

Tarea: CTF-VacacionEX

Alumno: Quintana Escamilla Roberto Carlos

¿Qué tipo de ataques realiza el grupo Lapsus\$?

La vulnerabilidad CVE-2017-0144 es también conocida como "EternalBlue", y **es una vulnerabilidad de ejecución remota de código** que afecta al protocolo SMB (Server Message Block) utilizado por los sistemas operativos Microsoft Windows. Fue descubierto en marzo de 2017 y fue explotado por el ransomware WannaCry en mayo del mismo año.

Esta vulnerabilidad permite a un atacante enviar un paquete especialmente diseñado al puerto SMB de un sistema vulnerable, lo que le permite ejecutar código malicioso de forma remota en el sistema afectado sin necesidad de autenticación. Esto podría permitir al atacante tomar el control total del sistema afectado y llevar a cabo diversas acciones malintencionadas, como el robo de datos, el cifrado de archivos y la propagación del malware a otros sistemas de la red.

Es importante tener en cuenta que Microsoft lanzó un parche para esta vulnerabilidad poco después de su descubrimiento, por lo que es fundamental mantener los sistemas actualizados para evitar la explotación de esta vulnerabilidad.

¿A qué tipo de ataque pertenece esta vulnerabilidad?

La vulnerabilidad CVE-2017-0144 (EternalBlue) pertenece a la categoría de ataques de ejecución remota de código (RCE, por sus siglas en inglés). Esto significa que un atacante puede ejecutar código malicioso en un sistema afectado de forma remota, sin necesidad de autenticación, explotando esta vulnerabilidad.

Este tipo de ataques son especialmente peligrosos ya que permiten al atacante tomar el control total del sistema afectado y llevar a cabo diversas acciones malintencionadas, como el robo de datos, la instalación de malware adicional, el cifrado de archivos, entre otros. Por esta razón, es fundamental mantener los sistemas actualizados y protegerse contra este tipo de vulnerabilidades, para evitar posibles consecuencias negativas.

"La vulnerabilidad CVE-2017-0144 es una falla de seguridad en el protocolo SMB (Server Message Block) de Microsoft Windows. Esta vulnerabilidad se conoce comúnmente como "EternalBlue".

Se trata de una vulnerabilidad de ejecución remota de código (RCE) que permite a un atacante enviar un paquete especialmente diseñado a un sistema vulnerable y ejecutar código malicioso en él sin necesidad de autenticación. Esto significa que un atacante puede tomar el control completo del sistema afectado y robar información confidencial o utilizarlo para llevar a cabo ataques adicionales.

Esta vulnerabilidad fue descubierta por la Agencia de Seguridad Nacional (NSA) de los Estados Unidos y posteriormente se filtró a la red en un grupo de herramientas de hacking llamado "Shadow Brokers". Esta vulnerabilidad fue explotada por el ransomware WannaCry

en mayo de 2017, causando un gran impacto a nivel mundial al afectar a sistemas de todo tipo de organizaciones, incluyendo hospitales, empresas y gobiernos.

Microsoft lanzó un parche de seguridad para esta vulnerabilidad en marzo de 2017, pero muchos sistemas no fueron actualizados a tiempo, lo que permitió que los atacantes pudieran explotar esta vulnerabilidad de forma masiva. Desde entonces, es esencial mantener los sistemas operativos actualizados y protegidos con medidas de seguridad adecuadas para evitar este tipo de vulnerabilidades.”

Vía chat GTP prompt “Describe la vulnerabilidad CVE-2017-0144”

¿Cuándo se dio a conocer dicho grupo?

El grupo Lapsus\$ se dio a conocer por primera vez en octubre de 2020, cuando se publicaron informes sobre su actividad en foros de seguridad y noticias.

¿Cuáles son las motivaciones de dicho grupo?

