Vigilando de Cerca

Reporte Especializado de Ciberseguridad de Trend Micro para Latinoamérica y el Caribe

TREND MICRO™

En partnership con

OEA Más derechos para más gente

AVISO LEGAL DE TREND MICRO

La información proporcionada en este documento es solo para fines educativos y de información general. No tiene la intención y no debe interpretarse como un asesoramiento legal. La información contenida en este documento puede no ser aplicable a todas las situaciones y puede no reflejar la situación más actual. No se debe confiar en nada de lo contenido en este documento ni actuar en consecuencia sin el beneficio de asesoramiento legal basado en los hechos y circunstancias particulares presentados y nada de lo aquí contenido debe interpretarse de otra manera. Trend Micro se reserva el derecho de modificar el contenido de este documento en cualquier momento sin previo aviso.

Las traducciones de cualquier material a otros idiomas están destinadas únicamente como una conveniencia. La precisión de la traducción no está garantizada ni implícita. Si surge alguna pregunta relacionada con la precisión de una traducción, consulte la versión oficial del documento en el idioma original. Cualquier discrepancia o diferencia creada en la traducción no es vinculante y no tiene ningún efecto legal a efectos de cumplimiento o aplicación.

Si bien Trend Micro realiza esfuerzos razonables para incluir información precisa y actualizada en este documento, Trend Micro no ofrece garantías ni declaraciones de ningún tipo en cuanto a su precisión, vigencia o integridad. Usted acepta que el acceso, el uso y la confianza en este documento y su contenido es bajo su propio riesgo. Trend Micro renuncia a todas las garantías de cualquier tipo, expresas o implícitas. Ni Trend Micro ni ninguna de las partes involucradas en la creación, producción o entrega de este documento serán responsables de ninguna consecuencia, pérdida o daño, incluidos los daños directos, indirectos, especiales, consecuentes, la pérdida de beneficios comerciales o los daños especiales que surjan de acceso, uso o incapacidad de uso, o en relación con el uso de este documento, o cualquier error u omisión en el contenido del mismo. El uso de esta información constituye la aceptación de su uso en una condición "tal cual".

Escrito y publicado por

Trend Micro Research

Imagen de stock usada con licencia de Shutterstock.com

ÍNDICE

El Panorama de Ciberseguridad de Lationamérica y el Caribe

En septiembre de 2021, Trend Micro publicó su reporte de ciberseguridad de la primera mitad del 2021, titulado "Ataques Desde Todos los Ángulos".[1] Ese reporte, busca ayudar a las organizaciones a potenciar su protección, ofrece una vista completa de los retos de ciberseguridad que las organizaciones y los usuarios alrededor del mundo han estado enfrentando.

Sin embargo, una mirada más de cerca puede ofrecer una vista mucho más detallada, como al mirar a través de un microscopio. Por esta razón, Trend Micro, en colaboración con el Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo de la Organización de los Estados Americanos (OEA/CICTE), examinó los datos del panorama de amenazas que concierne a los estados miembros de la OEA y comparó los hallazgos regionales de las Américas con las tendencias globales identificadas en el reporte de ciberseguridad de la primera mitad de año 2021. Estos datos fueron suplementados con respuestas a una encuesta que se distribuyó a través de CSIRTAmericas, una red de equipos gubernamentales de respuesta a incidentes de seguridad informática (CSIRTs) de los estados miembros de la OEA, a través de la cual se recopilaron datos de 22 miembros de la red a lo largo de la región y de otros oficiales públicos.

El objetivo del análisis del panorama regional de amenazas es entender cómo es que las entidades de América Latina y el Caribe ven al ransomware, los ataques dirigidos, las estafas, los esquemas de trabajo remoto y la adopción de tecnologías relativamente nuevas como temas de seguridad, aportando así perspectivas de valor y una visión integral de las amenazas comunes y distintas que se encuentran a lo largo de la región. (Los detalles de la metodología y el aviso legal completo sobre el proceso de recopilación de datos pueden encontrarse en la sección de Anexos de este reporte.)
Nuestros hallazgos pertinentes incluyen:

- Las amenazas en línea como el ransomware, los ataques dirigidos y las estafas fueron temas importantes de seguridad. Esto no sorprendente, debido a que estas amenazas se propagaron de forma desenfrenada en el 2021, particularmente afectando a organizaciones de alto perfil en industrias críticas.
- Los ajustes debido a la pandemia de COVID-19 y los esquemas de trabajo remoto fueron una preocupación importante cuando inició esta. Aunque muchas empresas ya habían hecho ciertos ajustes necesarios, algunas aún buscaban tener medidas de seguridad más definidas.
- La pandemia de COVID-19 fue catalizadora de una adopción más amplia de nuevas tecnologías como la nube y el internet de las cosas (IoT) o el internet industrial de las cosas (IIoT), pero las fallas de configuración y la falta de educación de los usuarios sobre estas tecnologías puso inadvertidamente a las organizaciones bajo riesgo.
- En términos de comparar los datos de los estados miembros de la OEA con las tendencias globales, algunos hallazgos fueron similares. Por otra parte, para algunas amenazas, otros hallazgos difirieron, como los tipos de amenazas más detectados o las industrias más afectadas.

A lo largo de 2021, las ciberamenazas vinieron desde todos los ángulos, necesitando de protección interconectada para correos electrónicos, redes, páginas web, endpoints y todas las demás capas. La buena noticia es que, a través de un mejor entendimiento de las detecciones de Trend Micro de estas amenazas, principalmente a través de la infraestructura de la Trend Micro™ Smart Protection Network™, las entidades pueden proteger sus sistemas a través de pasos accionables, comenzando desde algunos muy sencillos que pueden rendir mucho en el largo plazo.

Este reporte fue preparado y publicado por Trend Micro en colaboración con Programa de Ciberseguridad de OEA/CICTE. Las opiniones y contenido expresados en este documento son aquellos de los autores, se presentan exclusivamente para propósitos informativos y no representan la opinión o posición oficial de la OEA, su Secretaría General o sus estados miembros.

Ransomware, Ataques Dirigidos y Otras Amenazas Activas

El ransomware, los ataques dirigidos y las estafas continuaron proliferando y evolucionando, involucrando herramientas cada vez más avanzadas y dirigiéndose hacia blancos más grandes.

Los encuestados calificaron las amenazas como el ransomware, los ataques dirigidos y las estafas basándose en su nivel de importancia y frecuencia percibidos respecto a sus organizaciones y cómo se enfrentan a estos retos de cibersegurdad. Una gran mayoría respondió "bastante," mientras que la segunda respuesta más frecuente fue "mucho." Como resultado, este tipo de ataques fueron los que obtuvieron las calificaciones más importantes en la encuesta.

Figura 1. Cómo los encuestados calificaron como un reto de seguridad a las amenazas en línea (ransomware, ataques dirigidos y estafas)

Ransomware

En este punto, el ransomware no necesita de una introducción, especialmente con los ataques masivos de ransomware que llegaron a las noticias en el 2021. Las preocupaciones sobre los efectos de esta amenaza se hicieron evidentes en la encuesta. "El constante incremento en el número de ataques de ransomware, así como el gran impacto que tienen en sus víctimas es una de las preocupaciones fundamentales de cada institución y organización," dijo uno de los encuestados. En muchos casos, las medidas de seguridad con las que contaban las entidades no fueron capaces de mantener el ritmo de la intensidad de las campañas modernas.

Estas preocupaciones se vieron exacerbadas por el incremento en los ataques de alto perfil de ransomware moderno[2], como se vio en eventos de interés global como aquellos lanzados por Sodinokibi (también conocido como REvil)[3] y DarkSide en el procesador de carnes JBS[4] y el proveedor de combustibles Colonial Pipeline[4], respectivamente. Ambas familias de ransomware fueron de las más detectadas durante la primera mitad del 2021.

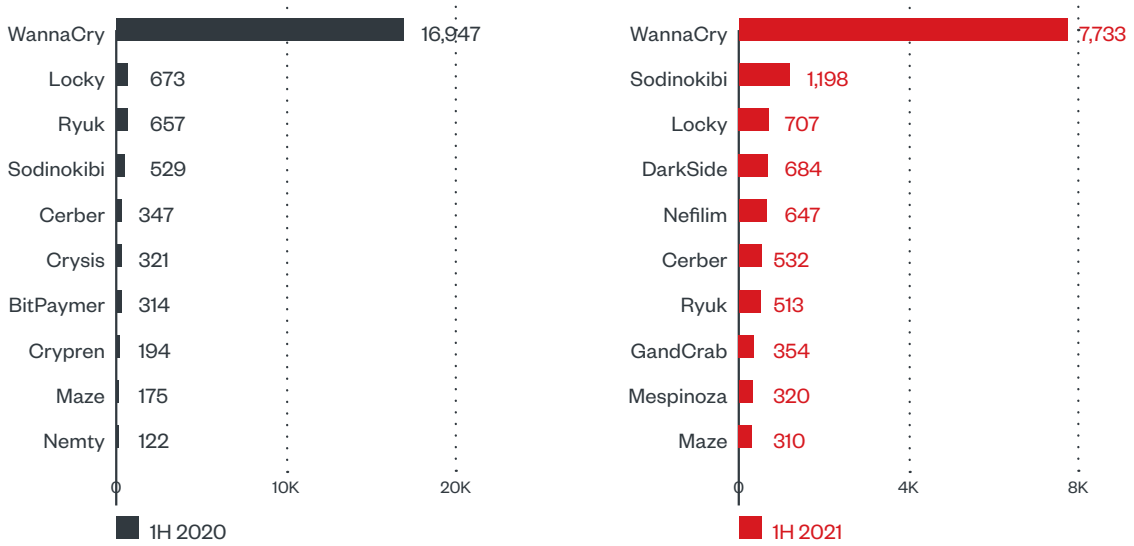

Figura 2. El top 10 de familias de ransomware a lo largo de los estados miembros de la OEA en términos de detecciones de archivos de familias de ransomware en la primera mitad del 2020 y la primera mitad del 2021

WannaCry continuó siendo la familia de ransomware más detectada, manteniendo el liderazgo documentado en los reportes de Trend Micro de años recientes. Continuó siéndolo aún con el hecho de que es una familia relativamente antigua considerada como previa al ransomware moderno y los actores maliciosos detrás de ella no habían iniciado ataques activamente. La persistencia de esta familia muestra cómo un gusano de red puede perseverar si no se parchan adecuadamente los dispositivos, si es que se parchan en primer lugar. Sin embargo, de manera similar a los hallazgos del reporte de ciberseguridad del primer semestre del 2021, a lo largo de los estados miembros de la OEA, las detecciones de WannaCry disminuyeron más de la mitad desde la primera mitad del 2020 hasta la primera mitad del 2021.

