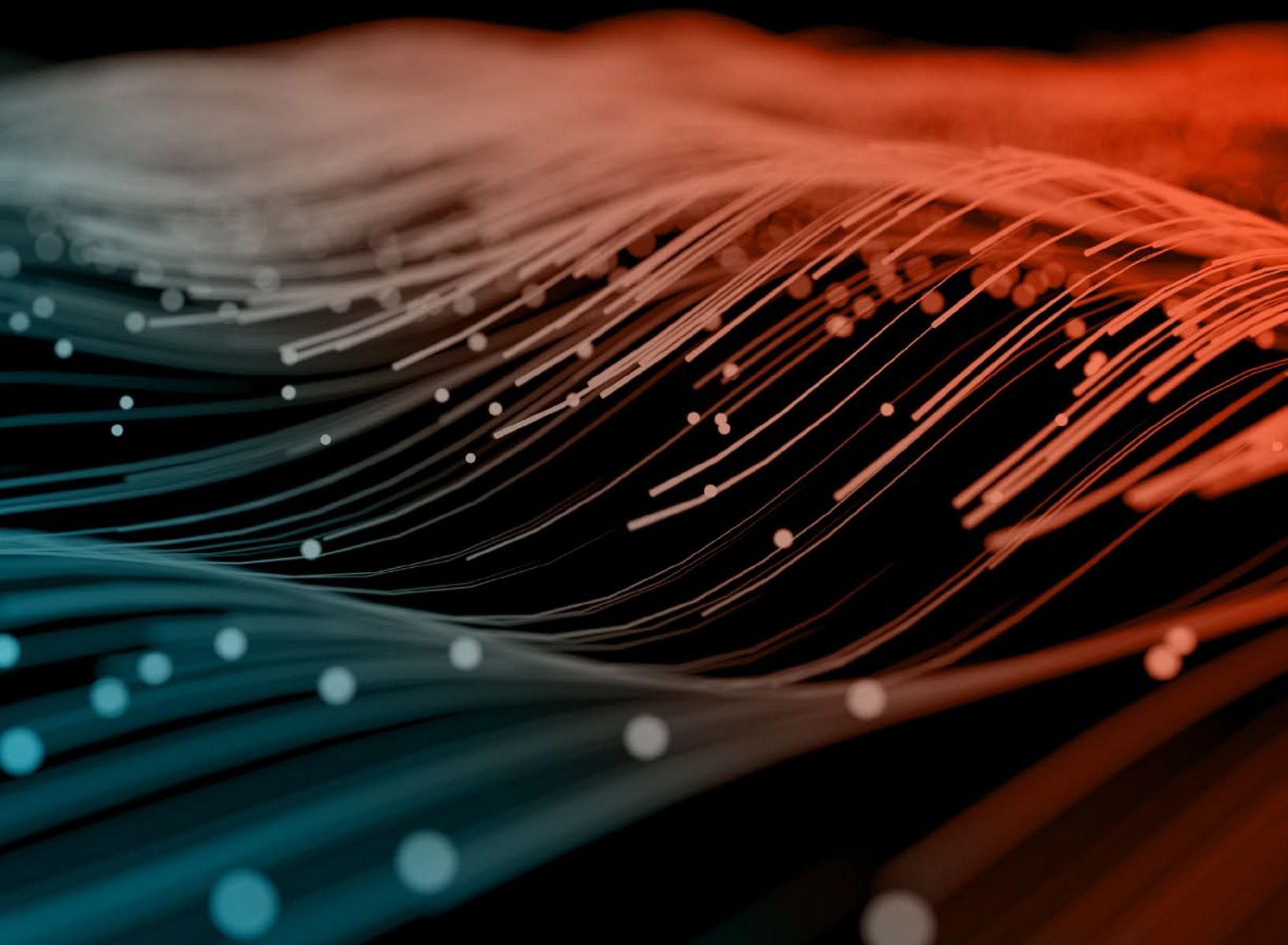
PRISMA CLOUD | UNIT 42 BY PALO ALTO NETWORKS

INFORME SOBRE AMENAZAS EN LA NUBE (primera mitad de 2021)

La dicotomía de la COVID-19: impacto y oportunidades para la seguridad en la nube



Contenido

Prefacio

Al principio de la pandemia de COVID-19, la demanda de servicios en la nube experimentó un rápido repunte. En tan solo unos meses, el porcentaje de empleados que teletrabajaban se disparó, pasando del 20 al 71 %.[1] Además, las empresas aumentaron rápidamente su inversión en la nube durante el tercer trimestre de 2020 (julio-septiembre), un incremento del 28 % con respecto al mismo trimestre de 2019.[2] Este desarrollo cronológico no es casualidad, pues la Organización Mundial de la Salud (OMS) declaró la pandemia por COVID-19 en marzo de 2020. Entre que se produjo una avalancha de teletrabajo y que las organizaciones aceleraron sus planes de migración a la nube, el tercer trimestre de 2020 fue testigo de un aumento interanual gigantesco.

Gracias a los datos obtenidos con los sensores que tenemos repartidos por todo el mundo, nuestro selecto equipo de investigadores de amenazas en la nube **halló una correlación entre el incremento de la inversión en la nube derivado de la COVID-19 y los incidentes de seguridad**.[3] En todo el mundo, las organizaciones aumentaron sus cargas de trabajo en la nube en más de un 20 % (entre diciembre de 2019 y junio de 2020), lo que trajo consigo un aluvión de incidentes de seguridad. Según nuestros estudios, los programas de seguridad en la nube de las organizaciones, independientemente de su localización geográfica, todavía están en mantillas en lo relativo a la automatización de los controles de seguridad (p. ej., DevSecOps y estrategias shift-left), lo que nos lleva a la conclusión de que **el rápido aumento de los recursos en la nube y de la complejidad y la falta de unos controles de seguridad automatizados que estén integrados en todo el ciclo de desarrollo es una combinación nefasta**. De hecho, un estudio anterior concluyó que el 65 % de los incidentes de seguridad en la nube que se hicieron públicos se debieron a errores de configuración cometidos por los propios clientes. Estas son las consecuencias para las empresas que operan en la nube y a gran escala sin controles de seguridad automatizados.

Comparación entre el crecimiento de la nube y los incidentes de seguridad en la nube

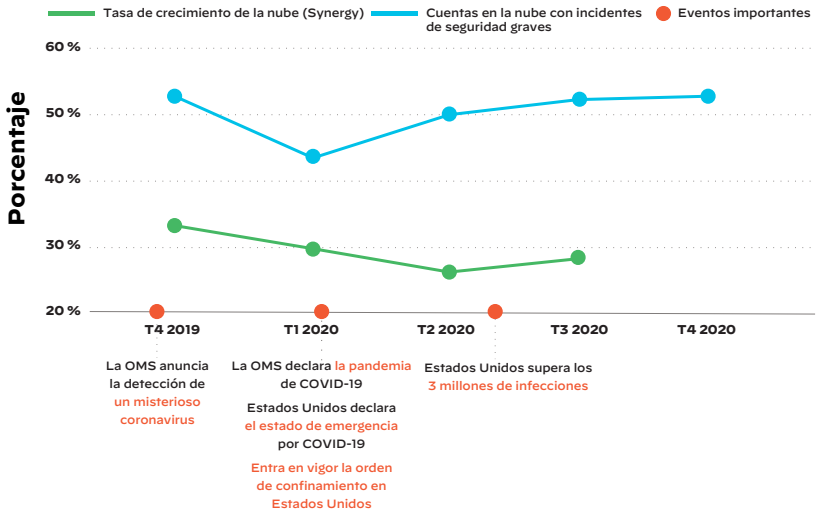


Figura 1: Crecimiento de la nube e incidentes de seguridad

Siga leyendo para conocer las amenazas en la nube más recientes que podrían estar afectando a su organización y descubra por qué centrarse en una plataforma de seguridad con unas normas comunes puede contribuir en buena medida a madurar su programa de seguridad en la nube.

