EUROPEAN UNION AGENCY
FOR CYBERSECURITY

INFORME «PANORAMA DE AMENAZAS» DE LA ENISA RELACIONADAS CON ATAQUES A LA CADENA DE SUMINISTRO

JULIO DE 2021

ACERCA DE LA ENISA

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) es la agencia de la Unión cuyo objetivo es alcanzar un elevado nivel común de ciberseguridad en toda Europa. Creada en 2004 y reforzada mediante el Reglamento sobre la Ciberseguridad de la UE, la Agencia de la Unión Europea para la Ciberseguridad contribuye a la política de seguridad cibernética de la UE, mejora la fiabilidad de los productos, servicios y procesos de TIC mediante programas de certificación de la ciberseguridad, coopera con los Estados miembros y con los organismos de la UE y ayuda a Europa a prepararse para los desafíos del día de mañana en materia de ciberseguridad. A través del intercambio de conocimientos, el desarrollo de capacidades y las campañas de sensibilización, la Agencia coopera con sus partes interesadas clave para fortalecer la confianza en la economía conectada, para impulsar la resiliencia de la infraestructura de la Unión y, por último, para proteger digitalmente a la sociedad y a la ciudadanía de Europa. Para más información sobre la ENISA y su trabajo, puede consultar: www.enisa.europa.eu.

CONTACTO

Si desea ponerse en contacto con los autores, rogamos escriba a etl@enisa.europa.eu.
Las consultas de los medios de comunicación acerca de este informe deben realizarse a través de press@enisa.europa.eu.

EDITORES

Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras, Agencia de la Unión Europea para la Ciberseguridad
Sebastián García, Verónica Valeros, Universidad Técnica Checa en Praga

AGRADECIMIENTOS

Nos gustaría dar las gracias a los miembros y observadores del Grupo de Trabajo ad hoc de ENISA sobre el panorama de amenazas cibernéticas por su valiosa información y comentarios para validar este informe. También queremos agradecer a Volker Distelrath (Siemens) y Konstantinos Moulinos (ENISA) por sus comentarios.

AVISO LEGAL

MENCIÓN DE COPYRIGHT

ISBN: 978-92-9204-509-8 – DOI: 10.2824/168593

ÍNDICE

RESUMEN EJECUTIVO

Los ataques a la cadena de suministro han sido un problema de seguridad durante muchos años, pero parece que la comunidad se enfrenta a un mayor número de ataques más organizados desde principios de 2020. Es posible que, debido a la implementación de sistemas de seguridad más robustos por parte de las organizaciones, los ataques se hayan desplazado con éxito a los proveedores. Se ha logrado tener un impacto significativo en términos de tiempo de parada de los sistemas, pérdidas monetarias y daños a la reputación, por nombrar solo algunos. La importancia de las cadenas de suministro se atribuye al hecho de que los ataques pueden afectar a un gran número de clientes que recurren al proveedor afectado. Por lo tanto, los efectos en cascada de un solo ataque pueden tener un impacto que se propague de forma general.

Este informe tiene como objetivo identificar y estudiar los ataques a la cadena de suministro que se han descubierto desde enero de 2020 hasta principios de julio de 2021. Según las tendencias y patrones observados, los ataques a la cadena de suministro aumentaron en número y sofisticación en el año 2020 y esta tendencia se mantiene en 2021, lo que supone un riesgo creciente para las organizaciones. Se estima que habrá cuatro veces más ataques a la cadena de suministro en 2021 que en 2020. La mitad de los ataques se atribuyen a actores de amenazas persistentes avanzadas (APT, Advanced Persistence Threat), por lo que su complejidad y recursos superan con creces a los ataques no selectivos más comunes y, por lo tanto, cada vez es mayor la necesidad de nuevos métodos de protección que incorporen a los proveedores para garantizar la seguridad de las organizaciones.

En este informe se presenta el panorama de amenazas de la Agencia en relación con los ataques a la cadena de suministro, elaborado con el apoyo del Grupo de Trabajo ad hoc sobre el panorama de amenazas cibernéticas[1].

Entre los aspectos más destacados del informe se encuentran los siguientes:

- Se describe una **taxonomía** para clasificar los ataques a la cadena de suministro con el fin de analizarlos de forma sistemática y comprender la forma en que se manifiestan.
- Entre enero de 2020 y principios de julio de 2021 se registraron **veinticuatro ataques a la cadena de suministro**, que se han estudiado en este informe.
- Alrededor del **50 % de los ataques se atribuyeron a conocidos grupos de amenazas persistentes avanzadas** por parte de la comunidad de seguridad.
- Alrededor del **42 % de los ataques analizados aún no se han atribuido a un grupo concreto**.
- Alrededor del **62 % de los ataques a clientes** se aprovecharon de su **confianza en el proveedor**.
- En el **62 % de los casos**, **el software malicioso fue la técnica de ataque** empleada.
- Si se consideran los activos objetivo, en el **66 % de los incidentes** los agresores **se centraron en el código de los proveedores** para comprometer aún más a los clientes objetivo.
- Alrededor del **58 % de los ataques a la cadena de suministro tenían como objetivo** obtener acceso a los **datos** (principalmente datos de clientes, incluidos datos personales y propiedad intelectual e industrial) y alrededor del **16 %** querían obtener acceso a **personas**.
- **No todos los ataques deben designarse como ataques a la cadena de suministro**, pero debido a su naturaleza, muchos de ellos son vectores potenciales de nuevos ataques a la cadena de suministro en el futuro.

[1] Consulte https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes

- **Las organizaciones deben actualizar su metodología de ciberseguridad teniendo en cuenta los ataques a la cadena de suministro** e incorporar a todos sus proveedores en su protección y verificación de seguridad.

1. INTRODUCCIÓN

Los ataques a la cadena de suministro han sido un problema de seguridad durante muchos años, pero parece que la comunidad se está enfrentado a un mayor número de ataques más organizados desde 2020. Puede ser que, debido a la implantación de sistemas de seguridad más robustos por parte de las empresas, los agresores han desplazado su atención hacia los proveedores y han conseguido causar un impacto significativo en términos de tiempo de parada de los sistemas, pérdidas monetarias y daños a la reputación, por nombrar solo algunos. El objetivo de este informe es identificar y estudiar los ataques a la cadena de suministro descubiertos entre enero de 2020 y principios de julio de 2021.

El devastador y multiplicador efecto de los ataques a la cadena de suministro se vio con toda su fuerza con el ataque de SolarWinds[2]. SolarWinds se considera uno de los mayores ataques a la cadena de suministro de los últimos años, sobre todo teniendo en cuenta las entidades afectadas, que incluían organizaciones gubernamentales y grandes empresas. Recibió una gran atención por parte de los medios de comunicación y dio lugar a iniciativas políticas en todo el mundo[3]. Más recientemente, en julio de 2021, con el ataque a Kaseya[4], se planteó la necesidad de prestar más atención a los ataques a la cadena de suministro que afectan a los proveedores de servicios gestionados. Lamentablemente, estos dos ejemplos no son casos aislados y el número de ataques a la cadena de suministro ha aumentado constantemente durante el último año. Esta tendencia subraya aún más la necesidad de que los responsables políticos y la comunidad de seguridad diseñen e introduzcan nuevas medidas de protección para abordar posibles ataques a la cadena de suministro en el futuro y mitigar su impacto.

A través de un cuidadoso estudio y análisis, este informe traza los ataques a la cadena de suministro basándose en los incidentes identificados desde enero de 2020 hasta principios de julio de 2021. Cada incidente se ha desglosado en sus elementos clave, como las técnicas de ataque y los activos de proveedores y clientes que se ven afectados por los adversarios. La introducción de una taxonomía en los ataques a la cadena de suministro facilitará su clasificación y puede ser el punto de partida de un enfoque más estructurado para analizar dichos ataques y establecer controles de seguridad dedicados para mitigarlos. La taxonomía propuesta también ayuda a clasificar, comparar y debatir estos ataques utilizando una base común. Se analizan las similitudes entre la taxonomía propuesta y otros sistemas conocidos.

Este informe también analiza las similitudes entre el ciclo de vida de los ataques a la cadena de suministro y los ataques más conocidos de las amenazas persistentes avanzadas (APT). En el anexo se incluye un resumen de los incidentes más destacados en la cadena de suministro desde 2020, cada uno de los cuales se ha desglosado con arreglo a la taxonomía mencionada.

El núcleo del informe es un análisis de todos los incidentes de la cadena de suministro notificados con el fin de identificar sus características y técnicas clave. El análisis responde a las preguntas siguientes: ¿cuáles son las técnicas más utilizadas en los ataques a la cadena de suministro?, ¿cuáles son los principales activos de los clientes que persiguen los agresores? y ¿cuál es la relación entre los ataques y los activos perseguidos?

Con el aumento de la atención prestada a los ataques a la cadena de suministro, muchos otros incidentes de seguridad relacionados también se clasificaron como relacionados con la cadena de suministro, es decir, se asumió que eran ataques a la cadena de suministro. Por lo tanto, analizamos qué constituye un ataque a la cadena de suministro y por qué muchos ataques no son realmente ataques a la cadena de suministro, mostrando algunos

[2] Russian SolarWinds hackers launch email attack on government agencies, The Guardian. https://www.theguardian.com/technology/2021/may/28/russian-solarwinds-hackers-launch-assault-government-agencies. Accessed on 08/07/2021.
[3] Consulte https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html
[4] Ransomware Attack Affecting Likely Thousands of Targets Drags On, WSJ, https://www.wsj.com/articles/ransomware-group-behind-meat-supply-attack-threatens-hundreds-of-new-targets-11625285071. Consultado el 9 de julio de 2021.

ejemplos. Es importante comprender el panorama de amenazas relativo a los ataques a la cadena de suministro, ya que una clasificación errónea de los incidentes puede llevar a análisis de tendencias y conclusiones erróneas.

El informe también incluye una serie de recomendaciones dirigidas a los responsables políticos y a las organizaciones, en particular a los proveedores, cuya adopción puede aumentar la postura general de ciberseguridad contra los ataques a la cadena de suministro.

Este informe tiene la siguiente estructura:

- El **capítulo 1** ofrece una breve introducción al tema de la cadena de suministro y al panorama de amenazas específico de la ENISA.
- En el **capítulo 2** se analiza qué constituye un ataque a la cadena de suministro y se introduce una taxonomía estructurada para clasificar incidentes relevantes relacionados también con sistemas consolidados de inteligencia sobre amenazas.
- El **capítulo 3** ofrece una visión general del ciclo de vida de un ataque típico a la cadena de suministro.
- En el **capítulo 4** se describen los principales ataques a la cadena de suministro ocurridos a finales de 2020 y principios de 2021.
- El **capítulo 5** ofrece una cronología de los incidentes relevantes y un análisis exhaustivo de los mismos.
- El **capítulo 6** aborda el problema de la clasificación errónea de los incidentes como ataques a la cadena de suministro.
- El **capítulo 7** presenta recomendaciones técnicas y de alto nivel para mejorar la seguridad de la cadena de suministro y mitigar el impacto de los ataques a la misma.
- En el **anexo A** se resumen 24 incidentes de la cadena de suministro identificados y analizados en este informe.

2. ¿QUÉ ES UN ATAQUE A LA CADENA DE SUMINISTRO?

***Cadena de suministro* hace referencia al ecosistema de procesos, personas, organizaciones y distribuidores involucrados en la creación y entrega de una solución o producto final**[5]. En ciberseguridad, la cadena de suministro incluye una amplia gama de recursos (equipos y programas informáticos), almacenamiento (en la nube o en local), mecanismos de distribución (aplicaciones web, tiendas virtuales) y programas informáticos de gestión.

Hay cuatro elementos clave en una cadena de suministro:

- *Proveedor*: es una entidad que suministra un producto o servicio a otra entidad.
- *Activos del proveedor*: son elementos valiosos utilizados por el proveedor para producir el producto o servicio.
- *Cliente*: es la entidad que consume el producto o servicio producido por el proveedor.
- *Activos del cliente*: son elementos valiosos propiedad del objetivo.

Una entidad puede ser una persona física, un grupo de personas u organizaciones. Los activos pueden ser personas, programas informáticos, documentación, finanzas, equipos informáticos u otros.

Un ataque a la cadena de suministro es una combinación de al menos dos ataques. El primer ataque es contra un proveedor que luego se utiliza para atacar al objetivo y obtener acceso a sus activos. El objetivo puede ser el cliente final u otro proveedor. Por lo tanto, para que un ataque se clasifique como de cadena de suministro, tanto el proveedor como el cliente deben ser objetivos.

2.1. TAXONOMÍA DE LOS ATAQUES A LA CADENA DE SUMINISTRO

Este informe propone una taxonomía para caracterizar los ataques a la cadena de suministro y estructurar su posterior análisis. Esta taxonomía considera los cuatro elementos clave de una cadena de suministro, así como las técnicas utilizadas por los agresores. La taxonomía puede ayudar a las organizaciones a comprender las distintas partes de un ataque a la cadena de suministro, compararlas con otros ciberataques similares y, lo que es más importante, identificar los incidentes como ataques a la cadena de suministro.

La taxonomía debe utilizarse como una plantilla orientativa en la que, ante un nuevo ataque potencial a la cadena de suministro, la comunidad puede tratar de analizarlo identificando y trazando cada uno de los cuatro elementos distintivos de la taxonomía. Si no se ataca a ningún cliente o a ningún proveedor, probablemente no se trate de un ataque a la cadena de suministro[6].

La taxonomía, tal como se presenta en el cuadro 1, tiene una sección para el proveedor y otra para el cliente. En el caso del proveedor, la primera parte se denomina «Técnica de ataque utilizada para comprometer la cadena de suministro» e identifica **cómo** fue atacado el proveedor. La segunda parte se denomina «Activos del proveedor afectados por el ataque a la cadena de suministro» e identifica **cuál** fue el objetivo del ataque al proveedor.

En el caso del cliente, la primera parte se denomina «Técnicas de ataque utilizadas para comprometer al cliente» e identifica **cómo** fue atacado el cliente. La segunda parte se denomina «Activos del cliente afectados por el ataque a la cadena de suministro» e identifica **cuál** fue el objetivo del ataque contra el cliente.

Para cada uno de estos cuatro elementos distintivos de la taxonomía, hemos definido los elementos que caracterizan mejor un ataque a la cadena de suministro. Al seleccionar los elementos correspondientes, es posible

[5] Beamon, B. M. (1998). Supply chain design and analysis: Models and methods. International journal of production economics, 55(3), 281-294.
[6] Consulte la sección «No todo puede considerarse un ataque a la cadena de suministro» para ver más ejemplos.

comprender mejor lo que se sabe o no de un ataque. La taxonomía es conceptualmente diferente de la base de conocimientos MITRE ATT&CK® y no pretende sustituirla, sino complementarla. Las técnicas de ataque definidas en la taxonomía propuesta e ilustradas en el cuadro 1 están, en algunos casos, relacionadas con técnicas de ataque relevantes identificadas en el sistema MITRE ATT&CK®, y están marcadas en consecuencia con el respectivo identificador MITRE ATT&CK® entre corchetes, por ejemplo [T1189]. Las subsecciones siguientes aclaran cada una de las cuatro partes de la taxonomía y cómo identificar sus elementos.

Cuadro1: Taxonomía propuesta para los ataques a la cadena de suministro. Consta de cuatro partes: (i) técnicas de ataque utilizadas contra el proveedor, (ii) activos del proveedor atacados, (iii) técnicas de ataque utilizadas contra el cliente, (iii) activos del cliente atacados.

PROVEEDOR		CLIENTE	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro	Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Infección de software malicioso	Programa informático preexistente	Relación de confianza [T1199]	Datos
Ingeniería social	Bibliotecas de programas informáticos	Ataque drive-by [T1189]	Datos personales
Ataque de fuerza bruta	Código	Phishing [T1566]	Propiedad intelectual e industrial
Aprovecharse de la vulnerabilidad del software	Configuraciones	Infección de software malicioso	Programas informáticos
Aprovecharse de la vulnerabilidad de configuración	Datos	Ataque físico o modificación	Procesos
Información procedente del dominio público (OSINT)	Procesos	Falsificación	Ancho de banda
	Equipos informáticos		Finanzas
	Personas		Personas
	Proveedor		

Una taxonomía de incidentes de ciberseguridad de la UE[7] se utiliza para las actividades de coordinación de la respuesta a incidentes y para compartir información a escala de la Unión. Dado que la taxonomía es conceptualmente diferente y no permite un análisis detallado de los incidentes en la cadena de suministro, recomendamos la utilización complementaria de ambas taxonomías.

2.2. TÉCNICAS DE ATAQUE UTILIZADAS PARA COMPROMETER UNA CADENA DE SUMINISTRO

Las técnicas de ataque se refieren a «cómo» tuvo lugar el ataque y no a «qué» se utilizó para atacar. Por ejemplo, esta categoría distingue si se atacó al proveedor con una contraseña encontrada en línea (información procedente del dominio público) o si la contraseña se obtuvo de manera forzada (ataque de fuerza bruta). Sin embargo, no es relevante para la taxonomía si la contraseña encontrada en línea se filtró, se trataba de un contraseña por defecto o si fue vendida en el mercado negro. Las siguientes categorías de técnicas de ataque cubren las técnicas de ataque

[7] Cybersecurity incident taxonomy, Publications of the NIS Cooperation Group, julio de 2018. https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group. Consultado el 28 de julio de 2021.

más utilizadas en los ataques a la cadena de suministro analizados en este informe. Es evidente que es posible que se haya utilizado más de una técnica en un ataque concreto y, en varios casos, es posible que las entidades no tengan el conocimiento sobre cómo accedieron los agresores a su infraestructura, o esta información no fue divulgada o debidamente denunciada.

Cuadro2: Técnicas de ataque utilizadas para comprometer al proveedor de la cadena. Cada técnica identifica cómo ocurrió el ataque y no el objetivo del mismo. En el mismo ataque pueden utilizarse varias técnicas.

TÉCNICAS DE ATAQUE UTILIZADAS PARA COMPROMETER UNA CADENA DE SUMINISTRO	
Infección de software malicioso	por ejemplo, un programa espía utilizado para robar las credenciales de los empleados.
Ingeniería social	por ejemplo, phishing, aplicaciones falsas, allanamiento de error tipográfico, suplantación de identidad de la red WiFi, convencer al proveedor para que haga algo.
Ataque de fuerza bruta	por ejemplo, adivinar una contraseña SSH, adivinar un inicio de sesión en Internet.
Aprovecharse de la vulnerabilidad del software	por ejemplo, inyección SQL o desbordamiento de búfer en una aplicación.
Aprovecharse de la vulnerabilidad de configuración	por ejemplo, aprovecharse de un problema de configuración.
Ataque físico o modificación	por ejemplo, modificar equipos informáticos, intrusión física.
Información procedente del dominio público (OSINT)	por ejemplo, búsqueda de credenciales, claves API, nombres de usuario en línea.
Falsificación	por ejemplo, imitación de USB con fines maliciosos.

2.3. ACTIVOS DEL PROVEEDOR AFECTADOS POR EL ATAQUE A LA CADENA DE SUMINISTRO

Los activos del proveedor objetivo de los agresores se refieren a «cuál» fue el objetivo del ataque contra el proveedor, lo que permitió montar más ataques posteriormente. Los activos objetivo suelen tener una relación directa con el objetivo final y suele ser posible comprender las intenciones finales del agresor analizando la lista de activos afectados. En algunos casos, debido a la falta de información divulgada o denunciada por el proveedor, no es posible disponer de información sobre los activos objetivo. Esto también puede ocurrir cuando los proveedores no tienen los conocimientos o la experiencia necesarios para identificar los activos que fueron atacados.

Cuadro3: Activos del proveedor atacados. Cada elemento identifica los activos del proveedor atacados. En el mismo ataque pueden utilizarse varias técnicas que podrían afectar a varios activos.

ACTIVOS DEL PROVEEDOR AFECTADOS POR EL ATAQUE A LA CADENA DE SUMINISTRO	
Programa informático preexistente	por ejemplo, programas informáticos utilizados por el proveedor, servidores web, aplicaciones, bases de datos, sistemas de supervisión, aplicaciones en la nube, microprogramas. No incluye bibliotecas de programas informáticos.
Bibliotecas de programas informáticos	por ejemplo, bibliotecas de terceros, paquetes de programas informáticos instalados de terceros como npm, ruby, etc.
Código	por ejemplo, código fuente o programa informático producido por el proveedor.
Configuraciones	por ejemplo, contraseñas, claves API, reglas de cortafuegos, URL.
Datos	por ejemplo, información sobre el proveedor, valores de sensores, certificados, datos personales de clientes o de los propios proveedores, datos personales.
Procesos	por ejemplo, actualizaciones, copias de seguridad o procesos de validación, procesos de firma de certificados.
Equipos informáticos	por ejemplo, equipos informáticos fabricados por el proveedor, chips, válvulas, USB.
Personas	por ejemplo, personas físicas objetivo con acceso a datos, infraestructura u otras personas.

2.4. TÉCNICAS DE ATAQUE UTILIZADAS PARA COMPROMETER A UN CLIENTE

Este elemento de la taxonomía se refiere a las técnicas de ataque utilizadas para comprometer al cliente a través de su proveedor. En este elemento de la taxonomía, identificamos «cómo» se atacó al cliente y no con «qué». Es una técnica y no un tipo específico de ataque. Por ejemplo, si el cliente actualiza sus programas informáticos del proveedor y es infectado por un tipo de software malicioso, el ataque se debe tanto a una «relación de confianza» como a una «infección de software malicioso». Es evidente que se puede aplicar más de una técnica en varios casos. Es posible que los clientes no siempre conozcan la técnica utilizada por los agresores para acceder a sus activos a través de sus proveedores, pero tienen los medios para identificar que la técnica utilizada no estaba dentro de su perímetro.

Cuadro4: Técnicas de ataque utilizadas para comprometer al cliente. Cada técnica identifica cómo ocurrió el ataque y no el objetivo del mismo. En el mismo ataque pueden utilizarse varias técnicas.

TÉCNICAS DE ATAQUE UTILIZADAS PARA COMPROMETER A UN CLIENTE	
Relación de confianza [T1199]	por ejemplo, confiar en un certificado, confiar en una actualización automática, confiar en una copia de seguridad automática.
Ataque drive-by [T1189]	por ejemplo, scripts maliciosos en un sitio web para infectar a los usuarios con software malicioso.

TÉCNICAS DE ATAQUE UTILIZADAS PARA COMPROMETER A UN CLIENTE	
Phishing [T1566]	por ejemplo, mensajes que suplantan la identidad del proveedor, notificaciones de actualizaciones falsas.
Infección de software malicioso	por ejemplo, troyano de acceso remoto (RAT), puerta trasera, programa de secuestro.
Ataque físico o modificación	por ejemplo, modificar equipos informáticos, intrusión física.
Falsificación	por ejemplo, crear un USB falso, modificar una placa base o suplantar al personal del proveedor.

