¿Qué es el malware? Todo lo que necesitas saber sobre virus, troyanos y software malicioso.

Los ataques cibernéticos y el malware son una de las mayores amenazas en Internet. Aquí aprenderas sobre los diferentes tipos de malware y cómo evitar ser víctima de ataques.

¿Qué es el malware?

Malware es la abreviatura de software malicioso. Es un software desarrollado por ciberatacantes con la intención de obtener acceso o causar daño a una computadora o red, a menudo mientras la víctima no se da cuenta del hecho de que ha habido un compromiso. Una descripción alternativa común del malware es 'virus informático', aunque existen grandes diferencias entre estos tipos de programas maliciosos.

¿Cuál fue el primer virus informático?

El origen del primer virus informático es objeto de acalorados debates. Para algunos, la primera instancia de un virus informático, un software que se mueve de un host a otro sin la entrada de un usuario activo, fue Creeper, que apareció por primera vez a principios de la década de 1970, 10 años antes de que el término real 'virus informático' fuera acuñado por El informático estadounidense Profesor Leonard M. Adleman.

Seguridad

Creeper se ejecutó con el sistema operativo Tenex utilizado en ARPANET, la Red de la Agencia de Proyectos de Investigación Avanzada, y saltó de un sistema a otro, mostrando un mensaje de "SOY EL GRIEGO: ¡Atrápame si puedes!" en máquinas infectadas, antes de transferirse a otra máquina. En su mayor parte, cuando encontró una nueva máquina, se retiró de la computadora anterior, lo que significa que no era capaz de extenderse a varias computadoras a la vez.

Si bien Creeper no se creó para fines maliciosos o para realizar cualquier actividad más allá de causar molestias leves, podría decirse que fue el primer ejemplo de software que funciona de esta manera.

Poco después, se creó una nueva forma de software para operar de manera similar, pero con el objetivo de eliminar Creeper. Se llamaba Reaper.

Alternativamente, algunos creen que el título del primer virus de computadora debería ir a uno llamado Brain, porque a diferencia de Creeper, podría auto-replicarse sin la necesidad de eliminarse primero de un sistema anterior, algo que muchas formas de código malicioso ahora hacen.

El gusano de Morris

Morris Worm tiene la notoria distinción del primer gusano informático en llamar la atención de los principales medios de comunicación porque, a las pocas horas de haberse conectado a Internet, había infectado a miles de computadoras. Se estima que el daño de la productividad perdida ha costado entre $ 100,000 y $ 10,000,000.

Al igual que Brain y Creeper antes, el gusano Morris no está clasificado como malware, porque es otro ejemplo de un experimento que salió mal.

El software fue diseñado para tratar de averiguar el tamaño de la floreciente Internet con una serie de escaneos en 1988, pero los errores en el código llevaron a que se ejecutaran operaciones de denegación de servicio involuntarias, a veces varias veces en la misma máquina, lo que hace que algunas computadoras lentamente se volvieron inútiles.

Como resultado del gusano Morris, Internet estuvo brevemente segmentada durante varios días para evitar una mayor propagación y limpiar las redes.

¿Cuál es la historia del malware?

Si bien Creeper, Brain y Morris son ejemplos tempranos de virus, nunca fueron malware en el sentido más verdadero.

El malware y el código malicioso detrás de él están diseñados específicamente para causar daños y problemas en los sistemas informáticos, mientras que los descritos anteriormente se encuentran causando problemas por accidente, aunque los resultados siguen siendo perjudiciales.

Con el nacimiento de la web y la capacidad de conectarse a computadoras en todo el mundo, a principios de los años 90, las empresas de Internet despegaron cuando la gente buscaba proporcionar bienes y servicios utilizando esta nueva tecnología.

Sin embargo, como con cualquier otra forma de nueva tecnología, hubo quienes buscaron abusar de ella con el propósito de ganar dinero, o en muchos casos, solo para causar problemas.

Además de poder propagarse a través de discos, tanto en disquetes como en variedades de CD-Rom, la mayor proliferación de correo electrónico personal permitió a los atacantes propagar malware y virus a través de archivos adjuntos de correo electrónico, que ha sido especialmente potente contra aquellos sin ningún tipo de protección contra malware.

