CROWDSTRIKE

2025

INFORME SOBRE EL PANORAMA DE AMENAZAS EN AMÉRICA LATINA

Tabla de Contenidos

Resumen ejecutivo

El informe sobre el panorama de las amenazas en América Latina para el 2025 de CrowdStrike proporciona insights clave sobre la actividad cibernética en América Central, América del Sur, el Caribe y México, y ofrece inteligencia sobre intrusiones selectivas, cibercrimen y hacktivismo. Diseñado para informar a las partes interesadas de la región, el informe examina las amenazas emergentes y las tácticas de los adversarios, equipando a las organizaciones con la inteligencia necesaria para navegar por el cambiante panorama de seguridad de América Latina (LATAM).

Este informe es elaborado por el equipo de Counter Adversary Operations de CrowdStrike, que integra a dos grupos estrechamente alineados. El equipo de Inteligencia de CrowdStrike ofrece informes procesables que identifican nuevos adversarios, rastrean tus actividades y supervisan las amenazas cibernéticas emergentes en tiempo real. El equipo OverWatch de CrowdStrike aprovecha esta inteligencia y realiza una cacería de amenazas proactiva a través de la telemetría del cliente detectando y abordando la actividad maliciosa antes de que se intensifique.

A lo largo del 2024, Inteligencia de CrowdStrike observó tendencias macro y micro que dan forma a la postura de ciberseguridad de LATAM. Las macrotendencias cibernéticas que trascendieron los límites regionales y las fronteras de los estados-nación incluyen el refuerzo por parte de los gobiernos de sus infraestructuras nacionales de ciberseguridad, así como la colaboración y el intercambio de conocimientos con socios extranjeros. A nivel microeconómico, las tendencias incluyen a gobiernos que abordan asuntos políticos delicados, como la inclusión de proveedores chinos de tecnología en el proceso de licitación de contratos públicos, la gestión eficaz de la tecnología de IA y gobiernos que anuncian investigaciones sobre el armamento nacional de spyware para vigilar a oponentes políticos.

América Latina siguió siendo un objetivo creciente para los actores de ciberamenazas tanto regionales como globales. En el momento de este informe, Inteligencia de CrowdStrike rastrea a seis adversarios identificados, OCULAR SPIDER, BLIND SPIDER, ODYSSEY SPIDER, PLUMP SPIDER, SAMBA SPIDER y SQUAB SPIDER, que están basados en la región o que la tienen como objetivo principal. Estos adversarios cuentan también con la ayuda de adversarios regionales, tales como ROBOT SPIDER, quienes operan el crypter como servicio (CaaS) *CryptersAndTools*(o *Fsociety*). Para evitar la detección, los actores de amenazas enfocados en América Latina continúan priorizando la evasión de defensas mediante la adopción de tácticas, técnicas y procedimientos (TTPs) novedosos, incluidos el uso de lenguajes de programación más modernos, como Rust; esta actividad resalta el interés de los actores de amenazas de adaptarse al ecosistema de cibercrimen actual.

Aunque los adversarios con vínculos al estado de China, Colombia, la República Popular Democrática de Corea (RPDC) y Rusia representan una pequeña fracción de la actividad global que tiene por objetivo LATAM, sus estrategias de ataque dependen en gran medida de factores geopolíticos, prioridades sectoriales y acontecimientos externos; por lo tanto, suelen alinear las operaciones con los objetivos estratégicos nacionales y las tendencias emergentes.

Los acontecimientos geopolíticos y la percepción de problemas de gobernanza nacional específicos de cada país fueron los principales impulsores de la actividad hacktivista global contra los países de LATAM, mientras que las entidades gubernamentales regionales aprovecharon la tecnología de vigilancia para apaciguar el malestar o la disidencia.

A medida que el panorama de las amenazas cibernéticas en LATAM continúa evolucionando, las organizaciones deben mantenerse vigilantes contra una diversa gama de adversarios, desde grupos cibercriminales hasta actores respaldados por el Estado y hacktivistas. Al aprovechar las estrategias de seguridad basadas en la inteligencia, las partes interesadas regionales pueden reforzar sus defensas, mitigar los riesgos y adelantarse a las amenazas emergentes en un panorama de amenazas cada vez más complejo.

Figura 1. Tendencias cibernéticas en América Latina

CONVENCIÓN DE NOMBRES

ADVERSARIO	ESTADO-NACIÓN O CATEGORÍA
BEAR	RUSIA
BUFFALO	VIETNAM
CHOLLIMA	RPDC (COREA DEL NORTE)
CRANE	REPÚBLICA DE COREA
HAWK	SIRIA
JACKAL	HACKTIVISTA
KITTEN	IRÁN
LEOPARD	PAKISTÁN
LYNX	GEORGIA
OCELOT	COLOMBIA
PANDA	REPÚBLICA POPULAR CHINA
SAIGA	KAZAJISTÁN
SPHINX	EGYPT
SPIDER	CIBERCRIMEN
TIGER	INDIA
WOLF	TURQUÍA

Descripción general de las tendencias cibernéticas

América Central

MACROTENDENCIAS

A lo largo del 2024, los gobiernos centroamericanos tomaron medidas destinadas a aprobar legislación cibernética para fortalecer su infraestructura nacional de ciberseguridad, incluido el establecimiento de marcos legales y el intento de alinear su legislación cibernética nacional con las convenciones cibernéticas internacionales. Esta legislación cibernética provocó que algunos gobiernos, como el de El Salvador, crearan agencias nacionales de ciberseguridad. En otros países, como Nicaragua, estas leyes suscitaron gran preocupación por las posibles infracciones de la privacidad de los datos (Figura 2).

En el 2024, los gobiernos centroamericanos organizaron o asistieron a foros con socios extranjeros, incluidas reuniones bilaterales con Estados Unidos y la Unión Europea (UE), casi con toda seguridad en un esfuerzo por compartir las prácticas recomendadas de ciberseguridad para fortalecer su postura cibernética nacional.

Figura 2. Tendencias cibernéticas en Centroamérica

El ejemplo más destacado de un gobierno centroamericano que aprovecha el compromiso bilateral con EE. UU. y la UE es Costa Rica. Desde que un ataque del ransomware de WIZARD SPIDER afectó al gobierno costarricense, Costa Rica ha recibido una afluencia de apoyo internacional, lo que incluye el aporte por parte de EE. UU. de 25 millones de dólares para la construcción del Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés) nacional de ciberseguridad del país.[1]

En octubre del 2024, el gobierno costarricense anunció un nuevo laboratorio de ciberinteligencia, un laboratorio forense y una red segura de intercambio de información para instituciones públicas, financiados en parte por la UE.[2]

1 http://wired.com/story/costa-rica-ransomware-conti/
https://weforum.org/stories/2024/05/latin-america-cybersecurity-report-ransomware-attacks/
https://cr.usembassy.gov/united-states-announces-25-million-to-strengthen-costa-ricas-cybersecurity/

2 https://elpais.cr/2024/10/22/costa-rica-tendra-laboratorio-forense-para-enfrentar-la-ciberdelincuencia/

MICROTENDENCIAS

La adopción de las tecnologías de la información y la comunicación (TIC) y de la tecnología de vigilancia chinas en América Central ha sido desigual; algunos países diplomáticamente más cercanos a EE. UU. siguen desconfiando de la inversión china adicional en infraestructuras, mientras que otros países han dado la bienvenida a las empresas tecnológicas chinas.

En el 2023, el gobierno de Costa Rica intentó imponer regulaciones de ciberseguridad que sirvieron como una prohibición de facto a Huawei como proveedor nacional de tecnología 5G; sin embargo, en febrero del 2024, un tribunal costarricense suspendió temporalmente esta prohibición mientras revisaba su validez legal.[3] Luego, a finales del 2024, el presidente de Costa Rica emitió un decreto que mantenía la prohibición de Huawei, alegando motivos de seguridad nacional.[4]

Además, funcionarios del gobierno costarricense presentaron una denuncia contra Huawei con acusaciones que incluían soborno, fraude y tráfico de influencias.[5] En un evento separado pero relacionado, funcionarios de EE. UU. y Costa Rica publicaron una declaración conjunta en diciembre del 2024 en la que afirmaban que una "revisión integral de ciberseguridad de la infraestructura esencial de Costa Rica... reveló que actores maliciosos con sede en China se habían infiltrado en las redes del país centroamericano".[6]

En contraste, Panamá fue más acogedora con la inversión china en TIC. En mayo del 2024, Huawei anunció que había elegido Panamá como sitio de su primer Centro de Ciberseguridad y Transparencia para América Latina, y afirmaron haber elegido a Panamá por su ubicación geográfica y enfatizaron que la creación de este centro era para intercambiar información sobre ciberseguridad y mostrar la voluntad de la empresa de "mostrar su transparencia".[7]

En el último año, la preocupación por el cibercrimen facilitado por la IA ha aumentado en América Central. En febrero del 2024, el gobierno costarricense alertó sobre el aumento de víctimas de estafas con videos falsos generados por IA en los que aparecían rostros de personajes públicos.[8] En julio del 2024, el gobierno de Belice alertó sobre un falso mensaje generado por IA del Ministro de Salud que "no fue sancionado ni producido por el gobierno".[9]

La información pública disponible sobre gobiernos centroamericanos que utilizan spyware comercial para vigilar a oponentes políticos o realizar vigilancia interna era limitada.

MÉXICO[10]

El 1 de octubre del 2024, Claudia Sheinbaum Pardo asumió la presidencia de México. Como aliada de su predecesor, Andrés Manuel López Obrador (AMLO), es casi seguro que Sheinbaum impulsará una agenda similar. Al final del mandato de AMLO, la postura de ciberseguridad del gobierno mexicano seguía siendo un trabajo en progreso y era en gran medida reaccionaria en respuesta a incidentes cibernéticos ampliamente publicitados.

---

3 https://www.rcrwireless.com/20240214/5g/costa-rican-court-suspends-exclusion-huawei-5g-provider
https://www.bnamericas.com/en/news/costa-rican-court-suspends-5g-cybersecurity-regulations

4 https://ticotimes.net/2024/12/18/costa-rica-and-u-s-jointly-identify-alleged-cyber-intrusions-from-china

5 https://observador.cr/gobierno-denuncia-penalmente-a-huawei-y-a-5-funcionarios-del-ice-por-contratos-otorgados-durante-la-ultima-decada

6 https://dialogo-americas.com/articles/costa-rica-us-cybersecurity-collaboration-uncovers-chinese-espionage/
https://x.com/usembassysjo/status/1869047401224290614

7 https://prensa.com/economia/huawei-elige-a-panama-para-crear-su-primer-centro-regional-de-ciberseguridad-y-transparencia

8 https://ticotimes.net/2024/02/28/costa-rica-issues-warning-over-surge-in-deep-fake-video-scams

9 https://lovefm.com/belize-battles-rising-cybercrime-with-advanced-ai-amidst-misinformation-concerns/

10 Nota: México se encuentra geográficamente en el continente norteamericano. Sin embargo, el país también se considera LATAM por factores socioculturales (p. ej., el uso oficial de la lengua española), lazos históricos con América Central (p. ej., poblaciones indígenas) y conexiones sociales con la región.

Desde que asumió el cargo, Sheinbaum ha centrado la innovación tecnológica en sus planes de desarrollo económico comprometiéndose a crear un centro de Ciberseguridad e Inteligencia Artificial, así como a producir de forma autónoma y nacional drones de bajo costo y tecnologías de diagnóstico y telecomunicaciones encriptadas.[11]A mediados de noviembre del 2024, el gobierno mexicano anunció planes para una Agencia Nacional de Transformación Digital y Telecomunicaciones que sería responsable de la implementación de proyectos nacionales de identidad digital, computación en la nube y tecnología satelital.[12] Además, sigue pendiente un proyecto de ley de ciberseguridad, en gran parte debido a la falta de cohesión entre legisladores y partes interesadas. De aprobarse, la legislación obligaría a crear un Centro Nacional de Ciberseguridad, que encabezaría las políticas de ciberseguridad y su implementación.[13]

América del Sur

MACROTENDENCIAS

En el 2024, los gobiernos sudamericanos se centraron en elaborar estrategias digitales nacionales, autorizar la creación de entidades nacionales de ciberseguridad y penalizar el cibercrimen. La mayor parte de la legislación cibernética dio prioridad a la elaboración
de estrategias cibernéticas o digitales nacionales, y algunos países (como Chile) establecieron además Equipos Nacionales y de Defensa de Respuesta a Incidentes de Seguridad Informática (CSIRT). Otros países, como Uruguay, aprobaron una legislación cibernética que describe su estrategia nacional de ciberseguridad a la vez que establece sanciones para cibercrímenes como el acoso en línea, las brechas de datos, el robo de identidad y el acceso no autorizado a sistemas informáticos (Figura 3).

Los gobiernos sudamericanos reforzaron su postura nacional en materia de ciberseguridad mediante acuerdos bilaterales con homólogos regionales y mundiales centrados en la cooperación en ciberdenfesa y la adhesión a convenios internacionales sobre cibercrimen. Por ejemplo, en marzo del 2024 y abril del 2024, respectivamente, los gobiernos de Argentina y Uruguay firmaron Memorándums de entendimiento (MDE) con EE. UU. para fortalecer la cooperación bilateral en ciberdefensa y las alianzas tecnológicas público-privadas.[14]

Figura 3. Tendencias cibernéticas en América del Sur

11 https://elpais.com/mexico/2024-10-02/estas-son-las-100-promesas-de-claudia-sheinbaum-como-presidenta-de-mexico.html

12 https://eleconomista.com.mx/politica/gobierno-presenta-agencia-transformacion-digital-y-telecomunicaciones-20241114-734183.html

13 https://es.wired.com/articulos/presentan-nuevo-proyecto-de-ley-para-garantizar-la-ciberseguridad-en-mexico

14 https://www.zona-militar.com/en/2024/03/26/argentina-signs-a-memorandum-of-understanding-with-the-u-s-to-strengthen-collaboration-in-cyberdefense-issues/ https://en.mercopress.com/2024/04/11/key-cooperation-deal-between-the-us-and-uruguay-signed

En noviembre del 2024, el Ministro del Interior chileno y varios representantes de la UE firmaron un acuerdo para cooperar en materia de ciberseguridad y "aumentar la ciberresiliencia" de los países de LATAM.[15] En septiembre del 2024, Paraguay se convirtió en signatario de una versión ampliada de un convenio sobre cibercrimen impulsado por la UE que actualizaba las disposiciones sobre intercambio de datos entre los proveedores de servicios de Internet (ISP) con sede en los países signatarios y las autoridades gubernamentales.[16]

Los gobiernos sudamericanos organizaron o asistieron a ejercicios militares bilaterales o multilaterales que incluían simulaciones de ciberseguridad y destacaban la creciente necesidad de abordar las operaciones cibernéticas defensivas en la estrategia militar. Por ejemplo, en agosto del 2024, Chile y Brasil celebraron su primer ejercicio bilateral Cyber Shield en Santiago de Chile, a fin de desarrollar capacidades ciberdefensivas militares y civiles haciendo que los participantes se enfrentaran a varias situaciones e incidentes para los que tenían que redactar rápidamente una respuesta a una crisis cibernética simulada.[17]

Por otra parte, en septiembre del 2024, seis unidades navales sudamericanas participaron en un ejercicio de ciberseguridad denominado UNITAS 24, que incluía ejercicios prácticos de operaciones cibernéticas.[18] Por último, en noviembre del 2024, CRUZEX, uno de los mayores ejercicios militares multinacionales de América Latina, amplió su alcance para incluir una situación cibernética.[19]

Irán emprende una "diplomacia tecnológica" con sus socios regionales de LATAM

En el 2024, Irán profundizó sus intereses regionales sudamericanos a través de lo que ha denominado "diplomacia tecnológica" e invirtió en alianzas selectivas con un pequeño grupo de gobiernos autoritarios hostiles a la influencia estadounidense en la región, particularmente Venezuela y Cuba. A finales del 2024, el Ministro de Tecnología de la Información y las Comunicaciones de Irán (MICT) visitó Venezuela y Cuba para firmar varios MDE sobre el desarrollo cooperativo de tecnología avanzada, incluidas las TIC, la IA, la gobernanza electrónica, la ciberseguridad y las operaciones de información.[20] Esta última gira de estado por América Latina es indicativa de las iniciativas tradicionales de la anterior administración presidencial iraní, lo que demuestra la continuidad de la política Irán-América Latina a través de las transiciones políticas y las administraciones presidenciales iraníes.

