TREND MICRO | research

TURNING THE TIDE

Predicciones de seguridad de Trend Micro para 2021

TURNING THE TIDE

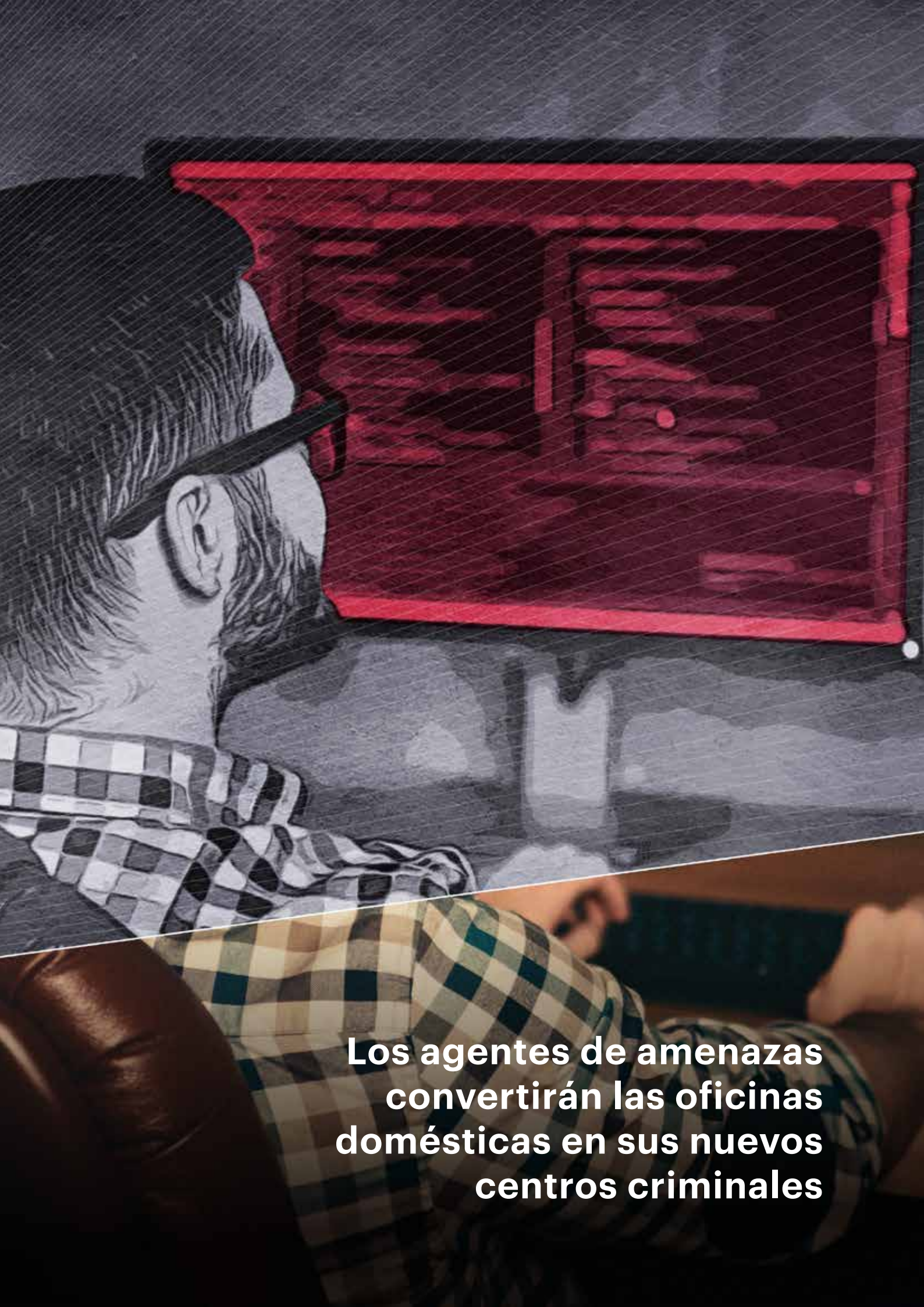
Predicciones de seguridad de Trend Micro para 2021

La pandemia del coronavirus (Covid-19) ha cambiado la forma de operar de muchas organizaciones, ya que el trabajo a distancia se ha convertido en la norma. Sin embargo, el paso de una oficina habitual a un puesto de trabajo en el hogar - potencialmente como un acuerdo a largo plazo - plantea nuevos riesgos de seguridad para las empresas a medida que más agentes de amenazas intentan sacar provecho del malestar relacionado con el Covid-19.

Ya afirmamos en nuestras predicciones de seguridad para 2020 que el viejo paradigma, donde las redes están tradicionalmente aisladas detrás de un firewall corporativo, quedaría atrás. Las configuraciones y protecciones tradicionales ya no serían adecuadas en un ecosistema que demanda una amplia gama de servicios y plataformas.

Cuando la pandemia del Covid-19 nos golpeó, las organizaciones rápidamente tuvieron que enfrentarse a esta realidad. Ha puesto sobre la mesa recordatorios aleccionadores de problemas perennes y advertencias desatendidas que han acosado a la ciberseguridad durante años. También ha mostrado cómo las organizaciones de todo el mundo corren un riesgo importante de sufrir interrupciones por ciberataques, crisis mundiales y otros posibles puntos de inflexión. Si bien el riesgo siempre ha estado presente, la pandemia no ha hecho más que subrayar la gravedad del problema: ¿cómo están equipados o preparados los sectores para tales escenarios?

En 2021, las organizaciones se esforzarán por hacer frente a los efectos de gran alcance, al tiempo que se comprometerán a mantenerse seguras a medida que crezca la dependencia online. Examinamos los desarrollos que no solo son plausibles, sino que también deben ser anticipados. Analizamos los factores que impulsan el futuro próximo de la ciberseguridad y cómo las organizaciones tendrán que adaptarse a medida que las amenazas y las tecnologías ejerzan su influencia. Nuestro informe tiene por objeto facultar a las organizaciones y a los responsables de la toma de decisiones para que elaboren una respuesta estratégica adecuada que pueda resistir al cambio y la disrupción.



