Las 7 etapas de las amenazas avanzadas y el robo de datos

¿A qué debe prestar atención?

1. Reconocimiento
Recopilación de información en línea para construir señuelos dirigidos

2. Señuelo
Dos tipos: correo electrónico y Web

3. Redirección
El usuario es dirigido a un servidor oculto.

4. Kit de explotación
El sistema del usuario es inspeccionado en busca de una vulnerabilidad abierta.

5. Archivo *dropper*
Si existe una vulnerabilidad, se envía un archivo que contiene malware.

6. Llamada 'a casa'
Llama a casa para extender el ataque con más malware.

7. Robo de datos
El delito cibernético busca datos para robar en los sistemas internos.

Etapas de las amenazas avanzadas

Etapa 1: Reconocimiento

La etapa inicial se centra en el reconocimiento. Los delincuentes informáticos que envían ataques dirigidos acceden a credenciales e investigan en línea perfiles, ID de correo electrónico, información sobre organigramas empresariales, pasatiempos e intereses en perfiles sociales para tener más información sobre sus víctimas. El objetivo es recabar inteligencia para construir señuelos que son muy personalizados y tienen una gran probabilidad de éxito.

Etapa 2: Señuelos

Los señuelos de la web se aprovechan de la curiosidad humana. Mediante una técnica de envenenamiento de los resultados del motor de búsqueda (SEO), mediante el uso de eventos de celebridades o desastres naturales comúnmente utilizados como señuelos, los atacantes han ingresado en los círculos sociales privados entre amigos dentro de las redes sociales.

Los correos electrónicos enviados como señuelos generalmente no tienen características sociales y no se basan en eventos particulares. Pueden traspasar sus defensas perimetrales de filtros antispam debido a que tienen formatos comunes. Los cinco temas más utilizados para señuelos de correo electrónico son: notificaciones de pedidos, confirmaciones de boletos, avisos de entrega, mensajes de correo electrónico de prueba e información sobre declaración de impuestos.

Los ataques dirigidos llegan en menor cantidad a personas determinadas (a menudo tratan sobre eventos conocidos o reuniones que se obtienen a través de perfiles sociales), mientras que los ataques masivos usan video, noticias o señuelos de celebridades en las redes sociales.

¿Qué tan satisfecho está usted con la capacidad de sus defensas actuales para analizar el contenido de los círculos sociales privados e identificar señuelos y proteger a los usuarios? ¿La inteligencia sobre amenazas se comparte y correlaciona entre la web y el correo electrónico? ¿Reconoce y refleja que el 92% del spam de correo electrónico posee una URL? En la actualidad, una buena defensa del correo electrónico comienza con una gran defensa de la web.

Etapa 3: Redirección

Los usuarios generalmente son dirigidos a una encuesta, una oferta de un falso antivirus o una página web falsa donde lo espera un kit de explotaciones. Las redirecciones maduras son inyecciones de SQL y de iFrame que conducen a los usuarios a ciegas por un camino a servicios web, contenido y, a menudo, a ofertas que no desean. El uso de malware en publicidades web (malvertising) también redirecciona a ciegas a los usuarios dentro de sitios populares. Las redirecciones más recientes incluyen publicaciones en muros en redes sociales, plug-in falsos, certificados falsos y javascript muy ofuscado.

El objetivo de una redirección ciega u oculta, o de un señuelo, es conducir a los usuarios por un camino deseado a una encuesta, una oferta de antivirus falso o una página web falsa para ser analizados por un kit de explotaciones. Como las redirecciones con frecuencia son dinámicas y cambian rápidamente, las defensas deben poder evaluar los vínculos web en tiempo real.

websense®

Etapa 4: Kits de explotaciones

Una de las etapas más poderosas y eficaces de una amenaza avanzada es el kit de explotaciones (p. ej., Blackhole). En el pasado, el objetivo era engañar a los usuarios, redireccionarlos por un camino y luego enviar un archivo de malware a sus sistemas. Esto lograba ser detectado rápidamente por los laboratorios de amenazas y, así, el ataque tenía una vida útil muy corta. Sin embargo, en unos pocos minutos o en una hora, muchas personas podían ser atacadas. El objetivo del kit de explotaciones es más similar al de un francotirador: disparar un tiro con un archivo que esparce malware únicamente cuando encuentra una puerta abierta a vulnerabilidades probadas. Si no encuentra ninguna vulnerabilidad abierta, redirecciona al usuario a una página web limpia y permanece oculto.

