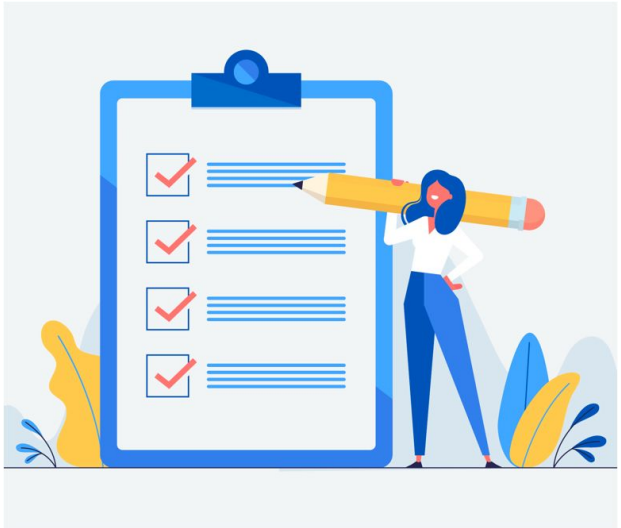
Actividad Tipos de Amenazas

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 : <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 2

Nota : <Poner el link>

¿Qué tipo de amenaza es?

De tipo Gusano, ya que su propagación se dio a partir de la red. (BackdoorDiplomacy apuntó a servidores con puertos expuestos a Internet, probablemente explotando vulnerabilidades sin parchear o la pobre implementación de la seguridad de carga de archivos.)

¿Cómo comienza y cómo se propaga esta amenaza?

BackdoorDiplomacy utiliza software de código abierto para el reconocimiento y la recopilación de información, y hace uso de la técnica DLL search order hijacking para instalar su backdoor: Turian. Finalmente, BackdoorDiplomacy emplea de manera separada un ejecutable para detectar medios extraíbles, probablemente unidades flash USB, y copiar su contenido en la papelera de reciclaje de la unidad principal.

¿Hay más de una amenaza aplicada ?

BackdoorDiplomacy y APT15 usan las mismas técnicas y tácticas para droppear sus backdoors en los sistemas, la anteriormente mencionada DLL search order hijacking.

¿Qué solución o medida recomendarían?

1. Intentar copiar todos los archivos en la unidad a un archivo protegido con contraseña y coloca el archivo en un directorio codificado.
2. Usar un dominio de servidor C&C compartido, un backdoor de Linux

Mesa 3

Nota : <Poner el link>

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

¿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 4

Nota:https://www.welivesecurity.com/la-es/2021/02/02/kobalos-amenaza-linux-afecta-infraestructuras-informaticas-alto-rendimiento/

¿Qué tipo de amenaza es?

Malware multiplataforma.

¿Cómo comienza y cómo se propaga esta amenaza?

Kobalos, es un malware que utiliza una versión maliciosa modificada o troyanizada de OpenSSH que proporciona acceso remoto al sistema de archivos y puede generar sesiones de terminal, lo que permite a los atacantes ejecutar comandos arbitrarios. También al abrir un puerto TCP y esperar una conexión entrante (a veces llamada puerta trasera pasiva)

Mesa 4

Nota: https://www.welivesecurity.com/la-es/2021/02/02/kobalos-amenaza-linux-afecta-infraestructuras-informaticas-alto-rendimiento/

¿Hay más de una amenaza aplicada ?

R/- no solo hay una y sirve para robar credenciales basicamentes

¿Qué solución o medida recomendarían ?

Mantener actualizados los sistemas operativos.

Utilizar soluciones de antivirus para detectar el malware y sus actividades sospechosas.

Configurar la autenticación de dos factores para conectarse a servidores SSH.

Analizar el tráfico de red buscando tráfico que no sea SSH en el puerto atribuido a un servidor SSH.

Mesa 5

Nota : Descubren Navegador Tor troyanizado utilizado para robar bitcoins en la darknet | WeLiveSecurity

¿Qué tipo de amenaza es? Troyano

¿Cómo comienza y cómo se propaga esta amenaza? utilizando mensajes de spam en varios foros rusos. Los delincuentes comenzaron a utilizar el servicio web pastebin.com para promover los dos dominios relacionados con el falso Navegador Tor. Específicamente, crearon cuatro cuentas.

¿Hay más de una amenaza aplicada ? Este Navegador Tor troyanizado es una forma atípica de malware que fue diseñado para robar monedas digitales de aquellos que visitan mercados de la darknet y los usuarios perdieron anonimato, que es uno de los objetivos de ese navegador.

