Cyber Security Month
October 2021

BDO CIBER INFORME DE INTELIGENCIA SOBRE AMENAZAS - PRIMER SEMESTRE DE 2021

Encuentre su Punto Ciego

BDO

INTRODUCCIÓN

2021 ha sido un año especialmente interesante, ya que viene de la mano de la recuperación parcial del mundo de COVID-19 y, con ella, de medidas parciales de distanciamiento social. Aun así, el mundo está más conectado que nunca, ya que la mano de obra sigue estando alejada en cierta medida, y desafortunadamente, eso significa que la ciberseguridad se ha vuelto cada vez más relevante para prácticamente todo el mundo. Además, tanto las empresas como los gobiernos y los individuos tienden a ver la seguridad de la información de forma retroactiva, donde los problemas se analizan a menudo después de que se producen, y esto presenta un alto riesgo al tiempo que ofrece poco valor para evitar que se repitan.

A pesar de que los campos dentro de las esferas de la seguridad de la información están llenos de una increíble cantidad de datos desorganizados y altamente técnicos, deben ser aprovechados para generar inteligencia de calidad que aumente la conciencia de las probables amenazas, evalúen el riesgo y reevalúen las prioridades y los recursos que aseguran los intereses de una organización.

Dicho esto, nuestro reporte pretende informar a los responsables de la toma de decisiones, que no siempre tienen conocimientos técnicos, con información de nivel C-Suite que respalde las decisiones empresariales cuando se enfrentan a riesgos de ciberseguridad, y permita que los procedimientos preventivos y de mitigación adecuados estén listos cuando sea necesario.

COMPRENSIÓN DE NUESTROS DATOS

El informe presenta un análisis de los incidentes de ciberseguridad confirmados que determinamos dañaron, amenazaron o impactaron negativamente los activos de datos de la organización, directa o indirectamente a través de redes y sistemas más amplios.

Para garantizar la relevancia y la consistencia, distingue deliberadamente entre incidentes e infracciones :

- Los **Incidentes** son definidos como el daño cometido o el intento de daño a la Confidencialidad, Integridad o Acceso de los activos de datos de la organización por una parte no autorizada.
- Las **Infracciones** ocurren cuando la víctima o una parte no autorizada ha confirmado que los activos de datos privados de una organización han sido comprometidos, robados o divulgados sin autorización.

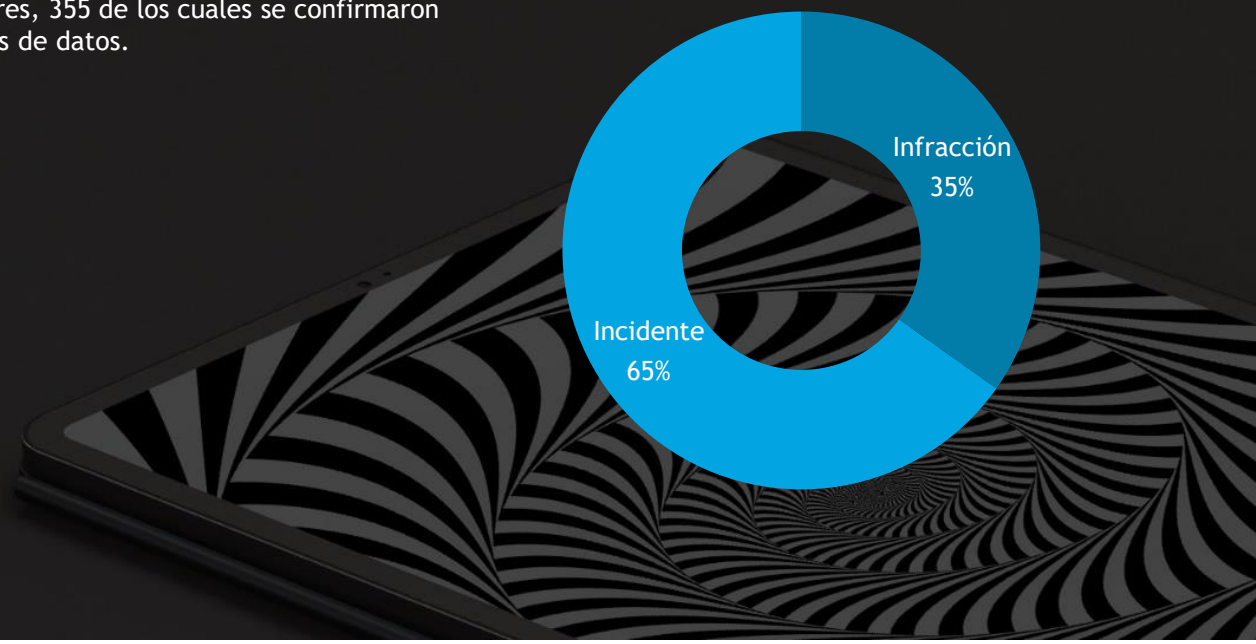
También nos referimos a los actores de la amenaza como grupos, bandas, familias y cepas indistintamente, dado el alto grado de incertidumbre asociado a la atribución en el ámbito cibernético, que como explicaremos más adelante, se ha vuelto complejo por los esquemas de afiliación.

Por último, dado que todos los datos recogidos se hacen públicos, es probable que las cifras reales sean más elevadas, ya que revelar información suele entrar en conflicto con los intereses de la víctima. En este contexto, el informe se refiere a las grandes lagunas de datos típicas de la seguridad de la información como No Definidas (N/D).

RESUMEN EJECUTIVO

Tras recopilar y procesar miles de incidentes notificados públicamente en el primer semestre de 2021, analizamos 1021 incidentes que cumplían nuestros estándares, 355 de los cuales se confirmaron como infracciones de datos.

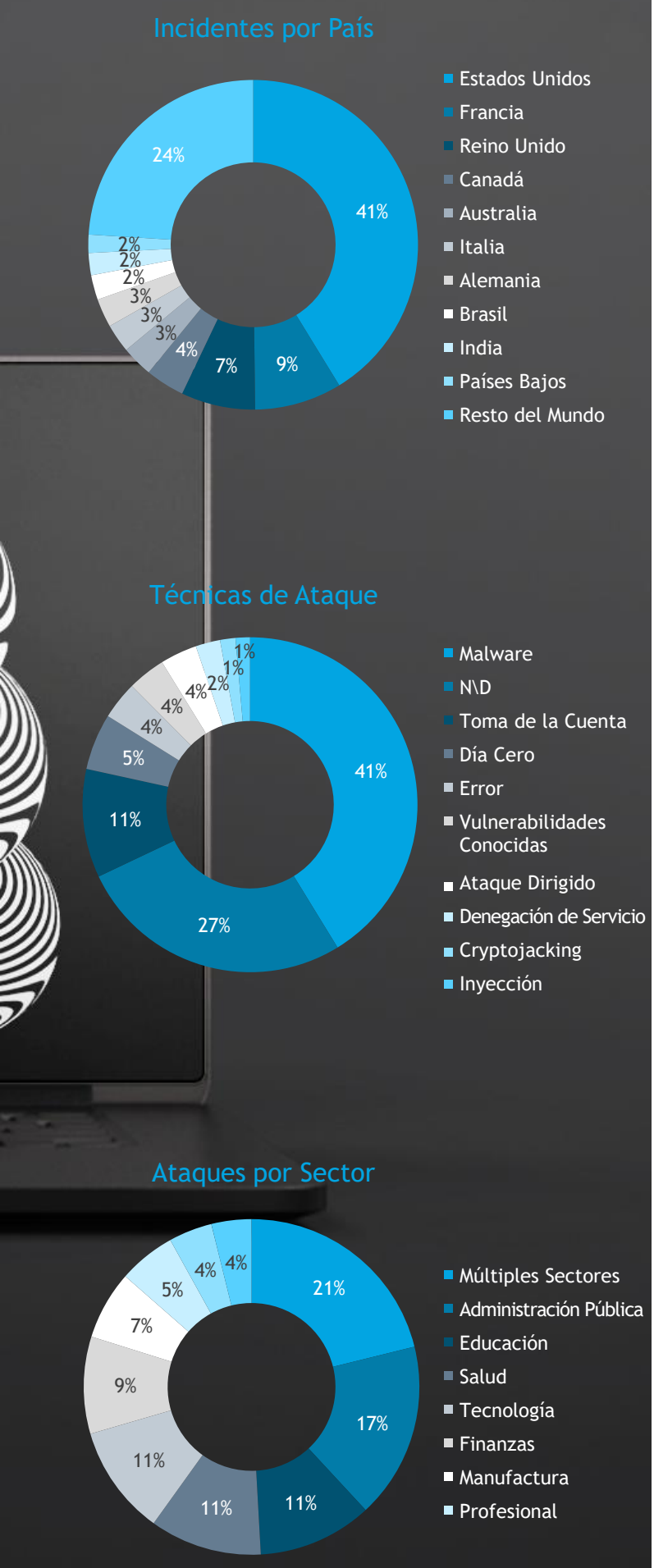
INCIDENTE versus INFRACCIONES



DETERMINACIONES CLAVE

Hemos identificado áreas clave que plantean riesgos considerables que pueden y deben ser gestionados en cierta medida. Las principales conclusiones son:

- El mercado del Ransomware como Servicio (RaaS) crece en escala y tipo y continúa dominando el panorama de las amenazas en general. A pesar de que el monto total del pago de los rescates exigidos en el primer semestre de 2021 es de 306 millones de dólares, los grupos de extorsionistas están más que dispuestos a negociar.
- Las vulnerabilidades de los programas informáticos siguen siendo demasiado frecuentes a pesar de que existen medidas preventivas viables, en concreto, una adecuada Inteligencia sobre Ciberamenazas.
- Los sectores débilmente defendidos, como el de las infraestructuras críticas y el de los servicios esenciales, siguen siendo atacados, ya que se presentan como objetivos muy rentables y de bajo riesgo.
- El elemento humano sigue siendo la mayor vulnerabilidad, ya que los empleados, a todos los niveles, no están suficientemente informados de las amenazas existentes y emergentes.



Lugar

No es de extrañar que Estados Unidos sea el país con la mayor parte de los ataques, con un 41%, mientras que casi todos los países del G7 se encuentran entre los diez primeros (con un 76% de los ataques), excepto Japón, que se queda fuera, en el puesto 11. Si bien es lógico que las principales economías del mundo sigan siendo el objetivo de los actores con motivaciones financieras, también hay que tener en cuenta que estos países también tienen regímenes regulatorios relativamente más fuertes, lo que significa que los datos pueden reflejar divulgaciones de infracciones confirmadas en lugar de incidentes reales.

Principales Técnicas de Ataque

El malware sigue liderando las Técnicas de Ataque utilizadas por los actores de las amenazas, representando el 47% de todos los incidentes, de los cuales el 79% es Ransomware, una táctica que constituyó el 33% de todos los ataques en total. Cabe señalar que existe un alto nivel de complejidad en todos los incidentes, lo que significa que existe un importante solapamiento entre todas las categorías. Por ejemplo, los programas maliciosos se distribuyen a menudo a través de troyanos, otra táctica incluida en la categoría de programas maliciosos. Para simplificar, el informe clasifica las Técnicas y Tácticas como ataques Primarios y Secundarios.

Sectores Primarios

Las industrias múltiples lideran la Distribución Meta con un 21%, seguidas por la Administración Pública con un 17%, y los sectores de Educación, Salud y Tecnología con un 11%. Esto se debe probablemente a que la Administración Pública, la Salud y la Educación carecen de suficientes recursos de ciberseguridad e infraestructura de TI. El aumento de la digitalización y la conectividad a través del 5G hizo que todos los sectores experimentaran problemas de ciberseguridad derivados de los servicios de las API, los dispositivos del IoT y la infraestructura de la nube a través de redes inalámbricas insuficientemente protegidas entre los distintos proveedores.

ADMINISTRACIÓN PÚBLICA

El malware ocupa el primer lugar de los ataques a la Administración Pública, con un 47%, seguido de los Ataques Dirigidos, con un 12%, y de los Ataques de Denegación de Servicio, que ocupan el tercer lugar, con un 5%. Esto tiene sentido si se tiene en cuenta que las entidades locales y federales son una presa fácil para los grupos de Ramsonware, los hacktivistas y los actores de amenazas patrocinados por el Estado.

SALUD

Los datos demuestran que los actores de las amenazas están dispuestos a explotar prácticamente cualquier tipo de organización para obtener beneficios económicos, y esto se ha manifestado en gran medida por la focalización constante en las instituciones de la salud. Mientras que los errores de desconfiguración eran tradicionalmente la principal fuente de filtraciones de datos personales de clientes y pacientes, el 54% de los incidentes conocidos registrados fueron el resultado de Malware, ya que los ciberdelincuentes encuentran en los hospitales y clínicas las víctimas perfectas para la extorsión, mientras que la Toma de Cuentas ocupó el segundo lugar con un 13%. En el primer semestre de 2021, el Departamento de Salud y Servicios Humanos de los Estados Unidos abrió 349 investigaciones sobre violaciones, en comparación con 121 en el primer semestre de 2020, lo que supone un aumento del 180%. [1]

EDUCACIÓN

La educación tuvo un año especialmente difícil, ya que las clases en línea pospandémicas continuaron en 2021 hasta cierto punto. Los actores de la ciberdelincuencia con motivación económica que intentan acceder a los datos y sistemas vieron cómo el Malware también se situaba a la cabeza de este sector con un 49%, seguido de la Toma de Cuentas con un 10% y las Vulnerabilidades de Día Cero con un 7% en el vertical de Educación.

