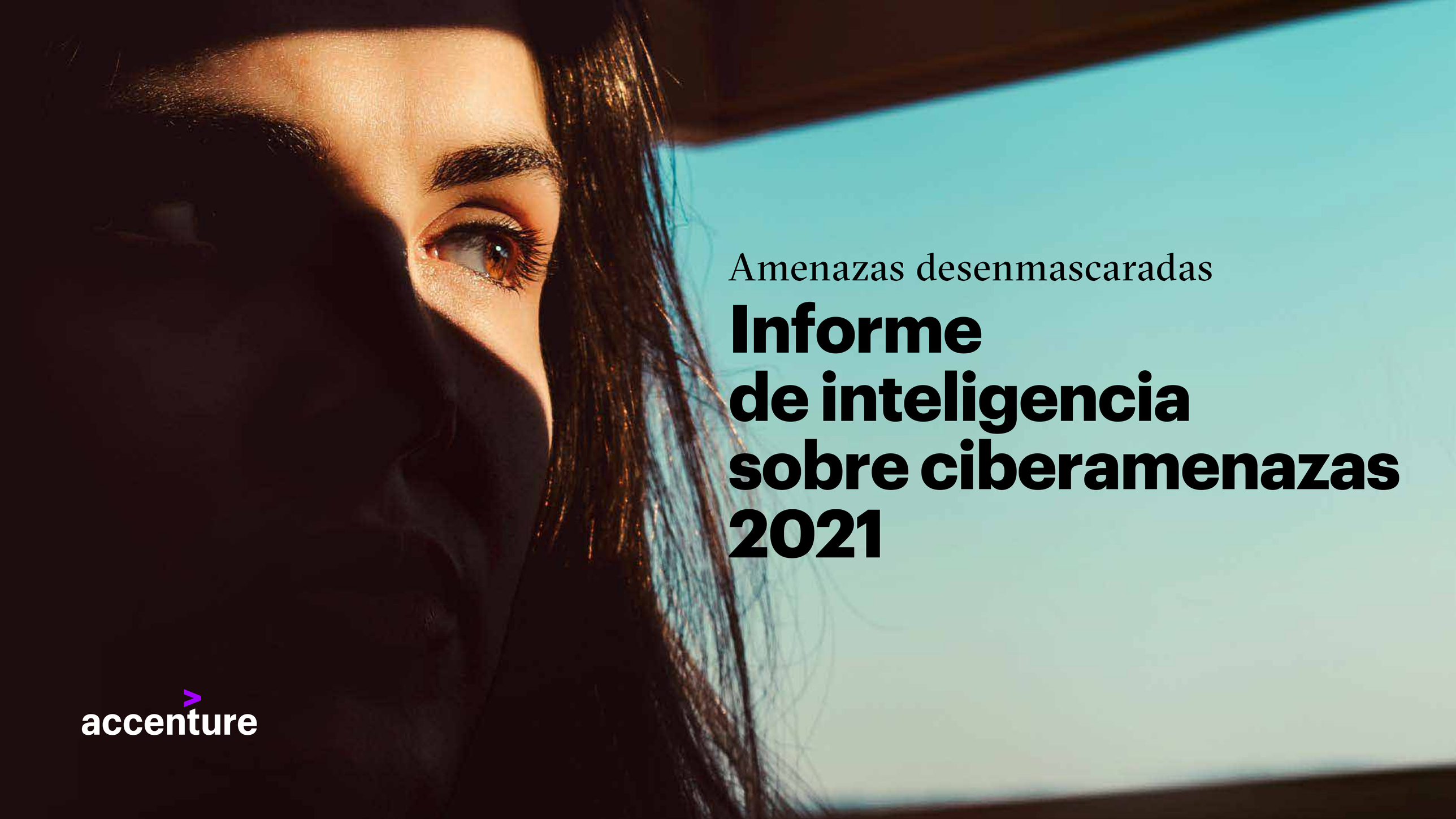


Amenazas desenmascaradas

Informe de inteligencia sobre ciberamenazas 2021

accenture

Prólogo

El equipo de Ciberinteligencia de Amenazas de Accenture (CTI Accenture) lleva más de 20 años creando una inteligencia relevante y procesable sobre las amenazas a la ciberseguridad. Sin embargo, a causa del rápido avance de las ciberamenazas, la inteligencia necesita ser oportuna para ser relevante. Como resultado, estamos cambiando nuestro informe anual de Cyber Threatscape por una revisión más frecuente que ayude a los responsables de tomar decisiones a planificar y actuar de forma más rápida.

En este primer número, destacamos las tendencias en ciberamenazas de principios de 2021 y las perspectivas de los expertos sobre las amenazas a los entornos de tecnología operacional (TO). En una era de incertidumbre sin precedentes, con tantos dispositivos distribuidos por las redes de las empresas, es un desafío para los profesionales en seguridad adaptarse al ritmo de las demandas en este campo.

Los incidentes de SolarWinds y Colonial Pipeline, las interrupciones a gran escala y el costo de las operaciones de secuestro de datos (ransomware) ilustran el impacto cada vez mayor de las ciberamenazas en el riesgo empresarial en todos los segmentos de la industria.
Este riesgo es cada vez más difícil de controlar y de mitigar tanto en los entornos de TI como de TO.

Si bien el funcionamiento de los sistemas industriales se ve facilitado por la virtualización en la nube y los avances de los dispositivos conectados a Internet, estas tecnologías también están introduciendo nuevas vulnerabilidades y riesgos en los entornos operacionales.

La crisis mundial del secuestro de datos ha entrado en una nueva fase a medida que los perpetradores de amenazas adoptan tácticas de presión más fuertes y procuran nuevos objetivos, en particular, la fabricación y la infraestructura crítica. El impacto del secuestro de datos se ha extendido y los ataques suelen poner de manifiesto las debilidades en la posición de seguridad de las empresas. No obstante, a pesar de que Colonial Pipeline ha admitido recientemente el pago de 4,4 millones de dólares[1], las víctimas no pueden asumir que el pago de un rescate restaurará los datos o evitará las fugas de información[2] y reconocen que el pago promedio por rescate ha caído de 110.532 dólares en septiembre de 2020 a 78.398 dólares en marzo de 2021.[3]

Como hemos visto con el ataque a SolarWinds, la seguridad de las cadenas de suministro de software y los vectores de ataque de terceros están en el punto de mira. En general, el secuestro de datos tiende a ser más rápido y diverso, lo que dificulta enormemente la defensa previa a la infección.

La gestión del riesgo empresarial es una tarea grupal que requiere una variedad de capacidades, un equipo cohesivo, una excelente ejecución de las tareas básicas y una buena disposición a adaptarse a condiciones cambiantes.

Los responsables en seguridad deben demostrar a los directivos y al consejo de administración no solo que entienden la criticidad de la continuidad de las operaciones, sino también la importancia de trabajar mancomunadamente con toda la empresa para gestionar el riesgo de manera eficaz.

Para obtener más información, consultá nuestra extensa biblioteca de seguridad a través de nuestros blogs de **Threat Intelligence**, **Cyber Defense** y **OT Security** y nuestra reciente cumbre de seguridad de la TO **Operation: Next**.

