# Actividad Tipos de Amenazas Cartoons

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 que actúa en conjunto con otros dos virus.**

¿Cómo comienza y cómo se propaga esta amenaza?

**Softwares de secuestro usados para atacar empresas para secuestrar información de sus servicios y luego pedir rescate. Se pueden encontrar en archivos adjuntos de correos electrónicos no deseados o al hacer clic en vínculos que aseguran venir de bancos, o instituciones legales. Encripta la información que tenemos y no queda legible, sale un cartel que nos pide dinero para chantajearnos.**

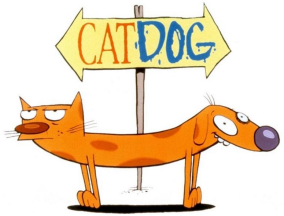
¿Hay más de una amenaza aplicada ?

**Este ransomware particular que es el Ryuk, trabaja en asociación con otros dos virus, uno es el Emotec y el Trickbot. Mientras que uno se encarga de registrar el tráfico de la red, el otro se encarga de robar las credenciales de inicio de sesión. Finalmente, Ryuk se encarga de encriptar todos los datos y los recursos de la red.**

¿Qué solución o medida recomendarían ?

- **PREVENCIÓN: con backups diarios y puntos de restauración del sistema. Se recomienda no pagar. Filtro antispam. Muchos de los ataques por Ransomware se distribuyen a través de campañas masivas de correo electrónico. Máquinas virtuales. Emplear máquinas virtuales para aislar el sistema principal es otra técnica efectiva. En un entorno virtualizado la acción de los ransomware no suele materializarse.**

# 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 virus que da acceso a usuarios maliciosos al control del equipo infectado y dispositivos externos que estén conectados al mismo.

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

Comienza aprovechando la explotación de dispositivos vulnerables expuestas a Internet como servidores web e interfaces de gestión para equipos de red, con el fin de dropear y ejecutar un webshell. A través de este, utiliza software de código abierto para el reconocimiento y la recopilación de información, y hace uso de la técnica DLL search order hijacking para instalar su backdoor: Turian. Finalmente, emplea de manera separada un ejecutable para detectar medios extraíbles, y así recopilar y exfiltrar sus datos en la papelera de reciclaje de la unidad principal.

**¿Hay más de una amenaza aplicada ?**

Podría llegar a afectar alguna otra amenaza si el usuario malicioso  lo decide,ya que tiene el control.

**¿Qué solución o medida recomendarían ?**

Es recomendable instalar algún antivirus el cual se encargará de detectar el software malicioso y posterior a esto a eliminarlo. También es recomendable realizar copias de seguridad constantemente ya que al eliminar el software malicioso se puede seguir trabajando con la información contenida en las copias de seguridad sin ningún problema.También es importante tener cuidado con los programas que se instalan en el equipo, que los mismos sean seguros.

# Mesa 3

Nota : Cuidado con Vyveva, el nuevo backdoor del grupo Lazarus | WeLiveSecurity

**¿Qué tipo de amenaza es?**

Es un Troyano backdoor, un tipo de virus diseñado para dar acceso a usuarios maliciosos al control de un equipo infectado de manera remota.

**¿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 más de una amenaza aplicada ?**

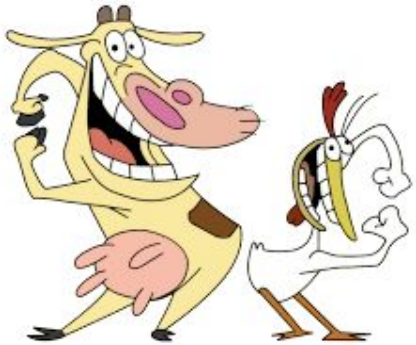
Al tener el control del equipo podría llegar a afectar con algún otro malware.

**¿Qué solución o medida recomendarían ?**

La eliminación manual de un backdoor no es fácil y, de hecho, lo mejor es recurrir a una herramienta para su eliminación automática; los antivirus cuentan con esta opción, de manera que cuando encuentran un virus lo marcan para su posterior eliminación

También es recomendable realizar copias de seguridad constantemente para que cuando sea eliminado el malware se puedan recuperar los documentos afectados

# 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?

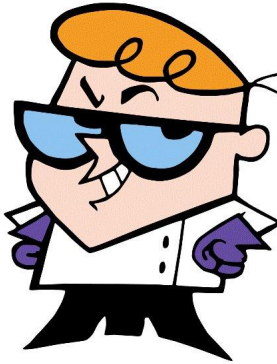
Malware Kobalos - Tipo Troyano Backdoor

¿Cómo comienza y cómo se propaga esta amenaza?

¿Hay más de una amenaza aplicada ?

¿Qué solución o medida recomendarían ?

# 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 troyano - malware

¿Cómo comienza y cómo se propaga esta amenaza? Se creó una versión de Tor troyanizado y se abrieron sitios web con dominio casi idéntico al oficial ofreciendo la descarga haciéndole creer al usuario que estaba descargandolo desde la página de TOR, se promocionan esos sitios falsos haciendo spam en diferentes foros buscando posicionarlo en las búsquedas de google y lograr así que los usuarios entren.