Varias formas de software malicioso causaron problemas a los usuarios de computadoras de la década de 1990, realizando acciones que van desde eliminar datos y corromper los discos duros, hasta molestar a las víctimas al reproducir sonidos o poner mensajes ridículos en sus máquinas.

Muchos se pueden ver ahora, en modo seguro con el malware real eliminado, en el Malware Museum en Internet Archive.

Algunos de los ataques pueden haber parecido simples, pero fueron estos los que sentaron las bases para el malware tal como lo conocemos hoy, y todo el daño que ha causado en todo el mundo.casino-disk-destroyer-internet-archive.jpg

Casino Disk Destroyer, una forma de malware en los años 90, hizo que las víctimas jugaran un juego de azar antes de que destruyera el contenido del disco.Imagen: Archivo de Internet

¿Cuáles son los diferentes tipos de malware?

Al igual que el software legítimo, el malware ha evolucionado a lo largo de los años y viene equipado con diferentes funciones según los objetivos del desarrollador.

Los autores de malware a veces combinan las características de diferentes formas de malware para hacer que un ataque sea más potente, como el uso de ransomware como una distracción para destruir la evidencia de un ataque troyano.

¿Qué es un virus de computadora?

En esencia, un virus informático es una forma de software o código que puede copiarse en las computadoras. El nombre se ha asociado con la realización adicional de tareas maliciosas, como corromper o destruir datos. Si bien el software malicioso ha evolucionado para ser mucho más diverso que solo los virus informáticos, todavía hay algunas formas de virus tradicionales, como el gusano Conficker de 15 años, que aún pueden causar problemas en los sistemas más antiguos. El malware, por otro lado, está diseñado para proporcionar a los atacantes muchas más herramientas maliciosas.

¿Qué es el malware troyano?

Una de las formas más comunes de malware, el caballo de Troya, es una forma de software malicioso que a menudo se disfraza como una herramienta legítima que engaña al usuario para que lo instale para que pueda llevar a cabo sus objetivos maliciosos.

Su nombre, por supuesto, proviene de la historia de la antigua Troya, con los griegos escondidos dentro de un caballo de madera gigante, que según ellos fue un regalo para la ciudad de Troya. Una vez que el caballo estuvo dentro de las murallas de la ciudad, un pequeño equipo de griegos emergió del interior del caballo gigante de madera y tomó la ciudad.

Así como los griegos usaron un caballo de Troya para engañar a Troy para que permitiera que las tropas entraran a la ciudad, el malware troyano se disfraza para infiltrarse en un sistema.Imagen: Getty

El malware troyano funciona de la misma manera, ya que se infiltra en su sistema, a menudo disfrazado como una herramienta legítima como una actualización o una descarga Flash, y luego, una vez dentro de su sistema, comienza sus ataques.

Una vez instalado en el sistema, dependiendo de sus capacidades, un troyano puede potencialmente acceder y capturar todo (inicios de sesión y contraseñas, pulsaciones de teclas, capturas de pantalla, información del sistema, detalles bancarios y más) y enviarlo todo en secreto a los atacantes. A veces, un troyano puede incluso permitir a los atacantes modificar datos o desactivar la protección antimalware.

El poder de los caballos de Troya lo convierte en una herramienta útil para todos, desde piratas informáticos en solitario, hasta pandillas criminales y operaciones patrocinadas por el estado que se dedican al espionaje a gran escala.

¿Qué es el spyware?

El spyware es un software que monitorea las acciones llevadas a cabo en una PC y otros dispositivos. Eso podría incluir el historial de navegación web, las aplicaciones utilizadas o los mensajes enviados. El spyware puede llegar como un malware troyano o puede descargarse en los dispositivos de otras maneras.

Por ejemplo, alguien que descargue una barra de herramientas para su navegador web puede encontrar que viene con software espía con el fin de monitorear su actividad en Internet y el uso de la computadora, o anuncios maliciosos pueden soltar secretamente el código en una computadora a través de una descarga automática.