Howard Marshall

Howard Marshall
Managing Director, Accenture Security

Tendencias clave

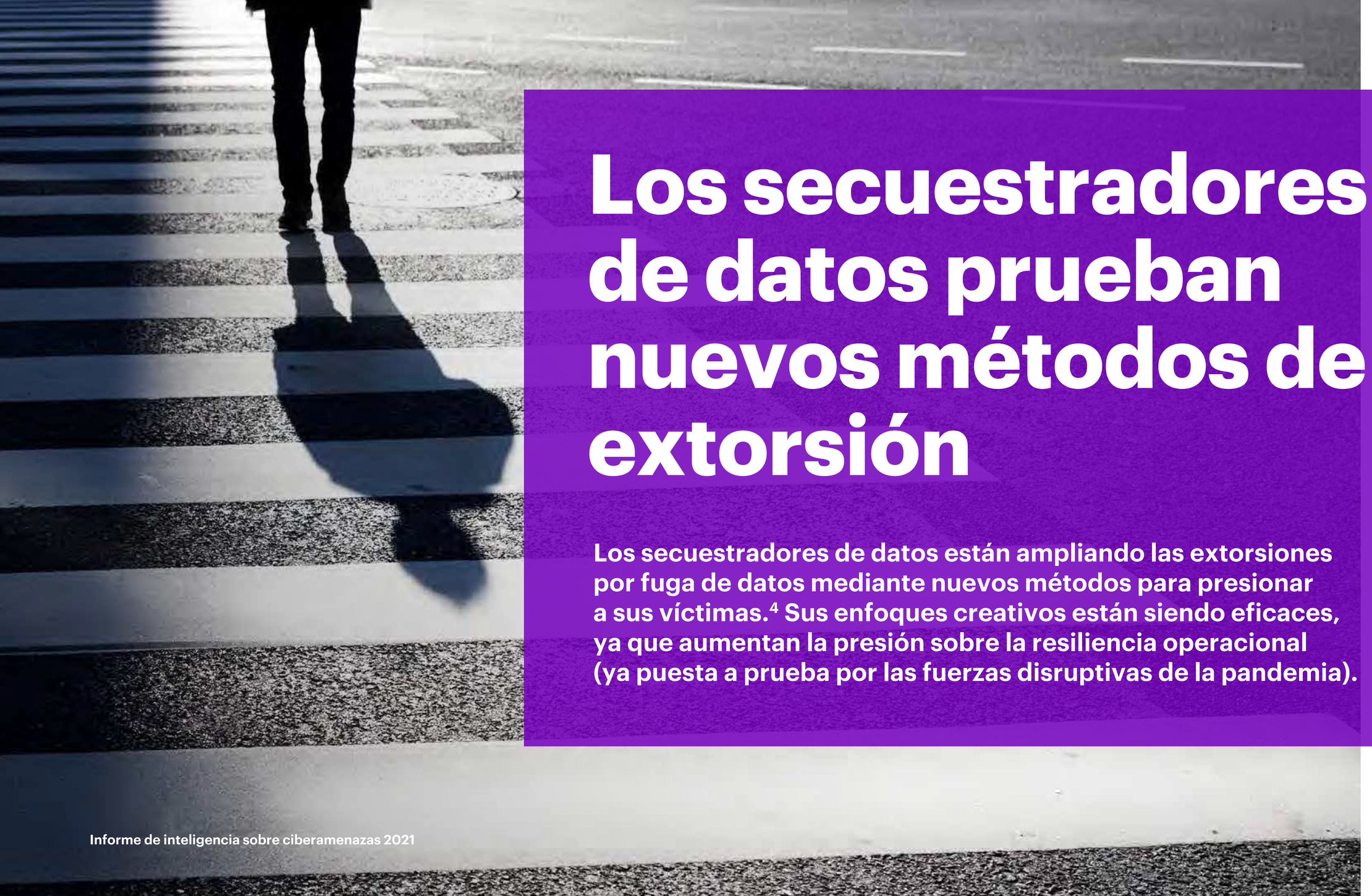
Tras el análisis realizado en el primer semestre de 2021, Accenture CTI identificó cuatro tendencias que están afectando a los entornos de TI y de TO:

Los secuestradores de datos prueban nuevos métodos de extorsión

Cobalt Strike está en auge

El crimeware de alto volumen puede invadir la TO desde el espacio de la TI

Los actores de la Dark Web desafían las redes de TI y TO



Los secuestradores de datos prueban nuevos métodos de extorsión

Los secuestradores de datos están ampliando las extorsiones por fuga de datos mediante nuevos métodos para presionar a sus víctimas.[4] Sus enfoques creativos están siendo eficaces, ya que aumentan la presión sobre la resiliencia operacional (ya puesta a prueba por las fuerzas disruptivas de la pandemia).

Los actores de las amenazas se enfocan en nuevos sectores y usan tácticas de mayor presión para escalar las consecuencias de la infección y desplegar las cargas útiles con rapidez para que los métodos de detección más fiables no lleguen a detectarlas. Las opciones de repsuesta son cada vez más complicadas.

Las organizaciones deben centrarse en la preparación, la prevención y las defensas previas a la encriptación.

¿Qué está ocurriendo?

Los objetivos están cambiando

Los pequeños fabricantes siguen siendo los blancos típicos,[5] pero los casos de los primeros meses de 2021 se han enfocado en infraestructuras críticas —el secuestro de datos a Colonial Pipeline de mayo de 2021 paralizó la distribución de combustible en gran parte del sureste de Estados Unidos— y en proveedores upstream como las compañías de seguros que cuentan con abundantes datos.[6] Los operadores de secuestros de datos interrumpen la producción en organizaciones que no pueden permitirse detener su actividad y se sienten presionadas para pagar los rescates. Un grupo de atacantes aprovechó el producto de un proveedor de la nube para vulnerar entidades jurídicas, de transporte, geofísicas y logísticas.[7]

Las tácticas se endurecen

Los secuestradores de datos suelen prometer que desencriptarán los sistemas de sus víctimas y destruirán los datos robados tras recibir el rescate[8], pero estas promesas son poco fiables. El negociador de ransomware de Coveware reportó múltiples casos de fines de 2020 en los que los datos se destruyeron en lugar de encriptarse, impidiendo su recuperación incluso tras el pago del rescate.[9] Otro grupo extorsionó a sus víctimas y publicó los datos robados sin siquiera desplegar el ransomware, ya que aparentemente consideraba que la exposición era más intimidante para sus víctimas que la inutilización de sus máquinas.[10]

La extorsión se vuelve personal
Las nuevas tácticas de exposición, iniciadas en 2020, han ido ganado terreno. Así, la extorsión por fuga de datos agrega a la lista de responsabilidades de las víctimas el temor al daño en su reputación. Un informe ha bautizado como "extorsión cuádruple" el accionar de ciertos grupos que no solo encriptan archivos y amenazan con filtrar datos, sino que también amenazan con ataques de denegación de servicio distribuido (DDoS)[11 12 13] a los que no pagan o bien se ponen en contacto con los clientes o socios comerciales de las víctimas, instándolos a que los presionen para que paguen los rescates.[14 15 16 17] DarkSide, el grupo cuyo ransomware el FBI ha señalado como responsable del ataque a Colonial,[18] es uno de los primeros en ofrecer los cuatro servicios como parte de su servicio de afiliación.[19] Los atacantes que se valen de Clop se centraron en la información de los altos directivos y buscaron material para realizar el chantaje.[20]

Los operadores del ransomware Babuk se han unido a los que utilizan Clop y Snatch para obtener una mayor exposición de los datos robados de sus víctimas con comunidades activistas antisistema.[21] Después de que el pirateo de Colonial Pipeline llevara a los administradores de los principales foros clandestinos a prohibir que se hablara de ransomware, Babuk anunció una nueva plataforma en la que cualquiera podía publicar los datos robados.[22]

Las tácticas, técnicas y procedimientos (TTP) son más avanzadas
Los secuestradores de datos están desarrollando rápidamente nuevas herramientas y técnicas. Los perpetradores explotan nuevas vulnerabilidades, por ejemplo, mecanismos alternativos de distribución, como el hosting de terceros.[23] Accenture CTI identificó notables tácticas de evasión defensiva para operadores del ransomware Hades, que se valen de herramientas y acciones desde el teclado para desactivar las defensas de los endpoints.[24]

¿Qué será lo próximo?

Cómo ayudar a afrontar el impacto del secuestro de datos:

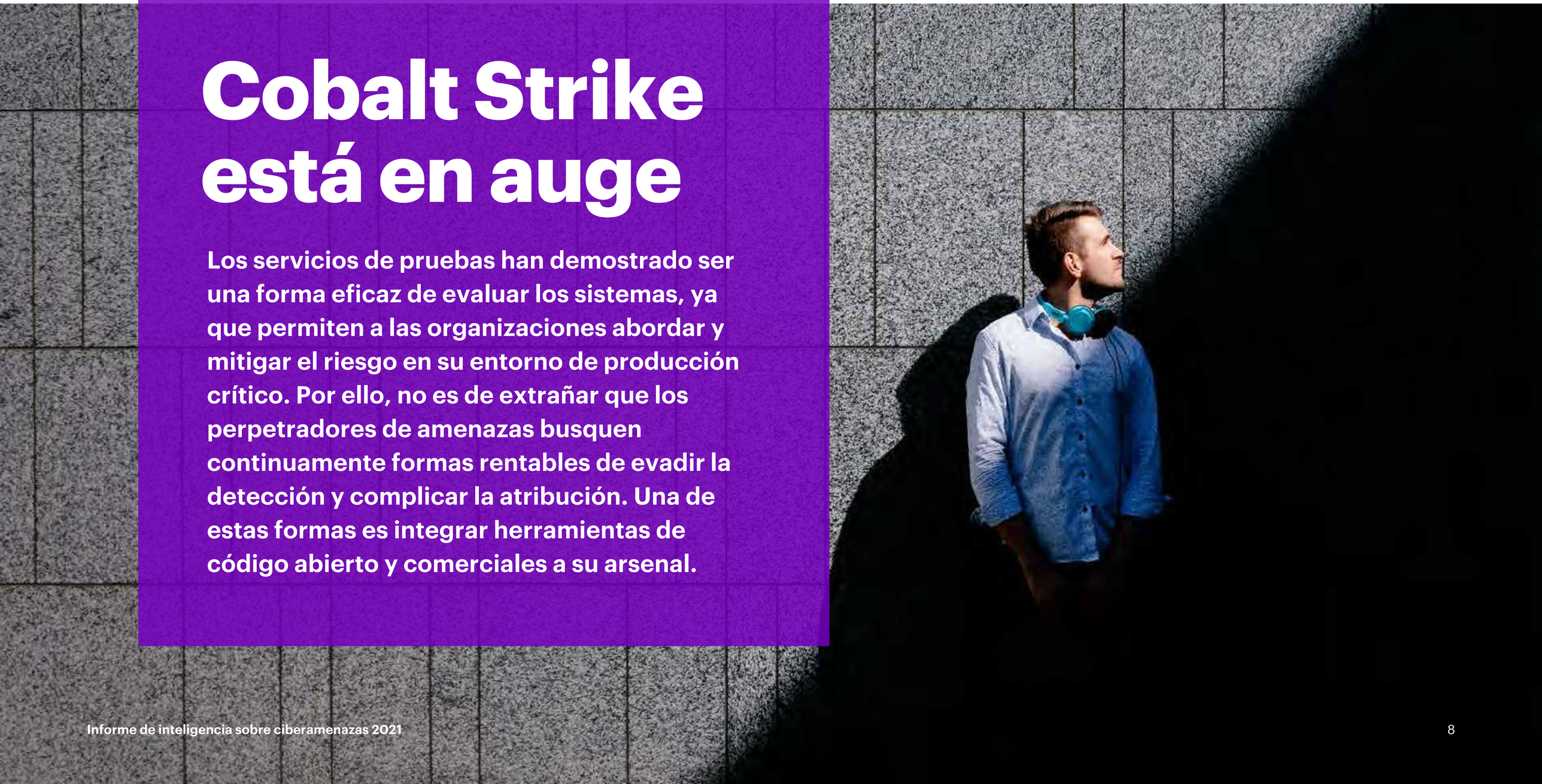
- **Cortar los ataques de raíz:** Las organizaciones enfocadas en la defensa previa a la preparación, la prevención y la encriptación pueden afrontar con mayor eficacia la crisis del ransomware.[25 26] La segregación y las medidas de confianza cero pueden limitar los movimientos de los perpetradores de amenazas en caso de que se produzcan brechas.

