Ransomware Avaddon: principales características

welivesecurity.com/la-es/2021/05/31/ransomware-avaddon-principales-caracteristicas/

May 31, 2021

Analizamos cuáles son las principales características del ransomware Avaddon a partir de alguna de las muestras de este malware analizadas durante el segundo trimestre de 2021.

Facundo Muñoz
31 May 2021 - 10:00AM

Analizamos cuáles son las principales características del ransomware Avaddon a partir de alguna de las muestras de este malware analizadas durante el segundo trimestre de 2021.

Actualizado el 14 de junio de 2021
El ransomware Avaddon cerró sus operaciones el 11 de junio y compartió las claves de descifrado para que las víctimas que no pagaron puedan recuperar sus archivos del cifrado de manera gratuita. El grupo detrás de Avaddon envió las claves al portal BleepingComputer, el cual a su vez compartió las claves con investigadores de seguridad de Emsisoft y Coverware que confirmaron su legitimidad y crearon un descifrador que está disponible para su descarga aquí. En total, los atacantes enviaron 2.934 claves de descifrado. Cada una de estas claves corresponde a una víctima en particular.

Qué es Avaddon

Avaddon es un ransomware cuyos primeros ataques fueron detectados a finales del año 2019 y que a mediados del 2020 comenzó a reclutar afiliados en foros de hacking para su programa de Ransomware-as-a-Service (RaaS), ofreciendo múltiples opciones y amplia capacidad para ser configurado para el servicio. Los ataques de Avaddon han afectado a empresas y organizaciones de todo el mundo, incluidos varios países de América Latina.

Lectura relacionada: Crecen las víctimas del ransomware Avaddon en América Latina

Muchos grupos de ransomware adoptaron la modalidad extorsiva del doxing; es decir, el robo de información de los sistemas comprometidos previo al cifrado para luego amenazar a las víctimas con publicar la información en caso de no querer llegar a un acuerdo para el pago del rescate. En el caso de Avaddon, si bien de acuerdo con las muestras analizadas y los hashes públicos que observamos no detectamos la capacidad de robar información desde el equipo infectado, los operadores detrás de este ransomware cuentan con un sitio en la red TOR creado principalmente para este fin en el que publicaron supuesta información de las víctimas.

Además del doxing, otra estrategia extorsiva que el grupo dice llevar adelante son los ataques de DDoS sobre los sitios de las víctimas para de esta manera interrumpir el funcionamiento y que los usuarios no puedan acceder.

Por último, una vez que Avaddon logra acceso a una red realiza primero tareas de reconocimiento para identificar principalmente bases de datos, backup y copias shadow, y también buscando la forma escalar privilegios dentro de la red.

Según publicó el Centro de Ciberseguridad de Australia en mayo de 2021, el monto promedio que solicitan los atacantes para recuperar los archivos es de 0.73 bitcoins, que equivale aproximadamente 40.000 dólares.

Tabla de contenidos en este artículo:

Principales características del ransomware Avaddon

Estas son algunas de sus principales características:

- Como vector de propagación suele utilizar correos de phishing que buscan engañar al usuario haciéndole creer que hay una imagen comprometedora de ellos en el adjunto, aunque también se ha visto utilizar en sus comienzos archivos Excel con macros maliciosas, y más adelante hacer uso de credenciales de acceso débiles en servicios de acceso remoto, como RDP y redes VPN.
- Desarrollado en C++ y no utiliza herramientas de empaquetado ni ofuscación.
- Utiliza técnicas para dificultar el análisis: anti-VM, anti-debugging, utilización de tablas de strings cifradas encapsuladas en objetos.
- Busca archivos en discos locales y discos de red, teniendo como prioridad el cifrado de bases de datos.
- Doble cifrado con combinación de algoritmos AES-256 y RSA-2048.
- Los archivos cifrados en la muestras analizadas quedan con una extensión generalmente de 10 caracteres como .BeCecbaDBB, aunque se han visto que en las primeras los archivos quedaban con otras extensiones como .avdn.
- Termina procesos que puedan impedir el cifrado de archivos.
- Utiliza comandos de Windows para eliminar copias de seguridad del sistema, y copias shadow.

Cómo se distribuye Avaddon

El método de distribución qué más se ha visto en el caso de Avaddon es a través de correos de phishing que incluyen un archivo JScript malicioso adjunto que utiliza una segunda extensión “.ZIP” para hacerle creer a la potencial víctima que se trata de un archivo comprimido que contiene una foto comprometedora que ha sido descubierta en la web. El código JScript a su vez ejecuta comandos de Powershell para descargar el ransomware de un servidor web y guardarlo en el directorio %TEMP% del equipo de la víctima para luego ejecutar el malware.