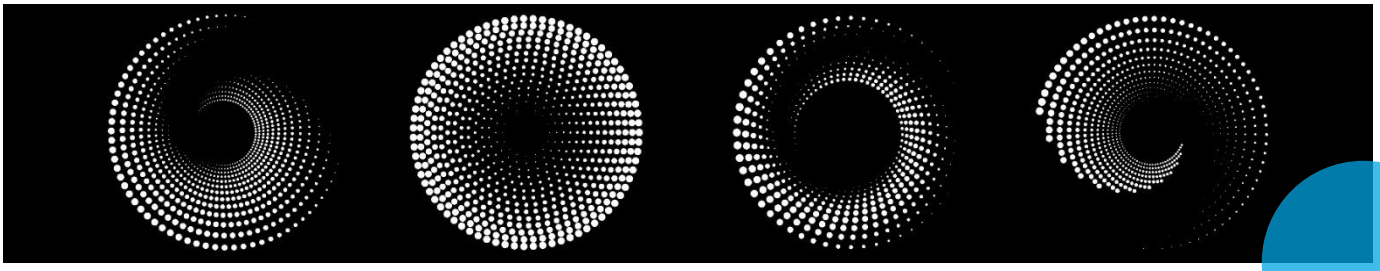
FINANZAS Y SEGUROS

El sector de los Servicios Financieros y de Seguros también experimentó una amplia gama de problemas derivados de la adopción forzosa de tecnologías que presentan cambios significativos para toda la industria. Esto llevó al aumento natural de la cooperación entre las instituciones financieras tradicionales como los bancos y la industria FinTech, y los proveedores de tecnología en general, presentando los desafíos de la cadena de suministro derivados de nuevos socios con los que comparten bases de datos de clientes.

Mientras que el liderazgo del Malware, con un 31%, y la Toma de Cuentas, en segundo lugar, con un 17%, coinciden con otros verticales; la diferencia con este sector fue evidente, ya que las técnicas relacionadas con la Criptomoneda, que representaron un 7%, se impusieron a las más comunes Vulnerabilidades de Software y Errores, en tercer lugar. Esto se debe probablemente a que la banca digital ha experimentado una aceleración de las transferencias en línea durante la pandemia de COVID-19, una tendencia que se prevé que continúe en los próximos años.

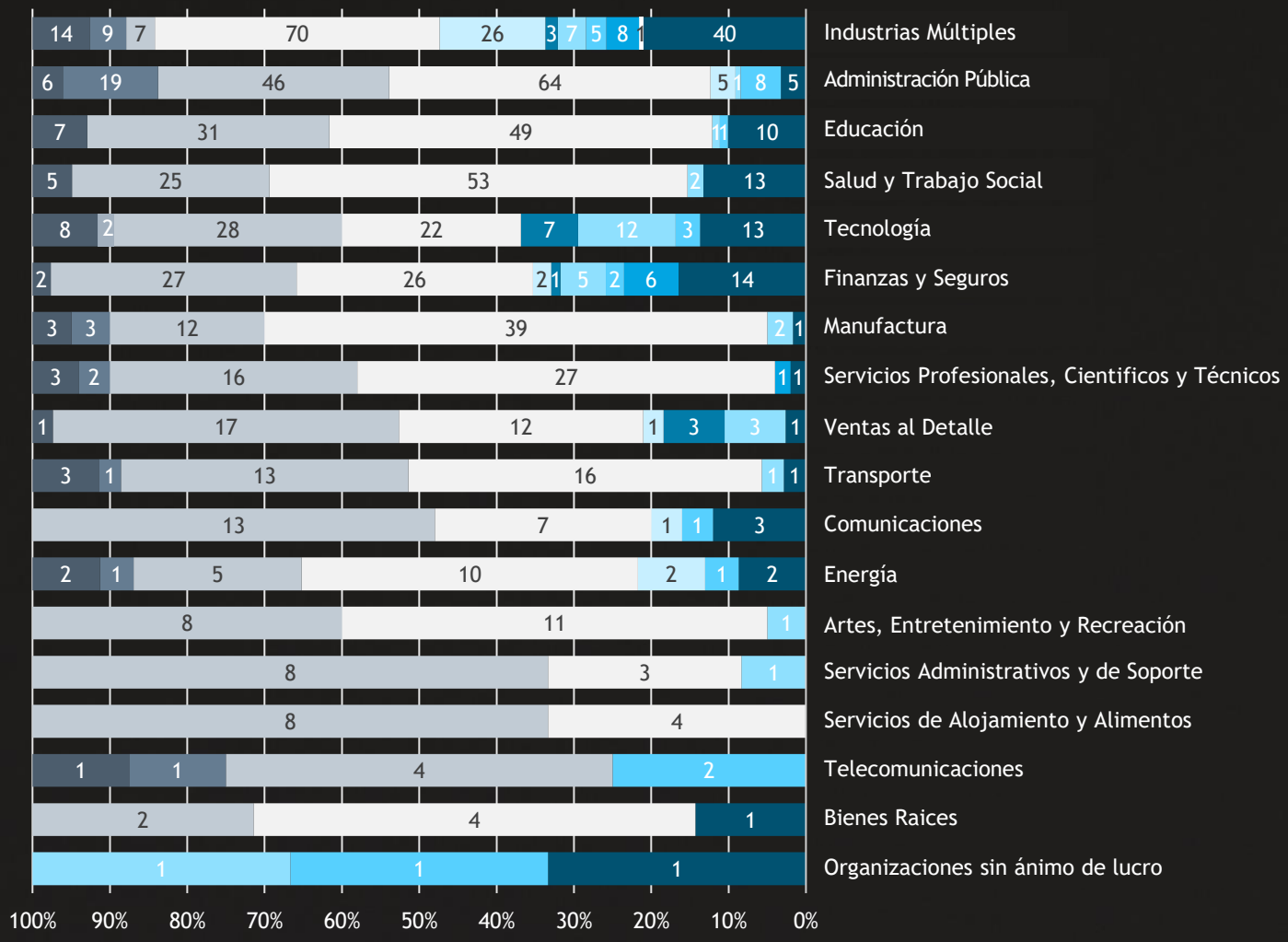
MANUFACTURA

A medida que los avances en la tecnología de la información han conducido inevitablemente a una mayor digitalización en la fabricación, la TI ha facilitado con éxito las mejoras en la tecnología operativa (OT) y los Sistemas de Control Industrial (ICS), lo que ha llevado al crecimiento del Internet Industrial de las Cosas (IOT Dicho esto, los actores de las amenazas trataron de explotar la tensión en la cadena de suministro de la manufactura. Una vez más, el Malware lidera con un asombroso 65% de los ataques, mientras que los Ataques Dirigidos y las Vulnerabilidades de Día Cero ocupan el segundo lugar con un 5%, mientras que el Error y la Toma de Control de Cuentas ocuparon el 3% y el 2% de la distribución de los ataques.



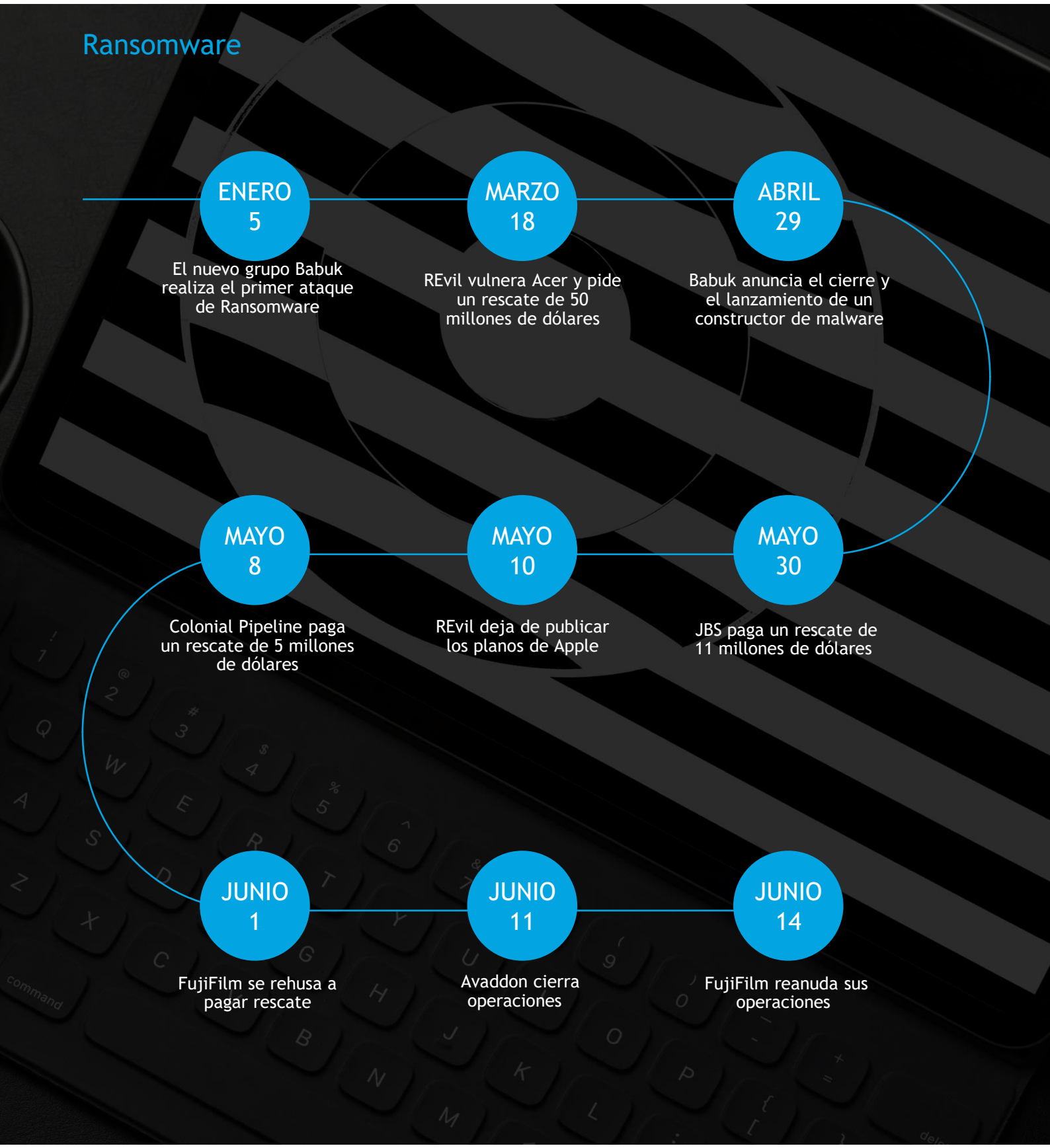
1 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

DESGLOSE POR SECTORES



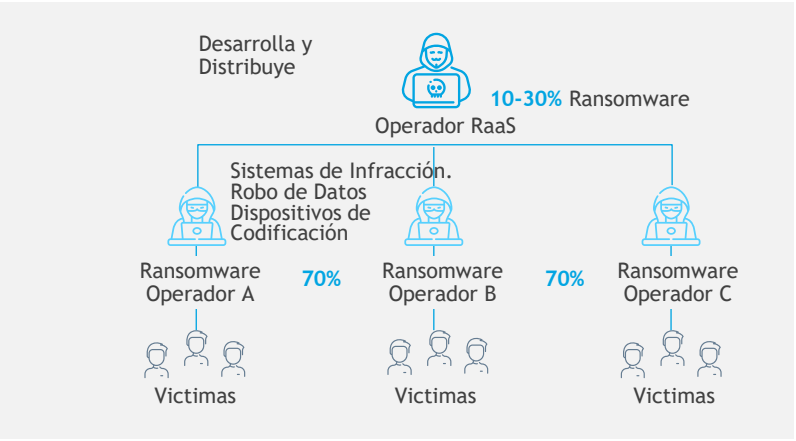
INCIDENTES NOTABLES

Ransomware



EXTORCIONOMÍA

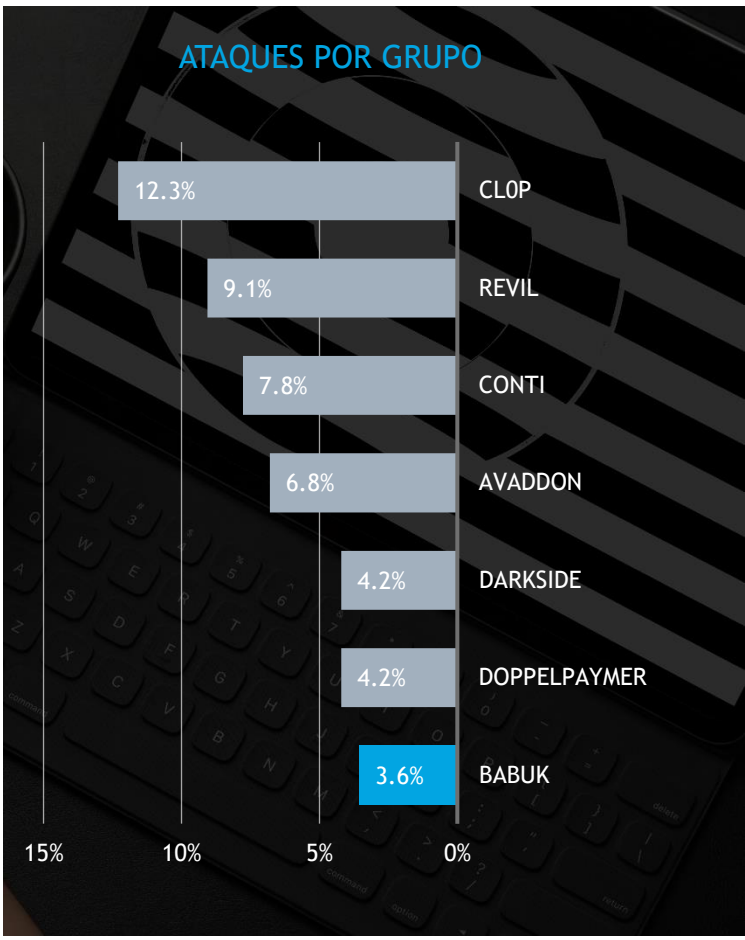
El Ransomware sigue siendo la mayor amenaza para las organizaciones, representando el 33% del total de incidentes, de los cuales aproximadamente el 28% fueron ataques confirmados. Su dominio puede atribuirse probablemente al modelo de negocio del Ransomware como Servicio (RaaS), en el que los operadores desarrollan y distribuyen el Ransomware a los afiliados, que luego realizan el reconocimiento y la ejecución de los ataques. El primero recoge entre el 10% y el 30% de los beneficios, mientras que el segundo se queda con el resto. Esto ha dado lugar a un mercado de RaaS autosuficiente que ha visto una variación de crecimiento particular en los esquemas, y es quizás el resultado de algunos factores clave.