- **Colaborar e informar:** Colaborar con los socios de la industria, los consorcios y las fuerzas de seguridad para lograr un mayor conocimiento de las amenazas.

- **Actualizar los planes de riesgo y mitigación:** Aplicar una estrategia de mitigación de riesgos adecuada que incluya aspectos como el despliegue de controles o los mecanismos de transmisión segura de datos.

Cobalt Strike está en auge

Los servicios de pruebas han demostrado ser una forma eficaz de evaluar los sistemas, ya que permiten a las organizaciones abordar y mitigar el riesgo en su entorno de producción crítico. Por ello, no es de extrañar que los perpetradores de amenazas busquen continuamente formas rentables de evadir la detección y complicar la atribución. Una de estas formas es integrar herramientas de código abierto y comerciales a su arsenal.



Desde al menos diciembre de 2020, Accenture CTI ha observado, a partir de investigaciones internas y de informes públicos,[27] un notable aumento en los actores de amenazas que utilizan versiones piratas de la solución comercial de pruebas de penetración Cobalt Strike.

Este software pirata ha permitido realizar campañas de gran impacto, entre ellas los ataques recientemente descubiertos a SolarWinds, así como los prolíficos ataques del ransomware de tipo "name-and-shame", que amenazan con publicar información de sus víctimas.

Accenture CTI invierte importantes recursos en herramientas que identifican, desencriptan y rastrean las configuraciones de Cobalt Strike en hábitats naturales.[28]

El componente de puerta trasera Beacon de Cobalt Strike contiene marcas de agua comerciales que permiten a los analistas monitorear las campañas y detectar tendencias en las ubicaciones de las versiones Cobalt Strike crackeadas o pirateadas.

Los debates públicos en torno al éxito prolífico de una herramienta maliciosa suelen dar lugar al desarrollo de nuevas técnicas de detección de seguridad, que lleva a los perpetradores de amenazas a equiparse con nuevas herramientas. Sin embargo, debido a numerosos factores, como el aumento de la personalización, el uso abusivo del exitoso Cobalt Strike aumenta la popularidad de la herramienta pirateada, una tendencia que seguramente continuará a lo largo de 2021.

Las organizaciones necesitan adoptar nuevas herramientas defensivas que puedan contrarrestar esta amenaza creciente.

¿Qué está ocurriendo?

Cobalt Strike está proliferando

Aunque la plataforma se utiliza desde hace más de una década, el número de ataques con Cobalt Strike aumentó supuestamente un 163 % entre 2019 y 2020.[29] La aparición de Cobalt Strike pirateado que se utiliza de forma abusiva como una alternativa al malware se debe a numerosas razones.

Además de ser cada vez más accesible, las versiones recientes de Cobalt Strike son más personalizables que las anteriores. Como observó Accenture CTI en la brecha reciente de SolarWinds,[30] los perpetradores de amenazas están explotando la maleabilidad de comando y control de Cobalt Strike para personalizar la configuración predeterminada del elemento de puerta trasera Beacon y así evitar la detección.

Las herramientas de ataque están evolucionando

Los perpetradores de las amenazas están personalizando sus propios cargadores para lanzar Cobalt Strike. En particular, los atacantes desarrollaron varios cargadores personalizados de Cobalt Strike para facilitar la campaña contra SolarWinds.[31] Accenture CTI ha observado que la popularidad de la herramienta ha aumentado en los tres primeros meses de 2021.

Más allá de la intensificación del uso de Cobalt Strike por parte de grupos oportunistas de ransomware que utilizan la técnica de "name and shame" como REvil (también conocido como Sodinokibi) y Egregor, los operadores de ransomware Hades también han abusado de la herramienta para desplegar su ransomware.[32] Estos ataques de ransomware afectaron a múltiples víctimas entre diciembre de 2020 y marzo de 2021.

Accenture CTI también observó una carga útil del tipo Beacon con Cobalt Strike en el malware alojado en la infraestructura, probablemente asociada con el nuevo grupo de ciberespionaje HAFNIUM.[33] Al parecer, HAFNIUM utilizó ataques de día cero contra vulnerabilidades críticas de Microsoft Exchange, que Microsoft reveló públicamente en marzo de 2021.[34]

El malware se está fusionando

Accenture CTI ha identificado superposiciones entre la infraestructura del malware de robo de información EvilGrab y el Beacon de Cobalt Strike en la actividad de principios de 2021.[35] Existe una posibilidad concreta de que las superposiciones observadas entre EvilGrab y Cobalt Strike sean precursoras para que grupos sofisticados que han utilizado EvilGrab en el pasado adopten Cobalt Strike contra nuevos objetivos en lo que queda de 2021.

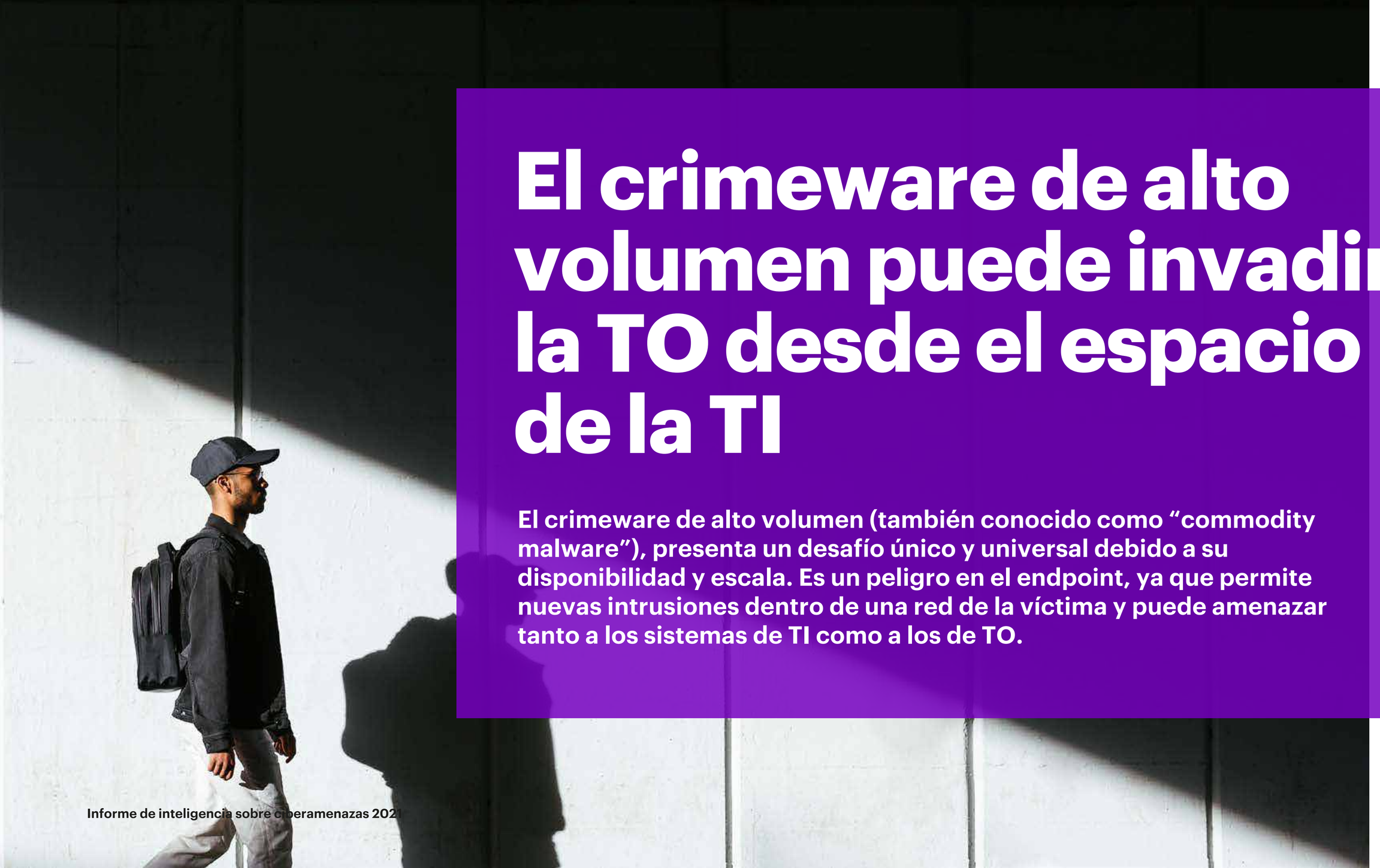
¿Qué será lo próximo?

