Panorama de amenazas para el sector financiero de LATAM en 2025

Evaluación de los objetivos de los actores de amenazas y estrategias de defensa para las instituciones del sector financiero latinoamericano

DIGI AMERICAS

Duke | PRATT SCHOOL of ENGINEERING

En colaboración con

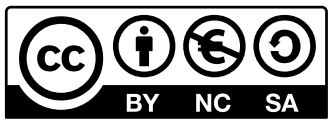
Recorded Future®

DIGI AMERICAS ALLIANCE MEMBERS

aws Apple Batuta CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE

Google kriptos LUMU mastercard netskope paloalto NETWORKS fluid attacks we hack your software

Resecurity Schneider Electric SISAP Sistemas Aplicativos Telefónica tenable Trellix TREND MICRO



CC BY-NC-SA: Esta licencia permite a los reutilizadores distribuir, modificar, adaptar y crear a partir del material en cualquier medio o formato únicamente con fines no comerciales y siempre que se cite al creador. Si usted modifica, adapta o construye a partir del material, deberá licenciar el material modificado bajo idénticos términos. Los contenidos expresados en este documento se presentan exclusivamente con fines informativos y no representan la opinión o posición oficial del Centro de Política y Derecho de la Ciberseguridad, ni de ninguno de sus miembros. Para más información, por favor póngase en contacto con admin@digiamericas.org

Créditos

Universidad de Duke

Rupal Kharod
Arturo Ehuan
Justin Hayes
Emmanuel Petrov
Sakthi Vinayak
Shefali Ahuja
Aditya Srikar
Lucy Li
Diego Sanchez

Digi Americas Alliance

Alain Karioty
Alexis Steffaro
Andy Kotz
Belisario Contreras
Brett DeWitt
Carlos Torales
Christian Torres
Cory Bullock
Fernando Quintero
Gene Yoo
Ghassan Dreibi
Hernan Armbruster
Jordana Siegel
Jorge Blanco
José Juan Haro
Mario de la Cruz Sarabia
Mauricio Benavides
Mauricio Nanne
Norberto (Bert) Milan
Patrick Ford
Rafael Alvarez
Ricardo Villadiego
Stephen Fallas

DIGI AMERICAS ALLIANCE MEMBERS

aws Apple Batuta CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE
Google kriptos LUMU netskope paloalto NETWORKS fluid attacks we hack your software
Resecurity Schneider Electric SISAP Sistemas Aplicativos Telefónica tenable Trellix TREND MICRO

Resumen ejecutivo

América Latina se encuentra entre las regiones menos preparadas para los ciberataques, según el Índice de Ciberseguridad de la ONU.[1] Esta vulnerabilidad se debe a la falta de inversión en ciberseguridad, la escasez de profesionales cualificados y la debilidad de los marcos normativos.[2] Aunque tras la pandemia del COVID-19 surgió una revolución digital en sectores como las tecnologías financieras y el comercio electrónico, estos avances no se vieron acompañados de medidas de seguridad adecuadas. Como señala la fundadora de la Red Latinoamericana de Investigación en Ciberseguridad, Louise Marie Hurel, "el espíritu emprendedor e innovador de América Latina no viene acompañado de una preocupación por la seguridad".[3]

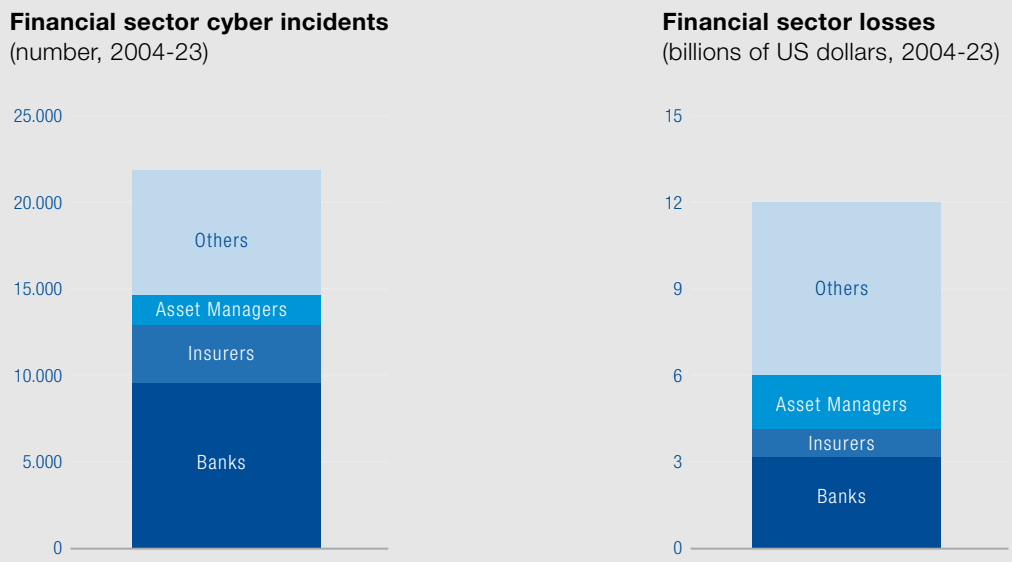
La creciente amenaza se ve ejemplificada por incidentes de gran repercusión, como el ataque de ransomware al Ministerio de Hacienda de Costa Rica y al sistema judicial de Brasil, que subrayan la necesidad de hacer frente a la proliferación de la amenaza. Además, sólo 7 de los 32 países de la región tienen planes para proteger sus infraestructuras críticas, y sólo 20 cuentan con Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT por sus siglas en inglés) operativos. A medida que el panorama global de las ciberamenazas madura, con un aumento del 34,5% en las violaciones de datos y del 84% en los ataques de ransomware en 2023, los desafíos de ciberseguridad de América Latina son cada vez más urgentes.[4]

La investigación Panorama de amenazas para el sector financiero de LATAM de la Universidad de Duke, que utiliza datos del Intelligence Graph de Recorded Future, analiza los tres principales grupos de actores de amenazas que tienen como objetivo el sector financiero latinoamericano y los controles sugeridos que se pueden implementar para evitar los ciberataques y mitigar su impacto. El extenso análisis de datos identificó finalmente a cinco agresivos actores de amenazas: CL0P, LockBit, Horabot, Blind Eagle, y Mispadu.

Las brechas cibernéticas se han vuelto cada vez más comunes en las instituciones financieras latinoamericanas, con distintos desafíos de ciberseguridad. Los datos de 2023 revelan que los países latinoamericanos experimentan la tasa más alta de ataques de ransomware a organizaciones, con un 79% de incidentes relacionados con ransomware, en comparación con el promedio mundial del 53%.[5] Este informe explora los enfoques y motivaciones de los principales actores de amenazas: CL0P, Mispadu, Horabot, Blind Eagle, y LockBit, y la conclusión de que estos actores de amenazas utilizaron TTP similares.

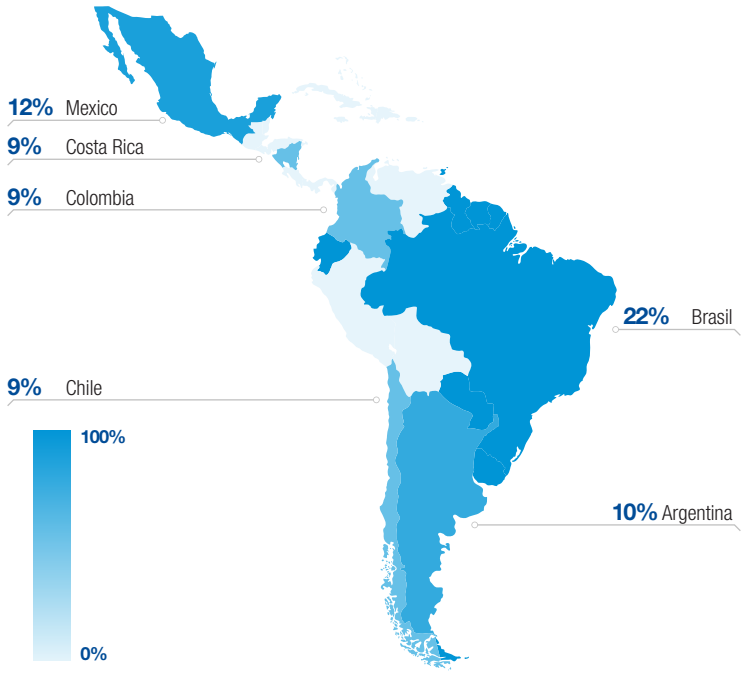
[1] https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx
[2] https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx
[3] https://www.americasquarterly.org/article/new-aq-hackers-paradise-why-latin-america-is-so-vulnerable/#:~:text=%E2%80%9CLatin%20America's%20entrepreneurial%20and%20innovative,cyberbreaches-%20start%20from%20human%20error.
[4] https://go.flashpoint.io/2024-global-threat-intelligence-report-download
[5] https://www.ptsecurity.com/ww-en/analytics/latam-cybersecurity-threatscape-2022-2023- en/

Figura 1: Ciberincidentes y pérdidas en el sector financiero



La región de América Latina presenta vulnerabilidades dentro de las instituciones financieras que son únicas dentro del panorama mundial y requieren una cuidadosa consideración. Los principales países objetivo de los grupos de actores de amenazas incluyen Brasil, México, Argentina, Colombia y Perú. Estos países representaron el 50% de los países víctimas que los atacantes eligieron como blanco en 2023, con el 12% del total de ataques cibernéticos en el mundo ocurriendo en América Latina.[6]

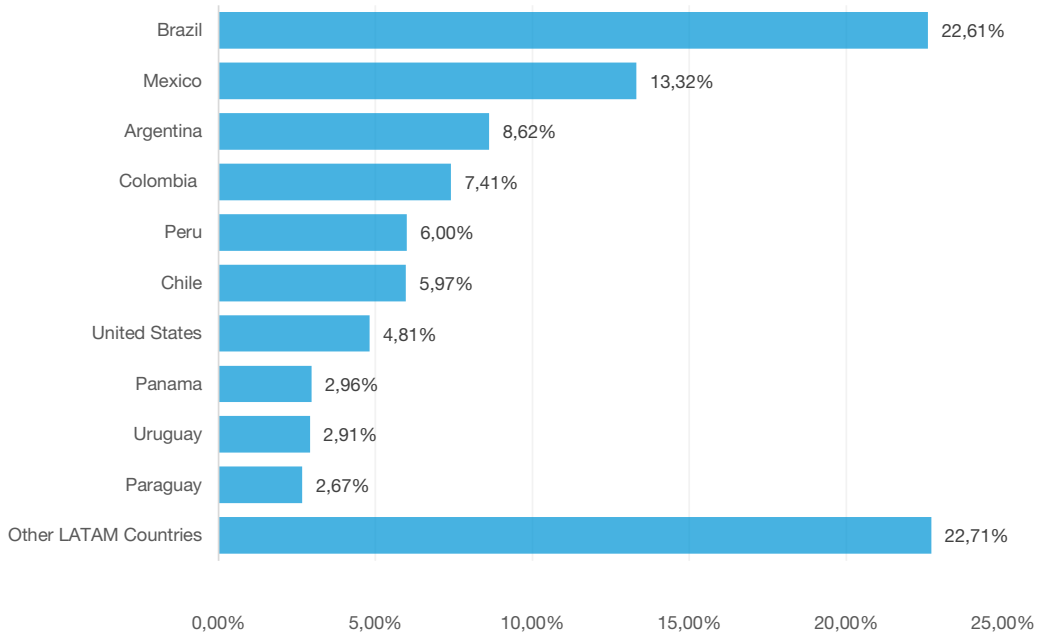
Figura 2: Distribución de ataques exitosos en América Latina



En 2023, LATAM se enfrentó a 1.498 ataques de ransomware y 6.048 ataques de phishing por parte de 33 grupos distintos (SOCRader, 2024, pp. 4–5).[7] Se cree que la insuficiente inversión en ciberseguridad, las economías volátiles y un entorno muy poco regulado han magnificado los riesgos institucionales.

[6] https://www.ibm.com/reports/threat intelligence
[7] https://doi.org/CyberThreatIntelligenceAnalysis

Figura 3: Distribución de las amenazas de la Dark Web por país de objetivo principal



Los datos recopilados para crear este informe ofrecen una amplia comprensión de la evolución del panorama de las amenazas, al tiempo que tienen en cuenta las limitaciones de la inteligencia de fuente abierta, como los procesos laboriosos, la eficacia limitada y la posibilidad de pasar por alto las amenazas más pequeñas al priorizar a los actores de amenazas de mayor perfil.[8] Este informe proporciona observaciones vitales para mejorar las recomendaciones sobre defensas de ciberseguridad que pueden crear un ecosistema financiero latinoamericano más resistente.

El sector de servicios financieros de LATAM debería considerar el uso de una estrategia de defensa de ciberseguridad que esté informada sobre el actor de la amenaza para mitigar los impactos de los ciberataques. Las organizaciones de la industria de servicios financieros que utilizan una estrategia informada pueden prepararse para las tácticas, técnicas y procedimientos (TTP) comunes utilizados por los actores de amenazas. Al revisar e incorporar las TTPs mapeadas que utilizan estos grupos de actores de amenazas, los ciberdefensores pueden implementar controles de ciberseguridad de manera más efectiva.

[8] https://www.ptsecurity.com/ww-en/analytics/latam-cybersecurity-threatscape-2022-2023-en/

Tabla de contenido

Resumen ejecutivo 3
1 Introducción 9
1.1 Objectivos 9
2 Antecedentes 10
2.1 Falta de información sobre las amenazas 10
2.2 Vulnerabilidades históricas de ransomware 11
2.2.1 Introducción 11
2.2.2 Análisis de patrones de vulnerabilidad 12
2.2.3 Análisis de brechas e impacto futuro 12
2.2.4 Mejoras en la postura de seguridad desde 2018 hasta la actualidad 13
2.2.5 Análisis del impacto futuro 14
2.3 Pérdidas por ransomware para la industria de servicios financieros 14
2.3.1 Caso práctico 1 - Ataque dirigido de LockBit 3.0 contra un banco brasileño 14
2.3.2 Caso práctico 2 - Ataque del ransomware de Play a una empresa financiera chilena 15
2.4 Capacidades de respuesta al ransomware 15
2.4.1 Evaluación de la infraestructura de respuesta regional 15
2.4.2 Capacidades de respuesta técnica y limitaciones de recursos 16
2.4.3 Coordinación de la respuesta transfronteriza 18
2.4.4 Mecanismos de intercambio de información y su impacto en la vulnerabilidad del sector financiero 18
2.4.5 Variación en los marcos de coordinación público-privada 18
3 Tendencias de la industria 20
3.1 Principales actores de ciberamenazas dirigidas a la industria financiera en América Latina 20
3.1.1 Necesidad de más profesionales de la ciberseguridad 20
3.1.2 Mayor presupuesto en ciberseguridad para hacer frente al aumento de las ciberamenazas 21
3.1.3 Razones para las inversiones 22
3.1.4 Cambio de la banca tradicional a la banca en línea y basada en aplicaciones 23
3.2 Factores socioeconómicos contextuales que influyen en la exposición al riesgo 23
3.2.1 Rápido crecimiento de la tecnología financiera 23
3.2.2 Dependencia de sistemas obsoletos 23
3.2.3 Disparidades económicas y digitales 24
4 Lagunas normativas 25
4.1 Requisitos de notificación de ataques de ransomware y falta de normas 25
5 Perfiles de los actores de amenazas 27
5.1 CL0P 27
5.1.1 Perfil de las víctimas y análisis del impacto 27
5.1.2 Capacidades y funcionalidad del malware 27
5.1.3 Evolución de las operaciones de CL0P 28
5.1.4 Impacto en la infraestructura financiera 29
5.1.5 Deficiencias en materia de normativa y políticas 30
5.1.6 Estructura del mercado y contexto de la transformación digital 31

5.1.7 Presiones de rentabilidad que crean compromisos de seguridad 31
5.1.8 Vulnerabilidades específicas del sector 31
5.1.9 Carencias en el sector público que crean riesgos descendentes 32
5.1.10 La convergencia de vulnerabilidades crea una oportunidad estratégica para CL0P 32
5.1.11 Implicaciones de cara al futuro 33
5.1.12 Tácticas, técnicas y procedimientos de CL0P 33
5.1.13 Recomendaciones técnicas/tácticas de CL0P 38
5.2 LockBit 45
5.2.1 Actividad relevante del actor de amenazas 45
5.2.2 Antecedentes 46
5.2.3 Correlación 46
5.2.4 Técnicas, tácticas y procedimientos de LockBit 46
5.2.5 Recomendaciones Técnicas/Tácticas de LockBit 50
5.3 Mispadu 56
5.3.1 Métodos de Mispadu y explotación de la infraestructura de LATAM 57
5.3.2 Tácticas, técnicas y procedimientos 57
5.3.3 Tácticas, técnicas y procedimientos de Mispadu 58
5.4 Horabot 62
5.4.1 Capacidades y funcionalidad del malware 62
5.4.2 Correlación entre Horabot y Mispadu 63
5.4.3 Tácticas, técnicas y procedimientos de Horabot 64
5.5 Blind Eagle 67
5.5.1 Actividad relevante del actor de amenazas 67
5.5.2 Antecedentes 68
5.5.3 Correlación 68
5.5.4 Recomendaciones 68
5.5.5 Técnicas, tácticas y procedimientos 69
5.5.6 Mitigación de Blind Eagle 71
6 Recomendaciones estratégicas para la ciberseguridad en el sector financiero de América Latina 73
6.1 Implementación de controles de seguridad específicos para la región 73
6.2 Establecer redes de CSIRT del sector financiero 73
6.3 Reforzar la respuesta a incidentes transfronterizos 73
6.4 Reforzar la concienciación sobre la seguridad centrada en el ser humano 73
6.5 Transformación digital segura y control de acceso 73
6.6 Mejorar la gestión y supervisión de riesgos de terceros 73
6.7 Armonizar los requisitos de presentación de informes 73
6.8 Mejorar el intercambio de información 73
6.9 Reforzar la infraestructura de ciberseguridad 74
6.10 Mejorar la educación en ciberseguridad y el desarrollo de la fuerza laboral 74
6.11 Reforzar los marcos normativos 74
6.12 Fomentar la colaboración internacional 74
7 Apéndice 75
7.1 Datos segmentados 75
7.2 Definiciones 82
7.3 Vulnerabilidades, exposiciones e indicadores de compromiso comunes 83
7.4 Indicadores de compromiso (IOC) 83
7.5 Evidencia forense 84

1 Introducción

En los últimos años, el sector financiero en América Latina ha experimentado una rápida transformación digital, impulsada por la expansión de los servicios fintech, el aumento de la penetración de Internet y una creciente demanda de banca digital. Sin embargo, este progreso tecnológico ha superado el desarrollo de sólidas prácticas de ciberseguridad, dejando a las instituciones financieras cada vez más vulnerables a sofisticadas amenazas cibernéticas. A medida que la ciberdelincuencia se vuelve más organizada y oportunista, el sector financiero, que ya es un objetivo de gran valor, se enfrenta a mayores riesgos que amenazan la estabilidad económica, la confianza de los consumidores y la seguridad nacional.

Este documento investiga el panorama de la ciberseguridad en el mercado financiero latinoamericano, con especial atención a los actores, métodos y vulnerabilidades sistémicas que definen la actual postura de riesgo de la región. Basándose en datos de inteligencia sobre amenazas, estudios de casos regionales y opiniones de investigadores de seguridad, este estudio pretende analizar las motivaciones y tácticas de los principales actores de amenazas que tienen como objetivo los sistemas financieros latinoamericanos. También explora los retos estructurales, como las lagunas normativas, la escasez de talento y la falta de inversión, que dificultan una defensa eficaz de la ciberseguridad.

El objetivo de esta investigación es doble: en primer lugar, proporcionar una visión global del entorno de amenazas en evolución al que se enfrentan las instituciones financieras en América Latina y, en segundo lugar, recomendar estrategias prácticas basadas en las amenazas para mejorar la resistencia cibernética en la región. Se hace especial hincapié en las actividades de cinco grandes grupos de actores de amenazas (CL0P, LockBit, Mispadu, Blind Eagle, y Horabot) cuyas operaciones ejemplifican tendencias más amplias en la ciberdelincuencia dirigida al sector financiero.

Las siguientes secciones de este documento se organizan del siguiente modo: La Sección 2 describe el panorama de las amenazas y presenta los principales grupos de ciberdelincuentes activos en la región. La Sección 3 evalúa la preparación de la región en materia de ciberseguridad, las vulnerabilidades institucionales y las estrategias nacionales de respuesta. La Sección 4 destaca las lagunas normativas que existen actualmente en América Latina. La Sección 5 se sumerge en 5 APTs diferentes, su actividad en la región, sus TTPs, y recomendaciones a las organizaciones sobre cómo hacer frente a estas amenazas. Por último, la Sección 6 ofrece una serie de recomendaciones estratégicas para la ciberseguridad en el sector financiero de América Latina.

1.1 Objetivos

El equipo de investigación evaluó datos de código abierto de la plataforma Recorded Future para formar una evaluación de cómo diferentes grupos de actores de amenazas podrían utilizar TTPs similares al atacar empresas de servicios financieros en LATAM. Este informe ofrece un análisis con cuatro objetivos principales:

(1) Identificar los principales grupos de actores de amenazas que atacan a instituciones financieras latinoamericanas y sus bases operativas.

(2) Analizar las TTP empleadas por estos actores de amenazas.

(3) Evaluar el impacto de sus estrategias sobre las instituciones financieras de la región.

(4) Formular recomendaciones prácticas para mitigar las TTP identificadas, aprovechando el marco MITRE ATT&CK y los conocimientos para profesionales de la ciberseguridad.

2 Antecedentes

Los ataques cibernéticos a instituciones financieras en América Latina han aumentado significativamente en los últimos cinco años, lo que refleja la tendencia mundial de aumento de las amenazas cibernéticas, que han crecido a una tasa anual del 25% en la última década, a partir de 2024.[9] Según el Informe de Estabilidad Financiera Global 2024,[10] el riesgo de pérdidas extremas relacionadas con la cibernética se ha más que cuadruplicado desde 2017, alcanzando los 2.500 millones de dólares. Además, el 2024 LATAM CISO Report destaca que países como Costa Rica, México, Brasil y Argentina atribuyen la frecuencia y el éxito de estos ataques a las brechas en la preparación de la respuesta. Estas brechas van desde deficiencias en las capacidades técnicas hasta fallas en la comunicación entre las entidades de los sectores público y privado entre 2020 y 2025. Sólo alrededor de la mitad de los países encuestados contaban con una estrategia nacional de ciberseguridad centrada específicamente en el sector financiero o habían implementado normativas específicas de ciberseguridad.

En consecuencia, América Latina por sí sola representó el 12% del total de ciberataques en todo el mundo en 2022, superando a Oriente Medio y África, que comprendieron el 7%, a pesar de estar comparativamente infradotada de recursos.[11] Los atacantes se dirigieron principalmente a organizaciones e individuos en Brasil, México y Argentina, que en conjunto representaron el 44% de todos los ataques. Estos países tienen las mayores economías e instituciones financieras de América Latina, lo que los convierte en objetivos atractivos para los ciberdelincuentes.[12] A medida que los incidentes cibernéticos siguen aumentando, la estabilidad financiera de la región está cada vez más en riesgo, dado que las instituciones financieras se encuentran entre los objetivos clave de los actores de ciberamenazas y constituyen una parte significativa de los sectores de interés. Sólo el sector financiero y de seguros representa el 39,47% de los incidentes cibernéticos revelados en América Latina.[13] Si no se abordan, estas amenazas podrían tener graves repercusiones económicas, lo que pone de relieve la necesidad de adoptar medidas de ciberseguridad sólidas.

2.1 Falta de información sobre las amenazas

Las instituciones financieras latinoamericanas se enfrentan a una mayor susceptibilidad a los ciberataques debido a una combinación de factores, entre los que se incluyen los siguientes.

1. Falta de concienciación y formación sobre ciberseguridad en las instituciones financieras: El principal reto no es solo la falta general de concienciación sobre la ciberseguridad, sino una brecha de formación y aprendizaje dentro de las instituciones financieras. Los empleados necesitan una formación completa en ciberseguridad, mientras que los consumidores requieren campañas de concienciación contra las posibles ciberamenazas.

2. La ausencia de normas y reglamentos de ciberseguridad, que deja a muchas instituciones financieras vulnerables a las ciberamenazas: Las organizaciones optan por no implementar voluntariamente los marcos de ciberseguridad (NIST CSF) o ISO 27001, dejándose expuestas a ciberataques de grupos de actores de amenazas que solo deben encontrar una vulnerabilidad para comprometer a una empresa víctima.

3. Inversión insuficiente en tecnología a nivel de hardware y software: El uso de software obsoleto genera brechas de seguridad en las infraestructuras críticas y debilita las defensas de la región frente a los ciberataques. La disparidad tecnológica entre los países latinoamericanos y sus homólogos más desarrollados de Norteamérica y Europa agrava estas vulnerabilidades, dificultando que la región pueda contrarrestar eficazmente las ciberamenazas sofisticadas.[14]

El impacto financiero de las brechas de ciberseguridad ha sido asombroso en todo el mundo. Según IBM Security, “el costo promedio de la violación de datos en 2020 se estimó en 3,86 millones de dólares”, incluido el coste de los honorarios legales, las multas de cumplimiento, el daño a la reputación y la pérdida de confianza de los clientes.[15] En mayo de 2021, el ataque de ransomware a Colonial Pipeline paralizó la distribución de combustible en todo Estados Unidos, interrumpiendo la infraestructura crítica y causando escasez generalizada. El ataque, atribuido al grupo de ransomware DarkSide, obligó a la empresa a detener

[9] https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe
[10] https://www.ptsecurity.com/ww-en/analytics/latam-cybersecurity-threatscape-2022-2023-en/
[11] https://www.ibm.com/reports/threat-intelligence
[12] https://www.statista.com/statistics/802640/gross-domestic-product-gdp-latin-america-caribbean-country/
[13] https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe
[14] 10.3390/informatics10030071 10.47460/athenea.v3i9.43
[15] https://www.ibm.com/reports/threat intelligence

sus operaciones, lo que provocó compras de pánico y subidas de precios del combustible. En respuesta, Colonial Pipeline pagó un rescate de 4,4 millones de dólares para recuperar el acceso a sus sistemas, pero las repercusiones económicas persistieron mucho tiempo después, como interrupciones en la cadena de suministro y un mayor escrutinio normativo.[16] Este incidente puso de manifiesto vulnerabilidades críticas de ciberseguridad en los sistemas de control industrial, destacando la urgente necesidad de marcos de ciberseguridad más sólidos y estrategias proactivas de mitigación de riesgos para prevenir ataques similares a gran escala.

Las vulnerabilidades explotadas en el ataque a Colonial Pipeline, y el daño resultante, ponen de relieve la susceptibilidad de América Latina a las ciberamenazas debido a la insuficiencia de los marcos regulatorios, la debilidad de la infraestructura de ciberseguridad y la menor concienciación de las empresas y los consumidores, que los ciberdelincuentes manipulan para obtener beneficios económicos. América Latina tiene el porcentaje más alto de ataques de ransomware, con un 79% en comparación con la media mundial del 53%, y el 94% de los ataques se atribuyen a intrusiones en sistemas, ingeniería social y ataques básicos a aplicaciones web.[17] El costo promedio de una violación de datos ha aumentado a 4,45 USD,[18] y al más alto desde 2020 a USD 2,46M en América Latina.[19] América Latina tiene los niveles más bajos de preparación en ciberseguridad, lo que la hace la más susceptible a los ataques según el Índice Global de Ciberseguridad 2020. Esto seguirá afectando a la economía de la región.

2.2 Vulnerabilidades históricas de ransomware

2.2.1 Introducción

El sector financiero de América Latina experimentó un aumento significativo de ataques cibernéticos sofisticados entre 2018 y 2024, destacando vulnerabilidades críticas en la infraestructura digital de la región. Este análisis examina 12 incidentes importantes que tuvieron como objetivo bancos, instituciones financieras y sistemas gubernamentales en todo Chile, Brasil, México, Argentina y otros países latinoamericanos. Los ataques, que van desde el atraco de 10 millones de dólares al Banco de Chile en 2018 [20] [21] hasta la filtración de datos de 2024 Bankingly que afectó a 135.000 clientes,[22] demuestran un panorama de amenazas en evolución dominado por el ransomware y los grupos de amenazas avanzadas persistentes (APT).

La investigación revela un patrón preocupante: los atacantes se dirigen cada vez más a proveedores de servicios de terceros y plataformas de tecnología financiera para vulnerar varias instituciones simultáneamente. Las organizaciones dependen cada vez más de diversos proveedores externos, lo que las expone a distintos riesgos cibernéticos. Los proveedores de software y SaaS (Software as a Service) se enfrentan a vulnerabilidades y ataques a la cadena de suministro, donde los fallos en aplicaciones ampliamente utilizadas, como la solución Managed File Transfer de Progress Software, pueden conducir a la exfiltración masiva de datos.[23] Del mismo modo, los entornos de infraestructura como servicio pueden presentar riesgos debidos a errores de configuración, deficiencias en el control de acceso y cortes del servicio, que pueden interrumpir las operaciones empresariales. La brecha de Bankingly, relacionada con una plataforma de tecnología financiera digital basada en SaaS, comprometió a siete bancos latinoamericanos debido a cubos de almacenamiento mal configurados que carecían de la autenticación adecuada, exponiendo datos confidenciales de clientes.[24] Estos incidentes ponen de manifiesto la necesidad de reforzar la gestión de riesgos de terceros, la supervisión continua y los modelos de seguridad de confianza cero para mitigar las amenazas en cascada.

La mayoría de los ataques siguieron un patrón similar: compromiso inicial a través de phishing o sistemas vulnerables, movimiento lateral a través de redes, exfiltración de datos y, a menudo, despliegue de ransomware. El impacto financiero de estos incidentes es sustancial, con pérdidas que superan el 1% del PIB de algunos países y que pueden llegar al 6% si el objetivo son infraestructuras críticas.[25] Una pérdida del 1% del PIB debido a la ciberdelincuencia equivale a 25.000 millones de USD para Brasil, 15.000 millones de USD para México y 6.100 millones de USD para Argentina, mientras que una pérdida del 6% podría alcanzar los 150.000 millones de USD, 90.000 millones de USD y 36.600 millones de USD, respectivamente. Economías más pequeñas como Chile (entre 3.900

[16] https://www.cnn.com/business/live-news/us-cyberattacks-cybersecurity-06-08-21/index.html
[17] https://latinlawyer.com/guide/the-guide-corporate-compliance/fifth-edition/article/mitigating risk-data-breaches-and-cyber-incidents-surge-in-latin america#:~:text=Globally%2C%20the%20average%20cost%20of,regions%20included%20in%2 0the%20report.
[18] https://latinlawyer.com/guide/the-guide-corporate-compliance/fifth-edition/article/mitigating risk-data-breaches-and-cyber-incidents-surge-in-latin america#:~:text=Globally%2C%20the%20average%20cost%20of,regions%20included%20in%2 0the%20report
[19] https://www.americaeconomia.com/en/business-industries/cybersecurity-new-center-concern latin-american-companies
[20] https://www.trendmicro.com/en_us/research/18/f/new-killdisk-variant-hits-latin-american-financial-organizations-again.html
[21] https://www.zdnet.com/article/north-korea-s-apt38-hacking-group-behind-bank-heists-of-over-100-million/
[22] https://cybernews.com/security/bankingly-dataleak/#:~:text=On%20May%2024th%2C%20the,anyone%20online.&text=identified%20seven%20Azure%20 Blob,anyone%20online.&text=authentication.%20The%20misconfiguration%20exposed,anyone%20online.&text=of%20ne arly%20135%2C000%20 clients,anyone%20online
[23] https://unit42.paloaltonetworks.com/threat-brief-moveit-cve-2023-34362/
[24] https://cybernews.com/security/bankingly-dataleak/#:~:text=On%20May%2024th%2C%20the,anyone%20online.&text=identified%20seven%20Azure%20 Blob,a nyone%20online.&text=authentication.%20The%20misconfiguration%20exposed,anyone%20online.&text=of%20nearly%20135%2C000%20 clients,anyone%20online
[25] https://latam.cs4ca.com/wp-content/uploads/2024-Annual-Report-The-State-of-OT-Cyber-Security-in-LATAM.pdf

y 23.500 millones de dólares) y Colombia (entre 3.200 y 19.300 millones de dólares) también se enfrentan a grandes riesgos.[26] Con Brasil, México y Argentina entre los más afectados, los ciberataques amenazan la continuidad de las empresas, la confianza de los inversores y la estabilidad económica a largo plazo en toda la región. La magnitud del daño económico potencial subraya la urgente necesidad de reforzar las medidas de ciberseguridad, especialmente en la gestión de riesgos de terceros y la protección de infraestructuras críticas en el sector financiero de América Latina.

2.2.2 Análisis de patrones de vulnerabilidad

Esta sección analiza las vulnerabilidades técnicas prevalentes, las debilidades específicas de la industria en el sector financiero y los retos regionales de seguridad, proporcionando a las organizaciones una visión de los patrones de riesgo comunes. Al comprender estas vulnerabilidades, las empresas pueden identificar lagunas en su postura de seguridad e implementar defensas proactivas. Las conclusiones de esta sección pretenden ayudar a las organizaciones a reconocer los patrones de vulnerabilidad recurrentes, comprender su impacto potencial en el negocio y tomar medidas preventivas para mitigar los riesgos antes de que se conviertan en incidentes de seguridad. La sección 6: Recomendaciones estratégicas, al final de este documento, ofrece soluciones prácticas para abordar estas vulnerabilidades con eficacia.

Vulnerabilidades técnicas comúnmente observadas:

- Segmentación débil de la red.
- Controles de acceso interno insuficientes.
- Protocolos inadecuados de respuesta a incidentes.
- Susceptibilidad de los empleados a la ingeniería social.
- Dependencia excesiva de los sistemas heredados.
- Seguridad de terceros deficiente.
- Supervisión limitada de las transacciones internas.

Patrones y vulnerabilidades específicos del sector (Finanzas):

- Segmentación inadecuada de la red entre sistemas críticos.
- Débiles controles de acceso en las redes internas.
- Autenticación insuficiente en los sistemas de terceros proveedores de servicios.
- Infraestructura vulnerable de cara al público.
- Troyanos bancarios sofisticados que utilizan autoridades legítimas para engañar a los usuarios.

Patrones y vulnerabilidades específicos de cada región:

- Fuerte dependencia de la ingeniería social dirigida a la confianza regional en las autoridades financieras.
- Sofisticadas campañas de phishing que explotan preocupaciones relacionadas con los impuestos
- Naturaleza transfronteriza de las operaciones bancarias que crea inconsistencias de seguridad.
- Adopción generalizada de la banca digital en las zonas rurales a través de canales potencialmente vulnerables.
- Los sistemas centralizados de procesamiento de pagos (como el SPEI de Brasil) se convierten en objetivos de gran valor.[27]

2.2.3 Análisis de brechas e impacto futuro

Esta sección examina las principales brechas de ciberseguridad en América Latina, centrándose en sus causas fundamentales, las mejoras recientes y los riesgos futuros previstos. El análisis pone de relieve problemas sistémicos, como la falta de inversión, las infraestructuras obsoletas y la colaboración insuficiente, que contribuyen a la persistencia de los problemas de seguridad. Mediante la revisión de incidentes pasados y su impacto en las instituciones financieras, las organizaciones pueden comprender mejor la evolución de las amenazas. Además, esta sección explora los riesgos emergentes de los ciberataques impulsados por la IA, las vulnerabilidades de la cadena de suministro y los riesgos geopolíticos. La sección 6: Recomendaciones estratégicas, al final de este documento, proporciona soluciones concretas para abordar estas vulnerabilidades y fortalecer la resiliencia de la ciberseguridad regional.