2.5. ACTIVOS DE CLIENTES AFECTADOS POR UN ATAQUE A LA CADENA DE SUMINISTRO

Los activos de los clientes son el objetivo principal y final de los agresores, y suelen ser la razón de ser de un ataque a la cadena de suministro. Estos activos pueden variar dependiendo del sector de la industria y del tipo de servicio ofrecido. Este elemento concreto de la taxonomía pretende facilitar la comprensión del impacto del ataque y también permitir comparaciones relativas a los objetivos de los agresores. Algunos activos pueden haber sido blanco directo de los agresores, mientras que otros pueden haber sido afectados involuntariamente. Los ataques típicos a la cadena de suministro suelen afectar a más de un cliente. Es posible que el cliente no sea consciente del objetivo del adversario (por ejemplo, el ataque no tuvo éxito o se detectó rápidamente).

Cuadro5: Activos del cliente atacados. Cada elemento identifica los activos del cliente atacados. En el mismo ataque pueden utilizarse varias técnicas. Suelen ser el objetivo final del ataque.

ACTIVOS DE CLIENTES AFECTADOS POR UN ATAQUE A LA CADENA DE SUMINISTRO	
Datos	por ejemplo, datos de pago, fuentes de vídeo, documentación, correos electrónicos, planes de vuelo, datos de ventas y financieros, propiedad intelectual e industrial.
Datos personales	por ejemplo, datos de clientes, documentos del personal, credenciales.
Programas informáticos	por ejemplo, acceso al código fuente del producto del cliente, modificación del programa informático del cliente.
Procesos	por ejemplo, documentación de procesos internos de funcionamiento y configuraciones, inserción de nuevos procesos maliciosos, documentos de esquemas.
Ancho de banda	por ejemplo, utilizar el ancho de banda para la denegación de servicio distribuido (DDoS), enviar correo electrónico no deseado o infectar a otros a gran escala.
Finanzas	por ejemplo, robar criptomoneda, secuestrar cuentas bancarias, transferencias de dinero.

Personas	por ejemplo, personas físicas que son objetivos debido a su posición o conocimiento.

2.6. CÓMO HACER USO DE LA TAXONOMÍA

A continuación, se muestra un ejemplo de cómo la aplicación de la taxonomía a un caso real puede ayudar a identificar sus características particulares y facilitar la comprensión de las características del ataque.

Codecov es una empresa que proporciona programas informáticos para herramientas de pruebas y cobertura de código. La empresa suministra herramientas a otras empresas como IBM y Hewlett Packard Enterprise. En abril de 2021, Codecov informó de que los agresores obtuvieron algunas de sus credenciales válidas de una imagen en Docker[8] debido a un error en la forma en que se crearon esas imágenes Docker. Una vez que los agresores obtuvieron estas credenciales, las utilizaron para comprometer un «script bash de carga» que utilizan los clientes de Codecov[9]. Una vez que los clientes descargaron y ejecutaron este script, los agresores pudieron extraer datos de los clientes de Codecov, incluida información delicada que les permitiría acceder a los recursos del cliente[10]. Varios clientes de Codecov informaron de que los agresores podían acceder a su código fuente utilizando información robada procedente de la violación de la seguridad del sistema de Codecov[11]. El ataque no se atribuyó a ningún adversario específico. La Figura 1 (abajo) muestra los pasos de este ataque concreto.

Utilizando esta información, podemos identificar los cuatro elementos de la taxonomía propuesta. El ataque al proveedor hace referencia a cómo los agresores consiguieron acceder al proveedor y, en este caso, fue «aprovechando una vulnerabilidad de configuración». En este ataque, los agresores tienen como objetivo el activo del «código» del proveedor. Una vez identificados los elementos en el caso del proveedor en la taxonomía, podemos pasar al modo en que el cliente fue atacado. En el caso Codecov es a través de una «relación de confianza» con el proveedor que no se ha asegurado ni verificado. Se informó de que el activo final del cliente objetivo del ataque era el código fuente, es decir, «programas informáticos».

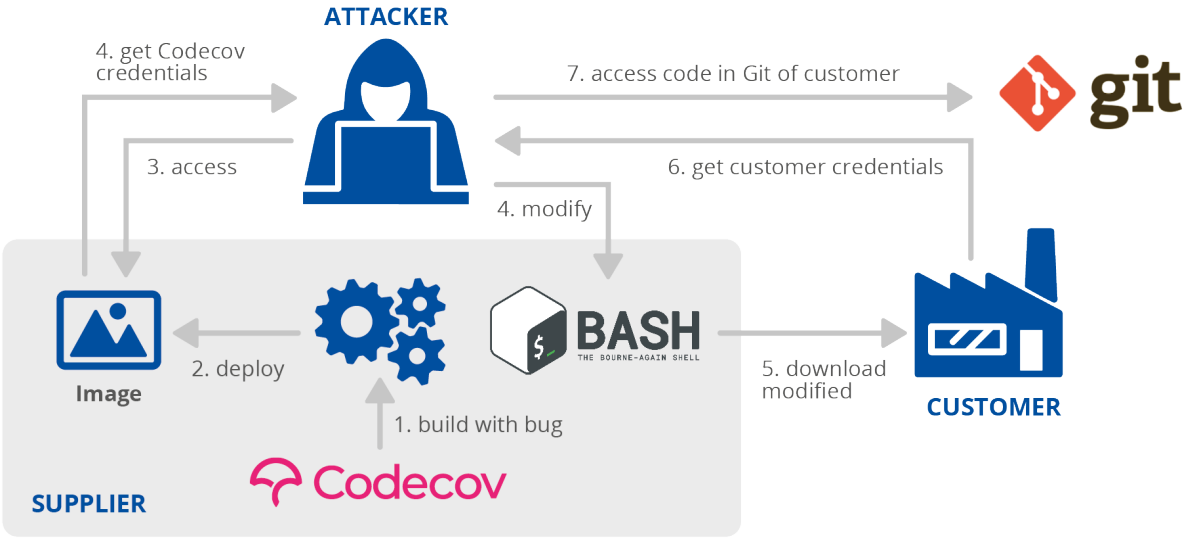
Cuadro6: Taxonomía de ataques a la cadena de suministro aplicada al ataque que afecta a la empresa Codecov. Los agresores aprovecharon una vulnerabilidad de configuración en Codecov que se utilizó para modificar el código del proveedor. Los agresores abusaron de la relación de confianza entre Codecov y sus clientes para extraer los datos necesarios para acceder al código fuente de los programas informáticos del cliente.

PROVEEDOR	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro
Aprovecharse de la vulnerabilidad de configuración	Código

CLIENTE	
Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Relación de confianza [T1199]	Programas informáticos

[8] Codecov supply chain attack breakdown, GitGuardian, https://blog.gitguardian.com/codecov-supply-chain-breach/. Consultado el 27 de junio de 2021.
[9] Bash Uploader Security Update, Codecov, https://about.codecov.io/security-update/. Consultado el 27 de junio de 2021.
[10] Codecov hackers gained access to Monday.com source code, Bleeping Computer. https://www.bleepingcomputer.com/news/security/codecov-hackers-gained-access-to-mondaycom-source-code/. Consultado el 27 de junio de 2021.
[11] Rapid7 Source Code Breach in Codecov Supply-Chain Attack, The Hacker News, https://thehackernews.com/2021/05/rapid7-source-code-breached-in-codecov.html. Consultado el 27 de junio de 2021.

Figura 1. Gráfico de cómo funcionó el ataque a la cadena de suministro de Codecov. El proceso de creación de contenedores Codecov tenía un error que estaba presente en los contenedores alojados en línea (1). Los agresores accedieron al contenedor y obtuvieron las credenciales de Codecov (2). A continuación, modificaron el script bash de Codecov (3) que se actualizó en los clientes (4). El script bash malicioso filtró las credenciales del cliente al agresor (5), que las utilizó para acceder a los datos de los clientes (6).



2.7. TAXONOMÍA DE LA CADENA DE SUMINISTRO Y OTROS SISTEMAS

2.7.1. Base de conocimientos MITRE ATT&CK®

MITRE ATT&CK® es una base de conocimientos y un modelo de comportamiento de los ciberadversarios. La taxonomía propuesta en el informe difiere de MITRE ATT&CK®[12] porque los objetivos de ambas son muy diferentes. Por lo tanto, no es posible utilizar MITRE ATT&CK® en la taxonomía de la cadena de suministro, ya que hemos preferido hacer hincapié en los cuatro aspectos que suelen caracterizar un ataque a la cadena de suministro y, en particular, en la relación proveedor-cliente. Aunque MITRE ATT&CK® identifica completamente las diferentes opciones y los niveles en el ciclo de vida de todos los ataques, no se ha desarrollado aún su cobertura de los detalles de una cadena de suministro.

Por ejemplo, en la categoría «Acceso inicial» de MITRE ATT&CK®, existe una técnica denominada «Compromiso de la cadena de suministro»[13]. Esto es muy útil para que las empresas identifiquen una cadena de suministro como un riesgo, pero demasiado genérico cuando se centra explícitamente en los ataques a la cadena de suministro en sí. La taxonomía propuesta identifica todos los detalles del propio ataque a la cadena de suministro y, por tanto, podría complementar potencialmente la base de conocimientos MITRE ATT&CK®.

2.7.2. Sistema Cyber Kill Chain® de Lockheed Martin

La taxonomía propuesta también tiene un propósito diferente al conocido sistema Cyber Kill Chain® de Lockheed Martin[14]. La cadena de muerte cibernética es un sistema diseñado para identificar los pasos que siguen los agresores para lograr sus objetivos. Si bien estos pasos pueden considerarse como parte de un ataque a la cadena de suministro, son demasiado genéricos para clasificar, entender y comparar los ataques a la cadena de suministro. La taxonomía que se presenta aquí propone un análisis más detallado de estos ataques y, lo que es más importante, ayuda a identificar los dos ataques implicados en un único ataque a la cadena de suministro, al proveedor y al cliente.

[12] MITRE ATT&CK®, MITRE, https://attack.mitre.org/. Consultado el 8 de julio de 2021.
[13] Supply Chain Compromise, Technique T1195 – Enterprise, MITRE ATT&CK®, https://attack.mitre.org/techniques/T1195/. Consultado el 8 de julio de 2021.
[14] Cyber Kill Chain®, Lockheed Martin, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. Consultado el 8 de julio de 2021.

3. EL CICLO DE VIDA DE UN ATAQUE A LA CADENA DE SUMINISTRO

Puede observarse que un ataque a la cadena de suministro suele consistir en un ataque a uno o varios proveedores y, posteriormente, en un ataque al objetivo final, es decir, al cliente. Cada uno de estos ataques puede asemejarse mucho al ciclo de vida de los ataques de APT.

Aunque es difícil ponerse de acuerdo en una definición única de lo que es un ataque de APT, a lo largo de este informe se considera que un ataque de APT es cualquier ataque dirigido, que obtiene acceso no autorizado a una organización (normalmente ejecución de código), que se extiende durante un largo periodo de tiempo y que su objetivo final está en una relación específica con el objetivo (a diferencia de, por ejemplo, la minería de criptomonedas). Por supuesto, tal definición no es completa y pueden existir muchas otras. Sin embargo, es importante contar con una definición para entender que los ataques a la cadena de suministro suelen ser selectivos, complejos y costosos, y que los agresores probablemente los planean durante mucho tiempo. El mero hecho de que en los incidentes típicos de la cadena de suministro se produzcan al menos dos tipos de ataques con éxito, es un indicador tanto del grado de sofisticación de los adversarios, como de su persistencia e intención de tener éxito.

Cabe destacar que la comunidad consideró que muchos ataques APT no eran «avanzados» teniendo en cuenta la calidad de su código, los programas intrusos y el software malicioso. Sin embargo, puede considerarse que la denominación de «avanzado» se refiere a toda la operación y no necesariamente solo al código. Al final, planificar, organizar, desarrollar y ejecutar dos ataques en dos organizaciones es una tarea compleja.

Estas distinciones son cruciales para entender **que una organización podría ser vulnerable a un ataque a la cadena de suministro incluso cuando sus propias defensas sean bastante buenas** y, por lo tanto, los agresores intentan explorar nuevos canales potenciales para infiltrarse en ellas convirtiendo a sus proveedores en objetivo. Además, el impacto potencial de los ataques a la cadena de suministro que afectan a numerosos clientes del mismo proveedor es probablemente inmenso. Esta es otra de las razones por las que este tipo de ataques son cada vez más frecuentes, ya que proporcionan a los adversarios un medio para aumentar potencialmente su reputación y, posiblemente, obtener grandes beneficios financieros.

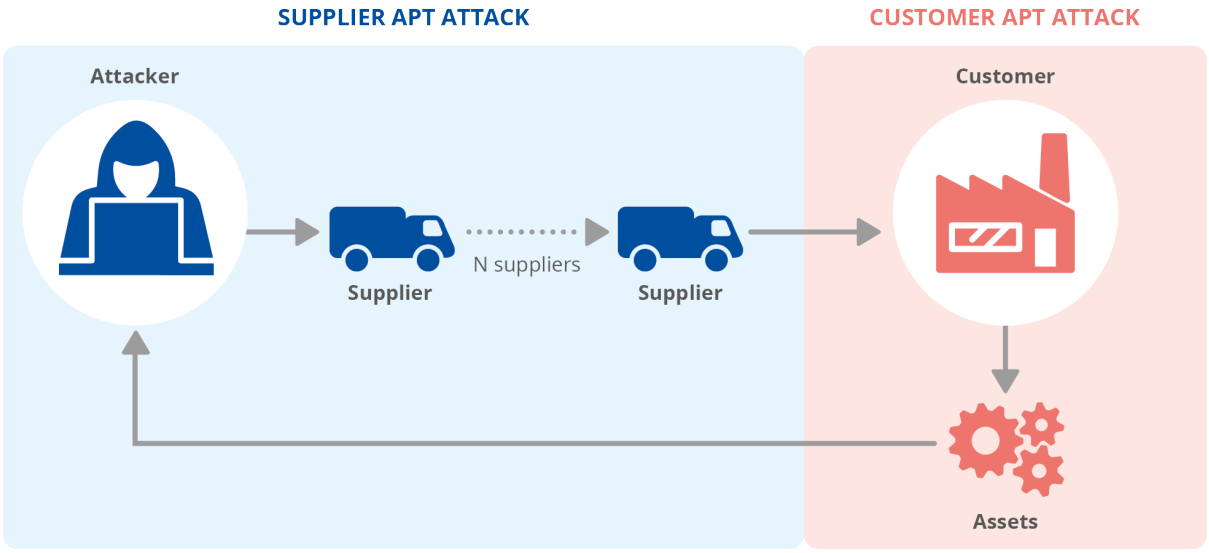
Otra característica de los ataques a la cadena de suministro es la complejidad de su tratamiento y los esfuerzos necesarios para mitigar y hacer frente a dichos ataques. El mero hecho de que se vean afectadas al menos dos organizaciones y la utilización, muy probablemente, de sofisticados vectores de ataque complica la gestión de un incidente, el análisis forense y la gestión global del mismo. El hecho de que la relación proveedor-consumidor esté en continua evolución y tanto los proveedores como los clientes estén actualizando constantemente sus sistemas introduce la necesidad de una seguridad continua de la cadena de suministro y de una evaluación y gestión activas del riesgo.

El ciclo de vida de un ataque a la cadena de suministro tiene dos partes principales: el ataque al proveedor y el ataque al cliente. Cada uno de estos ataques suele ser complejo y requiere un vector de ataque, un plan de acción y una ejecución cuidadosa. Estos ataques pueden tardar meses en tener éxito y, en muchos casos, pueden pasar desapercibidos durante mucho tiempo. El ciclo de vida de un ataque a la cadena de suministro se muestra en la figura 2.

El primer ataque del ciclo de vida se llama «Ataque de APT al proveedor» y se centra en comprometer a uno o más proveedores. El segundo ataque del ciclo de vida se denomina «ataque de APT al cliente» y se centra en el objetivo

final del ataque. Estas dos partes están vinculadas por el acceso al proveedor, pero pueden ser muy diferentes en las técnicas y vectores de ataque utilizados, y el tiempo dedicado al ataque.

Figura2: El ciclo de vida de los ataques a la cadena de suministro puede verse como dos ataques de APT interrelacionados. El primer ataque afecta a uno o varios proveedores y el segundo, a los clientes. Estos ataques requieren una planificación y ejecución cuidadosas.



En al menos once ataques de todos los casos estudiados en este informe, las investigaciones confirmaron que los ataques a la cadena de suministro fueron realizados por grupos conocidos de APT. Estas atribuciones de ciberataques fueron realizadas por las empresas de seguridad responsables de los informes a los que se hace referencia en el Anexo A. En los otros trece casos los incidentes no se investigaron a fondo o no fue posible su atribución. Estas atribuciones de ciberataques respaldan la idea de que ambas partes del ciclo de vida de un ataque a la cadena de suministro pueden asemejarse al trabajo de los ataques de APT. Cabe señalar que la atribución de los agresores es muy difícil, propensa a errores, imprecisa y supone un reto desde el punto de vista político, pero no es imposible.

Dado que cada parte del ataque a la cadena de suministro puede considerarse un ataque de APT, su ciclo de vida individual debería seguir las mismas fases que otros ataques de APT. Estas etapas se detallan, por ejemplo, en las tácticas para empresas MITRE ATT&CK®[15].

[15] MITRE ATT&CK® Tactics - Enterprise Versión 9, MITRE, https://attack.mitre.org/tactics/enterprise/. Consultado el 29 de junio de 2021.

4. PRINCIPALES ATAQUES A LA CADENA DE SUMINISTRO

Esta sección presenta un resumen de los ataques más destacados a la cadena de suministro desde enero de 2020 hasta principios de julio de 2021, junto con una clasificación conforme a la taxonomía propuesta. Se han seleccionado estos casos debido al gran impacto producido en la comunidad o porque resaltan determinadas características (indicadas en los elementos de la taxonomía) que son importantes. La lista completa y la descripción de todos los ataques a la cadena de suministro desde enero de 2020 hasta principios de julio de 2021 están disponibles en el Anexo A.

4.1. SOLARWINDS ORION: GESTIÓN DE TI Y SEGUIMIENTO ELECTRÓNICO REMOTO

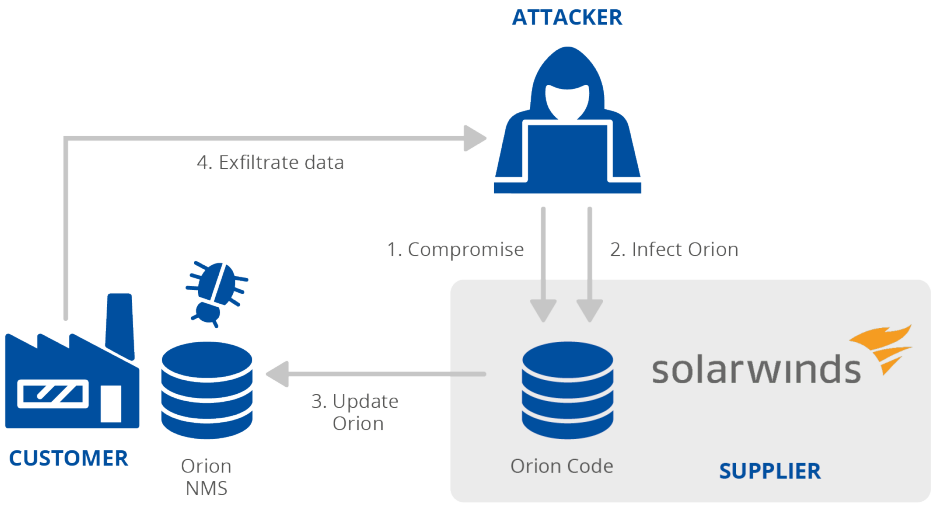
SolarWinds es una empresa que suministra programas informáticos de gestión y vigilancia[16]. Orion es el producto de sistema de gestión de red (NMS) de SolarWinds[17]. En diciembre de 2020 se descubrió que Orion había sido comprometido. Una investigación exhaustiva demostró que los agresores obtuvieron acceso a la red de SolarWinds, posiblemente aprovechando una vulnerabilidad de día cero en una aplicación o dispositivo de terceros, un ataque de fuerza bruta o a través de ingeniería social. Una vez comprometida la red, los agresores recopilaron información durante un largo periodo de tiempo. El software malicioso se inyectó en Orion durante el proceso de compilación[18,19]. Los clientes descargaban los programas informático afectados, lo que se utilizó para recopilar y robar información[20]. El ataque se atribuyó al grupo APT29[21,22].

Cuadro7: Taxonomía de ataques a la cadena de suministro aplicada al ataque contra SolarWinds. Los agresores utilizaron múltiples técnicas de ataque para comprometer los programas informáticos de SolarWinds Orion. Modificaron el código del proveedor y abusaron de la relación de confianza de los clientes de SolarWinds para actualizar a los clientes con software malicioso. El objetivo final de los agresores eran los datos de los clientes.

PROVEEDOR		CLIENTE	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro	Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Aprovecharse de la vulnerabilidad del software, Ataque de fuerza bruta, Ingeniería social	Procesos, código	Relación de confianza [T1199], Infección de software malicioso	Datos

[16] What You Need To Know About the SolarWinds Supply-Chain Attack, SANS Institute, https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/. Consultado el 8 de julio de 2021.
[17] Orion Platform - Scalable IT Monitoring, SolarWinds, https://www.solarwinds.com/solutions/orion. Consultado el 8 de julio de 2021.
[18] An Investigative Update of the Cyberattack, Orange Matter, https://orangematter.solarwinds.com/2021/05/07/an-investigative-update-of-the-cyberattack/. Consultado el 8 de julio de 2021.
[19] SUNSPOT Malware: A Technical Analysis, CrowdStrike, https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/. Consultado el 8 de julio de 2021.
[20] Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor, FireEye Inc, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html. Consultado el 8 de julio de 2021.
[21] SolarWinds: Advancing the Story, RiskIQ Community Edition, https://community.riskiq.com/article/9a515637. Consultado el 8 de julio de 2021.
[22] Russian hacker group 'Cozy Bear' behind Treasury and Commerce breaches, The Washington Post, https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html. Consultado el 8 de julio de 2021.

Figura3: Gráfico del ataque a la cadena de suministro de SolarWinds. Los agresores pusieron en peligro a SolarWinds y modificaron el código del programa informático de ORION. Las instancias de ORION de los clientes se actualizaron con software malicioso, lo que permitió a los agresores acceder a los datos de los clientes.



4.2. MIMECAST: SERVICIOS DE CIBERSEGURIDAD EN LA NUBE

Mimecast es un proveedor de servicios de ciberseguridad en la nube. Entre los servicios que proporciona, Mimecast ofrece servicios de seguridad del correo electrónico, que requieren que los clientes se conecten de forma segura a los servidores Mimecast para utilizar sus cuentas de Microsoft 365. En enero de 2021, se descubrió que los agresores habían comprometido a Mimecast (a través del proveedor de SolarWinds). Tras el ataque, los agresores accedieron a un certificado emitido por Mimecast utilizado por los clientes para acceder a los servicios de Microsoft 365, lo que les permitió interceptar las conexiones de redes y conectarse a las cuentas de Microsoft 365 para robar información[23,24]. El ataque fue atribuido al grupo APT29[25]. El compromiso de los sistemas del proveedor ha sido supuestamente vinculado a SolarWinds, pero no hay información concreta que lo valide.