Matthew Chiodi
Director de Seguridad, Nube Pública, Palo Alto Networks

1. *How the Coronavirus Outbreak Has – and Hasn't – Changed the Way Americans Work* (disponible en inglés), Pew Research Center, 9 de diciembre de 2020, https://www.pewresearch.org/social-trends/2020/12/09/how-the-coronavirus-outbreak-has-and-hasnt-changed-the-way-americans-work.
2. *COVID-19 Boosts Cloud Service Spending by $1.5 Billion in the Third Quarter* (disponible en inglés), Synergy Research Group, 5 de diciembre de 2020, https://www.srgresearch.com/articles/covid-19-boosts-cloud-service-spending-15-billion-third-quarter.
3. Incidentes de seguridad, definidos como eventos que ocasionaron la infracción de las políticas de seguridad y pusieron los datos confidenciales en riesgo.

Resumen ejecutivo

Con el objetivo de entender el impacto de la COVID-19 en la estrategia de seguridad de las organizaciones en todo el mundo, el equipo de inteligencia sobre amenazas en la nube Unit 42 analizó los datos de cientos de cuentas en la nube entre octubre de 2019 y febrero de 2021 (antes y después del inicio de la pandemia). **Nuestros estudios concluyen que, en el segundo trimestre de 2020 (de abril a junio), los incidentes de seguridad en la nube se incrementaron en nada menos que un 188 %. Descubrimos que, si bien es cierto que las organizaciones fueron capaces de migrar muy rápidamente más cargas de trabajo a la nube en respuesta a la pandemia, muchos meses más tarde tuvieron dificultades a la hora de automatizar la seguridad en la nube y mitigar los riesgos inherentes a estos entornos.** Aunque la infraestructura como código (IaC, por sus siglas en inglés) ofrece a los equipos de DevOps y de seguridad una forma predecible de aplicar las medidas de seguridad, sus inmensas posibilidades todavía están por explotar.

Este informe detalla el alcance del impacto de la COVID-19 en el panorama de las amenazas en la nube y explica qué tipos de riesgos prevalecen en cada sector y región geográfica. También ofrece medidas prácticas que pueden tomar las organizaciones para reducir los riesgos de seguridad asociados a las cargas de trabajo en la nube.

Los sectores esenciales de la lucha contra la COVID-19 sufren un pico de incidentes de seguridad

Al poco de que estallara la pandemia, las organizaciones experimentaron una gran expansión de las implementaciones de cargas de trabajo en la nube; expansión que vino acompañada de un repunte en el número de incidentes de seguridad en la nube. Cabe destacar que **los incidentes de seguridad en la nube en los sectores de venta minorista, fabricación industrial y administraciones públicas aumentaron un 402, 230 y 205 %, respectivamente.** Y no es de extrañar, ya que estos fueron algunos de los sectores que más presión tuvieron por adaptarse y ampliar sus capacidades para afrontar la pandemia: el de venta minorista, para cubrir las necesidades básicas, y el de fabricación industrial y las administraciones públicas, para garantizar los suministros y prestar asistencia frente a la COVID-19.

Los sectores que desempeñan funciones esenciales para combatir la crisis sanitaria tienen dificultades para proteger sus cargas de trabajo en la nube, lo que pone de relieve el peligro de no invertir lo suficiente en seguridad en la nube. Estos picos en los incidentes de seguridad en la nube dejan claro que, por mucho que las empresas puedan aumentar rápidamente sus recursos de teletrabajo gracias a la nube, los controles de seguridad automatizados en torno a los ciclos de DevOps y los de integración y entrega continuas (CI/CD, por sus siglas en inglés), que también son imprescindibles, quedan rezagados.

El *cryptojacking* en la nube va a menos

Mientras la pandemia causaba estragos, criptomonedas como el bitcoin (BTC), el ethereum (ETH) y el monero (XMR) ganaban popularidad y valor de mercado. A pesar de todo, el *cryptojacking* está en declive: entre diciembre de 2020 y febrero de 2021, solo el 17 % de las organizaciones con infraestructura en la nube mostraron signos de esta actividad, en comparación con el 23 % entre julio y septiembre de 2020. **Se trata de la primera caída registrada desde que Unit 42 empezó a hacer un seguimiento de las tendencias en *cryptojacking* en 2018.** Parece que las organizaciones están bloqueando el *cryptojacking* de un modo cada vez más proactivo. Una buena forma de conseguirlo consiste en implementar medidas de protección de cargas de trabajo en tiempo real que frustren la capacidad de los atacantes de ejecutar software de criptominería malicioso en los entornos en la nube de las empresas sin levantar sospechas.

Se siguen exponiendo públicamente datos confidenciales alojados en la nube

Nuestros resultados indican que el 30 % de las organizaciones exponen contenido sensible en Internet, como información de identificación personal (PII, por sus siglas en inglés), de propiedad intelectual y datos médicos y financieros. Cualquiera que conozca o adivine las URL puede acceder a estos datos; datos que, cuando se exponen directamente en Internet, plantean a las organizaciones importantes riesgos asociados con el acceso no autorizado y las infracciones de la normativa. Este grado de exposición sugiere que las organizaciones no terminan de aplicar los controles de acceso adecuados para los cientos de depósitos de almacenamiento de datos que pueden operar en la nube, especialmente cuando dichos depósitos están distribuidos entre distintos proveedores y cuentas.

01

Resultados basados en la evidencia

Principales incidentes de seguridad en la nube durante la pandemia de COVID-19

Los estudios de Unit 42 revelaron que, durante la pandemia de COVID-19, aumentaron los riesgos de seguridad de diversa índole: desde datos en la nube sin cifrar hasta la exposición pública de recursos en la nube o configuraciones no seguras en los puertos. La figura 2 detalla más de una docena de categorías de incidentes de seguridad cuya frecuencia se amplificó notablemente.