En algunos casos, el spyware se vende activamente como software diseñado para fines tales como los padres que monitorean el uso de Internet de sus hijos y está diseñado para ser ignorado explícitamente por el software antivirus y de seguridad. Sin embargo, hay varios casos en los que los empleadores utilizan estas herramientas para espiar la actividad de los empleados y las personas que utilizan software espía para espiar a sus cónyuges.

¿Qué es el ransomware?

Si bien algunas formas de malware dependen de ser sutiles y permanecer ocultas durante el mayor tiempo posible, ese no es el caso del ransomware.

A menudo entregado a través de un archivo adjunto o enlace malicioso en un correo electrónico de phishing, el ransomware encripta el sistema infectado, bloqueando al usuario hasta que pague un rescate, entregado en bitcoin u otra criptomoneda, para recuperar sus datos.

Puede sonar simple, pero el ransomware funciona: los ciberdelincuentes se embolsaron más de $ 1 mil millones de ataques de ransomware solo en 2016, y un informe de Europol lo describe como "eclipsado" la mayoría de las otras amenazas cibercriminales globales en 2017.cerber-ransomware.png

El ransomware exige un pago a cambio de devolver archivos cifrados.Imagen: Malwarebytes

¿Qué es el malware limpiador?

El malware Wiper tiene un objetivo simple: destruir por completo o borrar todos los datos de la computadora o red objetivo. La eliminación podría tener lugar después de que los atacantes hayan eliminado secretamente los datos del objetivo de la red, o podría lanzarse con la pura intención de sabotear el objetivo.

Una de las primeras formas principales de malware de limpiaparabrisas fue Shamoon, que apuntó a las compañías de energía sauditas con el objetivo de robar datos y luego borrarlos de la máquina infectada. Los casos más recientes de ataques de limpiaparabrisas incluyen StoneDrill y Mamba, el último de los cuales no solo elimina archivos, sino que deja inutilizable el disco duro.

Uno de los limpiadores de más alto perfil de los últimos tiempos fue el ransomware Petya. Inicialmente se pensó que el malware era ransomware. Sin embargo, los investigadores descubrieron que no solo no había forma de que las víctimas recuperaran sus datos mediante el pago del rescate, sino que también el objetivo de Petya era destruir irremediablemente los datos.

¿Qué es un gusano informático?

Un gusano es una forma de malware que está diseñado para propagarse de un sistema a otro sin la intervención de los usuarios de esos sistemas.

Los gusanos a menudo explotan vulnerabilidades en sistemas operativos o software, pero también son capaces de distribuirse a través de archivos adjuntos de correo electrónico en los casos en que el gusano puede obtener acceso a la libreta de contactos en una máquina infectada.

Puede parecer un concepto básico, pero los gusanos son algunas de las formas de malware más exitosas y duraderas que existen. El gusano SQL Slammer de 15 años sigue causando problemas al activar los ataques DDoS, mientras que el gusano Conficker de 10 años todavía se encuentra entre las infecciones cibernéticas más comunes.

El brote de ransomware Wannacry del año pasado infectó más de 300,000 computadoras en todo el mundo, algo que hizo gracias al éxito de las capacidades de gusanos que lo ayudaron a propagarse rápidamente a través de redes infectadas y en sistemas sin parches.

¿Qué es el adware?

El objetivo final de muchos ciberdelincuentes es ganar dinero, y para algunos, el adware es la forma de hacerlo. El adware hace exactamente lo que dice: está diseñado para enviar anuncios maliciosos al usuario, a menudo de tal manera que la única forma de deshacerse de ellos es hacer clic en el anuncio. Para los cibercriminales, cada clic genera ingresos adicionales.

En la mayoría de los casos, los anuncios maliciosos no están ahí para robar datos de la víctima o causar daños al dispositivo, solo lo suficientemente molesto como para presionar al usuario a hacer clic repetidamente en ventanas emergentes. Sin embargo, en el caso de los dispositivos móviles, esto puede conducir fácilmente al agotamiento extremo de la batería o inutilizar el dispositivo debido a la afluencia de ventanas emergentes que ocupan toda la pantalla.El adware muestra anuncios emergentes intrusivos que no desaparecerán hasta que se haga clic en ellos.

