Ataques de cadena de suministro ¿Qué son? ¿Cómo protegernos?

Los **ataques de cadena de suministro** son una ciberamenaza menos conocida por el público en general, pero tienen el potencial de causar daños graves y a gran escala. En este artículo explicaremos qué son los ataques de cadena de suministro, cómo funcionan y cómo podemos protegernos.

En este artículo hablamos de: [ocultar]

¿Qué es un ataque de cadena de suministro?

Antes de explicar qué es un ataque de cadena suministro, empecemos definiendo qué es la cadena de suministro dentro del contexto de la informática y la ciberseguridad.

En este caso, la cadena de suministro la forman los proveedores de servicios digitales externos, como pueden ser los proveedores de Internet, los proveedores de software o hardware, etc., que cualquier empresa u organismo público actual puede contratar para llevar a cabo diferentes tipos de funciones y tareas o para dar a su vez determinados servicios a sus propios clientes.

En la actualidad, la creación de un producto de software o hardware puede depender de la interacción de diferentes fabricantes y desarrolladores y es habitual que el cliente habitual no sea consciente de cuántos actores están detrás de la fabricación de su ordenador, de su móvil o del programa que utiliza para trabajar en remoto.

Por lo tanto, un ataque de cadena de suministro, o ***supply chain attack*** como se denomina en inglés, es aquel ataque capaz de comprometer a los propios proveedores de servicios digitales externos, afectando, a través de ello, a un gran número de usuarios intermedios o finales del servicio contratado.

Los **ciberataques de cadena de suministro** son un medio utilizado para desplegar después otros ciberataques en los usuarios intermedios y finales, como por ejemplo, un ataque del ransomware Sodinokibi (https://protecciondatos-lopd.com/empresas/sodinokibi/) o implementar herramientas maliciosas que permitan el robo de información (https://protecciondatos-lopd.com/empresas/robo-datos-informaticos/) confidencial.

¿Cómo funcionan los ataques de cadena de suministro?

Cuando un grupo de cibercriminales se pone como objetivo realizar un ataque de cadena de suministro, buscará el eslabón más débil de dicha cadena, aquel que «menos esfuerzo» le requiera para instalar su método de ataque. Lo habitual es que busquen protocolos de red no seguros, servidores desprotegidos o con medidas de protección insuficientes o cualquier vulnerabilidad que les permita insertar sus herramientas maliciosas.

Generalmente, se insertan códigos maliciosos en el software para ocultar el malware que después se usará para atacar a los usuarios intermedios o finales del programa infectado. Puesto que el software o la actualización de software proviene del proveedor de confianza, y están firmados y certificados, los clientes y usuarios descargan el programa sin saber que de paso están instalando un malware en sus sistemas y abriendo la puerta a los cibercriminales.