Los agentes de amenazas convertirán las oficinas domésticas en sus nuevos centros criminales

Turning the Tide

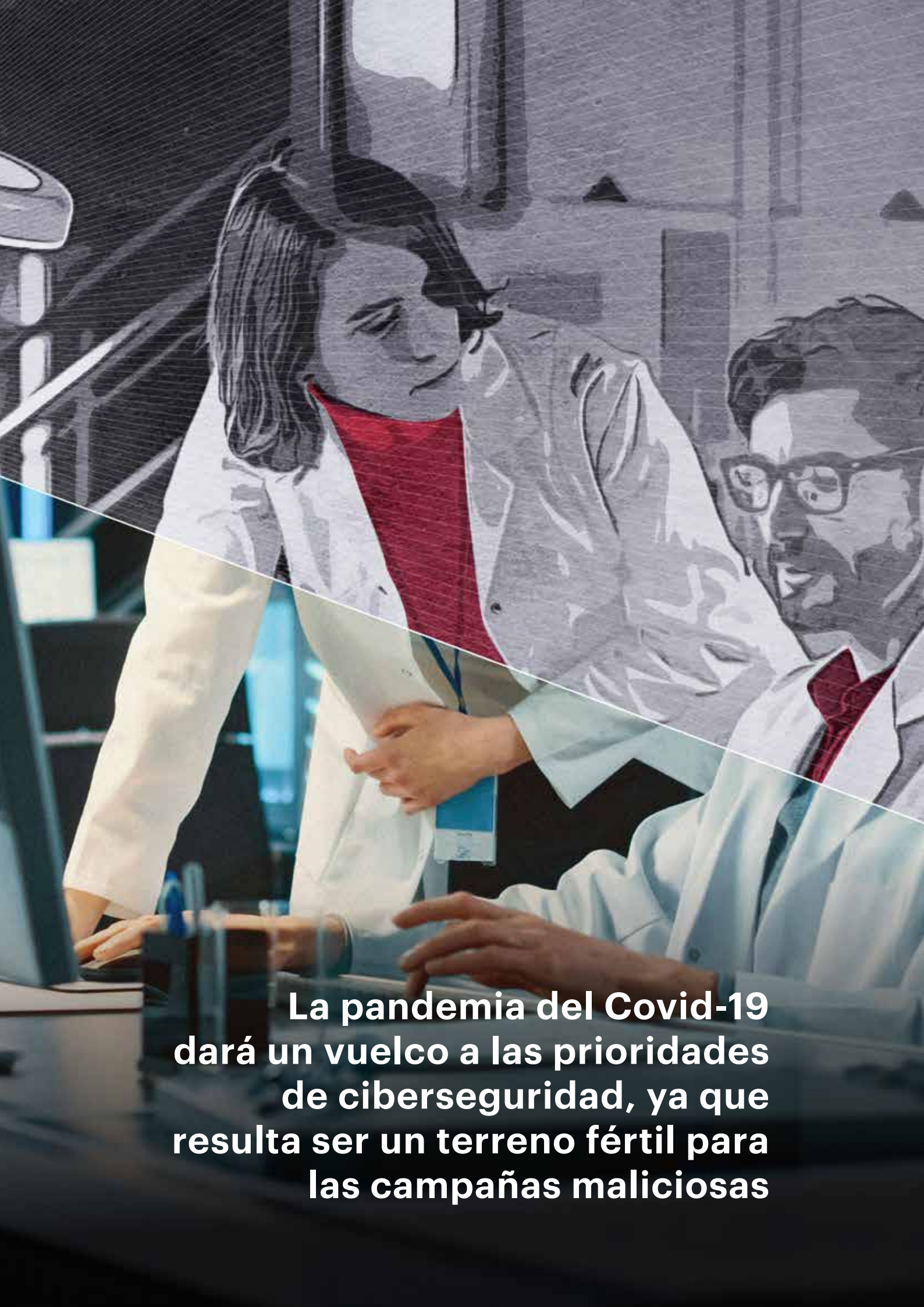
La pandemia en curso y los cierres resultantes en muchas partes del mundo han obligado a una afluencia de empleados a un territorio desconocido: trabajo remoto y, en muchos casos, trabajo desde casa a tiempo completo. Como resultado, muchos empleados y empresas están empezando a darse cuenta de la viabilidad de trabajar desde casa en el futuro. En estas circunstancias, los usuarios y las empresas tendrán que proteger las instalaciones y configuraciones de trabajo desde casa de las amenazas, no solo para los equipos de TI que de repente necesitan asegurar a toda la fuerza laboral remota, sino también para los usuarios individuales que necesitan tomar precauciones.

Los límites entre el trabajo y la vida privada se han roto a medida que se trabaja con proveedores de servicios de Internet (ISP) en el hogar, con routers y máquinas que posiblemente no tengan parches, otros dispositivos conectados en segundo plano y miembros de la familia que comparten ordenadores mientras trabajan para diferentes organizaciones. Si bien las redes privadas virtuales (VPN) pueden proteger las conexiones con los lugares de trabajo, los usuarios que viven en el domicilio deberán tener cuidado con las vulnerabilidades de las VPN que podrían provocar ataques remotos.[1, 2]

Las redes domésticas también se convertirán en puntos de lanzamiento de ataques para los agentes de amenazas que buscan secuestrar máquinas y saltar a otros dispositivos en la misma red, con el objetivo de ganar un punto de apoyo corporativo. Los actores maliciosos aprovecharán el software instalado o las vulnerabilidades "wormable" no parcheadas, saltando de una máquina de un trabajador remoto a otra hasta encontrar un objetivo adecuado. Este ataque a la cadena de suministro se extenderá a otros usuarios en el futuro. Los empleados que accedan de forma remota a información confidencial y crítica (por ejemplo, recursos humanos, ventas y soporte técnico) también serán blanco activo de ataques de robo de datos en 2021. La falta de un sistema de detección de intrusiones o de un firewall, junto con el ancho de banda de Internet de alta velocidad, hará que sea especialmente fácil para los agentes de amenazas pasar de una red corporativa a la siguiente.

Los routers siempre han sido vistos como blancos fáciles para los ataques remotos a los dispositivos conectados. Los ciberdelincuentes ofrecerán routers hackeados como un nuevo servicio en el que venderá acceso a las redes domésticas. El acceso como servicio surgirá como un modelo de negocio lucrativo para los delincuentes, que podrían establecer huellas persistentes y ofrecer acceso a redes domésticas de alto valor (como las de los ejecutivos o los administradores de TI) a otros agentes de amenaza. Las organizaciones con redes convergentes serán los principales objetivos para esto; se encontrarán en el punto de mira de los ciberdelincuentes que buscan obtener beneficios vendiendo el acceso a redes de tecnología operativa (OT). Un punto débil explotado en el espacio de la tecnología de la información (TI) puede resultar rentable para los agentes de amenazas que planean sacar provecho del acceso a la red OT en 2021.

Contar con políticas de seguridad detalladas de la empresa ayudará a las organizaciones a garantizar que el intercambio de datos entre las oficinas y los empleados que trabajan desde casa esté protegido adecuadamente, y que las instalaciones de la oficina en el hogar no se conviertan en una puerta de entrada para diversas formas de ciberdelincuencia. Un plan de respuesta ante incidentes tendrá que esbozar la forma en que una organización se ocupará de la seguridad en una red con máquinas discretas. Las organizaciones deben aconsejar a los empleados que trabajan desde casa sobre la seguridad de los routers domésticos y de Internet de las cosas (IoT), así como sobre el uso de una red privada virtual (VPN). Esto debería incluir una sesión informativa sobre los riesgos de la reutilización de las contraseñas y el uso de las contraseñas predeterminadas de los routers y del IoT. También recomendamos segmentar las redes domésticas para aislar los equipos corporativos (es decir, utilizar una red de área local virtual [VLAN] y dedicarla solo al trabajo de oficina).