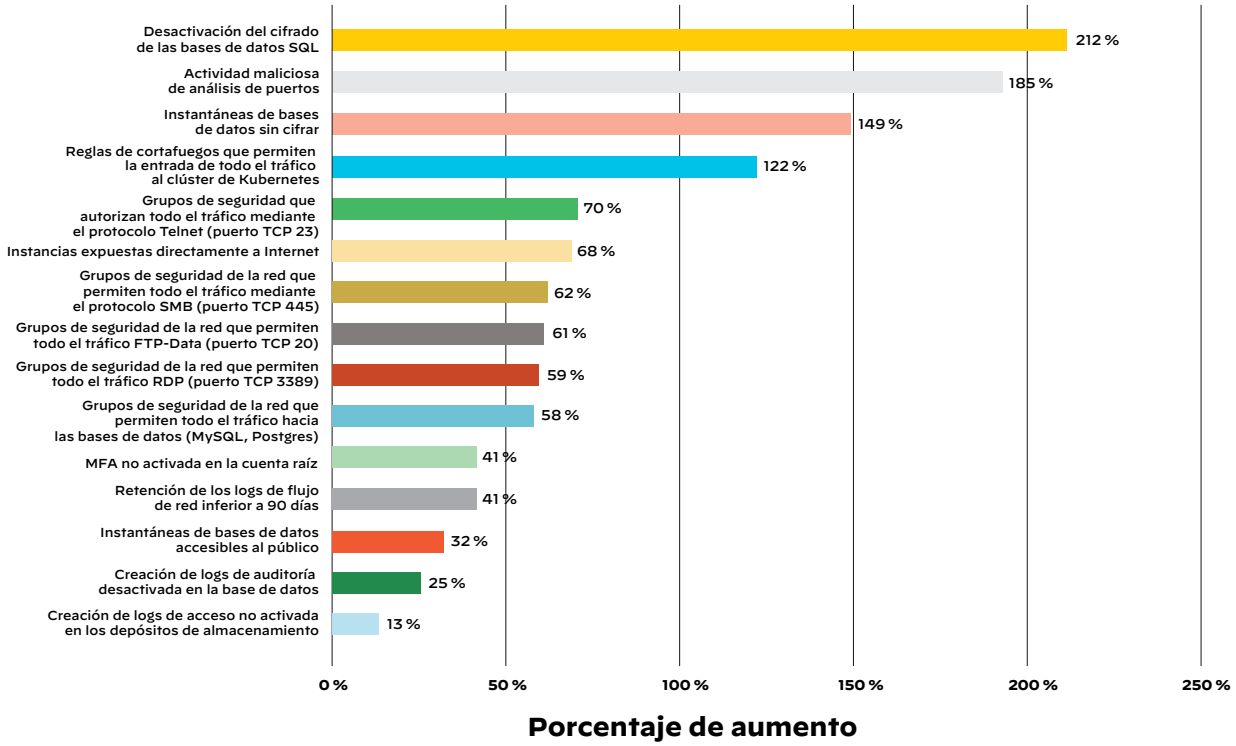


Figura 2: Incidentes de seguridad que más aumentaron durante la pandemia

Tomados como un todo, **estos incidentes reflejan que la mayoría de las organizaciones no han sabido adaptar los recursos de gobernanza de la nube y automatización de la seguridad al incremento de las cargas de trabajo en la nube**. Muchos de estos errores de configuración pueden resolverse con plantillas de infraestructura como código (IaC). Tal y como se abordó en otros informes previos, estas plantillas, siempre y cuando se analicen sistemáticamente para detectar vulnerabilidades habituales en la seguridad, ayudan a proteger la infraestructura en la nube desde el desarrollo hasta la producción.

Por ejemplo, dejar de cifrar las bases de datos SQL y relacionales (p. ej., SQL Database de Microsoft Azure®) —ambas entre los tipos de bases de datos que más han visto crecer la frecuencia de los incidentes de seguridad— es un error fácil de detectar y corregir auditando automáticamente los entornos en la nube para buscar indicios de errores de configuración. Aunque el análisis de puertos no es un tipo de amenaza nuevo, el aumento de su prevalencia conforme ha ido evolucionando la pandemia sugiere que los atacantes se han dedicado activamente a buscar vulnerabilidades originadas por una gobernanza de la nube ineficaz.

Los problemas de falta de gobernanza y automatización de la seguridad no son nuevos. Aunque la frecuencia de las alertas relacionadas con incidentes de seguridad en la nube de diversos tipos ha crecido a lo largo del último año, nuestras conclusiones sobre los tipos de incidentes más prevalentes son bastante similares a las de los informes anteriores.

Esto sugiere que, pese a que el año pasado las organizaciones migraron más cargas de trabajo a la nube, continúan cometiendo errores e imprudencias graves en materia de seguridad. Muchos de estos errores pueden resolverse utilizando bien las plantillas de IaC, herramientas que muchos equipos ya usan, pero sin sacarles el máximo partido. La mayoría de estas plantillas se crean siguiendo un sencillo proceso de tres pasos: diseño, programación e implementación. Lo que está dando problemas a los equipos de DevOps y de seguridad es, en realidad, que estas plantillas no se están sometiendo a revisiones de seguridad automatizadas. En ese sentido, las plantillas de IaC son como el código de las aplicaciones y deben examinarse para identificar problemas de seguridad cada vez que se crean o se actualizan.

Según nuestros estudios, sin embargo, mientras la pandemia se propagaba implacablemente, los equipos o bien no utilizaban plantillas de IaC, o bien no las analizaban en busca de vulnerabilidades de seguridad habituales. De haberlo hecho, no habrían cometido errores como no cifrar datos potencialmente confidenciales o dejar desactivada la creación de logs, una función imprescindible de la supervisión y auditoría de la seguridad en entornos en la nube.

Impacto de la COVID-19 en la seguridad en la nube por región

Si bien el impacto de la pandemia en el crecimiento de la nube se hizo patente en todas las regiones, en algunas fue más acusado que en otras, como se puede observar en la figura 3.

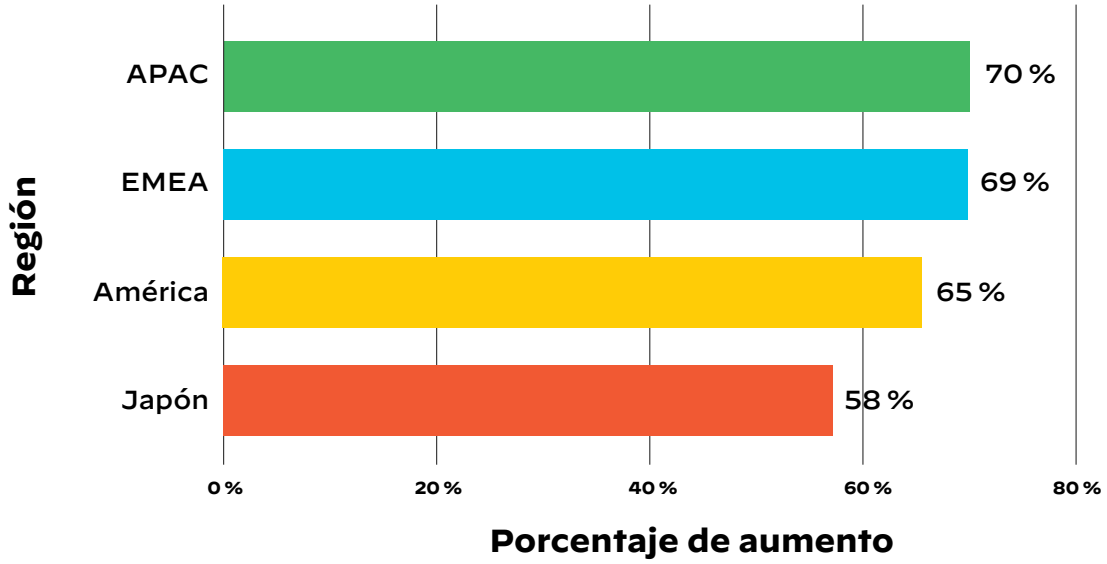


Figura 3: Aumento de las cargas de trabajo en la nube por región

En términos generales, donde más lenta fue la adopción de la nube durante la pandemia de COVID-19 fue en Japón. Como resultado, solo el 32 % de las organizaciones japonesas tenía configuraciones poco seguras que permitían todo el tráfico de la red (TCP y UDP, en cualquier puerto) en al menos una de sus máquinas virtuales (MV) en la nube, y solo el 39 % de ellas expusieron el puerto 22 (SSH) en al menos uno de sus servicios SSH en la nube.

En cambio, en todo el mundo, el 60 % de las organizaciones permitieron la entrada de todo el tráfico de la red en sus plataformas en la nube y el 58 % de ellas expusieron el puerto 22.