Análisis de las causas de origen:

1. Subinversión crónica en ciberseguridad: América Latina se enfrenta a importantes vulnerabilidades de ciberseguridad debido a la falta de inversión.[28] Según la Organización de Estados Americanos (OEA), los países latinoamericanos destinan menos del 1% del PIB a infraestructuras de ciberseguridad,[29] lo que deja a los sistemas financieros vulnerables a ataques avanzados. La región tiene la puntuación media de ciberseguridad más baja a nivel mundial, con un 10,2 sobre 20.[30]

2. Colaboración transfronteriza insuficiente: Existe una falta de armonización entre las legislaciones nacionales, lo que crea desafíos para las empresas multinacionales.[31] Sin embargo, esfuerzos recientes, como la Alianza Digital UE-ALC, pretenden reforzar las asociaciones birregionales.[32]

[26] https://www.statista.com/statistics/802640/gross-domestic-product-gdp-latin-america-caribbeancountry/#:~:text=In%202024%2C%20Brazil%20and,and%20the&text=were%20expected%20to%20be,and%20the&text=countries%20with%20the%20largest,and% 20the&text=domestic%20product%20%28GDP%29%20in,and%20the
[27] https://www.wired.com/story/mexico-bank-hack/
[28] https://www.centerforcybersecuritypolicy.org/insights-and-research/insights-from-the-annual-latam-ciso-summit-costa-rica
[29] https://grcoutlook.com/cybersecurity-risks-latin-america-versus-asia-a-rising-concern/
[30] https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe
[31] https://www.wired.com/story/mexico-bank-hack/
[32] https://www.eeas.europa.eu/eeas/europe-and-latin-america-caribbean-step-cooperation-cybersecurity_en

3. Infraestructura y software obsoletos: Muchas empresas aún operan con sistemas anticuados o utilizan software pirata, lo que deja brechas que los atacantes pueden explotar fácilmente.[33]

4. Déficit de recursos en ciberseguridad: Hay una necesidad urgente de actualizar las técnicas de los equipos actuales y fomentar la próxima generación de profesionales de la ciberseguridad.[34]

5. Legislación y aplicación inadecuadas: Las leyes de ciberseguridad de algunos países están obsoletas o se aplican de forma deficiente. Sólo tres de los 21 países de América Latina cuentan con una estrategia nacional de seguridad digital definida.[35]

6. Falta de concienciación pública: Muchos países latinoamericanos aún no han difundido ampliamente los peligros de Internet. Faltan programas preventivos a pesar de que algunos países han adoptado estrategias cibernéticas nacionales.[36]

2.2.4 Mejoras en la postura de seguridad desde 2018 hasta la actualidad

La postura de seguridad de las instituciones financieras latinoamericanas se ha transformado significativamente entre 2018 y 2024. En 2018, como lo demuestra el ataque al Banco de Chile, las instituciones financieras se basaron principalmente en medidas de seguridad reactivas, como la desconexión del sistema, la investigación forense después de la brecha y la restauración a partir de copias de seguridad. El banco no fue consciente del malware en sus sistemas hasta que se enfrentó a la alerta KillMBR, que provocó una desconexión generalizada del sistema. En comparación con las mejores prácticas, como la detección proactiva de amenazas, la segmentación de la red y la supervisión en tiempo real, la respuesta al incidente del banco carecía de una identificación temprana de la amenaza, una contención precisa y controles de seguridad para evitar pérdidas financieras.[37]

El caso del sistema SPEI de México en 2018 destacó aún más la débil segmentación de red prevalente y las limitadas capacidades de monitoreo de la época. El atraco expuso graves vulnerabilidades en el Sistema de Pagos Electrónicos Interbancarios (SPEI), con hackers identificados como parte del grupo APT38, un grupo de actores de amenazas con motivaciones financieras que se cree que está respaldado por Corea del Norte.[38] APT38 se infiltró en las redes bancarias, comprometió los puntos finales que gestionaban las transacciones SPEI e inyectó solicitudes de pago fraudulentas. Aprovechando la escasa seguridad de la red, que incluía una segmentación y unos controles de acceso deficientes, pudieron alterar las instrucciones de transferencia sin activar alarmas inmediatas, robando en última instancia entre 15 y 20 millones de dólares y trasladando los fondos a cuentas de mulas antes de blanquearlos internacionalmente.[39]

A partir de 2024, el panorama de la seguridad de las instituciones financieras latinoamericanas ha avanzado significativamente, con organizaciones que adoptan protocolos de respuesta a incidentes más estructurados y mejoran la coordinación a través de equipos CERT nacionales. Un ejemplo notable es la rápida contención del ataque del ransomware Black Basta por parte de la Aduana chilena, lo que demuestra una mayor capacidad de respuesta y colaboración.[40] Sin embargo, a pesar de estos avances, las instituciones financieras siguen lidiando con un panorama de amenazas en evolución impulsado por la rápida digitalización, el aumento de la interconectividad y las vulnerabilidades emergentes en SaaS de terceros y las integraciones de software.

Un buen ejemplo es la violación de 2024 Bankingly, que afectó a 135.000 clientes en varios países de LATAM, exponiendo datos críticos debido a errores de configuración en Azure Blob Storage.[41] La filtración fue rastreada hasta buckets Azure Blob Storage mal configurados utilizados por Bankingly para almacenar datos de clientes. Estos errores de configuración dejaron los datos expuestos a accesos no autorizados, poniendo de manifiesto vulnerabilidades significativas en las integraciones de terceros y en las configuraciones de servicios en la nube.[42]

Del mismo modo, la fuga de datos del Banco Português de Gestão, causada por un error de configuración en los sistemas de Nearsoft, expuso datos financieros de clientes muy sensibles debido a la falta de controles de autenticación. Resulta alarmante que Nearsoft no cumpliera normas de seguridad fundamentales como la ISO 27001 y la PCI DSS, dejando los datos sin cifrar y vulnerables a accesos no autorizados.[43] Estos incidentes ponen de manifiesto la persistencia de brechas de

[33] https://www.datto.com/blog/ransomware-and-cybersecurity-in-latin-america/
[34] https://www.centerforcybersecuritypolicy.org/insights-and-research/insights-from-the-annual-latam-ciso-summit-costa-rica
[35] https://www.wired.com/story/mexico-bank-hack/
[36] https://latam.cs4ca.com/wp-content/uploads/2024-Annual-Report-The-State-of-OT-Cyber-Security-in-LATAM.pdf
[37] https://www.infosecurity-magazine.com/news/bank-of-chile-suffers-10m-loss/
[38] https://attack.mitre.org/groups/G0082/
[39] https://latam.cs4ca.com/wp-content/uploads/2024-Annual-Report-The-State-of-OT-Cyber-Security-in-LATAM.pdf
[40] https://therecord.media/chile-black-basta-ransomware-attack-customs-department
[41] https://cybernews.com/security/bankingly-dataleak/#:~:text=On%20May%2024th%2C%20the,anyone%20online.&text=identified%20seven%20Azure%20Blob,anyone%20online.&text=authentication.%20The%20misconfiguration%20exposed,anyone%20online.&text=of%20ne arly%20135%2C000%20clients,anyone%20online
[42] https://cybernews.com/security/bankingly-dataleak/#:~:text=On%20May%2024th%2C%20the,anyone%20online.&text=identified%20seven%20Azure%20Blob,anyone%20online.&text=authentication.%20The%20misconfiguration%20exposed,anyone%20online.&text=of%20ne arly%20135%2C000%20clients,anyone%20online
[43] https://cybernews.com/security/banco-portugues-de-gestao-data-leak/

seguridad derivadas de una gestión de riesgos deficiente, una configuración incorrecta de la nube y una supervisión inadecuada de los proveedores. Como tales, ponen de relieve los riesgos asociados a la infraestructura digital moderna. Aunque las instituciones financieras han reforzado sus defensas, estos incidentes revelan que los errores de configuración de la seguridad y la supervisión insuficiente siguen siendo puntos débiles clave. Subsanar estas deficiencias será esencial para mitigar futuros riesgos y mantener una postura de seguridad sólida en un ecosistema financiero cada vez más digital.

2.2.5 Análisis del impacto futuro

1. Ciberataques impulsados por IA: Los actores de amenazas están aprovechando cada vez más la IA para crear malware destructivo, sofisticadas campañas de phishing, falsificaciones profundas convincentes y operaciones avanzadas de ciberespionaje que explotan las vulnerabilidades de la infraestructura.[44] El principal reto a la hora de hacer frente a estos sofisticados ataques es la grave escasez de profesionales con conocimientos especializados para comprender y diseñar marcos adecuados de gestión de riesgos. El éxito depende de la creación de competencias técnicas para evaluar y mitigar eficazmente estas sofisticadas amenazas emergentes mediante una gobernanza y unos controles adecuados.

2. Explotación de las vulnerabilidades de la transformación digital: A medida que los países latinoamericanos promueven una mayor digitalización para fomentar el crecimiento socioeconómico, se vuelven más vulnerables a los ciberdelincuentes. El mayor uso de la tecnología también aumenta el potencial de ataques.[45]

3. Vulnerabilidades de la cadena de suministro: En particular, el 54% de las grandes organizaciones identificaron los desafíos de la cadena de suministro como la mayor barrera para lograr la resiliencia cibernética. La creciente complejidad de las cadenas de suministro, junto con la falta de visibilidad de los niveles de seguridad de los proveedores, se ha convertido en uno de los principales riesgos de ciberseguridad.[46]

4. Influencias geopolíticas: Las tensiones geopolíticas están contribuyendo a un entorno de ciberseguridad más incierto. Por ejemplo, el 97% de las organizaciones vieron un aumento de las amenazas cibernéticas desde el inicio de la guerra entre Rusia y Ucrania en 2022, lo que demuestra el profundo efecto de las tensiones geopolíticas en la ciberseguridad.[47]

5. Disparidades regionales: Se prevé que América Latina experimente un mayor aumento de los ciberataques que otras regiones. En el segundo trimestre de 2024, los ciberataques aumentaron un 53% interanual en América Latina, y es probable que esta tendencia continúe.[48]

2.3 Pérdidas por ransomware para la industria de servicios financieros

A partir de 2024, la industria de servicios financieros en LATAM se ha convertido en el objetivo principal de los ataques de ransomware, lo que refleja una tendencia más amplia de escalada de las amenazas cibernéticas en la región. Brasil, México y Chile han sido los países más afectados, con grupos de ransomware como LockBit 3.0, Akira y Play identificados como los actores detrás de los ataques. Estos grupos utilizan métodos sofisticados, como la explotación de vulnerabilidades en el software y el despliegue de modelos de ransomware como servicio (RaaS). Se estima que las pérdidas financieras atribuidas a incidentes de ransomware en el sector financiero de LATAM superarán los cientos de millones de dólares en 2024, ya que las organizaciones enfrentan costos relacionados con el pago de rescates, la recuperación de datos, el tiempo de inactividad operativa y el daño a la reputación. Este aumento de los ataques subraya la necesidad crítica de medidas sólidas de ciberseguridad en las instituciones financieras de la región.

2.3.1 Caso práctico 1 - Ataque dirigido de LockBit 3.0 contra un banco brasileño

En julio de 2024, el grupo de ransomware LockBit 3.0 llevó a cabo un ataque muy dirigido contra una importante institución financiera brasileña. Los atacantes aprovecharon una vulnerabilidad en la infraestructura de escritorio virtual del banco para obtener acceso no autorizado y cifrar archivos operativos críticos. Para presionar aún más a la víctima, LockBit 3.0 amenazó con publicar los datos confidenciales robados en foros de la dark-web a menos que la institución accediera a su petición de rescate de 2,5 millones de dólares en Bitcoin.

El ataque provocó importantes daños operativos y financieros. El banco sufrió una prolongada inactividad de los servicios bancarios en línea, lo que interrumpió las transacciones de los clientes y el acceso a sus cuentas. Esto no sólo erosionó la confianza de los clientes, sino que también sometió a la institución a un escrutinio reglamentario. Además, los costos financieros fueron más allá de la petición de rescate e incluyeron gastos de recuperación del sistema, investigaciones forenses y esfuerzos de relaciones públicas para restaurar su reputación.

[44] https://insightcrime.org/news/four-ways-ai-is-shaping-organized-crime-in-latin-america/
[45] https://grcoutlook.com/cybersecurity-risks-latin-america-versus-asia-a-rising-concern/
[46] https://www.weforum.org/publications/global-cybersecurity-outlook-2025/digest/
[47] https://www.accenture.com/content/dam/accenture/final/accenture-com/document/Accenture-State-Cybersecurity.pdf
[48] https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/

2.3.2 Caso práctico 2 - Ataque ransomware de Play a una empresa financiera chilena

También en julio de 2024, el grupo de ransomware Play atacó una empresa financiera chilena desplegando una variante de Linux diseñada específicamente para explotar entornos VMware ESXi. Los atacantes se infiltraron en la infraestructura virtualizada de la empresa, cifraron datos críticos de los servidores y dejaron una nota de rescate exigiendo 1,8 millones de dólares en criptomoneda.

El ataque causó amplias repercusiones financieras y operativas a la empresa. Además de la petición de rescate, la organización incurrió en gastos relacionados con la restauración de sus sistemas informáticos y el refuerzo de sus defensas de ciberseguridad. El incidente también causó daños a la reputación, ya que clientes y socios expresaron su preocupación por la capacidad de la empresa para proteger datos confidenciales. Estas pérdidas acumuladas subrayaron aún más la creciente amenaza del ransomware para el sector de servicios financieros de LATAM.

En conclusión, el ransomware sigue siendo una amenaza apremiante y creciente para la industria de servicios financieros en LATAM, con países como Brasil, Chile y México emergiendo como objetivos principales en 2024. Grupos de ransomware como LockBit 3.0 y Play han demostrado una creciente sofisticación explotando vulnerabilidades en infraestructuras virtualizadas y aprovechando modelos RaaS para escalar sus operaciones. Las pérdidas financieras incurridas superan con creces el pago de rescates, abarcando la restauración del sistema, el tiempo de inactividad y el daño a la reputación, ascendiendo colectivamente a cientos de millones de dólares en toda la región. A medida que el sector financiero en LATAM continúa digitalizándose, las organizaciones deben priorizar estrategias integrales de ciberseguridad, incluyendo la gestión de vulnerabilidades, la capacitación de los empleados y los sistemas avanzados de detección de amenazas, para mitigar el impacto de estos ataques generalizados. La resiliencia del sector de servicios financieros depende de medidas proactivas para contrarrestar las tácticas cambiantes de los operadores de ransomware.

2.4 Capacidades de respuesta al ransomware

La creciente tendencia de ataques de ransomware en LATAM ha expuesto brechas críticas en las capacidades regionales de respuesta que crean vulnerabilidades inmediatas para el sector de servicios financieros. Esta sección examina cómo los marcos institucionales, las capacidades técnicas y los mecanismos de coordinación en LATAM contribuyen a una elevada exposición al riesgo de ransomware para las instituciones financieras.

2.4.1 Evaluación de la infraestructura de respuesta regional

Datos comparativos recientes, incluido el Informe Global sobre Ransomware de Fortinet, revelan matices importantes en las capacidades de respuesta de LATAM en relación con otras regiones.[49] [50] [51] Mientras que las organizaciones latinoamericanas demuestran capacidades más fuertes en detección rápida de ataques y resistencia a la ingeniería social[52], esta fortaleza relativa en capacidades de detección debe ser contextualizada dentro de las limitaciones más amplias de la infraestructura regional. Es decir, los datos sugieren que mientras que las capacidades individuales de las empresas pueden estar desarrollándose, persisten las lagunas en la infraestructura de respuesta sistémica. El panorama desigual de divulgación y el número limitado de países de LATAM con planes establecidos para la protección de infraestructuras críticas (por no hablar del sector de servicios financieros) es una prueba de esta carencia.

Un estudio de 2022 introduce un índice exhaustivo de divulgación de la ciberseguridad que examina las prácticas en los principales mercados de LATAM entre 2016 y 2020 en una escala de 0 a 1. La investigación desarrolló un marco de 27 elementos en cuatro dimensiones: gobernanza (5 elementos), estrategia (6 elementos), gestión de riesgos (13 elementos) e implicaciones financieras (3 elementos). Estas dimensiones se basaron en normas internacionales, como la ISO 27000, las directrices de la SEC, el GDPR y los marcos de la OCDE, el BID, la OEA y la GRI.[53]

La investigación revela un panorama complejo de divulgación de ciberseguridad en el sector financiero de LATAM, con las instituciones financieras manteniendo los niveles de divulgación más altos en todos los sectores, aumentando de 0,28 en 2016 a 0,52 en 2020.[54] Esta posición de liderazgo es particularmente evidente en Argentina, donde las instituciones financieras comprenden el 57% de las empresas de la muestra, con el 86% presentando informes del Formulario 20-F de la SEC.[55] Sin embargo, a pesar de esta madurez relativa, persisten importantes lagunas en la divulgación de la gobernanza. Mientras que la participación del consejo en la supervisión de la ciberseguridad mejoró de 0,18 en 2016 a 0,53 en 2020, la divulgación de los comités especializados se mantuvo débil en 0,24 en 2020, y la divulgación de la supervisión de los comités de auditoría obtuvo solo 0,20.[56]

[49] https://www.fortinet.com
[50] https://doi.org/10.1145/3429741
[51] https://doi.org/10.3390/su14031390
[52] https://www.fortinet.com
[53] https://doi.org/10.3390/su14031390
[54] https://doi.org/10.3390/su14031390
[55] https://doi.org/10.3390/su14031390
[56] https://doi.org/10.3390/su14031390

La carencia de gobernanza es especialmente preocupante dada la evolución del malware financiero que explota contextos regionales e institucionales, como implementaciones bancarias específicas. Al realizar un estudio longitudinal del malware financiero brasileño entre 2012 y 2020, los investigadores revelaron cómo las tácticas maliciosas evolucionan rápidamente en función de las nuevas oportunidades de ataque. Por ejemplo, los actores de amenazas están adaptando la ingeniería social y los scripts de malware a contextos bancarios locales que divergen de las tendencias globales o históricas (por ejemplo, malware dirigido a tarjetas de crédito con PIN, código VBE en portugués brasileño).[57] El ransomware no es una excepción a estas tácticas en evolución. Por lo tanto, es necesario establecer la tolerancia al riesgo al más alto nivel a través de la gobernanza de la ciberseguridad a nivel directivo para garantizar que las contramedidas locales sean conscientes del contexto (es decir, atentas a las características geográficas y empresariales).

Otras preocupaciones incluyen los resultados relativos a la divulgación de la gestión de riesgos (0,40 en 2020); la alineación con las normas internacionales de seguridad (0,39 en 2020); y la divulgación continua de la inversión en ciberseguridad, mejorando solo de 0,02 en 2016 a 0,21 en 2020.[58] Estas puntuaciones sugieren que, si bien las instituciones financieras pueden tener marcos de seguridad establecidos, luchan por comunicar eficazmente sus inversiones en seguridad y su alineación con las normas internacionales. La investigación identifica correlaciones claras entre los marcos regulatorios y la calidad de la divulgación, con los primeros en adoptar leyes de protección de datos y estrategias nacionales de ciberseguridad, como Argentina (2016) y Brasil (2018), mostrando divulgaciones más sólidas del sector financiero que países como Perú, donde las puntuaciones de divulgación más bajas (0,25 en 2020) se correlacionan con la ausencia de una estrategia nacional.[59]

Las tendencias sugieren un patrón más amplio: mientras que las instituciones financieras de LATAM lideran en divulgación de ciberseguridad en comparación con otros sectores, su desempeño varía significativamente en función de la madurez regulatoria y los marcos nacionales de ciberseguridad. El papel crítico del sector en la infraestructura nacional y las redes financieras internacionales hace que estas deficiencias sean particularmente preocupantes, lo que sugiere la necesidad de prácticas de divulgación más estandarizadas y una mejor alineación con las normas internacionales en toda la región.

La naturaleza exhaustiva de los resultados de la investigación indica implicaciones significativas para las capacidades de respuesta ante incidentes de ransomware en las instituciones financieras de LATAM. La disparidad entre las puntuaciones de divulgación estratégica (0,53) y las puntuaciones de gestión de riesgos operativos (0,40) sugiere vulnerabilidades potenciales en la ejecución real de la respuesta ante incidentes.[60] Especialmente preocupantes son las bajas puntuaciones obtenidas en la divulgación de los procedimientos de respuesta ante incidentes (0,36) y en la eficacia de la supervisión (0,47). Estas puntuaciones indican posibles lagunas en las capacidades operativas de respuesta que podrían afectar directamente a la capacidad de una institución para detectar, contener y recuperarse de los ataques de ransomware.[61] Cuando se combinan con los hallazgos previamente discutidos sobre las prácticas de divulgación y los marcos regulatorios, estas brechas sugieren que, mientras que las instituciones financieras de LATAM pueden tener planes básicos de respuesta al ransomware, su preparación operativa real para ataques complejos puede ser insuficiente.

Esta suposición tiene fundamento. El Banco Interamericano de Desarrollo informa de que sólo siete de los 32 países latinoamericanos han establecido planes para la protección de infraestructuras críticas, mientras que sólo 20 cuentan con CSIRT operativos.[62] Este panorama de respuesta fragmentada ha creado retos específicos para las instituciones financieras que operan a través de las fronteras. Por ejemplo, esta brecha fue particularmente aguda durante el incidente de ransomware de septiembre de 2023 en Colombia, donde el radio de explosión se extendió a entidades financieras en Argentina, Panamá y Chile debido a los limitados mecanismos de coordinación.[63]

2.4.2 Capacidades de respuesta técnica y limitaciones de recursos

Aunque las organizaciones de LATAM demuestran una mayor capacidad de detección inicial, existen variaciones regionales significativas en la preparación técnica que crean vulnerabilidades. Por ejemplo, la emergencia del ransomware Costa Rica 2022 revela cómo las ventajas relativas de la detección pueden verse socavadas por las limitaciones posteriores de la respuesta. Incluso después de la detección, el gobierno costarricense gastó aproximadamente 24 millones de dólares en operaciones de respuesta, y sólo la fase de rehabilitación costó a la Caja de la Seguridad Social más de 18 millones de dólares.[64] Esta escala de impacto sugiere que el ciclo completo de respuesta se enfrenta a importantes limitaciones. Una de ellas son las disparidades intersectoriales en la preparación técnica.

[57] https://doi.org/10.1145/3429741
[58] https://doi.org/10.3390/su14031390
[59] https://doi.org/10.3390/su14031390
[60] https://doi.org/10.3390/su14031390
[61] https://doi.org/10.3390/su14031390
[62] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[63] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[64] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf

Basándose en datos empíricos para 2020, los patrones de divulgación de la ciberseguridad de las instituciones financieras de LATAM indican que las inversiones están muy orientadas hacia iniciativas estratégicas como los sistemas de gestión de la seguridad (con una puntuación de 0,68) y los programas de concienciación (con una puntuación de 0,72). Los elementos operativos críticos, como los procedimientos de respuesta ante incidentes, sólo obtuvieron una puntuación de 0,36, y las actividades de prueba y supervisión sólo alcanzaron el 0,47.[65] Un modelo de buenas prácticas demostraría una inversión y madurez equilibradas en los ámbitos estratégico y operativo. Por ejemplo, en lugar de limitarse a informar de la adopción generalizada de sistemas de gestión de la seguridad, las instituciones deberían demostrar inversiones concertadas en capacidades de detección y respuesta ante incidentes, pruebas de penetración y evaluaciones de vulnerabilidad periódicas, y parámetros cuantificables de la eficacia de los programas de seguridad. La divulgación debe mostrar que las inversiones en seguridad se distribuyen a través de áreas operativas críticas, incluyendo la infraestructura de detección y respuesta, pruebas y monitorización continuas, y capacidades de inteligencia de amenazas y defensa proactiva. Esto reflejaría un programa de seguridad centrado en la reducción de riesgos tangibles y no sólo en el cumplimiento de las políticas, con parámetros claros que demuestren el impacto operativo de las inversiones en seguridad.

Esta disparidad entre estrategia y aplicación también es evidente en los patrones de asignación de recursos más allá del sector privado. En comparación con los proveedores de servicios financieros de LATAM, el sector público muestra una aplicación de las mejores prácticas generales de seguridad notablemente inferior a la de las instituciones del sector privado.[66] Esto puede crear vulnerabilidades potenciales en el ecosistema financiero más amplio, donde los sistemas públicos y privados están interconectados.[67]

Además, los problemas documentados en la asignación de recursos podrían afectar a las futuras capacidades de respuesta al ransomware. Mientras que las organizaciones de Norteamérica y Europa, Oriente Medio y África están planeando inversiones más sustanciales en herramientas de acceso a la red de confianza cero (ZTNA), las organizaciones de LATAM informan de planes de inversión en seguridad más limitados.[68] Como medida proactiva y reactiva de respuesta a incidentes, las herramientas ZTNA pueden microsegmentar las redes empresariales para contener el ransomware, evitando el movimiento lateral, la filtración de datos y el acceso no autorizado a servicios críticos a través de controles de denegación de acceso de grano fino. Por lo tanto, este déficit de inversión podría agravar las limitaciones existentes en la infraestructura de respuesta, especialmente para las instituciones financieras que operan en distintas regiones y que deben mantener la paridad con las normas de seguridad mundiales al tiempo que interactúan con los sistemas de los sectores público y privado.

Como banco multinacional, el Santander es un buen ejemplo de esta complejidad. Las operaciones del Santander en los mercados de LATAM, la UE y EE.UU. ilustran la compleja interacción entre las divulgaciones voluntarias y obligatorias en materia de ciberseguridad. En Brasil, donde el Índice Global de Ciberseguridad muestra la puntuación de desarrollo regional más alta (97,68) y las medidas legales más estrictas (20,0), el Santander debe navegar tanto por las estrictas regulaciones locales como por los requisitos obligatorios de información del Formulario 20-F de la SEC.[69] Esto contrasta con sus operaciones en Argentina, donde la puntuación de ciberseguridad-madurez es significativamente más baja (50,12), aunque el banco sigue manteniendo obligaciones de información a la SEC junto con marcos de divulgación locales menos desarrollados.[70]

Esta disparidad afecta a la mitigación de amenazas y a la respuesta ante incidentes, en particular a la coordinación de la inteligencia sobre amenazas y la respuesta con entidades públicas u operadores de servicios críticos. En Brasil, los informes del Santander reflejan los sólidos acuerdos de cooperación bilateral y multilateral del país (puntuación de 19,41 en medidas de cooperación), lo que permite compartir información sobre amenazas y coordinar incidentes de forma más eficaz.[71] Sin embargo, en Argentina, aunque los requisitos del formulario 20-F de la SEC garantizan la presentación de informes básicos sobre riesgos cibernéticos, la puntuación más baja en madurez de la ciberseguridad nacional sugiere posibles lagunas en la coordinación local de la respuesta a las amenazas.

Las operaciones europeas del banco se enfrentan a una complejidad adicional a través de los requisitos de cumplimiento del GDPR, que han influido en las prácticas de divulgación de LATAM a través de lo que los investigadores identifican como la “adaptación del modelo europeo de regulaciones relacionadas con la privacidad de los datos”.[72]Esto crea una dinámica interesante en la que las operaciones de Santander en LATAM a menudo se benefician de las normas más estrictas de la UE, especialmente en países como Brasil, que han modelado sus leyes de protección de datos

[65] https://doi.org/10.3390/su14031390
[66] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[67] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[68] https://www.fortinet.com
[69] https://doi.org/10.3390/su14031390
[70] https://doi.org/10.3390/su14031390
[71] https://doi.org/10.3390/su14031390
[72] https://doi.org/10.3390/su14031390

según los marcos europeos. La investigación muestra que esta influencia reguladora ha generado un aumento de las normas y de la difusión de información sobre ciberseguridad en toda la región, aunque su aplicación varía significativamente de un país a otro.[73]

Esta realidad multijurisdiccional obliga al Santander a mantener el máximo común denominador en las prácticas de seguridad, adaptando al mismo tiempo los enfoques de divulgación para cumplir los distintos requisitos regionales, desde el cumplimiento del formulario 20-F de la SEC hasta las normas GDPR de la UE o los marcos normativos locales. Si bien la postura de seguridad general de las instituciones podría beneficiarse teóricamente del cumplimiento del máximo común denominador de los requisitos de seguridad en todas las jurisdicciones, la implementación práctica a nivel local presenta desafíos considerables.

Los distintos entornos institucionales de los países de LATAM crean lagunas operativas en la implementación de la seguridad. Por ejemplo, mientras que las operaciones brasileñas del Santander se benefician de marcos nacionales sólidos y de una infraestructura de seguridad madura, sus sucursales en los países vecinos pueden tener dificultades para mantener capacidades equivalentes debido a las limitaciones de recursos y a ecosistemas de seguridad locales menos desarrollados. Estas disparidades se manifiestan en varias áreas críticas: disponibilidad de capital humano para operaciones de seguridad, capacidades avanzadas de detección y registro, y coordinación de respuesta a incidente.

Cuando las organizaciones se limitan a cumplir las normas mínimas en regiones con marcos menos maduros, corren el riesgo de crear vulnerabilidades de seguridad que podrían afectar a su red operativa más amplia. Estas disparidades resultan especialmente problemáticas en la seguridad de la cadena de suministro, donde las sucursales específicas de un país que operan con distintos niveles de madurez en materia de seguridad pueden crear puntos de entrada vulnerables a la red institucional más amplia. Además, cuando las instituciones deben mejorar las operaciones locales para cumplir normas de seguridad más estrictas —ya sea por los requisitos del formulario 20-F de la SEC o por el cumplimiento del GDPR europeo— pueden encontrarse con que los recursos locales son insuficientes para apoyar la transición. Esta limitación de recursos es especialmente grave en los mercados en los que tanto el capital humano como la infraestructura técnica para la ciberseguridad están por detrás de las normas internacionales.

2.4.3 Coordinación de la respuesta transfronteriza

La naturaleza interconectada de los sistemas financieros de LATAM amplifica el riesgo de deficiencias de coordinación en la respuesta transfronteriza. Aunque existen algunos acuerdos bilaterales, como entre Costa Rica y Panamá, los marcos de respuesta regional global siguen siendo limitados.[74] Además, la relativa ventaja de LATAM en la detección temprana puede no traducirse en una gestión eficaz de incidentes transfronterizos.[75] El ataque de septiembre de 2023 al proveedor de servicios de Internet de Colombia, IFX Networks, demuestra esta vulnerabilidad, donde a pesar de la detección paciente-cero, el ataque aún se propagó a 78 entidades públicas adicionales y 762 empresas privadas a través de múltiples países.[76] Aunque este radio de alcance puede atribuirse a muchos factores, incluidas las capacidades de detección y corrección, demuestra principalmente una falta generalizada de procedimientos de compromiso de terceros. Exacerbada por la incapacidad del gobierno para determinar y revelar el alcance de las entidades afectadas, las organizaciones fueron incapaces de cortar o aislar las conexiones comprometidas como parte de sus cadenas de suministro.[77]

2.4.4 Mecanismos de intercambio de información y su impacto en la vulnerabilidad del sector financiero

Las limitaciones significativas en los mecanismos regionales de intercambio de información pueden obstaculizar los esfuerzos de respuesta al ransomware de las instituciones financieras. Durante el ataque de ransomware de 2023 en Colombia, el asesor presidencial para la transformación digital emitió nueve boletines informativos antes de que concluyera el suceso. Sin embargo, la falta de protocolos estandarizados de intercambio intersectorial dio lugar a una distribución desigual de inteligencia sobre amenazas críticas.[78] Este vacío en el intercambio coordinado de información dio lugar a ventanas de vulnerabilidad prolongadas en las que los sistemas financieros interconectados permanecieron expuestos.[79]

2.4.5 Variación en los marcos de coordinación público-privada

Existen importantes lagunas en la coordinación público-privada en la mayoría de los países de LATAM que afectan directamente a la resiliencia del sector financiero.[80] Por ejemplo, mientras que Ecuador cuenta con 14 CSIRT dedicados a ofrecer servicios de respuesta ante incidentes a las empresas, no

[73] https://doi.org/10.3390/su14031390
[74] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[75] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[76] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[77] https://elpais.com/america-colombia/2023- 09-14/el-gobierno-aun-no-sabe-cuantas-entidades-estan-afectadas-por-el-hackeo-a-ifx networks.html
[78] https://therecord.media/colombia government-ministries-cyberattack
[79] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[80] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf

existe ningún CSIRT financiero.[81] Además, aunque estos equipos de respuesta abarcan infraestructuras críticas y ámbitos comerciales como los sectores de las telecomunicaciones y la energía, que podrían abordar algunos intereses coincidentes del sector financiero, no disponen de ningún mecanismo formal para comunicarse entre sí.[82] Como centro financiero regional, Panamá también se enfrenta a retos de coordinación público-privada para garantizar los servicios críticos. A pesar del lanzamiento de la Agenda Digital Nacional, el país está luchando para fortalecer las "plataformas de interoperabilidad sectorial" y estimular la inversión privada en el ecosistema digital.[83]

Sin embargo, también hay ejemplos de coordinación intersectorial exitosa. En Chile, la Ley Marco de Ciberseguridad se aprobó en 2023 para mejorar la rendición de cuentas sobre el control de la seguridad y las capacidades de respuesta ante incidentes para los proveedores de servicios esenciales. La ley creó CSIRT específicos del sector y la Agencia Nacional de Ciberseguridad (ANCI), que define las normas para los proveedores de servicios esenciales (por ejemplo, servicios financieros) y emite multas por incumplimiento de las normas nacionales de ciberseguridad.[84]

Las organizaciones privadas también han asumido un papel cada vez más central en el desarrollo y la aplicación de medidas de ciberseguridad, con la aparición de organismos especializados para abordar los retos específicos de cada sector. Un ejemplo notable es la Alianza Chilena de Ciberseguridad, formada mediante la colaboración de nueve importantes instituciones que abarcan sectores críticos, incluidos socios del sector financiero.[85] Esta alianza ejemplifica cómo las asociaciones de múltiples partes interesadas entre la industria privada, los organismos gubernamentales y las instituciones académicas pueden crear un sólido intercambio de información intersectorial durante los incidentes de ciberseguridad. El desarrollo de institutos especializados, como el Instituto Nacional de Ciberseguridad de Chile, refuerza aún más este ecosistema al centrarse en la concienciación sobre la seguridad y la creación de confianza entre las partes interesadas, tanto individuales como empresariales.[86] El aumento de las asociaciones comerciales centradas en la tecnología, como Chiletec, que cuenta con más de 100 empresas tecnológicas chilenas, proporciona una infraestructura adicional para coordinar los esfuerzos en materia de ciberseguridad.[87]

La integración de la coordinación público-privada de la ciberseguridad en Colombia demuestra un enfoque sofisticado de la resiliencia del sector financiero, particularmente a través de la colaboración entre entidades gubernamentales (ColCERT, CCOC, MINTIC) e iniciativas del sector privado como el CSIRT de Asobancaria.[88] Esta asociación ejemplifica cómo los marcos regulatorios pueden fusionarse eficazmente con las capacidades operativas lideradas por la industria para crear mecanismos de defensa contundentes.

El impacto operativo de esta coordinación es especialmente notable en el sector financiero. Según datos recientes, el sistema financiero colombiano ha demostrado una notable resistencia: de los casi 20.000 millones de ciberataques del año pasado, sólo dos lograron penetrar.[89] Esta tasa de éxito puede atribuirse al despliegue del CSIRT de Asobancaria, compuesto por 17 expertos en ciberseguridad que han procesado más de 300 eventos de seguridad y gestionado más de 450 alertas tempranas solo a principios de 2024.[90]

La escala de esta colaboración es evidente en la forma en que el CSIRT de Asobancaria funciona como punto focal nacional e internacional para la gestión de crisis y la respuesta a incidentes en el sector financiero. Su centro de operaciones y programa de intercambio de información se ha establecido como uno de los centros de operaciones de ciberseguridad más avanzados de América Latina, sirviendo como modelo de cómo las asociaciones público-privadas pueden mejorar la resiliencia cibernética de todo el sector. Esto es particularmente significativo dada la posición de Colombia como el segundo país más atacado por ciberataques en América Latina. El éxito de este enfoque proporciona información valiosa para otras naciones de LATAM que buscan desarrollar marcos de ciberseguridad público-privados similares, en particular en la protección de la infraestructura financiera crítica.

