RANSOMWARE

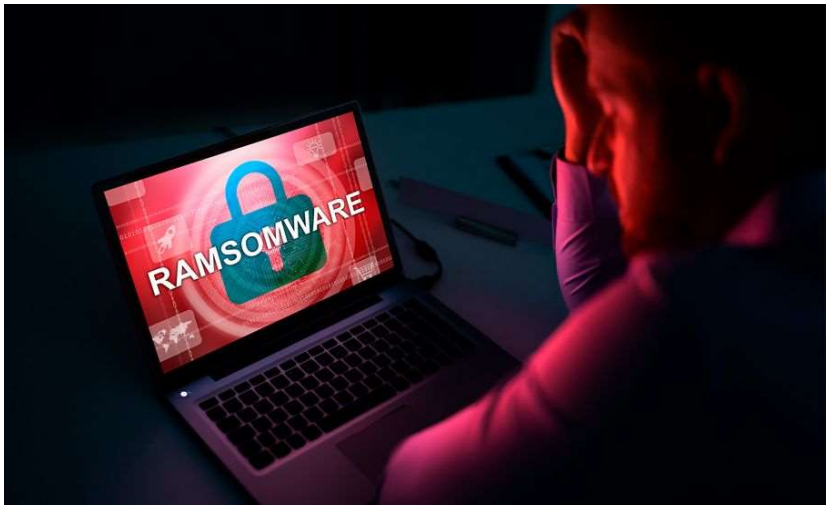

Ilustración asociada a Ransomware
Fuente: https://teuno.com/blogs/soluciones-eficientes-software-anti-ransomware

I. DEFINICIÓN

Ransomware es un malware diseñado para cifrar archivos en el sistema de una víctima, luego el atacante exigir un rescate (un pago) a cambio de la clave de descifrado necesaria para recuperar los archivos.

II. VECTORES DE ATAQUE

Los ciberdelincuentes utilizan varias formas para infectar a las víctimas, entre ellas se tiene:

1. **Explotación de Vulnerabilidades de software:** los atacantes se aprovechan vulnerabilidades existentes en los sistemas operativos, aplicaciones o software de equipo, para instalar el malware.

2. **Ingeniería Social:** Los atacantes usan esta técnica para que las victimas instalen el malware, haciéndoles creer de que están realizando una acción legítima, por ejemplo: actualizar un programa.

3. **Correo Electrónico Malicioso (Phishing):** Los atacantes envían correos electrónicos fraudulentos que parecen ser legítimos, pero en realidad contienen archivos adjuntos o enlaces maliciosos. Si el destinatario hace clic en el enlace o abre el archivo adjunto, el ransomware se ejecuta en su sistema.

4. **Descargas y Sitios Web Comprometidos:** Redireccionamiento a las víctimas a sitios web infectados a fin de que la victima descargue el malware, aprovechando vulnerabilidades del navegador, entre otros.

5. **Redes y Conexiones no Seguras:** Si una red no está protegida, los atacantes pueden propagar ransomware a través de conexiones no seguras. Esto puede ocurrir en redes corporativas o incluso en redes domésticas si no se toman medidas de seguridad.

6. **Dispositivos USB y Otros Dispositivos Extraíbles:** Estos dispositivos pueden ser utilizados para propagar ransomware si se insertan en sistemas sin protección. Los atacantes pueden dejar unidades USB maliciosas en lugares públicos para que las personas las encuentren y las inserten en sus sistemas.

7. **Ataques de Fuerza Bruta:** Los atacantes pueden utilizar ataques de fuerza bruta para lograr acceso remoto al sistema, puede ser ataque al Protocolo de Escritorio Remoto (RDP), y luego ingresar al sistema y ejecutar algún tipo de ransomware.

8. **Descargas de Software No Confiable:** Descargar software pirateado (keygens y crackers de software) o de fuentes no confiables puede exponer a los usuarios, ya que puede incluirse este malware en las descargas.

9. **Por medio de Intermediarios de acceso inicial (IAB)**: Los IAB son grupos criminales que venden acceso ilegítimo a redes corporativas, los IAB usualmente anuncian los accesos robados en los foros de la dark web, donde su precio de venta dependerá del tipo y tamaño de la empresa a la que tengan acceso y del tipo de acceso.