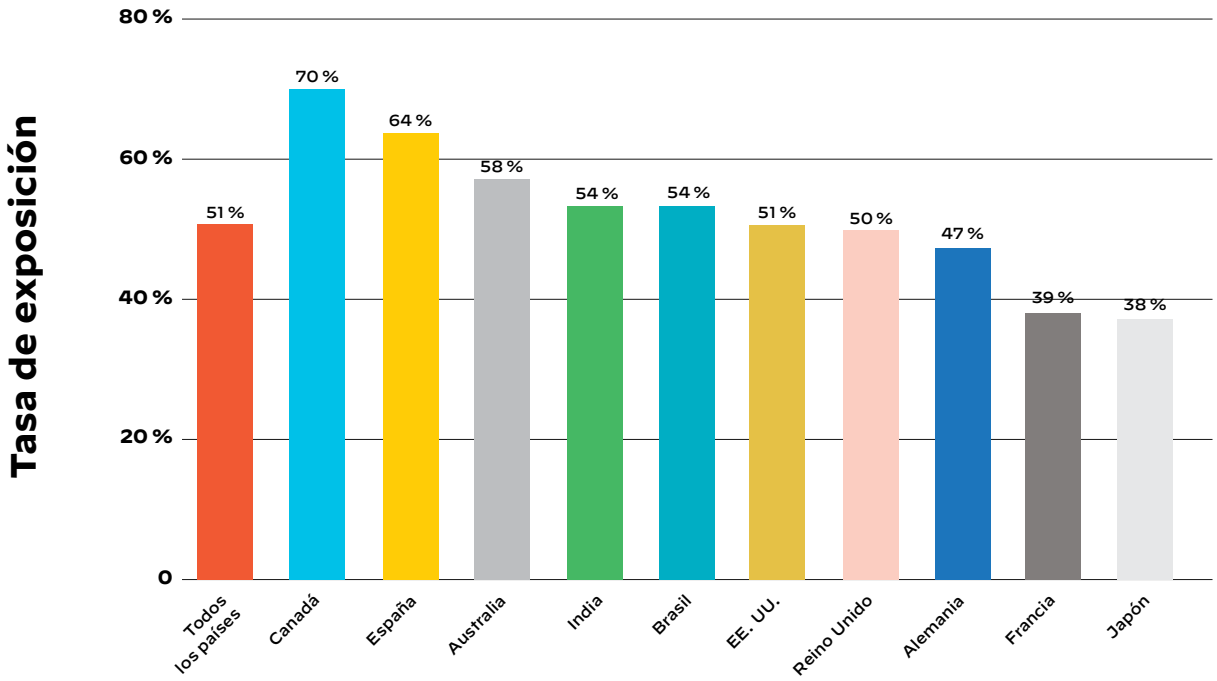


Figura 4: Porcentaje de organizaciones que expusieron su RDP por país

La exposición del protocolo de escritorio remoto (RDP, puerto 3389) de Windows también varió significativamente de una región a otra (véase la figura 4). Dado que el RDP es uno de los vectores de ataque más extendidos, esta exposición no se puede dejar de vigilar. Los atacantes pueden utilizar puertos RDP abiertos para introducirse en la red de una empresa e interrumpir sus operaciones o robar datos confidenciales. En este sentido, fueron las organizaciones canadienses las más golpeadas: un 70 % de ellas expusieron su RDP.

Si se compara el crecimiento de cargas de trabajo por región con la exposición del RDP por país, hay un patrón claro con la COVID-19 como telón de fondo: los investigadores de Unit 42 hallaron una correlación directa entre esta y el incremento de incidentes de seguridad. En todos los principales proveedores de nube, la exposición media del RDP aumentó en un 27 %.

De nuevo, no proteger los puertos cruciales es un error que puede tener consecuencias devastadoras para la empresa. Sin embargo, es posible prevenirlo combinando infraestructura IaC segura con una plataforma de seguridad común que aplique medidas de protección que funcionen de manera ininterrumpida.

Impacto de la COVID-19 en la seguridad en la nube por sector

El volumen de cargas de trabajo en la nube aumentó prácticamente en todos los sectores, siendo el energético la única excepción, debido probablemente a la baja demanda y a los recortes en la producción de petróleo y gas durante la pandemia. Destacan los sectores de la fabricación de productos químicos, de las administraciones públicas y de las ciencias de la vida y farmacéutico, que experimentaron los aumentos más significativos en términos de uso de la nube; una tendencia motivada, probablemente, por el repunte de las operaciones en respuesta a la pandemia.

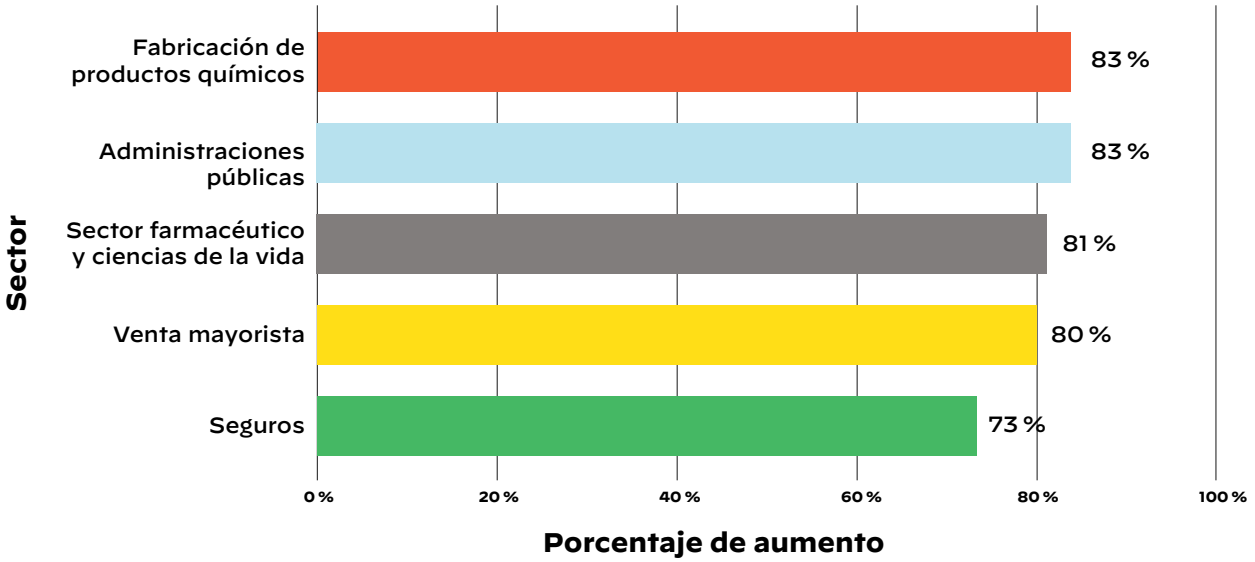


Figura 5: Porcentaje de organizaciones que han visto aumentar sus cargas de trabajo en la nube por sector

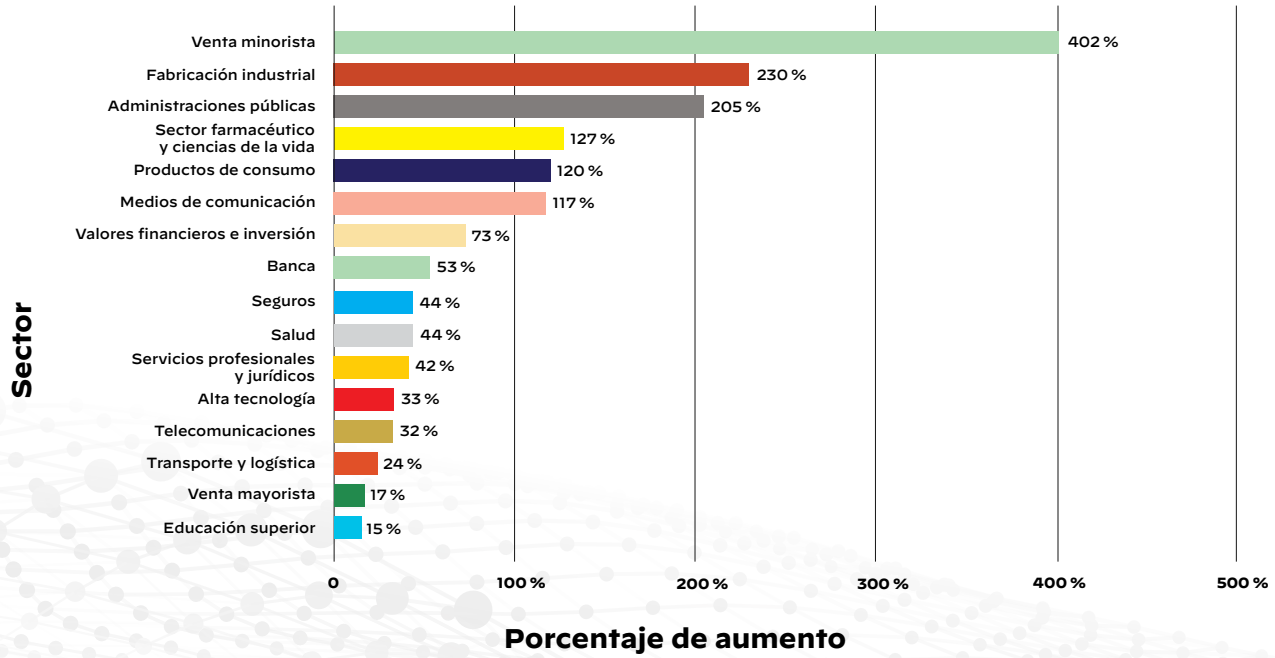


Figura 6: Aumento porcentual de los incidentes de seguridad por sector

Nota: Las cifras no incluyen los sectores cuyas muestras fueron insuficientes.

Nuestros estudios muestran que, cuando las cargas de trabajo en la nube de una organización aumentan súbitamente, el número de incidentes de seguridad se dispara, muchas veces hasta el punto de que los equipos de DevOps y de seguridad se ven sobrepasados. Por ejemplo, entre los sectores de venta minorista, fabricación industrial y administraciones públicas, los incidentes de seguridad en la nube aumentaron un 402, 230 y 205 %, respectivamente. Y no es de extrañar, ya que estos fueron algunos de los sectores que trabajaron bajo presión para adaptarse y ampliar sus capacidades para afrontar la pandemia: el de venta minorista, para cubrir las necesidades básicas, y el de fabricación industrial y las administraciones públicas, para garantizar los suministros y prestar asistencia frente a la COVID-19. Estos incidentes, además de ampliar las superficies de ataque de los entornos en la nube, dificultaron las tareas de auditoría de seguridad e investigación forense.

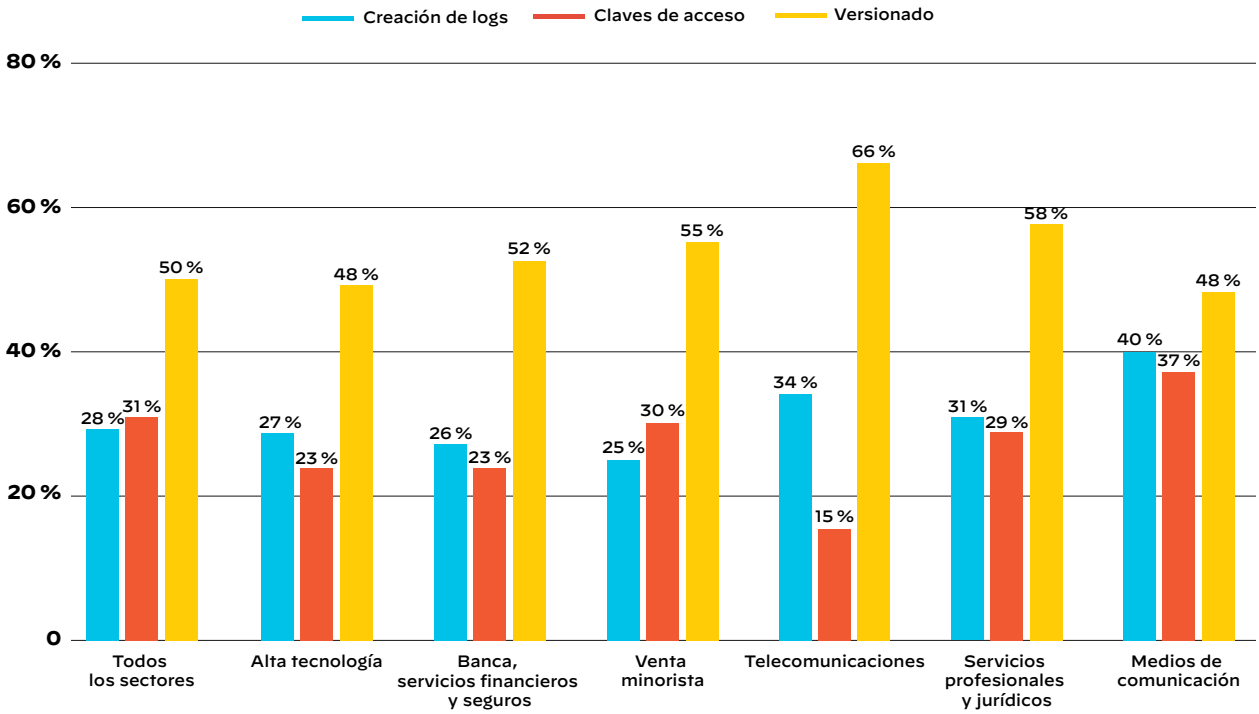


Figura 7: Porcentaje de organizaciones que activan los controles de seguridad clave, por sector

Con todo, hubo diferencias en la forma de gestionar la seguridad de las empresas entre unos sectores y otros (véase la figura 7). Por ejemplo, el 40 % de las organizaciones mediáticas de todo el mundo aplicaron controles de creación de logs de acceso a cada uno de sus contenedores de almacenamiento en la nube. Sin embargo, solo el 25 % de las organizaciones de venta minorista lo hicieron. Aunque, de momento, se desconoce el motivo, los investigadores de Unit 42 hipotetizan que las organizaciones mediáticas tienden a tomarse muy en serio al acceso al contenido, sobre todo teniendo en cuenta las consecuencias del ciberataque sufrido por Sony Pictures en 2014.

El sector de los medios de comunicación fue, asimismo, el que mejor gestionó la rotación de las claves de acceso: un 37 % las cambiaba cada 90 días como máximo, mientras que en las organizaciones de telecomunicaciones solo lo hacían el 15 %. De nuevo, los investigadores de Unit 42 atribuyen esta diferencia a que las organizaciones mediáticas tienden a priorizar la gestión de accesos. Por otro lado, aunque el sector de las telecomunicaciones fue el que mantuvo los segundos mejores controles de creación de logs, obtuvo la puntuación más baja en gestión de claves, lo que indica que el sector prioriza la supervisión por encima del control de accesos.

El control de versiones en los contenedores de almacenamiento en la nube es una medida de seguridad importante, pues identifica si una organización dada es capaz de recuperarse tras un ataque al almacenamiento en la nube o de unos simples errores de corrupción de archivos. En el sector de las telecomunicaciones, el 66 % de las organizaciones implementaron el control de versiones en todos sus contenedores de almacenamiento en la nube, mientras que las de medios de comunicación y alta tecnología fueron las que menos lo hicieron, con solo un 48 %. Para los investigadores de Unit 42, resulta llamativo que los modelos de priorización de la seguridad de los sectores de los medios de comunicación y las telecomunicaciones estén, básicamente, invertidos. Así, aunque ambos parecen conceder importancia a los controles de creación de logs y supervisión, donde el sector de los medios de comunicación favorece la aplicación de políticas de claves de acceso, el de telecomunicaciones se decanta por los controles de versiones. Digamos que el sector de las telecomunicaciones protege los datos con el mismo empeño con el que los medios de comunicación controlan los accesos.