La pandemia del Covid-19 dará un vuelco a las prioridades de ciberseguridad, ya que resulta ser un terreno fértil para las campañas maliciosas

Turning the Tide

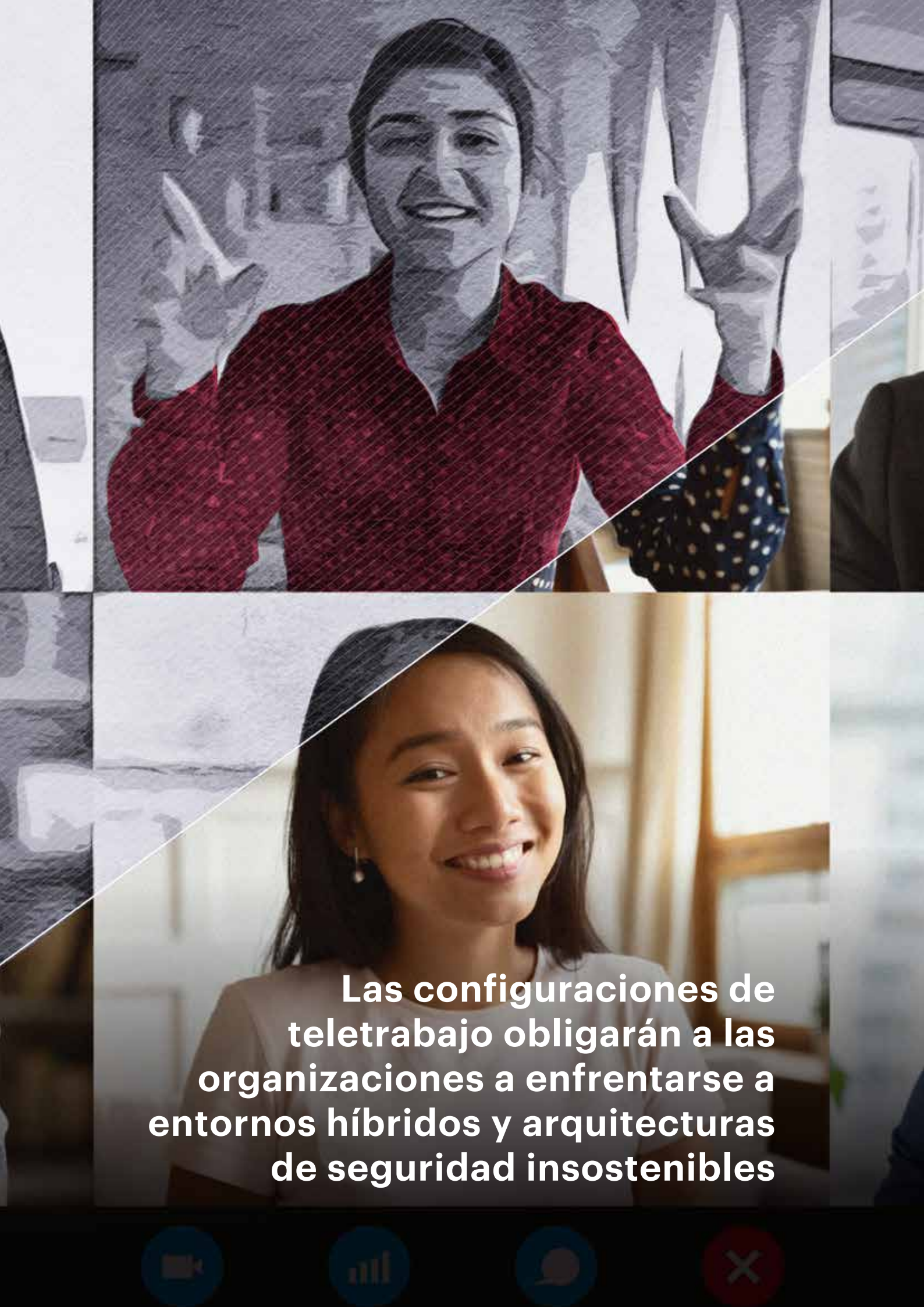
Los agentes de amenaza ven cualquier evento importante como una oportunidad para la manipulación o el sabotaje, y no es diferente para la pandemia del coronavirus; están cambiando de táctica y explotando los temores colectivos relacionados con el Covid-19. En nuestro resumen de seguridad de mediados de año para 2020,[3] observamos un aumento dramático de los correos electrónicos fraudulentos, el spam y los intentos de phishing relacionados con el Covid-19 desde el comienzo de la crisis de salud pública. Los ciberdelincuentes seguirán apostando por las oportunidades de la ingeniería social y permanecerán activos con campañas que utilicen señuelos temáticos del coronavirus.

El Covid-19 seguirá presentando a las empresas de todo el mundo desafíos en materia de ciberseguridad. El comercio electrónico, por ejemplo, ha tenido un crecimiento sostenido en los últimos años, y la pandemia lo ha reforzado. El crimen organizado intentará irrumpir en la logística a medida que aumenten las compras online y se entreguen más paquetes. Delitos como el sabotaje de la producción, el tráfico y el transporte de mercancías falsificadas surgirán como su modus operandi en medio de la pandemia.

El sector de la salud, en particular, será el centro de atención. Como muchos médicos se han pasado a la telemedicina y la prestación de servicios médicos se ha vuelto aún más crítica, la seguridad informática de los sistemas sanitarios será puesta a prueba. Los equipos de seguridad no solo tendrán que hacer frente a los riesgos de seguridad asociados a los datos de los pacientes y a los ataques de malware[4],sino también a la posibilidad de espionaje médico.

Los grupos de amenaza reconocerán los laboratorios de vacunas contra el coronavirus, en particular, los dirigidos a las instituciones que se han identificado públicamente como dedicadas a la investigación relacionada con el Covid-19. Los agentes maliciosos intentarán obtener inteligencia sobre los esfuerzos de respuesta y robar las investigaciones en curso sobre las vacunas y remedios relacionados. Este posible robo de información médica puede frenar sus esfuerzos de investigación y poner en peligro la entrega y el suministro de opciones de tratamiento.

Las campañas de desinformación también dificultarán a los usuarios la tarea de desentrañar las muchas incertidumbres de la pandemia. Los agentes de amenazas se inclinarán por utilizar la información errónea para atraer a los usuarios a hacer clic en archivos adjuntos y enlaces maliciosos en transacciones fraudulentas. Estas estafas se enviarán a través de correos electrónicos, apps falsas, dominios maliciosos y redes sociales, con el fin de proporcionar información sobre la salud, supuestas vacunas y las correspondientes listas de espera.[5] Por el contrario, el tema de las vacunas, cuando estén disponibles, se utilizará como un señuelo de phishing.