¿Qué es una botnet?

Una botnet, abreviatura de red de robots, involucra a los ciberdelincuentes que usan malware para secuestrar en secreto una red de máquinas en números, que pueden variar desde un puñado hasta millones de dispositivos comprometidos. Si bien no es un malware en sí mismo, estas redes generalmente se crean infectando dispositivos vulnerables.

Cada una de las máquinas está bajo el control de una sola operación de ataque, que puede emitir comandos de forma remota a todas las máquinas infectadas desde un solo punto.

Al emitir comandos a todas las computadoras infectadas en la red zombie, los atacantes pueden llevar a cabo campañas coordinadas a gran escala, incluidos los ataques DDoS, que aprovechan el poder del ejército de dispositivos para inundar a una víctima con tráfico, abrumando su sitio web o servicio. hasta cierto punto se desconecta.

Otros ataques comunes llevados a cabo por botnets incluyen campañas de adjuntos de correo electrónico no deseado, que también se pueden utilizar para reclutar más máquinas

en la red, e intentos de robo de datos financieros, mientras que botnets más pequeñas también se han utilizado en intentos de comprometer objetivos específicos.

Las botnets están diseñadas para permanecer silenciosas y garantizar que el usuario sea completamente ajeno a que su máquina esté bajo el control de un atacante.

A medida que más dispositivos se conectan a Internet, más dispositivos se convierten en objetivos para las botnets. La infame botnet Mirai, que desaceleró los servicios de Internet a fines de 2016, fue parcialmente alimentada por dispositivos de Internet de las Cosas, que podrían conectarse fácilmente a la red gracias a su seguridad inherentemente deficiente y la falta de herramientas de eliminación de malware.

¿Qué es el malware minero de criptomonedas?

El aumento de alto perfil de bitcoin ha ayudado a impulsar la criptomoneda al ojo público. En muchos casos, las personas ni siquiera lo compran, sino que dedican una parte de la potencia informática de su red informática o sitio web a explotarlo.

Si bien hay muchos casos de usuarios de Internet que participan activamente en esta actividad en sus términos, es tan popular que la demanda ha ayudado a subir el precio de las tarjetas gráficas para juegos de PC, los ciberatacantes también están abusando de la minería de criptomonedas.

No hay nada oculto o ilegal en la minería de criptomonedas en sí mismo, pero para adquirir la mayor cantidad de moneda posible, ya sea bitcoin, Monero, Etherium u otra cosa, algunos ciberdelincuentes usan malware para capturar PC en secreto y ponerlas a trabajar en una botnet. , todo sin que la víctima sea consciente de que su PC se ha visto comprometida.

Se cree que una de las redes de criptomonedas cibercriminales más grandes, la botnet Smominru, consta de más de 500,000 sistemas y ha hecho que sus operadores tengan al menos $ 3.6 millones de dólares.

Por lo general, un minero de criptomonedas entregará código malicioso a una máquina de destino con el objetivo de aprovechar la potencia de procesamiento de la computadora para ejecutar operaciones de minería en segundo plano.

El problema para el usuario del sistema infectado es que su sistema puede ser ralentizado casi por completo por el minero usando grandes porciones de su poder de procesamiento, lo que para la víctima parece que está sucediendo sin ninguna razón.istock-bitcoin-and-other-currency.jpg

El aumento de la criptomoneda ha llevado a un aumento de los delincuentes que usan malware para extraerlo a través de sistemas comprometidos.

Las PC y los servidores de Windows se pueden usar para la minería de criptomonedas, pero los dispositivos de Internet de las cosas también son objetivos populares para comprometerse con el fin de adquirir fondos ilícitamente. La falta de seguridad y la naturaleza inherentemente conectada de muchos dispositivos IoT los convierte en objetivos atractivos para los mineros de criptomonedas, especialmente porque es probable que el dispositivo en cuestión haya sido instalado y quizás olvidado.

El análisis de Cisco Talos sugiere que un solo sistema comprometido con un minero de criptomonedas podría generar 0.28 Monero por día. Puede sonar como una pequeña cantidad, pero una red esclavizada de 2,000 sistemas podría agregar los fondos hasta $ 568 por día, o más de $ 200,000 al año.

