Seguridad de la información

Ransomware o 'secuestro de datos'

Malware

Malware es un término que abarca cualquier tipo de software malicioso diseñado para dañar o explotar cualquier dispositivo, servicio o red programable. Los delincuentes cibernéticos generalmente lo usan para extraer datos que pueden utilizar como chantaje hacia las víctimas para obtener ganancias financieras. Dichos datos pueden variar desde datos financieros, hasta registros de atención médica, correos electrónicos personales y contraseñas.

¿Qué es el ransomware?

El ransomware hace referencia a un tipo de malware que luego de comprometer un equipo secuestra la información para luego extorsionar a las víctimas, solicitando pago en criptomonedas para recuperar la información.

Las clases de ransomware más frecuentes son dos:

Ransomware de bloqueo.

Este tipo de ransomware está diseñado para bloquear funciones básicas del equipo. Puede, por ejemplo, impedir el acceso al escritorio del sistema y restringir parcialmente el uso del teclado y del mouse. La víctima puede interactuar únicamente con la ventana en la que se le exige el pago de un rescate.

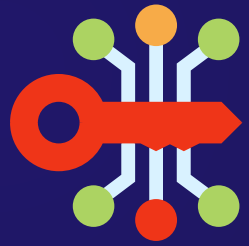
Ransomware de cifrado.

Este tipo de ransomware está diseñado para cifrarlos archivos más importantes de la víctima, como sus documentos, fotos y videos. El funcionamiento del equipo no se ve afectado en modo alguno. La víctima entra en pánico porque ve que sus archivos siguen allí, pero no puede abrirlos. Esta clase de malware muestra una leyenda en la que se exige el pago de un rescate y, por lo general, una cuenta regresiva. “Pague antes de que se agote el tiempo o perderá sus archivos”, advierte el software.

¿Qué es el phishing?

El phishing es un tipo de ataque cibernético basado en la suplantación de identidad que permite a los infractores obtener información confidencial de los usuarios y las empresas. Normalmente, el objetivo es obtener credenciales de acceso y detalles de tarjetas de crédito que permitan obtener beneficio de este acto delictivo.

¿Qué es un exploit?



Un exploit es una pieza de software, datos o secuencia de comandos que se aprovecha de una vulnerabilidad para provocar un comportamiento no intencionado o para obtener acceso no autorizado a datos confidenciales.

¿Cómo se puede infectar un equipo?

La forma de distribución más común del ransomware es a través de correos de phishing con archivos adjuntos o enlaces que intentan engañar a los usuarios y convencerlos para descargar la amenaza.

Otras formas de distribución son mediante ataques a conexiones remotas, como el escritorio remoto, aprovechando el uso de contraseñas débiles.

También a través de sitios web comprometidos utilizados para redirigir a sus visitantes a diferentes tipos de exploit el cual aprovecha un fallo en el sistema y lograr la instalación de un malware

Tipos de phishing

CEO

Es un ejemplo de phishing en el que los ciberdelincuentes se hacen pasar por un CEO o alto ejecutivo de una empresa

Facturas falsas

Los atacantes se hacen pasar por una empresa proveedora o cliente para solicitar el pago de una factura fraudulenta.

Mensajería instantánea

Los atacantes aprovechan esta nueva situación para mandar enlaces fraudulentos, suplantar la identidad de otras personas o crear una situación de negocio amigable para tratar de engañar al receptor.

Cambio de contraseña

Es habitual la suplantación de identidad de grandes empresas como Microsoft, LinkedIn, Google y muchas otras para enviar correos electrónicos de cambio de contraseña.

Archivos adjuntos

Envían correos electrónicos que contienen archivos adjuntos malintencionados. También pueden contener archivos HTML para suplantar el inicio de sesión de servicios conocidos o incluir formularios falsos con la única intención de obtener datos de usuarios o tarjetas de crédito.

Tipos de exploits

Vulnerabilidad conocida

Un ejemplo muy claro es el exploit EternalBlue, que puso contra las cuerdas a muchos dispositivos con Windows en todo el mundo. Se aprovechaba de un fallo de seguridad en Windows y rápidamente Microsoft lanzó parches para corregirlo.

De día cero

Aquí entra en juego la rapidez de los investigadores de seguridad para lanzar una protección lo antes posible. El tiempo que tarden en lanzar parches va a suponer una oportunidad para los ciberdelincuentes.

Vulnerabilidad remota

Va a ser un fallo que está presente en algo externo, como puede ser la red en la que está conectado. Van a aprovecharse de ello para lograr tomar el control de ese dispositivo. Puede ocurrir que, por ejemplo, haya un ordenador vulnerable dentro de la red donde estamos conectados.

Vulnerabilidad local

En esta ocasión, el atacante necesita que haya un fallo de seguridad en nuestro equipo, en el dispositivo que pretenden atacar. Puede ser una vulnerabilidad que haya en Windows o en algún programa que utilicemos, por ejemplo. Esa va a ser la vía de entrada que puede usar para tomar el control.

Recomendaciones de ciberseguridad

1. No abrir correos ni mensajes de dudosa procedencia
2. Desconfiar de los enlaces y archivos adjuntos en los mensajes o correos
3. Mantener actualizadas las plataformas de administrativa y software de seguridad
4. Mantener actualizadas las plataformas de antivirus
5. Presta atención a los detalles en los mensajes y redes sociales
6. Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas
7. Revisar los controles de seguridad AntiSpam Y SanBoxing
8. Concientizar a los usuarios sobre amenazas en la web
9. Verificar la autenticidad de los sitios web
10. Realizar escaneos completos con el antivirus

ANATOMÍA DE UN ATAQUE RANSOMWARE

Distribución

Identificar páginas o cualquier información que pueda conducir a la víctima a acceder al enlace fraudulento

Infección

Es a partir de esta acción que el código entra en actividad, desactivando copias y sistemas de reparación y recuperación de errores, programas de defensa

Comunicación

El malware comienza a comunicarse con los servidores de clave de cifrado, obteniendo la clave pública que permite que los datos de la víctima sean encriptados.

Búsqueda de archivos

Realiza una exploración sistemática en la computadora de la víctima buscando archivos de sistema específicos, que sean importantes para el usuario

Cifrado

Es en esta etapa que se lleva a cabo el proceso de mover y renombrar los archivos identificados en el paso anterior

Pedido de rescate

Primero aparece un aviso en la pantalla de la computadora infectada. Es por este medio que el hacker avisa que ha secuestrado los datos y que sólo los devolverá si el usuario realiza el pago de un rescate.