Las configuraciones de teletrabajo obligarán a las organizaciones a enfrentarse a entornos híbridos y arquitecturas de seguridad insostenibles

Turning the Tide

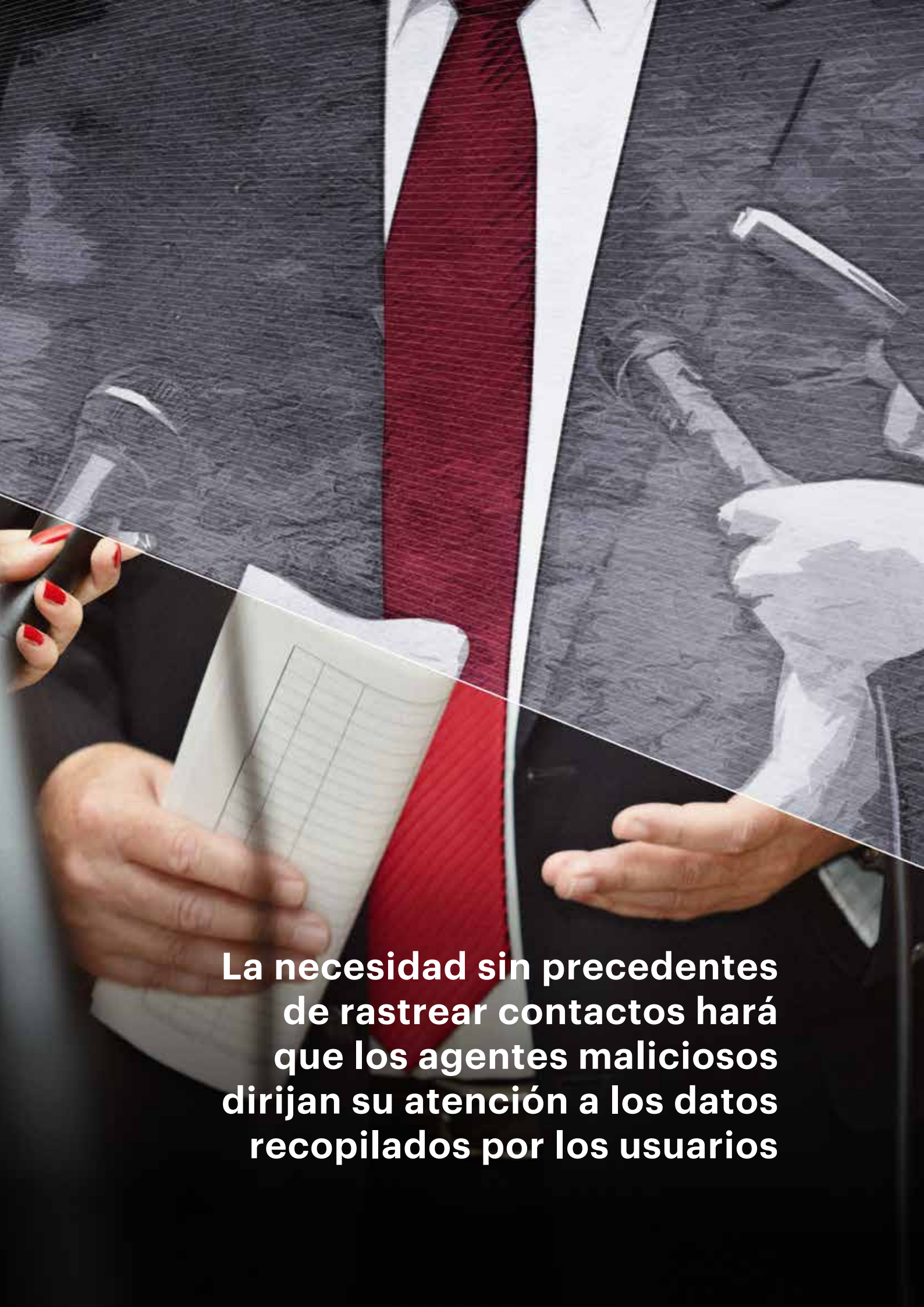
A medida que el teletrabajo se afiance aún más en 2021, los entornos híbridos -en los que el trabajo y los datos personales se mezclan en una sola máquina- supondrán un importante reto para las organizaciones que tengan menos control sobre el uso de los empleados. La mezcla de tareas personales y laborales (es decir, el uso de un equipo para realizar diversas actividades online) difumina las líneas relativas al lugar donde se almacenan y procesan los datos. Si se infecta un dispositivo de trabajo, ¿cómo se considerarán los datos personales en la limpieza? ¿Existe alguna forma de rastrear los datos impresos o exportados? Esta disminución de la visibilidad de las empresas sobre lo que ocurre en los dispositivos se agrava cuando los empleados acceden a las apps personales desde los dispositivos.

A medida que las diversas tecnologías utilizadas en el trabajo remoto ocupen los titulares de las noticias sobre cuestiones de seguridad, los modelos zero-trust cobrarán impulso en 2021 como un enfoque eficaz para potenciar las fuerzas de trabajo distribuidas. Al eliminar la confianza implícita en cualquier cosa dentro o fuera de la red, todo se verifica antes.[6] Mediante la microsegmentación, una arquitectura zero-trust da a los usuarios acceso solo a los recursos específicos necesarios dentro de ciertos perímetros. Esa aplicación garantizará una postura de seguridad sólida al dificultar la penetración de los agentes de amenazas en la red. El enfoque zero-trust se integra fácilmente con el perímetro de servicio de acceso seguro (SASE) respaldado en la nube lo que proporciona a los equipos de seguridad una visibilidad crítica de todo el tráfico entrante y saliente.

A raíz de la pandemia, las organizaciones han modificado su infraestructura de TI y han acelerado su paso a la nube. Las infraestructuras que normalmente se tropezarían con la actualización de las tecnologías están acelerando los programas de transformación. Aquellos que confían en las soluciones tradicionales on-premise no podrán mantenerse al día con las demandas actuales que el software y las aplicaciones seguras basadas en la nube pueden llevar a cabo. El objetivo de las organizaciones, independientemente del sector o la industria, será garantizar que sean lo suficientemente versátiles y ágiles para hacer frente a los desafíos que se presenten.

Desde el viaje virtual hasta el entretenimiento a distancia, habrá un continuo surgimiento de nuevos modelos de negocios a medida que diversas entidades abran nuevos caminos en las plataformas digitales. Las soluciones tecnológicas emergentes ayudarán en el trabajo diario de las oficinas domésticas a través de apps habilitadas para IA. Antes de enfrentarse inevitablemente a formas de esquemas criminales digitales, estas apps primero tendrán dificultades para despegar y comercializarse.

En respuesta a la pandemia en curso, las organizaciones han comprendido la necesidad de reorientar su seguridad y de cubrir a los trabajadores remotos para la continuidad del negocio. Los equipos de TI tendrán que revisar los enfoques de seguridad para acomodar las configuraciones de trabajo remoto a largo plazo. Las organizaciones harían bien en esbozar políticas de trabajo desde el hogar (incluida la coordinación con los proveedores de servicios gestionados), manejo de datos y, en la medida de lo posible, hacer cumplir la línea que separa el uso personal y empresarial de los dispositivos.



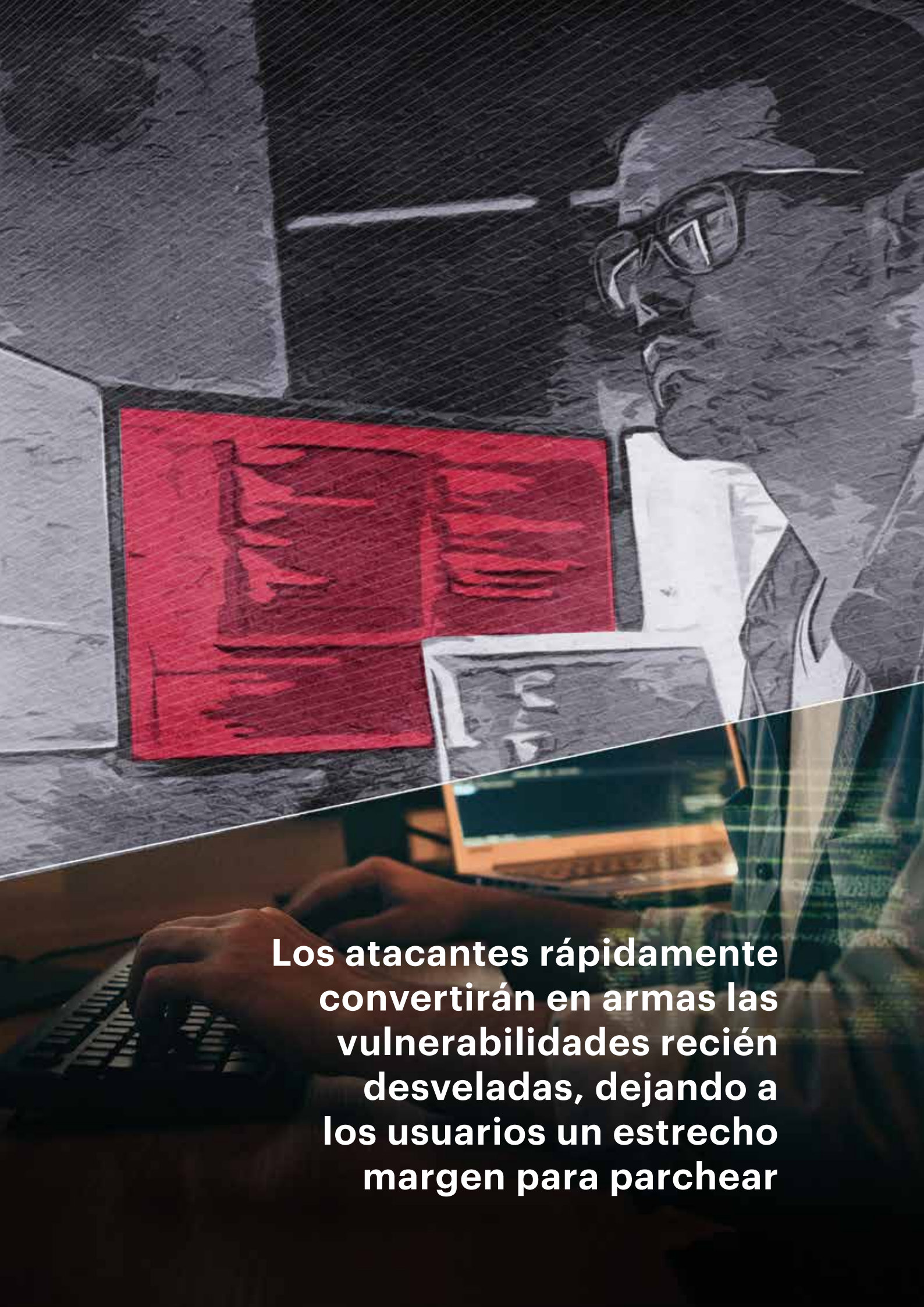
La necesidad sin precedentes de rastrear contactos hará que los agentes maliciosos dirijan su atención a los datos recopilados por los usuarios

Los niveles sin precedentes de recopilación de datos[7] en los esfuerzos por monitorizar y vigilar el estado de salud de las personas atraerán a los delincuentes y activistas políticos que intentan obtener esos datos. La prisa por aplicar estas medidas aumentará el riesgo de exponer o filtrar los datos de los usuarios.

El acceso rápido a los datos podría ser crucial para luchar contra el brote, pero la flexibilización de las medidas de privacidad de los datos conlleva sus propios problemas. Las grandes bases de datos, junto con las implementaciones apresuradas, son objetivos de gran valor para los agentes maliciosos que buscan comprometer los datos recopilados y posiblemente retenidos. Los grupos de ciberdelincuentes pueden abusar de ello de diferentes maneras, incluida la extracción de información de identidad y su venta en el underground.

La falta de protocolos y protecciones estrictas deja a los servidores o bases de datos vulnerables a la explotación. Los gobiernos tendrán que prepararse y tomar las medidas adecuadas para proteger los datos de los hackers.

Los esfuerzos por frenar la propagación de la enfermedad podrían incluir también cuarentenas y cierres, lo que tendrá repercusiones económicas en varias cadenas de suministro. Las repercusiones económicas y operativas crearán restricciones presupuestarias en las operaciones de seguridad de las organizaciones, lo que planteará a los equipos de seguridad el reto de mantener (o aumentar) la cobertura con asignaciones financieras más estrictas.



Los atacantes rápidamente convertirán en armas las vulnerabilidades recién desveladas, dejando a los usuarios un estrecho margen para parchear