¿Cómo se entrega el malware?

En el pasado, antes de la difusión generalizada de la World Wide Web, el malware y los virus debían ser entregados manualmente, físicamente, a través de un disquete o CD Rom.

En muchos casos, el malware todavía se entrega mediante el uso de un dispositivo externo, aunque hoy en día es más probable que se entregue mediante una unidad flash o una memoria USB. Hay instancias de memorias USB que se dejan en aparcamientos fuera de las organizaciones seleccionadas, con la esperanza de que alguien tome una por curiosidad y la conecte a una computadora conectada a la red.

Sin embargo, ahora es más común el malware que se entrega en un correo electrónico de phishing con cargas distribuidas como un archivo adjunto de correo electrónico.

La calidad de los intentos de correo electrónico no deseado varía ampliamente: algunos esfuerzos para entregar malware involucrarán a los atacantes con un esfuerzo mínimo, tal

vez incluso enviando un correo electrónico que contenga nada más que un archivo adjunto nombrado al azar.

En este caso, los atacantes esperan encontrar a alguien lo suficientemente ingenuo como para seguir adelante y hacer clic en los archivos adjuntos o enlaces de correo electrónico sin pensarlo, y que no tienen instalado ningún tipo de protección contra malware.

Una forma un poco más sofisticada de enviar malware a través de un correo electrónico de phishing es cuando los atacantes envían grandes cantidades de mensajes, alegando que un usuario ha ganado un concurso, necesita verificar su cuenta bancaria en línea, ha perdido una entrega, debe pagar impuestos o incluso es necesario asistir a la corte, y varios otros mensajes que, al verlos por primera vez, pueden atraer al objetivo a reaccionar instantáneamente.

Por ejemplo, si el mensaje tiene un archivo adjunto que explica (falsamente) que un usuario está siendo convocado a la corte, el usuario puede hacer clic en él debido a la descarga, abrir el archivo adjunto del correo electrónico, o hacer clic en un enlace, para obtener más información. Esto activa el malware, con los gustos de ransomware y troyanos a menudo entregados de esta manera.

Si los atacantes tienen un objetivo específico en mente, el correo electrónico de phishing puede adaptarse específicamente para atraer a las personas dentro de una organización, o incluso solo a un individuo. Es este medio de entregar malware que a menudo se asocia con las campañas de malware más sofisticadas.

Sin embargo, hay muchas otras formas de propagación del malware que no requieren la acción del usuario final, a través de redes y otras vulnerabilidades de software.

¿Qué es el malware sin archivos?

A medida que los ataques tradicionales de malware se ralentizan con tácticas de prevención, incluido el uso de sistemas antivirus o antimalware robustos, y los usuarios se vuelven cautelosos ante correos electrónicos inesperados y archivos adjuntos extraños, los atacantes se ven obligados a buscar otras formas de soltar sus cargas maliciosas.Un medio cada vez más común de esto es a través del uso de malware sin archivos. En lugar de depender de un método tradicional de compromiso, como descargar y ejecutar archivos maliciosos en una

computadora, que a menudo se pueden detectar mediante soluciones de software antivirus, los ataques se ejecutan de una manera diferente.

En lugar de requerir la ejecución de un archivo descartado, los ataques de malware sin archivos se basan en aprovechar exploits de día cero o lanzar scripts desde la memoria, técnicas que pueden usarse para infectar puntos finales sin dejar un rastro revelador.

Esto se logra porque los ataques utilizan los propios archivos y servicios confiables del sistema para obtener acceso a los dispositivos y lanzar actividades nefastas, todo mientras no se detecta porque el antivirus no registra irregularidades.

La explotación de la infraestructura del sistema de esta manera permite a los atacantes crear archivos y carpetas ocultos o crear secuencias de comandos que pueden utilizar para comprometer los sistemas, conectarse a redes y, finalmente, comandar y controlar servidores, lo que proporciona un medio para realizar una actividad sigilosa.

