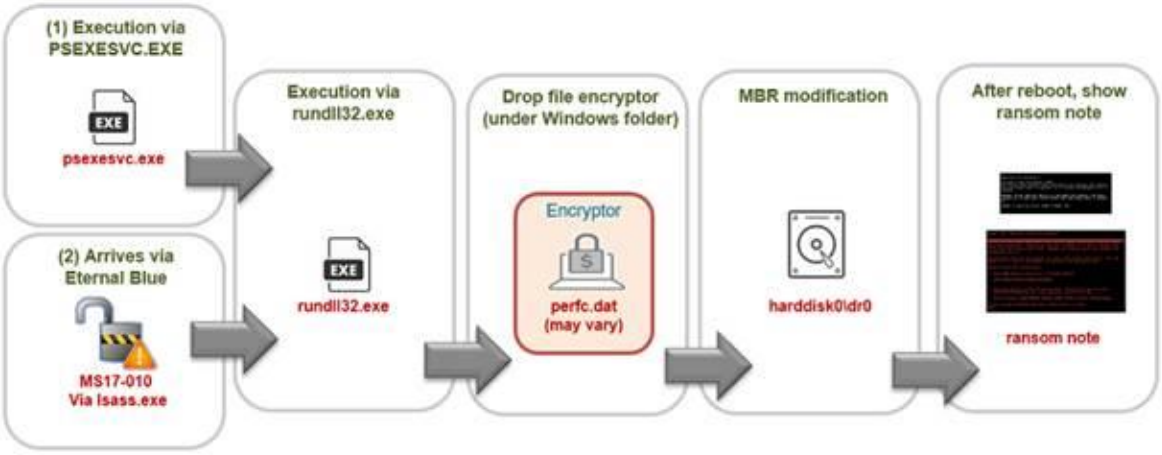
Este ataque es un derivado de un Ransomware que son dirigidos al sistema operativo Windows de Microsoft. Este aprovecha una debilidad en el sistema operativo Windows, derivado de un ataque que se había desarrollado por la Seguridad Nacional de Estados Unidos.

Y a partir de esto ¿por qué llega a infectar o a tener acceso y que hace tan relevante este tipo de Ransomware? La respuesta es acerca de su origen y su aprovechamiento de una vulnerabilidad. Esta vulnerabilidad es ubicada en el protocolo de Server Message Block (SMB) de Microsoft.

Protocolo SMB

Este protocolo de red permite el compartir archivos, impresoras y puertos seriales, entre nodos de una red computacional. En un entorno de red, los servidores ponen a disposición de los clientes sistemas de archivos y recursos. El protocolo SMB puede usarse a través de internet sobre el protocolo TCP/IP o sobre otros protocolos de red. A partir de esto, un programa puede acceder a los archivos en un servidor remoto, recursos. Los sistemas operativos de Windows a partir de Windows 95 son compatibles con este protocolo.

A partir de la funcionalidad y los privilegios que tiene este protocolo, la NSA desarrollo un exploit (fragmento o secuencia de comandos que aprovecha un error o vulnerabilidad para provocar un comportamiento no intencional en un software) aprovecha una vulnerabilidad encontrada en el protocolo SMB, denotado como 'CVE-2017-0144' (este encontrados desde la versión SMBV1 en Windows Vista SP2). Esta vulnerabilidad puede permite a los atacantes remotos ejecutar código arbitrario a través de paquetes diseñados. Este exploit es denominado como EternalBlue.



Características

Para la propagación se utiliza un gusano de red, que utiliza la vulnerabilidad con EternalBlue.

Tamaño	3.723.264 bytes
Fecha interna	20/11/2010 10:03
Compilador	Microsoft Visual C++ 6.0
Nombre	mssecsvc.exe

Secciones utilizadas por el gusano.

Nombre	Tamaño	Uso
.text	36.864	Almacenamiento de las instrucciones en código máquina
.rdata	4.096	Datos de cadenas, constantes e información de directorios
.data	159.744	Variables globales inicializadas del programa
.rsrc	3,518.464	Contiene información de recursos para un módulo. Consta de una estructura de directorio de recursos.

También hay un fichero PE que se encuentra en los recursos.

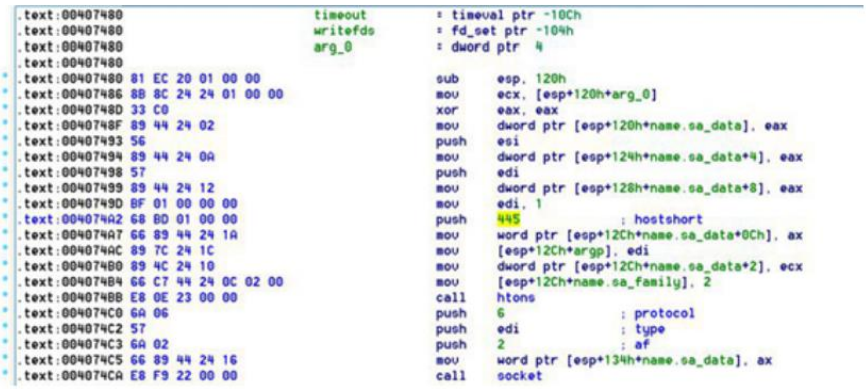
Tamaño	3.514.368 bytes
Fecha interna	20/11/2010 10:05
Compilador	Microsoft Visual C++ 6.0
Detalles	Archivo ZIP con contraseña “WNcry@2ol7”
Nombre	tasksche.exe

Este fichero contiene varios ejecutables utilizados para el ataque.