La principal motivación del grupo Lapsus\$ es el lucro económico. Buscan obtener beneficios financieros a través de los ataques de ransomware y extorsionando a las empresas afectadas.

¿En qué consiste la vulnerabilidad?

La vulnerabilidad, denominada como CVE-2017- 0144 o “EternalBlue” en el catálogo Common Vulnerabilities and Exposures (CVE), se presentó en la versión 1 del servidor SMB (SMBv1). Esta vulnerabilidad permite a un atacante enviar un paquete especialmente diseñado al puerto SMB de un sistema vulnerable, lo que le permite ejecutar código malicioso de forma remota en el sistema afectado sin necesidad de autenticación.

La vulnerabilidad CVE-2017-0144 se refiere específicamente a la vulnerabilidad en el protocolo de red SMBv1 de Microsoft Windows. Esta vulnerabilidad afecta a múltiples versiones del sistema operativo Windows, incluyendo Windows Vista, Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 y Windows Server 2016.

¿Qué sistema operativo tenía la empresa?

debido a la naturaleza de la vulnerabilidad usada contra la empresa FinMex que fue el uso de un “eternal Blue”, es evidente que el sistema operativo que tiene es windows, así que se asume que al menos el sistema operativo vulnerado podría ir desde Windows XP hasta windows 10

¿Cuáles pueden ser las ubicaciones de el/los atacante(s)?

Según la IP encontrada nos marca que la posible ubicación está en China.

```
1.0.63.255
```

```
{
  "ip": "1.0.63.255",
  "country_code": "CN",
  "country_name": "China",
  "region_name": "Guangdong",
  "city_name": "Guangzhou",
  "latitude": 23.127361,
  "longitude": 113.26457,
  "zip_code": "510140",
  "time_zone": "+08:00",
  "asn": "-",
  "as": "-",
  "isp": "ChinaNet Guangdong Province Network",
}
```

Por metadatos de la imagen nos da como posible ubicación Tailandia

Metadata GoogleMap

Exif Xmp Iptc Maker ALL Custom

Workspace

Tag name	Value
SemanticStyle	{0=1,1=0,2=0,3=0}
GPS	----
GPSLatitudeRef	North
GPSLatitude	16.772639°
GPSLongitudeRef	West
GPSLongitude	99.780061°
GPSAltitudeRef	Above Sea Level
GPSAltitude	2.366368221 m
GPSSpeedRef	km/h
GPSSpeed	0
GPSTimeOfDay	True North
GPSTimeOfDay	163.1253281
GPSTimeOfDay	True North
GPSTimeOfDay	163.1253281
GPSTimeOfDay	12.09765335 m
GPSTimeOfDay	----
GPSTimeOfDay	MPF0
MPFVersion	0100

login | registrarse Follow Tweet

Inicio Como llegar Sistema de Coordenadas Convertidor Pais Estados Mapa Personalizado

Dirección unnamed road, อำเภอศรีมอหริ, Provincia de Sukhothai

Obtener Coordenadas GPS

GD (grados decimales)*

Latitud 16.7726389

Longitud 99.78006111111111

Obtener Dirección

GMS (grados, minutos, segundos)*

Latitud N S 16 ° 46 ' 21.5 "

Longitud E O 99 ° 46 ' 48.219 "

Obtener Dirección

unnamed road, อำเภอศรีมอหริ, Provincia de Sukhothai 64160, Tailandia
Latitud: 16.772639 | Longitud: 99.780061

Obtener Altitud

no se puede no permitir ofrecer nuestros servicios. Al utilizar nuestros servicios, aceptas el uso que hacemos de los cookies.

¿Qué medidas adicionales debería tomar FinMex para protegerse de futuros ataques cibernéticos?