[81] https://doi.org/10.1007/978-3-030-60467-7_24
[82] https://doi.org/10.1007/978-3-030-60467-7_24
[83] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[84] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[85] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[86] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[87] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[88] https://doi.org/10.25062/9789585216549
[89] https://www.mintic.gov.co/portal/inicio/
[90] https://www.mintic.gov.co/portal/inicio/

3 Tendencias de la industria

3.1 Principales actores de ciberamenazas dirigidas a la industria financiera en América Latina

El desarrollo de programas de ciberseguridad organizacional en América Latina se refleja en la expansión del ransomware como una ciberamenaza significativa. El Índice Nacional de Ciberseguridad (NCSI, por sus siglas en inglés) resaltó el vacío de políticas y regulaciones robustas de ciberseguridad en toda la región LATAM y, más aún, reveló los riesgos y consecuencias de los ataques de ransomware para las instituciones financieras.[91] Según el informe LATAM CISO 2024, en abril de 2022, el Ministerio de Hacienda de Costa Rica se enfrentó a un ataque de ransomware de 10 millones de dólares por parte del actor de amenazas Conti, con sede en Rusia, que cerró los sistemas de declaración de impuestos y causó agitación económica y mandatos para trabajadores más cualificados en ciberseguridad.[92]

A medida que se exploran los crecientes riesgos cibernéticos dentro del sector financiero, las tendencias de la industria latinoamericana en cuanto a trabajadores cualificados, capital, inversiones y preferencias de los usuarios son vitales para este ecosistema. En última instancia, proporcionan perspectivas cuantificables sobre los vacíos y las mejores prácticas que los profesionales de la ciberseguridad deben priorizar para abordar sus necesidades de ciberhigiene.

3.1.1 Necesidad de más profesionales de la ciberseguridad

Según Vergara Cobos en el informe “2024 América Latina y el Caribe”, entre 2023 y 2024, la industria mundial de la ciberseguridad creció un 14%, y la brecha global de mano de obra aumentó a 4M, lo que representa el doble de la tasa de crecimiento del sector de TI y cuatro veces la de la economía mundial. Esto presenta un potencial significativo para la creación de empleo a través de inversiones en formación y concienciación cibernética.[93] Se prevé que el sector de la ciberseguridad en LATAM crezca un 8% en 2025, con un crecimiento de la mano de obra cualificada del 15%.[94]

Aunque el crecimiento de la industria y el desarrollo de la mano de obra están a la par a nivel mundial, la preparación cibernética regional de América Latina sugiere una baja confianza en la capacidad de sus naciones para resolver ciberataques con su infraestructura crítica actual. América del Norte y Europa muestran los niveles de confianza más altos con un 15%. Mientras tanto, África y América Latina tienen los niveles de confianza más bajos con un 36%, y el 42% de los profesionales de la seguridad de estas regiones dudan de la capacidad de su país para resolver ciberataques.[95] Los países latinoamericanos buscan desesperadamente profesionales que puedan proteger sus activos digitales.[96] A medida que la higiene cibernética y los problemas relacionados con la formación sobre concienciación de amenazas dificultan los esfuerzos de contención, la actualización de las estrategias nacionales y el desarrollo de protocolos de incidentes han aumentado en prioridad para los profesionales de seguridad latinoamericanos.[97] Una mano de obra cualificada no se considera tradicionalmente parte de la infraestructura física crítica. Sin embargo, es esencial para la seguridad de la infraestructura y es un vacío crucial en LATAM que los CISO deben priorizar. El factor humano sigue siendo uno de los puntos más vulnerables dentro de una organización.[98]

La formación y las asociaciones mundiales en el mundo académico pueden ser una inversión en una mano de obra cualificada en ciberseguridad. La escasez de profesionales de la ciberseguridad hace que las instituciones financieras sean vulnerables a los ataques avanzados que sufren muchas de ellas en la región, como indica un informe de la Unión Internacional de Telecomunicaciones (UIT). Los planes de infraestructuras críticas para ciberataques sólo están establecidos en siete de los 32 países de LATAM, y 20 de los 32 cuentan con CSIRT. La evaluación del Banco Interamericano también señala que LATAM requiere mejoras significativas en la capacidad de profesionales cualificados.[99] Esto pone de relieve la urgencia de una mejora regional en la preparación cibernética.[100]

Aspectos destacados: La mejora crítica de la formación de los profesionales de TI, los planes de respuesta a incidentes y las políticas de ciberseguridad son prioridades para mejorar la postura cibernética

[91] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[92] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[93] https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe
[94] https://www.nucamp.co/blog/coding-bootcamp-mexico-mex-mexico-cybersecurity-job-market-trends-and-growth-areas-for-2025
[95] https://www.nucamp.co/blog/coding-bootcamp-mexico-mex-mexico-cybersecurity-job-market-trends-and-growth-areas-for-2025
[96] https://www.nucamp.co/blog/coding-bootcamp-mexico-mex-mexico-cybersecurity-job-market-trends-and-growth-areas-for-2025
[97] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[98] https://mexicobusiness.news/cybersecurity/news/beyond-spending-strategic-investment-cybersecurity-2025
[99] https://www.mordorintelligence.com/industry-reports/latin-america-cyber-security-market
[100] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf

de LATAM. La planificación, los libros de trucos y los ejercicios de evaluación con terceras organizaciones son esenciales. Debido a la falta de personal capacitado y de herramientas para comunicar los desafíos entre los sectores en respuesta, la preparación se revela constantemente como uno de los desafíos más apremiantes Las iniciativas de capacitación y educación pueden ayudar a abordar la escasez de profesionales capacitados en ciberseguridad en la región.

3.1.2 Mayor presupuesto en ciberseguridad para hacer frente al aumento de las ciberamenazas

En América Latina, los bancos son las organizaciones más atacadas, seguidas de cerca por las instituciones sanitarias y educativas. En cuanto a países concretos, Brasil es el que sufre más ciberataques, seguido de México y Colombia. Sin embargo, la frecuencia y la gravedad de los ciberataques en otros países latinoamericanos no se reducen.[101]

Debido a la tecnología emergente como la IA y el empeoramiento de los ciberataques en 2024, América Latina ha aumentado sus inversiones para superar la ciberdelincuencia.[102] El costo de los ciberataques en 2023 fue de 6 billones de USD a nivel global y de 2,4 millones de USD en América Latina. Se espera que en 2025 aumente un 60% a nivel global y un 76% en América Latina, lo que supone un máximo histórico para la región desde 2020.[103] Cabe destacar que, mientras que el 77% de las organizaciones latinoamericanas planean aumentar los presupuestos de ciberseguridad, solo el 25% de las organizaciones en LATAM han adoptado planes integrales de ciberseguridad.[104] El gasto global en ciberseguridad superará 1 billón de USD en 2025, lo que crea oportunidades para abordar la confianza de América Latina en la preparación de la ciberseguridad.[105] El presupuesto para ciberseguridad a menudo refleja las condiciones económicas de un área, que se está convirtiendo en una prioridad de gasto a medida que una organización comprende la necesidad de garantizar los datos y la confianza en su marca.[106]

Aspectos destacados: Estados Unidos se ha comprometido a proporcionar hardware avanzado, formación especializada y apoyo logístico, ofreciendo 25 millones de USD hasta 2026 para ayudar a Costa Rica a mejorar sus capacidades de ciberseguridad. En junio de 2022, el gobierno costarricense asignó 24 millones de USD para respuesta a incidentes y operaciones de seguridad. La gravedad del panorama de amenazas de LATAM no se atribuye al aumento de los fondos sembrados en su compromiso con la ciberdefensa. Más bien se debe a que el país se ha convertido en el primero del mundo en declarar el estado de emergencia debido a un ciberataque.[107]

Como se destaca en la Figura 4 se estima que el mercado latinoamericano de ciberseguridad será de 9,54 mil millones de USD en 2025. Se espera que alcance los 13,35 mil millones de USD en 2030, con una CAGR del 6,95% de 2025 a 2030, impulsada por la rápida digitalización de los servicios financieros y la infraestructura bancaria.[108] Los presupuestos reflejan los planes actuales más establecidos para la preparación cibernética y la respuesta a los ciberataques, mientras que las inversiones dan fe de la concienciación y la preparación proactiva para crear una postura cibernética regional más eficaz. El aumento de las inversiones en soluciones y servicios de preparación cibernética sugiere un impacto en el creciente reconocimiento de la importancia de la ciberseguridad en América Latina.[109]

Figura 4: Mercado latinoamericano de la ciberseguridad

[101] https://www.americaeconomia.com/en/business-industries/cybersecurity-new-center-concern-latin-american-companies
[102] https://www.americaeconomia.com/en/business-industries/cybersecurity-new-center-concern-latin-american-companies
[103] https://www.americaeconomia.com/en/business-industries/cybersecurity-new-center-concern-latin-american-companies
[104] https://mexicobusiness.news/cybersecurity/news/beyond-spending-strategic-investment-cybersecurity-2025
[105] https://mexicobusiness.news/cybersecurity/news/beyond-spending-strategic-investment-cybersecurity-2025
[106] https://www.pwc.com/gx/en/services/forensics/gecs/2024-global-economic-crime-survey.pdf
[107] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[108] https://www.mordorintelligence.com/industry-reports/latin-america-cyber-security-market
[109] https://www.mordorintelligence.com/industry-reports/latin-america-cyber-security-market

3.1.3 Razones para las inversiones

La digitalización de la industria financiera en LATAM requiere más inversiones en ciberseguridad, lo que incluye el aprendizaje automático y la IA para mejorar la detección de amenazas y las capacidades de respuesta. De lo contrario, muchas nuevas empresas regionales de tecnología financiera se convertirán en objetivos muy atractivos para los ciberdelincuentes. En general, esto sugiere la necesidad de más inversiones en ciberseguridad en América Latina.

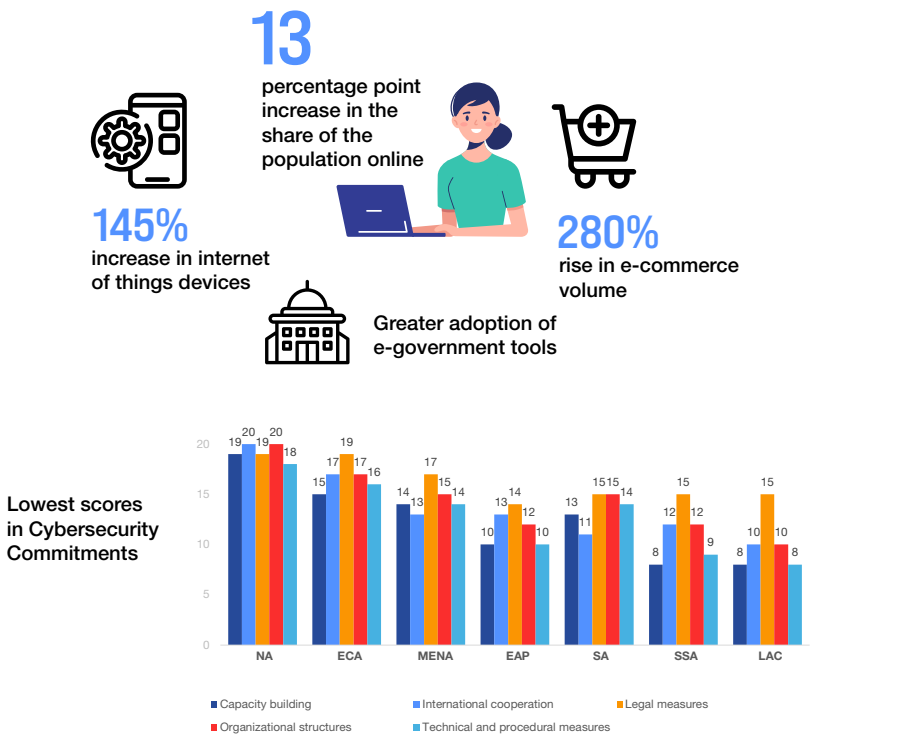
Desafortunadamente, el aumento de la digitalización no está escalando con el riesgo asociado con el sector gubernamental, y es imperativo que se aborden las amenazas de ransomware debido a la falta de madurez en los programas y políticas de ciberseguridad organizacional para la infraestructura crítica en LATAM.[110]

Aspectos destacados: Es imperativo abordar los riesgos cibernéticos en relación con la protección de datos y la seguridad nacional. Debido a los importantes ataques de ransomware, 200 profesionales de la seguridad de nivel ejecutivo de los sectores público y privado coinciden en dar prioridad a la ciberseguridad.[111]

Invertir en ciberseguridad puede generar efectos económicos positivos, con un aumento previsto del 1,5% del PIB per cápita si se mejoran las ciberprotecciones y se reducen los incidentes cibernéticos de 50 a siete incidentes graves. La "Economía de la ciberseguridad para los mercados emergentes" informa de cómo la digitalización ha superado la capacidad de ciberseguridad de la región. En 2024, América Latina y el Caribe serán las regiones menos protegidas, con una puntuación cibernética media de 10,2 sobre 20, y las de mayor crecimiento del mundo en cuanto a incidentes cibernéticos revelados, con una tasa de crecimiento anual del 25% en los últimos 10 años.[112] La rápida digitalización en América Latina ha incrementado las amenazas cibernéticas, específicamente en el sector financiero.

El uso de Internet corresponde a la proporción de la población que utiliza Internet. La Figura 5 destaca que LATAM pasó del 68% al 81% entre 2019 y 2023, según la UIT.

Figura 5: Efecto de la digitalización de ALC



Fuente: Economía de la ciberseguridad para los mercados emergentes (2024).[113]

[110] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[111] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[112] https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe
[113] https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe

3.1.4 Cambio de la banca tradicional a la banca en línea y basada en aplicaciones

Las instituciones financieras, tanto en América Latina como en el resto del mundo, se centran en mejorar la experiencia del usuario a través de aplicaciones fáciles de usar y funciones basadas en la web. Sin embargo, este cambio ha creado nuevas vulnerabilidades en los sofisticados métodos de ingeniería social y phishing, principalmente en los mercados de banca en línea.[114] La conveniencia impulsa las soluciones de banca digital y móvil preferidas por los consumidores latinoamericanos, y los usuarios aceptan con demasiada frecuencia nuevas tecnologías o soluciones basadas en la facilidad de uso frente a los requisitos de seguridad, lo que aumenta el riesgo de ataques de ingeniería social como el phishing.[115]

Aspectos destacados: Colombia se centra en mejorar el rastreo de incidentes; Costa Rica ha priorizado las asociaciones internacionales para las capacidades de respuesta, como la ciencia forense digital y la capacitación de mano de obra calificada; y Chile estableció estándares cibernéticos en su iniciativa Agenda Digital 2035 para abordar la digitalización y la ciberseguridad.[116] Para garantizar que las medidas de ciberseguridad no afecten negativamente a la experiencia del usuario, las instituciones financieras y los bancos deben ser conscientes de las preferencias de los usuarios por los servicios digitales.

Las inversiones en ciberseguridad para la industria financiera en América Latina están aumentando. Sin embargo, la industria debe mejorar la cultura de la conciencia cibernética y adoptar soluciones innovadoras para hacer frente a las amenazas en curso para proteger los activos y clientes. Una postura de seguridad mejorada ayudará a enfrentar el complejo panorama de amenazas cibernéticas de cibercriminales organizados, actores patrocinados por el estado y amenazas internas.

3.2 Factores socioeconómicos contextuales que influyen en la exposición al riesgo

3.2.1 Rápido crecimiento de la tecnología financiera

El sector de la tecnología financiera en América Latina ha crecido considerablemente en los últimos seis años, impulsado por factores socioeconómicos como el aumento de la adopción de la telefonía móvil y el gran número de personas subbancarizadas. Este crecimiento se caracteriza por un aumento del 340% en el número de empresas de tecnología financiera, que pasó de 703 en 18 países en 2017 a 3.069 en 26 países en 2023.[117] Notablemente, esta expansión supera el crecimiento observado en mercados más establecidos como Estados Unidos, donde la innovación en tecnología financiera ha sido significativa pero limitada a su mercado más maduro. Sin embargo, este rápido desarrollo ha expuesto nuevas vulnerabilidades, ya que muchas empresas emergentes de fintech en América Latina a menudo carecen de las sólidas medidas de ciberseguridad comunes en mercados más establecidos. Un estudio del FMI destaca que estos retos de ciberseguridad se derivan de factores como la escasa concienciación, el software obsoleto, las normas insuficientes, las deficiencias en infraestructuras críticas y la limitada formación profesional.[118]

3.2.2 Dependencia de sistemas obsoletos

Debido al desarrollo de las infraestructuras y a los mediocres sistemas tecnológicos y de datos, muchas empresas económicas de América Latina dependen a menudo de sistemas obsoletos. Un análisis publicado en la revista Informatics de MDPI identifica el uso de software obsoleto como una vulnerabilidad crítica en los países latinoamericanos.[119] Esta dependencia de tecnología obsoleta hace que estos sistemas sean vulnerables a amenazas más recientes, ya que a menudo carecen de actualizaciones y parches de seguridad esenciales. Incluso cuando las actualizaciones están disponibles, la arquitectura subyacente de estos sistemas anticuados puede seguir siendo susceptible debido a limitaciones de hardware. En consecuencia, las instituciones financieras con sistemas tan deficientes pueden ser blanco fácil de los ciberdelincuentes. Abordar este problema requiere una inversión sustancial en la modernización de la infraestructura informática y la aplicación de protocolos de mantenimiento. Animar a las instituciones financieras a pasarse a la nube proporcionaría sistemas modernos, más seguros y actualizaciones automatizadas. Según el informe del Foro Económico Mundial sobre los retos de la ciberseguridad en América Latina, la adopción de marcos de gestión de riesgos (RMF) y el uso de tecnologías de nube pública para mejorar la resiliencia cibernética y proteger las infraestructuras vitales podrían combatir los ataques de ransomware.[120] Para aprovechar plenamente las ventajas de la infraestructura de seguridad de la nube, las instituciones financieras tendrían que contratar o confiar en terceros para garantizar la existencia de controles de seguridad consistentes.

[114] https://www.mordorintelligence.com/industry-reports/latin-america-cyber-security-market
[115] https://www.statista.com/statistics/1481783/online-bankingpenetration-latin-america-forecast/:~:text=Online%20banking%20penetration%20in%20Latin%20America%20increased%20gradually%20between%202019,to%2033%20percent%20in%202023
[116] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[117] https://www.iadb.org/en/news/study-fintech-ecosystem-latin-america-and-caribbean-exceeds-3000-startups
[118] https://www.imf.org/en/Publications/fintech-notes/Issues/2023/03/28/The-Rise-and-Impact-of-Fintech-in-Latin-America-531055
[119] https://www.mdpi.com/2227-9709/10/3/71
[120] https://www.weforum.org/stories/2024/05/latin-america-cybersecurity-report-ransomware attacks/

3.2.3 Disparidades económicas y digitales

América Latina presenta importantes disparidades económicas y digitales en todo su territorio, lo que se traduce en una pronunciada brecha digital. En 2022, el 67,3% de los hogares de la región tenía acceso a Internet, frente al 91,1% en los países de la OCDE.[121] Esta disparidad plantea retos para las pequeñas y medianas empresas (pymes), que son vitales para la economía de la región.[122] Muchas de estas empresas operan con presupuestos limitados, lo que restringe su capacidad para invertir en medidas sólidas de ciberseguridad. Esta limitación financiera las convierte en objetivos atractivos para los ciberdelincuentes, ya que las PYME carecen a menudo de las defensas avanzadas que se encuentran en las grandes empresas. Invertir en infraestructura digital para reducir la brecha digital entre particulares y PYME puede mejorar la ciberseguridad y mitigar riesgos destacados.

[121] https://www.undp.org/latin-america/blog/missed-connections-incomplete-digital-revolution-latin-america-and-caribbean-0
[122] https://www.iadb.org/en/news/ninety-six-percent-banks-latin-america-and-caribbean-view-small-and-medium-enterprises#:~:text=Ninety%2Dsix%20percent%20of%20the,policy%20for%20SMEs%20in%20place.

4 Lagunas normativas

4.1 Requisitos de notificación de ataques de ransomware y falta de normas

Los requisitos de notificación de ciberseguridad en LATAM son incoherentes, lo que provoca vulnerabilidades en la capacidad de la región para combatir eficazmente las ciberamenazas.

Por ejemplo, considerar lo siguiente:

1. La Ley General de Protección de Datos (LGPD) de Brasil obliga a las organizaciones a informar de las violaciones a la Autoridad Nacional de Protección de Datos (ANPD) en un plazo de dos días hábiles y notificar a las personas afectadas.[123]

2. Colombia exige a las organizaciones que informen de las violaciones de los códigos de seguridad a la Delegatura para la Protección de Datos Personales y a los interesados afectados.[124]

3. México obliga a notificar las "vulnerabilidades de datos" que afecten a los derechos de las personas, pero no especifica un plazo.

4. Argentina se limita a recomendar la notificación voluntaria como mejor práctica.[125]

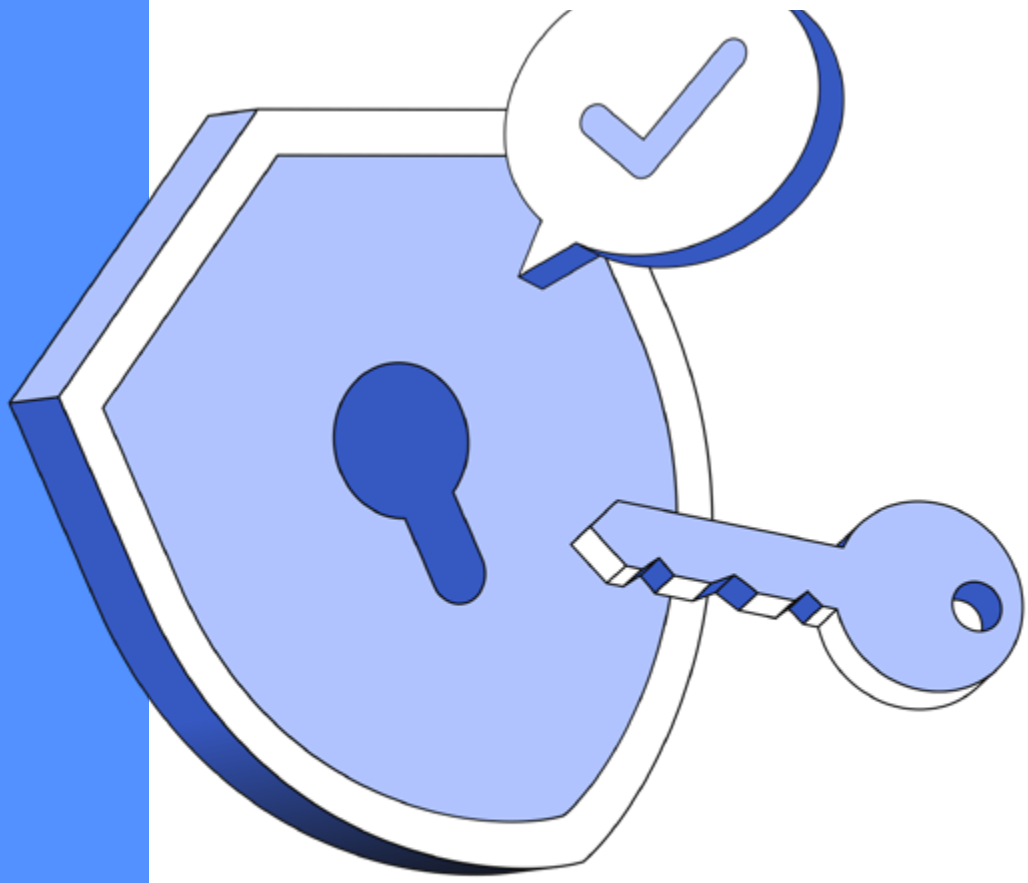
5. Muchos países, como Perú, Ecuador y Costa Rica, carecen por completo de marcos integrales de información.[126]

Este panorama normativo fragmentado crea importantes lagunas, lo que hace que LATAM sea cada vez más susceptible a los ataques de ransomware. Los países con informes obligatorios limitados o inexistentes, como las naciones centroamericanas, se enfrentan a retos a la hora de rastrear y responder a las amenazas debido al insuficiente intercambio de datos y coordinación de inteligencia sobre amenazas.[127] La falta de normas de seguridad armonizadas da lugar a prácticas incoherentes en toda la región, lo que deja puntos débiles que los ciberdelincuentes pueden explotar.[128] Además, la infraestructura de ciberseguridad inadecuada, la educación insuficiente y los recursos limitados exacerban estas vulnerabilidades, especialmente en sectores como el manufacturero y el financiero, que han enfrentado más de 100 incidentes de ransomware desde 2023.[129] [130]

La ausencia de marcos de información estrictos también retrasa los tiempos de respuesta a las intrusiones, lo que permite a los operadores de ransomware explotar aún más los sistemas comprometidos.[131] La rápida transformación digital en LATAM, especialmente en los servicios financieros, ha superado los desarrollos regulatorios, creando superficies de ataque adicionales.[132] [133] Sin requisitos sólidos de notificación de incidentes y estrategias de defensa coordinadas, muchas naciones de LATAM están luchando para combatir las amenazas de ransomware cada vez más sofisticadas dirigidas a instituciones gubernamentales y financieras.[134] [135]

---

[123] https://iapp.org/news/a/reporting-cyber-incident-requirements-in-some-latin-american-jurisdictions
[124] https://iapp.org/news/a/reporting-cyber-incident-requirements-in-some-latin-american-jurisdictions
[125] https://iapp.org/news/a/reporting-cyber-incident-requirements-in-some-latin-american-jurisdictions
[126] https://www.dacbeachcroft.com/en/What-we-think/Stepping-up-in-Latin-America-Chile-enacts-a-new-Cybersecurity-Law
[127] https://www.moodys.com/web/en/us/insights/credit-risk.html
[128] https://www.moodys.com/web/en/us/insights/credit-risk.html
[129] https://www.cloudsek.com/whitepapers-reports/latin-america-latam-cyber-threat-landscape-2023-24
[130] https://www.recordedfuture.com/research/latin-american-governments-targeted-by-ransomware
[131] https://www.datto.com/blog/ransomware-and-cybersecurity-in-latin-america/
[132] https://www.datto.com/blog/ransomware-and-cybersecurity-in-latin-america/
[133] https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/trustwave-spiderlabs-reveals-the-ransomware-threats-targeting-latin-american-financial-and-government-sectors/
[134] https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/trustwave-spiderlabs-reveals-the-ransomware-threats-targeting-latin-american-financial-and-government-sectors/
[135] https://industrialcyber.co/analysis/recorded-future-detects-escalation-of-ransomware-attacks-across-latam-government-entities/



5 Perfiles de los actores de amenazas

5.1 CL0P

CL0P surgió a principios de 2019 como un derivado de la familia de ransomware Cryptomix.[136] El grupo de ransomware evolucionó rápidamente de utilizar métodos tradicionales de despliegue de ransomware a un sofisticado grupo de ciberamenazas dirigido a empresas globales.[137] El ransomware del grupo se caracteriza por su exclusiva extensión de archivo ".clop" y la distintiva cadena "Don't Worry CL0P" en sus notas de rescate.[138] Las operaciones iniciales del grupo se basaban principalmente en el despliegue tradicional de ransomware a través de campañas de phishing. Sin embargo, su metodología sufrió una transformación significativa al adoptar un modelo RaaS. Esta transición resultó crucial, ya que les permitió aprovechar las relaciones con actores de amenazas sofisticados, como TA505, FIN11 y UNC 2546, para las operaciones de implementación.

5.1.1 Perfil de las víctimas y análisis del impacto

El análisis de la lista de víctimas de CL0P sugiere que el grupo de ransomware se dirige principalmente a grandes empresas con ingresos superiores a los 5 millones de dólares.[139] Las principales entidades que son objetivo de CL0P pertenecen a los siguientes sectores: banca y finanzas, sanidad, industria manufacturera, educación y energía.[140] Las actividades de CL0P han sido frecuentes en Estados Unidos, Reino Unido, Alemania, Canadá, Brasil y México, que representan el 77,3% de sus ataques.[141]

El impacto de las operaciones de CL0P en los países latinoamericanos ha sido sustancial, especialmente en Brasil y México.[142] En LATAM, donde los marcos de ciberseguridad son incipientes, las organizaciones se enfrentan a vulnerabilidades amplificadas debido a los sistemas interconectados y a las limitadas capacidades de respuesta ante incidentes. Además, las instituciones financieras de América Latina se enfrentan a una doble amenaza: ataques directos a los sistemas bancarios y compromisos de la cadena de suministro, como el exploit de día cero MOVEit, que afectó a cientos de organizaciones.

Impacto y escala de las operaciones de CL0P:

- Las actividades de CL0P registraron un aumento del 340% de víctimas en comparación con el trimestre anterior, debido potencialmente a la explotación de la vulnerabilidad de día cero MOVEit.[143]
- Se espera que el grupo gane entre 75 y 100 millones de dólares extorsionando a las víctimas en su campaña masiva de robo de datos MOVEit.[144]

5.1.2 Capacidades y funcionalidad del malware

La sofisticación técnica de CL0P es evidente en sus cadenas de ataque cuidadosamente estructuradas. Sus vectores de acceso iniciales han evolucionado desde simples campañas de phishing hasta sofisticadas técnicas de explotación de día cero.[145] El grupo mantiene un variado conjunto de herramientas, que incluye malware especializado, como SDBot para el movimiento lateral, Cobalt Strike para actividades posteriores a la explotación, y herramientas personalizadas como FlawedAmmyy/FlawedGrace para operaciones de mando y control.[146]

El uso por parte de CL0P de TrueBot, un componente de malware avanzado asociado al Silence Group, demuestra sus conexiones con sofisticados actores de amenazas financieras. La capacidad de TrueBot para desplegar cargas útiles adicionales manteniendo la ocultación mediante mecanismos de autoeliminación demuestra su interés por la seguridad operativa.[147] Además, la asociación del malware con TA505 y su uso de una puerta trasera exclusiva llamada FlawedGrace, indica la posición de CL0P dentro de un sofisticado ecosistema de ciberamenazas.[148] La penetración inicial del grupo en la red suele seguir un enfoque orquestado en varias fases:

1. La explotación de aplicaciones web de cara al público utilizando el shell web LEMURLOOT, escrito en lenguaje de codificación C# y camuflado como un archivo ASP. NET. 2. Operaciones de recolección de credenciales que permiten el movimiento lateral y el acceso a datos sensibles. 3. Operaciones de robo de datos en las que se presta especial atención a la seguridad operativa, centrándose más en la exfiltración que en el cifrado.[149]

[136] https://www.sangfor.com/blog/cybersecurity/Cl0p ransomware-gang-what-you-need-to-know
[137] https://unit42.paloaltonetworks.com/cl0p-group-distributes-ransomware-data-with-torrents/
[138] https://www.sangfor.com/blog/cybersecurity/Cl0p ransomware-gang-what-you-need-to-know
[139] https://www.sangfor.com/blog/cybersecurity/Cl0p ransomware-gang-what-you-need-to-know
[140] https://www.securin.io/blog/all-about-clop-ransomware/
[141] https://socradar.io/dark-web-threat-profile-clop-ransomware/
[142] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware spotlight-clop
[143] https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q3- 2023/
[144] https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q3- 2023/
[145] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware spotlight-clop
[146] https://blog.talosintelligence.com/breaking-the-silence-recent-truebot-activity/
[147] https://em360tech.com/tech-article/what-is-cl0p-ransomware
[148] https://em360tech.com/tech-article/what-is-cl0p-ransomware
[149] https://em360tech.com/tech-article/what-is-cl0p-ransomware

5.1.3 Evolución de las operaciones de CL0P

1. Cambio en el vector de ataque: Al principio, CL0P se basaba principalmente en campañas de phishing con documentos habilitados para macros para distribuir el dropper malicioso Get2.[150] En campañas recientes, han pasado a explotar vulnerabilidades de día cero en aplicaciones de transferencia de archivos muy utilizadas.[151] [152]

2. Focalización en la filtración de datos: Aunque sus ataques iniciales incluían tanto el cifrado de archivos como el robo de datos, las últimas campañas se han centrado más en la exfiltración de datos sin cifrar necesariamente los archivos.[153] [154]

3. Escala de los ataques: Las campañas recientes se han dirigido a un número significativamente mayor de víctimas simultáneamente a través de ataques a la cadena de suministro. Por ejemplo, el exploit MOVEit en 2023 afectó hasta a 400 organizaciones.[155]

4. Sofisticación de las técnicas: CL0P ha evolucionado para utilizar técnicas de evasión más avanzadas, incluyendo firmas digitales para eludir la detección de terminales.[156]

5. Expansión a nuevas plataformas: Inicialmente dirigido solo a sistemas Windows, CL0P desarrolló una variante Linux a finales de 2022, ampliando su cartera de víctimas potenciales.[157]

6. Enfoque del rescate: Las campañas recientes han visto a CL0P contactando directamente a ejecutivos de alto nivel con demandas de rescate, en lugar de dejar notas de rescate tradicionales en los sistemas infectados.[158]

7. Cronología de la explotación: CL0P ha mostrado una mayor paciencia y planificación estratégica, con pruebas que sugieren que pueden haber estado preparando el exploit MOVEit desde 2021.[159]

El hecho de que CL0P haya pasado de cifrar dispositivos a centrarse únicamente en la exfiltración de datos hace que sus ataques sean potencialmente más sigilosos y difíciles de detectar. Este cambio en el modus operandi podría permitir a CL0P operar sin ser detectado durante períodos más largos, ya que no hay signos inmediatos de compromiso, como archivos cifrados o notas de rescate.

El paso a la exfiltración de datos es una evolución lógica de las tácticas de CL0P por varias razones:

1. Menor riesgo de detección: Sin cifrado de archivos, hay menos indicadores obvios de compromiso (IOC), lo que dificulta que las organizaciones identifiquen rápidamente un ataque en curso.

2. Acceso ampliado: Al no alertar a las víctimas a través del cifrado, CL0P puede potencialmente mantener el acceso a los sistemas durante períodos más largos, lo que permite un robo de datos más completo.

3. Operaciones simplificadas: Al centrarse únicamente en la exfiltración de datos se agiliza el proceso de ataque, lo que potencialmente permite a CL0P dirigirse a más víctimas simultáneamente.

4. Aumento de la presión: La amenaza de filtrar datos confidenciales puede ser tan eficaz como el cifrado de archivos para obligar a las víctimas a pagar, sin la complejidad añadida de proporcionar herramientas de descifrado.

El éxito de este enfoque es evidente en las recientes campañas de CL0P, como el ataque 2023 MOVEit, en el que afirmaron haber vulnerado cientos de empresas aprovechando una vulnerabilidad de día cero (CVE-2023-34362) para descargar masivamente los datos de las organizaciones sin cifrar los archivos.[160] Al adoptar este enfoque más sigiloso, CL0P puede aumentar potencialmente la tasa de éxito de sus ataques y la probabilidad de que se paguen rescates, ya que las organizaciones pueden sentirse más presionadas para evitar la filtración de datos confidenciales.

