Grupo 1

● ¿Qué tipo de amenaza es?

El malware de rescate, o ransomware, es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos.

● ¿Cómo comienza y cómo se propaga esta amenaza?

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 Emotec, 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.

● ¿Hay más de una amenaza aplicada?

Una vez que Emotec ha realizado su trabajo, empieza el turno de Trickbot, que se encarga de los ataques laterales, entre otros, el robo de las credenciales de inicio de sesión. Una vez que ambos malware han acabado con su labor, Ryuk es el encargado de encriptar todos los datos. La gravedad de éste radica en su capacidad de infección y es que, no sólo encripta los equipos sino también la práctica totalidad de los recursos de la red. Además es hace imposible la restauración del sistema ya que desabilita esa opción en Windows, por lo que solo mediante el pago a los ciberdelicuentes permitiría la desencriptación de los datos.

● ¿Qué solución o medida recomendarían?

Mantén el sistema operativo actualizado y no uses versiones sin soporte oficial. Abre Windows Update o la Mac App Store e instala todas las actualizaciones de seguridad del sistema. Lo sé, es incómodo que Windows se reinicie cada dos por tres o tarde una eternidad en apagar porque hay una actualización pendiente, pero asegúrate de que todos los parches se descargan solos porque es crucial para que estés protegido contra los ataques

No usar sistemas operativos antiguos: No uses sistemas obsoletos: Windows XP, por ejemplo, no tiene parche de seguridad contra el último ataque de ransomware. Es molesto tener que mantenerse al día, ¡pero Windows XP tiene ya dieciséis años!

Configura una copia de seguridad automática de tus archivos. No es tan fastidioso como crees: solo necesitas un disco duro externo. En Windows 10 ve a Configuración > Actualizaciones y seguridad > Copia de seguridad > “Agregar unidad” y asegúrate de que todas tus carpetas importantes estén seleccionadas para copiarse periódicamente en el disco externo. En Mac, ve a Aplicaciones > Preferencias del sistema > Time Machine > “Seleccionar disco de copia de seguridad” para hacer lo mismo. Estas copias se realizan automáticamente en segundo plano cuando se detectan cambios en tus documentos. También puedes usar la nube: Google Fotos tiene espacio ilimitado para tus imágenes, pero hay opciones de pago como Amazon, iCloud y Dropbox que puedes usar para realizar copias en Internet. más vale prevenir que curar y llorar por lo perdido. otra opción son tener un disco externo USB para copiar los archivos importantes.

No abras enlaces ni archivos sospechosos, especialmente si te llegan por correo electrónico o redes sociales. Cualquiera puede dejar un Word, un PDF o una imagen infectada en tu ordenador, pero lo más probable es que el virus te llegue por correo electrónico. Si no confías en el remitente o no esperabas que esa persona te escribiese, no abras ningún archivo ni enlace. También las páginas web pueden inyectarte malware sin que hagas doble clic sobre ningún archivo. Para luchar contra eso, actualiza siempre el navegador además del sistema.

Desconfía de los archivos .exe y ten cuidado con las extensiones ocultas. Windows como Mac ocultan las extensiones de los archivos conocidos por defecto; entonces, si alguien te manda un archivo llamado “archivo.pdf.exe”, tú solo verás “larchivo.pdf”. Pero cuidado: los .exe son archivos ejecutables que podría instalar un virus en tu PC. En Windows puedes solucionarlo en Configuración > Opciones del explorador > Ver, y desmarcando la opción “Ocultar las extensiones de archivo para tipos de archivo conocidos”. En Mac puedes hacer lo mismo desde Finder > Preferencias > “Ocultar extensiones de nombres de archivo”. Nunca abras un exe de una fuente desconocida o de poca confianza.

Ten el antivirus de Microsoft actualziado y descarga algún programa antimalware reputado. Si estás en Windows, asegúrate de que el antivirus de Windows Defender y el firewall de Windows estén activados y actualizados. También puedes descargar un programa antimalware o antivirus buenos