¿Qué solución o medida recomendarían ? No confiar en mensajes spam, verificar bien la veracidad de los sitios. Verificar el origen del link de descarga. Una forma de solucionarlo es formatear el equipo.

Mesa 6

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

¿Qué tipo de amenaza es? Un backdoor y un troyano

¿Cómo comienza y cómo se propaga esta amenaza? Estos actúan como un troyano al click del usuario, permitiendo al atacante controlar la computadora afectada.Con archivos adjuntos en correos electrónicos, en formato PDF o .zip.

¿Hay más de una amenaza aplicada ? En este caso hablamos de dos amenazas implicadas, **BalkanDoor** y **BalkanRAT**

¿Qué solución o medida recomendarían ?Para mantenerse a salvo, los usuarios que se desempeñen en áreas de negocios, así como sus superiores, deben 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 8

Nota :

https://www.welivesecurity.com/la-es/2021/05/11/ataque-ransomware-compania-oleoducto-colonia-pipeline-afecta-suministro-combustible-estados-unidos/

¿Qué tipo de amenaza es?

Es un ransomware o software de secuestro.

¿Cómo comienza y cómo se propaga esta amenaza?

El usuario es el que accede a través de ocultos o links que llegan a su correo electrónico desde bancos o instituciones legales, también se encuentran en redes para compartir archivos como las P2P, así se propaga y te bloquea el sistema.

¿Hay más de una amenaza aplicada?

No, no hay más amenazas implicadas.

¿Qué solución o medida recomendarían?

Ser cuidados con las descargas y aplicaciones no autorizadas, evitar páginas peligrosas, usar un software antimalware.
Se pueden prevenir realizando capacitaciones al personal.

Mesa 9

Nota : https://www.welivesecurity.com/la-es/2020/08/17/phishing-netflix-intenta-hacer-creer-cuenta-suspendida/

¿Qué tipo de amenaza es?

Phishing

¿Cómo comienza y cómo se propaga esta amenaza?

Inicia con la creación de un sitio web fraudulento. Se distribuye a través de correo electrónico

¿Hay más de una amenaza aplicada?

No, únicamente Phishing

¿Qué solución o medida recomendarían ?

Verificar la dirección del remitente.

Acceder a la página oficial de Netflix para verificar el estado de la cuenta.

Se recomienda utilizar sitios que identifiquen la posible existencia de malware: https://opentip.kaspersky.com/

Mesa 10

Nota :
https://www.welivesecurity.com/la-es/2020/04/29/programa-quedate-casa-engano-busca-robar-informacion-usuarios/

¿Qué tipo de amenaza es?
Robo de identidad

¿Cómo comienza y cómo se propaga esta amenaza?
Por medio de redes sociales a partir de cadenas de mensajes

¿Hay más de una amenaza aplicada?
Si, ya que pueden incrustar virus, gusanos, entre otros; en nuestros dispositivos

¿Qué solución o medida recomendarían?
No abrir cadenas, hacer campañas para evitar reenviar mensajes que no son de fuentes comprobadas y denunciar los mensajes

Mesa 11

Nota :

https://www.welivesecurity.com/la-es/2020/07/27/club-premier-league-cerca-perder-millon-libras-estafa/

¿Qué tipo de amenaza es?/ phishing y ransomware

¿Cómo comienza y cómo se propaga esta amenaza?/ El Phishing empieza con el envío de links que no corresponden a donde realmente se quiere dirigir creando una suplantación de identidad y el ransomware con una posible infección por archivos en correos o conexiones remotas inseguras generando una encriptación de información sensible para las organizaciones para posterior pedir rescate.

¿Hay más de una amenaza aplicada? Si, se presentaron dos tipos de amenazas.

¿Qué solución o medida recomendarían? Se recomienda una mejor inversión en infraestructura y buen manejo de políticas de seguridad.

Mesa 7

Nota:https://www.welivesecurity.com/la-es/2021/07/05/ataque-masivo-ransomware-revil-comprometio-mas-1000-companias-mundo/

¿Qué tipo de amenaza es? Es un ransomware

¿Cómo comienza y cómo se propaga esta amenaza?

Comienza utilizando un instalador de una actualización automática del software de gestión de IT de la compañía Kaseya.

¿Hay más de una amenaza aplicada ? No, no hay más de una amenaza.

¿Qué solución o medida recomendarían ? Se recomienda que las empresas que tengan servidores comprometidos o afectados 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. Además, se recomienda 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.