Para ayudar a hacer frente al impacto de las amenazas a las estructuras de pruebas, debemos:

- **Realizar un análisis de la red:** Monitorear la presencia de marcas de agua de Beacon en las muestras de Cobalt Strike para encontrar y entender las nuevas campañas de Cobalt Strike y defenderse mejor contra las TTP que son tendencia.

- **Familiarizarse con la actividad de Cobalt Strike:** Aprender cómo las experiencias pasadas pueden ayudar a hacer frente a la amenaza.

- **Reforzar la postura de defensa:** Emplear nuevas herramientas de defensa para seguir el ritmo de la evolución de los desafíos.



El crimeware de alto volumen puede invadir la TO desde el espacio de la TI

El crimeware de alto volumen (también conocido como “commodity malware”), presenta un desafío único y universal debido a su disponibilidad y escala. Es un peligro en el endpoint, ya que permite nuevas intrusiones dentro de una red de la víctima y puede amenazar tanto a los sistemas de TI como a los de TO.

QakBot, IcedID, DoppelDridex y Hancitor son ejemplos de amenazas de crimeware de alto volumen que siguen activas en febrero y marzo de 2021. El equipo de reconocimiento de actividades clandestinas de Accenture CTI rara vez ha visto a los perpetradores de amenazas vender estos tipos de malware en la Dark Web porque los actores pertinentes mantienen el malware seguro, lo que reduce las oportunidades de identificar las campañas de spam de forma temprana.

Las organizaciones deben considerar la prevención, por encima de la respuesta, para defenderse eficazmente contra el crimeware de alto volumen.

¿Qué está ocurriendo?

El commodity malware de primera fase es una amenaza notable porque permite el despliegue de más malware en el endpoint. Los atacantes usan commodity malware de seguimiento, como instancias de Cobalt Strike pirateadas y abusadas para aumentar el riesgo de que la infección se extienda por toda la infraestructura de una organización e incluso llegue a los activos de TO.

Estas son algunas de las campañas de malware activas observadas por Accenture CTI:

Qakbot e IcedID
Según la investigación de Accenture CTI, en marzo de 2021, los actores de amenazas utilizaron campañas de spam de gran volumen para enviar crimeware a través de documentos de Excel comprimidos.

Las macros maliciosas incrustadas en los documentos de Excel descargan el crimeware desde URLs con rutas que terminan en "[0-9]{5},[0-9]{9,10}.dat." Valiéndose de un conjunto de actividades de muestra, los analistas de Accenture CTI observaron la descarga de cargas útiles tanto de Qakbot como de IcedID durante estas campañas. Un alto porcentaje de las cargas útiles eran de Qakbot, un malware duradero que data de 2007 y que puede actuar como una puerta trasera. La DLL Gziploader de IcedID envía información desde el sistema de la víctima a su servidor C2 junto con los parámetros de cookies HTTP de IcedID "_gads" y "_gat" y el servidor C2 devuelve la carga útil principal de IcedID, que es un troyano bancario que también actúa como descargador para desplegar el malware de seguimiento.[36]

DoppelDridex
Una importante campaña de spam de marzo de 2021 atraía a los usuarios con un correo electrónico que aparentaba ser de intuit[.]com. Los correos electrónicos de esta campaña incluían asuntos como "Factura/recibo de venta" y "Recibo de orden de compra" y archivos adjuntos con nombres como "Recibo_de_pago [número].xls". El archivo adjunto malicioso de Excel contenía dos hojas ocultas con cadenas invisibles en la celda A15. Al ejecutarse, una macro decodificaba múltiples URLs, descargaba el cargador DoppelDridex de las URLs y lo ejecutaba a través del proceso regsvr32 de Windows; a continuación, el cargador descargaba el malware DoppelDridex incrustado en la memoria y lo ejecutaba.[37] Los atacantes que se separaron del grupo responsable de Bitpaymer y Dridex alegaron haber creado el malware DoppelDridex.[38]

Hancitor
En febrero y marzo de 2021, campañas de spam distribuyeron el commodity malware Hancitor.
Los atacantes difundieron Hancitor a través de correos electrónicos con un formato de orden de DocuSign y enlaces a URLs de Google Docs que alojaban documentos de Microsoft Word maliciosos. Los documentos de Word descargaban una DLL de Hancitor incrustada en los sistemas de las víctimas. Hancitor establecía contacto con el dominio C2 api.ipify[.]org para informar la dirección IP externa de la máquina establecida como objetivo, se contactaba con su C2 en las URL utilizando la ruta "/8/forum.php" y descargaba el Ficker Stealer en los dominios .ru. Hancitor también podía entregar el malware Cobalt Strike si el sistema víctima tenía un entorno Microsoft Active Directory.[39] La actividad de Hancitor está relacionada con el grupo de amenazas MAN1, una empresa criminal que Accenture CTI ha vinculado con el malware bancario Dyre.[40]

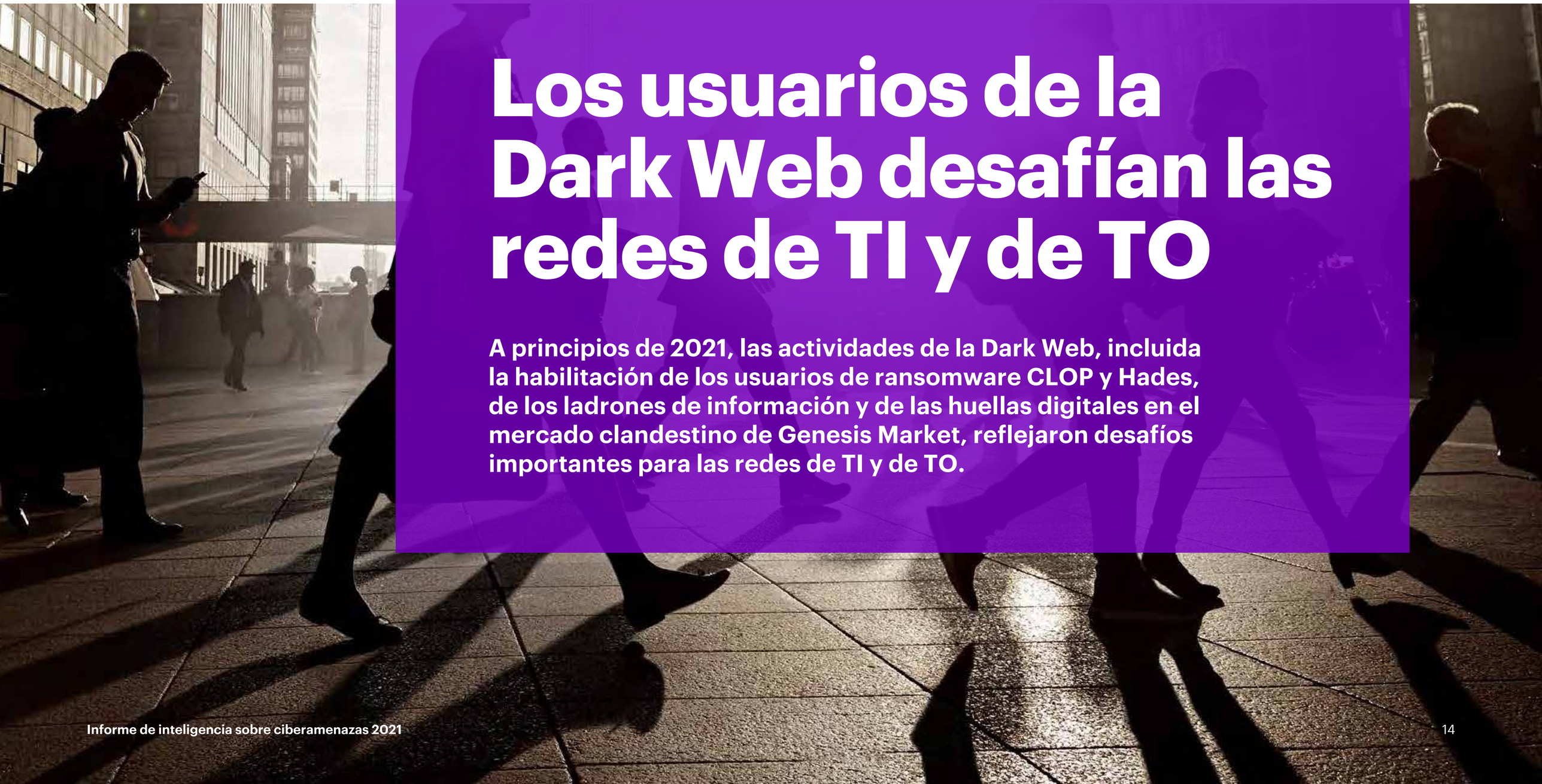
¿Qué será lo próximo?