III. MEDIDAS PARA EVITAR SER VÍCTIMA DE RANSOMWARE

1. **Realizar copias de seguridad periódicas:** Realizar copias de seguridad de los datos críticos y guardarlos fuera de línea o en sistemas que no estén conectados a la red. Las copias de seguridad sean accesibles y recuperables en caso de un ataque.

2. **Actualizar y Parchear el Software:** Mantener todo el software actualizado con los últimos parches de seguridad. Los atacantes a menudo explotan vulnerabilidades conocidas en software desactualizado.

   Actualizar el software de todos los equipos a su última versión y parches de seguridad de software como: lectores PDF, software de ofimática como Microsoft Office, compresores y descompresores como WINRAR o WinZip, entre otros.

3. **Educar a los Usuarios:** Capacitar a los empleados en prácticas de seguridad cibernética. Como identificar correos electrónicos de phishing, enlaces maliciosos y archivos adjuntos sospechosos.

4. **Filtrar Correo Electrónico y Web:** Utilizar soluciones de filtrado de correo electrónico y web para bloquear correos electrónicos y sitios web maliciosos conocidos. Esto puede evitar que los correos electrónicos de phishing lleguen a la bandeja de entrada de los usuarios.

5. **Segmentación de red (VLANs):** Dividir la red en segmentos y limita los permisos de acceso para reducir la propagación de

ransomware en caso de una infección. Los sistemas críticos deben estar en segmentos separados, segmentación para servidores de producción, equipos de trabajadores, red de invitados, etc.

6. **Restricción de privilegios:** Limitar los privilegios de los usuarios y las cuentas de servicio para evitar que el ransomware se propague a sistemas críticos. Utiliza el principio de "mínimo privilegio", limitar quién y a que recursos de red se puede acceder.

7. **Monitoreo continuo de red:** Implementar soluciones de monitoreo de seguridad que detecten actividades inusuales o comportamientos de ransomware en tiempo real.

8. **Plan de respuesta a incidentes:** Desarrollar y probar un plan de respuesta a incidentes que incluya pasos específicos frente a un ataque de ransomware. Esto incluye la comunicación, la contención y la restauración de sistemas.

9. **Gestión de vulnerabilidades:** Establecer un proceso de gestión de vulnerabilidades que identifique, evalúe y priorice las vulnerabilidades en tu entorno y aplique parches o medidas de mitigación según corresponda.

10. **Configurar políticas de aseguramiento/hardening:** Para los sistemas operativos de servidores y *endpoints* MS Windows y GNU/Linux; (directorio activo y servidores Windows y GNU/Linux Críticos), se puede descargar la plantilla de aseguramiento desde https://www.cisecurity.org/cis-benchmarks.

11. **Restringir el acceso remoto y a recursos de red:** Restringir el uso de protocolos como: SMB, SSH y RDP a través de Firewall y VPN, esta configuración aplica para servidores y dispositivos de usuario final.

12. **Bloquear el acceso a la red:** No permitir el acceso a la red de usuarios anónimos o sin autenticación a recursos compartidos de la red o de usuarios, el acceso a estas carpetas debe utilizar una autenticación antes de acceder al recurso.

13. **Segmentación de usuarios privilegiados en el directorio activo:** Eliminar usuarios invitados y administradores que no se estén usando, eliminar usuarios sin credenciales y revisar los privilegios de los grupos y usuarios.

14. **Bloquear tráfico malicioso:** De ser posible bloquear conexiones entrantes y salientes hacia destinos atípicos, como: China, Rusia, Romania, Japón, Corea, Irán, Nigeria, Eslovenia, Uganda, Ucrania, Vietnam, entre otros, así como el tráfico que pueda ser considerado malicioso.

15. **Controlar conexiones a Internet:** Bloquear el uso de conexiones o nodos de la red TOR, bloquear conexiones entrantes y salientes hacia dominios como: *.noip.com, *.discordapp.com, *.con-ip.com, *.duckdns.org, *.ngrok.io, *. ngrok.com, *. localxpose.io, *. zrok.io, *. localhost.run, entre otras.

    Estos dominios en sí mismos no son peligrosos, pero los servicios que ofrecen pueden ser utilizados por ciberdelincuentes para ocultar y facilitar actividades maliciosas. Es importante tener precaución y supervisar cualquier actividad sospechosa que involucre estos dominios, especialmente si se realizan en contextos inusuales o no esperados.

16. **Bloquear el uso de PROXYs y VPNs no autorizadas:** Permitir solo el uso de PROXYs y VPNs autorizados, ya que pueden ser utilizados para saltar los filtros de seguridad perimetral.