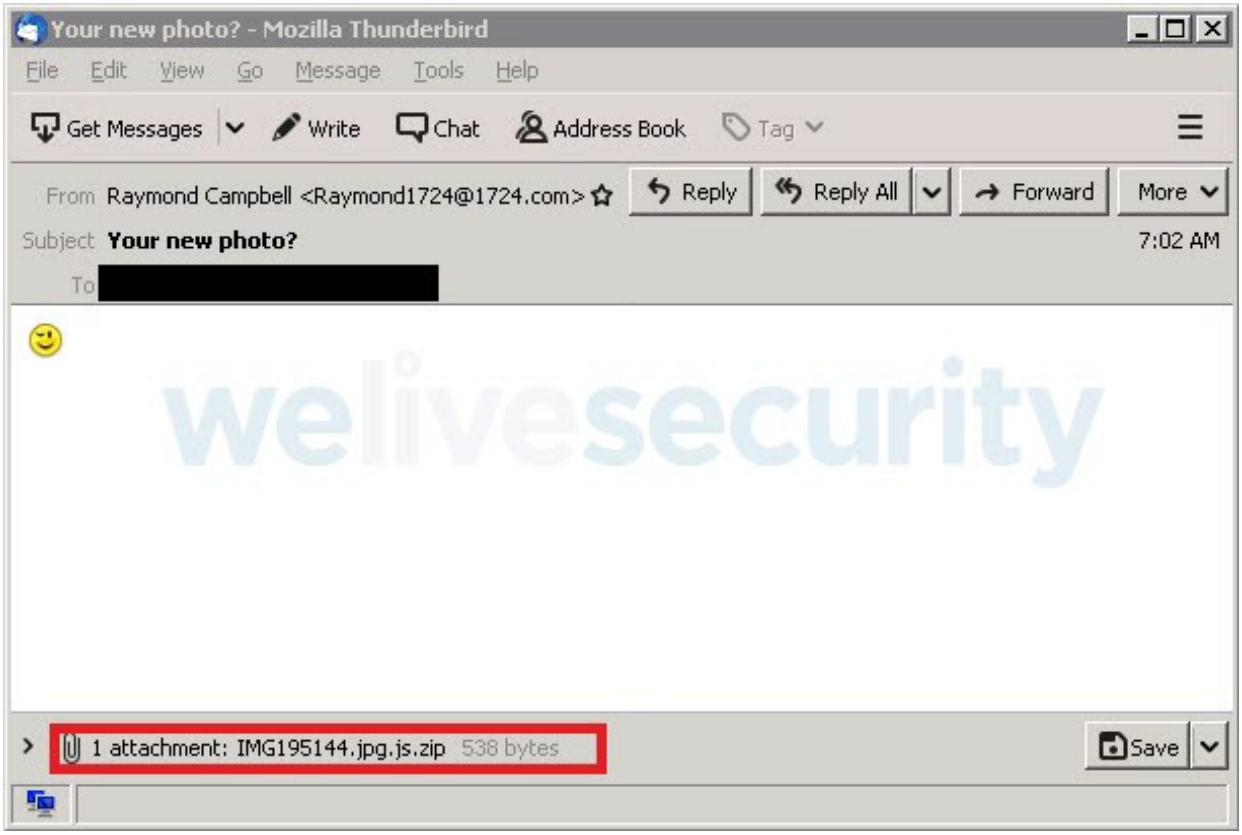

Imagen 1. Ejemplo de correo de phishing que contiene adjunto malicioso.

Cabe destacar que una vez ejecutado el ransomware, este no llevara a cabo sus funciones en el equipo comprometido si este posee una configuración de lenguaje del teclado o si el identificador del lenguaje del sistema es de alguno de los países que conforman la Comunidad de Estados Independientes, principalmente el ruso.

Mecanismos para lograr establecer persistencia

Antes de establecer persistencia en el sistema, Avaddon intenta elevar sus privilegios a través de un bypass en el User Account Control (UAC), que es bien conocido y ha sido utilizado por varias familias de malware. Si tiene éxito, se copia así mismo en la carpeta AppData\Roaming del usuario actual.

