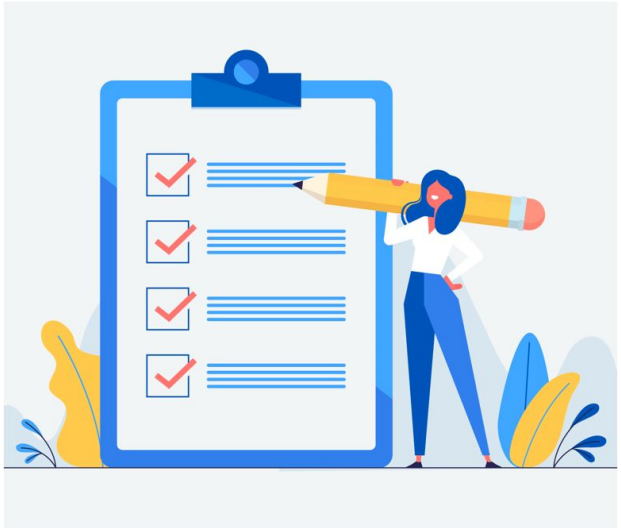
Actividad Tipos de Amenazas

Utilizando este documento de presentación, cada mesa deberá resolver y completar en cada hoja , que le corresponde según su número de mesa.



Mesa 1 Gabriela Esparza, Eugenia Guatelli, Rodrigo Heluani, Daniel Delgado, Constanza Sauan, Carolina Pérez

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

¿Qué tipo de amenaza es?

Ryuk es un ransomware

¿Cómo comienza y cómo se propaga esta amenaza?

Ryuk llevaba oculto meses antes de ejecutarse, depende de otro tipos de virus que pudo haber ingresado por phishing en este caso EMOTEC, un troyano. Luego activa Trickbot, que se encarga de ataques laterales y robo de credenciales de inicio de sesión, por último Ryuk se encarga de encriptar

¿Hay más de una amenaza aplicada ?

Si ya que fueron infectados por 3 amenazas en total

¿Qué solución o medida recomendarían ?

Como medida preventiva, tener backups de sistema actualizados y capacitación al personal sobre los peligros del phishing, practicas de cifrado y encriptación de datos sensibles

Como medida reactiva, formateo total del sistema.

Mesa 2 Mariela Vallejos, Agustina Parker, Ailen Adid,Rodrigo Ravina, Felipe Beltrán, Tomás Correa

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

¿Qué tipo de amenaza es?
Troyano - (Backdoor)

¿Cómo comienza y cómo se propaga esta amenaza?
Ingresan a través de un archivo infectados ejecutables.

¿Hay más de una amenaza aplicada ?
Sí, ataca OS, los extraíbles y las herramientas de acceso remoto.

¿Qué solución o medida recomendarían ?
Desconectarse de la red, revocar todas las credenciales, entrenar al personal en seguridad informática. Llevar las unidades de disco a otras pc para ser revisadas, sin conectarse a la red. Otra opción seria formatear los servidores y reiniciar con un backup que haya estado offline antes del ataque.

Mesa 3

Nota:

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

Agustin Damelio, Tomas Montivero, Belen Wurch, Augusto Landra, Magaly Catanzariti

Nota :

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

¿Qué tipo de amenaza es? Malware, específicamente un backdoor genérico

¿Cómo comienza y cómo se propaga esta amenaza? El método que más hemos visto es en el cual 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 más de una amenaza aplicada ? Kobaloes está contenida en una sola función.

¿Qué solución o medida recomendarían ? Tenés que utilizar un antivirus actualizado y potente, como ESET que lo detectaron

Mesa 5

Nota :

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

¿Qué tipo de amenaza es? **Es un adware**

¿Cómo comienza y cómo se propaga esta amenaza? **Comienza con un troyano, que se instala un programa y se propaga a través de anuncios**

¿Hay más de una amenaza aplicada ? **Si, el botnets ya que realizan crímenes digitales con el robo de bitcoins**

¿Qué solución o medida recomendarían ? **Formatear la maquina, antivirus adecuado. Proteger la identidad con detección de intrusos, realizar actualizaciones periódicas, y no abrir links dudosos.**

Mesa 6

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 7

Nota : Link

¿Qué tipo de amenaza es? Es un Ransomware (REvil)

¿Cómo comienza y cómo se propaga esta amenaza? A través de un ataque de cadena de suministro, que consiste en comprometer proveedores digitales de servicios externos (en este caso, un software de gestión de IT de la compañía Kaseya) como instrumento para infiltrarse desde allí en una organización objetivo.

¿Hay más de una amenaza aplicada ? No.

¿Qué solución o medida recomendarían? Delimitar los permisos del software instalado, política de backups, virtualización (las máquinas virtuales son “descartables”), delimitar los permisos de red.

Mesa 8

José Emanuel Nieva Toppa, Maria Lourdes Martinez, Gastón Odetti Di Fiori, Candela Vidal, Nicolas Peretti, Gaston Demergasso

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? **Ramsomware DarkSide**

¿Cómo comienza y cómo se propaga esta amenaza? **Se atacó a la compañía mediante ataques de fuerza bruta a las credenciales del RDP, provocando el corte del suministro de nafta, diesel y otros productos refinados.**

¿Hay más de una amenaza aplicada? **NO**

¿Qué solución o medida recomendarían? **Parches de seguridad, detección de intrusos, Control de acceso y Encriptación. Y luego implementar auditorías para prevenir nuevamente este tipo de problemas.**

Mesa 9

Sofía Lancuba, Ximena Vasco, Julieta Gonzalez

Link: 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? Comienza normalmente con un correo electrónico el cual está diseñado para parecer que es Confiable y apelan a la inmediatez de la acción.

¿Hay más de una amenaza aplicada ? si, el robo de la identidad ya que al ingresar al link aparece un formulario donde te piden los datos de tarjeta.

¿Qué solución o medida recomendarían ? Ante la más mínima duda sobre la legitimidad de un correo, nunca debemos hacer click en el enlace que se incluye en un mensaje que llega de manera inesperada. Sobre todo, sin antes verificar su procedencia y comprobar que sea de un sitio oficial.

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? **Se trata de un Troyano**

¿Cómo comienza y cómo se propaga esta amenaza? **Comienza cuando el usuario completa sus datos y se propaga cuando este lo reenvia a sus contactos**

¿Hay más de una amenaza aplicada ? **Vishing - Keylogger**

¿Qué solución o medida recomendarían?

- **Instalar un antivirus y un firewall y mantenlos actualizados.**
- **Mantener actualizados tanto software como hardware, para evitar quedar expuesto por vulnerabilidades conocidas.**
- **No pulses en enlaces de descarga o archivos que te lleguen a través de emails sospechosos o en redes sociales.**
- **Si descargas a través de páginas de poca confianza o sistemas P2P, antes de ejecutar el programa o abrir el archivo, pásale el escáner con el antivirus.**
- **Si descargas programas o archivos gratuitos, hazlo siempre desde fuentes de confianza, preferiblemente, desde webs oficiales.**

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 ?