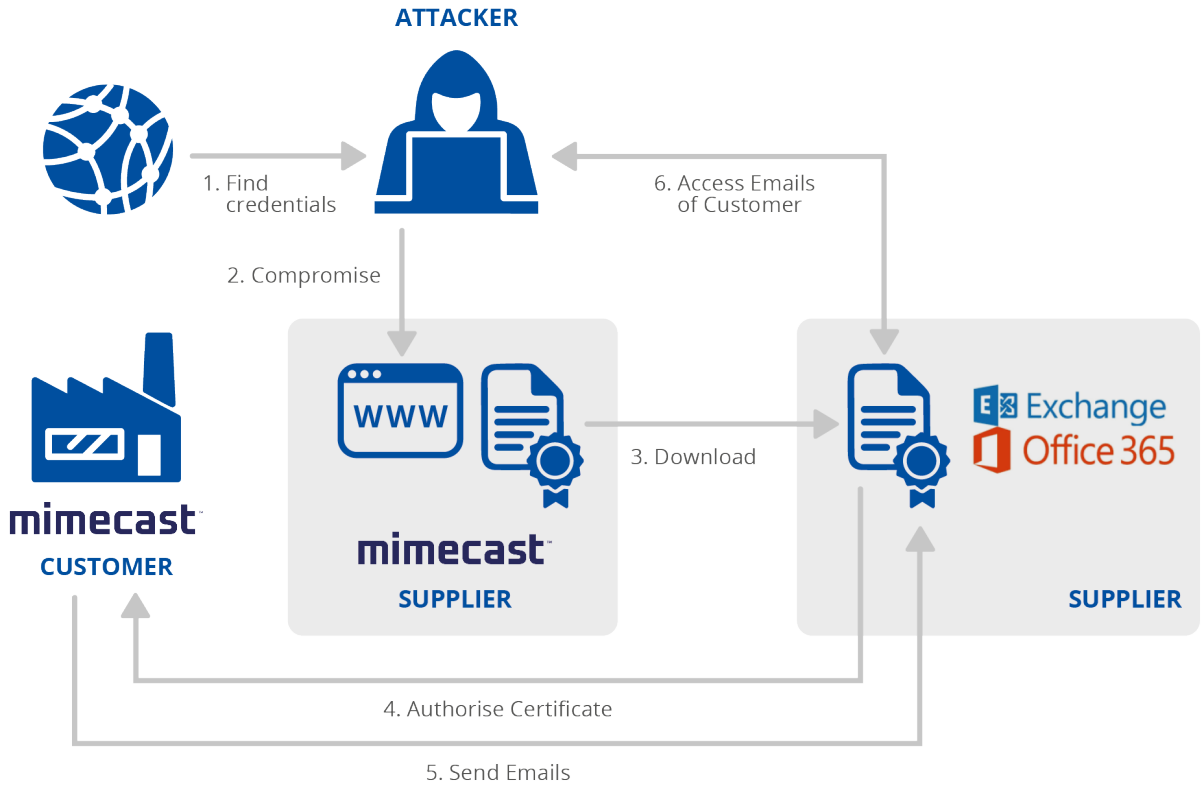
Cuadro8: Taxonomía de ataques a la cadena de suministro aplicada al ataque contra Mimecast. Se desconoce cómo atacaron los agresores los datos de los proveedores, concretamente un certificado emitido por Mimecast. Los agresores abusaron de la relación de confianza de los clientes que subían sus datos a Mimecast. Los agresores accedieron a los datos de los clientes en Mimecast.

PROVEEDOR	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro
Desconocido	Datos

CLIENTE	
Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Relación de confianza [T1199]	Datos

[23] Important Update from Mimecast, Mimecast Blog, https://www.mimecast.com/blog/important-update-from-mimecast/. Consultado el 8 de julio de 2021.
[24] Mimecast Certificate Hacked in Supply-Chain Attack, Threatpost, https://threatpost.com/mimecast-certificate-microsoft-supply-chain-attack/162965/. Consultado el 8 de julio de 2021.
[25] Important Security Update, Mimecast Blog, https://www.mimecast.com/blog/important-security-update/. Consultado el 8 de julio de 2021.

Figura4: Gráfico del ataque a la cadena de suministro de Mimecast. Los agresores encontraron credenciales que les permitieron comprometer al proveedor y acceder a sus certificados. A continuación, utilizaron los certificados para acceder a los datos del cliente después de que este hubiera validado y confiado en el certificado.



4.3. LEDGER: MONEDERO DE HARDWARE

Ledger es una empresa que suministra tecnología de monederos de hardware para criptomonedas. En julio de 2020, los agresores obtuvieron credenciales válidas para acceder a la base de datos de comercio electrónico de Ledger[26]. Los datos robados se publicaron en un foro en línea[27]. Los agresores utilizaron los datos robados para el phishing en línea y la extorsión de los usuarios[28,29] así como para robar el dinero de los usuarios a través de un ataque físico tras suministrarles monederos Ledger falsificados que, al conectarse a un ordenador que les solicitaba las claves de seguridad, infectaban el ordenador con software malicioso y enviaban la información robada a los agresores[30]. No se identificó a los agresores del ataque.

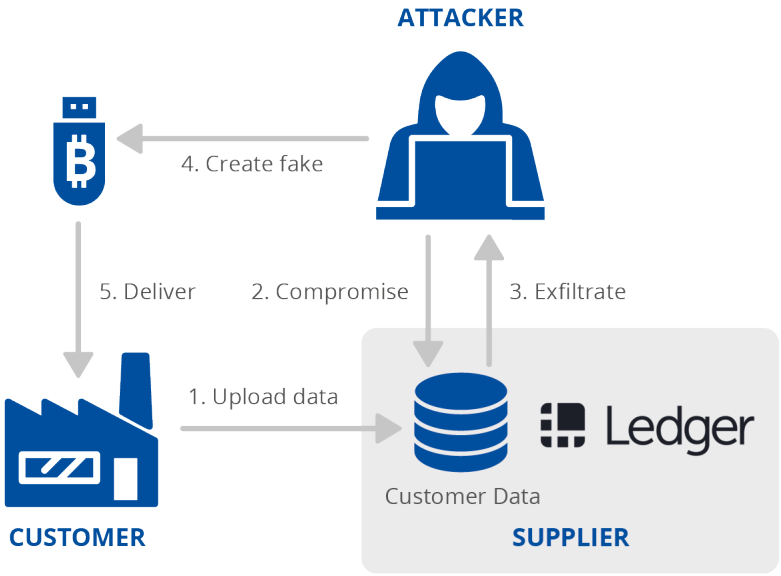
Cuadro9: Taxonomía de ataques a la cadena de suministro aplicada al ataque contra Ledger. Los agresores utilizaron técnicas de información procedente del dominio público para encontrar credenciales válidas para acceder a los documentos de Ledger y robar datos de clientes. Con esos datos, los agresores abusaron de la relación de

[26] Addressing the July 2020 e-commerce and marketing data breach -- A Message From Ledger's Leadership, Ledger, https://www.ledger.com/addressing-the-july-2020-e-commerce-and-marketing-data-breach. Consultado el 8 de julio de 2021.
[27] Hackers Leak Customer Info From Crypto Wallet Ledger, Investopedia, https://www.investopedia.com/hackers-leak-customer-info-from-crypto-wallet-ledger-5093577. Consultado el 8 de julio de 2021.
[28] Message by LEDGER's CEO - Update on the July data breach. Despite the leak, your crypto assets are safe, Ledger, https://www.ledger.com/message-ledgers-ceo-data-leak. Consultado el 8 de julio de 2021.
[29] Threat Actors Target Ledger Data Breach Victims in New Extortion Campaign, Bitdefender HOTforSecurity, https://web.archive.org/web/20210520120353/https://hotforsecurity.bitdefender.com/blog/threat-actors-target-ledger-data-breach-victims-in-new-extortion-campaign-25820.html, Consultado el 8 de julio de 2021.
[30] Inside The Scam: Victims Of Ledger Hack Are Receiving Fake Hardware Wallets, Nasdaq, https://www.nasdaq.com/articles/inside-the-scam%3A-victims-of-ledger-hack-are-receiving-fake-hardware-wallets-2021-06-17. Consultado el 8 de julio de 2021.

confianza de los clientes en Ledger enviando correos electrónicos de suplantación de identidad y falsas unidades USB de monederos para criptomonedas para robar criptomonedas a los clientes.

PROVEEDOR		CLIENTE	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro	Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
OSINT	Datos	Relación de confianza [T1199], Phishing [T1566], Falsificación	Finanzas

Figura5: Gráfico del ataque a la cadena de suministro de Ledger. Los agresores encontraron credenciales de Ledger en línea, accedieron a la base de datos de sus clientes y utilizaron la información para atacarlos.



4.4. KASEYA: SERVICIOS DE GESTIÓN DE TI COMPROMETIDOS POR UN PROGRAMA DE SECUESTRO

Kaseya es un proveedor de servicios de programas informáticos especializado en herramientas de supervisión y gestión remotas. Ofrece programas informáticos VSA (Virtual System/Server Administrator) para que sus clientes los descarguen y también para trabajar a través de sus propios servidores en la nube. Los MSP (proveedores de servicios gestionados) pueden utilizar los programas informáticos VSA en sus instalaciones o pueden obtener una licencia para los servidores en la nube VSA de Kaseya. A su vez, los MSP ofrecen varios servicios de TI a otros clientes[31]. En julio de 2021, los agresores aprovecharon una vulnerabilidad de día cero en los propios sistemas de Kaseya (CVE-2021-30116[32]), lo que les permitió ejecutar comandos de forma remota en los dispositivos VSA de los clientes de Kaseya. Kaseya puede enviar actualizaciones remotas a todos los servidores VSA y, el viernes 2 de julio

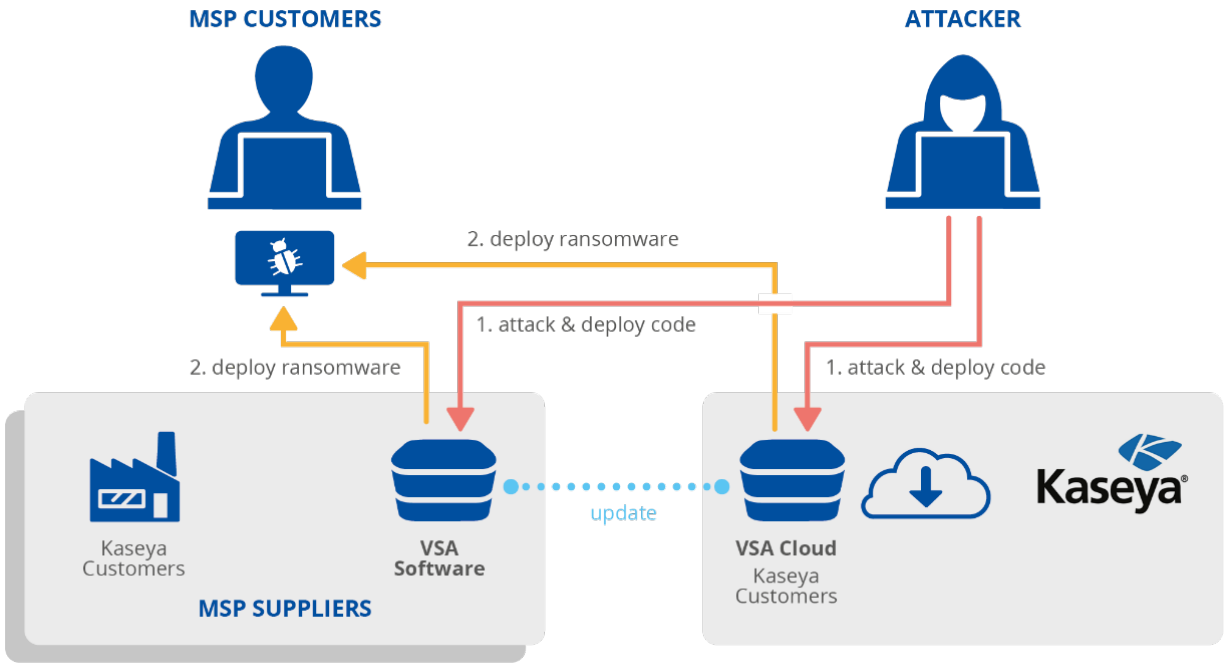
[31] Ransomware Hits Hundreds of US Companies, Security Firm Says, NBC10 Philadelphia, https://www.nbcphiladelphia.com/news/national-international/new-ransomware-attack-paralyzes-hundreds-of-u-s-companies/2868462/. Consultado el 8 de julio de 2021.
[32] CVE-2021-30116, MITRE, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30116. Consultado el 8 de julio de 2021.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

de 2021, se distribuyó una actualización a los VSA de los clientes de Kaseya que ejecutó código de los agresores. A su vez, este código malicioso instaló un programa de secuestro[33,34] en los clientes gestionados por ese VSA.

Cuadro10: Taxonomía de ataques a la cadena de suministro aplicada al ataque contra Kaseya. Al aprovechar una vulnerabilidad del software, los agresores obtuvieron acceso a los programas informáticos de Kaseya. Los agresores aprovecharon este acceso para instalar programas de secuestro en la infraestructura de los clientes. El ataque tenía como objetivo los datos y recursos financieros de los clientes de Kaseya mediante la petición de un rescate.

PROVEEDOR		CLIENTE	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro	Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Aprovecharse de la vulnerabilidad del software	Programa informático preexistente	Relación de confianza [T1199], Infección de software malicioso	Datos, finanzas

Figura6: Gráfico del ataque a la cadena de suministro de Kaseya. Los agresores instalaron código en las instancias VSA de los MSP (todavía se está investigando si en la nube o en las instalaciones). A su vez, se aprovecharon de los MSP para instalar software malicioso y programas de secuestro en sus clientes.



4.5. UN EJEMPLO DE MUCHAS INCÓGNITAS: SISTEMA DE GESTIÓN DE PASAJEROS SITA

El caso de SITA es especialmente relevante debido a que siguen siendo **desconocidos** muchos de los componentes de los ataques a la cadena de suministro, así como las posibles implicaciones de su impacto. Este caso ilustra que

[33] Kaseya VSA vulnerability opens a thousand-plus business doors to ransomware, Blocks and Files, https://blocksandfiles.com/2021/07/04/kaseya-vsa-vulnerability-opens-1000-plus-business-doors-to-let-in-ransomware/. Consultado el 8 de julio de 2021.
[34] Hundreds of Businesses, From Sweden to U.S., Affected by Cyberattack, The New York Times, https://www.nytimes.com/2021/07/02/technology/cyberattack-businesses-ransom.html. Consultado el 8 de julio de 2021.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

puede haber muchas circunstancias en las que los detalles de los ataques nunca se publican, por imposibilidad técnica o por decisiones políticas y de marketing de las empresas. Hay un equilibrio entre el beneficio para la comunidad, que puede mejorar su seguridad al conocer los detalles de cómo se comprometió la seguridad de otras empresas, y los beneficios para las empresas individuales, por ejemplo, financieros, de reputación y de mercado[35].

SITA es una empresa especializada en tecnología de información aérea e información de transporte. El sistema de gestión de pasajeros de SITA se utiliza para proporcionar a las aerolíneas información sobre los pasajeros en el momento del embarque, incluido el riesgo que los pasajeros pueden representar para un país[36].

En marzo de 2021, se reveló que los agresores habían comprometido los servidores de SITA para obtener acceso a los datos de los pasajeros de los clientes de SITA. Algunos de los clientes de SITA también informaron de violaciones de datos, como Air India, Singapore Airlines y Malaysia Airlines[36].

A raíz de los informes sobre filtraciones de datos en Internet, Air India también denunció que sus redes estaban comprometidas y que se habían robado datos.[37] El ataque a las redes internas de Air India estaba supuestamente relacionado con el incidente de SITA, ya que una empresa de seguridad descubrió que el nombre de un ordenador dentro de Air India era «SITASERVER4». Hasta la fecha, se desconoce cómo accedieron los agresores a los servidores de SITA y tampoco se sabe cómo accedieron a Air India o si lo hicieron realmente. El ataque interno a las redes de Air India se atribuyó al grupo APT41[37].

El número de variables desconocidas en este incidente es un ejemplo del panorama de amenazas cuando se trata de ataques a la cadena de suministro. El nivel de madurez en relación con las investigaciones cibernéticas y la preparación de muchas organizaciones también debería extenderse a sus proveedores, debido a la forma en que están interrelacionados.

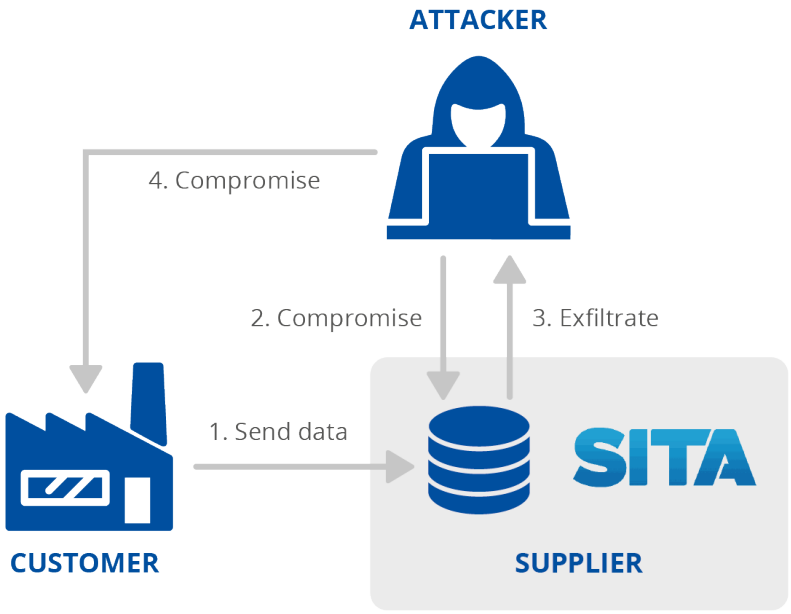
Cuadro11: Taxonomía de ataques a la cadena de suministro aplicada al ataque contra SITA. Se desconoce cómo accedieron los agresores al proveedor. Los agresores accedieron a datos del proveedor sobre sus clientes. Se desconoce cómo los agresores lograron infiltrarse en Air India. La información disponible indica que el objetivo principal de los agresores eran los datos de los clientes.

PROVEEDOR	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro
Desconocido	Datos

CLIENTE	
Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Desconocido	Datos personales

[35] Investors in SolarWinds sold millions in stock before Russia breach revealed, The Washington Post, https://www.washingtonpost.com/technology/2020/12/15/solarwinds-russia-breach-stock-trades/. Consultado el 9 de julio de 2021.
[36] SITA Advance Passenger Processing, SITA, https://www.sita.aero/solutions/sita-at-borders/border-management/sita-advance-passenger-processing/. Consultado el 8 de julio de 2021.
[37] Big airline heist: APT41 likely behind massive supply chain attack, Group-IB, https://blog.group-ib.com/colunmtk_apt41. Consultado el 8 de julio de 2021.

Figura 7: Gráfico del ataque a la cadena de suministro de SITA. Los agresores robaron datos de pasajeros de las empresas clientes de SITA. Hasta la fecha, se desconoce cómo accedieron los agresores a los servidores de SITA y tampoco se sabe cómo accedieron a Air India o si lo hicieron realmente.



5. ANÁLISIS DE INCIDENTES EN LA CADENA DE SUMINISTRO

En esta sección presentamos un análisis de los ataques a la cadena de suministro basado en los ataques denunciados desde principios de 2020 hasta principios de julio de 2021. El análisis se centra en los ataques conocidos públicamente a la cadena de suministro. En el anexo A puede encontrarse una descripción detallada. Como se comenta más adelante, algunos ataques parecían ser ataques a la cadena de suministro, pero no lo eran, por lo que no se incluyeron en el análisis. En el cuadro 12 figura un resumen de todos los incidentes analizados en el informe.

Cuadro12: Resumen de los ataques a la cadena de suministro identificados, analizados y validados desde enero de 2020 hasta principios de julio de 2021.