El primero es, sin duda, el creciente uso de los métodos de Doble, Triple y Cuádruple Extorsión. Mientras que los ataques tradicionales de Ransomware consisten en cifrar los datos y obligar a la víctima a pagar para desbloquearlos, en la Doble Extorsión, los operadores de Ransomware también cifran y amenazan con liberar datos sensibles para coaccionar a las víctimas a pagar. La Triple/Cuádruple Extorsión se produce cuando los grupos van más allá amenazando a las víctimas con ataques de denegación de servicio distribuido (DDoS) contra sus sistemas, y/o hacen que sus clientes y socios participen en el pago de los rescates directamente.

El crecimiento de los esquemas RaaS también puede estar estrechamente relacionado con los avances en la criptomoneda, que tranquiliza a los aspirantes a ciberdelincuentes con el anonimato. Por último, el aumento en 2021 posiblemente se produjo después de que muchos foros destacados de ciberdelincuencia prohibieran los temas relacionados con el Ramsonware después de que esta práctica recibiera una atención considerable por parte de las autoridades, lo que obligó a los operadores de Ramsonware a promocionar sus servicios a través de métodos alternativos.

CADENA - "NEW KIDS ON THE BLOCK"



La primera operación de Ramsonware en 2021 fue registrada por varios investigadores de seguridad que identificaron el nuevo Ramsonware Babuk después de que afectara al menos a cinco empresas a mediados de enero. Tras sólo unos meses de actividad, el grupo Babuk publicó su intención de abandonar el negocio de la extorsión en su sitio de filtraciones, afirmando haber logrado su objetivo. A diferencia de otros grupos que publican sus claves de descifrado después de cerrar, Babuk declaró que en su lugar publicaría el código fuente de su malware de cifrado de archivos. A finales de junio, el constructor Babuk Locker se filtró en Internet y se utilizó para atacar múltiples objetivos en varios sectores de todo el mundo, lo que situó al grupo en el séptimo lugar en cuanto a ataques totales durante el primer semestre de 2021.

La entrada y salida de Babuk en el espacio de cuatro meses, y su posterior regreso sólo dos meses después de retirarse, representa un patrón común entre las familias de Ramsonware, que curiosamente se asemeja a los comportamientos económicos de las empresas normales que entran en mercados muy rentables.

ENTRADA EN EL MERCADO, ESTRATEGIAS DE SALIDA

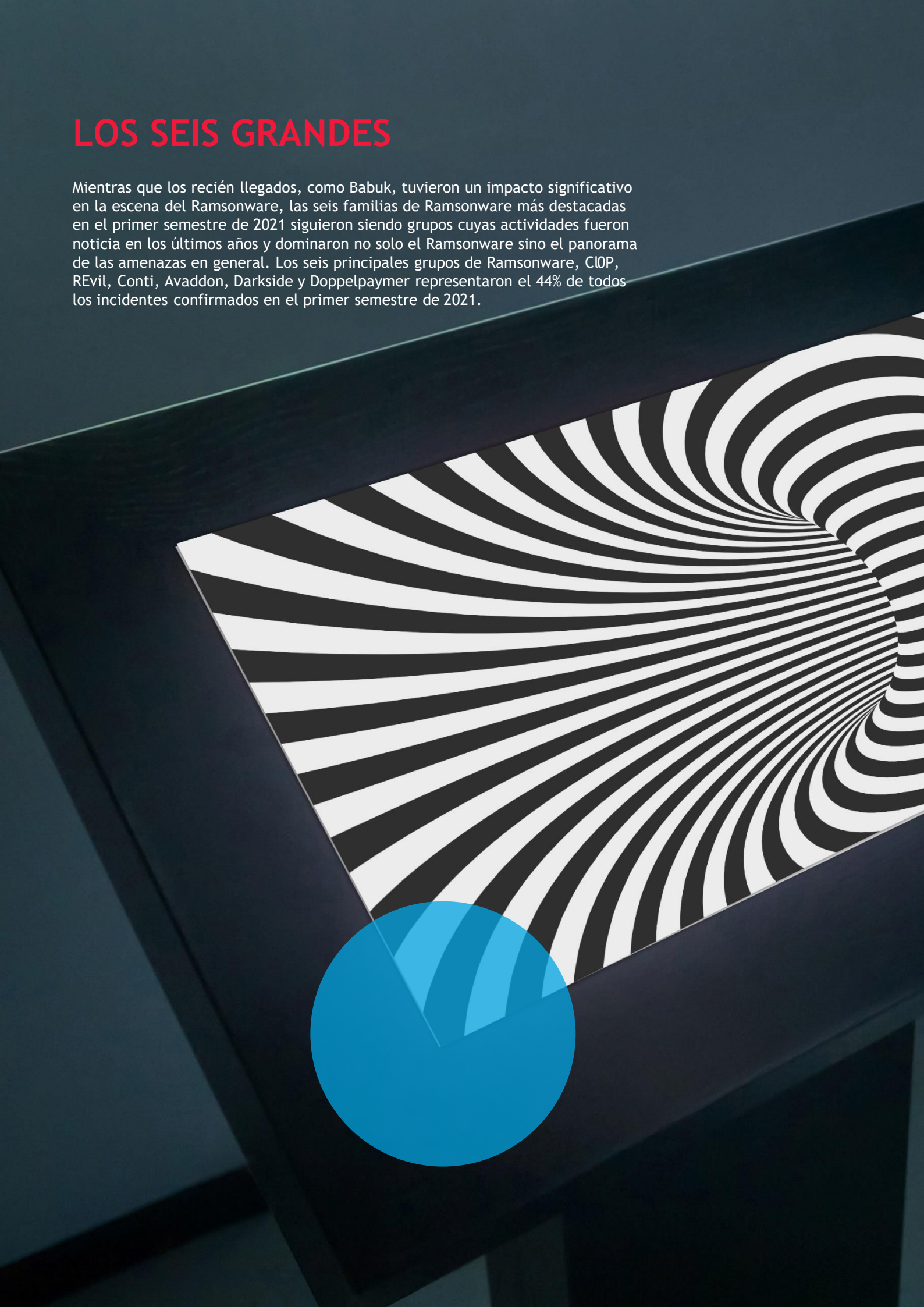
Fuente: Equipo de MalwareHunter

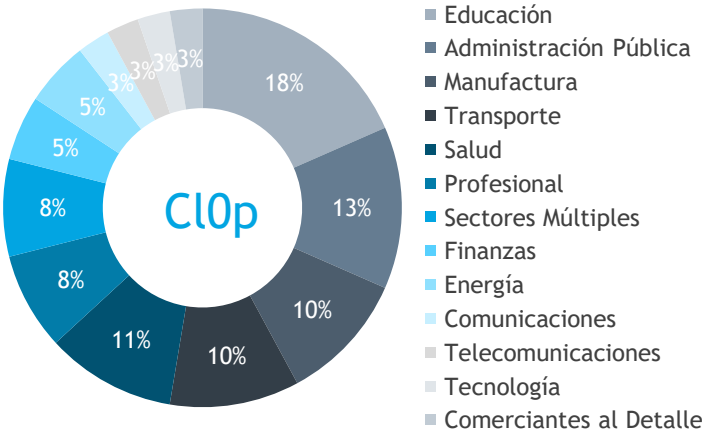
Si bien es probable que varios grupos de Ramsonware de alto perfil estén pasando desapercibidos o sean arrestados, los nuevos grupos ya han comenzado a llenar el vacío. Esto se debe probablemente a que muchos de los grupos más antiguos han decidido reiniciar o cambiar de marca sus operaciones reclutando nuevos afiliados. El aumento de la sindicación entre ciberdelincuentes experimentados y aficionados es el resultado de la creciente demanda de variantes de RaaS que se venden en la web oscura y que son suministradas por grupos que cierran tras llamar la atención de las autoridades.[2] En este contexto, los ataques de Ramsonware han aumentado considerablemente tanto en frecuencia como en tamaño, ya que las variantes pueden adquirirse fácilmente por una cuota de afiliación tan baja como $100. Dicho esto, el Ramsonware sigue siendo un negocio demasiado rentable como para abandonarlo. Cuando Babuk regresó, distribuyó el riesgo filtrando su constructor, al tiempo que ampliaba su sector operando una nueva plataforma de filtración que ofrecía nuevos esquemas de afiliación para los actores que creaban sus propias cepas de Babuk para unirse, incluyendo la opción de iniciar sus propias operaciones de RaaS.[3] Además, sólo lanzaron una versión antigua de su malware y crearon una nueva para volver a las operaciones de extorsión centrándose en las redes corporativas, afirmando supuestamente que los recientes ataques a objetivos más pequeños utilizando su constructor más antiguo no fueron realizados por ellos.[4]

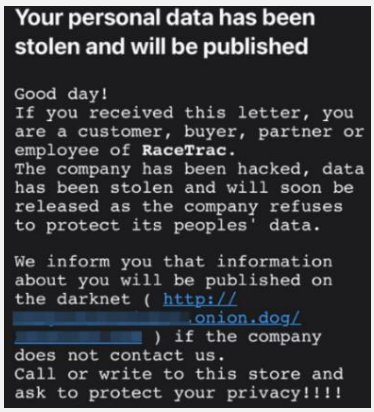
2 https://www.virsec.com/blog/were-it-not-illegal-ransomware-as-a-service-raas-would-be-a-practically-perfect-business-model
Figure 1 - https://www.digitalshadows.com/uploads/2021/05/ransomware-operator.jpg
3 https://securityaffairs.co/wordpress/119467/cyber-crime/babuk-locker-ransomware-builder.html?utm_source=rss&utm_medium=rss&utm_campaign=babuk-locker-ransomware-builder
https://www.technadu.com/builder-babuk-locker-ransomware-leaked-online/286444/
4 https://www.bleepingcomputer.com/news/security/babuk-ransomware-is-back-uses-new-version-on-corporate-networks/

LOS SEIS GRANDES

Mientras que los recién llegados, como Babuk, tuvieron un impacto significativo en la escena del Ramsonware, las seis familias de Ramsonware más destacadas en el primer semestre de 2021 siguieron siendo grupos cuyas actividades fueron noticia en los últimos años y dominaron no solo el Ramsonware sino el panorama de las amenazas en general. Los seis principales grupos de Ramsonware, CLOP, REvil, Conti, Avaddon, Darkside y Doppelpaymer representaron el 44% de todos los incidentes confirmados en el primer semestre de 2021.



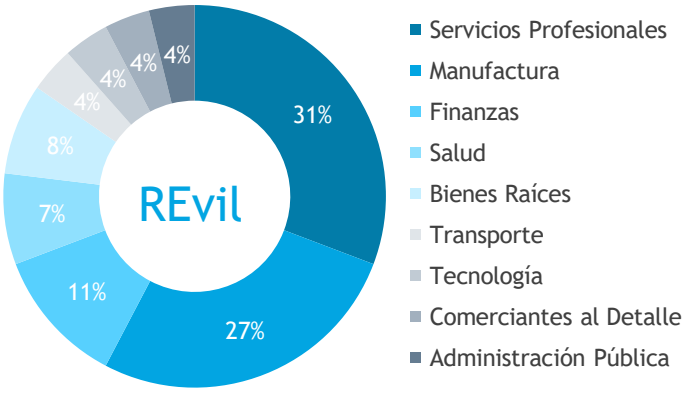




Fuente: KrebsOnSecurity

La mayoría de las víctimas de Clop en el primer semestre de 2021 fueron el resultado del ataque a la cadena de suministro en los servidores de la Aplicación de Transferencia de Archivos (FTA) de Accellion, que eran utilizados por múltiples organizaciones en todo el mundo. No está claro si Cl0p hackeó los servidores de Accellion o si otros grupos le dieron acceso a los datos. En cualquier caso, Clop logró obtener los datos de múltiples objetivos de alto perfil, como el gigante petrolero Royal Shell, la empresa de nube y cumplimiento Qualys, los bancos estadounidenses Morgan Stanley y Flagstar, el bufete de abogados internacional Jones Day, la multinacional canadiense fabricante de aviones Bombardier y cientos de otras organizaciones.

