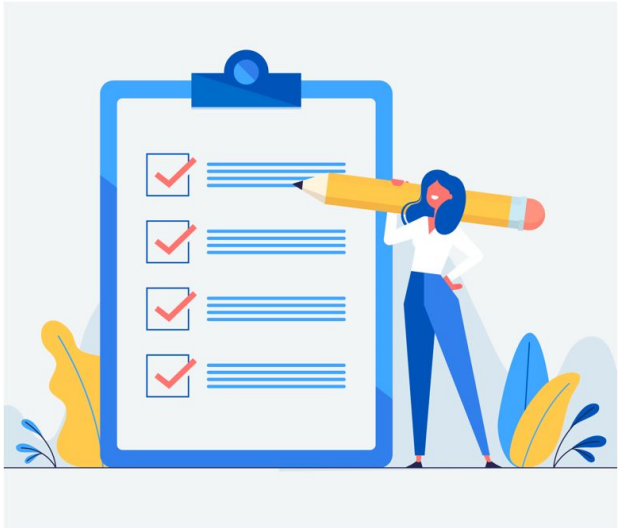
Actividad Tipos de Amenazas

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 (Ryuk).

¿Cómo comienza y cómo se propaga esta amenaza? Vulnerabilidad en la seguridad del sistema.

¿Hay más de una amenaza aplicada? Phishing (Emotec) y Trickbot.

¿Qué solución o medida recomendarían? Respaldos de seguridad y enseñar a los empleados a no caer en phishing.

Mesa 2

Nota :

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

¿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 3

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

¿Qué tipo de amenaza es? R/ Es un Backdoor para realizar tareas de espionaje.

¿Cómo comienza y cómo se propaga esta amenaza?R/ Aunque Vyveva se ha estado utilizando desde al menos diciembre de 2018, aún se desconoce su vector de compromiso inicial. Para propagarse, esta amenaza usa un instalador que primero establece el ID de configuración de infección, que identifica de manera única a cada víctima, en un valor generado aleatoriamente, y luego lo almacena en el registro.

¿Hay más de una amenaza aplicada ?R/

Además del Backdoor también hay un TOR library, un Installer, un Loader y un Dropper.

¿Qué solución o medida recomendarían ?R/

Apartar/desconectar de la red las máquinas en las que se detectó la amenaza, y utilizar antivirus del tipo correspondiente para chequear el estado de las demás.

Mesa 4

Nota : <Poner el link>

¿Qué tipo de amenaza es? .Troyano

¿Cómo comienza y cómo se propaga esta amenaza?

¿Hay más de una amenaza aplicada ?

¿Qué solución o medida recomendarían ?

Mesa 5

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

¿Qué tipo de amenaza es? Troyano.

¿Cómo comienza y cómo se propaga esta amenaza? Haciendo clic en “Actualizar el Navegador Tor” en una página falsa. Promoviendo el sitio en foros.

¿Hay más de una amenaza aplicada ? Sí, es un ransomware y spyware.

¿Qué solución o medida recomendarían ? Ser cuidadoso con las descargas y apps no autorizadas. Evitar páginas peligrosas (verificar la url).

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**

¿Cómo comienza y cómo se propaga esta amenaza?

- **utiliza una campaña relacionado a los impuestos. Con el contenido de los correos relacionados al tema impositivo, incluyendo los enlaces incluidos y los PDF utilizados como señuelo.**

¿Hay más de una amenaza aplicada ?

- **La finalidad de esta amenaza era acceder y apropiarse de la información sensible de las personas que accedieron a los archivos infectados.**

¿Qué solución o medida recomendarían ?

- **Es importante el analizar con un antivirus los archivos de los cuales no tenemos confianza con el fin de buscar software malicioso.**

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? Comienza mediante una infiltración al programa de suministros utilizada por diferentes compañías, en la cual mediante una actualización con permisos de administrador se propagó en todas las compañías.

¿Hay más de una amenaza aplicada ? No, ninguna más solamente el cifrado de los datos

¿Qué solución o medida recomendarían ?

Durante el ataque: desconectarse de la red, no entregar ninguna información, y empezar a restaurar los archivos mediante una copias de seguridad limpias, utilizar firewall y antivirus de buena reputación. Y Mantener un backup de la información constante.

Nota : Mesa 8

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? *Comienza aprovechando —entre otras vías de acceso inicial— las conexiones remotas como el RDP para acceder a los sistemas de las víctimas. El ransomware DarkSide impactó a Colonial Pipeline, la compañía de oleoducto más importante de Estados Unidos, provocando el corte del suministro de nafta, diesel y otros productos refinados para un tramo de aproximadamente 8850 kilómetros que va desde Texas hasta Nueva York.*

¿Hay más de una amenaza aplicada ? *No.*

¿Qué solución o medida recomendarían ? *Pagar el ransom por una cuestión de que el no mover el aceite en este caso podría ser más costoso que el pago de rescate.*

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?

Con la recepción de un correo electrónico, donde se suplanta la identidad del remitente y solicita datos sensibles.

¿Hay más de una amenaza aplicada ? Robo de datos

¿Qué solución o medida recomendarían ?

- Nunca debemos hacer clic en el enlace que se incluye en un mensaje que llega de manera inesperada.
- Verificar su procedencia y comprobar que sea de un sitio oficial.
- Modificar sus credenciales de acceso en el sitio en caso de haber sido víctima del engaño.
- En caso de haber ingresado datos de tarjetas de crédito o débito comunicarse con su entidad financiera a la brevedad.

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? Phishing

¿Cómo comienza y cómo se propaga esta amenaza? Phishing es el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito. Las víctimas reciben un mensaje de correo electrónico o un mensaje de texto que imita a una persona u organización de confianza, como un compañero de trabajo, un banco o una oficina gubernamental.

¿Hay más de una amenaza aplicada ? No

¿Qué solución o medida recomendarían ?

- No abra correos electrónicos de remitentes que no le sean familiares.

-No haga clic en un enlace dentro de un correo electrónico a menos que sepa exactamente a dónde le lleva.

-Para aplicar esa capa de protección, si recibe un correo electrónico de una fuente de que la que no está seguro, navegue manualmente hasta el enlace proporcionado escribiendo la dirección legítima del sitio web en la dirección legítima del sitio web en su navegador.

-Busque el certificado digital del sitio web.

-Si se le pide que proporcione información confidencial, compruebe que la URL de la página comienza con “HTTPS” en lugar de simplemente “HTTP”. La “S” significa “seguro”. No es una garantía de que un sitio sea legítimo, pero la mayoría de los sitios legítimos

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 ?