Más allá de WannaCry, uno de los hallazgos más notables en el top 10 fue el incremento de detecciones de ransomware moderno, el cual utiliza herramientas y técnicas similares a aquellas utilizadas por amenazas avanzadas persistentes (APTs) para lograr infiltraciones más avanzadas.

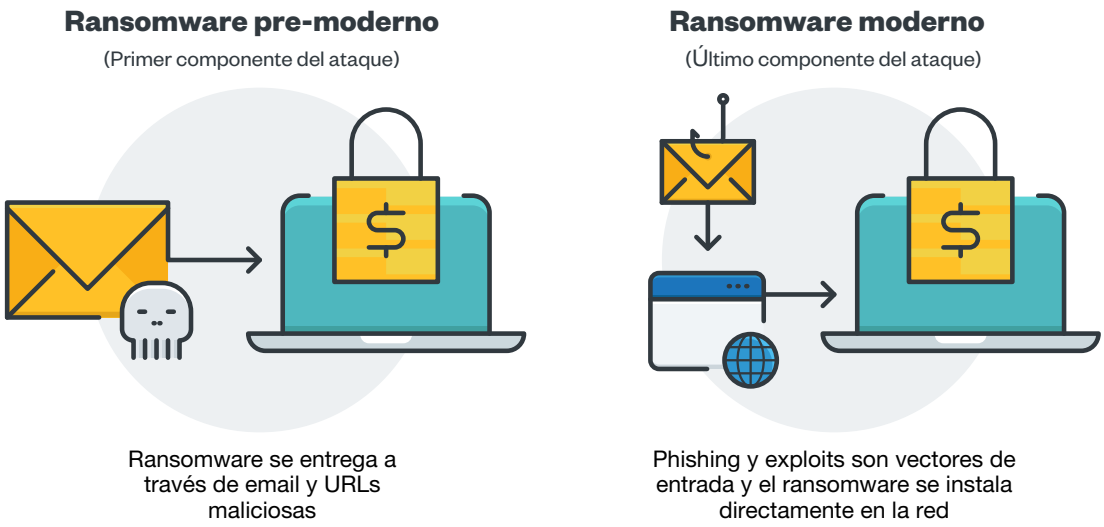

Figura 3. Las diferencias entre el ransomware pre-moderno y moderno

Entre las familias de ransomware moderno, Sodinokibi casi duplicó sus detecciones desde la primera mitad del 2020 y se convirtió en el segundo tipo más detectado a lo largo de los estados miembros de la OEA en la primera mitad del 2021. Mientras tanto, DarkSide entró al top 10.

Este incremento en los rankings también se vio en las tendencias globales: Sodinokibi subió de lugar en el 2021 a comparación del 2020, con 2,119 detecciones, y DarkSide ingresó al top 10 con 830. Esta correlación podría ser atribuida al hecho de que más de la mitad de las detecciones globales totales consistieron en detecciones en las Américas, con 1,119 para Sodinokibi y 684 para DarkSide.

Además de que los ataques de ransomware moderno se volvieron más sofisticados, otra cosa que es alarmante es que los atacantes naturalmente van detrás de las infraestructuras críticas, incluyendo gobiernos. A pesar de esto, algunos de los encuestados no estaban seguros o confiados sobre cómo las medidas de seguridad se estaban implementando para combatir estas campañas de rápido avance.

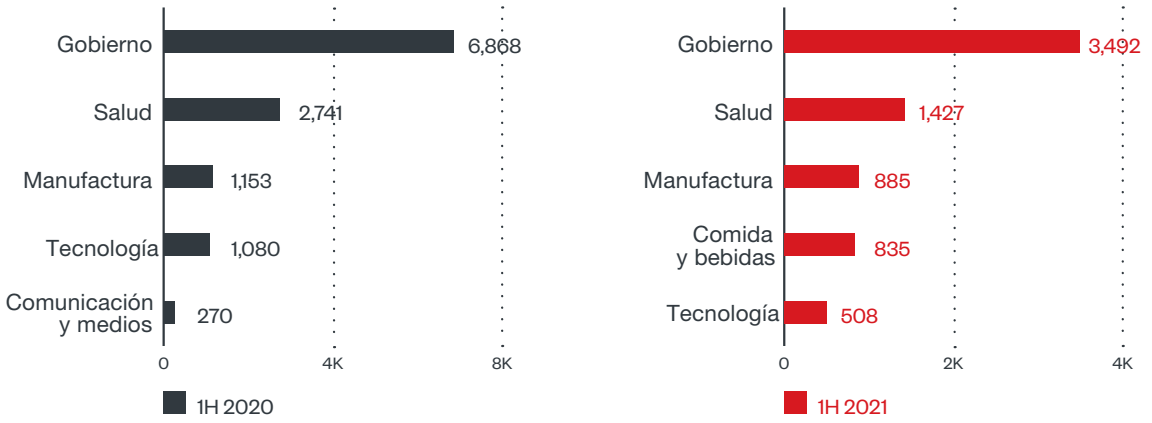

Figura 4. El top 5 de industrias afectadas a lo largo de los estados miembros de la OEA en la primera mitad del 2020 y la primera mitad del 2021.

Las cinco industrias más afectadas por los ataques de ransomware a lo largo de los estados miembros de la OEA en la primera mitad del 2021 fueron en su mayoría los mismos que en la primera mitad del 2020, el gobierno siendo el que presentó más detecciones de este tipo de ataque. Sin embargo, estos hallazgos fueron ligeramente diferentes de las detecciones a lo largo de todas las regiones en el reporte de ciberseguridad de la primera mitad del año, donde la banca, a pesar de no haber estado presente en el top 5 en la primera mitad del 2020, superó al gobierno como el sector con más detecciones. El top 5 global consistió de banca, gobierno, manufactura, salud y alimentos y bebidas.

Ataques Dirigidos

De acuerdo con las tendencias globales, las campañas más dirigidas de ciberamenazas atacaron a entidades en Asia. Sin embargo, algunos de los ciberataques globales no eran necesariamente específicos a una región y se dirigieron hacia ciertas plataformas que se utilizaron sin importar las fronteras. Estos incluyeron los ataques lanzados por el grupo TeamTNT dirigidos hacia las credenciales de vendors de nube[6] y los clusters de Kubernetes.[7] (Describimos más a detalle estos ataques en la sección de la nube y IoT de este reporte.) También observamos ataques que usaban el loader de PlugX[8], una herramienta de acceso remoto (RAT), contra entidades en gobiernos y otras industrias.

Para proteger sus sistemas contra estos ciberataques, las entidades necesitan de medidas robustas y proactivas de ciberseguriad. Sin embargo, las restricciones de presupuesto para adquirir personal experimentado y herramientas de ciberseguridad pueden ser un obstáculo para fortalecer esta industria. Esto se vio reflejado en las respuestas de la encuesta que tocaron el tema de las amenazas en línea, así como los ajustes al trabajo remoto y la adopción de nuevas tecnologías. Un factor importante fue señalado por un encuestado, quien destacó la posibilidad de que estos ciberataques podrían no estarse reportando, dando una falsa sensación de seguridad a una empresa.

Malware

Para el malware en general, la familia más detectada a lo largo de los estados miembros de la OEA en la primera mitad del 2021 fue Webshell, el cual fue el tercero más detectado en el reporte de ciberseguridad global de 2021, siendo los mineros de criptomonedas los primeros. WannaCry estuvo en los primeros lugares en la primera mitad de 2020, bajando al quinto lugar en la primera mitad del 2021..

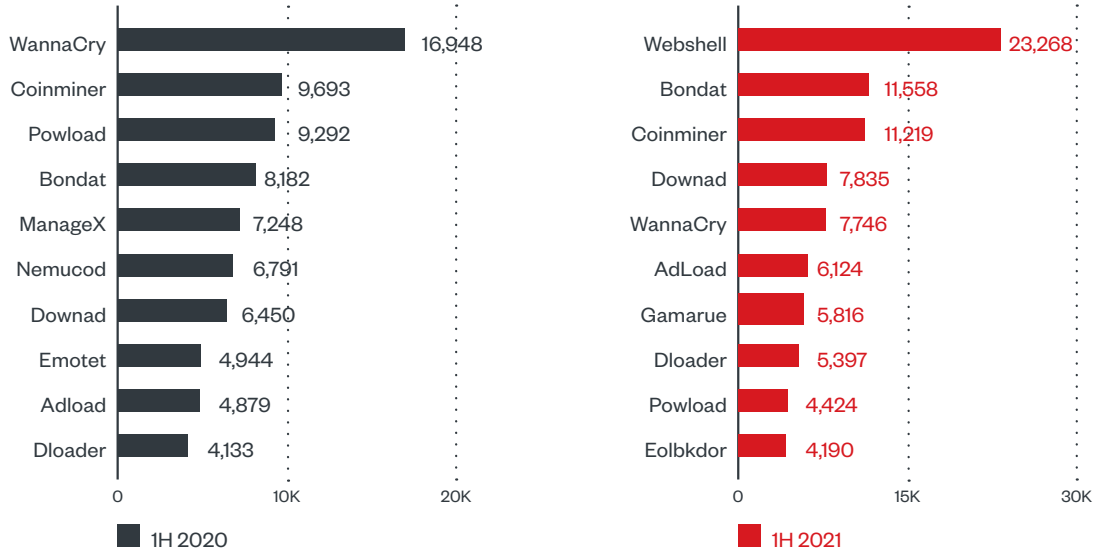

Figura 5. El top 10 de familias de malware a lo largo de estados miembros de la OEA en términos de detecciones en la primera mitad del 2020 y la primera mitad del 2021

Estados Unidos reportó el mayor número de detecciones de malware, con 163 millones, mientras que Brasil y Canadá reportaron cada uno más de 20 millones de detecciones.

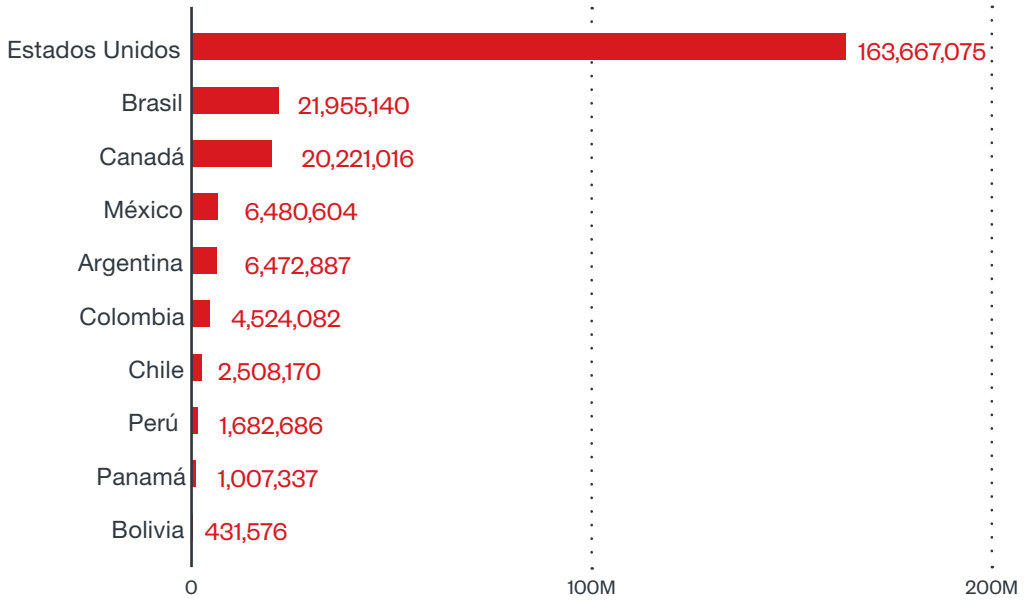

Figura 6. El top 10 de los estados miembros de la OEA en términos de detecciones de malware en la primera mitad del 2021

Amenazas en línea

Las amenazas a correos electrónicos y las URLs maliciosas, las cuales pueden usarse como puntos de entrada para el ransomware, los ataques dirigidos y las estafas, fueron persistentes a lo largo de los estados miembros de la OEA, así como alrededor del mundo. Como aquellos en términos de detecciones de malware, el top de estados miembros de la OEA en términos de detección de amenazas de correo electrónico y URLs maliciosas incluyó a Estados Unidos, Brasil y Canadá, con las detecciones en Estados Unidos excediendo aquellas en otros estados miembros de la OEA.

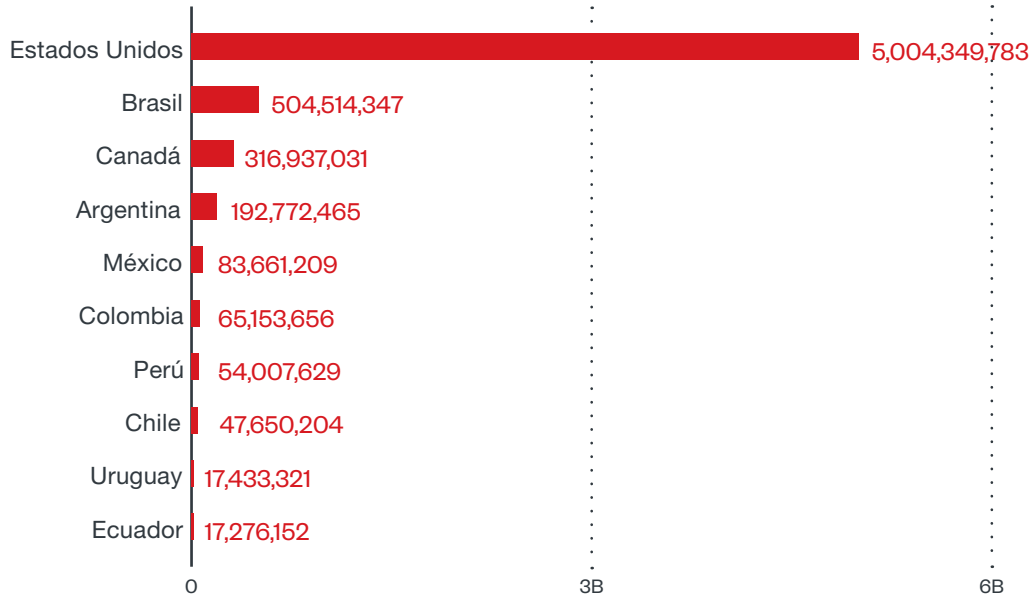

Figura 7. El top 10 de estados miembros de la OEA en términos de detecciones de amenazas de correo electrónico en la primera mitad del 2021

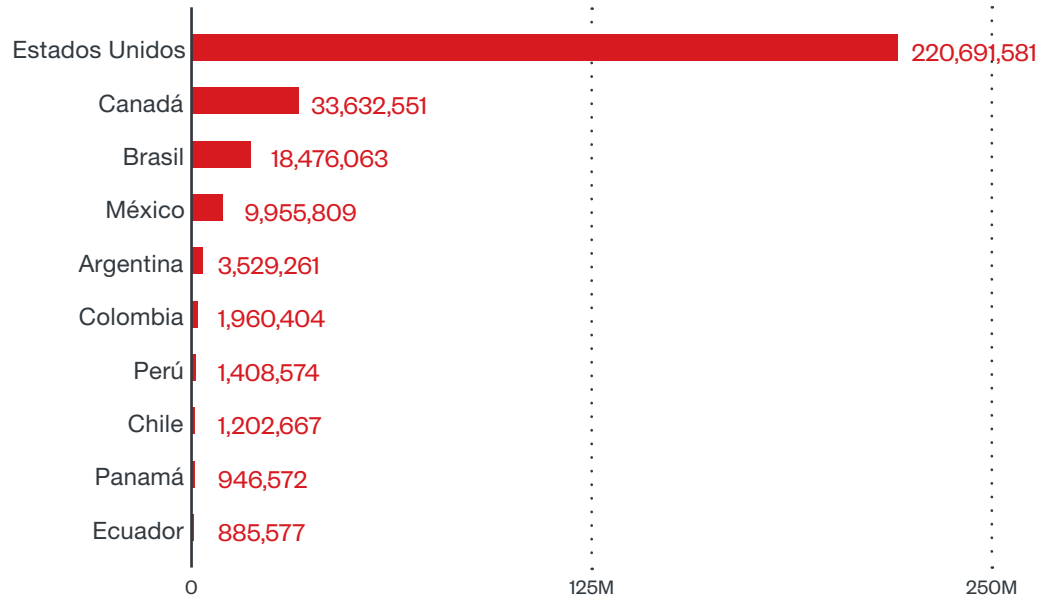

Figura 8. El top 10 de estados miembros de la OEA en términos de detecciones de URLs maliciosas en la primera mitad del 2021

Para evitar estas amenazas, asegurarse de que los empleados siguen mejores prácticas básicas de ciberseguridad es de gran ayuda, En los resultados de las encuestas existe un número importante de respuestas que mencionaron la necesidad de crear campañas para incrementar el conocimiento de seguridad desde los niveles más básicos de una organización. Un encuestado reconoció cómo las personas con conocimientos técnicos limitados podrían ser más vulnerables y comprometer como consecuencia la seguridad institucional. Incluso errores simples por parte de los usuarios, como malas prácticas al navegar en internet y falta de conocimientos sobre cómo podría el ransomware ingresar a un sistema, podrían afectar negativamente a una organización entera.

Amenazas Relacionadas con Esquemas de Trabajo Remoto y Covid-19

La pandemia de COVID-19 presentó ciertos riesgos de ciberseguridad debido a que aceleró la adopción del trabajo remoto o trabajo desde casa (WFH), donde los empleados trabajan desde su casa o residencia en vez de hacerlo desde sus oficinas, usando computadoras y otros dispositivos empresariales conectdos a su red residencial.. La encuesta también investigó cómo las entidades en la región de americas se estaban adaptando al cambio abrupto en los esquemas de trabajo, en términos tanto de operaciones como de la protección de los sistemas.