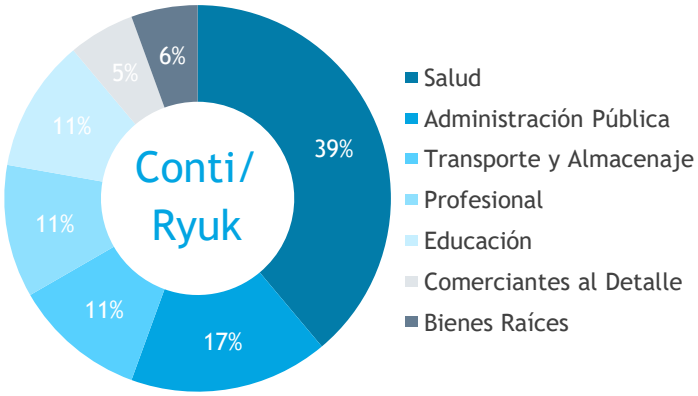
Nuestros datos muestran que Cl0p se dirigió más al sector de la Educación, que representó el 18% de sus víctimas, seguido por la Administración Pública y el Transporte, con un 10% cada uno, mientras que la Salud, los Servicios Profesionales, las Industrias Múltiples y la Manufactura representaron el 8% de la distribución de los ataques. Las actividades de Cl0p fueron especialmente notables debido a su triple táctica de extorsión, que consistía en ponerse en contacto con los clientes y socios de la víctima a través de la información de contacto obtenida de los datos robados, con el fin de animarles a presionar a la empresa víctima para que pagara el rescate o, de lo contrario, se filtrarían sus datos personales.



También conocido como Sodin/Sodinokibi, el grupo de caza mayor Ramsonware es quizás el más notorio de todos dado el número de empresas lucrativas de alto perfil en su lista de víctimas. A finales de 2020, REvil afirmó que había ganado más de 100 millones de dólares en un año utilizando el modelo RaaS, y que su objetivo es ganar al menos 2.000 millones de dólares.[5] Un tercio de los objetivos de REvil se encontraban en los sectores de Servicios Profesionales, Científicos y Técnicos, así como en el de Manufactura, mientras que Finanzas, Bienes Raíces y Educación representaron aproximadamente una décima parte cada uno..

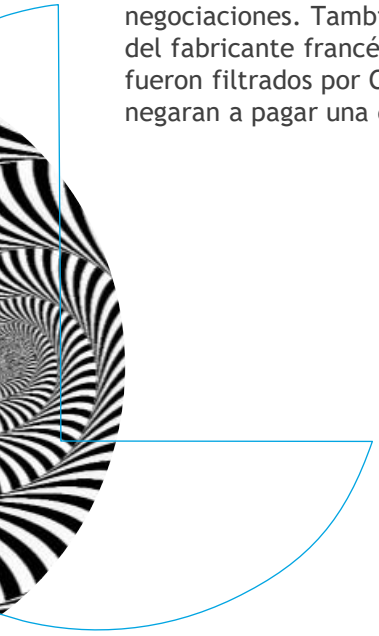
Entre las operaciones de REvil más destacadas registradas este año se encuentran los ataques al gigante de la informática y la electrónica Acer, el 18 de marzo, por el que se pidió un rescate de 50 millones de dólares, el más alto jamás registrado. El 20 de abril, el grupo saltó a los titulares al atacar a Quanta Computer, el fabricante de computadoras portátiles de Apple, exigiendo al parecer también 50 millones de dólares. Después de que Quanta se negara a negociar, REvil exigió a Apple que pagara el rescate o, de lo contrario, filtraría detalles técnicos del hardware actual y futuro, publicando los planos de las computadoras portátiles cada día que no se pagara el rescate. El 10 de mayo, todos los datos relacionados con el incidente de Quanta fueron retirados repentinamente del sitio de la darknet del grupo. A pesar de que Apple no ha hecho ningún comentario sobre la filtración, dado el historial de REvil de cumplir sus amenazas, muchos expertos han especulado que los datos robados fueron retirados después de que se acordara discretamente alguna forma de pago entre ambas partes. La capacidad del grupo para obtener importantes rescates se confirmó el 30 de mayo, cuando atacó los sistemas informáticos del mayor procesador de carne del mundo, JBS SA, cerrando sus operaciones en Estados Unidos y Australia. Al parecer, REvil exigió un rescate de 22,5 millones de dólares, y el 9 de junio JBS confirmó que había pagado 11 millones de dólares.[6]

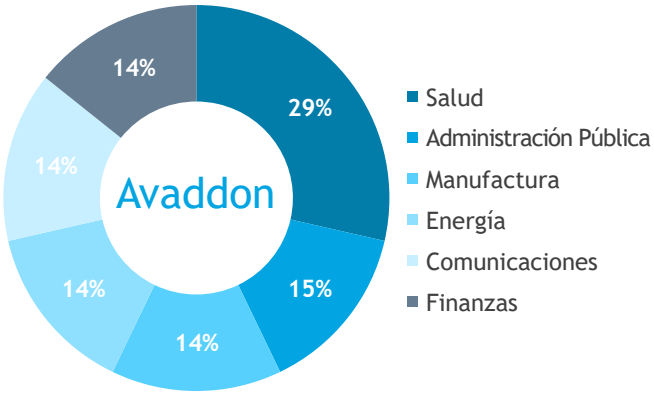
5 https://www.bleepingcomputer.com/news/security/fbi-revil-cybergang-behind-the-jbs-ransomware-attack/
6 https://www.bleepingcomputer.com/news/security/jbs-paid-11-million-to-revil-ransomware-225m-first-demanded/



La familia de Ramsonware Conti/Ryuk tiene un historial centrado en salud y administración pública.[7] Esta tendencia se mantuvo en 2021, y la salud humana representó el 39% de sus objetivos. A finales de mayo, el FBI identificó al menos 16 intentos de ataques de Ramsonware Conti dirigidos a redes de atención sanitaria y de primeros auxilios de Estados Unidos, entre las que se encontraban agencias policiales, servicios médicos de emergencia, centros de despacho 9-1-1 y municipios, desde principios de año. La Administración Pública ocupó el segundo lugar, con un 17% del total de incidentes, más de la mitad de los cuales estaban dirigidos a organizaciones con más de 1.000 empleados.

Aunque la mayoría de sus víctimas no se han hecho públicas, entre los ataques confirmados se encuentra la empresa británica de venta de ropa Fat Face, que recibió una petición de rescate de 2 millones de dólares tras ser atacada el 17 de enero. Más concretamente, el 2 de marzo, el distrito escolar del condado de Broward recibió una petición de rescate de 40 millones de dólares, que se redujo a 10 millones después de que el distrito escolar no ofreciera más de 500 mil dólares, lo que provocó la filtración de los datos tras el fracaso de las negociaciones. También se confirmó que los datos del fabricante francés de vasos de papel CEE Schisler fueron filtrados por Conti después de que también se negaran a pagar una demanda exorbitante.





Avaddon es otro grupo conocido por su proclividad a atacar a organizaciones de salud; nuestros datos muestran que un tercio de todos sus objetivos pertenecían de hecho al sector sanitario. Este es un hecho especialmente preocupante dado que el grupo y sus afiliados también son conocidos por amenazar a las víctimas que no pagan con ataques DDoS, otro ejemplo de triple extorsión, que en el sector de la salud puede ser literalmente mortal. Administración Pública, Manufactura, Energía, Comunicaciones y Finanzas representaron aproximadamente una proporción igual de la lista de objetivos restantes.

Curiosamente, el 11 de junio, después de decidir el cierre de sus operaciones, Avaddon compartió las claves de descifrado de sus víctimas con el medio de comunicación BleepingComputer, que a pesar de decidir no nombrar a los objetivos corporativos previamente desconocidos, sí proporcionó información valiosa después de que los investigadores de seguridad analizaran los identificadores únicos adjuntos a las claves liberadas.

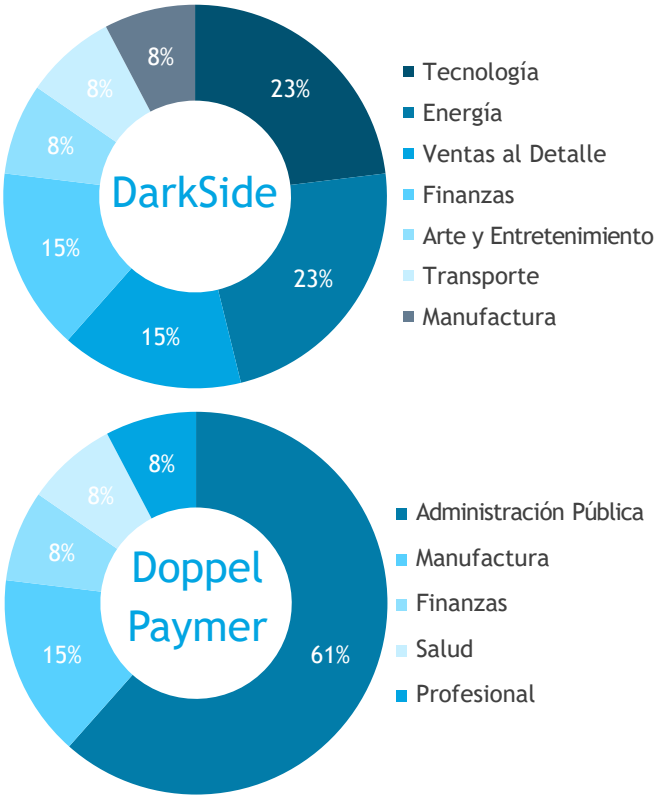
No es de extrañar que el total de víctimas de Avaddon a lo largo de los años residiera principalmente en Estados Unidos, seguido de Canadá. Los tres principales sectores atacados en los últimos años son Ventas al Detalle, con un 12,5%, Manufactura, con un 12,2%, y Finanzas, con un 7,5%. Lo más interesante es que más del 50% de las víctimas de Avaddon tenían ingresos inferiores a 10 millones de dólares, mientras que el grupo utilizaba una regla "5x5" para formular sus demandas de rescate. Avaddon calculaba el 5% de los ingresos anuales, estimados como una quinta parte de los ingresos totales, para iniciar las negociaciones antes de bajar el precio del rescate durante éstas. Por ejemplo, si una empresa víctima obtuvo unos ingresos totales de 10 millones de dólares, los ingresos anuales se calcularían en 2 millones de dólares, y el precio inicial del rescate será de 100 mil dólares. Avaddon bajaría el precio durante las negociaciones, y el rescate final sería probablemente de unos 70.000 dólares. Utilizando esta información, los investigadores de seguridad habrían calculado que las ganancias totales de Avaddon eran de algo menos de 90 millones de dólares.

7 https://us-cert.cisa.gov/ncas/alerts/aa20-302a

Aunque DarkSide es un grupo de Ramsonware relativamente nuevo que surgió en 2020, varios expertos en seguridad creen que es una rama o una antigua afiliada de REvil, dadas las similitudes de su malware y sus prácticas de caza mayor. Los sectores de la Tecnología y la Energía son los más afectados, ya que ambos representan aproximadamente una cuarta parte de los objetivos de DarkSide, mientras que los sectores de Comerciantes al Detalle y Servicios Financieros representan un 15% cada uno, y los sectores de Artes, Transportes y Manufactura un 8% de las víctimas de DarkSide.

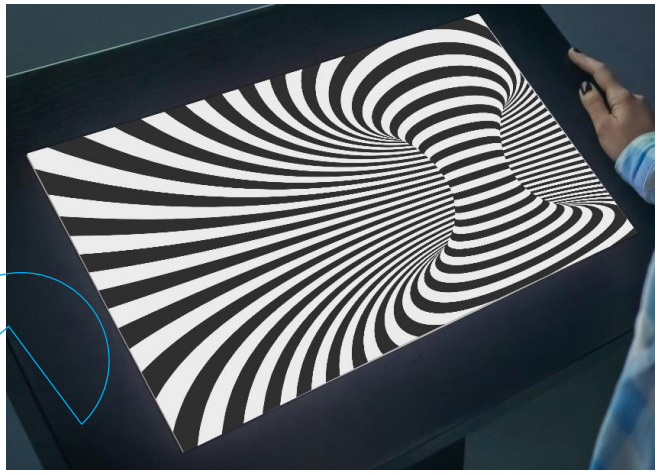
Al igual que REvil, el grupo ha demostrado su capacidad para obtener grandes pagos de rescate. El 24 de abril, el grupo cerró las operaciones en Estados Unidos de Brenntag AG, el segundo mayor distribuidor de productos químicos de Norteamérica, que confirmó haber pagado un rescate de 4,4 millones de dólares. Sin embargo, DarkSide se hizo notoriamente famoso el 7 de mayo, después de atacar a la Colonial Pipeline Company, que opera un importante sistema de transporte de combustible en toda la costa este de los Estados Unidos, deteniendo todas las operaciones de los oleoductos. DarkSide exigió entre 4,4 y 5 millones de dólares, que los operadores de Colonial Pipeline pagaron.[8] A pesar de que las autoridades estadounidenses recuperaron más tarde casi la mitad de los 75 bitcoins utilizados para pagar el rescate, Colonial habría perdido millones en ingresos por el cierre del 45% del combustible que suministra a lo largo de 5.500 millas (8851 km) en toda la costa este, durante cinco días.

