Ataques a la cadena de suministro

Datos básicos

DESCRIPCIÓN

Los ataques a la cadena de suministro pertenecen a dos categorías principales: estafa de correo electrónico y software de terceros. En estos ataques, los ciberdelincuentes comprometen a distribuidores o proveedores de servicios para poder atacar posteriormente a sus clientes y partners. El compromiso inicial del proveedor se realiza a menudo mediante ataques de phishing o malware. Una vez dentro del sistema del proveedor, los ciberdelincuentes pueden suplantar cuentas de correo electrónico para iniciar el ataque de phishing, fraude de facturas u otros tipos de ataque contra los clientes. Una vez que los atacantes han conseguido infiltrarse en los sistemas de los clientes, pueden robar datos confidenciales, instalar ransomware o utilizar el acceso para desencadenar una nueva oleada de ataques de phishing o estafas por correo electrónico.

HERRAMIENTAS EN EL MERCADO

Las amenazas contra la cadena de suministro incluyen normalmente phishing de credenciales (usurpación de cuentas), malware (Stuxnet, NotPetya, Sunburst, Kwampirs) y amenazas de impostores, como las estafas Business Email Compromise (BEC).

TIPOS

- **Business Email Compromise (BEC, o estafa por correo electrónico).** Los ciberdelincuentes se hacen pasar por alguien en quien confía el destinatario, por lo general un partner comercial, un distribuidor o un proveedor. Piden al destinatario que realice una transferencia bancaria, pague una factura falsa o alterada, desvíe fondos de nóminas o cambie los datos bancarios para futuros pagos. En algunas estrategias de estafas por correo electrónico, el ciberdelincuente puede comprometer la cuenta de correo electrónico real del proveedor para hacerse pasar por él e incluso incorporarse a conversaciones de correo electrónico existentes.

- **Ataques a la cadena de suministro de software.** Los ciberdelincuentes consiguen acceder a los sistemas de un proveedor de servicios gestionados o de software e infectan futuras compilaciones que después se distribuyen a clientes y partners. Estos ataques son poco habituales comparados con los señalados anteriormente, pero pueden afectar a un gran número de víctimas en un solo incidente.

FACTORES DE RIESGO

- Contratar a proveedores en servicios profesionales y de consultoría.
- No emplear la protección de ciberseguridad adecuada.
- Facilitar acceso a personal negligente o sin formación de concienciación en seguridad.
- Complejidad de la cadena de suministro. Las empresas recurren cada vez más a una variedad de plataformas cloud y servicios SaaS.

Noticias sobre ataques a la cadena de suministro

Target tendrá que pagar 18,5 M$ por una fuga de datos de 2013 que afectó a 41 millones de consumidores

Las credenciales robadas a un proveedor de Target permitieron a los ciberdelincuentes infiltrarse en los sistemas del gigante del comercio minorista y robar datos de pago confidenciales de más de 41 millones de clientes.

Los hackers atacan la cadena de suministro de las vacunas contra la COVID-19

Ataque de phishing contra ejecutivos de 44 empresas de varios continentes en un intento de comprometer la cadena de suministro mundial de la vacuna contra la COVID-19.

La ONG Red Kit Community Housing sufre la pérdida de 1,2 millones de dólares en una estafa de tipo BEC

Los ciberdelincuentes falsificaron el dominio de un proveedor para robar casi 1 millón de libras esterlinas en alquileres de una asociación de viviendas cooperativas cerca de Londres en el Reino Unido.

Anatomía de un ataque a la cadena de suministro

1. **Infiltración**

   Los agresores utilizan una gran variedad de métodos para la infiltración inicial:

- Ataques por fuerza bruta con herramientas automatizadas para intentar combinaciones de nombre de usuario y contraseña hasta encontrar una coincidencia.

- Suplantar a un contacto de confianza para enviar phishing, mensajes de impostores o enlaces/adjuntos con malware, como registradores de pulsaciones o ladrones de contraseñas.

- Usurpación de la cuenta de un proveedor de confianza.