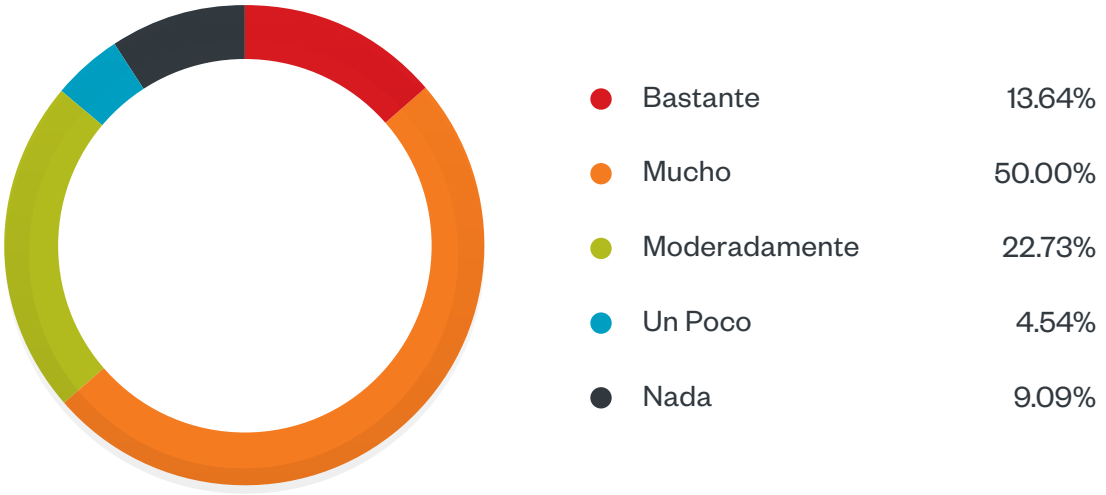

Figura 9. Cómo el ajuste a los esquemas de trabajo remoto seguro debido al COVID-19 (en términos tanto de operaciones como de la protección de los sistemas) fue calificado como un reto de seguridad por los respondientes de la encuesta.

A la pregunta de la encuesta que le solicitaba a los encuestados calificar el grado en el que percibían los ajustes relacionados con el trabajo remoto como un reto, la mayoría contestó que “mucho,” la segunda valoración más alta en la encuesta. Esta respuesta fue seguida de “moderadamente” y después por “bastante.”

Aunque el tema se consideró como una preocupación importante para los encuestados, no fue calificada de forma tan alta como las amenazas en línea. Tal vez esto pueda atribuirse a que han sido alrededor de 2 años desde el inicio de la pandemia y muchas organizaciones se han estado ajustando a los esquemas de trabajo remoto.

Amenazas al Trabajo Remoto

No obstante, como se destacó en el reporte de ciberseguridad del primer semestre del 2021, los temas relacionados con el trabajo remoto continuaron afectando a las organizaciones. Ya que los sistemas que permiten el trabajo remoto dependen fuertemente de los sistemas en línea y móviles, este cambio fue aprovechado por los actores maliciosos a través de estafas y malware que involucraba estos sistemas.

Uno de los retos más grandes sobre este tema, de acuerdo con la encuesta, fue la falta de preparación para la transición. Debido a que la pandemia incrementó la urgencia de un cambio abrupto al trabajo remoto, muchas entidades apenas tuvieron días para prepararse. "Las organizaciones han tenido que dar un gran salto hacia el trabajo remoto aún cuando no siempre estuvieron lo suficientemente preparadas en los procesos y en los controles de seguridad, representando un alto riesgo en términos de ciberseguridad," comentó un encuestado. Y, como destacó la misma persona, con un tiempo tan limitado, asegurar la continuidad de las operaciones fue prioridad por encima de la protección de los sistemas. Esto se ilustra a través de una respuesta en la encuesta que mencionaba cómo la organización del encuestado optó por priorizar la facilidad de las comunicaciones sin evaluar a profundidad si las herramientas que se estaban utilizando eran seguras.

Esto pudo haber sido resultado de varios factores, como la falta de medidas de seguridad previamente establecidas, la necesidad de herramientas antimalware y medios seguros para la comunicación y el acceso, y asuntos internos, según fue mencionado en las respuestas. En estas también se destaca la dificultad de convencer a algunos directivos sobre la importancia de invertir en herramientas de seguridad.

A su vez, esto afecta el nivel de los conocimientos de seguridad de los usuarios. Como algunos de los encuestados destacaron, los usuarios pueden no estar completamente conscientes de los riesgos que corren ellos y en los que colocan a sus organizaciones cuando sus esquemas de trabajo remoto no están protegidos, o cuando confían demasiado en correos, plataformas o aplicaciones.

Por ejemplo, en los escenarios profesionales, persiste el compromiso de correos electrónicos corporativos (Business Email Compromise, o BEC por sus siglas en inglés) y, debido a los esquemas de trabajo remoto, podría ser más complicado verificar los correos. Como se destacó en el reporte de ciberseguridad de la primera mitad del 2021, una razón posible para la continuada proliferación de las estafas BEC es que los actores maliciosos podrían haber ido detrás de las entidades involucradas en los programas de vacunación contra la COVID-19.

Las detecciones de intentos de BEC (especialmente fraude dirigido a los directores ejecutivos, o CEO de las empresas) a lo largo de los estados miembros de la OEA presentó una disminución del 43% en la primera mitad del 2021 comparado con el mismo periodo en el 2020. Los Estados Unidos reportaron el número más alto de detecciones de intentos de BEC, mientras que Canadá se ubicó en segundo lugar.

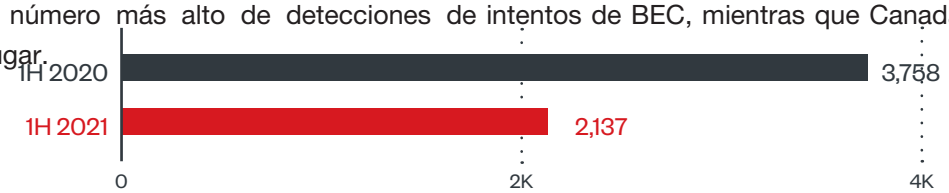

Figura 10. Detecciones de intentos de BEC (fraude del CEO) a lo largo de estados miembros de la OEA en la primera mitad del 2020 y la primera mitad del 2021

Figura 11. El índice de los estados miembros de la OEA en términos de detecciones de intentos de BEC en la primera mitad del 2021

Los sistemas que se usaron durante las cuarentenas, como las plataformas de banca en línea y sus aplicaciones móviles, también fueron víctimas de ciberataques. Respecto a las detecciones de malware de banca en línea, Estados Unidos se colocó en primer lugar con más de 7,000 detecciones, mientras que Brasil y México reportaron cada uno aproximadamente 3,000, y Canadá reportó más de 700.

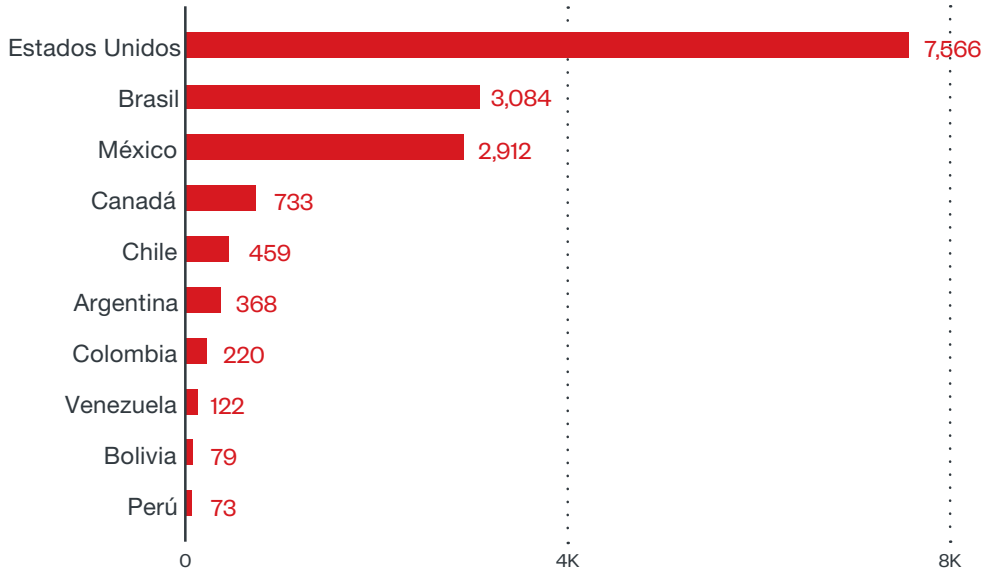

Figura 12. El top 10 de estados miembros de la OEA en términos de detecciones de malware de banca en línea en la primera mitad del 2021

En términos de aplicaciones maliciosas de Android, hubo casi un incremento del doble comparado con el número correspondiente a la primera mitad del 2020. La gran mayoría de las aplicaciones maliciosas de Android bloqueadas se observaron en los Estados Unidos, con más de 750,000, mientras que Brasil tuvo más de 66,000 y México y Canadá tuvieron cada uno más de 20,000. Las tendencias globales también mostraron un incremento en las aplicaciones maliciosas de Android bloqueadas, aunque el incremento no fue tan significativo como lo fue en la región de las Américas.