Aunque algunos informes afirman que los operadores de Ramsonware no estaban al tanto de los ataques de Colonial y que los llevó a cabo un afiliado, este es un punto en gran medida discutible dado que RaaS prolifera importantes capacidades de interrupción a múltiples actores. Además, el ataque, de gran repercusión, atrajo la atención no sólo de las fuerzas del orden, sino también del gobierno federal de Estados Unidos, lo que provocó la interrupción de las actividades recientes del grupo, lo que se espera que facilite otro patrón de cambio de marca de Ramsonware. Además, llevó la cuestión del Ramsonware a la esfera geopolítica, culminando con una declaración conjunta del G7 al gobierno ruso por su falta de aplicación de la ley contra los grupos de Ramsonware de habla rusa en junio, y una cumbre entre el presidente estadounidense Joe Biden y su homólogo ruso Vladimir Putin días después.



En diciembre de 2020, el FBI emitió una Notificación de la Industria Privada (PIN) en relación con el aumento de los ataques de DoppelPaymer Ransomware en Infraestructuras Críticas e industrias de todo el mundo, incluyendo entre las víctimas del grupo una cantidad desproporcionada de instituciones y organizaciones gubernamentales.[9]

Muchas de las entidades del sector privado o público que DoppelPaymer afirmó haber vulnerado nunca han aparecido en la prensa. Dicho esto, nuestros datos parecen coincidir con la advertencia del FBI. La Administración Pública representó dos tercios de sus objetivos, entre los que destaca la violación de la Oficina del Fiscal General de Illinois el 10 de abril de 2021. El sector de Manufactura fue el segundo más atacado, con un 15%, mientras que los sectores de Servicios Financieros y de Seguros, Salud y Servicios Profesionales recibieron un 8% del total de ataques cada uno.



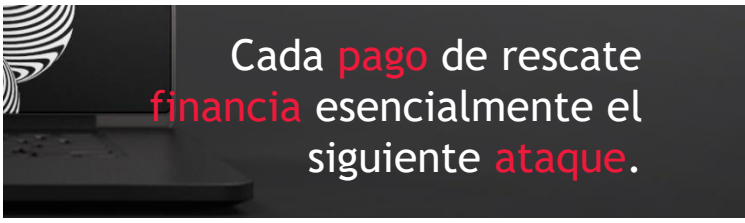
8 https://cybernews.com/security/us-colonial-pipeline-hack-an-earthquake-in-the-critical-infrastructure-industry/

9 https://www.ic3.gov/Media/News/2020/201215-1.pdf

“LOW HANGING FRUIT” (FRUTA A BAJA ALTURA)

No es de extrañar que la Administración Pública, la Salud, la Educación y otros servicios que conforman las infraestructuras críticas encabecen las listas de víctimas del Ramsonware. A pesar de que los activos de datos, los sistemas y las redes de estos sectores son tan vitales que cualquier interrupción tiene efectos debilitantes en la seguridad, la economía y los servicios esenciales para millones de ciudadanos, la mayoría tiene una higiene de ciberseguridad deficiente. Esto casi garantiza alguna forma de pago. Por otro lado, dado que los ciberdelincuentes entienden que los costos de cierre de las grandes empresas son de millones o decenas de millones, y cuando se enfrentan a un precio para volver a operar en línea, el pago de un rescate es algo habitual.

El 28 de mayo, el Sturdy Memorial Hospital, un centro de 126 camas de la ciudad con sede en Massachusetts, confirmó que había pagado un rescate no revelado a un grupo no identificado a cambio de la promesa de que destruiría los datos robados. Al parecer, contenía números de reclamos de seguros de pacientes, historial médico, información sobre tratamientos, números de seguridad social, rutas bancarias y números de tarjetas de crédito de 57.400 personas. Este tipo de incidentes se produjeron de forma constante durante el primer semestre de 2021, lo que pone de manifiesto las debilidades inherentes al sector de salud.



¿DEBE USTED PAGAR?

Aunque los ataques de Ramsonware no son nada nuevo, el uso de la "triple" y "cuádruple extorsión" ha planteado cuestiones estratégicas a las empresas, a saber, ¿se deben pagar rescates? Al testificar ante el Congreso el 8 de junio, la defensa del director general de Colonial Pipeline, Joseph Blount Blount, refleja estas preocupaciones, diciendo que Colonial entendía que la decisión de pagar el rescate era exclusivamente suya, lo que significa que la empresa buscaba defender sus intereses. Sin embargo, cada pago de rescate financia esencialmente el siguiente ataque.

JBS, que es el segundo mayor productor de carne de Estados Unidos, emitió un comunicado el 3 de junio en el que afirmaba que había podido limitar la pérdida de suministro a menos de un día de producción, y que las pérdidas de producción global se recuperarían "totalmente“ para fines de la siguiente semana. A pesar de su optimismo proyectado, la interrupción de una quinta parte del procesamiento de la carne de res en Estados Unidos tiene efectos potencialmente significativos en el mercado, además de la escasez de suministro a corto plazo, como el aumento de los precios de la carne de res y otras proteínas. Las interrupciones de los principales distribuidores de alimentos tienen consecuencias estratégicas más importantes que las pérdidas monetarias a corto plazo. JBS también abastece a más de 150 países, lo que significa que los riesgos potenciales asociados a las interrupciones más prolongadas de la cadena de suministro de alimentos a nivel mundial, junto con el precedente del pago de rescates, se traduce en una mayor probabilidad de que los actores de la amenaza se sientan atraídos progresivamente por objetivos similares de bajo riesgo y alta rentabilidad.

Otro factor que puede surgir es el sector de los seguros, especialmente con las entidades que carecen de recursos cibernéticos. Al parecer, las tarifas de los ciberseguros mundiales han aumentado hasta un 40% debido al incremento de los ataques de Ramsonware.[10] Cuanto más paguen las empresas, se espera que las aseguradoras cibernéticas empiecen a cobrar a los clientes que no apliquen las mejores prácticas de ciberseguridad, obligándoles incluso a ceder el control de la negociación del rescate y la recuperación por completo durante la suscripción para reducir el impacto.[11]

La conclusión es que, a corto plazo, es más rentable pagar. Más allá del corto plazo, estos ataques plantean importantes retos estratégicos a las empresas, ya que permiten a los ciberdelincuentes dictar con éxito la economía de la extorsión. El costo de reconstruir los sistemas puede ser significativamente más alto que los montos de los rescates, que, como se revela en las claves liberadas de Avaddon, están diseñados para incentivar a las empresas a pagar. Sin embargo, se prevé que los gobiernos y las aseguradoras penalicen el pago de rescates que financien el próximo incidente cibercriminal, probablemente mediante la promulgación de leyes que obliguen a hacer públicos los pagos de rescates y eleven las primas de los seguros.

10 https://www.reuters.com/technology/cyber-reinsurance-rates-rocket-july-renewals-willis-re-2021-07-01/

11 https://www.insurancebusinessmag.com/us/news/cyber/global-cyber-insurance-pricing-spikes-32--report-259795.aspx

NEGOCIANDO UN "NO"

A diferencia de los sistemas in situ, que pueden ser vulnerados, mantener copias de seguridad seguras y fuera de línea es esencial para tener un proceso de recuperación que, a la larga, es mucho más rentable que pagar un rescate. La clave es probar, y volver a probar constantemente, el tiempo que tarda un posible proceso de restauración de datos si se produce un ataque de este tipo. Hay que simular, formular y ejecutar una recuperación eficiente en tiempo y costo. De este modo, se desarrollan sistemas de copia de seguridad más resistentes y mejor configurados que identifican los problemas clave que pueden surgir durante los incidentes reales, como las aplicaciones del sistema central que son esenciales para la recuperación de datos y, por lo tanto, también deben ser objeto de una copia de seguridad, o saber cuánto tiempo tardarían en producirse las transferencias de datos con antelación en lugar de descubrir que podrían tardar semanas o meses en tiempo real una vez que se produce el ataque.

La estrategia de copias de seguridad se ejemplificó mejor cuando el conglomerado multinacional japonés FujiFilm rompió el molde tras una serie de ataques de Ramsonware de gran repercusión, al negarse a pagar y, en su lugar, confiar en las copias de seguridad para reanudar las operaciones comerciales. El 2 de junio la empresa apagó parte de los sistemas informáticos para evitar un posible ataque de Ramsonware después de que un actor no autorizado accediera a los servidores de su sede en Tokio. El 4 de junio apagó toda su red, bloqueando el acceso a sus sistemas de correo electrónico, facturación e informes internos, y el 14 de junio empezó a operar con servidores y ordenadores confirmados como seguros. La empresa tardó entre 10 y 14 días en reanudar las operaciones normales y la comunicación con sus clientes y socios, y declaró que no había encontrado pruebas de que se hubiera filtrado información al exterior.

Sin embargo, aunque su plan de recuperación podría haber sido mucho peor, la empresa perdió entre 10 y 14 días de inactividad a pesar de no haber pagado. Además, aunque no nombró a un operador específico de Ramsonware, los expertos afirmaron que los sistemas de Fujifilm estaban infectados por la red de bots Qbot de acceso remoto (RAT) desde el 15 de mayo.[12] Los operadores del troyano Qbot han sido históricamente utilizados por los actores de la amenaza para obtener acceso remoto a las redes que fueron previamente infectadas. Esto significa que, a pesar de las estrategias de recuperación de las organizaciones, sigue existiendo el riesgo potencial de futuros ataques de Ramsonware que utilicen las mismas vulnerabilidades.

> **No era una contraseña del tipo Colonial123.**
> Joseph Blount, Gerente General de Colonial Pipeline

Este fue el caso cuando el director general de Colonial, Blount, confirmó que los afiliados de DarkSide accedían a la red de la empresa mediante un sistema de red privada virtual (VPN) heredado que no utilizaba la autenticación multifactor, lo que significa que se accedía mediante una contraseña sin un segundo paso como un mensaje de texto de contraseña única (OTP). La autenticación de dos factores, que requiere autenticaciones multifactoriales para acceder a todas las aplicaciones internas, es una salvaguarda común empleada por prácticamente todas las grandes empresas. Blount afirmó que Colonial Pipeline invirtió más de 200 millones de dólares en la seguridad de sus sistemas en los últimos 5 años; sin embargo, este incidente subraya la realidad de que la escasa higiene de la ciberseguridad no impidió la vulneración más sencilla.[13]

NEGOCIANDO UN PRECIO MÁS BAJO

Los escasos detalles publicados sobre los rescates pagados, incluyendo las claves liberadas de Avaddon, nos muestran que los ciberdelincuentes, en general, están más que dispuestos a negociar. Si se presenta el riesgo de una vulneración, los grupos de Ramsonware no deben ser percibidos como algo diferente a las partes competidoras que entran en negociaciones. En lugar de conceder que los actores de la amenaza tienen todo el poder, las organizaciones deben determinar qué influencia tienen y formar una estrategia de negociación. De hecho, tras el fuerte aumento de los ataques de Ramsonware en los últimos años, ha surgido toda una nueva industria de negación de Ramsonware, con muchas empresas que ofrecen servicios dedicados al tema.

Las víctimas también deben entender que el pago de un rescate no impide que se produzcan nuevos ataques, si las malas prácticas y las vulnerabilidades que permitieron que se produjera un ataque en primer lugar siguen existiendo, los grupos de Ramsonware atacarán a la empresa que pagó una y otra vez mientras siga existiendo la oportunidad de bajo riesgo y alto beneficio.

12 https://www.bleepingcomputer.com/news/security/fujifilm-resumes-normal-operations-after-ransomware-attack/
13 https://cybernews.com/news/one-password-allowed-hackers-to-disrupt-colonial-pipeline-ceo-tells-senators/

VULNERABILIDADES DE SOFTWARE

Las vulnerabilidades de software representaron el 13% de todos los ataques en el primer semestre de 2010, con un 8% de vulnerabilidades de día Cero. Al menos el 5% fueron resultado de Vulnerabilidades y Exposiciones Comunes (CVE) conocidas, la mayoría de las cuales tienen parches.

Entre diciembre de 2020 y enero de 2021, varios usuarios del producto File Transfer Appliance (FTA) de Accellion, un software de grado empresarial heredado, se vieron afectados por dos ataques de día cero, y aunque los parches se publicaron ya el 2 de diciembre, las vulnerabilidades del software de terceros ya habían sido explotadas.[14] El 22 de febrero Accellion confirmó que el grupo de ciberdelincuencia financiera FIN11 y el Cl0p Ramsonware estaban detrás de los ataques, que para entonces habrían afectado a unas 100 empresas de todo el mundo. Se desconoce si Cl0p consiguió infiltrarse en los servidores de TLC no parcheados o si obtuvo los datos de los hackers, pero parece que el grupo no cifró los archivos de las víctimas y, en su lugar, intentó extorsionarlas amenazándolas con que los datos se volcarían en su sitio de filtraciones si no pagaban. [15]

REDUCCIÓN DE SUPERFICIES DE ATAQUE

Los ataques a la cadena de suministro se producen cuando los actores de la amenaza atacan a un único proveedor vulnerable de terceros para vulnerar a varias organizaciones que utilizan versiones sin parches del dispositivo de software. Estos ataques altamente sofisticados se han vuelto muy prolíficos desde que el ataque a la cadena de suministro patrocinado por el estado en SolarWinds vio a múltiples organizaciones en los Estados Unidos ser golpeadas en 2020.