Si una empresa descubre que tiene sistemas vulnerables a la CVE-2017-0144 (EternalBlue), debería tomar las siguientes medidas adicionales para protegerse:

1. **Aplicar parches y actualizaciones:** es fundamental instalar los parches y actualizaciones que Microsoft ha lanzado para corregir esta vulnerabilidad. Si la empresa tiene un sistema de gestión de parches, debe asegurarse de que esté actualizado y que se hayan aplicado todos los parches críticos.
2. **Evaluar y fortalecer la seguridad de la red:** es importante evaluar la seguridad de la red y aplicar medidas adicionales para fortalecerla. Por ejemplo, podría ser necesario actualizar los firewalls, restringir el acceso a los puertos SMB, configurar reglas de acceso para permitir únicamente el tráfico de red necesario, entre otras medidas.
3. **Revisar y mejorar las políticas de seguridad:** la empresa debería revisar sus políticas de seguridad y asegurarse de que sean adecuadas para prevenir y responder a ataques de este tipo. Esto podría incluir políticas de contraseñas, autenticación de usuarios, acceso remoto, respaldos de información, etc.
4. **Realizar auditorías de seguridad:** se recomienda realizar auditorías de seguridad regulares para identificar posibles vulnerabilidades y mejorar las medidas de seguridad. Esto podría incluir pruebas de penetración, análisis de vulnerabilidades, entre otros.
5. **Capacitar al personal:** es importante que el personal de la empresa esté capacitado en seguridad informática y conozca los riesgos asociados a esta vulnerabilidad y cómo prevenirlos. La capacitación podría incluir cómo identificar correos electrónicos sospechosos, cómo evitar la descarga de archivos maliciosos, cómo usar contraseñas seguras, entre otros temas relevantes.

¿Cuáles son las recomendaciones para este incidente?

Si una empresa ha sido atacada por la vulnerabilidad CVE-2017-0144 (EternalBlue) y ha instalado un ransomware que ha bloqueado el acceso a sus archivos y datos críticos, se recomienda:

1. **Aislar los sistemas afectados:** es importante aislar los sistemas afectados de la red para evitar que el malware se propague a otros sistemas.

2. No pagar el rescate: aunque pueda parecer tentador, no se recomienda pagar el rescate exigido por los atacantes, ya que no garantiza que se recuperen los datos y puede alentar a los atacantes a continuar con este tipo de ataques.

3. Restaurar desde una copia de seguridad: si la empresa tiene una copia de seguridad reciente y no está afectada por el ransomware, se recomienda restaurar los datos desde la copia de seguridad. Es importante asegurarse de que la copia de seguridad esté actualizada y sea confiable.

4. Contactar a profesionales de seguridad informática: se recomienda contactar a profesionales de seguridad informática para evaluar la situación, recuperar los datos y tomar medidas para prevenir futuros ataques. También pueden ayudar en la identificación de la vulnerabilidad que permitió el ataque y en la implementación de medidas para evitar futuros ataques.

5. Informar del incidente: se recomienda informar del incidente a las autoridades pertinentes, ya que esto puede ayudar en la identificación de los atacantes y en la prevención de futuros ataques. También puede ser necesario informar a los clientes y otros afectados sobre el incidente.

6. Aprender de la experiencia: es importante aprender de la experiencia y tomar medidas para mejorar la seguridad informática de la empresa, como actualizar los sistemas, aplicar parches de seguridad, fortalecer la política de contraseñas, entre otras medidas.

¿Con qué se tomó la foto?

Con un iphone 13.

Las coordenadas de la imagen son:

Metadata GoogleMap	
Exif Xmp Iptc Maker ALL Custom	
Workspace	
Tag name	Value
SemanticStyle	{0=1,1=0,2=0,3=0}
---- GPS ----	
GPSLatitudeRef	North
GPSLatitude	16.772639°
GPSLongitudeRef	West
GPSLongitude	99.780061°
GPSAltitudeRef	Above Sea Level
GPSAltitude	2.366368221 m
GPSSpeedRef	km/h
GPSSpeed	0
GPSImgDirectionRef	True North
GPSImgDirection	163.1253281
GPSTDestBearingRef	True North
GPSTDestBearing	163.1253281
GPSHPositioningError	12.09765335 m
---- MPF0 ----	
MPFVersion	0100

