Cenário de Riscos Cibernéticos para o Setor Financeiro da América Latina em 2025

Uma Análise do Comportamento de Ameaças e das Táticas de Proteção das Instituições Financeiras na Região

DIGI AMERICAS

Duke | PRATT SCHOOL of ENGINEERING

Em parceria com

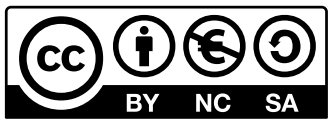
Recorded Future®

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



Direitos sob Licença CC BY-NC-SA: A distribuição, modificação ou reinterpretação deste conteúdo é permitida, desde que voltada a fins não comerciais e com a devida menção aos autores originais. Qualquer adaptação do conteúdo deverá manter a mesma licença. Todas as informações contidas neste relatório são exclusivamente informativas e não constituem posicionamento institucional do Center for Cybersecurity Policy and Law ou de seus integrantes. Para dúvidas ou solicitações, entre em contato com: admin@digiamericas.org

Créditos

Universidade 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

Resumo Executivo

De acordo com o Índice de Cibersegurança da ONU, a América Latina está entre as regiões com menor nível de prontidão para enfrentar ataques cibernéticos.[1] Essa fragilidade é resultado de investimentos insuficientes em cibersegurança, da escassez de profissionais especializados e de marcos regulatórios ainda pouco robustos.[2] Embora setores como fintech e comércio eletrônico tenham passado por uma intensa transformação digital após a pandemia de COVID-19, esses avanços não foram acompanhados por mecanismos de proteção à altura. Como ressalta Louise Marie Hurel, fundadora da Rede Latino-Americana de Pesquisa em Cibersegurança, “o espírito empreendedor e inovador da região não vem acompanhado de uma cultura de segurança”.[3]

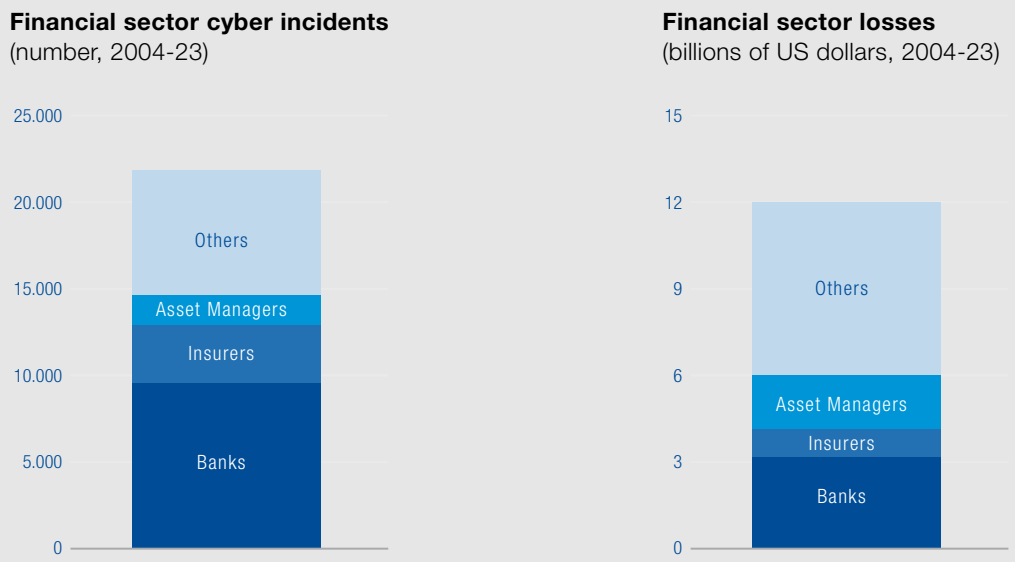
O levantamento destaca que ataques de alto impacto, como os que atingiram o Ministério da Fazenda da Costa Rica e o judiciário do Brasil, ilustram a urgência de reforçar defesas no continente. A análise revela que apenas sete países latino-americanos dispõem de planos para salvaguardar infraestrutura crítica, e só 20 mantêm CSIRTs plenamente operacionais. Com a incidência global de violações de dados crescendo 34,5% e os ataques de ransomware subindo 84% em 2023, a lacuna de proteção na região exige resposta imediata no âmbito financeiro.[4]

A pesquisa LATAM Threat Landscape, conduzida pela Universidade Duke com base nos dados do Intelligence Graph da Recorded Future, examina os três principais grupos de ação maliciosa que têm como alvo o setor financeiro latino-americano e recomenda controles para prevenir ataques e mitigar seus impactos. A análise detalhada identificou CL0P, LockBit, Horabot, Blind Eagle, e Mispadu como os atores mais agressivos.

As violações cibernéticas em instituições financeiras latino-americanas têm se tornado cada vez mais frequentes e apresentam desafios específicos de segurança. Dados de 2023 indicam que a região registra a maior porcentagem de ataques envolvendo ransomware em organizações: 79% dos incidentes, contra uma média global de 53%.[5] Este relatório detalha as táticas e motivações dos principais grupos de ameaça: CL0P, Mispadu, Horabot, Blind Eagle, e LockBit, evidenciando a utilização de padrões TTPs análogos que intensificam o impacto sobre o setor.

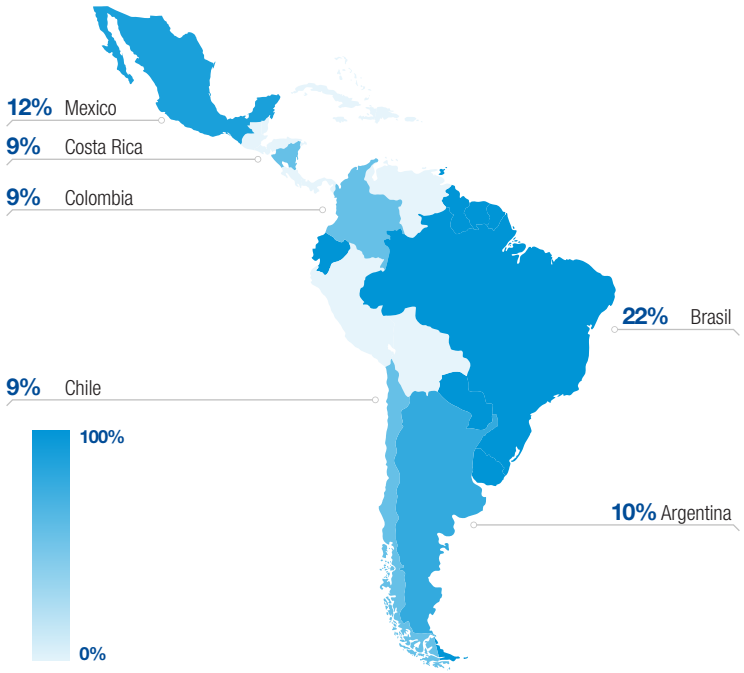
[1] https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx
[2] https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx
[3] https://www.americasquarterly.org/article/new-aq-hackers-paradise-why-latin-america-is-so-vulnerable/#:~:text=%E2%80%9CLatin%20America's%20entrepreneurial%20and%20innovative,cyberbreaches-%20start%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: Incidência e Impactos de Ciberataques no Setor Financeiro



As instituições financeiras da América Latina enfrentam fragilidades que se destacam em relação ao restante do mundo. O ambiente regional é especialmente propício à atuação de agentes maliciosos, com Brasil, México, Argentina, Colômbia e Peru despontando como os principais alvos. Em 2023, metade dos países vítimas de ataques estavam localizados na América Latina, que também concentrou 12% das ocorrências globais de crimes cibernéticos.[6]

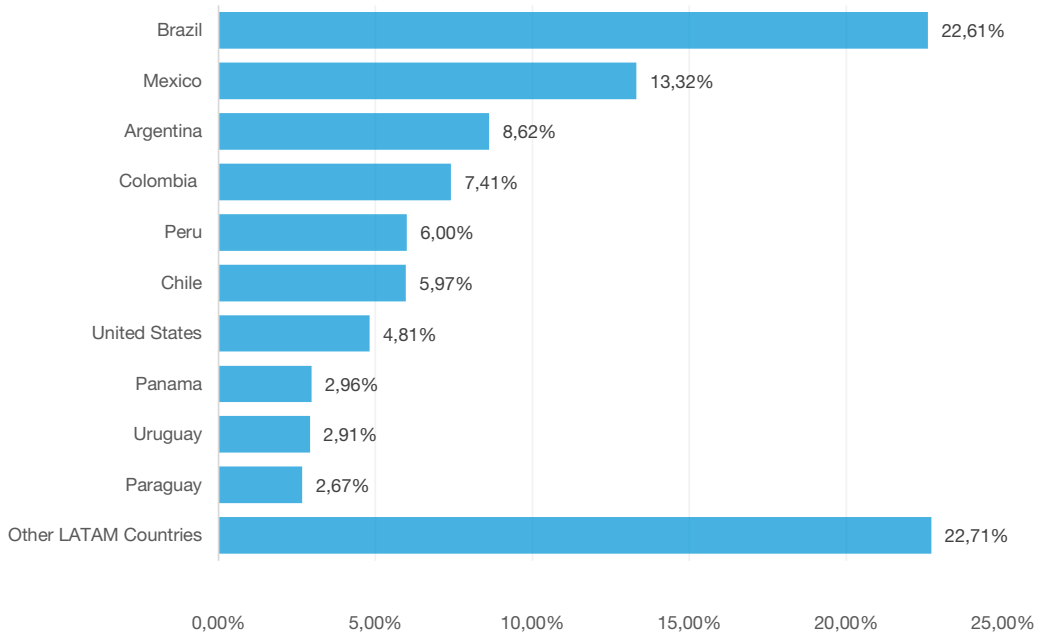
Figura 2: Distribuição dos Ataques Bem-Sucedidos na América Latina



Ao longo de 2023, a América Latina foi palco de 1.498 ataques do tipo ransomware e 6.048 casos de phishing, organizados por 33 grupos distintos, segundo dados da SOCRader (2024, pp. 4–5).[7] A escassez de recursos destinados à segurança digital, aliada à instabilidade econômica e à ausência de regulação adequada, ampliou significativamente a exposição das instituições financeiras a riscos cibernéticos.

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

Figura 3: Países da América Latina Mais Visados na Dark Web



As evidências apresentadas neste relatório refletem um retrato abrangente do cenário de ameaças digitais, embora reconheçam os limites da coleta de dados abertos, que é marcada por processos longos, cobertura incompleta e risco de negligência a ameaças de menor visibilidade.[8] Ainda assim, os achados aqui reunidos oferecem diretrizes valiosas para o fortalecimento das práticas de segurança, com o objetivo de aumentar a robustez estrutural do setor financeiro latino-americano.

O setor financeiro da América Latina deve considerar a adoção de uma estratégia de defesa cibernética baseada no perfil dos cibercriminosos, com foco na mitigação dos impactos dos ataques. Instituições do setor que aplicam uma abordagem informada conseguem se preparar melhor para táticas, técnicas e procedimentos (TTPs) recorrentes entre os atacantes. A análise e a incorporação dos TTPs mapeados por esses grupos permitem que os times de defesa cibernética implementem controles com maior eficácia.

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

Índice

Resumo Executivo 3
1 Introdução 9
1.1 Objetivos 9
2 Contexto 10
2.1 Desalinhamento e Falta de Preparo 10
2.2 Riscos Históricos Associados ao Ransomware 11
2.2.1 Introdução 11
2.2.2 Análise de Tendências em Vulnerabilidades Cibernéticas 12
2.2.3 Análise de Lacunas e Impactos Futuros 12
2.2.4 Evolução da Maturidade em Segurança Cibernética: 2018 a 2024 13
2.2.5 Tendências Futuras e Potencial de Impacto 13
2.3 Impacto Econômico do Ransomware no Setor Financeiro Latino-Americano 14
2.3.1 Estudo de Caso 1: LockBit 3.0 compromete banco brasileiro por meio de infraestrutura virtual 14
2.3.2 Estudo de Caso 2: Play Ransomware mira infraestrutura virtual de empresa chilena 14
2.4 Capacidade de Enfrentamento ao Ransomware 15
2.4.1 Diagnóstico da Infraestrutura de Resposta na Região 15
2.4.2 Preparação Técnica e Limitações de Recursos 16
2.4.3 Coordenação de Resposta Transfronteiriça 17
2.4.4 Mecanismos de Troca de Informação e Exposição no Setor Financeiro 18
2.4.5 Fragilidade nos Modelos de Colaboração Público–Privada 18
3 Panorama do Setor 20
3.1 Perfis de Ameaças que Miram a Indústria Financeira na América Latina 20
3.1.1 Déficit de Profissionais de Segurança Digital 20
3.1.2 Ajuste Orçamentário em Cibersegurança Frente ao Aumento das Ameaças 21
3.1.3 Fundamentos para a Expansão dos Investimentos em Cibersegurança 22
3.1.4 Transição de Agências Físicas para Bancos Online e via Aplicativos 23
3.2 Fatores Socioeconômicos com Influência na Vulnerabilidade Cibernética 23
3.2.1 Expansão Rápida das Fintechs 23
3.2.2 Dependência de Sistemas Obsoletos 23
3.2.3 Desigualdade de Acesso e Vulnerabilidade Digital 24
4 Lacunas Regulatórias 25
4.1 Ausência de Padrões Uniformes para Notificação de Incidentes com Ransomware 25
5 Perfis de Ameaça Ativa no Setor Corporativo 27
5.1 CL0P 27
5.1.1 Perfil das Vítimas e Dimensão dos Ataques 27
5.1.2 Arquitetura Técnica e Recursos do Malware 27
5.1.3 Panorama da transformação operacional do grupo CL0P 28
5.1.4 Impacto na Infraestrutura Financeira 29
5.1.5 Lacunas na Regulamentação e em Políticas Públicas 30
5.1.6 Panorama do Setor Bancário Latino-Americano e Aceleração Digital 31

5.1.7 Conflito Entre Pressão por Lucros e Investimentos em Segurança 31
5.1.8 Fragilidades Específicas do Setor Financeiro 31
5.1.9 Riscos em Cadeia Derivados de Fragilidades no Setor Público 32
5.1.10 Convergência de Vulnerabilidades Criando Oportunidade Estratégica para o CL0P 32
5.1.11 Implicações Futuras 33
5.1.12 Táticas, Técnicas e Procedimentos do CL0P 34
5.1.13 Indicadores Técnicos e Estratégias de Contenção para Ameaças Avançadas como o CL0P 38
5.2 LockBit 44
5.2.1 Atividade Operacional Relevante 44
5.2.2 Contexto Operacional 45
5.2.3 Estratégias de Extorsão e Modus Operandi 45
5.2.4 Táticas e Ferramentas de Comprometimento 45
5.2.5 Recomendações Técnicas e Táticas Contra o LockBit 49
5.3 Mispadu 55
5.3.1 Estratégias do Mispadu: Como o Malware Explora Fragilidades da Infraestrutura Digital na América Latina 55
5.3.2 Táticas e Técnicas para Garantir Persistência e Lucro 56
5.3.3 Perfil Operacional do Mispadu: Táticas, Técnicas e Procedimentos Utilizados 56
5.4 Horabot 59
5.4.1 Capacidades Técnicas do Horabot 60
5.4.2 Semelhanças Operacionais entre Horabot e Mispadu 61
5.4.3 Táticas, Técnicas e Procedimentos do Horabot 61
5.5 Blind Eagle 64
5.5.1 Atividade Relevante do APT Blind Eagle 65
5.5.2 Contexto 65
5.5.3 Correlação 65
5.5.4 Recomendações 65
5.5.5 Techniques, Tactic and Procedures 65
5.5.6 Mitigações para o Blind Eagle 68
6 Recomendações Estratégicas para Fortalecer a Segurança Cibernética no Setor Financeiro Latino-Americano 71
6.1 Adaptação dos Controles de Segurança à Realidade Regional 71
6.2 Formação de Redes Setoriais de CSIRTs Financeiros 71
6.3 Melhoria da Capacidade de Resposta Multinacional 71
6.4 Fortalecimento da Segurança Baseada em Pessoas 71
6.5 Transformação Digital Segura e Gestão de Acesso 71
6.6 Fortalecimento da Gestão de Terceiros e Monitoramento Contínuo 71
6.7 Padronização de Requisitos Regulatórios 72
6.8 Melhoria na Troca de Informações 72
6.9 Expansão da Infraestrutura de Defesa Cibernética 72
6.10 Capacitação Profissional e Educação em Cibersegurança 72
6.11 Fortalecimento dos Instrumentos Regulatórios 72
6.12 Cooperação Internacional Estratégica 72
7 Apêndice 73
7.1 Dados Segmentados 73
7.2 Definições 80
7.3 Panorama de Vulnerabilidades e Indicadores de Comprometimento no Setor Financeiro 81
7.4 Indicadores de Comprometimento (IOCs) 81

1 Introdução

A digitalização do setor financeiro na América Latina avançou de forma acelerada nos últimos anos, impulsionada pela popularização dos serviços de fintech, pela conectividade em expansão e pelo aumento da adesão ao banco digital por parte da população. No entanto, esse progresso ocorreu mais rápido do que a evolução das políticas e práticas de cibersegurança. Com isso, o sistema financeiro da região se tornou um alvo ainda mais exposto à ação de grupos criminosos digitais cada vez mais bem estruturados. Em um ambiente onde o crime cibernético se profissionaliza rapidamente, os riscos à integridade financeira, à confiança do usuário e à estabilidade nacional se multiplicam.

Este relatório examina o ecossistema de ciberameaças que afetam o setor financeiro latino-americano, com foco nos principais agentes por trás dos ataques, nas estratégias que eles empregam e nas fragilidades que tornam o ambiente propício à exploração. A análise combina dados de inteligência de ameaças, estudos de casos regionais e observações de especialistas para traçar um retrato aprofundado das motivações e métodos dos grupos mais ativos na região. Também são discutidas barreiras estruturais relevantes, como a ausência de regulamentações adequadas, a escassez de talentos especializados e a baixa priorização de investimentos em segurança da informação.

A proposta do estudo é oferecer, de um lado, um diagnóstico detalhado do cenário de risco que se desenha para instituições financeiras latino-americanas e, de outro, propor caminhos concretos para fortalecer a capacidade de defesa digital no setor. O relatório dá atenção especial à atuação de cinco grupos cibercriminosos: CL0P, LockBit, Mispadu, Blind Eagle, e Horabot, cujas ações representam padrões recorrentes nas ameaças que visam instituições financeiras.

A estrutura do documento se organiza da seguinte forma: a Seção 2 contextualiza o cenário atual e apresenta os principais grupos cibercriminosos em atividade na região. A Seção 3 analisa o nível de preparação cibernética dos países, as vulnerabilidades institucionais e as respostas estratégicas adotadas até o momento. A Seção 4 discute os principais vazios regulatórios que ainda persistem. Na Seção 5, são detalhadas cinco APTs (ameaças persistentes avançadas), seu histórico de ataques na região, seus métodos de operação e orientações específicas para enfrentamento. A Seção 6 encerra o relatório com recomendações estratégicas para elevar o patamar de resiliência digital no setor financeiro da América Latina.

1.1 Objetivos

Com base em dados da plataforma Recorded Future, a equipe de análise buscou entender como diferentes grupos maliciosos têm replicado padrões semelhantes de ataque contra empresas de serviços financeiros na América Latina. A investigação foi guiada por quatro metas centrais:

(1) Mapear os principais grupos de ameaça com foco no setor financeiro da região, incluindo suas bases operacionais.

(2) Entender as práticas táticas e técnicas utilizadas por esses grupos em seus ataques.

(3) Avaliar os efeitos dessas ações sobre as instituições financeiras e os sistemas que as sustentam.

(4) Elaborar recomendações específicas para neutralizar essas táticas, utilizando o modelo MITRE ATT&CK e diretrizes úteis para profissionais da área de segurança cibernética.

2 Contexto

Nos últimos cinco anos, os ataques cibernéticos contra o setor financeiro latino-americano aumentaram consideravelmente, refletindo um crescimento global que vem mantendo uma média de 25% ao ano desde 2014.[9] Conforme mostra o Relatório Global de Estabilidade Financeira de 2024,[10] o risco de prejuízos severos causados por crimes digitais mais do que quadruplicou desde 2017, chegando à marca de 2,5 bilhões de dólares. Já o Relatório LATAM CISO 2024 aponta falhas estruturais como um dos principais fatores por trás do sucesso e da frequência desses ataques em países como Brasil, Argentina, México e Costa Rica. Entre 2020 e 2025, essas falhas envolveram desde limitações técnicas até lacunas graves de coordenação entre agentes públicos e privados. Apenas metade dos países analisados havia adotado uma estratégia nacional de cibersegurança com foco específico no setor financeiro, ou implementado regulamentações próprias para essa área.

Esse cenário colocou a América Latina como responsável por 12% dos ataques cibernéticos em escala global em 2022, superando regiões como Oriente Médio e África, que juntas representaram 7% dos incidentes, mesmo operando com capacidades similares.[11] A maior concentração de ataques se deu em três países: Brasil, México e Argentina, cujos sistemas financeiros robustos se tornaram alvos prioritários de grupos criminosos. A escalada desses incidentes levanta preocupações sobre a resiliência financeira da região, especialmente considerando que instituições financeiras estão entre os principais focos de ataques e compõem uma parte expressiva do universo afetado.[12] À medida que os incidentes aumentam, a estabilidade financeira da região fica cada vez mais ameaçada, já que o setor financeiro é um dos principais alvos de agentes maliciosos e representa uma fatia relevante dos setores visados. Só o setor financeiro e de seguros responde por 39,47% dos incidentes cibernéticos divulgados na América Latina.[13] Diante disso, a falta de resposta adequada pode acarretar consequências econômicas sérias, reforçando a urgência de investimentos sólidos em segurança cibernética.

2.1 Desalinhamento e Falta de Preparo

O aumento da vulnerabilidade das instituições financeiras latino-americanas a ataques cibernéticos está ligado a uma combinação de fatores estruturais.

1. Baixo nível de capacitação interna e ausência de cultura de segurança digital: A fragilidade começa pela escassez de conhecimento técnico nas equipes. Sem uma política sólida de treinamento, os funcionários seguem despreparados para lidar com ameaças, e os clientes continuam sem acesso a campanhas que os alertem sobre fraudes e golpes digitais.

2. Falta de padronização e regulação efetiva: Muitas instituições deixam de adotar frameworks reconhecidos internacionalmente, como o NIST CSF ou a ISO 27001. Essa escolha voluntária de não seguir boas práticas abre brechas significativas, exploradas por grupos que precisam encontrar apenas uma vulnerabilidade para comprometer toda uma organização.

3. Baixo investimento em tecnologia, tanto no nível de infraestrutura quanto na camada de software, tem sido um dos principais fatores que ampliam os riscos de segurança digital na América Latina. A persistência no uso de sistemas desatualizados compromete diretamente ambientes críticos, abrindo espaço para ações maliciosas que comprometem a integridade do setor financeiro e dificultam a defesa contra ameaças avançadas. A diferença tecnológica em relação a países mais desenvolvidos, como os da Europa e América do Norte, aprofunda esse cenário de fragilidade regional.[14]

O custo financeiro dos ataques cibernéticos tem sido significativo em todo o mundo. Segundo a IBM Security, em 2020, o custo médio de uma violação de dados girava em torno de US$ 3,86 milhões, levando em conta despesas judiciais, penalidades regulatórias, perdas de reputação e erosão da confiança dos clientes.[15] Um exemplo emblemático foi o ataque de ransomware à Colonial Pipeline em maio de 2021, que interrompeu a distribuição de combustível em diversas regiões dos EUA, gerando escassez e pânico entre consumidores. O ataque, atribuído ao grupo DarkSide, levou a empresa a pagar US$ 4,4 milhões em resgate, mas os danos foram muito além da paralisação temporária: houve

[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

impactos na cadeia de abastecimento e intensificação das exigências regulatórias.[16] O episódio expôs pontos fracos em sistemas de controle industrial, reforçando a necessidade urgente de estratégias mais proativas e arquiteturas de segurança mais rígidas para mitigar riscos de grande escala.

O mesmo tipo de fragilidade revelado no caso da Colonial Pipeline se aplica de forma ainda mais crítica à realidade latino-americana. A região enfrenta um cenário regulatório fragmentado, infraestrutura cibernética deficiente e baixo engajamento da população e do setor privado em práticas preventivas. Esses fatores tornam o ambiente ideal para cibercriminosos que atuam com foco financeiro. A América Latina lidera em proporção de ataques por ransomware, atingindo 79% do total de ataques registrados, frente a uma média global de 53%. Em 94% desses casos, as técnicas envolvidas foram intrusão de sistemas, engenharia social e exploração de aplicações web pouco protegidas.[17] Atualmente, o custo médio global de uma violação de dados subiu para US$ 4,45 milhões,[18] e na América Latina o valor chegou a US$ 2,46 milhões, o mais alto desde 2020.[19] De acordo com o Global Cybersecurity Index 2020, a região ocupa as últimas posições em preparação cibernética, o que amplia sua exposição e limita sua capacidade de resposta.[20] Sem avanços concretos, o impacto econômico desses ataques deve continuar crescendo nos próximos anos.

2.2 Riscos Históricos Associados ao Ransomware

2.2.1 Introdução

O setor financeiro da América Latina vivenciou uma escalada significativa de ataques cibernéticos sofisticados entre 2018 e 2024, evidenciando fragilidades críticas na infraestrutura digital da região. Esta análise examina 12 incidentes relevantes que afetaram bancos, instituições financeiras e sistemas governamentais em países como Chile, Brasil, México, Argentina e outros. Os ataques, que vão desde o roubo de US$ 10 milhões ao Banco do Chile em 2018 [21] [22] até o vazamento de dados da Bankingly em 2024, que afetou 135 mil clientes,[23] refletem um cenário de ameaças em constante evolução, marcado por ransomwares e grupos de ameaças persistentes avançadas (APT).

O estudo revela uma mudança clara de foco por parte dos atacantes: os provedores terceirizados e as plataformas de tecnologia financeira tornaram-se os novos vetores preferenciais para ataques em larga escala. À medida que o ecossistema financeiro passa a depender cada vez mais de soluções terceirizadas, surgem novos pontos de exposição. Fornecedores de software e plataformas SaaS, por exemplo, se tornam alvos em cadeias de suprimentos digitais, como evidenciado no caso da falha no software de transferência de arquivos da Progress Software, que resultou na exfiltração massiva de dados.[24] Ambientes IaaS também impõem riscos, com falhas de configuração e lacunas em controles de acesso que podem levar à paralisação de operações. A violação da Bankingly, provocada por buckets de armazenamento expostos por ausência de autenticação adequada, resultou na exposição de dados bancários sensíveis de sete instituições da região.[25] Tais ocorrências escancaram a urgência de uma política robusta de gestão de terceiros, somada a práticas de monitoramento contínuo e modelos baseados em confiança zero para mitigar riscos em cascata.

Os ataques analisados seguem um roteiro semelhante: invasão inicial via phishing ou sistemas expostos, movimentação lateral para ganhar controle da rede, roubo de dados e, em muitos casos, ativação de ransomwares. Os prejuízos econômicos já ultrapassam 1% do PIB em alguns países, podendo chegar a 6% quando a infraestrutura crítica é atingida.[26] A título de comparação, uma perda equivalente a 1% do PIB representa US$ 25 bilhões no Brasil, US$ 15 bilhões no México e US$ 6,1 bilhões na Argentina. No pior cenário, com perdas estimadas em 6% do PIB, os danos subiriam para US$ 150 bilhões, US$ 90 bilhões e US$ 36,6 bilhões, respectivamente. Economias de porte intermediário, como as do Chile (US$ 3,9 a US$ 23,5 bilhões) e da Colômbia (US$ 3,2 a US$ 19,3 bilhões), também enfrentam riscos expressivos.[27] Com Brasil, México e Argentina entre os países mais

---

[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.cisa.gov/news events/cybersecurity-advisories/aa23-158a
[21] https://www.trendmicro.com/en_us/research/18/f/new-killdisk-variant-hits-latin-american-financial-organizations-again.html
[22] https://www.zdnet.com/article/north-korea-s-apt38-hacking-group-behind-bank-heists-of-over-100-million/
[23] 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
[24] https://unit42.paloaltonetworks.com/threat-brief-moveit-cve-2023-34362/
[25] 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
[26] https://latam.cs4ca.com/wp-content/uploads/2024-Annual-Report-The-State-of-OT-Cyber-Security-in-LATAM.pdf
[27] https://www.statista.com/statistics/802640/gross-domestic-product-gdp-latin-america-caribbeancountry/#:~:text=In%202024%2C%20Brazil%20 and,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

afetados, os ataques cibernéticos colocam em risco a continuidade dos negócios, a confiança dos investidores e a estabilidade econômica de longo prazo na região. A magnitude do impacto potencial reforça a necessidade urgente de medidas mais eficazes de cibersegurança, especialmente no gerenciamento de riscos com terceiros e na proteção de infraestruturas críticas no setor financeiro latino-americano.

2.2.2 Análise de Tendências em Vulnerabilidades Cibernéticas

Nesta seção, são avaliadas vulnerabilidades técnicas frequentes, fragilidades típicas do setor financeiro e desafios regionais específicos enfrentados por instituições da América Latina. O objetivo é fornecer às organizações uma base concreta para identificar padrões de risco que se repetem e ajustar suas estratégias de segurança de forma proativa. O entendimento desses pontos fracos permite não só antecipar impactos operacionais, como também reforçar medidas de proteção antes que falhas evoluam para incidentes críticos. As recomendações práticas para tratamento desses riscos podem ser encontradas na Seção 6: Recomendações Estratégicas.

