

ÍNDICE

Introducción………………………………………………..pag 3

Definición…………………………………………………..pag 4

Tipos………………………………………………………..pag 5

Protección……………………………………………....….pag 9

Ejemplos……………………………………………….......pag 10

Conclusión………………………………………………….pag 16

Introducción

El ransomware fue una de las amenazas más activas durante 2020 y también de las más efectivas. Esto se puede deber al incremento del teletrabajo Estos ataque se centran en sectores como la salud. En la actualidad además de cifrar la información para pedir un rescate también se extorsiona a la víctima con la amenaza de publicar la información si no paga. Este método se utilizó por primera vez a finales de 2019 y se fue consolidando en 2020.

Para producir este tipo de ataques se necesita forzar el acceso a las credenciales para esto se utilizan otros procesos como el phishing (conseguir los datos a través de correos electrónicos fingiendo ser una entidad de confianza) e ingeniería social.

El aumento de estos ataques también está relacionado con que los atacantes ofrecen códigos maliciosos en la dark web para asociarse con otros que eran la distribución y así dividirse las ganancias.

Normalmente detrás de un ransomware hay otros malware como botnets (conjunto de dispositivos informáticos que se ejecutan de manera automática y autónoma), backdoor (es un troyano1 que abre una puerta trasera en el sistema permitiendo que un hacker remoto tome el control del equipo) o RDP comprometido (es un protocolo que permite la comunicación en la ejecución de una aplicación entre un cliente y un servidor)

1  Troyano: es un malware que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado para poder robar tu información confidencial y obtener acceso de puerta trasera a tu sistema

Definición

El ransomware es un tipo de malware que se utiliza para obligar a las personas a pagar por un rescate.

En su inicio el ransomware ataca a los equipos particulares aunque en la actualidad la mayoría de estos ataques son contra las empresas. Geográficamente se centran en occidente en países como Reino Unido, Estados Unidos y Canadá que son los más afectados

El ransomware se puede propagar a los dispositivos a través de archivos adjuntos, enlaces de correos electrónicos, páginas web con descarga oculta o un dispositivo extraíble infectado como USB, discos duros extraíbles.

Cuando el dispositivo se infecta el malware bloquea el acceso a los datos del sistema o los cifra de forma que el usuario no los puede utilizar. El atacante pide un rescate y así la víctima recupera el acceso o los datos



Tipos

Scareware

Es un malware que engaña a los usuarios para que visiten sitios infectados. Aparecen como antivirus legítimos que han detectado un malware en el dispositivo y para eliminarlo tienen que pagar por un antivirus falso que es el malware destinado a robar la información.

Se puede detectar porque si no se ha instalado en el dispositivo ninguna aplicación de esa compañía no va buscar posibles malware. También se puede detectar porque en el caso de que el dispositivo tuviera el malware no se pagaría por la eliminación de la infección.



Bloqueadores de pantalla

Al encender el dispositivo aparece una ventana que ocupa toda la pantalla que indica que se han detectado actividades ilegales y que debe de pagar una multa. Normalmente utilizan el logo del FBI o del departamento de justicia

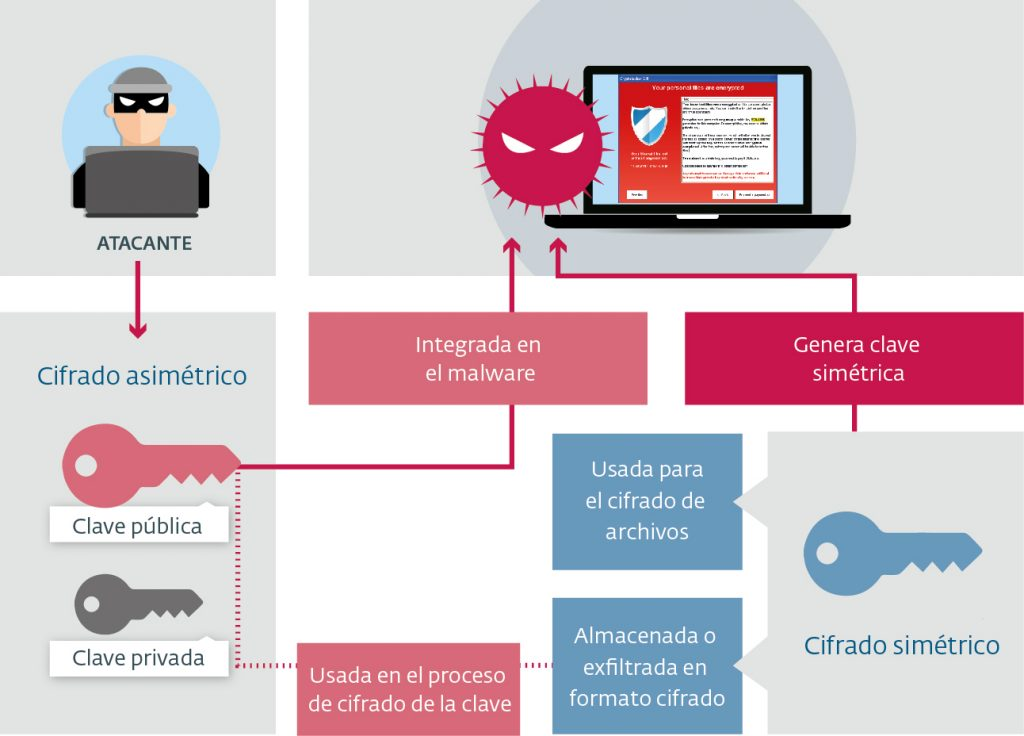
En el caso de que se sospeche que se comete algún delito informático el FBI seguiría los canales legales