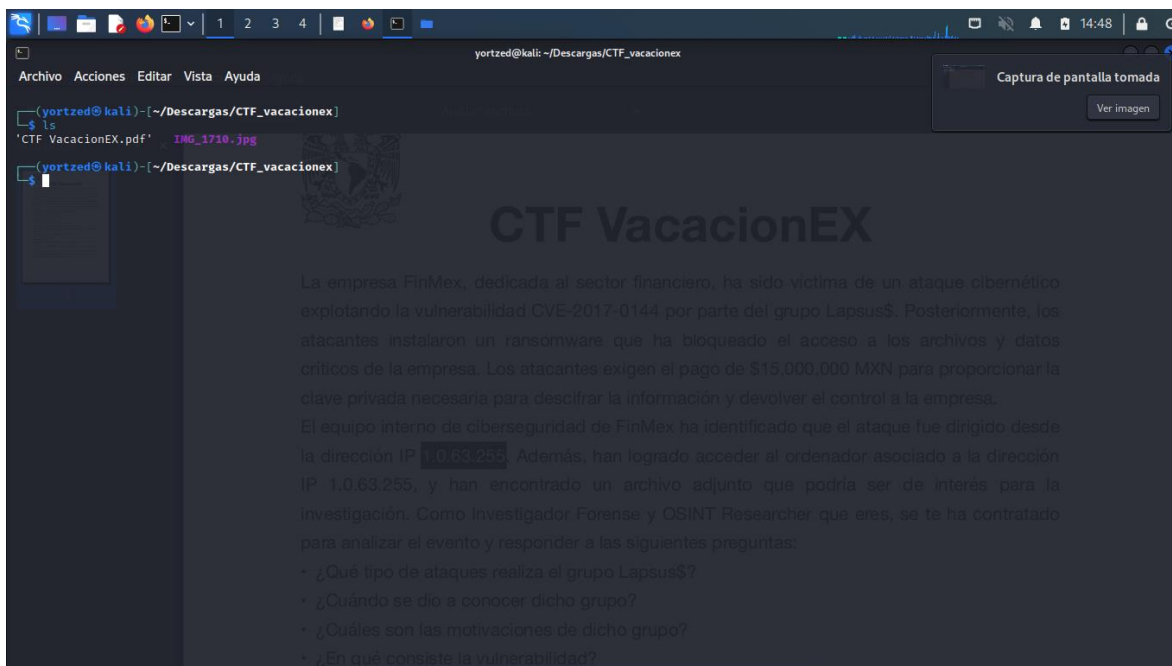
Bandera he información adicional

Al descargar los archivos proporcionados encontramos un archivo .gz . Podemos descomprimirlo con `gzip -d`. Posteriormente encontraremos otro archivo comprimido pero esta vez tipo tar con lo que usaremos el comando `tar` con los parámetros `-xvf`

```
yortzed@kali: ~/Descargas
Archivo Acciones Editar Vista Ayuda
(yortzed@kali)-[~]
└─$ cd Descargas
(yortzed@kali)-[~/Descargas]
└─$ ls
CTF_vacacionex.tar.gz  lab_RobertoQ.ovpn  OperaGXSetup.exe
(yortzed@kali)-[~/Descargas]
└─$ gzip -d CTF_vacacionex.tar.gz
(yortzed@kali)-[~/Descargas]
└─$ ls
CTF_vacacionex.tar  lab_RobertoQ.ovpn  OperaGXSetup.exe
```

```
yortzed@kali: ~/Descargas
Archivo Acciones Editar Vista Ayuda
-rw-r--r-- 1 yortzed yortzed 3591312 abr 6 17:21 OperaGXSetup.exe
(yortzed@kali)-[~/Descargas]
└─$ tar -xvf CTF_vacacionex.tar
CTF_vacacionex/
CTF_vacacionex/._DS_Store
tar: Se desestima la palabra clave de la cabecera extendida desconocida 'SCHIMY.flags'
tar: Se desestima la palabra clave de la cabecera extendida desconocida 'LIBARCHIVE.xattr.com.apple.FinderInfo'
CTF_vacacionex/._DS_Store
CTF_vacacionex/._CTF VacacionEX.pdf
tar: Se desestima la palabra clave de la cabecera extendida desconocida 'LIBARCHIVE.xattr.com.apple.quarantine'
