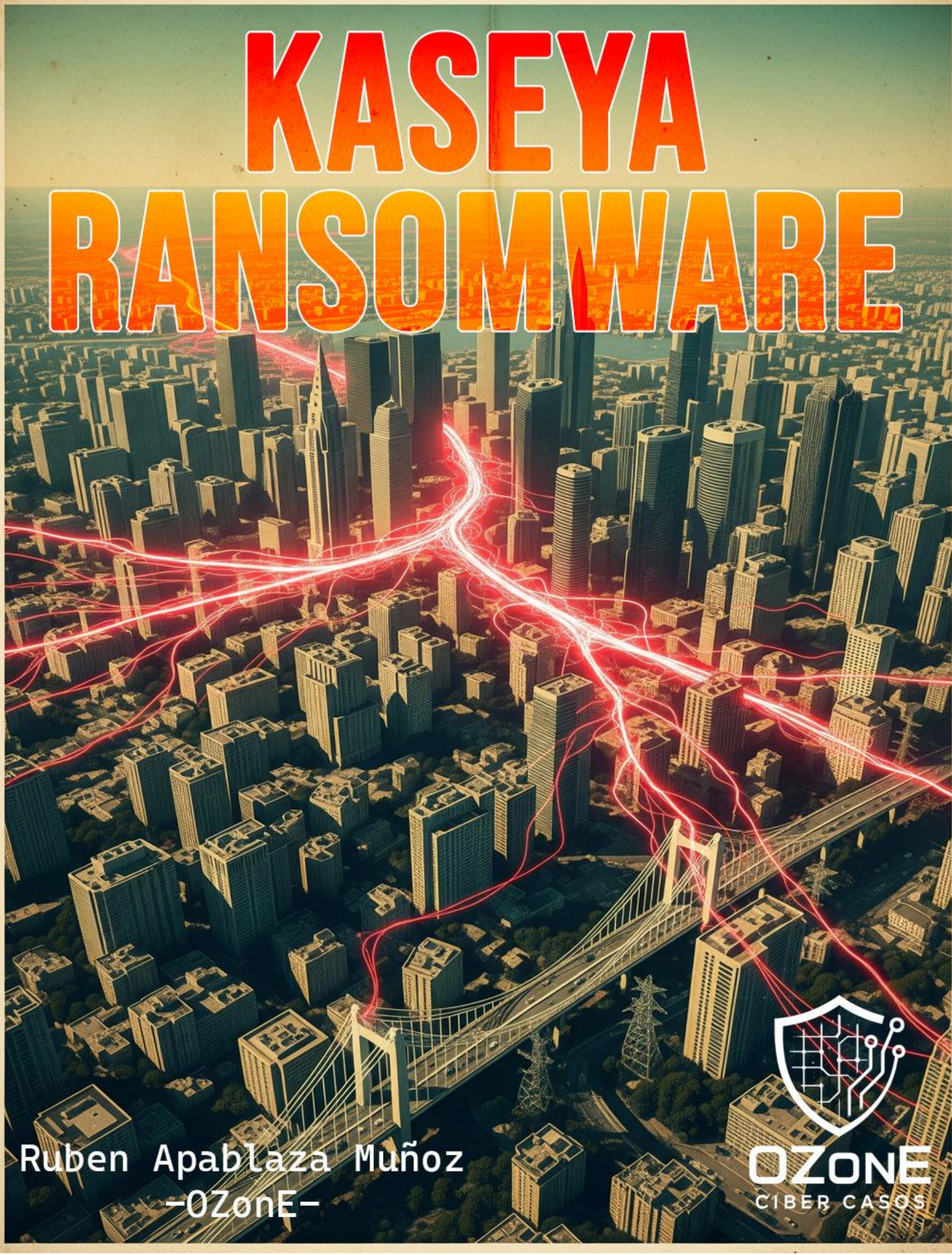
KASEYA RANSOMWARE



Ruben Apablaza Muñoz
-OZonE-

OZONE
CIBER CASOS

Caso Kaseya – Resumen Ejecutivo

Empresa afectada:

- Kaseya, Inc. – Miami, Florida, EE.UU.
- Software de administración remota para MSPs

Fecha del ataque:

- Viernes 2 de julio de 2021 (antesala del 4 de julio en EE.UU.)

Grupo responsable:

- REvil (Sodinokibi) – ransomware especializado en cadenas de suministro

Método de ataque:

- Vulnerabilidades críticas en **Kaseya VSA**
- Despliegue de ransomware vía actualización maliciosa
- Afectó a ~50 MSPs y 800–1.500 empresas globalmente

Impacto:

- Cifrado masivo de sistemas de clientes
- Interrupción significativa de servicios
- Solicitudes de rescate millonarias

Respuesta:

- Intervención de **FBI y CISA**
- Kaseya liberó parches de seguridad urgentes
- Discusión de posibles acciones legales por MSPs (sin demandas formales reportadas)

Terminología

Sigla / Término	Tipo	Significado / Descripción
VSA	Software	Virtual System/Server Administrator, software de administración remota de Kaseya
MSP	Organización	Managed Service Provider, proveedor de servicios gestionados
MSSP	Organización	Managed Security Service Provider, proveedor de servicios de seguridad gestionados
IOC	Concepto / Seguridad	Indicator of Compromise, indicador de compromiso
ET	Concepto / Tiempo	Eastern Time, zona horaria de la Costa Este de EE. UU.
IPO	Concepto / Finanzas	Initial Public Offering, oferta pública inicial
DIVD	Organización	Dutch Institute for Vulnerability Disclosure, instituto holandés para divulgación de vulnerabilidades
ConnectWise Manage	Software	Plataforma de software PSA utilizada por MSPs junto con Kaseya VSA
PSA	Concepto / Software	Professional Services Automation, automatización de servicios profesionales
Huntress	Empresa / Software	Empresa de ciberseguridad especializada en detección y respuesta a amenazas
Sodinikibi	Ransomware / Malware	Otro nombre de REvil, grupo de ransomware
CISA	Agencia / Gobierno	Cybersecurity & Infrastructure Security Agency, agencia de seguridad de infraestructura y ciberseguridad
CVE-2021-30116	Vulnerabilidad	Vulnerabilidad de Kaseya VSA que permite ejecución remota de código no autorizado
CVE-2021-30119	Vulnerabilidad	Vulnerabilidad de Kaseya VSA relacionada con acceso no autorizado a funciones administrativas
CVE-2021-30120	Vulnerabilidad	Vulnerabilidad de Kaseya VSA que permite la manipulación de archivos críticos a distancia

Introducción al caso

El ciberataque a Kaseya ocurrido el **2 de julio de 2021** es considerado uno de los ataques de ransomware más grandes de la historia dirigidos a la cadena de suministro. A diferencia de **WannaCry (2017),** que se recuerda como el ataque de ransomware más grande en cuanto a cantidad de dispositivos y sistemas afectados, el ataque a Kaseya -también conocido como **Sodinikibi** - destacó por el impacto directo en proveedores de servicios gestionados **(MSP)** y, a través de ellos, en cientos de empresas en todo el mundo.