Aunque hay menos pruebas concretas del cambio explícito de CL0P al sigilo, los expertos en ciberseguridad reconocen que los grupos están adoptando únicamente la extorsión de datos para eludir las defensas tradicionales. La exfiltración de datos proporciona a los grupos de ransomware una mayor ventaja sobre sus víctimas de varias maneras:

1. Potencial de extorsión prolongada: Una vez robados los datos, los ciberdelincuentes pueden seguir explotándolos para extorsiones adicionales mucho después del incidente inicial, incluso si se paga el rescate original.[161]

[150] https://www.nuspire.com/blog/a-deep-dive-into-cl0p-ransomware/
[151] https://em360tech.com/tech-article/what-is-cl0p-ransomware
[152] https://www.criticalstart.com/threat-research-cl0p-ransomware-increases-activity
[153] https://em360tech.com/tech-article/what-is-cl0p-ransomware
[154] https://www.criticalstart.com/threat-research-cl0p-ransomware-increases-activity
[155] https://www.criticalstart.com/threat-research-cl0p-ransomware-increases-activity
[156] https://em360tech.com/tech-article/what-is-cl0p-ransomware
[157] https://www.criticalstart.com/threat-research-cl0p-ransomware-increases-activity
[158] https://em360tech.com/tech-article/what-is-cl0p-ransomware
[159] https://em360tech.com/tech-article/what-is-cl0p-ransomware
[160] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware double-extortion-and-beyond-revil-clop-and-conti
[161] https://www.grcilaw.com/blog/top-3-reasons ransomware-groups-are-focusing-more-on-data-exfiltration-than-encryption

2. Demandas a medida: Los datos filtrados permiten a los atacantes personalizar sus demandas de extorsión en función de la sensibilidad y el valor de la información robada.[162] [163]

3. Aumento de la presión: La amenaza de filtrar datos sensibles puede ser más eficaz que el cifrado de archivos para obligar a las víctimas a pagar, ya que explota el miedo a las multas reglamentarias, el daño a la reputación y la desventaja competitiva.[164] [165]

4. Evasión de copias de seguridad: Aunque las organizaciones pueden restaurar archivos cifrados a partir de copias de seguridad, no pueden recuperar datos que ya han sido robados, lo que hace que las soluciones de copia de seguridad tradicionales sean ineficaces contra los ataques modernos de ransomware.[166]

5. Potencial de ataque secundario: Los datos comprometidos pueden alimentar futuras brechas de seguridad a través de tácticas como el relleno de credenciales, la ingeniería social y los ataques de reutilización de contraseñas.[167]

6. Mayor rentabilidad: Los datos robados pueden ser más valiosos que el pago de rescates, ya que pueden venderse en la web oscura o utilizarse para chantajes continuos.[168]

Este cambio hacia la exfiltración de datos demuestra la evolución de las tácticas de los grupos de ransomware a medida que se adaptan a la mejora de las defensas de las organizaciones y buscan formas más eficaces de presionar a las víctimas para que paguen rescates.[169] [170]

El grupo de ransomware ha evolucionado significativamente su metodología operativa desde su aparición en 2019, convirtiéndose en uno de los grupos de ransomware más temidos en 2023. El enfoque del grupo en vulnerabilidades de día cero en aplicaciones de transferencia de archivos (FTA por sus siglas en inglés) está impulsado por varios factores:

1. Uso generalizado: Los FTA se utilizan comúnmente en entornos corporativos, proporcionando a los atacantes numerosos puntos de entrada potenciales.[171]

2. Potencial de ataque a la cadena de suministro: Explotar las vulnerabilidades de las FTA permite a CL0P comprometer potencialmente a múltiples organizaciones de forma simultánea.[172] [173]

3. Exfiltración eficaz de datos: Las FTA están diseñadas para la transferencia eficiente de datos, facilitando el robo de grandes cantidades de datos.

4. Requisitos de cumplimiento: Muchas FTA, como MOVEit, están aprobadas para su uso en industrias reguladas, lo que significa que a menudo contienen datos altamente sensibles.[174]

5. Objetivos de alto valor: Las organizaciones que utilizan FTA a menudo incluyen grandes empresas y agencias gubernamentales, que son objetivos lucrativos para los ataques de ransomware.[175] [176]

6. Sigilo: Acceder a los sistemas a través de herramientas legítimas de transferencia de archivos puede hacer que las actividades maliciosas parezcan normales, ayudando a los atacantes a evadir la detección.

Este enfoque ha demostrado ser altamente efectivo para CL0P, como lo evidencian sus ataques exitosos contra Accellion FTA, GoAnywhere MFT y MOVEit Transfer, cada uno afectando a cientos de organizaciones y potencialmente exponiendo los datos de millones de personas.[177] [178]

5.1.4 Impacto en la infraestructura financiera

El carácter sistemático de las operaciones de CL0P contra instituciones financieras ha revelado vulnerabilidades fundamentales en las arquitecturas de seguridad de todo el sector. El éxito del grupo en la explotación de sistemas gestionados de transferencia de archivos ha puesto de manifiesto puntos débiles críticos en el enfoque del sector financiero respecto a la transferencia segura de datos y la integración de software de terceros.[179] La campaña MOVEit constituye un ejemplo particularmente instructivo, en el que una única vulnerabilidad en una plataforma ampliamente utilizada condujo a compromisos en múltiples instituciones financieras.[180]

[162] https://www.grcilaw.com/blog/top-3-reasons ransomware-groups-are-focusing-more-on-data-exfiltration-than-encryption
[163] https://www.vadesecure.com/en/blog/data-exfiltration-why ransomware-is-about-more-than-the-ransom
[164] https://www.grcilaw.com/blog/top-3-reasons ransomware-groups-are-focusing-more-on-data-exfiltration-than-encryption
[165] https://www.infosecurity-magazine.com/news/ransomware defense-evasion-data/
[166] https://www.grcilaw.com/blog/top-3-reasons ransomware-groups-are-focusing-more-on-data-exfiltration-than-encryption
[167] https://www.grcilaw.com/blog/top-3-reasons ransomware-groups-are-focusing-more-on-data-exfiltration-than-encryption
[168] https://www.infosecurity-magazine.com/news/ransomware defense-evasion-data/
[169] https://www.vadesecure.com/en/blog/data-exfiltration-why ransomware-is-about-more-than-the-ransom
[170] https://www.infosecurity-magazine.com/news/ransomware defense-evasion-data/
[171] https://cyberint.com/blog/dark-web/cl0p-ransomware/
[172] https://cyberint.com/blog/dark-web/cl0p-ransomware/
[173] https://www.cisa.gov/sites/default/files/2023- 06/aa23-158a-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability_5.pdf
[174] https://cyberint.com/blog/dark-web/cl0p-ransomware/
[175] https://cyberint.com/blog/dark-web/cl0p-ransomware/
[176] https://www.cisa.gov/sites/default/files/2023- 06/aa23-158a-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability_5.pdf
[177] https://cyberint.com/blog/dark-web/cl0p-ransomware/
[178] https://www.cisa.gov/sites/default/files/2023- 06/aa23-158a-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability_5.pdf
[179] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware spotlight-clop
[180] https://securityandtechnology.org/blog/2023-rtf-global-ransomware-incident-map

Además, el impacto va más allá de la interrupción operativa inmediata. Las instituciones financieras afectadas por las operaciones de CL0P se han enfrentado a complejos retos para mantener el cumplimiento normativo y desarrollar políticas actualizadas mientras gestionan los escenarios de compromiso en curso. Sólo en Perú, el 47% de los CISO enumeran el cumplimiento de regulaciones geográficamente fragmentadas y excesivamente prescriptivas como su responsabilidad más estresante. De todas las industrias, la industria de servicios financieros es la más preocupada por las regulaciones fragmentadas, con un 67% de los CISO globales del sector anticipando que las regulaciones internacionales se volverán más complejas y difíciles de manejar en el próximo año. En consecuencia, la comprensión de CL0P de los marcos normativos del sector financiero les ha permitido estructurar sus demandas de extorsión de forma que creen la máxima presión dentro de un mosaico de obligaciones normativas emergentes [26]. Basándose en su campaña MOVEit, CL0P ha demostrado la sincronización anticipada de las liberaciones y demandas de extorsión, ya que libera por lotes los datos de las víctimas para maximizar la presión.[181]

Con más de 1.600 intentos de ciberataque por segundo contra empresas latinoamericanas, las instituciones financieras de LATAM se han enfrentado a retos específicos debido a la naturaleza interconectada de las redes financieras regionales.[182] La explotación de infraestructuras compartidas y plataformas de software comunes ha creado efectos en cascada en múltiples instituciones.[183] Este impacto regional se ejemplifica en las secuelas de la campaña GoAnywhere MFT, donde múltiples instituciones regionales descubrieron compromisos a través de dependencias de infraestructura compartida.[184]

5.1.5 Deficiencias en materia de normativa y políticas

1. Marcos limitados para la protección de infraestructuras críticas

Una vulnerabilidad fundamental se deriva de los marcos incipientes de América Latina para la protección de las infraestructuras críticas. Según el Banco Interamericano de Desarrollo, sólo siete de los 32 países latinoamericanos han establecido planes para proteger las infraestructuras críticas frente a los ciberataques, y sólo 20 acreditan la existencia de CSIRT.[185] Esta inmadurez normativa afecta especialmente a las instituciones financieras, que carecen de protocolos de seguridad específicos para el sector federal y de requisitos de notificación de incidentes estandarizados en todas las jurisdicciones de LATAM.[186]

2. Coordinación fragmentada de respuesta a incidentes

La ausencia de una gobernanza centralizada de ciberseguridad crea importantes retos de coordinación durante los incidentes de ciberseguridad. Esta brecha fue evidente tanto en la crisis del ransomware de Costa Rica en 2022 como en el ataque a IFX Networks en Colombia en septiembre de 2023, que afectó inicialmente a 20 entidades públicas e indirectamente a otras 78 entidades públicas y 762 empresas privadas -incluidas instituciones financieras- en múltiples países de LATAM.[187] La falta de protocolos estandarizados de respuesta a incidentes en toda la región crea oportunidades para que los actores de amenazas como CL0P aprovechen las lagunas en la coordinación transfronteriza. CL0P ha demostrado una sofisticada comprensión de estas deficiencias, como lo demuestra su sistemático ataque a plataformas de software empresarial ampliamente utilizadas que pueden afectar a múltiples instituciones simultáneamente.

3. Requisitos de notificación obligatorios insuficientes

Muchos países latinoamericanos carecen de requisitos obligatorios integrales de notificación de violaciones, en particular para las instituciones financieras. Esta brecha regulatoria se alinea con las tácticas documentadas de CL0P de explotar las asimetrías de información y retrasar la detección de incidentes.[188] La ausencia de requisitos estrictos de notificación puede ampliar la ventana de oportunidad para que bandas sofisticadas como CL0P mantengan su persistencia y amplíen su acceso dentro de redes comprometidas.

4. Retos en la implementación de la protección de datos

Si bien países como Brasil, Argentina, México, Panamá y Colombia han promulgado leyes de protección de datos, su implementación y aplicación siguen siendo inconsistentes. Esto genera vulnerabilidades para las instituciones financieras que manejan datos sensibles de sus clientes, lo que se alinea con el enfoque demostrado de CL0P en el robo de datos y las operaciones de extorsión en múltiples etapas dirigidas a proveedores de servicios financieros.

El uso de FlawedAmmyy/FlawedGrace para operaciones de comando y control refleja una adaptación específica a los controles de seguridad del sector financiero regional, permitiéndoles mantener un acceso persistente.

[181] https://www.cisa.gov/sites/default/files/2023- 06/aa23-158a-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability_5.pdf
[182] https://www.cisa.gov/sites/default/files/2023- 06/aa23-158a-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability_5.pdf
[183] https://www.cisa.gov/sites/default/files/2023- 06/aa23-158a-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability_5.pdf
[184] https://www.cisa.gov/sites/default/files/2023- 06/aa23-158a-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability_5.pdf
[185] https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf
[186] https://iapp.org/news/a/reporting-cyber-incident-requirements-in-some-latin-american-jurisdictions
[187] https://www.metabaseq.com/e-book/cyber-readiness-in-latin-american-public-sectors/
[188] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf

5.1.6 Estructura del mercado y contexto de la transformación digital

El mercado bancario latinoamericano sigue siendo el de más rápido crecimiento a nivel mundial, con unos ingresos antes del costo del riesgo que crecen a una tasa anual compuesta del 12% desde 2012, alcanzando los 418.000 millones de dólares en 2017.[189] Desde 2020, el sector de la banca minorista de LATAM casi ha duplicado su tasa compuesta de crecimiento anual de los ingresos (medida en billones de USD) de 2013 a 2019.[190] Además, LATAM ha experimentado un crecimiento significativo en los ingresos por pagos en línea y se prevé que supere a todas las demás regiones hasta 2027.[191]. Este rápido crecimiento histórico, combinado con tasas de penetración bancaria relativamente bajas del 30-50% en comparación con el 90%+ en los mercados desarrollados, crea presión para una rápida transformación digital que a menudo supera la implementación de la seguridad.[192] Con el número de consumidores de LATAM que prefieren los pagos móviles y con tarjeta duplicándose desde 2021, los bancos de LATAM están cambiando a una estrategia de entrega mobile-first mientras priorizan las inversiones en TI para mejorar las experiencias de los usuarios.[193]

5.1.7 Presiones de rentabilidad que crean compromisos de seguridad

Si bien los bancos latinoamericanos fueron alguna vez los más rentables a nivel mundial, con un ROE del 14% en 2017, continúan enfrentando importantes desafíos de rentabilidad. Los gastos operativos promedian el 3,9% de los activos, un 1,5% más que la siguiente región más cercana.[194] Esta presión sobre los costos crea vulnerabilidades a medida que las entidades equilibran las inversiones en transformación digital con el gasto en seguridad. Además, los servicios de financiación al consumo e hipotecarios (que representan más de un tercio de los ingresos después de riesgos) son especialmente atractivos para los actores de amenazas debido a su alta concentración de datos sensibles de los clientes.[195]

5.1.8 Vulnerabilidades específicas del sector

1. Presiones de la transformación digital

El sector de servicios financieros latinoamericano está experimentando una rápida transformación digital, particularmente acelerada por la bancarización (el nivel de acceso y el grado de uso de los servicios financieros y bancarios) después de la pandemia de COVID-19. Esto crea una superficie de ataque ampliada que el CL0P ha demostrado ser capaz de explotar. La adopción de soluciones de transferencia gestionada de archivos (MFT) a menudo supera las implementaciones de seguridad, como lo demuestra el amplio impacto de la campaña MOVEit de CL0P en las instituciones financieras de la región.[196] Las instituciones financieras deben asegurarse de que cuentan con los “conocimientos técnicos” adecuados en materia de seguridad y resiliencia operativa antes de incorporar la tecnología para garantizar la seguridad y solidez de la institución.

2. Factores de vulnerabilidad operativa

Las vulnerabilidades del sector bancario pueden atribuirse a tres arquetipos de mercado distintos identificados en la región[197]:

- Mercados impulsados por la eficiencia: Estos mercados, como el chileno, donde las estructuras de costos son reducidas, lo que puede derivar en una inversión insuficiente en infraestructura de seguridad. Con un índice de gasto operativo inferior al 3.4% de los activos, el presupuesto destinado a seguridad tiende a ser limitado.
- Mercados equilibrados: Mercados como Brasil combinan una generación de ingresos moderada (4,5-7% de los activos) con unos costos operativos de rango medio, lo que crea posibles lagunas de seguridad a la hora de equilibrar prioridades de inversión contrapuestas.
- Mercados impulsados por los ingresos: Los mercados como Argentina generan altos ingresos, pero operan con gastos operativos superiores al 5.5% de los activos, lo que podría afectar la eficiencia de las operaciones de seguridad a pesar de una mayor inversión.

3. Retos para el desarrollo de la mano de obra

Una vulnerabilidad crítica de la industria se deriva de la grave escasez de profesionales de la ciberseguridad en toda América Latina. Por ejemplo, sólo Chile se enfrenta a un déficit anual de aproximadamente 6.000 profesionales de TI.[198] Esta carencia de capital humano afecta particularmente la capacidad de las instituciones financieras para hacer lo siguiente:

- Implementar controles de seguridad sofisticados.
- Mantener operaciones de seguridad efectivas.
- Responder rápidamente a las amenazas emergentes.
- Adaptarse a la evolución de las metodologías de ataque.

[189] https://www.mckinsey.com/industries/financial-services/our-insights/lessons-from-leaders-in-latin-americas-retail-banking-market
[190] https://www.mckinsey.com/industries/financial-services/our-insights/global-banking-annual-review
[191] https://www.mckinsey.com/industries/financial-services/our-insights/global-banking-annual-review
[192] https://www.mckinsey.com/industries/financial-services/our-insights/lessons-from-leaders-in-latin-americas-retail-banking-market
[193] https://www.mckinsey.com/industries/financial-services/our-insights/global-banking-annual-review
[194] https://www.mckinsey.com/industries/financial-services/our-insights/lessons-from-leaders-in-latin-americas-retail-banking-market
[195] https://www.mckinsey.com/industries/financial-services/our-insights/lessons-from-leaders-in-latin-americas-retail-banking-market
[196] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[197] https://www.mckinsey.com/industries/financial-services/our-insights/lessons-from-leaders-in-latin-americas-retail-banking-market
[198] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf

La escasez de mano de obra se alinea con las tácticas documentadas de CL0P de explotar las deficiencias en la supervisión de la seguridad y las capacidades de respuesta ante incidentes.

4. Dependencias de infraestructura

Las instituciones financieras latinoamericanas suelen depender de infraestructuras compartidas y plataformas tecnológicas comunes, lo que crea vulnerabilidades sistémicas que el CL0P ha demostrado ser experto en explotar. El ataque a IFX Networks de septiembre de 2023 demostró cómo el compromiso de un único proveedor de servicios podría afectar a múltiples instituciones financieras de varios países.[199] Esta interdependencia se ve exacerbada por la carencia existente en los marcos de protección de las infraestructuras de la región.

5.1.9 Carencias en el sector público que crean riesgos descendentes

1. Disparidades en la asignación de recursos

Los presupuestos de ciberseguridad del sector público en América Latina están sistemáticamente por detrás de las inversiones del sector privado. Esto crea desafíos particulares para las instituciones financieras que deben interactuar con los sistemas gubernamentales, especialmente en áreas como las siguientes:

- Recaudación de impuestos y presentación de informes.
- Sistemas de cumplimiento normativo.
- Infraestructuras nacionales de pago.
- Servicios de verificación de identidad.

La metodología de ataque de CL0P a menudo explota estas interconexiones público-privadas, como se demostró en los incidentes de Costa Rica y Colombia.[200]

5.1.10 La convergencia de vulnerabilidades crea una oportunidad estratégica para CL0P

La combinación de carencias reglamentarias y tendencias del sector crea múltiples vectores que se alinean con la sofisticada metodología de selección de objetivos y los patrones operativos de CL0P:

1. Oportunidades de explotación en varias fases

La preferencia documentada de CL0P por las operaciones de extorsión en varias etapas ha demostrado su eficacia en América Latina debido a la convergencia de varios factores:

- Retraso en las capacidades de detección debido a la escasez de mano de obra.
- Complejos requisitos de coordinación transfronteriza.
- Marcos incoherentes de notificación de incidentes.
- Interconectividad regional de los sistemas financieros.

Este entorno permite al CL0P maximizar tanto el acceso inicial como las oportunidades de movimiento lateral.[201]

2. Zona de ataque del sector financiero

Las iniciativas de transformación digital del sector de los servicios financieros, combinadas con los requisitos de cumplimiento normativo, crean una superficie de ataque ampliada que CL0P ha demostrado saber explotar. El sofisticado conocimiento que tiene el grupo de los patrones operativos del sector financiero se pone de manifiesto en los siguientes ataques:

- Sistemas gestionados de transferencia de archivos esenciales para la presentación de informes reglamentarios.
- Protocolos deficientes de autenticación y control de acceso
- Proveedores de servicios compartidos que dan servicio a múltiples instituciones
- Sistemas de pago y liquidación transfronterizos
- Plataformas bancarias centrales con despliegues regionales.

Esta orientación se ajusta a las capacidades documentadas de su paquete de malware avanzado, que incluye TrueBot y FlawedGrace, adaptadas específicamente a los controles de seguridad del sector financiero.[202]

3. Efectos de amplificación regional

La naturaleza interconectada de los mercados financieros latinoamericanos crea oportunidades para que los actores de amenazas amplifiquen el impacto de compromisos individuales. Este efecto multiplicador hace que la región sea especialmente atractiva para operaciones sofisticadas de ransomware que buscan el máximo apalancamiento para las demandas de extorsión.

[199] https://www.metabaseq.com/e-book/cyber-readiness-in-latin-american-public-sectors/
[200] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[201] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[202] https://blog.talosintelligence.com/breaking-the-silence-recent-truebot-activity/

5.1.11 Implicaciones de cara al futuro

Evolución del panorama de amenazas

La combinación de las deficiencias normativas y las presiones del sector sugieren que las instituciones financieras latinoamericanas seguirán siendo el objetivo de sofisticados actores de amenazas. La capacidad demostrada por CL0P para adaptar sus tácticas a las vulnerabilidades regionales indica lo siguiente:

- Es probable que aumente la sofisticación de los ataques
- Los incidentes transfronterizos serán cada vez más comunes
- Se seguirán aprovechando los compromisos de la cadena de suministro
- Se ampliarán las operaciones de extorsión en varias fases.

5.1.12 Tácticas, técnicas y procedimientos de CL0P

Tácticas	Técnicas	Procedimientos
Reconocimiento (TA0043)	T1592: Recopilación de información sobre el host	Utiliza tácticas de phishing e ingeniería social para recopilar información sobre sus objetivos
	T1589.002: Direcciones de correo electrónico	Obtiene acceso a las credenciales del objetivo a través de phishing, ingeniería social y IAB.
	T1589.001: Credenciales	Por determinar
	T1590: Recopilación de información de la red de la víctima	Accede a la información de la red del objetivo a través de phishing, ingeniería social y IABs
	T1589: Recopilación de información sobre la identidad de la víctima	Accede a la información de la red del objetivo mediante phishing, ingeniería social
Desarrollo de recursos (TA0042)	T1586: Cuentas comprometidas	Compromete las cuentas existentes con técnicas como phishing, ingeniería social y, IABs
Acceso inicial (TA0001)	T1133: Vulneración de servicios remotos externos	Acceso a la red de la empresa a través de cuentas de usuario comprometidas
	T1190: Explotación de aplicaciones de cara al público	Análisis de aplicaciones de cara al público para identificar y explotar vulnerabilidades de día cero
	T1566: Phishing (Suplantación de identidad)	Envía correos electrónicos de suplantación de identidad a los objetivos para acceder a sus sistemas y extraer datos y credenciales.
	T1091: Replicación a través de medios extraíbles	Comprueba si hay unidades del sistema disponibles (a menudo se hace para infectar unidades USB)
	T1078.003: Cuentas locales	Por determinar
Ejecución (TA0002)	T1059.001: PowerShell	Por determinar
	T1059.003: Windows Command Shell	Por determinar
	T1047: Windows Management Instrumentation	Consulta la información de la BIOS (a través de WMI, Win32_Bios)

Tácticas	Técnicas	Procedimientos
	T1106: Native API	Por determinar
	T1053.003: Cron	Por determinar
	T1053.005: Scheduled Task	Por determinar
	T204.002: Archivo malicioso	Por determinar
Persistencia (TA0003)	T1098: Manipulación de cuentas	Utiliza cuentas comprometidas para escalar privilegios de admin o crear nuevas cuentas con privilegios de admin.
	T1574.001: Ejecución del registro/ carpeta de inicio	Almacena archivos en el directorio de inicio de Windows
	T1037.004: RC Scripts	Por determinar
	T1136: Crear cuenta	Utiliza cuentas comprometidas para escalar a privilegios de admin o crear nuevas cuentas con privilegios de admin.
	T1543.002: Systemd Service	Por determinar
	T1133: Servicios remotos externos	Por determinar
	T1574.002: DLL Side-Loading	Intenta cargar DLLs faltantes
	T1053.003: Cron	Por determinar
	T1053.005: Scheduled Task	Por determinar
	T1505: Componente de software de servidor	Por determinar
	T1505.001: SQL Stored Procedure	Por determinar
	T1505.003: Web Shell	Por determinar
	T1078: Cuentas válidas	Utiliza cuentas comprometidas para escalar a privilegios de admin. o crear nuevas cuentas con privilegios de admin.
	T1078.003: Cuentas locales	Utiliza cuentas comprometidas para escalar a privilegios de admin. o crear nuevas cuentas con privilegios de admin.
Escalado de privilegios (TA00 04)	T1548.002: Evasión del control de cuentas de usuario	Ejecuta código malicioso con privilegios de administrador
	T1098: Manipulación de cuentas	Utiliza cuentas comprometidas para escalar a privilegios de admin. o crear nuevas cuentas con privilegios de admin.
	T1574.001: Ejecución del registro/ carpeta de inicio	Almacena archivos en el directorio de inicio de Windows
	T1037.004: RC Scripts	Por determinar
	T1543.002: Systemd Service	Por determinar
	T1068: Explotación para escalada de privilegios	Explota vulnerabilidades conocidas en software o aplicaciones para escalar privilegios
	T1574.002: DLL Side-Loading	Intenta cargar DLLs faltantes
	T1053.003: Cron	Por determinar

Tácticas	Técnicas	Procedimientos
	T1053.005: Scheduled Task	Elimina las instantáneas de volumen para impedir la recuperación del sistema
	T1078.003: Cuentas locales	Utiliza cuentas comprometidas para escalar a privilegios de admin. o crear nuevas cuentas con privilegios de admin.
Defense Evasion (TA0005)	T1222.002: Modificación de permisos de archivos y directorios de Linux y Mac	Por determinar
	T1497.001: System Checks	Hace referencia a cadenas anti-VM dirigidas a Xen
	T1078: Cuentas válidas	Utiliza cuentas comprometidas para escalar a privilegios de admin. o crear nuevas cuentas con privilegios de admin.
	T1078.003: Cuentas locales	Utiliza cuentas comprometidas para escalar a privilegios de admin. o crear nuevas cuentas con privilegios de admin.
	T1218.007: Msiexec	Por determinar
	T1218.010: Regsvr32	Por determinar
	T1218.011: Rundll32	Por determinar
	T1553.002: Code Signing	Por determinar
	T1112: Modify Registry	Utiliza claves de registro para establecer persistencia y desactivar sistemas de seguridad en sistemas infectados
	T1070.002: Borrar registros del sistema Linux o Mac	Por determinar
	T1574.002: DLL Side-Loading	Intenta cargar DLLs faltantes
	T1140: Desofuscar/Decodificar archivos o información	Por determinar
	T1622: Debugger Evasion	La muestra puede tener en cuenta la MV o el depurador; consulta la información del disco (a menudo se utiliza para detectar máquinas virtuales)
	T1548.002: Bypass User Account Control	Ejecuta código malicioso con privilegios de administrador.
Acceso a credenciales (TA0006)	T1003.001: LSASS Memory	Por determinar
	T1552.007: Container API	Por determinar
Discovery (TA0007)	T1622: Debugger Evasion	La muestra puede ser consciente de la máquina virtual o del depurador; consulta información del disco (a menudo se utiliza para detectar máquinas virtuales)

Tácticas	Técnicas	Procedimientos
	T1083: File and Directory Discovery	Enumera el sistema de archivos, lee archivos INI, enumera archivos en Windows, enumera archivos recursivamente y obtiene el tamaño de los archivos.
	T1135: Network Share Discovery	Enumera recursos compartidos de red
	T1057: Process Discovery	Consulta una lista de todos los procesos en ejecución y enumera procesos
	T1012: Query Registry	Consulta o enumera valores del registro y consulta o enumera claves del registro
	T1082: System Information Discovery	Consulta la información de la BIOS (a través de WMI, Win32 Bios), consulta la información de volumen (nombre, número de serie, etc.) de un dispositivo, lee políticas de software y obtiene información de disco
	T1497.001: System Checks	Por determinar
Movimiento lateral (TA0008)	T1021.002 SMB/Windows Admin Shares	Por determinar
	T1021.002 SSH	Por determinar
	T1021.006 Windows Remote Management	Por determinar
	T1091: Replication Through Removable Media	Comprueba si hay unidades de sistema disponibles (a menudo se hace para infectar unidades USB)
	T1021.001: Remote Desktop Protocol	Por determinar
Collection (TA0009)	T1005: Data from Local System	Recopila información de disco
Command and Control (C2) (TA0011)	T1071.001: Web Protocols	Utiliza el protocolo de capa de aplicación para descargar malware y claves de cifrado
	T1573.001: Symmetric Cryptography	
	T1105: Ingress Tool Transfer	Por determinar
	T1104: Multi-Stage channels	Por determinar
	T1571: Non-Standard Port	Por determinar
Exfiltración (TA0010)	T1041: Exfiltration Over C2 Channel	Establece conexión con el servidor C2 a través de HTTPS para descargar el malware y las claves de cifrado
	T1052.001: Exfiltration Over USB	Comprueba si hay unidades del sistema disponibles (a menudo se hace para infectar unidades USB)
	T1567.002: Exfiltration to Cloud Storage	Por determinar
Impacto (TA00 40)	T1485: Data Destruction	Por determinar
	T1486: Data Encrypted for Impact	Por determinar
	T1565: Data Manipulation	Por determinar
	T1496: Resource Hijacking	Por determinar
	T1489: Service Stop	Por determinar

Indicadores de compromiso (IoC):

Hashes:

- 004ba25f40b641a3a276b84ebdc44971
- 00773e87ad74417abaf825839c4dd014
- 00a276d2a09a49b684237013d26a91dc
- 00a60855a14e458896d70c052e22e11c
- 00e815ade8f3ad89a7726da8edd168df13f96ccb6c3daaf995aa9428bfb9ecf
- 010428443d5547a58995767d14d1c785
- 013f0f61bf96431e8a10e3cb982f4af5
- 01a0e1d97f97455a8da6012977169b40
- 01dc7dc6ad774b39a36d13d55d273a52

Internet Domain Name:

- 4ad.onion
- abcwdl.co.uk
- aclara.com
- adaresec.com
- aha.org
- ajoomal.com
- alektum.com
- alogent.com
- amerisave.com
- amf.se
- androidauthority.com
- antiy.cn
- arrow.com
- awaze.com
- axisbank.com

Malware Signature:

- BlackByte Ransomware
- IceFire Ransomware
- Conti Ransomware
- Akira Ransomware
- AtomSilo Ransomware
- Money Message Ransomware
- Karma Ransomware
- Snatch
- AvosLocker Ransomware
- Black Kingdom Ransomware
- Monti Ransomware
- Rorschach

IP Address:

- 103.151.172.28
- 109.172.45.28
- 109.172.45.77
- 141.98.82.201
- 143.244.188.172
- 146.70.116.20
- 147.78.47.219
- 147.78.47.231
- 147.78.47.235
- 147.78.47.241
- 157.230.143.100
- 158.255.2.244
- 158.255.2.245
- 158.255.225.25

Mentioning the CVEs, etc.:

- CVE-2021-30116
- CVE-2023-27532
- CVE-2023-40044
- CVE-2023-36884
- CVE-2018-4878
- CVE-2017-0144
- CVE-2017-11882
- CVE-2022-41040
- CVE-2019-11043
- CVE-2023-20269
- CVE-2021-26084
- CVE-2021-34527
- CVE-2023-3519
- CVE-2019-19781
- CVE-2023-28252
- CVE-2019-15846
- CVE-2021-45105
- CVE-2019-7192

5.1.13 Recomendaciones técnicas/tácticas de CL0P

Las siguientes recomendaciones tácticas están diseñadas para proporcionar mitigaciones técnicas a las técnicas de MITRE ATT&CK de CL0P. Las técnicas se clasifican en función del nivel de criticidad, determinado por su impacto y riesgo potenciales para la continuidad del negocio, la seguridad de los datos y la resistencia operativa.

Basadas en el gráfico de conocimientos de mitigación D3FEND de MITRE, estas recomendaciones esbozan instrucciones prescriptivas, resultados deseados y consideraciones clave para la implementación y la asignación de recursos. Estas recomendaciones no pretenden ser exhaustivas, sino más bien las más adecuadas para mitigar la respectiva técnica ATT&CK.

Recomendaciones sobre técnicas de ataque de alta criticidad:

T1190 (Explotación de aplicaciones de cara al público)

1. Despliegue y configuración de cortafuegos de aplicaciones web (WAF) para filtrar el tráfico malicioso: Desplegar y configurar cortafuegos de aplicaciones web (WAF) para filtrar el tráfico malicioso: Implementar WAFs para inspeccionar y bloquear intentos de exploits dirigidos a aplicaciones web, incluyendo inyección SQL, cross-site scripting (XSS) y ejecución remota de código (RCE). Configurar conjuntos de reglas para detectar patrones de ataque conocidos y comportamientos de solicitud anómalos. Actualizar periódicamente las políticas WAF para hacer frente a las amenazas emergentes y reducir los falsos positivos. Los WAF proporcionan una capa esencial de protección al filtrar el tráfico de exploits antes de que llegue a la aplicación.

2. Segmentar los servicios de cara al exterior de los sistemas internos: Utilizar una zona desmilitarizada (DMZ) o una infraestructura de alojamiento aislada para separar las aplicaciones de cara al público de las redes internas. Aplicar reglas estrictas de cortafuegos para controlar el flujo de tráfico entre estos segmentos y limitar la exposición de los recursos sensibles. Implementar controles de acceso para evitar el movimiento lateral de los servicios comprometidos. La segmentación de la red reduce la superficie de ataque y mitiga el impacto de una brecha exitosa.

3. Escanear y parchear regularmente las aplicaciones orientadas al exterior: Se recomienda llevar a cabo análisis frecuentes de vulnerabilidades en los sistemas expuestos al público con el fin de identificar posibles deficiencias antes de que sean explotadas por actores malintencionados. Asimismo, resulta fundamental establecer un proceso estructurado de gestión de parches que garantice la aplicación oportuna de actualizaciones de seguridad, dando prioridad a aquellas que abordan vulnerabilidades críticas. Para ello, se sugiere el uso de herramientas automatizadas que permitan supervisar las versiones de software y asegurar el cumplimiento de las políticas de actualización. La adopción de estrategias proactivas de escaneo y parcheo constituye una medida eficaz para reducir el riesgo de explotación de vulnerabilidades previamente identificadas.

T1566 (Phishing)

1. Implementar soluciones avanzadas de filtrado del correo electrónico para detectar y bloquear los intentos de phishing: Implemente puertas de enlace de correo electrónico seguras (SEG) con funciones de filtrado basadas en IA para analizar los encabezados del correo electrónico, el contenido del cuerpo y los archivos adjuntos en busca de indicadores de phishing. Configure reglas para bloquear o marcar los correos electrónicos que contengan enlaces sospechosos, archivos adjuntos inesperados o intentos de suplantación de identidad. Utilice fuentes de información sobre amenazas para actualizar los mecanismos de filtrado frente a la evolución de las tácticas de phishing. El filtrado avanzado reduce la probabilidad de que los correos electrónicos de phishing lleguen a los usuarios finales.

2. Combinar la detección de homogeneidad con la formación de los usuarios para evitar los ataques de suplantación de dominio: Despliegue herramientas que detecten la similitud de dominios para identificar dominios parecidos utilizados en campañas de phishing. Implemente una supervisión continua para detectar dominios recién registrados que imiten dominios internos o de confianza. Imparta sesiones de formación periódicas a los empleados para concienciarlos sobre las tácticas de ingeniería social, las técnicas de manipulación de dominios y los indicadores de correo electrónico sospechoso. Proporcione ejercicios prácticos, simulaciones de phishing y ejemplos del mundo real para reforzar las habilidades de reconocimiento. Un enfoque combinado de detección automática y usuarios formados reduce significativamente el riesgo de ser víctima de la suplantación de dominios y los ataques de spear-phishing.

3. Implantar mecanismos anti-spoofing y de autenticación del correo electrónico para verificar la legitimidad del remitente: Implemente un marco de política de remitentes (SPF) para verificar los remitentes de correo electrónico

autorizados; DomainKeys Identified Mail (DKIM) para garantizar la integridad de los mensajes; y Domain-Based Message Authentication, Reporting, and Conformance (DMARC) para definir políticas de gestión de correos electrónicos no autorizados. Aplique estos mecanismos de autenticación dentro de la organización y anime a los socios externos a adoptarlos. Configure las políticas de seguridad del correo electrónico para rechazar o poner en cuarentena los mensajes que no superen las comprobaciones de autenticación. Estas medidas reducen el riesgo de suplantación de identidad por correo electrónico y de ataques de suplantación de identidad basados en phishing.

T1078 (Cuentas válidas - Cuentas de dominio)

1. Supervisar continuamente las cuentas de dominio en busca de accesos no autorizados: Implemente herramientas de análisis del comportamiento de los usuarios (UBA) y de detección de anomalías para identificar desviaciones en los patrones de inicio de sesión, como ubicaciones inusuales, intentos fallidos excesivos o inicios de sesión fuera del horario laboral. Configure alertas automáticas para actividades sospechosas e intégrelas con una plataforma de gestión de eventos e información de seguridad (SIEM) para su investigación. La supervisión proactiva ayuda a detectar cuentas comprometidas antes de que puedan ser explotadas.