tar: Se desestima la palabra clave de la cabecera extendida desconocida 'LIBARCHIVE.xattr.com.apple.metadata:kMDLabel_govsuixdjw3ataargk3urnjsey'
tar: Se desestima la palabra clave de la cabecera extendida desconocida 'LIBARCHIVE.xattr.com.apple.metadata:kMDItemUserTags'
tar: Se desestima la palabra clave de la cabecera extendida desconocida 'LIBARCHIVE.xattr.com.apple.macl'
tar: Se desestima la palabra clave de la cabecera extendida desconocida 'LIBARCHIVE.xattr.com.apple.lastuseddate#PS'
tar: Se desestima la palabra clave de la cabecera extendida desconocida 'LIBARCHIVE.xattr.com.apple.FinderInfo'
CTF_vacacionex/CTF VacacionEX.pdf
CTF_vacacionex/._IMG_1710.jpg
tar: Se desestima la palabra clave de la cabecera extendida desconocida 'LIBARCHIVE.xattr.com.apple.quarantine'
tar: Se desestima la palabra clave de la cabecera extendida desconocida 'LIBARCHIVE.xattr.com.apple.macl'
tar: Se desestima la palabra clave de la cabecera extendida desconocida 'LIBARCHIVE.xattr.com.apple.lastuseddate#PS'
CTF_vacacionex/IMG_1710.jpg
(yortzed@kali)-[~/Descargas]
└─$ ls
CTF_vacacionex  CTF_vacacionex.tar  lab_RobertoQ.ovpn  OperaGXSetup.exe
(yortzed@kali)-[~/Descargas]
└─$
```

Verificamos que archivos hay contenido en la carpeta con el comando `ls`.



Si utilizamos el un visor pdf para “CTF_Vaciones.pdf” notaremos las instrucciones del ejercicio.