Vulnerabilidades Técnicas Recorrentes:

- Segmentação fraca da rede
- Controles de acesso interno insuficientes
- Protocolos inadequados de resposta a incidentes
- Suscetibilidade de funcionários à engenharia social
- Dependência excessiva de sistemas legados
- Segurança deficiente de terceiros
- Monitoramento limitado de transações internas

Fragilidades Específicas do Setor Financeiro:

- Segmentação inadequada da rede entre sistemas críticos
- Controles de acesso frágeis em redes internas
- Autenticação insuficiente em sistemas de prestadores de serviços terceirizados
- Infraestrutura pública exposta a falhas
- Cavalos de Troia bancários sofisticados que se passam por autoridades legítimas

Desafios e Padrões Específicos da América Latina:

- Forte dependência de engenharia social explorando a confiança nas autoridades financeiras
  Campanhas de phishing sofisticadas explorando temas fiscais
- Operações bancárias transnacionais que geram inconsistências de segurança
- Adoção generalizada de serviços bancários digitais em áreas rurais por meio de canais potencialmente frágeis
- Sistemas centralizados de processamento de pagamentos (como o SPEI no Brasil) se tornando alvos de alto valor[28]

2.2.3 Análise de Lacunas e Impactos Futuros

Esta seção apresenta uma análise aprofundada das principais deficiências que enfraquecem a postura de cibersegurança da América Latina, abordando tanto suas origens quanto seus possíveis desdobramentos. Questões estruturais como investimento insuficiente, obsolescência tecnológica e baixa articulação institucional continuam alimentando um cenário de risco elevado. A revisão de episódios passados que impactaram instituições financeiras da região permite mapear tendências em evolução e antecipar riscos crescentes. Entre os pontos emergentes, destacam-se ameaças movidas por inteligência artificial, fragilidades nas cadeias de suprimento digital e tensões geopolíticas com efeitos indiretos sobre o setor financeiro. Soluções práticas para o enfrentamento desses desafios estão detalhadas na Seção 6: Recomendações Estratégicas.

Causas Estruturais Identificadas:

1. Investimento estruturalmente insuficiente: A baixa prioridade dada à cibersegurança nos orçamentos nacionais expõe os sistemas financeiros latino-americanos a ameaças cada vez mais sofisticadas.[29] Segundo dados da OEA, a alocação média não ultrapassa 1% do PIB,[30] e a pontuação geral da região em maturidade cibernética é de apenas 10,2 em 20, a mais baixa do mundo.[31]

2. Falta de alinhamento jurídico entre países: A ausência de padronização legal dificulta iniciativas coordenadas, sobretudo para empresas com atuação multinacional.[32] Iniciativas como a Aliança Digital entre União Europeia e América Latina buscam preencher esse vácuo, mas ainda têm alcance limitado.[33]

3. Ambiente tecnológico ultrapassado: A dependência de infraestruturas antigas ou softwares não licenciados permanece um ponto crítico, abrindo brechas técnicas exploráveis por grupos maliciosos.[34]

4. Déficit de mão de obra especializada: A escassez de profissionais capacitados afeta tanto a resposta a incidentes quanto o desenvolvimento de políticas preventivas. A formação e requalificação de talentos na área cibernética é urgente.[35]

5. Legislação ineficaz ou inexistente: Muitos países operam com marcos legais desatualizados ou com baixa

[28] https://www.wired.com/story/mexico-bank-hack/
[29] https://www.centerforcybersecuritypolicy.org/insights-and-research/insights-from-the-annual-latam-ciso-summit-costa-rica
[30] https://grcoutlook.com/cybersecurity-risks-latin-america-versus-asia-a-rising-concern/
[31] https://blogs.worldbank.org/en/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe
[32] https://www.wired.com/story/mexico-bank-hack/
[33] https://www.eeas.europa.eu/eeas/europe-and-latin-america-caribbean-step-cooperation-cybersecurity_en
[34] https://www.datto.com/blog/ransomware-and-cybersecurity-in-latin-america/
[35] https://www.centerforcybersecuritypolicy.org/insights-and-research/insights-from-the-annual-latam-ciso-summit-costa-rica

capacidade de aplicação. Apenas três nações latino-americanas possuem uma estratégia digital nacional clara e funcional.[36]

6. Baixo nível de conscientização pública: A falta de campanhas educativas voltadas à população agrava o problema. Mesmo onde existem estratégias nacionais, poucas foram traduzidas em ações concretas de prevenção e engajamento popular.[37]

2.2.4 Evolução da Maturidade em Segurança Cibernética: 2018 a 2024

Entre 2018 e 2024, a maturidade cibernética das instituições financeiras na América Latina avançou de forma significativa. Em 2018, a resposta a incidentes era amplamente reativa, como demonstrado no caso do Banco do Chile, onde a instituição só detectou o ataque após o disparo do alerta KillMBR, que resultou na paralisação de diversos sistemas. A resposta consistiu basicamente em desconectar os sistemas, investigar os danos e restaurar os dados por meio de backups, que é uma abordagem que contrastava com práticas mais maduras, como monitoramento contínuo, segmentação de rede e contenção automatizada. A ausência de detecção antecipada e de medidas eficazes de mitigação contribuiu diretamente para os prejuízos sofridos.[38]

No mesmo ano, o ataque ao sistema SPEI no México expôs vulnerabilidades severas nas estruturas de rede e nas práticas de controle de acesso.[39] O ataque expôs vulnerabilidades críticas no Sistema de Pagos Electrónicos Interbancarios (SPEI), com os hackers sendo identificados como integrantes do grupo APT38, supostamente ligado à Coreia do Norte.[40] O grupo invadiu redes bancárias, comprometeu os terminais que processavam transações via SPEI e injetou ordens de pagamento fraudulentas. A fragilidade da segmentação de rede e a ausência de sistemas de alerta possibilitaram a execução do golpe sem detecção imediata, resultando no desvio de valores entre 15 e 20 milhões de dólares, posteriormente distribuídos por contas de fachada no exterior.[41]

Em 2024, no entanto, o setor apresentou sinais claros de amadurecimento. Organizações passaram a adotar protocolos mais robustos de resposta a incidentes e a atuar de forma mais coordenada com centros nacionais de resposta a emergências cibernéticas (CERTs). A atuação da Alfândega do Chile no caso do ransomware Black Basta ilustra essa evolução: a contenção foi rápida, e a comunicação entre as partes envolvidas foi eficaz.[42] Ainda assim, o cenário segue desafiador, com a digitalização acelerando a exposição a novos vetores de ataque, principalmente em serviços terceirizados e integrações em nuvem.

Um exemplo emblemático dessa nova frente de vulnerabilidade foi a violação da plataforma Bankingly, que expôs informações de 135 mil clientes na região.[43] A origem do problema esteve em configurações incorretas de buckets do Azure Blob Storage, utilizados para armazenar dados sensíveis. A ausência de autenticação adequada permitiu o acesso indevido às informações, revelando lacunas importantes em processos de integração com provedores de nuvem e gestão de terceiros.[44]

O vazamento de dados do Banco Português de Gestão, originado por falhas nos sistemas da Nearsoft, reforça um padrão preocupante de negligência em segurança cibernética. A ausência de controles de autenticação e a não conformidade com padrões críticos como ISO 27001 e PCI DSS resultaram na exposição de informações financeiras altamente sensíveis. Os dados estavam armazenados sem criptografia, deixando-os acessíveis a qualquer pessoa com conexão aos sistemas afetados.[45] O incidente exemplifica os riscos associados a uma governança frágil sobre fornecedores de tecnologia, erros na configuração de ambientes em nuvem e ausência de fiscalização efetiva. Apesar dos avanços institucionais na construção de defesas, esses episódios deixam claro que erros operacionais e supervisão inadequada continuam sendo pontos de fragilidade relevantes. Corrigir essas falhas será fundamental para manter a integridade operacional num ecossistema cada vez mais dependente de infraestrutura digital.

2.2.5 Tendências Futuras e Potencial de Impacto

1. Ciberataques baseados em inteligência artificial: Grupos maliciosos vêm incorporando IA para ampliar a escala e a sofisticação de suas operações. Isso inclui o uso de algoritmos para gerar malwares autônomos, manipular vítimas por meio de phishing hiperrealista, disseminar conteúdos falsificados por deepfake e

[36] https://www.wired.com/story/mexico-bank-hack/
[37] https://latam.cs4ca.com/wp-content/uploads/2024-Annual-Report-The-State-of-OT-Cyber-Security-in-LATAM.pdf
[38] https://www.infosecurity-magazine.com/news/bank-of-chile-suffers-10m-loss/
[39] https://latam.cs4ca.com/wp-content/uploads/2024-Annual-Report-The-State-of-OT-Cyber-Security-in-LATAM.pdf
[40] https://attack.mitre.org/groups/G0082/
[41] https://latam.cs4ca.com/wp-content/uploads/2024-Annual-Report-The-State-of-OT-Cyber-Security-in-LATAM.pdf
[42] https://therecord.media/chile-black-basta-ransomware-attack-customs-department
[43] 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
[44] 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
[45] https://cybernews.com/security/banco-portugues-de-gestao-data-leak/

realizar espionagem digital avançada.[46] O principal entrave à contenção dessas ameaças é a escassez de profissionais altamente qualificados capazes de criar mecanismos de governança à altura da complexidade técnica envolvida. O fortalecimento da base técnica e de processos será determinante para mitigar esses riscos.

2. Ameaças impulsionadas pela digitalização acelerada: A busca por modernização digital como pilar de crescimento econômico torna os países latino-americanos mais suscetíveis a ataques. O aumento na dependência de sistemas digitais amplia diretamente a superfície de exposição a vulnerabilidades.[47]

3. Riscos estruturais na cadeia de suprimentos digital: A falta de visibilidade sobre o nível de segurança dos fornecedores tornou-se um dos gargalos mais críticos para organizações de grande porte. Mais da metade delas reconhece a cadeia de suprimentos como o principal entrave à construção de resiliência cibernética. O aumento da complexidade dessas cadeias só agrava o problema.[48]

4. Impacto de tensões geopolíticas na segurança digital: Cenários de conflito internacional têm afetado diretamente o volume e o tipo de ataques. Desde o início da guerra Rússia–Ucrânia, 97% das organizações relataram um aumento significativo nas ameaças digitais, evidenciando como a instabilidade geopolítica molda o panorama global de riscos cibernéticos.[49]

5. Desigualdade regional na escalada dos ataques: A América Latina já apresenta crescimento acelerado em incidentes cibernéticos e tende a se distanciar ainda mais de outras regiões em termos de frequência e impacto. No segundo trimestre de 2024, o volume de ataques subiu 53% em relação ao mesmo período de 2023, uma tendência que projeta um cenário de risco crescente para o futuro próximo.[50]

2.3 Impacto Econômico do Ransomware no Setor Financeiro Latino-Americano

Ao longo de 2024, as instituições financeiras da América Latina passaram a figurar como alvos prioritários de grupos de ransomware, refletindo a escalada regional das ameaças cibernéticas. Brasil, México e Chile lideram em número de incidentes, com a atuação de grupos sofisticados como LockBit 3.0, Akira e Play. Esses grupos se aproveitam de falhas técnicas para comprometer sistemas, muitas vezes por meio de brechas em softwares ou por meio da oferta de ransomware como serviço (RaaS). As perdas acumuladas no setor são estimadas em centenas de milhões de dólares, somando os custos de pagamento de resgates, tempo de inatividade operacional, recuperação de dados e gestão de crise reputacional. Esse cenário evidencia a necessidade de revisões estruturais na segurança digital do setor financeiro.

2.3.1 Estudo de Caso 1: LockBit 3.0 compromete banco brasileiro por meio de infraestrutura virtual

Em julho de 2024, o grupo LockBit 3.0 executou um ataque direcionado contra uma grande instituição bancária brasileira, explorando falhas na infraestrutura de desktop virtual para acessar e criptografar dados críticos. Para pressionar o pagamento, os criminosos ameaçaram vazar as informações roubadas em plataformas da dark web, caso o banco não pagasse 2,5 milhões de dólares em Bitcoin.

O incidente comprometeu a operação de serviços bancários digitais por um período prolongado, afetando o atendimento ao cliente e gerando desconfiança generalizada. Além da interrupção dos serviços, a instituição teve que arcar com custos adicionais envolvendo recuperação de sistemas, investigações técnicas e campanhas de comunicação para restaurar a confiança de clientes e reguladores.

2.3.2 Estudo de Caso 2: Play Ransomware mira infraestrutura virtual de empresa chilena

No mesmo mês, o grupo Play lançou um ataque contra uma empresa do setor financeiro no Chile, utilizando uma versão do malware projetada para atacar ambientes VMware ESXi em servidores Linux. Após infiltrar-se na infraestrutura virtualizada, os invasores criptografaram dados sensíveis e exigiram um resgate de 1,8 milhão de dólares em ativos digitais.

O ataque à empresa financeira chilena gerou consequências amplas, tanto do ponto de vista operacional quanto financeiro. Além do valor exigido pelos criminosos, a organização precisou arcar com custos significativos para reestabelecer seus sistemas de TI e fortalecer sua estrutura de segurança digital. A reputação da empresa também foi diretamente afetada, uma vez que clientes e parceiros questionaram sua capacidade de proteger informações sensíveis. Esse tipo de impacto reforça a urgência de tratar o ransomware como uma ameaça estrutural ao setor financeiro latino-americano.

Conclui-se, portanto, que o ransomware representa uma das ameaças mais graves e em crescimento para as instituições financeiras da América Latina. Em 2024, países como Brasil, Chile e México tornaram-se alvos centrais de campanhas conduzidas por grupos como LockBit 3.0 e Play, que utilizam infraestrutura virtualizada como vetor de ataque e operam em escala por meio do modelo de ransomware como serviço. Os danos causados por essas operações ultrapassam os

[46] https://insightcrime.org/news/four-ways-ai-is-shaping-organized-crime-in-latin-america/
[47] https://grcoutlook.com/cybersecurity-risks-latin-america-versus-asia-a-rising-concern/
[48] https://www.weforum.org/publications/global-cybersecurity-outlook-2025/digest/
[49] https://www.accenture.com/content/dam/accenture/final/accenture-com/document/Accenture-State-Cybersecurity.pdf
[50] 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/

pagamentos exigidos, envolvendo também paralisação de serviços, custos técnicos e impactos reputacionais, totalizando centenas de milhões de dólares em prejuízos. Com a digitalização financeira se acelerando, é imperativo que instituições adotem estratégias de defesa mais integradas, incluindo monitoramento contínuo, capacitação de equipes e políticas de gestão de riscos, para que essa ameaça seja contida. A continuidade operacional do setor financeiro depende diretamente da capacidade de adaptação frente às novas táticas empregadas por operadores de ransomware.

2.4 Capacidade de Enfrentamento ao Ransomware

O aumento expressivo de ataques de ransomware na América Latina tem evidenciado falhas relevantes nos mecanismos de resposta, revelando fragilidades institucionais que afetam diretamente o setor financeiro. Esta seção examina de que forma os modelos organizacionais, a infraestrutura técnica e os níveis de coordenação regional influenciam a exposição das instituições a esse tipo de ameaça.

2.4.1 Diagnóstico da Infraestrutura de Resposta na Região

Relatórios recentes, como o Global Ransomware Report da Fortinet, fornecem dados comparativos úteis para contextualizar a capacidade de reação da América Latina em relação a outras regiões.[51] [52] [53] As instituições latino-americanas demonstram avanços notáveis em áreas como detecção rápida de ataques e resistência a técnicas de engenharia social[54]. No entanto, esses avanços em nível organizacional não anulam as limitações mais amplas observadas na estrutura regional. A ausência de políticas públicas consistentes, o baixo número de países com estratégias definidas para proteger infraestruturas críticas e o cenário fragmentado de divulgação de incidentes indicam um déficit sistêmico na preparação regional.

Um estudo conduzido em 2022 propôs um índice de divulgação em cibersegurança, analisando os principais mercados da América Latina entre 2016 e 2020 com base em uma escala de 0 a 1. O índice foi construído sobre 27 critérios distribuídos entre quatro dimensões: governança (5 critérios), estratégia (6), gestão de riscos (13) e impactos financeiros (3). O framework foi elaborado com base em normas reconhecidas internacionalmente, como ISO 27000, as diretrizes da SEC, GDPR, além dos modelos propostos por OCDE, BID, OEA e GRI.[55]

A análise aponta para um panorama multifacetado da transparência em cibersegurança no setor financeiro da América Latina. Embora o setor apresente os maiores índices de divulgação entre todos os segmentos econômicos, com um crescimento de 0,28 em 2016 para 0,52 em 2020, persistem fragilidades relevantes, especialmente no campo da governança corporativa.[56] O destaque da Argentina nesse contexto é notável: 57% das empresas analisadas pertenciam ao setor financeiro, e 86% delas entregaram relatórios compatíveis com o Formulário 20-F da SEC.[57] Ainda assim, a divulgação sobre governança cibernética no nível de conselho segue abaixo do esperado. A supervisão direta dos conselhos de administração teve avanço (de 0,18 para 0,53 entre 2016 e 2020), mas a criação de comitês especializados continua limitada (0,24 em 2020), assim como a atuação dos comitês de auditoria (0,20).[58]

Essa fragilidade é crítica frente à sofisticação crescente de malwares adaptados a contextos locais. Um estudo de longo prazo focado em malwares financeiros no Brasil entre 2012 e 2020 demonstrou como as técnicas criminosas evoluem com base em particularidades regionais e institucionais. Atores maliciosos têm ajustado seus ataques a bancos locais, com códigos em português brasileiro, direcionados a sistemas com cartões baseados em PIN, por exemplo.[59] Essa adaptação contínua, que também é observada no uso de ransomware, exige que os conselhos de administração estabeleçam diretrizes de risco cibernético mais robustas e sensíveis ao contexto nacional e organizacional.

Além da governança, a pesquisa identificou lacunas na transparência de outros aspectos cruciais. A divulgação sobre práticas de gestão de riscos ficou em 0,40; a aderência a padrões internacionais de segurança, como ISO e GDPR, marcou 0,39; e a comunicação sobre investimentos em cibersegurança teve avanço modesto, saindo de 0,02 em 2016 para 0,21 em 2020.[60] Esses números indicam que, embora muitas instituições tenham estruturas técnicas em vigor, sua capacidade de articular, justificar e comunicar esses investimentos ainda é limitada. A correlação entre marcos regulatórios e qualidade da divulgação é evidente: países que adotaram estratégias nacionais de cibersegurança e leis de proteção de dados mais cedo, como Argentina e Brasil, apresentam níveis de maturidade superiores aos de países como o Peru, cuja pontuação de 0,25 em 2020 reflete a ausência de uma política nacional clara para o tema.[61]

[51] https://www.fortinet.com
[52] https://doi.org/10.1145/3429741
[53] https://doi.org/10.3390/su14031390
[54] https://www.fortinet.com
[55] https://doi.org/10.3390/su14031390
[56] https://doi.org/10.3390/su14031390
[57] https://doi.org/10.3390/su14031390
[58] https://doi.org/10.3390/su14031390
[59] https://doi.org/10.1145/3429741
[60] https://doi.org/10.3390/su14031390
[61] https://doi.org/10.3390/su14031390

Os dados sugerem uma tendência estrutural: embora o setor financeiro da América Latina lidere na transparência sobre cibersegurança em relação a outros setores econômicos, essa liderança é irregular e altamente dependente da maturidade regulatória e das políticas nacionais de segurança digital. Considerando a importância estratégica do setor financeiro para a estabilidade nacional e sua integração com redes financeiras globais, essas falhas representam riscos sistêmicos. O cenário atual exige uma padronização mais consistente nos processos de divulgação e maior aderência a padrões internacionais.

A amplitude das conclusões da pesquisa aponta para limitações operacionais significativas na capacidade de resposta a ataques de ransomware nas instituições financeiras da região. A diferença entre os índices de divulgação estratégica (0,53) e de gestão operacional de riscos (0,40) revela um possível descompasso entre planejamento e execução.[62] A baixa pontuação na divulgação de procedimentos de resposta a incidentes (0,36) e na avaliação de eficácia de monitoramento (0,47) sugere que muitas instituições não estão plenamente preparadas para detectar, conter e recuperar-se de ataques com alto grau de complexidade.[63] Esses números, quando avaliados em conjunto com os dados regulatórios apresentados anteriormente, indicam que boa parte das instituições possui planos básicos, mas ainda carece de capacidade operacional madura.

Essa avaliação é reforçada por dados do Banco Interamericano de Desenvolvimento, que mostram que apenas sete países da América Latina contam com planos nacionais voltados à proteção de infraestrutura crítica, e somente 20 possuem CSIRTs (equipes de resposta a incidentes cibernéticos) ativas.[64] Essa fragmentação institucional representa um desafio, sobretudo para instituições com presença regional. O caso do ataque à Colômbia em setembro de 2023 ilustra isso de forma clara. A falta de mecanismos de coordenação regional permitiu que os efeitos do ataque ultrapassassem fronteiras, atingindo entidades na Argentina, no Panamá e no Chile.[65]

2.4.2 Preparação Técnica e Limitações de Recursos

Embora algumas organizações da região tenham melhorado sua capacidade de detecção inicial, diferenças significativas entre os países revelam disparidades críticas na capacidade técnica de resposta. O incidente de ransomware que afetou a Costa Rica em 2022 demonstra essa realidade. Apesar da rápida identificação do ataque, o país precisou desembolsar aproximadamente 24 milhões de dólares em esforços de contenção e recuperação.

A fase de reabilitação da Previdência Social, sozinha, consumiu mais de 18 milhões.[66] Esses números indicam que a infraestrutura técnica da região enfrenta restrições severas ao longo de todo o ciclo de resposta. Um dos fatores mais evidentes é a desigualdade entre setores em termos de prontidão técnica para enfrentar incidentes desse porte.

Dados consolidados de 2020 revelam que, entre as instituições financeiras da América Latina, os investimentos em cibersegurança continuam concentrados em ações de caráter estratégico, como a implementação de sistemas de gestão (pontuação 0,68) e campanhas de conscientização (0,72). Por outro lado, elementos operacionais essenciais, como os protocolos de resposta a incidentes, receberam atenção significativamente menor (0,36), enquanto os processos de teste e monitoramento ficaram aquém do ideal (0,47).[67]. Um modelo de governança maduro exigiria um equilíbrio mais claro entre estratégia e execução operacional. Isso significaria, por exemplo, sair do discurso genérico sobre adoção de sistemas e demonstrar investimentos tangíveis em capacidades técnicas de detecção e resposta, execução regular de testes de penetração, análise de vulnerabilidades e uso de métricas objetivas para mensurar o desempenho das ações de segurança. O conteúdo reportado deve demonstrar que os aportes estão sendo canalizados também para estruturas operacionais críticas como inteligência de ameaças, defesa ativa e monitoramento contínuo. Um programa com esse perfil revela compromisso com mitigação real de riscos e evidencia, com dados concretos, como os recursos aplicados impactam as operações.

Esse desequilíbrio entre planejamento e execução não se restringe à iniciativa privada. No setor público, a defasagem é ainda mais visível. Em comparação com as instituições financeiras da região, órgãos públicos adotam com menor frequência práticas reconhecidas de segurança digital,[68] criando potenciais brechas sistêmicas em um ecossistema onde os ambientes público e privado são interconectados.[69]

A situação se torna ainda mais delicada diante de limitações documentadas na distribuição de recursos, o que compromete a capacidade de resposta a ataques como os de ransomware. Enquanto empresas da América do Norte, Europa, Oriente Médio e África planejam ampliar significativamente os investimentos em soluções de acesso com confiança zero (ZTNA), os planos na América Latina continuam restritos.[70] Ferramentas ZTNA são fundamentais por possibilitarem o isolamento interno das redes, dificultando movimentações não autorizadas, vazamento de dados e comprometimento de sistemas

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

críticos. A escassez desses recursos tende a fragilizar ainda mais a infraestrutura de resposta, especialmente para instituições financeiras que precisam manter padrões globais de segurança ao operar em múltiplas jurisdições e integrar-se tanto a redes privadas quanto públicas.

O caso do Santander ilustra bem esse cenário multifacetado. Com presença significativa em mercados como América Latina, União Europeia e Estados Unidos, o banco precisa adaptar sua estratégia de divulgação de cibersegurança à combinação de exigências obrigatórias e diretrizes voluntárias. No Brasil, que lidera os índices regionais com alta pontuação em desenvolvimento institucional (97,68) e solidez normativa (20,0), o Santander opera sob exigências locais rigorosas, além das obrigações de reporte à SEC através do formulário 20-F.[71] Já na Argentina, onde o índice de maturidade em cibersegurança é inferior (50,12), o banco enfrenta um cenário regulatório menos estruturado, mas ainda assim segue sujeito às mesmas obrigações internacionais.[72]

A assimetria entre jurisdições tem impacto direto na capacidade de conter ameaças e reagir a incidentes, sobretudo em áreas que envolvem compartilhamento de inteligência e articulação com órgãos públicos ou operadores de serviços essenciais. No Brasil, os relatórios do Santander evidenciam o apoio de acordos de cooperação robustos, tanto bilaterais quanto multilaterais (pontuação de 19,41 em medidas colaborativas), o que fortalece os canais de troca de informações e facilita a mobilização conjunta em situações críticas.[73] Na Argentina, embora o banco mantenha o cumprimento das exigências mínimas previstas pelo formulário 20-F da SEC, a baixa pontuação nacional em maturidade cibernética levanta dúvidas quanto à eficácia da coordenação local diante de incidentes complexos.

Na Europa, o Santander opera em um ambiente ainda mais regulado, onde o cumprimento do GDPR impõe padrões elevados de proteção e transparência. Essa exigência, segundo pesquisadores, vem influenciando práticas de divulgação em várias operações latino-americanas do grupo, configurando uma espécie de transplante normativo do modelo europeu para a região.[74]Em países como o Brasil, onde a legislação local foi inspirada diretamente no GDPR, isso tem trazido ganhos de padronização e elevado os parâmetros exigidos para proteção de dados e comunicação de riscos. Ainda assim, a aderência a essas exigências varia amplamente conforme o país.[75]

Diante desse mosaico regulatório, o Santander precisa operar com um padrão de segurança elevado que esteja à altura das jurisdições mais exigentes, ajustando ao mesmo tempo sua comunicação de riscos e controles internos para cada contexto regulatório, seja ele baseado em normas da SEC, do GDPR ou em legislações locais. Embora essa abordagem possa, em tese, fortalecer o conjunto das práticas de segurança, sua aplicação prática em cada país é limitada pela realidade local, especialmente quando há escassez de recursos.

As disparidades institucionais nos países latino-americanos criam lacunas operacionais relevantes. Enquanto o Brasil oferece um ambiente mais maduro, com políticas públicas consolidadas e infraestrutura de segurança bem desenvolvida, outras praças enfrentam dificuldades concretas para atingir níveis similares. Essa diferença se manifesta em fatores como escassez de profissionais qualificados para a área de segurança, limitações em ferramentas de detecção e registro, e deficiências na articulação de respostas coordenadas.

Quando o banco atua com base apenas nos padrões mínimos de regiões menos desenvolvidas, corre o risco de abrir brechas que comprometem todo o ecossistema operacional. Isso é especialmente crítico na cadeia de suprimentos, onde filiais em países com baixa maturidade digital podem se tornar vetores de exposição para toda a estrutura institucional. E mesmo quando a exigência vem de fora, seja pela SEC ou pelo GDPR, adaptar operações locais para atender a padrões mais elevados nem sempre é viável. A limitação de mão de obra especializada e a falta de infraestrutura compatível com as exigências globais colocam entraves concretos à implementação plena das medidas de segurança necessárias.