Para ayudar a hacer frente al impacto del commodity malware en los entornos de TO, debemos:

• Parchear los sistemas de los endpoints, aplicar un cortafuegos a los posibles vectores de infección, actualizar el software antivirus, mantener copias de seguridad fuera de línea o aisladas y utilizar listas blancas de aplicaciones.

• Llevar a cabo regularmente programas de concienciación sobre phishing (suplantación de identidad) para todo el personal, segmentar los dominios de Active Directory por función o criticidad y mantener un principio de mínimo privilegio para cada grupo de usuarios y cuentas.

• Eliminar o desactivar los servicios que suelen verse atacados y que no son esenciales, si se considera oportuno.



Los usuarios de la Dark Web desafían las redes de TI y de TO

A principios de 2021, las actividades de la Dark Web, incluida la habilitación de los usuarios de ransomware CLOP y Hades, de los ladrones de información y de las huellas digitales en el mercado clandestino de Genesis Market, reflejaron desafíos importantes para las redes de TI y de TO.

A principios de 2021, las actividades de la Dark Web, incluida la habilitación de los usuarios de ransomware CLOP y Hades, de los ladrones de información y de las huellas digitales en el mercado clandestino de Genesis Market, reflejaron desafíos importantes para las redes de TI y de TO.

A medida que los perpetradores de amenazas se congregan en foros de la Dark Web para compartir e intercambiar herramientas, TTPs y datos de las víctimas, están mejorando sus tácticas de presión, aprendiendo a eludir las protecciones de seguridad y encontrando nuevas formas de monetizar los registros de malware.

Las organizaciones necesitan compartir información entre los defensores para comprender, prevenir, identificar y responder a la actividad de las amenazas.

¿Qué está ocurriendo?

Los actores del ransomware CLOP y Hades están cambiando las reglas del juego

Los informes públicos de principios de 2021 vincularon a los perpetradores del ransomware CLOP con una serie de vulneraciones de datos globales que explotaban una vulnerabilidad recientemente descubierta en el ampliamente utilizado Accellion File Transfer Appliance (FTA).[41] Tras revisar la cronología de los ataques al FTA de Accellion, las listas "name-and-shame" de CLOP en la Dark Web, las declaraciones de las víctimas y los insights de las iniciativas de respuesta a incidentes de Accenture, Accenture CTI concluyeron que los usuarios del ransomware CLOP probablemente se asociaron con los responsables de explotar la vulnerabilidad del FTA de Accellion.[42] [43] [44] [45] La rentabilidad y la gestión de las víctimas a escala podrían dar lugar a incrementos de los ataques y a imitaciones en el transcurso del año.

Los usuarios del ransomware Hades también ganaron terreno a principios de 2021 y demostraron su capacidad para eludir las herramientas de detección y respuesta de endpoints (EDR)[46] y llegar a los dispositivos perimetrales.[47] Los usuarios de Hades desactivaron manualmente las defensas o utilizaron herramientas personalizadas para evadirlas; este conjunto de habilidades podría amenazar las redes de TO.[48]
Accenture CTI considera que los usuarios del ransomware Hades son unos de los grupos más peligrosos tanto para las redes de TI como las de TO, dado que eluden las EDR. Los esquemas de los operadores abarcan ahora la captura y la encriptación de los datos de la empresa y el paso de las redes de TI a las de TO.

Los operadores de ransomware rara vez tienen éxito cuando intentan comprometer las redes de TO, pero puede que ni siquiera necesiten hacerlo para lograr sus objetivos. Tanto en el ataque de febrero de 2021 al constructor de barcos Beneteau como en el de mayo de 2021 a Colonial Pipeline, la mera presencia de los atacantes dentro de la red de TI forzó apagados preventivos de la TO y provocó efectos a corto plazo comparables a una infección de la TO. Apagar la TO, aunque sea una medida preventiva, quizás se vuelva más habitual en futuros ataques contra organizaciones dependientes de TO.[49] [50]

La información es fácil de comprar y aún más fácil de usar

Desde principios de 2021, Accenture CTI ha observado un ligero, pero notable aumento en la actividad de atacantes que venden registros de malware, los que forman parte de datos derivados del malware de robo de información.[51] Los ladrones de información pueden recopilar y registrar una gran cantidad de información sensible del sistema, del usuario y de la empresa, como por ejemplo:

- Información del sistema
- Marcadores del navegador web
- Cookies de la sesión web
- Credenciales de inicio de sesión (sitios web, protocolo de escritorio remoto (RDP), protocolo de shell seguro (SSH))
- Datos de tarjetas de pago
- Direcciones de carteras de criptomonedas

Un atacante puede utilizar los registros de malware para hacerse pasar por un usuario legítimo de la red y evitar ser detectado, obteniendo el acceso inicial al sistema de la víctima mediante el uso de credenciales válidas. Los perpetradores de amenazas suelen utilizar los registros de malware para acceder a los recursos web de una organización e intentar acceder a cuentas de administrador con privilegios, en los servidores web de la organización. En algunos casos, pueden intentar acceder a las computadoras de la red de la víctima a través de servicios como RDP o SSH. Una acción alternativa común es que los atacantes vendan los registros de malware directamente a los hackers, o que los vendan en masa a los mercados de "registros de malware" de la Dark Web, como Genesis Market o Russian Market.

Accenture CTI considera que los registros de malware que los usuarios de la Dark Web venden en Genesis Market suponen una amenaza especialmente grave para los activos de TI y de TO de las organizaciones. Genesis Market ha reducido drásticamente las barreras de entrada para la explotación de registros de malware al compilar y vender registros de malware en un formato que los anuncios de Genesis denominan "bots" o "plug-ins". Incluso los actores de amenazas con menos conocimientos técnicos pueden utilizar intuitivamente un complemento con el navegador web de libre acceso de Genesis.

¿Qué será lo próximo?

Para ayudar a afrontar el impacto de la Dark Web en las redes de TO, debemos:

- **Llevar a cabo un monitoreo responsable:** Buscar alertas tempranas de posibles accesos no autorizados a través de un monitoreo responsable de la Dark Web, ya sea directamente o mediante un proveedor de inteligencia sobre ciberamenazas.
- **Aumentar el intercambio de inteligencia sobre el análisis de respuesta a incidentes:** Compartir información para identificar las firmas de las amenazas y su atribución, planificar y ejecutar la defensa y la respuesta y preparar la defensa de la red y las operaciones de negocio para una futura actividad de las amenazas.
- **Preparar un plan de continuidad de las operaciones:** Anticipar y desarrollar planes de contingencia para un posible robo de credenciales de administrador, una derivación de los sistemas de EDR y apagados físicos (ya sea como medida preventiva o reactiva), para preparar las operaciones de la red y del negocio para futuras apariciones de un ransomware o eventos similares.

En el punto de mira: al borde de la seguridad

Los dispositivos perimetrales, tales como los objetos del Internet de las Cosas (IoT), los conmutadores y los enrutadores, operan en el límite de una red para controlar los datos que fluyen dentro y fuera de la organización. En la frontera entre los entornos de TI y de TO, son fundamentales para la seguridad de la TO, ya que las brechas pueden suponer un acceso directo a los entornos de TO, eludiendo por completo las redes de TI.

Sin embargo, los bajos índices de monitoreo de la red[52] dificultan la identificación de los vectores de ataque y las causas de la intrusión por parte de los responsables de la respuesta a incidentes en el ámbito de la TO y les impiden elaborar recomendaciones sobre cómo proteger los sistemas de TO. Como resultado, asegurar los dispositivos perimetrales se ha convertido en algo tan importante como la seguridad de los propios sistemas de control industrial (ICS).