MICROTENDENCIAS

Los gobiernos sudamericanos adoptaron diversos enfoques para incorporar la tecnología china a su infraestructura cibernética nacional, con precios altamente competitivos que pueden erosionar la preocupación por la seguridad.

En abril del 2024, mientras Colombia construía su red 5G, expertos del sector privado advertían sobre los riesgos asociados a la tecnología proporcionada por empresas chinas.[21] Estas advertencias se realizaron tras la publicación de un informe del sector privado titulado "La huella de la tecnología china en Colombia", en el que se describía la contrapartida que supone el aumento de la sofisticación técnica para la privacidad.[22]

---

15 https://infobae.com/america/agencias/2024/11/08/chile-y-la-ue-firman-un-acuerdo-de-cooperacion-en-ciberseguridad-para-latinoamerica/

16 https://coe.int/en/web/cybercrime/-/paraguay-becomes-the-47th-state-to-sign-the-second-additional-protocol-to-the-convention-on- cybercrime

17 https://dialogo-americas.com/articles/chile-brazil-strengthen-cyber-defense-through-binational-exercise/

18 https://www.defensa.com/centro-america/armada-republica-dominicana-primera-ejercicios-cyber-unitas-24

19 https://www.southcom.mil/MEDIA/NEWS-ARTICLES/Article/3970832/cyber-operations-takes-stage-at-cruzex-2024/

20 https://www.tehrantimes.com/news/505807/Tehran-Caracas-sign-MOUs-on-ICT

21 https://dialogo-americas.com/articles/experts-warn-about-risks-from-chinas-5g-technology-in-colombia/

22 https://dialogo-americas.com/articles/warning-risks-of-chinese-technology-in-colombia/
https://asiapowerwatch.com/colombia-is-unprepared-to-handle-the-risks-of-chinese-tech-investment/

Por otra parte, en abril del 2024, el presidente brasileño Luiz Inácio Lula da Silva desestimó las preocupaciones de seguridad en relación con los acuerdos para establecer un grupo de trabajo sobre semiconductores con China y ampliar la participación china en el desarrollo de la tecnología de ciberseguridad y la infraestructura de dispositivos móviles 5G de Brasil.[23] A enero del 2025, Argentina, Bolivia, Brasil, Chile, Colombia, Ecuador, Perú, Surinam y Uruguay utilizaban o tenían previsto utilizar equipos Huawei en sus redes 5G.[24]

Los gobiernos sudamericanos tomaron medidas para hacer frente a la desinformación electoral generada por la IA, a la vez que intentaban descubrir vías para aprovechar la IA para el crecimiento socioeconómico. Por ejemplo, en febrero del 2024, el Tribunal Superior Electoral (TSE) de Brasil adoptó nuevas normas para hacer frente a la difusión de desinformación electoral en línea y restringir el uso de IA durante el proceso de campaña electoral de cara a las elecciones municipales de octubre del 2024.[25] Las nuevas regulaciones incluían normas de responsabilidad más estrictas y otras obligaciones para las plataformas en línea, y exigían que los materiales de las campañas divulgaran, colocaran marcas de agua o etiquetaran claramente el contenido generado por IA.

En marzo del 2024, la Alianza Digital Unión Europea-América Latina y Caribe (UE-ALC) debatió sobre cómo identificar y mitigar los riesgos de la IA a la vez que se aprovechan las oportunidades de crecimiento socioeconómico.[26] En agosto del 2024, representantes de 17 países de América Latina Central y del Sur se reunieron en Colombia y firmaron una declaración centrada en la gobernanza de la IA, la creación de ecosistemas y la educación.[27]

En el 2024, los gobiernos sudamericanos realizaron varias investigaciones públicas vinculadas a la vigilancia de oponentes políticos o miembros de la sociedad civil, una de las cuales dio lugar a una investigación policial y a posteriores arrestos.

En enero del 2024, las fuerzas de seguridad brasileñas investigaron a los aliados del expresidente brasileño Jair Bolsonaro por supuestamente realizar vigilancia electrónica extrajudicial a los oponentes políticos de Bolsonaro. La vigilancia supuestamente recopiló información sobre al menos 30.000 brasileños, incluidos dos jueces del Supremo Tribunal Federal (STF) y un aliado clave del actual Presidente Luiz Inácio Lula da Silva, como parte de un plan para sembrar de forma sistemática la desconfianza en el sistema electoral.[28]

En diciembre del 2024, la policía federal brasileña realizó sus primeras detenciones como consecuencia de esta investigación y detuvo a un antiguo miembro del gabinete de Bolsonaro por supuesta obstrucción a la obtención de evidencia. Por otro lado, en septiembre del 2024, el presidente de Colombia, Gustavo Petro, solicitó a la fiscalía investigar a la Dirección de Inteligencia de la Policía de Colombia (DIPOL) por la presunta compra del spyware *Pegasus* del Grupo NSO en el 2021, durante el gobierno del expresidente Iván Duque. En una emisión televisada, Petro especuló que él u otros políticos, activistas y civiles colombianos habían sido objetivo del spyware.[29]

---

23 https://www.reuters.com/technology/brazil-paves-way-semiconductor-cooperation-with-china-2023-04-14/

24 https://www.cfr.org/backgrounder/china-influence-latin-america-argentina-brazil-venezuela-security-energy-bri

25 https://freedomhouse.org/country/brazil/freedom-net/2024

26 https://www.eeas.europa.eu/eeas/exploring-potential-artificial-intelligence-latin-america-caribbean_en

27 https://www.bnamericas.com/en/news/latin-american-countries-adopt-sweeping-ai-declaration

28 https://g1.globo.com/politica/blog/andreia-sadi/post/2024/01/25/espionagem-ilegal-da-abin-atingiu-30-mil-pessoas-e-dados-foram-guardados-dados-em-israel-diz-chefe-da-pf.ghtml
https://apnews.com/article/brazil-bolsonaro-coup-plot-braga-netto-eaa04eb1ded433addc1eee2167f8b8e0

29 https://elpais.com/america-colombia/2024-09-05/petro-revela-un-documento-que-vincula-a-la-inteligencia-policial-de-la-era-duque-con-la-compra-del-software-espia-pegasus.html

CASOS ATÍPICOS

En el 2024, la postura del gobierno venezolano en materia de ciberseguridad era anómala con respecto al impulso de la región en el refuerzo de sus prácticas nacionales de ciberseguridad y que, en cambio, se centró en reprimir la disidencia, difundir información errónea, criminalizar la libertad de expresión y militarizar la legislación para mantenerse en el poder. Por ejemplo, en agosto del 2024,
el gobierno venezolano argumentó la existencia de "ciberataques" infundados para explicar el retraso en los resultados de las elecciones presidenciales. Organizaciones internacionales, como las Naciones Unidas, rechazaron estas afirmaciones y señalaron que sus investigaciones no descubrieron ninguna prueba que sugiriera que el sistema electoral de Venezuela hubiera sido víctima de un ciberataque.[30] Estos esfuerzos sugieren que es probable que el gobierno esté utilizando los incidentes de ciberseguridad como arma para obtener beneficios políticos.

En los últimos 12 meses, la administración del presidente venezolano Nicolás Maduro también censuró el contenido en línea. Por ejemplo, antes de las elecciones presidenciales de julio del 2024, Maduro supuestamente ordenó a los proveedores de servicios de Internet que bloquearan el acceso a al menos 50 medios de comunicación locales independientes y sitios web sin fines de lucro.[31]

En abril del 2024, el gobierno venezolano consideró una legislación que podría reprimir las plataformas de redes sociales, incluida una ley que criminalizaba los "mensajes prohibidos" (probablemente refiriéndose a contenido crucial del gobierno) e imponía duras sanciones; la legislatura venezolana pospuso el debate sobre el proyecto de ley en agosto del 2024.[32]

Además, en noviembre del 2024, el gobierno de Guyana acusó al gobierno venezolano de orquestar una operación cibernética ofensiva que incluía ataques de ransomware y phishing contra objetivos guyaneses para socavar la soberanía de Guyana sobre la región de Essequibo, una zona rica en petróleo que Guyana y Venezuela reclaman en una disputa territorial prolongada.

Según informa la prensa local, el gobierno guyanés identificó las organizaciones y operaciones individuales que componen el programa cibernético de Venezuela, incluidos nombres y fotografías.[33] La Inteligencia de CrowdStrike no puede corroborar estas afirmaciones actualmente; sin embargo, si las afirmaciones son ciertas, esta campaña demostraría un insight único del uso por parte de Venezuela de capacidades cibernéticas ofensivas fuera de sus propias fronteras.

---

30 https://www.voanews.com/a/no-evidence-venezuela-vote-hacked-carter-center-election-monitor-says/7734334.html
https://www.washingtonpost.com/world/2024/08/13/venezuela-election-results-un-report/

31 https://freedomhouse.org/country/venezuela/freedom-net/2024

32 https://freedomhouse.org/country/venezuela/freedom-net/2024

33 https://dpi.gov.gy/national-defence-institute-hosts-groundbreaking-ceo-cybersecurity-workshop-in-guyana/

El Caribe

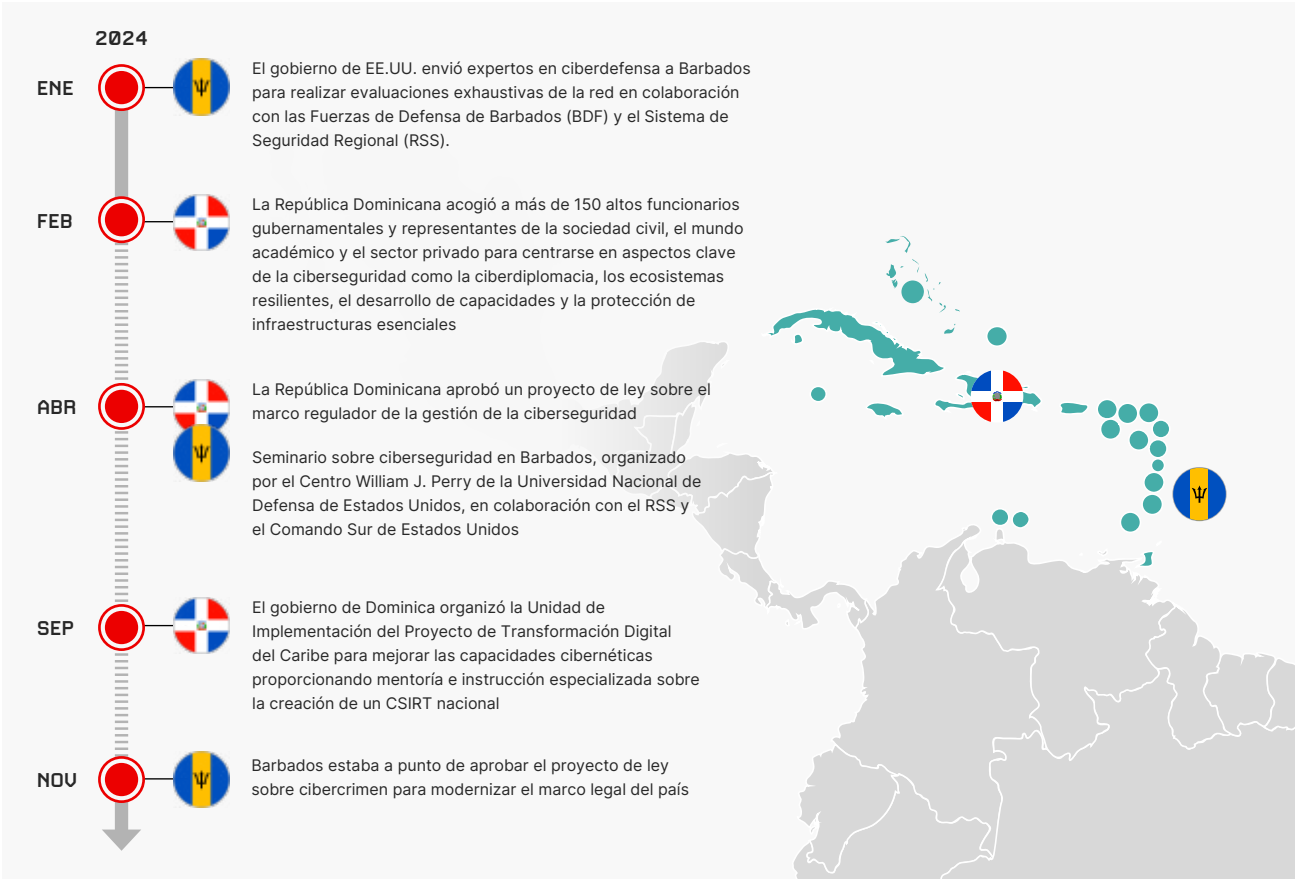

Figura 4. Tendencias cibernéticas en el Caribe

MACROTENDENCIAS

A lo largo del 2024, la Inteligencia de CrowdStrike no observó que los gobiernos caribeños aprobaran numerosas leyes cibernéticas. Sin embargo, la República Dominicana y Barbados elaboraron proyectos de ley centrados en los marcos de gestión reglamentaria de la ciberseguridad (Figura 4).[34] El proyecto de ley de República Dominicana sobre gestión de la ciberseguridad fue aprobado por el senado en abril del 2024, y el proyecto de ley de ciberseguridad de Barbados está a la espera de ser votado por el senado.[35]

Numerosos gobiernos caribeños organizaron o asistieron a reuniones bilaterales o multilaterales centradas en el intercambio rutinario de información sobre ciberseguridad y en el desarrollo de capacidades; sin embargo, a finales de enero del 2024 y principios de febrero del 2024, el gobierno de Barbados se dirigió a EE. UU. solicitando asistencia para la evaluación de la red tras una serie de ciberataques apuntados a entidades públicas y privadas.[36]

Por otra parte, en febrero del 2024, la República Dominicana acogió a funcionarios de alto rango de Sudamérica, el Caribe y la UE para debatir sobre ciberdiplomacia y protección de infraestructuras esenciales. Además, en septiembre del 2024, el gobierno de Dominica organizó la Unidad de Implementación del Proyecto de Transformación Digital del Caribe, cuyo objetivo era crear un CSIRT nacional.[37]

---

34 https://dominicantoday.com/dr/local/2024/04/10/senate-approves-cybersecurity-bill-and-other-legislative-measures/ https://www.thestkittsnevisobserver.com/bad-news-for-cybercriminals-as-barbados-bill-almost-ready-for-vote/

35 https://www.barbadosparliament.com/bills/details/741

36 https://dialogo-americas.com/articles/us-and-barbados-collaborate-on-cybersecurity/

37 https://dominicanewsonline.com/news/homepage/news/caribbean-digital-transformation-project-provides-training-to-boost- national-cyber-security/

MICROTENDENCIAS

Según parece, los gobiernos caribeños empezaron a desarrollar políticas y marcos de IA, probablemente con el fin de desarrollar un enfoque estructurado para incorporar la IA a las estrategias de gobierno digital.

Por ejemplo, en septiembre del 2024, la Comisión Económica para América Latina y el Caribe (CEPAL) analizó un estudio sobre la preparación frente a la IA y las estrategias de gobierno digital para los países del Caribe, centrado específicamente en los Pequeños Estados Insulares en Desarrollo (PEID).[38] En septiembre del 2024, el equipo especial de IA de Jamaica, creado en el 2023 para proporcionar una "base empírica para el desarrollo de una política nacional de IA", presentó sus conclusiones a la oficina del Primer Ministro jamaicano sobre cómo incorporar la IA a los sectores educativo, empresarial y gubernamental de Jamaica.[39] En noviembre del 2024, el parlamento de Granada anunció que introduciría herramientas de IA en el 2025 para uso de los legisladores, pero no ha proporcionado más información.[40]

La información pública disponible sobre las incursiones tecnológicas chinas en la región del Caribe es limitada. A enero del 2025, solo dos países caribeños, la República Dominicana y Trinidad y Tobago, utilizaban o tenían previsto utilizar equipo Huawei en sus redes 5G.[41]

La información disponible públicamente sobre gobiernos caribeños que utilizan spyware comercial para beneficio político o vigilancia nacional es limitada.

CASOS ATÍPICOS

Al igual que Venezuela, Cuba fue un caso atípico en el 2024, ya que no reforzó su política y postura de ciberseguridad nacional, y en cambio promulgó políticas que subyugaron a su población nacional, incluida la restricción del servicio de Internet durante las protestas públicas supuestamente planeando llevar a cabo operaciones de información (IO) que tienen por objetivo a las elecciones presidenciales de EE. UU., y la actualización de sus instalaciones de vigilancia electrónica.