Si bien Accellion recibió críticas generalizadas por los fallos de su producto FTA, de 20 años de antigüedad, el sin embargo, esto no hace más que mostrar cómo muchas organizaciones siguen confiando en sistemas de TI heredados con mayores superficies de ataque propensas a inevitables explotaciones de día cero. En su última actualización de parches, Accellion hizo hincapié en su plan de retirar su producto FTA en abril, después de trabajar en la transición de los clientes a su nueva plataforma Kiteworks durante casi tres años. Sin embargo, en mayo, sólo el 75% de sus clientes había migrado, lo que significa que el 25% seguía siendo susceptible de sufrir ataques. En junio, unas 300 organizaciones se vieron afectadas por el ataque a la cadena de suministro, y se confirmó que al menos 37 sufrieron violaciones de datos significativas en el primer semestre de 2021. El parche final se publicó el 1 de marzo, a pesar de que la vulnerabilidad persistió durante casi tres meses.

PARCHEADO

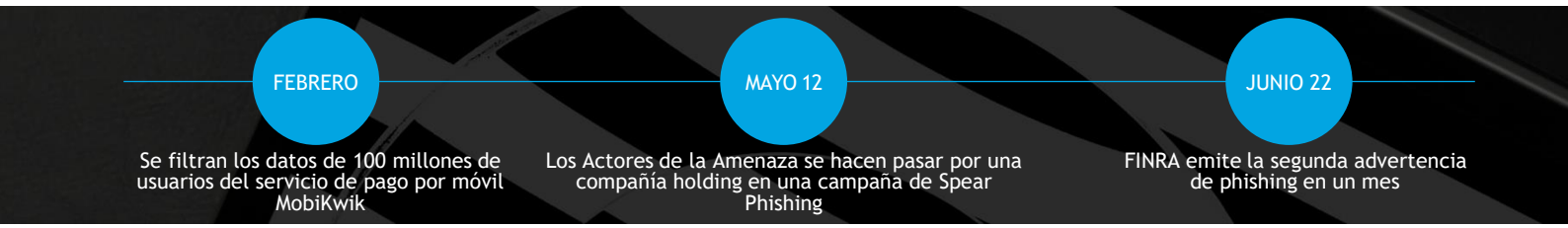
Estos ataques ponen de manifiesto la incapacidad de mitigar los daños potenciales mediante el empleo de dos de las prácticas de ciberseguridad más cruciales, la inteligencia de amenazas y la gestión de vulnerabilidades, o Gestión de Vulnerabilidades basada en Amenazas, para identificar activamente las amenazas potenciales y relevantes antes de que se conviertan en ciberataques activos.

El Banco de la Reserva de Nueva Zelanda (RBNZ), que fue atacado el 25 de diciembre de 2020, planteó estas preocupaciones, alegando que el servicio de alerta de correo electrónico de Accellion no les avisó de la vulneración hasta el 6 de enero.[16]

La falta de recepción de información sobre amenazas pone de manifiesto la ausencia de prácticas efectivas de gestión de amenazas y vulnerabilidades, necesarias no sólo para estar al día de las alertas y los avisos, sino también para identificar información procesable, como los indicadores de peligro (IOC), y otras novedades esenciales para proteger los servicios potencialmente expuestos..

14 https://techcrunch.com/2021/07/08/the-accellion-data-breach-continues-to-get-messier/
15 https://www.zdnet.com/article/fireeye-links-0-day-attacks-on-fta-servers-extortion-campaign-to-fin11-group/
16 https://www.rbnz.govt.nz/news/2021/05/reserve-bank-taking-action-to-respond-to-data-breach-reports

VULNERABILIDADES HUMANAS



La variable más constante en casi todos los incidentes de ciberseguridad es la vulnerabilidad humana. Las acciones humanas involuntarias, o los errores, como hacer clic en enlaces maliciosos, desconfigurar los sistemas, las aplicaciones, las bases de datos e incluso los controles de seguridad, conducen con demasiada frecuencia a consecuencias de gran alcance para las organizaciones víctimas.

CORREO ELECTRÓNICO

El vector de ataque inicial más común (método o vía utilizada para acceder o penetrar en el sistema de un objetivo) registrado este año fue el correo electrónico, y esto se debe probablemente a la fatiga del correo electrónico, donde los usuarios inevitablemente hacen clic en enlaces maliciosos incrustados en los correos electrónicos. El 94% de los programas maliciosos, incluido el Ramsonware, se distribuyen por correo electrónico, y el 80% de ellos lo hacen mediante phishing. Esto se debe a que los ciberdelincuentes, en particular los grupos de Ramsonware, perfeccionan continuamente las estrategias de phishing por correo electrónico utilizando tácticas de ingeniería social que juegan con las emociones de los usuarios, los intereses sociales, la carga de trabajo, etc.

Además, los ciberdelincuentes siguieron demostrando su capacidad para llevar a cabo un amplio reconocimiento de objetivos de alto perfil con el fin de identificar información clave, como los intereses o los socios del objetivo, para aumentar la probabilidad de que se haga clic en un enlace malicioso en las campañas de spear-phishing dirigidas. Por ejemplo, el 4 de abril los investigadores de seguridad descubrieron una nueva campaña que distribuía el backdoor more_eggs a través de ofertas de trabajo no solicitadas dirigidas a perfiles de LinkedIn cuyas descripciones de trabajo se identificaban como altos ejecutivos. El descargador more_eggs, que puede distribuir múltiples malwares, muestra cómo la ingeniería social compleja, como los señuelos personalizados, puede utilizarse para distribuir técnicas de ataque multivectoriales.

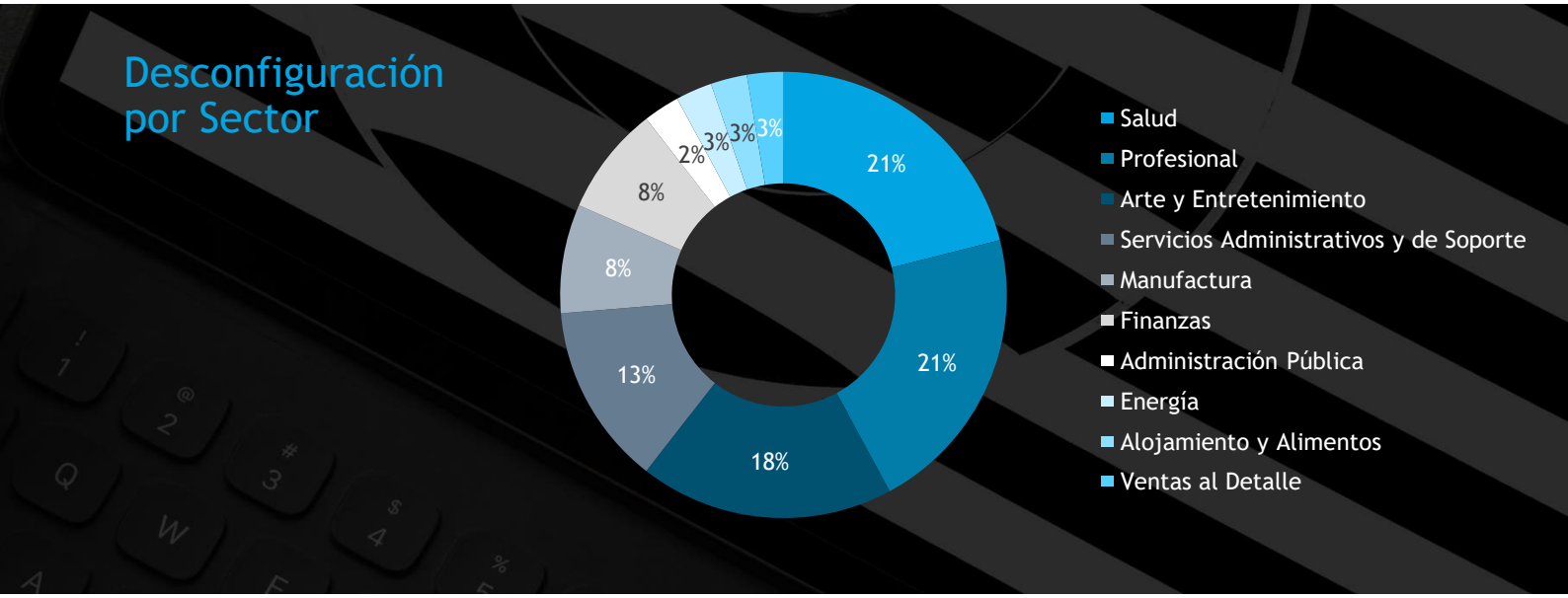
En abril, Microsoft reveló que los actores de la amenaza utilizaban formularios de contacto corporativos legítimos para enviar correos electrónicos de phishing que amenazaban a los objetivos empresariales con demandas, intentando infectarles con malware para robar información utilizando URLs legítimas de Google. Del mismo modo, el 12 de mayo el FBI reveló que los actores de la amenaza se hicieron pasar por Truist, el sexto mayor holding de Estados Unidos, en una campaña de spear-phishing que intentaba infectar a los destinatarios con un troyano de acceso remoto (RAT). Otros incidentes notables se produjeron el 22 de junio, cuando la Autoridad Reguladora de la Industria Financiera (FINRA), que supervisa a más de 624.000 agentes de bolsa, empresas de valores y mercados de valores de todo Estados Unidos, advirtió de una campaña de phishing en curso por segunda vez en el mismo mes. Al igual que en su primera advertencia del 7 de junio, FINRA advirtió que la campaña de phishing suplantó al organismo regulador, y amenazó a los destinatarios con sanciones a menos que proporcionaran la información solicitada por los atacantes. [17]

La prevención de las vulnerabilidades del correo electrónico radica en la educación continua de los usuarios, ya sea una secretaria de oficina o los ejecutivos de la C-Suite, sobre cómo son los nuevos ataques. El problema, sin embargo, radica en el panorama extremadamente dinámico de la ciberseguridad, en el que surgen nuevas amenazas mientras persisten las antiguas a través de nuevos enfoques cada vez más sofisticados de las estrategias de ingeniería social.

17 https://www.bleepingcomputer.com/news/security/us-brokerage-firms-warned-of-ongoing-phishing-with-penalty-threats/

DESCONFIGURACIÓN

Las acciones no intencionadas llevadas a cabo por actores internos siempre han sido un problema; sin embargo, las desconfiguraciones de sistemas, aplicaciones y bases de datos, descubiertas por investigadores de seguridad o demasiado tarde después de que los datos hayan sido descargados en un sitio de filtración de la red oscura, es un problema particularmente creciente, que representa el 5% de todos los incidentes en el primer semestre de 2021.



Muchas infracciones en la nube son el resultado de actores de amenazas que aprovechan los errores en una implementación en la nube, sin siquiera usar malware. Una vez que se obtiene acceso a los repositorios en línea mal configurados o débilmente configurados en las nubes públicas, los actores no autorizados no sólo pueden localizar fácilmente los activos de datos valiosos, sino también exfiltrar los datos utilizando la misma configuración errónea. La salud y los servicios profesionales compartieron el primer puesto con ambos, con un 21%, seguidos por las Artes, el Entretenimiento y la Recreación, con un 18%, mientras que las Finanzas y la Manufactura representaron el 8% de los incidentes.

Entre las violaciones más destacadas se encuentra la de la empresa de riesgos y cumplimiento LogicGate, que confirmó el 23 de febrero que una parte no autorizada accedió a las copias de seguridad de sus clientes tras obtener las credenciales de su servidor de almacenamiento en la nube alojado en Amazon Web Services (AWS). La empresa india de pagos por móvil MobiKwik, que también alojaba sus datos en AWS, informó el 30 de marzo de que en algún momento de febrero de 2021 se filtraron en la web oscura los datos de casi 100 millones de usuarios. Del mismo modo, Mercedes Benz USA reveló que 1,6 millones de registros de clientes fueron filtrados el 11 de junio, y el 12 de junio, el Grupo Volkswagen de América confirmó que 3,3 millones de datos de sus clientes estaban siendo vendidos en un foro de hacking después de ser robados de un servidor expuesto de Microsoft Azure.

OPERACIONES DE AMENAZAS CIBERNÉTICAS

IDENTIFICACIÓN

Inteligencia sobre amenazas cibernéticas para la dirección ejecutiva

Este informe presenta múltiples violaciones de datos que demuestran cómo la falta de soluciones de gestión de riesgos respaldadas por la inteligencia puede resultar en un daño duradero para las empresas, los socios y los clientes. Por ello, los líderes que toman decisiones de negocio a partir de procesos de gestión de riesgos cibernéticos necesitan inteligencia de amenazas cibernéticas de nivel estratégico.

