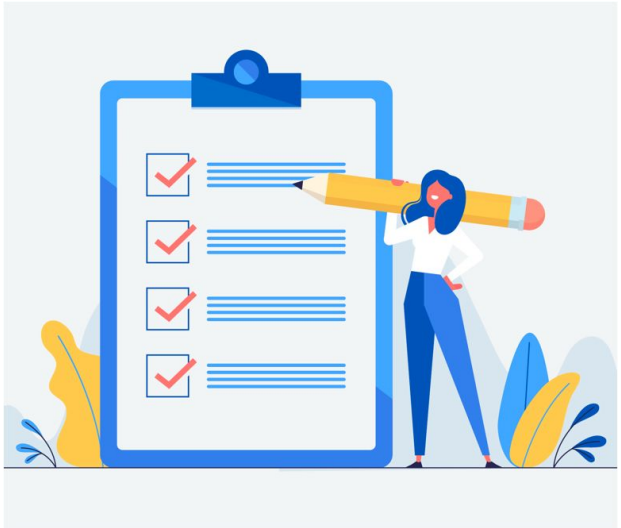
# Actividad Tipos de Amenazas

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? -Empezó con un ataque de phishing basado en **Emotec**, un troyano que cambia su código cada poco tiempo a fin de no ser detectado y que tiene la capacidad de interceptar, registrar, y guardar todo el tráfico de red, luego uso **Trickbot** que se encarga del robo de las credenciales de inicio de sesión, y para finalizar usó el Ransomware **Ryuk** para encriptar los datos.

¿Hay más de una amenaza aplicada ? -Si, ya que el virus para poder acceder al sistema, tuvo que hacer uso de Emotec y trickbot.

¿Qué solución o medida recomendarían ? -Una medida puede ser tener un sistema de backup que es una copia que se realiza frecuentemente a los datos.

# Mesa 2

Nota : <Backdoor Diplomacy: actualizando de Quarian a Turian, un backdoor utilizado contra organizaciones diplomáticas | WeLiveSecurity>

**¿Qué tipo de amenaza es?** Es una amenaza DLL search order hijacking.

**¿Cómo comienza y cómo se propaga esta amenaza?** Como vectores de infección inicial, el grupo ha estado aprovechando la explotación de dispositivos vulnerables expuestos a Internet, como servidores web e interfaces de gestión para equipos de red. Una vez dentro de un sistema, sus operadores utilizan herramientas de código abierto para escanear el entorno y realizar movimiento lateral

**¿Hay más de una amenaza aplicada ?** En este caso si, se realizó a través de un backdoor personalizado que llamamos Turian que deriva del backdoor Quarian.

**¿Qué solución o medida recomendarían ?** Tener un buen antivirus que ofrezca protección en tiempo real, tenerlo actualizado con regularidad, no ingresar a páginas sospechosas. La eliminación manual del backdoor no es fácil, lo mejor es recurrir a una herramienta para su eliminación automática; los antivirus cuentan con esta opción, cuando encuentran un virus lo marcan eliminarlo.

# Mesa 3

Nota :

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

¿Qué tipo de amenaza es?  Spyware

¿Cómo comienza y cómo se propaga esta amenaza?ha sido desplegado en ataques dirigidos, ya que solo encontramos dos máquinas víctimas, ambas son servidores propiedad de una empresa de logística de carga ubicada en Sudáfrica

¿Hay más de una amenaza aplicada ? Total control de la información

¿Qué solución o medida recomendarían ? Lo recomendable seria hacer backup cronologicamente y proteger el dispositivo con un antivirus

# Mesa 4

**integrantes:** Shirrly Mejia, Maye Avendaño, Ana Maria Galaza, Jeronimo Botero, Tomás Gonzales.

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

**¿Qué tipo de amenaza es?**
Kobalos es un backdoor genérico en el sentido de que contiene muchos comandos que no revelan la intención de los atacantes. En resumen, Kobalos garantiza el acceso remoto al sistema de archivos, brinda la capacidad de generar sesiones de terminal y permite establecer conexiones de proxy con otros servidores infectados por Kobalos.