Proceso

WannaCry escanea la red interna y externa del dispositivo. Este hace uso de la vulnerabilidad EternalBlue como método de distribución dentro de las redes internas, realizando conexiones con el puerto 445 (puerto utilizado por el protocolo SMB) en busca de equipos no actualizados, para poder propagarse a través de ellos y poder llegar a infectarlos, un proceso de contaminación parecido a los Worms. El gusano es inyectado y se ejecuta de manera remota en el código LSASS.exe.

Este ejecutable es un proceso de Windows conocido como Servicio de Autoridad de Seguridad Local. Utilizado para el reforzamiento de las políticas de seguridad, verificación de autentificación, manejo de cambios de contraseñas y creación de fichas de acceso.



Proceso de infección local a Remota

Hay otro proceso que utiliza WannaCry para el ataque remoto es “taskse.exe”. Este ejecutable tiene la función de enumerar y tener registro de las sesiones de los usuarios conectados al equipo. WannaCry envía parámetros a taskse.exe la ruta completa al archivo “@WanaDecryptoy@.exe” aunque existen algunas muestras que ponen la ruta completa al malware “taskche.exe”.

La primera acción es cargar la biblioteca “Wtsapi32.dll” y obtiene las siguientes funciones

- WTSEnumerateSessionsA: Recupera lista de sesiones de una sesión remota de escritorio.
- WTSFreeMemory: Liberación de memoria asignada en los servicios remotos de escritorio.

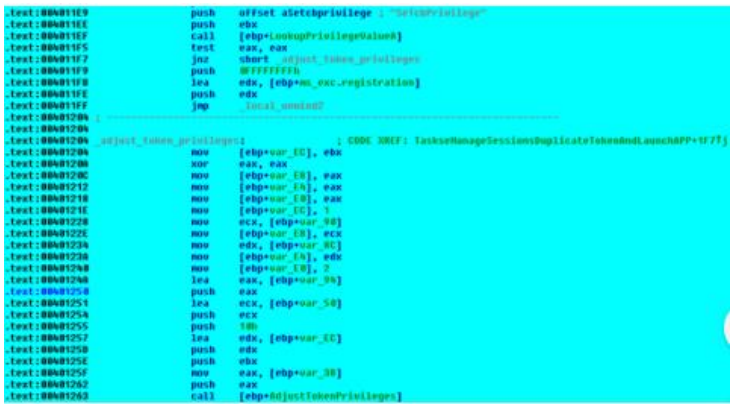
Se enumeran las sesiones con WTSEnumerateSessionsA, y se comprueba que exista una sesión. Si se encuentra, devolverá 2 sesiones, una del usuario local y otra nula. El último valor irá incrementando. Por cada sesión, se llama a otra función para realizar un proceso de suplantación de usuario, en esta función carga la biblioteca advapi32.dll y obtiene las siguientes funciones.

- OpenProcessToken: Obtiene el token de acceso de un proceso.
- LookupPrivilegeValueA: Regresa el identificador único local utilizado para la representación local de privilegios
- AdjustTokenPrivileges: Habilita o deshabilita los privilegios especificados del acceso del token.
- DuplicateTokenEx: Crea un nuevo token de acceso que se duplica en un token existente.
- CreateProcessAsUserA: Creación nuevos procesos y un hilo primario, se ejecuta en el contexto de seguridad del usuario por un token especificado.

Después de esto se carga la biblioteca kernel32.dll (obtención de dirección base) obtiene las funciones:

- WTSGetActiveConsoleSessionId: Regresa el identificador de la sesión de la sesión en consola (asociada con la consola física).
- GetCurrentProcess: Regresa un pseudo manejador para el proceso actual.
- CloseHandle: Cierra un objeto manejador.

Luego se obtienen las funciones de la biblioteca “userenv.dll”, CreateEnvironmentBlock, DestroyEnvironmentBlock, estos utilizado recuperar y eliminar variables de entorno para el usuario. Y por último obtiene de la librería “wtaspi32.dll” la función WTSQueryUserToken Obtiene un token de acceso primario de usuario por medio de un ID.