Entender los kits de explotaciones es importante para el análisis de amenazas avanzadas y el desarrollo de defensas en tiempo real. Blackhole utiliza cifrado criminal, que dificulta la detección con motores antivirus y herramientas de desofuscación genéricas. Si su única defensa en el gateway web es un antivirus, las probabilidades de que los kits de explotaciones logren ingresar en sus sistemas con éxito a través de aplicaciones vulnerables son muy altas.

Etapa 5: Archivos *dropper*

Esta etapa es la que la mayoría de las personas considera el foco de sus defensas que miran hacia adelante: analizar todos los archivos que ingresan en la red en busca de malware. El problema hoy es que los archivos *dropper* utilizan empaquetadores dinámicos para que no estén disponibles las firmas y los patrones conocidos; de este modo, muy pocos motores antivirus detectan los archivos *dropper* en el momento del análisis de amenazas.

¿Qué tiene usted además de antivirus para estar protegido contra las amenazas avanzadas y el robo de datos? Uno de los archivos *dropper* más populares es un antivirus falso, o el escaneo y la oferta falsos para limpiar su sistema. Aunque tradicionalmente estaban centrados en los sistemas de Windows, ahora se están viendo nuevas versiones en computadoras Apple con nombres como *Mac Defender o Protector.*

Etapa 6: Llamada ‘a casa’

Esta etapa y la siguiente sugieren que ningún conjunto de defensas es 100% eficaz y que la contención es la nueva defensa para estar protegido contra el robo de datos. El delito cibernético únicamente necesita un punto de entrada a una red para comenzar una infiltración que tiene por objeto el robo de datos.

Para cualquier ataque exitoso en línea, es habitual llamar ‘a casa’ para acceder a descargas y herramientas de malware y para enviar información de vuelta a los sistemas infectados. El problema es que la mayoría de las defensas están enfocadas únicamente hacia adelante y no analizan el tráfico saliente en busca de sistemas infectados. El uso de DNS dinámicos es un método común de ataque para evitar la detección de la llamada a casa en direcciones estáticas. Sin embargo, también se presta a una nueva defensa para el análisis de la llamada ‘a casa’. Los sistemas infectados y las redes bots que llaman a servidores de comando y control son bloqueados y no pueden utilizar DNS dinámicos mientras los usuarios pueden optar por continuar en sitios confiables. El reconocimiento de la ubicación geográfica es otra defensa contra la llamada ‘a casa’; sin embargo, las comunicaciones de malware, el hospedaje y el phishing están principalmente dentro de los Estados Unidos, dominios que pocas políticas bloquearán. También se está utilizando el reconocimiento del destino en el contexto de la prevención de la pérdida de datos. El análisis contextual de los datos, el usuario, el destino y otras variables es una ventaja para las políticas; de este modo, la información confidencial no es enviada al correo web personal o a las cuentas de redes sociales ni se publica en aplicaciones de almacenamiento privado en la nube.

¿Qué defensas posee usted que analicen el tráfico saliente en busca de comunicaciones de amenazas avanzadas que llaman ‘a casa’?

Etapa 7: Robo de datos

Esto es precisamente lo que buscan los atacantes. La capacidad para contener un ataque y detener el robo de datos plantea muchos interrogantes. ¿Sus defensas pueden detectar archivos con contraseña que salen de su red o el uso de cifrado criminal en archivos salientes? También hay que tener en cuenta el robo de datos donde la información confidencial se exporta en pequeños volúmenes (escapes) a pedido para evitar la detección durante un período de tiempo definido. ¿Sus defensas contra el robo de datos le proporcionan informes forenses que muestran qué datos fueron bloqueados y se les impidió salir de su organización?

Para obtener más información sobre cómo Websense puede proteger a su organización, visite www.websense.com/triton7siete

websense