La COVID-19 y la seguridad de los datos

Las empresas están favoreciendo el almacenamiento en la nube debido a su fiabilidad, disponibilidad y escalabilidad. Según nuestros estudios, el 64 % de los datos en la nube contienen información confidencial (p. ej., PII, propiedad intelectual y datos médicos y financieros). De ese 64 %, el 69 % contiene PII y el 34 %, propiedad intelectual (véase la figura 8).

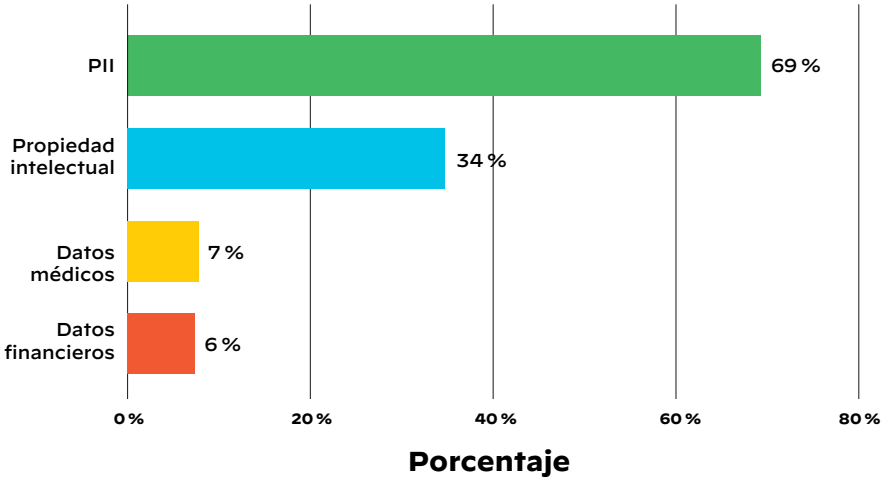


Figura 8: Prevalencia de datos confidenciales almacenados en nubes por tipo

Pese al aumento del volumen de los datos almacenados en la nube, hubo muchas organizaciones que no aplicaron los controles de seguridad adecuados a los suyos. Nuestros estudios indican que, en todo el mundo, el 35 % de las empresas permitieron que sus recursos de almacenamiento en la nube fueran accesibles por Internet. Aunque, en casos muy específicos, esta configuración puede ser necesaria, lo más probable es que se trate de un descuido y que la falta de supervisión y de auditorías de seguridad hiciera que el error pasara inadvertido.

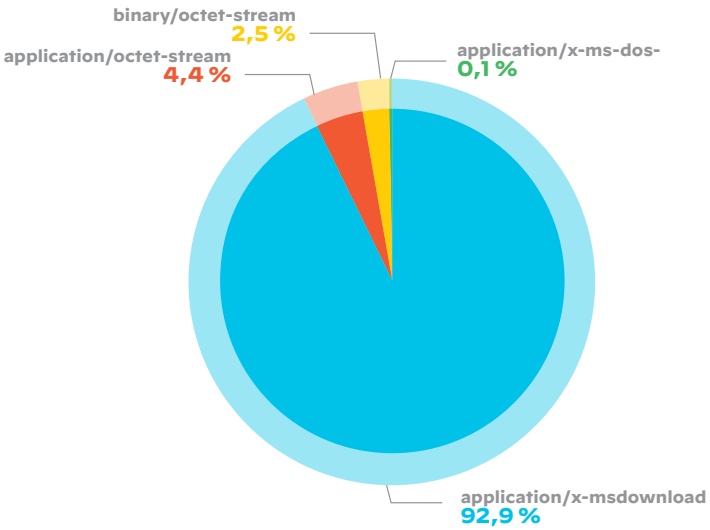


Figura 9: Tipos de malware encontrados en el almacenamiento en la nube

Tener datos accesibles públicamente representa un riesgo particularmente grave para las empresas, pues parece ser que el 30 % de las organizaciones de todo el mundo que tiene datos en la nube de acceso público almacenan datos confidenciales. **Este dato llama mucho la atención, pues cualquiera que conozca las URL adecuadas podría acceder a los datos sin necesidad de contraseña ni ningún otro mecanismo de autenticación**. En los últimos años, ha habido numerosos incidentes en los que los investigadores o atacantes han encontrado datos confidenciales almacenados en la nube que se habían hecho públicos sin querer. Por ejemplo, en distintos entornos de almacenamiento en la nube expuestos al público, los investigadores de vpnMentor encontraron información PII de más de 30 000 individuos, mientras que los de The Register hallaron más de 500 000 archivos confidenciales de miles de clientes.

Además de los datos confidenciales, el almacenamiento en la nube puede contener malware. Los investigadores de Unit 42 constataron que el 92,9 % del malware que contenían los entornos de almacenamiento en la nube estaba formado por archivos ejecutables (.exe) o de biblioteca de enlace dinámico (.dll). Este porcentaje coincide con los resultados de VirusTotal, según los cuales la mayoría del malware está dirigido a los sistemas Windows, con los archivos ejecutables como vehículo de introducción más habitual.

La buena noticia es que encontramos malware en menos del 0,01 % de los datos almacenados en la nube. Para ese 0,01 %, sin embargo, sigue siendo esencial investigar cómo llegó el malware al almacenamiento y quién podría tener acceso a él.

02

La nube, la COVID-19 y las criptomonedas

Aunque las fluctuaciones en el mercado de las criptomonedas y los problemas de seguridad derivados de ellas no se pueden atribuir únicamente a la COVID-19, nuestros estudios revelan conexiones interesantes entre las criptomonedas, la nube y el impacto de la pandemia.

Los investigadores de Unit 42 analizaron datos asociados con el monero (XMR), una criptomoneda muy popular entre los hackers debido a que sus mecanismos de protección del anonimato son muy robustos y a que es muy fácil de extraer en la nube. Los estudios se realizaron entre diciembre de 2020 y febrero de 2021.

Tendencias en la minería de criptomonedas y eventos del mercado

Nuestros resultados indican que las **conexiones a fondos de criptominería de XMR conocidos aumentaron un 65 %** durante este periodo, con picos y valles muy pronunciados en el número total de conexiones.

De particular interés fue el hecho de que tres instancias del número mínimo de conexiones de red tuvieran lugar cuando los precios de mercado eran más altos (véase la figura 10). Esta tendencia podría sugerir que los operadores de criptominería desarrollan el grueso de sus actividades en mercados bajistas y, en cuanto suben los precios, cierran las operaciones para vender las ganancias. También es digna de mención la disminución sostenida que experimentaron las conexiones de red de XMR entre el 24 de diciembre de 2020 y el 3 de enero de 2021, lo que sugiere que hasta las operaciones de criptominería ilícitas necesitan descansar por Navidad.