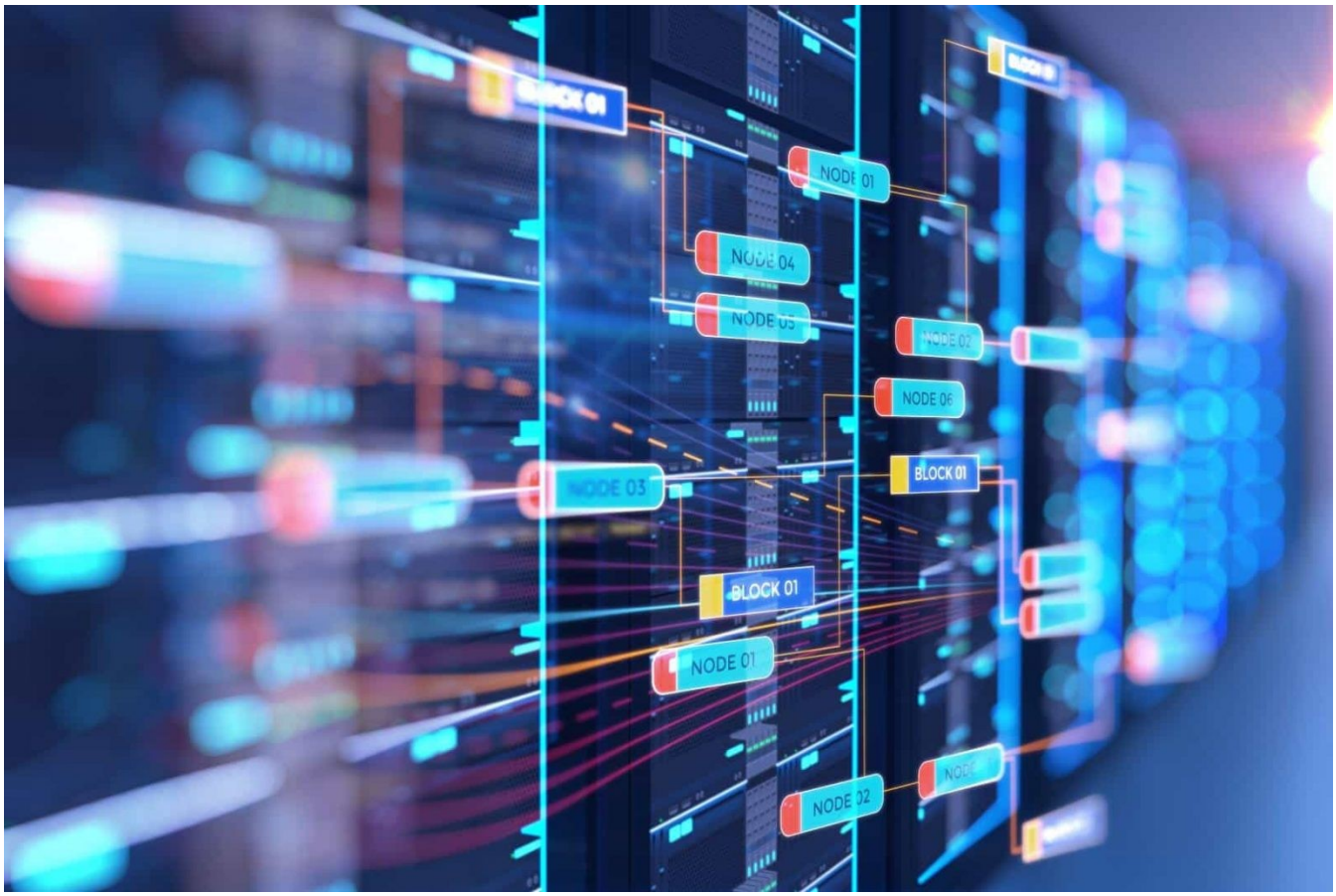
Normalmente, los proveedores no son conscientes de que sus programas, aplicaciones o actualizaciones han sido comprometidas, hasta que ya es demasiado tarde.

Tipos de ataques de cadena de suministro

Existen varias formas de realizar **ataques a la cadena de suministro**, los más habituales son los siguientes:

- Insertar código malicioso en software, en programas instaladores o actualizaciones de software.

- Instalación de componentes maliciosos en el hardware (por ejemplo, un chip, como ocurrió con las placas base que fabricaba SuperMicro, en las que se detectó un chip que no figuraba en el diseño).
- Creación de software malicioso que se usa para crear otros software.
- Código malicioso firmado con las claves privadas del proveedor de servicio.
- Ataques backdoor en hardware y software.
- Malware instalado en dispositivos externos que se conectan en algún momento a la red interna.



¿Por qué es tan peligroso el ciberataque a la cadena de suministro?

El ataque de cadena de suministro resulta especialmente peligroso por el potencial que tiene para afectar a miles de víctimas, puesto que los servicios o productos infectados

pueden estar contratados por varias empresas, que a su vez ofrecen ese servicio o producto o uno distinto, pero que hace uso de este, a sus clientes.

Así, si la función del código malicioso es habilitar una puerta trasera en un software oficial, para después, a través de ella, poder acceder a los sistemas de todas las víctimas que han instalado ese software, el daño que se puede causar es exponencial.

Además, como ya dijimos, el ataque de cadena de suministro funciona como un medio para desplegar otro tipo de ataques, por ejemplo, desplegando una herramienta para el cifrado de datos (https://protecciondatos-lopd.com/empresas/cifrado-datos/) y provocando el consecuente ataque de ransomware (https://protecciondatos-lopd.com/empresas/ransomware/). O conseguir robar información sensible de las víctimas.

Ejemplos más recientes de ataque de cadena de suministro

Son varios los ejemplos de ataques de cadena de suministro que han ocurrido en los últimos años, pero uno de los más sonados y recientes fue el sufrido por la empresa SolarWinds.

Uno de los productos que comercializa esta compañía es una plataforma de monitoreo de redes informáticas llamada Orion. En algún momento, alguien consiguió vulnerar la seguridad de la compañía y crear una versión de Orion que incluía un malware, al que una de sus víctimas, la empresa de seguridad FireEye, bautizó como Sunburst.

Esta versión infectada de Orion la descargaron en torno a 18.000 clientes de SolarWinds en todo el mundo, confiando en el origen oficial de la descarga. Las infraestructuras de todos estos clientes se vieron inmediatamente comprometidas, dejando «al descubierto» redes internas, correos electrónicos, bases de datos, etc. Los clientes de SolarWinds en su mayoría son otras empresas, como la citada FireEye o Microsoft, y organismos públicos, como el Departamento de Justicia de EE. UU.

Pero el primer ataque que llamó la atención sobre la cadena de suministro, fue el sufrido por Target en 2013, cuando sus puntos de venta se vieron comprometidos por un malware que robaba los datos de las tarjetas de crédito de sus clientes. Los cibercriminales consiguieron acceder a la red de Target a través de credenciales robadas o filtradas de la empresa que se ocupaba del mantenimiento de sus sistemas de aire acondicionado.

¿Cómo protegerse de un ataque de cadena de suministro? Consejos

A nivel de usuario poco podemos hacer para protegernos de un ataque de cadena de suministro, más allá de contar con las medidas de seguridad habituales, pero que probablemente sean insuficientes para frenar el ataque. Depende de cada actor de la cadena de suministro el reforzar la seguridad de sus sistemas para evitar esas inserciones de códigos maliciosos o malware en sus productos.

Para ello se recomienda a las empresas y organismos públicos asegurarse de que sus proveedores de servicios cuentan con las medidas de seguridad necesarias para prevenir este tipo de ataques. En ese sentido, se recomienda también auditar la propia cadena de suministro, saber qué empresas se tienen contratadas y evaluar qué nivel de acceso a la red propia tienen.

También es recomendable enfocar adoptar un enfoque de seguridad proactivo, es decir, contar con herramientas y soluciones de seguridad que detecten y prevengan los ataques antes de que estos se produzcan.

Monitorear la red y los sistemas en tiempo real y comprobar comportamientos sospechosos, como pueden ser el uso de credenciales fuera del horario laboral o el abuso de las herramientas de administración del sistema, puesto que son señales inequívocas de que alguien ajeno a la compañía podría haber entrado en sus sistemas y estar

moviéndose por ellos.

Además, reforzar la propia seguridad con medidas como la autenticación multifactor, implementar políticas privilegios mínimos tanto para empleados como para proveedores, mantenerse informado sobre alertas de brechas de seguridad que afecten a sus proveedores, actualizar siempre los sistemas para solucionar vulnerabilidades, entre otras.

Grupo Atico34 es una consultora especializada en Protección de Datos, Igualdad, Propiedad Intelectual y Compliance.

P° de la Castellana, 95, 15
28046 - Madrid

grupo@atico34.com (mailto:grupo@atico34.com)

914 896 419 (tel:914896419)

Soluciones

Protección de Datos (https://protecciondatos-lopd.com/auditoria/proteccion-datos/)

DPO (https://protecciondatos-lopd.com/delegado-proteccion-datos-precios/)

Compliance (/auditoria/cumplimiento-normativo/)

Igualdad (https://protecciondatos-lopd.com/auditoria/consultora-igualdad/)

Propiedad Intelectual (https://protecciondatos-lopd.com/consultoria/propiedad-intelectual-industrial/)

IT Services (https://protecciondatos-lopd.com/consultoria/tic/)

Ciberseguridad (https://protecciondatos-lopd.com/consultoria/ciberseguridad/)

More

Partners (https://protecciondatos-lopd.com/partners/)

Blog (https://protecciondatos-lopd.com/prensa/>Prensa
 <a href=)

System status (https://protecciondatos-lopd.com/status/)

Contacto (https://protecciondatos-lopd.com/contacto/)

Oficinas (https://protecciondatos-lopd.com/oficinas/) Madrid (https://protecciondatos-lopd.com/madrid/) Barcelona (https://protecciondatos-lopd.com/barcelona/) Valencia (https://protecciondatos-lopd.com/valencia/) Bilbao (https://protecciondatos-lopd.com/bilbao/) Zaragoza (https://protecciondatos-lopd.com/zaragoza/) Mallorca (https://protecciondatos-lopd.com/mallorca/) Sevilla (https://protecciondatos-lopd.com/sevilla/) Málaga (https://protecciondatos-lopd.com/malaga/) Asturias (https://protecciondatos-lopd.com/asturias/)