En febrero del 2024, el gobierno cubano revocó un aumento planeado de cinco veces en los precios del combustible debido a un "ciberataque" no especificado; el viceministro de Economía cubano hizo una afirmación sin fundamento en la que atribuía el aumento a un "virus del extranjero".[42] En marzo del 2024, una organización de derechos humanos sin fines de lucro identificó al menos una interrupción de Internet en Santiago de Cuba tras una protesta pública, que la organización consideró que podría haber estado dirigida por el gobierno.[43] En junio del 2024, la comunidad de inteligencia de EE. UU. habría evaluado que el gobierno cubano probablemente realizaría IO durante las elecciones estadounidenses del 2024 para influir en la percepción de los votantes sobre los candidatos que el gobierno cubano considera hostiles a Cuba.[44]

Cuba también buscó mejorar su cooperación actual con el gobierno chino. En julio del 2024, el Centro de Estudios Estratégicos e Internacionales (CSIS), un laboratorio de ideas con sede en Washington, D.C., publicó un informe en el que se detallaban cuatro sitios activos actualizados en Cuba que realizaban operaciones de vigilancia electrónica probablemente vinculadas al gobierno chino.

Según los informes, estos sitios se encuentran entre los lugares más probables en Cuba para apoyar los esfuerzos de China a fin de llevar a cabo inteligencia de señales (SIGINT) sobre los EE. UU. El informe muestra tres sitios de vigilancia alrededor de La Habana y uno en el sureste de Cuba aproximadamente a 70 millas de la base naval de EE. UU. en la Bahía de Guantánamo.[45]

---

38 https://www.cepal.org/en/events/virtual-expert-group-meeting-harnessing-artificial-intelligence-ai-and-digital-government
https://caribbean.eclac.org/information-resources/website/selected-publications-harnessing-ai-caribbean

39 https://jis.gov.jm/cabinet-to-receive-artificial-intelligence-task-force-report/

40 https://www.jamaicaobserver.com/2024/11/27/grenada-parliament-introduce-use-ai-2025/

41 https://www.cfr.org/backgrounder/china-influence-latin-america-argentina-brazil-venezuela-security-energy-bri

42 https://www.reuters.com/world/americas/cuba-delays-feb-1-fuel-price-hike-cites-cyberattack-2024-01-31/

43 https://freedomhouse.org/country/cuba/freedom-net/2024

44 https://www.miamiherald.com/news/nation-world/world/americas/cuba/article289243045.html
https://www.dni.gov/files/ODNI/documents/assessments/NIC-Declassified-ICA-Foreign-Threats-to-the-2022-US-Elections-Dec2023.pdf

45 https://features.csis.org/hiddenreach/china-cuba-spy-sigint/

Descripción general del cibercrimen

La región de América Latina se enfrenta a varias amenazas de cibercrimen por parte de adversarios regionales y globales. Hasta la fecha, la Inteligencia de CrowdStrike ha identificado a seis adversarios con base o que tienen por objetivo principal a América Latina: OCULAR SPIDER, BLIND SPIDER, ODYSSEY SPIDER, PLUMP SPIDER, SAMBA SPIDER y SQUAB SPIDER. Aunque estos adversarios atacan casi exclusivamente a América Latina, los adversarios de caza mayor (BGH) y los adversarios globales del cibercrimen también se enfocan cada vez más a la región (Figura 5).

Otros adversarios como ROBOT SPIDER y OCULAR SPIDER desempeñaron papeles clave en el ecosistema del cibercrimen de LATAM en el 2024: ROBOT SPIDER a través de un sitio web dedicado al servicio de crypters, y OCULAR SPIDER como operador detrás de la destacada oferta de ransomware como servicio (RaaS, por sus siglas en inglés) *RansomHub*.

A lo largo del 2024, Inteligencia de CrowdStrike observó que AVIATOR SPIDER, con sede en Nigeria, RENAISSANCE SPIDER, con sede en Rusia, y SOLAR SPIDER atacaron por primera vez a entidades de la región de LATAM. Aunque AVIATOR SPIDER y SOLAR SPIDER siguieron mostrando sus tradicionales objetivos en el sector de la aviación y el sector financiero, respectivamente, estos adversarios han tenido por objetivo históricamente otras regiones geográficas.

De forma similar, RENAISSANCE SPIDER se dirige principalmente a entidades con sede en Europa Oriental. Sin embargo, en campañas separadas de enero del 2024, el adversario atacó a entidades del sector agrícola colombiano y del sector legal peruano.

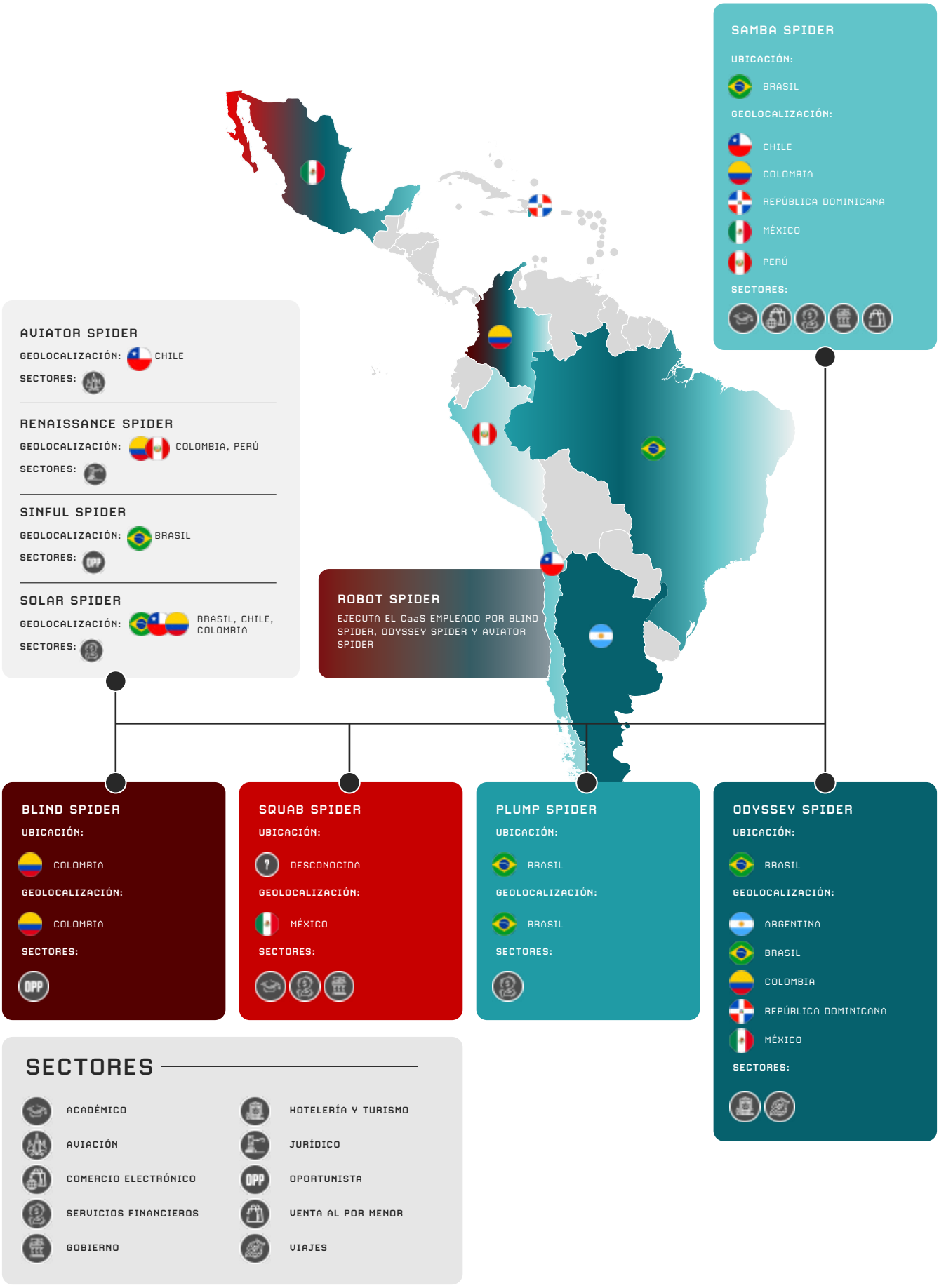

Figura 5. Adversarios de cibercrimen que se encuentran en la región de América Latina o la tienen por objetivo

Adversarios basados en LATAM

BLIND SPIDER

El adversario de cibercrimen BLIND SPIDER (también conocido como *APT-C-36* y *Blind Eagle*) atacó activamente a los sectores público y privado colombianos desde abril del 2018; sin embargo, también atacó de forma intermitente a Chile y Ecuador. BLIND SPIDER realiza campañas oportunistas de spam de gran volumen empleando contenido de phishing con temática financiera y legal, y suplantando la identidad de las autoridades gubernamentales colombianas. BLIND SPIDER distribuye documentos PDF señuelo con enlaces maliciosos que conducen a la descarga de archivos protegidos con contraseña alojados en servicios legítimos de alojamiento de archivos.

BLIND SPIDER utilizó consistentemente el crypter *Fsociety* (o *CryptersAndTools*) de ROBOT SPIDER y otros crypters genéricos para proteger y distribuir las payloads útiles de herramientas de acceso remoto (RAT) genéricas (p. ej., *AsyncRAT*, *njRAT Lime* y *Remcos*). Es probable que el adversario intente robar información confidencial relacionada con servicios financieros y correos electrónicos.

Desde mediados del 2024 hasta enero del 2025, BLIND SPIDER continuó apuntando a entidades con sede en Colombia. Si bien mantuvo su contenido de phishing con temática financiera y legal, el adversario alteró de manera regular sus métodos de entrega, incluido el uso de documentos PDF señuelo, enlaces maliciosos y, más recientemente, archivos de gráficos vectoriales escalables (SVG).

BLIND SPIDER continúa usando los encriptadores de ROBOT SPIDER (que emplean esteganografía), ya que el nombre de BLIND SPIDER apareció en una lista de clientes de ROBOT SPIDER filtrada en octubre del 2024. BLIND SPIDER también utilizó *HijackLoader* y *Roda Crypter* para distribuir sus payloads útiles RAT.

ODYSSEY SPIDER

ODYSSEY SPIDER (también conocido como *TA558*) es un adversario de cibercrimen con sede en Brasil, activo desde finales del 2018. Este adversario se dirigió sistemáticamente a los sectores de la hotelería y los viajes, principalmente en la región de LATAM y, con menor frecuencia, en América del Norte y el suroeste de Europa. Si bien ODYSSEY SPIDER varía periódicamente sus TTPs, suele emplear phishing basado en reservaciones de hotel para distribuir RATs de uso generalizado y la herramienta de captura de pantalla *CapturaTela*. ODYSSEY SPIDER utiliza descargadores de script personalizados, el cargador multietapa *Alosh* y el crypter de ROBOT SPIDER para proteger sus payloads.

Es probable que ODYSSEY SPIDER monetice sus intrusiones robando información de tarjetas de crédito de hoteles. Esta evaluación se basa en la herramienta de captura de pantalla *CapturaTela* del adversario, que toma y extrae capturas de pantalla durante un proceso de reservación en línea. Inteligencia de CrowdStrike también identificó un panel PHP, diseñado para validar información de tarjetas de crédito brasileñas, alojado en la infraestructura de ODYSSEY SPIDER.

En el 2024, Inteligencia de CrowdStrike observó que ODYSSEY SPIDER tenía por objetivo principal los sectores de la hotelería y los viajes en Argentina, Brasil, Colombia y México. El adversario aprovechó la infraestructura maliciosa de temática hotelera, incluidos dominios afectados pertenecientes a hoteles de LATAM. De forma similar, ODYSSEY SPIDER adaptó sus descargadores a objetivos del sector hotelero abriendo sitios web legítimos de reservas de hoteles y mostrando archivos señuelo relacionados con las reservas. ODYSSEY SPIDER también se dirigió a EE. UU., aprovechando la temporada de impuestos del país a principios del 2024 y principios del 2025.

PLUMP SPIDER

El adversario del cibercrimen PLUMP SPIDER, con sede en Brasil, tiene por objetivo empresas brasileñas que ofrecen servicios financieros desde noviembre del 2023. El adversario se hace pasar por personal de soporte de TI durante llamadas de phishing de voz (vishing) para incitar a los objetivos a descargar herramientas de monitoreo y administración remotos (RMM) y SoftEther VPN. PLUMP SPIDER suele desplegar herramientas de reconocimiento personalizadas del protocolo ligero de acceso a directorios (LDAP) para obtener credenciales de usuario y ha utilizado una herramienta personalizada a fin de obtener saldos de cuentas de usuario para una plataforma de pago. Es probable que el adversario monetice sus intrusiones realizando pagos fraudulentos.

Entre enero del 2024 y enero del 2025, PLUMP SPIDER creó y utilizó varios dominios que imitaban servicios de TI, en los que alojaba sus supuestas herramientas de administrador Ammyy Admin, DWAgent, HopToDesk, RustDesk, Supremo, TeamViewer y SoftEther VPN. Aunque el adversario utilizó principalmente estos dominios para engañar a las víctimas en sus llamadas de vishing, también utilizó el dominio `suporte[.]re` en una posible campaña de phishing con un documento PDF señuelo casi idéntico al empleado en una campaña de ODYSSEY SPIDER en junio del 2023. El dominio albergaba un crypter que compartía considerables solapamientos con la herramienta *CryptersAndTools* (también conocida como *Fsociety*) de ROBOT SPIDER.

SAMBA SPIDER

SAMBA SPIDER es un adversario de cibercrimen con sede en Brasil que opera el troyano bancario *Mispadu*, que apareció por primera vez en el 2019. Este adversario ataca a instituciones financieras y entidades de comercio electrónico en países de habla hispana y portuguesa, con el objetivo de capturar información de identificación personal (IIP). En el 2024, SAMBA SPIDER mantuvo un ritmo operativo constante aprovechando la actualización regular de la cadena de infección empleada para distribuir *Mispadu*. Actualmente, SAMBA SPIDER ataca a entidades de habla hispana y portuguesa en República Dominicana, México, Chile, Colombia, Perú, Italia, Portugal y España.

A lo largo del 2024, SAMBA SPIDER propagó campañas de spam por correo electrónico utilizando una cadena de infección actualizada, que incluye componentes de scripting nuevos y actualizados. Las campañas entregaban una payload de primera etapa con el prefijo de nombre de archivo `*Factura*_`.

SQUAB SPIDER

SQUAB SPIDER (también conocido como *FIN13*) es un adversario de cibercrimen que ataca principalmente a instituciones financieras con sede en México. Según estudios de la industria, este adversario estuvo activo desde al menos el 2016.[46] SQUAB SPIDER utiliza una amplia gama de webshells para explotar servidores web vulnerables con el fin de obtener acceso inicial y se basa en *BLUEAGAVE* bind shells o simples escuchas para el movimiento lateral. Aunque los métodos de monetización de SQUAB SPIDER no están confirmados, el hecho de que el adversario tenga por objetivo a bases de datos o archivos de registro específicos es más coherente con un comportamiento de cibercrimen selectivo que con el robo oportunista de datos y la extorsión.

En mayo del 2024 y agosto del 2024, Inteligencia de CrowdStrike identificó tres intrusiones de SQUAB SPIDER en dos entidades gubernamentales mexicanas y una institución académica con sede en México. Estas intrusiones suponen un cambio con respecto a los ataques históricos del adversario contra instituciones financieras. A pesar de la ampliación del alcance de los objetivos del adversario, mantuvieron TTPs consistentes, incluidos la afectación de servidores web vulnerables para el acceso inicial, el despliegue de escuchas (webshells JSP de baja prevalencia) y la realización de sus típicos comandos de reconocimiento. El adversario fue observado por última vez a finales de enero del 2024 apuntando a una empresa de telecomunicaciones.

Caza mayor

En el 2024, Inteligencia de CrowdStrike documentó un total de 291 víctimas basadas en LATAM nombradas en sitios web de filtración de datos de extorsión y ransomware.[47] Aunque esta cifra solo representa aproximadamente el 5% de los 5276 incidentes documentados en todo el mundo, supone un aumento del 15% con respecto a los 254 incidentes documentados en la región en el 2023. No hay evidencia que sugiera que los adversarios de BGH tengan por objetivo la región de LATAM en la misma medida que Norteamérica y Europa.

