Píldora Informativa

GPIT

Ransomware

No. 007

Gerencia de plataformas e infraestructura tecnológica
GPIT
Grupo Seguridad Informática - GSI
seguridad.informacion@unad.edu.co
Tel: 601-3443700 Ext 1687

Fecha del Reporte

Agosto 22 de 2023

Alcance

Un ataque de ransomware puede variar según diversos factores, como la naturaleza del malware, la capacidad del sistema de seguridad para detectarlo y prevenirlo, y la cantidad de datos y sistemas afectados. En general, el ransomware puede tener un alcance amplio y afectar a una amplia variedad de organizaciones y usuarios individuales, incluyendo:

- **Pequeñas y grandes empresas:** El ransomware puede afectar a empresas de cualquier tamaño y tipo, desde pequeñas empresas hasta grandes corporaciones.
- **Instituciones gubernamentales y educativas:** Las organizaciones gubernamentales y educativas también son objetivos frecuentes del ransomware.
- **Usuarios individuales:** Los usuarios individuales también pueden ser víctimas del ransomware, especialmente si no tienen medidas de seguridad adecuadas en sus dispositivos.

El alcance del ransomware puede ser aún más amplio si el malware se propaga a través de la red de la organización o si los sistemas afectados no están aislados correctamente. Además, los ataques de ransomware pueden tener un impacto significativo en las operaciones de una organización, ya que pueden causar interrupciones en el servicio, la pérdida de datos valiosos y la violación de la privacidad del usuario. Es importante tomar medidas preventivas para evitar ataques de ransomware y estar preparado para responder rápidamente en caso de un ataque.

Objetivo

Un ataque de ransomware consiste en cifrar los archivos del usuario y exigir un rescate a cambio de su liberación. Los atacantes buscan obtener una ganancia financiera extorsionando a las víctimas mediante la demanda de un pago en criptomonedas para desbloquear los archivos cifrados. Además del lucro, pueden incluir la interrupción de las operaciones empresariales, la obtención de información confidencial, la propagación del malware a través de redes informáticas, el sabotaje de la competencia, entre otros. Es importante tener en cuenta que el ransomware es un delito informático y, en muchos casos, los atacantes nunca cumplen su promesa de liberar los archivos después de recibir el pago, por lo que es recomendable no ceder a las demandas de rescate y buscar ayuda de expertos en seguridad informática para recuperar los archivos de manera segura.

Evite un ransomware

Son programas maliciosos que se utilizan para cifrar los archivos del usuario y exigir un rescate a cambio de su liberación. Estos ataques pueden ser devastadores para los individuos y las empresas, ya que pueden resultar en la pérdida de datos valiosos y comprometer la seguridad de la información.

Figura No. 1 Fuente https://www.muycomputerpro.com/2021/05/15/mas-ataques-de-ransomware

A continuación, se presentan algunos consejos que pueden ayudar a prevenir los ataques de ransomware:

1. **Mantén tu software actualizado:** Asegúrate de que todos tus programas, sistemas operativos y software de seguridad estén actualizados con las últimas versiones y parches de seguridad.

2. **Utiliza software de seguridad:** Instala y utiliza software antivirus, antimalware y firewall en todos los dispositivos que uses para acceder a internet, incluyendo computadoras, teléfonos inteligentes y tabletas.

3. **No hagas clic en enlaces sospechosos:** No hagas clic en enlaces de correo electrónico, mensajes de texto o redes sociales de remitentes desconocidos o sospechosos.

4. **No descargues archivos de fuentes no confiables:** No descargues archivos de sitios web no confiables o desconocidos, especialmente si se te pide que desactives tu software de seguridad para hacerlo.

5. **Haz copias de seguridad de tus datos:** Haz copias de seguridad regularmente de tus datos en un dispositivo externo o en la nube. De esta manera, si tu dispositivo es atacado, puedes recuperar tus datos sin tener que pagar un rescate.

6. **Ten cuidado con los correos electrónicos de phishing:** No proporciones información personal o financiera a través de correos electrónicos de remitentes desconocidos o sospechosos. Los estafadores utilizan a menudo el phishing para recopilar información valiosa y realizar ataques de ransomware.

7. **Utiliza contraseñas seguras:** Utiliza contraseñas seguras y cambia tus contraseñas regularmente. No utilices la misma contraseña para múltiples cuentas.

Recuerda que la mejor defensa contra el ransomware es la prevención. Siguiendo estos consejos, puedes ayudar a proteger tus dispositivos y tus datos valiosos de los ataques de ransomware.

Grupo Seguridad de las Información
https://gpit.unad.edu.co/seguridad-de-la-informacion
Teléfono: (601) 3443700 Ext 1687