**¿Cómo comienza y cómo se propaga esta amenaza?**
Comienza para robar credenciales en supercomputadoras y servidores de redes académicas y de investigación con sistema operativo Linux

**¿Hay más de una amenaza aplicada ?**
En la mayoría de los sistemas comprometidos por Kobalos, el cliente SSH está comprometido para robar credenciales. Este ladrón de credenciales no se parece a ninguno de los clientes OpenSSH maliciosos que hemos visto anteriormente, y hemos examinado decenas de ellos en los últimos ocho años.

**¿Qué solución o medida recomendarían ?**
Conectarse a servidores SSH configurar antes el doble factor de autenticación (2FA). Kobalos es otro caso en el que el 2FA podría haber mitigado la amenaza, ya que el uso de credenciales robadas parece ser una de las formas en que se puede propagar a diferentes sistemas.

# Mesa 5

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

https://docs.google.com/document/d/1rvR2UpxFAzJm8sFl09AFYzB_HRxrurD3l8T2tZl2HS0/edit

¿Qué tipo de amenaza es?

Troyano

¿Cómo comienza y cómo se propaga esta amenaza?

El sitio decía que distribuía una versión oficial de Tor pero era una versión modificada, cuando el usuario lo abre pide actualizar y descarga un instalador adicional. Esta versión tiene deshabilitada una comprobación de firma digital para los complementos instalados para el Navegador Tor. Por lo tanto, los atacantes pueden modificar cualquier complemento y el navegador lo cargará sin alertar acerca del fallo en la verificación de firma digital.

¿Hay más de una amenaza aplicada ?

Desde nuestro punto de vista no, solo es un troyano donde aplicaron varias técnicas como Execution, Persistence, Collection, Command and Control, Impact.

¿Qué solución o medida recomendarían ?

Cuando se quiera descargar el navegador Tor en este caso, o para otros, siempre se debe verificar que el sitio sea el oficial, con esto evitamos que los ciberdelincuentes ataquen nuestros equipos, de igual manera contar con un buen antivirus para proteger nuestro equipo y datos.

# Mesa 6

Nota : Ataque a departamentos financieros en los Balcanes utiliza un backdoor y un RAT | WeLiveSecurity

**¿Qué tipo de amenaza es?**backdoor y un troyano.

**¿Cómo comienza y cómo se propaga esta amenaza?** correos electrónicos maliciosos.

**¿Hay más de una amenaza aplicada ?**Sí, BalkanDoor qué es un backdoor simple, y BalkanRAT qué es un troyano con distintas herramientas como keyloggers, script AutoHotKey

**¿Qué solución o medida recomendarían ?** 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. Ante una infección se recomienda usar software anti malware y él formateo del computador.

# Mesa 7

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

Link Doc. Google:

¿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 8

Nota :

https://docs.google.com/document/d/1yj0jk_bgUyNIv5Rh27zMYRIAn9c8JpnLbMYms7lm5vY/edit?usp=sharing

¿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 9

Nota :

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

## ¿Qué tipo de amenaza es?

Es una suplantación de identidad (phishing), ya que, se hacen pasar por Netflix para robar los datos de las tarjetas de créditos.

## ¿Cómo comienza y cómo se propaga esta amenaza?

Comienza con la llegada de un correo electrónico, informando que tiene pagos atrasados en Netflix, posteriormente el usuario abona el pago y le roban los datos de la tarjeta.

## ¿Hay más de una amenaza aplicada ?

No, solamente es phishing.

## ¿Qué solución o medida recomendarían ?

Verificar que el mail sea válido, comprobando 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?

Adware, ya que es un tipo de virus de publicidad

¿Cómo comienza y cómo se propaga esta amenaza?

Empieza por un mensaje que se envía masivamente por whatssapp y se propaga masivamente a los que lo reciben

¿Hay más de una amenaza aplicada ?

Unicamente Robo de información

# 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 ?