El país más afectado en el 2024 fue Brasil, con un total de 119 víctimas, seguido de México y Argentina, con 45 y 29 víctimas, respectivamente (Figura 6). Perú, Colombia y Chile también representaron cada uno a más de 10 víctimas en sitios específicos de filtración de datos (DLS).

Los sectores más afectados fueron la tecnología, los servicios financieros, la consultoría y los servicios profesionales, el comercio minorista y la atención médica.

46 https://cloud.google.com/blog/topics/threat-intelligence/fin13-cybercriminal-mexico

47 Esta cifra solo representa a las víctimas que no pagaron el rescate.

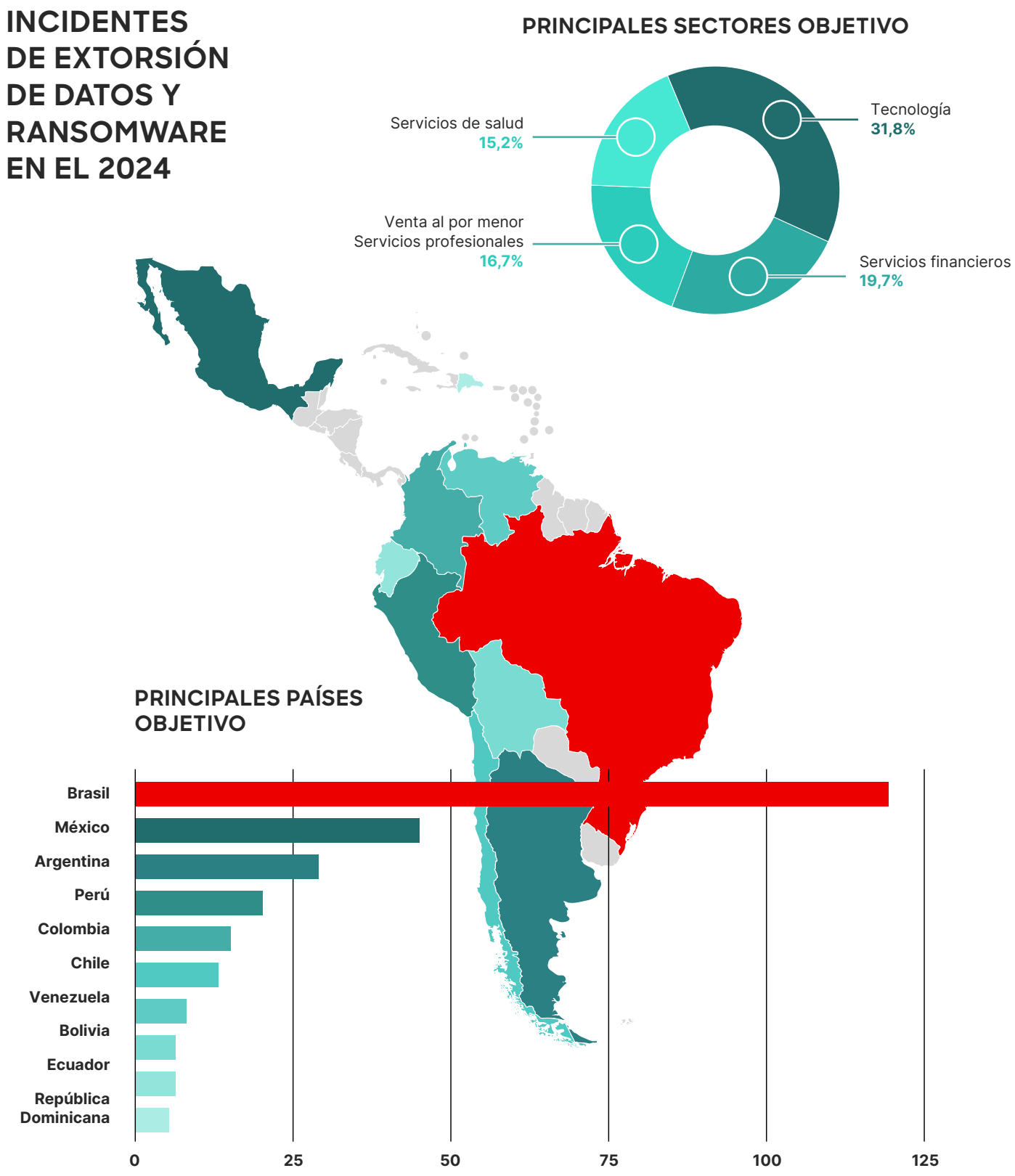

Figura 6. Incidencia de extorsión de datos y ransomware por país y sector

RansomHub, el ransomware como servicio (RaaS) de OCULAR SPIDER y *LockBit*, el RaaS de BITWISE SPIDER fueron las amenazas de ransomware dominantes en LATAM en el 2024. Otras amenazas de ransomware incluyeron *Akira* de PUNK SPIDER, *Dispossessor* y *EightBase*, asociados con BRAIN SPIDER, *Medusa* de FROZEN SPIDER y *Rhysida de* VICE SPIDER.

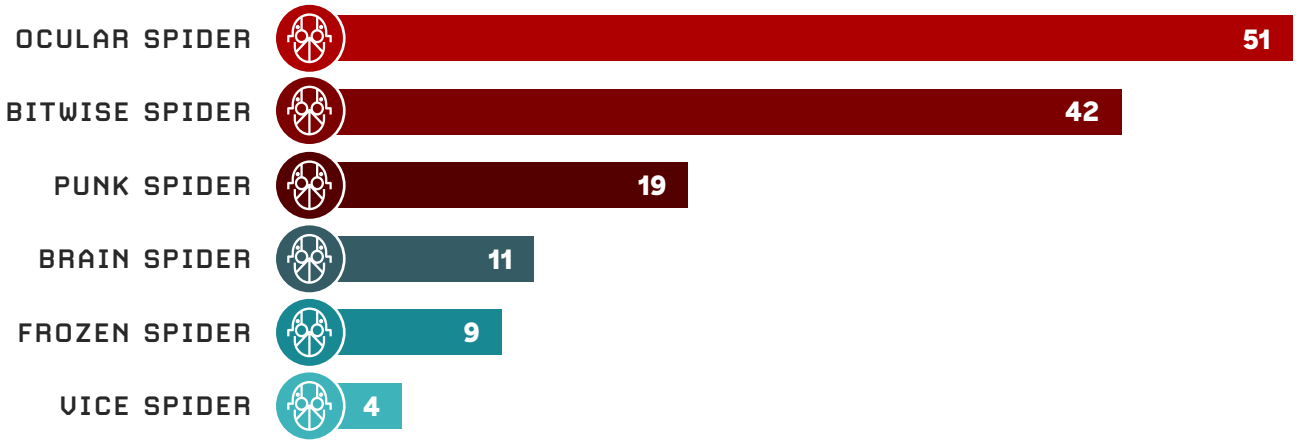

Figura 7. Amenazas de ransomware dominantes en el 2024 y número de incidentes

Aunque es probable que estos adversarios de caza mayor no se dirijan específicamente a la región de LATAM, representan una amenaza importante debido a su gran impacto, como demostró el ataque de ransomware *Conti* de WIZARD SPIDER de abril del 2022 contra el gobierno de Costa Rica. El incidente provocó la suspensión de varias plataformas gubernamentales y financieras costarricenses y llevó a la declaración de un estado de emergencia nacional.

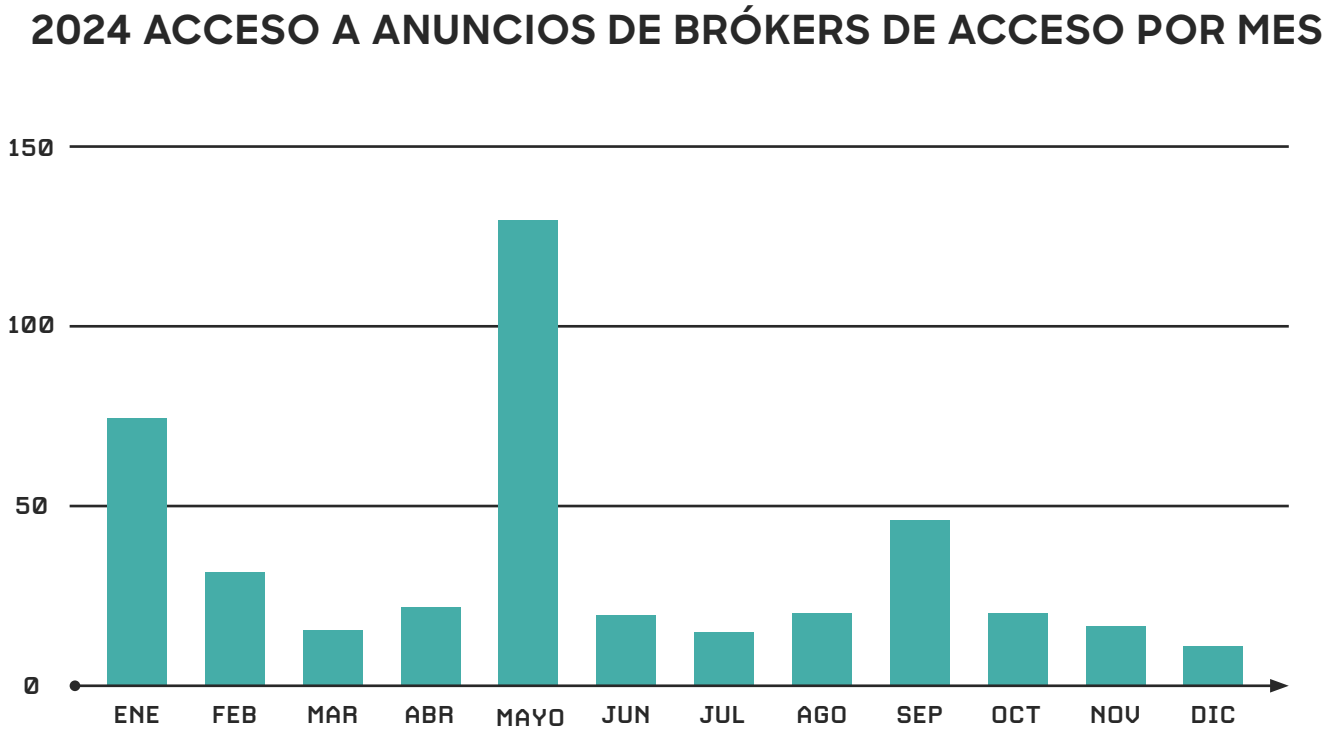

Figura 8. Anuncios de bróker de acceso por mes

Ecosistema clandestino

Los actores de ciberamenazas del cibercrimen en LATAM se benefician de un amplio ecosistema clandestino que proporciona acceso a la red, credenciales filtradas y diversos malware o crypters. Si bien estos actores de ciberamenazas generalmente recurren a foros de cibercrimen en inglés y ruso empleados por los actores del cibercrimen globales, Inteligencia de CrowdStrike identificó varios canales y foros de Telegram dirigidos a usuarios de habla hispana.

Los adversarios del cibercrimen en LATAM también operaron sus propios foros y sitios web. En el 2024, un actor de ciberamenazas que anuncia vulnerabilidades de sitios web basados en LATAM anunció la creación de un nuevo foro para hablantes de inglés y español. En el 2024, ROBOT SPIDER, con sede en Brasil, lanzó un sitio web dedicado a publicitar su servicio crypter junto con su canal de Telegram.

En el 2024, la operación policial internacional "Kaerb" desmanteló el sitio web iServer, dirigido a usuarios hispanohablantes de Argentina, Chile, Colombia, Ecuador, Perú y España. El servicio iServer permitía a los actores del cibercrimen recopilar credenciales de usuario para desbloquear teléfonos robados y eludir el Modo Perdido.

BRÓKERS DE ACCESO

Los adversarios de caza mayor suelen colaborar con brókers de acceso, que obtienen y venden acceso a las redes objetivo; comprender las TTP de los brókers de acceso puede ayudar a mitigar la amenaza del ransomware.

En el 2024, 107 brókers de acceso anunciaron acceso a la red a 428 entidades con sede en LATAM (Figura 8). Estas entidades se ubicaban principalmente en Brasil, México, Colombia, Argentina y Perú, los cinco países de LATAM más afectados por ransomware.

El número de anuncios de brókers de acceso marca un aumento notable con respecto al 2023, cuando 93 brókers de acceso anunciaron acceso a la red a 311 entidades con sede en LATAM. Este aumento de la publicidad también estuvo acompañado de una reducción en el precio promedio de acceso a la red, de $3,385 USD en el 2023 a $1,355 USD en el 2024.

Con 146 anuncios, un bróker de acceso, activo en un foro de cibercrimen en inglés y ruso, representó casi el 35% del total del 2024 y casi el 87% de los anuncios en mayo del 2024, un mes atípico junto con enero del 2024 (Figura 8). Sin embargo, con 1177 anuncios de acceso a la red a nivel global, es probable que el bróker de acceso no tenga como objetivo específico la región LATAM, sino que obtenga su acceso mediante campañas masivas de robo de información, credenciales filtradas o mediante la explotación de vulnerabilidades sin parchear.

La vulnerabilidad de día cero de Qualitor afecta a entidades brasileñas

En septiembre del 2024, un actor de ciberamenazas atacó de forma oportunista a una empresa tecnológica con sede en Brasil para explotar CVE-2024-44849, que afecta a Qualitor 8.24, una solución brasileña de gestión de servicios de TI (ITSM). Es probable que el actor de ciberamenazas empleó un exploit disponible públicamente antes de la fecha de explotación.

Aunque Inteligencia de CrowdStrike no observó otros aprovechamientos de vulnerabilidades específicas de la región en el 2024, los sistemas con componentes orientados a Internet siguen siendo susceptibles de explotación oportunista a través de exploits comunes, ataques de fuerza bruta y sistemas mal configurados.

CREDENCIALES FILTRADAS

A lo largo del 2024, Inteligencia de CrowdStrike recuperó más de 1000 millones de credenciales pertenecientes a personas y organizaciones con sede en LATAM relacionadas con filtraciones de datos y registros de robos de malware. La Figura 9 muestra estadísticas sobre las credenciales robadas en varios países de LATAM, lo que destaca la escala de las operaciones criminales en la región. El gráfico contiene el número total de credenciales filtradas para cada país y la proporción de credenciales relacionadas con instituciones gubernamentales, lo que incluye los servicios públicos para los ciudadanos.

Brasil tuvo el mayor número de credenciales filtradas en el 2024, probablemente como reflejo de su gran población, el aumento de la actividad en línea y la rápida digitalización. México, Argentina, Colombia y Perú también registraron un elevado número de credenciales filtradas, lo que indica el crecimiento de su economía digital y su exposición a las amenazas cibernéticas.
Las credenciales robadas pueden dar lugar a fraude financiero, robo de identidad y otras brechas, todo lo cual puede afectar a personas y organizaciones.