PROVEEDOR	CATEGORÍA DEL PROVEEDOR	AÑO	IMPACTO	GRUPOS A LOS QUE SE ATRIBUYE EL ATAQUE
Mimecast	Programas informáticos de seguridad	2021	Global	APT29
SITA	Aviación	2021	Global	APTA41
Ledger	Cadena de bloques	2021	Global	-
Verkada	Seguridad física	2021	Global	Hacktivist Group
BigNox NoxPlayer	Programas informáticos	2021	Regional	-
Stock Investment Messenger	Programas informáticos financieros	2021	Regional	Thallium APT
ClickStudios	Programas informáticos de seguridad	2021	Regional	-
Apple Xcode	Programas informáticos de desarrollo	2021	Global	-
SITIO WEB DE LA PRESIDENCIA DE MYANMAR	Administración pública	2021	Regional	Mustang Panda APT
Ucrania SEI EB	Administración pública	2021	Regional	-
Codecov	Programas informáticos para empresas	2021	Global	-
Fujitsu ProjectWEB	Colaboración en la nube	2021	Regional	-
Kaseya	Gestión de los sistemas informáticos	2021	Global	REvil Group
MonPass	Autoridad de certificación	2021	Regional	Winnti APT Group
SYNNEX	Distribuidor de tecnología	2021	Regional	APT 29
Microsoft Windows HCP	Programas informáticos	2021	Global	-
SolarWinds	Gestión en la nube	2020	Global	APT29
Accellion	Programas informáticos de seguridad	2020	Global	UNC2546

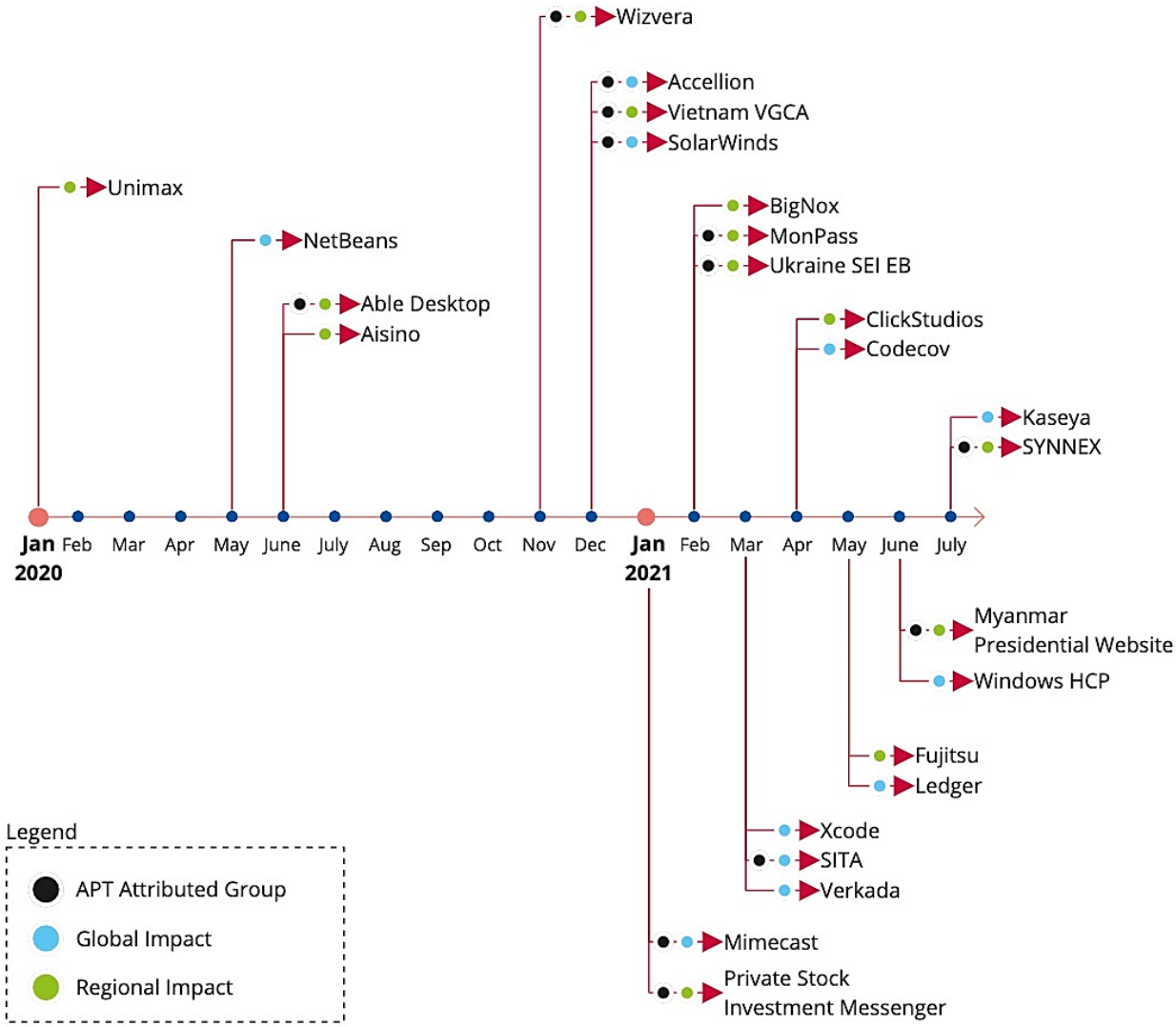
Wizvera VeraPort	Gestión de la identidad	2020	Regional	Lazarus APT
Able Desktop	Programas informáticos para empresas	2020	Regional	TA428
Aisino	Programas informáticos financieros	2020	Regional	-
Vietnam VGCA	Autoridad de certificación	2020	Regional	TA413, TA428
NetBeans	Programas informáticos de desarrollo	2020	Global	-
Unimax	Telecomunicaciones	2020	Regional	-

5.1. CRONOLOGÍA DE LOS ATAQUES A LA CADENA DE SUMINISTRO

El análisis muestra que, de veinticuatro ataques confirmados a la cadena de suministro, ocho (33 %) se notificaron en 2020 y dieciséis (66 %) entre enero de 2021 y principios de julio de 2021. **Basándose en estos datos, la tendencia prevé que en 2021 puede haber cuatro veces más ataques a la cadena de suministro que en 2020.**

En la figura 8 se muestra una cronología de los ataques analizados en este informe, destacando aquellos incidentes que se atribuyeron a grupos de APT y si tuvieron un impacto global o regional. El impacto se clasifica en cada ataque como global o regional. Se considera que los ataques tienen un impacto global si su base de clientes es global o si el número de usuarios finales posiblemente afectados es de millones. Por otra parte, se considera que los ataques que afectan a los usuarios de una región o un país específico, o que afectan solo a un grupo de usuarios, tienen un impacto regional.

Figura 8: Cronología de los ataques a la cadena de suministro notificados desde enero de 2020 hasta principios de julio de 2021. El mes indicado en la ilustración se refiere al mes en que se reportó el incidente y no al momento en que ocurrió el ataque. Los incidentes atribuidos a grupos de APT están marcados con puntos negros, los incidentes con impacto global están marcados con puntos de color violeta y los incidentes con impacto regional están marcados con puntos de color verde. En el anexo A figura un resumen detallado de cada incidente.



5.2. COMPRENDER EL FLUJO DE ATAQUES

Cada uno de los incidentes mostrados en la figura 7 se ha analizado, resumido y clasificado con arreglo a la taxonomía propuesta. La taxonomía apoya y facilita el estudio de los ataques a la cadena de suministro en su conjunto de forma estructurada.

La figura 8 es un diagrama de Sankey[38] que ilustra el flujo de las técnicas de ataque y los activos más comunes observados en los ataques a la cadena de suministro que se han estudiado en este informe. **Las técnicas de ataque [ST] se utilizan contra los activos del proveedor [SA], que se utilizan en técnicas de ataque [CT] para comprometer los activos de los clientes [CA].**

De la figura 8 se desprende claramente que la mayoría de las técnicas de ataque utilizadas para comprometer al proveedor (primera columna [ST]) pertenecen a las categorías siguientes:

- **Desconocido (66 %)**, seguido de

[38] Los diagramas de Sankey son un tipo específico de diagramas de operaciones lógicas, en el que el ancho de las flechas es proporcional a la cantidad de operaciones lógicas.

- **Aprovechamiento de la vulnerabilidades del software (16 %)**.

En cuanto a los activos de los proveedores atacados (segunda columna [SA]), la mayoría de los ataques tenían como objetivo poner en peligro:

- **Código (66 %)**,
- **Datos (20 %),**
- **Procesos (12 %)**.

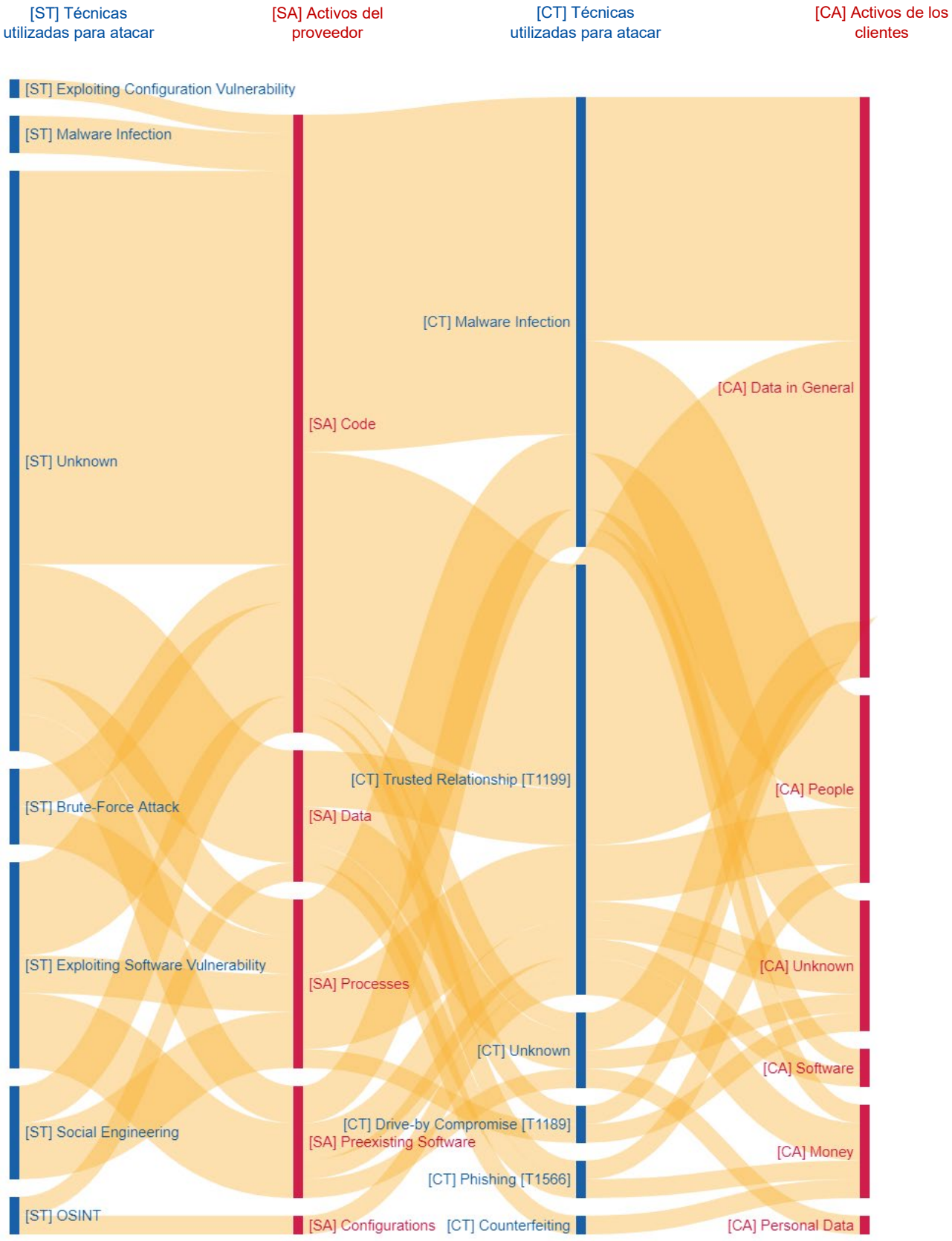
Los activos de los proveedores comprometidos se utilizan como vector de ataque para comprometer a los clientes. Estos ataques se producen principalmente (tercera columna [CT]):

- **abusando de la confianza del cliente (62 %)** en el proveedor, o
- utilizando **software malicioso (62 %)**.

Independientemente de la técnica utilizada, la mayoría de los ataques a la cadena de suministro tienen por objeto obtener acceso a (cuarta columna [AC]):

- **Datos del cliente (58 %)**,
- **Personas clave (16 %)** y
- **Recursos financieros (8 %)**.

Figura 9: Análisis de incidentes en la cadena de suministro basado en la taxonomía propuesta. El diagrama de Sankey muestra el flujo de técnicas de ataque [ST] contra los activos del proveedor [SA], que luego se utilizan en técnicas de ataque [CT] para comprometer los activos de los clientes [CA]. La amplitud de las conexiones entre los distintos elementos aumenta cuando la relación se ha observado en un mayor número de ataques a la cadena de suministro.


[ST] Técnicas utilizadas para atacar
[SA] Activos del proveedor
[CT] Técnicas utilizadas para atacar
[CA] Activos de los clientes
[ST] Exploiting Configuration Vulnerability
[ST] Malware Infection
[ST] Unknown
[ST] Brute-Force Attack
[ST] Exploiting Software Vulnerability
[ST] Social Engineering
[ST] OSINT
[SA] Code
[SA] Data
[SA] Processes
[SA] Preexisting Software
[SA] Configurations
[CT] Malware Infection
[CT] Trusted Relationship [T1199]
[CT] Unknown
[CT] Drive-by Compromise [T1189]
[CT] Phishing [T1566]
[CT] Counterfeiting
[CA] Data in General
[CA] People
[CA] Unknown
[CA] Software
[CA] Money
[CA] Personal Data

5.3. AGRESORES ORIENTADOS A OBJETIVOS

Al considerar los activos objetivo, en el **66 %** de los incidentes, los agresores se centraron en el **código** de los proveedores para comprometer aún más a los clientes objetivo. En el **20 %** de los incidentes analizados, el objetivo de los agresores eran los **datos** y en el **12 %** los objetivos del ataque contra el proveedor eran **procesos internos**. Esto es clave para entender dónde centrar los esfuerzos en términos de protección de la ciberseguridad. Las organizaciones deben centrar sus esfuerzos en validar el código y los programas informáticos de terceros para garantizar que no se han manipulado.

Los activos finales de los clientes afectados por estos ataques a la cadena de suministro parecen ser principalmente datos de clientes, incluidos datos personales y propiedad intelectual e industrial. Este fue el caso en el 58 % de los incidentes de la cadena de suministro analizados. Los agresores también atacaron en menor medida otros activos, como personas, programas informáticos y recursos financieros.

5.4. LA MAYORÍA DE LOS VECTORES DE ATAQUE PARA COMPROMETER A LOS PROVEEDORES SIGUEN SIENDO DESCONOCIDOS

Nuestros resultados indican que en el **66 %** de los ataques a la cadena de suministro analizados, **los proveedores no sabían**, o no fueron transparentes, sobre cómo se vieron comprometidos. Por el contrario, menos del **9 %** de los clientes afectados por ataques a la cadena de suministro desconocían cómo se produjeron los ataques. **Esto pone de manifiesto la brecha, en términos de madurez, en la notificación de incidentes de ciberseguridad entre los proveedores y las empresas orientadas al usuario final.**

Teniendo en cuenta que el **83 %** de los proveedores pertenecen al sector **tecnológico**, la falta de conocimiento sobre cómo se produjeron los ataques podría indicar un **bajo nivel de madurez** en lo que respecta a la ciberdefensa en la infraestructura de los proveedores o la falta de voluntad para compartir la información correspondiente. Hay otros factores que pueden contribuir a la falta de comprensión de cómo se ven comprometidos los proveedores, como la complejidad y sofisticación de los ataques y la lentitud para descubrirlos, lo que a su vez puede dificultar la investigación.

5.5. ATAQUES SOFISTICADOS ATRIBUIDOS A GRUPOS DE APT

Más del **50 % de los ataques a la cadena de suministro se atribuyeron a** grupos de ciberdelincuencia conocidos, como APT29, APT41, Thallium APT, UNC2546, Lazarus APT, TA413 y TA428. El análisis muestra que los grupos de APT parecen tener una ligera preferencia por los objetivos con impacto regional, y que un número significativo de estos ataques tenían como objetivo obtener acceso a los datos de los clientes.

De los veinticuatro incidentes analizados, diez no se atribuyeron a ningún grupo determinado. La razón principal de esta falta de atribución puede ser que siete de estos ataques ocurrieron en los últimos siete meses. Este tipo de incidentes pueden tardar más tiempo en investigarse e incluso entonces, en ciertos casos, siguen sin poder atribuirse a un grupo concreto. Sin embargo, dada la sofisticación de estos ataques, los proveedores deben esperar ser el objetivo de los grupos organizados de ciberdelincuentes y prepararse en consecuencia.

6. NO TODO PUEDE CONSIDERARSE UN ATAQUE A LA CADENA DE SUMINISTRO

Desde enero de 2020 hasta principios de julio de 2021, hubo muchos incidentes que inicialmente **parecían** ser ataques a la cadena de suministro o que se consideraban parte de un probable ataque futuro a la cadena de suministro. Se notificaron muchas de las vulnerabilidades del software tradicionales detectadas como un «riesgo» para futuros ataques a la cadena de suministro. En algunos casos se trataba de vulnerabilidades que se creía que se habían introducido intencionadamente en el programa informático o en el equipo informático, pero que luego se descubrió que eran bugs o errores involuntarios. Muchos de estos casos no podían considerarse como ataques a la cadena de suministro, ya que no implicaban poner en peligro a un proveedor.

Al menos en tres ocasiones, los agresores atacaron bibliotecas o dependencias de software. En uno de estos casos, notificado en diciembre de 2020, los agresores cargaron paquetes maliciosos en el depósito de RubyGems[39]. En marzo de 2021 se informó de un caso muy similar, cuando un investigador de seguridad consiguió cargar paquetes NPM maliciosos utilizando nombres que se sabe que son los de componentes o infraestructuras utilizados por empresas conocidas[40]. Se informó de un tercer caso en abril de 2021, cuando los agresores cargaron un paquete NPM malicioso tratando de suplantar deliberadamente un paquete conocido en un ataque denominado brandjacking[41]. En todos estos casos, los agresores no pusieron en peligro los paquetes existentes ni los depósitos de software, por lo que, al no haber un ataque claro a los activos de los proveedores, no los consideramos ataques a la cadena de suministro.

En muchos casos, se descubrieron las vulnerabilidades del software pero no se utilizaron en los ataques, o se descubrió que eran errores y que no se habían introducido intencionalmente. El primer ejemplo de este caso se notificó en febrero de 2020, en el que un investigador de seguridad reveló una vulnerabilidad de día cero en el microprograma desarrollado por la empresa Xiaongmai y utilizado para DVR, NVR y cámaras IP[42]. Otros ejemplos son las vulnerabilidades notificadas en las extensiones de código de Visual Studio en mayo de 2021[43] y en los mercados de software libre y de código abierto (FOSS) basados en Pling en junio de 2021[44]. En todos estos casos, se descubrieron vulnerabilidades, aunque no se había informado de ningún ataque activo que las hubiera utilizado en el momento de redactar este informe. Como se ha mencionado en secciones anteriores, un ataque a la cadena de suministro implica al menos dos ataques, a saber, contra un proveedor y contra un cliente. No se considera un ataque a la cadena de suministro si no se ataca a un cliente o a un proveedor.

Además, hubo otros casos de ataques a la ciberseguridad y vulnerabilidades que no pueden considerarse ataques a la cadena de suministro. Uno de esos casos fue el ataque a los sistemas de Centreon. Centreon es una empresa que presta servicios de supervisión de TI y ofrece una herramienta de supervisión informática de código abierto. En enero de 2021, se descubrió que los agresores habían aprovechado instancias públicas obsoletas de Centreon para

[39] Russian Sandworm hackers only hit orgs with old Centreon software, Bleeping Computer, https://www.bleepingcomputer.com/news/security/russian-sandworm-hackers-only-hit-orgs-with-old-centreon-software/. Consultado el 8 de julio de 2021.
[40] Malicious NPM packages target Amazon, Slack with new dependency attacks, Bleeping Computer, https://www.bleepingcomputer.com/news/security/malicious-npm-packages-target-amazon-slack-with-new-dependency-attacks/. Consultado el 8 de julio de 2021.
[41] Damaging Linux \& Mac Malware Bundled within Browserify npm Brandjack Attempt, Sonatype, https://blog.sonatype.com/damaging-linux-mac-malware-bundled-within-browserify-npm-brandjack-attempt. Consultado el 8 de julio de 2021.
[42] Full disclosure: 0day vulnerability (backdoor) in firmware for Xiaongmai-based DVRs, NVRs and IP cameras, Habr, https://habr.com/en/post/486856/. Consultado el 8 de julio de 2021.
[43] Newly Discovered Bugs in VSCode Extensions Could Lead to Supply Chain Attacks, The Hacker News, https://thehackernews.com/2021/05/newly-discovered-bugs-in-vscode.html. Consultado el 8 de julio de 2021.
[44] Unpatched Flaw in Linux Pling Store Apps Could Lead to Supply-Chain Attacks, The Hacker News, https://thehackernews.com/2021/06/unpatched-critical-flaw-affects-pling.html. Consultado el 8 de julio de 2021.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

comprometer la infraestructura de los clientes[45,46,47]. Los agresores, que se cree que pertenecían al grupo Sandworm APT, llevaron a cabo su campaña durante tres años hasta que fueron descubiertos. El objetivo del ataque era extraer información de los clientes afectados. El ataque estaba dirigido a proveedores de servicios TI franceses. Este es un caso en el que se ha aprovechado una vulnerabilidad de software concreta en un programa informático instalado por los clientes. Sin embargo, el proveedor no se vio comprometido y las vulnerabilidades no fueron intencionadas.

[45] Sandworm Intrusion Set Campaign Targeting Centreon Systems, CERT-FR, https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf. Consultado el 8 de julio de 2021.
[46] France Reveals 3-Year Long Supply Chain Attack, Secure World Expo, https://www.secureworldexpo.com/industry-news/france-supply-chain-attack-centreon-software. Consultado el 8 de julio de 2021.
[47] Russian Sandworm hackers only hit orgs with old Centreon software, Bleeping Computer, https://www.bleepingcomputer.com/news/security/russian-sandworm-hackers-only-hit-orgs-with-old-centreon-software/. Consultado el 08 de julio de 2021.

7. RECOMENDACIONES

Los ataques a la cadena de suministro **aprovechan la interconexión de los mercados globales**. Cuando varios clientes confían en el mismo proveedor, se amplifican las consecuencias de un ciberataque contra este proveedor, pudiendo tener un impacto nacional a gran escala o incluso traspasar fronteras. En el caso de algunos productos, como los programas informáticos y los códigos ejecutables, la existencia de una cadena de suministro es opaca o incluso está completamente oculta para el usuario final. Los programas informáticos del usuario final dependen, directa o indirectamente, del programa informático suministrado por el proveedor. Estas dependencias incluyen paquetes, bibliotecas y módulos, todos ellos utilizados de forma generalizada para reducir los costes de desarrollo y acelerar los plazos de entrega.

A medida que las organizaciones vayan mejorando la protección frente a los ciberataques, se prestará una atención mayor a los proveedores. El cálculo es simple: los proveedores se están convirtiendo en el eslabón más débil de la cadena de suministro. Al mismo tiempo, los clientes demandan productos más ciberseguros pero que tengan un coste bajo, dos necesidades que no siempre es posible conciliar.

Como hemos observado en numerosos incidentes de ataques a la cadena de suministro, las organizaciones son cada vez más conscientes de la necesidad de **evaluar la madurez de la ciberseguridad de sus proveedores** y el **nivel de exposición al riesgo derivado de la relación cliente-proveedor**. Los clientes deben evaluar y tener en cuenta la calidad general de los productos y las prácticas de ciberseguridad de sus proveedores, incluyendo si aplican procedimientos de desarrollo seguro. Además, los clientes deben actuar con mayor diligencia a la hora de seleccionar y analizar a sus proveedores, y en la gestión del riesgo derivado de estas relaciones.

Para **gestionar el riesgo de ciberseguridad de la cadena de suministro**, los clientes deben[48]:

- identificar y documentar los tipos de proveedores de servicios y productos;
- definir criterios de riesgo para diferentes tipos de proveedores y servicios (por ejemplo, dependencias importantes de proveedores y clientes, dependencias de software crítico, puntos únicos de fallo);
- evaluar los riesgos de la cadena de suministro de acuerdo con sus propias evaluaciones del impacto y requisitos de la continuidad de la actividad;
- definir medidas para el tratamiento de riesgos basadas en buenas prácticas;
- vigilar los riesgos y amenazas de la cadena de suministro, basándose en fuentes de información internas y externas y en los resultados de la supervisión y revisión del rendimiento de los proveedores;
- informar a su personal del riesgo.