2.4.3 Coordenação de Resposta Transfronteiriça

A integração dos sistemas financeiros latino-americanos amplia os riscos derivados da ausência de coordenação eficiente em respostas que envolvem múltiplos países. Embora existam iniciativas bilaterais, como o acordo entre Costa Rica e Panamá, a região ainda carece de uma estrutura robusta de resposta coletiva. Mesmo os avanços em detecção precoce não têm sido suficientes para conter ameaças em nível regional.[76] O ataque cibernético de setembro de 2023 à IFX Networks, fornecedora de serviços de internet da Colômbia, ilustra esse ponto de vulnerabilidade. Apesar da identificação inicial do vetor de ataque, a falha em aplicar medidas coordenadas resultou na propagação do incidente para 78 órgãos públicos e 762 empresas privadas em diversos países.[77] O caso evidenciou, acima de tudo, a inexistência de mecanismos estruturados para enfrentar riscos associados a terceiros. A ausência de relatórios

[71] https://doi.org/10.3390/su14031390
[72] https://doi.org/10.3390/su14031390
[73] https://doi.org/10.3390/su14031390
[74] https://doi.org/10.3390/su14031390
[75] https://doi.org/10.3390/su14031390
[76] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[77] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf

claros sobre a extensão dos impactos dificultou a desconexão de sistemas comprometidos, impedindo respostas eficazes nas cadeias operacionais.[78]

2.4.4 Mecanismos de Troca de Informação e Exposição no Setor Financeiro

Deficiências nos fluxos regionais de compartilhamento de dados continuam a comprometer a capacidade de reação do setor financeiro frente a ataques como ransomware. No episódio colombiano de 2023, a assessoria presidencial emitiu nove comunicados ao longo do evento, mas a ausência de padrões formais para repasse de dados entre setores resultou em distribuição irregular das informações mais críticas.[79] Como consequência, instituições financeiras conectadas por redes interdependentes permaneceram vulneráveis por períodos prolongados, ampliando a exposição sistêmica.[80]

2.4.5 Fragilidade nos Modelos de Colaboração Público–Privada

A maioria dos países latino-americanos enfrenta lacunas importantes nas estruturas de cooperação entre setor público e iniciativa privada, o que impacta diretamente a robustez do setor financeiro.[81]. No Equador, por exemplo, há 14 CSIRTs voltados ao suporte de incidentes cibernéticos no setor privado, mas nenhum especializado em finanças.[82] Esses centros atuam em áreas como energia e telecomunicações, que compartilham algumas interseções com os sistemas financeiros, mas operam de forma isolada, sem canais estruturados de comunicação entre si.[83] No caso do Panamá, um polo financeiro estratégico da região, mesmo após a implantação da Agenda Digital Nacional, ainda existem entraves para consolidar plataformas de interoperabilidade entre setores e atrair capital privado para fortalecer o ecossistema de segurança digital. Essa falta de integração compromete tanto a defesa de ativos críticos quanto a agilidade de resposta a riscos emergentes.[84]

Apesar das fragilidades observadas na região, há modelos de coordenação intersetorial que vêm se consolidando com êxito. O Chile é um caso emblemático: em 2023, o país aprovou a Lei de Marco de Cibersegurança com o objetivo de fortalecer os controles de segurança e ampliar a capacidade de resposta a incidentes por parte de operadores de serviços essenciais. A legislação instituiu CSIRTs especializados por setor e criou a Agência Nacional de Cibersegurança (ANCI), encarregada de definir padrões específicos para setores estratégicos, como o financeiro, e aplicar sanções a quem descumprir os regulamentos nacionais.[85]

O setor privado chileno também tem assumido protagonismo crescente na construção da agenda de cibersegurança, com a criação de entidades específicas voltadas às demandas de cada setor. A Alianza Chilena de Ciberseguridad, composta por nove instituições-chave que representam áreas críticas da economia, incluindo finanças, é um bom exemplo desse avanço.[86] A iniciativa reforça como colaborações entre empresas, governo e academia são capazes de estabelecer canais eficazes de troca de informações em situações de crise. Complementando esse ecossistema, o Instituto Nacional de Ciberseguridad do Chile desempenha um papel fundamental na promoção da cultura de segurança digital entre empresas e cidadãos.[87] Além disso, o fortalecimento de associações como a Chiletec, que representa mais de 100 empresas de tecnologia, reforça a base institucional disponível para ações coordenadas de prevenção e resposta a ameaças cibernéticas.[88]

A Colômbia também adota uma abordagem integrada que serve de referência na região. A coordenação entre órgãos estatais (ColCERT, CCOC, MINTIC) e o setor financeiro, por meio do CSIRT da Asobancaria,[89] mostra como é possível fundir a estrutura regulatória do Estado com a agilidade operacional do setor privado para construir uma defesa resiliente e eficiente.

Os resultados dessa sinergia são notáveis. Dados recentes revelam que, em um cenário com quase 20 bilhões de tentativas de ataque no último ano, apenas dois acessos não autorizados foram bem-sucedidos no sistema financeiro colombiano.[90] Esse resultado está diretamente ligado à atuação do CSIRT da Asobancaria, que, com uma equipe técnica de 17 profissionais especializados, conseguiu processar mais de 300 eventos e emitir mais de 450 alertas preventivos nos primeiros meses de 2024.[91]

A estrutura de colaboração entre o setor financeiro colombiano e seus parceiros institucionais atingiu um nível de maturidade notável, refletido na atuação estratégica do CSIRT da Asobancaria. Operando como ponto de articulação nacional e internacional para crises e incidentes cibernéticos, a entidade é hoje referência em resiliência digital. Seu Centro de Operações e o

[78] https://elpais.com/america-colombia/2023- 09-14/el-gobierno-aun-no-sabe-cuantas-entidades-estan-afectadas-por-el-hackeo-a-ifx networks.html
[79] https://therecord.media/colombia government-ministries-cyberattack
[80] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[81] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[82] https://doi.org/10.1007/978-3-030-60467-7_24
[83] https://doi.org/10.1007/978-3-030-60467-7_24
[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://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[89] https://doi.org/10.25062/9789585216549
[90] https://www.mintic.gov.co/portal/inicio/
[91] https://www.mintic.gov.co/portal/inicio/

programa de intercâmbio de informações figuram entre os mais sofisticados da América Latina e servem como modelo de como alianças público–privadas bem estruturadas podem elevar o padrão de segurança em setores críticos. Isso ganha ainda mais relevância considerando que a Colômbia ocupa a segunda posição no ranking de países latino-americanos mais visados por ataques cibernéticos. O êxito dessa experiência oferece parâmetros concretos para outras nações da região que buscam proteger suas infraestruturas financeiras com mecanismos colaborativos similares.

3 Panorama do Setor

3.1 Perfis de Ameaças que Miram a Indústria Financeira na América Latina

A evolução das políticas internas de cibersegurança nas organizações da região ocorre em paralelo ao crescimento acelerado das ameaças de ransomware. O Índice Nacional de Cibersegurança (NCSI) evidencia a fragilidade normativa ainda presente em muitos países da América Latina, destacando o custo operacional e os riscos que o setor financeiro enfrenta diante de ataques com alta capacidade de disrupção.[92] Um caso emblemático citado pelo relatório LATAM CISO 2024 envolve o Ministério da Fazenda da Costa Rica, alvo em abril de 2022 de um ataque de US$10 milhões liderado pelo grupo russo Conti. O incidente paralisou serviços fiscais e exigiu medidas emergenciais, inclusive reforço na contratação de especialistas em segurança digital.[93]

Com o setor financeiro cada vez mais exposto, o fortalecimento de capacidades locais passa a depender diretamente de tendências como qualificação de mão de obra, captação de investimentos e mudanças no comportamento dos usuários. Esses indicadores oferecem um diagnóstico preciso das prioridades operacionais para elevar o padrão de proteção e corrigir deficiências no ambiente digital das instituições.

3.1.1 Déficit de Profissionais de Segurança Digital

De acordo com Vergara Cobos, no relatório "2024 América Latina e Caribe", o setor global de cibersegurança cresceu 14% entre 2023 e 2024, mas a lacuna de profissionais qualificados chegou a 4 milhões, que é o dobro do ritmo de expansão do setor de TI e quatro vezes superior ao da economia mundial. Isso revela um espaço significativo para criação de empregos por meio de investimentos em capacitação técnica e ações de conscientização.[94] No caso da América Latina, a projeção é de que o mercado de segurança digital cresça 8% em 2025, com aumento de 15% no volume de profissionais especializados.[95]

Apesar de o crescimento da indústria de cibersegurança e o avanço da qualificação profissional acompanharem as tendências globais, a avaliação da prontidão digital na América Latina revela um cenário de baixa confiança na capacidade regional de mitigar ataques com a infraestrutura existente. Regiões como América do Norte e Europa demonstram maior otimismo, enquanto América Latina e África apresentam os níveis mais baixos de confiança: 42% dos profissionais de segurança nessas localidades acreditam que seus países não estão preparados para lidar com ataques cibernéticos.[96] Essa percepção tem impulsionado uma corrida por talentos capazes de proteger ativos digitais estratégicos na região.[97] A falta de políticas de higiene cibernética eficazes e a carência de programas sólidos de conscientização têm dificultado a contenção de incidentes, colocando a atualização das estratégias nacionais e a criação de protocolos bem definidos no centro das prioridades dos gestores de segurança.[98] Embora historicamente não seja tratada como parte da infraestrutura crítica física, uma força de trabalho altamente capacitada tornou-se peça-chave para a proteção de sistemas essenciais, uma carência que os líderes de segurança da informação na América Latina precisam endereçar com urgência. O fator humano segue como o elo mais vulnerável nas cadeias de segurança.[99]

A aposta em programas de capacitação técnica e colaborações acadêmicas internacionais representa uma oportunidade concreta de reverter esse déficit. A falta de profissionais especializados já tem deixado o setor financeiro particularmente exposto a ameaças avançadas, conforme indica a União Internacional de Telecomunicações (UIT). Atualmente, apenas 7 dos 32 países da região possuem planos específicos para infraestrutura crítica em caso de ataques cibernéticos, e apenas 20 contam com CSIRTs ativos. O Banco Interamericano de Desenvolvimento também aponta a formação de capital humano como um dos principais gargalos da região em termos de capacidade cibernética.[100] Isso evidencia a urgência necessária para que se melhore a prontidão em relação a eventos cibernéticos na região.[101]

Ponto Crítico: A construção de uma força de trabalho qualificada, a implementação de planos de resposta operacionais e o desenvolvimento de políticas robustas de cibersegurança são pilares para reforçar a resiliência digital da região. A criação de protocolos formais, a realização de simulações práticas e o envolvimento de terceiros especializados são medidas indispensáveis. A

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

falta de equipes treinadas e de mecanismos eficazes de comunicação entre setores durante crises reforça o diagnóstico de que a preparação continua sendo um dos maiores desafios da América Latina. Programas de educação técnica e certificações regionais podem ser parte da solução.

3.1.2 Ajuste Orçamentário em Cibersegurança Frente ao Aumento das Ameaças

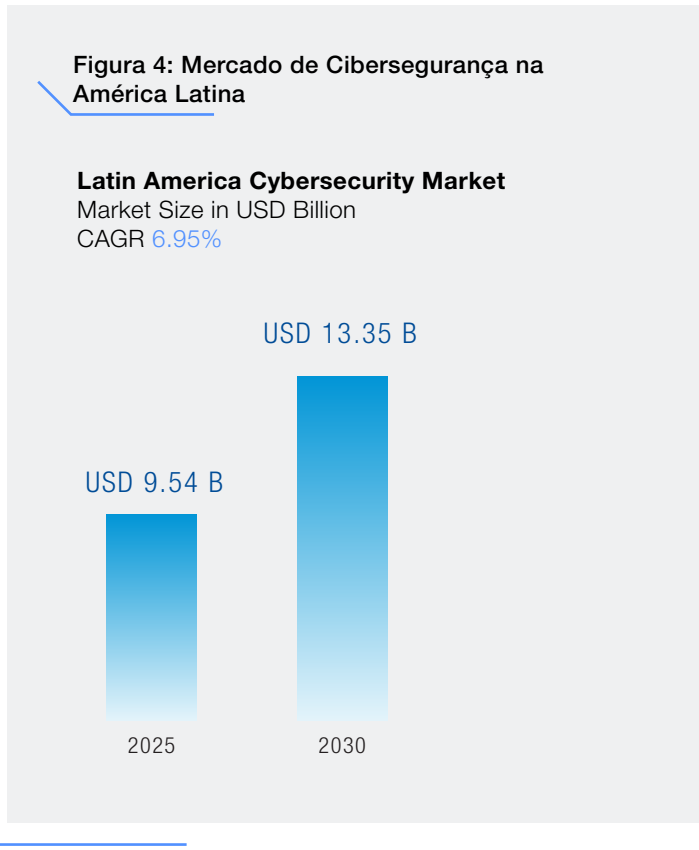
O setor financeiro segue como o principal alvo de ataques cibernéticos na América Latina, com instituições de saúde e educação figurando logo atrás. Em termos nacionais, o Brasil lidera em volume de incidentes, seguido por México e Colômbia. Ainda assim, os demais países da região continuam enfrentando ataques frequentes e de alta complexidade, o que reforça a natureza generalizada da ameaça.[102]

O avanço de tecnologias disruptivas como inteligência artificial e o agravamento do cenário de ameaças em 2024 levaram os países da região a intensificar seus investimentos em segurança digital.[103] Em 2023, as perdas globais com ataques cibernéticos atingiram USD 6 trilhões, sendo USD 2,4 milhões correspondentes à América Latina. Para 2025, projeta-se um aumento de 60% no impacto global e de 76% na região, o maior patamar registrado desde 2020.[104] Embora 77% das organizações da América Latina tenham planos de aumentar seus orçamentos em segurança cibernética, apenas 25% adotaram estratégias abrangentes.[105] A previsão de gastos globais em cibersegurança para 2025 ultrapassa USD 1 trilhão, o que cria oportunidades para melhorar a percepção de prontidão digital na América Latina.[106] A definição de orçamentos nessa área costuma refletir as condições econômicas locais, tornando-se uma prioridade à medida que as organizações reconhecem a importância da segurança de dados e da confiança na marca.[107]

Destaque: Os Estados Unidos anunciaram um pacote de ajuda no valor de USD 25 milhões até 2026 para reforçar as capacidades de defesa digital da Costa Rica, incluindo equipamentos, treinamentos especializados e apoio logístico. Antes disso, em junho de 2022, o governo costa-riquenho já havia investido USD 24 milhões em operações de segurança e resposta a incidentes. O destaque da região nesse cenário não se resume ao volume de investimentos, mas também ao fato de a Costa Rica ter se tornado o primeiro país do mundo a declarar estado de emergência em decorrência de um ataque cibernético, um marco que sinaliza a urgência do tema.[108]

Como destacado na Figura 4, o mercado de cibersegurança na América Latina deverá movimentar USD 9,54 bilhões em 2025, chegando a USD 13,35 bilhões até 2030, com uma taxa composta de crescimento (CAGR) de 6,95% ao ano. Esse avanço será impulsionado, sobretudo, pela digitalização acelerada dos serviços financeiros e das estruturas bancárias.[109] Os orçamentos já refletem um amadurecimento nos planos de preparação e resposta a incidentes, enquanto os novos investimentos indicam uma postura mais proativa por parte das instituições. O aumento do aporte em soluções de cibersegurança mostra que a região está, gradualmente, incorporando a segurança digital como parte estratégica de sua agenda institucional.[110]

Figura 4: Mercado de Cibersegurança na América Latina



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

3.1.3 Fundamentos para a Expansão dos Investimentos em Cibersegurança

A transformação digital no setor financeiro latino-americano vem exigindo aportes crescentes em segurança cibernética. A adoção de soluções baseadas em inteligência artificial e aprendizado de máquina é essencial para melhorar a capacidade de detecção e resposta frente a ameaças avançadas. Sem esses recursos, startups de fintechs da região, que operam com forte base digital, tendem a se tornar alvos preferenciais de ataques. O cenário atual reforça a necessidade de ampliar significativamente os investimentos em proteção digital na região.

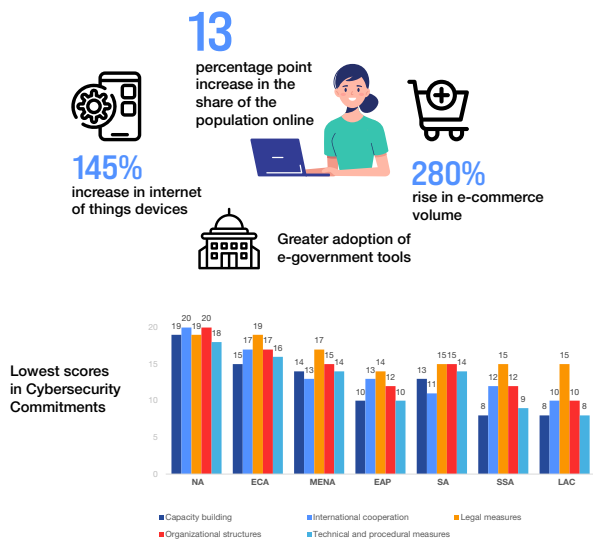
No entanto, a velocidade da digitalização não tem sido acompanhada por uma evolução equivalente nas estruturas de segurança pública. As ameaças de ransomware continuam ganhando força, enquanto programas institucionais de cibersegurança e políticas voltadas à proteção de infraestrutura crítica seguem com baixa maturidade em grande parte dos países latino-americanos.[111]

Destaque: A proteção de dados e a segurança nacional passaram a figurar como questões centrais no debate sobre cibersegurança. Após uma série de ataques de ransomware com impacto significativo, um grupo de 200 executivos de segurança da informação, que representaram tanto o setor público quanto o privado, concordaram em apontar a cibersegurança como prioridade absoluta.[112]

Além dos aspectos de defesa, os investimentos em segurança digital podem gerar benefícios macroeconômicos concretos. Um estudo estima que, com a redução do número de grandes incidentes cibernéticos de 50 para apenas 7 por ano, o PIB per capita regional poderia crescer até 1,5%. O relatório "Cybersecurity Economics for Emerging Markets" destaca que o ritmo da digitalização superou a capacidade técnica e institucional de defesa digital. Em 2024, América Latina e Caribe ocupam o último lugar global em proteção cibernética, com uma média de 10,2 pontos em 20, e apresentam a maior taxa de crescimento anual de incidentes divulgados no mundo: 25% ao ano na última década.[113] A aceleração digital, especialmente no setor financeiro, tem contribuído diretamente para o aumento da exposição a ameaças.

A expansão do acesso à internet ilustra esse movimento. Conforme dados da UIT, a porcentagem da população conectada na América Latina saltou de 68% em 2019 para 81% em 2023, conforme indicado na Figura 5.

Figura 5: Efeito da Digitalização na América Latina e Caribe (LAC)



Fonte: Cybersecurity Economics for Emerging Markets (2024).[114]

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

3.1.4 Transição de Agências Físicas para Bancos Online e via Aplicativos

O setor bancário na América Latina está cada vez mais orientado à entrega de soluções digitais centradas na experiência do usuário, com destaque para o desenvolvimento de aplicativos e plataformas online de fácil utilização. No entanto, esse movimento estratégico trouxe novas brechas de segurança, em especial nos mercados onde a digitalização bancária avançou mais rapidamente, já que facilita a proliferação de ataques de engenharia social e campanhas de phishing.[115] A conveniência segue como principal fator de adesão dos consumidores latino-americanos às soluções bancárias digitais, mesmo quando isso implica riscos consideráveis à segurança, especialmente quando os critérios de adoção priorizam a usabilidade em vez da proteção.[116]

Destaque: Iniciativas nacionais reforçam a busca por equilíbrio entre digitalização e resiliência cibernética. A Colômbia tem investido no fortalecimento da rastreabilidade de incidentes. A Costa Rica tem buscado cooperação internacional para ampliar sua capacidade de resposta, com foco em perícia digital e capacitação técnica. Já o Chile incluiu padrões de cibersegurança em sua Agenda Digital 2035, alinhando diretrizes de transformação digital à proteção de dados.[117]
A manutenção de uma boa experiência do usuário requer que instituições financeiras estejam atentas às preferências do público digital, sem comprometer os níveis de segurança.

Embora os aportes em cibersegurança no setor financeiro estejam aumentando, o avanço na construção de uma cultura organizacional orientada à segurança ainda é insuficiente. A adoção de soluções mais sofisticadas, voltadas à prevenção de riscos emergentes, é fundamental para proteger clientes e ativos financeiros em um cenário dominado por ameaças organizadas, atores patrocinados por Estados e riscos internos.

3.2 Fatores Socioeconômicos com Influência na Vulnerabilidade Cibernética

3.2.1 Expansão Rápida das Fintechs

A evolução do ecossistema de fintechs na América Latina tem sido impulsionada por fatores como alta penetração de dispositivos móveis e grande contingente de pessoas sem acesso bancário formal. Entre 2017 e 2023, o número de empresas do setor cresceu 340%, passando de 703 fintechs em 18 países para mais de 3.000 em 26 países, um ritmo que supera até mesmo mercados maduros como o dos Estados Unidos.[118].
No entanto, esse dinamismo veio acompanhado de novos riscos: muitas dessas empresas emergentes não adotam os mesmos padrões de cibersegurança das instituições financeiras tradicionais. Segundo o Fundo Monetário Internacional, os principais fatores que limitam a maturidade em cibersegurança entre as fintechs latino-americanas incluem baixa sensibilização interna, uso de sistemas desatualizados, ausência de normativas técnicas robustas, falhas estruturais em infraestrutura crítica e carência de profissionais qualificados. Esse conjunto de fragilidades representa um risco sistêmico crescente à medida que a digitalização se consolida como o novo padrão da indústria.[119]

3.2.2 Dependência de Sistemas Obsoletos

Em razão da limitação tecnológica e da infraestrutura ainda em consolidação, muitas empresas latino-americanas seguem dependentes de sistemas antigos. Estudos recentes, como o publicado na revista Informatics da MDPI, apontam o uso de softwares desatualizados como uma das principais brechas de segurança da região.[120] Essa dependência torna os sistemas vulneráveis a ameaças mais modernas, devido à ausência de correções e atualizações essenciais. Mesmo quando tais atualizações existem, restrições no hardware de base podem manter as falhas expostas. Para o setor financeiro, essa obsolescência representa um risco crítico, visto que torna as instituições alvos preferenciais de ataques. A superação desse problema exige aportes robustos na modernização da infraestrutura de TI e na adoção de políticas de manutenção contínua. Incentivar a migração para soluções em nuvem oferece uma alternativa viável, já que essas plataformas proporcionam maior segurança, atualizações automáticas e arquitetura resiliente. O Fórum Econômico Mundial sugere que a implementação de estruturas de gerenciamento de risco (RMFs) e a adoção da nuvem pública são essenciais para aumentar a capacidade de resposta a ataques de ransomware e proteger ativos estratégicos.[121] Para extrair o máximo valor dessas soluções, é imprescindível contar com equipes especializadas ou provedores externos que assegurem a aplicação consistente de controles de segurança.

[115] https://www.mordorintelligence.com/industry-reports/latin-america-cyber-security-market
[116] 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
[117] https://digiamericas.org/wp-content/uploads/2024/05/LATAM-CISO-REPORT-2024_.pdf
[118] https://www.iadb.org/en/news/study-fintech-ecosystem-latin-america-and-caribbean-exceeds-3000-startups
[119] https://www.imf.org/en/Publications/fintech-notes/Issues/2023/03/28/The-Rise-and-Impact-of-Fintech-in-Latin-America-531055
[120] https://www.mdpi.com/2227-9709/10/3/71
[121] https://www.weforum.org/stories/2024/05/latin-america-cybersecurity-report-ransomware attacks/

3.2.3 Desigualdade de Acesso e Vulnerabilidade Digital

As diferenças socioeconômicas e o acesso desigual à internet acentuam o risco digital na América Latina. Em 2022, apenas dois terços dos domicílios da região tinham acesso à rede, enquanto nos países da OCDE o índice ultrapassava 91%.[122] Esse cenário impacta diretamente as PMEs, que são a espinha dorsal da economia latino-americana,[123] mas enfrentam limitações orçamentárias que comprometem a adoção de sistemas de defesa digital. Sem recursos para implantar camadas de segurança robustas, essas empresas se tornam alvos preferenciais de ataques, especialmente porque carecem da estrutura tecnológica das grandes corporações. Investir em conectividade e infraestrutura digital para reduzir a lacuna tecnológica, tanto entre cidadãos quanto entre empresas, é essencial para reforçar a segurança e mitigar riscos crescentes.

[122] https://www.undp.org/latin-america/blog/missed-connections-incomplete-digital-revolution-latin-america-and-caribbean-0
[123] 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 Lacunas Regulatórias

4.1 Ausência de Padrões Uniformes para Notificação de Incidentes com Ransomware

A heterogeneidade nos requisitos legais de notificação de incidentes cibernéticos na América Latina compromete diretamente a capacidade regional de resposta coordenada a ataques digitais, em especial os de ransomware. O cenário é marcado por fragmentação normativa e práticas desiguais entre países.

Alguns exemplos ilustram esse panorama:

1. No Brasil, a LGPD impõe que incidentes sejam reportados à ANPD em até dois dias úteis, além da obrigatoriedade de notificar os usuários afetados.[124]

2. A Colômbia adota exigências similares, com reporte à Delegatura para la Protección de Datos Personales e às partes impactadas.[125]

3. O México exige notificação de vulnerabilidades de dados, mas não estipula prazos formais.

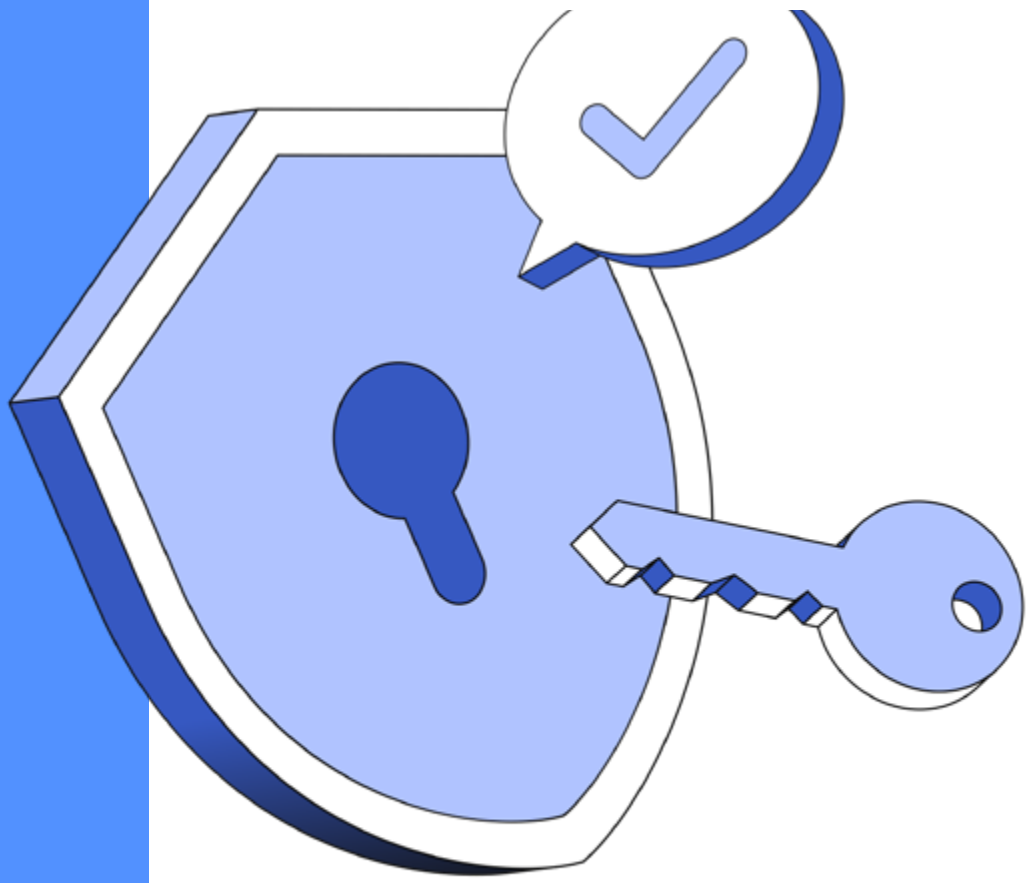
4. A Argentina trata o tema apenas como uma recomendação voluntária.[126]

5. Já países como Peru, Equador e Costa Rica operam sem estrutura normativa abrangente nesse campo.[127]

Esse mosaico regulatório deixa brechas amplas na defesa institucional da região. Países sem exigências obrigatórias ou prazos definidos enfrentam obstáculos reais para rastrear ataques, compartilhar dados de ameaça e implementar ações coordenadas.[128] A ausência de padrões comuns permite disparidades operacionais que tornam os sistemas vulneráveis à ação de cibercriminosos.[129] Essa fragilidade é acentuada pela limitação de infraestrutura cibernética, baixa formação especializada e escassez de recursos. Setores sensíveis, como o industrial e o financeiro, já contabilizam mais de 100 incidentes de ransomware desde 2023, evidenciando o impacto direto dessa lacuna normativa.[130] [131]

A inexistência de obrigações formais para notificação compromete ainda mais a velocidade e eficiência das respostas, ampliando o tempo de exploração dos sistemas comprometidos.[132] Enquanto a digitalização do setor financeiro avança rapidamente, a regulação não acompanha o mesmo ritmo. Isso expande a superfície de ataque e expõe instituições a riscos que poderiam ser mitigados com marcos legais mais sólidos.[133] [134] Sem uma estratégia conjunta para reporte e contenção de incidentes, muitos países da região continuarão em desvantagem frente à sofisticação crescente dos ataques direcionados ao setor público e às finanças.[135] [136]

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



5 Perfis de Ameaça Ativa no Setor Corporativo

5.1 CL0P

O grupo CL0P emergiu em 2019 como uma variação sofisticada do ransomware Cryptomix,[137] evoluindo rapidamente de campanhas tradicionais de phishing para um ecossistema altamente profissionalizado de ataques cibernéticos.[138] Com a introdução da extensão ".clop" nos arquivos sequestrados e a assinatura “Don't Worry CL0P” nas mensagens de resgate, o grupo rapidamente estabeleceu uma identidade própria.[139] A adoção do modelo Ransomware-as-a-Service (RaaS) marcou uma virada estratégica, permitindo ao grupo terceirizar a distribuição do malware por meio de parcerias com atores especializados como TA505, FIN11 e UNC 2546.

5.1.1 Perfil das Vítimas e Dimensão dos Ataques

O histórico de vítimas revela um foco do CL0P em grandes corporações com receitas superiores a USD 5 milhões anuais,[140] operando em setores críticos como finanças, saúde, indústria, energia e educação.[141] Os ataques se concentram majoritariamente em países como Estados Unidos, Reino Unido, Alemanha, Canadá, Brasil e México, que juntos somam mais de 77% das ações identificadas.[142]

Na América Latina, os impactos têm sido particularmente severos em Brasil e México, refletindo fragilidades estruturais nos ecossistemas digitais locais.[143] A combinação de conectividade crescente, baixa maturidade em resposta a incidentes e fragmentação regulatória amplia a superfície de exposição. Instituições financeiras enfrentam riscos em duas frentes: ataques diretos aos sistemas bancários e invasões indiretas por falhas na cadeia de fornecedores, como demonstrado no ataque envolvendo a vulnerabilidade zero-day do MOVEit, que comprometeu centenas de entidades.