La política importa. El 4 de diciembre de 2020, el expresidente Trump firmó la Ley de Mejora de la Ciberseguridad del Internet de las Cosas de 2025.[53] Esta ley alienta a las agencias gubernamentales a trabajar en colaboración para que las políticas de seguridad del IoT sean coherentes con las recomendaciones del Instituto Nacional de Estándares y Tecnología (NIST).[54] La ley promete una mayor seguridad para los dispositivos perimetrales y aborda algunos desafíos de larga data. El 12 de mayo de 2021, el Presidente Biden firmó la Orden Ejecutiva sobre la Mejora de la Ciberseguridad de la Nación que incluye instrucciones para crear programas piloto de etiquetado de ciberseguridad para educar a los ciudadanos sobre las capacidades de seguridad de los dispositivos de IoT y las prácticas de desarrollo de software.[55]

Las políticas estrictas sobre dispositivos perimetrales pueden incentivar a las organizaciones a asignar fondos de muchas partes de la empresa para reforzar las iniciativas de seguridad. Si se invierte en los lugares adecuados, los responsables de la seguridad pueden proteger los dispositivos perimetrales en entornos de TO mediante una combinación de monitoreo, respuesta e inteligencia.

Abordar los dispositivos perimetrales

En febrero de 2021, Accenture CTI descubrió que un perpetrador de amenazas anunciaba el acceso de la VPN de Citrix a una “gran corporación de recursos” en un reputado foro en lengua rusa especializado en malware y ransomware.[56] Citrix es una puerta de enlace VPN que suele colocarse en los límites de la TO para conectar y correlacionar varios protocolos de Internet de diferentes redes.

Los atacantes suelen acceder a redes y sistemas vulnerables como Citrix explotando vulnerabilidades conocidas que no tienen parches o que los proveedores aún están parcheando. A fines de 2019, la campaña de amenazas aún activa conocida como Fox Kitten (también conocida como UNC757)[57] accedió a empresas de varios sectores, incluido el energético, a través de vulnerabilidades de VPNs n-day[58]

Los ciberdelincuentes con motivaciones financieras han utilizado el acceso a las VPN para lanzar un ataque de ransomware y dirigirlo a los sistemas de TO: saben que los fabricantes y otros usuarios de ICS son especialmente vulnerables al tiempo de inactividad y pueden ser más proclives a pagar rescates para que sus sistemas vuelvan a estar en línea.

Por su parte, los perpetradores de las amenazas de ciberespionaje pueden utilizar el acceso a las VPN para entrar en las redes de TO y robar datos o esconderse con la intención de lanzar un ataque destructivo más adelante. Ambos tipos de atacantes pueden acceder a los dispositivos perimetrales, lo cual podría conducir a la interrupción de las operaciones críticas de negocio y a la pérdida de ingresos.

Defender los dispositivos perimetrales

Estas son algunas capacidades de seguridad conocidas que las organizaciones pueden utilizar para aumentar la seguridad de sus dispositivos perimetrales:

Centro de Operaciones de Seguridad (SOC) de TO
A diferencia de un SOC tradicional que se enfoca principalmente en los activos de TI, un SOC de TO monitoriza los eventos de seguridad tanto en los entornos de TI como de TO para obtener visibilidad de las amenazas y los riesgos. El monitoreo de los dispositivos perimetrales en el límite de un entorno de TO es un componente clave para la ciberseguridad general y la ciberresiliencia. Un SOC de TO junto con un sistema de detección y respuesta gestionada (MDR) puede ayudar a defenderse de las ciberamenazas y reducir la exposición a las mismas.[59]

Respuesta a incidentes (IR) de TO
La IR de la TO es esencial para descubrir cómo acceden los perpetradores de las amenazas a los entornos de TO a través de los dispositivos perimetrales si se produce una brecha de seguridad. Obtener un insight de cómo los atacantes acceden a los dispositivos perimetrales y atraviesan un entorno de TO permite a una entidad asegurar las fronteras de sus TI y TO. Los datos obtenidos de las actividades de IR de la TO también pueden ayudar a informar los ejercicios de los red teams para identificar las vulnerabilidades de los dispositivos perimetrales antes de que se pr19oduzca una brecha. La IR de la TO es un componente clave de la seguridad en el contexto de la convergencia de la TO y la TI, así como de la seguridad operativa en su conjunto.

Inteligencia sobre ciberamenazas (CTI)
La inteligencia sobre ciberamenazas tradicional proporciona información sobre los perpetradores que atacan a las TI o a las TO, pero suele abordar solamente la seguridad de los dispositivos perimetrales durante el despliegue de los sistemas altamente especializados. Accenture CTI lleva la seguridad de TO un paso más allá con inteligencia de vulnerabilidades clave y monitoriza los principales dispositivos perimetrales, sus proveedores y sus números de versión para que los clientes sean conscientes de las amenazas para sus entornos de TI, de TO y en la nube.

Accenture CTI ofrece una mejor visibilidad de las amenazas generales a la red e informa a los responsables de la toma de decisiones sobre cómo priorizar la seguridad en torno a posibles objetivos y amenazas.

Dado que las vulnerabilidades de los dispositivos perimetrales como blancos de ataque van en aumento, es fundamental que las organizaciones empiecen a cambiar sus culturas de seguridad y pasen de ser reactivas a adoptar un enfoque proactivo de la seguridad perimetral.

References

1. Eaton, Collin and Volz, Dustin, "Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom" ("El director de Colonial Pipeline cuenta por qué pagó a los hackers un rescate de 4,4 millones de dólares"), Wall Street Journal, 19 de mayo de 2021.

2. "Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands" ("Los pagos por ransomware caen mientras menos empresas pagan las demandas de extorsión por filtración de datos"), Coveware, 1 de febrero de 2021.

3. "Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound" (Los vectores de ataque del ransomware cambian a medida que proliferan los nuevos exploits de vulnerabilidad del software"), Coveware, 26 de abril de 2021.

4. "Informe Cyber Threatscape 2020" Accenture, 19 de octubre de 2020. Mansfield, Paul, "Tracking and combatting an evolving danger: Ransomware extortion" ("Seguimiento y lucha contra un peligro en evolución: la extorsión del ransomware"), Accenture, 15 de diciembre de 2020.

5. Accenture Cyber Threat Intelligence, "Ransomware Roundup from iDefense Analysis" ("Resumen de ransomware del iDefense Analysis"), 8 de abril de 2021. Informes de IntelGraph.

6. Accenture Cyber Threat Intelligence, "Ransomware Attack on Cyber Insurer Highlights Risks to Cyber Insurance Sector and its Customers" ("El ataque de ransomware a una ciberaseguradora pone de manifiesto los riesgos para el sector de los ciberseguros y sus clientes"), 8 de abril de 2021. Informes de IntelGraph.

7. Accenture Cyber Threat Intelligence, "CLOP Ransomware Operators Leak CGG Data on Name-and-Shame Site on 1 March 2021" ("Los operadores del ransomware CLOP filtran datos CGG en un sitio 'name-and-shame' el 1 de marzo de 2021"), 10 de marzo de 2021. Informe de IntelGraph; Accenture Cyber Threat Intelligence, "CLOP Ransomware Operators Leakers CSX Documents on Name-and-Shame Site on 2 March 2021" ("Los operadores del ransomware CLOP filtran documentos CSX en un sitio 'name-and-shame' el 2 de marzo de 2021"), 10 de marzo de 2021. Informes de IntelGraph.

8. Mansfield, Paul, "Tracking and combatting an evolving danger: Ransomware extortion" (Seguimiento y lucha contra un peligro en evolución: la extorsión por ransomware"), 15 de diciembre de 2020, Kodzhibaev, Azim et al, "Interview with a Lockbit Ransomware Operator" ("Entrevista con un operador del ransomware Lockbit"), Talos, 4 de enero de 2021.

9. "Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands", Coveware, 1 de febrero de 2021. El promedio de rescates pagados disminuyó un 34%, pasando de 233.817 dólares en el tercer trimestre a 154.108 dólares en el cuarto. "Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound"

10. Moore, Andrew et al, "Cyber Criminals Exploit Accellion FTA for Data Theft and Extortion" ("Los ciberdelincuentes aprovechan el FTA de Accellion para el robo de datos y la extorsión"), 22 de febrero de 2021. FireEye; Accenture Cyber Threat Intelligence, "SITREP: Accellion FTA", 20 de febrero de 2021. Informes de IntelGraph.

11. Accenture Cyber Threat Intelligence, "Ransomware Gang Extortion Techniques Evolve in 2020 to Devastating Effect" ("Las técnicas de extorsión de las bandas de ransomware evolucionan en 2020 con un efecto devastador"), 6 de noviembre de 2020 Informes de IntelGraph.

12. Mansfield, Paul, "Tracking and combatting an evolving danger: Ransomware extortion", 15 de diciembre de 2020.

13. "What We Know About the DarkSide Ransomware and the US Pipeline Attack" (Lo que sabemos sobre el ransomware DarkSide y el ataque al oleoducto estadounidense"), TrendMicro, 12 de mayo de 2021.

14. Accenture Cyber Threat Intelligence, "Ransomware Gang Extortion Techniques Evolve in 2020 to Devastating Effect", 6 de noviembre de 2020. Informes de IntelGraph.