Ransomware de cifrado

Este tipo de ransomware secuestra los archivos y los cifra exigiendo un pago para recuperarlos. Incluso si pagas no hay garantía de que se devuelvan los datos

Fue el primer ransomware, se originó sobre los años 80



Se puede evitar y solucionar con los siguientes consejos:

* Usar una solución confiable y habilita las medidas proactivas, como el sistema HIPS y la protección Anti-Phishing.
* Tener conductas seguras como pueden ser configurar el equipo para que muestre las extensiones ocultas de los archivos y no abrir enlaces ni mensajes de origen desconocido.
* Tener un backup de tus archivos recientes, válido y offline, por lo que te conviene proyectar la creación de copias de seguridad en forma periódica.
* Evitar guardar las carpetas de backups en unidades asignadas en tu equipo. El ransomware criptográfico es capaz de cifrar los backups ubicados en carpetas que se encuentren en dispositivos USB, en la nube y en cualquier otro lugar al que se pueda acceder como carpetas del sistema



Cómo protegerse del ransomware

Lo primero es prevenir un posible ataque para eso podemos utilizar programas con protección en tiempo real que proteja a los programas más vulnerables y que impida el secuestro de los archivos

También se debe de crear copias de seguridad regularmente en la nube con un cifrado de alto nivel o en un dispositivo extraíble que de desconecte al terminar la copia para evitar la infección

Otra medida importante es tener el software siempre actualizado para evitar posibles vulnerabilidades del sistema que ya están solucionadas



Ejemplos

Filtrado el próximo MacBook Pro de 16″

Se produjo el 22 de abril de 2021

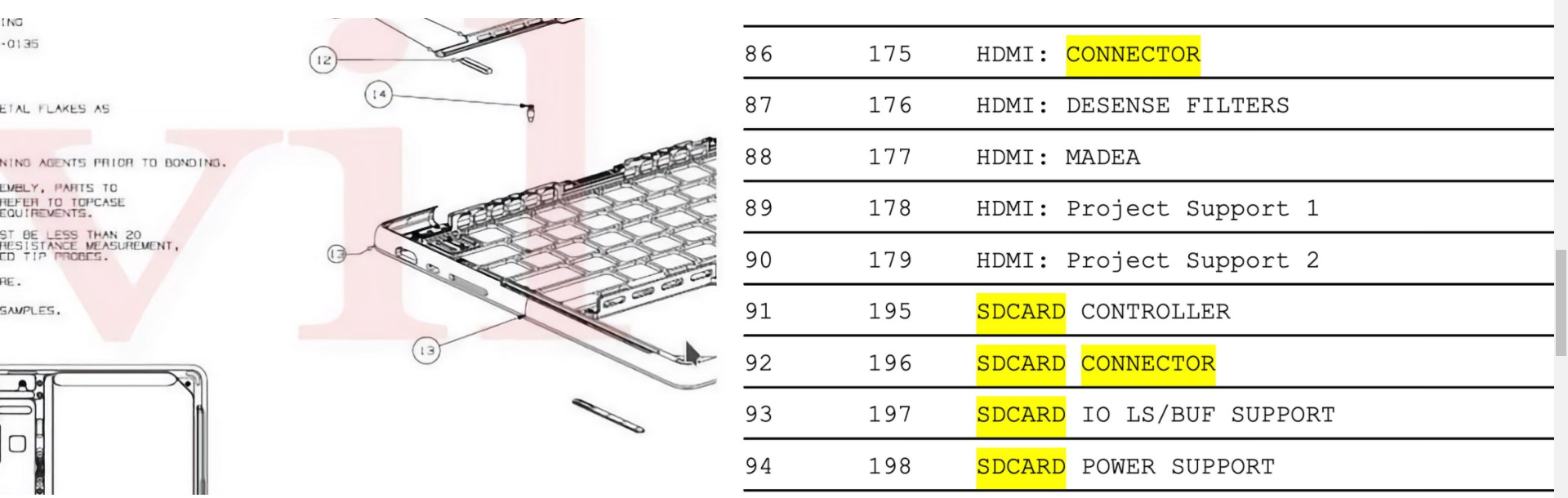
Una organización cibercriminal conocida como REvil robo los planos de los últimos MacBook que Apple presentará este año. Amenazan con publicarlos en la dark web si no reciben un rescate de 50 millones de euros por ellos.