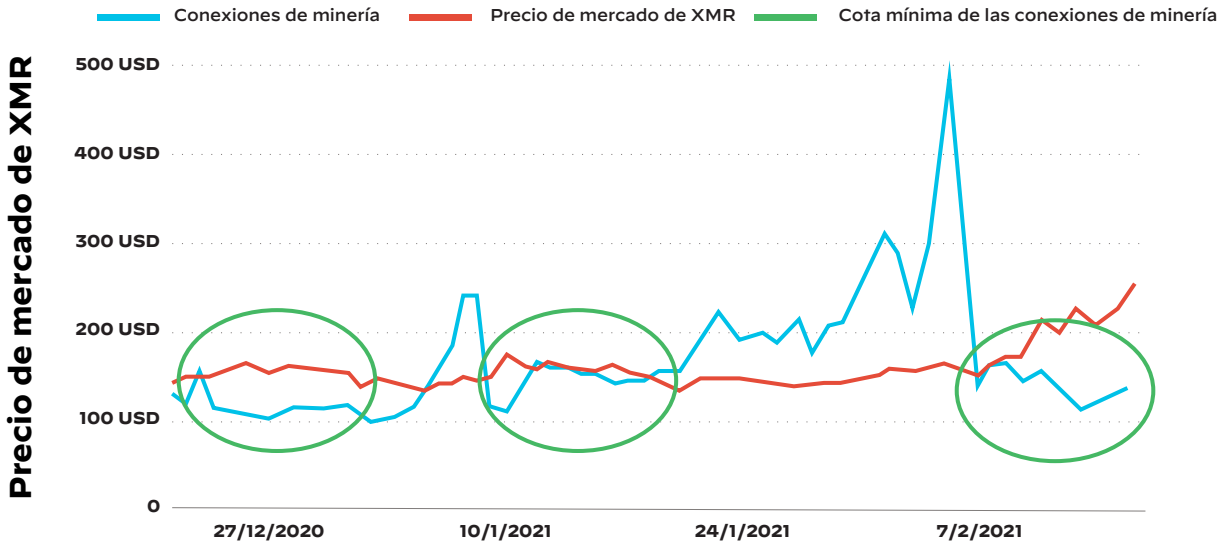


Figura 10: Comparación de las conexiones de criptominería y el precio del XMR

El impacto de la pandemia en las operaciones de minería

Los investigadores de Unit 42 percibieron una correlación clara entre la actividad de minería de XMR y los eventos relacionados con la pandemia. La figura 11 detalla la frecuencia con que los fondos de minería de XMR realizaban conexiones de red y cómo se incrementaban durante fechas clave de la pandemia.

Figura 11: Conexiones a fondos de minería y fechas clave

Aunque la cantidad de datos disponibles no permite extraer conclusiones definitivas, parece plausible que los acontecimientos políticos y sanitarios tengan un efecto claro en las operaciones de criptominería maliciosas, al menos en el caso del XMR.

El declive del *cryptojacking*

Pese al aumento en la actividad de minería, el *cryptojacking* (es decir, el uso no autorizado de una infraestructura para ejecutar operaciones de criptominería) ha disminuido durante la pandemia de COVID-19. Según nuestros estudios, en todo el mundo, el 23 % de las organizaciones que tenían cargas de trabajo en la nube fueron víctimas del *cryptojacking* entre julio y septiembre de 2020, a diferencia de solo el 17 % entre diciembre de 2020 y febrero de 2021. **Se trata de la primera caída registrada desde que en 2018 empezamos a hacer un seguimiento de las actividades de *cryptojacking*.**

Aunque el XMR es la criptomoneda más popular para las operaciones de minería en la nube, hay criptomonedas más extendidas en términos de cuota de mercado. Los investigadores de Unit 42 analizaron las conexiones de red de ethereum (ETH), bitcoin (BTC), litecoin (LTC) y dash. En cada caso, las conexiones de minería de XMR superaban de largo al resto de operaciones de minería de criptomoneda, que entre todas concentraban, de media, el 1 % del total de conexiones de red de XMR (véase la figura 12).

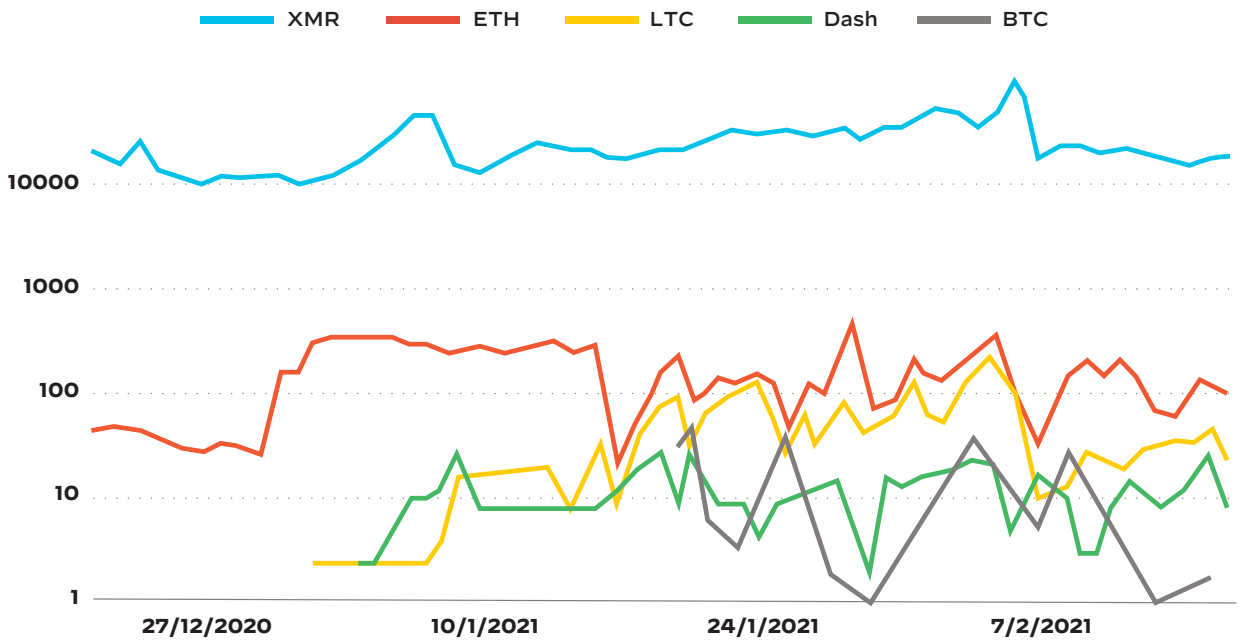


Figura 12: Conexiones de minería por criptomoneda

El ETH, considerado una de las criptomonedas más extendidas, tiene el mayor número de conexiones de red a fondos de minería de criptomoneda (sin contar con el XMR). No es de extrañar, ya que el ETH encabeza con mucha ventaja el mercado de las criptomonedas en términos de funcionalidad. Aunque extraer ETH mediante el uso de procesos basados en la CPU no es muy eficiente, todos los proveedores de servicios en la nube (CSP, por sus siglas en inglés) proporcionan instancias de MV basadas en la unidad de procesamiento gráfico (GPU, por sus siglas en inglés), que son mucho más eficientes que las CPU en criptominería.

Sorprendentemente, se observó que el BTC, el LTC y el dash realizaron conexiones de red a sus propios fondos de minería. Las operaciones de los procesos de minería y de prueba de trabajo para monedas de cadenas de bloques, como el BTC, el LTC y el dash, consumen más memoria y, para ser rentables, requieren un hardware especializado denominado «minero de circuito integrado para aplicaciones específicas» (ASIC, por sus siglas en inglés). Dada su ineficiencia en las operaciones de minería con CPU o GPU basadas en la nube y que su proporción coste-beneficio es negativa, toda conexión de red a estos fondos de minería que se realice desde una infraestructura en la nube empresarial debe considerarse altamente sospechosa.