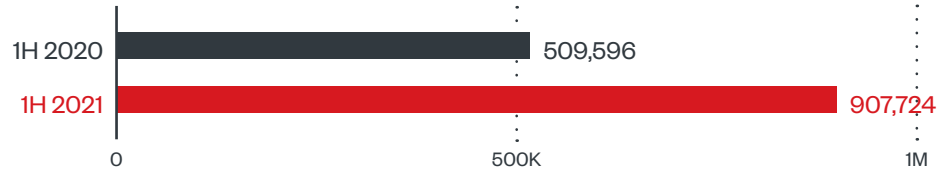

Figura 13. El número de aplicaciones maliciosas de Android bloqueadas a lo largo de los estados miembros de la OEA en la primera mitad del 2020 y en la primera mitad del 2021

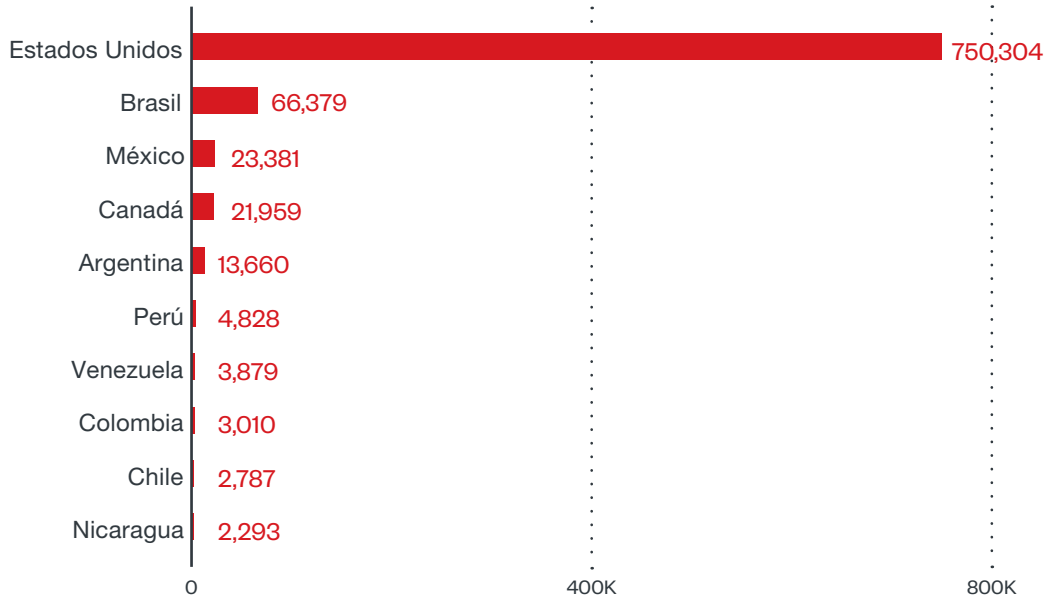

Figura 14. El top 10 de estados miembros de la OEA en términos de aplicaciones maliciosas de Android bloqueadas en la primera mitad del 2021

Amenazas relacionadas a la COVID-19

La pandemia de COVID-19 también fue utilizada por los actores maliciosos como un señuelo para esquemas de ingeniería social, agregando amenazas adicionales al trabajo remoto.

Tanto en las tendencias globales como en los datos específicos a la región de las Américas, Estados Unidos reportó el mayor número de detecciones de amenazas relacionadas con COVID-19 en la primera mitad del 2021, aunque las detecciones disminuyeron más de la mitad a comparación del mismo periodo en el 2020. Mientras tanto, algunos de los números de los estados miembros, particularmente Colombia, incrementaron de forma significativa durante la primera mitad del 2021 respecto a la primera mitad del 2020, lo cual podría indicar esfuerzos adicionales de parte de los actores maliciosos para desplegar ataques relacionados con la COVID-19 en estos países[9].

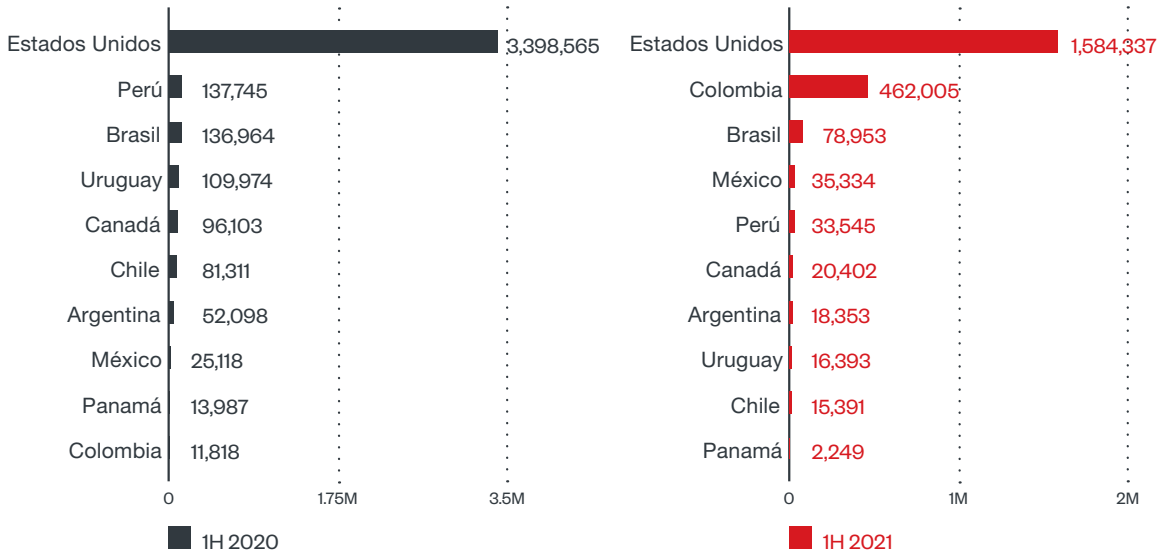

Figura 15. El top 10 de estados miembros de la OEA en términos de detecciones de amenazas relacionadas con la COVID-19 (correos de spam, URLs maliciosos y malware) en la primera mitad del 2020 y la primera mitad del 2021

Como se destacó en el reporte de ciberseguridad del primer semestre del 2021, la desinformación sirvió como un catalizador para las estafas relacionadas con la pandemia. Específicamente, los programas de vacunación y los registros de pruebas fueron de los señuelos más utilizados.

Amenazas a la Nube y IoT

Incluso antes de la pandemia de COVID-19 y de que iniciara la transición a gran escala al trabajo remoto, muchas entidades ya estaban adoptando tecnologías relativamente nuevas, como plataformas basadas en la nube y sistemas IoT o IIoT. Este cambio también trae consigo sus propias consideraciones para la mayoría de las organizaciones. La adopción de estas tecnologías debería administrarse para asegurar que los beneficios de su uso sean mayores que sus riesgos.

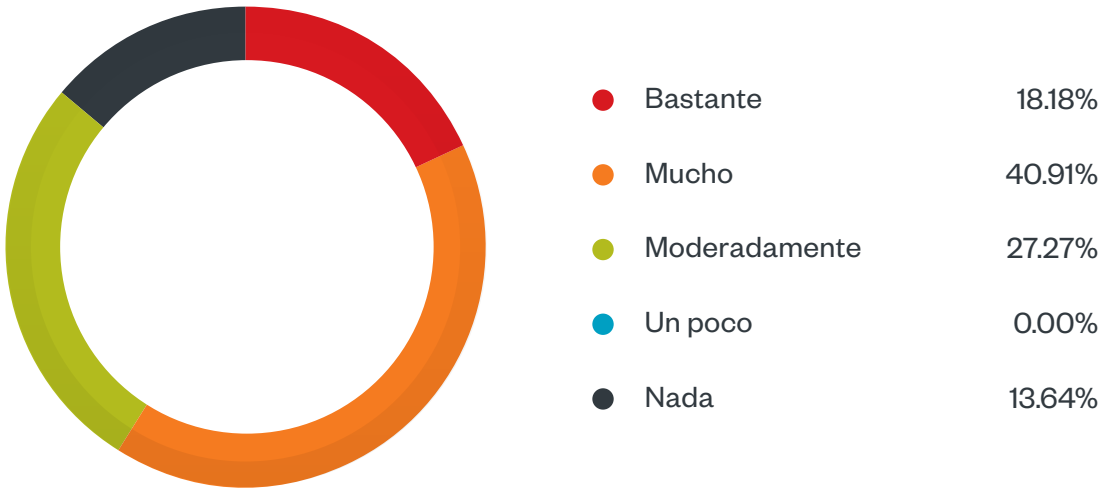

Figura 16. Cómo el ajuste a tecnologías relativamente nuevas como la nube y IoT o IIoT fue calificado como un reto de seguridad por los encuestados

En la encuesta, cuando se les pidió calificar el cambio hacia las tecnologías relativamente nuevas en términos del reto que representaban, la mayoría de los encuestados las calificaron como algo que les preocupaba "mucho." La opción con el siguiente número más alto de respuestas fue "moderadamente," seguido de "bastante" y después "nada."

Amenazas a la Nube

Algunas entidades han dado por sentada la seguridad de estas plataformas. Como enfatizó un encuestado, algunas personas podrían mantener sus sistemas con contraseñas y configuraciones de seguridad por defecto, sin saber los peligros de dejar las cosas en este estado.

Las fallas de configuración y la falta de parches y actualizaciones a los sistemas han estado entre las causas más comunes de infiltraciones exitosas a los sistemas. En el 2021, los sistemas en la nube mal configurados fueron un blanco consistente de los actores maliciosos. Como se mencionó previamente, TeamTNT se dirigió hacia las plataformas en la nube en sus campañas en el 2021.

