“Universidad Internacional de La Rioja en México”

Ciberdelitos y Regulación de la Ciberseguridad

Proyecto:

Actividad individual 2: Vectores de ataque

Profesor:

Óscar Manuel Lira Arteaga

Autor:

Juan Luis Cruz Aristeo.

Fecha de entrega:

22/07/2024

Índice

Introducción

En la actualidad es importante que los profesionales de la ciberseguridad tengan un conocimiento amplio sobre el tema de vectores de ataque, ya que si nos adentramos en este término encontramos que los vectores de ataque son rutas para acceder a un servidor, host o la red misma y pueden ser utilizados por usuarios con mala intenciones. Si investigamos vectores de ataques en la web, se pueden encontrar definiciones de algunos, pero también encontraremos muchas noticias acerca de corporaciones que fueron víctimas de algún ataque.

Es por esto que todos los profesionales de la ciberseguridad siempre deben de estar actualizándose con las nuevas tendencias de tecnologías que están siendo usadas para poder penetrar y comprometer la seguridad de una corporación. Como se menciona con anterioridad los vectores de ataque aprovechan vulnerabilidades sobre el software o hardware, pero no se limita a solo la infraestructura de una corporación, en realidad también el personal de una empresa forma de estos vectores ya que el personal es la parte más vulnerable para poder introducirse a una empresa y acceder a datos sensibles, causar daño o tomar control de sistemas.

Pero entonces, ¿qué es un vector de ataque? En realidad, si hablamos de hardware, software y personal, los vectores de ataque son formas que pueden introducirse por medio de estas tres áreas mencionadas, por ejemplo, en el caso del hardware un vector de ataque podría ser una falla en el sistema de acceso y mediante esto un usuario puede realizar un Ataque de Interferencia Electromagnética (EMI), que se utiliza para comprometer o explotar vulnerabilidades en dispositivos físicos, en este caso (EMI) generar señales electromagnéticas con el fin de alterar el funcionamiento normal de un dispositivo electrónico. En el caso de un vector de ataque software un ejemplo claro podría ser phising que es un vector que en donde los atacantes se acceden a datos importantes engañando a su víctima o con archivos adjuntos implantan un RAMSOMWARE que es un tipo de malware diseñado para mantener cautivo un sistema informático o los datos que contiene hasta que se realice un pago.

Es así que ahora podemos entender la importancia de conocer sobre el tema de vectores de ataque, el objetivo de este proyecto es estudiar un delito especifico, el cual será el ataque RAMSOMWARE el cual desarrollaremos a profundidad, conociendo como funciona, como

conseguirlo y como defenderse ante él, esto para poder entender más a fondo el tema de vectores de ataque.

RAMSOMWARE

¿Qué es RAMSOMWARE?

El ransomware es un tipo de malware que fue diseñado para mantener cautivo un sistema informático o los datos que contiene hasta que se realice un pago. Este tipo de ataque causa pérdidas económicas e interrupciones significativas.

Se caracteriza por lo siguiente:

- Cifrado de datos: cifra los datos del sistema infectado, lo que los hace inaccesibles.
- Demanda de rescate: Los atacantes exigen un pago, prometiendo un programa de descifrado o un código, una vez hecho el pago.
- Resultados inciertos: realmente los atacantes no están obligados a dar el programa o el código después del pago de las víctimas, usualmente siempre terminan estafados.
- Método de propagación: es propagado por correos electrónicos o atreves de vulnerabilidades del sistema.

Un ejemplo claro del potencial que tiene este vector de ataque es el siguiente: En 2017, el ransomware WannaCry se propagó a través de una vulnerabilidad en los sistemas Windows, cifrando los datos y exigiendo un pago en Bitcoin para descifrarlos. Afectó a más de 200,000 computadoras en 150 países (FlashStart, 2024).

Con esto podemos entender el impacto que tiene un ataque ransomware rescatando lo siguiente:

Impacto: El impacto de un ataque ransomware puede paralizar las operaciones de una organización al hacer inaccesibles los datos y sistemas críticos.

Consecuencias: Las consecuencias pueden ser pérdida de datos, costos de recuperación, interrupciones operativas y daños a la reputación.