Utiliza dos tipos de métodos para ser ejecutado en el próximo inicio del sistema, o cuando la víctima inicia sesión en el sistema:

- Registrando una Tarea Programada (Scheduled Task)
- Registrandose en {HKLM|HKU}\Software\Microsoft\Windows\CurrentVersion\Run

Cifrado de archivos de este ransomware

Una vez concluido el proceso de persistencia, Avaddon prepara el sistema terminando los procesos que puedan interferir con el acceso a los archivos. Para esto descifra dos listas de nombres asociados a software tales como: Microsoft SQL, Microsoft Word, QuickBooks,

Remotely Anywhere, VMWare, y Java entre otros, así como también tres soluciones de seguridad: Symantec, 360 Secure Browser, G Data Security Software. Los nombres de estos procesos son:

- DefWatch, ccEvtMgr, ccSetMgr, SavRoam, dbsrv12, sqlservr, sqlagent, Intuit.QuickBooks.FCS, dbeng8, sqladhlp, QBIDPService, Culserver, RTVscan, vmware-usbarbitator64, vmware-converter, VMAuthdService, VMnetDHCP, VMUSBArbService, VMwareHostd, sqlbrowser, SQLADHLP, sqlwriter, msmdsrv, tomcat6, QBCFMonitorService
- exe, sqlmangr.exe, RAgui.exe, QBCFMonitorService.exe, supervise.exe, fdhost.exe, Culture.exe, wxServerView.exe, winword.exe, GDscan.exe, QBW32.exe, QBDBMgr.exe, qbupdate.exe, axlbridge.exe, 360se.exe, 360doctor.exe, QBIDPService.exe, wxServer.exe, httpd.exe, fdlauncher.exe, MsDtSrvr.exe, tomcat6.exe, java.exe, wdswfsafe.exe

Luego utiliza varias herramientas de Windows para ejecutar comandos con el fin de borrar los backups de seguridad, y copias shadow:

```
WMIC.exe wmic SHADOWCOPY DELETE /nointeractive
wbadmin.exe wbadmin DELETE SYSTEMSTATEBACKUP
wbadmin.exe wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
wbadmin.exe wbadmin DELETE SYSTEMSTATEBACKUP -keepVersions:0
 vssadmin.exe vssadmin Delete Shadows /All /Quiet
 bcdedit.exe bcdedit /set {default} recoveryenabled No
 bcdedit.exe bcdedit /set {default} bootstatuspolicy ignoreallfailures
 WMIC.exe wmic SHADOWCOPY DELETE /nointeractive
 wbadmin.exe wbadmin DELETE SYSTEMSTATEBACKUP
 wbadmin.exe wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
 wbadmin.exe wbadmin DELETE SYSTEMSTATEBACKUP -keepVersions:0
vssadmin.exe vssadmin Delete Shadows /All /Quiet
 bcdedit.exe bcdedit /set {default} recoveryenabled No
 bcdedit.exe bcdedit /set {default} bootstatuspolicy ignoreallfailures
 WMIC.exe wmic SHADOWCOPY DELETE /nointeractive
 wbadmin.exe wbadmin DELETE SYSTEMSTATEBACKUP
 wbadmin.exe wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
 wbadmin.exe wbadmin DELETE SYSTEMSTATEBACKUP -keepVersions:0
 vssadmin.exe vssadmin Delete Shadows /All /Quiet
 bcdedit.exe bcdedit /set {default} recoveryenabled No
 bcdedit.exe bcdedit /set {default} bootstatuspolicy ignoreallfailures
```


Imagen 2. Comandos ejecutados por Avaddon.

Finalmente, utiliza la API SHEmptyRecycleBinW para eliminar los contenidos de la papelera de reciclaje para evitar que el usuario pueda recuperar algún archivo o versión previa de algún archivo que la víctima haya eliminado con anterioridad.

Avaddon comienza el proceso de cifrado de archivos en el disco local y discos de red, evitando los siguientes directorios:

- C:\PERFLOGS
- C:\PROGRAM FILES (X86), C:\PROGRAM FILES, C:\PROGRAMDATA
- C:\USERS\{Nombre de usuario}\APPDATA
- C:\USERS\{Nombre de usuario}\APPDATA\LOCAL\TEMP
- C:\USERS\PUBLIC
- C:\WINDOWS

Los archivos que encuentra son descartados por su extensión, a fin de evitar cifrar archivos que puedan causar fallos en el sistema:

.exe, .bin, .sys, .ini, .dll, .lnk, .dat, .drv, .rdp, .prf, .swp

También tiene un listado de extensiones las cual son de alta prioridad, estas pertenecen archivos relacionados con base de datos SQL:

.mdf, .mds, .sql

Los datos son cifrados utilizando una combinación de AES-256 y RSA-2048. Los datos cifrados se reescriben en el archivo original y se añade al final un marcador de cifrado que le permite a Avaddon evitar archivos que ya han sido cifrados previamente, así como también identificar los archivos cifrados y descifrarlos si la victima paga para obtener el descifrador que ofrecen los criminales.

```
if ( CryptAcquireContextW(
        &phProv,
        0,
        L"Microsoft Enhanced RSA and AES Cryptographic Provider",
        0x18u,
        0xF0000000) )
{
    phKey = 0;
    if ( CryptGenKey(phProv, 0x6610u, 1u, &phKey) )
    {
        v7 = (v5 + 16);
        if ( *(v5 + 36) >= 8u )
            v7 = *pVictimFileToEncrypt;
        dwFileAttributes = GetFileAttributesW(v7) & 0xFFFFFFFE;
        v9 = (v5 + 16);
        if ( *(v5 + 36) >= 8u )
            v9 = *pVictimFileToEncrypt;
        SetFileAttributesW(v9, dwFileAttributes);
        pVictimFile = (v5 + 16);
        if ( *(v5 + 36) >= 8u )
            pVictimFile = *pVictimFileToEncrypt;
        hFile = CreateFileW(pVictimFile, 0xC0000000, 0, 0, 3u, 0x80u, 0);
        hObject = hFile;
        if ( hFile != INVALID_HANDLE_VALUE )
        {
            if ( *(v5 + 40) == 3 )
                bFileEncrypted = AVDN_EncryptFileA(this, phKey, hFile);
            else
                bFileEncrypted = AVDN_EncryptFileWithFlags(phKey, hFile, *(v5 + 40));
            if ( bFileEncrypted )
            {
                CloseHandle(hObject);
```

Imagen 3. Función de cifrado en Avaddon.

En las muestras que analizamos, los archivos que son cifrados correctamente son renombrados con la extensión .BeCecbaDBB. Como podemos observar en la Imagen 4, el tipo de archivos que comúnmente cifra son documentos, imágenes, archivos de audio y archivos de video.