Se trató de un ataque altamente sofisticado, que combinó la explotación de varias vulnerabilidades críticas en el software Kaseya VSA:

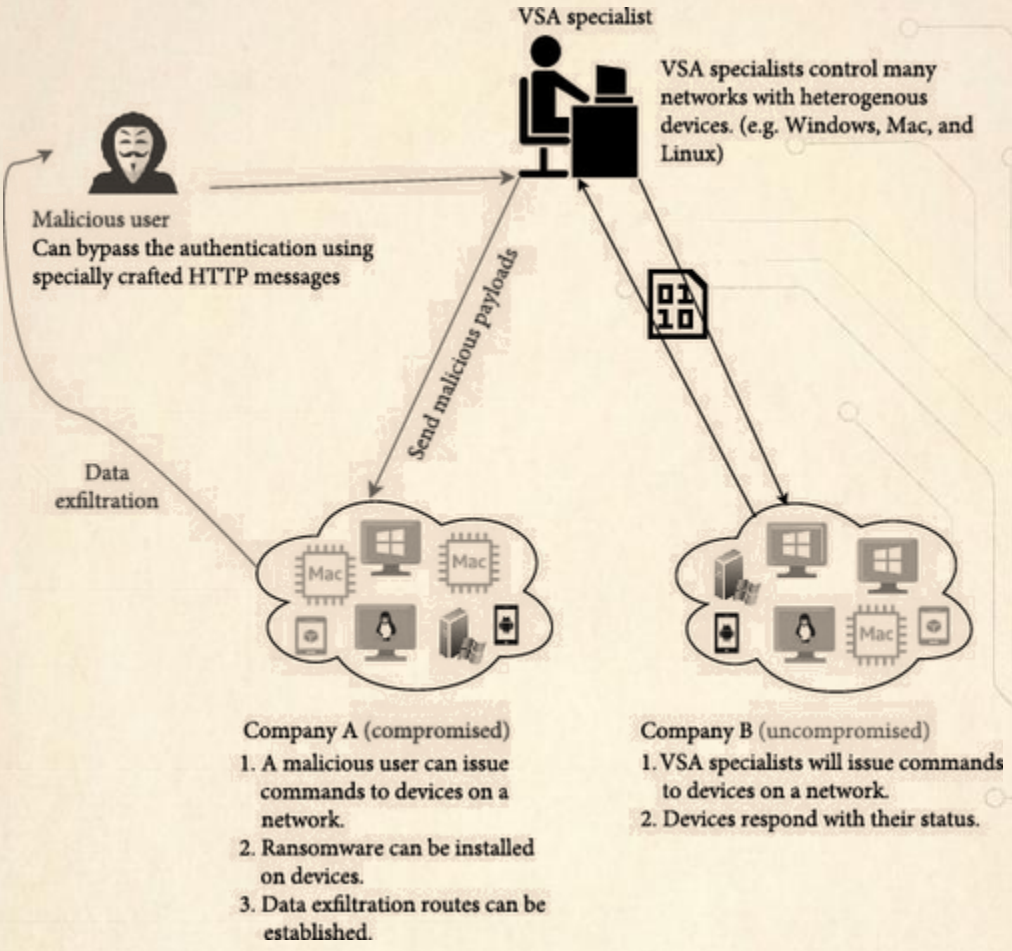
- **CVE-2021-30116:** filtración de credenciales y fallo de lógica de negocio
- **CVE-2021-30119:** vulnerabilidad de Cross-Site Scripting (XSS)
- **CVE-2021-30120:** fallo en la autenticación de dos factores

El malware que aprovechaba estas fallas se distribuyó mediante una actualización maliciosa denominada "Kaseya VSA Agent Hot Fix", lo que permitió al grupo atacante **REvil** (Sodinokibi) desplegar ransomware de forma masiva, afectando a unos 50 MSPs y entre 800 y 1.500 organizaciones a nivel global.

Kaseya VSA

- **Administrador Virtual de Sistemas (VSA):** plataforma de software que permite a los equipos de TI y a los Proveedores de Servicios Gestionados (MSP) supervisar y administrar de forma remota múltiples computadoras y redes desde una sola consola. Sus funciones incluyen la implementación de parches, la instalación de software y el monitoreo de la seguridad.
- En el ataque de 2021, Kaseya VSA se convirtió en el **vector de ataque** en un ataque a la cadena de suministro. Aquí están los elementos clave de su rol:
  - **Punto central de confianza:** Los atacantes **sabían que los MSP confían en el software VSA** de Kaseya para administrar las redes de sus clientes. En lugar de atacar a cada empresa individualmente, comprometieron el software central. Esto les dio acceso privilegiado a los sistemas de los clientes de los MSP.
  - **Mecanismo de propagación:** Una vez que los atacantes obtuvieron acceso a los servidores VSA, pudieron "emitir cargas maliciosas" o **actualizaciones falsas** a todas las computadoras conectadas. Estas computadoras, **al considerar la actualización como legítima porque provenía de una fuente de confianza (Kaseya VSA), la aceptaron e instalaron el ransomware sin sospecharlo.**
  - **El multiplicador de daño:** Gracias a Kaseya VSA, los ciberdelincuentes lograron **en un solo ataque** lo que de otra forma les habría llevado miles de intentos individuales. Al comprometer a unos 50 MSP (según las cifras iniciales), lograron infectar a un estimado de

1,500 clientes finales. Esto hizo del ataque uno de los más grandes y sofisticados de la historia del ransomware.



Esquema de la metodología de ataque.

VSA es una herramienta de monitorización y gestión remota diseñada para automatizar las tareas de TI en endpoints gestionados. Sin embargo, los atacantes utilizaron solicitudes http especialmente diseñadas para eludir los mecanismos de autenticación del portal de VSA. Esto les permitió obtener acceso administrativo y utilizar maliciosamente las funciones de scripting de VSA. Esto les permite enviar cargas maliciosas a través de VSA y potencialmente, exfiltrar datos.

Grupo de hackers REvil

- El grupo de hackers **REvil**, también conocido como **Sodinokibi**, fue una de las bandas de ransomware más notorias y prolíficas del mundo, activa desde 2019. Se especializaron en el modelo de **"ransomware como servicio" (RaaS)**, donde desarrollaban el malware y alquilaban su uso a "afiliados" a cambio de un porcentaje de los rescates pagados.

Tácticas y operaciones clave

- REvil era conocido por sus ataques de **doble extorsión**. No solo cifraban los datos de sus víctimas y exigían un rescate para desbloquearlos, sino que también robaban información sensible y amenazaban con publicarla si no se pagaba. Esto aumentaba la presión sobre las empresas para que cedieran a sus demandas.

Algunos de sus ataques más destacados incluyen:

- **JBS Foods (2021):** El ataque a la empresa cárnica más grande del mundo, por el que exigieron y recibieron un rescate de 11 millones de dólares.
- **Acer y Colonial Pipeline:** Aunque no se les atribuye directamente el ataque a Colonial Pipeline, se les ha relacionado con el modus operandi y la banda que lo llevó a cabo, DarkSide. REvil también exigió una cifra récord de 50 millones de dólares a la compañía tecnológica Acer.
- **Kaseya VSA (2021):** Su ataque más notorio, un ataque a la cadena de suministro que comprometió el software de Kaseya para infectar a miles de empresas en al menos 17 países. Exigieron un rescate global de 70 millones de dólares.

Desmantelamiento y consecuencias

- Tras el ataque a Kaseya y la presión internacional, el grupo se volvió un objetivo de alta prioridad para **gobiernos de todo el mundo**, incluido Estados Unidos. En octubre de 2021, sus sitios web de filtración se volvieron inaccesibles, lo que llevó a especulaciones sobre su desaparición.
- Finalmente, en enero de 2022, el Servicio Federal de Seguridad de Rusia (FSB) anunció que había desmantelado el grupo a petición de Estados Unidos. Se incautaron grandes sumas de dinero y se detuvo a varios miembros. Más tarde, algunos de ellos, como Yaroslav Vasinskyi, el presunto responsable del ataque a Kaseya, fueron extraditados y procesados en EE. UU.
- A pesar de estos esfuerzos, el modelo de RaaS ha demostrado ser resiliente. Aunque REvil fue desmantelado, otros grupos han surgido utilizando tácticas similares, lo que demuestra la naturaleza persistente de esta amenaza.

Cronología

5 de febrero de 2019

- Piratas informáticos atacan un complemento específico de ConnectWise para la plataforma Kaseya VSA [i].

https://www.brodersendarknews.com/p/operacion-cronos-lockbit-ransomware-takedown

3 de septiembre de 2020

- Se anuncia la **posible salida a bolsa de Kaseya.**

  "Si se concreta una IPO de Kaseya, el plazo objetivo parece ser **2021** aproximadamente."