En marzo, Trend Micro rastreó las actividades de TeamTNT y encontró un binario que contenía un shell script codificado que se utilizaba para recopilar credenciales de la nube. En esta campaña, el grupo comprometió una instancia en la nube, ejecutando un script, y después buscaba credenciales desplegadas a través del servicio de metadatos en la nube. El script creaba un archivo y lo subía a un servidor web remoto, el cual funcionaba para el grupo como un directorio abierto, y que a su vez les permitió a los investigadores de Trend Micro acceder a los archivos que se encontraban ahí. El servidor, además de ser un repositorio de datos robados, también contenía herramientas de minería de criptomonedas en Linux que el grupo desplegaba en los sistemas afectados. Trend Micro detectó más de 4,000 instancias afectadas en esta campaña.

En mayo, Trend Micro descubrió que TeamTNT continuaba dirigiéndose hacia credenciales de la nube, esta vez comprometiendo clusters en Kubernetes, una plataforma de código abierto ampliamente utilizada para la administración de aplicaciones en containers, y explotarlos para minería de criptomonedas. Trend Micro confirmó que casi 50,000 direcciones IP fueron comprometidas a lo largo de múltiples clusters.

Un tema consistente a lo largo de estos incidentes de ciberseguridad fue la presencia de elementos de minería de criptomonedas. Los mineros de criptomonedas, los cuales fueron los más detectados globalmente, fueron el tercer tipo de malware más detectado a lo largo de los estados miembros de la OEA en la primera mitad del 2021. Como fue el caso con las tendencias globales, MalXMR fue la familia de malware más detectada, y sus detecciones a lo largo de estados miembros de la OEA se incrementaron al doble respecto a la primera mitad del 2020.

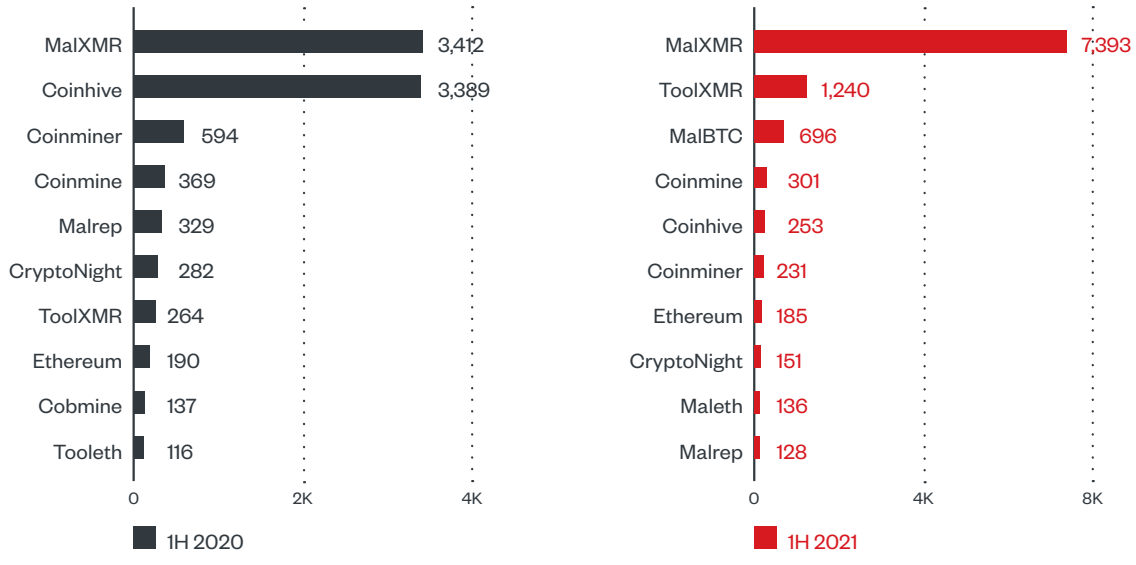

Figura 17. El top 10 de familias de malware de minería de criptomonedas en términos de detecciones a lo largo de estados miembros de la OEA en la primera mitad del 2020 y la primera mitad del 2021.

Amenazas a IoT

El IoT y las conexiones que habilitó también fueron abusadas por los actores maliciosos. Uno de los medios por los cuales los cibercriminales aprovecharon el IoT fue a través de botnets[10]. Un botnet es una red de computadoras o dispositivos secuestrados, o bots controlados de forma remota por un hacker a través de un malware de botnet implantado en los sistemas infectados.

Las detecciones relacionadas con botnets a lo largo de los estados miembros de la OEA consistieron en su mayoría de aquellas que se encontraron en el hemisferio norte. Las detecciones de esta subregión también comprendieron una porción importante de las detecciones globales de botnets: más del 10% de las conexiones de botnets y más del 30% de los servidores de comando y control (C&C) para botnets.

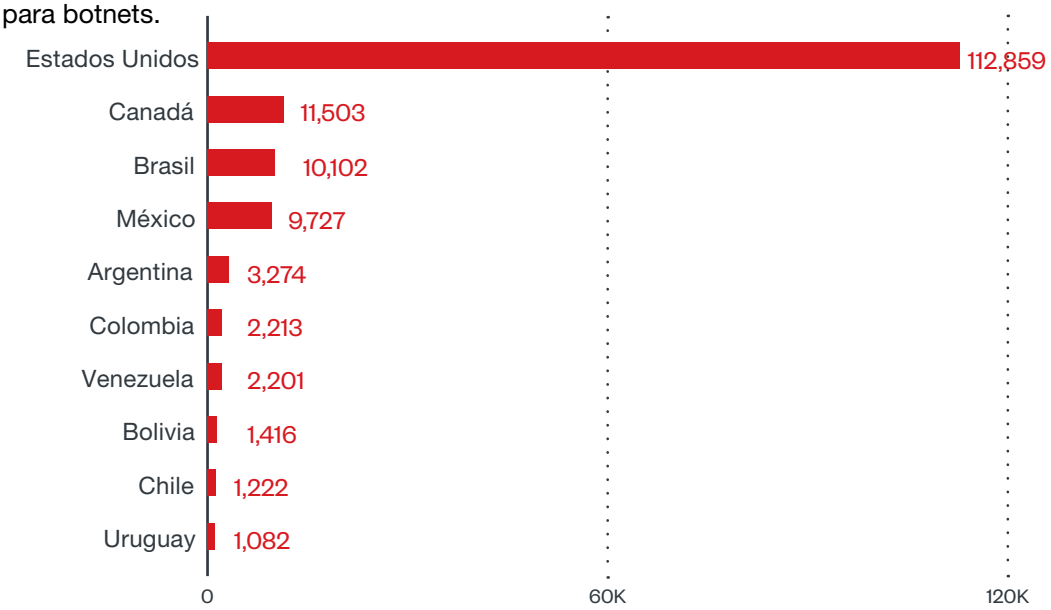

Figura 18. El top 10 de estados miembros de la OEA en términos de detecciones de conexiones de botnets en la primera mitad del 2021

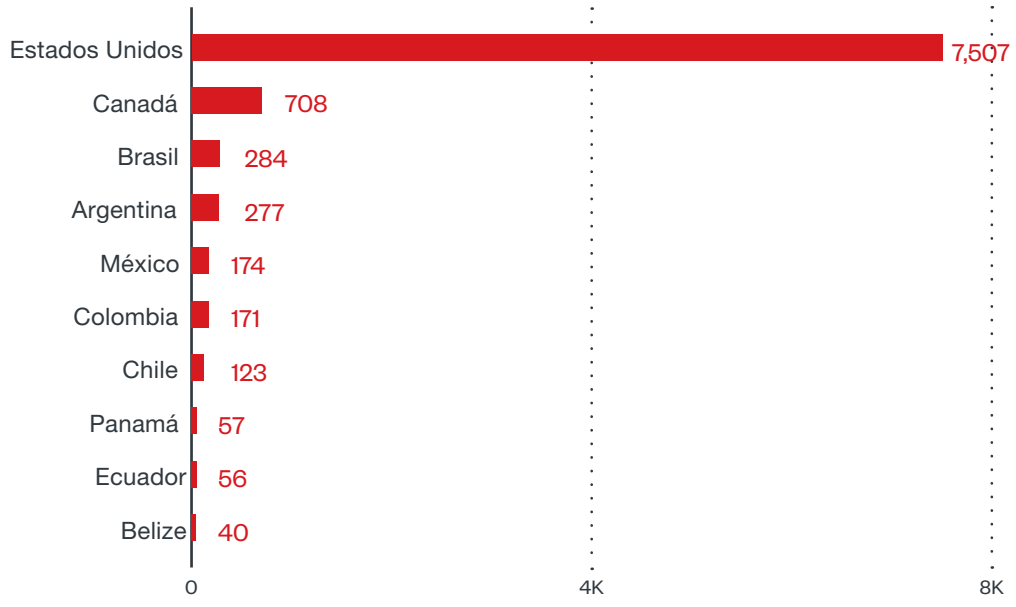

Figura 19. El top 10 de los estados miembros de la OEA en términos de detecciones de servidores C&C de botnets en la primera mitad del 2021

Una de las familias de malware de botnets IoT que Trend Micro observó en el 2021 fue VPNFilter,[11] una ciberamenaza antigua que aún se encuentra activa al día de hoy. Este malware compromete routers y dispositivos de almacenamiento a través de cuentas backdoor y se aprovecha de dispositivos de vendors conocidos.