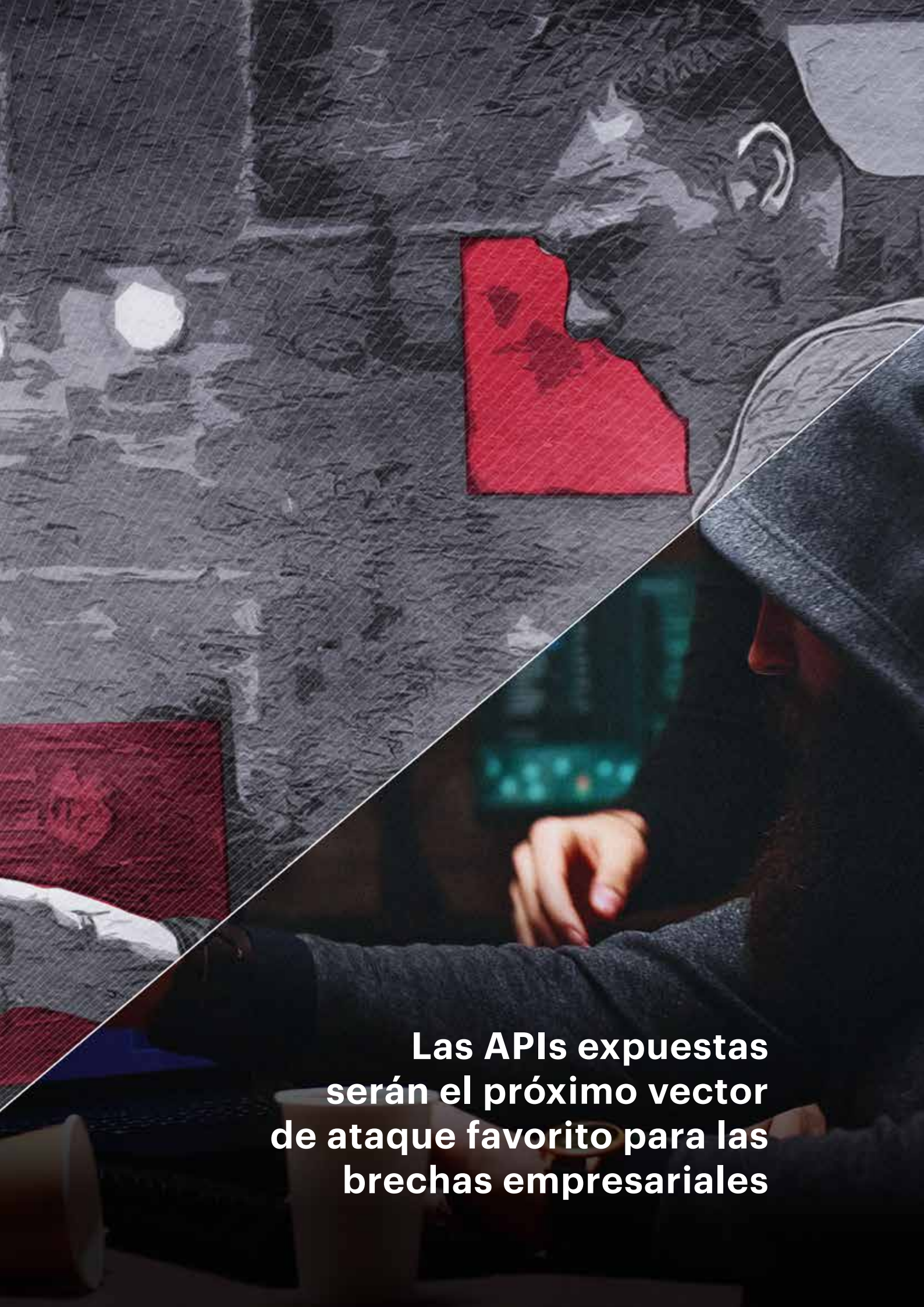
Turning the Tide

Mientras que las vulnerabilidades zero-day tienden a robar el protagonismo cuando se trata de ataques, las vulnerabilidades conocidas o n-day plantearán importantes preocupaciones en 2021. Mientras que las vulnerabilidades zero-day se refieren a fallos o errores que acaban de ser revelados pero que permanecen sin parchear, las vulnerabilidades n-day son las que han sido conocidas públicamente y pueden tener parches desplegados. Hay innumerables vulnerabilidades conocidas hoy en día, y muchas organizaciones descubrirán que tienen una exposición considerable en sus respectivas huellas digitales.

En 2021, habrá una rápida adopción de las vulnerabilidades y exploits de tipo n-day liberadas por la comunidad de investigación. Los atacantes utilizarán activamente como armas los nuevos fallos revelados en sus marcos de ataque. En Operation Poisoned News, los agentes de amenaza extrajeron el código de una prueba de concepto (POC) de n-day y aprovecharon varios errores de escalada de privilegios publicados por Project Zero[8] de Google. Los agentes de Earth Kitsune tenían un modus operandi similar: modificaron los exploits lanzados por Project Zero y Zero Day Initiative (ZDI) de Trend Micro.[9]

Las vulnerabilidades n-day resultarán ser una mina de oro para los agentes de amenazas que buscan debilidades que estén fácilmente disponibles para su uso. Los exploits denunciados en los ataques también pueden tener documentos de divulgación pública para su consulta, lo contrario de los zero-days, que requieren mucho tiempo y son difíciles de encontrar y explotar.

Prevemos que también surgirán mercados de vulnerabilidades n-day para comerciar o vender errores conocidos explotables, en los que los hallazgos de vulnerabilidad se modifican de acuerdo con las necesidades del agente de la amenaza. No es descabellado especular que los vendedores también ofrecerán personalización de exploits en función del ataque. Si bien esto permitirá a los agentes relativamente inexpertos elaborar ataques, será especialmente atractivo para los grupos de agentes de amenazas que son conocidos por aprovechar los fallos existentes de zero-day y n-day en objetivos de alto valor. Además, los grupos de atacantes sofisticados aumentarán el uso de herramientas de prueba de penetración, incluido el ampliamente utilizado Cobalt Strike, cuyo código fuente supuestamente se filtró en noviembre de 2020.[10]



Las APIs expuestas serán el próximo vector de ataque favorito para las brechas empresariales