15. Mansfield, Paul. "Tracking and combatting an evolving danger: Ransomware extortion". 15 de diciembre de 2020.

16. Accenture Cyber Threat Intelligence, "iDefense Global Research Intelligence Digest", 31 de marzo de 2021. Informes de IntelGraph

17. Abrams, Lawrence, "Ransomware gang plans to call victim's business partners about attacks" ("Una banda de ransomware planea informar sobre los ataques a los socios comerciales de las víctimas"), 6 de marzo de 2021. Smilianets, Dmitry, "'I scrounged through the trash heaps... now I'm a millionaire:' An interview with REvil's Unknown" ("'He buscado en los montones de basura, ahora soy millonario:' Una entrevista con el Desconocido REvil"), 16 de marzo de 2021.

18. "FBI Statement on Compromise of Colonial Pipeline Networks" ("Declaración del FBI sobre el compromiso de las redes de Colonial Pipeline"), FBI, 10 de mayo de 2021.

19. "What We Know About the DarkSide Ransomware and the US Pipeline Attack" Trend Micro, 14 de mayo de 2021.

20. Cimpanu, Catalin, "Some ransomware gangs are going after top execs to pressure companies into paying" ("Algunas bandas de ransomware van por los altos cargos para presionar a las empresas a pagar), 9 de enero de 2021.

21. Accenture Cyber Threat Intelligence, "Transparency Activists Publicize Ransomware Victims' Data in a New Twist on Hybrid Financial-Political Threat" ("Los activistas de la transparencia publican datos de las víctimas del ransomware en un nuevo giro de la amenaza híbrida financiero-política"), 8 de enero de 2021. Informes de IntelGraph.

22. Accenture Cyber Threat Intelligence, "Colonial Pipeline Attack Impacts Ransomware Groups Operating on the Dark Web" ("El ataque a Colonial Pipeline afecta a los grupos de ransomware que operan en la Dark Web"), 17 de mayo de 2021. Informes de IntelGraph.

23. Ilascu, Ionut, "Hackers use black hat SEO to push ransomware, trojans via Google" ("Los hackers utilizan el SEO de sombrero negro para difundir ransomware y troyanos a través de Google"), Bleeping Computer, 1 de marzo de 2021.

24. Welling, Eric, "It's getting hot in here! Unknown threat group using Hades ransomware to turn up the heat on their victims" ("¡Está haciendo calor aquí! Un grupo desconocido de atacantes utiliza el ransomware Hades para 'subir la temperatura' de sus víctimas"), Accenture, 26 de marzo de 2021.

25. Michael, Melissa, "Episode 49| Ransomware 2.0, con Mikko Hypponen" F-Secure, 19 de enero de 2021.

26. Toby L, "The rise of ransomware" ("El auge del ransomware"), National Cyber Security Centre, 29 de enero de 2021.

27.“Adversary Infrastructure Report 2020: A Defender’s View” (“Informe sobre Infraestructura Adversaria 2020: la visión de un defensor”), Recorded Future, 7 de enero de 2021.

28.Cunliffe, Amy, “The development of Mimir (Amy Cunliffe, Accenture)” (“El desarrollo de Mimir”) Videos CREST, 9 de abril de 2021.

29.“Threat Landscape Trends – Q3 2020” (“Tendencias del entorno de amenazas para el tercer trimestre de 2020”), Symantec, 18 de diciembre de 2020.

30.“Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor” (“Un atacante altamente evasivo aprovecha la cadena de suministro de SolarWinds para comprometer a múltiples víctimas globales con la puerta trasera SUNBURST”), FireEye, 13 de diciembre de 2020.

31.“Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop“ (Una visión detallada de la activación de segunda etapa de Solorigate: de Sunburst a Teardrop y Raindrop), Microsoft, 20 de enero de 2021.

32.Welling, Eric, “It’s getting hot in here! Unknown threat group using Hades ransomware to turn up the heat on their victims” Accenture, 26 de marzo de 2021.

33.Accenture Cyber Threat Intelligence, “Microsoft Exchange On-Premise Zero-Day Vulnerabilities Related Malware Activity in March 2021” (“Actividad de malware relacionada con las vulnerabilidades de día cero in situ de Microsoft Exchange en marzo de 2021”), 10 de marzo de 2021. Informes de IntelGraph.

34.“HAFNIUM targeting Exchange Servers with 0-day exploits“ (HAFNIUM apunta a los servidores Exchange con exploits de 0 días) Microsoft, 2 de marzo de 2021.

35.Accenture Cyber Threat Intelligence, “EvilGrab and Cobalt Strike Beacon Observed having Shared Infrastructure and Communicating” (“Se ha observado que EvilGrab y Cobalt Strike Beacon comparten infraestructura y se comunican”), 3 de febrero de 2021. Informes de IntelGraph.

36.Accenture Cyber Threat Intelligence, “Spam Campaign Distributes Gziploader to Deploy IcedID (a.k.a. BokBot) Malware in March 2021” (“Una campaña de spam distribuye Gziploader para desplegar el malware IcedID (también conocido como BokBot) en marzo de 2021”), 14 de abril de 2020. Informes de IntelGraph.

37.Accenture Cyber Threat Intelligence, “Technical Analysis of DoppelDridex” (“Análisis técnico de DoppelDridex”), 27 de abril de 2021. Informes de IntelGraph.

38.Stone-Gross, Brett; Frankoff, Sergei; and Hartley, Bex, “BitPaymer Source Code Fork: Meet DoppelPaymer Ransomware and Dridex 2.0” (“Bifurcación del código fuente de BitPaymer: conozca el ransomware DoppelPaymer y Dridex 2.0”), 12 de julio de 2019.

39.Accenture Cyber Threat Intelligence, “iDefense Global Research Intelligence Digest”, 6 de abril de 2021. Informes de IntelGraph.

40.Accenture Cyber Threat Intelligence, “MAN1,” 16 de julio de 2016. Informes de IntelGraph.

41.Seals, Tara, “Accellion FTA Zero-Day Attacks Show Ties to Clop Ransomware, FIN11” (“Los ataques de día cero del FTA de Accellion muestran vínculos con el ransomware Clop y FIN11”), Threatpost, 22 de febrero de 2021.

42.Accenture Cyber Threat Intelligence, “SITREP: Accellion FTA”, 5 de marzo de 2021. Informes de IntelGraph.

43.Accenture Cyber Threat Intelligence, “CLOP Ransomware Operators Leak Qualys Documents on Name-and-Shame Site on 3 and 4 March 2021” 4 de marzo de 2021. Informes de IntelGraph.

44.Accenture Cyber Threat Intelligence, “CLOP Ransomware Operators Leak CGG Data on Name-and-Shame Site on 1 March 2021”, 10 de marzo de 2021. Informe de IntelGraph.

45.Accenture Cyber Threat Intelligence, “CLOP Ransomware Operators Leakers CSX Documents on Name-and-Shame Site on 2 March 2021”, 10 de marzo de 2021. Informes de IntelGraph.

46.Welling, Eric, “It’s getting hot in here! Unknown threat group using Hades ransomware to turn up the heat on their victims” Accenture, 26 de marzo de 2021.

47.Accenture Cyber Threat Intelligence, “Hades Ransomware Affects Large Corporate Networks from December 2020 to March 2021” (“El ransomware Hades afecta a las grandes redes corporativas desde diciembre de 2020 hasta marzo de 2021”), 9 de abril de 2021. Informe de IntelGraph.

48.Accenture Cyber Threat Intelligence, “Hades Ransomware Affects Large Corporate Networks from December 2020 to March 2021” 9 de abril de 2021. Informes de IntelGraph.

49.Arghire, Ionut, “Boat Building Giant Beneteau Says Cyberattack Disrupted Production” (“El gigante de la construcción de barcos Beneteau dice que el ciberataque interrumpió su producción”), Security Week, 1 de marzo de 2021.

50.Bertrand, Natasha et al, “Colonial Pipeline did pay ransom to hackers, sources now say” (“Colonial Pipeline sí pagó el rescate a los hackers, dicen ahora las fuentes”), CNN, 13 de mayo de 2021.

51.Accenture Cyber Threat Intelligence, “Monthly Reconnaissance Report” (“Informe mensual de reconocimiento”), 1 de abril de 2021.

52.Filkins, Barbara, Wylie, Doug, “SANS 2019 State of OT/ICS Cybersecurity Survey” (“Encuesta SANS 2019 sobre el estado de la ciberseguridad de TO/ICS”), SANS, junio de 2019. Un poco más del 50% de los encuestados informó de un monitoreo continuo para detectar vulnerabilidades, y solo 1/3 de las 25 tecnologías de monitoreo de la seguridad TO/ICS evaluadas eran usadas por todos los encuestados.

53.Congreso de los Estados Unidos, “PUBLIC LAW 116–207—DEC. 4, 2020”, 4 de diciembre de 2020.

54.Congreso de los Estados Unidos, “PUBLIC LAW 116–207—DEC. 4, 2020”, 4 de diciembre de 2020.

