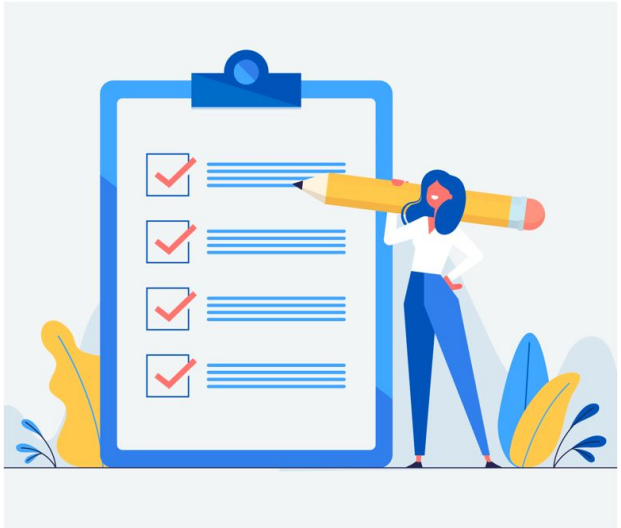
Actividad Tipos de Amenazas

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?

- Ransomware: por nombre Ryuk es el encargado de encriptar todos los datos

hace imposible la restauración del sistema.

¿Cómo comienza y cómo se propaga esta amenaza?

- Ryuk necesita ayuda de otros virus para iniciar Emotet y trickbot y tiempo para contaminar la red.
- Se propaga a través del correo electrónico con suplantación de identidad
- **Trickbot**, que se encarga de los ataques laterales, entre otros, el robo de las credenciales de inicio de sesión

¿Hay más de una amenaza aplicada ?

- Emotec: Ataque de phishing
- Trickbot: que se encarga de los ataques laterales. Como el robo de credenciales.

¿Qué solución o medida recomendarían ?

- Actualizar frecuentemente el SO.
- Respaldar la información con regularidad.

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?

Es un backdoor personalizado llamado Turian (virus troyano bastante difícil de detectar) que deriva del backdoor Quarian, funciona en el segundo plano del sistema y se esconde del usuario. Proporciona al atacante un acceso remoto al PC comprometido no autorizado y explota las vulnerabilidades del sistema para espiar al usuario, administrar sus archivos, instalar programas adicionales o peligrosas amenazas, controlar el sistema del PC al completo y atacar a otros anfitriones.

Mesa 2

¿Cómo comienza y cómo se propaga esta amenaza?

Los backdoors no son capaces de propagarse a sí mismos e infectar sistemas sin el conocimiento del usuario. La mayoría de estos parásitos deben ser manualmente instalados en paquetes junto a otros programas. Hay cuatro modos principales usados por estas amenazas para entrar en el sistema.

- Los usuarios de PC menos atentos pueden instalarlos accidentalmente en sus ordenadores.
- Los backdoors son a menudo instalados por otros parásitos, como virus, e introyanos cluso spywares
- Incluso los programas legítimos pueden tener características de acceso remoto indocumentadas.
- Algunos backdoors infectan el ordenador explotando ciertas vulnerabilidades de programas. Funcionan de manera similar a gusanos y se difunden automáticamente sin el conocimiento del usuario.

MESA 2

¿Hay más de una amenaza aplicada ?

- Los backdoors son a menudo instalados por otros parásitos, como virus, e incluso troyanos y spywares. De este modo en los ataques con backdoor, es posible, encontrar más de una amenaza, teniendo en cuenta que además, tienen la capacidad de propagarse por el sistema del mismo modo que lo hacen los virus de tipo gusano y pueden ser usados para futuros ataques gracias a su baja detectabilidad.

¿Qué solución o medida recomendarían ?

- **Los antivirus cuentan con el software necesario para rastrear, marcar y eliminar el malware. Este proceso viene explicado paso a paso por el propio antivirus.**

Mesa 3

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

¿Qué tipo de amenaza es?

Malware / Troyano

¿Cómo comienza y cómo se propaga esta amenaza?

El backdoor presenta capacidades para exfiltrar archivos, modificar la fecha de estos (timestomping), recopilar información sobre la computadora de la víctima y sus unidades, y otras funciones comunes de backdoor, como ejecutar código arbitrario especificado por los operadores del malware. Esto indica que lo más probable es que el objetivo de esta operación haya sido realizar tareas de espionaje.

Mesa 3

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

¿Hay más de una amenaza aplicada ?

Principalmente la amenaza está en los comandos que se activan con los cuales se modifican los archivos, y la posibilidad de espionaje en el computador infectado.

¿Qué solución o medida recomendarían ?

A pesar del malware avanzado que usan los piratas informáticos de Lazarus APT, sus ataques aún se pueden mitigar con el uso de un paquete de software anti-malware de buena reputación.

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?

Backdoor

¿Cómo comienza y cómo se propaga esta amenaza?

Kobalos se propaga en las maquinas que usen el cliente SSH. Al usarlo, la máquina comprometida tendrá sus credenciales capturadas. Estas credenciales podrán entonces ser usadas por los atacantes para instalar Kobalos en los nuevos servidores.

Mesa 4

¿Hay más de una amenaza aplicada ?

Kobalos no se dirige exclusivamente a los HPC: se descubrio que un gran ISP asiático, un proveedor de soluciones de seguridad para endpoints de Estados Unidos, así como algunos servidores personales, también fueron comprometidos por esta amenaza.

¿Qué solución o medida recomendarían ?

Desde una perspectiva de red, es posible detectar Kobalos buscando tráfico que no sea SSH en el puerto atribuido a un servidor SSH.