La naturaleza misma del malware sin archivos significa que no solo es difícil de detectar, sino también difícil de proteger por algunas formas de software antivirus. Pero puede ser útil garantizar que los sistemas estén parcheados, actualizados y que los usuarios restringidos no puedan adoptar privilegios de administrador.

¿Solo las PC con Windows reciben malware?

Hubo un tiempo en que muchos ingenuamente creían que solo los sistemas Microsoft Windows podían ser víctimas de malware. Después de todo, el malware y los virus se habían concentrado en estos, los sistemas informáticos más comunes, mientras que los que usaban otros sistemas operativos estaban libres de su alcance. Pero si bien el malware sigue siendo un desafío para los sistemas Windows, especialmente aquellos que ejecutan versiones anteriores e incluso obsoletas del sistema operativo, el malware está lejos de ser exclusivo de las PC de Microsoft

Malware de Mac

Durante muchos años, persistió el mito de que las Mac eran completamente inmunes a las infecciones maliciosas. A lo largo de los años 90, hubo algunas formas de malware que infectaron Macs, a pesar de estar diseñadas principalmente para sistemas Windows. Los

gustos de Concept y Laroux estaban a punto de infectar Macs usando programas de oficina de Microsoft.

Sin embargo, a mediados de los años 00, los atacantes habían comenzado a crear formas de malware específicamente diseñadas para atacar Apple Macs, y ahora, mientras que las máquinas Windows soportan la peor parte de los ataques de malware basados en computadoras y computadoras portátiles, las Macs ahora son objetivos regulares para el cibercrimen.

Ahora es normal que los investigadores de ciberseguridad descubran troyanos de puertas traseras, descargas de software comprometidas y ataques de ransomware dirigidos a sistemas Mac.

MacRansom es una forma de ransomware dirigido a Mac.

¿Qué es el malware móvil?

El auge de los teléfonos inteligentes y las tabletas en la última década ha cambiado fundamentalmente nuestra relación con Internet y la tecnología. Pero, como cualquier forma de nueva tecnología, los delincuentes pronto se dieron cuenta de que podían explotar los teléfonos inteligentes para su propio beneficio ilícito, y estos dispositivos móviles no solo contienen grandes cantidades de información personal, sino que incluso pueden permitir que los piratas informáticos supervisen nuestra ubicación.

Si hay un tipo de malware que puede infectar computadoras, ya sea un troyano, ransomware, ladrón de información o adware emergente, entonces los delincuentes han estado trabajando en amenazas de malware que pueden llevar a cabo las mismas tareas en los teléfonos inteligentes.

La cantidad de datos transportados en dispositivos móviles los convierte en un objetivo aún más valioso para los piratas informáticos, particularmente si un grupo de piratería sofisticado o una operación de espionaje respaldada por el estado está buscando comprometer un objetivo particular con el propósito de espiar.

Las capacidades inherentes de un teléfono inteligente significan que, en última instancia, es posible, con el uso del malware correcto, que esos grupos ubiquen físicamente los objetivos

o incluso escuchen conversaciones y les tomen fotos usando las capacidades de micrófono y cámara incorporadas en los teléfonos.

Desafortunadamente, muchas personas aún no se dan cuenta de que su teléfono móvil es algo que puede ser víctima de ataques cibernéticos, aunque pueden protegerse con buenas prácticas de usuario y software antivirus móvil.

¿Qué es el malware de Android?

Los teléfonos Android sufren la mayoría de los ataques de malware en los teléfonos inteligentes, con la mayor participación de Google en el mercado móvil y la naturaleza abierta del ecosistema, lo que lo convierte en un objetivo atractivo para los ciberdelincuentes.

Los atacantes pueden infectar a sus objetivos engañándolos para que descarguen aplicaciones maliciosas de tiendas de terceros y el malware a menudo ha llegado al mercado oficial de aplicaciones de Google Play.

Estas aplicaciones maliciosas a menudo están diseñadas para parecerse a herramientas o juegos útiles originales o, en algunos casos, imitan aplicaciones legítimas, como lo demuestra una versión falsa de WhatsApp que se descargó más de un millón de veces.