¿Hay más de una amenaza aplicada ? El troyano fue diseñado para robar monedas digitales de aquellos que visitan mercados de la darknet.

¿Qué solución o medida recomendarían ? Instalar un antivirus y realizar análisis periódicos del sistema.

Contar con un antivirus actualizado y un firewall: • El antivirus avisará si se ha descargado un archivo que incluye un virus troyano y los eliminará en caso de que el dispositivo esté infectado. • El firewall evitará que los troyanos puedan transmitir información desde el ordenador o recibir órdenes, si se llega a infectar.

# Mesa 6

Nota: https://www.welivesecurity.com/la-es/2019/08/23/ataque-departamentos-financieros-balcanes-utiliza-bac

## ¿Qué tipo de amenaza es? Backdoor y troyano de puerta trasera (RAT)

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

La amenaza se propaga a través de correos electrónicos maliciosos "malspam". Han sido organizados previam
considera que se trata de una única campaña a largo plazo que se extiende a largo plazo por paises como Cro
Montenegro, Bosnia y Herzegovina.
El archivo ejecutable es un WinRAR auto extraíble cuyo nombre e icono son modificados para parecerse a un archivo PDF y así engañar al usuario. Una vez que se ejecuta, está configurado para desempaquetar su contenido, abrir el PDF utilizado como señuelo para evitar cualquier sospecha y ejecutar silenciosamente BalkanRAT o BalkanDoor.
BalkanDoor se ejecuta como un servicio de Windows, permitiéndole desbloquear la pantalla sin necesidad de iniciar sesión. En el caso de BalkanRat utiliza un software de escritorio remoto legitimo y utiliza herramientas adicionales y scripts para ocultar su presencia a la victima.

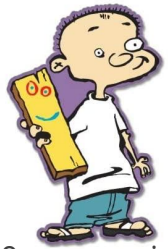
## ¿Hay más de una amenaza aplicada ?

Si profe Roberto, una amenaza trabaja por interfaz gráfica (balkanrat) y la otra amenaza trabaja a través de comandos (balkandoor)

## ¿Qué solución o medida recomendarían ?

Deben seguir las reglas básicas de ciberseguridad: 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.

# 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 para cifrar la información.

**¿Cómo comienza y cómo se propaga esta amenaza?**
Por medio de un instalador de una actualización automática de un software muy usado, seguido de una propagación a máquinas de clientes

**¿Hay más de una amenaza aplicada ?**
Se evidencia la existencia de un virus Gusano por la facilidad de poder moverse entre servidores e infectar los mismos.

**¿Qué solución o medida recomendarían** ?

A. Realizar backups de datos importantes y de manera regular, alojando la info en un medio externo para no tener que pagar por un rescate.
B. Una vez infectado el equipo aislarlo de la red o apagarlo para evitar extender la amenaza.
C. Mantener buenas políticas de seguridad a nivel empresarial.
D. Uso de Máquinas virtuales para aislar el sistema principal.Actualización constante del SO con los últimos parches de seguridad.
E. Un cortafuegos bien configurado e instalar una solución antimalware o obtener algún tipo de herramienta Anti Ransomware.

# Mesa 8

Nota :

https://www.welivesecurity.com/la-es/2021/05/11/ataque-ransomware-compania-oleoducto-c

line-afecta-suministro-combustible-estados-unidos/

¿Qué tipo de amenaza es?  virus ransomware

¿Cómo comienza y cómo se propaga esta amenaza? comienza con la descarga de un archivo malicioso enviado el correo electrónico, el cual secuestra la información y los atacantes cobran un valor por el rescate.

¿Hay más de una amenaza aplicada ? No

¿Qué solución o medida recomendarían ? Capacitación del personal para prevenir descargas o aperturas de correos maliciosos.

# Mesa 9

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

¿Qué tipo de amenaza es?

Se trata de la amenaza phishing

¿Cómo comienza y cómo se propaga esta amenaza?

Comienza con el envío de un mail a tu correo electrónico, suplantando la identidad de una empresa conocida y pidiendo que reingrese información bancaria.

¿Hay más de una amenaza aplicada ?

No, sólo el robo de datos personales sensibles y privados.

¿Qué solución o medida recomendarían ?

Capacitación para no caer en este tipo de estafas.

Chequear que las páginas a las que accedemos sean las certificadas y sean seguras.

# 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?

Se inicia a través de mensajes de WhatsApp, y a su vez se replica a través de las propias víctimas, indicándoles el reenvío del mensaje.

¿Hay más de una amenaza aplicada ?

En principio no, solamente se ponen en riesgo los datos personales a través de la plataforma que se le hace llegar al usuario.

¿Qué solución o medida recomendarían ?

En primer lugar, y como sugiere el mismo artículo, googlear para buscar mayor información de la amenaza o bien del mensaje recibido. En general suelen aparecer resultados en la búsqueda con denuncias o quejas de usuarios que nos permiten mantenernos a salvo del phishing.

# 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 ?