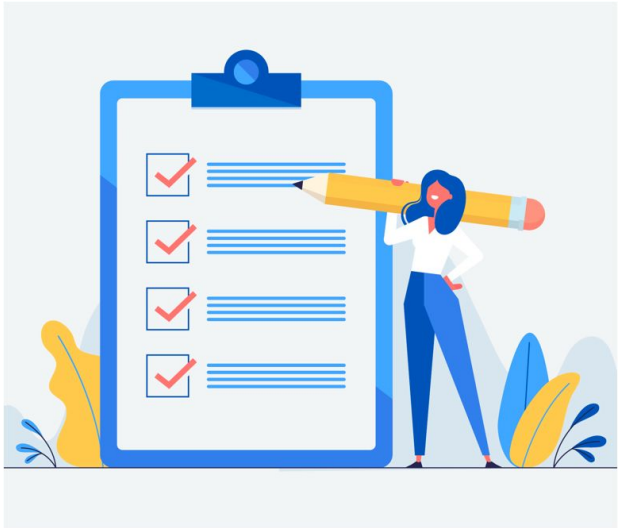
Actividad Tipos de Amenazas

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? Es ransomware Ryuk

¿Cómo comienza y cómo se propaga esta amenaza? Ryuk se propaga con la ayuda de otros virus. Ataca por medio de phishing (envío de correos electrónicos) 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.

¿Hay más de una amenaza aplicada ?Si, Ryuk se encarga de encriptar los datos pero previamente esos datos son traidos por **Emotec** y **Trickbot**, este último se encarga de los ataques laterales, entre otros, el robo de las credenciales de inicio de sesión.

¿Qué solución o medida recomendarían ?

Recomendamos instruir a los empleados para detectar este tipo de amenazas. También recomendamos hacer un backup de los datos . Además se recomienda invertir en ciberseguridad, como ser antivirus de calidad y profesionales expertos en el área

Mesa 2

Nota:https://www.welivesecurity.com/la-es/2021/06/10/backdoordiplomacy-actualizando-quarian-turian-backdoor-utilizado-contra-organizaciones-diplomaticas/

¿Qué tipo de amenaza es? Spyware - Robo de información dirigido a organizaciones gubernamentales y empresariales.

¿Cómo comienza y cómo se propaga esta amenaza? Inicia afectando servidores web e interfaces de gestión para equipos de red. Se propaga a través de backdoors dejándolas abiertas y expuestas.

¿Hay más de una amenaza aplicada?

Robo de datos, cifrado de red y exposición de la backdoor para latentes amenazas a los sistemas.

¿Qué solución o medida recomendarían?

Invertir en seguridad informática y antihacking para preservar la calidad e integridad de los datos para así , evitar el robo mediante vulnerabilidades por el uso de interfaces de gestión.

Mesa 3

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

¿Qué tipo de amenaza es?

BACKDOOR

¿Cómo comienza y cómo se propaga esta amenaza?

Aunque Vyveva se ha estado utilizando desde al menos diciembre de 2018, aún se desconoce su vector de compromiso inicial. Nuestros datos de telemetría sugieren que ha sido desplegado en ataques dirigidos, ya que solo encontramos dos máquinas víctimas, ambas son servidores propiedad de una empresa de logística de carga ubicada en Sudáfrica.

¿Hay más de una amenaza aplicada ?

Si, hay mas de una amenaza aplicada y muestra similitudes con muestras antiguas de Lazarus.

¿Qué solución o medida recomendarían ?

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. Este proceso viene explicado paso a paso por el propio antivirus que estemos usando, por lo que generalmente es sencillo de hacer. También podemos recurrir a otros programas de limpieza, como CCleaner o Malwarebytes Anty-malware, para usarlos tras realizar el análisis con el antivirus.

Mesa 4

Nota : <Click aquí>

Malware de Backdoor

La infección inicia a través de modo troyano que muta. Una vez en la máquina abre puertos y se esparce por la red. Tiene un acceso al protocolo SSH, utiliza puertos TPC, espera una conexión entrante en el mismo. Para atacar a sus víctimas, estas son equipos de alto rendimiento, agencias gubernamentales, servidores etc.

Lo recomendable en estos casos es implementar una autenticación de dos pasos.

Mesa 5

Nota :

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

¿Qué tipo de amenaza es? Virus Troyano.

¿Cómo comienza y cómo se propaga esta amenaza? Comienza pidiendo una actualización del navegador y luego redirige al usuario a un segundo sitio malicioso.

¿Hay más de una amenaza aplicada ? Si. Un troyano que infecta y luego ejecuta scripts maliciosos.

¿Qué solución o medida recomendarían ? Tener el sistema operativo actualizado. Navegar solo en páginas oficiales. Usar maquina virtual. Contar con algún antivirus confiable.

Mesa 6

Nota : https://www.welivesecurity.com/la-es/2019/08/23/ataque-departamentos-financieros-balcanes-utiliza-backdoor-rat/

¿Qué tipo de amenaza es?
Son troyanos. Un backdoor y un troyano de acceso remoto (BalkanDoor y BalkanRAT)

¿Cómo comienza y cómo se propaga esta amenaza?
Los atacantes han estado distribuyendo sus herramientas a través de correos electrónicos maliciosos (“malspam”) con enlaces que conducen a un archivo malicioso. Los enlaces incluidos en los correos de malspam y que son utilizados para la distribución de BalkanRAT y BalkanDoor, imitan la identidad de sitios web legítimos de instituciones oficiales. Con frecuencia, los enlaces que conducen a un archivo ejecutable se disfrazan como enlaces a un PDF. El archivo ejecutable es un WinRAR auto extraíble cuyo nombre e icono son modificados para parecerse a un archivo PDF y así engañar al usuario. Una vez que se ejecuta, está configurado para desempaquetar su contenido, abrir el PDF utilizado como señuelo para evitar cualquier sospecha y ejecutar silenciosamente BalkanRAT o BalkanDoor.

¿Hay más de una amenaza aplicada?
Sí, son dos amenazas distintas pero similares. Ambas controlan el ordenador de forma remota pero BalkanRAT controla el S.O. a través de la interfaz gráfica y BalkanDoor a través de líneas de comando.

¿Qué solución o medida recomendarían ?
Se pueden resolver de forma manual mediante la supresión de todas las claves de registro y archivos, sacarlos de la lista de inicio y anular el registro de todos los archivos DLL correspondientes.

Mesa 8

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 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 ?