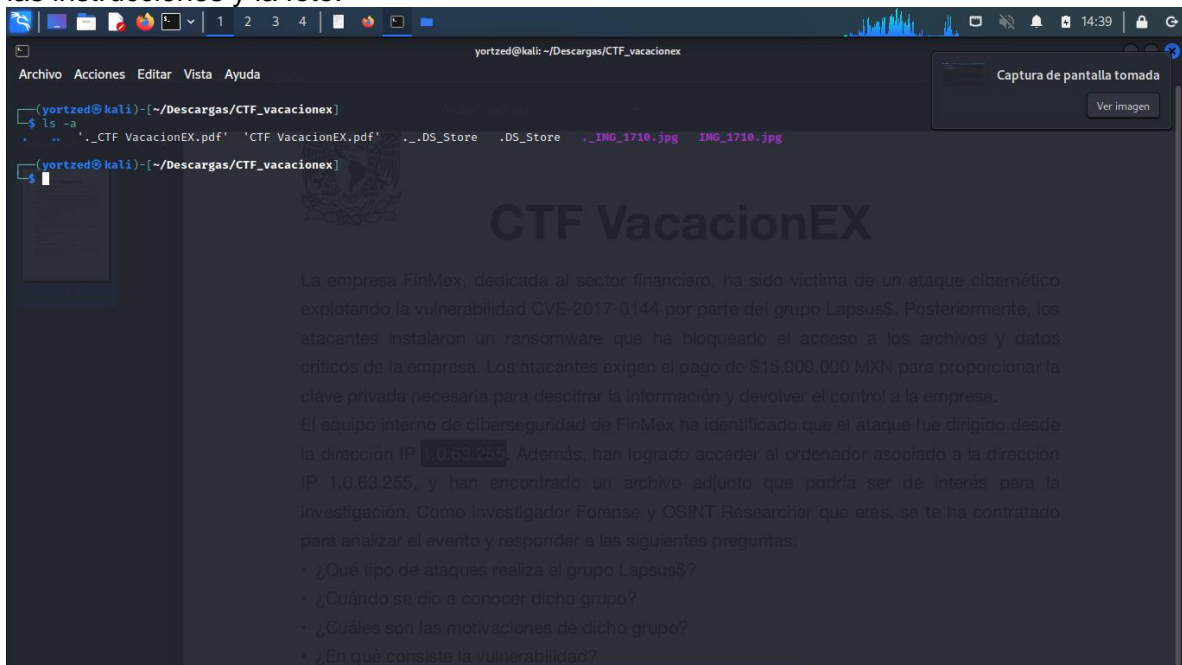


Mientras que la imagen se muestra de la siguiente manera.



Flag: flag: UNAM{57egnograPhy_15_c007}

Si utilizamos el comando ls con el parametro -a notaremos archivos ocultos ademas de las instrucciones y la foto.



Aplicando un cat a cat './_IMG_1710.jpg' obtenemos

```
MINGW64/c/Users/2im3q/Desktop/CTF_vacacionex/CTF_vacacionex
2im3q@DESKTOP-QBL05CF MINGW64 ~/Desktop/CTF_vacacionex/CTF_vacacionex
$ ls
'CTF VacacionEX.pdf'  IMG_1710.jpg
2im3q@DESKTOP-QBL05CF MINGW64 ~/Desktop/CTF_vacacionex/CTF_vacacionex
$ ls -la
./ ../ .DS_Store ._DS_Store '._CTF VacacionEX.pdf' '._IMG_1710.jpg' 'CTF VacacionEX.pdf' IMG_1710.jpg
2im3q@DESKTOP-QBL05CF MINGW64 ~/Desktop/CTF_vacacionex/CTF_vacacionex
$ cat '._IMG_1710.jpg'
Mac OS X
2im3q@DESKTOP-QBL05CF MINGW64 ~/Desktop/CTF_vacacionex/CTF_vacacionex
$
```

NOTA IMPORTANTE: notamos que el ejercicio fue desarrollado con Mac OS X además

- "com.apple.lastuseddate" parece ser una etiqueta que indica la última fecha en que se utilizó una aplicación o un archivo.
- "com.apple.macl4" parece ser una etiqueta que se utiliza para registrar información de control de acceso basada en etiquetas (LBAC, por sus siglas en inglés) en macOS.
- "com.apple.quarantine" parece ser una etiqueta que se utiliza para registrar información de seguridad sobre el origen de una aplicación o archivo, y se utiliza para controlar la ejecución de aplicaciones descargadas de Internet en macOS.
- "Firefox" parece ser el nombre de un navegador web.
- "6F88354D-0AC7-4697-9BC6-3FCE2EA7BE78" es un identificador único (UUID) que se utiliza para identificar un objeto o archivo en macOS.

Via chat gtp prompt {Analiza la siguiente cadena "Mac OS X

2?qATTRq[REDACTED]com.apple.lastuseddate#PS[REDACTED]Hcom.apple.macl4=com.apple.quarantine[REDACTED]5d[REDACTED]?/[REDACTED]
3[REDACTED];L# [REDACTED]9[REDACTED]Nq/0083;63e5cc7f;Firefox;6F88354D-0AC7-4697-9BC6-3FCE2EA7BE78}

Si aplicamos la misma técnica podemos obtener información redundante.