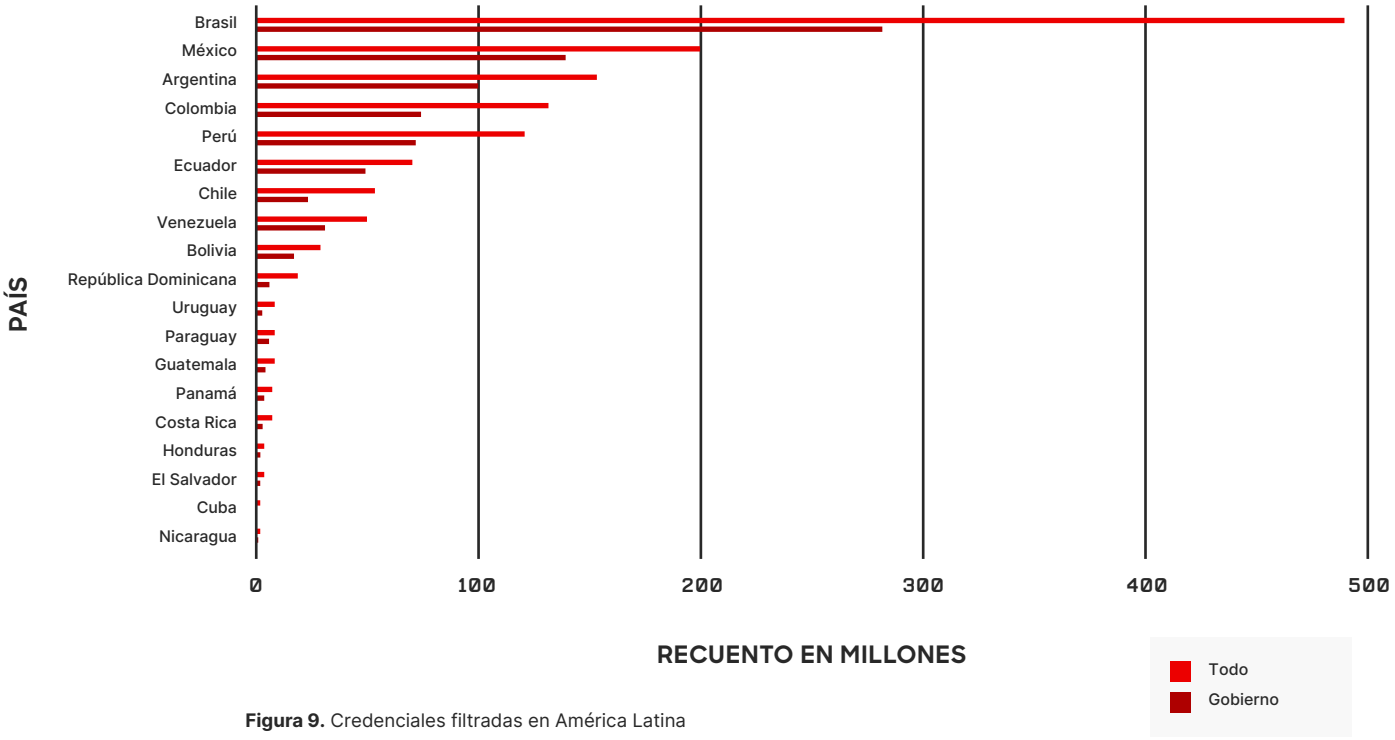

Figura 9. Credenciales filtradas en América Latina

CRYPTER DE ROBOT SPIDER COMO SERVICIO

El adversario de cibercrimen ROBOT SPIDER emplea su crypter como servicio (CaaS) *CryptersAndTools* (*Fsociety*) para habilitar los adversarios de cibercrimen en LATAM. Desde el 2017, *CryptersAndTools* ofrece un crypter multietapa, e Inteligencia de CrowdStrike observó que atacantes en LATAM (BLIND SPIDER, ODYSSEY SPIDER y PLUMP SPIDER) y AVIATOR SPIDER, con sede en Nigeria, emplean este crypter.

Históricamente, ROBOT SPIDER anunció el *crypter protector de CryptersAndTools* a través de un canal de Telegram; sin embargo, en septiembre del 2024, el adversario comenzó a usar un sitio web para anunciar a una base de clientes mayor. El sitio web en inglés del adversario ofrece servicios semiprofesionales que incluyen soporte técnico las 24 horas y actualizaciones regulares a fin de adaptarse a múltiples zonas horarias (Figura 10).

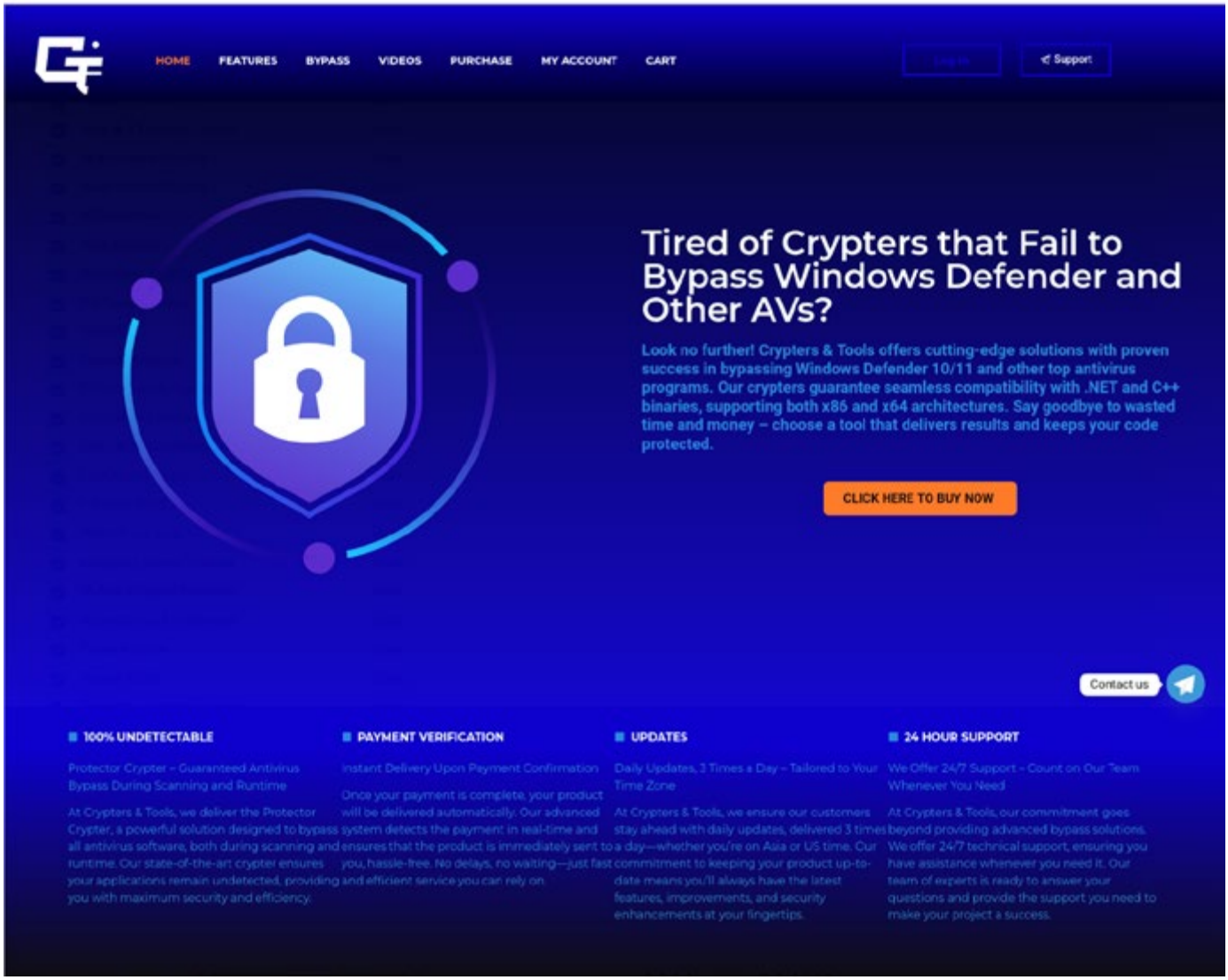

Figura 10. Sitio web *CryptersAndTools* de ROBOT SPIDER

A mediados del 2024, ROBOT SPIDER también comenzó a vender el código fuente de su crypter por $6,000 USD. En diciembre del 2023, el adversario ofreció un curso de creación de crypters que probablemente proporcionaría a los clientes conocimientos con el fin de desarrollar herramientas similares a su crypter multietapa. Este curso dificultó la atribución de incidentes. Por ejemplo, en septiembre del 2024, Inteligencia de CrowdStrike identificó un incidente de ransomware *Makop* y una campaña de RENAISSANCE SPIDER que empleaba crypters, probablemente basados en el crypter de ROBOT SPIDER.

El cargador de scripts PowerShell de ROBOT SPIDER utiliza constantemente el nombre de variable `$codigo` y la misma función `$oWjuxd`; el uso del mismo nombre facilita la atribución. Este script de PowerShell decodifica un script de PowerShell de siguiente etapa que descarga un cargador .NET de ROBOT SPIDER (también conocido como *AndeLoader*) integrado en una imagen JPG entre los marcadores `<<BASE64_START>>` y `<<BASE64_END>>`.

El script de PowerShell invoca la función de exportación `VAI` para ejecutar el cargador .NET. El adversario usó constantemente el mismo JPG, a menudo con variaciones del nombre `deathnote.jpg`.

Familias de malware dominantes

A lo largo del 2024, Inteligencia de CrowdStrike observó actualizaciones de un conocido malware de cibercrimen de América Latina que aprovecha nuevas técnicas enfocadas en mejorar la evasión de defensas, que se detallaron en esta publicación del blog CrowdStrike del 2024.[48] Cabe destacar que los desarrolladores de familias de malware con sede en América Latina comenzaron a adoptar el lenguaje de programación Rust empleado exclusivamente en componentes de descarga.

Esta adopción resalta el interés de los desarrolladores en adaptarse al ecosistema actual del cibercrimen mediante el uso de nuevos lenguajes de programación para el desarrollo de malware en un intento de obstaculizar el análisis y evadir las detecciones basadas en host. Inteligencia de CrowdStrike observó las siguientes actualizaciones:

- ***Mispadu* (también conocido como *URSA*):** Durante abril y junio del 2024, SAMBA SPIDER realizó campañas aprovechando nuevas cadenas de infección, que incluían componentes nuevos o actualizados, para propagar *Mispadu*. La versión 100 de *Mispadu* es la última versión de malware observada durante el 2024.
- ***Kiron* (también conocido como *Grandoreiro*):** En enero del 2024, la operación Grandoreiro de las fuerzas del orden resultó en la incautación de infraestructura y el arresto de personas radicadas en Brasil. A pesar de la incautación, el malware continuó aprovechando varias actualizaciones en las que los desarrolladores probaron nuevos métodos de distribución, agregaron una extensión del navegador y adoptaron Rust durante un breve período.
- ***Caiman* (también conocido como *Grandoreiro*):** en junio del 2024, los desarrolladores actualizarán la cadena de ofuscación luego de una pausa de un mes de *Caiman*, que comenzó a mediados de mayo del 2024.
- ***Astaroth* (también conocido como *Guildma*):** Durante el 2024, los desarrolladores de *Astaroth* no lanzaron ninguna actualización significativa, solo agregaron una derivación de clave para descifrar cadenas y realizaron ajustes menores en la ofuscación y el protocolo de red.
- ***Culebra* (también conocido como *Mekotio*):** A finales de julio del 2024, los desarrolladores de *Culebra* actualizaron el componente de descarga del malware, propagado como un componente de PowerShell que mantenía varias técnicas de la versión Delphi empleada durante el 2023 y la primera mitad del 2024.
- ***Salve* (también conocido como *Casbaneiro*):** a mediados de marzo del 2024, los desarrolladores de *Salve* actualizan la cadena de infección para incluir un descargador basado en Rust; esta actividad ocurrió luego de una probable pausa que comenzó en noviembre del 2023.

Durante el 2024, otros actores de ciberamenazas aprovecharon campañas de malware a través de sitios web de phishing que suplantaban la identidad de entidades con sede en México. Si bien las campañas parecen similares, es muy probable que diferentes actores de ciberamenazas operaran las actividades aprovechando *Doit* (también conocido como *TimbreStealer*), *BotnetFenix*y *Belero*. El uso de TTP similares destaca el intercambio de conocimientos entre actores de ciberamenazas centrados en América Latina.

Los actores de ciberamenazas emplean principalmente *Doit*, un ladrón de información observado por primera vez en el 2022, para apuntar a México. Los desarrolladores de malware actualizan *Doit* tres veces aprovechando una primera versión de AutoIt, una reescritura de C++ y una versión modular final de C++, que es la última versión en distribución (Figura 11).

48 Ver también https://www.crowdstrike.com/en-us/blog/latin-america-malware-update/

Figura 11. Sitios web de phishing para la distribución de *Doit*

BotnetFenix es un ladrón de múltiples etapas de América Latina, identificado por primera vez en enero del 2023. El malware incluye un descargador de PowerShell y el cargador *RustSimpleLoader*, basado en Rust. En el 2024, un actor de ciberamenazas distribuyó *BotnetFenix* mediante sitios web de smishing y phishing, entre los que se encuentran sitios de CAPTCHA falsos (Figura 12).

Figura 12. Sitios web de phishing para la distribución de *BotnetFenix*

A mediados del 2023, un actor criminal distribuyó de manera oportunista un troyano bancario para América Latina no identificado basado en Visual Basic (VB), denominado *Belero*, a través de sitios web de phishing (Figura 13).

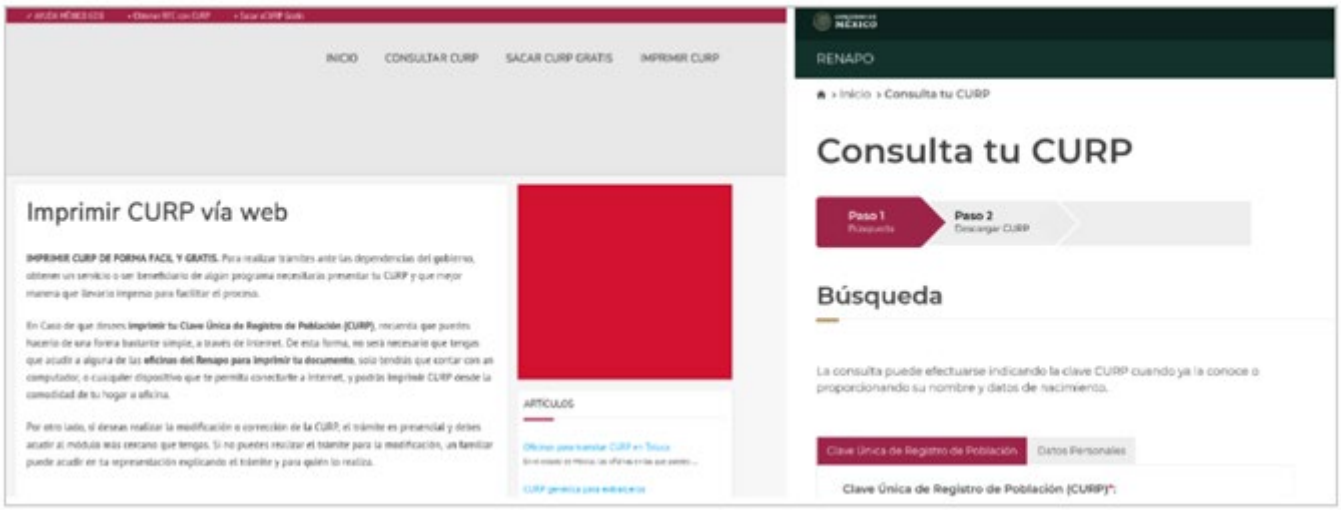

Figura 13. Sitios web de phishing para la distribución de *Belero*

Inteligencia de CrowdStrike observó otras operaciones criminales de baja prevalencia en la región:

- En julio del 2024, un actor de ciberamenazas aprovechó las payloads de *HijackLoader* que contenía *Remcos* empleando señuelos en español, que suplantaban una solución no auténtica de CrowdStrike.
- *EvolvedThief* (también conocido como *Chaes* o *SolarSys*) es un troyano bancario modular para América Latina que se implementó inicialmente en varios lenguajes de programación y scripting. A finales de diciembre del 2023, los desarrolladores de malware liberaron una versión reescrita Python para apuntar a usuarios de habla portuguesa.
- *QuasarRAT* (también conocido como *BlotchyQuasar*) es una variante de *Quasar* con capacidades de troyano bancario. En mayo del 2024, un actor de ciberamenazas aprovechó una campaña de correo electrónico no deseado para apuntar a un usuario con sede en Colombia a fin de difundir el malware. Este actor de ciberamenazas llevó a cabo campañas centradas en Colombia desde al menos el 2020. Aunque los TTPs de actividad son similares a BLIND SPIDER, la infraestructura de comando y control (C2) y el uso de una variante *Quasar* indican que otro actor de ciberamenazas probablemente realizó esta actividad.

Las aplicaciones de préstamos abusivos para dispositivos móviles distribuyen *malware* SpyLoan

En noviembre del 2024, Inteligencia de CrowdStrike detectó muestras del malware *SpyLoan* provenientes de una aplicación de préstamos abusivos, supuestamente originada en México y disponible en tiendas legítimas, como Google Play. Además de su baja transparencia y altas tasas de interés, estas aplicaciones emplean funciones de spyware para robar datos personales de los usuarios, que luego se emplean para obligarlos a reembolsar, a menudo mediante acoso o amenazas de violencia. Según reportes de la prensa mexicana, las aplicaciones de préstamos abusivos no reguladas son populares en México a pesar de los intentos de las autoridades mexicanas por frenar su prevalencia.

