DGTIC UNAM
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Ataques más comunes

CURSOS EN LÍNEA

Ataques más comunes

Existe una inmensa cantidad de ataques informáticos que, a su vez, utilizan diferentes tácticas, técnicas y pueden estar orientados a diferentes vectores de la superficie de ataque de un sistema informático.

El análisis de la gran mayoría de ataques está fuera de los alcances técnicos y temporales del curso. Así que nos concentrarnos en aquellos a los que, como usuarios, encontraremos de manera frecuente en nuestras actividades.

Explotación de vulnerabilidades

Los ataques informáticos son posibles por la presencia de vulnerabilidades de los sistemas de información (ya sea en el software y hardware, en los sistemas operativos, la infraestructura de red, o inclusive en las personas que los operan) y por la existencia de amenazas que cuentan con la capacidad y motivación para explotarlas. La explotación en este sentido, son todas aquellas técnicas utilizadas para aprovecharse de las vulnerabilidades.

Existen dos modalidades principales de explotación de vulnerabilidades: malware e ingeniería social. En este documento nos enfocaremos en aquellas relacionadas al malware.

Malware

El término malware describe una amplia gama de software malintencionado que está diseñado para afectar los sistemas, dispositivos, redes, así como a sus usuarios. El malware infecta sistemas para después realizar acciones que lo perjudican. Por ejemplo, el robo de información, daño a los datos o al sistema. Por lo tanto, el malware es el medio o artefacto que ha sido creado para realizar un ataque.

El malware se aprovecha de las vulnerabilidades de los sistemas informáticos para lograr que realicen acciones específicas que no realizarían en un estado normal. A continuación, revisaremos los tipos principales de malware.

Será necesario recordar que, si bien el malware puede considerarse como un ataque en sí, muchas veces representa solo el primer paso de un ataque más elaborado.

Virus

La mayoría de usuarios de computadoras han tenido que lidiar alguna vez con un virus informático. De hecho, es un problema tan frecuente que la mayoría de las personas tienden a llamar virus a todo tipo de malware.

Los virus informáticos toman este nombre de los virus biológicos ya que al igual que estos, los se propagan creando copias de sí mismos. Cuando un usuario abre un archivo infectado, el virus se ejecuta para agregarse a sí mismo a otros archivos (o código) y comenzar a replicarse.

Figura 1. Existen virus persistentes capaces de pasar sin ser detectados por los sistemas de seguridad convencionales.

La característica principal de los virus es que se esparcen a través de los sistemas por medio de una acción que realizan los usuarios. Por ejemplo: abrir un archivo adjunto de un correo electrónico de dudosa procedencia, o bien, descargar un archivo de un sitio web no seguro, o insertando una unidad de memoria infectada. Por lo tanto, la mejor manera de protegerse de un virus es la comprensión de los riesgos y consecuencias que estás acciones, aparentemente inocentes, podrían desencadenar. Es decir, se requiere que nosotros como usuarios seamos conscientes de este riesgo y no abrir o ejecutar de manera descuidada cualquier tipo de archivo si se desconoce su procedencia.

Además, será necesario verificar que el sistema cuente con una solución antivirus activada y actualizada para que permita la detección y mitigación de este tipo de malware.

Los virus no se esparcen sin la ayuda o una acción del usuario.

Gusanos

Los gusanos informáticos son un tipo de malware muy peligroso pues, a diferencia de los virus, puede replicarse a sí mismo sin la participación del usuario y sin la necesidad de agregarse a otro archivo. Este tipo de malware está diseñado para aprovecharse de las vulnerabilidades de los sistemas (aplicaciones o sistemas operativos) para instalarse. Una vez que un gusano se ha instalado en un sistema, es capaz de identificar conexiones a la red local y a internet para buscar otros sistemas y continuar replicándose a sí mismo.

Los gusanos pueden replicarse a sí mismos sin la necesidad de un archivo anfitrión y sin la necesidad de que el usuario realice una acción.

Algunos de los medios que utiliza este malware para su propagación son los correos electrónicos, los protocolos de red, así como las conexiones a internet.

Como se ha mencionado, los gusanos tienen éxito en los dispositivos vulnerables. Por esto, es importante mantener los sistemas operativos y aplicaciones actualizados con los últimos parches de seguridad instalados.

Figura 2. Dadas sus capacidades, los gusanos son un terrible tipo de malware.