17. **Instalar soluciones antimalware y mantenerlas actualizadas:** Verificar que la consola antivirus está activada en todos los

endpoints de la infraestructura, si es posible ejecutar un escaneo periódico en todos los endpoints.

18. **Bloquear el uso de Powershell y cmd.exe:** Bloquear estos servicios a usuarios que no los necesitan.

19. **Actualización periódica de firmas se equipos de seguridad perimetral:** Verificar y actualizar de manera periódica la configuración y firmware de los dispositivos de seguridad como *Firewalls* o *Web Application Firewall*, entre otros.

20. **Actualización periódica del software de servicios de compartición de archivos:** Actualizar a los últimos parches de seguridad del fabricante y que estos servicios no cuenten con accesos permisivos a todos los usuarios o accesos externos.

21. **Contraseñas seguras:** Implementar una política de contraseñas seguras para funcionarios y administradores y el cambio frecuente de las mismas (mensual, trimestral o semestral).

22. **Restringir el uso de Macros en documentos:** Si es posible implementar una configuración que bloquee las MACROS de los documentos de Microsoft Office y lectores PDF, así como el uso de JavaScript, y que estos documentos siempre sean vistos en vista protegida cuando provienen de ubicaciones desconocidas.

23. **Controlar el uso de herramientas para compartición en la nube:** El uso de herramientas como SharePoint, GoogleDrive o Dropbox, ya que sin control pueden ayudar a distribuir la infección a otras máquinas, implemente controles de autenticación y acceso.

24. **Actualizar los navegadores web:** Actualizar los navegadores web de los usuarios a su última versión; Google Chrome, Mozilla Firefox, Firefox Developer, Opera, Microsoft Edge. Evitar el uso

de navegadores como Internet Explorer, sin soporte de mantenimiento.

25. **Usar Directivas de configuración:** A través de directivas de configuración de dominio, habilitar en los usuarios finales y servidores del dominio de red, medidas de seguridad como:
    - Filtro Smart Screen
    - Control de cuentas de usuario (User Account Control)
    - Auditoria de eventos
    - Firewall local del sistema operativo

Ninguna medida es infalible, pero combinando estas prácticas, se puede fortalecer la seguridad de una organización contra ataques de ransomware y estar mejor preparado para responder en caso de un incidente.

IV. QUE HACER ANTE UN ATAQUE DE RANSOMWARE

Ante un ataque de ransomware, es fundamental actuar con rapidez y seguir un conjunto de pasos específicos para minimizar el daño y aumentar las posibilidades de recuperación. Algunos pasos a seguir son:

1. **Aislar el Sistema o Red:** Si se detecta actividad de ransomware en una computadora o en la red, aislar inmediatamente el sistema afectado desconectándolo de la red y apagándolo si es necesario. Esto ayudará a evitar que el ransomware se propague a otros sistemas.

2. **Confirmar el Ataque:** Asegurarse de que se trata de un ataque de ransomware. Los ataques de *ransomware* suelen mostrar una nota de rescate en la pantalla de la víctima. Tomar capturas de pantalla o fotografías de la pantalla para documentar la nota de rescate.

3. **No Pagar el Rescate:** No pagar el rescate exigido por los atacantes. No hay garantía de que se obtendrá la clave de

descifrado después de realizar el pago, y pagar solo alienta a los ciberdelincuentes.

4. **Informar del Ataque:** Notificar de inmediato al equipo de seguridad cibernética de la organización o a las autoridades locales. Cuanto antes se informe, mejor será la respuesta y la posibilidad de rastrear a los atacantes.

5. **Restauración desde una Copia de Seguridad:** Si se cuenta con copias de seguridad actualizadas y seguras, utilizar estas copias para restaurar los datos y sistemas afectados. Asegurarse de que las copias de seguridad sean de confianza y no estén comprometidas.

6. **No Borrar Evidencia:** No borrar ningún archivo o evidencia del ataque, hasta que se haya evaluado completamente la situación y se haya informado a las autoridades. La evidencia podría ser útil en la investigación.

7. **Contactar con la autoridad:** De ser víctima, contacte a las Autoridades competentes en base a la Normativa Legal Vigente.

8. **Recopilar Información:** Documentar todos los detalles del ataque, incluyendo la nota de rescate, la dirección de Bitcoin utilizada para el rescate (si está disponible), y cualquier información sobre cómo se propagó el ransomware.