Medidas de Prevención y Mitigación:

No todo es malo, recordemos que lo importante para prevenir este tipo de ataques es conocer medidas y mecanismos de seguridad, hoy en día se conocen diferentes formas de poder prevenir este tipo de ataque, como, por ejemplo:

1. **Educación y conciencia:** Es importante que el personar sea capacitado para reconocer y evitas correos electrónicos de Phishing y no olvidar que el personal es la parte más vulnerable de la organización.
2. **Actualizaciones de seguridad:** Los equipos responsables de esta parte, siempre deben mantener los sistemas y software actualizados para protegerse ante vulnerabilidades.
3. **Respaldo de datos:** Si realizamos copias de seguridad regulares de los datos críticos y las almacenamos en ubicaciones seguras, desconectadas de la red principal, podemos tener un plan de rescate de datos en caso de un ataque.
4. **Soluciones de Seguridad:** Finalmente implementar software de seguridad y antivirus actualizado para detectar y bloquear las amenazas.

Lo más importante es que los equipos encargados de los sistemas de una organización, siempre estén en constante actualización de nuevas formas en las que los ciberdelincuentes, se filtran a las corporaciones y cometen este tipo de ataque, de esta forma podrían implementar mecanismos de seguridad para prevenir a la organización.

¿Cómo es el proceso de un ataque Ransomware?

Ahora que ya conocemos que son los vectores de ataque y la definición de un ataque RANSOMWARE, podemos empezar a desarrollar el ejemplo para entender cómo funciona, con ejemplos y evidencia real.

Por lo que sabemos, el ransomware es un tipo de malware que cifra los archivos de una víctima, haciéndolos inaccesibles, y luego exige un rescate (generalmente en criptomonedas) para devolver el acceso a los datos.

Pero todo empieza de la siguiente forma:

1. Vector de ataque:

   Entre los vectores de ataque, encontramos correos electrónicos de fishing, enlaces maliciosos, descargas de software infectado y vulnerabilidades en softwares sin parchear.

   La ingeniería social forma parte importante pues los atacantes suelen usar estas técnicas para engañar a las víctimas y hacer que ejecuten archivos maliciosos.

   Ejemplo de filtración por medio de correo electrónico

Correo electrónico (Phishing)

2. Ejecución del Malware:

Una vez que el archivo malicioso es ejecutado, el ransomware se descarta y se instala en el sistema de la víctima. Donde se asegura de persistir en el sistema, deshabilitando herramientas de seguridad y evitando su detección.

Posteriormente el ransomware escanea el sistema en busca de archivos valiosos como documentos, imágenes y bases de datos los cuales son analizados por medio de un algoritmo, posteriormente cifra estos archivos por medio de AES O RSA que son cifrados fuertes, lo que los hace inaccesibles para el usuario.

AES: Es un método moderno de cifrado de datos, su función es asegurar que la información será y privada y segura, transforma datos en un formato ilegible mediante una clave de cifrado. Solo aquellos que tengan la clave correcta pueden leer la información.

RSA: este algoritmo usa cifrado y firma digital, incluyendo un par de claves una publica y una privada, la pública se usa para cifrar datos y la privada para descifrarlos. Se usa para proteger la comunicación en línea y verificar la identidad de los remitentes.

Ejemplo de cuando ya fue afectado un pc:

RECOPILACION DE INFORMACION.

Investigación de casos prácticos: Ahora que ya conocemos a profundidad que es un RANSOMWARE como funciona y que afecta. Para complementar aún más la información y poder observar un caso real de cómo es o podría ser en caso real.

Se invita a ver el siguiente video:

Webinar: ¡Ataque de ransomware en vivo! | ManageEngine LATAM

https://www.youtube.com/watch?v=VnP8a65VUqY

Este webinar, me parece un video muy completo sobre la explicación de lo que es el tema de ataques RANSOMWARE, durante el video se explica a detalle definiciones y su impacto en los sistemas informáticos. Nos brinda contexto sobre la historia sobre malware en general, sobre su origen y evolución. Para después entrar a fondo en el ataque Ransomware, detallando su funcionamiento, propagación y consecuencias en una organización.