Descripción general del vínculo con los estados

En el 2024, Inteligencia de CrowdStrike observó que varios adversarios vinculados con China, Colombia, Corea del Norte y Rusia apuntan a la región de América Latina (Figura 14). Sin embargo, los adversarios con vínculo estatal representaban una fracción de la actividad documentada, probablemente debido a sus objetivos de recolección de inteligencia, la priorización de objetivos relacionados y, en general, un enfoque mayor en el sigilo. Por lo tanto, si bien estos adversarios suelen mostrar una mayor sofisticación que sus contrapartes del cibercrimen, la amenaza que representan depende de un sector de la entidad, su ubicación geográfica y eventos externos, como las elecciones.

Los adversarios vinculados con China y Corea del Norte son responsables de un mayor volumen de actividad que tiene por objetivo la región de América Latina que los adversarios vinculados con Irán y Rusia.

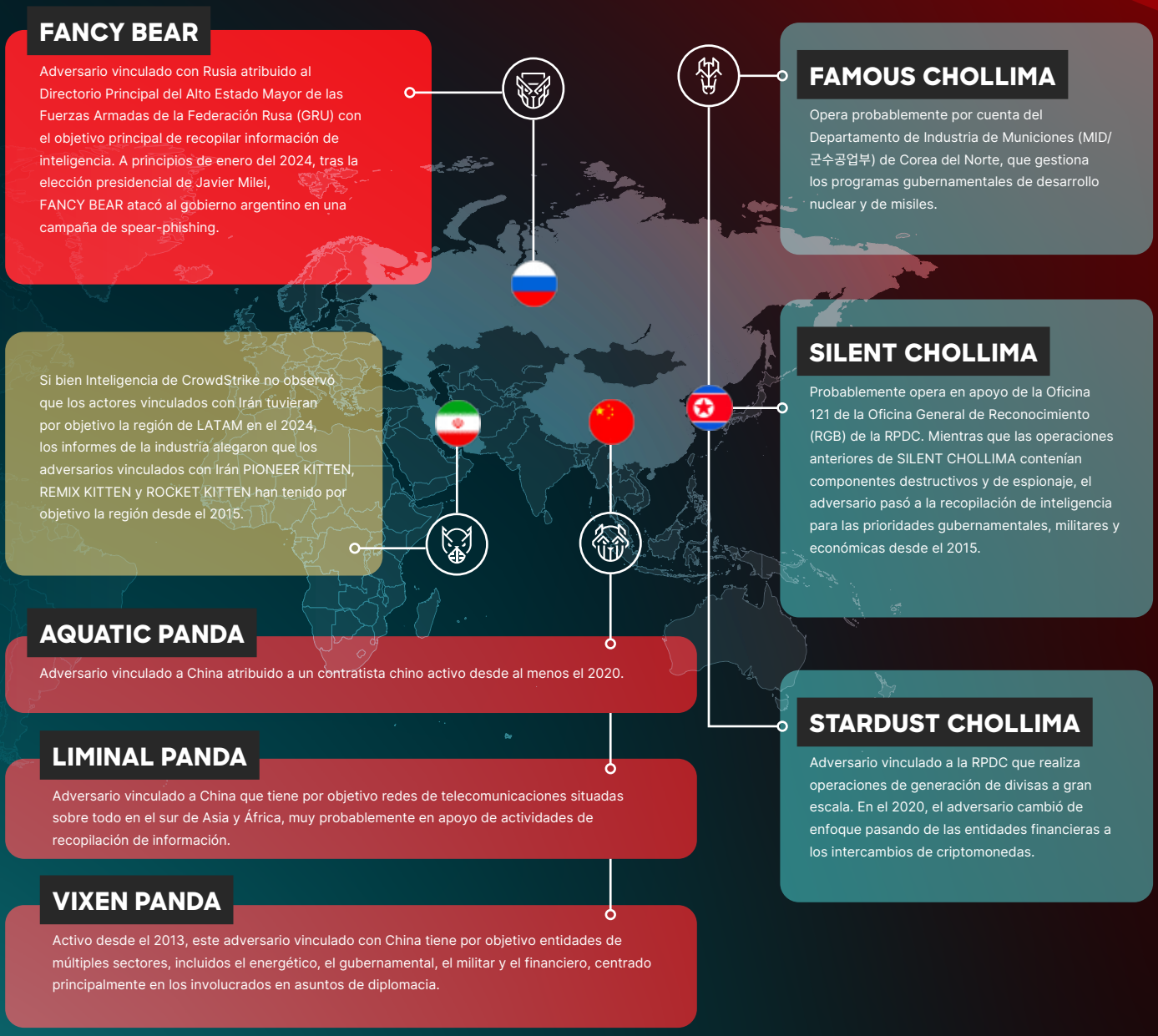

Figura 14. Mapa de adversarios de estados nación que tienen a América Latina por objetivo

Adversarios vinculados con China

Aunque no se limita al 2024, Inteligencia de CrowdStrike observó que los adversarios vinculados con China AQUATIC PANDA, LIMINAL PANDA y VIXEN PANDA tienen por objetivo la región de América Latina y se concentran principalmente en América Central y del Sur. Un comunicado de prensa conjunto entre el Ministerio de Defensa Nacional de la República de Paraguay y la Embajada de Estados Unidos en Paraguay también afirmó que ETHEREAL PANDA (un adversario ampliamente alineado con un actor de ciberamenazas identificado públicamente como *FLAX TYPHOON*) tuvo por objetivo a Paraguay a finales del 2024.[49] Sin embargo, Inteligencia de CrowdStrike no puede verificar actualmente esta afirmación.

En el 2024, VIXEN PANDA empleó una caja de retransmisión operativa (ORB) rastreada como ORB02 para probablemente realizar intrusiones a nivel mundial, lo que incluye apuntar a entidades en América del Sur. Además, en el 2022 y el 2023, VIXEN PANDA empleó *Ketrican* para apuntar a ministerios de relaciones exteriores en América del Norte y del Sur.

Inteligencia de CrowdStrike y los informes más amplios de la industria indican que VIXEN PANDA, al menos desde el 2019, ha tenido por objetivo a organizaciones gubernamentales y no gubernamentales (ONG) en una variedad de países de la región de América Latina, como Argentina, Brasil, Chile, Colombia, República Dominicana, Ecuador, El Salvador, Guatemala, Honduras, México, Panamá, Perú y Venezuela.

En noviembre del 2024, Inteligencia de CrowdStrike determinó que LIMINAL PANDA, un adversario principalmente enfocado en redes de telecomunicaciones y muy probablemente empleado en apoyo de iniciativas de recopilación de inteligencia, probablemente obtuvo acceso a proveedores de telecomunicaciones ubicados en América Central y del Sur, según el análisis de registros de servidores DNS externos (eDNS). Es probable que el adversario empleara servidores de telecomunicaciones afectados para atacar también a proveedores en otras regiones geográficas y demuestre experiencia en redes de telecomunicaciones, lo que incluye el entendimiento de las interconexiones entre proveedores y protocolos de dispositivos móviles.

AQUATIC PANDA, atribuido a un contratista chino, probablemente apuntó a entidades con sede en América del Sur entre el 2022 y el 2024. En el 2022, el adversario probablemente apuntó a servidores de correo electrónico pertenecientes a entidades gubernamentales y de telecomunicaciones en América del Sur. En el 2023, AQUATIC PANDA probablemente realizó reconocimiento contra entidades en Brasil. La evidencia también indica que el adversario tenía por objetivo entidades militares en Perú.

Actividades vinculadas con China no atribuidas

En el 2024, Inteligencia de CrowdStrike observó campañas de *SysloggerRAT* que apuntaban a entidades minoristas, deportivas y logísticas con sede en Sudamérica. *SysloggerRAT* es un troyano de acceso remoto (RAT, por sus siglas en inglés) basado en Linux, escrito en Golang y asociado principalmente con intrusiones selectivas vinculadas con China.

En el 2023, informes de la industria afirmaron que un actor de ciberamenazas desconocido vinculado con China estaba perpetrando ciberamenazas que afectaban a entidades gubernamentales sudamericanas; aunque esta actividad no se atribuyó a ningún adversario conocido, Inteligencia de CrowdStrike evalúa que es probable que esté asociada a un actor que emplea TTP coherentes con adversarios vinculados con China.

49 https://www.southcom.mil/MEDIA/NEWS-ARTICLES/Article/3979394/us-strengthens-cybersecurity-partnership-with-paraguay/

Adversarios vinculados con Corea del Norte

Durante el último año, Inteligencia de CrowdStrike observó a adversarios vinculados con Corea del Norte, FAMOUS CHOLLIMA, Silent Chollima y STARDUST CHOLLIMA llevar a cabo posibles campañas oportunistas en la región de América Latina para obtener ganancias financieras y, con menor frecuencia, espionaje cibernético.

En el 2024, CrowdStrike observó actividad de FAMOUS CHOLLIMA en Argentina, Brasil y Uruguay. El adversario obtiene ilícitamente trabajo independiente o equivalente a tiempo completo para ganar un salario que puede canalizar a Corea del Norte. Cuando se emplea, FAMOUS CHOLLIMA también puede implantar malware para recopilar información que probablemente pueda usar para el desarrollo tecnológico y de defensa de Corea del Norte. Las campañas de este actor de ciberamenazas en América Latina son oportunistas más que dirigidas.

A finales del 2023, Inteligencia de CrowdStrike observó a SILENT CHOLLIMA implantar *NineRAT* en una entidad agrícola colombiana, probablemente para apoyar las iniciativas de Corea del Norte para resolver su actual escasez de alimentos. En octubre del 2024, CrowdStrike identificó a STARDUST CHOLLIMA implantando el malware *MinKit para macOS* en una entidad de criptomonedas con sede en México. El adversario empleó *MinKit* para implantar malware adicional como *StreamInjector*, *GillySocket* y *ExtendedReach*.

Actividades dirigidas no atribuidas

En el 2024, Inteligencia de CrowdStrike observó incidentes no atribuidos que apuntaban a proveedores de telecomunicaciones en América del Sur. Entre estas actividades se encontraban el grupo de actividades *LightBasin* y un adversario no identificado que instaló una versión *socat* modificada.

El clúster de actividades *LightBasin* es un adversario no atribuido que se observó que apuntaba a proveedores de telecomunicaciones e instituciones financieras de todo el mundo desde mediados del 2020, entre los que se encuentran los que tienen su sede en América Central y del Sur.

Descripción general no estatal

A lo largo del 2024, Inteligencia de CrowdStrike observó a hacktivistas globales, así como probablemente a hacktivistas latinoamericanos, que llevaron a cabo diversas operaciones cibernéticas con motivaciones ideológicas y políticas en el Caribe, América Central y del Sur y México. Una revisión de los incidentes de hacktivistas durante el año pasado indica que los hacktivistas que apuntan a la región generalmente están motivados por eventos geopolíticos y problemas percibidos de gobernanza interna.

Entre los acontecimientos geopolíticos que impulsaron las campañas de hacktivistas se encuentran las elecciones presidenciales de julio del 2024 en Venezuela, el deterioro de las condiciones de vida y las violaciones de los derechos humanos en Cuba, la percepción de corrupción gubernamental en Guatemala y la actual guerra entre Israel y Hamás.

Hacktivismo para exponer a las organizaciones criminales transnacionales (OCT)

Si bien históricamente los hackers activistas/hacktivistas rara vez atacaron a las OCT (probablemente debido a la amenaza de represalias violentas), durante el 2024, Inteligencia de CrowdStrike observó operaciones cibernéticas limitadas, presuntamente destinadas a exponer o debilitar a las OCT. En abril del 2024, la entidad de hacktivistas *AFS_Nemesis* (AFS es el acrónimo de AntiFentySec) anunció el desarrollo de un software para exponer a los cárteles mexicanos por su participación en las cadenas de suministro de fentanilo.

En mayo del 2024, *GhostSec* filtró datos y publicó un expediente que supuestamente revelaba vínculos entre entidades públicas y privadas mexicanas y organizaciones transnacionales con sede en México. En julio del 2024, el grupo filtró datos presuntamente robados que, según se informa, incluían la ubicación de escondites de armas y dinero, y demostraban vínculos adicionales entre el gobierno de un estado mexicano y las OCT. Inteligencia de CrowdStrike no puede verificar la autenticidad de los datos.

Dado que los hacktivistas frecuentemente apuntan a organizaciones con afiliación gubernamental percibidas como corruptas o injustamente violentas, es probable que las entidades de hacktivistas continúen exponiendo a las OCT, especialmente a aquellas con vínculos percibidos con el gobierno.

El hacktivismo adyacente a los acontecimientos geopolíticos refleja las tendencias históricas a la selección de objetivos

En consonancia con la actividad anterior al 2024, las entidades de hacktivistas siguen afirmando que las operaciones cibernéticas tienen como objetivo principal apuntar al Gobierno o a entidades con afiliación gubernamental en respuesta a injusticias percibidas contra civiles o violaciones de derechos humanos.

Un hacktivista global afirmó que muchas operaciones cibernéticas tenían como objetivo, casi con certeza, las elecciones presidenciales venezolanas de julio del 2024 debido a las generalizadas denuncias internacionales de fraude electoral y la ilegitimidad percibida del gobierno del presidente Nicolás Maduro. Es probable que las operaciones tuvieran como objetivo protestar contra el gobierno de Maduro y demostrar solidaridad con los manifestantes locales.

Por ejemplo, afiliados de *Anonymous* afirmaron tener como blanco una aplicación de dispositivo móvil estatal que, según se informa, facilitaba la vigilancia contra manifestantes, así como docenas de sitios web asociados al Gobierno, probablemente mediante ataques de denegación de servicio distribuido (DDoS). Además, a principios de agosto del 2024, el grupo activista hacker *GlorySec* afirmó haber atacado el sitio web del partido de Maduro y filtrado información supuestamente relacionada con el gobierno venezolano y las cuentas de redes sociales del sector de medios, como parte de la campaña del grupo que apuntaba a Venezuela en vísperas de las elecciones de julio del 2024. Entre septiembre y octubre del 2024, afiliados de *Anonymous* afirmaron haber realizado ataques de DDoS[50] y operaciones de piratería y filtración[51] que tenían por objetivo a entidades no estatales o del sector privado que los hacktivistas percibían como partidarios del régimen de Maduro.

50 https://x.com/White_Hunters/status/1837708682882379989

51 https://x.com/YourAnonHunters/status/1851363295963320823
https://x.com/YourAnonHunters/status/1851361153684779223
https://t.me/AnonHuntersLATAM/7463

De manera similar, hacktivistas globales llevaron a cabo operaciones cibernéticas para presuntamente apoyar las protestas internas contra el Gobierno cubano y crear conciencia sobre los vínculos de este con China. En marzo del 2024, un afiliado de *Anonymous* llevó a cabo una serie de probables operaciones cibernéticas que apuntaban a varias entidades cubanas en solidaridad con los cubanos que protestaban por los continuos cortes de energía y la escasez generalizada de alimentos. En septiembre del 2024, el grupo hacktivista *GhostSec*, afiliado con *Anonymous, que llevó a cabo sistemáticamente operaciones cibernéticas contra el Gobierno cubano, a menudo en paralelo con protestas públicas, anunció la reactivación de su operación CubaLibra para exponer los vínculos entre los gobiernos de Cuba y China.*

Un hacktivista global también atacó a varias entidades gubernamentales debido a la percepción de corrupción. En enero del 2024, afiliados de *Anonymous* afirmaron haber realizado un ataque de DDoS contra entidades guatemaltecas que, según los hacktivistas, impidieron la transferencia democrática del poder del expresidente Alejandro Giammattei al actual presidente Bernardo Arévalo.

En abril del 2024, la entidad hacktivista *Cult of the Dead Cat* (*CoDC*) afirmó realizar una operación de hackeo y filtración de datos dirigida a un ministerio del Gobierno ecuatoriano, probablemente relacionada con el referéndum sobre las enmiendas constitucionales para apoyar las medidas anticrimen adoptadas bajo el estado de emergencia. En mayo del 2024, un afiliado de *Anonymous* afirmó haber realizado un ataque DDoS contra una entidad de las fuerzas de seguridad nicaragüenses, en el que alegó violaciones no especificadas de los derechos ciudadanos.[52]

La Tabla 1 proporciona una descripción general de entidades hacktivistas adicionales que tienen por objetivo entidades latinoamericanas o con sede en países latinoamericanos.