El grupo REvil está especializado en este tipo de malware y tiene un blog en la dark web donde publica datos sobre sus ataques como quienes son sus víctimas, la cifra de rescate, y los datos sensibles que publicarían si no reciben el dinero.

En este blog explican que su víctima inicial es Quanta Computer (fabrican una gran parte de los MacBook).

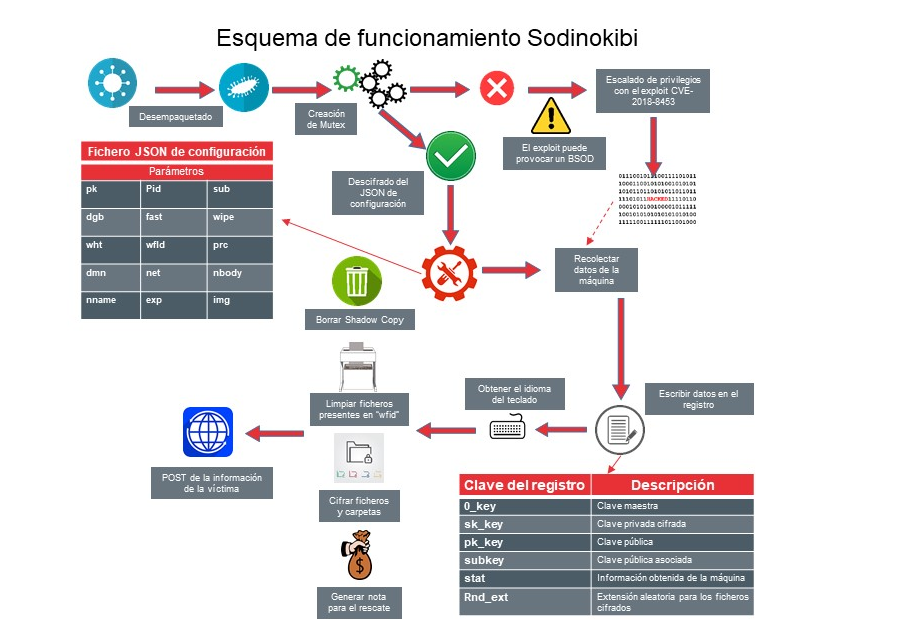
Quanta Computer reconoció que ha sufrido un ataque pero no el robo de la información. Como esta empresa no ha pagado el rescate se cambió de objetivo a Apple la cual tiene hasta el 1 de mayo para pagar el rescate. REvil ha amenazado con publicar cada día más planos de estos ordenadores hasta que se realice el pago

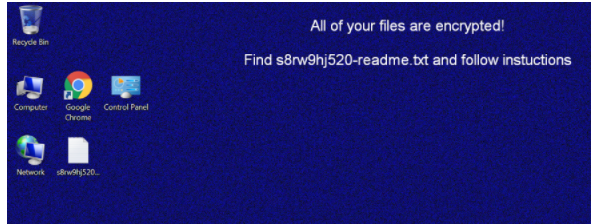
En el mes de marzo REvil ha exigido rescate a empresas como Acer (50 millones), Pierre Fare (25 millones) y Asteelflash (24 millones)



Este ataque se produjo utilizando un REvil (también conocido como Sodinokibi) que sigue el modelo RaaS. Este malware intenta obtener privilegios en el sistema utilizando vulnerabilidades consiguiendo así los datos de inicio y realizar el cifrado de los datos