Lo más importante es que demuestra el comportamiento de un ataque ransomware en dispositivos infectados, se observa la eliminación de archivos y la encriptación de los mismos. Todo esto en un sistema controlado sandbox, de igual forma en el video se analiza como las alertas de seguridad se propagan de un dispositivo a otro lo que provoca la infección de varios dispositivos con ransomware. Se destaca la importancia de detectar y combatir el malware en tiempo real.

Análisis del código fuente de un ransomware escrito en Python

https://www.welivesecurity.com/la-es/2020/07/29/analisis-codigo-fuente-ransomware-escrito-python/

Este artículo de WeLiveSecurity se analiza el código fuente de un ransomware que fue escrito en leguaje Python. Este ransomware, se identifica como Python/fulecoder.AX, estuvo activo entre los años 2017 y 2018. En el análisis encontramos información de cómo el ransomware cifra archivos específicos mediante AES 256 en modo CBC para el cifrado. También se menciona sobre el proceso de generación de la clave de cifrado y el mensaje que exige el pago

Durante el desarrollo del análisis encontramos los siguientes apartados:

- Análisis de las funciones: como se hace posible que el programa se ejecute.

```
for root, subfiles, files in os.walk(drive):
    if not root.startswith('C:\\Windows'):
        if 'recycle.bin' in root.lower():
            pass
        else:
            for file in files:
                file_pnt = os.path.join(root, file)
                if os.path.basename(file_pnt).endswith(suffix) or 'RECOVER.txt' in os.path.basename(file_pnt) or
                    os.path.basename(file_pnt) in os.path.basename(sys.executable):
                    pass
                else:
                    extension = str(os.path.splitext(file_pnt)[1])
                    if '.bak' in extension or 'backup' in file_pnt.lower():
                        try:
                            os.remove(file_pnt)
                        except:
                            pass

                    else:
                        if extension.lower() in valid_extension:
                            try:
                                createAdamantium(grandpaSlacks(frilename), str(file_pnt))
                                print(file_pnt)
                                os.remove(str(file_pnt))
                            except:
                                print('------ ' + file_pnt)
```