ENTIDAD HACKTIVISTA	DESCRIPCIÓN DE LA ACTIVIDAD REGIONAL DE LA ENTIDAD HACKTIVISTA
CiberInteligencia El Salvador	Activo desde al menos julio del 2023, *CiberInteligencia El Salvador* reivindicó una serie de supuestas operaciones de hackeo y filtración que tienen por objetivo entidades públicas salvadoreñas. Que apuntaran al grupo probablemente fue motivado por quejas contra el gobierno salvadoreño, además del descontento por la supuesta postura de ciberseguridad del gobierno y los problemas de inseguridad interna. A pesar de los indicios de mayo del 2024 de que estaban expandiendo su objetivo a entidades del sector privado y potencialmente a otros países de América Latina, el grupo continuó apuntando a entidades del gobierno salvadoreño, incluso tan recientemente como a fines de septiembre del 2024.[53]
GhostSec	*GhostSec* participó en varias campañas regionales de hackeo y filtración de datos con varios países latinoamericanos como objetivo, con el argumento de corrupción gubernamental, mala gestión o violaciones de derechos humanos, como el ampliamente difundido fraude electoral venezolano.
LulzSec Muslims	A lo largo de agosto del 2024, el grupo hacktivista pro palestino y pro Islam *LulzSec Muslims* afirmó liderar varias operaciones cibernéticas que tenían por objetivo a entidades con sede en Argentina en respuesta al apoyo percibido a Israel por parte del gobierno argentino. La supuesta actividad era parte de una campaña más amplia que apuntaba a varios países que *LulzSec Muslims* consideraban partidarios de Israel.
SiegedSec (disuelto)	*SiegedSec*, una entidad hacktivista desde al menos febrero del 2022 hasta que anunció su disolución en julio del 2024, afirmó una probable brecha oportunista de un proveedor de soluciones de seguridad electrónica con sede en México, con el entretenimiento y la supuesta falta de "seguridad básica" de la entidad víctima como motivos.
USDoD	Desde al menos el 2020 y hasta agosto del 2024, la entidad hacktivista *USDoD* se centró en campañas de intrusión selectiva de alto perfil que apuntaban principalmente al ejército estadounidense, a las fuerzas del orden y a los contratistas de defensa. Tras un informe de atribución de Inteligencia de CrowdStrike de agosto del 2024, la persona brasileña, que casi con toda seguridad estaba detrás del personaje *USDoD*, reconoció la atribución. A mediados de octubre del 2024, las autoridades brasileñas arrestaron a la persona.

Tabla 1. Cobertura del hacktivismo en América Latina

52 https://x.com/YourAnonHunters/status/1792568293737250976
53 https://t.me/guacamayal/6068

El impacto de Guacamaya en el ecosistema hacktivista de América Latina

Durante el 2022, la entidad hacktivista *Guacamaya* se atribuyó al menos tres importantes campañas cibernéticas que tenían por objetivo a compañías petroleras y mineras de los sectores público y privado de Latinoamérica, así como a entidades gubernamentales latinoamericanas. *Guacamaya* normalmente ha explotado vulnerabilidades reconocidas públicamente en sistemas sin parchear para acceder a las redes de las víctimas y posteriormente filtrar los datos mediante las plataformas de publicación de filtraciones *Enlace Hacktivista* y *Distributed Denial of Secrets* (*DDoSecrets*).

Específicamente, *Guacamaya* publicó un video que pretende mostrarlos explotando CVE-2021-26855 en Microsoft Exchange (divulgado por primera vez en marzo del 2021) para obtener acceso inicial a una entidad minera, recolectar credenciales de la Autoridad de Seguridad Local (LSA) para movimiento lateral y usar técnicas de living-off-the-land para borrar datos.

Aunque no se informó públicamente sobre la actividad de *Guacamaya* en el 2024, es casi seguro que sus operaciones pasadas estimularon acciones policiales en México en marzo del 2023, una investigación criminal en Colombia en octubre del 2022 y sanciones estadounidenses que tenían como blanco a una subsidiaria guatemalteca de un conglomerado minero con sede en Suiza en noviembre del 2022.

Guacamaya probablemente envalentonó a las nacientes entidades hacktivistas con motivaciones ideológicas y fomentó campañas cibernéticas similares. Por ejemplo, en marzo del 2022, *Guacamaya* publicó su campaña de hackeo y filtración “Mining Secrets” y un video tutorial que mostraba cómo llevaron a cabo la operación cibernética, casi con toda seguridad como una herramienta para compartir conocimientos con las entidades hacktivistas emergentes. La entidad también hacktivista *CiberInteligencia El Salvador* invocó el nombre de *Guacamaya* en sus operaciones cibernéticas, probablemente para ganar reputación.

Conclusión

A lo largo del 2024, CrowdStrike observó varias tendencias que definieron la postura de ciberseguridad de la región. Es probable que estas tendencias continúen en el 2025, ya que tienen su origen en cuestiones políticas que aún no fueron totalmente resueltas o reconciliadas por los gobiernos regionales.

Inteligencia de CrowdStrike observó varias tendencias cibernéticas macro que trascendieron las fronteras regionales y las fronteras entre estados, como gobiernos que reforzaron su infraestructura de ciberseguridad nacional y se involucraron en la colaboración y el intercambio de conocimientos con socios extranjeros. Las dos excepciones notables fueron los regímenes autoritarios de Cuba y Venezuela, ambos presuntamente involucrados en operaciones cibernéticas ofensivas y en la subyugación en línea de sus respectivas poblaciones nacionales. Estas tendencias seguramente continuarán en el 2025, según una revisión de la legislación cibernética planeada y los foros multilaterales programados.

Inteligencia de CrowdStrike también observó varias microtendencias cibernéticas, como gobiernos que luchan con asuntos políticos delicados relacionados con la inclusión de proveedores de tecnología chinos en el proceso de licitación de contratos públicos, la gestión eficaz de la tecnología de IA y gobiernos que anuncian investigaciones sobre el armamento nacional de spyware para vigilar a oponentes políticos. Es probable que estas tendencias persistan en el corto plazo, debido a la política volátil de los gobiernos regionales hacia los proveedores de tecnología chinos, las incipientes estrategias de gobernanza de la IA y la fluctuante voluntad política respecto de la legalidad del spyware para vigilar a los oponentes políticos.

Durante el 2024, Inteligencia de CrowdStrike observó numerosas amenazas cibernéticas predominantes que tenían como blanco la región. Inteligencia de CrowdStrike observó que la mayoría de los ciberataques que tienen por objetivo a América Latina y el Caribe fueron realizados por actores de cibercrimen y caza mayor, seguidos por el activista hacker/hacktivista global y regional y las amenazas globales y regionales del estado nación. En el 2025, es probable que surjan temas similares, ya que los actores de ciberamenazas demostraron resiliencia y adaptabilidad en la evolución persistente de sus TTP para continuar apuntando a la región.

Los ransomwares como servicio (RaaS, por sus siglas en inglés) RansomHub y *LockBit* representaron las amenazas de ransomware dominantes en América Latina en el 2024. Además, el conocido malware de cibercrimen en América Latina continúa evolucionando debido a que los operadores aprovechan técnicas novedosas, como la adopción de nuevos métodos de ofuscación y lenguajes de programación, para mejorar la evasión defensiva. Esto demuestra que los desarrolladores se adaptan al cambiante ecosistema del cibercrimen para intentar obstaculizar el análisis y evadir la detección basada en host. Es probable que esto continúe en el futuro, debido a las continuas adaptaciones de los TTP de los actores de ciberamenazas.

Los hacktivistas globales y probablemente radicados en América Latina llevaron a cabo diversas operaciones cibernéticas con motivaciones ideológicas y políticas para apuntar a entidades del sector gubernamental y privado durante el 2024. Las actividades declaradas de los grupos y sus supuestas motivaciones sugieren que los hacktivistas que tenían como blanco a América Latina y el Caribe generalmente estaban motivados por eventos geopolíticos y problemas percibidos de gobernanza interna. En el corto plazo, los acontecimientos geopolíticos probablemente seguirán sirviendo como catalizadores para las campañas cibernéticas de hacktivistas, según una revisión de los acontecimientos geopolíticos del año pasado que estuvieron marcados o acompañados por una actividad posterior de hacktivistas.

Por último, Inteligencia de CrowdStrike no observó una cantidad significativa de actividad de adversarios vinculados con Rusia, Irán o Corea del Norte que apuntaran a entidades del sector gubernamental y privado en América Latina y el Caribe durante el 2024. Sin embargo, los actores de ciberamenazas vinculados con China representaban el mayor número de intrusiones identificadas, con operaciones cibernéticas que predominantemente tenían por objetivo entidades de América Central y del Sur.

Los actores de ciberamenazas vinculados con China probablemente seguirán siendo al menos la principal y más consistente amenaza de intrusión patrocinada por el Estado, dado el objetivo continuo del país de proyectar influencia económica y diplomática en América Latina. Además, a falta de un cambio en los objetivos de política exterior, la escasa información sugiere que los adversarios vinculados con Rusia, Irán y Corea del Norte priorizaron la recopilación de inteligencia cibernética en la región, sin que estos países tengan muchos motivos para llevar a cabo operaciones destructivas o disruptivas.

Recomendaciones

1 Protege todo el ecosistema de identidad

Los adversarios están apuntando cada vez más a identidades con ayuda del robo de credenciales, la evasión de la autenticación multifactor (MFA) y la ingeniería social, mientras se mueven de manera encubierta y de forma lateral entre entornos en local, en la nube y de software como un servicio (SaaS) mediante relaciones de confianza. Esto les permite hacerse pasar por usuarios legítimos, escalar el acceso y evadir la detección.

Las organizaciones deberían adaptar una solución de autenticación multifactor (MFA) resistente al phishing, como claves de seguridad de hardware, para así prevenir el acceso no autorizado. Las políticas de identidad y acceso son fundamentales, incluido el acceso justo a tiempo, revisiones periódicas de la cuenta y controles de acceso condicional. Las herramientas de detección de amenazas contra la identidad deben monitorear el comportamiento entre los endpoints y en local, la nube y los entornos de software como un servicio (SaaS) para señalar un aumento de privilegios, el acceso no autorizado y la creación de cuentas backdoor. Integrar estas herramientas con plataformas de Detección y Respuesta Extendidas (XDR) garantiza una visibilidad integral y una defensa unificada contra los adversarios.

Además, las organizaciones deben educar a sus usuarios con el fin de que reconozcan los intentos de vishing y phising mientras mantienen un monitoreo proactivo para detectar y responder a las amenazas basadas en la identidad.

2 Elimina las brechas de visibilidad entre dominios

El aumento del uso de técnicas hands-on-keyboard y de herramientas legítimas por parte de los adversarios dificultan más la detección y la respuesta. A diferencia de los malware tradicionales, estos métodos les permiten a los atacantes evadir las medidas de seguridad tradicionales ejecutando comandos y empleando software legítimos para imitar operaciones normales.

Para contrarrestar esto, las organizaciones deben modernizar sus detecciones y estrategia de respuesta. Las soluciones de Detección y Respuesta Extendidas (XDR) y de información de seguridad y gestión de eventos (SIEM) de próxima generación brindan visibilidad unificada entre endpoint, redes, entornos de la nube y sistemas de identidad, lo cual le permite a los analistas correlacionar comportamientos sospechosos y ver la ruta completa de ataque.

La cacería de amenazas proactiva y la inteligencia sobre amenazas mejoran aun más la detección a través de la identificación de posibles patrones de ataque y brindan insights respecto a las tácticas, técnicas y TTP de los adversarios. Con la inteligencia en tiempo real, las organizaciones pueden mantenerse informadas respecto a amenazas emergentes, anticipar ataques y priorizar esfuerzos de seguridad cruciales.

3 Defiende la nube como infraestructura central

Los adversarios centrados en la nube están aprovechando las configuraciones erróneas, credenciales robadas y herramientas de manejo de la nube para infiltrarse en sistemas, moverse de forma lateral y mantener un acceso persistente para actividades maliciosas, como el robo de datos y la implementación de ransomware.

Las plataformas de protección de aplicaciones nativas para la nube (CNAPP) con capacidades de detección y respuesta en la nube (CDR) son fundamentales para contrarrestar estas amenazas.

Estas soluciones brindan a los operadores una vista unificada de su postura de seguridad de la nube, lo cual les ayuda a detectar con rapidez, priorizar y corregir configuraciones erróneas, vulnerabilidades y amenazas de adversarios. Además, aplicar controles de acceso estrictos (tales como acceso basado en los roles y políticas condicionales) limita la exposición a los sistemas cruciales y garantiza un monitoreo continuo de anomalías, incluido el inicio de sesión desde ubicaciones inesperadas.

Las auditorias periódicas también son fundamentales para mantener la seguridad. Las herramientas automatizadas pueden descubrir configuraciones de almacenamiento demasiado permisivas, API expuestas y vulnerabilidades sin parchear. Las revisiones frecuentes de los entornos de la nube garantizan que se aborden de forma oportuna los permisos sin usar y las configuraciones obsoletas.

4 Prioriza las vulnerabilidades mediante un enfoque centrado en los adversarios

Los adversarios explotan cada vez más vulnerabilidades reveladas públicamente y emplean encadenamiento de exploit, en que combinan múltiples vulnerabilidades para obtener acceso rápido, escalar privilegios y eludir las defensas. Estos ataques de múltiples etapas a menudo se basan en recursos públicos, como exploits de prueba de concepto y blogs técnicos, lo cual le permite a los adversarios crear payloads efectivas y difíciles de detectar.

Para contrarrestar estas amenazas, las organizaciones deben priorizar parchear de forma regular o actualizar sistemas fundamentales, en especial servicios orientados a Internet que son atacados con frecuencia, como servidores de sitios web y gateways de redes privadas virtuales (VPN, por sus siglas en inglés). Monitorear señales sutiles de encadenamiento de exploit, tales como fallas inesperadas o intentos de aumento de privilegios puede ayudar a detectar ataques antes de que progresen.

Las herramientas como CrowdStrike Falcon® Exposure Management, creadas con priorización de IA nativa, les permiten a los equipos reducir el ruido y concentrarse en las vulnerabilidades que más importan, en especial aquellas que afectan a sistemas cruciales y de alto riesgo. Cuando se adoptan enfoques de seguridad proactivos, se descubren exposiciones entre las superficies de ataque y se aprovecha la automatización, las organizaciones pueden mitigar amenazas sofisticadas y limitar las oportunidades de los adversarios.

5 Conoce a tu adversario y mantente preparado

Cuando se desarrolla un ciberataque en minutos, o incluso en segundos, estar preparado puede marcar la diferencia entre la contención y la catástrofe. Un enfoque basado en la inteligencia permite a los equipos de seguridad ir más allá de las defensas reactivas, gracias a comprender qué adversario los tienen por objetivo, cómo opera y cuáles son sus objetivos. Con la inteligencia sobre amenazas, la creación de perfiles de adversarios y el análisis de tradecraft, los equipos de seguridad pueden priorizar recursos, adaptar defensas y cazar de manera activa las amenazas antes de que escalen. La inteligencia sobre amenazas de CrowdStrike no solo detecta amenazas conocidas, anticipa tradecraft nuevas y en evolución, lo que garantiza que los defensores estén siempre un paso adelante. Cuando se integra perfectamente la inteligencia en un flujo de trabajo de seguridad, las organizaciones pueden acelerar los tiempos de respuesta, perturbar a los adversarios y convertir la inteligencia en acción.

A pesar de que la tecnología es crucial para detectar y detener intrusiones, el usuario final sigue siendo un eslabón fundamental en la cadena para detener brechas. Las organizaciones deben comenzar programas de sensibilización para los usuarios, a fin de combatir la amenaza continua de phishing y técnicas de ingeniería social relacionadas. Para los equipos de seguridad, la práctica hace al maestro. Fomenta un entorno que realice rutinariamente ejercicios de simulación y de equipos rojo/azul para identificar brechas y eliminar las debilidades en sus prácticas y respuestas de ciberseguridad.

Plataforma CrowdStrike Falcon

IA y nativo para la nube

Potencia el efecto de la red en los datos de seguridad provenientes de crowdsourcing mientras elimina la sobrecarga de gestionar complicadas soluciones en local.

Un solo agente liviano

Proporciona una implementación escalable y sin fricción y detiene todo tipo de ataques al tiempo que elimina la sobrecarga del agente y los escaneos programados.

Charlotte AI

Impulsa la cartera de CrowdStrike de capacidad de IA generativa en la plataforma CrowdStrike Falcon® aprovechando la escala de petabytes de la inteligencia automatizada de CrowdStrike, y enriquecida aún más por expertos en seguridad, para acelerar los flujos de trabajo de los analistas.