Las nuevas tecnologías ofrecen beneficios prometedores, pero algunos de los encuestados reconocieron que no están libres de riesgos. Estos riesgos incluyen el incremento de la superficie de ataque: "Las nuevas tecnologías como IoT y 5G representan un alto riesgo a la seguridad, ya que expanden significativamente la superficie de ataque y dan lugar a nuevas amenazas que se están volviendo cada vez más sofisticadas," dijo uno de los encuestados

Además de la amenaza que representan los botnets, Trend Micro también identificó los riesgos y escenarios de ciberataques en otras tecnologías IoT como las redes de campus de 5G[12] y LoRaWAN.[13] Un mejor conocimiento de las amenazas y las herramientas adecuadas para evaluar la seguridad, como la herramienta LoRaPWN[14] para LoRaWAN, pueden ayudar a prevenir los daños que resultan de las amenazas.

Sin embargo, la falta de experiencia y confianza entre los usuarios podría a veces obstaculizar una facilitación segura. Esta curva de aprendizaje, aunque es parte inevitable del proceso, también podría exponer inadvertidamente a los sistemas y, a su vez, poner en riesgo a toda la organización.

Para mitigar los riesgos, de acuerdo con un encuestado, debe enfatizarse la importancia de reforzar las políticas técnicas de la ciberseguridad, especialmente cuando se trata de estas plataformas. Las políticas establecidas, incluyendo la configuración adecuada y las actualizaciones puntuales, pueden ayudar en la adopción segura de las nuevas tecnologías.

Conclusión

Como en el resto del mundo, una ola de ciberamenazas afectó a entidades en la región de las Américas durante el primer semestre del 2021. Aunque algunos de los hallazgos fueron similares a aquellos de las tendencias globales de acuerdo con los datos recopilados, otros mostraron resultados diferentes. Esto podría tal vez atribuirse a cómo los actores maliciosos, atraídos por blancos lucrativos, influenciados por las políticas de ciberseguridad de un país o una región y otras motivaciones, ajustaron las tácticas y herramientas que utilizaron dependiendo del país o la región que buscaban infiltrar.

Con un mejor entendimiento de las ciberamenazas que afectaron a los estados miembros de la OEA, la pregunta ahora es: ¿cómo puede usarse este conocimiento para prepararnos mejor para el futuro?

Durante la encuesta, se le preguntó a los encuestados cómo anticipaban que su industria o país enfrentaría los retos que se desarrollarían en los siguientes 6 a 12 meses. Las opciones incluían que estos retos podrían volverse aún mayores o que mejorarían. La mayoría escogió la primera opción.

Figura 20. Cómo los encuestados anticiparon que su industria o país lidiará con los retos que se están desarrollando en los próximos 6 a 12 meses

Una de las razones principales por la cual la mayoría de los encuestados esperan que los desafíos se vuelvan aún mayores fueron las dificultades que podrían surgir al intentar mantener el paso con las nuevas tecnologías, así como actualizaciones a las existentes, especialmente en los esquemas de trabajo remoto o híbrido donde cada vez están implementando éstas. “La velocidad con la cual la tecnología y las soluciones interconectadas se están desarrollando e implementando no es la misma que la aplicación de los controles,” dijo un encuestado. “Aún hay una falta de conocimiento acerca de los riesgos a nivel general.”

Asimismo, llama la atención la continua evolución de las ciberamenazas, como expresó un encuestado: “Las amenazas se van a volver más sofisticadas precisamente porque los criminales van a aprovechar los nuevos ambientes.” La falta de presupuesto también fue destacada en algunas respuestas como una de las razones.

Al otro lado del espectro, algunos encuestados creían que las preocupaciones de ciberseguridad podrían administrarse mejor en los siguientes 6 a 12 meses. Esto se debió en su mayoría al haberse podido ajustar a meses del inicio de la pandemia, así como la implementación de estrategias estándar de ciberseguridad, como las estrategias nacionales de ciberseguridad (NCSs) y las herramientas de seguridad.

Respecto a las preocupaciones de seguridad (además de las ya mencionadas en las preguntas de la encuesta) que los encuestados estaban anticipando que escalarán en los próximos 12 meses, los encuestados mencionaron lo siguiente: ciberamenazas como el abuso de VPNs (redes virtuales privadas) y el phishing, la situación actual en el país como una elección venidera que podría incentivar a los cibercriminales a ir detrás de los servicios públicos y personal y recursos inadecuados para la ciberseguridad.

Mirando hacia el Futuro

La incertidumbre y preocupaciones que rodean a las amenazas no son sin fundamento, ya que las amenazas continúan evolucionando rápidamente. El reporte de predicciones de ciberseguridad para el 2022 de Trend Micro, titulado “Hacia un Nuevo Momentum,”[15] predice en qué se enfocarán en este año los actores maliciosos, con la idea de equipar a las entidades con el conocimiento sobre qué deben cuidar. Los temas de ciberseguridad destacados en el reporte de predicciones reflejan aquellos que han emergido en la región de las Américas:

- Los operadores de ransomware se enfocarán en la extorsión sobre la encriptación, y los servidores de empresas que están desprotegidos servirán como foco de los ataques de ransomware.
- Con el enfoque de los equipos de seguridad en el ransomware, existirá una oportunidad para los ataques tradicionales y ataques-como-servicio para mejorar sus herramientas.
- Los actores maliciosos continuarán encontrando nuevos propósitos para vulnerabilidades más antiguas así como la explotación de nuevas vulnerabilidades, incluyendo fallas encontradas en las plataformas que se utilicen para trabajo remoto.
- Los datos de IoT, especialmente la información de autos conectados, serán un blanco para los cibercriminales y las empresas necesitarán tomar medidas contra las brechas de datos.
- Botnet-como-servicio, Diseñado para comprometer y controlar de forma simultánea plataformas basadas en la nube y IoT, surgirán como una amenaza rampante.

La importancia de la Preparación en el Panorama de Ciberseguridad

En el 2021, las entidades en los estados miembros de la OEA y países alrededor del mundo tuvieron que defenderse contra las amenazas que provenían desde todos los ángulos. Ahora que estas amenazas han sido identificadas, ¿qué pueden hacer las entidades para continuar el camino hacia adelante? La buena noticia es que, al conocer cuáles son las amenazas prevalentes en el panorama de ciberseguridad, las entidades pueden tomar acciones para incrementar la seguridad de sus sistemas.

De acuerdo con los resultados de la encuesta y los datos presentados en este reporte, las entidades se beneficiarán de tomar las siguientes medidas para mejorar su postura general de ciberseguridad:

Incrementar el conocimiento de los usuarios en las mejores prácticas para evitar las amenazas. Pasos sencillos como nunca hacer click en vínculos o descargar archivos adjuntos en correos provenientes de desconocidos, mantener el software y las aplicaciones parchados y actualizados y utilizar autenticación multifactor, entre otras mejores prácticas, pueden ayudar a proteger a las entidades contra las ciberamenazas. Es por lo tanto crítico asegurar que los empleados conocen estos pasos, ya que estas medidas pueden fácilmente pasarse por alto.

Establecer políticas y estrategias de ciberseguridad específicas y accionables. A nivel administrativo, las entidades deben priorizar el establecimiento de políticas y estándares de ciberseguridad. Por ejemplo, las entidades pueden implementar el modelo Zero Trust, un enfoque arquitectónico que asume que cualquier usuario o dispositivo desconocido que intente conectarse a los sistemas y aplicaciones de una organización, sin importar si el usuario o dispositivo ya se encuentra dentro de la red o no, debe ser verificado antes de que se le otorgue el acceso y se la considere de confianza.

Evaluar los riesgos cibernéticos y configurar adecuadamente las nuevas tecnologías. La pandemia de COVID-19 ha cambiado de manera indefinida la forma de trabajar, y se continuarán adoptando más herramientas para facilitar el trabajo remoto o híbrido. Las entidades, por lo tanto, deben continuar evaluando los riesgos de las tecnologías incorporadas y asegurar que están configuradas apropiadamente. Las entidades también deben de emplear controles para aplicaciones y accesos, especialmente si sus empleados acceden a aplicaciones y datos críticos fuera de la oficina.

Destinar recursos para obtener las herramientas necesarias para una protección mejorada. Las entidades deben de adoptar soluciones de ciberseguridad que ayuden a ofrecer visibilidad para el monitoreo proactivo, detección avanzada de amenazas para detectar de forma más temprana los ciberataques y datos correlacionados a lo largo de múltiples capas (correo electrónico, endpoints, servidores, workloads en la nube y redes) para ofrecer una perspectiva más amplia sobre los hallazgos, entre muchos otros beneficios. Estos pueden ayudar a las entidades asegurar una protección continua contra las ciberamenazas persistentes.

En lo general, un enfoque de ciberseguridad que esté interconectado a lo largo de todas las capas, con la optimización de las herramientas de ciberseguridad que puedan detectar y bloquear la diversificación de los ciberataques, puede habilitar la protección de una entidad contra los actores maliciosos que pueden infiltrar los sistemas desde distintos puntos de entrada

Anexos

Metodología

Los datos presentados en este reporte toman en cuenta los datos de la infraestructura de Trend Micro Smart Protection Network. Los datos cubren Las fechas desde el 1 de enero al 30 de junio de 2021, e incluyen a los siguientes países en la región de las Américas:

- Antigua y Barbuda
- Argentina
- Bahamas
- Barbados
- Belize
- Bolivia
- Brasil
- Canadá
- Chile
- Colombia
- Costa Rica
- Cuba
- Dominica
- República Dominicana
- Ecuador
- El Salvador
- Granada
- Guatemala
- Guyana
- Haití
- Honduras
- Jamaica
- México
- Nicaragua
- Panamá
- Paraguay
- Perú
- San Cristóbal y Nieves
- Santa Lucía
- San Vicente y las Granadinas
- Suriname
- Trinidad y Tobago
- Estados Unidos
- Uruguay
- Venezuela

Aviso de Responsabilidad de Datos

Los datos analizados para y presentados en este reporte provienen de los sensores de Trend Micro Smart Protection Network (SPN), el equipo de Philippines Threat Hunting, el equipo de Mobile App Reputation Service (MARS), la solución Smart Home Network (SHN), IoT Reputation Service (IoTRS) e investigadores.