Para ser más precisos, el personal de la alta dirección necesita CTI para la gestión ejecutiva en forma de informes menos técnicos y sesiones informativas difundidas en varios formatos y plazos, que proporcionen una visión más amplia del panorama de amenazas de una organización. La CTI a nivel ejecutivo ofrece una visión estratégica y práctica en una amplia gama de áreas, como los riesgos asociados a la adopción de acciones específicas, las tácticas, técnicas y procedimientos (TTP) de los actores de las amenazas, los sectores e industrias a los que se dirigen y otros avances generales en materia de seguridad. En términos prácticos, tener una amplia visión de las tendencias puede generar opciones para abordar los impactos inmediatos, apoyar las decisiones de inversión en seguridad para el próximo trimestre y desarrollar una hoja de ruta de seguridad a largo plazo.

Modelado de Amenazas en S-SDLC

Cuando se trata de implementar la seguridad en el desarrollo de aplicaciones, a menudo se hace como una idea tardía, ya que los desarrolladores le dan menos prioridad debido a la falta de perspicacia en materia de ciberseguridad o porque los problemas de seguridad, en general, pueden obstaculizar los plazos de producción. Esto conduce finalmente a vulnerabilidades críticas que aumentan el riesgo y los costos de remediación que se vuelven mucho más grandes cuando se implementan después de las etapas de diseño del ciclo de vida de desarrollo de software (SDLC). Dicho esto, el modelado de amenazas puede ser una forma fácil y rentable de implementar la seguridad en la fase de diseño del SDLC.

El modelado de amenazas es el proceso de seguridad mediante el cual se pueden identificar, categorizar y analizar las amenazas con el fin de reducir el riesgo mediante la elaboración de soluciones a los posibles daños. Dicho esto, el modelado de amenazas debe implementarse para abordar las vulnerabilidades previstas durante las primeras etapas del SDLC, así como en las etapas posteriores cuando se realizan cambios en la arquitectura.

Además, mientras que el DevOps tradicional combina el desarrollo de software con los equipos de operaciones de TI en una sola unidad que comparte habilidades y un objetivo común, el modelado de amenazas puede llevar el pensamiento sinérgico un paso más allá incorporando la seguridad desde el principio mediante el desarrollo de una cultura DevSecOps. En este contexto, el arquitecto de seguridad, las operaciones y los desarrolladores de infraestructuras pueden comunicar sus aportaciones dentro de un equipo completo para fomentar una cultura de colaboración, que permita a los miembros del equipo comprender las funciones, los objetivos y los puntos débiles de los demás, y mejorar las operaciones empresariales en general. Por lo tanto, una modelización eficaz de las amenazas puede permitir a las organizaciones identificar posibles ataques, vulnerabilidades y mitigaciones en el contexto de la protección del software, las aplicaciones o los sistemas antes de que surjan, facilitando al mismo tiempo una mejor cultura general de desarrollo de software.

MODELADO DE AMENAZAS EN S-SDLC

Gestión de Vulnerabilidades Basada en Amenazas (Riesgo)

Prácticamente todas las organizaciones emplean alguna forma de gestión de la vulnerabilidad para identificar los puntos débiles de la infraestructura de sus sistemas antes de que sean explotados por agentes maliciosos. Sin embargo, en la realidad, las organizaciones se enfrentan a un número increíble de amenazas potenciales, lo que a menudo conduce a una priorización inexacta y a la pérdida de tiempo en el procesamiento de la remediación de las vulnerabilidades no críticas en lugar de mitigar las amenazas críticas a tiempo, aumentando así el riesgo de violación. Además, los procesos de mitigación ineficaces suelen provocar incoherencias y tensiones entre los equipos de operaciones de seguridad, cuyo propósito es eliminar todos los fallos de seguridad, y las operaciones de TI, cuyo objetivo principal es perpetuar la disponibilidad del sistema.

Aquí es donde la Gestión de Vulnerabilidades Basada en Amenazas (Riesgo) puede priorizar correctamente contra las vulnerabilidades más críticas y utilizar procesos de remediación más manejables mediante el uso de inteligencia de amenazas para identificar factores como los valores de los activos, la gravedad del impacto y la intención del actor malicioso.

Este enfoque facilita un marco de clasificación de riesgos más realista que permite una priorización eficaz, en la que las vulnerabilidades altamente críticas se parchean inmediatamente, mientras que las no críticas menos urgentes pueden gestionarse posteriormente o incluso supervisarse para el desarrollo de riesgos si la optimización del negocio lo permite.

Cero Confianza

Las violaciones casi siempre implican alguna forma de intrusión en un “perímetro”, como un sistema o una red, a la que sigue un movimiento lateral posterior una vez dentro mediante la escalada de privilegios. Este perímetro, por desgracia, se ha ampliado a medida que los datos y las aplicaciones se trasladan cada vez más a la nube, mientras que el número de puntos finales también ha aumentado debido al importante crecimiento del trabajo a distancia en el marco de COVID-19. Dicho esto, el enfoque de la Arquitectura de Cero Confianza (ZTA) presenta una solución viable para gestionar de forma proactiva las conexiones seguras al basarse en la suposición de que una organización está comprometida y que las conexiones entre cada usuario, dispositivo, aplicación y conjunto de datos deben validarse continuamente para cumplir ciertas condiciones de uso. Aunque la idea de asegurar en exceso las conexiones entre las unidades de negocio parece una receta para el estancamiento del flujo de trabajo, puede utilizarse para limitar el riesgo cibernético sin impedir el crecimiento.

Al envolver una defensa alrededor de cada conexión de una manera dinámica que ajusta los derechos de control de acceso y los privilegios en función del estado de riesgo, las unidades de negocio pueden seguir funcionando sin problemas mientras permanecen seguras. Gracias a la inteligencia sobre amenazas que aprovecha la ubicación, el uso de aplicaciones y otras variables que enriquecen los datos de cada usuario, dispositivo y conexión, los administradores pueden utilizar los perfiles de riesgo para ajustar los privilegios, lo que mantiene la seguridad al adaptarse a los niveles de riesgo cambiantes en función del contexto. Ir más allá de los marcos binarios de denegación/permiso de acceso permite a los usuarios que suponen un riesgo mayor o menor acceder a los activos pertinentes, como las herramientas necesarias para completar las tareas empresariales. En este contexto, los administradores del sistema pueden conceder a los usuarios latitud a medida que plantean más o menos riesgo, al tiempo que toman medidas directas para limitar o ampliar el acceso.

La filosofía de Cero Confianza se ha vuelto cada vez más relevante en todos los sectores en los últimos años, y en los sectores de infraestructuras críticas durante 2021 tras los recientes ataques de alto perfil de Ramsonware. Según el Informe de Adopción de Cero Confianza de Microsoft 2021, el 96% de los responsables de la toma de decisiones en materia de seguridad afirmaron que Cero Confianza se ha convertido en algo fundamental para el éxito de su organización, el 76% de los cuales ya está en proceso de implementación (un aumento del 20% en 2020), mientras que el 73% espera que sus presupuestos de Cero Confianza aumenten en los próximos dos años. En el mismo sentido, el Decreto Ejecutivo del Presidente Joe Biden sobre la mejora de la Ciberseguridad de la Nación, emitido el 12 de mayo de 2021, define explícitamente la implantación de la ZTA como una prioridad clave de la seguridad nacional tras los ataques a sus infraestructuras críticas.

18 https://www.microsoft.com/security/blog/2021/07/28/zero-trust-adoption-report-how-does-your-organization-compare/

19 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

DETECCIÓN

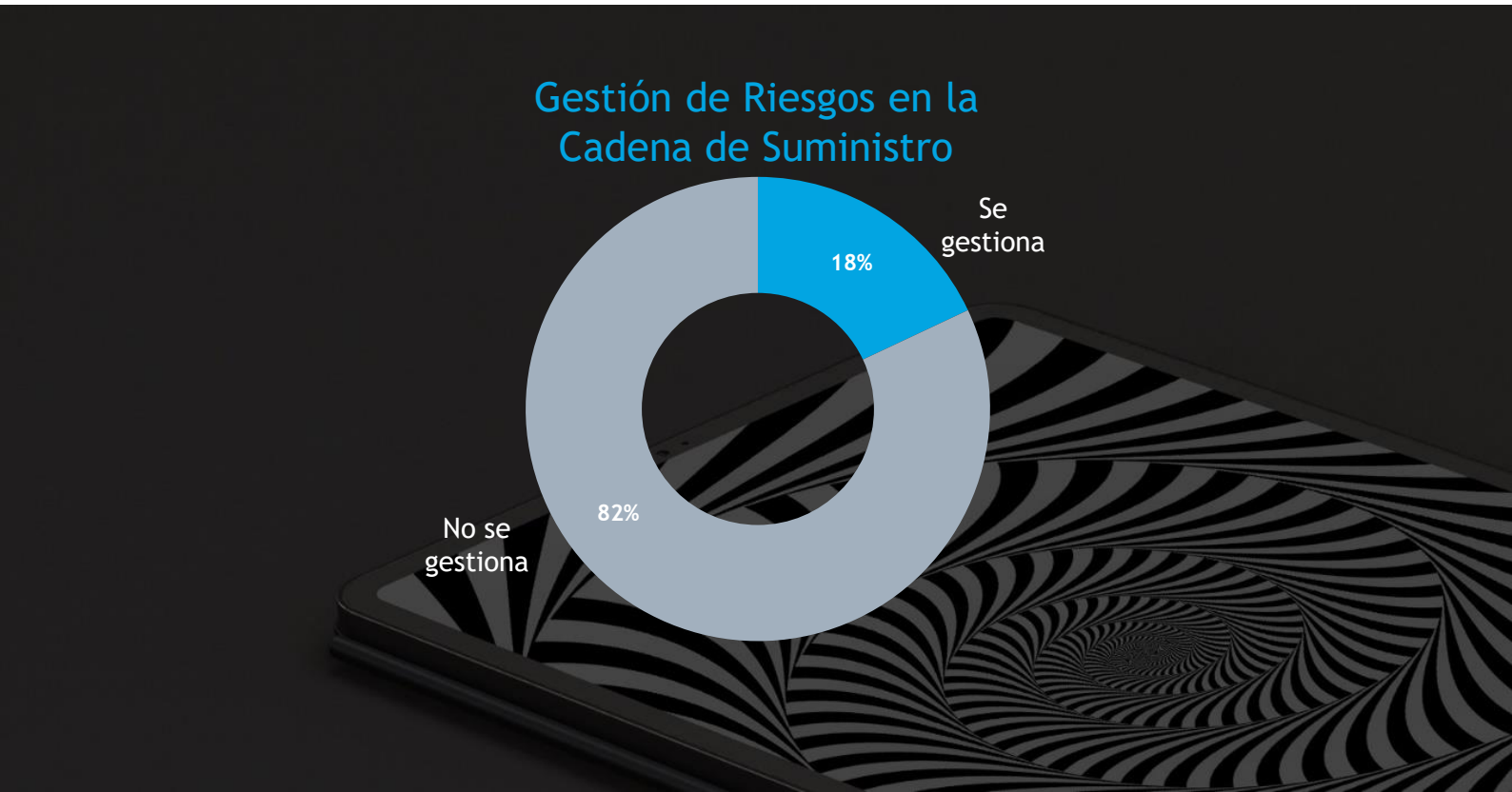
Monitoreo Continuo de la Superficie de Ataque

El mapeo inicial de la superficie de ataque de cualquier organización ya no puede considerarse relevante, ya que la expansión e inversión de las empresas en la digitalización y la migración a la nube exponen más superficies de Internet, y con ello, nuevos vectores de ataque. Aunque el monitoreo de la superficie de ataque (ASM) ha existido por algún tiempo, las organizaciones deben ahora llevar a cabo el Monitoreo Continuo de la Superficie de Ataque (CASM) para identificar no sólo las vulnerabilidades en los activos conocidos, sino las emergentes y desconocidas, tales como los nuevos puntos finales en entornos descentralizados, como los dispositivos del personal a distancia..

CASM aumenta la atribución de nuevos activos y descubre vulnerabilidades en los sistemas y servicios a través de la enumeración de la superficie de ataque externa y el movimiento lateral mediante la realización de pruebas de penetración continuas y el escaneo de vulnerabilidades, así como la evaluación de aplicaciones. Además, en la actualidad, varias plataformas CASM presentan una madurez suficiente para ofrecer soluciones de inteligencia sobre ciberamenazas, gestión de evaluación de vulnerabilidades y respuesta a incidentes con suficiente apoyo.