Dimensão e Intensidade das Ações do CL0P:

- O grupo CL0P aumentou sua base de vítimas em 340% no último trimestre, com crescimento impulsionado principalmente pela exploração da vulnerabilidade zero-day do MOVEit.[144]
- A estimativa de ganhos com a campanha de extorsão baseada no vazamento de dados é de USD 75 a 100 milhões, posicionando a operação entre as mais lucrativas do tipo.[145]

5.1.2 Arquitetura Técnica e Recursos do Malware

A sofisticação técnica do CL0P fica evidente na estruturação detalhada das cadeias de ataque. Seus vetores de acesso inicial evoluíram de simples campanhas de phishing para a exploração de vulnerabilidades zero-day altamente avançadas.[146]. O grupo opera com um arsenal variado de ferramentas, incluindo malwares especializados como SDBot (para movimentação lateral), Cobalt Strike (para ações pós-exploração) e ferramentas personalizadas como FlawedAmmyy/FlawedGrace (usadas para comando e controle).[147]

O uso do TrueBot, um malware avançado associado ao grupo Silence, reforça os vínculos do CL0P com atores especializados em ameaças ao setor financeiro. A capacidade do TrueBot de implantar cargas adicionais enquanto mantém discrição com mecanismos de autodeleção revela uma abordagem focada em segurança operacional.[148] Além disso, o uso do backdoor exclusivo FlawedGrace, também associado ao TA505, reforça o papel do CL0P dentro de um ecossistema cibernético altamente sofisticado.[149] O processo de invasão geralmente segue uma abordagem orquestrada em múltiplas etapas:

1. Exploração de aplicações web públicas por meio do web shell LEMURLOOT, escrito em C# e disfarçado como um arquivo ASP.NET. 2. Operações de coleta de credenciais que permitem movimentação lateral e acesso a dados sensíveis. 3. Operações de roubo de dados com foco na exfiltração, evitando criptografia, e com atenção à segurança operacional.[150]

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

5.1.3 Panorama da transformação operacional do grupo CL0P

1. Mudança no vetor de ataque: O grupo criminoso abandonou sua estratégia original baseada em campanhas de phishing com anexos maliciosos [151] e passou a explorar falhas zero-day em soluções amplamente utilizadas para transferência de arquivos, alterando radicalmente sua porta de entrada nos sistemas-alvo.[152] [153]

2. Foco na exfiltração de dados: O foco atual recai sobre a extração de dados sensíveis. Em vez de criptografar arquivos como no passado, o CL0P tem priorizado operações que exfiltram informações confidenciais sem interferir diretamente nos sistemas das vítimas.[154] [155]

3. Escala dos ataques: Ataques recentes têm sido conduzidos em larga escala, aproveitando-se de vulnerabilidades em fornecedores para atingir diversas empresas ao mesmo tempo. O caso do MOVEit, em 2023, afetou aproximadamente 400 organizações.[156]

4. Sofisticação das técnicas: O grupo passou a adotar mecanismos mais sofisticados para evitar a detecção, como o uso de assinaturas digitais para burlar soluções de segurança em endpoints.[157]

5. Expansão para novas plataformas: A atuação, antes restrita ao ecossistema Windows, foi expandida com o desenvolvimento de uma versão do malware compatível com Linux no final de 2022, ampliando a superfície de ataque.[158]

6. Abordagem de resgate: Houve também mudança na forma de pressionar as vítimas: em vez das notas de resgate deixadas nos sistemas, o CL0P tem buscado contato direto com executivos da alta liderança, tornando a negociação mais direta e potencialmente mais impactante.[159]

7. Linha do tempo da exploração: Há evidências de que o ataque ao MOVEit foi cuidadosamente preparado desde 2021, o que demonstra maior disciplina operacional e visão de longo prazo.[160]

O abandono da criptografia e a priorização da extração silenciosa de dados revelam uma mudança significativa no modelo de atuação do CL0P. Essa abordagem permite que o grupo opere de maneira furtiva, sem levantar suspeitas imediatas, dificultando a identificação do ataque por parte das vítimas.

Essa nova direção tática se sustenta em quatro pilares principais:

1. Menor risco de detecção: Ao eliminar o uso de criptografia, os sinais típicos de invasão (IOCs) desaparecem, dificultando a resposta rápida das equipes de segurança.

2. Acesso prolongado: Ao evitar alertar a vítima por meio da criptografia, o CL0P pode manter o acesso aos sistemas por mais tempo, permitindo um roubo de dados mais abrangente.

3. Operação simplificada: Ao simplificar o ataque, o grupo reduz seus custos operacionais e pode ampliar a quantidade de alvos comprometidos simultaneamente.

4. Maior pressão: A ameaça de exposição de dados sensíveis tem se mostrado tão eficaz quanto a interrupção dos sistemas via criptografia, sem os riscos associados à entrega de ferramentas de descriptografia.

A eficácia da mudança de estratégia adotada pelo CL0P ficou evidente em ofensivas recentes, como no caso MOVEit em 2023. Nessa operação, o grupo alegou ter comprometido os dados de centenas de organizações ao explorar uma falha zero-day crítica (CVE-2023-34362), permitindo o acesso em massa a informações sensíveis sem realizar qualquer tipo de criptografia.[161] Com essa abordagem silenciosa, o CL0P eleva a taxa de sucesso das campanhas e, ao mesmo tempo, aumenta a pressão sobre as vítimas, que buscam evitar danos reputacionais ou vazamentos com consequências regulatórias.

Apesar de ainda haver pouca comprovação formal sobre a adoção oficial dessa estratégia furtiva, analistas de segurança da informação já reconhecem uma tendência consolidada: grupos de ransomware estão se afastando da criptografia e focando exclusivamente na extorsão de dados. A razão é clara: essa tática oferece uma série de benefícios estratégicos:

[151] https://www.nuspire.com/blog/a-deep-dive-into-cl0p-ransomware/
[152] https://em360tech.com/tech-article/what-is-cl0p-ransomware
[153] https://www.criticalstart.com/threat-research-cl0p-ransomware-increases-activity
[154] https://em360tech.com/tech-article/what-is-cl0p-ransomware
[155] https://www.criticalstart.com/threat-research-cl0p-ransomware-increases-activity
[156] https://www.criticalstart.com/threat-research-cl0p-ransomware-increases-activity
[157] https://em360tech.com/tech-article/what-is-cl0p-ransomware
[158] https://www.criticalstart.com/threat-research-cl0p-ransomware-increases-activity
[159] https://em360tech.com/tech-article/what-is-cl0p-ransomware
[160] https://em360tech.com/tech-article/what-is-cl0p-ransomware
[161] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware double-extortion-and-beyond-revil-clop-and-conti

1. Extorsão prolongada: Com os dados em mãos, os criminosos podem reativar ameaças a qualquer momento, inclusive após um pagamento inicial, mantendo um ciclo contínuo de pressão.[162]

2. Exigências direcionadas: A posse de informações específicas permite personalizar o valor dos resgates, alinhando-os ao impacto potencial do vazamento.[163] [164]

3. Intensificação da pressão: Ao explorar diretamente os riscos legais, danos de imagem e perda de vantagem competitiva, os extorsionistas aumentam a probabilidade de receber pagamento.[165] [166]

4. Superação dos backups: A recuperação de arquivos via backup torna-se irrelevante diante da realidade do roubo de dados, já que uma vez que são exfiltrados, não há como desfazer o dano.[167]

5. Geração de novas ameaças: As informações obtidas podem ser reutilizadas para ataques posteriores, incluindo tentativas de acesso a outros sistemas ou manipulação de credenciais.[168]

6. Monetização expandida: O valor de mercado dos dados roubados pode superar em muito o resgate direto, seja por venda na dark web ou pela continuidade da exploração extorsiva.[169]

A migração das operações do CL0P para estratégias baseadas em exfiltração de dados reflete um movimento claro de adaptação frente ao fortalecimento das defesas corporativas. Em vez de insistirem em métodos tradicionais, os grupos de ransomware têm buscado abordagens mais eficazes para manter a pressão sobre suas vítimas e aumentar suas chances de retorno financeiro.[170] [171]

Desde sua estreia em 2019, o CL0P tem refinado continuamente sua atuação, consolidando-se até 2023 como uma das ameaças mais impactantes do cenário global. O foco estratégico em vulnerabilidades zero-day presentes em ferramentas de transferência de arquivos (FTAs) está diretamente ligado a fatores que ampliam seu alcance e potencial ofensivo:

1. Alta penetração no mercado corporativo: Ferramentas como essas são amplamente utilizadas em ambientes empresariais, o que proporciona ao grupo múltiplas portas de entrada em larga escala.[172]

2. Ataques em efeito cascata: A exploração de brechas em FTAs permite comprometer toda uma cadeia de parceiros e fornecedores, potencializando o impacto com esforço reduzido.[173] [174]

3. Extração otimizada de grandes volumes: A infraestrutura dos FTAs, pensada para desempenho, facilita a movimentação de quantidades significativas de dados de maneira ágil e silenciosa.

4. Ambientes regulados com dados críticos: Muitos FTAs, como o MOVEit, são autorizados para uso em setores regulados e, por isso, costumam armazenar dados altamente sensíveis.[175]

5. Perfil atrativo das vítimas: Grandes corporações e órgãos públicos, principais usuários dessas soluções, representam oportunidades de extorsão mais rentáveis.[176] [177]

6. Baixa visibilidade das ações maliciosas: Ao explorar sistemas legítimos, o grupo consegue disfarçar suas ações sob o tráfego normal de rede, evitando alertas de segurança.

A eficácia desse modelo operacional foi amplamente comprovada nos ataques bem-sucedidos contra plataformas como Accellion FTA, GoAnywhere MFT e MOVEit Transfer. Cada um desses episódios envolveu o comprometimento de centenas de entidades, com impactos que se estendem à exposição de dados de milhões de pessoas.[178] [179]

5.1.4 Impacto na Infraestrutura Financeira

As ações coordenadas do grupo CL0P contra instituições financeiras expuseram falhas estruturais relevantes nos modelos de segurança amplamente adotados pelo setor. A capacidade do grupo de comprometer sistemas gerenciados de transferência de arquivos colocou em evidência fragilidades críticas tanto no controle de fluxos de dados sensíveis quanto na integração de soluções de terceiros.[180] Um único

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

ponto de falha, como demonstrado na ofensiva contra a plataforma MOVEit, foi suficiente para provocar incidentes em diversas instituições simultaneamente, ampliando o alcance do dano.[181]

O impacto, no entanto, não se limita à interrupção de serviços. As instituições afetadas também enfrentam dificuldades prolongadas para manter a conformidade regulatória em meio a compromissos de segurança em andamento. O desenvolvimento de políticas internas mais robustas torna-se desafiador num cenário já marcado por regulamentações complexas e desarticuladas entre diferentes jurisdições. No Peru, por exemplo, quase metade dos líderes de segurança da informação (47%) identificam o cumprimento de normas regulatórias desconectadas geograficamente como a parte mais desgastante do trabalho.

Em escala global, o setor financeiro se destaca como o mais sensível à fragmentação normativa, com 67% dos CISOs prevendo que a gestão dessas exigências se tornará ainda mais difícil no curto prazo. O CL0P tem capitalizado sobre essa vulnerabilidade estratégica: seu conhecimento aprofundado sobre os mecanismos regulatórios do setor permite elaborar demandas de extorsão altamente personalizadas, explorando ao máximo os riscos legais e reputacionais [26].

Durante a campanha MOVEit, o grupo demonstrou domínio tático ao escalonar a divulgação de dados das vítimas em blocos, pressionando continuamente as organizações ao longo do tempo em vez de realizar uma liberação única.[182]

A realidade da América Latina acrescenta camadas adicionais de complexidade. Com mais de 1.600 tentativas de ataque digital por segundo em empresas da região, o ambiente operacional das instituições financeiras está sob ataque constante.[183] A interconexão das redes bancárias e o uso comum de infraestruturas e softwares regionais criam um terreno fértil para efeitos em cadeia.[184] Um exemplo concreto desse fenômeno foi a campanha GoAnywhere MFT, na qual várias instituições descobriram violações interligadas através de dependências compartilhadas, revelando a vulnerabilidade sistêmica do ecossistema financeiro regional.[185]

5.1.5 Lacunas na Regulamentação e em Políticas Públicas

1. Estruturas Limitadas para Proteção de Infraestruturas Críticas

A proteção cibernética das infraestruturas críticas na América Latina ainda é incipiente, o que expõe vulnerabilidades estratégicas. Dados do BID revelam que apenas 7 dos 32 países latino-americanos possuem planos estruturados contra ameaças digitais nesse setor, e só 20 têm CSIRTs operando de forma reconhecida.[186] Essa lacuna pesa especialmente sobre o setor financeiro, que continua desprotegido pela ausência de normas federais unificadas para segurança cibernética e pela inexistência de requisitos claros de reporte de incidentes em nível regional.[187]

2. Coordenação Fragmentada na Resposta a Incidentes

A inexistência de um modelo coordenado de governança em cibersegurança complica a resposta a ataques de grande escala. Isso foi evidente em eventos recentes como o ataque de ransomware à Costa Rica em 2022 e a ofensiva contra a IFX Networks na Colômbia em 2023, que começou atingindo 20 órgãos públicos, mas rapidamente se espalhou, afetando mais 78 instituições públicas e 762 empresas privadas, inclusive do setor financeiro.[188] A despadronização nos protocolos de resposta facilita a atuação de grupos como o CL0P, que tem capitalizado sobre essas falhas ao explorar brechas em plataformas corporativas amplamente utilizadas.

3. Exigências Insuficientes de Notificação Obrigatória

Muitos países da América Latina ainda não implementaram regras claras e abrangentes para a notificação obrigatória de violações de segurança, especialmente no setor financeiro. Essa falha normativa favorece táticas como as do grupo CL0P, que se aproveita da assimetria de informações e da demora na detecção de incidentes.[189] A ausência de exigências rigorosas de reporte estende a janela de atuação desses grupos, permitindo que mantenham presença por mais tempo dentro das redes comprometidas.

4. Desafios na Aplicação das Leis de Proteção de Dados

Apesar de avanços legislativos em países como Brasil, México e Colômbia, a aplicação das leis de proteção de dados ainda encontra obstáculos operacionais e falhas de fiscalização. Essa inconsistência compromete

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

a segurança de informações sensíveis mantidas por instituições financeiras, ampliando a exposição a ameaças como as promovidas pelo CL0P, que têm foco declarado em roubo de dados e extorsão progressiva. O uso recorrente de ferramentas como FlawedAmmyy e FlawedGrace sinaliza o grau de adaptação técnica do grupo às vulnerabilidades específicas do setor financeiro regional.

5.1.6 Panorama do Setor Bancário Latino-Americano e Aceleração Digital

A América Latina se mantém como a região de maior expansão bancária do mundo, sustentando um crescimento anual médio de 12% na receita bruta desde 2012, que alcançou US$ 418 bilhões em 2017. Desde 2020, o setor de varejo bancário duplicou sua taxa de crescimento anual em relação ao período entre 2013 e 2019, em termos de receita em trilhões de dólares.[190] Paralelamente, a evolução das receitas com pagamentos digitais tem colocado a região na liderança global até, pelo menos, 2027.[191]. Esse crescimento vertiginoso, somado à baixa bancarização regional, que é de 30% a 50%, frente a mais de 90% nos mercados desenvolvidos, acelera a adoção de soluções digitais, muitas vezes sem o devido acompanhamento das estratégias de segurança.[192] A mudança de comportamento do consumidor, com uma preferência crescente por pagamentos móveis e cartões desde 2021, tem impulsionado os bancos a priorizarem modelos digitais centrados no mobile, ao mesmo tempo em que redirecionam investimentos em TI para fortalecer a experiência do cliente.[193]

5.1.7 Conflito Entre Pressão por Lucros e Investimentos em Segurança

Apesar do histórico de rentabilidade robusta, com um retorno sobre patrimônio (ROE) de 14% em 2017, os bancos da região lidam com desafios relevantes em eficiência operacional. As despesas giram em torno de 3,9% dos ativos totais, um patamar 1,5% acima da segunda região mais onerosa.[194] Esse cenário financeiro exige decisões estratégicas sobre alocação de recursos, o que frequentemente leva a concessões em cibersegurança. Áreas como crédito ao consumidor e financiamento habitacional, que somam mais de um terço da receita líquida ajustada ao risco, representam um risco adicional, por concentrarem volumes elevados de dados sensíveis que atraem agentes maliciosos.[195]

5.1.8 Fragilidades Específicas do Setor Financeiro

1. Transformação Digital como Vetor de Risco

A digitalização acelerada no setor financeiro latino-americano, impulsionada pela expansão do acesso bancário pós-pandemia, tem ampliado a superfície de ataque das instituições. Grupos como o CL0P têm explorado essas fragilidades com ataques estruturados, como demonstrado no caso da campanha MOVEit, que atingiu um número expressivo de bancos na região. Um dos principais pontos de vulnerabilidade é a adoção prematura de soluções como os sistemas de transferência gerenciada de arquivos (MFT), que muitas vezes entram em operação sem protocolos de segurança maduros.[196] Para sustentar o ritmo de inovação com responsabilidade, instituições devem garantir que contam com expertise sólida em segurança digital e resiliência operacional antes de integrar novas tecnologias aos seus ambientes críticos.

2. Principais Fatores Operacionais de Risco no Setor Financeiro da América Latina

As fragilidades operacionais no setor bancário regional estão associadas a três modelos de mercado distintos observados na América Latina[197]:

- Mercados com foco em eficiência, como o chileno, adotam estruturas enxutas com despesas operacionais inferiores a 3,4% dos ativos. Essa busca por eficiência, no entanto, geralmente vem acompanhada de investimentos limitados em segurança, deixando brechas que comprometem a resiliência cibernética.
- Mercados equilibrados, como o brasileiro, apresentam geração de receita moderada (entre 4,5% e 7% dos ativos) e custos operacionais intermediários. Esse equilíbrio força instituições a priorizarem investimentos, muitas vezes colocando segurança em segundo plano.
- Mercados com foco em receita, como o argentino, geram alta rentabilidade, mas operam com custos acima de 5,5% dos ativos. Apesar do volume de recursos, a eficiência nas práticas de segurança digital pode ser deficitária, dificultando a mitigação de riscos com eficácia.

3. Carência Crítica de Capital Humano em Segurança Cibernética

Um dos gargalos estruturais mais significativos é a escassez de talentos em cibersegurança. Estima-se que só o Chile precise suprir, anualmente, uma lacuna de cerca de 6 mil profissionais de TI.[198] Para o setor

[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

financeiro, esse déficit compromete diretamente a capacidade de:

- Adotar soluções de segurança avançadas
- Sustentar operações de segurança robustas
- Reagir com agilidade a ameaças emergentes
- Acompanhar a sofisticação crescente das táticas de ataque

Esse desequilíbrio entre demanda e oferta de profissionais favorece atores como o CL0P, que exploram falhas operacionais e lacunas na capacidade de resposta a incidentes.

4. Riscos Sistêmicos Gerados por Infraestruturas Compartilhadas

A dependência de plataformas comuns e serviços compartilhados entre instituições financeiras na região tem gerado riscos sistêmicos relevantes. O episódio envolvendo a IFX Networks, em setembro de 2023, revelou como o comprometimento de um único provedor pode gerar impactos em escala, atingindo múltiplas instituições financeiras de diferentes países.[199] Esse nível de interdependência, somado à falta de políticas de proteção de infraestrutura crítica na região, amplia a exposição a ataques coordenados como os promovidos pelo CL0P.

5.1.9 Riscos em Cadeia Derivados de Fragilidades no Setor Público

1. Assimetrias na Distribuição de Recursos Públicos

Os orçamentos de cibersegurança do setor público na América Latina ficam constantemente atrás dos investimentos feitos pelo setor privado. Isso gera desafios significativos para instituições financeiras que precisam se conectar a sistemas governamentais, especialmente nas áreas de:

- Arrecadação de impostos e envio de declarações
- Plataformas de conformidade regulatória
- Infraestruturas nacionais de pagamento
- Serviços de verificação de identidade

As metodologias de ataque do grupo CL0P costumam explorar justamente esses pontos de interconexão entre sistemas públicos e privados, como ficou evidente nos incidentes registrados na Costa Rica e na Colômbia.[200]

5.1.10 Convergência de Vulnerabilidades Criando Oportunidade Estratégica para o CL0P

A soma de lacunas regulatórias com tendências estruturais da indústria abre múltiplas frentes de ataque que coincidem com a metodologia sofisticada do CL0P e seu modo de operação:

1. Operações de Extorsão em Etapas

O modelo de ataque multiestágio adotado pelo CL0P é especialmente eficaz no cenário latino-americano, favorecido por fatores como:

- Déficit de profissionais especializados em segurança cibernética, o que compromete a capacidade de detecção precoce
- Complexidade envolvida na articulação entre diferentes países diante de incidentes
- Ausência de padrões consistentes para reporte de violações
- Integração dos sistemas financeiros nacionais em redes regionais

Esse cenário permite ao CL0P obter acesso inicial com facilidade e ampliar o alcance dentro das redes comprometidas.[201]

2. Superfície Ampliada no Ecossistema Bancário

A digitalização dos serviços financeiros e as exigências de compliance regulatório ampliaram os pontos de entrada possíveis para cibercriminosos. O CL0P demonstra um conhecimento técnico refinado da dinâmica operacional do setor e tem direcionado suas ofensivas a componentes críticos, incluindo:

- Sistemas de transferência de arquivos usados em processos regulatórios
- Brechas em protocolos de autenticação e controle de acesso
- Terceirizados que prestam serviços simultaneamente a diversas instituições
- Infraestruturas de pagamento e compensação transfronteiriças
- Plataformas bancárias core utilizadas regionalmente

As ferramentas utilizadas, como TrueBot e FlawedGrace, foram projetadas especificamente para contornar os mecanismos de proteção típicos do setor financeiro.[202]

[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/

3. Potencial de Propagação Regional

A forte interconexão entre os sistemas financeiros da América Latina aumenta o potencial de impacto de um único incidente. Essa capacidade de amplificação, onde o comprometimento de uma entidade pode desencadear efeitos sistêmicos em escala regional, torna o ambiente ainda mais atrativo para grupos de ransomware que buscam alavancagem máxima em seus esquemas de extorsão.

5.1.11 Implicações Futuras

Cenário de Ameaças em Evolução

A combinação entre falhas regulatórias e pressões do setor indica que instituições financeiras da América Latina continuarão sendo alvo de grupos cibercriminosos sofisticados. A capacidade demonstrada do CL0P de adaptar suas táticas às vulnerabilidades regionais aponta para as seguintes tendências:

- Aumento do nível de sofisticação dos ataques
- Maior frequência de incidentes com impacto transfronteiriço
- Continuidade de ataques por meio de cadeias de suprimento comprometidas
- Expansão de operações de extorsão em múltiplas fases

5.1.12 Táticas, Técnicas e Procedimentos do CL0P

Táticas	Técnicas	Procedimentos
Reconhecimento (TA0043)	T1592: Coleta de informações do host	Usa técnicas de phishing e engenharia social para obter informações sobre os alvos
	T1589.002: Endereços de e-mail	Obtém credenciais das vítimas por meio de phishing, engenharia social e acesso via brokers (IABs)
	T1589.001: Credenciais	A ser determinado
	T1590: Coleta de informações da rede da vítima	Acesso à infraestrutura de rede via phishing, engenharia social e IABs
	T1589: Coleta de informações da rede da vítima	Obtém dados de identidade e rede usando phishing e engenharia social
Desenvolvimento de Recursos (TA0042)	T1586: Comprometimento de contas	Se apropria de contas existentes por meio de phishing, engenharia social e IABs
Acesso Inicial (TA0001)	T1133: Comprometimento de serviços remotos externos	Acessa redes corporativas por meio de contas comprometidas
	T1190: Exploração de aplicativos com acesso público	Faz varredura de sistemas expostos para encontrar e explorar vulnerabilidades do tipo zero-day
	T1566: Phishing	Envia e-mails fraudulentos para obter acesso e extrair dados e credenciais
	T1091: Replicação por mídia removível	Verifica se há dispositivos conectados (como pendrives) para infectá-los
	T1078.003: Contas locais	A ser determinado
Execução (TA0002)	T1059.001: PowerShell	A ser determinado
	T1059.003: Windows Command Shell	A ser determinado
	T1047: Windows Management Instrumentation	Consulta informações da BIOS usando WMI (via WMI, Win32_Bios)
	T1106: Native API	A ser determinado
	T1053.003: Cron	A ser determinado
	T1053.005: Tarefa Agendada	A ser determinado
	T204.002: Arquivo Malicioso	A ser determinado
Persistence (TA0003)	T1098: Manipulação de Contas	Usa contas comprometidas para obter privilégios de administrador ou criar novas contas com esse nível de acesso
	T1574.001: Pasta de Inicialização/ Registro	Armazena arquivos na pasta de inicialização do Windows
	T1037.004: Scripts RC	A ser determinado
	T1136: Criação de Conta	Cria novas contas com privilégios administrativos usando contas já comprometidas
	T1543.002: Serviço Systemd	A ser determinado
	T1133: Serviços Remotos Externos	A ser determinado

Táticas	Técnicas	Procedimentos
	T1574.002: DLL Side-Loading	Tenta carregar DLLs ausentes para execução maliciosa
	T1053.003: Cron	A ser determinado
	T1053.005: Tarefa Agendada	A ser determinado
	T1505: Componente de Software de Servidor	A ser determinado
	T1505.001: Procedimento Armazenado em SQL	A ser determinado
	T1505.003: Web Shell	A ser determinado
	T1078: Contas Válidas	Utiliza contas comprometidas para obter ou escalar privilégios administrativos
	T1078.003: Contas Locais	Usa contas locais comprometidas para criar ou escalar acessos com privilégios de administrador
Privilege Escalation (TA0004)	T1548.002: Burla o Controle de Conta de Usuário	Executa código malicioso com privilégios de administrador
	T1098: Manipulação de Contas	Usa contas comprometidas para obter ou escalar acesso administrativo
	T1574.001: Pasta de Inicialização/ Registro	Armazena arquivos na pasta de inicialização do Windows
	T1037.004: Scripts RC	A ser determinado
	T1543.002: Serviço Systemd	A ser determinado
	T1068: Exploração para Escalada de Privilégio	Explora vulnerabilidades conhecidas em software para elevar o nível de acesso
	T1574.002: DLL Side-Loading	Executa DLLs maliciosas ausentes
	T1053.003: Cron	To be determined
	T1053.005: Tarefa Agendada	Exclui cópias dos volumes para impedir a recuperação do sistema
	T1078.003: Contas Locais	Usa contas locais comprometidas para escalar privilégios administrativos
Evasão de Defesa(TA0005)	T1222.002: Modificação de Permissões de Arquivos e Diretórios em Linux e Mac	A ser determinado
	T1497.001: Verificações de Sistema	Referências a strings anti-VM direcionadas ao Xen
	T1078: Contas Válidas	Usa contas comprometidas para obter privilégios administrativos ou criar novas contas com esse nível de acesso
	T1078.003: Contas Locais	Usa contas locais comprometidas para escalar privilégios administrativos
	T1218.007: Msiexec	A ser determinado
	T1218.010: Regsvr32	A ser determinado
	T1218.011: Rundll32	A ser determinado

Táticas	Técnicas	Procedimentos
	T1553.002: Assinatura de Código	A ser determinado
	T1112: Modificação de Registro	Usa chaves de registro para manter persistência e desativar sistemas de segurança em máquinas infectadas
	T1070.002: Limpeza de Logs em Linux ou Mac	A ser determinado
	T1574.002: DLL Side-Loading	Tenta carregar DLLs ausentes
	T1140: Desofuscar ou Decodificar Arquivos ou Informações	A ser determinado
	T1622: Evasão de Depurador	A amostra pode detectar máquinas virtuais ou ambientes de debug por meio de leitura de disco
	T1548.002: Burla o Controle de Conta de Usuário	Executa código malicioso com privilégios de administrador
Acesso a Credenciais (TA0006)	T1003.001: Memória do LSASS	A ser determinado
	T1552.007: API de Contêiner	A ser determinado
Descoberta (TA0007)	T1622: Evasão de Depurador	A amostra pode detectar máquinas virtuais ou depuradores por meio de leitura de disco
	T1083: Descoberta de Arquivos e Diretórios	Varre o sistema de arquivos, lê arquivos INI, enumera diretórios e obtém tamanhos de arquivos
	T1135: Descoberta de Compartilhamentos de Rede	Identifica compartilhamentos em rede
	T1057: Descoberta de Processos	Lista todos os processos em execução
	T1012: Consulta ao Registro	Consulta valores e chaves de registro do sistema
	T1082: Descoberta de Informações do Sistema	Coleta informações da BIOS (via WMI), volume de disco, políticas de software e dados de armazenamento
	T1497.001: Verificações de Sistema	A ser determinado
Movimentação Lateral (TA0008)	T1021.002 Compartilhamentos SMB/ Admin do Windows	A ser determinado
	T1021.002 SSH	A ser determinado
	T1021.006 Gerenciamento Remoto do Windows	A ser determinado
	T1091: Replicação por Mídia Removível	Verifica unidades disponíveis no sistema (frequentemente para infectar dispositivos USB)
	T1021.001: Protocolo de Área de Trabalho Remota (RDP)	A ser determinado
Collection (TA0009)	T1005: Dados do Sistema Local	Coleta informações de disco
Command and Control (C2) (TA0011)	T1071.001: Protocolos Web	Usa protocolos de camada de aplicação para baixar malware e chaves de criptografia
	T1573.001: Criptografia Simétrica	
	T1105: Transferência de Ferramentas de Entrada	A ser determinado
	T1104: Canais em Múltiplas Etapas	A ser determinado
	T1571: Porta Não Padrão	A ser determinado

Exfiltração de Dados (TA0010)	T1041: Exfiltração via Canal C2	Estabelece conexão com servidor C2 via HTTPS para baixar malware e chaves de criptografia
	T1052.001: Exfiltração via USB	Verifica unidades conectadas ao sistema (geralmente para infectar USBs)
	T1567.002: Exfiltração para Armazenamento em Nuvem	A ser determinado
Impact (TA0040)	T1485: Destruição de Dados	A ser determinado
	T1486: Criptografia de Dados com Propósito de Impacto	A ser determinado
	T1565: Manipulação de Dados	A ser determinado
	T1496: Uso Indevido de Recursos	A ser determinado
	T1489: Interrupção de Serviços	A ser determinado

Indicadores de Comprometimento (IoCs):

Hashes:

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

Domínios de Internet:

- 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

Assinaturas de Malware:

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

Endereços IP:

- 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

Falhas de Segurança (CVEs) mencionadas:

- 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 Indicadores Técnicos e Estratégias de Contenção para Ameaças Avançadas como o CL0P

As recomendações abaixo foram desenhadas para mitigar tecnicamente as técnicas utilizadas pelo CL0P, conforme o framework MITRE ATT&CK. Elas foram organizadas com base no grau de criticidade, considerando impacto potencial, continuidade do negócio, segurança da informação e resiliência operacional.