Sin embargo, si bien los piratas informáticos han utilizado la tienda Google Play para distribuir malware de Android, las campañas más sofisticadas diseñarán socialmente objetivos seleccionados para descargar malware con fines de espionaje en su dispositivo.Se sabe que el malware de Android se hace pasar por aplicaciones legítimas dentro de Play Store; esta se disfraza como un limpiador que le dice al usuario que necesita descargar una actualización maliciosa adicional.Imagen: ESET

¿Puede mi iPhone infectarse con malware?

Cuando se trata de iPhone, el ecosistema está mucho más protegido contra el malware debido al enfoque de jardín cerrado de Apple para las aplicaciones.

Sin embargo, aunque el malware en iPhones es raro, no es una entidad desconocida: las pandillas de piratas informáticos han encontrado formas de comprometer los dispositivos de objetivos seleccionados en campañas de espionaje, como aquellos que explotaron las

vulnerabilidades de Trident para instalar el spyware Pegasus para espiar los derechos humanos. activistas en el Medio Oriente.

¿Qué es el malware de Internet de las cosas?

Como ha demostrado el aumento del malware en dispositivos móviles, si algo está conectado a Internet, es una posible vía de ataques cibernéticos.

Entonces, si bien el auge de los dispositivos conectados a Internet de las cosas ha traído una serie de beneficios para los usuarios, en la industria, el lugar de trabajo y el hogar, también ha abierto las puertas a nuevos esquemas de ciberdelincuencia.

La prisa por subirse al tren de IoT significa que algunos dispositivos se apresuran sin pensar en la seguridad cibernética, lo que significa que sigue siendo relativamente simple para los piratas informáticos infectar dispositivos conectados, que van desde sistemas de control industrial, hasta productos para el hogar e incluso juguetes para niños.

Uno de los medios más comunes en los que se explota la inseguridad de los dispositivos IoT es con ataques de malware que infectan secretamente productos y los conectan a una botnet.

Los dispositivos como enrutadores, sistemas de iluminación inteligentes, videograbadoras y cámaras de vigilancia pueden infectarse fácilmente y el daño eventual puede ser espectacular, como lo demuestra el caos en línea causado por el ataque DDoS de la botnet Mirai.

La red de dispositivos infectados por Mirai consistía en gran parte de productos IoT y era tan poderosa que detuvo grandes extensiones de Internet, ralentizó o impidió el acceso a una serie de servicios populares.

Si bien los dispositivos infectados con Mirai continuaron funcionando normalmente, ese no fue el caso para aquellos que encontraron sus productos IoT infectados con BrickerBot, una forma de malware IoT que resultó en que el Equipo de Respuesta a Emergencias Cibernéticas (CERT) de Homeland Security emitiera nuevas advertencias. Los dispositivos infectados con BrickerBot tienen su almacenamiento dañado, lo que los hace completamente inutilizables e irrecuperables.

Al igual que los hackers pueden convertir los teléfonos móviles en dispositivos de vigilancia, lo mismo puede decirse de las cámaras conectadas a Internet en el hogar. Ya ha habido una serie de casos en los que se ha descubierto que la seguridad de la cámara IoT es tan básica que el malware ha infectado una gran cantidad de dispositivos.

A diferencia de los teléfonos móviles, los dispositivos IoT a menudo se enchufan y se olvidan, con el riesgo de que la cámara IoT que configuró pueda ser fácilmente accesible para los extraños, que podrían usarla para espiar sus acciones, ya sea en su lugar de trabajo o en su casa.

Tal es el alcance de la preocupación de seguridad con el IoT, la policía advirtió sobre las amenazas que representan los dispositivos conectados, mientras que los organismos gubernamentales están trabajando para encontrar formas de legislar los dispositivos IoT más temprano que tarde, por lo que no nos queda un legado tóxico de miles de millones de dispositivos que pueden infectarse fácilmente con malware.boiling-kettle.jpg

Los objetos cotidianos se conectan cada vez más a Internet de las cosas, y son un objetivo atractivo para el malware.Imagen: iStock

El malware como herramienta para la guerra cibernética internacional

Con las evidentes capacidades ofensivas del malware, no es de extrañar que se haya convertido en una herramienta común en el oscuro mundo del espionaje internacional y la guerra cibernética.