¿Cómo mitigar este ataque y otros en un futuro?

1. Aplicar los parches de seguridad: Microsoft ha publicado parches de seguridad para las versiones afectadas de Windows que corrigen la vulnerabilidad explotada por EternalBlue. Es importante asegurarse de que todos los sistemas estén actualizados con los parches más recientes.

2. Deshabilitar SMBv1: SMBv1 es la versión más antigua del protocolo SMB y es vulnerable a ataques. Se recomienda deshabilitar SMBv1 en todos los sistemas y utilizar versiones más recientes de SMB.
3. Configurar un firewall: Configurar un firewall puede ayudar a bloquear el tráfico malicioso que intenta explotar la vulnerabilidad de EternalBlue.
4. Limitar el acceso a los puertos SMB: Limitar el acceso a los puertos SMB a solo los sistemas necesarios puede reducir la exposición a posibles ataques.
5. Implementar medidas de seguridad adicionales: Además de las medidas anteriores, es recomendable implementar medidas de seguridad adicionales, como la autenticación de dos factores, el cifrado de datos y el monitoreo constante de la red para detectar cualquier actividad sospechosa.

Conclusión:

En conclusión, este trabajo se ha logrado identificar la posible ubicación de atacantes, lo cual puede ser reportado a las autoridades competentes en caso de ser necesario para que de esta forma se tomen medidas necesarias, para que se pueda corregir y tomar medidas pertinentes a futuro para que este problema no ocurra de nuevo, también se recomienda que el pago de un rescate sea solo como última opción, para finalizar el tiempo es lo que más se juega en contra en este tipo de situaciones ya que implica ser más rápido que los atacantes.

Referencias:

International IT. (2022, 6 julio). Lapsus\$: ¿Quién está detrás del grupo de hackers? <https://www.internationalit.com/post/lapsus-qui%C3%A9n-est%C3%A1-detr%C3%A1s-del-grupo-de-hackers?lang=es>

ChatGPT. (2023, 11 de abril). Cuál es la vulnerabilidad CVE-2017-0144? [Mensaje de chat]. Recuperado de <https://www.openai.com/>

ChatGPT. (2023, 11 de abril). Si una empresa descubre que tiene sistemas vulnerables a la CVE-2017-0144 (EternalBlue), debería tomar las siguientes medidas adicionales para protegerse

Usuario. (2023, 11 de abril). Cuáles son las recomendaciones para una empresa que fue atacada por la vulnerabilidad CVR-2017-0144 e instalaron un ransomware que ha bloqueado el acceso a sus archivos y datos críticos?,

ChatGPT. (2023, 11 de abril). Describe la vulnerabilidad CVE-2017-0144 . Recuperado de <https://chat.openai.com/chat/c0ba9cac-832a-4bf7-811e-d2769c78fa69>

ChatGPT. (2023, 11 de abril). Analiza la siguiente cadena "Mac OS X 2?qATTRq[REDACTED]com.apple.lastuseddate#PS[REDACTED]Hcom.apple.macl4=com.apple.quarantine[REDACTED]5d[REDACTED]?/[REDACTED]3[REDACTED];L#[REDACTED]9[REDACTED]Nq/0083;63e5cc7f;Firefox;6F88354D-0AC7-4697-9BC6-3FCE2EA7BE78". } <https://chat.openai.com/chat/c0ba9cac-832a-4bf7-811e-d2769c78fa69>

ChatGPT. (2023, 11 de abril). La vulnerabilidad CVE-2017-0144 (EternalBlue) pertenece a la categoría de ataques de ejecución remota de código (RCE, por sus siglas en inglés)].

ChatGPT. (2023, 11 de abril). Si una empresa ha sido atacada por la vulnerabilidad CVE-2017-0144 (EternalBlue) y ha instalado un ransomware que ha bloqueado el acceso a sus archivos y datos críticos, se recomienda lo siguiente