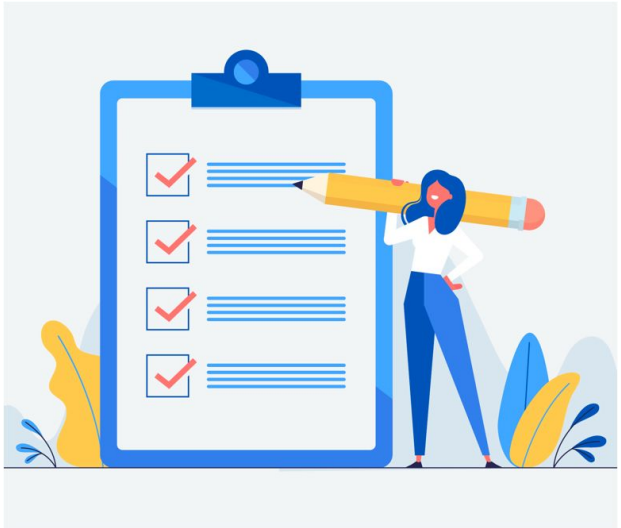
Actividad Tipos de Amenazas

Utilizando este documento de presentación, cada mesa deberá resolver y completar en cada hoja , que le corresponde según su número de mesa.



Mesa 1

Nota : <Ryuk: el ransomware que atacó al Ministerio de Trabajo (revistabyte.es)>

¿Qué tipo de amenaza es?

Ransomware Restringen el acceso a su sistema y archivos.

¿Cómo comienza y cómo se propaga esta amenaza?

A través de correos de phishing con archivos adjuntos o enlaces. Mediante ataques a conexiones remotas, como el Protocolo de Escritorio Remoto (RDP), aprovechando el uso de contraseñas débiles. También a través de la explotación 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.

¿Hay más de una amenaza aplicada ?

Su principal característica es que Ryuk no trabaja sólo: necesita la ayuda de otros virus para poder ejecutarse. Normalmente, su primera acción la realiza a través de un ataque de phishing basado en Emotec, un troyano que cambia su código cada poco tiempo a fin de no ser detectado por las soluciones de seguridad y que tiene la capacidad de interceptar, registrar, y guardar todo el tráfico de red.

¿Qué solución o medida recomendarían ?

En primer instancia, recomendaríamos apagar la computadora y desconectarla de la red. Identificar la amenaza, si es posible; utilizar una herramienta específica para recuperar el acceso a los archivos.

Finalmente, antes de pagar el rescate, recomendamos recuperar la información a través de un backup -que siempre se debe tener debido a la importancia de la información- y por otro lado recomendamos al Ministerio de Trabajo presupuesto en cirberseguridad.

Mesa 2: Este es nuestro enlace

1. **¿Qué tipo de amenaza es?**

   Es una amenaza tipo Backdoor (puerta trasera)

2. **¿Cómo comienza y cómo se propaga esta amenaza?**

   Comienzos: Como vectores de infección inicial, el grupo ha estado aprovechando la explotación de dispositivos vulnerables expuestos a Internet, como servidores web e interfaces de gestión para equipos de red.
   Propagación: Estas “puertas traseras” permiten al usuario malicioso controlar el equipo infectado, pudiendo enviar y recibir archivos, ejecutarlos o eliminarlos, mostrar mensajes, borrar o robar datos, reiniciar el equipo, etc. Es decir, puede controlar el equipo como si estuviese sentado delante de él y a los mandos.

Mesa 2: Este es nuestro enlace

3. ¿Hay más de una amenaza aplicada?

Sí, se observó a los operadores cargar droppers de backdoors. Los operadores intentaron disfrazar sus droppers de backdoor y evadir la detección de varias maneras. Un dropper es una amenaza de tipo troyano que permite instalar backdoors.

4. ¿Qué solución o medida recomendarían ?

Protección recomendada (backdoor): La eliminación manual de un backdoor no es fácil y, de hecho, lo mejor es recurrir a una herramienta para su eliminación automática; los antivirus cuentan con esta opción, de manera que cuando encuentran un virus lo marcan para su posterior eliminación.

Protección recomendada (Dropper): Si ningún antivirus funciona, puedes tratar de eliminar el virus Trojan Dropper manualmente. Una opción válida, es usar el administrador de tareas y analizar aquellos procesos sospechosos. Si ves un programa que no uses o se vea sospechoso, analízalo.

Mesa 3

Nota: https://www.welivesecurity.com/la-es/2021/04/08/vyveva-nuevo-backdoor-grupo-apt-lazarus/

¿Qué tipo de amenaza es?

Es un Troyano

¿Cómo comienza y cómo se propaga esta amenaza?

A menudo, los troyanos se propagan a través de un archivo infectado adjunto a un correo electrónico o se esconden tras una descarga de juegos, aplicaciones, películas o tarjetas de felicitación gratuitos. Pueden realizar diferentes tareas, pero, en la mayoría de los casos, crean una puerta trasera que permite la administración remota a un usuario no autorizado y es utilizado para el robo de datos personales.

¿Hay más de una amenaza aplicada?

Los daños o violaciones de privacidad que puede causar este virus es el uso de la webcam sin permiso, borrar el disco, modificar la agenda de contactos, robo de información (como datos bancarios e información personal), cambiar configuraciones en el sistema operativo, modificar carpetas y archivos, efectuar llamadas y enviar SMS, hasta geolocalizar al usuario por GPS.

¿Qué solución o medida recomendarían?

Para protegerte de los troyanos, lo principal es contar con un antivirus actualizado y un firewall. El antivirus te avisará si has descargado un archivo que incluye un virus troyano y los eliminará en caso de que ya estés infectado.