Com base na matriz de mitigação D3FEND da MITRE, essas diretrizes trazem orientações práticas, resultados esperados e considerações-chave sobre sua implementação e alocação de recursos. Não são exaustivas, mas focam em mitigar os vetores mais críticos.

Medidas Estratégicas Contra Ameaças Cibernéticas de Alto Impacto:

T1190 (Ameaças por Aplicações Abertas ao Público)

1. Implemente e configure firewalls de aplicação web (WAFs) para filtrar tráfego malicioso: Adoção de firewalls específicos para aplicações web, com regras calibradas para bloquear ataques como SQL Injection, XSS e execução remota de código. O ajuste contínuo dessas regras, com base em padrões emergentes, garante que tentativas maliciosas sejam barradas antes de atingir a camada lógica da aplicação. Esse controle reduz exposição e amplia a resiliência digital.

2. Separe serviços voltados para o público de sistemas internos: A arquitetura de rede deve contemplar zonas isoladas (DMZ) para que os serviços públicos não tenham conexão direta com dados sensíveis ou estruturas críticas. Com a implantação de firewalls de alta restrição e política de acesso restritivo, a estratégia dificulta movimentações laterais em caso de comprometimento. O objetivo é mitigar riscos estruturais em eventuais invasões.

3. Realize varreduras e atualizações regulares em aplicações com acesso externo: A manutenção da segurança passa por varreduras frequentes em sistemas externos e uma rotina bem definida de aplicação de patches. A automação do controle de versões e o foco em vulnerabilidades críticas são pilares desse processo, que busca manter a infraestrutura em conformidade com as melhores práticas e longe de brechas exploráveis.

T1566 (Ataques de Phishing e Engenharia Social)

1**. Implante soluções avançadas de filtragem de e-mail para bloquear tentativas de phishing:** Soluções de filtragem com capacidade analítica avançada são essenciais para revisar e-mails em múltiplos níveis, desde os cabeçalhos ao conteúdo e anexos, sinalizando ou bloqueando mensagens com indícios de fraude. O uso de dados de inteligência atualizados alimenta essas ferramentas, mantendo-as efetivas diante de novas ameaças.

2. Detecção de domínios falsificados aliada à educação corporativa: A estratégia envolve o uso de tecnologias que identificam domínios similares aos legítimos, comuns em tentativas de phishing, além do monitoramento proativo de registros suspeitos. Paralelamente, o engajamento dos usuários é reforçado por treinamentos contínuos e realistas, com simulações práticas e exposição a casos verídicos, fomentando uma cultura interna mais preparada contra esse tipo de golpe.

3. Verificação formal de remetentes por autenticação de e-mails: A implementação dos padrões SPF, DKIM e DMARC cria uma camada robusta de validação para e-mails recebidos. Com regras configuradas para rejeição ou quarentena de mensagens não validadas, e incentivo à adoção desses padrões por parceiros externos, a organização fortalece sua linha de defesa contra falsificações de remetente e fraudes por e-mail.

T1078 (Uso Indevido de Contas Válidas)

1. Monitoramento contínuo com foco em comportamentos fora do padrão: Ferramentas de inteligência comportamental e detecção de anomalias estão em operação para identificar logins feitos em horários não comerciais, tentativas mal-sucedidas em excesso e acessos de localizações atípicas. A

integração com plataformas SIEM garante resposta imediata. Essa abordagem ajuda a identificar contas invadidas antes que possam ser exploradas de forma efetiva.

2. Fortalecimento da autenticação e restrição de privilégios: Todas as contas críticas estão protegidas com autenticação multifator obrigatória. Os acessos seguem o princípio do menor privilégio, com RBAC e concessão temporária via JIT (Just-in-Time) para atividades sensíveis. Contas inativas são revistas de forma contínua, garantindo que não permaneçam ativas além do necessário. A política reduz drasticamente o risco de movimentações não autorizadas com credenciais reais.

3. Governança rigorosa sobre o ciclo de vida das contas: Auditorias frequentes asseguram que apenas contas válidas e ativas estejam em uso. Processos automatizados regem a criação, modificação e encerramento das contas, com base em cargo e vínculo do colaborador. O desligamento de funcionários ativa protocolos que desativam imediatamente os acessos, reduzindo a superfície de ataque associada a credenciais obsoletas.

T1041 (Exfiltração por Canais de C2)

1. Controle rigoroso de fronteira com foco em integridade do tráfego: A rede é protegida por filtros aplicados tanto na entrada quanto na saída, permitindo apenas conexões autorizadas a destinos confiáveis. Protocolos potencialmente exploráveis são bloqueados. As unidades de negócio críticas, especialmente as ligadas a finanças, operam com segmentação dedicada e monitoramento de bloqueios documentado. Há atenção ao impacto operacional, assegurando que os filtros não comprometam o tráfego legítimo.

2. Mapeamento do comportamento-padrão de aplicações financeiras: Sistemas de monitoramento avaliam em tempo real o tamanho, frequência e complexidade das trocas de dados entre clientes e servidores. Qualquer variação estatística fora do esperado aciona alertas. Além disso, perfis históricos alimentam análises comparativas. O processo é ajustado para garantir desempenho mesmo sob cargas elevadas.

3. Vigilância contínua de protocolos com base em metadados: Sessões são analisadas com foco em atributos técnicos, como padrões de tempo e comportamento de protocolo. Ferramentas de análise estatística identificam comunicações suspeitas, apoiadas por limiares adaptáveis com base em uso prévio. O armazenamento de dados e o processamento desses logs são considerados estratégicos, servindo tanto para detecção quanto para análise forense.

T1003.001 (Comprometimento da Memória do LSASS e Exfiltração de Credenciais)

1. Use ferramentas de monitoramento de processos que detectem tentativas específicas de acesso à memória do serviço LSASS e processos relacionados. Para isso, é essencial configurar a coleta detalhada de atributos de execução (incluindo credenciais, caminho da imagem e contexto de segurança). Alertas automáticos devem ser acionados diante de qualquer tentativa não autorizada de inicialização de processos que toquem o LSASS, respeitando listas de ferramentas previamente autorizadas. Essa prática exige consideração sobre a carga de processamento e o volume de armazenamento necessário para os registros contínuos.

2. Implemente mecanismos de isolamento baseados em hardware com tecnologias como IOMMU para impedir o acesso indevido à memória entre processos: Configure políticas rígidas de controle de acesso à memória, evitando que fontes não autorizadas acessem diretamente a memória do LSASS. Utilize soluções de monitoramento para identificar violações nas fronteiras de isolamento, garantindo que processos legítimos de autenticação sigam funcionando normalmente. Avalie os requisitos de hardware e o impacto no desempenho do sistema.

3. Configure respostas automáticas de encerramento para qualquer processo não autorizado que tente acessar a memória do LSASS: Implemente controles de acesso adequados e permissões para garantir que apenas ferramentas legítimas possam encerrar processos. Registre e envie alertas sobre todas as finalizações, com detalhes do processo encerrado e motivo. Considere os riscos de falsos positivos e defina procedimentos claros de escalonamento para as equipes de segurança.

Medidas Recomendadas para Técnicas de Alto Risco:

T1059.001 (Execução via PowerShell)

1. A política de execução do PowerShell deve restringir sua operação a scripts com assinatura digital válida. Configure o PowerShell para aceitar somente scripts validados por assinatura, bloqueando scripts suspeitos ou maliciosos. Restrinja seu uso a administradores para reduzir a superfície de ataque.

2. **Desative ou restrinja o serviço WinRM (Gerenciamento Remoto do Windows) para impedir execuções remotas:** Limite ou desative o acesso ao WinRM para evitar o uso remoto do PowerShell por agentes mal-intencionados. Use regras de firewall para liberar acesso somente a máquinas confiáveis.

3. Use o Modo de Linguagem Restrita do PowerShell e controle de aplicações: Ative o Modo Restrito para limitar funcionalidades sensíveis, como a execução de APIs arbitrárias do Windows. Use ferramentas de lista branca para definir quais scripts e aplicativos podem rodar, reduzindo o risco de exploração.

T1068 (Uso indevido de privilégios para obter acesso elevado)

1. Gestão ativa de vulnerabilidades como medida preventiva: A empresa deve manter um processo contínuo de detecção e correção de falhas em seus ativos tecnológicos. Isso envolve não apenas varreduras automatizadas, mas também auditorias técnicas regulares, permitindo a identificação antecipada de riscos críticos. A aplicação sistemática de atualizações e o uso de ferramentas para padronizar configurações fortalecem o ambiente contra possíveis brechas. Essa rotina contribui diretamente para a conformidade normativa e para a mitigação de riscos operacionais.

2. Redução da exposição por meio de controles mínimos de acesso: Recomenda-se uma revisão criteriosa dos serviços e ferramentas em uso, com a desativação de funcionalidades supérfluas. A adoção de modelos como RBAC e soluções de governança de acesso permite restringir permissões a níveis estritamente necessários. A revisão contínua desses privilégios limita a movimentação não autorizada dentro da rede corporativa e reduz significativamente as possibilidades de elevação indevida de permissões.

3. Fortalecimento do sistema contra tentativas de exploração: A organização deve adotar mecanismos avançados de proteção, como verificação da integridade do kernel e sistemas antifraude voltados à memória e ao comportamento de processos. Ferramentas EDR se tornam fundamentais para identificar ações suspeitas com agilidade. A configuração de alertas e registros permite respostas rápidas a modificações não autorizadas, aumentando a robustez da infraestrutura frente a ameaças sofisticadas.

T1021.001 (Protocolo de Área de Trabalho Remota - RDP)

1. Controle e monitoramento do acesso via RDP: O acesso remoto deve ser limitado a partir de uma arquitetura de rede segmentada e políticas de firewall bem definidas. O uso de conexões RDP precisa ser vinculado a redes privadas virtuais ou a ambientes que sigam o modelo zero trust, sempre com autenticação multifator ativa. As permissões devem ser concedidas exclusivamente a IPs autorizados. Essa estratégia mitiga significativamente os riscos de ataques automatizados e violações de credenciais.

2. Monitoramento inteligente para comportamento fora do padrão: O uso de ferramentas analíticas voltadas para padrões anômalos permite identificar indícios de tentativas maliciosas. Falhas excessivas de login, localizações geográficas inconsistentes e conexões incomuns são indicadores críticos. Com alertas bem configurados, é possível reagir com agilidade, encurtando o tempo de exposição e fortalecendo a postura defensiva da organização frente a ameaças persistentes.

3. Audite e controle ferramentas de acesso remoto: É essencial manter visibilidade total sobre quais softwares de acesso remoto estão em uso. Apenas aplicações oficialmente homologadas devem ser permitidas, e qualquer tentativa de execução de ferramentas não autorizadas deve ser bloqueada por políticas de controle estritas. Auditorias recorrentes ajudam a manter a conformidade e reduzem a superfície de ataque por meio do controle rigoroso das soluções em operação.

T1021.002 (Compartilhamentos Administrativos SMB/ Windows)

1. Controle e monitore o tráfego SMB na rede para detectar acessos não autorizados: Estabeleça segmentações na rede e regras de firewall para limitar o tráfego SMB apenas aos sistemas autorizados. Acompanhe os registros de autenticação SMB e identifique padrões incomuns de acesso, como conexões inesperadas ou muitas tentativas de login com falha. Essa análise ajuda a evitar acessos indevidos e vazamento de dados via SMB.

2. Bloqueie o uso remoto de credenciais administrativas locais: Restrinja logins remotos com contas de administrador local por meio da aplicação de políticas de grupo e da implementação do LAPS (Local Administrator Password Solution). Garanta senhas únicas e complexas para cada sistema. Impedir o reaproveitamento de credenciais reduz o risco de movimentações laterais em caso de comprometimento.

3. Acompanhe tentativas de execução remota via WMI e compartilhamentos SMB: Utilize monitoramento em endpoints para detectar uso da classe Win32_Process do WMI e criação de processos remotos via SMB. Correlacione essas atividades com técnicas conhecidas de ataque para identificar possíveis movimentações laterais ou execuções remotas de código. Detectar comportamentos anômalos antecipadamente é essencial para evitar comprometimentos.

T1574.002 (Carregamento Lateral de DLL)

1. Implemente controles rigorosos de aplicação para bloquear execuções não autorizadas de DLLs: Adote listas de permissões para que apenas aplicativos e bibliotecas confiáveis sejam executados. Verifique a assinatura digital dos arquivos para impedir a execução de DLLs adulteradas ou não assinadas. Essa barreira evita que atacantes explorem falhas nos controles de execução.

2. Mantenha os softwares atualizados para corrigir falhas relacionadas ao carregamento lateral de DLL: Estabeleça um processo eficiente de gestão de patches para mitigar riscos conhecidos. Revise as dependências dos aplicativos e substitua bibliotecas vulneráveis por versões seguras. A atualização contínua dos sistemas reduz a superfície de ataque.

3. Ative mecanismos de detecção comportamental para identificar técnicas de DLL side-loading: Utilize ferramentas EDR para reconhecer comportamentos suspeitos como DLLs sendo carregadas de diretórios não convencionais, injeções inesperadas em processos com privilégios elevados ou padrões de acesso à memória fora do normal. Detecções baseadas em heurística e aprendizado de máquina ajudam a identificar desvios de comportamento no carregamento de DLLs.

T1548.002 (Burlando o Controle de Conta de Usuário)

1. Reforce as configurações do Controle de Conta de Usuário (UAC) e monitore tentativas de contorna-las: Ative o UAC no modo "Sempre Notificar" para exigir aprovação explícita antes de qualquer ação administrativa. Realize avaliações periódicas para identificar máquinas com configurações frágeis e aplique as melhores práticas de segurança. Evitar a autoelevação automática impede que atacantes abusem de utilitários do sistema para contornar o UAC. Configurações fortalecidas reduzem a superfície de ataque e limitam tentativas de escalonamento não autorizado.

2. Monitore a execução de processos em busca de tentativas suspeitas de contornar o UAC: Acompanhe o uso de ferramentas e processos conhecidos por bypassar o UAC, como eventvwr.exe e sdclt.exe, que elevam privilégios sem consentimento. Implemente regras de detecção em endpoints que correlacionem esses eventos com tentativas de escalonamento de privilégio, identificando comportamentos fora do padrão. O uso de análises comportamentais ajuda a detectar técnicas de bypass de forma antecipada.

3. Aplique listas de bloqueio de executáveis para impedir elevação indevida de privilégios: Use políticas de controle de aplicações para bloquear ferramentas administrativas não confiáveis frequentemente exploradas nesse tipo de ataque. Mantenha uma lista atualizada de métodos de bypass conhecidos. A imposição de políticas rigorosas pelo sistema operacional ajuda a impedir que usuários comuns executem binários de alto risco. Restringir a execução de softwares não autorizados fortalece a segurança dos endpoints.

T1133 (Serviços Remotos Externos)

1. Aplique controles automáticos de encerramento de sessão em todos os serviços remotos externos, como VPNs e ferramentas de gerenciamento remoto, com regras rígidas de inatividade: Configure desconexões forçadas após períodos sem uso e registre todos os eventos de encerramento para fins de auditoria. As políticas devem equilibrar necessidades legítimas de negócio e a prevenção de persistência não autorizada por sessões abandonadas. Avalie o impacto na produtividade e ofereça canais de suporte para usuários que necessitem de exceções.

2. Segmente a rede com proxies, gateways e firewalls para controlar e monitorar os caminhos de acesso remoto: Estabeleça uma estratégia de defesa em profundidade que exija que todas as conexões remotas passem por pontos de verificação de segurança. Mantenha registros detalhados de acesso e configure barreiras rígidas que evitem acessos diretos a sistemas internos, garantindo a continuidade operacional por meio de canais seguros. Leve em conta a complexidade da implementação e o impacto sobre o desempenho da rede.

3. Implemente autenticação multifator (MFA) para todas as contas vinculadas a serviços remotos externos, como VPNs e ferramentas de gestão remota: Adote uma solução robusta que combine múltiplos fatores de autenticação, ciente dos riscos de interceptação. Registre detalhadamente todas as tentativas de autenticação e estabeleça processos para lidar com falhas legítimas ou bloqueios. Considere o impacto na experiência do usuário, os recursos de suporte necessários e a existência de métodos alternativos para acessos críticos.

Risco de Persistência Oculta (Evasão e Comprometimento Prolongado):

T1140: (Desofuscar/Decodificar Arquivos ou Informações)

1. Monitore e registre a execução de processos para detectar tentativas de extração ou descriptografia de arquivos: Implante ferramentas de monitoramento para identificar a execução de utilitários ou scripts usados para extrair ou manipular arquivos. Correlacione essa atividade com modificações não autorizadas ou comportamentos inesperados no sistema a fim de detectar ações maliciosas, minimizando falsos positivos.

2. Restrinja e valide a execução de scripts para impedir decodificações não autorizadas: Configure o registro detalhado de execuções de scripts, especialmente aquelas fora do escopo das tarefas administrativas usuais. Bloqueie execuções não autorizadas e analise os scripts capturados em busca de intenções maliciosas. Monitorar essa atividade ajuda a identificar tentativas de automação de desofuscação ou decodificação de payloads.

3. Detecte e bloqueie o uso indevido de utilitários nativos com potencial de desofuscação: Acompanhe o uso de ferramentas internas do sistema que possam ser exploradas para decodificar, extrair ou modificar arquivos. Estabeleça alertas para execuções suspeitas e relacione esses eventos com a atividade do sistema. Identificar o uso indevido desses utilitários logo no início previne acessos indevidos e a execução de códigos maliciosos.

T1070.002: (Limpeza de Logs em Sistemas Linux ou Mac)

1. Criptografe e centralize o armazenamento de logs: Utilize protocolos robustos de criptografia para proteger os registros tanto em trânsito quanto armazenados. Adote soluções de registro centralizado que encaminhem os logs para armazenamento remoto seguro com mecanismos de verificação de integridade, como hash criptográfico. Essa abordagem garante a integridade forense e impede alterações maliciosas.

2. Aplique controles de acesso rigorosos aos logs: Defina permissões granulares para que somente processos autorizados e administradores possam modificar ou apagar registros. Implemente frameworks de controle obrigatório de acesso (MAC) para aplicar políticas de segurança diretamente no sistema operacional. Realize auditorias periódicas nos acessos para prevenir abusos de privilégio.

3. Monitore e gere alertas sobre tentativas de adulteração dos logs: Configure ferramentas de segurança para rastrear alterações, exclusões ou limpezas inesperadas de arquivos de log. Ative alertas em tempo real para notificar as equipes de segurança sempre que houver tentativa de manipulação não autorizada. Correlacione eventos de diferentes fontes para reconhecer padrões maliciosos. O monitoramento contínuo permite mitigar ameaças antes que se agravem.

T1574.00: (Chaves de Execução no Registro/ Pasta de Inicialização)

1. Implemente monitoramento de integridade de arquivos com foco em chaves de execução do Registro do Windows e na pasta de inicialização, com alertas em tempo real ou quase em tempo real para modificações: Utilize comparações com configurações-base para rastrear qualquer alteração nas áreas de inicialização automática, mantendo registros detalhados de auditoria. Configure listas de permissões com entradas legítimas conhecidas e estabeleça processos de controle de mudanças para alterações autorizadas. Avalie o impacto no desempenho e os requisitos de armazenamento gerados pelo monitoramento contínuo e pelos registros de auditoria.

2. Aplique políticas rígidas de lista de permissões de aplicativos para impedir que executáveis não autorizados sejam adicionados às áreas de inicialização ou às chaves de execução: Estabeleça políticas que permitam apenas aplicativos confiáveis ou assinados durante a inicialização, mantendo um inventário completo dos softwares autorizados. Configure alertas automáticos para tentativas de violação dessas políticas, garantindo que atualizações legítimas de software não sejam interrompidas. Considere a carga administrativa envolvida na manutenção dessas listas e o impacto sobre os processos de implantação de software.

3. Implemente monitoramento contínuo das configurações de inicialização do sistema vinculadas ao registro e à pasta de inicialização: Estabeleça capacidades analíticas capazes de detectar alterações incomuns nessas configurações, mantendo um histórico base de inicializações legítimas. Configure respostas automáticas para mudanças não autorizadas.

T1078.003: (Contas Locais – Persistência)

1. Monitore a criação, modificação e o uso de contas locais em todos os sistemas: Alertas em tempo real para atividades suspeitas envolvendo contas locais ajudam a detectar acessos fora do horário normal, elevações de privilégio não autorizadas ou padrões incomuns de uso. Configure o registro detalhado de todas as operações envolvendo contas locais e mantenha um perfil de comportamento normal como referência. Avalie a necessidade de espaço para armazenar esses registros e a capacidade de processar eventos em tempo real.

2. Estabeleça bloqueio automático de contas baseado em comportamentos suspeitos ou violações de políticas: Adote políticas progressivas de bloqueio que aumentam o tempo de restrição conforme ocorrem novas violações, mantendo procedimentos adequados para desbloqueios legítimos. Configure notificações para as equipes de segurança quando houver bloqueios por atividades suspeitas e implemente mecanismos de acesso alternativo para manter serviços críticos operando. Embora essas medidas removam possíveis agentes maliciosos, é necessário avaliar o impacto para usuários legítimos e os protocolos de atendimento em desbloqueios.

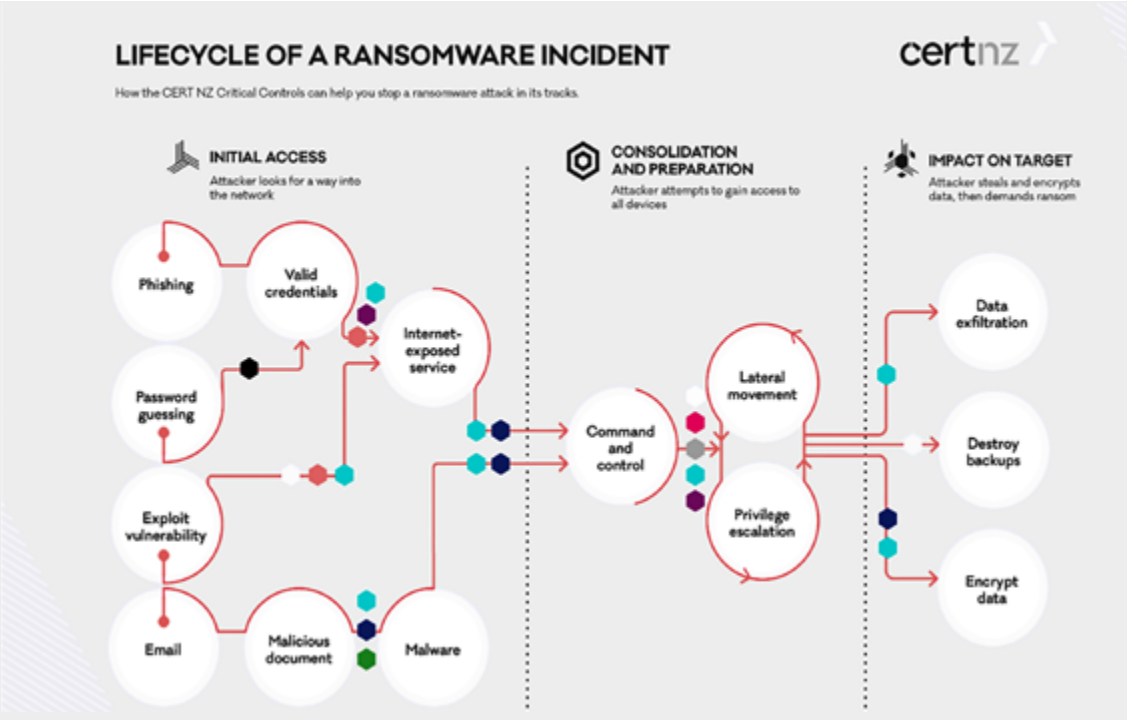
3. Aplique controle rigoroso de permissões e restrições de acesso a todas as contas locais, com base no princípio do menor privilégio (PoLP): Realize revisões periódicas de permissões e implemente detecção automática de mudanças não autorizadas, mantendo a documentação detalhada dos níveis de acesso aprovados. Estabeleça alertas para tentativas de alteração de permissões e mantenha políticas de gestão de mudanças adequadas para atualizações legítimas. Avalie o impacto operacional e o custo administrativo da gestão granular de permissões.

5.2 LockBit

5.2.1 Atividade Operacional Relevante

O grupo de ransomware LockBit permanece como um dos atores mais ativos no cenário global de ameaças, com foco em organizações de médio e grande porte, incluindo casos notórios como Royal Mail, Ion Group e TSMC.[203] Os vetores iniciais de acesso costumam envolver a compra de credenciais em mercados clandestinos, exploração de vulnerabilidades não corrigidas, acesso facilitado por insiders e o uso de exploits ainda desconhecidos (zero-day). O grupo opera com presença confirmada nas principais regiões econômicas: América do Norte, Europa, Ásia e América Latina. Em fevereiro de 2024, as autoridades lançaram uma ação coordenada de grande escala que resultou no congelamento de mais de 200 carteiras de criptomoedas, imposição de sanções, além do desmantelamento de 34 servidores e 14 mil contas relacionadas à operação.[204] Embora essa ofensiva tenha desestabilizado temporariamente suas atividades, o LockBit continua, mesmo assim, sendo a principal organização de ransomware em operação, demonstrando resiliência frente às medidas legais.[205]

Figura 6: Etapas de um Incidente com Ransomware



Fonte: 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

O LockBit adota um modelo de negócios baseado em RaaS (Ransomware-as-a-Service), no qual afiliados são recrutados para executar os ataques utilizando o ecossistema técnico fornecido pelo grupo.[207] Isso gera ampla variação nas técnicas e ferramentas utilizadas nos ataques, tornando a detecção mais desafiadora. Uma prática recorrente entre os afiliados é a entrada inicial via falhas de segurança não corrigidas ou uso de credenciais comprometidas. Uma vez dentro do ambiente corporativo, ferramentas como o Mimikatz são frequentemente utilizadas para coleta de credenciais e escalonamento de privilégios, o que viabiliza a movimentação lateral e o posterior comprometimento dos dados, seja por meio de extração ou criptografia.

Os impactos financeiros atribuídos ao LockBit têm sido especialmente críticos no setor bancário e de serviços financeiros da América Latina. A atuação de grupos como o LockBit tem gerado perdas significativas e interrupções operacionais em serviços públicos e empresas privadas.[208] Desde abril de 2022, nações como Costa Rica, Peru, México, Equador, Brasil e Argentina têm registrado ataques com características atribuídas a agentes russófonos, reforçando a atuação contínua do LockBit sobre alvos estratégicos na região.[209]

5.2.2 Contexto Operacional

O LockBit, ativo desde setembro de 2019, passou por diversas iterações até alcançar sua versão mais recente, a 3.0, descoberta em junho de 2022. Durante o ano de 2022, a operação manteve a liderança no cenário global de ransomware, concentrando mais de um terço das vítimas identificadas nos três primeiros trimestres.[210] Sua atuação é especialmente significativa na América Latina. Em outubro de 2022, um ataque a uma instituição financeira brasileira resultou em uma exigência de 50 bitcoins (cerca de 1 milhão de dólares), provocando vazamento de dados sensíveis e interrupção temporária no atendimento aos clientes.