  "Las ambiciones de Kaseya de salir a bolsa no son únicas. Su rival Datto también está preparando una posible salida a bolsa , y SolarWinds MSP podría escindirse de su matriz SolarWinds y convertirse en su propia empresa cotizada en bolsa ."[ii]

https://www.cantechletter.com/2024/02/kaseya-ipo-an-overview/

1 de abril de 2021

- Investigadores del Instituto Holandés para la Divulgación de Vulnerabilidades **(DIVD)** [iii] identificaron la primera de lo que rápidamente se consideraron **siete vulnerabilidades** - todas fáciles de detectar, algunas potencialmente catastróficas - en un sistema de gestión de TI conocido como Administrador Virtual del Sistema **(VSA)** [iv].

https://www.linkedin.com/company/divd-nl/posts/

6 de abril de 2021

- El DIVD habían encontrado 2200 sistemas vulnerables y comunicaron sus hallazgos a Kaseya, la empresa responsable de VSA. **Kaseya parcheó cuatro de las siete** vulnerabilidades en los días y semanas siguientes, pero tres permanecieron.
- Una de las vulnerabilidades es la **CVE-2021-30121** [v] que fue una de las llaves utilizadas por los ciberatacantes para perpetrar el ataque.
- **Victor Gevers** [vi] , director del DVID declara posterior al ataque, en relación a la **antesala del ataque** del 2 de julio de 2021, "Realmente creo que se estaban esforzando al máximo; publicaban ofertas de trabajo, contrataban a nuevos especialistas en seguridad, contrataban a empresas de seguridad externas, revisaban el código fuente, verificaban sus perímetros y trabajaban arduamente en su estrategia de seguridad. Pero era mucho a la vez".

https://www.cyberhelden.nl/episodes/episode-3/

2 de julio de 2021

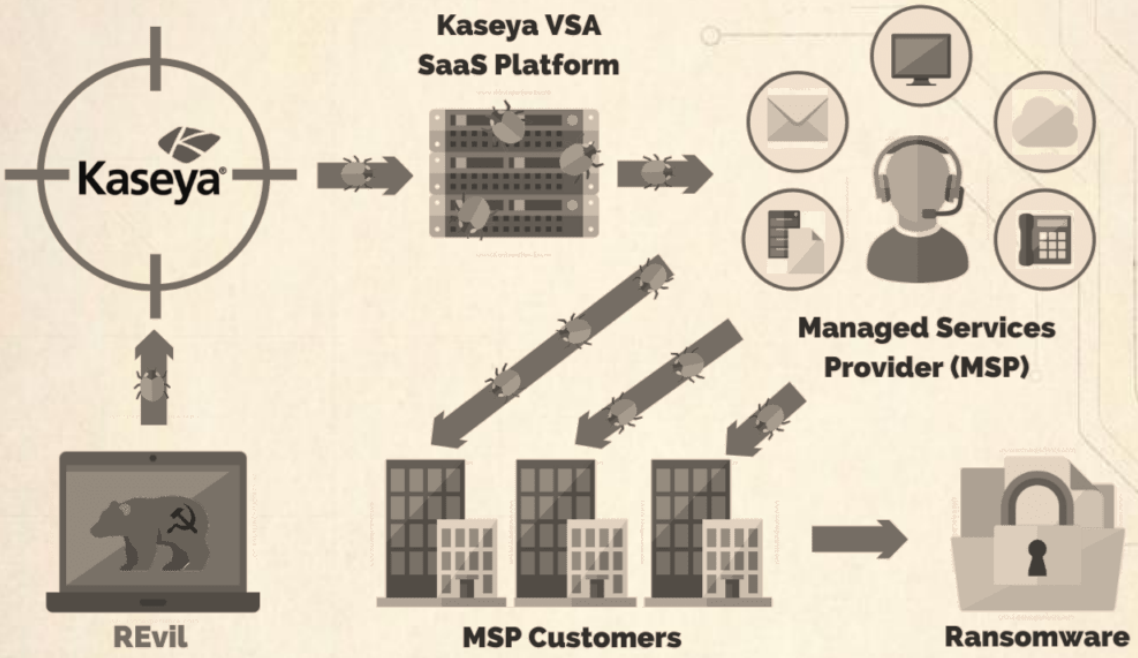
2238 sistemas comprometidos. Fuente DIVD.

Durante la mañana del día viernes se dispararon las alertas, recordar que el **4 de julio** es un **feriado** importante en EEUU.

- ConnectWise, empresa que ofrece soluciones complementarias para MSPs que se integran con las solución VSA de Kaseya, desactiva temporalmente todas las integraciones locales y en la nube de Kaseya con ConnectWise Manage como medida de precaución.
- Debido a que inicialmente no se conocía la causa del problema, **Kaseya apagó inmediatamente los servidores internos SaaS** como medida de precaución.
- Aunque no es un protagonista directo del caso, las declaraciones al medio MSSP Alert por parte de **John Hammond** , investigador sénior de seguridad de Huntress [vii] , proveedor de servicios de detección y respuesta gestionadas (MDR) que apoya a los MSP, ofreció una perspectiva externa que sin duda vale la pena consignar y considerar:
- "Recibimos la primera notificación a las 12:35 ET de hoy y hemos tenido que poner manos a la obra para responder y concienciar a la comunidad. **El ransomware sí tiene una firma digital**. El equipo de Kaseya ha sido muy receptivo con nuestra inteligencia de amenazas".
- "No podemos dejar de enfatizar que **desconocemos cómo se infiltra esto** en el VSA de Kaseya. De momento, nadie lo sabe".
- "Tenemos conocimiento de cuatro MSP donde todos los clientes están afectados: tres en EE. UU. y uno en el extranjero".

- "Los MSP con **miles de puntos finales** están siendo atacados".
- “Hemos visto que, cuando un MSP se ve comprometido, tenemos pruebas de que se ha propagado a través del VSA a todos los clientes del MSP.”
- “El VSA de Kaseya puede estar alojado localmente o en la nube. Actualmente, todos sus servidores en la nube están fuera de línea por mantenimiento de emergencia”.
- A la pregunta “¿Esto indica que Kaseya ha sufrido una vulneración?” el investigador respondió: “Actualmente, entre la media docena de MSP que sabemos que están comprometidos, el **único punto en común es Kaseya VSA**”.
- "Basándonos en todo lo que estamos viendo ahora mismo, creemos firmemente en este REvil/Sodinikibi".
- Actualmente, tenemos tres socios de Huntress afectados, con aproximadamente **200 empresas** cifradas.
- "El ejecutable legítimo de Windows Defender se utilizó para cargar de forma lateral una DLL maliciosa".
- A las 16:11 ET (dos horas después de que el equipo de seguridad recibiera las alertas), Kaseya informó de un posible ataque al software VSA contra un “pequeño número” de clientes aunque Huntress afirma que la cifra es de más de 200. Además de recomendar el apagado a sus clientes, estos últimos comenzaron a recibir notificaciones urgentes para apagar sus servidores VSA y evitar que sus datos se vieran comprometidos.
- Siguiendo el protocolo, **Kaseya notificó a las agencias de seguridad cibernética gubernamentales y policiales**. Una coalición de inteligencia cibernética formó una estrategia para la contención y la comprensión de los detalles de lo que había sucedido.

- **CISA emite una alerta** sobre el ataque [viii], indicando que la agencia está monitoreando los detalles sobre un "ataque de ransomware en la **cadena de suministro** contra Kaseya VSA y los múltiples proveedores de servicios administrados (MSP) que emplean el software VSA".



Kaseya VSA Ransomware Attack Explained ix

3 de julio de 2021

2254 sistemas comprometidos. Fuente DIVD.

- Kaseya anuncia que ha sido víctima de un ciberataque sofisticado. Las recomendaciones de dejar los servidores VSA inactivos seguían vigentes.
- Expertos externos aconsejaron a Kaseya que cualquier cliente afectado por ransomware no hiciera clic en enlaces **ni pagara un rescate**.
- El equipo de Kaseya emitió numerosos avisos sobre la vulnerabilidad y garantizó a los clientes la remediación de las vulnerabilidades actuales.
- Los ejecutivos de Kaseya **comenzaron a contactar directamente a los clientes afectados para determinar el alcance del impacto** y determinar la mejor manera de ayudarlos.
- El equipo de investigación y desarrollo replicó el vector de ataque y colaboró con una empresa de informática forense para identificar cualquier IOC.
- La **recomendación para los servidores locales era permanecer fuera de línea hasta que se pudieran publicar los parches**. Asimismo, los servidores SaaS y VSA alojados permanecieron fuera de línea.
- De los más de 30.000 clientes, unos **50 proveedores fueron atacados** y comprometidos antes de que Kaseya cerrara VSA.
- Al infiltrarse en los portales de internet, los atacantes podían emitir cargas maliciosas de forma muy eficiente a través de VSA.
- Tras el ataque, **la Casa Blanca**, en colaboración con varias agencias del gobierno federal, emitió directrices a Kaseya.

- El presidente de EE.UU., **Joe Biden**, se manifestó sobre el ataquex. "La idea inicial fue que no era el gobierno **ruso**, **pero todavía no estamos seguros**", también señalo que había ordenado a las agencias de inteligencia estadounidenses que investigaran, y que Estados Unidos responderá si determinan que Rusia es responsable.
- Tras un ataque importante, el objetivo es proteger los datos de daños adicionales. Debido a la naturaleza modular del sistema de seguridad de Kaseya, el alcance de la brecha fue VSA.

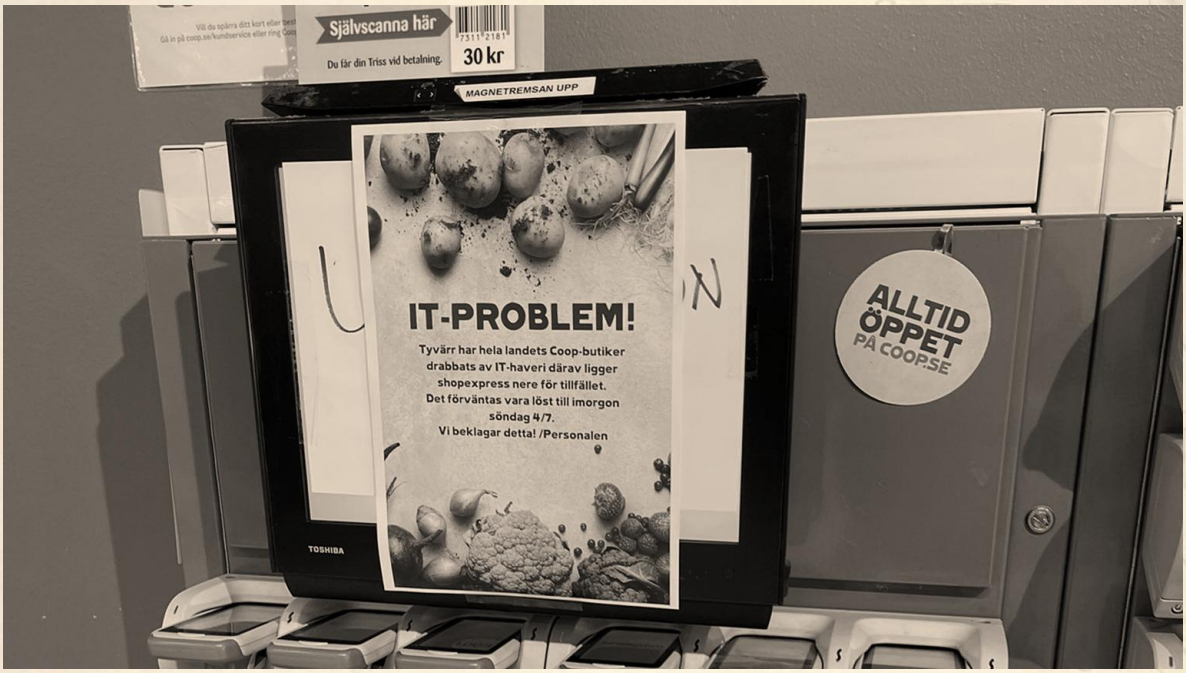
https://www.letelegramme.fr/monde/joe-biden-sous-pression-avec-la-cyberattaque-contre-lediteur-kaseya-3816706.php

4 de julio de 2021

591 sistemas comprometidos. Fuente DIVD.

- **Fred Voccola**, CEO de Kaseya, concedió una entrevista sobre el incidente de VSA en Good Morning America, de la cadena ABC.
- Antes de la reunión, se puso a disposición de los clientes de VSA una nueva herramienta de detección de vulnerabilidades. Como resultado, muchos usuarios pudieron sentirse seguros sabiendo que su sistema no estaba comprometido.
- El equipo de Respuesta a Incidentes de **FireEye Mandiant** [xi], una destacada firma especializada en ciberseguridad es contratada por Kaseya. El objetivo de Kaseya era comprender con confianza el alcance del problema y remediar sus impactos.
- Se informa que entre 50 y 60 clientes (MSP) de Kaseya fueron afectados, no se mencionó cuántos clientes finales y puntos finales de MSP sufrieron ataques de ransomware.
- El ataque afecta a víctimas en al menos **17 países**, incluidos Reino Unido , Sudáfrica , Canadá , Argentina , México , Indonesia , Nueva Zelanda y Kenia.
- La cadena de supermercados sueca **Coop** anunció que la mayoría de sus **800 tiendas** permanecerán cerradas por segundo día el domingo debido a que su proveedor de software de caja registradora se encuentra dañado.
- También se vieron afectados una cadena de farmacias suecas, una cadena de gasolineras, los ferrocarriles estatales y la radiodifusión pública SVT.
- Dos grandes empresas de servicios holandesas, VelzArt y Hoppenbrouwer Techniek , se vieron afectadas

- Debido a la presencia internacional de los clientes de VSA, el **FBI colaboró** con clientes extranjeros para establecer y aplicar un proceso de gestión de incidentes.



https://www.bleepingcomputer.com/news/security/coop-supermarket-closes-500-stores-after-kaseya-ransomware-attack/

5 de julio de 2021

138 sistemas comprometidos. Fuente DIVD.

- **VSA es el único producto de Kaseya afectado** por el ataque y todos los demás módulos de IT Complete no se vieron afectados, dice la compañía.
- **REvil exigió un rescate de 70 millones de dólares** en Bitcoin. El dinero se pagaría a los hackers para que descifraran los archivos de todos los sistemas comprometidos [xii].
- El director ejecutivo de Kaseya, Fred Voccola, habló con Anne Neuberger, asesora adjunta de seguridad nacional de EE. UU., sobre el ataque. Voccola declaró a la Casa Blanca que Kaseya no tenía conocimiento de **ninguna infraestructura crítica afectada** por el ransomware ni de **víctimas relacionadas con la seguridad nacional.**

https://grahamcluley.com/kaseya-offers-universal-decryptor-to-customers-following-ransomware-attack/

6 de julio de 2021

88 sistemas comprometidos. Fuente DIVD.

- Kaseya **cambió** la dirección IP subyacente de sus servidores VSA.
- Kaseya esperaba que sus servidores SaaS volvieran a estar en línea el 6 de julio entre las 4:00 p. m. y las 7:00 p. m. ET, pero surgió un problema que retrasó el reinicio.
- Kaseya ha desarrollado un parche para clientes con **entornos locales** y espera que esté disponible dentro de las 24 horas (o menos) después de que se hayan activado los servidores SaaS de la empresa.
- El comunicado de la compañía emitido al mediodía (hora del Este de EE. UU.) también describió las medidas de seguridad adicionales que están implementadas.
- **Altos funcionarios del equipo de seguridad nacional de la administración Biden planean reunirse con altos funcionarios del Kremlin,** según la secretaria de prensa de la Casa Blanca, Jen Psaki.
- En un video lanzado en **Youtube** [xiii], Fred Voccola (CEO de Kaseya) explicó que el retraso se debe a las nuevas mejoras de seguridad planificadas y no a un problema de restauración, afirmó que la decisión de retrasar el reinicio de SaaS fue totalmente suya.