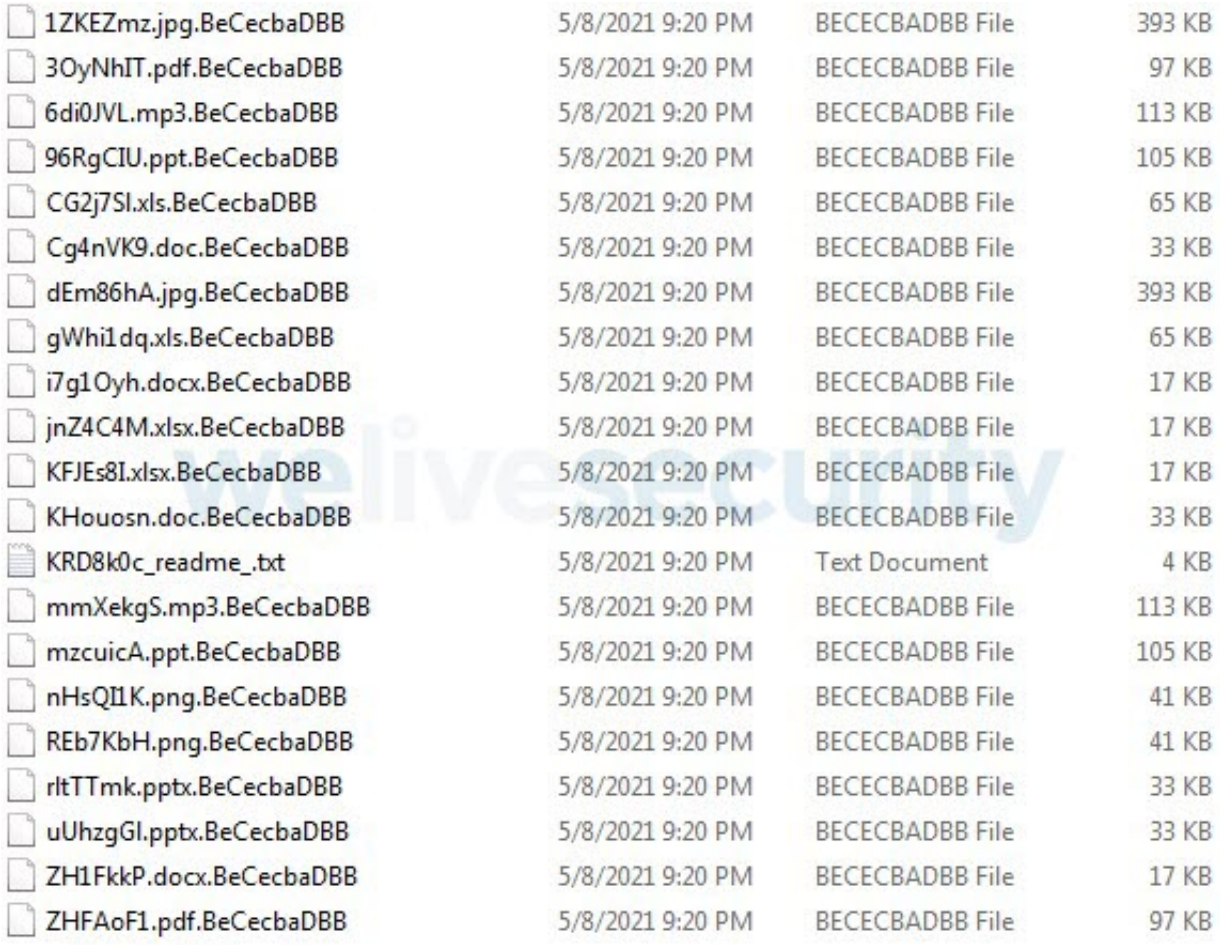

Imagen 4. Vista de una carpeta con varios tipos de archivos que fueron cifrados por Avaddon.

Finalmente, el ransomware crea un archivo .TXT que contiene la nota de rescate {aleatorio}_readme_.txt como podemos observar en la Imagen 5.

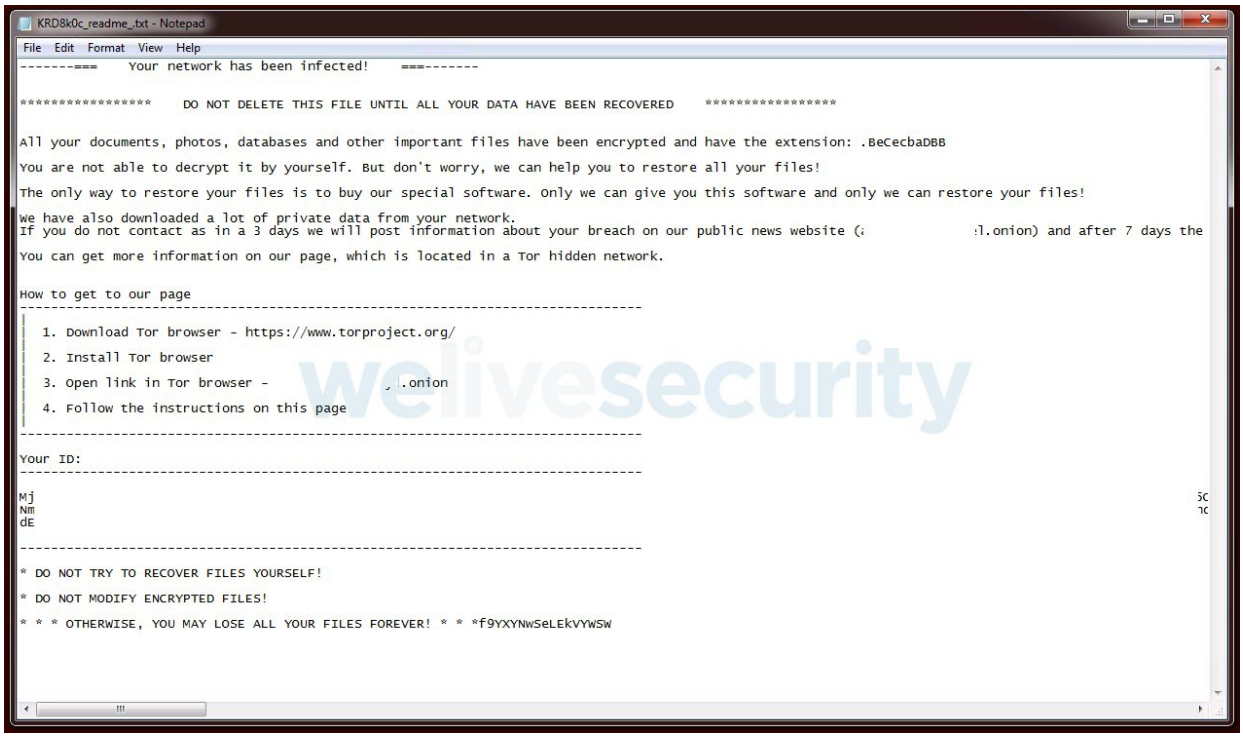

Imagen 5. Nota de rescate de Avaddon en texto plano que es utilizada por varias configuraciones.