2. **Reconocimiento**

- Una vez que el ciberdelincuente ha robado credenciales de inicio de sesión válidas, puede empezar a aprovechar la red y la reputación del distribuidor. Supervisan las comunicaciones entre el proveedor y sus clientes en busca de posibles objetivos.

3. **Ataque**

- Una vez finalizado el reconocimiento, el atacante puede utilizar los sistemas del proveedor comprometido para apoderarse de credenciales, remitir facturas fraudulentas o enviar malware a los clientes.

Datos de investigación

Durante un período de una semana en febrero de 2021, Proofpoint analizó datos de 3000 organizaciones de un gran número de sectores en EE. UU., Reino Unido y Australia. Durante ese tiempo, la gran mayoría sufrió ataques a la cadena de suministro.

98 % recibió una amenaza de un proveedor al que habían suplantado o comprometido.

Los ataques fueron igualmente probables en todos los países y sectores de la muestra.

De esas amenazas, en casi tres cuartos se utilizó phishing o suplantación.

<30 % de los mensajes de correo electrónico enviados desde dominios de proveedores contenían malware.

CÓMO HA CONTRIBUIDO EL DELITO COMO SERVICIO A LOS ATAQUES A LA CADENA DE SUMINISTRO

La Internet oscura (Dark Web) es un conocido mercado de kits de exploits y malware personalizado que se emplea para vender servicios como alquileres de redes de bots y software para lanzar ataques de ransomware. Como en el caso de la mayoría de los proveedores SaaS, los ciberdelincuentes proporcionan herramientas y plataformas para llevar a cabo ataques a la cadena de suministro, de ransomware y otros tipos de ciberdelitos. Incluso sin conocimientos técnicos avanzados, ahora los ciberdelincuentes pueden lanzar ataques fácilmente.

Cómo proteger su organización

Para hacer frente al fraude de la cadena de suministro y a los ataques a la cadena de suministro de software ofrecemos algunos controles de seguridad fundamentales que deberían considerar las organizaciones.

Fraude de la cadena de suministro

El fraude de facturas de proveedores es de largo el ataque BEC más sofisticado, ya que combina la suplantación de la identidad proveedor y el aprovechamiento de cuentas comprometidas de ese proveedor.

Las estafas BEC a menudo se inician por un mensaje de correo electrónico de una persona de confianza o que usurpa su identidad después de comprometer su cuenta. Las estafas BEC no tienen payload (carga maliciosa), por lo que resultan muy difíciles de detectar para las gateways tradicionales, que solo se basan en la reputación y en el análisis en entorno aislado (sandbox).

Estas son las medidas que se pueden adoptar para detener los ataques más comunes (y costosos) a la cadena de suministro.

Visibilice los riesgos de fraude contra la cadena de suministro

Para comprender, comunicar y reducir mejor los riesgos responda a las siguientes preguntas:

- ¿Cuáles son los riesgos de ataques BEC a los que nos exponemos?
- ¿Qué usuarios son los más vulnerables?
- ¿Qué proveedores ponen en riesgo nuestras actividades?
- ¿Qué deberíamos hacer para reducir los riesgos?

Debería saber quiénes son los usuarios más atacados de su empresa mediante amenazas de impostores y quiénes son los más susceptibles de caer en la trampa de estas estafas.

Al mismo tiempo, disponer de una visibilidad granular de los detalles de las amenazas BEC e identificar los temas de estafas BEC más comunes, como el fraude mediante facturas de proveedores y el desvío de nóminas, puede ayudarle a conocer y comunicar los riesgos de ataques BEC.

Detecte y bloquee las amenazas de impostores antes de que se infiltren en su entorno

Detener los ataques contra proveedores que se llevan a cabo a través del correo electrónico significa identificar todas las tácticas de estafa por correo electrónico, incluida la falsificación de display names, el uso de "lookalike domains" (dominios parecidos) y el fraude sofisticado de proveedores. Busque una solución que analice los mensajes de forma dinámica en busca de distintas tácticas asociadas con el fraude mediante facturas de proveedores, por ejemplo:

- Cambios de la dirección de respuesta
- Uso de direcciones IP maliciosas
- Uso de dominios de proveedores cuya identidad ha sido usurpada
- Palabras o frases empleadas habitualmente en ataques de fraude de proveedores

(La mayoría de las soluciones de protección del correo electrónico se basan en reglas estáticas o en datos contextuales limitados que requieren una optimización manual).