Gestión de Riesgos de Terceros (TPRM)

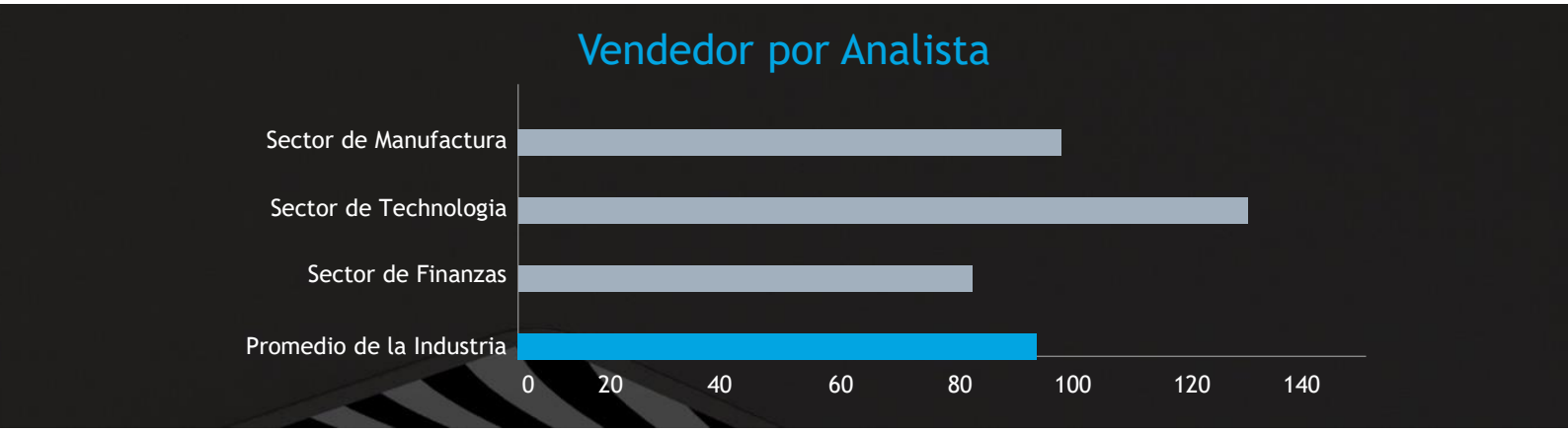
La subcontratación de TI ha aumentado sustancialmente en los últimos años en general, y prácticamente todas las organizaciones dependen de terceros para algún servicio. Sin embargo, esto significa que cuando los vendedores o proveedores se ven afectados por ciberataques, puede haber impedimentos significativos para que las operaciones funcionen sin problemas, mientras que los impactos a largo plazo pueden llegar a ser devastadores. Si un proveedor de la nube, un MSP u otro proveedor, como los servicios de envío, deja de funcionar, también lo hacen su sitio web, sus aplicaciones, los plazos de entrega, etc., y esto puede afectar negativamente los resultados y la reputación.. De hecho, según una encuesta que realizamos, el 82% de las organizaciones no gestionan regularmente los riesgos de la cadena de suministro cibernética, y sólo entre el 7% y el 15% evalúan a sus terceros. Una estrategia viable de gestión de riesgos que se centre en la identificación y reducción de los riesgos asociados a los vendedores, proveedores, prestadores de servicios o cualquier otro socio cuyos sistemas se solapen con la organización puede realizarse mediante la Gestión de Riesgos de Terceros (TPRM).



DETECCIÓN

Entender cómo utiliza usted múltiples terceros puede identificar qué salvaguardias tiene cada uno de ellos, a qué normas y reglamentos del sector están sometidos, y le permite emplear las mejores prácticas universalmente aplicables para mitigar los riesgos asociados a ellos. En este contexto, TPRM permite a las organizaciones priorizar a los proveedores en función de las puntuaciones de riesgo, dando la posibilidad de concentrar el tiempo y los recursos en los proveedores de alto riesgo mediante la realización de una diligencia debida más estricta, evaluaciones en profundidad o in situ y la validación, al tiempo que se limitan los datos compartidos, como la información de los clientes, a las funciones más críticas. Alternativamente, la cooperación con los proveedores de riesgo medio y bajo puede continuar con mayor libertad para que las operaciones puedan funcionar sin impacto.

Nuestro estudio demostró que, en los tres meses siguientes al establecimiento del proceso de TPRM, al menos 98 conclusiones cerradas tenían por lo menos un 38% de alta prioridad. Además, más del 70% de las organizaciones evaluaron a sus terceros a través de un cuestionario estandarizado, en lugar de personalizarlo para satisfacer sus necesidades, mientras que en el ámbito de la gestión del sector sólo había una media de un analista por cada 100 terceros. Aquí es donde el ciclo de vida de la TPRM puede aprovechar la automatización para aumentar la coherencia y la eficiencia, desde la identificación y la incorporación de nuevos proveedores, hasta la formación de evaluaciones de riesgo, puntuaciones, propietarios y mitigaciones, la gestión de las adquisiciones y los contratos, y la realización de informes y el seguimiento.



RESPUESTA

SOAR

Las organizaciones a menudo carecen de recursos humanos suficientes para hacer frente a una cantidad abrumadora de datos de eventos de seguridad para emplear una respuesta eficaz a los incidentes IR. Aquí es donde la automatización puede facilitar la agregación, el enriquecimiento, la correlación y la investigación eficientes de los datos mediante el enfoque de próxima generación en la respuesta a incidentes, a saber, la orquestación, automatización y respuesta de seguridad (SOAR). Las soluciones SOAR están diseñadas para integrar todas las herramientas y aplicaciones de seguridad existentes de forma abierta y organizada centralmente, al tiempo que automatizan el flujo de trabajo para reducir el tiempo de respuesta entre la violación y el descubrimiento.

El aspecto de la Orquestación en el enfoque SOAR utiliza una serie de libros de jugadas que definen las amenazas y explican cómo gestionarlas. Estos flujos de trabajo automatizados integran múltiples tecnologías de seguridad para responder a las amenazas. El aspecto de la automatización aprovecha a las máquinas para que realicen las tareas que normalmente hacen los humanos y automatiza la toma de decisiones para que los procesos de IR sean más eficaces y coherentes a escala, dejando a los humanos más tiempo para ocuparse de tareas y objetivos analíticos más complejos.

Sin embargo, los SAOR sólo son tan eficaces como los datos que se utilizan para construirlos, y aquí es donde la CTI de alta calidad que agrega los datos analizados se vuelve inteligente. La integración de estas capacidades mejora la productividad y la concienciación de los analistas del SOC, los encargados de responder a los incidentes y otro personal de seguridad, al reunir a varios profesionales, procesos y tecnologías de seguridad con diferentes puntos fuertes y débiles, al tiempo que se reduce la pérdida de tiempo y la fatiga mediante la automatización. En este sentido, SOAR ofrece una visión general totalmente integrada de los datos sobre las amenazas externas para tener una comprensión más clara del desarrollo de la situación, y proporciona las respuestas necesarias para remediar las respectivas amenazas.

RECUPERACIÓN

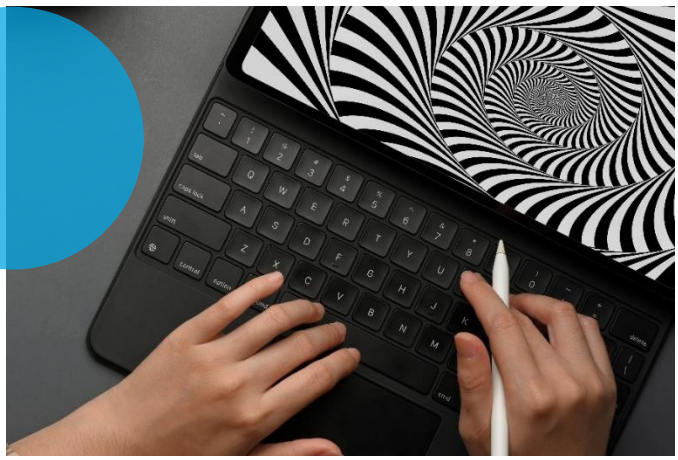
Plan de Copia de Seguridad y Recuperación basado en la amenaza

Disponer de un Plan de Copia de Seguridad y Recuperación de Desastres (BDRP) que describa detalladamente los procesos, los activos, el personal y las acciones necesarias en caso de desastre es esencial para recuperar los activos comprometidos en ciberataques como los ataques DDoS o Ransomware.

Un BDRP debe convertirse en una política clave para la mayoría de las empresas, especialmente las menos competentes técnicamente, ya que desempeñan un papel vital a la hora de garantizar la continuidad del negocio tanto a corto plazo tras un pero, como a largo plazo si se diseñan y aplican correctamente. Aunque cada organización es única, hay elementos universalmente críticos que pueden beneficiarse de algunas de las mejores prácticas del BDRP

Copias de Seguridad Protegidas Fuera de Línea

Los datos siempre deben ser respaldados en sistemas locales aislados y fuera de línea, resistentes y mejor configurados, de diferentes tipos, como las copias de seguridad completas programadas y las incrementales que se respaldan en un horario más frecuente. Además, todo, incluyendo los catálogos de copias de seguridad, los procesos y las aplicaciones internas críticas, como las que facilitan la transferencia de archivos, también deberían estar respaldados y protegidos para contrarrestar los ataques más sofisticados de Ramsonware que cifran múltiples tipos de activos. Un BDRP también debe tener en cuenta dónde se encuentran los sitios de recuperación de desastres, la infraestructura de TI y otras operaciones de recuperación de misión crítica, especialmente teniendo en cuenta que estas áreas están diseñadas para apoyar las prioridades de la organización, mientras que son remotas.



Identificación del RTO y del RPO

A la hora de diseñar e implantar los procesos de recuperación de desastres, las organizaciones deben definir el Objetivo de Tiempo de Recuperación (RTO) y el Objetivo de Punto de Recuperación (RPO) previstos. El RTO preestablece un plazo para la recuperación total y parcial del sistema y del funcionamiento, medido en unidades de tiempo como horas, días o semanas. Por otro lado, el RPO se refiere a la tolerancia a la pérdida de negocio, y se mide por el número de activos que es aceptable que se pierdan antes de determinar lo que define un daño impactante. Ambas son métricas esenciales para medir el progreso del BDRP y deben perfeccionarse regularmente mediante auditorías de seguridad. Además, estas métricas proporcionan puntos de referencia a otras secciones del BDRP en cada etapa.

Establecimiento de Funciones

Las organizaciones también deben establecer un equipo de recuperación de desastres y de negociación formado por diverso personal y deben identificar las funciones de cada equipo y de sus miembros, dentro y fuera del proceso de recuperación de desastres. Esto debe incluir no sólo a los profesionales técnicos, sino también a los ejecutivos no técnicos, como los asesores jurídicos familiarizados con las leyes y reglamentos, los expertos en seguros, otros consejos externos y los negociadores profesionales, y también debe determinar quién negocia. Definir claramente las funciones que se asignan a cada persona o equipo es fundamental para agilizar los esfuerzos y las comunicaciones del BDRP una vez que el proceso de recuperación está en marcha, y lo que es más importante, prepara a la dirección mediante capacitación previa.

Además, tener una amplia experiencia en un consejo de recuperación de desastres también debería determinar si los rescates deben ser pagados, y las organizaciones víctimas pueden beneficiarse en gran medida de tener negociadores profesionales y ejecutivos como el Director de Seguridad de la Información (CISO) y el Gerente de Operaciones (COO) listos para comprometerse con los respectivos actores de la amenaza inmediatamente. Esto puede permitir ganar tiempo para dar sentido a la situación y dar ventaja a la recuperación de desastres, o reducir la demanda de rescate de manera significativa para aminorar el impacto. Además, teniendo en cuenta que sólo el 28% de los incidentes de Ramsonware se confirmaron como violaciones, tener expertos preparados puede ayudar a obtener pruebas reales de que los datos han sido realmente comprometidos o robados.

RECUPERACIÓN

Creación de Planes de Comunicación

Un plan de comunicación minucioso y cuidadosamente elaborado que se establezca antes de que surja repentinamente la necesidad de uno es vital para limitar el daño a largo plazo a la reputación de una organización. Los operadores de Ramsonware y los ciberdelincuentes son plenamente conscientes de que las organizaciones están sujetas a las percepciones de las partes interesadas internas y externas, y deben determinarse procedimientos definidos sobre cómo ponerse en contacto con proveedores, socios y clientes.

Esto debe incluir las respuestas por defecto al pago y al no pago de las demandas de rescate, la consideración de los factores legales para la divulgación de las infracciones, y debe hacer un esfuerzo general para controlar cómo se está percibiendo la situación en general. Deben determinarse los canales de comunicación, ya sean formales, oficiales, de noticias o de medios sociales, para controlar la narrativa y evitar la cobertura mediática negativa y la publicidad no deseada.

Realización de Pruebas Regulares

Es necesario realizar auditorías y pruebas constantes del BDRP para que no sólo sea práctico, sino también pertinente a lo largo del tiempo. Las pruebas periódicas garantizan que los procesos de recuperación de desastres sigan funcionando a medida que las empresas y organizaciones crecen en tamaño y tipo.

En este contexto, las copias de seguridad reconfiguradas, el RTO, el RPO, la comunicación y las funciones deben probarse y perfeccionarse constantemente en simulaciones de restauración de datos para identificar los problemas críticos que probablemente surjan durante los incidentes reales. Esto aumenta la probabilidad de continuidad del negocio y apoya las inversiones que actualizan la recuperación eficiente.

OPHIR ZILBIGER

Líder de Cibernética Global
Socio, Jefe del Centro de Ciberseguridad
de BDO Israel
OphirZ@bdo.co.il

NOAM HENDRUKER

Socio
Jefe del Grupo de Consultoría Cibernética
Centro de Ciberseguridad de BDO, Israel
NoamH@bdo.co.il

GILAD YARON

Director
Jefe de la División de Privacidad y GRC
Centro de Ciberseguridad de BDO, Israel
GiladY@bdo.co.il

TOMMY BABEL

Director
Líder de la Práctica de Conciencia de la Situación
Centro de Ciberseguridad de BDO, Israel
TommyB@bdo.co.il

BDO