Para **gestionar la relación con los proveedores**, los clientes deben:

- gestionar proveedores a lo largo de todo el ciclo de vida de un producto o servicio, incluidos procedimientos para gestionar productos o componentes al final de su vida útil;
- clasificar los activos y la información que se comparten con o son accesibles para los proveedores, y definir los procedimientos pertinentes para su acceso y tratamiento;
- definir las obligaciones de los proveedores para la protección de los activos de la organización, para el intercambio de información, para los derechos de auditoría, para la continuidad de la actividad, para la selección del personal y para la gestión de incidentes en términos de responsabilidades, obligaciones de notificación y procedimientos;
- definir requisitos de seguridad para los productos y servicios adquiridos;
- incluir todas estas obligaciones y requisitos en los contratos; acordar normas para la subcontratación y posibles requisitos en cascada;

[48] Derivado de los controles de ciberseguridad de las normas ISO/IEC 27002, ISO 9001 e ISO 31000.

- supervisar la calidad del servicio y realizar auditorías de seguridad rutinarias para verificar la conformidad de los requisitos de ciberseguridad en los contratos; esto incluye la gestión de incidentes, vulnerabilidades, parches, requisitos de seguridad, etc.;
- recibir garantías de los proveedores de servicios y productos de que no se incluyen a sabiendas prestaciones ocultas ni puertas traseras;
- garantizar que se tienen en cuenta las disposiciones legales y reglamentarias;
- definir procesos para gestionar cambios en los acuerdos con proveedores, por ejemplo, cambios en herramientas, tecnologías, etc.

Por otra parte, los proveedores deben garantizar el **desarrollo seguro de productos y servicios** que sea coherente con las prácticas de seguridad comúnmente aceptadas[49]. Los proveedores deben:

- garantizar que la infraestructura utilizada para diseñar, desarrollar, fabricar y entregar productos, componentes y servicios sigue las prácticas de ciberseguridad[50,51];
- implementar un proceso de desarrollo, mantenimiento y soporte de productos que sea coherente con los procesos de desarrollo de productos comúnmente aceptados;
- implementar un proceso de ingeniería seguro que sea coherente con las prácticas de seguridad comúnmente aceptadas[52, 53],
- considerar la aplicabilidad de las normas técnicas en función de la categoría de productos y los riesgos[54],
- ofrecer declaraciones de conformidad a los clientes para las normas conocidas, como ISO/IEC 27001, IEC 62443-4-1, IEC 62443-4-2 (o normas específicas como la CSA Cloud Controls Matrix (CCM) para servicios en la nube), y garantizar y certificar, en la medida de lo posible, la integridad y el origen de los programas informáticos de código abierto utilizado en cualquier parte de un producto,
- definir objetivos de calidad, como el número de defectos o vulnerabilidades identificados externamente o asuntos de seguridad denunciados externamente, y utilizarlos como instrumento para mejorar la calidad general;
- mantener datos precisos y actualizados sobre el origen del código o los componentes de programas informáticos, y sobre los controles aplicados a los componentes, herramientas y servicios de programas informáticos internos y de terceros presentes en los procesos de desarrollo de software,
- realizar auditorías periódicas para garantizar el cumplimiento de las medidas anteriores.

Además, como todo producto o servicio se construye a partir de componentes y programas informáticos o se basa en ellos, los proveedores **deben implementar buenas prácticas para la gestión de vulnerabilidades**[55], tales como:

- el seguimiento de las vulnerabilidades de seguridad notificadas por fuentes internas y externas que incluye los componentes de terceros utilizados,
- el análisis de riesgos de vulnerabilidades mediante el uso de un sistema de calificación de vulnerabilidades (por ejemplo, CVSS[56]),
- políticas de mantenimiento para el tratamiento de vulnerabilidades identificadas dependiendo del riesgo,
- procesos para informar a los clientes,

[49] por ejemplo, IEC 62443-4-1.
[50] por ejemplo, los de la norma ISO/IEC 27001.
[51] Estas pueden incluir medidas técnicas, como (a) separación de entornos; (b) auditoría de relaciones de confianza; (c) establecimiento de autenticación multifactor basada en el riesgo y acceso condicional en toda la organización; (d) minimización de las dependencias de productos que forman parte de los entornos utilizados para desarrollar, construir y editar programas informáticos; (e) cifrado de datos; f) supervisión de operaciones y avisos y respuesta ante incidentes de ciberseguridad reales así como tentativas.
[52] por ejemplo, IEC 62443-2-4
[53] Estas pueden incluir la utilización de herramientas automatizadas o procesos comparables para mantener cadenas de suministro de código fuente fiables, garantizando así la integridad del código; o la utilización de herramientas automatizadas o procesos comparables que comprueben la existencia de vulnerabilidades conocidas y potenciales y las corrijan.
[54] Normas como la IEC 62443-4-2 ofrecen un conjunto completo de requisitos de seguridad que se clasifican en requisitos aplicables a todos los productos, aplicables a los programas informáticos (SAR), aplicables a los dispositivos integrados (EDR), aplicables a los dispositivos de ordenador central (HDR) y aplicables a los dispositivos de red (NDR).
[55] Encontrará más información sobre la gestión de vulnerabilidades y parches en las normas IEC 62443-4-1, IEC 62443-2-4 e IEC TR 62443-2-3.
[56] Consulte https://www.first.org/cvss/specification-document ;.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

- verificación y prueba de parches para garantizar que se cumplen los requisitos operativos, de seguridad, legales y de ciberseguridad y que el parche es compatible con componentes de terceros no predefinidos;
- procesos de entrega segura de parches y documentación relativa a los parches a los clientes, o
- participar en un programa de divulgación de vulnerabilidades que incluya un proceso de información y divulgación.

Los proveedores deben gestionar las vulnerabilidades mediante parches. Asimismo, los clientes deben vigilar el mercado en busca de posibles vulnerabilidades o recibir las respectivas notificaciones de vulnerabilidades de sus proveedores. Algunas **buenas prácticas para la gestión de parches** son[57]:

- mantener un inventario de activos que incluya información relevante para los parches,
- utilizar recursos de información para identificar vulnerabilidades técnicas relevantes,
- evaluar los riesgos de las vulnerabilidades identificadas y disponer de una política de mantenimiento documentada e implementada,
- recibir parches únicamente de fuentes legítimas y probarlos antes de su instalación,
- aplicar medidas alternativas en caso de que no se disponga o no se pueda aplicar un parche;
- aplicar procedimientos de reversión y procesos eficaces de copia de seguridad y restauración.

Aparte de lo que los clientes y proveedores pueden hacer individualmente, hay iniciativas que pueden tener lugar a nivel sectorial. Google introdujo, en junio de 2021, un sistema de extremo a extremo para garantizar la integridad de los artefactos de software en toda la cadena de suministro de programas informáticos denominado SLSA (Supply chain Levels for Software Artifacts)[58]. El objetivo de SLSA es mejorar el estado del sector, especialmente la información de dominio público, para defenderse de las amenazas más urgentes a la integridad. Aunque SLSA se centra en los ataques a la cadena de suministro de programas informáticos y no en los demás tipos, es un buen punto de partida que puede beneficiar a las organizaciones.

En junio de 2021, MITRE lanzó un conjunto de recomendaciones más general pero exhaustivo para defenderse de las amenazas informáticas, conocido como el proyecto MITRE D3FEND[59]. MITRE D3FEND es un sistema o base de conocimientos estructurada que permite a las organizaciones encontrar alivios concretos para evitar ataques específicos, como se muestra en el sistema MITRE ATT&CK®. El proyecto no es específico de la cadena de suministro ni de los ataques de APT, sino que las recomendaciones pueden utilizarse para aumentar el nivel básico de seguridad de las organizaciones.

Sin embargo, no todos los riesgos de la cadena de suministro pueden mitigarse mediante la aplicación de buenas prácticas por parte de clientes, proveedores u organizaciones. En particular, no se pueden identificar exhaustivamente las funciones ocultas y las capacidades de acceso indocumentado (puertas traseras) en componentes de equipos informáticos mediante las certificaciones más comunes o las pruebas de penetración estándar. Además, las vulnerabilidades de día cero, es decir, las vulnerabilidades que solo un grupo específico conoce y utiliza, siguen siendo un problema. Por consiguiente, puede ser necesario actuar a nivel nacional o incluso europeo. Los servicios competentes nacionales podrían realizar evaluaciones de riesgos para la seguridad nacional en relación con los riesgos de la cadena de suministro, que tengan en cuenta a los agentes conocidos para obtener medidas sobre la contratación de proveedores a escala nacional. Además, los ataques a la cadena de suministro pueden estar patrocinados por agentes estatales con capacidades avanzadas y, en este caso, puede ser necesaria la asistencia de las autoridades correspondientes para mitigar los riesgos de los ataques patrocinados por los estados.

[57] Derivadas de la ISO/IEC 27002.
[58] Google Online Security Blog: Introducing SLSA, an End-to-End Framework for Supply Chain Integrity, Google, https://security.googleblog.com/2021/06/introducing-slsa-end-to-end-framework.html. Consultado el 8 de julio de 2021.
[59] MITRE D3FEND™, D3FEND Matrix, versión 0.9.2-BETA-3, https://d3fend.mitre.org/. Consultado el 29 de junio de 2021.

8. CONCLUSIONES

A medida que aumenta el coste de los ataques directos contra organizaciones bien protegidas, los agresores prefieren atacar su cadena de suministro, lo que supone la motivación adicional de un impacto potencial a gran escala que traspasa fronteras. Este cambio ha supuesto que se notifiquen un **número mayor de casos de ataques a la cadena de suministro**, con una previsión **de cuatro veces más ataques a la cadena de suministro en 2021 que en 2020**. La naturaleza global inherente a las cadenas de suministro actuales aumenta el impacto potencial de estos ataques y amplía la superficie de ataque para los agresores. Este informe abarca una serie de ataques conocidos pero, en realidad, puede haber más ataques a la cadena de suministro que no se detectan, no se investigan o se atribuyen a otras causas.

Especialmente en el ámbito de los programas informáticos, los ataques a la cadena de suministro socavan la confianza en el ecosistema de los programas informáticos. Los incidentes descritos resaltan la posibilidad de que agentes maliciosos **comprometan la cadena de suministro de los programas informáticos desde sus primeras etapas** (fase experimental). Es necesario desarrollar nuevos enfoques para asegurar la cadena de suministro mediante el diseño. En esta dirección, hay nuevas iniciativas como Google SLSA y MITRE D3FEND bastante prometedoras.

El análisis de este informe muestra que todavía hay un gran número de factores desconocidos en los incidentes investigados. **El 66 % de los vectores de ataque utilizados en los proveedores siguen siendo desconocidos**. La falta de transparencia o de capacidad de investigación supone un grave riesgo para la confianza de la cadena de suministro. El primer paso para mejorar la seguridad de todos los elementos de la cadena de suministro y proteger a los clientes finales es mejorar el proceso de transparencia y responsabilidad.

Los ataques a la cadena de suministro pueden ser complejos, requieren una cuidadosa planificación y a menudo tardan meses o años en ejecutarse. Aunque **más del 50 % de estos ataques se atribuyen a grupos de amenazas persistentes avanzadas o a agresores conocidos**, la eficacia de los ataques a la cadena de suministro puede convertir a los proveedores en un objetivo interesante para otros tipos de agresores más genéricos en el futuro. Por lo tanto, es fundamental que las organizaciones pongan el foco de su seguridad no solo en sus propias organizaciones, sino también en sus proveedores. Este es especialmente el caso de los proveedores de servicios en la nube y los proveedores de servicios gestionados, donde los ataques recientes ponen de manifiesto la creciente necesidad de controles de ciberseguridad en estos sectores.

Debido al aumento de las interdependencias y las complejidades, el impacto de los ataques sobre los proveedores puede tener **consecuencias de largo alcance**. Esto no solo se debe al gran número de afectados, sino que, especialmente en los casos en que se extrae información clasificada, es motivo de preocupación para la seguridad nacional o puede tener consecuencias de naturaleza geopolítica.

En este complejo entorno para las cadenas de suministro, tanto el establecimiento de **buenas prácticas a escala de la UE como las acciones de coordinación son importantes** para ayudar a todos los Estados miembros a desarrollar capacidades similares, con el fin de alcanzar un nivel común de seguridad.

ANEXO A: RESUMEN DE LOS ATAQUES DE LA CADENA DE SUMINISTRO

En esta sección se presenta un resumen de los veinticuatro incidentes de la cadena de suministro identificados y analizados en el presente informe. Cada incidente se identifica por el proveedor implicado en el ataque. La taxonomía propuesta en este informe se aplica a cada caso. Además, se incluye un gráfico que ilustra cómo se produjo el ataque para mayor claridad. La información incluida en los resúmenes se refiere a la información disponible en el momento de redactar este informe.

LISTA DE INCIDENTES EN LA CADENA DE SUMINISTRO:

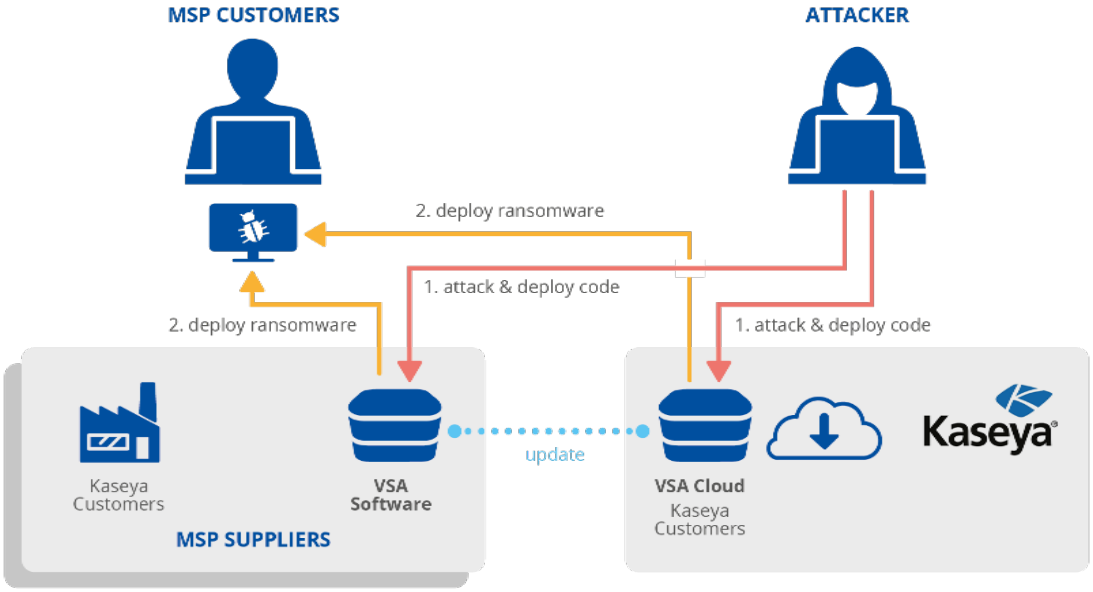
A.1 KASEYA: GESTIÓN DE UN SOFTWARE DE TI

Kaseya[60] es un proveedor de servicios de programas informáticos especializado en herramientas de supervisión y gestión remotas. Ofrece programas informáticos VSA (Virtual System/Server Administrator) y proporciona sus propios servidores en la nube. Los MSP (proveedores de servicios gestionados) pueden utilizar los programas informáticos VSA en sus instalaciones o pueden obtener una licencia para los servidores en la nube VSA de Kaseya. A su vez, los MSP ofrecen varios servicios de TI a otros clientes[61].

En julio de 2021, los agresores aprovecharon una vulnerabilidad de día cero en los sistemas de Kaseya (CVE-2021-30116[62]). Los agresores consiguieron ejecutar comandos de forma remota en los dispositivos VSA de los clientes de Kaseya. Kaseya puede enviar actualizaciones remotas a todos los servidores VSA y, el viernes 2 de julio de 2021, se distribuyó una actualización a los VSA de los clientes de Kaseya que ejecutó código de los agresores. A su vez, este código malicioso instaló un programa de secuestro[63,64] en los clientes gestionados por ese VSA.

PROVEEDOR	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro
Aprovecharse de la vulnerabilidad del software	Programa informático preexistente

CLIENTE	
Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Relación de confianza [T1199], Infección de software malicioso	Datos, Finanzas

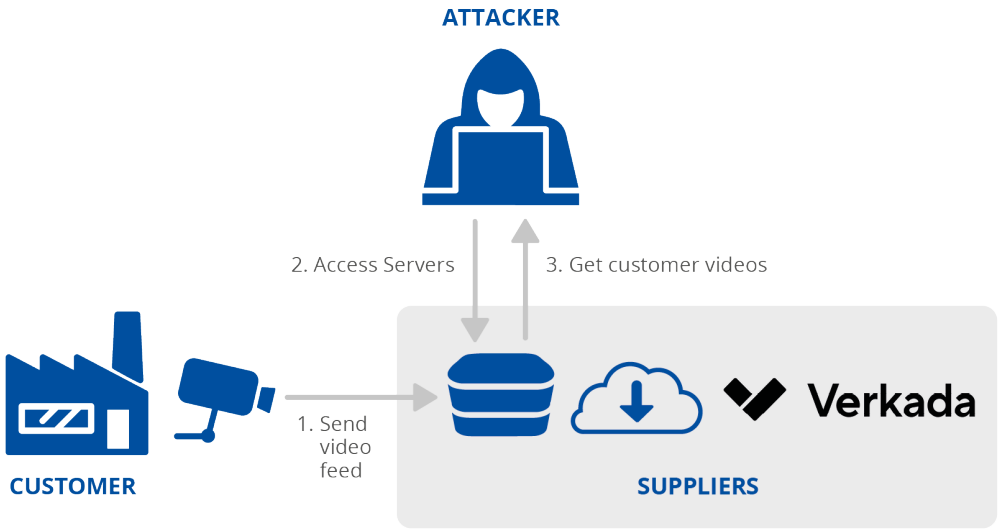


[60] IT Management Software - for MSPs and IT Teams, Kaseya, https://www.kaseya.com/. Consultado el 9 de julio de 2021.
[61] Ransomware Hits Hundreds of US Companies, Security Firm Says, NBC10 Philadelphia, https://www.nbcphiladelphia.com/news/national-international/new-ransomware-attack-paralyzes-hundreds-of-u-s-companies/2868462/. Consultado el 9 de julio de 2021.
[62] CVE-2021-30116, MITRE, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30116, Consultado el 9 de julio de 2021.
[63] Kaseya VSA vulnerability opens a thousand-plus business doors to ransomware, Blocks and Files, https://blocksandfiles.com/2021/07/04/kaseya-vsa-vulnerability-opens-1000-plus-business-doors-to-let-in-ransomware/, Consultado el 9 de julio de 2021.
[64] Hundreds of Businesses, From Sweden to U.S., Affected by Cyberattack, The New York Times, https://www.nytimes.com/2021/07/02/technology/cyberattack-businesses-ransom.html. Consultado el 9 de julio de 2021.

A.2 VERKADA: SOLUCIONES DE VIGILANCIA DE LA SEGURIDAD BASADAS EN LA NUBE

Verkada ofrece soluciones de vigilancia de la seguridad basadas en la nube a más de 5 000 clientes[65]. En marzo de 2021, se vio comprometido un servidor de producción. Esto permitió a los agresores, que obtuvieron las credenciales privilegiadas, acceder a las cámaras de seguridad alojadas en las instalaciones de los clientes[66]. Supuestamente, las credenciales se encontraron «en Internet»[67]. Los agresores obtuvieron acceso a los vídeos e imágenes de los clientes de más de 150 000 cámaras situadas en escuelas, cárceles, hospitales, comisarías de policía y fábricas de Tesla[68]. Un grupo hacktivista reivindicó el ataque[69].

PROVEEDOR		CLIENTE	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro	Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
OSINT	Configuraciones, Datos	Relación de confianza [T1199]	Datos



[65] The Future of Physical Security for the Enterprise: About Verkada, Verkada, https://www.verkada.com/about/. Consultado el 9 de julio de 2021.
[66] Verkada Security Update, Verkada, https://www.verkada.com/security-update/. Consultado el 9 de julio de 2021.
[67] Verkada Mass Hack, IPVM, https://ipvm.com/reports/verkada-hack.Consultado el 9 de julio de 2021.
[68] A hacker who exposed Verkada's surveillance camera snafu has been raided, The Verge, https://www.theverge.com/2021/3/12/22328344/tillie-kottmann-hacker-raid-switzerland-verkada-cameras. Consultado el 9 de julio de 2021.
[69] Tesla (TSLA), Cloudfare (NET) Breach in Verkada Security Camera Hack, Bloomberg, https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams. Consultado el 9 de julio de 2021.

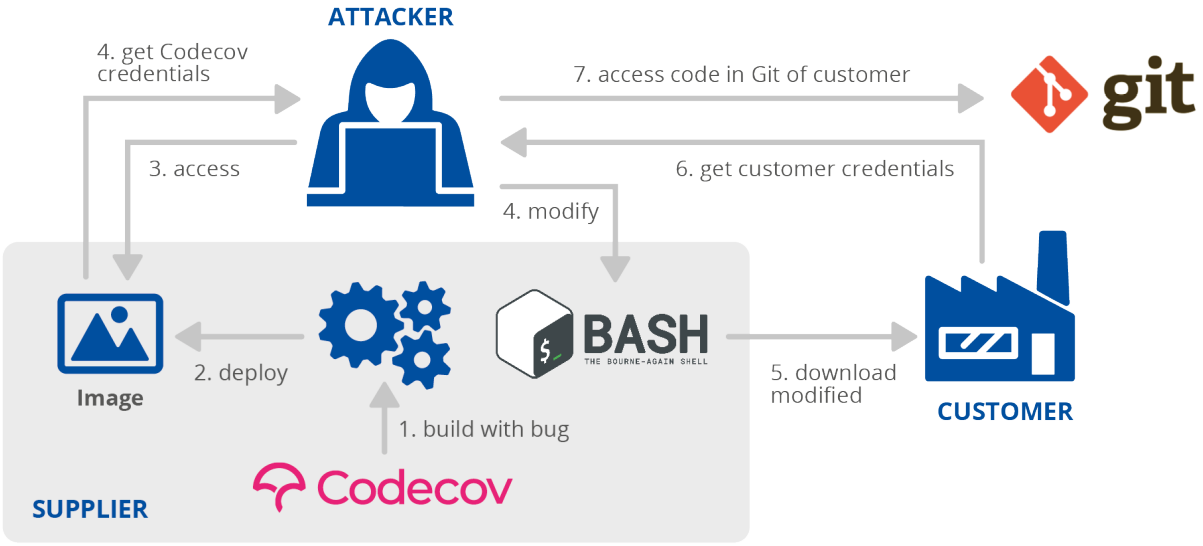
A.3 CODECOV: SOLUCIONES DE GESTIÓN DE CÓDIGO Y AUDITORÍA

Codecov es una empresa que proporciona programas informáticos para herramientas de pruebas y cobertura de código. La empresa suministra herramientas a otras empresas como IBM y Hewlett Packard Enterprise. En abril de 2021, Codecov informó de que los agresores obtuvieron algunas de sus credenciales válidas de una imagen en Docker debido a un error en la forma en que se crearon esas imágenes Docker.