Los productos de ESET detectan el malware Kobalos.

Mesa 5

Nota :

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

¿Qué tipo de amenaza es?

Troyano

¿Cómo comienza y cómo se propaga esta amenaza?

Al hacer clic en el botón “Actualizar el Navegador Tor”, el visitante es redirigido a un segundo sitio web con la posibilidad de descargar un instalador de Windows.

Se propaga utilizando dos sitios web que afirman distribuir la versión oficial del navegador Tor en ruso.

Mesa 5

¿Hay más de una amenaza aplicada ?

Hay más de una amenaza debido a que el troyano lleva implícito un navegador Tor controlado por delincuentes (Spyware).

¿Qué solución o medida recomendarían ?

Paso 1: Descarga e instala un antivirus actualizado. **Paso 2**: Desconectarse de internet.

Mesa 5

Paso 3: Borrar caché y coockies. **Paso 4:** Reinicia la computadora en "Modo a prueba de fallos" **Paso 5:** **d**eshabilites la Restauración de Sistema o el "System Restore". Algunas veces los virus pueden esconder archivos en la Restauración de Sistema . **Paso 6**: haz un escaneo completo de la computadora. **Paso 7**: Si ves que el antivirus tiene problemas para remover un virus tienes que ejecutar MSCONFIG. **Paso 8**: Luego de que todos los virus hayan sido puestos en cuarentena o removidos reinicia la PC, conéctate a internet y ejecuta Windows Update para descargar aquellas actualizaciones que sean recomendadas para tu equipo.

Paso 9: Windows, en su página oficial recomienda que utilicemos una herramienta anti-spyware para proceder a la búsqueda y eliminación del programa espía.

Mesa 6

Nota :

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

¿Qué tipo de amenaza es?

Malware, de tipo troyano.

¿Cómo comienza y cómo se propaga esta amenaza?

Comienza con email (phishing), se registra bajo el nombre de algún servicio y empieza a ejecutar scripts, se conecta a un servidor y solicita comandos.

Mesa 6

Nota :

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

¿Hay más de una amenaza aplicada ?

Si, 2 normalmente una técnica de backdoor y otra de acceso remoto, suelen nombrarlos como BalkanDoor y BalkanRAT

¿Qué solución o medida recomendarían ?

No abrir correos sospechosos, examinar los archivos y enlaces adjuntos, y mantener actualizados los equipos y los sistemas 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? = **Rasomware**

¿Cómo comienza y cómo se propaga esta amenaza? Comienza a través de una actualización de una empresa de IT que daba soporte a muchas otras empresas.

¿Hay más de una amenaza aplicada ? La única amenaza fue la **Rasomware.**

¿Qué solución o medida recomendarían ?

No actualizar los servidores ni equipos, desconectar el equipo o equipos del servidor, utilizar herramienta de analisis que provee la empresa.

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?

Ataques de fuerza bruta a las credenciales del RDP

¿Hay más de una amenaza aplicada ?

No

¿Qué solución o medida recomendarían ?

Que siempre tengan backups actualizados en la nube. (Preventivo)

Generar una intranet (Preventivo)

Tener actualizado el antivirus (Preventivo)

Apagarlos equipos (Reactivos)

Pasar antivirus. (Reactivos)

Mesa 9

Nota : Ver información

¿Qué tipo de amenaza es? **Phishing**

¿Cómo comienza y cómo se propaga esta amenaza?

Comienza con la suplantación de una compañía famosa, en este caso de un servicio que cada vez se vuelve parte de la canasta familiar, se propaga a través de correo electrónico, las personas mal intencionadas tienen acceso a bases de datos con direcciones electrónicas que les permiten iniciar la búsqueda de sus víctimas.

¿Hay más de una amenaza aplicada ?

¿Qué solución o medida recomendarían ?

- El usuario debe validar la procedencia del correo revisando el dominio desde donde llega la información
- Abstenerse de dar clic en los enlaces llamativos
-

Integrantes: LuzMila Camacho, Melina Septur ,Sole Caudana y Andres Lopez

Mesa 10

Nota : Link

¿Qué tipo de amenaza es? Phishing.

¿Cómo comienza y cómo se propaga esta amenaza? Comienza con una serie de preguntas que los usuarios van respondiendo y se propaga compartiendo el contenido entre usuarios.

¿Hay más de una amenaza aplicada ? La amenaza aplicada es contra la identidad del usuario.

¿Qué solución o medida recomendarían ? Verificar dominio, protocolo seguro https , verificar el contenido en la medida en que se pueda, no entrar a entidades bancarias por link , mantener actualizado los browser, etc.

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? → **Business Email Compromise (BEC)**, forma de delito cibernético que utiliza el fraude por correo electrónico para sus ataques.

¿Cómo comienza y cómo se propaga esta amenaza? → Inició a través de un correo electrónico con el que suplantaron la identidad del Director del Club, luego intentaron concretar una negociación de transferencia, la cual fue frustrada por uno de los Bancos.

Mesa 11

Nota :

¿Hay más de una amenaza aplicada ? → No, lo que se menciona en el artículo son otros casos de referencia de ataques cibernéticos donde utilizaron **Ransomware.**

¿Qué solución o medida recomendarían ? → Se recomienda verificar las direcciones de correo electrónico para estar seguros de que provienen de una fuente confiable.

Abstenerse de dar click en imagenes, links (enlaces) o descargar archivos adjuntos a los correos que tienen un emisor desconocido.

Validar e investigar el contenido del correo.

Finalmente si se tienen dudas reportar la dirección de correo como Phishing y bloquear al remitente.