03

Conclusión y recomendaciones

La principal conclusión que se desprende de nuestros datos no deja margen para la duda: **las organizaciones no han invertido lo suficiente en gestionar la nube ni han automatizado los controles de seguridad necesarios para proteger la migración a la nube de sus cargas de trabajo**. A cambio, han generado riesgos importantes para las empresas, como la exposición de datos confidenciales sin cifrar a Internet y la posibilidad de sufrir brechas por dejar abiertos puertos poco seguros. Aunque los informes sobre amenazas en la nube publicados en 2020 por nuestro equipo Unit 42 ya habían identificado problemas similares, la secuencia de crisis desatadas por la pandemia de COVID-19 ha empeorado y generalizado aún más la situación.

De cara a esta amenaza, las organizaciones deben crear un programa de seguridad en la nube que proteja por igual todas las fases del ciclo de vida de desarrollo del software. Así, además de ganar en el mercado, las organizaciones podrán poner en marcha programas de seguridad en la nube sostenibles capaces de adaptarse a cualquier tipo de contingencia futura.

Áreas de interés estratégico en seguridad en la nube

En materia de seguridad en la nube, los investigadores de Unit 42 recomiendan centrarse en unas áreas estratégicas concretas.

Conocer la situación de la organización y procurarse una visibilidad profunda de la nube

El primer paso para facilitar la seguridad y el cumplimiento normativo en la nube consiste en comprender cómo utilizan la nube hoy sus desarrolladores y equipos. Esto implica saber en todo momento qué está pasando en sus entornos en la nube, incluidas las capas de API y de las cargas de trabajo.

Instalar barreras de protección

Pregúntese qué configuraciones no deberían existir nunca en su entorno, como por ejemplo una base de datos que reciba tráfico directo de Internet. Pese a ser una práctica desaconsejada, nuestros estudios sobre amenazas han demostrado que, a nivel mundial, esta configuración errónea está presente en el 28 % de los entornos en la nube. En teoría, las barreras de protección corrigen este tipo de errores de configuración automáticamente. Si su organización no lo hace ya, sería conveniente que considerara seriamente la opción de utilizar plantillas de IaC para implementar barreras de seguridad mientras realiza la transición hacia una estrategia shift-left. Asegúrese de analizar estas plantillas para que los errores de configuración de la seguridad más habituales no queden sin detectar.

Adoptar y aplicar estándares de seguridad

Es sumamente complicado automatizar lo que está sin estandarizar, y muchos equipos hablan de la automatización sin contar con ningún estándar de seguridad. No empiece desde cero: el Center for Internet Security (CIS) ofrece directrices para las principales plataformas en la nube. Considere la opción de automatizar y codificar estos estándares mediante el uso de infraestructura IaC.

Formar al personal y contratar ingenieros de seguridad que sepan programar

A diferencia de la mayoría de los centros de datos tradicionales, los entornos de nube pública están basados en API. Una gestión adecuada del riesgo en la nube pasa por que los equipos de seguridad sepan utilizar estas API para gestionar la seguridad de las cargas de trabajo a gran escala. Si su equipo de seguridad no cuenta con ingenieros que sepan programar y automatizar los procesos de seguridad del ciclo de CI/CD, las API resultan difíciles de utilizar.

Integrar la seguridad en el equipo de DevOps

Intente responder al quién, qué, cuándo, dónde y cómo envía el código a la nube su organización. Hecho esto, su objetivo debería ser localizar los puntos de inserción menos disruptivos para los procesos y las herramientas de seguridad en su ciclo de CI/CD. En este sentido, es crucial conseguir el apoyo y el compromiso de sus equipos de DevOps cuanto antes. A partir de ahí, procure reducir la interacción humana cada vez más automatizando la mayor cantidad de operaciones posible.

¿Está listo para identificar las amenazas en su nube?

Prisma Cloud analiza más de 10 000 millones de incidentes al mes. Este análisis nos muestra que una configuración deficiente, comportamientos permisivos y la falta de políticas adecuadas conducen a muchas brechas que nos exponen a amenazas no identificadas y a acciones no deseadas de atacantes. Al detectar proactivamente los errores de configuración de seguridad y cumplimiento normativo y activar respuestas de flujo de trabajo automatizadas, Prisma Cloud le ayuda a satisfacer las necesidades de sus cargas de trabajo en la nube dinámicas de forma constante y segura.

Metodología

Todas las conclusiones vertidas en este informe están basadas en datos recopilados entre octubre de 2019 y febrero de 2021. Los estudios se centraron en organizaciones y sectores de todo el mundo, a saber: el continente americano; Europa, Oriente Medio y África (EMEA); y Japón y Asia-Pacífico (JAPAC).

Prisma Cloud de Palo Alto Networks

Los datos de tendencias de Prisma® Cloud utilizan varias fuentes de inteligencia sobre amenazas. El equipo Unit 42 empleó fuentes de datos privadas para recabar datos de alertas y eventos de organizaciones. Estos datos se anonimizaron y, a continuación, se analizaron y compararon con los resultados del informe sobre amenazas en la nube anterior para producir información sobre posibles tendencias.

WildFire de Palo Alto Networks

El servicio de prevención de malware basado en la nube WildFire® adopta un enfoque de varias técnicas único en el que confluyen los análisis dinámico y estático, técnicas innovadoras de aprendizaje automático y un entorno de análisis pionero basado en hardware para detectar y prevenir incluso las amenazas más evasivas.

AutoFocus de Palo Alto Networks

El servicio de inteligencia contextual sobre amenazas AutoFocus™ proporciona la inteligencia, el análisis y el contexto necesarios para entender qué ataques requieren una respuesta inmediata, además de permitir utilizar los indicadores para evitar ataques en el futuro.

Información general

Prisma Cloud

Prisma® Cloud de Palo Alto Networks es una plataforma sin rival en el sector por la cobertura que ofrece. Con ella, se consigue que las aplicaciones, los datos y todas las tecnologías nativas en la nube cuenten con la debida protección y cumplan la normativa, a lo largo de todo el ciclo de vida de desarrollo y en entornos de nube híbrida o de varias nubes.

Unit 42

Unit 42 es el equipo global de inteligencia sobre amenazas de Palo Alto Networks. Nuestros analistas son expertos tanto en la búsqueda y recopilación de las tácticas y técnicas empleadas por las ciberamenazas como en malware de ingeniería inversa, lo que les permite identificar el contexto técnico siempre que sea posible. Unit 42 tiende un puente entre la inteligencia sobre amenazas y los productos de Palo Alto Networks para garantizar que todo su catálogo de seguridad protege a los clientes.

Autores

Jay Chen, investigador de amenazas sénior, Seguridad en la Nube Pública, Palo Alto Networks

Nathaniel «Q» Quist, investigador de amenazas sénior, Seguridad en la Nube Pública, Palo Alto Networks

Matthew Chiodi, vicepresidente y director de Seguridad, Nube Pública, Palo Alto Networks

UNIT 42 BY PALO ALTO NETWORKS

Oval Tower
De Entrée 99 - 197
1101HE Ámsterdam

Tel.: +31 20 888 1883

www.paloaltonetworks.es

© 2021 Palo Alto Networks, Inc. Palo Alto Networks es una marca comercial registrada de Palo Alto Networks. Hay una lista de nuestras marcas comerciales disponible en https://www.paloaltonetworks.com/company/trademarks.html. El resto de las marcas mencionadas en este documento pueden ser marcas comerciales de sus respectivas empresas. Palo Alto Networks no asume ninguna responsabilidad por imprecisiones en este documento ni por la obligación de actualizar la información contenida en él. Palo Alto Networks se reserva el derecho a cambiar, modificar, transferir o revisar de otro modo esta publicación sin previo aviso. unit42_cloud-threat-report-1h-2021_040121-es