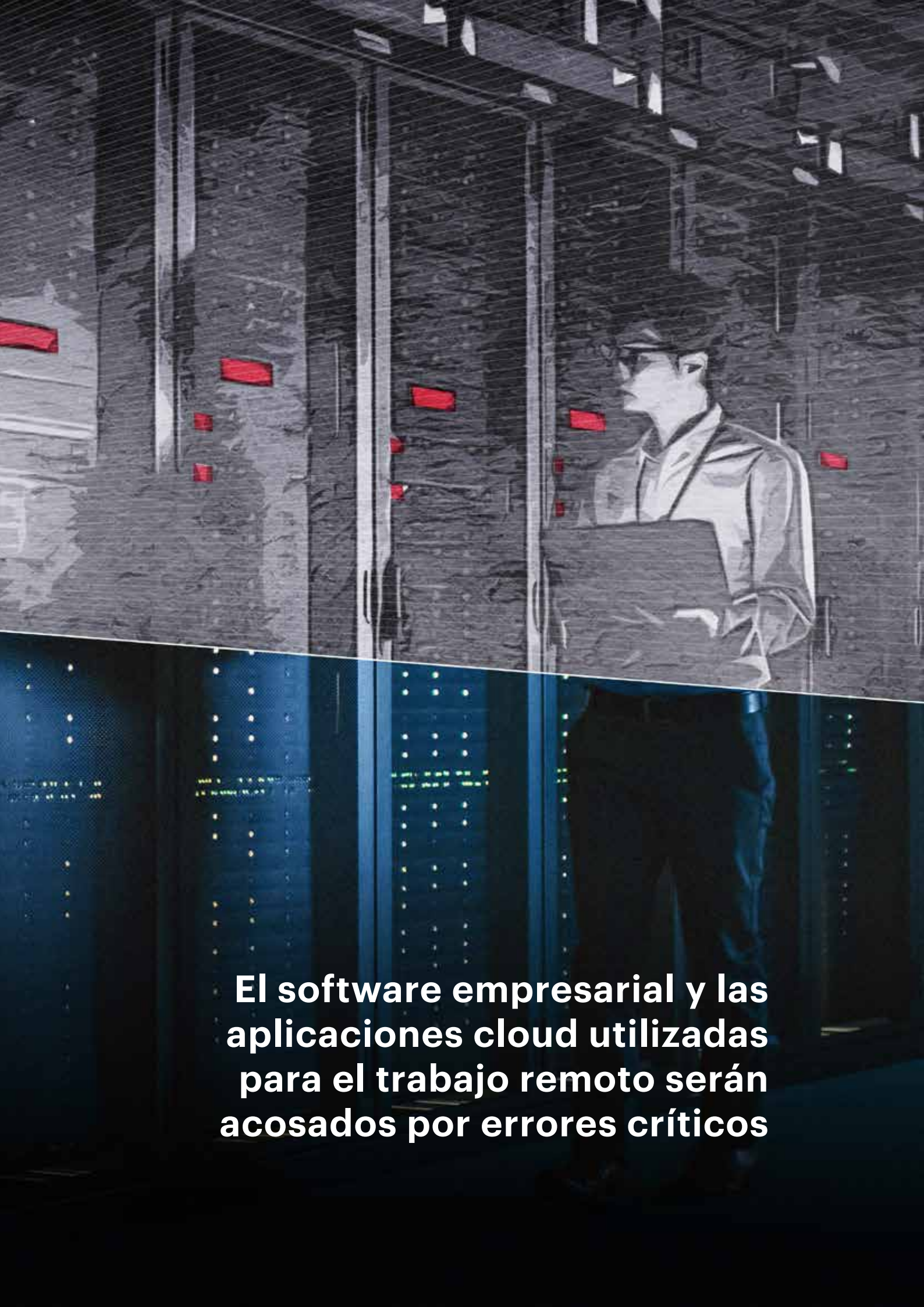
Turning the Tide

Una interfaz de programación de aplicaciones (API) es un intermediario de software que permite la comunicación entre cualquier aplicación, desde el intercambio de datos y la prestación de funcionalidad hasta la optimización de las operaciones y la conectividad del sistema, proporcionando protocolos, rutinas y herramientas para desplegar servicios y software en los dispositivos, incluido el IoT. Muchos negocios dependen de las API para proporcionar acceso a los sistemas internos e interactuar con los clientes a través de las aplicaciones.

La advertencia es que también están listos para la selección de los agentes de amenaza que buscan un punto de entrada en las redes de una organización. A medida que las API se hagan más prominentes en el espacio empresarial, también lo será su superficie de ataque. Las API se convertirán en un objetivo preferido, ya que también actúan como conductos para la integración de terceros, y predecimos que la seguridad de las API será una nueva área de interés para los adversarios en 2021.

Las API, aunque ya son comunes, tienen una seguridad aún incipiente. Introducen varios puntos débiles que podrían ser vectores para brechas de datos en aplicaciones empresariales. En algunos casos recientes se ha informado de que se ha obtenido acceso a la información personal de usuarios[11], [12] y se ha encontrado código fuente expuesto y acceso a servicios de backend.[13]

Los API también son relativamente fáciles de descubrir, tienen muchos parámetros abiertos para el compromiso y son intrínsecamente inseguras. Los mecanismos de defensa tradicionales que implican Captchas, JavaScript, o instrumentación SDK móvil no pueden ser utilizados eficazmente para prevenir un ataque automatizado[14], lo que significa que las API están solo parcialmente protegidas, si es que lo están. Recomendamos configurar el control de acceso y los mecanismos de autenticación con un enfoque de defensa en profundidad y supervisar regularmente los registros de acceso.



El software empresarial y las aplicaciones cloud utilizadas para el trabajo remoto serán acosados por errores críticos

Esperamos que el software y los servicios más importantes utilizados en el trabajo distribuido se encuentren con más vulnerabilidades divulgadas públicamente debido a una mayor investigación. Utilizando los detalles de las vulnerabilidades públicamente disponibles, los usuarios pueden comprobar sus sistemas en busca de problemas de seguridad, al tiempo que permiten a los investigadores y a los agentes de amenazas buscar agujeros similares en los sistemas, especialmente si los fallos descubiertos son relativamente nuevos. Los investigadores estarán particularmente atentos a los fallos críticos y variantes similares en el software empresarial y otras tecnologías de trabajo remoto. Tanto los ciberdelincuentes como los grupos de agentes de amenazas favorecerán las debilidades en el software popular como parte de sus campañas.

Las vulnerabilidades relacionadas con Microsoft Teams, así como con SharePoint, Office 365 y Exchange, se perseguirán en 2021. El procesamiento de información potencialmente sensible en estas plataformas de software de colaboración será una preocupación importante para las organizaciones con una fuerza laboral remota cada vez mayor, en particular en las industrias reguladas como los servicios financieros y la asistencia sanitaria.

Con un impulso renovado para pasar a los entornos cloud y utilizar herramientas de colaboración, se habla más que nunca de la seguridad en la nube. Para obtener la visibilidad del sistema y satisfacer las necesidades de escalabilidad, las organizaciones reúnen y almacenan datos masivos en múltiples fuentes y entornos. Sin embargo, estas nubes de registros serán fundamentales para los cibercrímenes modernos de alto perfil. Los entornos cloud a menudo guardan multitud de datos valiosos y sensibles que los delincuentes pueden utilizar para encontrar los puntos de acceso iniciales a las redes.

La adopción del uso de la tecnología cloud en 2020 continuará en el año 2021 para hacer frente al efecto de la pandemia en las operaciones. Esperamos que esta tendencia continúe creciendo incluso cuando la pandemia retroceda. Hacia finales de 2021, la mayoría de las cargas de trabajo se ejecutarán en la nube. Las organizaciones que migraron de forma rápida y al azar se enfrentarán a las implicaciones de seguridad. Predecimos que las brechas de datos y el compromiso exponencial en las infraestructuras cloud serán causados no por los proveedores de la nube, sino por las configuraciones incorrectas y los errores involuntarios de los usuarios.

Otras preocupaciones para los que adoptan la nube son los hackers que intentan apoderarse de los servidores en la nube y desplegar imágenes de contenedores maliciosos. Esperamos una proliferación de imágenes vulnerables que se ejecutan en diversas arquitecturas a medida que los usuarios confían sin restricciones en los servicios de contenedores y almacenes. Estas imágenes estarán destinadas a secuestrar repositorios y envenenar recursos.[15] Los datos expuestos serán un escollo común que dará lugar a brechas y ataques basados en la nube en las organizaciones.