2. Imponer la autenticación estricta y el acceso con menos privilegios: Exija la autenticación multifactor (MFA) para todas las cuentas con privilegios y aplique controles de acceso basados en funciones (RBAC) para limitar los permisos de las cuentas. Implemente controles de acceso justo a tiempo (JIT) para las cuentas con privilegios elevados a fin de minimizar los riesgos de acceso persistente. Revisar y desactivar periódicamente las cuentas inactivas para reducir las posibles superficies de ataque. Estas medidas limitan la capacidad de los adversarios para explotar credenciales válidas para el movimiento lateral.

3. Revisar y gestionar regularmente las cuentas de dominio: Realice auditorías periódicas de las cuentas de dominio para garantizar que sólo existen cuentas activas y necesarias. Implemente una gestión automatizada del ciclo de vida para la creación, modificación y desactivación de cuentas en base a las funciones del usuario y su situación laboral. Aplique procedimientos estrictos de desvinculación para desactivar inmediatamente las cuentas cuando los empleados abandonen la organización. Reducir las cuentas innecesarias ayuda a evitar que los adversarios aprovechen las credenciales inactivas.

T1041 (Filtración a través del canal C2)

1. Implantar filtros de tráfico entrante y saliente en los límites de la red, aplicando estrictos controles de salida a los destinos y protocolos conocidos: Implemente el filtrado en la capa de aplicación para permitir sólo los protocolos de transferencia de datos autorizados y bloquear los servicios de los que más se abusa. Configure reglas de filtrado para segmentar las distintas unidades de negocio, especialmente las que manejan datos financieros confidenciales, manteniendo registros de todos los intentos de conexión bloqueados. Considere el impacto en el rendimiento del tráfico empresarial legítimo y asigne recursos suficientes para el filtrado en tiempo real sin introducir latencia.

2. Establecer perfiles de referencia de los patrones normales de comunicación cliente-servidor específicos de las aplicaciones de servicios financieros y los flujos de datos: Despliegue soluciones de supervisión que puedan analizar las características de la carga útil (por ejemplo, tamaño, frecuencia y entropía) en todas las comunicaciones cliente-servidor. Configure alertas automatizadas para cualquier desviación estadística que pudiera indicar intentos de filtración de datos, al tiempo que mantiene perfiles históricos para el análisis de tendencias. Considerar los recursos computacionales necesarios para la elaboración de perfiles en tiempo real y el impacto potencial en el rendimiento del sistema.

3. Implementar una recopilación y un análisis exhaustivos de metadatos de protocolo centrados en las características de la sesión, los patrones de temporización y los atributos específicos del protocolo: Despliegue capacidades de análisis en tiempo real que puedan identificar valores estadísticos atípicos en el uso de protocolos, en particular protocolos que podrían utilizarse para la exfiltración de datos. Establezca umbrales adaptables basados en patrones históricos de uso de protocolos, manteniendo al mismo tiempo registros detallados para análisis forenses. Tenga en cuenta los requisitos de almacenamiento para la recopilación de metadatos y la sobrecarga de procesamiento para el análisis en tiempo real.

T1003.001 (LSASS Memory Dumping – Credential Theft)

1. Desplegar herramientas de monitoreo de procesos que rastreen específicamente los intentos de spawn dirigidos al espacio de memoria del servicio del subsistema de autoridad de seguridad local (LSASS) y los procesos del sistema relacionados: Configure el registro detallado

de los atributos del proceso (por ejemplo, contexto del usuario, ruta de la imagen y contenido de seguridad) para todos los eventos de creación de procesos. Implementar alertas automatizadas para cualquier intento de creación de procesos no autorizados dirigidos a LSASS, manteniendo al mismo tiempo listas blancas para herramientas de seguridad legítimas. Considerar la sobrecarga de procesamiento de la monitorización continua de procesos y los requisitos de almacenamiento para los registros de creación de procesos.

2. Implementar mecanismos de aislamiento basados en hardware utilizando tecnologías como IOMMU para prevenir el acceso no autorizado a la memoria entre procesos: Configure estrictos controles de acceso a la memoria que impidan el acceso directo al espacio de procesos de LSASS desde fuentes no autorizadas. Despliegue soluciones de monitorización para rastrear cualquier intento de violación de los límites de aislamiento de procesos, manteniendo al mismo tiempo la continuidad del negocio para los procesos de autenticación legítimos. Considere los requisitos de hardware y el impacto potencial en el rendimiento de los recursos del sistema.

3. Configurar respuestas automatizadas de terminación de procesos para cualquier proceso no autorizado que intente acceder al espacio de memoria LSASS: Implemente controles de acceso y permisos adecuados para las capacidades de terminación de procesos, garantizando al mismo tiempo que las herramientas de seguridad legítimas sigan funcionando. Configure el registro y las alertas para todos los eventos de terminación de procesos con un contexto detallado sobre el proceso terminado y la razón de la terminación. Tenga en cuenta el impacto potencial de los falsos positivos y establezca procedimientos de escalado claros para los equipos de seguridad.

Recomendaciones para técnicas de ataque de riesgo moderado a alto:

T1059.001 (Ejecución de PowerShell)

1. Configurar la política de ejecución de PowerShell para que sólo permita scripts firmados: Configure PowerShell para que sólo permita la ejecución de scripts firmados, evitando la ejecución de scripts no fiables o maliciosos. Restrinja el uso de PowerShell a los administradores para limitar la superficie de ataque. Hacer esto reduce la probabilidad de ataques maliciosos basados en PowerShell.

2. Deshabilitar o restringir el servicio de administración remota de Windows (WinRM) para evitar la ejecución remota: Deshabilite o limite el acceso al servicio WinRM para evitar que los atacantes ejecuten PowerShell de forma remota. Utilice reglas de cortafuegos para restringir el acceso a WinRM únicamente a hosts de confianza. Al hacerlo, se evita el uso no autorizado de PowerShell para la ejecución remota de comandos.

3. Utilizar el modo de lenguaje restringido de PowerShell y el control de aplicaciones: Active el modo de lenguaje restringido de PowerShell para restringir el acceso a funciones confidenciales, como la ejecución de API de Windows arbitrarias. Utilice herramientas de listas blancas de aplicaciones para controlar qué aplicaciones y secuencias de comandos pueden ejecutarse, reduciendo así las posibilidades de abuso. De este modo, se reduce el riesgo de que PowerShell se utilice para actividades maliciosas.

T1068 (Explotación para la escalada de privilegios)

1. Evaluar y remediar regularmente las vulnerabilidades del sistema: Realice escaneos rutinarios de vulnerabilidades y evaluaciones manuales de seguridad para identificar y mitigar las debilidades del sistema. Implemente un proceso estructurado de gestión de parches para abordar los fallos de seguridad críticos antes de su explotación. Utilice herramientas de gestión de la configuración para hacer cumplir las líneas básicas de seguridad y endurecer las directrices. Las evaluaciones periódicas ayudan a reducir la superficie de ataque y garantizan el cumplimiento de las políticas de seguridad

2. Restringir los servicios innecesarios y aplicar el mínimo privilegio: Desactive los servicios no esenciales del sistema y restrinja el uso de herramientas administrativas para minimizar los posibles vectores de ataque. Implemente soluciones RBAC y de gestión de privilegios para aplicar el principio del mínimo privilegio. Revise periódicamente los permisos de los usuarios y elimine los derechos de acceso excesivos para reducir las oportunidades de movimiento lateral. Estas medidas reducen significativamente el riesgo de escalada de privilegios.

3. Desplegar controles de detección y mitigación de exploits: Habilite mecanismos de seguridad como la verificación de la integridad del núcleo, los marcos de protección de exploits y la prevención de ataques basados en memoria. Utilice soluciones de detección y respuesta de puntos finales (EDR) para supervisar los indicadores de comportamiento de los intentos de escalada de privilegios. Configure el registro y las alertas para detectar y responder a inyecciones de procesos sospechosos o modificaciones no autorizadas. Estas técnicas mejoran la resistencia del sistema frente a los intentos de explotación.

T1021.001 (Protocolo de escritorio remoto)

1. Restringir y supervisar el acceso al protocolo de escritorio remoto (RDP): Limite el acceso RDP aplicando la segmentación de la red y reglas de cortafuegos que bloqueen las conexiones externas innecesarias. Exija VPN o acceso de red de confianza cero para el uso de escritorios remotos y aplique MFA para todas las sesiones RDP. Implemente controles de acceso estrictos mediante listas de direcciones IP autorizadas. Estas restricciones reducen la exposición a ataques de fuerza bruta e intentos de acceso no autorizados.

2. Detección y análisis de actividad RDP anormal: Despliegue herramientas de supervisión de red para analizar patrones de sesión RDP, incoherencias de geolocalización y excesivos intentos de inicio de sesión fallidos. Utilice la detección de anomalías basada en host y red para identificar comportamientos sospechosos, como inicios de sesión administrativos inesperados o conexiones persistentes. Implemente mecanismos de alerta para actividades RDP inusuales que permitan una investigación y respuesta rápidas. La supervisión reduce el tiempo de espera y ayuda a identificar posibles intrusiones.

3. Auditar y controlar las herramientas de acceso remoto: Mantenga un inventario estricto de las aplicaciones de acceso remoto aprobadas y prohíba el uso de herramientas no autorizadas mediante listas blancas de aplicaciones. Audite periódicamente los registros de los puntos finales y de la red en busca de indicadores de intentos de acceso remoto no autorizados. Aplique políticas de control de ejecución para evitar que se ejecute software de acceso remoto portátil no aprobado. De este modo se garantiza que sólo se utilicen las herramientas de gestión remota autorizadas, lo que reduce el riesgo de peligro.

T1021.002 (SMB/Comparticiones de administración de Windows)

1. Filtrar y supervisar el tráfico de red SMB para detectar accesos no autorizados: Aplique reglas de segmentación de red y cortafuegos para restringir el tráfico SMB sólo a los sistemas autorizados. Supervise los registros de autenticación SMB y detecte patrones de acceso anómalos, como conexiones inesperadas o un número excesivo de intentos de inicio de sesión fallidos. Analizar el tráfico ayuda a prevenir el acceso no autorizado y la filtración de datos a través de SMB.

2. Denegar el uso remoto de credenciales de administrador local para iniciar sesión en los sistemas: Restrinja el uso de cuentas de administrador local para inicios de sesión remotos aplicando la configuración de directivas de grupo e implementando la solución de contraseña de administrador local (LAPS). Asegúrese de que se utilizan contraseñas únicas y complejas para cada cuenta de administrador local del sistema. Evitar la reutilización de credenciales reduce el riesgo de movimiento lateral si una cuenta se ve comprometida.

3. Supervisar los intentos de ejecución remota mediante WMI y recursos compartidos SMB: Implemente la supervisión de extremos para detectar el uso de la clase Win32_Process de WMI y la creación de procesos remotos a través de SMB. Correlacione la actividad con técnicas de ataque conocidas para identificar posibles movimientos laterales o intentos de ejecución remota de código. La detección temprana de comportamientos anómalos ayuda a evitar que el sistema se vea comprometido sin autorización.

T1574.002 (Carga lateral de DLL)

1. Aplicar controles estrictos de las aplicaciones para evitar la ejecución no autorizada de bibliotecas de vínculos dinámicos (DLL): Utilice listas blancas de aplicaciones para permitir que sólo se ejecuten aplicaciones y bibliotecas de confianza. Implemente la verificación de firma de código para evitar la ejecución de DLL no firmadas o manipuladas. Restringir la ejecución de DLL garantiza que los adversarios no puedan explotar controles de aplicación débiles para la persistencia.

2. Actualizar periódicamente el software para parchear las vulnerabilidades de carga lateral de DLL: Mantenga un proceso eficaz de gestión de parches para abordar los riesgos conocidos de carga lateral de DLL. Revise las dependencias de las aplicaciones y elimine o sustituya las bibliotecas vulnerables por versiones seguras. Mantener el software actualizado reduce el riesgo de que los adversarios exploten mecanismos de carga de DLL obsoletos.

3. Habilitar detecciones basadas en el comportamiento para identificar técnicas de carga lateral de DLL: Utilice las funciones EDR para detectar anomalías como la carga de DLL en un proceso desde directorios no estándar, la inyección inesperada de DLL en aplicaciones con privilegios elevados o patrones anómalos de acceso a la memoria. Implemente detecciones heurísticas y basadas en aprendizaje automático para detectar desviaciones del comportamiento normal de carga de DLL.

T1548.002 (Anular el control de cuentas de usuario)

1. Refuerce la configuración del control de cuentas de usuario (UAC) y supervise los intentos de eludirlo: Habilite UAC en modo "Siempre notificar" para requerir aprobación explícita para acciones administrativas. Realice evaluaciones periódicas para identificar sistemas con configuraciones UAC deficientes y aplique las mejores prácticas de seguridad. Desactivar la auto-elevación evita que los atacantes aprovechen las utilidades del sistema para eludir los controles UAC. Reforzar las configuraciones UAC reduce la superficie de ataque y minimiza los intentos no autorizados de escalada de privilegios.

2. Supervisar la ejecución de procesos para detectar intentos sospechosos de eludir el UAC: Rastree la ejecución de herramientas y procesos conocidos de elusión de UAC, como eventvwr.exe y sdclt.exe, que pueden elevar privilegios sin el consentimiento del usuario. Implemente reglas de detección de puntos finales para correlacionar la ejecución de procesos con eventos de elevación de privilegios y detectar comportamientos anómalos. Las organizaciones deben utilizar análisis de comportamiento para identificar patrones indicativos de técnicas de elusión de UAC. La detección temprana de intentos no autorizados de elevación de privilegios permite una respuesta y mitigación oportunas.

3. Implementar listas de denegación de ejecutables para evitar la elevación de privilegios no autorizada: Utilice políticas de control de aplicaciones para bloquear la ejecución de utilidades administrativas no fiables de las que se suele abusar para eludir el UAC. Mantenga una lista de denegación actualizada de las técnicas de elusión conocidas para mitigar las amenazas de forma proactiva. Aplique políticas de ejecución estrictas utilizando controles de seguridad del sistema operativo para bloquear la ejecución de binarios de alto riesgo por parte de usuarios no administrativos. Impedir la ejecución de aplicaciones maliciosas o no aprobadas reduce la superficie de ataque y refuerza la seguridad del terminal.

T1133 (Servicios remotos externos)

1. Implementar controles automatizados de terminación de sesión para todos los servicios remotos externos, incluyendo VPN y herramientas de gestión remota con estrictos parámetros de tiempo de espera: Configure la desconexión forzosa de la sesión tras un periodo de inactividad, manteniendo al mismo tiempo registros detallados de todos los eventos de finalización con fines de auditoría. Asegúrese de que las políticas de finalización de sesión tienen en cuenta las necesidades legítimas de la empresa al tiempo que evitan la persistencia no autorizada a través de sesiones abandonadas. Considere el impacto en la productividad del usuario y establezca canales de comunicación claros para los usuarios que requieran sesiones prolongadas.

2. Implementar la segmentación de la red utilizando proxies, gateways y firewalls para controlar y supervisar todas las rutas de acceso remoto a la red: Despliegue un enfoque de defensa en profundidad que fuerce todas las conexiones remotas a través de puntos de control de seguridad designados mientras se mantienen registros de acceso detallados. Configure estrictos controles fronterizos que impidan el acceso remoto directo a los sistemas internos, garantizando al mismo tiempo la continuidad del negocio a través de canales de acceso debidamente protegidos. Considere la complejidad de implementar la segmentación y el impacto potencial en el rendimiento de la red y las necesidades legítimas de acceso remoto.

3. Implantar la MFA para todas las cuentas de servicios remotos externos, incluidas las VPN y las herramientas de gestión remota: Implemente una solución MFA sólida que combine múltiples factores de autenticación, al tiempo que es consciente de las posibles técnicas de interceptación de MFA. Configure el registro detallado de todos los intentos de autenticación al tiempo que mantiene los procedimientos adecuados para gestionar los problemas o bloqueos legítimos de la MFA. Considere el impacto en la experiencia del usuario, los requisitos de recursos de soporte y la necesidad de métodos de autenticación de respaldo para escenarios de acceso crítico.

Riesgo de sigilo y persistencia (evasión y compromiso a largo plazo):

T1140: (Desofuscar/Decodificar archivos o información)

1. Supervisar y registrar la ejecución de procesos para detectar intentos de extracción o descifrado de archivos: Implementar la supervisión de procesos para detectar la ejecución de utilidades de extracción de archivos y scripts que intenten descifrar o manipular archivos. Correlacione la actividad con modificaciones no autorizadas de archivos o comportamientos inesperados del sistema para identificar posibles actividades maliciosas al tiempo que reduce los falsos positivos.

2. Restringir y validar la ejecución de scripts para evitar intentos de descifrado no autorizados: Configure el registro para capturar las ejecuciones de secuencias de comandos, especialmente las que se producen fuera de las tareas administrativas

estándar. Restrinja la ejecución no autorizada de scripts y analice los scripts capturados para detectar posibles intenciones maliciosas. Supervisar la actividad de los scripts ayuda a identificar los intentos de los adversarios de automatizar la ofuscación o la descodificación de la carga útil.

3. Detección y bloqueo del uso indebido de las utilidades integradas utilizadas habitualmente para la ofuscación: Supervise el uso de las utilidades integradas en el sistema que pueden aprovecharse para descifrar, extraer o modificar archivos. Establezca alertas para ejecuciones no autorizadas o inesperadas y correlaciónelas con la actividad del sistema. Detectar a tiempo el uso indebido de estas utilidades puede evitar el acceso no autorizado a los datos y la ejecución de código malicioso.

T1070.002: (Clear Linux o Mac System Logs)

1. Cifrar y centralizar el almacenamiento de registros: Utilice protocolos de cifrado potentes para proteger los registros del sistema en reposo y en tránsito, evitando modificaciones no autorizadas. Implemente soluciones de registro centralizadas que reenvíen los registros a un almacenamiento remoto seguro con mecanismos de verificación de integridad, como hashing criptográfico. Los registros cifrados y centralizados garantizan la integridad forense y evitan que los atacantes manipulen las pruebas.

2. Aplicar estrictos controles de acceso a los registros: Aplique permisos de archivo granulares para restringir los derechos de modificación y eliminación de registros a los procesos y administradores del sistema autorizados. Implemente marcos de control de acceso obligatorio (MAC) para hacer cumplir las políticas de seguridad a nivel del sistema operativo. Auditar periódicamente los permisos de acceso a los registros para identificar y mitigar posibles abusos de privilegios. Estos controles ayudan a evitar que los atacantes borren las pruebas forenses.

3. Supervisar y alertar de los intentos de manipulación de los registros: Configure herramientas de supervisión de la seguridad para realizar un seguimiento de las modificaciones, eliminaciones y actividades de limpieza inesperadas de los archivos de registro. Implemente mecanismos de alerta en tiempo real para notificar a los equipos de seguridad cuando se detecte una manipulación no autorizada de los registros. Correlacione los eventos de registro a través de múltiples fuentes para identificar patrones de actividad maliciosa. La supervisión continua ayuda a detectar y mitigar las amenazas antes de que se intensifiquen.

T1574.00: (Carpeta de inicio/ejecución del registro)

1. Desplegar una supervisión de la integridad de los archivos centrada en las claves de ejecución del Registro de Windows y en la ubicación de la carpeta de inicio con alertas en tiempo real/ casi real en caso de modificaciones: Implemente comparaciones de línea de base que rastreen cualquier cambio en las ubicaciones de inicio automático mientras mantiene registros de auditoría detallados de todas las modificaciones. Configure listas blancas para las entradas de inicio conocidas como buenas, garantizando al mismo tiempo procedimientos adecuados de gestión de cambios para las modificaciones legítimas. Tenga en cuenta el impacto en el rendimiento de la supervisión continua y los requisitos de almacenamiento de los registros de auditoría.

2. Implementar controles estrictos de listas blancas de aplicaciones que impidan que se añadan ejecutables no autorizados a las ubicaciones de inicio o a las claves de ejecución: Configure políticas que sólo permitan que las aplicaciones de confianza/firmadas continúen a través de los procedimientos de inicio, manteniendo al mismo tiempo un inventario exhaustivo de las aplicaciones aprobadas. Configure alertas automáticas para cualquier intento de violación de las políticas de listas permitidas, al tiempo que garantiza la continuidad del negocio para las actualizaciones de software legítimas. Considere la sobrecarga administrativa de mantener listas de permitidos y el impacto en los procesos de despliegue de software.

3. Desplegar una supervisión continua de las configuraciones de inicialización del sistema relacionadas con el registro y la carpeta de inicio: Implemente capacidades de análisis que puedan detectar cambios anómalos en las configuraciones de inicio, manteniendo al mismo tiempo líneas de base de entradas de inicio legítimas. Configurar respuestas automatizadas a los cambios de configuración no autorizados.

T1078.003: (Cuentas locales - Persistencia)

1. Supervisar los patrones de creación, modificación y uso de cuentas locales en todos los sistemas: El despliegue de alertas en tiempo real para actividades sospechosas de cuentas locales puede ayudar a detectar posibles actividades maliciosas asociadas con el uso fuera de horario, la escalada de privilegios no autorizada o patrones de acceso inusuales. Configure un registro detallado de todas las operaciones de las cuentas locales, manteniendo al mismo tiempo las líneas de base del comportamiento normal de las cuentas. Tenga en cuenta los requisitos de almacenamiento de los registros de actividad de las cuentas y la sobrecarga de procesamiento para el análisis en tiempo real.

2. Implementar el bloqueo automático de cuentas activado por actividades sospechosas o infracciones de las políticas en cuentas locales: Implemente políticas de bloqueo progresivo que aumenten la duración del bloqueo con infracciones repetidas, manteniendo al mismo tiempo los procedimientos adecuados para el desbloqueo legítimo de cuentas. Configure notificaciones para los equipos de seguridad cuando las cuentas se bloqueen debido a actividades sospechosas, garantizando al mismo tiempo la continuidad del negocio mediante procedimientos adecuados de acceso de copia de seguridad para los servicios críticos. Aunque los mecanismos de bloqueo pueden desalojar a los actores de amenazas, hay que tener en cuenta el impacto en los usuarios legítimos y los protocolos de recursos del servicio de asistencia para las solicitudes seguras de desbloqueo de cuentas.

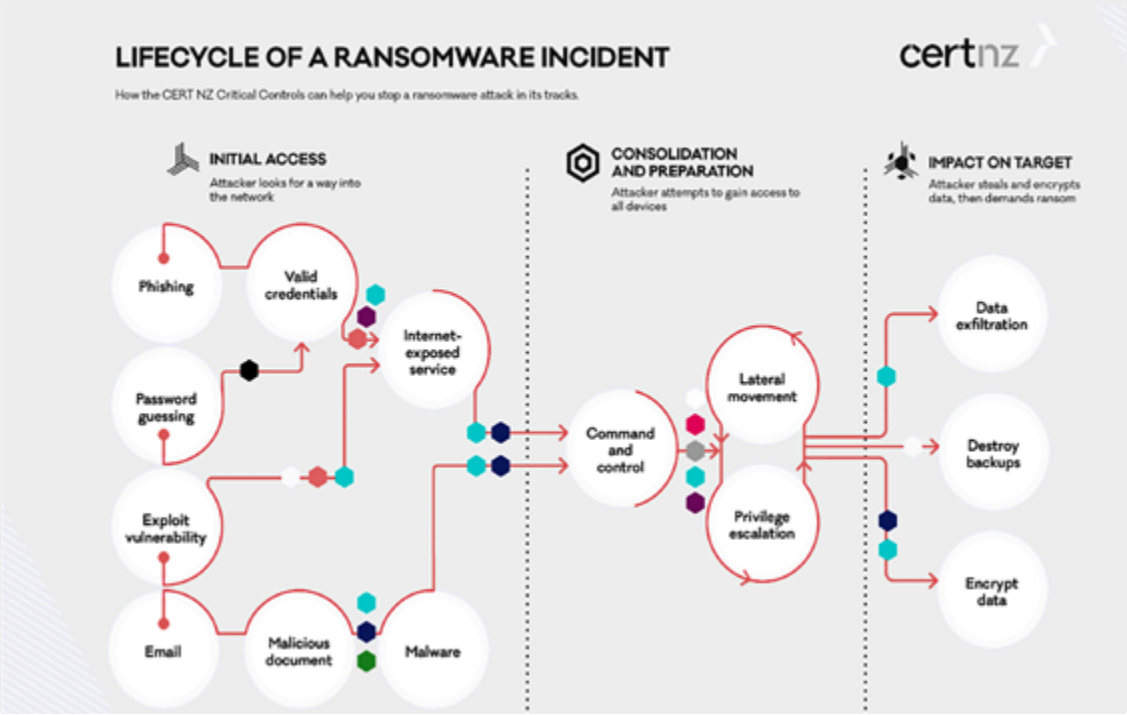
3. Implemente estrictos controles de permisos y restricciones de acceso para todas las cuentas locales basándose en el principio del mínimo privilegio (PoLP): Configure revisiones periódicas de los permisos y la detección automatizada de cambios de privilegios no autorizados, al tiempo que mantiene una documentación detallada de los niveles de acceso aprobados. Establezca alertas para cualquier intento de modificar los permisos de las cuentas, garantizando al mismo tiempo procedimientos adecuados de gestión de cambios para las actualizaciones legítimas de permisos. Tenga en cuenta la sobrecarga administrativa de la gestión de permisos granulares y el impacto en la eficiencia operativa.

5.2 LockBit

5.2.1 Actividad relevante del actor de amenazas

LockBit es un grupo de ransomware muy activo que ataca principalmente a empresas medianas y grandes, como Royal Mail, Ion Group y TSMC.[203] El grupo obtiene acceso inicial a las redes objetivo a través de accesos comprados, vulnerabilidades sin parchear, acceso interno y exploits de día cero. LockBit está diseñado para operar en Estados Unidos, Canadá, Europa, Asia y Latinoamérica. A finales de febrero de 2024, LockBit sufrió un importante desmantelamiento en el que se congelaron más de 200 cuentas de criptomoneda, se aplicaron sanciones y se cerraron 34 servidores y 14.000 cuentas.[204] Desde entonces, este desmantelamiento ha perturbado considerablemente las actividades de LockBit. Sin embargo, a pesar de la importante aplicación de la ley, LockBit sigue siendo la organización de ransomware más destacada.[205]

Figure 6: Ciclo de vida de un incidente de ransomware



Source: CISA[206]

[203] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware spotlight-lockbit
[204] https://globalinitiative.net/analysis/the-lockbit-takedown law-enforcement-trolls-ransomware-gang/
[205] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a
[206] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a

LockBit opera como un modelo RaaS, reclutando afiliados para ejecutar ataques de ransomware utilizando las herramientas y la infraestructura de LockBit. Esto da lugar a una variación significativa en los TTP de los distintos ataques.[207] Un método estándar utilizado por los afiliados de LockBit consiste en explotar vulnerabilidades no parcheadas o utilizar credenciales comprometidas para obtener acceso inicial a una red objetivo. Una vez dentro, a menudo despliegan herramientas como Mimikatz para extraer credenciales y escalar privilegios, permitiendo el movimiento lateral a través de la red. Los datos pueden ser alcanzados y comprometidos a través de estos métodos, lo que permite la exfiltración o cifrado de datos.

El impacto de LockBit ha sido profundo, especialmente en las instituciones financieras de América Latina, provocando importantes interrupciones y pérdidas financieras. Se informó que los grupos RaaS, incluido LockBit, han ejercido una presión continua sobre los sectores de servicios económicos y gubernamentales de la región.[208] Desde abril de 2022, países como Costa Rica, Perú, México, Ecuador, Brasil y Argentina se han enfrentado a ataques de ransomware, probablemente con la participación de actores de amenazas de habla rusa, incluido LockBit.[209]

5.2.2 Antecedentes

Lockbit se observó por primera vez en septiembre de 2019 y ha evolucionado a través de múltiples versiones, con la versión actual, LockBit 3.0, descubierta en junio de 2022. LockBit mantuvo la primera posición a lo largo de 2022, representando más de un tercio de las organizaciones víctimas en los primeros tres trimestres.[210] Lockbit mantiene una fuerte presencia en Latinoamérica. En octubre de 2022, se produjo un ransomware en un banco de Brasil utilizando el malware LockBit. Los atacantes solicitaron 50 bitcoins (el equivalente a 1 millón de dólares estadounidenses) y provocaron fugas de datos e interrupciones temporales en los servicios a los clientes.

Además de este incidente, las víctimas de LockBit abarcan diversos sectores. Entre los más significativos se encuentra el sector privado, donde LockBit ha atacado industrias que van desde las finanzas hasta la industria manufacturera.[211] El grupo también ha afectado a otros sectores de infraestructuras críticas, como la energía, la sanidad y el transporte.[212] Además, entidades gubernamentales se han visto afectadas, provocando crisis nacionales, como se ha visto en el caso de Costa Rica.[213] Estas industrias son especialmente atractivas para LockBit debido a su gran importancia, la sensibilidad de sus datos y su potencial para crear crisis nacionales. Sus considerables recursos financieros también los convierten en objetivos lucrativos, aumentando la probabilidad de que se paguen rescates.

5.2.3 Correlación

Los ataques de LockBit suelen utilizar una estrategia de doble extorsión para presionar a las víctimas a pagar, en primer lugar para recuperar el acceso a sus archivos cifrados y, en segundo lugar, para impedir que sus datos robados se hagan públicos. Esta técnica de doble extorsión, en particular, permite a LockBit no sólo beneficiarse del rescate de los datos, sino también recuperar los datos del usuario y potencialmente incluso utilizar la fuga de datos adicionales si la víctima no cumple.

LockBit y CL0P operan como RaaS, utilizando afiliados o agentes de acceso inicial (IAB) para desplegar el malware inicial o asegurar el acceso a los sistemas de una organización objetivo. Al igual que LockBit, CL0P ha adquirido notoriedad por sus ataques a gran escala, como la explotación de vulnerabilidades de día cero en software de uso generalizado como MOVEit. Además, ambos grupos utilizan técnicas como la carga lateral de DLL y mecanismos avanzados de persistencia para mantener el control de los sistemas comprometidos.

5.2.4 Técnicas, tácticas y procedimientos de LockBit

LockBit emplea sofisticados TTP para comprometer y controlar las redes de las víctimas. Para la escalada de privilegios, LockBit utiliza métodos como eludir el Control de Cuentas de Usuario (UAC) a través del método ucmDccwCOM de UACMe, aprovechando la ejecución de arranque o inicio automático de sesión y modificando las políticas de dominio a través de la directiva de grupo para permitir su control sobre los sistemas.

Además, emplea la suplantación de token para replicar y asumir los privilegios de otros procesos, provocando una infiltración más profunda en la red. LockBit también explota vulnerabilidades de zero-day y n-day para obtener acceso no autorizado y ejecutar código remoto, con casos notables que incluyen la explotación de la vulnerabilidad Fortra GoAnywhere MFT (CVE-2023-0669) y la vulnerabilidad Apache Log4j2.

[207] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a
[208] https://doi.org/102279083/1729705714101/module_128102279083_Global-Header
[209] https://www.recordedfuture.com/research/latin-american-governments targeted-by-ransomware
[210] https://global.ptsecurity.com/analytics/latam-cybersecurity-threatscape-2022-2023
[211] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a https://www.logpoint.com/wp-content/uploads/2023/07/etp-lockbit.pdf
[212] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a
[213] https://www.recordedfuture.com/research/latin-american-governments targeted-by-ransomware

LockBit utiliza herramientas como Splashtop para el acceso remoto y Cobalt Strike para navegar por las redes en movimiento lateral. Al dirigirse a los recursos compartidos SMB y utilizar Admin Shares o Domain Group Policy, los afiliados de LockBit logran un movimiento fluido a través de entornos comprometidos.

Para el mando y control, el grupo de ransomware se basa en varios protocolos y software, como FileZilla para la transferencia de archivos, ThunderShell para el acceso remoto basado en HTTP y Ligolo para crear túneles SOCKS5 seguros. Herramientas como Plink automatizan las actividades SSH, mientras que las utilizadas habitualmente en software de acceso remoto como AnyDesk y TeamViewer facilitan aún más la capacidad de LockBit para mantener el acceso a los sistemas infectados. La siguiente tabla, que representa las tácticas, técnicas y procedimientos de LockBit, muestra la flexibilidad de su funcionamiento y su persistencia, lo que supone una grave amenaza para la ciberseguridad en diversos sectores, especialmente en LATAM.[214]

Tactics	Techniques	Procedures
Ejecución (TA0002)	T1059.003: Windows Command Shell	Abusa del símbolo del sistema de Windows para acceder a casi cualquier parte del sistema
	T1072: Software Development Tools	Aprovecha los servicios del sistema para ejecutar o lanzar código malicioso como mecanismo de persistencia
	T1569.002: System Services	Utiliza PsExec para ejecutar comandos o cargas dañinas
Persistencia (TA0003)	T1547: Boot or Logon Autostart Execution	Habilita el inicio de sesión automático para la persistencia
	T1078: Valid Accounts	Utiliza cuentas de usuario comprometidas para mantener la persistencia en la red objetivo
Acceso inicial (TA0001)	T1189: Drive-By Compromise	Los afiliados a LockBit obtienen acceso a través de un usuario que visita un sitio web comprometido
	T1190: Exploit Public-Facing Application	Explota vulnerabilidades (por ejemplo, Log4Shell) en sistemas orientados a Internet.
	T1133: External Remote Services	Utiliza RDP para acceder a las redes de las víctimas.
	T1566: Phishing	Utiliza phishing y spear-phishing para obtener acceso a la red.
Escalado de privilegios (TA0004)	T1548: Abuse Elevation Control Mechanism	Utiliza técnicas para eludir el control de cuentas de usuario (UAC) (por ejemplo, el método ucmDccwCOM).
	T1547: Ejecución de arranque o inicio automático de sesión	Habilita el inicio de sesión automático para la escalada de privilegios
	T1484.001: Modificación de Políticas de Dominio: Modificación de Políticas del Grupo	Modifica la directiva de grupo para el movimiento lateral
	T1078: Cuentas válidas	Utiliza cuentas de usuario comprometidas para escalar privilegios
Defense Evasion (TA0005)	T1480.001: Execution Guardrails: Environmental Keying	Desencripta o continúa la ejecución sólo si se dan ciertos factores del entorno.

[214] https://www.logpoint.com/wp-content/uploads/2023/07/etp-lockbit.pdf

	T1562.001: Impair Defenses: Disable or Modify Tools	Desactiva las herramientas EDR (por ejemplo, mediante Backstab, Process Hacker, etc.)
	T1070.001: Eliminación de indicadores: Borrar registros de eventos de Windows	Borra los archivos del registro de sucesos de Windows para evitar su detección
	T1070.004: Eliminación de Indicadores: Eliminación de archivos	LockBit 3.0 se borra del disco tras su ejecución
	T1027: Información o archivos ofuscados	Cifra u ofusca la información del host y del bot durante la comunicación con los servidores C2
	T1027.002: Archivos o información ofuscados: empaquetado de software	Utiliza empaquetado de software o protección de máquinas virtuales para ocultar código
Acceso a credenciales (TA0006)	T1110: Fuerza bruta	Utiliza credenciales VPN o RDP de fuerza bruta para el acceso inicial
	T1555.003: Acceso a credenciales de almacenes de contraseñas: Credenciales de navegadores web	Recupera las credenciales almacenadas de Firefox utilizando PasswordFox
	T1003: OS Credential Dumping	Utiliza herramientas como ExtPassword o LostMyPassword para recuperar las credenciales del sistema
	T1003.001: OS Credential Dumping: LSASS Memory	Utiliza Microsoft Sysinternals ProDump o Mimikatz para obtener las credenciales de LSASS
Discovery (TA0007)	T1046: Network Service Discovery	Utiliza SoftPerfect Network Scanner, Advanced IP Scanner o Advanced Port Scanner para escanear las redes de las víctimas
	T1082: System Information Discovery	Enumera la información del sistema, incluido el nombre de host, la configuración y la información de dominio
	T1614.001: System Location Discovery: System Language Discovery	LockBit 3.0 evita infectar sistemas con configuraciones de idioma específicas basadas en una lista de exclusión.
Lateral Movement (TA0008)	T1021.001: Servicios remotos: Protocolo de escritorio remoto.	Utiliza Splashtop o un software de escritorio remoto similar para facilitar el movimiento lateral
	T1021.002: Servicios remotos: Server Message Block (SMB)/Admin Windows Shares	Utiliza Cobalt Strike para apuntar a los recursos compartidos SMB para el movimiento lateral
Collection (TA0009)	T1560.001: Archive Collected Data: Archive via Utility	Utiliza 7-zip para comprimir o cifrar datos antes de la exfiltración
Command and Control (TA0011)	T1071.002: Aplicación de protocolo de capa: Protocolos de transferencia de archivos	Utiliza FileZilla para comunicarse con C2
	T1071.001: Protocolo de capa de aplicación: Protocolos web	Utiliza ThunderShell para comunicarse mediante peticiones HTTP

	T1095: Protocolo de capa sin aplicación	Utiliza Ligolo para establecer túneles SOCKS5 o TCP a partir de conexiones inversas
	T1572: Protocol Tunneling	Utiliza PuTTY Link (Plink) para automatizar acciones SSH en Windows
	T1219: Software de acceso remoto	Utiliza AnyDesk, Atera RMM, ScreenConnect, o TeamViewer para acceso remoto
Exfiltración (TA0010)	T1567: Exfiltración a través del servicio web	Utiliza servicios de intercambio de archivos disponibles públicamente para filtrar datos
	T1567.002: Exfiltración por servicio web: Exfiltración a almacenamiento en la nube	Utiliza herramientas como Rclone o FreeFileSync para filtrar datos al almacenamiento en la nube (por ejemplo. g., MEGA)
Impacto (TA0040)	T1485: Destrucción de datos	Elimina los archivos de registro y vacía la papelera de reciclaje para evitar la recuperación de la información
	T1486: Datos cifrados por impacto	Cifra los datos en los sistemas de destino para interrumpir la disponibilidad de los recursos de red
	T1491.001: Desfiguración: Destrucción interna	Cambia el fondo de pantalla y los iconos del sistema a la marca LockBit
	T1490: Inhibir la recuperación del sistema	Elimina las instantáneas de volumen para evitar la recuperación del sistema
	T1489: Detención del servicio	Finaliza los procesos y servicios para facilitar el cifrado de y evitar la recuperación.

