

# 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 : <[Ryuk: el ransomware que atacó al Ministerio de Trabajo \(revistabyte.es\)](https://revistabyte.es/ryuk-el-ransomware-que-ataco-al-ministerio-de-trabajo/)>

¿Qué tipo de amenaza es?

Ransomware Restringen el acceso a su sistema y archivos.

¿Cómo comienza y cómo se propaga esta amenaza?

A través de correos de phishing con archivos adjuntos o enlaces. Mediante ataques a conexiones remotas, como el Protocolo de Escritorio Remoto (RDP), aprovechando el uso de contraseñas débiles. También a través de la explotación vulnerabilidades por ejemplo, mediante sitios web comprometidos utilizados para redirigir a sus visitantes a diferentes tipos de exploits—, así como también dispositivos USB, descarga de software pirata, entre otros.

¿Hay más de una amenaza aplicada ?

Su principal característica es que Ryuk no trabaja sólo: necesita la ayuda de otros virus para poder ejecutarse. Normalmente, su primera acción la realiza a través de un ataque de phishing basado en Emotet, un troyano que cambia su código cada poco tiempo a fin de no ser detectado por las soluciones de seguridad y que tiene la capacidad de interceptar, registrar, y guardar todo el tráfico de red.

¿Qué solución o medida recomendarían ?

En primer instancia, recomendaríamos apagar la computadora y desconectarla de la red. Identificar la amenaza, si es posible; utilizar una herramienta específica para recuperar el acceso a los archivos.

Finalmente, antes de pagar el rescate, recomendamos recuperar la información a través de un backup -que siempre se debe tener debido a la importancia de la información- y por otro lado recomendamos al Ministerio de Trabajo presupuesto en ciberseguridad.

# Mesa 2

Nota : [Este es nuestro enlace](#)

¿Qué tipo de amenaza es? Es una amenaza tipo Backdoor (puerta trasera)

¿Cómo comienza y cómo se propaga esta amenaza?

dar acceso a usuarios maliciosos al control de un equipo infectado de manera remota.

Estas “puertas traseras” permiten al usuario malicioso controlar el equipo infectado,

pudiendo env

iar y recibir archivos, ejecutarlos o eliminarlos, mostrar mensajes, borrar o robar datos,

reiniciar el equipo, etc. Es decir, puede controlar el equipo como si estuviese sentado

delante de él y a los mandos.

# Mesa 3

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

¿Qué tipo de amenaza es? Troyano

¿Cómo comienza y cómo se propaga esta amenaza? A menudo, los troyanos se propagan a través de un archivo infectado adjunto a un correo electrónico o se esconden tras una descarga de juegos, aplicaciones, películas o tarjetas de felicitación gratuitos. Pueden realizar diferentes tareas, pero, en la mayoría de los casos, crean una puerta trasera que permite la administración remota a un usuario no autorizado y es utilizado para el robo de datos personales.

¿Hay más de una amenaza aplicada?

Los daños o violaciones de privacidad que puede causar este virus es el uso de la webcam sin permiso, borrar el disco, modificar la agenda de contactos, robo de información efectuar llamadas y enviar SMS, hasta geolocalizar al usuario por GPS.

¿Qué solución o medida recomendarían?

Lo mejor es utilizar un antivirus fiable que pueda detectar y eliminar cualquier troyano de su dispositivo.

# 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?

¿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? Spywares

¿Cómo comienza y cómo se propaga esta amenaza?

Comienza una vez que se instala la actualización de la aplicación de Tor. Esto solo afecta a los usuarios de windows.

¿Hay más de una amenaza aplicada ?

¿Qué solución o medida recomendarían ?

# Mesa 6

Nota: <<https://www.welivesecurity.com/la-es/2019/08/23/ataque-departam>>

¿Qué tipo de amenaza es?= Un backdoor y un troyano de acceso remoto (RAT) que se nombran respectivamente, BalkanDoor y BalkanRAT.

¿Cómo comienza y cómo se propaga esta amenaza?= Comienza con una campaña publicitaria y se propaga por medio de correos electrónicos maliciosos.

¿Hay más de una amenaza aplicada?= BalkanDoor

¿Qué solución o medida recomendarían?

# Mesa 7

Nota: <[Ataque masivo del ransomware REvil comprometió más de 1000 compañías en mundo | WeLiveSecurity](#)>

¿Qué tipo de amenaza es?

Ransomware

Es un malware o código malicioso que tiene como objetivo cifrar los datos de la computadora de la víctima

es un **malware** o código malicioso que tiene como objetivo cifrar los datos de la computadora de la víctima impidiendo el acceso y solicitando un pago de “rescate” generalmente en bitcoins.

¿Cómo comienza y cómo se propaga esta amenaza?

¿Hay más de una amenaza aplicada?



# Mesa 8

Nota : <<https://bit.ly/3oHVkRR>>

¿Qué tipo de amenaza es? Ransomware

DarkSide sustrae información de los sistemas comprometidos antes de cifrar la información y en caso de no querer negociar el pago del rescate extorsiona a sus víctimas con filtrar la información en un sitio específicamente creado para ese fin

¿Cómo comienza y cómo se propaga esta amenaza? vulnerando las conexiones remotas como el RDP para acceder al sistema.

¿Hay más de una amenaza aplicada?

Si bien afecto a varias empresas el modo de operar siempre fue el mismo.

¿Qué solución o medida recomendarían ?

Como medida preventiva, invertir en fortalecer la ciberseguridad de la empresa. Ya afectados por la amenaza, el aislamiento de los equipos afectados de la red, inhabilitación de la red interna, bloqueo de credenciales RDP.

# Mesa 9

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 10

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 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 ?