A ação do LockBit não se limita ao setor financeiro. Seus alvos abrangem desde indústrias privadas até setores considerados críticos, como energia, saúde e transporte, além de órgãos governamentais.[211] Outros setores de infraestrutura crítica também foram impactados, como energia, saúde e transporte.[212] Entidades governamentais também foram afetadas, gerando crises nacionais, como no caso da Costa Rica.[213] Essas indústrias são particularmente visadas devido à sua importância estratégica, à sensibilidade das informações e ao potencial de gerar crises nacionais. Além disso, a capacidade financeira desses setores aumenta a probabilidade de pagamento do resgate.

5.2.3 Estratégias de Extorsão e Modus Operandi

A metodologia de dupla extorsão adotada pelo LockBit é amplamente consolidada: além de criptografar os dados e exigir resgate para liberação, o grupo ameaça publicar os dados exfiltrados, mesmo em casos onde as vítimas conseguem restaurar os sistemas internamente. Essa abordagem amplia a pressão e aumenta a taxa de sucesso nas negociações.

O LockBit compartilha com o CL0P o modelo de operação como serviço (RaaS), utilizando afiliados e intermediários especializados (Initial Access Brokers) para viabilizar a infecção inicial ou abrir caminho para a entrada em redes corporativas. Ambas as operações são conhecidas por explorar falhas de segurança em grande escala, como a vulnerabilidade no MOVEit. Além disso, técnicas como o carregamento lateral de DLLs e a implementação de mecanismos avançados de persistência são utilizadas para prolongar o controle dos sistemas comprometidos.

5.2.4 Táticas e Ferramentas de Comprometimento

A estrutura de ataque do LockBit é altamente técnica e diversificada. Entre os métodos de escalonamento de privilégios, destaca-se o bypass de UAC por meio do ucmDccwCOM (UACMe), bem como a modificação de políticas de domínio via GPO e o uso de execuções automáticas em processos de inicialização. Técnicas de falsificação de token são empregadas para assumir privilégios de outros processos, ampliando o alcance interno.

Também utiliza falsificação de tokens para replicar e assumir os privilégios de outros processos, facilitando a infiltração mais profunda na rede. O grupo explora vulnerabilidades tanto zero-day quanto n-day para acesso não autorizado e execução remota de código, com casos notórios como a falha no Fortra GoAnywhere MFT (CVE-2023-0669) e a vulnerabilidade no Apache Log4j2.

Ferramentas como Splashtop são usadas para acesso remoto, e o Cobalt Strike é utilizado para movimentação lateral dentro das redes. Alvos como compartilhamentos

[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

SMB, Admin Shares e políticas de grupo de domínio são explorados para garantir movimentação fluida nos ambientes comprometidos.

No que se refere ao controle da operação, o LockBit adota um leque de soluções: FileZilla para transferência de arquivos, ThunderShell para acesso remoto via HTTP, Ligolo para criação de túneis SOCKS5 e Plink para automação via SSH. Softwares legítimos como AnyDesk e TeamViewer também são utilizados para manter acesso persistente. A variedade e profundidade dessas táticas reforçam o alto grau de sofisticação operacional do LockBit e sua ameaça contínua a setores estratégicos, especialmente no contexto latino-americano.[214]

Táticas	Técnicas	Procedimentos
Execução (TA0002)	T1059.003: Windows Command Shell	Abusa do prompt de comando do Windows para acessar praticamente qualquer parte do sistema
	T1072: Ferramentas de Desenvolvimento de Software	Explora serviços do sistema para executar ou iniciar código malicioso como forma de persistência
	T1569.002: Serviços do Sistema	Utiliza PsExec para executar comandos ou cargas maliciosas
Persistência (TA0003)	T1547: Execução Automática no Boot/Login	Habilita logon automático para manter persistência
	T1078: Contas Válidas	Utiliza contas de usuários comprometidas para manter o acesso contínuo na rede
Acesso Inicial (TA0001)	T1189: Comprometimento via Navegação (Drive-By)	Afiliados do LockBit obtêm acesso quando o usuário visita um site comprometido
	T1190: Exploração de Aplicações com Acesso Externo	Explora vulnerabilidades (como o Log4Shell) em sistemas expostos à internet
	T1133: Serviços Remotos Externos	Explora RDP para obter acesso às redes das vítimas
	T1566: Phishing	Utiliza phishing e spear-phishing para invadir as redes
Escalonamento de Privilégio(TA0004)	T1548: Abuso de Mecanismo de Elevação de Privilégio	Emprega técnicas de bypass do UAC (ex: método ucmDccwCOM)
	T1547: Execução Automática no Boot/Login	Habilita logon automático como forma de escalonamento
	T1484.001: Modificação de Políticas de Domínio via GPO	Altera políticas de grupo para facilitar movimentação lateral
	T1078: Contas Válidas	Usa contas comprometidas para ganhar privilégios elevados
Evasão de Defesa (TA0005)	T1480.001: Barreiras de Execução – Chave Ambiental	Descriptografa ou prossegue com a execução apenas se certas condições ambientais forem atendidas
	T1562.001: Prejudicar Defesas – Desabilitar ou Modificar Ferramentas	Desativa ferramentas EDR (ex: Backstab, Process Hacker)
	T1070.001: Remoção de Indicadores – Limpar Logs do Windows	Apaga arquivos de log de eventos para evitar detecção

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

	T1070.004: Remoção de Indicadores – Exclusão de Arquivos	O LockBit 3.0 se apaga do disco após a execução
	T1027: Arquivos ou Informações Ofuscadas	Criptografa ou ofusca informações do host e do bot durante a comunicação com servidores C2
	T1027.002: Arquivos ou Informações Ofuscadas – Compactação de Software	Utiliza compactação de software ou proteção por máquina virtual para ocultar o código malicioso
Acesso a Credenciais (TA0006)	T1110: Força Bruta	Realiza ataques de força bruta para descobrir credenciais de VPN ou RDP
	T1555.003: Credenciais Armazenadas em Navegadores	Recupera credenciais salvas no Firefox com a ferramenta PasswordFox
	T1003: Coleta de Credenciais do Sistema Operacional	Usa ferramentas como ExtPassword ou LostMyPassword para extrair credenciais do sistema
	T1003.001: Coleta de Credenciais do Sistema Operacional: Dumping de LSASS	Utiliza o ProDump da Sysinternals ou o Mimikatz para extrair credenciais diretamente da memória LSASS
Reconhecimento (TA0007)	T1046: Descoberta de Serviços na Rede	Usa ferramentas como SoftPerfect Network Scanner, Advanced IP Scanner ou Port Scanner para mapear a rede da vítima
	T1082: Descoberta de Informações do Sistema	Coleta informações do sistema como nome do host, configurações e domínio
	T1614.001: Descoberta de Localização – Idioma do Sistema	O LockBit 3.0 evita infectar sistemas com determinados idiomas com base em uma lista de exclusão
Movimentação Lateral (TA0008)	T1021.001: Serviços Remotos – RDP.	Uses Splashtop or similar remote desktop software to facilitate lateral movement
	T1021.002: Serviços Remotos – SMB/Admin Shares do Windows	Utiliza o Cobalt Strike para explorar compartilhamentos SMB e se movimentar entre sistemas
Coleta (TA0009)	T1560.001: Arquivamento de Dados Coletados – Via Utilitário	Usa o 7-Zip para comprimir ou criptografar dados antes da exfiltração
Comando e Controle (TA0011)	T1071.002: Protocolo de Camada de Aplicação – FTP	Usa o FileZilla para se comunicar com os servidores de C2
	T1071.001: Protocolo de Camada de Aplicação – Web	Utiliza o ThunderShell para enviar comandos via requisições HTTP
	T1095: Protocolo Fora da Camada de Aplicação	Usa Ligolo para estabelecer túneis SOCKS5 ou TCP por conexões reversas
	T1572: Tunelamento de Protocolo	Emprega o Plink (PuTTY Link) para automatizar sessões SSH em ambientes Windows
	T1219: Software de Acesso Remoto	Utiliza AnyDesk, Atera RMM, ScreenConnect ou TeamViewer para manter acesso remoto

Exfiltração (TA0010)	T1567: Software de Acesso Remoto	Usa serviços de compartilhamento público de arquivos para exfiltrar os dados
	T1567.002: Exfiltração por Serviço Web: Exfiltração por Armazenamento em Nuvem	Utiliza ferramentas como Rclone ou FreeFileSync para enviar dados à nuvem (ex: MEGA)
Impacto (TA0040)	T1485: Destruição de Dados	Apaga arquivos de log e esvazia a lixeira para evitar recuperação de informações
	T1486: Criptografia de Dados	Criptografa os dados dos sistemas-alvo para interromper a disponibilidade dos serviços
	T1491.001: Desfiguração Interna	Altera o papel de parede e ícones do sistema com a identidade visual do LockBit
	T1490: Inibição da Recuperação do Sistema	Apaga as cópias de sombra do volume (shadow copies) para impedir a restauração do sistema
	T1489: Interrupção de Serviços	Finaliza processos e serviços críticos para facilitar a criptografia e impedir recuperação

Indicadores de Comprometimento (IOCs):

- Hashes de arquivos
- Endereços IP
- Nomes de domínio
- URLs maliciosas
- Notas de resgate

Vulnerabilidades Exploradas (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 Recomendações Técnicas e Táticas Contra o LockBit

Recomendações Estratégicas para Mitigar Riscos Técnicos de Alto Impacto

As medidas táticas abaixo visam mitigar técnicas amplamente utilizadas em ataques atribuídos ao LockBit. Elas se baseiam nas diretrizes do MITRE ATT&CK e são voltadas a empresas que buscam resiliência frente a ataques sofisticados, especialmente em ambientes com infraestrutura crítica ou dados sensíveis.

T1133 (Acessos Remotos Indevidos)

1. Aplicação de MFA em todo acesso remoto: Exija MFA para qualquer acesso remoto, mesmo quando houver integração com serviços em nuvem. Utilize métodos resistentes a phishing, como FIDO2 ou autenticação baseada em certificados. A MFA reduz significativamente o risco de acessos não autorizados, mesmo em caso de vazamento de credenciais.

2. Restrinja o acesso remoto por meio de segmentação de rede e listas de permissões: Limite acessos remotos apenas a faixas de IP autorizadas e aplique segmentação de rede para isolar serviços remotos dos sistemas financeiros críticos. Adote princípios de Zero Trust e RBAC (controle de acesso baseado em função) para reduzir a exposição. Essas medidas limitam a superfície de ataque e dificultam movimentações laterais.

3. Monitore e registre sessões de acesso remoto em busca de anomalias: Utilize soluções de SIEM para registrar e analisar as sessões remotas. Habilite mecanismos de detecção comportamental para identificar logins em horários fora do expediente, locais não usuais ou picos de atividade. O monitoramento em tempo real permite resposta imediata a acessos não autorizados.

T1078 (Contas Válidas)

1. Aplique o princípio do menor privilégio e segregue contas: Defina permissões com base no mínimo necessário (PoLP). Separe contas administrativas de contas de uso comum. Utilize acesso just-in-time (JIT) e RBAC para limitar acessos elevados contínuos. Essas práticas reduzem significativamente o risco de uso indevido de credenciais.

2. Reforce a autenticação e a segurança das credenciais: Exija MFA em todas as contas privilegiadas, preferencialmente com métodos resistentes a phishing. Implemente políticas rígidas de senhas (complexidade, tamanho) e incentive o uso de gerenciadores de senhas. Faça rodízio periódico de credenciais e desative contas inativas para mitigar riscos de acesso indevido.

3. Detecte e responda a usos não autorizados de contas: Monitore continuamente o comportamento das contas por meio de SIEM e ferramentas de análise comportamental (UEBA). Identifique comportamentos fora do padrão, como acessos a partir de locais desconhecidos, tentativas excessivas de login ou elevações de privilégio. Ative alertas automatizados e defina respostas em tempo real para contenção de incidentes.

T1566 (Phishing)

1. Implemente mecanismos avançados de segurança e filtragem de e-mails: Adote gateways de e-mail seguros (SEGs) e soluções robustas de proteção contra phishing para bloquear mensagens maliciosas antes que cheguem aos usuários. Ative protocolos de autenticação de e-mails baseados em domínio, como SPF, DKIM e DMARC, a fim de impedir falsificação de remetentes. Utilize sistemas de detecção baseados em IA para identificar e isolar tentativas de phishing em tempo real.

2. Realize treinamentos contínuos de conscientização e testes simulados de phishing: Capacite os colaboradores para identificar tentativas de phishing, reconhecendo técnicas de engenharia social, anexos maliciosos e links enganosos. Faça simulações regulares de ataques para medir o nível de preparo dos usuários e oferecer treinamentos direcionados com base nos resultados. Estimule uma cultura organizacional de atenção constante à segurança cibernética para reduzir o sucesso dessas ameaças.

3. Implemente proteções de navegação contra phishing e análise de URLs: Utilize filtros de navegação e serviços de reputação de domínios para bloquear sites de phishing já conhecidos. Aplique isolamento de navegador para usuários de alto risco e faça escaneamento automático de URLs em e-mails antes de liberar o acesso. Incentive o uso de gerenciadores de senhas para evitar roubo de credenciais, já que eles preenchem dados apenas em sites legítimos.

T1003 (Extração de Credenciais do Sistema Operacional)

1. Aplique mecanismos de proteção de credenciais para impedir acessos não autorizados: Configure o Windows Defender Credential Guard para proteger a memória do LSASS e bloquear ataques de extração de credenciais. Use soluções EDR para identificar acessos suspeitos a repositórios de credenciais. Remova privilégios administrativos desnecessários para reduzir a exposição. Essas medidas evitam que atacantes consigam extrair informações sensíveis.

2. Restrinja o acesso a processos sensíveis do sistema e habilite auditorias: Configure soluções de segurança de endpoint para monitorar e bloquear acessos indevidos ao LSASS e hives de registro que armazenam credenciais. Implemente auditoria de processos para registrar e alertar sobre tentativas de acesso a dados sensíveis. Revise regularmente os logs e conduza análises forenses em eventos suspeitos. O monitoramento de processos ajuda a identificar e evitar ataques de extração.

3. Use criptografia forte e minimize o armazenamento de credenciais: Adote padrões avançados de criptografia para guardar credenciais e siga as melhores práticas para gerenciamento de segredos. Aplique escalonamento de privilégios sob demanda (JIT) para limitar o acesso contínuo a contas críticas. Reduza o cache de senhas nos endpoints para diminuir a exposição. O fortalecimento da segurança no armazenamento de credenciais reduz a eficácia de ataques desse tipo.

T1486 (Ransomware – Criptografia de Dados com Fins de Impacto)

1. Implemente proteção avançada nos endpoints e detecção comportamental de ransomware: Utilize soluções de antivírus de nova geração (NGAV) e ferramentas EDR para identificar comportamentos típicos de ransomware, como criptografia em massa de arquivos, exclusão de backups e alterações não autorizadas no registro do sistema. Configure a contenção automática de dispositivos infectados para impedir a disseminação do ataque. A identificação precoce de atividades de criptografia reduz significativamente os danos.

2. Aplique políticas rigorosas de backup com armazenamento imutável e recuperação offline: Adote a estratégia de backup 3-2-1, mantendo cópias offline e imutáveis separadas do ambiente de produção. Realize testes frequentes dos procedimentos de restauração para garantir respostas rápidas em caso de ataque. Use criptografia e controles de acesso nos backups para evitar modificações não autorizadas. Backups seguros são essenciais para retomada após infecção por ransomware.

3. Implemente segmentação de rede e lista de permissões de aplicativos para conter a propagação: Separe as infraestruturas críticas das áreas de TI comuns com regras rigorosas de acesso e políticas de firewall. Utilize listas de permissões de aplicativos para bloquear a execução de softwares não autorizados, incluindo cargas de ransomware. Monitore alterações no sistema de arquivos e limite gravações em diretórios sensíveis. A segmentação limita o alcance de um ataque e reduz a superfície de exposição.

T1567.002 (Exfiltração via Serviços Web: Vazamento para Armazenamento em Nuvem)

1. Use soluções de prevenção contra perda de dados (DLP) para controlar transferências indevidas: Implemente sistemas DLP para monitorar, registrar e bloquear envios não autorizados de dados a serviços de armazenamento em nuvem como Google Drive, Dropbox e OneDrive. Estabeleça regras que identifiquem movimentações suspeitas e forcem a criptografia automática de dados financeiros sensíveis antes do envio. Essas soluções são fundamentais para proteger informações bancárias.

2. Restrinja o acesso a serviços de nuvem a partir da rede da instituição financeira: Utilize firewalls e proxies para impedir conexões com plataformas de nuvem não autorizadas. Adote soluções SASE para aplicar filtros de conteúdo e identificar uploads anômalos. Configure alertas para volumes altos de transferência ou acessos incomuns, que possam indicar tentativas de exfiltração. Limitar o acesso reduz as chances de vazamento de dados.

3. Criptografe dados financeiros sensíveis em repouso e em trânsito para evitar exposição: Utilize padrões robustos de criptografia (como AES-256 e TLS 1.2+) tanto para o armazenamento quanto para a transmissão de dados financeiros. Aplique controle de acesso rígido e autenticação multifator (MFA) para acesso à nuvem. Implemente registros e monitoramento contínuo das interações com o armazenamento em nuvem para identificar comportamentos suspeitos. A criptografia protege os dados mesmo em caso de vazamento.

Recomendações Estratégicas Frente a Técnicas Avançadas com Potencial de Comprometimento Crítico

T1547 (Execução Automática na Inicialização ou Logon)

1. Controle rigoroso de aplicações e bloqueio de mecanismos de persistência não autorizados: Implemente listas de permissões com ferramentas como o Windows Defender Application Control (WDAC) ou AppLocker, impedindo a execução de softwares maliciosos na inicialização do sistema. Restrinja privilégios administrativos para bloquear alterações não autorizadas no registro, criação de tarefas agendadas ou instalação de serviços. Exija verificação de assinatura digital para garantir que apenas aplicativos confiáveis permaneçam ativos. Essas medidas reduzem a possibilidade de persistência por meio da inicialização do sistema.

2. Monitore e audite as configurações de inicialização do sistema: Utilize soluções EDR para acompanhar alterações em locais de inicialização como o registro do Windows, tarefas agendadas e serviços. Configure alertas no SIEM para mudanças não autorizadas em entradas de execução automática. Realize auditorias frequentes nas configurações de inicialização e remova quaisquer mecanismos suspeitos de persistência. O monitoramento contínuo permite detectar e reagir antes que alterações sejam exploradas por atacantes.

3. Fortaleça a integridade do sistema e habilite inicialização segura: Ative o Secure Boot para impedir alterações não autorizadas no processo de boot e garantir o carregamento apenas de componentes confiáveis do sistema operacional. Aplique proteção contra adulteração em configurações críticas para impedir modificações nas entradas de autostart. Use sistemas de prevenção de intrusão baseados no host (HIPS) para bloquear tentativas suspeitas de persistência. O reforço dessas etapas reduz os riscos de malware em terminais bancários e caixas eletrônicos.

T1484.001 (Modificação de Política de Domínio: Modificação de GPO)

1. Controle de acesso baseado em funções (RBAC) para limitar alterações em políticas de domínio: Permita que apenas um grupo restrito de administradores possa modificar as GPOs. Use soluções de gerenciamento de acesso privilegiado (PAM) com controle de acesso sob demanda (JIT) para evitar mudanças não autorizadas. Revise periodicamente os privilégios administrativos e elimine acessos desnecessários. Isso reduz a capacidade do atacante de manipular políticas de segurança para movimentação lateral.

2. Monitoramento contínuo e registro de alterações em políticas de grupo: Implemente soluções SIEM para registrar e gerar alertas sobre modificações nas GPOs. Use ferramentas como Microsoft ATA ou Azure Sentinel para detectar alterações suspeitas que possam indicar atividade maliciosa. Faça revisões periódicas dos logs dos controladores de domínio para identificar intervenções não autorizadas. O acompanhamento dessas alterações permite resposta rápida a movimentações hostis.

3. Aplique configurações base de segurança e mantenha backups das GPOs: Implemente uma configuração segura baseada em benchmarks CIS ou diretrizes da Microsoft. Realize backups regulares dos objetos de política de grupo (GPOs) e habilite recursos de reversão para restaurar o ambiente em caso de comprometimento. Adote controle de versão e logs de auditoria para rastrear mudanças e desfazer alterações indevidas. A manutenção de baselines e backups sólidos assegura recuperação eficiente diante de ataques.

T1562.001 (Enfraquecer Defesas: Desativar ou Modificar Ferramentas)

1. Implemente proteção de endpoint com controles de segurança à prova de violação: Utilize soluções EDR com proteção contra adulterações para impedir que invasores desativem ferramentas de segurança. Limite o acesso administrativo aos softwares de segurança e aplique controle de acesso baseado em função (RBAC) para restringir permissões de modificação. Defina as configurações de segurança via políticas de grupo para evitar alterações não autorizadas. Essas medidas impedem que os atacantes desativem defesas durante incidentes.

2. Monitore e registre alterações em ferramentas de segurança: Configure o SIEM para registrar e gerar alertas sempre que ferramentas de segurança forem modificadas, como desativação de antivírus, desligamento de logs ou alteração em regras de firewall. Implante sistemas de prevenção de intrusão baseados no host (HIPS) para detectar e bloquear tentativas de modificação não autorizada nas configurações. O monitoramento constante permite identificar rapidamente tentativas de neutralizar mecanismos de defesa.

3. Restringe a execução de scripts e ferramentas administrativas usadas para desativar defesas: Ative o registro de blocos de script no PowerShell e imponha políticas de execução que evitem alterações indevidas em configurações de segurança. Restrinja o uso de ferramentas como Process Hacker, GMER e PsExec, frequentemente exploradas por atacantes para desabilitar proteções. Use listas de permissões para bloquear a execução de ferramentas que não sejam autorizadas. Tais ações preservam a integridade dos mecanismos de segurança.

T1046 (Descoberta de Serviços de Rede)

1. Reduza a exposição de serviços de rede por meio de firewalls e controles de acesso: Restrinja o tráfego de entrada e saída apenas aos serviços essenciais com regras rígidas de firewall. Desative serviços e protocolos desnecessários na infraestrutura bancária crítica. Implemente segmentação de rede para isolar sistemas sensíveis do restante do ambiente de TI. Reduzir a exposição dos serviços dificulta a exploração por parte de invasores.

2. Use monitoramento de rede e detecção de anomalias para identificar varreduras não autorizadas: Implemente sistemas de detecção de intrusos (IDS) e ferramentas de análise de tráfego (NTA) para identificar atividades de escaneamento anormais. Configure alertas no SIEM para tentativas excessivas de conexão ou consultas fora do padrão. Use tecnologias de engano, como honeypots, para identificar e rastrear tentativas de mapeamento da rede. O monitoramento contínuo viabiliza a detecção precoce de movimentações adversárias.

3. Fortaleça os protocolos de rede e exija autenticação robusta: Desative protocolos legados como SMBv1 e exija criptografia TLS em todas as comunicações. Implemente autenticação mútua para serviços sensíveis, evitando acessos não autorizados. Para serviços administrativos remotos, utilize autenticação baseada em certificados. O reforço dos protocolos de segurança dificulta a descoberta de serviços por parte de agentes maliciosos.

T1082 (Descoberta de Informações do Sistema)

1. Restringir o acesso a informações de sistema e hardware: Configure políticas de grupo para impedir que usuários sem privilégios administrativos acessem comandos como systeminfo, wmic e tasklist. Desative o acesso remoto a ferramentas de enumeração de sistema nos endpoints bancários. Isso dificulta que agentes maliciosos coletem dados detalhados sobre a infraestrutura da instituição.

2. Monitore endpoints para identificar atividades suspeitas de reconhecimento: Utilize soluções EDR para acompanhar e alertar sobre comandos de enumeração executados por usuários não autorizados. Configure regras no SIEM para registrar e sinalizar tentativas de acesso a informações do sistema. A detecção precoce dessas ações evita possíveis explorações posteriores.

3. Aplique controles de acesso rigorosos às ferramentas de gerenciamento de sistema: Restrinja o uso de utilitários como PowerShell, WMI e Agendador de Tarefas apenas a administradores autorizados. Adote escalonamento de privilégios sob demanda (JIT) para conceder acesso temporário apenas quando necessário. Audite regularmente os logs de acesso e investigue consultas incomuns em bancos de dados de sistema. Isso limita a capacidade dos invasores de mapear a infraestrutura bancária.

T1021.001 (Serviços Remotos: Protocolo de Área de Trabalho Remota – RDP)

1. Restringir o acesso RDP com autenticação forte e segmentação de rede: Implemente autenticação multifator (MFA) para todas as conexões RDP. Use firewalls para liberar acesso apenas a endereços IP autorizados. Utilize infraestrutura de desktop virtual (VDI) com autenticação intermediada para reduzir a exposição direta dos serviços RDP. Controles de acesso rígidos reduzem tentativas de acesso remoto não autorizado.

2. Monitore e registre atividades de sessão RDP para detectar acessos indevidos: Ative o registro detalhado das sessões RDP, incluindo tentativas de conexão bem-sucedidas e falhas. Configure o SIEM para gerar alertas em casos de uso anômalo, como logins a partir de locais incomuns ou repetidas falhas de autenticação. Aplique análise comportamental para identificar sessões comprometidas. O monitoramento contínuo permite uma resposta rápida a acessos indevidos.

3. HaReforce as configurações do RDP e implemente controles de segurança por sessão: Configure o RDP para usar autenticação em nível de rede (NLA), evitando conexões antes da autenticação. Exija criptografia TLS para todo o tráfego RDP. Limite o uso do RDP a janelas de manutenção predefinidas, com base em horários. Revise regularmente os logs de sessão para identificar comportamentos suspeitos. O reforço dessas configurações reduz os riscos de acesso indevido e movimentações laterais.

Técnicas de Baixo Perfil Usadas para Movimentação Lateral e Evasão: Controles Recomendados

T1059.003 (Windows Command Shell – Execução de scripts para automatizar ações maliciosas em sistemas financeiros)

1. Restringir a execução de scripts e comandos não autorizados via linha de comando: Implemente listas de permissões com o Windows Defender Application Control (WDAC) ou AppLocker para bloquear a execução não autorizada de cmd.exe e scripts .bat. Ative o bloqueio de scripts no PowerShell e aplique políticas de execução para impedir códigos maliciosos. Limite o acesso a interpretadores de linha de comando para usuários não administrativos. Isso impede que agentes maliciosos automatizem ações dentro dos sistemas financeiros.

2. Monitore e registre atividades suspeitas de linha de comando: Utilize soluções EDR para acompanhar o uso do terminal e identificar scripts que tentem modificar configurações do sistema. Configure alertas no SIEM para comandos suspeitos como net user, taskkill ou reg add. O monitoramento proativo permite que a equipe de segurança detecte e impeça execuções não autorizadas.

3. Aplique controles rigorosos sobre comandos administrativos: Implemente escalonamento de privilégios sob demanda (JIT) para limitar o acesso a interfaces administrativas como cmd.exe ou PowerShell. Exija autenticação multifator (MFA) para sessões privilegiadas. Registre todas as atividades de shell com fins forenses. Essas práticas dificultam a execução de scripts maliciosos com persistência em sistemas bancários.

T1072 (Ferramentas de Desenvolvimento de Software – Utilizadas para compilar e executar código malicioso em ambientes bancários)

1. Restringir a instalação e execução de ferramentas de desenvolvimento não autorizadas: Utilize listas de permissões para impedir a execução de compiladores, ambientes de script e frameworks que não tenham sido aprovados. Restringe permissões de instalação de ferramentas como Visual Studio, GCC e Python apenas a usuários autorizados. Impedir o uso dessas ferramentas reduz o risco de compilação e execução de código malicioso.

2. Monitore o uso de ferramentas de desenvolvimento em busca de anomalias: Implemente monitoramento em endpoints para rastrear a execução de ferramentas de desenvolvimento e detectar usos indevidos. Configure alertas no SIEM para identificar compilações ou execuções fora de ambientes controlados. A vigilância contínua permite a detecção rápida do uso indevido desses recursos por agentes maliciosos.

3. Aplique políticas rígidas de execução de código em sistemas financeiros: Exija verificação de assinatura digital antes de permitir a execução de scripts e binários. Utilize sandboxing para códigos não verificados, evitando que interajam diretamente com sistemas em produção. Analise o comportamento de arquivos compilados com EDR antes de permitir sua execução. Essas medidas reduzem significativamente o risco de implantação de código malicioso em redes bancárias.

T1110 (Força Bruta – Tentativas de quebrar credenciais bancárias para acesso não autorizado)

1. Aplique políticas rigorosas de senhas e mecanismos de bloqueio de contas: Exija senhas complexas com no mínimo 12 a 15 caracteres e implemente a expiração periódica obrigatória. Ative políticas de bloqueio de conta após múltiplas tentativas de login fracassadas, para inibir ataques de força bruta. Use listas de senhas proibidas para evitar o uso de senhas fracas ou previsíveis. Políticas robustas de autenticação reduzem significativamente a eficácia desse tipo de ataque.

2. Implante detecção de anomalias em tentativas de login e autenticação multifator (MFA): Aplique análise comportamental para identificar atividades anormais de login, como repetidas tentativas fracassadas vindas de um mesmo IP. Implemente MFA em todas as contas privilegiadas e acessos remotos para bloquear acessos indevidos mesmo quando credenciais são comprometidas. A combinação de detecção e MFA cria múltiplas camadas de defesa contra ataques por força bruta.

3. Restrinja o acesso externo aos portais de autenticação e aplique regras de geolocalização: Limite o acesso aos sistemas de login com listas de IPs permitidos e bloqueios geográficos para impedir tentativas de login de regiões de alto risco. Utilize ferramentas de detecção de ameaças relacionadas à identidade para identificar tentativas automatizadas de força bruta. Controlar o acesso aos portais de autenticação reduz a exposição a ataques baseados em quebra de senhas.