Mesa 4

Nota

:https://www.welivesecurity.com/la-es/2021/02/02/kobalos-amenaza-linux-afecta-in

fraestructuras-informaticas-alto-rendimiento/

¿Qué tipo de amenaza es?

¿Cómo comienza y cómo se propaga esta amenaza?

¿Hay más de una amenaza aplicada ?

¿Qué solución o medida recomendarían ?

Mesa 5

Nota :

https://www.welivesecurity.com/la-es/2019/10/22/navegador-tor-troyanizado-robar-bitcoins-darknet/

¿Qué tipo de amenaza es?

Spywares

¿Cómo comienza y cómo se propaga esta amenaza? Comienza una vez que se instala la actualización de la aplicación de Tor. Esto solo afecta a los usuarios de windows.

¿Hay más de una amenaza aplicada ? Esta amenaza fue diseñada para robar monedas digitales de aquellos que visitan mercados de la darknet.

¿Qué solución o medida recomendarían? La solución sería mantener actualizada la aplicación.

Mesa 6 - Martin Paliza, Maria Vanesa López, Sara Palacio, Mayra Torres, Diana Cardozo y Estefania Bermudez

Nota: <https://www.welivesecurity.com/la-es/2019/08/23/ataque-departam>

¿Qué tipo de amenaza es?= Un backdoor y un troyano de acceso remoto (RAT) que se nombran respectivamente, BalkanDoor y BalkanRAT.

¿Cómo comienza y cómo se propaga esta amenaza?= Comienza con una campaña publicitaria y se propaga por medio de correos electrónicos maliciosos.

¿Hay más de una amenaza aplicada?= BalkanDoor (el atacante envía un comando para desbloquear la pantalla) y BalkanRAT (pueden hacer lo que quieran en la computadora.)

¿Qué solución o medida recomendarían?= Seguir las reglas básicas de ciberseguridad: tener cuidado con los correos electrónicos y examinar tanto los archivos adjuntos como los enlaces que puedan venir en ellos; mantener actualizado sus equipos y utilizar una solución de seguridad confiable.

Mesa 7

Nota: <Ataque masivo del ransomware REvil comprometió más de 1000 compañías en mundo | WeLiveSecurity>

¿Qué tipo de amenaza es?

Ransomware
Es un malware o código malicioso que tiene como objetivo cifrar los datos de la computadora de la víctima impidiendo el acceso y solicitando un pago de “rescate” generalmente en bitcoins.

¿Cómo comienza y cómo se propaga esta amenaza?

Comenzó por la actualización con permisos de administrador que afectó a los MSP y estos a su vez infectaron los sistemas de sus clientes con la amenaza; fue un ataque de cadena de suministro utilizando un instalador de una actualización automática del software de gestión de IT de la compañía Kaseya.

¿Hay más de una amenaza aplicada?

No, en este caso particular no se robó la información previamente a la encriptación, algo que es una práctica común en este tipo de ataques.

Mesa 7

Nota: <Ataque masivo del ransomware REvil comprometió más de 1000 compañías en mundo | WeLiveSecurity>

¿Qué solución o medida recomendarían?

1. Se recomienda que aquellas empresas que tienen servidores que pueden haber sido comprometidos por este ataque que se mantengan informadas y que apaguen las máquinas potencialmente vulnerables o que al menos las aíslen de la red hasta que aparezca más información, mencionaron Goretsky y Camp.
2. Por su parte, la Agencia Nacional de Ciberseguridad de Estados Unidos junto al FBI publicaron una guía para los proveedor de servicios administrados afectados por este ataque así como para sus clientes, que incluye, entre otros puntos, descargar la herramienta de detección de Kaseya VSA, la cual analiza un sistema e indica si se detecta la presencia de algún Indicador de compromiso.

Mesa 8

Nota : <https://bit.ly/3oHVkRR>

¿Qué tipo de amenaza es? Randsomeware
DarkSide sustrae información de los sistemas comprometidos antes de cifrar la información y en caso de no querer negociar el pago del rescate extorsiona a sus víctimas con filtrar la información en un sitio específicamente creado para ese fin

¿Cómo comienza y cómo se propaga esta amenaza? Vulnerando las conexiones remotas como el RDP para acceder al sistema.

¿Hay más de una amenaza aplicada?
Si bien afecto a varias empresas el modo de operar siempre fue el mismo.

¿Qué solución o medida recomendarían ?
Como medida preventiva, invertir en fortalecer la cyberseguridad de la empresa. Ya afectados por la amenaza, el aislamiento de los equipos afectados de la red, inhabilitación de la red interna, bloqueo de credenciales RDP.

Mesa 9

Nota : <Poner el link>

¿Qué tipo de amenaza es?

¿Cómo comienza y cómo se propaga esta amenaza?

¿Hay más de una amenaza aplicada ?

¿Qué solución o medida recomendarían ?

Mesa 10

Nota : <Poner el link>

¿Qué tipo de amenaza es?

¿Cómo comienza y cómo se propaga esta amenaza?

¿Hay más de una amenaza aplicada ?

¿Qué solución o medida recomendarían ?

Mesa 11

Nota : <Poner el link>

¿Qué tipo de amenaza es?

¿Cómo comienza y cómo se propaga esta amenaza?

¿Hay más de una amenaza aplicada ?

¿Qué solución o medida recomendarían ?

Mesa 12

Nota : <Poner el link>

¿Qué tipo de amenaza es?

¿Cómo comienza y cómo se propaga esta amenaza?

¿Hay más de una amenaza aplicada ?

¿Qué solución o medida recomendarían ?