El fraude de facturas de proveedores es de largo el ataque BEC más sofisticado, ya que combina la suplantación de la identidad proveedor y el aprovechando de cuentas comprometidas de ese proveedor.

Mejore de la resiliencia de los usuarios frente a los ataques BEC a la cadena de suministro

Los ataques BEC se dirigen contra las personas y dependen de ellas para que, sin saberlo, lleven a cabo los ataques. Los ataques de impostores recurren a la ingeniería social y a la suplantación de la identidad, y por eso los usuarios constituyen a menudo su última línea de defensa. Esa es la razón por la que la reducción de riesgos de ataques BEC requiere a la vez tecnología y formación.

Prepare a sus usuarios para que identifiquen y denuncien los mensajes de correo electrónico de impostores. Esto les ofrecerá la posibilidad de adquirir los conocimientos y competencias necesarias para proteger su empresa contra estas amenazas activadas por personas.

Las etiquetas de advertencias de correo electrónico pueden ayudarle a identificar el riesgo que presenta cada mensaje. Por ejemplo, advertir a los usuarios cuando un mensaje procede de un remitente externo o de un dominio registrado recientemente les ayuda a tomar decisiones más informadas respecto a los mensajes sobre los que tienen dudas.

Proteja su marca del uso en estafas por correo electrónico

Las mismas preocupaciones que tiene su empresa respecto al riesgo que pueden presentar sus proveedores, las tienen sus clientes respecto a su empresa.

Los ciberdelincuentes pueden perjudicar su relación con sus clientes y partners comerciales utilizando el nombre y la marca de su empresa para robarles dinero. Aunque la falsificación de la marca no genera necesariamente pérdidas económicas a su empresa, puede dañar su reputación, erosionar la confianza de los clientes y en última instancia perjudicar seriamente a su empresa.

Impida que se envíen mensajes de correo electrónico fraudulentos empleando la certificación de correo DMARC, ya sea directamente por su empresa o a través de un tercero designado.

Ataques a la cadena de suministro de software

Además de los ataques a la cadena de suministro más comunes mencionados anteriormente, el uso cada vez mayor de software externo y gestionado ha creado un tipo adicional de riesgo para la cadena de suministro.

Si un proveedor comprometido proporciona software o servicios cloud, los ciberdelincuentes pueden alterar el código fuente e inyectar malware en el proceso de compilación o de actualización. A partir de ahí los programas o servicios infectados se distribuyen a clientes y partners, junto con la payload maliciosa incluida por el atacante.

Los usuarios suelen carecer de la capacidad para inspeccionar los programas de terceros que utilizan, lo que significa que deben confiar en que sus proveedores y distribuidores de software tengan las protecciones adecuadas. Si se suministra software comprometido a una organización, esta puede ser susceptible de sufrir una amplia gama de ataques, desde robo de datos a infecciones de ransomware.

Este tipo de ataques es especialmente difícil de prevenir. Las vulnerabilidades en software al que no se han aplicado los parches adecuados son uno de los vectores más comunes de ciberataque, por lo que la actualización de software a la última versión se recomienda como una de las mejores prácticas. Sin embargo, ahora también es un vector de ataque.

Más información

En un momento en el que los ataques a la cadena de suministro dominan titulares, parece claro que los servicios proveedores y contratistas externos presentan un riesgo grave para la seguridad de las organizaciones. Una solución de seguridad centrada en las personas que detecte nuevas herramientas, objetivos y tácticas de ataques puede ayudar a reducir ese riesgo.

Para obtener más información sobre cómo puede detener eficazmente los ataques a la cadena de suministro, visite **www.proofpoint.com/es**.

ACERCA DE PROOFPOINT

Proofpoint, Inc. es una compañía líder en ciberseguridad y cumplimiento de normativas que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentra el 75 % del Fortune 100, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en **www.proofpoint.com/es**.