T1572 (Túnel de Protocolo – Ocultação de tráfego malicioso para burlar controles de segurança)

1. Implemente inspeção profunda de pacotes (DPI) para detectar e bloquear túneis: Adote sistemas de detecção e prevenção de intrusão (IDS/IPS) com capacidade de DPI para analisar tráfego criptografado em busca de assinaturas de tunelamento. Utilize feeds de inteligência de ameaças para manter atualizadas as regras de detecção. A DPI garante a identificação e bloqueio de tentativas de túnel antes que alcancem sistemas críticos.

2. Restrinja conexões de saída apenas a protocolos e serviços autorizados: Configure firewalls para bloquear conexões de saída por protocolos comumente usados em túneis, como ICMP, DNS e HTTP em portas não padrão. Aplique políticas rigorosas de filtragem de saída para limitar as comunicações externas a domínios e IPs previamente aprovados. A limitação de tráfego não autorizado reduz a eficácia das técnicas de tunelamento.

3. Monitore o tráfego de rede em busca de padrões que indiquem tunelamento: Utilize ferramentas de análise de tráfego (NTA) para detectar transferências de dados incomuns, como cargas criptografadas em portas não esperadas. Configure alertas no SIEM para comportamentos suspeitos associados a túneis. O monitoramento contínuo permite que as equipes de segurança identifiquem e respondam rapidamente a tentativas de burlar os controles da rede.

T1071.002 (Protocolo de Camada de Aplicação: Protocolos de Transferência de Arquivos – Usados para preparar e transferir dados financeiros roubados)

1. Restrinja o uso não autorizado de protocolos de transferência de arquivos: Bloqueie transferências via FTP, SFTP e HTTP não autorizadas utilizando firewalls de rede e proxies web. Limite o envio de arquivos para repositórios internos ou nuvens previamente aprovadas. Para fins de auditoria, exija autenticação em todas as transferências e registre a atividade. Controlar o uso desses protocolos impede a exfiltração de dados financeiros por invasores.

2. Monitore e registre atividades de transferência de arquivos em busca de comportamentos suspeitos: Implemente ferramentas de monitoramento de segurança para acompanhar transferências inesperadas ou volumosas a partir de sistemas financeiros. Configure alertas no SIEM para uploads em grande escala a servidores externos ou padrões de envio fora do esperado. A auditoria frequente dos logs de transferência ajuda a identificar tentativas de vazamento de dados antes que causem prejuízos.

3. Criptografe dados financeiros sensíveis em repouso e em trânsito para evitar acessos indevidos: Aplique criptografia ponta a ponta em todas as transferências, utilizando protocolos seguros como SFTP, TLS e IPsec. Use soluções de prevenção contra perda de dados (DLP) para detectar e bloquear automaticamente o envio de informações bancárias sensíveis para destinos não autorizados. A combinação de criptografia e DLP mantém os dados protegidos, mesmo em caso de exfiltração.

T1219 (Software de Acesso Remoto – Permite que invasores mantenham controle persistente sobre sistemas bancários comprometidos)

1. Bloqueie ferramentas de acesso remoto não autorizadas e restrinja o uso de desktop remoto: Utilize listas de permissões para impedir a execução de ferramentas como TeamViewer, AnyDesk e VNC. Desative o acesso remoto (RDP) em sistemas financeiros críticos, a menos que seja estritamente necessário. Restrinja o acesso remoto a conexões via VPN com autenticação multifator (MFA). O bloqueio dessas ferramentas reduz a superfície de ataque para controle persistente.

2. Monitore e registre continuamente as sessões de acesso remoto: Implemente soluções de monitoramento em endpoints para acompanhar sessões remotas e identificar comportamentos de login incomuns. Utilize análise comportamental para detectar anomalias como sessões oriundas de localizações atípicas ou fora do horário comercial. O registro e a análise dessas atividades ajudam a detectar presença persistente de adversários.

3. Aplique segmentação de rede e limite privilégios de acesso remoto: Isole os serviços de acesso remoto das redes bancárias centrais usando segmentação de rede. Implemente acessos temporários sob demanda (JIT) para conceder permissões apenas quando necessário. Utilize soluções de gestão de acesso privilegiado (PAM) com gravação e auditoria obrigatórias de todas as sessões. Segmentação e controle de privilégios impedem o uso dessas ferramentas para movimentação lateral.

5.3 Mispadu

O Mispadu se consolidou como uma ameaça cibernética de alta complexidade, com impactos diretos sobre o ambiente financeiro latino-americano. Desde sua identificação em 2019, o malware evoluiu de forma agressiva: o que começou com ataques focados no Brasil e no México hoje atinge uma rede muito mais ampla, com presença registrada em vários países da América Latina e até mesmo em territórios europeus.[215] [216]
Sua capacidade destrutiva está no modo silencioso de atuação e na execução em múltiplos estágios, o que reduz a eficácia das ferramentas de segurança tradicionais. O alvo principal segue sendo usuários de língua espanhola e portuguesa, o que mantém a América Latina no centro de sua ofensiva.[217] [218] O trojan contorna com sucesso soluções antivírus populares e ferramentas de proteção de endpoints, o que o torna altamente eficaz no comprometimento de instituições financeiras e outros setores críticos.[219]

A atuação do Mispadu gera consequências concretas para o sistema financeiro:

- **Roubo de credenciais:** O malware utiliza mecanismos como registro de teclas e captura de tela para interceptar logins bancários, dados de cartões e outras informações confidenciais.[220]

- **Manipulação de transações em criptoativos:** Ao detectar carteiras de criptomoedas, substitui o endereço original por um controlado pelos criminosos, desviando valores em tempo real.[221]

- **Alcance massivo:** Em campanhas recentes, o Mispadu comprometeu sites governamentais e plataformas bancárias no Chile, México e Peru, afetando centenas de entidades financeiras.[222]

Uma campanha que ficou marcada envolveu o envio de cupons falsos de desconto, evidenciando a versatilidade do trojan na aplicação de táticas de engenharia social que exploram vulnerabilidades humanas.[223] Essa flexibilidade, aliada ao foco persistente em alvos financeiros regionais, transforma o Mispadu numa ameaça cíclica e adaptativa. Técnicas como ofuscação de código, uso de geofiltros e detecção de ambientes virtuais fazem parte de sua estratégia para evitar a detecção. De acordo com análises da Morphisec, o carregamento do trojan na memória é feito por meio de um script AutoIT descriptografado, o que dificulta ainda mais a interceptação. O vetor de infecção mais utilizado envolve arquivos PDF armados, enquanto o malware também se dedica a extrair credenciais de navegadores e e-mails, mantendo vigilância constante sobre as ações do usuário. Inicialmente focado na América Latina, o Mispadu já estende seus ataques a países europeus, empregando campanhas de phishing e arquivos infectados para ampliar sua rede de coleta de credenciais.[224]

5.3.1 Estratégias do Mispadu: Como o Malware Explora Fragilidades da Infraestrutura Digital na América Latina

A campanha do Mispadu é construída com precisão para tirar proveito das brechas estruturais que ainda persistem em muitos países latino-americanos. A ausência de regulação sólida em cibersegurança, somada à aplicação irregular de normas existentes, cria o ambiente ideal para a ação de grupos criminosos. O cenário de baixa maturidade digital e carência de educação em segurança da informação torna os usuários mais suscetíveis a golpes via e-mail, o que eleva substancialmente a taxa de sucesso das campanhas de phishing utilizadas pelo malware.[225] Boa parte das organizações na região ainda opera com sistemas legados e softwares desatualizados, o que abre espaço para que o Mispadu explore vulnerabilidades já conhecidas, especialmente em plataformas amplamente utilizadas como o WordPress.

Outro ponto de atenção é a fragilidade nas respostas a incidentes: com pouca capacidade de investigação e mitigação por parte das equipes locais, o malware consegue manter-se ativo por longos períodos sem ser detectado. Seu uso de cadeias de infecção encadeadas e técnicas avançadas de evasão, como a verificação de idioma e detecção de sandbox, reforça a dificuldade de contenção. O trojan filtra vítimas com base na linguagem do sistema operacional, garantindo que suas campanhas atinjam apenas o público desejado, o que maximiza o retorno da operação e reduz exposição indesejada. Por fim, o uso de brechas como a falha no Windows SmartScreen evidencia como o Mispadu capitaliza sobre a dependência de proteções padrão, ainda comum em boa parte das empresas locais. O resultado é um cenário onde o trojan atua com alta eficiência, sustentado por lacunas regulatórias e técnicas típicas da região.

[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/
[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

5.3.2 Táticas e Técnicas para Garantir Persistência e Lucro

O Mispadu adota uma estratégia robusta baseada em TTPs sofisticados que visam maximizar seu alcance e furtividade. O ponto de partida das campanhas normalmente é a engenharia social: e-mails fraudulentos induzem o usuário a abrir arquivos HTML ou PDFs protegidos por senha, mascarando o início da infecção.[226] O malware também se vale de publicidade maliciosa e de sites legítimos previamente comprometidos, muitos deles em WordPress, que funcionam como servidores de controle para distribuir os arquivos maliciosos.[227] A entrega do payload final acontece após múltiplas etapas, passando por scripts AutoIT ou VBScript ofuscados, reforçando o nível de complexidade do ataque.

Para evitar a detecção, o Mispadu aplica filtros técnicos, como a checagem de ambiente virtual e o idioma do sistema, acionando-se apenas em contextos que correspondem ao perfil esperado. Além disso, o uso de certificados falsificados permite driblar barreiras de segurança aparentando legitimidade.[228] Entre suas funcionalidades principais, estão o roubo de credenciais via backdoors que monitoram digitação, realizam capturas de tela e aplicam sobreposições falsas de navegação para extrair dados bancários e sensíveis. A operação é apoiada por uma arquitetura de comando e controle redundante e pelo uso de vulnerabilidades como a CVE-2023-36025, que afeta o SmartScreen do Windows, possibilitando que o malware burle avisos de segurança e se infiltre com discrição.[229]

5.3.3 Perfil Operacional do Mispadu: Táticas, Técnicas e Procedimentos Utilizados

Táticas	Técnicas	Procedimentos
Reconhecimento (TA0043)	N/A	N/A
Desenvolvimento de Recursos (TA0042)	N/A	N/A
Acesso Inicial (TA0001)	T1566.001: Phishing	Campanhas de spam, nas quais a vítima acessa o payload por link ou anexo malicioso
	T1190: Exploração de Aplicação Exposta	Exploração de falhas em sistemas ou serviços acessíveis via internet
Execução (TA0002)	T1204.002: Execução de Arquivo Malicioso pelo Usuário	Ativação do malware ao abrir anexos infectados ou arquivos baixados de sites comprometidos
Persistência (TA0003)	T1053.005: Tarefa Agendada	Criação de tarefas agendadas para garantir presença contínua no sistema
Escalada de Privilégio (TA0004)	T1055: Injeção de Processo T1055.012: Hollowing T1055.013: Doppelganging	Injeta o payload em processos legítimos para passar despercebido
Evasão de Defesas (TA0005)	T1036: T1036: Mascaramento	Disfarça-se como cupom de desconto
	T1027: Arquivos ou Informações Ofuscadas T1027.013: Arquivo Criptografado/ Codificado	Usa ofuscação e criptografia para evitar detecção por antivírus e ferramentas de análise
Acesso a Credenciais (TA0006)	T1555: Senhas Armazenadas T1555.003: Senhas de Navegadores	Rouba senhas de clientes de e-mail e navegadores
	T1003: Extração de Credenciais do Sistema Operacional T1003.008: etc/passwd e etc/ shadow	Utiliza ferramentas como WebBrowserPassView e MailPassView para extrair senhas

[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

	T1056: Captura de Entrada T1056.001: Keylogging T1056.003: Captura de Portal Web	Registra teclas digitadas e tira capturas de tela para roubar dados sensíveis
Descoberta (TA0007)	T1082: Descoberta de Sistema e Informações T1083: Descoberta de Arquivos e Pastas	Coleta nome do computador, versão do sistema operacional e idioma
Movimentação Lateral (TA0008)	N/A	N/A
Coleta (TA0009)	T1113: Captura de Tela	Contém comandos para realizar capturas de tela
	T1005: Dados do Sistema Local	Coleta histórico do navegador, credenciais e dados do sistema
Comando e Controle (C2) (TA0011)	T1573: Canal C2 Criptografado	Comunicação com servidores C2 via HTTPS ou canais criptografados para exfiltração de dados e execução de comandos.
	T1102: Serviço Web T1102.002: Comunicação Bidirecional	Uses an existing, legitimate external Web service as a means for relaying data to/from a compromised system.
	T1105: Transferência de Ferramentas	Usa serviços legítimos da web para troca de dados com sistemas comprometidos
Exfiltração (TA0010)	T1041: Exfiltração via Canal C2	Envia os dados coletados para o servidor de comando e controle
	T1567: Exfiltração via Serviço Web	Utiliza serviços web legítimos como canal alternativo para exfiltrar dados
Impacto (TA0040)	N/A	

Indicadores de Comprometimento (IOCs) do Mispadu

- O Mispadu exfiltra dados roubados, incluindo credenciais e informações do sistema, por meio de canais criptografados de comando e controle (C2).
- Hashes: 72e83b133a9e4cecd21fdb47334672f6, e5967a8274d40e0573c28b664670857e
- Endereços IP: 104.238.182.44, 140.82.47.181
- Domínios: germogenborya.top, russk22.icu, germogenborya.at

Outros IOCs relacionados ao Mispadu

- SHA256 do dropper C++ (versão sem ofuscação)
- dbb2e294a65eb3fa1bbe1a25c2baf352a01250d567cfa953d4f942c2b5f08e53
- SHA256 do dropper C++ (versão ofuscada)
- d56863d940d5ccd1922bbbdf65471c493701e3b10be5c522851c8efbdaeb9fae
- SHA256 do dropper .NET
- ac97f893f8243db3c5ccfbc89d83b97534c1b73d0289ccb61bfb2c035f539126
- SHA256 do dropper HTA
- f873062ff206ad60cb4b790c2ba83624c510f15dbc4905d5c96668f87999c16a
- SHA256 do downloader D2
- 7b6444e5be24ce95cdcac357cf20ddc77abda142a16202ab3677b7d29a1e0da3
- SHA256 do payload versão 96
- 78e3e51ddeac0519d434a8b192bae61bbaa278154a9511676c8a58079d95beb5

- URL do SmokeBot que distribuiu Mispadu
- http[:]//84.54.50[.]102/FX_432661.exe
- URL do SmokeBot com payload Rhadamanthys vinculado ao Mispadu
- http[:]//amx55[.]xyz/rh111.exe

Mispadu CVE: CVE-2023-3602

5.3.3 Mispadu Mitigations

Reconhecimento (TA0043)

- Monitore o tráfego de rede com IDS/IPS para identificar varreduras suspeitas.
- Implemente honeypots para detectar tentativas iniciais de reconhecimento.

Desenvolvimento de Recursos (TA0042)

- Acompanhe registros de domínios e fique atento a tentativas de falsificação que imitam a sua organização.
- Use feeds de inteligência de ameaças para rastrear a infraestrutura dos atacantes.

Acesso Inicial (TA0001)

T1566.001: Phishing

- Adote soluções de segurança de e-mail (DMARC, DKIM, SPF).
- Realize treinamentos regulares de conscientização sobre phishing com os colaboradores.
- Utilize sandboxing para anexos recebidos por e-mail.

T1190: Exploração de Aplicações com Acesso Público

- Faça varreduras regulares de vulnerabilidades e aplique patches em sistemas expostos.
- Utilize WAFs (firewalls de aplicações web) para bloquear tentativas de exploração.

Execução (TA0002)

T1204.002: Execução de Arquivo Malicioso pelo Usuário

- Aplique políticas de whitelisting para restringir execuções não autorizadas.
- Use soluções de EDR para identificar execuções suspeitas.

Persistência (TA0003)

T1053.005: Tarefa Agendada

- Audite tarefas agendadas com frequência e limite os privilégios dos usuários.
- Habilite o log de comandos PowerShell para detectar execuções anormais.

Escalada de Privilégios (TA0004)

T1055: Injeção de Processos (incluindo T1055.012 e T1055.013)

- Ative o Windows Defender Credential Guard para prevenir o roubo de credenciais.
- Implemente detecção comportamental para identificar processos injetados.

Evasão de Defesas (TA0005)

T1036: Mascaramento

- Implemente mecanismos de detecção heurística para arquivos disfarçados.
- Analise metadados de arquivos em busca de inconsistências.

T1027: Arquivos Ofuscados ou Codificados

- Utilize sandbox automatizada para análise de malware.
- Ative monitoramento em tempo real de integridade de arquivos.

Acesso a Credenciais (TA0006)

T1555: Coleta de Senhas Armazenadas

- Desative o preenchimento automático de senhas em navegadores e apps.
- Exija autenticação multifator (MFA) em sistemas críticos.

T1003: Extração de Credenciais do Sistema Operacional

- Monitore os logs de eventos do Windows para tentativas suspeitas de acesso ao LSASS.
- Desative o armazenamento de credenciais em texto claro na configuração do sistema.

T1056: Captura de Entrada (Keylogging, Captura em Portais Web)

- Implemente detecção de keyloggers baseada em comportamento.
- Aplique o princípio de menor privilégio para evitar a instalação de softwares não autorizados.

Descoberta (TA0007)

T1082: Descoberta de Sistema e Informações

- Restrinja o acesso a informações do sistema por meio de configurações de Política de Grupo.
- Monitore comandos executados em linha de comando para identificar tentativas de reconhecimento.

Coleta (TA0009)

T1113: Captura de Tela

- Aplique soluções de prevenção contra perda de dados (DLP) para restringir capturas de tela não autorizadas.
- Utilize ambientes de desktop virtual para dificultar a persistência de malwares.

T1005: Coleta de Dados Locais

- Aplique criptografia para dados armazenados e transmitidos.
- Implemente monitoramento de integridade de arquivos para detectar acessos não autorizados.

Comando e Controle (TA0011)

T1573: Canal Criptografado

- Monitore o tráfego de rede em busca de conexões criptografadas incomuns.
- Implemente inspeção e descriptografia de SSL/TLS sempre que possível.

T1102: Serviço Web

- Bloqueie domínios maliciosos conhecidos com base em feeds de inteligência de ameaças.
- Implemente detecção de anomalias para identificar tráfego de dados fora do padrão.

T1105: Transferência de Ferramentas para Dentro da Rede

- Restrinja o download de arquivos provenientes de fontes externas desconhecidas.
- Aplique filtros de conteúdo para impedir transferências não autorizadas.

Exfiltração (TA0010)

T1041: Exfiltração via Canal C2

- Implemente controles DLP para monitorar o fluxo de dados para fora da rede.
- Detecte padrões de exfiltração por meio de análise comportamental do tráfego de rede.

T1567: Exfiltração via Serviço Web

- Bloqueie transferências externas não autorizadas por meio de proxies web.
- Monitore chamadas de APIs para identificar movimentações anormais de dados.

Impacto (TA0040)

- Implement ransomware protection with endpoint rollback capabilities.
- Implemente segmentação de rede para limitar a movimentação lateral de malwares.

5.4 Horabot

O Horabot representa uma ameaça cibernética altamente segmentada que explora a fragilidade estrutural da segurança digital em países latino-americanos. Projetado para atingir exclusivamente falantes de espanhol, o malware combina múltiplos módulos para executar ataques com foco em instituições e usuários corporativos de setores-chave. Dados levantados pela Cisco Talos demonstram que os ataques seguem padrões regionais claros, com foco em economias com baixos níveis de maturidade em segurança da informação.[230]

O malware ganhou relevância a partir de 2020, ao ser detectado em campanhas de phishing com temas tributários.[231] Esses e-mails, disfarçados como comunicados de agências fiscais, são enviados com anexos HTML que redirecionam o usuário a uma aplicação maliciosa. A linguagem usada nas mensagens (espanhol) e a escolha estratégica de períodos próximos a prazos fiscais têm sido fundamentais para elevar a taxa de infecção. Os alvos estão concentrados no México, Uruguai, Brasil, Venezuela, Argentina, Guatemala e Panamá.[232] [233]

[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/

Primary Targets and Sectors:

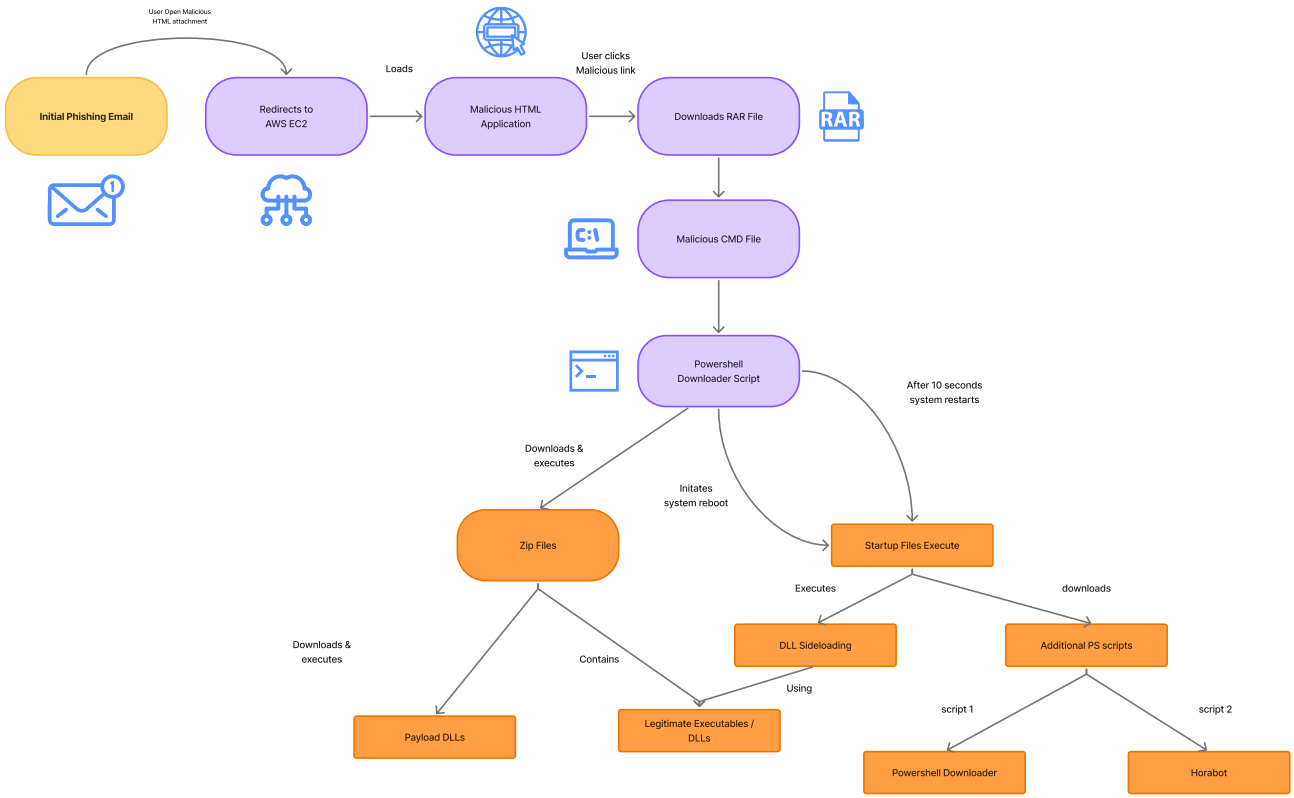
- O Horabot mira especialmente os setores de contabilidade, construção civil, engenharia, distribuição por atacado e investimentos.[234]
- Essas indústrias são naturalmente mais vulneráveis ao phishing, por lidarem com alto volume de comunicações por e-mail.[235]

5.4.1 Capacidades Técnicas do Horabot

A ameaça combina dois mecanismos principais: um trojan bancário e uma ferramenta de spam, utilizados em estágios distintos da infecção para ampliar o alcance e a eficácia dos ataques.

- Componente Bancário: Responsável pela coleta de dados sensíveis como logins de internet banking, tokens de autenticação, teclas digitadas e informações de sistema operacional. Essa funcionalidade compromete diretamente a integridade de contas financeiras, explorando falhas nos protocolos de segurança ainda presentes em parte do setor bancário regional.[236]
- Componente de Spam: Atua comprometendo contas de e-mail populares como Yahoo, Gmail e Outlook. Uma vez obtido o acesso, o malware extrai listas de contatos e utiliza os próprios servidores das organizações invadidas para disseminar e-mails de phishing com aparência legítima. Esse método reduz drasticamente a chance de bloqueio pelas defesas tradicionais de e-mail e amplia a disseminação do ataque dentro do ecossistema corporativo da vítima.[237]

Figura 7: Fluxo de Ataque



[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/

5.4.2 Semelhanças Operacionais entre Horabot e Mispadu

Horabot e Mispadu apresentam semelhanças marcantes em seus métodos, frequentemente mirando organizações da América Latina. Entre os pontos em comum observados, destacam-se:

- Vetores de Infecção Similares: Tanto Horabot quanto Mispadu operam por meio de campanhas de phishing com anexos HTML maliciosos. Esses arquivos, ao serem abertos, iniciam cadeias de infecção estruturadas em múltiplas etapas, projetadas para evitar detecção nas fases iniciais.

- Táticas MITRE Compartilhadas: Ambas as ameaças utilizam táticas mapeadas pelas técnicas T1204.001 (execução de link malicioso pelo usuário) e T1566 (phishing), o que evidencia o uso avançado de engenharia social para contornar barreiras tradicionais de filtragem e segurança de e-mail.

- Ofuscação e Criptografia como Evasão: Os dois malwares empregam mecanismos sofisticados de ofuscação e criptografia dos arquivos maliciosos. Essa abordagem dificulta a ação de soluções de segurança baseadas em assinaturas estáticas, permitindo que as ameaças operem de forma silenciosa por mais tempo.

- Foco Regional com Geolocalização: As campanhas de ambos os malwares são ajustadas geograficamente, com filtros de idioma e uso de termos codificados — como palavras em espanhol e nomes de instituições bancárias locais — direcionando os ataques com precisão a países como México e Brasil.