Se envía un ejecutable que utiliza el algoritmo RC4 con una clave diferente y una longitud variable. Una vez ejecutado se genera un identificador para evitar que múltiples procesos ingresen a la vez. A continuación se inutilizan las funciones de restauración del sistema y se desactivan las copias de seguridad para luego eliminar todas que están almacenadas en el sistema. Finalmente se cifra la información cambiando la extensión de los archivos a una extensión personalizada y se genera una nota de rescate en cada directorio donde se cifraron los datos con el nombre de [Extensión]-how-to-decrypt.text. En este documento se detalla toda la información que debe de conocer la víctima para poder descifrar sus archivos como el sitio web que se atopa en un navegador Tor donde se proporciona un descifrador de prueba gratuito para un máximo de 3 archivos como garantía antes del pago de rescate que es mediante bitcoins. Cómo se obtienen datos de la víctima estos se utilizan como método de extorsión para las víctimas que no acceden al pago de rescate mediante amenazas de que serán publicados en internet o vendidos a sus competidores





Babuk Locker

Es el primer ransomware de 2021. Infecta a un dispositivo, bloquea el funcionamiento y el acceso a los archivos con un fuerte cifrado y exigiendo una cantidad de dinero como rescate para liberarlos.

La codificación incluye un cifrado seguro lo que evita que las víctimas recuperen sus archivos si no pagan. La extensión codificada es \_ NIST\_K571 \_,

En cada carpeta se crea una nota de rescate llamada How To Restore Your Files.txt que contiene información sobre el ataque y un enlace a la red oscura donde la víctima puede negociar. Los rescates van desde los 65000 a los 85000 dolares

Este ransomware se dirige principalmente a empresas con sede en Italia, España y los Emiratos Árabes Unidos

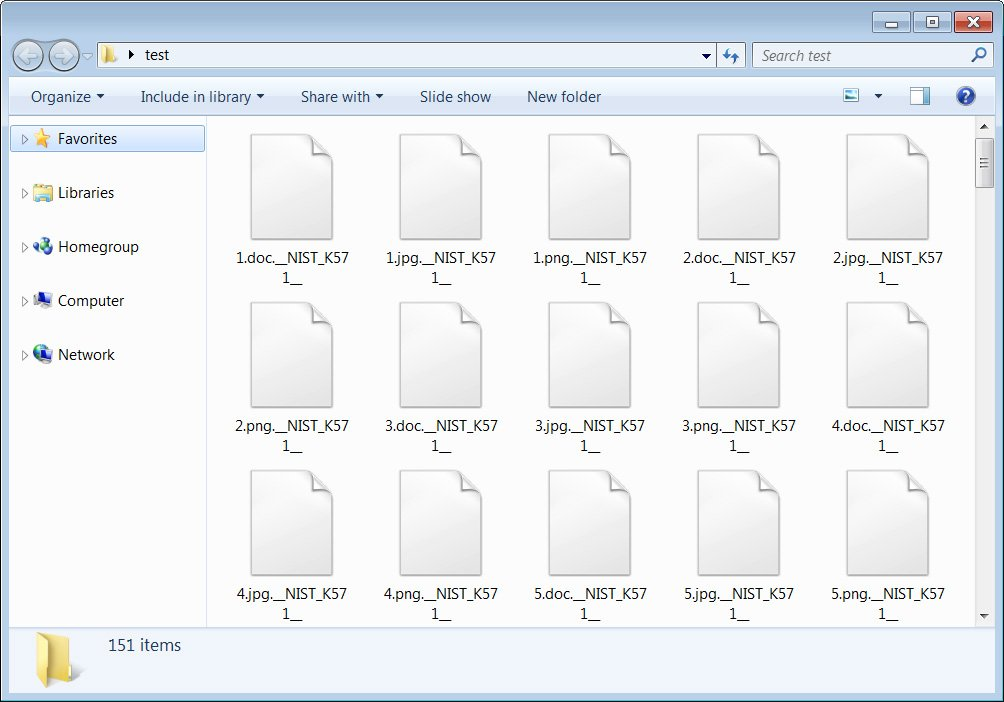
Algunas de las empresas afectadas son Phone House, Houston Rockets

En el caso de Phone House se habrían hecho con varias bases de datos de esta compañía de Oracle. Las bases de datos son

* INFOVENTAS: 7 gigabytes.
* PHONE: 31 gigabytes.
* POS: 1,6 gigabytes.
* PP: 19 gigabytes.
* SEGUROSPH: 951 megabytes.
* SMARTHOUSE: 11 gigabytes.
* TARVAR: 6 gigabytes.
* VENTASONLINE: 4,6 gigabytes.
* VISIOFRANK: 9,7 gigabytes.
* MK\_DWH: 23 gigabytes.