55.Casa Blanca, “Executive Order on Improving the Nation’s Cybersecurity” (“Decreto ejecutivo para mejorar la ciberseguridad del país”), 12 de mayo de 2021.

56.Accenture Cyber Threat Intelligence, “Threat Actor... Advertise Compromised Citrix Access to Three Large Corporations” (“Perpetrador de amenaza anuncia el acceso comprometido de Citrix a tres grandes empresas”), 26 de febrero de 2021, Informe de IntelGraph.

57.“Groups” (Grupos), MITRE, con acceso el 27 de mayo de 2021.

58.“Fox Kitten Campaign” (Campaña de Fox Kitten”), Clearsky Cyber Security, 16 de febrero de 2020.

59.“Managed Security” (“Seguridad gestionada”), Accenture, con acceso el 4 de abril de 2020.

Contactos

Joshua Ray
Managing Director
Accenture Security

Josh Ray es Managing Director de Ciberdefensa en Accenture a nivel mundial. Josh tiene más de 20 años de experiencia combinada entre comercial, gubernamental y militar en el campo de la ciberinteligencia, las operaciones contra amenazas y la seguridad de la información. Es licenciado en tecnología de la información por la Universidad George Mason, tiene un certificado ejecutivo en estrategia e innovación de la Escuela de Administración y Dirección de Empresas Sloan del MIT y ha servido honorablemente como miembro de la Marina de los Estados Unidos.

Howard Marshall
Managing Director
Accenture Security

Howard Marshall es Managing Director de Accenture Cyber Threat Intelligence (CTI) y dirige el equipo a nivel mundial. Antes de incorporarse, Howard fue subdirector adjunto de la rama de preparación, divulgación e inteligencia cibernética del FBI. Es licenciado en Ciencias Políticas y doctor en Derecho de la Universidad de Arkansas.

Jayson Jean
Senior Manager
Accenture Security

Jayson Jean es Director of Business Operations de Accenture CTI en Norteamérica y la región de Asia y el Pacífico, con responsabilidad en el desarrollo comercial de la cartera de Inteligencia sobre Ciberamenazas. Antes de ejercer este cargo, Jayson trabajó 14 años construyendo la dirección estratégica y liderando el desarrollo de productos para la gestión de vulnerabilidades en Accenture CTI.

Christopher Foster
Senior Principal
Security Innovation

Chris Foster es Director of Product Strategy de Accenture Cyber Threat Intelligence. Chris cuenta con más de 18 años de experiencia combinada en el campo de la inteligencia sobre amenazas al servicio de organizaciones del sector público y privado, entre ellas Booz Allen Hamilton, Chevron, el Departamento de Defensa de los Estados Unidos y el Departamento de Seguridad Nacional de los Estados Unidos. Posee una licenciatura de la Universidad Vanderbilt y un MBA de la Escuela de Negocios McCombs de la Universidad de Texas en Austin.

Valentino De Sousa
Senior Principal
Security Innovation

Valentino De Sousa dirige Accenture Cyber Threat Intelligence en Europa. Es miembro del grupo de trabajo ad hoc de ENISA sobre entornos de ciberamenazas. Algunas de sus funciones anteriores incluyen la dirección de diferentes equipos de inteligencia sobre amenazas responsables del análisis de malware, investigación y desarrollo, análisis de adversarios, campañas activas e indicadores principales de ataques inminentes.
Es licenciado en administración de empresas por la Universidad Americana de Roma y tiene un máster en estudios sobre terrorismo de la Universidad de East London.

Colaboradores

Patton Adams, Will Archer, Adam Bumgarner, Bianca Forbes, Roya Gordon, Hannaire Mekaouar, Nellie Ohr, Max Smith, Nancy Strutt.

Acerca de Accenture

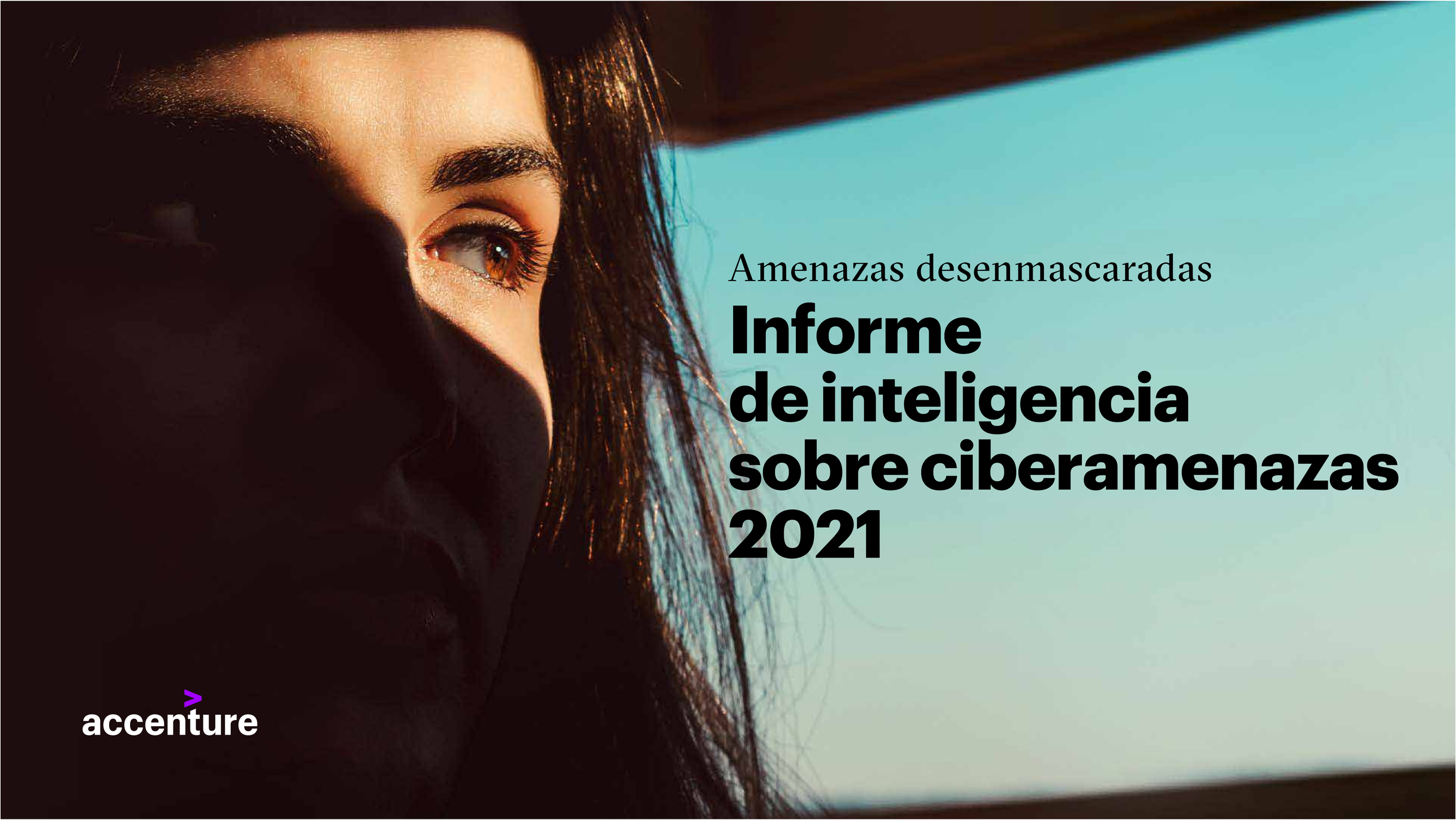
Accenture es una compañía global de servicios profesionales, líder en capacidades digitales, de nube y de seguridad. Combinamos una experiencia inigualable y habilidades especializadas en más de 40 sectores económicos, prestamos servicios de Estrategia y Consultoría, Interactivos, Tecnológicos y de Operaciones, impulsados por la red de centros de tecnología avanzada y operaciones inteligentes más grande del mundo.
Nuestros 674.000 empleados cumplen la promesa de la tecnología y el ingenio humano todos los días y prestan servicio a clientes en más de 120 países. Adoptamos el poder del cambio para crear valor y éxito compartido para nuestros clientes, profesionales, accionistas, socios y comunidades.
Visitanos en www.accenture.com

Acerca de Accenture Security

Accenture Security es un proveedor líder de servicios de ciberseguridad de extremo a extremo, que incluyen ciberdefensa avanzada, soluciones de ciberseguridad aplicada y operaciones de seguridad gestionadas. Ofrecemos innovación en seguridad, además de una escala global y una capacidad de entrega a nivel mundial a través de nuestra red de centros de tecnología avanzada y operaciones inteligentes. Con la colaboración de nuestro equipo de profesionales altamente capacitados, ayudamos a nuestros clientes a innovar de manera segura, desarrollar la resiliencia cibernética y crecer con confianza.
Seguinos en @AccentureSecure en Twitter o visitanos en www.accenture.com/security

12460906

210353



Amenazas desenmascaradas

Informe de inteligencia sobre ciberamenazas 2021

accenture