7 de julio de 2021

68 sistemas comprometidos. Fuente DIVD.

- Según Wall Street Joournal, **Kaseya recibió una advertencia sobre la vulnerabilidad que causó el ataque a principios de abril de 2021**, según el Instituto Holandés para la Divulgación de Vulnerabilidades (DIVD). Kaseya respondió con urgencia tras ser notificada de las vulnerabilidades, pero la compañía sigue trabajando para parchear completamente su software VSA.
- **El ataque evita los sistemas en idioma ruso**; el ciberataque utilizó código de ransomware "para evitar sistemas que tienen idiomas predeterminados de lo que era la región de la URSS", informa Trustwave , uno de los 250 principales MSSP.
- **Virginia Tech** sufre un ataque de ransomware que afectó a aproximadamente **600 computadoras** de Virginia Tech, **cliente de Kaseya VSA.**
- IT Glue , una división de Kaseya, ha publicado una carta abierta instando a ConnectWise a reactivar la integración con la plataforma de software de documentación MSP IT Glue. Kaseya e IT Glue, afirman que el ciberataque se limitó a VSA y no involucró a IT Glue[xiv]. Por su parte ConnectWise, declara en carta abierta a sus clientes que debido a lo sofisticado del ataque, **mantendrán la desactivación del servicio VSA de Kaseya hasta que se confirme oficialmente que no hay riesgos** asociados y ofrecen ayuda para realizar una auditoría.

8 de julio de 2021

- Algunas personas enviaban correos electrónicos spam maliciosos haciéndose pasar por el equipo de soporte de Kaseya. Kaseya modificó sus actualizaciones de correo electrónico para excluir enlaces o archivos adjuntos.
- Gobiernos locales afectados. Dos pequeños pueblos de Maryland, **Leonardtown y North Beach**, parecen ser los primeros afectados por el ataque de ransomware REvil contra Kaseya. Leonardtown obtiene sus servicios de TI de JustTech , un proveedor de servicios gestionados (MSP) en La Plata, Maryland [xv].

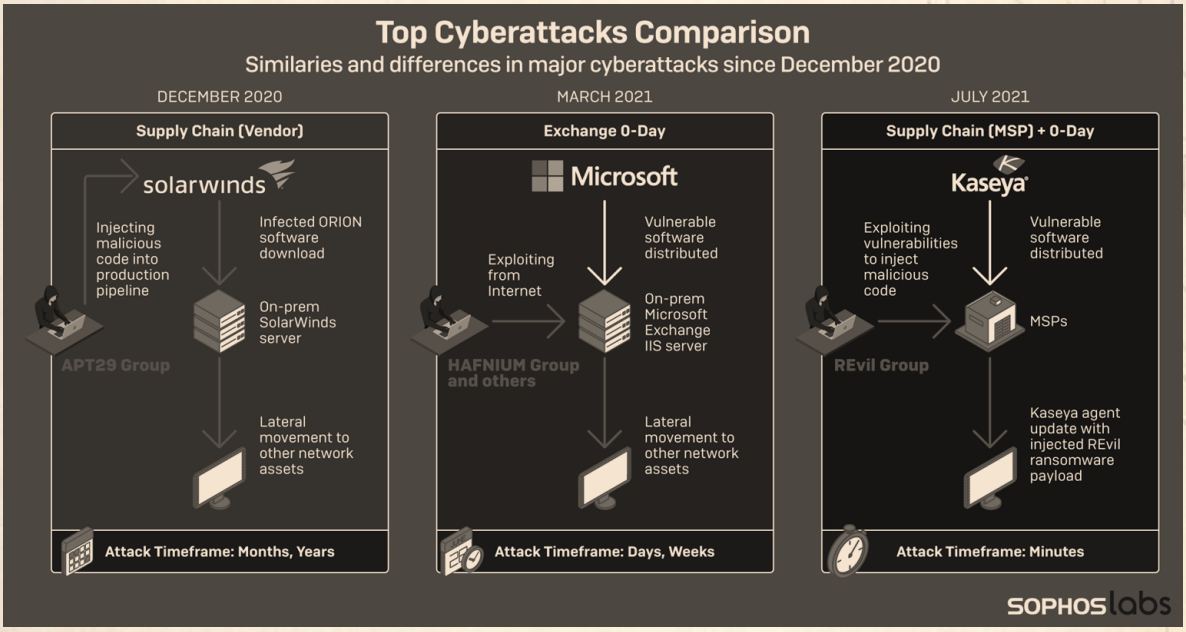
https://www.linkedin.com/pulse/shut-down-everything-global-ransomware-attack-takes-small-ramlet/

11 de julio de 2021

- **Ex-empleados afirman que Kaseya sabia de fallos críticos pero los ignoraron** [xvi].
- Kaseya sigue en camino para lanzar el parche local de VSA y comenzar la implementación en la infraestructura SaaS de VSA hoy (domingo, 11 de julio a las 16:00 EDT), según informó la compañía. Voccola reveló el objetivo del 11 de julio en un video publicado el 6 de julio. Las correcciones estaban programadas originalmente para el 6 de julio, pero Voccola detuvo la implementación para implementar medidas de seguridad adicionales, según declaró el mismo día.

12 de julio de 2021

- Después de un retraso el 6 de julio, la plataforma VSA basada en SaaS de Kaseya comenzó a **reactivarse** con mejoras de seguridad el domingo 11 de julio de 2021. La restauración de SaaS parece estar completa, aunque **Kaseya tuvo un mantenimiento de infraestructura de SaaS no planificado durante el día de la restauración.**



https://news.sophos.com/wp-content/uploads/2021/07/infographic.png

13 de julio de 2021

- **Guía de CISA para MSP de Kaseya**. CISA (Agencia de Seguridad Cibernética y de la Información) ha emitido esta guía para MSP y clientes que ejecutan el software VSA de Kaseya [xvii].
- **REvil desaparece.** Los sitios web gestionados por la banda de ransomware REvil se volvieron repentinamente **inaccesibles**, lo que desató la especulación generalizada de que el grupo había sido desconectado, posiblemente por el **gobierno estadounidense** [xviii].
- Integración de ConnectWise con IT Glue. **ConnectWise** , a las 10:00 a. m. ET, **reactivó una integración con IT Glue** , una plataforma de documentación para MSP propiedad de Kaseya. ConnectWise reactivó la conexión tras recibir garantías por escrito de Mandiant de que IT Glue no se vio afectado por el incidente de VSA. Kaseya contrató a Mandiant para investigar el ataque a VSA. ConnectWise también realizó una evaluación de riesgos y, posteriormente, reactivó las integraciones de ConnectWise Manage y Automate con IT Glue. Cuando se produjo el ataque a VSA, ConnectWise indicó que deshabilitaría la conexión con IT Glue por precaución.

21 de julio de 2021

- **Kaseya obtuvo un descifrador** para las víctimas del ataque del ransomware REvil y está trabajando para remediar la situación de los clientes afectados, según reveló la compañía el 22 de julio. Kaseya **no especificó si pagó algún tipo de extorsión** a la banda del ransomware REvil para obtener la clave. **Emsisoft ha confirmado que la clave es eficaz para desbloquear a las víctimas**, añade Kaseya. La clave fue entregada por el FBI, como admitiría la misma organización federal el 22 de septiembre de 2021.

23 de julio de 2021

- Los clientes deben firmar un **acuerdo de confidencialidad (NDA) para recibir la clave de descifrado** de la empresa de software xix. Esta práctica de confidencialidad no es infrecuente en el mercado cibernético, pero el NDA podría dificultar la comprensión del ataque y la recuperación en general, señala CNN.