Los datos obtenidos son los datos personales de los clientes y los empleados como: direcciones de correo y postales, DNI, NIE, numeros de telefonos, fecha de nacimientos, nacionalidades, cuentas bancarias de los recibos de seguros al comprar un dispositivo

En el caso de los Houston Rockets filtrando datos como contratos,acuerdos de no divulgación, información del cliente, datos financieros hasta un total de 500 gigabytes de archivos



Ryuk

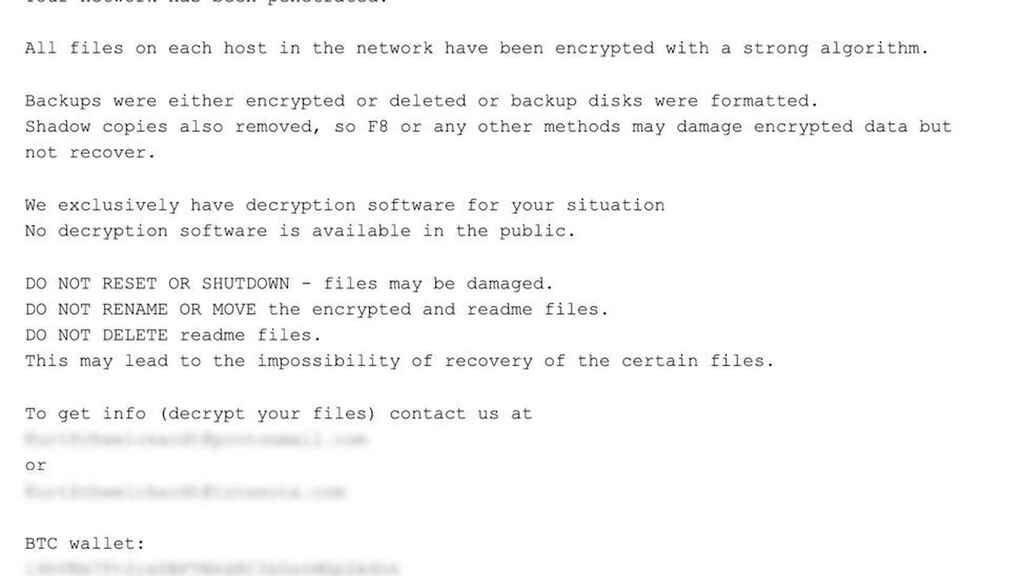
Se produjo el 10 de marzo

Apareció por primera vez en 2018 y se sospechó que tenía un origen en un grupo de hackers de Corea del Norte llamados Wizard. El objetivo es cifrar los datos y hacerlos inaccesibles y para desbloquearlos piden un rescate que normalmente hay que pagar en criptodivisas porque es más difícil de rastrear.

Los autores dejan un documento llamado RyukReadme.txt en el que se informa de las condiciones del rescate y cómo obtener la clave de descifrado

El Servicio Público de Empleo Estatal en España (SEPE) sufrió un ciberataque donde los datos personales, pagos de nóminas y las prestaciones por desempleo o ERTE no han estado afectadas aunque sí otros servicios

Parece que no se ha solicitado un rescate por este ataque según el director de este organismo



Conclusión

El aumento del teletrabajo y el ransomware están relacionados porque como la mayoría de los trabajadores es la primera vez que teletrabajan no tienen conocimientos suficientes de seguridad para protegerse de estos ataques. Los ciberdelincuentes aprovechan estas vulnerabilidades

En la actualidad se produce el escenario mejor para estes ataques: muchos dispositivos, distintas redes, distintas ubicaciones, y sin implementar un plan para trabajar remotamente de manera segura.

Algunos consejos para la protección en el teletrabajo:

* Utilizar los últimos parches y actualizaciones
* Tener un buen antivirus que prevenga la entrada de malwares
* evitar abrir enlaces o archivos que sean sospechosos

Pagar el rescate no es la opción recomendada. Porque nada asegura que la víctima recuperará los archivos cifrados y tampoco que los criminales no divulgarán los datos robados. Además, de esta manera se está financiando el ciberdelito y colaborando para que continúen los ataques.