9. **Escanear y Limpiar el Sistema:** Escanear el sistema afectado en busca de malware residual y limpia cualquier instancia del ransomware. Utiliza herramientas de seguridad confiables y actualizadas.

10. **Mejorar la Seguridad:** Identificar las vulnerabilidades o puntos débiles que permitieron que el ransomware infectara el sistema y tomar medidas para mejorar la seguridad, como

parchear software, fortalecer contraseñas y educar a los usuarios sobre la seguridad cibernética.

11. **Mejorar el Plan de Respuesta a Incidentes:** Desarrollar y revisar un plan de respuesta a incidentes que incluya los pasos específicos a seguir en caso de futuros ataques de ransomware.

12. **Monitoreo Continuo:** Implementar un monitoreo de seguridad continuo para detectar actividades inusuales en la red y sistemas que podrían indicar un ataque en curso o intentos de infiltración futuros.

13. **Concienciación de Usuarios:** Educar a los usuarios sobre cómo identificar el ransomware y los peligros del phishing, ya que la mayoría de los ataques de ransomware comienzan con correos electrónicos de phishing.

14. **Buscar información sobre el ransomware:** En el caso de que la organización se vea afectada por un ransomware, se puede visitar paginas especializadas en tratamiento de ransomware, a fin de establecer un panorama de la situación, algunas páginas pueden ser:

    - https://www.nomoreransom.org/es/decryption-tools.html#LockFile (herramientas de desencriptado en el caso de existir)
    - https://id-ransomware.malwarehunterteam.com/ (identificación de tipo de Ransomware y herramienta de desencriptado en el caso de existir)

La prevención es la clave para evitar ataques de ransomware. Considera las recomendaciones del Numeral III, de este documento. La respuesta efectiva a un ataque de ransomware es esencial para minimizar el impacto y recuperarse de manera más rápida y efectiva.

V. DESCARGO DE RESPONSABILIDAD

- La información en el presente documento; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VI. REFERENCIAS:

Administrador. (n.d.). *Ataque de ransomware*. Trend Micro. https://www.trendmicro.com/es_es/what-is/ransomware/ransomware-attack.html

Arroyo, R. (2023). Initial Access Brokers (IAB), una profesión con futuro. *Ciberseguridadtic*. https://ciberseguridadtic.es/datos/initial-access-brokers-iabs-una-profesion-con-futuro-20230118883.htm

BlackBerry. (n.d.). *Cómo BlackBerry protege contra la creciente amenaza de los ataques de ransomware | Todo lo que necesita saber para detener los ataques de ransomware más sofisticados de la actualidad.* https://www.blackberry.com/la/es/solutions/ransomware?

Chkadmin. (2021, febrero 18). *¿Qué es el Ransomware?* Check Point Software ES. https://www.checkpoint.com/es/cyber-hub/what-is-ransomware/

ESET. (n.d.). *¿Qué es el ransomware, cómo ataca y cómo evitarlo? | ESET*. https://www.eset.com/es/caracteristicas/ransomware/

IBM. (n.d.). *¿Qué es el ransomware? | IBM*. https://www.ibm.com/mx-es/topics/ransomware

Kaspersky. (2023a, abril 19). *El ransomware: qué es, cómo se lo evita, cómo se elimina*. latam.kaspersky.com. https://latam.kaspersky.com/resource-center/threats/ransomware

Kaspersky. (2023b, April 19). *El ransomware: qué es, cómo se lo evita, cómo se elimina*. latam.kaspersky.com. https://latam.kaspersky.com/resource-center/threats/ransomware

Kaspersky. (2023c, April 19). *Identificación de ransomware: en qué se diferencian los troyanos de cifrado*. latam.kaspersky.com. https://latam.kaspersky.com/resource-center/threats/ransomware-attacks-and-types

Nadeem, M. S. (2022). Las 5 mejores maneras de evitar ataques de ransomware. *Mailfence Blog*. https://blog.mailfence.com/es/protegerse-del-ransomware/

Rvega. (2022, August 3). *¿Cómo prevenir un ataque de ransomware?* Check Point Software ES. https://www.checkpoint.com/es/cyber-hub/how-to-prevent-ransomware/

Saguier, E. P. (2023, June 21). ¿Cómo prevenir un ataque de ransomware? Una guía rápida para proteger los datos de tu empresa. *Invgate*. https://blog.invgate.com/es/como-prevenir-un-ataque-de-ransomware