Spyware

El spyware es malware que recopila y comparte información con un atacante sin el consentimiento o conocimiento del usuario. Esta información puede ser usada para fines malicioso como, por ejemplo, robo de identidad, acceso a información financiera o espionaje. Por ejemplo, existe software que puede accionar y grabar con la cámara de los dispositivos como webcams y la cámara de los dispositivos móviles.

El spyware está muchas veces ligado con software que presenta anuncios con base en la información que recopila de nuestro navegador para presentar ofertas. Sin embargo, en su forma más agresiva, el spyware se encarga de comunicar información a un agente externo sin que el usuario pueda notarlo.

Figura 3. Un atacante podría registrar y monitorear sus acciones con el uso de spyware.

Entre las técnicas que utiliza este tipo de malware se puede identificar:

- *Keyloggers*. Un *keylogger* es un programa que realiza el registro de las teclas pulsadas. Con esta función, se capturan todas las teclas que el usuario presiona, típicamente, para la captura de nombres de usuario y contraseñas para acceder a cuentas bancarias o a otros recursos del usuario.
- Monitoreo del navegador de internet. En este modo, se registra la actividad del usuario en internet, así como de las conexiones abiertas en el equipo del usuario.
- Registro de discos de almacenamiento. También es posible que el spyware recopile y transmita la información contenida en los discos duros o en los espacios de almacenamiento en la nube en los que los usuarios guardan su información en busca de información sensible que resulte beneficiosa para el atacante.

En resumen, el spyware monitorea, registra y comparte la actividad del sistema al exterior. No es necesario decir que esto puede representar un grave problema para la información e integridad de las personas.

Caballos de Troya

Un caballo de Troya informático, comúnmente conocidos como Troyanos, es un tipo de malware que se hace pasar o que viene oculto dentro de software legítimo. De esta manera, aprovecha para infiltrarse en nuestros equipos y realizar acciones que pueden tener graves consecuencias.

Es muy común que este tipo de malware se haga pasar por videojuegos o aplicaciones de ofimática, aunque puede ser cualquier tipo de software que el usuario descarga de sitios no oficiales en los que se ofrece gratuitamente. Cuando el programa se ejecuta es posible que actúe tal y como se espera, sin embargo, el troyano lleva consigo código malicioso que puede realizar acciones indeseadas sin el conocimiento y consentimiento del usuario.

Figura 4. Los troyanos se hacen pasar por software legitimo para ingresar a los sistemas.

Los troyanos no se replican a sí mismos como los virus, pero pueden afectar considerablemente a los sistemas de información. Por ejemplo, existen versiones de troyanos que permiten el control remoto a personas maliciosas llamados RAT. Los RAT (*Remote Access Trojan*) son un tipo de troyanos que, una vez instalados en el sistema, puede ser utilizado como una puerta trasera que utilice una persona para acceder y controlar un dispositivo infectado de manera remota.

Además, los troyanos pueden realizar una gran variedad de acciones para afectar el sistema sin el conocimiento del usuario como puede ser la recolección y extracción de datos, o la descarga e instalación de otros programas, lo que aumenta el riesgo en los equipos.

En resumen, los troyanos engañan a los usuarios haciéndose pasar como otro tipo de software para, posteriormente, afectar de diferentes maneras el sistema. Para la protección ante este tipo de malware será necesario instalar programas solo de fuentes seguras. De hecho, en un ambiente laboral es recomendable que sean los administradores de sistemas quienes se encarguen de instalar el software para los usuarios. En un ambiente doméstico, usted será el responsable, así que vigile el tipo de software que instala. Nunca descargue software de sitios no seguros.

Ransomware

El ransomware es software que se encarga de la captura y encriptación de la información de un sistema para posteriormente solicitar una recompensa económica por su liberación. En este escenario, el atacante envía un mensaje al usuario informando que entregará la llave de descifrado una vez que haya recibido el rescate solicitado. De lo contrario, el atacante puede llegar a amenazar con destruir de manera permanente la información.

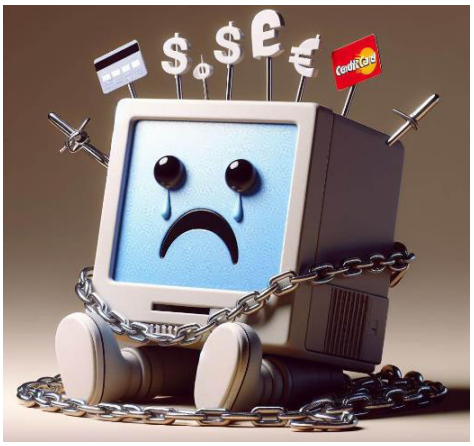

Figura 5. En un ataque de ransomware se solicita el pago de un rescate para la liberación de la información.