Forjando el futuro con la ciberseguridad

Las predicciones de seguridad de Trend Micro para 2021 reflejan la investigación y los conocimientos de nuestros expertos en seguridad sobre las tecnologías emergentes y los problemas de seguridad. Manténgase un paso por delante de las amenazas que hemos descrito con estas recomendaciones de seguridad para una respuesta e inteligencia proactiva a las amenazas globales:

Fomentar la educación y la capacitación de los usuarios. Los agentes de amenazas seguirán aprovechando el miedo que rodea al Covid-19, y los usuarios deben estar informados de las tácticas y los posibles vectores de ataque. Las organizaciones deben reforzar el conocimiento de las amenazas y extender las mejores prácticas corporativas al hogar. Compartir directamente lo que se debe y lo que no se debe hacer en materia de teletrabajo y desaconsejar el uso de dispositivos personales.

Mantener un estricto control de acceso a la red corporativa y a la oficina doméstica. Las organizaciones deben centrarse en la creación de políticas corporativas basadas en la seguridad y establecer un plan de respuesta a incidentes que abarque el perímetro de sus operaciones. Esto fortalecerá los servicios, las estaciones de trabajo y los datos corporativos, al tiempo que permitirá a las empresas trabajar de forma remota. Abstenerse de depositar una confianza implícita en los activos o las cuentas de usuario, independientemente de la ubicación.

Reiterar las medidas de seguridad básicas y los programas de gestión de parches. Los puntos débiles solo aparecerán durante los próximos meses de trabajo a distancia. Será imperativo actualizar y parchear regularmente las aplicaciones y sistemas que son más vulnerables que nunca. .

Aumentar la detección de amenazas con experiencia en seguridad. Garantizar la detección avanzada de amenazas y el manejo de incidentes durante las 24 horas del día en cargas de trabajo en la nube, correos electrónicos, endpoints, redes y servidores con la ayuda de analistas de seguridad dedicados. Obtener una mejor comprensión de los ataques y priorizar las alertas de seguridad a través de una completa inteligencia de amenazas y soluciones líderes en la industria.

Referencias

1. Cybersecurity and Infrastructure Security Agency. (January 10, 2020). *US-CERT.* “Continued Exploitation of Pulse Secure VPN Vulnerability.” Accessed on Nov. 10, 2020, at https://us-cert.cisa.gov/ncas/alerts/aa20-010a.

2. Charlie Osborne. (July 17, 2020). *ZDNet.* “Cisco releases security fixes for critical VPN, router vulnerabilities.” Accessed on Nov. 10, 2020, at https://www.zdnet.com/article/cisco-releases-fixes-for-critical-vpn-router-vulnerabilities/.

3. Trend Micro. (August 26, 2020). *Trend Micro.* “Securing the Pandemic-Disrupted Workplace.” Accessed on Nov. 10, 2020, at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/securing-the-pandemic-disrupted-workplace-trend-micro-2020-midyear-cybersecurity-report.

4. Cybersecurity and Infrastructure Security Agency. (October 28, 2020). *US-CERT.* “Ransomware Activity Targeting the Healthcare and Public Health Sector.” Accessed on Nov. 10, 2020, at https://us-cert.cisa.gov/ncas/alerts/aa20-302a.

5. Trend Micro. (April 24, 2020). *Trend Micro.* „Developing Story: COVID-19 Used in Malicious Campaigns.“ Accessed on Nov. 10, 2020, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains.

6. Mary K. Pratt. (January 16, 2020). *CSO Online.* “What is Zero Trust? A model for more effective security.” Accessed on Nov. 12, 2020, at https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html.

7. Elizabeth Beattie. (April 3, 2020). *Al Jazeera Media Network.* “We’re watching you: COVID-19 surveillance raises privacy fears.” Accessed on Nov. 11, 2020, at https://www.aljazeera.com/news/2020/4/3/were-watching-you-covid-19-surveillance-raises-privacy-fears.

8. Elliot Cao et al. (March 24, 2020). *Trend Micro.* “Operation Poisoned News: Hong Kong Users Targeted With Mobile Malware via Local News Links.” Accessed on Nov. 12, 2020, at https://blog.trendmicro.com/trendlabs-security-intelligence/operation-poisoned-news-hong-kong-users-targeted-with-mobile-malware-via-local-news-links/.

9. Nelson William Gamazo Sanchez et al. (October 19, 2020). *Trend Micro.* “Operation Earth Kitsune: Tracking SLUB’s Current Operations.” Accessed on Nov. 12, 2020, at https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-earth-kitsune-tracking-slub-s-current-operations.

10. Lawrence Abrams. (November 11, 2020). *BleepingComputer.* “Alleged source code of Cobalt Strike toolkit shared online.” Accessed on Nov. 17, 2020, at https://www.bleepingcomputer.com/news/security/alleged-source-code-of-cobalt-strike-toolkit-shared-online/.

11. Zack Whittaker. (August 20, 2020). *TechCrunch.* “Fearing coronavirus, a Michigan college is tracking its students with a flawed app.” Accessed on Nov. 11, 2020, at https://techcrunch.com/2020/08/19/coronavirus-albion-security-flaws-app/.

12. Guy Rosen. (September 28, 2018). *Facebook.* “Security Update.” Accessed on Nov. 11, 2020, at https://about.fb.com/news/2018/09/security-update/.

13. Danny Palmer. (April 2, 2019). *ZDNet.* “Security flaws in banking apps expose data and source code.” Accessed on Nov. 11, 2020, at https://www.zdnet.com/article/security-flaws-in-banking-apps-expose-data-and-source-code/.

14. Edward Amoroso. (June 5, 2020). *Help Net Security.* “Understanding cyber threats to APIs.” Accessed on Nov. 11, 2020, at https://www.helpnetsecurity.com/2020/06/05/api-security-threats/.

15. Trend Micro. (May 14, 2019). *Trend Micro.* “Container Security: Examining Potential Threats to the Container Environment.” Accessed on Nov. 12, 2020, at https://www.trendmicro.com/vinfo/us/security/news/security-technology/container-security-examining-potential-threats-to-the-container-environment.

TREND MICRO™ | research

TURNING THE TIDE

Predicciones de seguridad de Trend Micro para 2021

TREND MICRO™ RESEARCH

Trend Micro, líder mundial en ciberseguridad, ayuda a que el mundo sea seguro para el intercambio de información digital.

Trend Micro Research cuenta con la colaboración de expertos apasionados por descubrir nuevas amenazas, compartir conocimientos clave y apoyar los esfuerzos para detener a los ciberdelincuentes. Nuestro equipo global ayuda a identificar millones de amenazas a diario, lidera el sector en la divulgación de vulnerabilidades y publica investigaciones innovadoras sobre nuevas técnicas de amenazas. Trabajamos continuamente para anticiparnos a las nuevas amenazas y realizar investigaciones que inviten a la reflexión.

www.trendmicro.com

Para Raimund Genes (1963-2017)