26 de julio de 2021

- **Kaseya no pagó un rescate**, ni directa ni indirectamente a través de un tercero, para obtener la clave de descifrado para el ataque de ransomware REvil que ocurrió el 2 de julio de 2021, reveló la compañía de software MSP el 26 de julio de 2021xx.
- La compañía detalló que **obtuvo la herramienta de "un tercero"** y que cuenta con equipos que ayudan activamente a los clientes afectados, de los que no existen reportes de algún problema asociado con el nuevo descifrador.

https://australiancybersecuritymagazine.com.au/kaseya-denies-ransom-payment-as-decryptor-key-released/#prettyPhoto

4 de agosto de 2021

- Kaseya continuó ofreciendo actualizaciones. En consonancia con la filosofía de la compañía de proteger a sus clientes, se lanzaron numerosas versiones de actualizaciones de seguridad que reforzaron la seguridad de los sistemas VSA.
- Kaseya logró mitigar por completo el impacto del ransomware mediante **"el desarrollo"** de una clave de descifrado universal. Además, la organización emitió parches para los CVE identificados en el sistema de Kaseya.

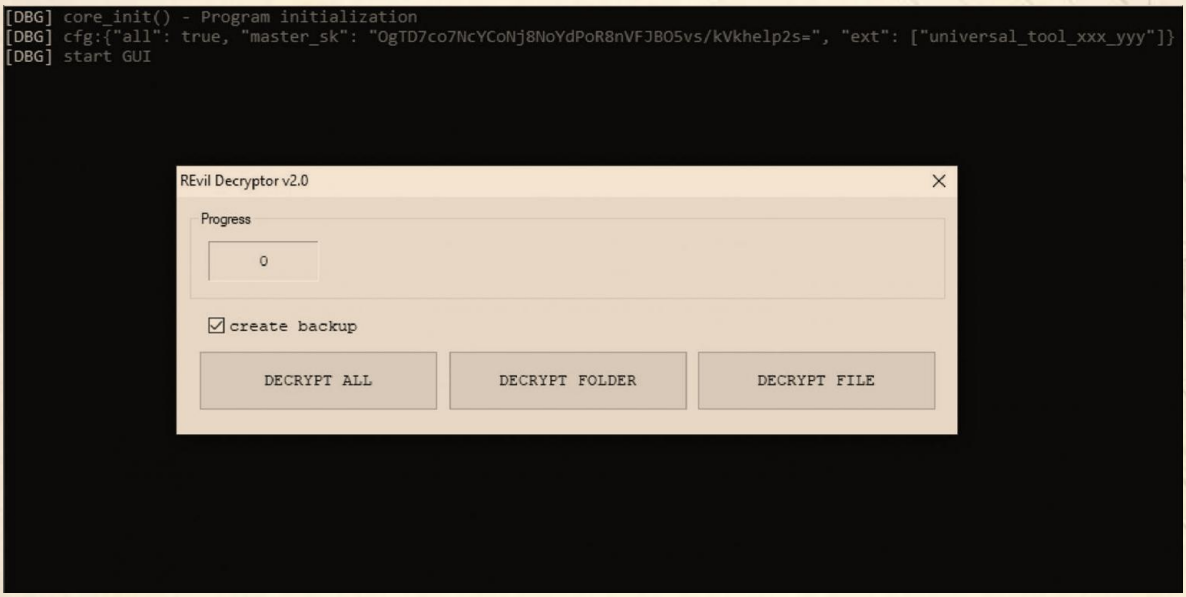
11 de agosto de 2021

La **clave de descifrado universal** del ataque de REvil a los clientes de Kaseya **se filtró en foros de hackers**, lo que permitió a los investigadores obtener un primer vistazo a la **misteriosa clave** xxi.

https://www.bleepingcomputer.com/news/security/kaseyas-universal-revil-decryption-key-leaked-on-a-hacking-forum/

22 de septiembre de 2021

- El **FBI admitió que ocultó** durante casi tres semanas una **clave de descifrado** que habría descongelado los sistemas de docenas de MSP y cientos de empresas paralizadas por el ataque del ransomware REvil al software VSA de Kaseya en julio de 2021 [xxii].



https://www.bleepingcomputer.com/news/security/kaseyas-universal-revil-decryption-key-leaked-on-a-hacking-forum/

17 de octubre de 2021

El grupo de ransomware REvil pasó a la **clandestinidad** tras el ataque a sitios Tor. REvil es el objetivo de numerosas agencias debido a sus recientes ataques a empresas de alto perfil en Estados Unidos. Durante octubre y noviembre, REvil se convirtió en un objetivo destacado para los grupos de defensa. Ha habido numerosos intentos de represalia.

https://www.theage.com.au/world/north-america/we-will-fight-back-revil-ransomware-hackers-charged-in-internation-operation-20211109-p5974n.html

9 de marzo de 2022

Yaroslav Vasinskyi, el presunto hacker de Kaseya VSA , fue **extraditado y procesado** ante un tribunal de Dallas, Texas. [xxiii.]

https://www.bbc.com/news/technology-59215167

20 de abril de 2022

El antiguo sitio web de filtraciones de REvil volvió a estar disponible. xxiv.

1 de mayo de 2024

Yaroslav Vasinskyi es condenado a 13 años de presidio [xxv].

https://edition.cnn.com/2024/05/01/politics/ransomware-attack-sentencing-revil

Febrero 2025

"Tuve que asumir la culpa por todos porque Estados Unidos no tenía poder para perseguir a los verdaderos responsables".

Yaroslav Vasinskyi [xxvi]

https://analyst1.com/ransomware-diaries-volume-7-i-had-to-take-the-guilt-for-everyone-the-kaseya-hacker-breaks-his-silence/

¿Qué salió mal?

Teoría.

Mi teoría es que basándose en la cronología y el análisis de los hechos, lo que salió mal fue la **convergencia de múltiples factores** que crearon una tormenta perfecta de vulnerabilidad, oportunidad y fallas en la respuesta, lo que potenció el éxito del ataque de REvil.

El ataque a Kaseya no fue el resultado de un solo error, sino de una alineación de fallos y circunstancias que se reforzaron mutuamente.

- **Vulnerabilidades técnicas y falta de parches**
  La base del ataque fue la existencia de vulnerabilidades conocidas y no parcheadas en el software VSA de Kaseya, específicamente la **CVE-2021-30121**. Aunque Kaseya había sido alertada por el **DIVD** y estaba trabajando en las correcciones, no lo hizo a tiempo. La declaración del director del DIVD, **Victor Gevers**, de que "era mucho a la vez" sugiere que la empresa estaba sobrecargada, lo que indica una posible **falta de priorización** de la seguridad en el desarrollo y mantenimiento del producto.

- **El momento estratégico del ataque**
  Los atacantes de REvil eligieron el momento perfecto; un viernes antes del fin de semana largo del **4 de julio en EE. UU.**, un periodo en el que muchas empresas operan con menos personal de seguridad. Esta elección les dio una **ventana de oportunidad** crucial para que el ransomware se propagara ampliamente **antes de que la respuesta** fuera totalmente efectiva.

- **La naturaleza de la cadena de suministro**
  Kaseya VSA era un objetivo de alto valor precisamente por su papel en la cadena de suministro. Era el **único punto de control** que los atacantes necesitaban comprometer para acceder a miles de empresas. **La confianza** que los MSP depositan en Kaseya para administrar sus sistemas **fue la clave** que los atacantes utilizaron para entrar en las redes de los clientes.

- **Falla en la gestión de crisis por parte del gobierno**
  La decisión del FBI de **retener la clave** de descifrado durante casi tres semanas es un elemento por decirlo de algún modo, **"CONTROVERSIAL".** Si bien su estrategia pudo haber sido intentar rastrear y detener a los atacantes, las consecuencias fueron devastadoras para las empresas paralizadas que no pudieron recuperar sus sistemas. Esta acción prolongó el daño del ataque y generó una brecha de confianza entre las víctimas y las agencias de gobierno.