Existen distintos tipos de técnicas en el ransomware, por ejemplo, aquellos donde se solicita el pago con criptomonedas para el desciframiento de la información encriptada. O bien, otro tipo de técnica de ransomware consiste en la amenaza de reportar al usuario a una autoridad por el tipo de información descubierta por el atacante, como pornografía, o se amenaza con revelar públicamente información sensible como fotografías o documentos personales del usuario halladas en el equipo.

Spam

El spam, conocido también como correo no deseado, se caracteriza por ser cualquier tipo de correo electrónico enviado masivamente a una gran cantidad de destinatarios, sin su consentimiento previo. Este tipo de mensajes suelen contener información irrelevante, anuncios, promociones de productos o servicios, e incluso en algunos casos contenido inapropiado. Aunque el spam en sí mismo no es considerado como malware, puede ser utilizado como vehículo para distribuirlo. Por ejemplo, los correos spam pueden contener archivos adjuntos maliciosos o enlaces

a sitios web fraudulentos que intentan engañar a los usuarios para que revelen información personal o descarguen software malicioso.

Figura 6. El spam o correo basura es un problema persistente en nuestras cuentas de correo electrónico.

A pesar de los esfuerzos por combatir el spam mediante filtros y sistemas de detección, sigue siendo un problema persistente que afecta a millones de usuarios en todo el mundo. La lucha contra el spam es constante y requiere de la colaboración tanto de usuarios como de proveedores de servicios de correo electrónico para minimizar su impacto y proteger la seguridad y privacidad en línea.

Bots

Técnicamente, un bot no es malware sino un sistema que se encuentra bajo el control de un atacante debido a una infección por malware. Es decir, existe malware especializado que permite el control remoto de los equipos de cómputo. Un sistema informático puede convertirse en un bot si se ha visto expuesto a un virus u otro código malicioso que concede acceso a un atacante. Así, una vez que el malware se instala en el equipo puede crear un canal de comunicación con un atacante remoto.

Figura 7. Un sistema infectado con malware puede convertirse en un bot controlado por un atacante.

De hecho, muchas computadoras de uso doméstico pueden llegar a convertirse, o son ya, un bot sin el conocimiento del usuario, pues es muy difícil su detección.

Entre las razones principales por la que un atacante desea tomar control de un sistema es principalmente por la información que contiene, pero también por su capacidad de procesamiento, almacenamiento y conexión a una red local o internet. Los actores maliciosos utilizan las capacidades de procesamiento de equipos ajenos para mantener su anonimato, o bien, para realizar ataques más elaborados con una red de bots.

Las redes de bots

Una red de bots es un gran número de sistemas bots que pueden ser controlados para realizar acciones coordinadas o evasivas por parte de actores maliciosos. Por ejemplo, pueden ser usadas para establecer comunicaciones con un servidor y provocar que este no pueda responder adecuadamente a las solicitudes recibidas provocando que deje de funcionar.

Existen personas con las capacidades técnicas, habilidades y motivación necesaria para crear estas redes de dispositivos con la intención de llevar a cabo ataques más avanzados. Las redes de bots le ofrecen al atacante, principalmente, un escondite, dado que sus acciones no pueden ser relacionadas con un solo dispositivo o dirección de red específica. Además, le ofrecen la capacidad de procesamiento y almacenamiento combinado.

Figura 8. Una red de bots es una técnica avanzada que utilizan los atacantes para llevar a cabo ofensivas complejas.

Pero no solo eso, pues el controlador de una red de bots puede sacar provecho económico al rentar la red para otras personas, utilizarla para el envío de correo malicioso, o para intentar deshabilitar un servicio por medio de múltiples solicitudes simultáneas, minería de criptomonedas o realizar ataques de fuerza bruta.

Conclusiones.

Los peligros del malware en un sistema de información son significativos y potencialmente devastadores. Estos programas maliciosos pueden robar datos confidenciales, corromper archivos y afectar la integridad de los sistemas. Además de que pueden ser el comienzo de un ataque informático más elaborado.

Es crucial que las organizaciones y los usuarios implementen medidas sólidas de seguridad para mitigar estos riesgos y proteger sus activos digitales. La vigilancia constante, actualizaciones de software, capacitación y soluciones de seguridad robustas son esenciales para hacer frente a las amenazas del mundo digital.

AUTOR

ELIER EMANUEL LÓPEZ BASILIO