XXXI SEMANA NACIONAL DE INVESTIGACIÓN Y DOCENCIA EN MATEMÁTICAS

Ransomware

Elaborado por:
Hugo Cano, Juan Hernández, Guillermo Velazquez
Maestra asesora:
Dra. María de Guadalupe Cota Ortiz

Introducción

Un ransomware es un programa de software malicioso que infecta tu computadora y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema. Es un tipo de malware criminal para ganar dinero que se puede instalar a través de enlaces engañosos incluidos en un mensaje de correo electrónico, mensaje instantáneo o sitio web. El ransomware tiene la capacidad de bloquear la pantalla de una computadora o cifrar archivos importantes predeterminados con una contraseña.

Ejemplos

WannaCry: En mayo de 2017, WannaCry se propagó por todo el planeta y llegó a atacar a millones de usuarios. Se aprovechó de una vulnerabilidad de Windows que permitía ejecutar código de forma remota. Afectó especialmente a usuarios de Windows XP.

Popcorn Time: Como el objetivo final de un atacante es propagar el ransomware en el mayor número posible de equipos para conseguir más dinero, ha surgido una táctica alternativa, social y siniestra a partes iguales, para pedir el rescate. Que le pide que infecte a otros dos usuarios con el malware. Si esos dos usuarios pagan el rescate, usted podrá recuperar sus archivos de forma gratuita.

Tipos de Ransomware

Doxing: mediante un archivo o un enlace malicioso, el atacante accede a sus datos personales confidenciales. A continuación, recibe un mensaje donde se le indica que, si no realiza un pago, el atacante publicará la información.

Scareware: El scareware es un software falso que asegura haber encontrado problemas en su equipo y que demanda un pago para solucionarlos, comúnmente suele bombardearlo con ventanas emergentes y mensajes de alerta.

Screenlockers: estos programas le impiden acceder en modo alguno a su equipo, smartphone o tableta. Suelen hacerse pasar por mensajes de una institución oficial.

Filecoders: estos programas, componen el 90 % de las cepas de ransomware. Esta clase de malware cifra y bloquea los archivos en los dispositivos infectados.

Cómo funciona un ataque Ransomware

Al contrario que la mayoría del malware, que requiere que usted descargue un archivo infectado o haga clic en un enlace malicioso, hay ransomware capaz de infiltrarse en un equipo sin acción alguna por parte del usuario. Otros ataques recurren a los métodos tradicionales.

Kits de exploits: atacantes maliciosos desarrollan kits de exploits que contienen código escrito previamente, diseñado para aprovechar vulnerabilidades en aplicaciones, redes o dispositivos.

Phishing: el ciberdelincuente se hace pasar por un contacto de confianza y le envía un correo electrónico que contiene un archivo adjunto o un enlace aparentemente legítimos.

Malvertising: los atacantes pueden distribuir el malware incrustándolo en falsos anuncios en línea, una práctica conocida como malvertising. Los ciberdelincuentes pueden poner sus anuncios en casi cualquier sitio web, incluso los de más confianza.

Descargas drive-by: los atacantes pueden preparar un sitio web con malware de modo que, cuando lo visite, se descargue de forma secreta y automática el malware en el dispositivo.

Prevención y eliminación

Los usuarios de computadoras deben comprobar que sus firewalls estén activados, evitar visitar sitios web de dudosa reputación y tener cuidado cuando abran cualquier mensaje de correo electrónico sospechoso. Si eliges una solución de software antivirus de eficacia certificada provista por una empresa de prestigio, podrás proteger tu computadora contra las amenazas de ransomware más recientes.

Muchas de las cepas de ransomware más conocidas ya están inactivas porque las vulnerabilidades que aprovechaban se han parcheado mediante actualizaciones de software. Eso significa que, si sigue utilizando software antiguo, es vulnerable: no deje de actualizarse.

Referencias

1. Guía esencial sobre el ransomware. 2021. Guía esencial sobre el ransomware. [online] Available at: <https://www.avast.com/es-es/c-what-is-ransomware#:~:text=El%20ransomware%20es%20un%20tipo,devolverle%20el%20acceso%20a%20estos.>

1. latam.kaspersky.com. 2021. ¿Qué es el ransomware?. [online] Available at: <https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware>