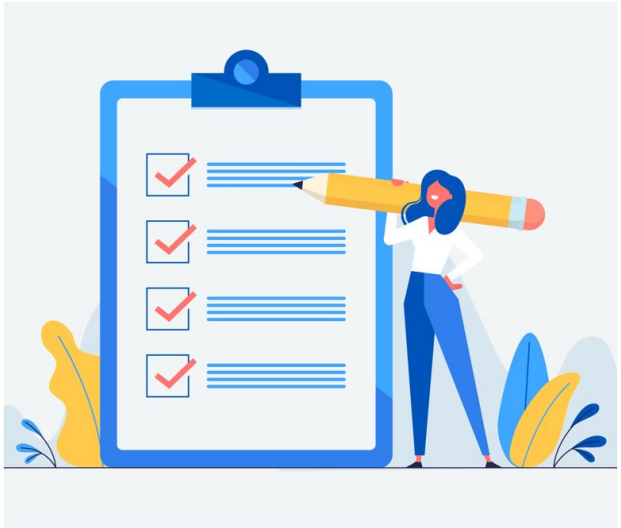
Actividad Tipos de Amenazas

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 : <https://revistabyte.es/ciberseguridad/ryuk-ministerio-de-trabajo/>

¿Qué tipo de amenaza es? Es un ransomware

¿Cómo comienza y cómo se propaga esta amenaza?

Comienza con 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.

¿Hay más de una amenaza aplicada ?

Si, ya que a la alta capacidad de infección se le suma la encriptación de los equipos y la anulación de la práctica total de los recursos de la red.

¿Qué solución o medida recomendarían?

Tomar medidas preventivas para evitar este tipo de situaciones en un futuro, como el aumento del presupuesto de ciberseguridad para adaptarse a amenazas cambiantes.

Nota : # Mesa 2

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

¿Qué tipo de amenaza es? Malware - Spyware

¿Cómo comienza y cómo se propaga esta amenaza?
Comienza con un escaneo previo de la entidad que será víctima del ataque, buscando vulnerabilidades ya sean puertos abiertos o en protocolos con implementaciones de seguridad pobres. Después de determinada la ruta de acceso, mediante varias herramientas disponibles, de manera opensource se realiza un ataque en el que se deposita un backdoor el cual nos brinda acceso al sistema de la víctima que nos permite realizar configuraciones que asegure la persistencia del acceso al mismo. Internamente se realizan configuraciones en el sistema víctima y estrategias encaminadas a contaminar medios extraibles, con la finalidad de maximizar el potencial de infección.

¿Hay más de una amenaza aplicada ?
Si, tiene amenazas múltiples en distintos frentes de ataque. Recopilan datos mediante medios extraíbles, explotación de servidores vulnerables y la instalación de backdoors.

¿Qué solución o medida recomendarían ?
La implementación de un correcto protocolo de seguridad (que incluya firewall, control de accesos, monitoreo de integridad de archivos y configuraciones, manejo de accesos al sistema de acuerdo a roles y técnicas de aislamiento y modularización del sistema con la finalidad de limitar la superficie de ataque de cada vector) que tome en cuenta los puntos de acceso.

a 3
as Alegria
nda Bueno
a Paola
Rodriguez
y Garzon
cela Ramírez

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

¿Qué tipo de amenaza es? Es un troyano que utiliza backdoors para infiltrarse

¿Cómo comienza y cómo se propaga esta amenaza? Comienza con un instalador, los propósitos principales del insta
son: crear un servicio que garantiza la persistencia de un Loader del Backdoor, y almacenar la configuración predeterm
del Backdoor embebida en el registro.

¿Hay más de una amenaza plicada?sí, hay más de una amenaza y Vyveva es otra herramienta más del extenso arsen

posee el grupo APT Lazarus.

¿Qué solución o medida recomendarían ? Desconectar la red para que el backdoors no entre en contacto y corremos

antivirus para realizar una limpieza o virus.

Solución:

• No descargar ningún archivo adjunto y analizarlo previamente con el antivirus.

• Mantener un protocolo de actualizaciones estricto de sistemas operativos, antivirus y todas las aplicaciones que se ejecutan en ellos.

• Mantener una conexión a internet lo más segura posible, utilizando siempre un firewall.