El punto de inflexión, o el momento en que el ataque podría haberse evitado, fue el **periodo de tiempo entre el 6 de abril y el 2 de julio de 2021**. Si, la antesala del ataque.

En este lapso, Kaseya **fue advertida de las vulnerabilidades** por el DIVD y según la cronología, comenzó a trabajar en los parches. Si Kaseya hubiera **priorizado la corrección de las vulnerabilidades críticas**, especialmente la que fue utilizada para el ataque, el **"vector de ataque"** habría sido **neutralizado.**

Aunque el momento y la naturaleza de la cadena de suministro potenciaron el ataque, la existencia de una vulnerabilidad sin parchear fue la condición necesaria para que todo lo demás pudiera ocurrir. **Si esa vulnerabilidad hubiera sido eliminada a tiempo, el ataque, en su forma exitosa, simplemente no habría sucedido.**

Contramedidas

desde experiencia del ataque

1. Verificación de la cadena de suministro

No es suficiente solo auditar nuestra propia red. Como se demostró, el eslabón más débil puede ser el proveedor.

- **Auditorías a proveedores**

  Exige a tus proveedores de software y servicios, especialmente aquellos con acceso a tu infraestructura, que realicen auditorías de seguridad periódicas e independientes. Pide ver los resultados y verifica su postura de seguridad, no solo confíes en su palabra.

- **"Least Privilege" para proveedores**

  Asegúrate de que los permisos que otorgas a los proveedores de software (como un VSA) sean los mínimos necesarios para que funcionen. En el caso de Kaseya, el software tenía un alto nivel de acceso a los sistemas de los clientes. Minimizar este acceso reduce el riesgo en caso de un compromiso.

2. Gestión de parches y actualizaciones

El ataque se basó en una vulnerabilidad conocida y no parcheada a tiempo.

- **Criterios de priorización de parches**

  No todos los parches son iguales. Crea un sistema de priorización de parches que se centre en las vulnerabilidades que afectan a servicios críticos o que tienen un impacto potencial en la cadena de suministro. **La vulnerabilidad de Kaseya VSA debería haber sido una prioridad absoluta.**

- **Comunicación de alerta rápida**

  Establece un **canal de comunicación de emergencia** con tus proveedores para recibir notificaciones sobre vulnerabilidades de alta gravedad. En el caso de Kaseya, el DIVD alertó a la empresa; la lección es que las empresas deben tener un canal de respuesta rápida para estas alertas.

3. Segmentación y aislamiento de redes

Si el VSA se hubiera aislado, el ataque no se habría propagado tan rápidamente.

- **Segmentación de redes**

  Divide tu red en segmentos más pequeños y aplica políticas de seguridad estrictas en los puntos de entrada. Si un sistema VSA o un software de terceros se ve comprometido, su acceso está limitado a un segmento de red pequeño, evitando que se propague a toda la red de tu empresa y a la de tus clientes.

4. Resiliencia en la práctica

La capacidad de recuperarse es tan importante como la capacidad de prevenir.

- **Pruebas de recuperación de desastres**

  No basta con tener copias de seguridad. Es vital **probarlas periódicamente** para asegurarte de que son funcionales y que puedes restaurar tus sistemas y datos rápidamente en caso de un ataque. Las copias de seguridad deben estar

separadas de la red para evitar que sean cifradas por el ransomware.

- **Planes de Respuesta a Incidentes (IRP)**

  Tu plan de respuesta no debe ser solo un documento. Debe ser un proceso **vivo**, con equipos de respuesta dedicados y capacitaciones regulares. **La rápida respuesta de Kaseya al apagar sus servidores fue clave para detener la propagación**, una medida que formaba parte de su plan de respuesta, aunque no pudo evitar el inicio del ataque.

En resumen, el enfoque no debe ser solo técnico (como la validación de entrada o el uso de un WAF), sino también **estratégico**. Se trata de gestionar el riesgo de terceros, construir una resiliencia proactiva y prepararse para lo inevitable a través de pruebas rigurosas.

Impacto económico

No existe una cifra única y oficial para las pérdidas económicas totales del ataque a Kaseya, ya que las pérdidas se distribuyeron entre miles de empresas afectadas en al menos 17 países. Sin embargo, los informes y análisis de varias fuentes de ciberseguridad y noticias permiten realizar algunas estimaciones respecto del costo de este ataque a partir de varios elementos:

1. **Demanda de rescate**

   La banda REvil exigió un rescate global de **70 millones de dólares en Bitcoin** para una clave de descifrado universal. Si bien Kaseya afirmó no haber pagado este rescate, la magnitud de la cifra refleja el valor que los atacantes consideraban que podían extraer. Algunos clientes más pequeños recibieron demandas de rescate individuales de entre 50.000 y 5 millones de dólares.

2. **Costo de la interrupción del negocio**

   Esta es probablemente la pérdida más significativa y **más difícil de cuantificar**. El ataque causó el cierre de operaciones para muchas empresas. Un ejemplo destacado fue la cadena de supermercados sueca **Coop**, que tuvo que cerrar la mayoría de sus **800 tiendas** durante días porque sus cajas registradoras estaban paralizadas. Otras víctimas incluyeron farmacias, ferrocarriles y escuelas. **La pérdida de ingresos y la interrupción de la productividad** para cientos o miles de empresas a nivel global es un costo incalculable.

3. **Costo de recuperación**

Las empresas afectadas tuvieron que incurrir en gastos significativos para recuperarse, que incluyen:

- **Servicios de respuesta a incidentes**

  La contratación de empresas forenses y de seguridad como Mandiant para investigar y remediar la brecha.

- **Costo de mano de obra**

  Horas de trabajo del personal de TI para restaurar sistemas, limpiar el malware y aplicar parches.

- **Nuevas inversiones en seguridad**

  Las empresas afectadas tuvieron que actualizar sus sistemas de seguridad, implementar nuevos controles y fortalecer sus defensas para evitar futuros ataques.

- **Daños a la reputación**

  Las empresas que sufrieron el ataque, especialmente los MSP, enfrentaron una pérdida de confianza por parte de sus clientes, lo que puede llevar a una pérdida de negocio a largo plazo.

4. **Costos Legales y de Cumplimiento**

   No hubo demandas más que las de Kaseya hacia REvil. En este sentido la legislación existente no recomendaba realizar algún tipo de demanda colectiva como lo señala un artículo de Scott & Scott LLP, "los MSPs que consideran emprender acciones legales contra Kaseya deben revisar detenidamente los términos de licencia y los acuerdos con sus usuarios finales. Kaseya ha establecido cláusulas en sus contratos que buscan limitar su responsabilidad, lo que podría dificultar la viabilidad de demandas legales por parte de los MSPs afectados"[xxvii].

En resumen, aunque el rescate de 70 millones de dólares acaparó los titulares, las **pérdidas económicas reales superan con creces esa cifra**, distribuidas en los costos de recuperación, la pérdida de ingresos y el daño a la reputación para un número considerable de empresas en todo el mundo. Un informe de Fortinet indica que el costo promedio para recuperarse de un ataque de ransomware puede superar los 10 millones de dólares[xxviii], y aunque no hay una cifra oficial para Kaseya, la escala del ataque sugiere que el costo total fue enorme.

Conclusión

El caso de Kaseya refleja con claridad la realidad actual en materia de ciberseguridad; **mientras más grande y visible es una empresa, mayor es la probabilidad de que se convierta en un objetivo atractivo** para los ciberatacantes. Además, confirma una práctica conocida en la comunidad, que los **fines de semana y las fechas festivas representan momentos críticos donde las organizaciones suelen estar más expuestas**, lo que incrementa las posibilidades de éxito para los atacantes.

Otro aspecto relevante es la **opacidad en torno al pago de los rescates**. Al igual que en los secuestros de personas, la información sobre si se realizan o no los pagos **rara vez se confirma**, **precisamente para evitar incentivar a los delincuentes**. Sin embargo, queda de manifiesto que este tipo de grupos criminales actúa de forma organizada y con una **"ética profesional"** propia, ya que si no cumplieran con devolver el acceso tras un pago, perderían credibilidad y disminuiría la motivación de las víctimas a ceder en el futuro.