Una vez que los agresores obtuvieron estas credenciales, las utilizaron para comprometer un «script bash de carga»[70] que utilizan los clientes de Codecov. Una vez que los clientes descargaron y ejecutaron este script, los agresores pudieron extraer datos de los clientes de Codecov, incluida información delicada que les permitiría acceder a los recursos de los clientes[71]. Varios clientes de Codecov informaron de que los agresores podían acceder a su código fuente utilizando información robada procedente de la violación de la seguridad del sistema de Codecov[71]. No se identificó a los agresores del ataque.

PROVEEDOR	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro
Aprovecharse de la vulnerabilidad de configuración	Código

CLIENTE	
Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Relación de confianza [T1199]	Programas informáticos



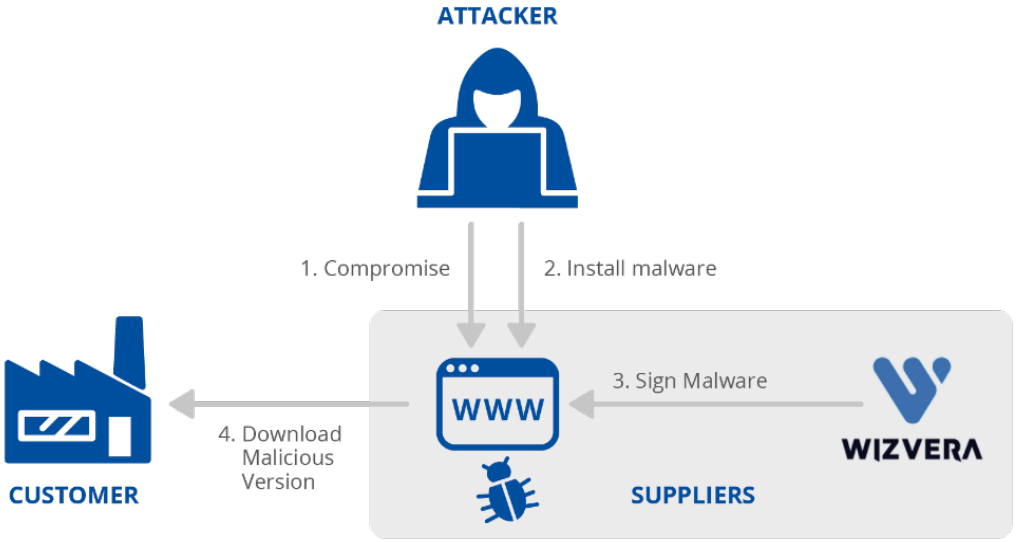
[70] Codecov supply chain attack breakdown, https://blog.gitguardian.com/codecov-supply-chain-breach/. Consultado el 27 de junio de 2021.
[71] Codecov hackers gained access to Monday.com source code, Bleeping Computer. https://www.bleepingcomputer.com/news/security/codecov-hackers-gained-access-to-mondaycom-source-code/. Consultado el 27 de junio de 2021.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

A.4 WIZVERA VERAPORT: PROGRAMA DE INSTALACIÓN DE INTEGRACIÓN

Wizvera es una empresa que ofrece soluciones de verificación de identidad, gestión de contraseñas y certificados en la nube[72]. Wizvera tiene un producto llamado VeraPort, un producto de instalación de integración que permite a los usuarios instalar software de seguridad requerido por sus empleadores[73]. En noviembre de 2020, los agresores atacaron un sitio web legítimo que tenía soporte de VeraPort. Sustituyeron la configuración de VeraPort del sitio web comprometido para distribuir software malicioso en lugar del software de seguridad esperado.

Wizvera firmó digitalmente la configuración[73]. VeraPort comprueba normalmente si el programa informático que se está descargando tiene una firma digital válida, pero no comprueba quién ha emitido el certificado. A través de este mecanismo, los usuarios de Corea del Sur que accedieron al sitio web comprometido descargaron el software malicioso. El ataque fue atribuido al grupo APT Lazarus[73].

PROVEEDOR		CLIENTE	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro	Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Desconocido	Procesos	Ataque drive-by [T1189], Infección de software malicioso	Datos



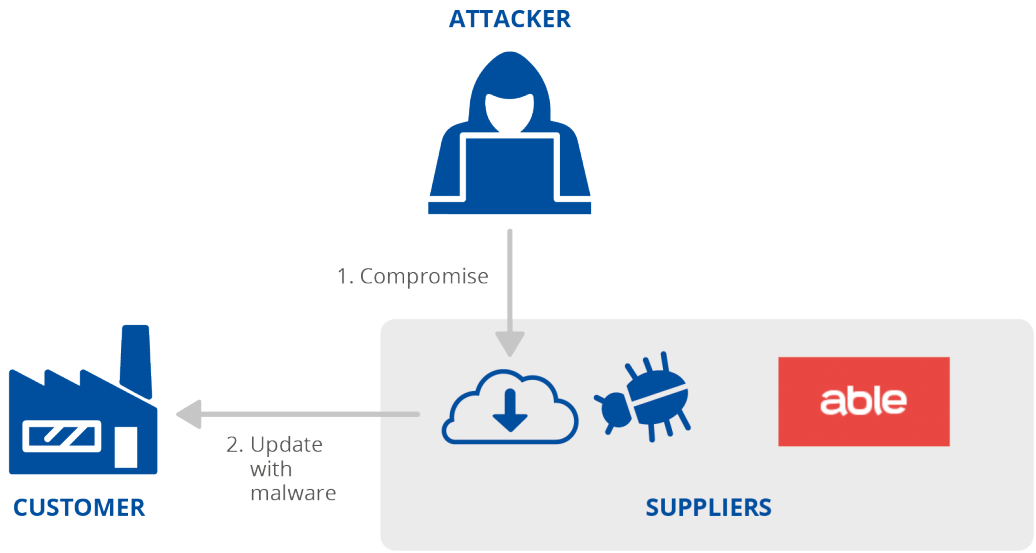
[72] Wizvera Company Profile & Funding, Crunchbase, https://www.crunchbase.com/organization/wizvera. Consultado el 9 de julio de 2021.
[73] Lazarus supply-chain attack in South Korea, WeLiveSecurity, https://www.welivesecurity.com/2020/11/16/lazarus-supply-chain-attack-south-korea/. Accessed Consultado el 9 de julio de 2021.

A.5 ABLE DESKTOP: PROGRAMA INFORMÁTICO DE CHAT

Able es una empresa con sede en Mongolia que suministra soluciones de programas informáticos a organismos públicos y empresas de la región[74]. En junio de 2020, los agresores parece que accedieron al backend de Able y comprometieron el sistema que entrega las actualizaciones de programas informáticos a todos los clientes. Los agresores añadieron software malicioso a la aplicación «Able Desktop» (un complemento que proporciona mensajería instantánea al producto principal de Able)[75]. Aunque se desconoce cómo se vio comprometido el proveedor, los agresores consiguieron obligar a los usuarios a instalar software malicioso[75]. A continuación, se utilizó el software malicioso para robar información de los dispositivos infectados de los clientes[75]. El ataque fue atribuido a APT TA428.

PROVEEDOR	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro
Desconocido	Código

CLIENTE	
Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Relación de confianza [T1199], Infección de software malicioso	Datos



[74] Able - Working online, Able, https://web.able.mn/, Consultado el 9 de julio de 2021.
[75] Operation StealthyTrident: corporate software under attack, WeLiveSecurity, https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/. Consultado el 9 de julio de 2021.

A.6 PROGRAMAS DE ASESORÍA FISCAL INTELIGENTE DE AISINO

Aisino Credit Information Company suministra programas informáticos de pago de impuestos a clientes internacionales a través de su departamento «Golden Tax», que incluye la «suite de software fiscal de Aisino». En junio de 2020, los investigadores revelaron que la «suite de software fiscal de Aisino» se había visto comprometida con el fin de incluir software malicioso[76]. Se desconoce cómo se vio comprometido el programa informático y cuál fue el objetivo del ataque[76]. El ataque iba dirigido a empresas de China, ya que este programa informático forma parte de un programa nacional en ese país[77]. No se identificó a los agresores del ataque.

PROVEEDOR	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro
Desconocido	Código

CLIENTE	
Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Relación de confianza [T1199], Infección de software malicioso	Desconocido

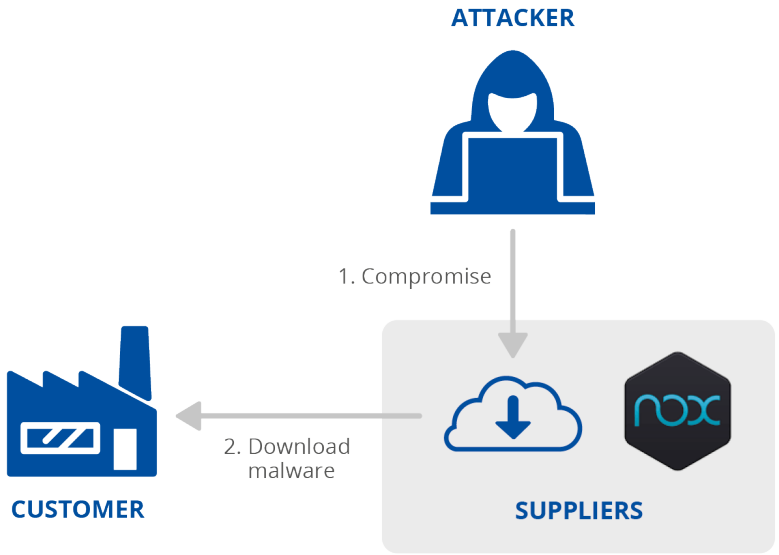
[76] The Golden Tax Department and Emergence of GoldenSpy Malware, Trustwave SpiderLabs, https://trustwave.azureedge.net/media/16929/the-golden-tax-department-and-emergence-of-goldenspy-malware.pdf. Consultado el 9 de julio de 2021.
[77] GoldenSpy Chapter 4: MalwareHelper Malware Embedded in Official Golden Tax Software, Trustwave, https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/goldenspy-chapter-4-goldenhelper-malware-embedded-in-official-golden-tax-software/. Consultado el 9 de julio de 2021.

A.7 BIGNOX NOXPLAYER: EMULADOR DE ANDROID PARA PC Y MAC

BigNox es una empresa que suministra programas informáticos de emulación. Su producto principal, NoxPlayer, es un emulador de Android muy popular para Windows y Mac[78]. En febrero de 2021, los investigadores informaron de que se había comprometido la infraestructura de NoxPlayer. Podía abusar del mecanismo de actualización de la herramienta y, en lugar de actualizaciones, distribuir software malicioso[79].

Una vez distribuida la carga útil inicial, los agresores pudieron recopilar información sobre sus víctimas y distribuir más software malicioso a objetivos específicos[79]. El objetivo de los agresores parece ser tener la capacidad de inspeccionar objetivos específicos[79]. No se identificó a los agresores del ataque.

PROVEEDOR		CLIENTE	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro	Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Desconocido	Código	Relación de confianza [T1199], Infección de software malicioso	Personas, Datos



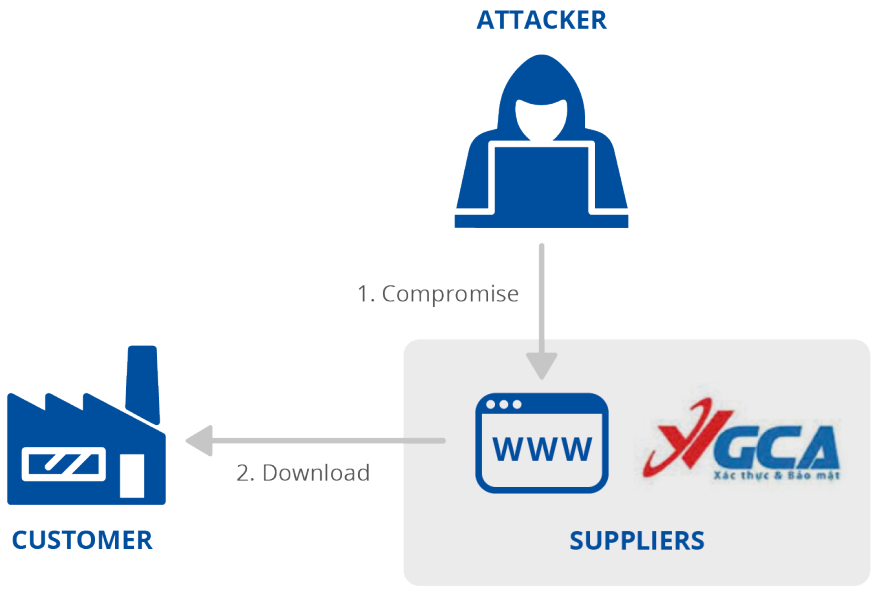
[78] NoxPlayer - Free Android Emulator on PC and Mac, BigNox, https://www.bignox.com/. Consultado el 9 de julio de 2021.
[79] Operation NightScout: Supply-chain attack targets online gaming in Asia, WeLiveSecurity, https://www.welivesecurity.com/2021/02/01/operation-nightscout-supply-chain-attack-online-gaming-asia/. Consultado el 9 de julio de 2021.

A.8 AUTORIDAD DE CERTIFICACIÓN DEL GOBIERNO DE VIETNAM (VGCA)

La autoridad vietnamita de certificación gubernamental (VGCA) proporciona certificados digitales y un conjunto de aplicaciones que ayudan a los ciudadanos y a las empresas a firmar documentos digitalmente[80]. En diciembre de 2020, los investigadores informaron de que el sitio web de la infraestructura de VGCA se vio comprometido con el fin de sustituir los binarios legítimos por aplicaciones troyanizadas[81]. El objetivo del ataque no está claro, pero los investigadores creen que podría formar parte de un ataque mayor[81]. Las herramientas utilizadas indican que los grupos de APT (TA413, TA428) pueden estar detrás del ataque[82].

PROVEEDOR	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro
Desconocido	Código

CLIENTE	
Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Relación de confianza [T1199], Infección de software malicioso	Personas



[80] Vietnam targeted in complex supply chain attack, ZDNet, https://www.zdnet.com/article/vietnam-targeted-in-complex-supply-chain-attack/. Consultado el 9 de julio de 2021.
[81] Operation SignSight: Supply-chain attack against a certification authority in Southeast Asia, WeLiveSecurity, https://www.welivesecurity.com/2020/12/17/operation-signsight-supply-chain-attack-southeast-asia/. Consultado el 9 de julio de 2021.
[82] Panda's New Arsenal: Part 3 Smanager, Hiroki Hada, https://insight-jp.nttsecurity.com/post/102glv5/pandas-new-arsenal-part-3-smanager. Consultado el 9 de julio de 2021.

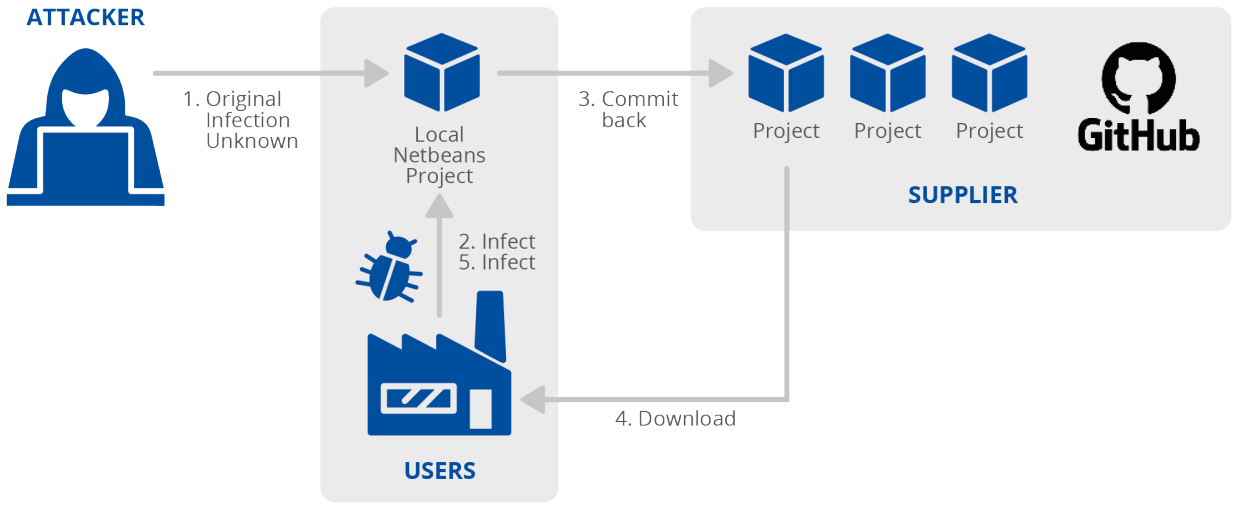
A.9 APACHE NETBEANS: PLATAFORMA DE DESARROLLO

NetBeans es una plataforma de desarrollo Java integrada de Apache. En mayo de 2020, los investigadores informaron de que algunos proyectos de NetBeans en GitHub contenían software malicioso sin el conocimiento de los propietarios. Todos los que descargasen y utilizaran estos proyectos se infectarían, troyanizando todos sus proyectos locales de NetBeans, y subiéndolos a GitHub.

Los usuarios también se infectaron con un software malicioso de RAT[83,84]. El objetivo del agresor parece ser la recopilación de información de dominio privado. Este ataque parece formar parte de un ataque a una cadena de suministro mayor. En este caso, los usuarios son tanto el proveedor como las víctimas. GitHub es el único medio de intercambio utilizado. No se identificó a los agresores del ataque.

PROVEEDOR	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro
Infección de software malicioso	Código

CLIENTE	
Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Infección de software malicioso	Programas informáticos, Datos



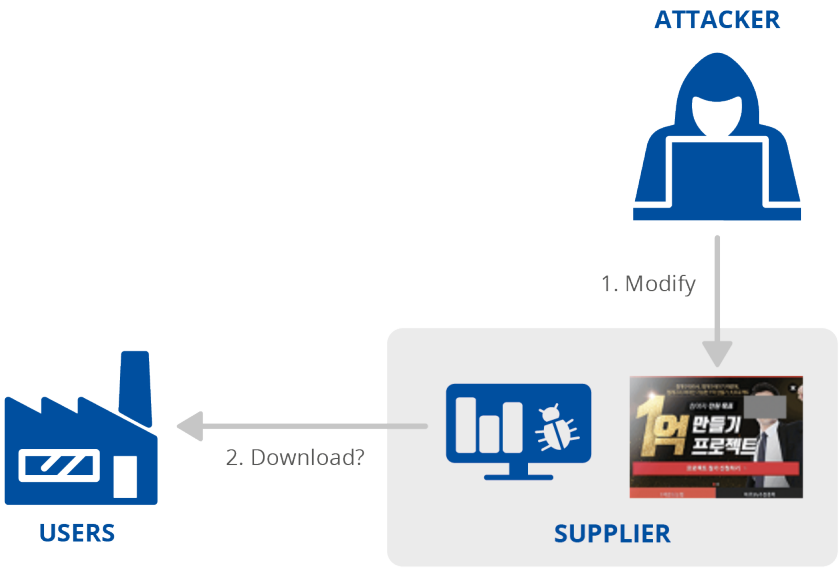
[83] The Octopus Scanner Malware: Attacking the open source supply chain, GitHub Security Lab, https://securitylab.github.com/research/octopus-scanner-malware-open-source-supply-chain/. Consultado el 9 de julio de 2021.
[84] Supply Chain Attack Event - Targeted Attacks on Java Projects in GitHub, NSFOCUS, https://nsfocusglobal.com/supply-chain-attack-event-targeted-attacks-on-java-projects-in-github/. Consultado el 9 de julio de 2021.

A.10 MENSAJERO DE INVERSIÓN EN ACCIONES PRIVADAS

En enero de 2021, los investigadores informaron de que el grupo Thallium APT tenía como objetivo a los inversores en bolsa, al comprometer una aplicación de mensajería de inversión en bolsa muy utilizada[85]. Los agresores troyanizaron los instaladores de la aplicación de mensajería para incluir el software malicioso[86]. El software malicioso se utilizó para espiar a los usuarios infectados[87]. No existe información fiable sobre el ataque o los métodos utilizados.

PROVEEDOR	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro
Desconocido	Código

CLIENTE	
Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Infección de software malicioso	Personas



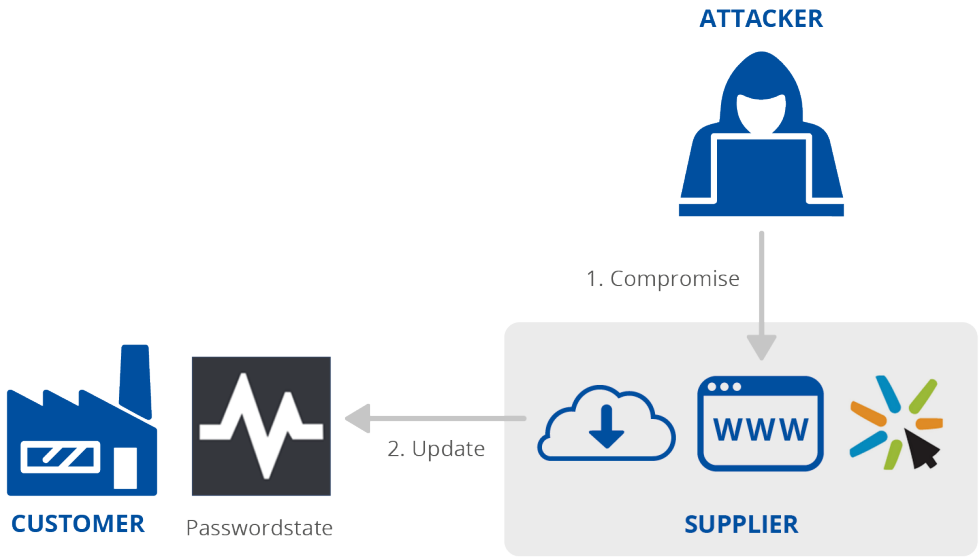
[85] Thallium Hacker Targeted Users of Private Stock Investment Messenger, Cyware Alerts - Hacker News, https://cyware.com/news/thallium-hacker-targeted-users-of-private-stock-investment-messenger-ac33d20d. Consultado el 9 de julio de 2021.
[86] Thallium Altered the Installer of a Stock Investment App, E Hacking News, https://www.ehackingnews.com/2021/01/thallium-altered-installer-of-stock.html. Consultado el 9 de julio de 2021.
[87] Thallium organization exploits private equity investment messenger to launch software supply chain attack, ESTsecurity, https://blog.alyac.co.kr/3489. Consultado el 9 de julio de 2021.

A.11 CLICKSTUDIOS PASSWORDSTATE: ADMINISTRADOR DE CONTRASEÑAS

ClickStudios es una empresa que ofrece soluciones de administración de contraseñas para empresas[88]. Su producto principal es una herramienta llamada Passwordstate. En abril de 2021, el mecanismo web «upgrade director» de Passwordstate utilizado para actualizar la herramienta se vio comprometido[89], redirigiendo a los usuarios a la descarga de software malicioso en lugar de las actualizaciones previstas. El software malicioso instalado fue diseñado para robar información de los sistemas afectados[89, 90]. No se identificó a los agresores del ataque.