Mesa 4

Nota : <Kobalos: amenaza para Linux que afecta a infraestructuras informáticas de alto rendimiento | WeLiveSecurity>

¿Qué tipo de amenaza es? Es un backdoor genérico denominado Kobalos.

¿Cómo comienza y cómo se propaga esta amenaza?

Kobalos está embebido en el ejecutable del servidor OpenSSH (sshd) y activará el código del backdoor si la conexión proviene de un puerto de origen TCP específico. Hay otras variantes independientes que no están embebidas en sshd. Estas variantes o se conectan a un servidor C&C que actuará como intermediario o esperan una conexión entrante en un puerto TCP determinado.

¿Hay más de una amenaza aplicada ?

Los expertos en seguridad informan que si bien la puerta trasera multiplataforma funciona en Linux, FreeBSD y Solaris, también hay artefactos que indican que pueden existir variantes de este malware para AIX e incluso para Windows.

¿Qué solución o medida recomendarían ?

conectarse a servidores SSH y configurar antes el doble factor de autenticación (2FA)

Mesa 5

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

¿Qué tipo de amenaza es?

Malware / troyano

¿Cómo comienza y cómo se propaga esta amenaza?

La amenaza comienza cuando se publican dos sitios web que aseguran distribuir una versión oficial del navegador TOR, esta comienza a ser propagada cuando visitantes de la dark net acceden para descargar dicha versión del navegador convencidos que es un sitio oficial. Ingresan a través de un banner que les figura en algunos sitios.

¿Hay más de una amenaza aplicada ?

La amenaza es el robo de monedas digitales de los que utilizan la darknet

¿Qué solución o medida recomendarían ?

Software especializado en detectar malware y eliminar virus. Antimalware: para una solución más genérica, es un software que puede detectar y eliminar varios tipos de malware.

Mesa 6

Nota : https://www.welivesecurity.com/la-es/2019/08/23/ataque-departamentos-financieros-balcanes-utiliza-backdoor-rat/
¿Qué tipo de amenaza es? -
BalkanDoor - RootKit
BalkanRAT - Troyano
¿Cómo comienza y cómo se propaga esta amenaza?
BalkanDoor - El dropper inicial desempaqueta todos los componentes, abre un PDF señuelo (en algunos casos) y ejecuta un script de instalación por lotes que asegura la persistencia del backdoor.
BalkanRAT - Su objetivo es utilizar una copia de Remote Utilities para el acceso remoto a una computadora o para la administración remota. Utiliza varias herramientas de instalación que ignoran el problema e instalan vulnerabilidades tanto 32 bits como en 64 bits. Usa comandos para ignorar los filtros del Firewall e instala en rootkit para el acceso.

¿Hay más de una amenaza aplicada ?
Si, BalkanRAT utiliza tanto el acceso remoto, como la vulneración de archivos y fuera de eso utiliza el RootKit para simular permisos de superusuario. Tiene la capacidad de ocultarse, con lo cual le da la categoría de “Spyware”.

¿Qué solución o medida recomendarían ?

Instalar un antivirus que bloquee el acceso no autorizado, como también la identificación de la amenaza.

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? Ransomware

¿Cómo comienza y cómo se propaga esta amenaza? Hubo una actualización con permisos de administrador que afectó los MSP y estos a su vez infectaron los sistemas de sus clientes con la amenaza.

¿Hay más de una amenaza aplicada ? No

¿Qué solución o medida recomendarían ? Apagar los equipos o aislarlos de la red hasta que...

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? Ransomware

¿Cómo comienza y cómo se propaga esta amenaza? Restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción. Se propaga a través del correo electrónico con suplantación de identidad, en el cual se utiliza software de explotación como Fiesta o Magnitud para tomar el control del sistema, cifrar archivos y así pedir el pago del rescate del computador.

¿Hay más de una amenaza aplicada ? No.

¿Qué solución o medida recomendarían ?

PASO 1: Aísle de inmediato los dispositivos infectados

PASO 2: Identifique el tipo de ataque de ransomware

PASO 3: Elimine el malware ransomware

PASO 4: Recupere los archivos cifrados

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? Se propaga mayormente por mail con un link hacia la página web del servicio de netflix.

¿Hay más de una amenaza aplicada ? No hay más amenazas aplicadas.

¿Qué solución o medida recomendarían ? Denunciar y asegurarse que el dominio pertenezca a la empresa que supuestamente envía el email.

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 ?