Es especialmente útil para aquellos involucrados en el juego de la geopolítica porque actualmente, a diferencia del caso con las armas convencionales, todavía no hay reglas o acuerdos que detallen quién puede y quién no puede ser objetivo de las armas cibernéticas.

Que la atribución de los ataques sigue siendo tan difícil también hace que el ciberespionaje sea una herramienta crucial para los estados-nación que desean mantener sus actividades en secreto.

Stuxnet es generalmente considerado como la primera instancia de malware diseñado para espiar y subvertir los sistemas industriales y en 2010 se infiltró en el programa nuclear de Irán, infectando centrífugas de uranio y sistemas irreparablemente dañinos. El ataque ralentizó las ambiciones nucleares de Irán durante años.

Si bien ningún estado ha tomado oficialmente el crédito por los ataques, se cree que Stuxnet fue obra de las fuerzas cibernéticas estadounidenses e israelíes.

Desde esa primera instancia de ataques de malware reportados públicamente por estados nacionales, la guerra cibernética se ha convertido en una herramienta utilizada por los gobiernos de todo el mundo. Se sospecha ampliamente que los actores de los estados nacionales estaban detrás de los ataques contra una planta de energía de Ucrania, pero no son solo los sistemas físicos y la infraestructura los objetivos de la guerra cibernética.

Mientras tanto, los actores de todos los lados de las divisiones diplomáticas continúan emprendiendo campañas de ciberespionaje contra objetivos potencialmente útiles.

¿Cómo se protege contra el malware?

Algunas de las prácticas de seguridad cibernética más básicas pueden ayudar en gran medida a proteger los sistemas, y a sus usuarios, de ser víctimas de malware.

Simplemente garantizar que el software esté parcheado y actualizado, y que todas las actualizaciones del sistema operativo se apliquen lo más rápido posible después de su lanzamiento, ayudará a proteger a los usuarios de ser víctimas de ataques con ataques conocidos.

Una y otra vez, los retrasos en los parches han llevado a las organizaciones a ser víctimas de ataques cibernéticos, lo que podría haberse evitado si los parches se hubieran aplicado tan pronto como fueron liberados.

Una de las razones por las cuales el Servicio Nacional de Salud del Reino Unido se vio tan afectado por el brote de WannaCry fue porque, a pesar de las advertencias de que deberían aplicarse, grandes extensiones de sistemas no habían sido parcheadas semanas después de que una actualización de seguridad para proteger contra el exploit EternalBlue estuviera disponible .

También es común que las campañas de ciberespionaje aprovechen las vulnerabilidades para las que han existido soluciones durante mucho tiempo y todavía comprometen con éxito los objetivos, porque nadie se molestó en aplicar los parches. La lección que se debe

aprender aquí es que a veces puede parecer lento e inconveniente aplicar parches, especialmente en toda una red, pero puede resultar una barrera efectiva contra el malware.

Instalar alguna forma de software de ciberseguridad también es un medio útil de protección contra muchas formas de ataque. Muchos proveedores actualizarán sus programas con nueva inteligencia de amenazas, que se aplica para buscar y detectar nuevo malware de forma semanal o incluso diaria, proporcionando la mayor protección posible contra el malware, en caso de que algo intente ingresar al sistema.

Por ejemplo, los visitantes de los sitios de abrevaderos deben estar protegidos de los ataques, mientras que los archivos sospechosos o peligrosos recibidos por correo electrónico pueden ser puestos en cuarentena.

También se debe ofrecer capacitación a los usuarios para garantizar que todos los que usan su red conozcan las amenazas cibernéticas que podrían enfrentar en Internet.

Enseñar a los usuarios sobre la navegación segura y los peligros de los correos electrónicos de phishing, o tener cuidado con lo que descargan y hacen clic, puede ayudar a evitar que las amenazas lleguen incluso a ser descargadas. Los usuarios reciben muchas críticas de algunos como una debilidad en la ciberseguridad, pero también pueden formar la primera línea de defensa contra los ataques de malware.