IOCs:

- Hashes de archivos.
- Direcciones IP
- Nombres de dominio
- URL maliciosas
- Notas de rescate

CVEs:

- Proxy Shell: CVE-2021-34473, CVE-2021-34523, CVE-2021-31207
- Paper Cut: CVE-2023-27350
- Citrix Bleed: CVE-2023-4966 (Latest)
- CVE-2022-22279
- CVE-2021-31207, CVE-2023-4966
- CVE-2021-22986
- CVE-2018-13379
- CVE-2021-36942
- CVE-2021-20028
- CVE-2020-0787
- CVE-2022-36537

5.2.5 Recomendaciones Técnicas/Tácticas de LockBit

Recomendaciones para las técnicas de ataque crítico con alto impacto en la seguridad de las empresas y los datos

Las recomendaciones tácticas que figuran a continuación están diseñadas para mitigar las técnicas de LockBit, siguiendo el marco ATT&CK de MITRE. Se clasifican en función del alcance de su impacto, con niveles de criticidad más altos que indican un mayor riesgo, como una posible toma de control de la red. Por lo tanto, estas recomendaciones esbozan consideraciones y acciones clave que pueden tomarse para mitigar las técnicas ATT&CK asociadas.

T1133 (Servicios remotos externos)

1. Imponer la autenticación multifactor (MFA) para todos los accesos remotos: Exija MFA y acceso remoto basado en la nube para evitar inicios de sesión no autorizados, incluso si las credenciales están comprometidas. Utilice métodos de autenticación resistentes al phishing, como FIDO2 o la autenticación basada en certificados. MFA reduce significativamente el riesgo de acceso no autorizado.

2. Restringir el acceso remoto con segmentación de red y listas de permisos: Limite el acceso remoto a los rangos de IP aprobados y aplique la segmentación de red para aislar los servicios remotos de los sistemas financieros críticos. Utilice Zero Trust Network Access (ZTNA) y controles de acceso basados en roles (RBAC) para minimizar la exposición. Restringir el acceso reduce la superficie de ataque y limita el movimiento lateral.

3. Supervisar y registrar las sesiones de acceso remoto para detectar anomalías: Implemente soluciones de gestión de eventos e información de seguridad (SIEM) para registrar y analizar las sesiones de acceso remoto. Active la detección de anomalías basada en el comportamiento para detectar intentos de inicio de sesión inusuales, como accesos fuera de horario o desde nuevas ubicaciones. La supervisión en tiempo real facilita la detección de accesos no autorizados y la respuesta a los mismos.

T1078 (Cuentas válidas)

1. Aplicar el principio del mínimo privilegio y la segmentación de cuentas: Limite los permisos de las cuentas basándose en el principio del menor privilegio (PoLP). Implemente cuentas separadas para tareas administrativas y no administrativas para reducir la exposición. Utilice el aprovisionamiento de acceso justo a tiempo (JIT) y RBAC para minimizar el acceso persistente de alto privilegio. Restringir el acceso ayuda a mitigar el riesgo de uso indebido de cuentas.

2. Reforzar la autenticación y la seguridad de las credenciales: Exija MFA para todas las cuentas privilegiadas y estratégicas, dando prioridad a los métodos resistentes a la suplantación de identidad, como FIDO2 o la autenticación basada en certificados. Aplique políticas de contraseñas sólidas, incluidos requisitos de longitud y complejidad, e implante gestores de contraseñas para reducir la reutilización de credenciales. Rote periódicamente las credenciales y desactive las cuentas inactivas para evitar accesos no autorizados.

3. Detección y respuesta al uso no autorizado de cuentas: Supervise la actividad de las cuentas utilizando soluciones SIEM y de análisis del comportamiento de usuarios y entidades (UEBA). Señale los comportamientos anómalos, como el acceso desde nuevas ubicaciones, los intentos de inicio de sesión excesivos o la escalada de privilegios. Habilite alertas automatizadas e implemente mecanismos de respuesta en tiempo real para detectar y contener posibles compromisos de cuentas.

T1566 (Phishing)

1. Implementar la seguridad y el filtrado avanzados del correo electrónico: Despliegue puertas de enlace de correo electrónico seguras (SEG) y soluciones avanzadas de protección contra la suplantación de identidad para filtrar los mensajes maliciosos antes de que lleguen a los usuarios. Active protocolos de autenticación de correo electrónico basados en dominios, como SPF, DKIM y DMARC, para evitar la suplantación de identidad en el correo electrónico. Utilice la detección de amenazas basada en IA para identificar y poner en cuarentena los intentos de phishing en tiempo real.

2. Llevar a cabo una formación continua de concienciación de los usuarios y pruebas de phishing simuladas: Enseñe a los empleados a reconocer los intentos de phishing, incluidas las tácticas de ingeniería social, los archivos adjuntos maliciosos y los enlaces engañosos. Realice periódicamente simulaciones de phishing para poner a prueba la concienciación de los usuarios y proporcione formación específica en función de los resultados. Refuerce una cultura de vigilancia de la ciberseguridad para reducir la probabilidad de éxito de los ataques de phishing.

3. Implementar protecciones antiphishing en los navegadores y análisis de URL: Utilice el filtrado web y los servicios de reputación de dominios para bloquear el acceso a sitios conocidos de phishing. Aísle los navegadores de los usuarios de alto riesgo y analice automáticamente las URL de los correos electrónicos en busca de indicadores maliciosos antes de permitir el acceso. Fomente el uso de gestores de contraseñas para evitar el robo de credenciales rellenándolas automáticamente sólo en sitios legítimos.

T1003 (OS Credential Dumping)

1. Implementar mecanismos de protección de credenciales para evitar el acceso no autorizado a las credenciales almacenadas: Configure Windows Defender Credential Guard para proteger la memoria LSASS y evitar ataques de volcado de credenciales. Utilice soluciones EDR para detectar intentos de acceso sospechosos dirigidos a los almacenes de credenciales. Deshabilite los privilegios administrativos innecesarios para limitar la exposición a las técnicas de volcado de credenciales. Estas protecciones ayudan a evitar que los atacantes extraigan las credenciales almacenadas.

2. Restringir el acceso a los procesos sensibles del sistema y aplicar la auditoría de procesos: Configure las soluciones de seguridad de los terminales para supervisar y bloquear el acceso no autorizado a los archivos LSASS y de registro que contengan credenciales almacenadas. Implemente la auditoría de procesos para registrar y alertar sobre los intentos de acceso a los almacenes de credenciales. Revise periódicamente los registros de seguridad y realice análisis forenses de los eventos sospechosos. Supervisar las interacciones de los procesos ayuda a detectar y prevenir los intentos de volcado de credenciales.

3. Implementar un cifrado fuerte de credenciales y minimizar el almacenamiento de credenciales: Utilice normas de cifrado sólidas para el almacenamiento de credenciales y aplique las mejores prácticas de seguridad para la gestión de secretos. Implemente la escalada de privilegios JIT para reducir el acceso persistente a cuentas de alto valor. Minimice el almacenamiento de contraseñas en caché en los terminales para limitar la exposición de las credenciales. Reforzar el almacenamiento de credenciales reduce el riesgo de ataques de volcado de credenciales.

T1486 (Datos cifrados por impacto – Ransomware)

1. Desplegar una sólida protección de los puntos finales y una detección del ransomware basada en el comportamiento: Implemente soluciones antivirus de nueva generación (NGAV) y EDR para supervisar los comportamientos específicos del ransomware, como el cifrado masivo de archivos, la eliminación de copias de seguridad y los cambios no autorizados en el registro. Configure la contención automática de los dispositivos infectados para evitar la propagación del ransomware. La detección temprana de la actividad relacionada con el cifrado ayuda a mitigar el impacto de los ataques de ransomware.

2. Aplicar políticas estrictas de copia de seguridad de datos con almacenamiento inmutable y recuperación sin conexión: Implemente una estrategia de copia de seguridad 3-2-1 con copias de seguridad fuera de línea e inmutables almacenadas por separado de los entornos de producción. Pruebe periódicamente los procedimientos de restauración de copias de seguridad para garantizar una rápida recuperación de los ataques de ransomware. Utilizar el cifrado de las copias de seguridad y controles de acceso para proteger los datos almacenados de modificaciones no autorizadas. Las copias de seguridad protegidas proporcionan un mecanismo de recuperación crítico en caso de infección por ransomware.

3. Implementar la segmentación de la red y la lista de aplicaciones permitidas para evitar la propagación del ransomware: Segmente la infraestructura bancaria crítica de los entornos informáticos generales utilizando controles de acceso estrictos y políticas de cortafuegos. Implemente listas de aplicaciones permitidas para impedir la ejecución no autorizada de cargas útiles de ransomware. Supervise los cambios en el sistema de archivos y restrinja el acceso de escritura a los directorios sensibles. Aislar los sistemas críticos reduce la superficie de ataque y limita el impacto de un brote de ransomware.

T1567.002 (Exfiltración a través de un servicio web: Exfiltración al almacenamiento en la nube)

1. Implantar soluciones de prevención de pérdida de datos (DLP) para supervisar y restringir las transferencias de datos no autorizadas: Implemente soluciones de DLP para supervisar, registrar y bloquear las transferencias de datos no autorizadas a servicios externos de almacenamiento en la nube como Google Drive, Dropbox y OneDrive. Configure políticas para detectar movimientos de datos anómalos y aplicar el cifrado automático de datos financieros confidenciales antes de su transferencia. Las soluciones DLP ayudan a prevenir la exfiltración no autorizada de datos bancarios sensibles.

2. Supervisar y restringir el acceso a los servicios de almacenamiento en la nube desde las redes de las instituciones financieras: Implemente controles de firewall y proxy para restringir el acceso a plataformas de almacenamiento en la nube no autorizadas. Utilice soluciones Secure Access Service Edge (SASE) para aplicar el filtrado de contenidos y detectar cargas de datos sospechosas. Configure alertas para transferencias de datos de gran volumen y patrones de acceso inusuales que indiquen intentos de exfiltración. Restringir el acceso a los servicios de almacenamiento externo minimiza los riesgos de exfiltración.

3. Cifrar los datos financieros confidenciales en reposo y en tránsito para evitar su exposición no autorizada: Utilice protocolos de cifrado fuertes (AES-256, TLS 1.2+) para todos los datos financieros sensibles almacenados o transmitidos dentro de la organización. Aplique controles de acceso estrictos y MFA para el acceso al almacenamiento en la nube. Implementar el registro y la supervisión de las interacciones de almacenamiento en la nube para detectar e investigar anomalías. Cifrar los datos confidenciales reduce el riesgo de divulgación no autorizada, incluso si se filtran.

Recomendaciones para técnicas de ataque de alto riesgo con graves riesgos operativos y de seguridad

T1547 (Ejecución de arranque o inicio de sesión automático)

1. Hacer cumplir el control de aplicaciones y evitar mecanismos de persistencia no autorizados: Implemente listas de aplicaciones permitidas mediante Windows Defender Application Control (WDAC) o AppLocker para evitar la ejecución no autorizada de malware al iniciar el sistema. Restrinja los privilegios administrativos para evitar modificaciones no autorizadas del registro, la creación de tareas programadas o la instalación de servicios. Aplique la verificación de firmas digitales para garantizar que sólo las aplicaciones de confianza puedan persistir. Estas medidas reducen la capacidad de los atacantes para establecer la persistencia a través de mecanismos de inicio.

2. Supervisar y auditar las configuraciones de inicio del sistema en busca de anomalías: Implemente soluciones EDR para supervisar las modificaciones de las ubicaciones de inicio, como el registro de Windows, las tareas programadas y las configuraciones de servicio. Configure alertas de gestión de eventos e información de seguridad (SIEM) para detectar cambios no autorizados en las entradas de inicio automático. Audite periódicamente la configuración de inicio del sistema para identificar y eliminar mecanismos de persistencia sospechosos. La supervisión continua ayuda a detectar y responder a modificaciones no autorizadas antes de que los adversarios puedan aprovecharlas.

3. Reforzar la integridad del sistema y aplicar mecanismos de arranque seguros: Active Secure Boot para evitar modificaciones no autorizadas en el arranque y garantizar que sólo se cargan componentes de confianza del sistema operativo. Implemente la protección contra manipulaciones en las configuraciones críticas del sistema para evitar que los adversarios modifiquen las entradas de arranque automático. Utilice sistemas de prevención de intrusiones basados en host (HIPS) para bloquear intentos de persistencia sospechosos. El endurecimiento de los procesos de arranque reduce el riesgo de persistencia de malware en terminales bancarios y cajeros automáticos.

T1484.001 (Modificación de políticas de dominio: Modificación de directivas de grupo)

1. Implementar el control de acceso basado en roles (RBAC) para restringir las modificaciones de políticas de dominio: Restringir los privilegios de modificación de directivas de grupo a un conjunto limitado de administradores. Utilice soluciones de gestión de acceso privilegiado (PAM) para aplicar el acceso justo a tiempo (JIT) y evitar cambios no autorizados. Revise y elimine periódicamente los privilegios administrativos innecesarios. Estas medidas limitan la capacidad del atacante para manipular las políticas de seguridad para el movimiento lateral.

2. Supervisar y registrar continuamente los cambios en las políticas de grupo: Implemente soluciones SIEM para registrar y alertar sobre las modificaciones de las directivas de grupo. Utilice Microsoft Advanced Threat Analytics (ATA) o Azure Sentinel para detectar cambios sospechosos en las directivas que indiquen un ataque. Revise regularmente los registros del controlador de dominio para identificar modificaciones no autorizadas. Supervisar los cambios en las directivas ayuda a detectar y responder a la actividad maliciosa antes de que se propague por la red.

3. Implementar configuraciones de referencia seguras y realizar copias de seguridad de los objetos de directiva de grupo (GPO): Implemente una configuración de línea de base segura utilizando puntos de referencia CIS o líneas de base de seguridad de Microsoft. Realice copias de seguridad periódicas de los objetos de directiva de grupo (GPO) y active las funciones de reversión para restaurar la configuración de seguridad en caso de peligro. Utilice el control de versiones y los registros de auditoría para rastrear los cambios y revertir las modificaciones no autorizadas. Las líneas de base y las copias de seguridad seguras garantizan una rápida recuperación en caso de alteraciones malintencionadas de las políticas.

T1562.001 (Deteriorar las defensas: desactivar o modificar las herramientas)

1. Implementar la protección de endpoints con controles de seguridad a prueba de manipulaciones: Implemente soluciones EDR con protección contra manipulaciones para evitar que los adversarios desactiven las herramientas de seguridad. Restrinja el acceso administrativo al software de seguridad y aplique un control de acceso basado en funciones (RBAC) para limitar los privilegios de modificación. Bloquee la configuración de seguridad con políticas de grupo para evitar cambios no autorizados. Estas protecciones evitan que los atacantes desactiven las defensas durante un ataque.

2. Supervisar y registrar las modificaciones de las herramientas de seguridad: Configure las soluciones SIEM para que registren y alerten de las modificaciones de las herramientas de seguridad, como la desactivación de antivirus, la desactivación del registro o el cambio de las reglas del cortafuegos. Implemente sistemas de prevención de intrusiones basados en host (HIPS) para detectar y bloquear los intentos no autorizados de modificar las configuraciones de seguridad. La supervisión periódica garantiza la rápida detección de los intentos de los adversarios de desactivar las herramientas de seguridad.

3. Restringir la ejecución de secuencias de comandos y herramientas administrativas utilizadas para desactivar las defensas: Implemente el registro de bloqueo de secuencias de comandos PowerShell y aplique políticas de ejecución para evitar que secuencias de comandos no autorizadas modifiquen las configuraciones de seguridad. Restrinja el uso de herramientas como Process Hacker, GMER y PsExec que los atacantes suelen utilizar para desactivar las defensas de seguridad. Utilizando aplicaciones que permitan el listado, bloquee la ejecución de herramientas de desactivación de seguridad no autorizadas. Estas medidas ayudan a mantener la integridad de las defensas de seguridad.

T1046 (Network Service Discovery)

1. Limitar la exposición de los servicios de red mediante cortafuegos y controles de acceso: Restrinja el tráfico entrante y saliente únicamente a los servicios esenciales mediante reglas estrictas de cortafuegos. Desactive los servicios y protocolos de red innecesarios en la infraestructura bancaria crítica. Implemente la segmentación de la red para aislar los sistemas de alto valor de los entornos informáticos generales. Restringir la exposición de los servicios reduce la superficie de ataque para el reconocimiento de adversarios.

2. Desplegar la supervisión de la red y la detección de anomalías para exploraciones no autorizadas: Utilice sistemas de detección de intrusiones (IDS) y herramientas de análisis del tráfico de red (NTA) para supervisar las actividades anómalas de exploración de la red. Configure soluciones SIEM para generar alertas sobre intentos excesivos de conexión a la red o consultas inusuales al servicio. Implemente tecnología de engaño (honeypots) para detectar y rastrear a los atacantes que intentan reconocer la red. La supervisión de la actividad de la red permite la detección temprana de los intentos de reconocimiento de los actores de amenazas.

3. Reforzar los protocolos de red e imponer una autenticación estricta: Desactive los protocolos heredados, como SMBv1, y aplique el cifrado TLS a todas las comunicaciones de red. Aplique la autenticación mutua a los servicios de red sensibles para impedir el acceso no autorizado. Exija autenticación basada en certificados para los servicios administrativos remotos. Reforzar los protocolos de seguridad de la red dificulta a los atacantes el descubrimiento de servicios.

T1082 (System Information Discovery)

1. Restringir el acceso a la información del sistema y del hardware: Configure políticas de grupo para impedir que los usuarios no administrativos accedan a comandos de información del sistema como systeminfo, wmic y tasklist. Deshabilite el acceso remoto a las herramientas de enumeración del sistema en los terminales bancarios. Evite que los adversarios recopilen información detallada sobre la infraestructura de las instituciones financieras.

2. Implementar la supervisión de terminales para detectar actividades de descubrimiento sospechosas: Utilice soluciones EDR para supervisar y alertar sobre comandos de enumeración del sistema ejecutados por usuarios no autorizados. Configure reglas SIEM para registrar y marcar los intentos de acceder a los detalles del sistema. La detección temprana de actividades de reconocimiento ayuda a evitar una mayor explotación.

3. Aplicar controles de acceso estrictos a las herramientas de gestión del sistema: Restrinja el acceso administrativo a utilidades de gestión del sistema como PowerShell, WMI y Task Scheduler. Utilice la escalada de privilegios justo a tiempo (JIT) para conceder acceso temporal sólo cuando sea necesario. Audite periódicamente los registros de acceso en busca de consultas inusuales a las bases de datos de información del sistema. Estas medidas limitan la capacidad de un atacante para recopilar información sobre la infraestructura bancaria.

T1021.001 (Servicios remotos: Remote Desktop Protocol – RDP)

1. Restringir el acceso RDP con autenticación reforzada y segmentación de red: Implemente MFA para todas las conexiones RDP. Restrinja el acceso RDP mediante cortafuegos, permitiendo sólo direcciones IP preaprobadas. Utilice una infraestructura de escritorio virtual (VDI) con autenticación por intermediario para limitar la exposición directa de los servicios RDP. Aplicar controles de acceso estrictos reduce los intentos de acceso remoto no autorizados.

2. Supervisar y registrar la actividad de las sesiones RDP para detectar accesos no autorizados: Habilite el registro de las sesiones RDP, capturando los intentos de conexión exitosos y fallidos. Configure las soluciones SIEM para generar alertas de uso anómalo de RDP, como inicios de sesión desde ubicaciones inusuales o intentos fallidos repetidos. Implemente análisis de comportamiento para detectar sesiones RDP comprometidas. La supervisión continua ayuda a detectar intentos de acceso remoto no autorizados.

3. Reforzar la configuración de RDP y aplicar controles de seguridad de sesión: Configure RDP para utilizar la autenticación a nivel de red (NLA) para evitar el acceso no autorizado antes de la autenticación. Imponga el cifrado TLS para todo el tráfico RDP. Utilice controles de acceso basados en el tiempo para limitar el acceso RDP a ventanas de mantenimiento predefinidas. Revise regularmente los registros de sesiones RDP para identificar actividades sospechosas. Endurecer las configuraciones RDP reduce el riesgo de acceso no autorizado y movimiento lateral.

Recomendaciones para las técnicas de ataque de impacto indirecto utilizadas para el movimiento lateral y la evasión

T1059.003 (Windows Command Shell – Ejecuta scripts para automatizar acciones maliciosas en sistemas financieros)

1. Restringir la ejecución de scripts y comandos de línea de comandos no autorizados: Implemente listas de aplicaciones permitidas mediante Windows Defender Application Control (WDAC) o AppLocker para bloquear la ejecución no autorizada de cmd. exe y secuencias de comandos por lotes. Aplique políticas de registro y ejecución de bloqueo de secuencias de comandos PowerShell para impedir la ejecución de secuencias de comandos malintencionadas. Limite el acceso de los usuarios no administrativos a los intérpretes de línea de comandos. Restringir la ejecución de intérpretes de comandos impide que los adversarios automaticen acciones maliciosas dentro de los sistemas financieros.

2. Supervisar y registrar la actividad sospechosa en la línea de comandos: Implemente soluciones EDR para rastrear el uso de la línea de comandos y detectar secuencias de comandos sospechosas que ejecuten modificaciones del sistema. Configure las alertas SIEM para señalar comandos shell inusuales como net user, taskkill o reg add. La supervisión proactiva de la actividad del shell permite a los equipos de seguridad detectar y mitigar la ejecución no autorizada de scripts.

3. Aplicar controles de acceso estrictos a la ejecución de comandos administrativos: Implemente la escalada de privilegios JIT para restringir el acceso a las interfaces de línea de comandos administrativas. Se requiere MFA para las sesiones privilegiadas que utilizan cmd.exe o PowerShell. Registre todas las actividades del shell administrativo para su análisis forense. Estas medidas limitan la capacidad de los adversarios para ejecutar scripts maliciosos y mantener la persistencia en los sistemas bancarios.

T1072 (Software Development Tools – Utilizadas para compilar y ejecutar código malicioso en entornos bancarios)

1. Restringir la instalación y ejecución de herramientas de desarrollo no autorizadas: Utilice listas de aplicaciones permitidas para evitar la ejecución no autorizada de compiladores, entornos de secuencias de comandos y marcos de desarrollo dentro de las redes bancarias. Limite los permisos de instalación de herramientas como Visual Studio, GCC y Python únicamente a los usuarios autorizados. El bloqueo de herramientas de desarrollo de software no aprobadas reduce el riesgo de que los adversarios compilen y ejecuten código malicioso.

2. Supervisar el uso de las herramientas de desarrollo para detectar anomalías: Implemente soluciones de supervisión de puntos finales para realizar un seguimiento de la ejecución de las herramientas de desarrollo de software e identificar el uso no autorizado. Configure reglas SIEM para generar alertas cuando se produzca la compilación o ejecución de código sospechoso fuera de los entornos de desarrollo aprobados. La supervisión continua garantiza la rápida detección del uso adverso de las herramientas de desarrollo.

3. Aplicar políticas estrictas de ejecución de código en los sistemas financieros: Se requiere la verificación de la firma digital de todos los ejecutables y scripts antes de su ejecución. Implemente un entorno aislado para la ejecución de código no verificado a fin de evitar la interacción directa con los sistemas de producción. Utilice EDR para analizar el comportamiento de los binarios compilados antes de permitir su ejecución. Aplicar controles de ejecución mitiga el riesgo de que se despliegue código malicioso en las redes bancarias.

T1110 (Fuerza bruta - Intentos de descifrar credenciales bancarias para acceso no autorizado)

1. Aplicar políticas de contraseñas seguras y mecanismos de bloqueo de cuentas: Exija contraseñas complejas con una longitud mínima de 12-15 caracteres y aplique la caducidad automática de contraseñas. Implemente políticas de bloqueo de cuentas tras varios intentos fallidos de inicio de sesión para evitar ataques de fuerza bruta. Utilice listas negras de contraseñas para impedir el uso de contraseñas estándar o fáciles de adivinar. Las políticas de autenticación fuerte reducen significativamente la efectividad de los ataques de brute-force.

2. Implementar la detección de anomalías en los intentos de inicio de sesión y la autenticación multifactor (MFA): Utilice análisis de comportamiento para detectar actividades de inicio de sesión anómalas, como repetidos intentos fallidos desde una misma dirección IP. Implemente MFA para todas las cuentas privilegiadas y puntos de acceso remoto para evitar el acceso no autorizado, incluso si las credenciales están en peligro. La detección de anomalías y la MFA crean múltiples capas de defensa contra los ataques de brute-force.

3. Restringir el acceso externo a los portales de autenticación y aplicar reglas de delimitación geográfica: Limite el acceso a los sistemas de autenticación utilizando listas blancas de IP y geovallas para bloquear los intentos de inicio de sesión desde regiones de alto riesgo. Utilice herramientas de detección de amenazas a la identidad para analizar las solicitudes de autenticación en busca de signos de intentos automatizados de fuerza bruta. Restringir el acceso a los portales de autenticación minimiza la exposición a la usurpación de credenciales y el uso de contraseñas por fuerza bruta.

T1572 (Protocol Tunneling – Oculta el tráfico de red malicioso para eludir los controles de seguridad)

1. Implementar la inspección profunda de paquetes (DPI) para detectar y bloquear la actividad de tunneling: Despliegue sistemas de detección y prevención de intrusiones en la red (IDS/IPS) con capacidades DPI para analizar el tráfico cifrado en busca de firmas de tunelización de protocolos. Utilice la información sobre amenazas para actualizar las reglas de detección de herramientas de tunelización conocidas. La DPI garantiza que los intentos de tunelización de protocolos no autorizados se identifiquen y bloqueen antes de llegar a los sistemas críticos.

2. Restringir las conexiones de red salientes sólo a protocolos y servicios aprobados: Configure los cortafuegos para bloquear las conexiones salientes no autorizadas que utilicen protocolos utilizados habitualmente para la creación de túneles, como ICMP, DNS y HTTP a través de puertos no estándar. Aplique políticas estrictas de filtrado de salida para limitar las comunicaciones externas a dominios y direcciones IP preaprobados. Reducir el tráfico saliente no autorizado minimiza la eficacia de las técnicas de tunneling.

3. Supervisar el tráfico de red en busca de anomalías indicativas de intentos de tunneling: Utilice herramientas de análisis de tráfico de red (NTA) para detectar patrones irregulares de transferencia de datos, como cargas útiles cifradas a través de puertos inesperados. Configure las soluciones SIEM para generar alertas cuando se detecten comportamientos sospechosos de tunelización. La supervisión continua ayuda a los equipos de seguridad a identificar y responder a los intentos de los adversarios de eludir los controles de seguridad.

T1071.002 (Application Layer Protocol: Protocolos de transferencia de archivos - Utilizados para la puesta en escena y la transferencia de datos financieros robados)

1. Restringir el uso no autorizado de protocolos de transferencia de archivos: Bloquee las transferencias de archivos FTP, SFTP y HTTP no autorizadas utilizando cortafuegos de red y proxies web. Limite las transferencias salientes de archivos al almacenamiento en la nube preaprobado y a los repositorios internos. A efectos de auditoría, se requiere autenticación para todas las transferencias de archivos y la actividad de registro. Restringir el uso del protocolo de transferencia de archivos evita que los adversarios exfiltren datos financieros.

2. Supervisar y registrar las actividades de transferencia de archivos para detectar comportamientos sospechosos: Despliegue herramientas de supervisión de seguridad para rastrear transferencias de archivos grandes o inesperadas desde sistemas financieros. Configure alertas SIEM para cargas de gran volumen a servidores externos o patrones de transferencia anómalos. Auditar regularmente los registros de transferencia de archivos ayuda a detectar intentos de exfiltración de datos antes de que provoquen pérdidas financieras.

3. Cifrar los datos financieros confidenciales en reposo y en tránsito para evitar accesos no autorizados: Aplique el cifrado de extremo a extremo en todas las transferencias de archivos mediante protocolos seguros como SFTP, TLS e IPsec. Implante soluciones de prevención de pérdida de datos (DLP) para detectar y bloquear automáticamente la transferencia de datos bancarios confidenciales a destinos no autorizados. Las políticas de cifrado y DLP garantizan que los datos financieros permanezcan seguros, aunque se filtren.

T1219 (Remote Access Software – Permite a los atacantes mantener un control persistente sobre los sistemas bancarios comprometidos)

1. Bloquear las herramientas de acceso remoto no autorizadas y restringir el acceso al escritorio remoto: Utilice listas de aplicaciones permitidas para impedir la ejecución de herramientas de acceso remoto no autorizadas, como TeamViewer, AnyDesk y VNC. Deshabilite el acceso remoto a escritorios (RDP) en sistemas financieros críticos a menos que se requiera explícitamente. Restrinja el acceso remoto a conexiones sólo VPN con aplicación de MFA. Bloquear las herramientas de acceso remoto no autorizadas reduce la superficie de ataque para el control persistente.

2. Supervisar y registrar continuamente las sesiones de acceso remoto: Implemente soluciones de supervisión de puntos finales para realizar un seguimiento de todas las sesiones de acceso remoto y detectar comportamientos de inicio de sesión inusuales. Utilice análisis de comportamiento para identificar anomalías, como sesiones remotas originadas en geolocalizaciones inusuales o durante horas no laborables. El registro y la supervisión de las actividades de acceso remoto ayudan a detectar la presencia persistente de agresores.

3. Imponer la segmentación de la red y limitar los privilegios de acceso remoto: Aísle los servicios de acceso remoto de las redes bancarias centrales mediante la segmentación de la red. Implemente el aprovisionamiento de acceso justo a tiempo (JIT) para conceder acceso remoto temporal sólo cuando sea necesario. Utilice soluciones de gestión de acceso a privilegios (PAM) para imponer un estricto registro y auditoría de sesiones para todas las conexiones remotas. La segmentación y las restricciones de privilegios impiden a los atacantes aprovechar las herramientas de acceso remoto para el movimiento lateral.

5.3 Mispadu

Mispadu es un troyano bancario altamente sofisticado que representa una amenaza significativa para el sector financiero, particularmente en LATAM. Descubierto originalmente en 2019, Mispadu ha ampliado su alcance más allá de sus objetivos iniciales en Brasil y México para incluir otros países de LATAM e incluso naciones europeas.[215] [216]

La efectividad del troyano para atacar instituciones financieras proviene de su estrategia de infección en varias etapas y su naturaleza sigilosa. Mispadu se centra principalmente en usuarios de habla hispana y portuguesa, lo que lo hace especialmente peligroso para bancos y cooperativas de crédito de LATAM.[217] [218] Su capacidad para eludir numerosas soluciones de protección de puntos finales, incluidos muchos productos antivirus conocidos, le ha permitido infiltrarse en una amplia gama de industrias, siendo el sector financiero uno de sus principales objetivos.[219]

El impacto de Mispadu en el sector financiero es sustancial:

- **Robo de credenciales:** El troyano roba credenciales bancarias, información de tarjetas de crédito y otros datos financieros confidenciales mediante técnicas de keylogging y captura de pantalla.[220]
- **Ataque a criptomonedas:** Mispadu monitoriza las direcciones de los monederos de criptomonedas y puede sustituirlas por direcciones controladas por el atacante, redirigiendo potencialmente las transacciones.[221]
- **Infecciones generalizadas:** En una campaña, Mispadu afectó a numerosos sitios web gubernamentales y plataformas de banca online en Chile, México y Perú, comprometiendo a cientos de instituciones financieras.[222]

[215] https://blog.morphisec.com/mispadu-infiltration-beyond-latam
[216] https://www.feedzai.com/blog/
[217] https://www.feedzai.com/blog/
[218] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/mispadu-banking-trojan-resurfaces
[219] https://blog.morphisec.com/mispadu-infiltration-beyond-latam
[220] https://www.feedzai.com/blog/
[221] https://www.feedzai.com/blog/
[222] https://www.metabaseq.com/threat/mispadu-banking-trojan/

Un ejemplo notable de la eficacia de Mispadu fue una campaña dirigida a los usuarios con cupones de descuento falsos, lo que demuestra la capacidad del troyano para adaptar sus tácticas de ingeniería social para atraer a las víctimas.[223] Esta adaptabilidad, combinada con su enfoque en las instituciones financieras de LATAM, hace de Mispadu una amenaza persistente y en evolución para el sector bancario de la región. Para eludir la detección, el malware utiliza técnicas avanzadas como la ofuscación, la detección sandbox y el geofencing. Los informes de inteligencia de Morphisec revelan que la carga útil final de Mispadu se entregó a través de un script AutoIT descifrado, que carga el troyano en la memoria. Los piratas informáticos han estado utilizando archivos PDF como arma de distribución, y Mispadu es conocido por robar contraseñas de navegador y correo electrónico y vigilar activamente la actividad de los usuarios. Inicialmente dirigido a América Latina, ahora afecta a Europa, robando credenciales a través de correos electrónicos de phishing y maliciosos.[224]

5.3.1 Métodos de Mispadu y explotación de la infraestructura de LATAM

Los métodos de la campaña Mispadu están estratégicamente diseñados para explotar las vulnerabilidades únicas presentes en los ecosistemas regulatorios, legales y de TI de LATAM. Uno de los principales factores es la falta de normativas estrictas en materia de ciberseguridad y su aplicación incoherente en toda la región, lo que proporciona un entorno de bajo riesgo para los ciberdelincuentes. Al dirigirse a regiones con escasa concienciación sobre ciberseguridad, Mispadu se asegura de que las campañas de phishing por correo electrónico alcancen mayores tasas de éxito, ya que es menos probable que los usuarios reconozcan y denuncien la actividad maliciosa.[225] Además, los sistemas y el software obsoletos que prevalecen en las organizaciones de LATAM facilitan que el malware explote vulnerabilidades conocidas, como las de plataformas CMS como WordPress.

Mispadu aprovecha la insuficiente capacidad de respuesta a incidentes en la región, lo que garantiza operaciones prolongadas sin ser detectado. La adopción de medidas antianálisis y cadenas de infección multicapa no sólo mejora la evasión, sino que también explota las limitadas capacidades forenses y de mitigación de los equipos regionales de ciberseguridad. El enfoque geográfico, que filtra a las víctimas según la configuración del idioma del sistema, garantiza que sólo se vean afectados los grupos demográficos previstos, lo que aumenta la eficacia y la rentabilidad de las campañas. Por último, al aprovechar el desvío de Windows SmartScreen, Mispadu elude las protecciones integradas, aprovechando la falta de madurez técnica y la dependencia de las configuraciones de seguridad por defecto en muchas organizaciones de LATAM. Estas estrategias ponen de manifiesto la eficacia del troyano a la hora de aprovechar las lagunas normativas y técnicas de la región para mantener sus operaciones maliciosas.