- Valid_extension: en este apartado encontramos como es que el malware encripta los archivos, especificando las extensiones de aquellos que son importantes.

```
valid_extension = ['.adf',
'.txt', '.exe', '.php', '.pl', '.log', '.vhd', '.vhdx', '.lic', '.cab', '.lib.7z', '.rar', '.m4a', '.wma',
'.avi', '.wmv', '.csv', '.d3dbsp', '.sie', '.sum', '.ibank', '.t13', '.t12', '.qdf', '.gdb',
'.tax', '.pkpass', '.bc6', '.bc7', '.bkp', '.qic', '.bkf', '.sidn', '.sidd', '.mddata', '.itl', '.itdb',
'.icxs', '.hvpl', '.hplg', '.hkdb', '.mdbackup', '.syncdb', '.gho', '.cas', '.svg', '.map', '.wmo', '.itm',
'.sb', '.fos', '.vdf', '.ztmp', '.sis', '.sid', '.ncf', '.menu', '.layout', '.dmp', '.blob',
'.esm', '.001', '.vtf', '.dazip', '.fpk', '.mlx', '.kf', '.iwd', '.vpk', '.tor', '.psk', '.rim',
'.w3x', '.fsh', '.ntl', '.arch00', '.lvl', '.snx', '.cfr', '.ff', '.vpp_pc', '.lrf', '.m2', '.mcmeta',
'.vfs0', '.mpqge', '.kdb', '.db0', '.mp3', '.upx', '.rofl', '.hkx', '.bar', '.upk', '.das', '.iwi',
'.litemod', '.asset', '.forge', '.ltx', '.bsa', '.apk', '.re4', '.sav', '.lbf', '.slm', '.bik', '.epk',
'.rgss3a', '.pak', '.big', '.unity3d', '.wotreplay', '.xxx', '.desc', '.py', '.m3u', '.flv', '.js', '.css',
'.rb', '.png', '.jpeg', '.p7c', '.p7b', '.p12', '.pfx', '.pem', '.crt', '.cer', '.der', '.x3f',
'.srw', '.pef', '.ptx', '.r3d', '.rw2', '.rwl', '.raw', '.raf', '.orf', '.nrw', '.mrwref', '.mef',
'.erf', '.kdc', '.dcr', '.cr2', '.crw', '.bay', '.sr2', '.srf', '.arw', '.3fr', '.dng', '.jpeg',
'.jpg', '.cdr', '.indd', '.ai', '.eps', '.pdf', '.pdd', '.psd', '.dbfv', '.mdf', '.wb2', '.rtf',
'.wpd', '.dxg', '.xf', '.dwg', '.pst', '.accdb', '.mdb', '.pptm', '.pptx', '.ppt', '.xlk', '.xlsb',
'.xlsm', '.xlsx', '.xls', '.wps', '.docm', '.docx', '.doc', '.odb', '.odc', '.odm', '.odp', '.ods',
'.odt', '.sql', '.zip', '.tar', '.tar.gz', '.tgz', '.biz', '.ocx', '.html', '.htm', '.3gp', '.srt',
'.cpp', '.mid', '.mkv', '.mov', '.asf', '.mpeg', '.vob', '.mpg', '.fla', '.swf', '.wav', '.qcow2',
'.vdi', '.vmdk', '.vmx', '.gpg', '.aes', '.ARC', '.PAQ', '.tar.bz2', '.tbk', '.djv', '.djvu',
'.bmp', '.cgm', '.tif', '.tiff', '.NEF', '.cmd', '.class', '.jar', '.java', '.asp', '.brd', '.sch',
'.dch', '.dip', '.vbs', '.asm', '.pas', '.ldf', '.ibd', '.MYI', '.MYD', '.frm', '.dbf', '.SQLITEDB',
'.SQLITE3', '.asc', '.lay6', '.lay', '.ms11 (Security copy)', '.sldm', '.sldx', '.ppsm',
'.ppsx', '.ppam', '.docb', '.mml', '.sxm', '.otg', '.slk', '.xlw', '.xlt', '.xlm', '.xlc', '.dif',
'.stc', '.sxc', '.ots', '.ods', '.hwp', '.dotm', '.dotx', '.docm', '.DOT', '.max', '.xml', '.uot',
'.stw', '.sxw', '.ott', '.csr', '.key', 'wallet.dat']
```


- GrandpaSlacks: En este apartado encontramos la función que aplica la función hash.

-

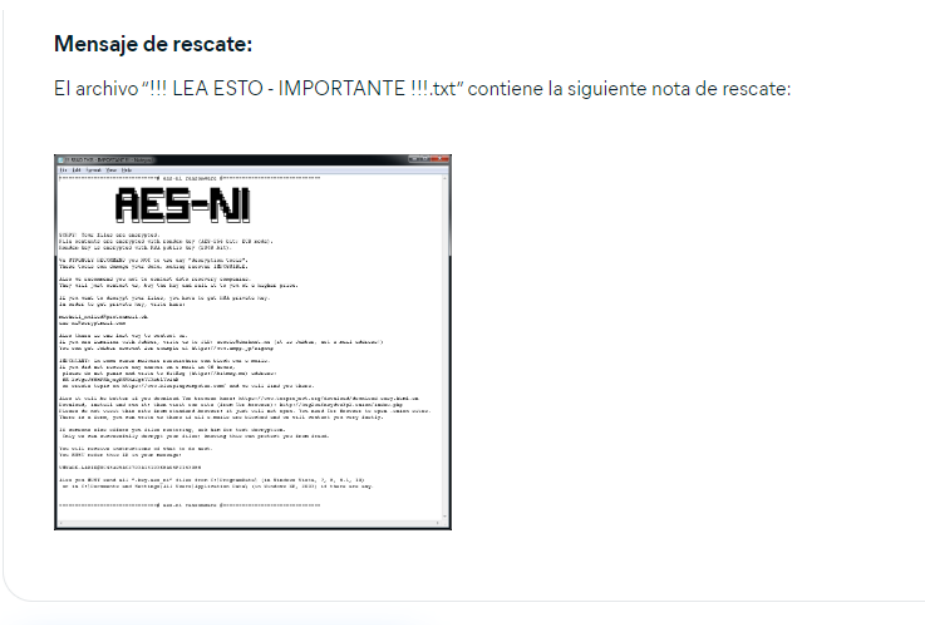
```
def grandpaSlacks(finger):
    return SHA3_256.new(finger).digest()
```

Sin duda es un artículo muy completo, el ejemplo práctico y de mucha utilidad para poner ampliar nuestro panorama con respecto al malware Ransomware.