PROVEEDOR	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro
Desconocido	Código

CLIENTE	
Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Relación de confianza [T1199], Infección de software malicioso	Datos



[88] Enterprise Password Management Software - Web based Server Password Manager, ClickStudios https://www.clickstudios.com.au/. Consultado el 9 de julio de 2021.
[89] ClickStudios PASSWORDSTATE Incident Management Advisory #01, ClickStudios, https://www.clickstudios.com.au/advisories/Incident_Management_Advisory-01-20210424.pdf. Consultado el 9 de julio de 2021.
[90] Moserpass supply chain, CSIS Security Group, https://www.csis.dk/newsroom-blog-overview/2021/moserpass-supply-chain/. Consultado el 9 de julio de 2021.

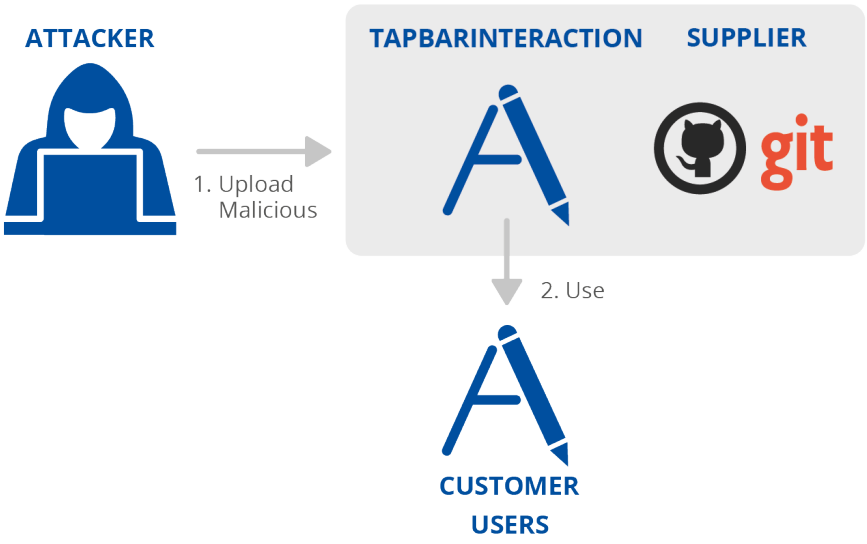
A.12 APPLE XCODE: ENTORNO DE DESARROLLO INTEGRADO

Apple Xcode es un entorno de desarrollo utilizado para desarrollar aplicaciones OSX e iOS[91]. En marzo de 2021, los investigadores informaron de que se estaba utilizando un proyecto de Xcode malicioso individual para infectar a los desarrolladores de Xcode con una puerta trasera[92]. El proyecto malicioso de Xcode era una copia de uno real. El proyecto de Xcode malicioso infectaba al usuario aprovechando una deficiencia de Xcode que permitía a los agresores ejecutar automáticamente un script cuando se lanzaba la compilación del proyecto[92].

No se han identificado los responsables de este ataque y ni siquiera está claro si los clientes realmente sufrieron algún ataque[93]. Tampoco está claro cómo se distribuyó el proyecto Xcode troyanizado a las víctimas potenciales, o si esto sucedió realmente.

PROVEEDOR	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro
Desconocido	Código

CLIENTE	
Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Infección de software malicioso	Desconocido

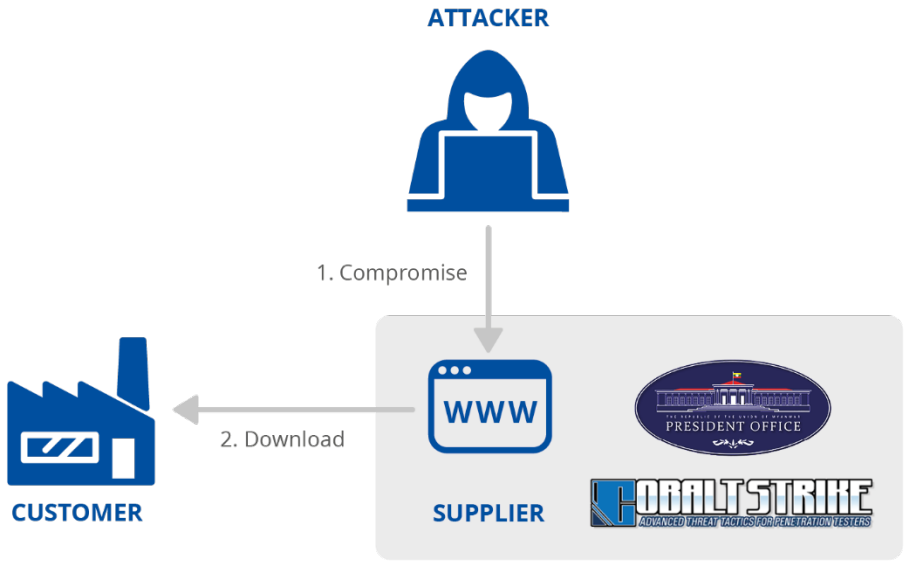


[91] Xcode 13 Overview, Apple Developer, https://developer.apple.com/xcode/. Consultado el 9 de julio de 2021.
[92] New macOS Malware XcodeSpy Targets Xcode Developers with EggShell Backdoor, SentinelLabs, https://labs.sentinelone.com/new-macos-malware-xcodespy-targets-xcode-developers-with-eggshell-backdoor/, Consultado el 9 de julio de 2021.
[93] XcodeSpy Mac Malware Targets Developers, SecureMac, https://www.securemac.com/news/xcodespy-mac-malware-targets-developers. Consultado el 9 de julio de 2021.

A.13 SITIO WEB DE LA PRESIDENCIA DE MYANMAR

En junio de 2021, los investigadores informaron de que los recursos alojados en el sitio web de la presidencia de Myanmar habían sido troyanizados para distribuir software malicioso[94]. El ataque no se atribuyó oficialmente a ningún grupo APT específico[95]; sin embargo, se destacaron las semejanzas con el grupo APT Mustang Panda[94,96].

PROVEEDOR		CLIENTE	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro	Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Desconocido	Código	Phishing [T1566], Infección de software malicioso	Personas



[94] «ESETresearch uncovered a supply chain attack on the Myanmar president office website», Twitter, https://twitter.com/ESETresearch/status/1400165767488970764. Consultado el 9 de julio de 2021.
[95] Backdoor malware found on the Myanmar president's website, again, The Record by Recorded Future, https://therecord.media/backdoor-malware-found-on-the-myanmar-presidents-website-again/. Consultado el 9 de julio de 2021.
[96] Cobalt Strike Beacons Being Hosted on Myanmar President's Website, Binary Defense, https://www.binarydefense.com/threat_watch/cobalt-strike-beacons-being-hosted-on-myanmar-presidents-website/. Consultado el 9 de julio de 2021.

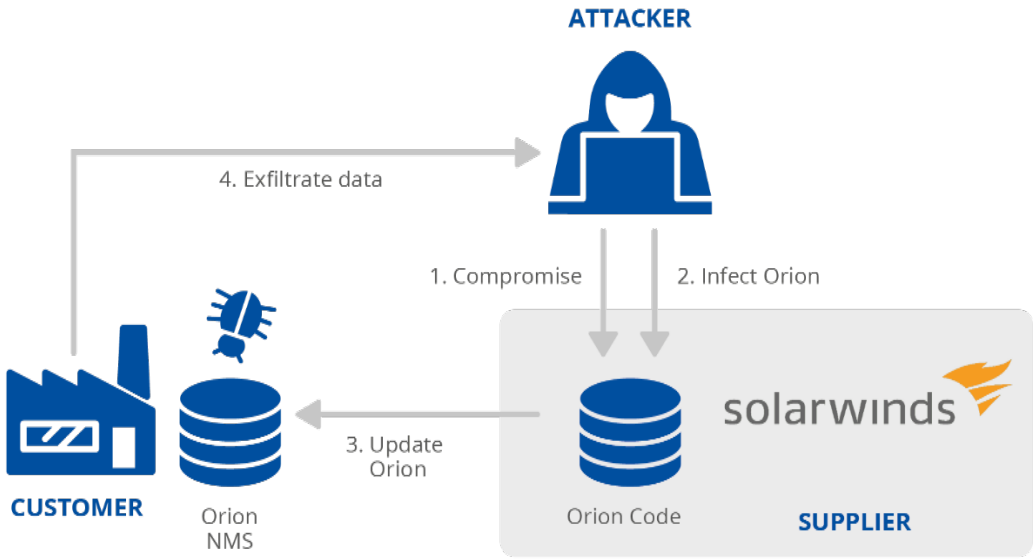
A.14 SOLARWINDS ORION: GESTIÓN DE TI Y SEGUIMIENTO ELECTRÓNICO REMOTO

SolarWinds es una empresa que suministra programas informáticos de gestión y vigilancia[97]. Orion es el producto de sistema de gestión de red (NMS) de SolarWinds[98]. En diciembre de 2020 se descubrió que Orion había sido comprometido. Una investigación exhaustiva demostró que los agresores obtuvieron acceso a la red de SolarWinds, posiblemente aprovechando una vulnerabilidad de día cero en una aplicación o dispositivo de terceros, un ataque de fuerza bruta o a través de ingeniería social[99]. Una vez comprometida la red, los agresores recopilaron información durante un largo periodo de tiempo.

Tras el ataque, se inyectó un software malicioso en el proceso de compilación de Orion[99,100]. A continuación, los clientes descargaron y ejecutaron directamente el programa informático, lo que aprovecharon los agresores para recopilar y robar información[101,102]. El ataque se atribuyó al grupo APT29[103].

PROVEEDOR		CLIENTE	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro	Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Aprovecharse de la vulnerabilidad del software, Ataque de fuerza bruta, Ingeniería social	Procesos, Código	Relación de confianza [T1199], Infección de software malicioso	Datos

[97] What You Need To Know About the SolarWinds Supply-Chain Attack, https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/. Consultado el 9 de julio de 2021.
[98] Orion Platform, SolarWinds, https://www.solarwinds.com/solutions/orion. Consultado el 9 de julio de 2021.
[99] An Investigative Update of the Cyberattack, Orange Matter, https://orangematter.solarwinds.com/2021/05/07/an-investigative-update-of-the-cyberattack/. Consultado el 9 de julio de 2021.
[100] Malware SUNSPOT: A Technical Analysis, CrowdStrike, https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/. Consultado el 9 de julio de 2021.
[101] Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor, ireEye Inc, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html. Consultado el 9 de julio de 2021.
[102] SUNBURST Additional Technical Details, FireEye Inc, https://www.fireeye.com/blog/threat-research/2020/12/sunburst-additional-technical-details.html. Consultado el 9 de julio de 2021.
[103] SolarWinds: Advancing the Story, RiskIQ Community Edition, https://community.riskiq.com/article/9a515637. Consultado el 9 de julio de 2021.

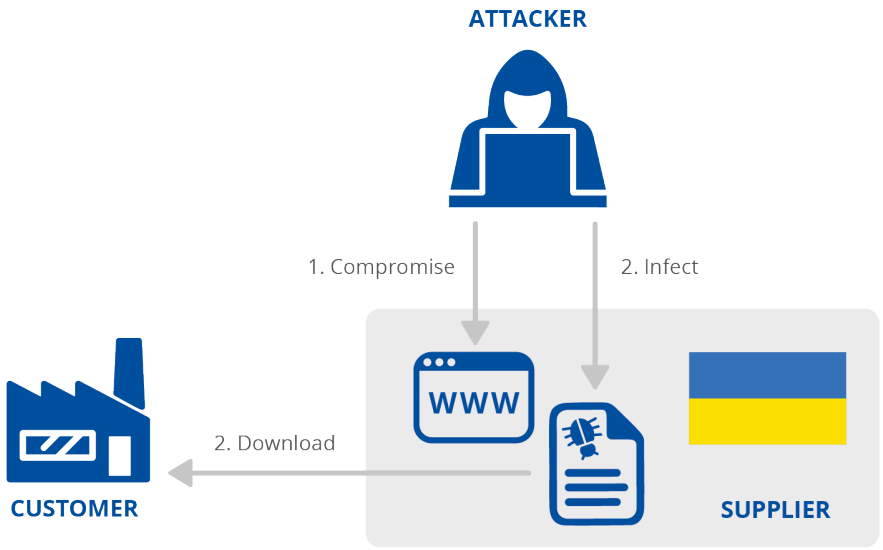

ATTACKER
4. Exfiltrate data
1. Compromise
2. Infect Orion
3. Update Orion
CUSTOMER
Orion NMS
Orion Code
solarwinds
SUPPLIER

A.15 UCRANIA SEI EB: SISTEMA DE INTERACCIÓN ELECTRÓNICA DE LOS ÓRGANOS EJECUTIVOS

Los organismos del sector público de Ucrania utilizan el sistema de interacción electrónica de órganos ejecutivos (SEI EB), un sistema de portales web diseñado para intercambiar documentación[104]. En febrero de 2021 se informó de que el sistema había sido atacado por agresores que lograron subir documentos maliciosos al portal[105]. Los documentos maliciosos infectarían posteriormente a los usuarios con software malicioso diseñado para recopilar y robar información. El ataque se atribuyó a varios grupos de amenazas persistentes avanzadas, pero no a ningún grupo concreto[104].

PROVEEDOR	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro
Desconocido	Código

CLIENTE	
Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Infección de software malicioso	Personas, Datos



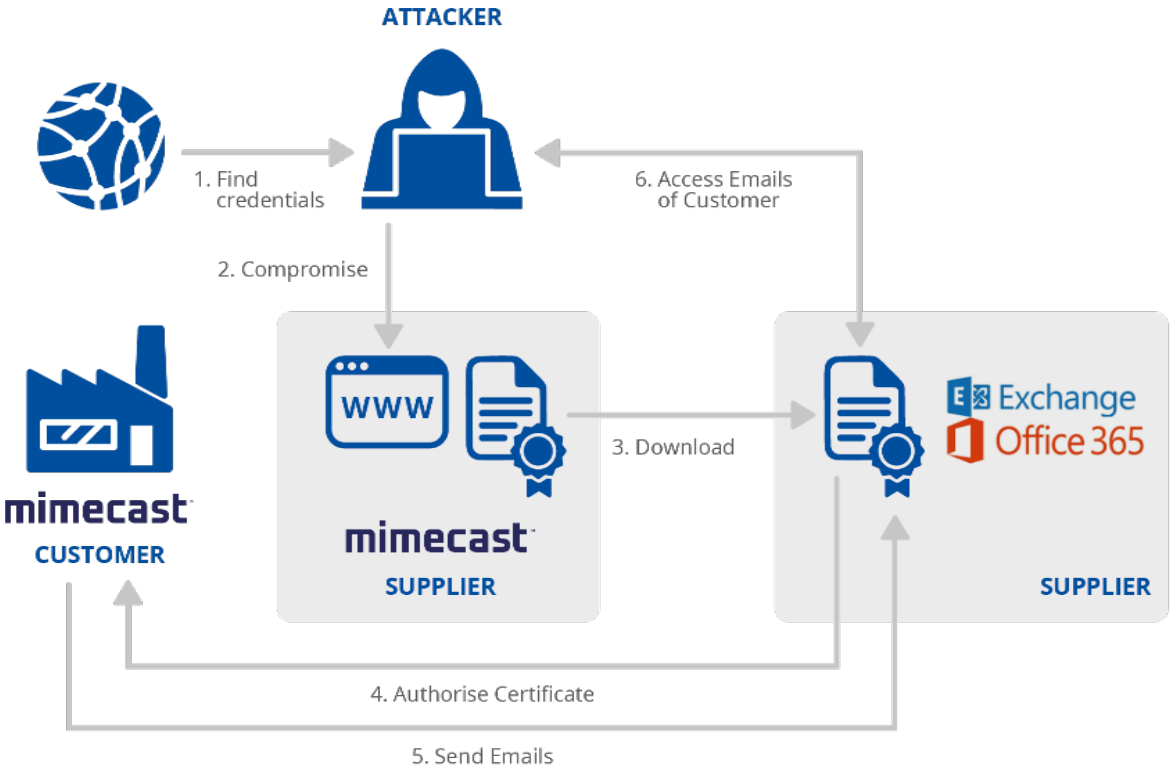
[104] Russian hackers aim cyber attack on Ukrainian government agencies, Teiss News, https://www.teiss.co.uk/russian-hackers-targeting-ukrainian-government-agencies/. Consultado el 9 de julio de 2021.
[105] The NCCC at the NSDC of Ukraine warns of a cyberattack on the document management system of state bodies, National Security and Defense Council of Ukraine, https://www.rnbo.gov.ua/en/Diialnist/4823.html. Consultado el 9 de julio de 2021.

A.16 MIMECAST: SERVICIOS DE CIBERSEGURIDAD EN LA NUBE

Mimecast es un proveedor de servicios de ciberseguridad en la nube[106]. Entre los servicios que proporciona, Mimecast ofrece servicios de seguridad del correo electrónico, que requieren que los clientes se conecten de forma segura a los servidores Mimecast para utilizar sus cuentas de Microsoft 365. En enero de 2021, se descubrió que los agresores habían comprometido a Mimecast (a través del proveedor de SolarWinds). Tras el ataque, los agresores accedieron a un certificado emitido por Mimecast utilizado por los clientes para acceder a los servicios de Microsoft 365, lo que les permitió interceptar las conexiones de redes y conectarse a las cuentas de Microsoft 365 para robar información[107,108]. El ataque fue atribuido al grupo APT29[109]. El compromiso de los sistemas del proveedor se ha vinculado a SolarWinds, pero no hay información fiable sobre los detalles de cómo ocurrió.

PROVEEDOR	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro
Desconocido	Datos

CLIENTE	
Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Relación de confianza [T1199]	Datos



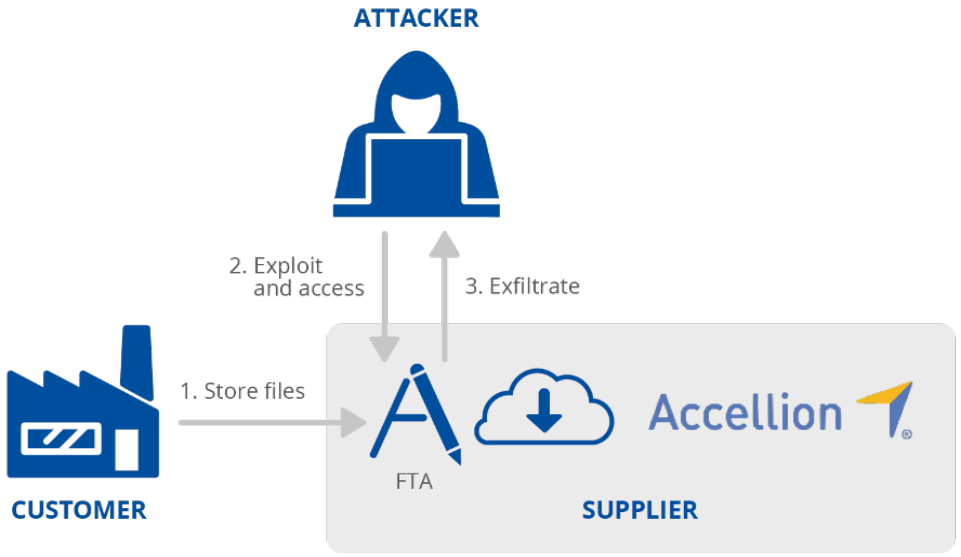
[106] Our Company, Mimecast, https://www.mimecast.com/company/. Consultado el 9 de julio de 2021.
[107] Important Update from Mimecast, Mimecast Blog, https://www.mimecast.com/blog/important-update-from-mimecast/.Consultado el 9 de julio de 2021.
[108] Mimecast Certificate Hacked in Supply-Chain Attack, Threatpost, https://threatpost.com/mimecast-certificate-microsoft-supply-chain-attack/162965/. Consultado el 9 de julio de 2021.
[109] Important Security Update, Mimecast Blog, https://www.mimecast.com/blog/important-security-update/. Consultado el 9 de julio de 2021.

A.17 ACCELLION: PROGRAMAS INFORMÁTICOS DE TRANSFERENCIA DE FICHEROS (FTA)

Accellion es una empresa que suministra software de seguridad a empresas, en particular aplicaciones para compartir archivos y colaborar de forma segura[110]. En diciembre de 2020, Accellion informó de que los agresores habían aprovechado múltiples vulnerabilidades de día cero en su programa informático de transferencia de ficheros (FTA) para obtener acceso a los archivos de los clientes[111,112] y extraerlos utilizando una Webshell. Los agresores extorsionaron a muchas empresas afectadas por estas vulnerabilidades con la amenaza de publicar sus archivos robados. El ataque se atribuyó a un grupo de ciberdelincuencia conocido como UNC2546[112].

PROVEEDOR	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro
Aprovecharse de la vulnerabilidad del software	Código

CLIENTE	
Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Relación de confianza [T1199]	Datos



[110] About Accellion, Accellion, https://www.accellion.com/company/. Consultado el 9 de julio de 2021.
[111] File Transfer Appliance (FTA) Security Assessment, Accellion, https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf. Consultado el 9 de julio de 2021.
[112] Cyber Criminals Exploit Accellion FTA for Data Theft and Extortion, FireEye Inc, https://www.fireeye.com/blog/threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html. Consultado el 9 de julio de 2021.

A.18 SISTEMA DE GESTIÓN DE PASAJEROS SITA

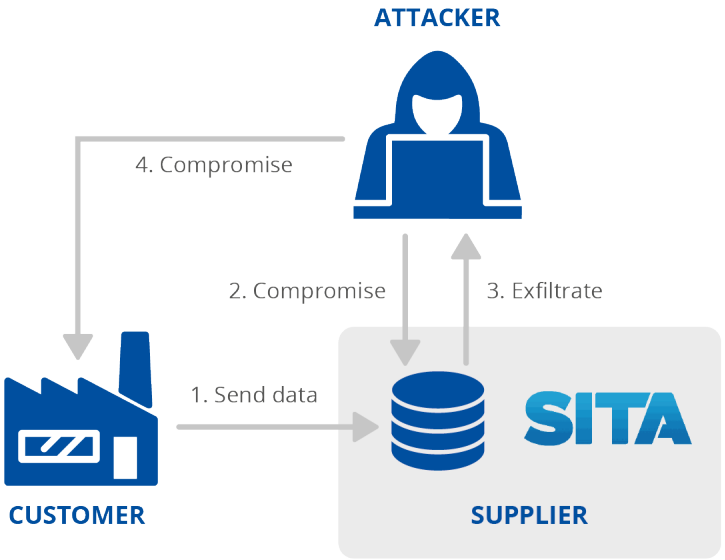
SITA es una empresa especializada en tecnologías de la información aérea y del transporte[113]. El sistema de gestión de pasajeros de SITA se utiliza para proporcionar a las aerolíneas información sobre los pasajeros en el momento del embarque, incluido el riesgo que los pasajeros pueden representar para un país[114]. En marzo de 2021, se reveló que los agresores habían comprometido los servidores de SITA para obtener acceso a los datos de los pasajeros de los clientes de SITA. Algunos de los clientes de SITA también informaron de violaciones de datos, como Air India, Singapore Airlines y Malaysia Airlines.