5.3.2 Tácticas, técnicas y procedimientos

Mispadu emplea una sofisticada serie de TTP diseñadas para maximizar su eficacia como troyano bancario. Sus campañas de infección suelen comenzar con ingeniería social a través de correos electrónicos de phishing, distribuyendo páginas HTML maliciosas o archivos PDF adjuntos protegidos con contraseña que atraen a los usuarios para que ejecuten el malware.[226]
El troyano también aprovecha anuncios maliciosos y sitios web legítimos comprometidos, incluidas plataformas vulnerables basadas en WordPress, para servir como servidores de Mando y Control (C2) para la entrega de la carga útil.[227] Además, Mispadu adopta cadenas de infección multietapa, utilizando scripts ofuscados y cargadores como AutoIT y VBScript para entregar su carga útil final, lo que es un sello distintivo de su complejidad operativa.

Para eludir la detección, Mispadu emplea técnicas antianálisis, como la detección de máquinas virtuales y comprobaciones de idioma, para garantizar que el malware sólo se ejecuta en entornos que coinciden con el perfil de la víctima objetivo. También utiliza certificados falsos para camuflar el malware y eludir las defensas de seguridad.[228] El malware incluye funciones para el robo de credenciales, empleando puertas traseras que le permiten capturar pulsaciones de teclas, hacer capturas de pantalla y mostrar falsas superposiciones del navegador para extraer información confidencial. Además, Mispadu aprovecha la infraestructura dual-C2 y técnicas avanzadas como la explotación de la vulnerabilidad Windows SmartScreen (CVE-2023-36025) para eludir las advertencias de seguridad, garantizando que sus cargas útiles se distribuyan de forma sigilosa y eficaz.[229]

[223] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/mispadu-banking-trojan-resurfaces
[224] https://www.morphisec.com/blog/mispadu-infiltration-beyond-latam/
[225] https://blog.morphisec.com/mispadu-infiltration-beyond-latam
[226] https://blog.morphisec.com/mispadu-infiltration-beyond-latam
[227] https://www.metabaseq.com/threat/mispadu-banking-trojan/
[228] https://www.feedzai.com/blog/
[229] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/mispadu-banking-trojan-resurfaces

5.3.3 Tácticas, técnicas y procedimientos de Mispadu

Tácticas	Técnicas	Procedimientos
Reconocimiento (TA0043)	NA	NA
Desarrollo de recursos (TA0042)	NA	NA
Acceso inicial (TA0001)	T1566.001: Phishing	Campañas de spam, la víctima es conducida a la carga útil por un enlace o archivo adjunto malicioso
	T1190: Explotación de aplicación de cara al público	Explotar una debilidad en un host o sistema orientado a Internet para acceder inicialmente a una red
Ejecución (TA0002)	T1204.002: Usuario de ejecución de archivos maliciosos: Malware	Se ejecuta cuando el usuario abre archivos adjuntos maliciosos o archivos descargados de sitios web comprometidos.
Persistencia (TA0003)	T1053.005: Scheduled Task/Job	Emplea tareas programadas para mantener la persistencia en los sistemas infectados.
Escalado de privilegios (TA0004)	T1055: Process Injection T1055.012: Process Hollowing T1055.013: Process Doppelganging	Inyecta su carga útil en procesos legítimos para evitar ser detectado.
Defense Evasion (TA0005)	T1036: Masquerading	Se hace pasar por un cupón de descuento
	T1027: Archivos o información ofuscados T1027.013: Archivo cifrado/ codificado	Utiliza la ofuscación y el cifrado para eludir la detección por parte de las herramientas de seguridad, incluyendo la detección anti-análisis y sandbox
Acceso a credenciales (TA0006)	T1555: Credenciales de almacenes de contraseñas T1555.003: Credenciales de navegadores web	Obtiene credenciales de clientes de correo y navegadores web.
	T1003: OS Credential Dumping T1003.008: etc/password and etc/ shadow	Utiliza herramientas como WebBrowserPassView y MailPassView para robar contraseñas de navegadores y clientes de correo electrónico.
	T1056: Input Capture T1056.001: Keylogging T1056.003: Web Portal Capture	Captura pulsaciones de teclas y capturas de pantalla para robar credenciales y datos confidenciales.
Discovery (TA0007)	T1082: System and Information Discovery T1083: File and Directory Discovery	Extrae la versión del sistema operativo, el nombre del ordenador y el ID de idioma.
Movimiento lateral (TA0008)	NA	NA
Collection (TA0009)	T1113: Captura de pantalla	Contiene un comando para realizar capturas de pantalla.
	T1005: Datos del sistema local	Recopila credenciales, historial del navegador e información del sistema de la máquina de la víctima.
Command and Control (C2) (TA0011)	T1573: Canal cifrado de mando y control (C2)	Se comunica con servidores C2 utilizando HTTPS u otros canales cifrados para la exfiltración de datos y la ejecución de comandos.

	T1102: Servicio Web T1102.002: Comunicación bidireccional	Utiliza un servicio Web externo existente y legítimo como medio para retransmitir datos a/desde un sistema comprometido.
	T1105: Transferencia de herramientas de entrada	Transfiere herramientas u otros archivos desde un sistema externo a un entorno comprometido.
Exfiltración (TA0010)	T1041: Exfiltración por canal C2	Envía los datos que recopila a su servidor de C&C.
	T1567: Exfiltración por servicio web	Utiliza un servicio web externo legítimo existente para filtrar datos en lugar de su canal de mando y control principal.
Impacto (TA0040)	NA	

Mispadu IOCs

- Mispadu exfiltra datos robados, incluidas credenciales e información del sistema, a través de canales C2 cifrados.
- Hashes: 72e83b133a9e4cecd21fdb47334672f6, e5967a8274d40e0573c28b664670857e IP addresses: 104.238.182.44, 140.82.47.181
- Dominio: germogenborya.top, russk22.icu, germogenborya.at

Otros Mispadu IOCs

- SHA256 C++ dropper non-obfuscated version
- dbb2e294a65eb3fa1bbe1a25c2baf352a01250d567cfa953d4f942c2b5f08e53
- SHA256 C++ dropper obfuscated version
- d56863d940d5ccd1922bbbdf65471c493701e3b10be5c522851c8efbdaeb9fae
- SHA256.NET dropper
- ac97f893f8243db3c5ccfbc89d83b97534c1b73d0289ccb61bfb2c035f539126
- SHA256HTA dropper
- f873062ff206ad60cb4b790c2ba83624c510f15dbc4905d5c96668f87999c16a
- SHA256D2 downloader
- 7b6444e5be24ce95cdcac357cf20ddc77abda142a16202ab3677b7d29a1e0da3
- SHA256 payload version 96
- 78e3e51ddeac0519d434a8b192bae61bbaa278154a9511676c8a58079d95beb5
- SmokeBot download URL that served Mispadu
- http[:]//84.54.50[.]102/FX_432661.exe
- SmokeBot download URL that served a Rhadamanthys payload connected to Mispadu
- http[:]//amx55[.]xyz/rh111.exe

Mispadu CVE: CVE-2023-3602

5.3.3 Mitigación Mispadu

Reconocimiento (TA0043)

- Supervise el tráfico de red en busca de actividades de exploración sospechosas mediante IDS/IPS.
- Despliegue honeypots para detectar intentos tempranos de reconocimiento.

Desarrollo de recursos (TA0042)

- Supervise los registros de dominios y busque dominios falsos que imiten a su organización.
- Utilice feeds de inteligencia de amenazas para rastrear la infraestructura del adversario.

Acceso inicial (TA0001)

T1566.001: Phishing

- Implemente soluciones de seguridad de correo electrónico (DMARC, DKIM, SPF).
- Impartir formación de concienciación de seguridad a los empleados sobre las amenazas de phishing.
- Utilizar sandboxing para los adjuntos de correo electrónico para detectar contenido malicioso.

T1190: Explotar aplicaciones de cara al público

- Realice escaneos de vulnerabilidad y parcheo regulares de las aplicaciones orientadas a Internet.
- Implementar cortafuegos de aplicaciones web (WAF) para detectar y bloquear intentos de explotación.

Ejecución (TA0002)

- T1204.002: Ejecución de usuario - Archivo malicioso
- Habilite la lista blanca de aplicaciones para restringir la ejecución no autorizada.
- Utilice herramientas EDR para identificar ejecuciones sospechosas.

Persistencia (TA0003)

T1053.005: Tarea/trabajo programado

- Audite regularmente las tareas programadas y restrinja los privilegios de los usuarios.
- Utilice el registro de PowerShell para detectar la ejecución anormal de secuencias de comandos.

Escalada de privilegios (TA0004)

T1055: Inyección de procesos (incluye T1055.012 y T1055.013)

- Habilite Windows Defender Credential Guard para evitar el robo de credenciales.
- Utilice la detección basada en el comportamiento para los procesos inyectados.

Defense Evasion (TA0005)

T1036: Masquerading

- Desplegar detección basada en heurística para malware enmascarado.
- Analizar metadatos de archivos en busca de anomalías en marcas de tiempo y firmas.

T1027: Información o archivos ofuscados

- Implemente el análisis automatizado de malware en un entorno sandbox.
- Habilitar la supervisión de la integridad de los archivos en tiempo real para detectar cambios inesperados.

Acceso a credenciales (TA0006)

T1555: Credenciales de almacenes de contraseñas

- Deshabilite el autocompletado de contraseñas en navegadores y aplicaciones.
- Imponga MFA para sistemas críticos.

T1003: Volcado de credenciales del SO

- Supervise los registros de eventos de Windows en busca de intentos de acceso LSASS anormales.
- Deshabilite el almacenamiento de credenciales sin cifrar en las configuraciones del SO.

T1056: Input Capture (registro de teclas, captura de portales web)

- Implemente la detección de keyloggers basada en el comportamiento.
- Imponga el acceso de mínimo privilegio para evitar instalaciones de software no autorizadas.

Discovery (TA0007)

T1082: Descubrimiento del sistema y de la información

- Restringir el acceso a la información del sistema mediante la configuración de politicas de grupo.
- Supervisar la actividad de la línea de comandos para detectar intentos de reconocimiento.

Collection (TA0009)

T1113: Captura de pantalla

- Implemente soluciones DLP para supervisar y restringir las capturas de pantalla no autorizadas.
- Utilice escritorios virtuales para limitar la persistencia del malware.

T1005: Datos del sistema local

- Aplique el cifrado de datos en reposo y en tránsito.
- Implemente la supervisión de la integridad de los archivos para detectar accesos no autorizados a los datos.

Comando y control (TA0011)

T1573: Canal Cifrado

- Supervise el tráfico de red para detectar conexiones cifradas inusuales.
- Implemente descifrado e inspección SSL/TLS cuando sea factible.

T1102: Servicio Web

- Bloquee dominios maliciosos conocidos utilizando feeds de inteligencia de amenazas.
- Despliegue detección de anomalías para identificar tráfico de datos irregular.

T1105: Ingress Tool Transfer

- Restringir las descargas de archivos de fuentes externas desconocidas.
- Utilizar soluciones de filtrado de contenidos para bloquear transferencias no autorizadas.

Exfiltración (TA0010)

T1041: Exfiltración a través del canal C2

- Implemente controles de DLP para supervisar los flujos de datos salientes.
- Detectar patrones de exfiltración de datos utilizando análisis de red.

T1567: Exfiltración a través de servicios web

- Bloquear las transferencias externas de archivos no autorizadas a través de proxies web.
- Implemente la supervisión de API para detectar movimientos anormales de datos.

Impacto (TA0040)

- Implemente protección contra ransomware con capacidades de reversión de endpoints.
- Utilice la segmentación de red para limitar la propagación de malware.

5.4 Horabot

Horabot es un sofisticado malware que ha sido diseñado para atacar a usuarios de habla hispana, principalmente en países latinoamericanos. Horabot utiliza técnicas multimodulares para robar información sensible y se propaga aún más, centrándose en los sistemas latinoamericanos. Según las pruebas recopiladas por Cisco Talos, existen patrones que revelan los ataques altamente dirigidos en estas regiones donde las medidas de ciberseguridad no son tan rigurosas.[230]

Horabot fue observado por primera vez como una amenaza significativa a finales de 2020, identificado por el equipo Talos de Cisco como parte de una campaña de phishing con temas relacionados con los impuestos para atraer a las víctimas.[231] Horabot se dirige a individuos y empresas en México, Uruguay, Brasil, Venezuela, Argentina, Guatemala y Panamá.[232] Estas campañas de malware normalmente se disfrazan de correos electrónicos legítimos de las agencias tributarias, presentando a los usuarios un adjunto HTML malicioso que al hacer clic redirige a los usuarios a una aplicación HTML maliciosa. Los correos electrónicos de phishing utilizan el español como idioma principal, lo que coincide con la región objetivo, y aprovechan los plazos fiscales regionales para engañar a los usuarios para que hagan clic en los archivos adjuntos maliciosos y aumenten la tasa de infección.[233]

Principales objetivos y sectores:

- Las principales entidades objetivo de Horabot pertenecen a los siguientes sectores: contabilidad, construcción, ingeniería, distribución mayorista e inversiones.[234]
- Por su naturaleza, las organizaciones de estos sectores suelen ser más susceptibles al phishing, ya que suelen enviar correos electrónicos transaccionales.[235]

5.4.1 Capacidades y funcionalidad del malware

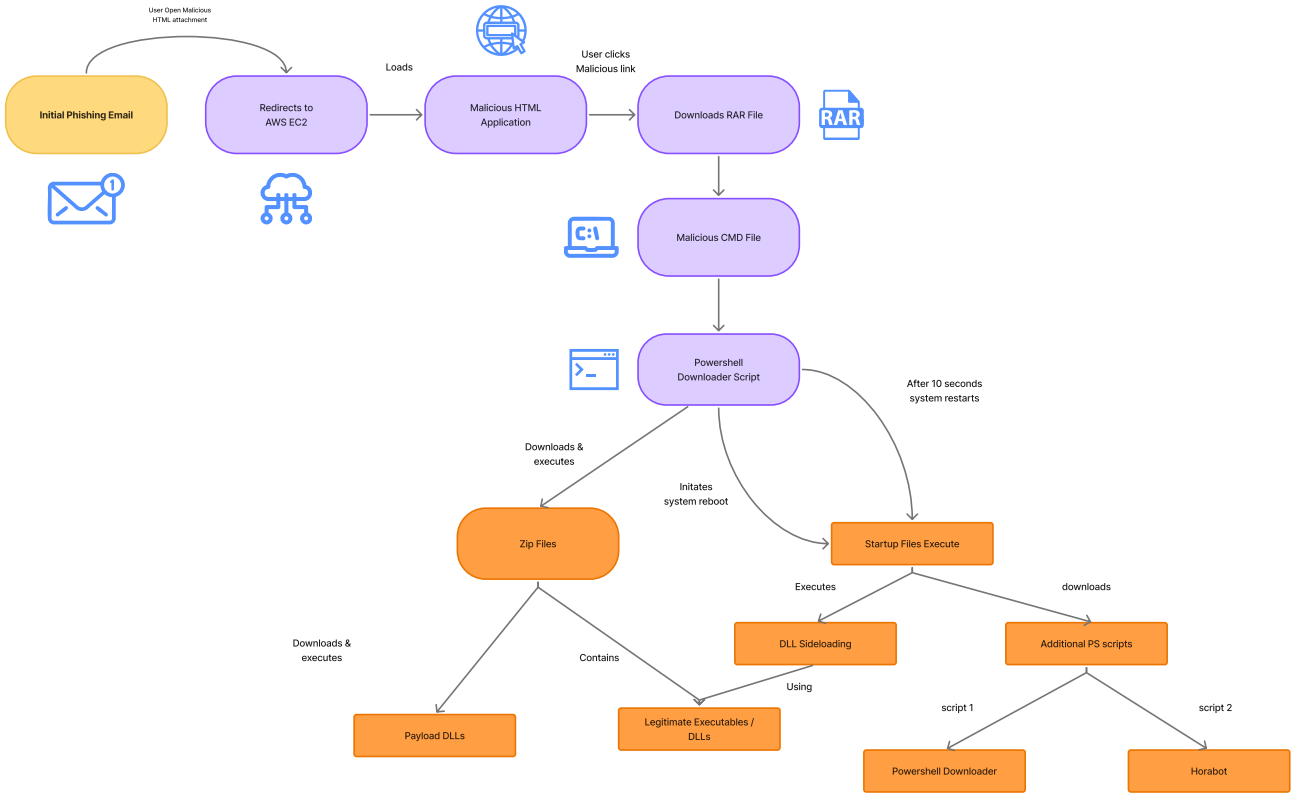
- Horabot utiliza troyanos bancarios y herramientas de spam y se despliega en diferentes etapas de la infección.

- El troyano bancario obtiene información sensible relacionada con credenciales de acceso bancario, información sobre sistemas operativos, pulsaciones de teclado, contraseñas de un solo uso y tokens blandos de aplicaciones bancarias. Esta funcionalidad explota directamente los protocolos de seguridad de las instituciones financieras latinoamericanas, poniendo en riesgo las cuentas de los usuarios y permitiendo el acceso no autorizado a los fondos.[236]

- La función de la herramienta de spam es comprometer las cuentas de Yahoo, Gmail y Outlook para recopilar y extraer las direcciones de correo electrónico de los contactos del objetivo. Una vez recopiladas estas direcciones, el malware envía correos electrónicos de phishing utilizando la cuenta de correo electrónico legítima de la víctima y el servidor de la organización, lo que aumenta la credibilidad de los correos electrónicos y disminuye la probabilidad de detección.[237]

[230] https://blog.talosintelligence.com/new-horabot-targets-americas/
[231] https://blog.talosintelligence.com/new-horabot-targets-americas/
[232] https://blog.talosintelligence.com/new-horabot-targets-americas/
[233] https://www.welivesecurity.com/2019/08/01/banking-trojans-amavaldo/
[234] https://blog.talosintelligence.com/new-horabot-targets-americas/
[235] https://www.welivesecurity.com/2019/08/01/banking-trojans-amavaldo/
[236] https://blog.talosintelligence.com/new-horabot-targets-americas/
[237] https://blog.talosintelligence.com/new-horabot-targets-americas/

Figure 7: Diagrama de flujo del ataque



5.4.2 Correlación entre Horabot y Mispadu

Horabot y Mispadu tienen sorprendentes similitudes en sus TTP, y ambos se dirigen con frecuencia a organizaciones latinoamericanas. Algunas similitudes que se han observado son:

Ambas familias de malware se han dirigido a instituciones financieras y usuarios de América Latina que hablan español, a través de ataques de phishing en su mayoría que involucran cargas útiles maliciosas basadas en HTML que inician cadenas de infección de varios pasos.

Aprovechan las técnicas MITRE ATT&CK T1204.001 (User Execution: Malicious Link) y T1566 (Phishing), lo que les permite propagarse eficientemente a través de tácticas de ingeniería social diseñadas para evadir la detección en servidores de correo electrónico legítimos.

Horabot y Mispadu suelen emplear técnicas de ofuscación y cifrado de la carga útil, con lo que evaden las detecciones estáticas basadas en firmas de las soluciones para endpoints.

Ambos malwares implementan filtros de geolocalización para atacar regiones de habla hispana y portuguesa. Las palabras clave en español y los nombres de instituciones financieras codificadas coinciden con su enfoque en América Latina, especialmente en México y Brasil.

5.4.3 Tácticas, técnicas y procedimientos de Horabot

Tácticas	Técnicas	Procedimientos
Desarrollo de recursos (TA0042)	T1584: Infraestructura de compromiso	Comprometer la infraestructura de terceros que se puede utilizar durante la selección de objetivos.
	T1584.005: Comprometer Infraestructura: Botnet	Comprometer numerosos sistemas de terceros para formar una red de bots que pueda utilizarse durante el ataque.
Acceso inicial (TA0001)	T1566: Phishing	Enviar mensajes de phishing para obtener acceso a los sistemas de las víctimas.
	T1566.001: Adjunto de Spear Phishing	Enviar mensajes de correo electrónico de phishing selectivo con un archivo adjunto malicioso para intentar acceder a los sistemas de las víctimas.
	T1190: Exploit Public-Facing Application	Intentar explotar una debilidad en un host o sistema orientado a Internet para acceder inicialmente a una red.
	T1078: Cuentas válidas	Obtener y abusar de las credenciales de cuentas existentes como medio para obtener acceso inicial, persistencia, escalada de privilegios o evasión de defensas.
Ejecución (TA0002)	T1059: Intérprete de comandos y scripts	Abusar de intérpretes de comandos y scripts para ejecutar comandos, scripts o binarios.
	T1059.001: Intérprete de comandos y scripts: PowerShell	Abusar de scripts y comandos PowerShell para su ejecución.
	T1204: Ejecución de usuario	Depender de acciones específicas de un usuario para obtener la ejecución.
	T1204.001: Ejecución de usuario: Enlace Malicioso	Depender de que un usuario haga clic en un enlace malicioso para obtener la ejecución.
	T1106: API Nativa	Interactuar con la interfaz de programación de aplicaciones (API) nativa del sistema operativo para ejecutar comportamientos.
Persistencia (TA0003)	T1574: Hijack Execution Flow	Ejecutar sus propias cargas maliciosas secuestrando la forma en que los sistemas operativos ejecutan los programas.
	T1574.002: Hijack Execution Flow: DLL Side-Loading	Ejecutan sus propias cargas maliciosas mediante la carga lateral de DLL.
	T1547.001: Ejecución de arranque o inicio automático de sesión: Claves de Ejecución del Registro / Carpeta de Inicio	Lograr la persistencia añadiendo un programa a una carpeta de inicio o haciendo referencia a él con una clave de ejecución del Registro.

	T1547.009: Ejecución de arranque o inicio automático de sesión: Modificación de accesos directos	Crear o modificar accesos directos que puedan ejecutar un programa durante el arranque del sistema o el inicio de sesión del usuario.
Defense Evasion (TA0005)	T1036: Enmascaramiento	Intentar manipular las características de sus artefactos para que parezcan legítimos o benignos ante los usuarios y/o las herramientas de seguridad.
	T1027: Archivos o información ofuscados	Intentar que un ejecutable o archivo sea difícil de descubrir o analizar cifrando, codificando u ofuscando de otro modo su contenido en el sistema o en tránsito.
	T1497: Virtualización/Evasión de Sandbox	Emplear diversos medios para detectar y evitar entornos de virtualización y análisis.
	T1070.004: Eliminación de Indicador: Borrado de archivos	Eliminar los archivos dejados por las acciones de su actividad de intrusión.
Acceso a credenciales (TA0006)	T1056.001: Captura de entrada: Keylogging	Registrar las pulsaciones de teclado del usuario para interceptar las credenciales a medida que el usuario las teclea..
	T1003: Volcado de Credenciales OS	Intentar volcar credenciales para obtener material de inicio de sesión y credenciales de cuentas, normalmente en forma de hash o contraseña en texto claro.
Discovery (TA0007)	T1082: System Information Discovery	Intentar obtener información detallada sobre el sistema operativo y el hardware, incluyendo versión, parches, hotfixes, service packs y arquitectura.
	T1083: File and Directory Discovery	Enumerar archivos y directorios o puede buscar en ubicaciones específicas de un host o recurso compartido de red determinada información dentro de un sistema de archivos.
Movimiento lateral (TA0008)	T1534: Internal Spear Phishing	El malware utiliza una herramienta de spam para exfiltrar la dirección de correo electrónico del contacto y envía un correo electrónico de phishing dirigido.
Collection (TA0009)	T1113: Captura de pantalla	Intenta realizar capturas de pantalla del escritorio para recopilar información en el transcurso de una operación.
Impacto (TA0040)	T1657: Robo financiero	El grupo de actores de amenazas exfiltró las credenciales de inicio de sesión bancaria de la víctima para acceder a sus cuentas bancarias y causar pérdidas financieras.

IOCs:

Nombres de dominio

- tributaria[.]website
- facturacionmarzo[.]cloud
- m9b4s2[.]site
- wiqp[.]xyz
- ckws[.]info
- amarte[.]store

Direcciones IP

- 139[.]177[.]193[.]74
- 185[.]45[.]195[.]226
- 216[.]238[.]70[.]224
- 51[.]38[.]235[.]152
- 137[.]220[.]53[.]87
- 212[.]46[.]38[.]43
- 191[.]101[.]2[.]101

URLs

- hxxps[://]tributaria[.]website/
- hxxps[://]tributaria[.]website/ESP/12/151222/UP/UP
- hxxps[://]tributaria[.]website/A/08/150822/AU/TST/INDEX[.]PHP?LIST
- hxxps[://]tributaria[.]website/a/09/01092022/au/tst/index[.]php?list
- hxxps[://]tributaria[.]website/a/08/150822/up/up
- hxxps[://]tributaria[.]website/esp/12/151222/up/up
- hxxps[://]tributaria[.]website/a/W_/X\\W_YY/au/au
- hxxps[://]tributaria[.]website/a/08/150822/au/au
- hxxp[://]tributaria[.]website:443/
- hxxps[://]tributaria[.]website/A/08/150822/AU/AU
- hxxps[://]tributaria[.]website/esp/12/151222/au/au
- hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/adjuntos_0703[.]html
- hxxp[://]139[.]177[.]193[.]74/esp/12/151222/au/adjuntos_0703[.]html
- hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/logs/index[.]php?CHLG
- hxxp[://]139[.]177[.]193[.]74/
- hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/tst/index[.]php?list
- hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/adjuntos_2102[.]html
- hxxp[://]139[.]177[.]193[.]74/09/01092022/au/adjuntos_2102[.]html
- hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/adjuntos_0102[.]htm
- hxxp[://]139[.]177[.]193[.]74:443/
- hxxps[://]facturacionmarzo[.]cloud/m/archivos[.]pdf[.]html
- hxxps[://]facturacionmarzo[.]cloud/e/archivos[.]pdf[.]html

Scripts maliciosos

- 63535100bbc1ba8ce9afb5883a59a4138e95c8e33a4585b8285ea7a39e0ead3e
- 720c126f372b68ff79ef13bd1ae6fc9a6aef10669269490d7e8fb589d7d49064
- ffd43b32655fc6f1e1c10f88660b68e2c2ad7da271b0f2e3eda70ccdcb3bcee4

Powershell Downloader

- aaf456575c8761f3af9b61e015282d9162325ed09b699732bf65b53ae7b7d252

Banking Trojan

39194718b460ea174784f6a7edbccd1e3324fe1043be806927cece7a86f15611
474b25badb40f524a7b2fe089e51eb7dbafd2e3e03a9f6750f72055d05b13d76

Spam Tool

07f7575af922da1aea5aa26436a3cfcd91b419bbf31d77bf6c9d921290bc04da

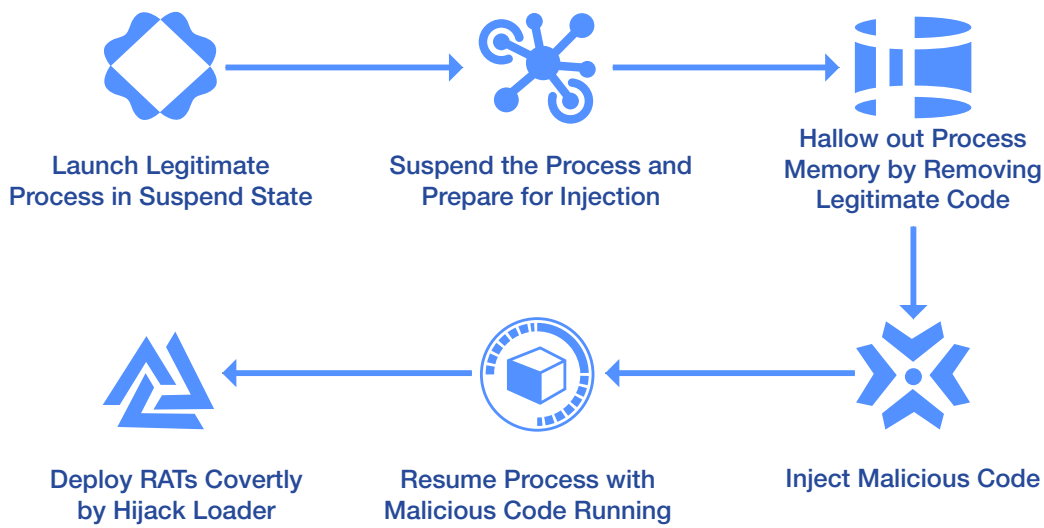
5.5 Blind Eagle

5.5.1 Actividad relevante del actor de amenazas

Blind Eagle (APT-C-36) es un sofisticado actor de amenazas latinoamericano conocido por sus operaciones de ciberespionaje que afectan a sectores como el gobierno, las finanzas y la energía en Colombia, Ecuador, Chile y Panamá.[238] Activo desde al menos 2018, Blind Eagle aprovecha constantemente las campañas de spear-phishing, haciéndose pasar por instituciones regionales legítimas para entregar troyanos de acceso remoto (RAT).[239] Estos ataques aprovechan las vulnerabilidades humanas a través de correos electrónicos engañosos con enlaces o archivos adjuntos maliciosos.

Las actividades de Blind Eagle ponen de manifiesto su capacidad de adaptación y su amplio conocimiento de las estructuras institucionales de América Latina. La creciente sofisticación técnica del grupo incluye técnicas como el process hollowing, un método sigiloso de inyección de código que les ayuda a eludir la detección y mantener un acceso persistente. En el vaciado de procesos, Blind Eagle comienza lanzando un proceso legítimo en estado suspendido y, a continuación, "vacía" su memoria eliminando el código legítimo. A continuación, inyectan su propio código malicioso, a menudo en forma de troyanos de acceso remoto como QuasarRAT o AsyncRAT, en este espacio de memoria vaciado. Una vez que el proceso se reanuda, ejecuta el código del atacante conservando su nombre original de confianza. Esto camufla la actividad maliciosa, ya que el proceso parece legítimo para los sistemas de detección de endpoints. Además, utilizan cargadores de malware personalizados, como Hijack Loader, para desplegar troyanos de acceso remoto de forma encubierta, manteniendo el control remoto sobre los dispositivos infectados y ajustando continuamente las tácticas para evitar ser detectados. El diagrama de flujo directo se muestra en la Figura 8.

Figura 8: Actividad de ataque de Blind Eagle



[238] https://securelist.com/blindeagle-apt/113414/
[239] https://research.checkpoint.com/2023/blindeagle-targeting-ecuador-with-sharpened-tools/

El impacto en las instituciones financieras ha sido sustancial, ya que las campañas de espionaje y robo de credenciales de Blind Eagle han interrumpido sistemas críticos y comprometida información sensible. Los estudios indican que América Latina ha experimentado un notable aumento de los costos de la ciberdelincuencia, siendo el sector financiero el más afectado. Según la Organización de Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID), los incidentes cibernéticos en América Latina cuestan a la región unos 90.000 millones de dólares anuales, de los cuales una parte significativa afecta a las instituciones financieras debido a las campañas de espionaje y robo de credenciales.[240] Mediante la captura de datos del navegador, a menudo a través de troyanos de keylogging y captura de pantalla, Blind Eagle puede desviar credenciales financieras, comprometiendo directamente la seguridad de las instituciones financieras de la región. Esta persistente amenaza a la ciberseguridad subraya la necesidad crítica de que las instituciones financieras mejoren sus defensas para seguir el ritmo de las tácticas cambiantes de Blind Eagle.

5.5.2 Antecedentes

Blind Eagle es un grupo de ciberespionaje que se concentra en América Latina, especialmente en los sectores gubernamental y financiero de Colombia y Ecuador.[241] Su principal método de explotación comienza con correos electrónicos de spear-phishing que disfrazan el malware de comunicaciones oficiales. Estos correos llevan adjuntos o enlaces diseñados para desplegar RATs como QuasarRAT y AsyncRAT en los sistemas de las víctimas, permitiendo a Blind Eagle acceso remoto completo.

QuasarRAT y AsyncRAT son herramientas populares para grupos como Blind Eagle debido a su accesibilidad y adaptabilidad: ambas son de código abierto y fácilmente personalizables, lo que las hace muy versátiles para necesidades específicas de espionaje. Además, estas RAT ofrecen potentes funciones como el registro de pulsaciones de teclado, la captura de pantallas y la extracción de datos, lo que permite a los atacantes capturar información confidencial y vigilar el comportamiento de los usuarios de forma eficaz. Sus técnicas de evasión incorporadas, como el cifrado y la ofuscación, les permiten eludir el software antivirus tradicional, lo que resulta esencial para el acceso encubierto sostenido necesario en las campañas de espionaje selectivo. Estos factores convierten a QuasarRAT y AsyncRAT en herramientas muy eficaces en las operaciones de Blind Eagle contra instituciones financieras y gubernamentales.

5.5.3 Correlación

Las tácticas de Blind Eagle se solapan con las de otros actores latinoamericanos, como el uso del spear-phishing y los troyanos de acceso remoto (RAT) para el robo de credenciales y el espionaje. El spear-phishing es una técnica común, utilizada por numerosos actores de amenazas para infiltrarse en las organizaciones a través de personajes regionales de confianza. Sin embargo, las características únicas de Blind Eagle radican en su amplio uso de la inyección de procesos, en particular el vaciado de procesos, y sus herramientas de distribución de malware personalizadas, como Hijack Loader, que se observan con menos frecuencia entre otros actores de amenazas.

La combinación del despliegue de RAT con técnicas avanzadas de ocultación permite a Blind Eagle mantener una presencia persistente en sistemas críticos, lo que plantea importantes dificultades para su detección y eliminación. A diferencia de otros atacantes más generalizados, sus operaciones están muy adaptadas a la región de LATAM, con correos electrónicos de phishing que incorporan un conocimiento detallado de los sistemas gubernamentales y financieros locales, lo que aumenta su eficacia y singularidad.

5.5.4 Recomendaciones

- Filtrado de correo electrónico: Implementar un filtrado robusto para capturar indicadores de spear-phishing como nombres de dominio falsificados y archivos adjuntos inusuales, reduciendo la probabilidad de que los correos electrónicos de phishing lleguen a los empleados.

- Detección y respuesta de endpoints (EDR): Refuerce las soluciones EDR para detectar actividades de inyección de procesos, como el vaciado de procesos, mejorando la visibilidad y permitiendo una respuesta rápida a las amenazas.

- Inteligencia sobre amenazas locales: Desarrollar inteligencia centrada en los actores de amenazas de LATAM para identificar patrones de ataque y anticiparse a las tácticas utilizadas por grupos como Blind Eagle, permitiendo estrategias de defensa proactivas.

- Capacitación de la fuerza laboral: levar a cabo simulacros regulares de phishing y establecer un canal de notificación de spam dedicado para TI/Seguridad, ayudando a los empleados a reconocer intentos de phishing y alertando a TI sobre posibles amenazas en tiempo real.

[240] https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf
[241] https://www.zscaler.com/blogs/security-research/blindeagle-targets-colombian-insurance-sector-blotchyquasar

5.5.5 Técnicas, tácticas y procedimientos

Blind Eagle emplea un conjunto distintivo de TTP que combina spear-phishing, inyección de procesos sofisticados y cargadores de malware personalizados para atacar a los sectores de alto valor de LATAM. Sus campañas comienzan con correos electrónicos de spear-phishing, a menudo dirigidos a gobiernos locales o entidades financieras, engañando a los destinatarios para que descarguen o abran archivos adjuntos maliciosos. Estos archivos adjuntos suelen desplegar RAT como QuasarRAT y AsyncRAT, herramientas que permiten a Blind Eagle vigilar, controlar y extraer datos confidenciales de forma remota.

Las TTP únicas del grupo incluyen técnicas avanzadas de inyección de procesos, como el vaciado de procesos, que permite al malware ejecutarse dentro de los espacios de memoria de aplicaciones legítimas. Esta técnica es fundamental para la estrategia de Blind Eagle, ya que permite a su malware mezclarse con procesos legítimos del sistema, reduciendo la probabilidad de detección por parte de las herramientas de seguridad convencionales y las defensas de los endpoints.

