DigitalHouse>
Coding School

Certified Tech Developer
The Ultimate Degree

Práctica integradora

Mesa 7
Integrantes:

Sara Ramírez Andrade
Ariana González Vidal
Florencia Caico
Ana Laura Fidalgo
Daiana Valentini
Maria Alejandra Pantano

Objetivo

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

Actividad

Deberán leer cada una de las noticias asignadas y responder en un documento de Google Presentations para todas las mesas, las siguientes consignas:

Amenaza: REvil, también conocido como Sodinokibi.

- ¿Qué tipo de amenaza es?

Ransomware

- ¿Cómo comienza y cómo se propaga esta amenaza?

En este caso, se trató de un ataque de cadena de suministro utilizando un instalador de una actualización automática del software de gestión de IT de la compañía Kaseya, que es utilizado comúnmente por proveedores de servicios administrados. Un proveedor de servicios administrados (MSP, por sus siglas en inglés) es una empresa ofrece servicios de gestión de tecnología de la información (IT) de manera remota. En este caso, la actualización con permisos de administrador afectó a los MSP y estos a su vez infectaron los sistemas de sus clientes con la amenaza. Kaseya notificó a las personas potencialmente afectadas con la recomendación de cerrar posibles servidores VSA de manera inmediata hasta tanto se publique el parche. Sin embargo, para muchas empresas ya había sido tarde y ya habían sido afectadas por el ransomware que cifró su información

Ransomware de cifrado o criptoransomware: utiliza la criptografía para cifrar los archivos del equipo comprometido impidiendo que el usuario pueda acceder a ellos. Este tipo de ransomware es el más común, el más moderno, y el más efectivo y, aunque pueda removerse del equipo con facilidad, la información que se ha visto comprometida es difícil o -mayormente- imposible de recuperar. Usualmente busca atacar extensiones de archivo que sean de interés para los usuarios, como archivos de ofimática, multimedia, bases de datos, etcétera. También es capaz de cifrar unidades extraíbles y unidades de red mapeadas dentro del computador. El principal síntoma de un equipo comprometido por un criptoransomware es el cambio de extensión en los archivos y la imposibilidad para abrirlos.

- ¿Hay más de una amenaza aplicada?

Si.

La forma de distribución más común del ransomware es a través de correos de phishing con archivos adjuntos o enlaces que intentan engañar a los usuarios mediante ingeniería social para convencerlos de descargar la amenaza. Otras formas de distribución son mediante ataques a conexiones remotas, como el Protocolo de Escritorio Remoto (RDP), aprovechando el uso de contraseñas débiles. También a través de la explotación de vulnerabilidades —por ejemplo, mediante sitios web comprometidos utilizados para redirigir a sus visitantes a diferentes tipos de exploits—, así como también dispositivos USB, descarga de software pirata, entre otros.

Como podemos deducir de lo anterior, gran parte de los ataques comienza con el engaño de las personas que hacen uso del sistema, utilizando alguna de las numerosas técnicas que conforman a la Ingeniería Social, y también mediante ataques a conexiones remotas como el RDP. No obstante, los atacantes también pueden procurar hacerse del control remoto del sistema aprovechando vulnerabilidades en equipos desactualizados, mal configurados y/o sin ninguna solución de seguridad instalada.

● ¿Qué solución o medida recomendarían?

- Parches para reparar vulnerabilidades en software
- Descifrador universal para el ransomware REvil
- Tener siempre backups hechos

El curso de acción a seguir tras verse comprometido por ransomware dependerá de las medidas de seguridad que se hayan tomado antes de sufrir el incidente. Si se cuenta con un backup, es posible restaurar la información desde allí. Si el backup está desactualizado, cabe evaluar cuánta información puede restaurarse y, de ser suficiente, evitar el pago. Si no se posee backup o este fue igualmente comprometido, quedará en manos de las víctimas decidir si desean correr el riesgo de efectuar el pago. Esta es una

práctica que desaconsejamos.

Si tenemos la habilidad necesaria, podemos extraer la muestra de ransomware del equipo para identificar qué variante específica es la que ha logrado colarse dentro del sistema, utilizando servicios como VirusTotal para analizar el archivo. También podemos escanear nuestro equipo con una solución de seguridad - si es que no tenemos ninguna ya- para que detecte el código malicioso y nos informe a qué familia de ransomware pertenece. Una vez que tengamos esta información, podemos utilizar motores de búsqueda para ver si existe alguna herramienta que nos permita recuperar los archivos. ¡Cuidado! Muchas páginas prometen herramientas de descifrado de archivos, pero en realidad buscan aprovecharse del pánico de los usuarios para instalar más malware en el equipo. Siempre dirígete a sitios de confianza. Ten en cuenta que, a decir verdad, para la mayor parte del ransomware no existe forma de recuperar los archivos una vez que estos se han visto afectados.

Una vez resueltas, volveremos a la sala principal en la cual el grupo debe compartir sus respuestas a los demás compañeros y compañeras, exponiendo la problemática y el análisis que realizaron.

1

1	https://revistabyte.es/ciberseguridad/ryuk-ministerio-de-trabajo/
2	https://www.welivesecurity.com/la-es/2021/06/10/backdoordiplomacy-actualizando-quarian-turian-backdoor-utilizado-contra-organizac iones-diplomaticas/
3	https://www.welivesecurity.com/la-es/2021/04/08/vyveva-nuevo-ba ckdoor-grupo-apt-lazarus/

4	https://www.welivesecurity.com/la-es/2021/02/02/kobalos-amenaza -linux-afecta-infraestructuras-informaticas-alto-rendimiento/
5	https://www.welivesecurity.com/la-es/2019/10/22/navegador-tor-troyanizado-robar-bitcoins-darknet/
6	https://www.welivesecurity.com/la-es/2019/08/23/ataque-departamentos-financieros-balcanes-utiliza-backdoor-rat/
7	https://www.welivesecurity.com/la-es/2021/07/05/ataque-masivo-ransomware-revil-comprometio-mas-1000-companias-mundo/
8	https://www.welivesecurity.com/la-es/2021/05/11/ataque-ransomware-compania-oleoducto-colonia-pipeline-afecta-suministro-combustible-estados-unidos/
9	https://www.welivesecurity.com/la-es/2020/08/17/phishing-netflix-intenta-hacer-creer-cuenta-suspendida/
10	https://www.welivesecurity.com/la-es/2020/04/29/programa-quedate-casa-engano-busca-robar-informacion-usuarios/
11	https://www.welivesecurity.com/la-es/2020/07/27/club-premier-league-cerca-perder-millon-libras-estafa/
12	https://www.welivesecurity.com/la-es/2021/03/25/fraudes-travespa ypal-que-deben-saber-quienes-venden-productos/