Herramientas gratuitas de descifrado de ransomware.

A continuación, añadimos una página que brinda herramientas para el descifrado de algunos tipos de ransomware, que nos permite descargarlos de forma gratuita.

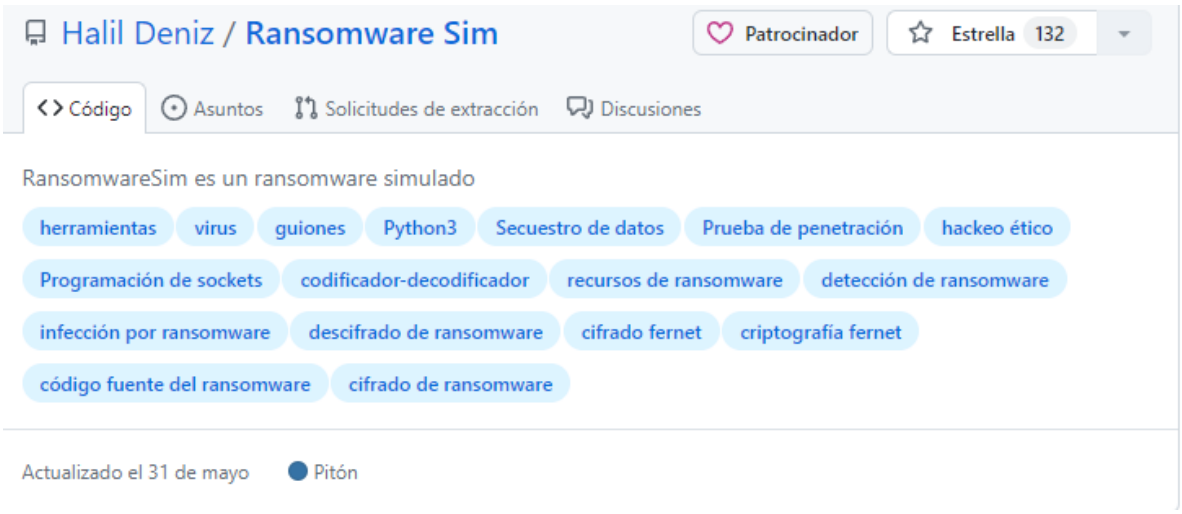
https://www.avast.com/ransomware-decryption-tools#pc

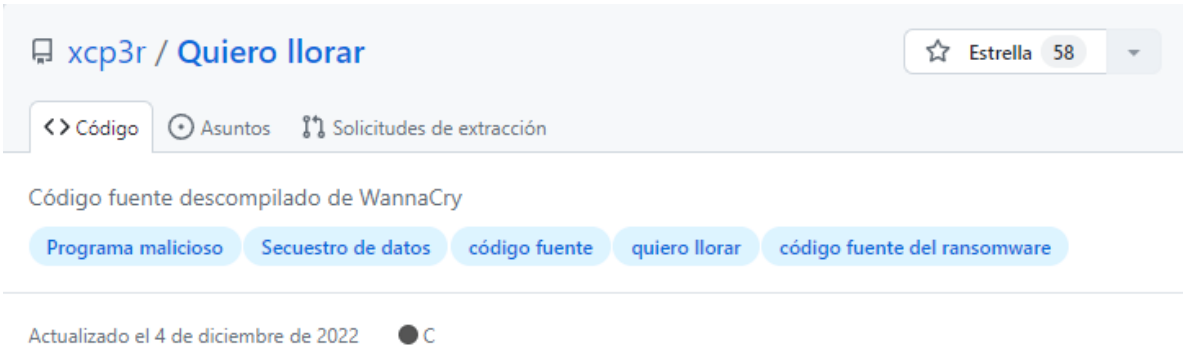


Códigos descompilados de diferentes tipos de Ransomware.