La situación de Kaseya también evidencia que, aunque se estuvieran aplicando correcciones, estas no fueron implementadas con la urgencia que el contexto exigía. Esto subraya la importancia de **establecer prioridades** claras **en la gestión de vulnerabilidades y parches**, entendiendo que una demora puede marcar la diferencia entre contener un riesgo o enfrentar un ataque a gran escala. En este sentido, la respuesta rápida (aunque no completamente suficiente) sí logró mitigar parte del daño, mostrando que **contar con un plan de respuesta a incidentes y ejecutarlo de manera disciplinada puede reducir el impacto de un ataque masivo**.

A la luz de todo lo anterior, el caso Kaseya también destaca dos aspectos críticos. Primero, la importancia de **la comunicación en tiempos de crisis**, demostrada por la aparición

del CEO de la compañía, Fred Voccola, en YouTube, **un acierto** que ayudó a calmar la incertidumbre de los clientes y **humanizar la respuesta de la empresa.** Segundo, las profundas **implicaciones políticas** que tiene este tipo de ciberataques, especialmente al trascender al ámbito **geopolítico** y tensar las relaciones entre **Rusia y EE. UU.** a raíz de las sospechas sobre el origen del grupo atacante.

Finalmente, este caso recuerda que la ciberseguridad no es responsabilidad exclusiva de un área técnica, sino un trabajo conjunto que involucra a toda la organización, a proveedores, socios estratégicos, la comunidad de seguridad y, como se demostró, también a los líderes políticos.

En conclusión, la experiencia de Kaseya refuerza la necesidad de estar preparados, de aprender de cada incidente y de comprender que la ciberseguridad es un esfuerzo continuo que exige prevención, colaboración y una respuesta oportuna y multifacética.

Sitios de interés

- **Kaseya responde con rapidez a un ciberataque sofisticado**
  Comunicado del 5 de julio de 2021 de la empresa Kaseya respecto del ciberataque que estaban sufriendo.
  https://www.kaseya.com/press-release/kaseya-responds-swiftly-to-sophisticated-cyberattack-mitigating-global-disruption-to-customers/

- **Análisis del ataque de ransomware Kaseya de 2021: Spearphishing combinado a través de la vulnerabilidad SSLVPN de SonicWall**
  Análisis muy completo a nivel técnico del ataque que complementa este informe con información detallada.
  https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/ise2/1655307

- **Ransomware Diaries Volume 7: "I Had to Take the Guilt For Everyone" – The Kaseya Hacker Breaks His Silence**
  Entrevista a Yaroslav Vasinskyi. Agosto 2025. Repleto de datos sobre REvil, motivaciones y otros. Muy bueno.
  https://analyst1.com/ransomware-diaries-volume-7-i-had-to-take-the-guilt-for-everyone-the-kaseya-hacker-breaks-his-silence/

Citas bibliográficas.

[i] **Hackers Target Particular ConnectWise Plugin to Kaseya VSA Platform**
https://www.msspalert.com/news/hackers-target-connectwise-plugin-to-kaseya-platform?utm_source=chatgpt.com

[ii] **Kaseya's Potential IPO: Call It A Milestone, Not An Exit**
https://www.channele2e.com/news/kaseyas-potential-ipo-call-it-a-milestone-note-an-exit

[iii] **DIVD CSIRT**
https://csirt.divd.nl/

[iv] **The Unfixed Flaw at the Heart of REvil's Ransomware Spree**
https://www.wired.com/story/revil-ransomware-kaseya-flaw-fix-disclosure-april/

[v] **CVE-2021-30121**
https://csirt.divd.nl/cves/CVE-2021-30121/

[vi] **Victor Gevers**
https://x.com/0xDUDE

[vii] **Huntress**
https://www.huntress.com/

[viii] **Kaseya VSA Supply-Chain Ransomware Attack**
https://www.cisa.gov/news-events/alerts/2021/07/02/kaseya-vsa-supply-chain-ransomware-attack

[ix] **Kaseya VSA Ransomware Attack Explained**
https://purplesec.us/breach-report/kaseya-ransomware-attack-explained/

[x] **This article is more than 4 years old**
Biden announces investigation into international ransomware attack
https://www.theguardian.com/technology/2021/jul/03/kaseya-ransomware-attack-us-sweden

[xi] **Mandiant**
https://www.mandiant.com/

[xii] **Hackers Demand $70 Million In Biggest Ransomware Attack On Record**
https://www.youtube.com/watch?v=HuHZQkMvcJk

[xiii] **Video del CEO de Kaseya, Fred Voccola**
https://www.youtube.com/watch?v=XfAyutRfy2A

[xiv] **An Open Letter to ConnectWise CEO, Jason Magee**
https://www.itglue.com/blog/an-open-letter-to-connectwise-ceo-jason-magee/

[xv] **Maryland towns impacted in Kaseya ransomware breach**
https://statescoop.com/kaseya-revil-ransomware-leonardtown-north-beach-maryland/

[xvi] **Former employees claim Kaseya knew of critical flaws but ignored them**
https://siliconangle.com/2021/07/11/former-employees-claim-kaseya-knew-critical-flaws-ignored/

[xvii] **Kaseya Ransomware Attack: Guidance for Affected MSPs and their Customers**
https://www.cisa.gov/news-events/news/kaseya-ransomware-attack-guidance-affected-msps-and-their-customers

[xviii] **Ransomware gang REvil's websites become unreachable**
https://www.reuters.com/technology/ransomware-gang-revils-websites-become-unreachable-2021-07-13/

[xix] **Kaseya Is Making Its Customers Sign Non-Disclosure Agreements to Obtain Ransomware Decryption Key**
https://gizmodo.com/kaseya-is-making-its-customers-sign-non-disclosure-agre-1847356517

[xx] **Kaseya dice que no pagó rescate a delincuentes tras el ciberataque**
https://www.swissinfo.ch/spa/kaseya-dice-que-no-pag%C3%B3-rescate-a-delincuentes-tras-el-ciberataque/46818512

[xxi] **Kaseya's universal REvil decryption key leaked on a hacking forum**
https://www.bleepingcomputer.com/news/security/kaseyas-universal-revil-decryption-key-leaked-on-a-hacking-forum/

[xxii] **FBI Withheld REvil Ransomware Decryptor Key As Some MSPs Suffered Encryption**
https://www.msspalert.com/news/fbi-withheld-revil-ransomware-decryptor-key-as-some-msps-suffered-encryption

[xxiii] **Sodinokibi/REvil Ransomware Defendant Extradited to United States and Arraigned in Texas**
https://www.justice.gov/archives/opa/pr/sodinokibirevil-ransomware-defendant-extradited-united-states-and-arraigned-texas

[xxiv] **Understanding REvil: REvil Threat Actors May Have Returned (Updated)**

https://unit42.paloaltonetworks.com/revil-threat-actors/

[xxv] **Member of ransomware gang sentenced to more than 13 years in prison over 2021 attack**
https://edition.cnn.com/2024/05/01/politics/ransomware-attack-sentencing-revil

[xxvi] **Diarios de Ransomware Volumen 7: «Tuve que asumir la culpa por todos» – El hacker de Kaseya rompe su silencio**
https://analyst1.com/ransomware-diaries-volume-7-i-had-to-take-the-guilt-for-everyone-the-kaseya-hacker-breaks-his-silence/?

[xxvii] **Seven Things MSPs Should Know Before Filing a Lawsuit Against Kaseya for the Recent Ransomware Attack**
https://scottandscottllp.com/seven-things-msps-should-know-before-filing-a-lawsuit-against-kaseya-for-the-recent-ransomware-attack/?utm_source=chatgpt.com

[xxviii] **Estadísticas de ransomware y tendencias de ransomware**
https://www.fortinet.com/lat/resources/cyberglossary/ransomware-statistics