Falcon Fusion SOAR

Proporciona capacidad nativa de Orquestación, Automatización y Respuesta de Seguridad (SOAR, por sus siglas en inglés), dentro de la plataforma Falcon para permitirte recopilar datos enriquecidos contextualmente y automatizar operaciones de seguridad, inteligencia sobre amenazas y respuesta a incidentes (IR), todo en una sola plataforma y a través de la misma consola, para mitigar las amenazas cibernéticas y las vulnerabilidades.

CrowdStrike Asset Graph

Resuelve uno de los problemas más complejos de los clientes en la actualidad: identificar activos, identidades y configuraciones con precisión en todos los sistemas, como la nube, en local, los dispositivos móviles, la Internet de las cosas (IoT) y más, y conectarlos entre sí en forma de gráfico.

CrowdStrike Intel Graph

Permite a los equipos de seguridad defender de forma proactiva contra amenazas emergentes con insights basados en inteligencia al mapear las relaciones entre actores de ciberamenazas, tácticas, vulnerabilidades y ataques del mundo real.

CrowdStrike Threat Graph

Emplea IA a escala de la nube para correlacionar billones de puntos de datos de múltiples fuentes de telemetría para identificar cambios en las tácticas adversarias y mapear tradecraft para predecir y prevenir automáticamente amenazas en tiempo real en toda la base de clientes global de CrowdStrike.

Falcon Foundry

Permite a los clientes y socios crear fácilmente aplicaciones personalizadas y sin código que aprovechen los datos, la automatización y la infraestructura a escala de nube de la plataforma Falcon para resolver tus desafíos de ciberseguridad más difíciles.

CrowdStrike Marketplace

Ofrece un mercado empresarial de colaboradores en tecnología donde puedes descubrir, probar, comprar y desplegar aplicaciones confiables de CrowdStrike y de otros colaboradores que amplían la plataforma CrowdStrike Falcon, sin agregar agentes o incrementar la complejidad.

Productos CrowdStrike

Seguridad de endpoints

FALCON PREVENT | ANTIVIRUS DE ÚLTIMA GENERACIÓN

Protege contra todos los tipos de amenazas, desde malware y ransomware hasta ataques sofisticados, y puede ser implantado en minutos, protegiendo inmediatamente sus endpoints.

FALCON INSIGHT XDR | DETECCIÓN Y RESPUESTA EXTENDIDAS (XDR)

Ofrece Detección y respuesta de endpoints (EDR) (EDR) y Detección y Respuesta Extendidas (XDR) unificadas y líderes en la industria con visibilidad en toda la empresa para detectar automáticamente la actividad de adversarios y responder en todos los endpoints y en todas las superficies de ataque clave.

FALCON DATA PROTECTION | PROTECCIÓN DE DATOS UNIFICADA

Proporciona visibilidad profunda en tiempo real de lo que sucede con datos confidenciales y detiene el robo de datos con la aplicación de políticas que siguen automáticamente al contenido, no a los archivos.

FALCON FIREWALL MANAGEMENT | FIREWALL BASADO EN EL HOST

Ofrece una gestión simple y centralizada del firewall del host, lo que facilita la administración y el control de las políticas de firewall del host.

FALCON DEVICE CONTROL | SEGURIDAD DE USB

Proporciona la visibilidad y el control preciso necesarios para permitir el uso seguro de los dispositivos USB en toda la organización.

FALCON FOR MOBILE | DETECCIÓN DE AMENAZAS EN DISPOSITIVOS MÓVILES

Protege contra amenazas a dispositivos iOS y Android extendiendo la XDR y la EDR a tu dispositivo móvil, con protección avanzada contra amenazas y visibilidad en tiempo real de la actividad de aplicaciones y redes.

FALCON FORENSICS | CIBERSEGURIDAD FORENSE

Te permite responder y recuperar rápidamente con recopilación de datos forense automatizada, enriquecimiento y correlación.

FALCON GO | CIBERPROTECCIÓN PARA PYMES

Brinda a las pequeñas empresas tranquilidad frente a las amenazas cibernéticas con antivirus de última generación, control de dispositivos y protección de dispositivos móviles fáciles de instalar.

FALCON INSIGHT PARA XIoT | XIoT PROTECCIÓN DE ACTIVOS

Ofrece una protección líder en el sector para dispositivos de Internet de las cosas ampliado (XIoT), como tecnología operativa, IoT y sistemas de control industrial, mediante visibilidad en tiempo real, detección y prevención de amenazas en entornos conectados.

Operaciones contra adversarios

FALCON ADVERSARY OVERWATCH | CACERÍA DE AMENAZAS

Proporciona protección las 24 horas del día, los 7 días de la semana en endpoints, identidades, workloads de la nube y SIEM de próxima generación ofrecida por expertos en cacería de amenazas impulsada por IA. También incluye inteligencia sobre amenazas incorporada para exponer la tradecraft de los adversarios, las vulnerabilidades y las credenciales robadas.

FALCON ADVERSARY INTELLIGENCE | AUTOMATIZACIÓN DE SOC

Reduce el tiempo de respuesta de días a minutos en todo el Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés) con automatización de inteligencia de extremo a extremo, lo que te permite enviar instantáneamente amenazas potenciales a un sandbox de malware avanzado, extraer indicadores de compromiso y desplegar contramedidas, todo mientras se monitorea continuamente para detectar fraudes y proteger tu marca, tus empleados y tus datos confidenciales.

FALCON ADVERSARY INTELLIGENCE | INTELIGENCIA SOBRE ADVERSARIOS

Ofrece informes de inteligencia líderes en la industria a tu alcance, junto con detecciones prediseñadas y cacería con un solo clic, para reducir el tiempo y el costo necesarios para comprender a los sofisticados adversarios estados nación, cibercrimen y hacktivistas, y defenderse contra ellos.

FALCON COUNTER ADVERSARY OPERATIONS ELITE | ANALISTA BAJO DEMANDA

Proporciona un analista asignado que aprovecha herramientas de investigación y cacería de amenazas impulsadas por IA, mejoradas por una profunda inteligencia adversaria, para detectar e interrumpir adversarios en tu entorno de TI y más allá.

Seguridad en la Nube

FALCON CLOUD SECURITY: SEGURIDAD PROACTIVA

Proporciona una gestión unificada de la postura de seguridad (USPM) y un contexto empresarial en todas las capas de la nube aprovechando la inteligencia sobre amenazas líder en la industria, las rutas de ataque de extremo a extremo y ExPRT.AI para que los equipos de nube puedan priorizar rápidamente su trabajo, neutralizar riesgos cruciales y no dejar a los adversarios espacio para atacar.

FALCON CLOUD SECURITY: CLOUD RUNTIME PROTECTION

Ofrece protección líder de workload de la nube (CWP) y detección y respuesta en la nube (CDR), lo que permite a los equipos del SOC detectar y responder a amenazas activas en nubes híbridas para que los adversarios sean detenidos en seco.

FALCON CLOUD SECURITY: CNAPP

Incluye las funciones y capacidades de Proactive Security y Cloud Runtime Protection para Falcon Cloud Security.

FALCON ADVERSARY OVERWATCH: CLOUD | CACERÍA DE AMENAZAS

Ofrece seguridad proactiva y protectora como servicios gestionados a través de la cacería de amenazas entre dominios Falcon Adversary OverWatch y Falcon Complete Next-Gen MDR, impulsados por inteligencia integrada de amenazas para proteger el plano de control de la nube, el sistema operativo host y el plano de datos.

Seguridad de SaaS

FALCON SHIELD | SEGURIDAD DE APLICACIONES SAAS

Permite a los equipos de seguridad proteger toda su pila de SaaS mediante la prevención, detección y habilitación de respuesta a amenazas; encontrar y solucionar proactivamente debilidades en su pila de SaaS; y mantener una seguridad continua para todas las configuraciones, usuarios humanos y no humanos, datos e IA generativa de SaaS

Protección de identidad

FALCON IDENTITY THREAT DETECTION

Proporciona visibilidad unificada entre identidades híbridas y detección de amenazas impulsada por IA para exponer las amenazas basadas en identidad antes de que escalen.

FALCON IDENTITY THREAT PROTECTION

Protege identidades híbridas con detección de amenazas impulsada por IA y análisis de comportamiento aprovechando la plataforma unificada de Falcon para detener ataques basados en identidad en tiempo real.

FALCON ADVERSARY OVERWATCH: IDENTITY | THREAT HUNTING

Proporciona cacería de amenazas a identidades gestionada las 24 horas, los 7 días de la semana, detecta proactivamente ataques basados en identidad, monitorea foros criminales en busca de credenciales robadas y aplica desafíos de MFA para evitar el acceso no autorizado.

SIEM de próxima generación

FALCON NEXT-GEN SIEM | SIEM

Te permite detener la brecha y optimizar tu SOC unificando la mejor detección de la industria, inteligencia sobre amenazas de clase mundial, búsqueda ultrarrápida e investigación dirigida por IA en una sola plataforma.

Seguridad y operaciones de TI

FALCON EXPOSURE MANAGEMENT | GESTIÓN DE EXPOSICIÓN

Proporciona visibilidad total de la superficie de ataque, prioriza las vulnerabilidades con IA y automatiza la remediación para reducir proactivamente el riesgo cibernético y prevenir las brechas.

FALCON EXPOSURE MANAGEMENT: CAASM

Te permite descubrir y monitorear activos gestionados y no gestionados en tiempo real y mapear visualmente los activos y sus relaciones, lo que revela insights de host profundos sobre aplicaciones, navegadores, CVE y configuraciones erróneas.

FALCON FILEVANTAGE | SUPERVISIÓN DE LA INTEGRIDAD DE LOS ARCHIVOS

Proporciona visibilidad centralizada, integral y en tiempo real que impulsa el cumplimiento y ofrece datos contextuales relevantes.

FALCON ADVERSARY OVERWATCH: SIEM DE PRÓXIMA GENERACIÓN | CACERÍA DE AMENAZAS

Caza de forma proactiva las amenazas avanzadas en toda la empresa mediante la correlación de los datos de CrowdStrike Falcon® Next-Gen SIEM propios y de terceros, lo que interrumpe los ataques en dispositivos periféricos, software como servicio (SaaS), correo electrónico, sistemas operativos y más.

CrowdStrike Services

Servicios gestionados

FALCON COMPLETE NEXT-GEN MDR | DETECCIÓN Y RESPUESTA GESTIONADA

Proporciona protección impulsada por expertos las 24 horas, los 7 días de la semana en endpoints, identidades, carga de trabajo en la nube y datos de terceros combinando experiencia en seguridad de élite, tecnología impulsada por IA y cacería proactiva de amenazas para detectar, interrumpir y corregir amenazas sofisticadas en minutos.

RESPUESTA A INCIDENTES

Proporciona respuesta de élite a incidentes las 24 horas del día, los 7 días de la semana, para contener amenazas, restaurar el orden y mitigar el impacto de la brecha.

Servicios de respuesta a incidentes | Proporciona respuesta y recuperación integrales en caso de una brecha cibernética, que abarca , investigación, remediación y recuperación , todo respaldado por inteligencia sobre amenazas de clase mundial y ofrecido por un equipo de respuesta a incidentes altamente experimentado.

Servicios de defensa activos | Proporciona respuesta entre dominios para recuperarse de una brecha con rapidez y precisión.

Retención de servicios | Proporciona acceso a pedido a la experiencia de CrowdStrike, desde la respuesta rápida hasta la resiliencia a largo plazo.

SERVICIOS DE ASESORAMIENTO ESTRATÉGICO

Desarrolla y madura el programa de seguridad para mejorar las defensas

Ejercicios de mesa | Simula escenarios de respuesta a incidentes que exponen los vacíos del proceso y mejoran la coordinación de todo el equipo, desde los analistas hands-on-keyboard hasta las partes interesadas ejecutivas.

Evaluación de madurez | Evalúa exhaustivamente la postura de seguridad de tu organización identificando vacíos, creando puntos de referencia de capacidades y proporcionando una hoja de ruta priorizada para fortalecer las defensas contra amenazas en evolución.

Preparación regulatoria y consultoría para directores de experiencia (CXO) | Te ayuda a comprender y prepararte para los mandatos regulatorios relacionados con la ciberseguridad, como las cambiantes responsabilidades de riesgo y gobernanza de la Junta Directiva.

Revisión del programa de riesgo interno | Fortalece tu estrategia de riesgo interno mediante la evaluación y optimización de tus capacidades actuales de detección, prevención y respuesta.

SERVICIOS DEL EQUIPO ROJO

Prueba y valida defensas a través de ataques emulados que exponen debilidades

Pruebas de penetración | Proporciona emulaciones de ataques que prueban la capacidad de detección y respuesta de tu personal, procesos y tecnología para identificar vulnerabilidades.

Ejercicio de Equipo Rojo/Equipo Azul | Aumenta la preparación para la respuesta bajo la guía de expertos, mientras un equipo rojo ataca los sistemas en un ejercicio simulado y un equipo azul monta la defensa.

Ejercicio de emulación de adversario | Mide la preparación para defenderse contra la infiltración de un adversario sofisticado que emplea una tradecraft avanzada.

Servicios del Equipo Rojo de IA | Expone vulnerabilidades en la pila de IA generativa que podrían ser explotadas mediante la puesta a prueba de integraciones de LLM para la exposición de datos confidenciales y manipulación de adversarios.

SERVICIOS DE EVALUACIÓN TÉCNICA

Audita y aborda los vacíos de seguridad en endpoints, nubes y aplicaciones de SaaS para reducir el riesgo de manera tangible

Evaluación de seguridad de software como un servicio (SaaS) | Evalúa entornos SaaS para detectar brechas de seguridad en configuraciones, controles de acceso, política de datos e integraciones de terceros.

Evaluación de riesgos técnicos | Destaca las vulnerabilidades, debilidades y vacíos de seguridad en el entorno de TI en todos los dispositivos de endpoint, aplicaciones e identidades de usuario.

Evaluación de seguridad de identidad | Audita las prácticas de seguridad de identidad y la postura de defensa para detectar debilidades, lo que incluye la configuración del dominio de Active Directory, la configuración de cuentas, la delegación de privilegios y las posibles rutas de ataque.

Evaluación de seguridad en la nube | Identifica configuraciones erróneas y vulnerabilidades en el entorno en la nube que podrían ser explotadas por adversarios.

Evaluación de afectación | Expone y aborda la actividad de amenazas no detectadas a través de una cacería de amenazas única disponible para endpoints, nubes y aplicaciones de SaaS.

CAPACITACIÓN Y MEJORA DE CAPACIDADES DE SEGURIDAD

Desarrolla la perspicacia en seguridad y acaba con el vacío de habilidades a través de CrowdStrike University, que ofrece capacitación a pedido, rutas de aprendizaje personalizadas y cinco certificaciones para una profunda experiencia en el módulo Falcon.

SERVICIOS DE PULSO CROWDSTRIKE

Proporciona consultoría continua mediante sesiones centradas en una cadencia recurrente, quincenal, mensual o bimensual, adaptadas a tus necesidades cambiantes. Estos compromisos se alinean con tus prioridades y se adaptan según sea necesario, lo que permite un progreso constante, una mayor resiliencia y una madurez estratégica que evoluciona a la velocidad del adversario.

Acerca de CrowdStrike

CrowdStrike (Nasdaq: CRWD) es un líder global en ciberseguridad que ha redefinido la seguridad moderna con una de las plataformas nativas para la nube más avanzadas del mundo para proteger áreas críticas de riesgo corporativo — endpoints y workloads de nube, identidad y datos.

Impulsado por la Nube de seguridad de CrowdStrike y una inteligencia artificial de clase mundial, la plataforma CrowdStrike Falcon® aprovecha indicadores de ataque en tiempo real, inteligencia sobre amenazas, el tradecraft cambiante de los adversarios y telemetría enriquecida de toda la empresa para ofrecer detecciones hiper precisas, protección y remediación automatizadas, cacería de amenazas de élite y observabilidad priorizada de vulnerabilidades.

Construida para ese fin en la nube con una arquitectura única y liviana de agente, la plataforma Falcon entrega implantación rápida y escalable, protección y desempeño superiores, complejidad reducida y un tiempo de valor inmediato.

CrowdStrike: Detenemos los ataques.

Obtén más información en: www.crowdstrike.com

Síguenos: Blog | X | LinkedIn | Facebook | Instagram | YouTube

Me gustaría comenzar una prueba gratuita: www.crowdstrike.com/free-trial-guide