Los datos son un resumen de la información recopilada por los sensores y los parámetros que tuvo el equipo de investigación durante la creación del reporte. Los datos podrían cambiar en retrospectiva debido a cualquier mejora aplicada a los sensores y parámetros en el futuro.

La mayoría de los datos proviene de los productos y soluciones que Trend Micro ha desplegado en el mercado. Un pequeño porcentaje de los datos proviene de fuentes externas (a través de la colocación de honeypots o el intercambio de datos con otras empresas). Por lo tanto, los datos presentados pueden considerarse como datos de clientes.

Los números de detecciones se derivan de la cobertura de los sensores de la SPN distribuidos de manera global. Por lo tanto, los datos se correlacionan fuertemente con cuántos productos Trend Micro vende y despliega en cada país, y cuántos clientes activan el mecanismo de retroalimentación, lo cual le permite a Trend Micro recopilar los datos de amenazas.

Como un ejemplo hipotético, si Trend Micro tiene una participación de mercado del 50% en Malasia y solamente una participación de mercado del 20% en Tailandia, los sensores naturalmente detectarían más amenazas en Malasia que en Tailandia, simplemente porque hay más sensores en Malasia. Sin embargo, esto no significaría necesariamente que existen más ciberamenazas en Malasia que en Tailandia.

Los sensores, por defecto, están desactivados. Los clientes pueden elegir activarlos para una mejor protección. Una vez que se detectan las ciberamenazas, estas son eliminadas de los ambientes de TI de los clientes.

No hay normalización aplicada a los datos.

Encuesta Regional

Para complementar los datos de la región de las Américas, se distribuyó un cuestionario a oficiales públicos y otros sectores en la región a través de la red CSIRTAmericas de la OEA/CICTE. Estos datos cualitativos sobre el estado actual de la ciberseguridad fueron más allá de los números y obtuvieron insights de las personas en posiciones clave en organizaciones con sede en los estados miembros de la OEA.

Aviso

La OEA y Trend Micro distribuyeron una encuesta en línea a varias organizaciones con sede en los estados miembros de la OEA. Los resultados de este cuestionario no son representativos de los 35 estados miembros; no puede asumirse que los resultados reflejan las posturas institucionales de cada parte interesada. Sin embargo, aunque se requiere un estudio más profundo para obtener un mejor entendimiento de los temas en cuestión y como se les percibe en la región, se espera que el análisis de los datos recopilados a través de la encuesta brinden alguna claridad hacia un mejor entendimiento de los retos de ciberseguridad en la región.

Algunas de las respuestas fueron traducidas del Inglés.

La encuesta se envió en septiembre de 2021. Se recibieron 22 respuestas.

Cuestionario Regional

Reporte Especializado Trend Micro OEA

1. ¿Cómo calificaría los siguientes temas en términos del reto que representan a su industria/país?
    - Lidiando con amenazas en línea (ransomware, ataques dirigidos, estafas, etc.)
    - Bastante
    - Mucho
    - Moderadamente
    - Un poco
    - Nada

    Por favor comparta detalles específicos sobre los retos que encuentra.

2. Ajustarse a esquemas seguros de trabajo remoto debido a la COVID-19 (tanto en términos de operaciones y de proteger a las organizaciones)

    - Bastante
    - Mucho
    - Moderadamente
    - Un poco
    - Nada

    Por favor comparta detalles específicos sobre los retos que encuentra.

3. Cambiar a nuevas tecnologías (plataformas basadas en la nube, IoT, IIoT, etc.)

    - Bastante
    - Mucho
    - Moderadamente
    - Un poco
    - Nada

    Por favor comparta detalles específicos sobre los retos que encuentra.

4. ¿Cómo anticipa que su industria/país lidiará con estos desafíos que se desarrollarán en los próximos 6 a 12 meses?

    - Anticipo que estos desafíos mejorarán en los próximos 6 a 12 meses
    - Anticipo que estos desafíos se volverán aún mayores en los próximos 6 a 12 meses

    Además de lo discutido anteriormente, ¿existe una amenaza o preocupación de seguridad que está anticipando usted que escale en los próximos 12 meses? Por favor detalle sobre la amenaza de ciberseguridad identificada.

Referencias

1. Trend Micro. (Sept. 14, 2021). *Trend Micro.* "Attacks from All Angles: 2021 Midyear Cybersecurity Report." Accessed on Nov. 3, 2021, at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/attacks-from-all-angles-2021-midyear-security-roundup.
2. Mayra Fuentes et al. (June 8, 2021). *Trend Micro.* "Modern Ransomware's Double Extortion Tactics and How to Protect Enterprises Against Them." Accessed on Nov. 3, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/modern-ransomwares-double-extortion-tactics-and-how-to-protect-enterprises-against-them.
3. Trend Micro Research. (Jan. 26, 2021). Trend Micro. "Examining A Sodinokibi Attack." Accessed on March 7, 2022, at https://www.trendmicro.com/en_us/research/21/a/sodinokibi-ransomware.html.
4. Ericka Pingol. (June 4, 2021). *Trend Micro.* "Modern Ransomware's Double Extortion Tactics and How to Protect Enterprises Against Them." Accessed on Nov. 3, 2021, at https://www.trendmicro.com/en_us/research/21/f/meat-supply-giant-jbs-suffers-cyberattack.html.
5. Trend Micro. (May 12, 2021). *Trend Micro.* "What We Know About the DarkSide Ransomware and the US Pipeline Attack." Accessed on Nov. 3, 2021, at https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html.
6. David Fiser and Alfredo Oliveira. (March 9, 2021). *Trend Micro.* "TeamTNT Continues Attack on the Cloud, Targets AWS Credentials." Accessed on Nov. 3, 2021, at https://www.trendmicro.com/en_us/research/21/c/teamtnt-continues-attack-on-the-cloud--targets-aws-credentials.html.
7. Magno Logan and David Fiser. (May 25, 2021). *Trend Micro.* "TeamTNT Targets Kubernetes, Nearly 50,000 IPs Compromised in Worm-like Attack." Accessed on Nov. 3, 2021, at https://www.trendmicro.com/en_us/research/21/e/teamtnt-targets-kubernetes--nearly-50-000-ips-compromised.html.
8. Gilbert Sison, Abraham Camba, and Ryan Maglaque. (Jan. 20, 2021). *Trend Micro.* "Investigation into PlugX Uncovers Unique APT Technique." Accessed on Nov. 3, 2021, at https://www.trendmicro.com/en_us/research/21/a/xdr-investigation-uncovers-plugx-unique-technique-in-apt-attack.html.
9. Jared S. Hopkins, Kim Mackrael, and Giovanni Legorano. (Aug. 12, 2021). *The Wall Street Journal*. "Covid-19 Vaccine Scammers Target Authorities in Dozens of Countries Including Italy and Colombia." Accessed on Nov. 3, 2021, at https://www.wsj.com/articles/covid-19-vaccine-scammers-target-authorities-in-dozens-of-countries-including-italy-and-colombia-11628760600.
10. Trend Micro. (n.d.). *Trend Micro.* "Botnet." Accessed on Nov. 3, 2021, at https://www.trendmicro.com/vinfo/us/security/definition/botnet.
11. Stephen Hilt, Fernando Merces. (Jan. 19, 2021). *Trend Micro.* "VPNFilter Two Years Later: Routers Still Compromised." Accessed on Nov. 3, 2021, at https://www.trendmicro.com/en_us/research/21/a/vpnfilter-two-years-later-routers-still-compromised-.html.
12. Philippe Z Lin et al. (May 27, 2021). *Trend Micro.* "The Transition to 5G: Security Implications of Campus Networks." Accessed on Nov. 3, 2021, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/the-transition-to-5g-security-implications-of-campus-networks.
13. Sébastien Dudek. (Jan. 26, 2021). *Trend Micro.* "Low Powered and High Risk: Possible Attacks on LoRaWAN Devices." Accessed on Nov. 3, 2021, at https://www.trendmicro.com/en_us/research/21/a/Low-Powered-but-High-Risk-Evaluating-Possible-Attacks-on-LoRaWAN-Devices.html.
14. Sébastien Dudek. (Feb. 19, 2021). *Trend Micro.* "Gauging LoRaWAN Communication Security with LoraPWN." Accessed on Nov. 3, 2021, at https://www.trendmicro.com/en_us/research/21/b/gauging-lorawan-communication-security-with-lorapwn.html.
15. Trend Micro (Dec. 7, 2021). *Trend Micro.* "Toward a New Momentum: Trend Micro Security Predictions for 2022." Accessed on Dec. 17, 2021 at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2022.

TREND MICRO™ RESEARCH

Trend Micro, líder global en ciberseguridad, ayuda a hacer del mundo un lugar más seguro para el intercambio de información digital.

Trend Micro Research está potenciado por expertos apasionados por el descubrimiento de nuevas amenazas, compartir insights clave y el apoyo a esfuerzos para detener a los cibercriminales. Nuestro equipo global ayuda a identificar millones de amenazas diariamente, lidera a la industria en revelaciones de vulnerabilidades y publica investigaciones innovadoras sobre nuevas técnicas de amenazas. trabajamos continuamente para anticipar nuevas amenazas y entregar investigaciones profundas.

www.trendmicro.com

TREND MICRO™ | research