Otra TTP notable es su uso del Hijack Loader, un cargador de malware personalizado que distribuye RAT de forma más encubierta enmascarando sus funciones. Este cargador se adapta al sistema de defensa del objetivo, ayudando tanto en la evasión inicial como en el acceso continuo. Su sofisticado enfoque regional también aprovecha el conocimiento local para aumentar la credibilidad de sus campañas de phishing, fortaleciendo su posición inicial en objetivos de alto valor.

Blind Eagle selecciona a las víctimas en función del valor potencial de los datos y de su importancia dentro de la infraestructura de LATAM. Sus técnicas de persistencia y adaptabilidad en el despliegue de RAT reflejan una estrategia deliberada y a largo plazo destinada a extraer datos sin ser detectados, lo que supone una amenaza duradera para el panorama de la ciberseguridad de LATAM.

Tactics	Techniques	Procedures
Desarrollo de recursos	T1583.001	BlindEagle utiliza servicios DDNS para crear dominios de tercer nivel. Esos dominios sirven como C2.
Desarrollo de recursos	T1586.002	BlindEagle controlaba una carpeta de Google Drive propiedad de una organización administrativa regional colombiana.
Desarrollo de recursos	T1587.001	BlindEagle opera BlotchyQuasar, que puede considerarse una variante personalizada de QuasarRAT.
Desarrollo de recursos	T1608.001	BlindEagle montó una muestra de BlotchyQuasar en una carpeta de Google Drive comprometida y de acceso público.
Acceso inicial	T1566.002	BlindEagle intentó obtener acceso inicial al sistema de la víctima mediante un correo electrónico de phishing que incluía un enlace para descargar el malware BlotchyQuasar.
Ejecución de usuario	T1204.002	BlindEagle cambió el nombre de la muestra de BlotchyQuasar para que fuera coherente con el señuelo del correo electrónico de phishing y empujó a la víctima a ejecutar manualmente el malware.

Ejecución de usuario	T1204.001	La cadena de ataque de BlindEagle comienza cuando la víctima hace clic en un enlace incluido en el cuerpo del correo electrónico y en el archivo PDF adjunto.
Acceso inicial	T1566	Blind Eagle se entrega a través de un correo electrónico de phishing que contiene el enlace para recuperar el archivo protegido por contraseña.
Persistencia	T1547.001	La persistencia se logra a través de las claves de ejecución del Registro / carpeta de inicio
Ejecución	T1059.001	El script VBS genera PowerShell para ejecutar Ande Loader
Defense Evasion, escalada de privilegios	T1055.012	Blind Eagle está utilizando el proceso de hollowing para inyectar la carga final

DNS

- hXXps://pastebin[.]com/raw/XAfmb6xp
- edificiobaldeares.linkpc[.]net
- equipo.linkpc[.]net
- perfect5.publicvm[.]com
- perfect8.publicvm[.]com
- rxms.duckdns[.]org:57832
- njnjnjs[.]duckdns.org
- 91.213.50[.]74

Hashes

- a73057824a65a5ac982e298a80febf61
- bd4505316254f00329431fb8b2888643
- d2fc372302180fbabe18c425aa4a0a72
- c944cb638364c74431bf1dbe7dd329ff
- 64e6ad512eff12e971efdd8979086c5c
- a1f5091ad4e12f922a8e760e0980ab66
- ad578125b337168c976ff5e7e1b190b8
- e21b4c9d9da81deea2381f9b988b0f99
- 07f661aeeb0774f0cb84b0a5e970c2a5
- c4a946903cc9e9a84763ac1731cdd7dd
- 75a40cc019c39e3c2800fb2fe5aba1d3
- 0fa40788b75896a452398b6a49cc62b6
- 59a4f7aed1e3a0718592fb536e987a1d
- 456211df625002df378cf0f4af9d1a6f
- 0f35306ad4fede9a9ba0276a5e788138
- 6044b126afb86682b4a3440e2924c079
- b432e8ff5797fbaf5808d95d46524647
- a31ff54f33ced7b4180f87afb18185a7
- e3239ac16c6fe9c99d6fac0867121a88
- 2784a9fc64d244b14e7d8e4d03f41265
- 3125ae6b1462b0b48dc06bc47d8ddbc7
- b83f6c57aa04dab955fadcef6e1f4139
- a68cac786b47575a0d747282ace9a4c75e73504d
- ec2dd6753e42f0e0b173a98f074aa41d2640390c163ae77999eb6c10ff7e2edd
- 18eb0a413b80a548d2b615e11fc580cd

5.5.6 Mitigación de Blind Eagle

Acceso inicial

- **T1566.001 – Spearphishing Attachment**
  - **Mitigación:**
    - » Implantar pasarelas de seguridad de correo electrónico con detección avanzada de phishing.
    - » Formar a los usuarios para que identifiquen los intentos de phishing, incluidos los archivos adjuntos sospechosos.
    - » Habilite el sandboxing de adjuntos para detectar cargas maliciosas antes de su entrega.

Ejecución

- **T1204.001 – Enlace malicioso en el correo electrónico**
- **T1204.002 – Ejecución de archivos maliciosos**
  - **Mitigación:**
    - » Habilitar listas blancas de aplicaciones para evitar la ejecución no autorizada.
    - » Utilice soluciones de navegación segura que marquen los enlaces maliciosos antes de hacer clic.
    - » Aplique el análisis de archivos adjuntos basado en el comportamiento.
- **T1059.001 – Intérprete de comandos y scripts: PowerShell**
- **T1059.003 – Intérprete de comandos y secuencias de comandos: Windows Command Shell**
- **T1059.005 – Intérprete de comandos y secuencias de comandos: Visual Basic**
  - **Mitigación:**
    - » Restringir PowerShell y los lenguajes de scripting mediante directiva de grupo.
    - » Habilitar el registro de PowerShell (Script Block Logging) para supervisar los scripts sospechosos.
    - » Deshabilite la ejecución de macros en las aplicaciones de Office a menos que sea necesario.

Persistencia

- **T1053.005 – Tarea programada**
  - **Mitigación:**
    - » Supervisar y restringir el permiso del usuario para crear tareas programadas.
    - » Audite regularmente los registros del Programador de tareas para detectar trabajos no autorizados.
- **T1547.001 – Claves de ejecución del registro / Carpeta de inicio**
  - **Mitigación:**
    - » Restrinja el acceso de escritura a las claves de registro utilizadas para la persistencia.
    - » Supervise las entradas del registro de ejecución automática y los elementos de inicio en busca de modificaciones sospechosas.

Defense Evasion

- **T1218.009 – Ejecución de proxy binario firmado: Regsvr32**
  - **Mitigación:**
    - » Restrinja la ejecución de regsvr32.exe si no es necesario.
    - » Utilice el control de aplicaciones (reglas ASR de Microsoft Defender, AppLocker).
    - » Supervise los procesos hijos generados por regsvr32.exe en busca de anomalías.


****
1010
10101
10101
10
0101
0101010
101010
1010101
1010101

6 Recomendaciones estratégicas para la ciberseguridad en el sector financiero de América Latina

6.1 Implementación de controles de seguridad específicos para la región

- Las instituciones financieras deben adoptar controles de seguridad adaptados a las arquitecturas y amenazas bancarias regionales.
- Establecer equipos dedicados de inteligencia de amenazas que analicen el malware específico de la región y los patrones de ataque (MITRE ATT&CK, NIST SP 800-53).
- Invertir en capacidades locales de caza de amenazas y colaboración con investigadores de seguridad regionales (ISO 27001, NIST 800-150).
- Realizar ejercicios de equipo rojo que reflejen los vectores de ataque locales y los requisitos normativos (NIST 800-115).

6.2 Establecer redes de CSIRT del sector financiero

- Desarrollar equipos de respuesta a incidentes específicos del sector siguiendo el modelo del CSIRT financiero de Colombia (ISO 27035, NIST 800-61).
- Fomentar la colaboración nacional y regional a través de asociaciones público-privadas.
- Implementar protocolos estructurados de intercambio de información para inteligencia sobre amenazas en tiempo real.

6.3 Reforzar la respuesta a incidentes transfronterizos

- Estandarizar los marcos de respuesta a incidentes entre jurisdicciones (NIST 800-61, ISO 27035).
- Establecer asociaciones directas con los CERT regionales y las fuerzas de seguridad internacionales.
- Realizar ejercicios de simulación multijurisdiccionales para poner a prueba la preparación de la respuesta.

6.4 Reforzar la concienciación sobre la seguridad centrada en el ser humano

- Implemente formación en ciberseguridad específica para cada función y simulaciones de phishing (NIST 800-50, ISO 27002).
- Aplicar medidas de autenticación fuerte, incluyendo MFA e higiene de credenciales seguras (NIST 800-63, ISO 27001).
- Fomentar una cultura en la que la seguridad sea lo primero para mitigar los riesgos de ingeniería social.

6.5 Transformación digital segura y control de acceso

- Integrar la arquitectura de confianza cero (NIST SP 800-207) para hacer cumplir el acceso de mínimo privilegio.
- Implantar la MFA adaptativa y la autenticación biométrica (ISO 27001, NIST 800-63B).
- Actualizar los sistemas obsoletos con principios de diseño seguro para cumplir las normas reglamentarias.

6.6 Mejorar la gestión y supervisión de riesgos de terceros

- Establecer evaluaciones continuas de riesgos de proveedores y comprobaciones de cumplimiento (ISO 27036, NIST 800-161).
- Hacer cumplir los requisitos de seguridad contractuales alineados con los estándares globales de ciberseguridad.
- Reforzar la supervisión de amenazas en tiempo real y la detección automatizada de incidentes.

6.7 Armonizar los requisitos de presentación de informes

- LATAM debería adoptar el Perfil CRI para agilizar el cumplimiento normativo, mejorar la resiliencia cibernética y unificar la gestión de riesgos bajo un marco estandarizado.[242]
- Desarrollar un marco regional de ciberseguridad con protocolos de información estandarizados (ISO 29147, NIST 800-61).
- Ordenar plazos de divulgación de infracciones similares a la LGPD de Brasil.
- Establecer una autoridad unificada de ciberseguridad para supervisar los esfuerzos de notificación y respuesta.

6.8 Mejorar el intercambio de información

- Crear una plataforma segura para el intercambio transfronterizo de inteligencia sobre amenazas.
- Reforzar las asociaciones público-privadas para una respuesta coordinada (NIST 800-150, ISO 27010).
- Desarrollar acuerdos de cooperación para una respuesta rápida a las ciberamenazas transnacionales.

[242] https://cyberriskinstitute.org/the-profile/

6.9 Reforzar la infraestructura de ciberseguridad

- Destinar el 2-3% del PIB a iniciativas de ciberseguridad (recomendaciones de ciberseguridad de la OCDE).
- Hacer cumplir las normas de cifrado fuerte y MFA en todos los sectores críticos (NIST 800-175, ISO 27001).
- Desarrollar estrategias nacionales de ciberseguridad priorizando la protección de infraestructuras críticas.

6.10 Mejorar la educación en ciberseguridad y el desarrollo de la fuerza laboral

- Lanzar programas de educación en ciberseguridad específicos para cada sector (marco NICE del NIST, ISO 27021).
- Realizar simulacros periódicos de ciberseguridad para poner a prueba la resiliencia (NIST 800-84).
- Establecer programas de certificación para crear una mano de obra cualificada.

6.11 Reforzar los marcos normativos

- Aplicar leyes exhaustivas de protección de datos donde no las haya (ISO 27701, GDPR, NIST Privacy Framework).
- Aplicar sanciones más estrictas por incumplimiento de la notificación de vulneraciones.
- Actualizar periódicamente las normativas de ciberseguridad para alinearlas con las amenazas y tecnologías emergentes.

6.12 Fomentar la colaboración internacional

- Participar en foros mundiales de ciberseguridad para intercambiar mejores prácticas (ENISA, Índice Global de Ciberseguridad de la UIT).
- Reforzar la cooperación con las fuerzas de seguridad internacionales para combatir la ciberdelincuencia (Convenio de Budapest sobre Ciberdelincuencia).
- Buscar asistencia técnica de países con capacidades avanzadas en ciberseguridad.
- Estas medidas, alineadas con las mejores prácticas internacionales, fortalecerán al sector financiero de América Latina frente a las amenazas cibernéticas emergentes, fomentando la resiliencia y la confianza en la economía digital de la región.

7 Apéndice

7.1 Datos segmentados

Estas identificaciones de amenazas, comúnmente denominadas técnicas, son los puntos en común entre los tres actores de la amenaza.

Datos CLOP para MITER

Reconocimiento: tácticas

mitre:T1592	T1592	MitreAttackIdentifier
mitre:T1589.002	T1589.002	MitreAttackIdentifier
mitre:T1589.001	T1589.001	MitreAttackIdentifier
mitre:T1589	T1589	MitreAttackIdentifier
mitre:T1590	T1590	MitreAttackIdentifier
mitre:TA0043	TA0043	MitreAttackIdentifier

Desarrollo de recursos:

mitre:T1586	T1586	MitreAttackIdentifier

Acceso inicial:

mitre:T1190	T1190	MitreAttackIdentifier
mitre:T1133	T1133	MitreAttackIdentifier
mitre:T1566	T1566	MitreAttackIdentifier
mitre:T1078.003	T1078.003	MitreAttackIdentifier
mitre:T1091	T1091	MitreAttackIdentifier
mitre:TA0001	TA0001	MitreAttackIdentifier

Ejecución:

mitre:T1059	T1059	MitreAttackIdentifier
mitre:T1059.001	T1059.001	MitreAttackIdentifier
mitre:T1059.003	T1059.003	MitreAttackIdentifier
mitre:T1106	T1106	MitreAttackIdentifier
mitre:T1053.003	T1053.003	MitreAttackIdentifier
mitre:T1053.005	T1053.005	MitreAttackIdentifier
mitre:T1204.002	T1204.002	MitreAttackIdentifier
mitre:T1047	T1047	MitreAttackIdentifier

Persistencia:

mitre:T1098	T1098	MitreAttackIdentifier
mitre:T1547.001	T1547.001	MitreAttackIdentifier
mitre:T1037.004	T1037.004	MitreAttackIdentifier
mitre:T1136	T1136	MitreAttackIdentifier
mitre:T1543.002	T1543.002	MitreAttackIdentifier
mitre:T1133	T1133	MitreAttackIdentifier
mitre:T1574.002	T1574.002	MitreAttackIdentifier

mitre:T1053.003	T1053.003	MitreAttackIdentifier
mitre:T1053.005	T1053.005	MitreAttackIdentifier
mitre:T1505	T1505	MitreAttackIdentifier
mitre:T1505.001	T1505.001	MitreAttackIdentifier
mitre:T1505.003	T1505.003	MitreAttackIdentifier
mitre:T1078	T1078	MitreAttackIdentifier
mitre:T1078.003	T1078.003	MitreAttackIdentifier

Escalado de privilegios:

mitre:T1548.002	T1548.002	MitreAttackIdentifier
mitre:T1098	T1098	MitreAttackIdentifier
mitre:T1547.001	T1547.001	MitreAttackIdentifier
mitre:T1037.004	T1037.004	MitreAttackIdentifier
mitre:T1543.002	T1543.002	MitreAttackIdentifier
mitre:T1068	T1068	MitreAttackIdentifier
mitre:T1574.002	T1574.002	MitreAttackIdentifier
mitre:T1053.003	T1053.003	MitreAttackIdentifier
mitre:T1053.005	T1053.005	MitreAttackIdentifier
mitre:T1078.003	T1078.003	MitreAttackIdentifier
mitre:T1078	T1078	MitreAttackIdentifier

Defense Evasion:

mitre:T1222.002	T1222.002	MitreAttackIdentifier
mitre:T1497.001	T1497.001	MitreAttackIdentifier
mitre:T1078.003	T1078.003	MitreAttackIdentifier
mitre:T1078	T1078	MitreAttackIdentifier
mitre:T1218.007	T1218.007	MitreAttackIdentifier
mitre:T1218.010	T1218.010	MitreAttackIdentifier
mitre:T1218.011	T1218.011	MitreAttackIdentifier
mitre:T1553.002	T1553.002	MitreAttackIdentifier
mitre:T1112	T1112	MitreAttackIdentifier
mitre:T1070.002	T1070.002	MitreAttackIdentifier
mitre:T1574.002	T1574.002	MitreAttackIdentifier
mitre:T1140	T1140	MitreAttackIdentifier
mitre:T1622	T1622	MitreAttackIdentifier
mitre:T1548.002	T1548.002	MitreAttackIdentifier

Acceso a credenciales:

mitre:T1003.001	T1003.001	MitreAttackIdentifier
mitre:T1552.007	T1552.007	MitreAttackIdentifier

Discovery:

mitre:T1622	T1622	MitreAttackIdentifier
mitre:T1083	T1083	MitreAttackIdentifier
mitre:T1135	T1135	MitreAttackIdentifier
mitre:T1057	T1057	MitreAttackIdentifier
mitre:T1012	T1012	MitreAttackIdentifier
mitre:T1082	T1082	MitreAttackIdentifier

Movimiento lateral:

mitre:T1021	T1021	MitreAttackIdentifier
mitre:T1021.001	T1021.001	MitreAttackIdentifier
mitre:T1021.002	T1021.002	MitreAttackIdentifier
mitre:T1021.004	T1021.004	MitreAttackIdentifier
mitre:T1021.006	T1021.006	MitreAttackIdentifier
mitre:T1091	T1091	MitreAttackIdentifier

Collection:

mitre:T1005	T1005	MitreAttackIdentifier

C&C:

mitre:T1071.001	T1071.001	MitreAttackIdentifier
mitre:T1573.001	T1573.001	MitreAttackIdentifier
mitre:T1105	T1105	MitreAttackIdentifier
mitre:T1104	T1140	MitreAttackIdentifier
mitre:T1571	T1571	MitreAttackIdentifier

Exfiltración:

mitre:T1041	T1041	MitreAttackIdentifier
mitre:T1052.001	T1052.001	MitreAttackIdentifier
mitre:T1567.002	T1567.002	MitreAttackIdentifier

Impacto:

mitre:T1485	T1485	MitreAttackIdentifier
mitre:T1486	T1486	MitreAttackIdentifier
mitre:T1565	T1565	MitreAttackIdentifier
mitre:T1496	T1496	MitreAttackIdentifier
mitre:T1489	T1489	MitreAttackIdentifier

MITER Móvil:

mitre:T1406.002	T1406.002	MitreAttackIdentifier

LockBit Data for MITER

1. Reconocimiento:
2. Desarrollo de recursos:
3. Acceso inicia:

mitre:T1190	T1190	MitreAttackIdentifier
mitre:T1078	T1078	MitreAttackIdentifier

4. Ejecución:

mitre:T1059	T1059	MitreAttackIdentifier

5. Persistencia:

mitre:T1543	T1543	MitreAttackIdentifier

6. Escalada de privilegios:
7. Defense Evasion:

mitre:T1562	T1562	MitreAttackIdentifier

8. Acceso a credenciales:

mitre:T1003	T1003	MitreAttackIdentifier

9. Discovery:

mitre:T1087	T1087	MitreAttackIdentifier

10. Movimiento lateral:

mitre:T1021.001	T1021.001	MitreAttackIdentifier

11. Collection:

mitre:T1560	T1560	MitreAttackIdentifier

12. C&C:
13. Exfiltración:
14.Impacto:

mitre:T1486	T1486	MitreAttackIdentifier

Datos de Mispadu para MITER

1. Reconocimiento:
2. Desarrollo de recursos:
3. Acceso inicial:

mitre:T1566	T1566	MitreAttackIdentifier
mitre:T1566.001	T1566.001	MitreAttackIdentifier
mitre:T1190	T1190	MitreAttackIdentifier

4. Ejecución:

mitre:T1204	T1204	MitreAttackIdentifier
mitre:T1204.002	T1204.002	MitreAttackIdentifier

5. Persistencia:
6. Escalada de privilegios:

mitre:T1055.012	T1055.012	MitreAttackIdentifier
mitre:T1055.013	T1055.013	MitreAttackIdentifier

7. Defense Evasion:

mitre:T1036	T1036	MitreAttackIdentifier
mitre:T1027	T1027	MitreAttackIdentifier

8. Acceso a credenciales:

mitre:T1056.001	T1056.001	MitreAttackIdentifier
mitre:T1056.003	T1555.003	MitreAttackIdentifier

9. Discovery:

mitre:T1082	T1082	MitreAttackIdentifier
mitre:T1083	T1083	MitreAttackIdentifier

10. Movimiento lateral:
11. Collection:

mitre:T1005	T1005	MitreAttackIdentifier
mitre:T1113	T1113	MitreAttackIdentifier

12. C&C:

mitre:T1573	T1573	MitreAttackIdentifier
mitre:T1105	T1105	MitreAttackIdentifier
mitre:T1102.002	T1102.002	MitreAttackIdentifier

13. Exfiltración:

mitre:T1041	T1041	MitreAttackIdentifier
mitre:T1567	T1567	MitreAttackIdentifier

Datos de Horabot para Mitre

1. Reconocimiento:
2. Desarrollo de recursos:

mitre:T1584	T1584	MitreAttackIdentifier
mitre:T1584.005	T1584.005	MitreAttackIdentifier

3. Acceso inicial:

mitre:TA0001	TA0001	MitreAttackIdentifier
mitre:T1566	T1566	MitreAttackIdentifier
mitre:T1566.001	T1566.001	MitreAttackIdentifier
mitre:T1190	T1190	MitreAttackIdentifier
mitre:T1078	T1078	MitreAttackIdentifier

4. Ejecución:

mitre:TA0002	TA0002	MitreAttackIdentifier
mitre:TA1059	TA1059	MitreAttackIdentifier
mitre:T1059.001	T1059.001	MitreAttackIdentifier
mitre:T1204	T1204	MitreAttackIdentifier
mitre:T1204.001	T1204.001	MitreAttackIdentifier
mitre:T1106	T1106	MitreAttackIdentifier

5. Persistencia:

mitre:TA0003	TA0003	MitreAttackIdentifier
mitre:T1574	T1574	MitreAttackIdentifier
mitre:T1574.002	T1574.002	MitreAttackIdentifier
mitre:T1547.009	T1547.009	MitreAttackIdentifier
mitre:T1547.001	T1547.001	MitreAttackIdentifier

6. Escalada de privilegios:

mitre:TA0004	TA0004	MitreAttackIdentifier

7. Defense Evasion:

mitre:TA0005	TA0005	MitreAttackIdentifier
mitre:T1036	T1036	MitreAttackIdentifier
mitre:T1027	T1027	MitreAttackIdentifier
mitre:T1497	T1497	MitreAttackIdentifier
mitre:T1070	T1070	MitreAttackIdentifier
mitre:T1070.004	T1070.004	MitreAttackIdentifier

8. Acceso a credenciales:

mitre:T1056.001	T1056.001	MitreAttackIdentifier
mitre:T1003	T1003	MitreAttackIdentifier
mitre:T1083	T1083	MitreAttackIdentifier

9. Discovery:

mitre:TA0007	TA0007	MitreAttackIdentifier
mitre:T1082	T1082	MitreAttackIdentifier

10. Movimiento lateral:
11. Collection:

mitre:TA0009	TA0009	MitreAttackIdentifier
mitre:T1115	T1115	MitreAttackIdentifier
mitre:T1113	T1113	MitreAttackIdentifier

12. C&C:

mitre:TA0011	TA0011	MitreAttackIdentifier

13. Exfiltración:
14. Impacto:

mitre:TA0040	TA0040	MitreAttackIdentifier

7.2 Definiciones

Tácticas, Técnicas y Procedimientos: Los comportamientos, estrategias y métodos más comunes utilizados por los atacantes para desarrollar y ejecutar ciberataques contra instituciones financieras.[243]

Phishing: El phishing es un tipo de ciberataque en el que el atacante utiliza diversas técnicas para atraer a las víctimas y hacerles revelar su información personal o empresarial. Varios tipos de phishing incluyen:

1. **Spear Phishing:** Es un tipo de ataque en el que se ataca a individuos de organizaciones, normalmente a través de un enlace malicioso que les pide que revelen sus credenciales de acceso. Esto conduce al acceso no autorizado de terceros a los datos de la empresa.

2. **Whaling:** Es un ataque de phishing dirigido a miembros ejecutivos/empleados de nivel C para que revelen información sensible.[244]

3. **Smishing:** Es un tipo de ataque en el que el agresor envía mensajes/enlaces maliciosos o fraudulentos a través de mensajes y, en la mayoría de los casos, se atrae a la gente para que revele nombres de usuario, contraseñas, etc.

4. **Vishing:** El phishing de voz se conoce comúnmente como Vishing. En este caso, los atacantes realizan llamadas fraudulentas representando a organizaciones y las engañan para que revelen sus datos mediante manipulación.

Malware: Se trata de software malicioso o un programa o simplemente una pequeña pieza de código que explota una vulnerabilidad.

Ransomware: Es un software malicioso que cifra los datos de la víctima y exige un rescate para descifrarlos. A menudo se envía a través de correos electrónicos de phishing o exploits al vulnerar.

Fileless Malware: Malware que opera sin instalar ningún archivo en el sistema infectado, lo que dificulta su detección.

Spyware: Software que vigila en secreto la actividad en línea de un usuario para recopilar información sensible.

Adware: Un tipo de spyware que muestra anuncios no deseados al usuario.[245]

Troyanos: Programas maliciosos disfrazados de software legítimo, a menudo descargados mediante tácticas de ingeniería social.[246]

Gusanos: Programas maliciosos autorreplicantes que se propagan rápidamente por las redes, pudiendo dañar archivos o instalar programas maliciosos adicionales.

Rootkits: Software que proporciona a un atacante un control sigiloso y persistente sobre un sistema comprometido.

Malware para móviles: Software malicioso diseñado específicamente para dispositivos móviles, a menudo distribuido a través de aplicaciones maliciosas o redes comprometidas.

Exploits: Software o código que aprovecha vulnerabilidades en sistemas operativos o aplicaciones para obtener acceso no autorizado.[247]

Scareware: Malware que intenta asustar a los usuarios haciéndoles creer que sus sistemas están infectados, a menudo promocionando software antivirus falso.

Keyloggers: Software que registra las pulsaciones de teclas introducidas en un dispositivo, capturando potencialmente información sensible.

Botnets: Redes de dispositivos comprometidos controlados por un atacante para lanzar diversas actividades maliciosas.

Malspam: Correos electrónicos no deseados que contienen adjuntos o enlaces maliciosos diseñados para distribuir programas maliciosos.

Wiper Attacks: Programas maliciosos diseñados para eliminar o corromper permanentemente los datos de los sistemas atacados, a menudo utilizados en la ciberguerra o el hacktivismo.

DOS/DDOS: Los ataques de denegación de servicio (DoS) son ciberataques cuyo objetivo es interrumpir una red, un servidor o un sitio web saturando el tráfico. Esto puede hacer que el objetivo sea inaccesible para los usuarios legítimos. Los ataques distribuidos de denegación de servicio (DDoS) son una variante más sofisticada de los ataques DoS. Implican la coordinación de múltiples sistemas comprometidos (conocidos como bots) para lanzar ataques simultáneos contra un objetivo, amplificando el impacto y haciéndolo más difícil de defender.

Ataques de inyección: Los ataques de inyección son un tipo de ciberataque en el que se inserta código malicioso en una aplicación o sistema vulnerable. Esto puede tener diversas consecuencias perjudiciales, como el acceso no autorizado, el robo de datos y la interrupción del sistema.[248]

[243] https://www.nextias.com/ca/current-affairs/14-09-2023/cybercrime-investigation-tool)
[244] https://es.cryoserver.com/blog/how-to-avoid-phishing-scams/
[245] https://top10antivirus.site/the-intricacies-of-spyware-a-breakdown-of-their-invasive-techniques/
[246] https://softwarelab.org/best-antivirus-with-firewall/
[247] https://www.mobiletracker.org/law-enforcement-implications-in-hacking-mobile-devices_wpg_881/
[248] https://www.securityjourney.com/post/owasp-top-10-injection-attacks-explained

Tipos comunes de ataques de inyección:

- **SQL Injection:** Aprovechamiento de vulnerabilidades en consultas SQL para ejecutar comandos no autorizados.
- **Command Injection:** Ejecución de comandos arbitrarios en el sistema operativo a través de parámetros de entrada vulnerables.
- **Cross-Site Scripting (XSS):** Inyección de scripts maliciosos en páginas web para robar datos del usuario o secuestrar sesiones.[249]
- **XML Injection:** Aprovechamiento de vulnerabilidades en el procesamiento de XML para inyectar código XML malicioso.
- **LDAP Injection:** Inyección de consultas LDAP maliciosas para obtener acceso no autorizado a servicios de directorio.

7.3 Vulnerabilidades, exposiciones e indicadores de compromiso comunes

El glosario de vulnerabilidades clasificadas más comunes en las instituciones financieras se ha analizado y evaluado en función del nivel de amenaza de la vulnerabilidad. La gestión de vulnerabilidades y amenazas es crucial para las instituciones financieras debido a la naturaleza sensible de los datos que manejan.[250] A continuación se presentan algunos glosarios y marcos comúnmente utilizados para las vulnerabilidades clasificadas y los indicadores de compromiso (IoCs).

Vulnerabilidades y exposiciones comunes (CVE):

- Una lista estandarizada de vulnerabilidades de ciberseguridad conocidas públicamente.
- Cada entrada de CVE incluye un número de identificación, una descripción y referencias a avisos de seguridad relacionados.
- Las instituciones financieras utilizan CVE para rastrear y evaluar las vulnerabilidades de sus sistemas.

Sistema común de puntuación de vulnerabilidades (CVSS):

- Un marco para evaluar la gravedad de las vulnerabilidades.[251]
- Asigna una puntuación basada en la explotabilidad y el Impacto, ayudando a las instituciones a priorizar su respuesta.

Base de datos nacional de vulnerabilidades (NVD):

- Un repositorio gubernamental estadounidense de datos de gestión de vulnerabilidades, que incluye entradas CVE, puntuaciones CVSS y metadatos adicionales.
- Ampliamente utilizada por las instituciones financieras para la evaluación y gestión de vulnerabilidades.

Centro de análisis e intercambio de información de servicios financieros (FS-ISAC):[252]

- Proporciona inteligencia sobre amenazas e información sobre vulnerabilidades específicamente adaptada al sector financiero.
- Comparte indicadores de compromiso e inteligencia sobre amenazas para ayudar a las instituciones financieras a protegerse.

Marco ATT&CK de MITRE:

- Proporciona una base de conocimientos sobre tácticas y técnicas de los adversarios basada en observaciones del mundo real.[253]
- Utilizado por las instituciones financieras para comprender y defenderse de métodos de ataque sofisticados.

7.4 Indicadores de compromiso (IOC)

- File Hashes: Valores únicos que representan archivos que podrían utilizarse para detectar actividad maliciosa.
- Direcciones IP: Direcciones asociadas con actividades maliciosas conocidas.
- URLs/Dominios: Los atacantes utilizan direcciones web para controlar malware o exfiltrar datos.
- Direcciones de correo electrónico: Direcciones implicadas en phishing u otros ataques basados en correo electrónico.

Estas herramientas y marcos ayudan a las instituciones financieras a gestionar y mitigar eficazmente las amenazas de ciberseguridad, garantizando la protección de sus datos sensibles.

[249] https://datapacket.net/website-security/
[250] https://neovera.com/cybersecurity-outlook-for-financial-institutions/
[251] https://hadrian.io/blog/tag/security-solutions
[252] https://www.ibm.com/reports/threat-intelligence
[253] https://nsarchive.gwu.edu/media/29421/ocr

7.5 Evidencia forense

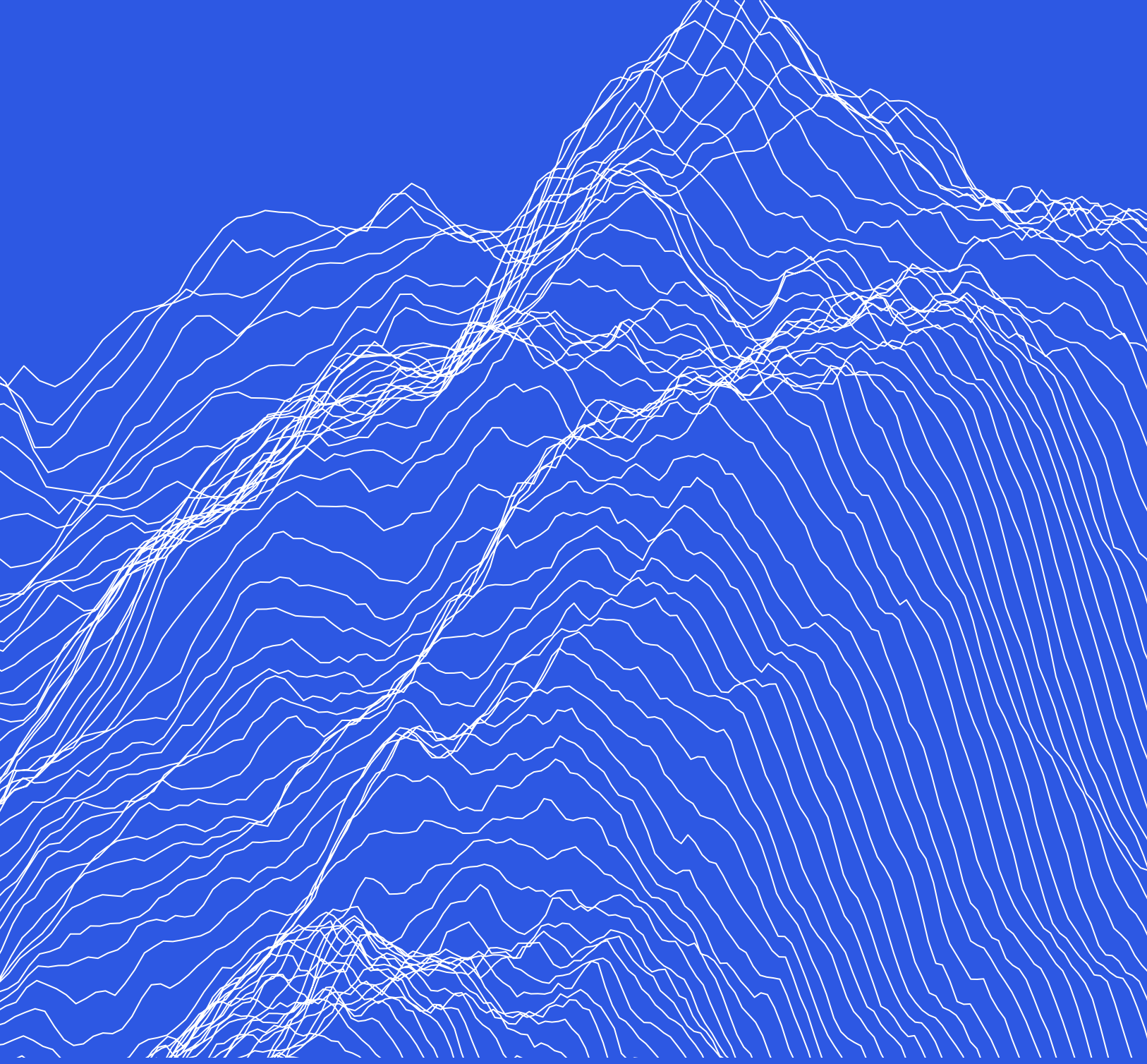
Las tres principales pruebas forenses de posibles intrusiones en un sistema host o red para Instituciones Financieras.[254]

- **Escalado de privilegios:** Indica que un atacante ha obtenido un acceso de nivel superior al inicialmente previsto, lo que le permite ejecutar acciones más dañinas.

- **Movimiento lateral:** Esto muestra que un atacante se ha movido de un sistema comprometido a otro dentro de la red, potencialmente propagando malware u obteniendo acceso a datos confidenciales.

- **Exfiltración de datos:** Este es el signo más crítico de una intrusión exitosa, ya que significa que los datos sensibles han sido robados y pueden ser utilizados con fines maliciosos.

[254] https://core.ac.uk/download/346450152.pdf



DIGI
AMERICAS