Por el uso de las funciones, se utilizan para obtener el manejador del proceso actual y acceder al token correspondiente, y con esto se concede el privilegio SeTcbPrivilege (creación de tokens para iniciar sesión, este es accesible a partir de SYSTEM) Si se tiene el privilegio a partir de WTSGetActiveConsoleSessionId y WTSQueryUserToken para poder obtener el token del usuario enumerado y mediante CreateProcessAsUser WannaCry puede ejecutarse en otras sesiones. A partir de este proceso, WannaCry usa taskse.exe para ataque de sesiones remotas.

Proceso de Cifrado

Ya después de la infección, WannaCry revisa si existen algunos de estos mutex:

- ‘Global\MsWinZonesCacheCounterMutexA0’

- ‘Global\MsWinZonesCacheCounterMutexW’
- ‘MsWinZonesCacheCounterMutexA’

Si existe alguno de estos mutex, el Ransomware no ejecutará el componente del cifrado. Si se ejecuta, WannaCry genera una clave de 128 bits única para cada archivo cifrado, creada mediante el cifrado AES (Advanced Encryption Standard), se guarda esta clave con una clave RSA dentro de un encabezado personalizado que el código dañino añade a los archivos. Al terminar de cifrar el archivo, este va a sobrescribir al archivo original.

Proceso de descifrado

Al generar las claves simétricas, se guarda en un fichero y se cifra con una clave pública que acompaña al malware. Solo se puede obtener la clave EAS con la clave creada por los atacantes. Se utiliza una herramienta Wana DecrypOr 2.0. Este es el “informante” el tiempo que le queda para realizar el pago de $300 bitcoins para el rescate de archivos. La herramienta se conecta servidores (TDL .onion) para tener contacto con los atacantes.

Prevención

Windows antes del ataque realizó un parche para impedir la explotación de esta vulnerabilidad. Los sistemas que disponen de este parche son:

- Windows XP
- Windows 2003
- Microsoft Windows Vista SP2

- Windows Server 2008 SP2 y R2 SP1
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2012 y R2
- Windows 10
- Windows Server 2016

Bibliografía

- Hofmann F. (2019) *Understanding the ELF File Format*. Consultado el 5 de mayo, 2020, en https://linuxhint.com/understanding_elf_file_format/
- C. M. Linn, M. Rajagopalan, S. Baker, C. Collberg, S. K. Debray, J. H. Hartman (2019) *Protecting Against Unexpected System Calls*. University of Arizona, Departament of Computer Science Texas. USA. Recuperado el 5 de mayo, 2020, de: https://www.usenix.org/legacy/event/sec05/tech/full_papers/linn/linn.pdf
- Syneidis Team (2017) *Ranking de los 12 tipos de malware más dañinos*. Encontrado el 5 de mayo, 2020, en https://www.syneidis.com/es/ranking-of-the-12-most-harmful-types-of-malware/
- Regan J (2005) *¿Qué es el malware? Cómo funciona el malware y cómo eliminarlo*. Encontrado el 5 de mayo, 2020, en https://www.avg.com/es/signal/what-is-malware
- Universidad de Jáen (2018) *GUIAS DE SEGURIDAD UJA Software malicioso (malware).* Servicio de Informática Vicerrectorado de Tecnologías de la Información y la Comunicación y Universidad Digital Andalucia. España. Encontrado el 4 de mayo, 2020, en https://www.ujaen.es/servicios/sinformatica/sites/servicio_sinformatica/files/uploads/guiaspracticas/Guias%20de%20seguridad%20UJA%20-%203.%20Malware.pdf
- OWASP (2020) *Code Injection*. Encontrado el 6 de mayo, 2020, en https://owasp.org/www-community/attacks/Code_Injection
- PandaSecurity (2018) *¿Qué es un Ransomware?* Encontrado el 12 de mayo, 2020, en https://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/
- Indiana University (2020) *ARCHIVED: What is Server Message Block (SMB)?* Encontrado el 12 de mayo, 2020, en https://kb.iu.edu/d/atue
- ESET (2020) *RANSOMWARE ¿Cómo protegerte? Conoce cómo evitar el secuestro de datos*. Encontrado el 12 de mayo, 2020, en https://www.eset.com/es/caracteristicas/ransomware/#
- PandaSecurity (2017) *Informe #WannaCry* Encontrado el 12 de mayo, 2020, en https://www.pandasecurity.com/spain/mediacenter/src/uploads/2017/05/1705-Informe_WannaCry-v160-es.pdf

- Campor V. (Desconocido). *Monitorización, detección y bloqueo de procesos de cifrado malicioso.* Encontrado el 12 de mayo, 2020, en http://diposit.ub.edu/dspace/bitstream/2445/117062/2/memoria.pdf
- Woods A (2014) *¿Qué es lsass.exe? ¿Debería eliminarlo?* Encontrado en 13 de mayo, 2020, en https://losvirus.es/lsass-exe/
- StackOverflow (2015) *EXE header information (.reloc & .rsrc meaning)* https://stackoverflow.com/questions/27214966/exe-header-information-reloc-rsrc-meaning
- Microsoft (2020) *Documentation*. Encontrado el 13 de mayo, 2020, en https://docs.microsoft.com/en-us/