Tras los informes sobre la filtración de datos en Internet, Air India también informó de que sus redes se habían visto comprometidas y se habían robado datos. El ataque a las redes internas de Air India estaba supuestamente relacionado con el incidente de SITA ya que una empresa de seguridad descubrió que el nombre de un ordenador dentro de Air India era «SITASERVER4».

Hasta la fecha, se desconoce cómo accedieron los agresores a los servidores de SITA y tampoco se sabe cómo accedieron a Air India o si lo hicieron realmente. El ataque interno a las redes de Air India se atribuyó al grupo APT41[115].

PROVEEDOR	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro
Desconocido	Datos

CLIENTE	
Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Desconocido	Datos personales



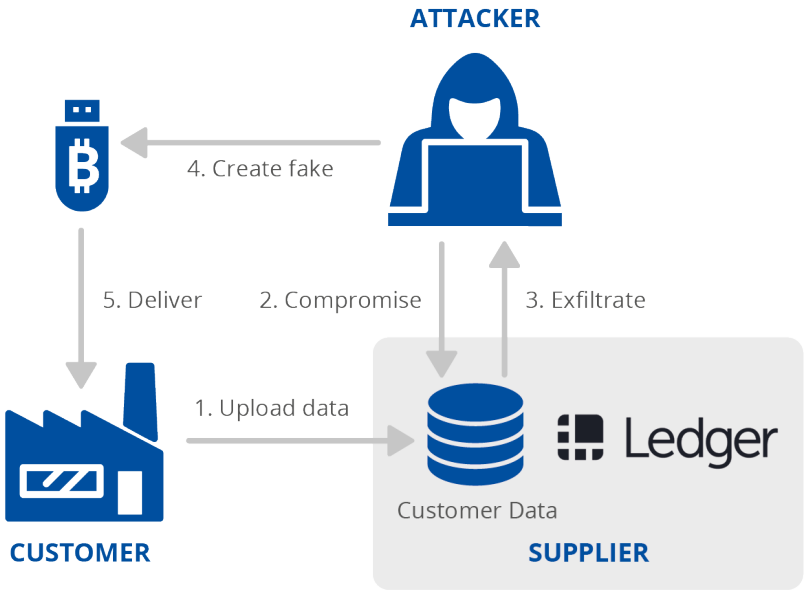
[113] About us, SITA, https://www.sita.aero/about-us/. Consultado el 9 de julio de 2021.
[114] SITA Advance Passenger Processing, SITA, https://www.sita.aero/solutions/sita-at-borders/border-management/sita-advance-passenger-processing/. Consultado el 9 de julio de 2021.
[115] Big airline heist: APT41 likely behind massive supply chain attack, Group-IB, https://blog.group-ib.com/colunmtk_apt41. Consultado el 9 de julio de 2021.

A.19 LEDGER: MONEDERO DE HARDWARE

Ledger es una empresa que suministra tecnología de monederos de hardware para criptomonedas[116]. En julio de 2020, los agresores obtuvieron credenciales válidas para acceder a la base de datos de comercio electrónico de Ledger[117]. Se desconoce la forma en que los agresores accedieron a estas credenciales. Los datos robados se publicaron en un foro en línea[118].

Los agresores utilizaron los datos robados para el phishing en línea y la extorsión de los usuarios[119,120], así como para robar el dinero de los usuarios a través de un ataque físico tras suministrarles monederos Ledger falsificados que, al conectarse a un ordenador, les solicitaba las claves de seguridad, infectaban el ordenador con software malicioso y enviaban la información robada a los agresores[121]. No se identificó a los agresores del ataque.

PROVEEDOR		CLIENTE	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro	Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Desconocido	Datos	Relación de confianza [T1199], Phishing [T1566], Falsificación	Finanzas



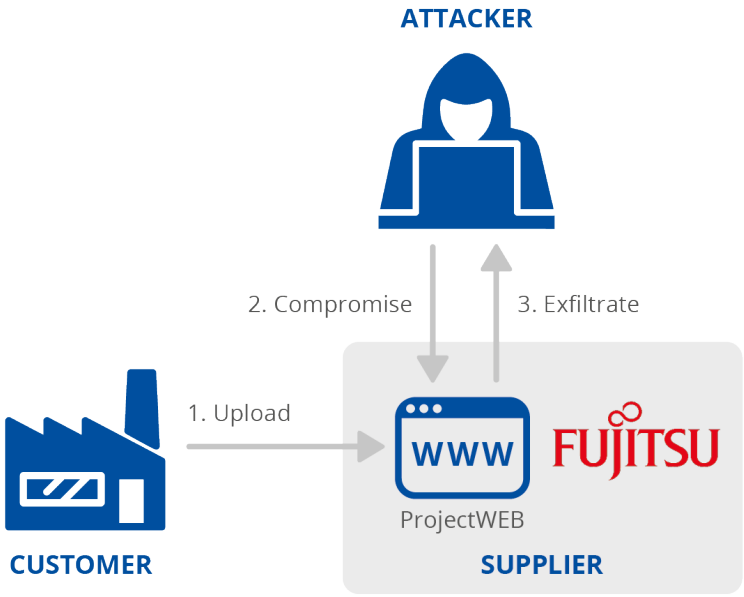
[116] Hardware Wallet, Ledger, https://www.ledger.com/. Consultado el 9 de julio de 2021.
[117] Addressing the July 2020 e-commerce and marketing data breach -- A Message From Ledger's Leadership | Ledger, https://www.ledger.com/addressing-the-july-2020-e-commerce-and-marketing-data-breach. Consultado el 9 de julio de 2021.
[118] Hackers Leak Customer Info From Crypto Wallet Ledger, Investopedia, https://www.investopedia.com/hackers-leak-customer-info-from-crypto-wallet-ledger-5093577. Consultado el 9 de julio de 2021.
[119] Message by LEDGER's CEO - Update on the July data breach. Despite the leak, your crypto assets are safe, Ledger, https://www.ledger.com/message-ledgers-ceo-data-leak. Consultado el 9 de julio de 2021.
[120] Threat Actors Target Ledger Data Breach Victims in New Extortion Campaign, HOTforSecurity, https://web.archive.org/web/20210520120353/https://hotforsecurity.bitdefender.com/blog/threat-actors-target-ledger-data-breach-victims-in-new-extortion-campaign-25820.html. Consultado el 9 de julio de 2021.
[121] Inside The Scam: Victims Of Ledger Hack Are Receiving Fake Hardware Wallets, Nasdaq, https://www.nasdaq.com/articles/inside-the-scam%3A-victims-of-ledger-hack-are-receiving-fake-hardware-wallets-2021-06-17. Consultado el 9 de julio de 2021.

A.20 FUJITSU PROJECTWEB: PROGRAMA INFORMÁTICO DE COLABORACIÓN Y GESTIÓN DE PROYECTOS

Fujitsu ProjectWEB es un programa informático en la nube que utilizan las empresas para la colaboración en línea, la gestión de un software y el intercambio de archivos[122]. Esta herramienta es muy popular entre los organismos públicos de Japón. En mayo de 2021, los agresores consiguieron acceder a información del sector público japonés[123] tras aprovecharse de las deficiencias de las instalaciones de ProjectWEB[122,124]. Debido a la ubicación de los servidores atacados, en el ataque también se robaron datos de control del tráfico aéreo japonés[122,125]. No se identificó a los agresores del ataque.

PROVEEDOR	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro
Desconocido	Código, Datos

CLIENTE	
Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Desconocido	Datos



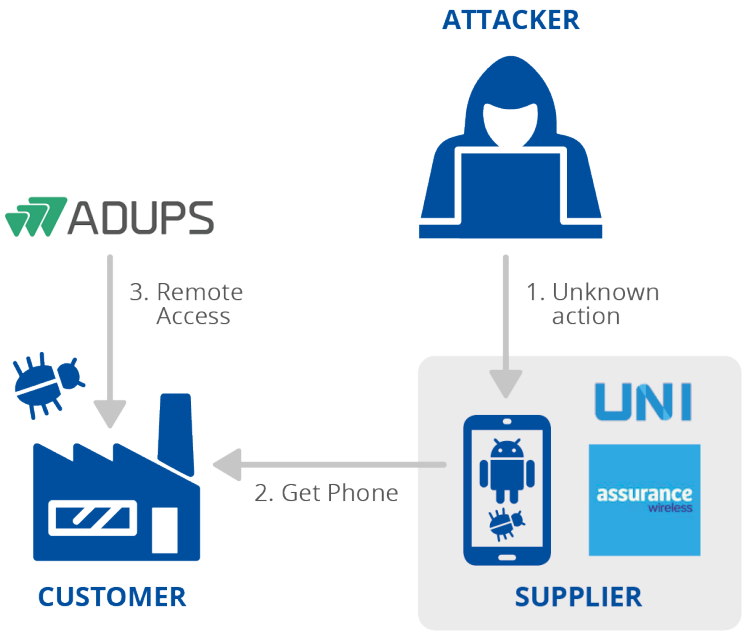
[122] Japanese government agencies suffered breaches after ProjectWEB hack, Teiss News, https://www.teiss.co.uk/japanese-government-agencies-suffered-breaches-following-fujitsus-projectweb-hack/. Consultado el 9 de julio de 2021.
[123] Japanese government agencies suffer data breaches after Fujitsu hack, Bleeping Computer, https://www.bleepingcomputer.com/news/security/japanese-government-agencies-suffer-data-breaches-after-fujitsu-hack/. Consultado el 9 de julio de 2021.
[124] Data theft via Fujitsu ProjectWEB, INCIBE-CERT, https://www.incibe-cert.es/en/early-warning/cybersecurity-highlights/data-theft-fujitsu-projectweb. Consultado el 9 de julio de 2021.
[125] Fujitsu pulls ProjectWEB tool offline after apparent supply chain attack sees Japanese infosec agency data stolen, The Register, https://www.theregister.com/2021/05/27/fujitsu_projectweb_supply_chain_attack/. Consultado el 9 de julio de 2021.

A.21 TELÉFONOS MÓVILES DE UNIMAX COMMUNICATIONS

Unimax, también conocida como UMX, suministra dispositivos móviles de bajo coste. Entre los clientes de UMX están las personas que reciben sus teléfonos a través del Programa Lifeline Assistance del gobierno estadounidense[126]. En enero de 2020, los investigadores informaron de que los dispositivos móviles contenían software malicioso preinstalado no extraíble diseñado para espiar a los usuarios[127,128]. No fue posible eliminar el software malicioso ni siquiera con un reinicio duro. Transsion, otro fabricante de dispositivos móviles que fue descubierto con software malicioso preinstalado, culpó a un proveedor no identificado de la cadena de suministro[126]. No se identificó a los agresores del ataque[126].

PROVEEDOR	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro
Desconocido	Código

CLIENTE	
Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Relación de confianza [T1199], Infección de software malicioso	Personas



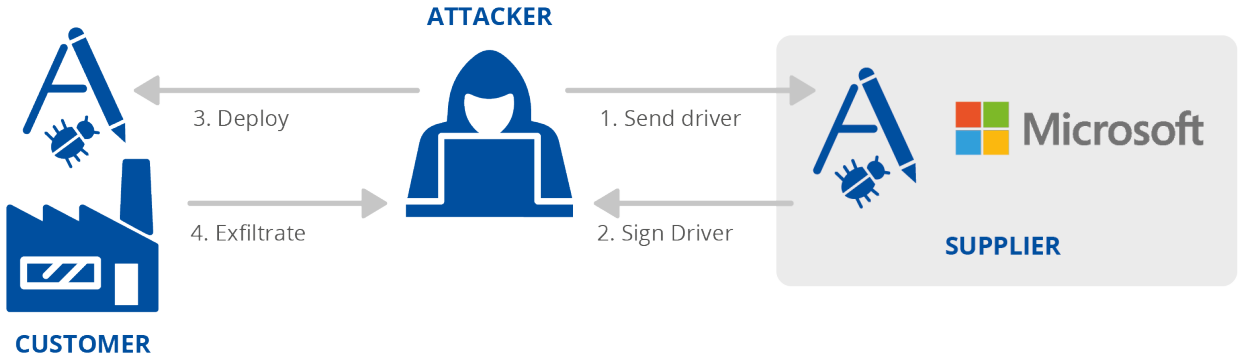
[126] Chinese Cell Phones Ship Preloaded with Malware, BlueVoyant, https://www.bluevoyant.com/blog/chinese-cell-phone-malware/. Consultado el 9 de julio de 2021.
[127] UMX Phone: US-funded Gov Phones come pre-installed with malicious apps, Malwarebytes Labs, https://blog.malwarebytes.com/android/2020/01/united-states-government-funded-phones-come-pre-installed-with-unremovable-malware/. Consultado el 9 de julio de 2021.
[128] We found yet another phone with pre-installed malware via the Lifeline Assistance program, Malwarebytes Labs, https://blog.malwarebytes.com/android/2020/07/we-found-yet-another-phone-with-pre-installed-malware-via-the-lifeline-assistance-program/.Consultado el 9 de julio de 2021.

A.22 PROGRAMA DE COMPATIBILIDAD DE LOS EQUIPOS DE MICROSOFT WINDOWS

En junio de 2021 se informó de que los agresores habían abusado de los procesos de firma de código que utiliza Microsoft para validar controladores de terceros con el fin de infiltrarse y distribuir un software malicioso rootkit [129]. A través de la firma válida, el software malicioso podía instalarse en los sistemas de los usuarios[130]. El ataque parecía estar dirigido al sector del juego en China[129]. No se identificó a los agresores del ataque.

PROVEEDOR	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro
Ingeniería social	Procesos

CLIENTE	
Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Relación de confianza [T1199]	Datos



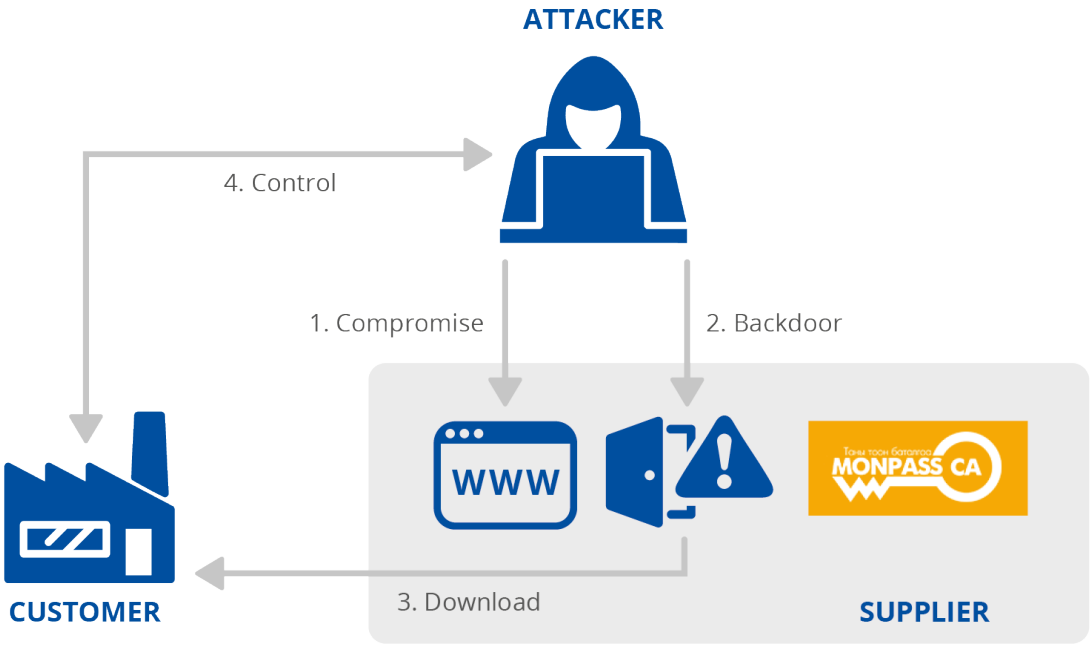
[129] Microsoft admits to signing rootkit malware in supply-chain fiasco, Bleeping Computer, https://www.bleepingcomputer.com/news/security/microsoft-admits-to-signing-rootkit-malware-in-supply-chain-fiasco/. Consultado el 9 de julio de 2021.
[130] Microsoft signed a malicious Netfilter rootkit, G DATA, https://www.gdatasoftware.com/blog/microsoft-signed-a-malicious-netfilter-rootkit. Consultado el 9 de julio de 2021.

A.23 AUTORIDAD DE CERTIFICACIÓN MONPASS

MonPass es la principal autoridad de certificación de Mongolia. En febrero de 2021, su sitio web se vio comprometido y se accedió al menos a un instalador binario por una puerta trasera con un binario de Cobalt Strike[131]. El sitio web se vio repetidamente comprometido y se encontraron varias Webshells y puertas traseras[132]. Los visitantes del sitio web de MonPass descargaron el código malicioso, que ejecutó el software malicioso tras la descarga. Se sabe que al menos un cliente ha sido infectado y que Avast Software ha identificado la infección[131].

PROVEEDOR	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro
Aprovecharse de la vulnerabilidad del software	Código

CLIENTE	
Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Ataque drive-by [T1189], Infección de software malicioso	Desconocido

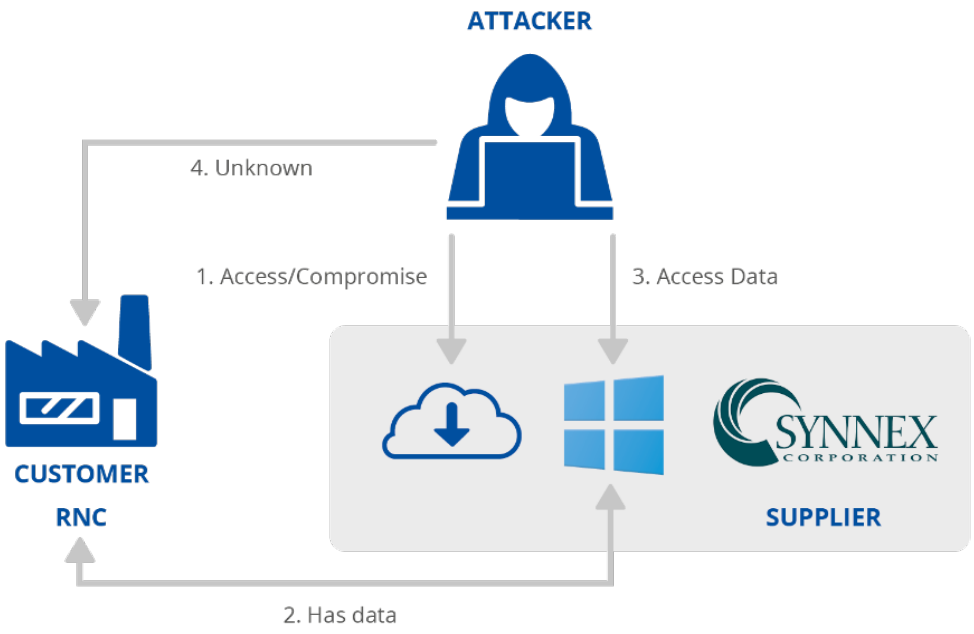


[131] Backdoored Client from Mongolian CA MonPass, Avast Threat Labs, https://decoded.avast.io/luigicamastra/backdoored-client-from-mongolian-ca-monpass/. Consultado el 9 de julio de 2021.
[132] Mongolian Certificate Authority Hacked to Distribution Backdoored CA Software, The Hacker News, https://thehackernews.com/2021/07/mongolian-certificate-authority-hacked.html. Consultado el 9 de julio de 2021.
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

A.24 EMPRESA DE DISEÑO Y DISTRIBUCIÓN SYNNEX IT

Synnex es un distribuidor e integrador de tecnología. En julio de 2021, se produjo un ataque sobre sus sistemas[133]. Synnex admitió que los ataques podrían haber estado relacionados con los recientes ataques a los MSP de Kaseya[134]. Los agresores utilizaron Synnex para acceder a las aplicaciones de los clientes dentro del entorno en la nube de Microsoft. Entre las aplicaciones atacadas estaba el Comité Nacional Republicano de Estados Unidos (RNC, por sus siglas en inglés), que informó de que había sido atacado a través de Synnex[135].

PROVEEDOR		CLIENTE	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos del proveedor afectados por el ataque a la cadena de suministro	Técnicas de ataque utilizadas para comprometer al cliente	Activos del cliente afectados por el ataque a la cadena de suministro
Aprovecharse de la vulnerabilidad del software	Código	Ataque drive-by [T1189], Infección de software malicioso	Desconocido



[133] Mega-distie SYNNEX attacked and Microsoft cloud accounts it tends tampered, The Register, https://www.theregister.com/2021/07/07/synnex_rnc_microsoft_attack/. Consultado el 9 de julio de 2021.
[134] SYNNEX Responds to Recent Cybersecurity Attacks and Media Mentions, SYNNEX Corporation, https://ir.synnex.com/news/press-release-details/2021/SYNNEX-Responds-to-Recent-Cybersecurity-Attacks-and-Media-Mentions/default.aspx. Consultado el 9 de julio de 2021.
[135] Russia 'Cozy Bear' Breached GOP as Ransomware Attack Hit, The Washington Post, https://www.washingtonpost.com/business/on-small-business/russia-cozy-bear-breached-gop-as-ransomware-attack-hit/2021/07/06/3e9e200a-de9b-11eb-a27f-8b294930e95b_story.html. Consultado el 9 de julio de 2021.

TP-05-21-171-EN-N

ACERCA DE LA ENISA

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) es la agencia de la Unión cuyo objetivo es alcanzar un elevado nivel común de ciberseguridad en toda Europa. Creada en 2004 y reforzada mediante el Reglamento sobre la Ciberseguridad de la UE, la Agencia de la Unión Europea para la Ciberseguridad contribuye a la política de seguridad cibernética de la UE, mejora la fiabilidad de los productos, servicios y procesos de TIC mediante programas de certificación de la ciberseguridad, coopera con los Estados miembros y con los organismos de la UE y ayuda a Europa a prepararse para los desafíos del día de mañana en materia de ciberseguridad. A través del intercambio de conocimientos, el desarrollo de capacidades y las campañas de sensibilización, la Agencia coopera con sus partes interesadas clave para fortalecer la confianza en la economía conectada, para impulsar la resiliencia de la infraestructura de la Unión y, por último, para proteger digitalmente a la sociedad y a la ciudadanía de Europa. Para más información sobre la ENISA y su trabajo, puede consultar: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-509-8
DOI: 10.2824/168593