Para terminar con el apartado de investigación se añaden repositorios de Github donde se pueden obtener códigos descompilados de ransomware para analizarlos con fines de estudio.

https://github.com/topics/ransomware-source-code





Mecanismos de defensa anti-RANSOMWARE

Para finalizar esta investigación, es necesario brindar mecanismos para defenderse ante este malware, por lo tanto, se harán descripciones de formas de defensa para no ser víctimas de RANSOMWARE.

1. Mantener software y sistemas actualizados: La herramienta principal ante cualquier malware es asegurarse de que los sistemas operativos estén actualizados con los últimos parches de seguridad. Esto con el objetivo de evitar que los cibercriminales exploten vulnerabilidades conocidas de softwares desactualizados para introducir en este caso ransomware en el sistema.
2. Implementar copias de seguridad regulares: Sin duda entre las opciones más destacas para poder estar prevenidos a un ataque RANSOMWARE es que se realicen copias de seguridad regulares de todos los datos importantes y asegurarse de que las copias se almacenen en un lugar seguro, preferiblemente desconectadas de la red principal, esta sería la forma más rápida de recuperar los datos de una encriptación por RANSOMWARE sin pagar un rescate.
3. Autenticación multifactor (MFA): Este mecanismo de seguridad se basa en añadir una capa adicional a la seguridad, ya que requiere múltiples formas de verificación antes de permitir el acceso a sistemas críticos, lo que ayuda a prevenir accesos no autorizados, incluso si las credenciales han sido comprometidas.
4. Controlar y limitar el acceso remoto: Este mecanismo trabaja limitando el uso de servicios de escritorio remoto(RDP) y otros accesos remotos. Solo en aquellos casos donde es necesario utilizar RDP, se debe asegurar que se configure adecuadamente ya que debe estar protegido con MFA y contraseñas robustas para evitar ataques o eventos inesperados.

5. Realizar pruebas de penetración y evaluaciones: Sin duda es de vital importancia que las organizaciones lleven a cabo pruebas de penetración para identificar y corregir puntos débiles en la seguridad de los sistemas antes que un usuario pueda explotarlos, siempre se debe documentar adecuadamente los resultados, con debidas evaluaciones de esta forma siempre se tiene un sistema de mejora.
6. Capacitación al personal: El eslabón más débil es el personal de las organizaciones, ya que son el vector de ataque más conocido, pues por medio de técnicas de ingeniería social, un ciberdelincuentes puede engañar a un usuario del equipo de la organización que no cuente con conocimiento sobre el tema y aprovecharse, mediante correos electrónicos. Por lo tanto, es de vital importancia capacitar a todo el personal.

Bibliografía

FlashStart. (2024). *El ransomware WannaCry: ¿Qué es y cómo protegerse?* Recuperado el 19 de julio de 2024, de https://flashstart.com/es/el-ransomware-wannacry-que-es/

Trend Micro. (n.d.). ¿Qué es el ransomware? Recuperado de https://www.trendmicro.com/es_mx/what-is/ransomware.html

Akamai. (n.d.). ¿Qué es el ransomware? Recuperado de https://www.akamai.com/es/glossary/what-is-ransomware

Microsoft. (n.d.). ¿Qué es el ransomware? Recuperado de https://www.microsoft.com/es-mx/security/business/security-101/what-is-ransomware

Kingston. (2023, 19 de marzo). ¿Qué es la encriptación XTS-AES? Recuperado de https://www.kingston.com/latam/blog/data-security/xts-encryption#:~:text=AES%20o%20Advanced%20Encryption%20Standard,parte%20de%20la%20especificaci%C3%B3n%20AES

INCIBE. (2022, 7 de julio). Detectada campaña de correos electrónicos con malware adjunto. Recuperado de https://www.incibe.es/ciudadania/avisos/detectada-campana-de-correos-electronicos-con-malware-adjunto