Certified Tech Developer

The Ultimate Degree

Práctica Integradora

Grupo 8

Sofía Tohme Garnero
Esteban Lucena
Antonela Dutruel

Objetivo

Vamos a poner en práctica los conocimientos que hemos adquirido hasta el momento. Se crearán 10 grupos, divididos en sus respectivas salas y realizarán la siguiente ejercitación.

Micro desafíos

Deberán leer cada una de las noticias asignadas y responder en un documento (ustedes deben abrirlo) las siguientes consignas:

- ¿Qué tipo de amenaza es?
  Ransomware.
- ¿Cómo comienza y cómo se propaga esta amenaza?
  El grupo de ransomware REvil es un núcleo que presta este servicio mediante el mantenimiento del malware y la estructura de pago a un “afiliado” (persona, empresa, etc.) para realizar este tipo de ataques. En este caso el objetivo fue la empresa Quanta, fabricante de productos de Apple, a la que le robaron información de huellas digitales de dispositivos Apple.
- ¿Hay más de una amenaza aplicada ?

> Sí, es un caso de doble extorsión. Como Quanta no expresó interés en pagar el rescate, robaron los planos de MacBook y Apple Watch para presionar a la empresa norteamericana (Apple), pidiendo un rescate por la información sensible hasta el 1ero de mayo.

Una vez resueltas volveremos a la sala principal en la cual el grupo debe compartir sus respuestas a los demás compañeros.

TRADUCCIÓN DE LA NOTICIA:

El proveedor de Apple, Quanta, dijo el miércoles que sufrió un ataque de ransomware del grupo de ransomware REvil, que ahora exige que el fabricante del iPhone pague un rescate de 50 millones de dólares para evitar la filtración de archivos confidenciales en la web oscura.

En una publicación compartida en su portal web "Happy Blog", el actor de amenazas dijo que tomó posesión de esquemas de productos de la compañía estadounidense, como MacBooks y Apple Watch, al infiltrarse en la red del fabricante taiwanés, alegando que está solicitando un rescate. a Apple después de que Quanta no expresó interés en pagar para recuperar los planos robados.

"Nuestro equipo está negociando la venta de grandes cantidades de dibujos confidenciales y gigabytes de datos personales con varias marcas importantes", dijeron los operadores de REvil. "Recomendamos que Apple vuelva a comprar los datos disponibles antes del 1 de mayo".

Desde que se detectó por primera vez en junio de 2019, REvil (también conocido como Sodinokibi o Sodin) se ha convertido en uno de los grupos de ransomware como servicio (RaaS) más prolíficos, siendo la pandilla la primera en adoptar la llamada técnica de extorsión "que desde entonces ha sido emulada por otros grupos para maximizar sus posibilidades de obtener ganancia

La estrategia busca presionar a las empresas víctimas para que paguen principalmente publicando un puñado de archivos robados a sus objetivos de extorsión antes de cifrarlos y amenazando con liberar más datos a menos y hasta que se cumpla la demanda de rescate.

El actor principal asociado con la publicidad y promoción de REvil en los foros de ciberdelincuencia en ruso se llama Desconocido, también conocido como UNKN. El ransomware también se opera como un servicio afiliado, en el que los actores de amenazas son reclutados para propagar el malware al violar a las víctimas de la red corporativa, mientras que los desarrolladores centrales se encargan de mantener el malware y la infraestructura de pago. Los afiliados suelen recibir entre el 60% y el 70% del pago del rescate.

Todos estos cambios agresivos en las tácticas han dado sus frutos, ya que los operadores de ransomware obtuvieron más de 350 millones de dólares en 2020, un aumento del 311% con respecto al año anterior, según la empresa de análisis de cadenas de bloques Chainalysis.

El último desarrollo también marca un nuevo giro en el juego de la doble extorsión, en el que un cartel de ransomware persigue al cliente de una víctima tras un intento fallido de negociar el rescate con la víctima principal.

Nos comunicamos con Quanta para hacer comentarios y actualizaremos la historia si recibimos una respuesta.

Sin embargo, en un comunicado compartido con Bloomberg, la compañía dijo que trabajó con expertos de TI externos en respuesta a "ataques cibernéticos en una pequeña cantidad de servidores Quanta", y agregó que "no hay impacto material en las operaciones comerciales de la compañía".

1	https://thehackernews.com/2021/05/new-stealthy-rootkit-infiltrated.html
2	https://thehackernews.com/2021/04/experts-uncover-new-banking-trojan.html
3	https://thehackernews.com/2021/04/alert-theres-new-malware-out-there.html
4	https://thehackernews.com/2019/10/42-adware-apps-with-8-million-downloads.html
5	https://thehackernews.com/2020/03/android-apps-ad-fraud.html

6	https://thehackernews.com/2021/02/first-malware-designed-for-apple-m1.html
7	https://thehackernews.com/2021/04/passwordstate-warns-of-ongoing-phishing.html
8	https://thehackernews.com/2021/04/hackers-threaten-to-leak-stolen-apple.html
9	https://thehackernews.com/2021/04/facebook-busts-palestinian-hackers.html
10	https://thehackernews.com/2021/02/chinese-hackers-using-firefox-extension.html
11	https://thehackernews.com/2021/04/cybercriminals-using-telegram-messenger.html
12	https://thehackernews.com/2021/05/researchers-uncover-iranian-state.html