Hay otros casos donde la nota es un archivo .HTML con una estética muy similar a la que utilizan en el sitio web de Avaddon.

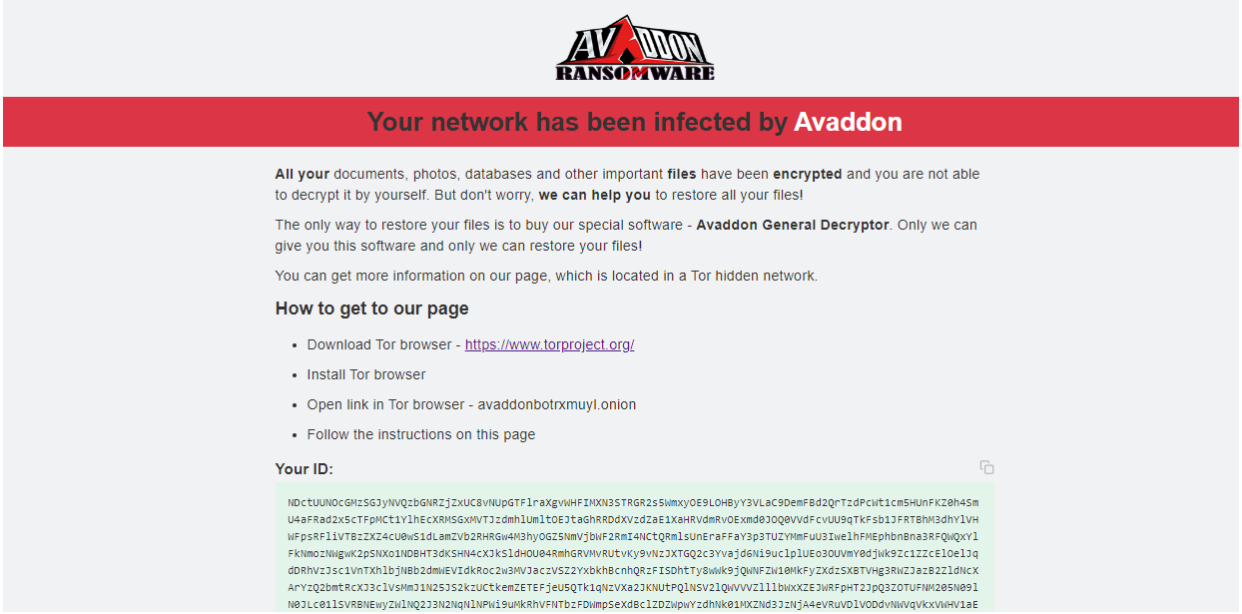

Imagen 6. Nota de rescate de otras versiones de Avaddon. (Fuente: @GrujaRS)

Consejos para prevenir un incidente

Considerando que la idea de pagar no debería ser la primera opción, ya que no solo es imposible saber si efectivamente los criminales proporcionarán el descifrador o no y que como ya se ha mencionado en reiteradas oportunidades pagando estimulamos la actividad

criminal al hacer que sea rentable para los atacantes, la primera opción tanto para empresas como usuarios debería ser la prevención.

Lectura recomendada: 11 formas de protegerte del ransomware

Teniendo esto en cuenta, algunas recomendaciones son.

- Hacer backup de la información de manera periódica
- Instalar una solución de seguridad confiable
- Utilizar una solución de cifrado de archivos
- Capacitar al personal sobre los riesgos que existen en Internet y cómo evitarlos
- Mostrar las extensiones ocultas de los archivos por defecto
- Analizar los adjuntos de correos electrónicos
- Deshabilitar los archivos que se ejecutan desde las carpetas AppData y LocalAppData
- Deshabilitar RDP cuando no sea necesario
- Actualizar el software de dispositivos de escritorio, móviles y de red
- Crear políticas de seguridad y comunicarlas a los empleados

31 May 2021 - 10:00AM

Suscríbase aquí para recibir actualizaciones sobre cualquier artículo nuevo en la sección crisis en Ucrania.

Newsletter

Discusión