5.4.3 Táticas, Técnicas e Procedimentos do Horabot

Tática	Técnica	Procedimento
Desenvolvimento de Recursos (TA0042)	T1584: Comprometimento de Infraestrutura	Compromete infraestruturas de terceiros para uso em campanhas de ataque
	T1584.005: Comprometimento via Botnet	Controla múltiplos sistemas comprometidos para montar botnets usadas nos ataques
Acesso Inicial (TA0001)	T1566: Phishing	Envia e-mails de phishing para obter acesso aos sistemas das vítimas
	T1566.001: Phishing com Anexo Direcionado (Spear Phishing)	Anexos maliciosos enviados por e-mail com foco específico
	T1190: Exploração de Aplicações com Acesso Público	Explora vulnerabilidades em serviços acessíveis pela internet
	T1078: Contas Válidas	Utiliza credenciais legítimas para obter acesso, manter persistência e escalar privilégios
Execução (TA0002)	T1059: Interpretador de Comandos e Scripts	Usa interpretadores de comando para executar instruções maliciosas
	T1059.001: Interpretador de commandos e scripts: PowerShell	Abusa do PowerShell para execução remota
	T1204: Execução pelo Usuário	Depende de ações do usuário para disparar a infecção
	T1204.001: Link Malicioso	Induz o usuário a clicar em links maliciosos para iniciar a execução
	T1106: API Nativa	Interage com APIs do sistema operacional para executar ações maliciosas
Persistência (TA0003)	T1574: Desvio de Fluxo de Execução	Sequestra processos legítimos para carregar payloads próprios
	T1574.002: Side-Loading de DLL	Carrega DLLs maliciosas em vez das legítimas

	T1547.001: Execução Automática via Registro/Pasta de Inicialização	Manter persistência configurando execução automática no registro do sistema ou pastas de inicialização
	T1547.009: Execução na Inicialização: Modificação de Atalhos	Criar ou alterar atalhos para garantir que programas maliciosos sejam executados no boot ou login
Evasão de Defesas (TA0005)	T1036: Mascaramento	Tentar alterar a aparência de arquivos ou processos maliciosos para que pareçam legítimos aos olhos de usuários e ferramentas de segurança
	T1027: Arquivos ou Informações Ofuscadas	Ofuscar, codificar ou criptografar arquivos e executáveis para dificultar a análise ou detecção, seja em trânsito ou em repouso
	T1497: Evasão de Virtualização/ Sandbox	Utilizar mecanismos para detectar e evitar ambientes de virtualização e análise automatizada
	T1070.004: Remoção de Indicadores: Exclusão de Arquivos	Apagar arquivos que foram criados ou utilizados durante a atividade maliciosa
Acesso a Credenciais (TA0006)	T1056.001: Captura de Entrada: Keylogging	Registrar as teclas digitadas pelo usuário para capturar credenciais à medida que são inseridas
	T1003: Extração de Credenciais do Sistema Operacional	Tentar extrair credenciais da máquina, obtendo senhas em texto claro ou hashes de autenticação
Descoberta (TA0007)	T1082: Descoberta de Informações do Sistema	Buscar informações detalhadas sobre o sistema operacional e o hardware, como versão, atualizações instaladas, arquitetura, entre outros
	T1083: Descoberta de Arquivos e Diretórios	Mapear arquivos e diretórios do sistema local ou em compartilhamentos de rede em busca de dados específicos
Movimentação Lateral (TA0008)	T1534: Spear Phishing Interno	O malware usa uma ferramenta de spam para exfiltrar endereços de e-mail e disparar mensagens de spear phishing dentro do ambiente da vítima
Coleta (TA0009)	T1113: Captura de Tela	Tentar capturar imagens da tela da vítima ao longo da operação para reunir informações
Impacto (TA0040)	T1657: Roubo Financeiro	O grupo de ameaça exfiltrou credenciais bancárias da vítima para acessar contas e causar perdas financeiras

Indicadores de Comprometimento (IOCs):

IOCs:

Domínios Maliciosos

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

Endereços 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 (Batch)

- 63535100bbc1ba8ce9afb5883a59a4138e95c8e33a4585b8285ea7a39e0ead3e
- 720c126f372b68ff79ef13bd1ae6fc9a6aef10669269490d7e8fb589d7d49064
- ffd43b32655fc6f1e1c10f88660b68e2c2ad7da271b0f2e3eda70ccdcb3bcee4

Ferramenta de Download via PowerShell

- aaf456575c8761f3af9b61e015282d9162325ed09b699732bf65b53ae7b7d252

Cavalo de Troia Bancário

- 39194718b460ea174784f6a7edbccd1e3324fe1043be806927cece7a86f15611
- 474b25badb40f524a7b2fe089e51eb7dbafd2e3e03a9f6750f72055d05b13d76

Ferramenta de Envio de Spam

- 07f7575af922da1aea5aa26436a3cfcd91b419bbf31d77bf6c9d921290bc04da

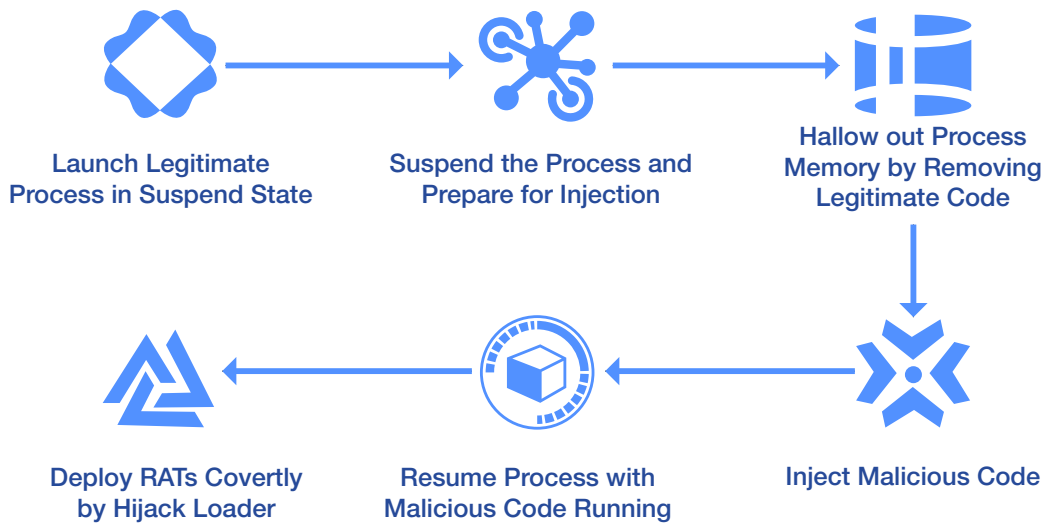
5.5 Blind Eagle

5.5.1 Atividade Relevante do APT Blind Eagle

O Blind Eagle (APT-C-36) é um agente de ameaça avançado, com atuação consolidada na América Latina, e histórico recorrente de espionagem digital contra setores estratégicos, em especial governos, instituições financeiras e companhias de energia da Colômbia, Equador, Chile e Panamá.[238] Atuante desde 2018, o grupo se destaca pela execução constante de campanhas de spear phishing direcionadas, utilizando o disfarce de entidades oficiais da região como veículo para a entrega de trojans de acesso remote (RATs).[239] As campanhas exploram diretamente fatores humanos, baseando-se em e-mails convincentes que incorporam links ou anexos com códigos maliciosos.

A operação do grupo demonstra alto grau de familiaridade com as estruturas institucionais latino-americanas, aliada a uma notável evolução técnica. Esse mecanismo envolve a inicialização de um processo legítimo em estado suspenso, seguido da remoção de seu código original da memória. Em seu lugar, o grupo injeta um payload malicioso, frequentemente trojans como QuasarRAT ou AsyncRAT. Ao retomar o processo, a execução continua sob o nome legítimo, dificultando a detecção por ferramentas de proteção de endpoint. O Blind Eagle também faz uso de loaders desenvolvidos sob medida, como o Hijack Loader, que permitem a instalação discreta de RATs e asseguram controle contínuo dos dispositivos infectados. Todo esse fluxo tático é visualizado na Figura 8.

Figura 8: Dinâmica Operacional do Blind Eagle



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

Os impactos financeiros têm sido severos. Suas ações já resultaram em falhas operacionais críticas e vazamento de informações confidenciais no setor financeiro. Conforme estudos realizados pela OEA e pelo BID, os incidentes cibernéticos custam cerca de US$ 90 bilhões por ano à América Latina, sendo o setor bancário e financeiro um dos mais prejudicados, especialmente devido a campanhas voltadas ao roubo de credenciais e espionagem corporativa.[240] Por meio da coleta de dados diretamente dos navegadores das vítimas, com técnicas como keylogging e captura de tela, o Blind Eagle compromete seriamente os mecanismos de segurança bancária das instituições afetadas. Dada a sofisticação e constância dessa ameaça, é essencial que o setor financeiro acelere o reforço de suas defesas, evoluindo no mesmo ritmo das técnicas adotadas por esse grupo.

5.5.2 Contexto

O Blind Eagle é um grupo de espionagem cibernética com atuação direcionada à América Latina, com ataques recorrentes contra instituições governamentais e financeiras na Colômbia e no Equador.[241] A estratégia inicial gira em torno de e-mails fraudulentos que simulam mensagens oficiais para disseminar malwares. Esses e-mails trazem links ou anexos que instalam trojans de acesso remoto como QuasarRAT e AsyncRAT, garantindo controle total sobre os sistemas invadidos.

QuasarRAT e AsyncRAT são especialmente populares entre grupos como o Blind Eagle porque são gratuitos, de código aberto e altamente personalizáveis. Esses RATs se moldam facilmente às exigências específicas de cada campanha de espionagem e incluem uma série de funcionalidades sofisticadas: registro de teclas digitadas, captura de tela em tempo real e extração de dados confidenciais. O valor dessas ferramentas se amplia ainda mais com recursos integrados de evasão, como criptografia de dados e técnicas de ofuscação, que dificultam sua detecção por soluções de segurança tradicionais. Essa combinação é fundamental para garantir o acesso contínuo e invisível necessário em operações prolongadas contra alvos de interesse, como instituições públicas e entidades financeiras.

5.5.3 Correlação

A metodologia adotada pelo Blind Eagle guarda semelhanças com a de outros agentes que operam na América Latina, especialmente na aplicação de spear-phishing e RATs voltados ao roubo de credenciais e à coleta de dados sensíveis. O uso de identidades e instituições locais falsas para enganar usuários é uma prática comum nesse cenário. Mas o Blind Eagle se destaca pelo uso intensivo de técnicas de injeção de código em processos, com destaque para o process hollowing, além de empregar mecanismos de entrega de malware desenvolvidos internamente, como o Hijack Loader, uma ferramentas raramente vistas em outros grupos da região.

Esse uso combinado de trojans de acesso remoto e técnicas furtivas permite ao grupo se infiltrar e permanecer por longos períodos dentro de sistemas críticos, com baixo risco de ser detectado. O grande diferencial está na regionalização: os e-mails são elaborados com base em conhecimento detalhado das estruturas institucionais e financeiras dos países-alvo, o que eleva substancialmente a taxa de sucesso das campanhas de comprometimento.

5.5.4 Recomendações

- **Blindagem de E-mails:** É essencial adotar sistemas de filtragem avançados, capazes de identificar sinais típicos de spear-phishing, como domínios alterados ou anexos suspeitos, a fim de impedir que os e-mails maliciosos alcancem os usuários.

- **Fortalecimento de EDRs (Detecção e Resposta em Endpoints):** O uso de soluções robustas de detecção e resposta em endpoints deve ser intensificado, especialmente com foco em identificar práticas de injeção de código como o process hollowing, que são frequentemente usadas por esse tipo de grupo.

- **Monitoramento Regional de Ameaças:** A criação de uma frente de inteligência voltada à identificação e análise de padrões específicos de ataque na América Latina é uma medida estratégica para antecipar ações de grupos como o Blind Eagle.

- **Treinamento Contínuo da Equipe:** Estabelecer uma rotina periódica de exercícios de phishing e implementar um canal direto de comunicação entre usuários e a equipe de segurança pode acelerar o processo de resposta a incidentes e reduzir a exposição a ataques.

5.5.5 Techniques, Tactic and Procedures

O Blind Eagle atua com uma combinação bem definida de estratégias que envolvem spear-phishing, injeção de código sofisticada e carregadores de malware desenvolvidos sob medida, sempre com foco em

[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

setores considerados críticos e de alto valor na América Latina. As campanhas geralmente se iniciam com e-mails cuidadosamente elaborados para se passarem por comunicações legítimas de instituições governamentais ou financeiras locais. Ao enganar o destinatário, esses e-mails induzem a abertura de anexos maliciosos, que por sua vez ativam trojans de acesso remoto como QuasarRAT e AsyncRAT. Com esses RATs instalados, o grupo consegue operar remotamente dentro do sistema da vítima, monitorando ações, controlando processos e extraindo informações sensíveis.

Um dos métodos mais característicos do Blind Eagle é o uso de técnicas avançadas de injeção de processos, especialmente o process hollowing. Essa técnica permite que o malware seja executado dentro da memória de processos legítimos do sistema operacional, o que o torna praticamente invisível às soluções de segurança tradicionais. É justamente essa capacidade de se disfarçar dentro do sistema que torna o método tão estratégico para o grupo.

O uso do Hijack Loader também se destaca entre os procedimentos do Blind Eagle. Trata-se de um carregador de malware criado pelo próprio grupo, capaz de entregar os RATs de forma camuflada, adaptando seu comportamento às defesas do sistema comprometido. Com isso, o loader garante não só a evasão durante a invasão inicial, mas também a continuidade do acesso ao longo do tempo. A operação como um todo é fortalecida por uma abordagem profundamente enraizada no contexto local: o grupo utiliza seu conhecimento sobre instituições, sistemas e práticas da região para tornar suas campanhas mais convincentes e aumentar a chance de sucesso logo no primeiro contato.

A escolha das vítimas é feita com base no valor que os dados podem ter e na importância estrutural que a organização ocupa dentro do ecossistema latino-americano. A persistência e a flexibilidade com que o grupo utiliza os RATs revelam uma estratégia planejada para o longo prazo, voltada à exploração silenciosa e contínua de dados estratégicos, o que configura um risco constante para o ambiente de segurança digital na região.

Tática	Técnica	Procedimento
Desenvolvimento de Recursos	T1583.001	O Blind Eagle utiliza serviços de DNS dinâmico (DDNS) para criar domínios de terceiro nível. Esses domínios funcionam como canais de comando e controle (C2).
Desenvolvimento de Recursos	T1586.002	O Blind Eagle controlava uma pasta no Google Drive vinculada a uma organização administrativa regional da Colômbia.
Desenvolvimento de Recursos	T1587.001	O grupo opera o BlotchyQuasar, que pode ser classificado como uma variante customizada do QuasarRAT.
Desenvolvimento de Recursos	T1608.001	Um arquivo do BlotchyQuasar foi disponibilizado pelo Blind Eagle em uma pasta do Google Drive comprometida e acessível publicamente.
Acesso Inicial	T1566.002	O Blind Eagle tentou obter acesso inicial ao sistema da vítima por meio de um e-mail de phishing com link para download do malware BlotchyQuasar.
Execução pelo Usuário	T1204.002	O grupo renomeou o arquivo BlotchyQuasar de forma a coincidir com a isca do e-mail de phishing e induzir o usuário a executar manualmente o malware.
Execução pelo Usuário	T1204.001	A cadeia de ataque do Blind Eagle começa quando a vítima clica no link presente no corpo do e-mail e no arquivo PDF anexado.
Acesso Inicial	T1566	O Blind Eagle é entregue via e-mail de phishing contendo um link para baixar um arquivo compactado protegido por senha.
Persistência	T1547.001	A persistência é mantida por meio das chaves Run do Registro do Windows e da pasta de Inicialização do sistema.
Execução	T1059.001	Um script em VBS é usado para acionar o PowerShell e executar o Ande Loader.
Evasão de Defesa, Escalada de Privilégio	T1055.012	O Blind Eagle utiliza a técnica de process hollowing para injetar a carga final do malware.

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 Mitigações para o Blind Eagle

Acesso Inicial

- **T1566.001** – Anexos utilizados em campanhas de spear-phishing
  - **Ações recomendadas:**
    » Empregar soluções de segurança para e-mails que combinem análise de phishing com inspeção de conteúdo avançada.
    » Investir em treinamentos contínuos para que os colaboradores saibam reconhecer tentativas de phishing e não abram arquivos inesperados.
    » Habilitar ambientes isolados (sandbox) para a execução de anexos suspeitos, reduzindo o risco de entrega de malware.

Execução de Carga Maliciosa

- **T1204.001 – Link malicioso presente no e-mail**
- **T1204.002 – Arquivo malicioso executado pelo usuário**
  - **Ações recomendadas:**
    » Implantar políticas de whitelisting de aplicações, permitindo apenas a execução de softwares previamente autorizados.
    » Adotar ferramentas de navegação segura capazes de bloquear o acesso a sites maliciosos antes mesmo de o link ser clicado.

» Realizar escaneamento de anexos com tecnologias baseadas em análise comportamental, aumentando a capacidade de identificar ameaças disfarçadas.

- **T1059.001 – Comandos e interpretação de scripts: PowerShell**
- **T1059.003 – Comandos e interpretação de scripts: Prompt de Comando**
- **T1059.005 – Comandos e interpretação de scripts: Visual Basic**
  - **Ações recomendadas:**
    » Aplicar restrições ao uso de PowerShell e outras linguagens de script por meio de políticas de controle centralizadas.
    » Ativar recursos de monitoramento como o Script Block Logging no PowerShell, que permitem detectar atividades incomuns ou suspeitas.
    » Desabilitar macros em documentos do Office, limitando sua execução apenas aos casos absolutamente necessários, conforme política corporativa.

Persistência no Sistema

- **T1053.005 – Tarefas Agendadas**
  - **Ações recomendadas:**
    » Controlar rigorosamente as permissões de usuários para impedir a criação arbitrária de tarefas agendadas no sistema.
    » Manter uma rotina de auditorias nos registros do Agendador de Tarefas a fim de identificar execuções não autorizadas ou comportamentos fora do padrão.

- **T1547.001 – Execução Automática via Registro / Pasta de Inicialização**
  - **Ações recomendadas:**
    » Limitar o acesso de escrita às chaves do Registro normalmente usadas para estabelecer persistência, reduzindo a superfície de ataque.
    » Monitorar continuamente as entradas de inicialização automática, tanto no Registro quanto nas pastas do sistema, buscando modificações não autorizadas.

Técnicas de Evasão de Mecanismos de Segurança

- **T1218.009 – Uso do regsvr32.exe para execução indireta de código (binário legítimo assinado)**
  - **Ações recomendadas:**
    » Desativar ou bloquear a execução do regsvr32.exe em ambientes onde essa ferramenta não for essencial.
    » Implementar políticas de controle de aplicações com ferramentas como Microsoft Defender ASR ou AppLocker, prevenindo usos indevidos.
    » Monitorar atentamente os processos iniciados pelo regsvr32.exe, com foco em identificar atividades incomuns ou que não estejam alinhadas ao uso esperado da ferramenta.


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

6 Recomendações Estratégicas para Fortalecer a Segurança Cibernética no Setor Financeiro Latino-Americano

6.1 Adaptação dos Controles de Segurança à Realidade Regional

Para responder de forma eficaz às ameaças direcionadas à infraestrutura bancária da América Latina, os controles de segurança precisam refletir as particularidades do ambiente local.

- Criar núcleos especializados de inteligência de ameaças voltados exclusivamente à análise de malwares e táticas que impactam o setor financeiro da região, com base em estruturas como MITRE ATT&CK e NIST SP 800-53.
- Fortalecer as capacidades internas de investigação proativa (threat hunting), incentivando parcerias técnicas com especialistas e pesquisadores latino-americanos (ISO 27001, NIST 800-150).
- Simular ataques realistas por meio de exercícios Red Team que levem em conta os vetores utilizados na região e as exigências regulatórias locais (NIST 800-115).

6.2 Formação de Redes Setoriais de CSIRTs Financeiros

- Criar equipes de resposta a incidentes específicas para o setor financeiro, tomando como referência o modelo do CSIRT bancário da Colômbia (ISO 27035, NIST 800-61).
- Estimular parcerias entre instituições públicas e privadas para consolidar uma base colaborativa de resposta a ameaças.
- Adotar protocolos formais de compartilhamento de inteligência em tempo real, otimizando a disseminação de indicadores de comprometimento e técnicas emergentes.

6.3 Melhoria da Capacidade de Resposta Multinacional

- Unificar os procedimentos de resposta a incidentes entre os países da região, alinhando-os a normas reconhecidas como NIST 800-61 e ISO 27035.
- Criar linhas diretas de cooperação com CERTs locais e forças internacionais de aplicação da lei para coordenação de ações.
- Realizar simulações práticas envolvendo múltiplas jurisdições para testar a prontidão conjunta em cenários de incidentes complexos.

6.4 Fortalecimento da Segurança Baseada em Pessoas

- Promover treinamentos de segurança cibernética customizados por função, acompanhados de campanhas recorrentes de simulação de phishing (NIST 800-50, ISO 27002).
- Tornar obrigatória a adoção de autenticação multifator e práticas rigorosas de gestão de senhas e credenciais (NIST 800-63, ISO 27001).
- Incentivar uma mentalidade corporativa em que a segurança seja uma responsabilidade compartilhada, reduzindo o impacto de ataques baseados em engenharia social.

6.5 Transformação Digital Segura e Gestão de Acesso

- Adotar a arquitetura de Zero Trust como modelo de segurança, alinhada ao NIST SP 800-207, para garantir que todos os acessos sejam validados com base no menor privilégio possível.
- Implantar autenticação multifator dinâmica e recursos biométricos como exigência para acesso a ambientes sensíveis (ISO 27001, NIST 800-63B).
- Promover a modernização dos sistemas legados com base em princípios de segurança embutida desde o design, assegurando conformidade com exigências regulatórias vigentes.

6.6 Fortalecimento da Gestão de Terceiros e Monitoramento Contínuo

- Implantar avaliações de risco contínuas e rotinas de checagem de conformidade nos fornecedores, utilizando normas como ISO 27036 e NIST 800-161.
- Formalizar exigências contratuais de segurança baseadas em padrões globais, tornando-as parte obrigatória da relação com terceiros.
- Utilizar ferramentas automatizadas para monitoramento em tempo real de anomalias e detecção de incidentes com alta precisão.

6.7 Padronização de Requisitos Regulatórios

- Incentivar a adoção do CRI Profile como estrutura de referência na América Latina, integrando requisitos regulatórios, práticas de resiliência e governança de risco sob um único modelo.[242]
- Criar uma estrutura regional de cibersegurança com diretrizes claras e formatos unificados para reportes técnicos (ISO 29147, NIST 800-61).
- Estabelecer regras com prazos formais para comunicação de violações de dados, nos moldes da LGPD brasileira.
- Centralizar a coordenação de notificações e respostas sob uma autoridade regional especializada em cibersegurança.

6.8 Melhoria na Troca de Informações

- Desenvolver uma plataforma protegida para a troca transfronteiriça de inteligência sobre ameaças cibernéticas.
- Estimular alianças entre setor público e privado para ações coordenadas, com base em frameworks como NIST 800-150 e ISO 27010.
- Firmar acordos regionais que garantam capacidade de resposta rápida a incidentes que envolvam mais de um país.

6.9 Expansão da Infraestrutura de Defesa Cibernética

- Destinar entre 2% e 3% do Produto Interno Bruto a projetos de fortalecimento da segurança cibernética, conforme diretrizes da OCDE.
- Estabelecer como obrigatórios os padrões de criptografia robusta e autenticação multifator para setores estratégicos (NIST 800-175, ISO 27001).
- Estruturar políticas nacionais com foco na proteção de infraestruturas críticas, garantindo continuidade operacional frente a ameaças digitais.

6.10 Capacitação Profissional e Educação em Cibersegurança

- Desenvolver programas educacionais específicos para os diferentes segmentos da indústria financeira, baseados em frameworks como o NIST NICE e a ISO 27021.
- Realizar simulações de resposta a incidentes de forma contínua, com foco em avaliar e aprimorar a capacidade de reação institucional frente a ameaças reais (NIST 800-84).
- Estabelecer trilhas de certificação que contribuam para a formação técnica de profissionais e para a consolidação de uma base qualificada de talentos no setor.

6.11 Fortalecimento dos Instrumentos Regulatórios

- Criar ou modernizar leis de proteção de dados nos países da região onde ainda não existem, tomando como referência modelos como ISO 27701, GDPR e o NIST Privacy Framework.
- Estabelecer sanções mais severas para organizações que descumprirem prazos ou omitirem notificações em casos de violação de dados.
- Atualizar regularmente o arcabouço legal de cibersegurança para acompanhar a evolução tecnológica e os novos cenários de risco.

6.12 Cooperação Internacional Estratégica

- Participar ativamente de fóruns internacionais sobre cibersegurança para promover a troca de experiências e adoção de boas práticas globais (ENISA, ITU Global Cybersecurity Index).
- Estreitar relações com agências internacionais de aplicação da lei, contribuindo para o combate coordenado ao cibercrime, com base em tratados como a Convenção de Budapeste.
- Buscar assistência técnica junto a países com maturidade elevada em segurança cibernética.

Ao alinhar-se a essas iniciativas e boas práticas reconhecidas internacionalmente, o setor financeiro latino-americano estará mais preparado para enfrentar ameaças digitais emergentes, promovendo não apenas resiliência operacional, mas também confiança no ambiente digital da região.

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

7 Apêndice

7.1 Dados Segmentados

Esses IDs de Ameaça, comumente chamados de Técnicas, representam os pontos em comum entre os três agentes de ameaça.

Dados do CLOP para o MITRE

Reconhecimento: táticas

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

Desenvolvimento de Recursos:

mitre:T1586	T1586	MitreAttackIdentifier

Acesso 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

Execução:

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

Persistência:

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

Escalada de Privilégios:

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

Evasão de Defesas:

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

Acesso a Credenciais:

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

Descoberta:

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

Movimentação 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

Coleta:

mitre:T1005	T1005	MitreAttackIdentifier

Comando e Controle (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

Exfiltração:

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 Mobile:

mitre:T1406.002	T1406.002	MitreAttackIdentifier

Dados do LockBit para o MITER

1. Reconheicmento:
2. Desenvolvimento de Recursos:
3. Acesso Inicial:

mitre:T1190	T1190	MitreAttackIdentifier
mitre:T1078	T1078	MitreAttackIdentifier

4. Execução:

mitre:T1059	T1059	MitreAttackIdentifier

5. Persistência:

mitre:T1543	T1543	MitreAttackIdentifier

6. Escalada de Privilégios:
7. Evasão de Defesas:

mitre:T1562	T1562	MitreAttackIdentifier

8. Acesso a Credenciais:

mitre:T1003	T1003	MitreAttackIdentifier

9. Descoberta:

mitre:T1087	T1087	MitreAttackIdentifier

10. Movimentação Lateral:

mitre:T1021.001	T1021.001	MitreAttackIdentifier

11. Coleta:

mitre:T1560	T1560	MitreAttackIdentifier

12. Comando e Controle (C&C):
13. Exfiltração:
14. Impacto:

mitre:T1486	T1486	MitreAttackIdentifier

Dados do Mispadu para o MITER

1. Reconhecimento:
2. Desenvolvimento de Recursos:
3. Acesso Inicial:

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

4. Execução:

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

5. Persistência:
6. Escalada de Privilégios:

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

7. Evasão de Defesas:

mitre:T1036	T1036	MitreAttackIdentifier
mitre:T1027	T1027	MitreAttackIdentifier

8. Acesso a Credenciais:

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

9. Descoberta:

mitre:T1082	T1082	MitreAttackIdentifier
mitre:T1083	T1083	MitreAttackIdentifier

10. Movimentação Lateral:
11. Coleta:

mitre:T1005	T1005	MitreAttackIdentifier
mitre:T1113	T1113	MitreAttackIdentifier

12. Comando e Controle (C&C):

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

13. Exfiltração:

mitre:T1041	T1041	MitreAttackIdentifier
mitre:T1567	T1567	MitreAttackIdentifier

Dados do Horabot para o MITER

1. Reconhecimento:
2. Desenvolvimento de Recursos:

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

3. Acesso Inicial:

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

4. Execução:

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. Persistência:

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 Privilégios:

mitre:TA0004	TA0004	MitreAttackIdentifier

7. Evasão de Defesas:

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. Acesso a Credenciais:

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

9. Descoberta:

mitre:TA0007	TA0007	MitreAttackIdentifier
mitre:T1082	T1082	MitreAttackIdentifier

10. Movimentação Lateral:
11. Coleta:

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

12. Comando e Controle (C&C):

mitre:TA0011	TA0011	MitreAttackIdentifier

13. Exfiltração:
14. Impacto:

mitre:TA0040	TA0040	MitreAttackIdentifier

7.2 Definições

Táticas, Técnicas e Procedimentos: Padrões operacionais mais utilizados por agentes mal-intencionados para arquitetar e executar ataques digitais direcionados a instituições financeiras, abrangendo desde métodos de invasão até estratégias de persistência.[243]

Phishing: Método de ataque baseado em engenharia social, no qual o criminoso manipula a vítima para obter informações sigilosas. As principais variações incluem:

1. Spear Phishing: Ameaça direcionada a colaboradores específicos, geralmente por e-mail, induzindo o clique em links que capturam credenciais e abrem brechas para acesso não autorizado aos sistemas da empresa.

2. Whaling: Variante que tem como alvo membros do alto escalão, buscando extrair dados estratégicos por meio de abordagens altamente personalizadas.[244]

3. Smishing: Técnica que utiliza mensagens de texto para enviar links ou conteúdos fraudulentos, induzindo o fornecimento de senhas ou dados bancários.

4. Vishing: Ataque realizado via chamadas telefônicas falsas, em que o criminoso se passa por representante de uma instituição confiável para obter informações confidenciais da vítima.

Malware: Categoria ampla que inclui qualquer código ou software projetado para explorar fragilidades em sistemas digitais com fins maliciosos.

Ransomware: Tipo de ataque que criptografa dados corporativos e exige resgate financeiro para desbloqueá-los. Frequentemente vinculado a campanhas de phishing ou exploração de falhas não corrigidas.

Malware sem arquivos (Fileless): Ameaça que se executa diretamente na memória do sistema, sem deixar rastros em disco, tornando sua detecção complexa para soluções tradicionais de segurança.

Spyware: Ferramenta de espionagem digital utilizada para acompanhar, sem consentimento, o comportamento online do usuário e extrair dados sensíveis.

Adware: Software que insere propagandas indesejadas no ambiente do usuário, frequentemente como subproduto de programas espiões.[245]

Trojans: Programas maliciosos que se disfarçam de aplicações legítimas para enganar o usuário, sendo frequentemente empregados em ataques de engenharia social.[246]

Worms: Malwares autorreplicantes capazes de se espalhar por redes inteiras sem interação humana, podendo corromper arquivos e instalar cargas adicionais.

Rootkits: Conjunto de ferramentas que garantem ao invasor controle total e oculto de um sistema comprometido, muitas vezes sem que o usuário perceba.

Malware voltado a dispositivos móveis: Ameaças projetadas especificamente para ambientes móveis, geralmente propagadas por apps maliciosos ou redes Wi-Fi comprometidas.

Exploits: Ferramentas desenvolvidas para tirar proveito de brechas técnicas em softwares ou sistemas, permitindo acesso não autorizado a informações ou estruturas corporativas.[247]

Scareware: Estratégia que utiliza o medo como gatilho, simulando infecções ou falhas críticas no sistema para convencer a vítima a instalar produtos falsos ou maliciosos.

Keyloggers: Softwares espiões criados para capturar tudo o que é digitado em um dispositivo, incluindo credenciais, números de cartão e outras informações estratégicas que podem ser exploradas em fraudes ou acessos indevidos.

Botnets: Conjuntos de equipamentos previamente invadidos e controlados remotamente por agentes maliciosos. Essas redes zumbis são usadas para realizar ataques em larga escala, disseminar malware ou manipular tráfego digital.

Malspam: Campanhas de e-mail em massa com anexos ou links perigosos, intencionalmente projetadas para instalar códigos maliciosos nos dispositivos dos destinatários. É uma via comum de propagação de infecções.

Ataques Wiper: Malwares destrutivos com foco na exclusão irreversível ou na danificação de dados corporativos. Frequentemente empregados em contextos de ciberconflito, sabotagem ou ativismo digital com fins desestabilizadores.

DOS/DDOS: Ações coordenadas para interromper a operação de sistemas online. No caso do DoS, o ataque parte de uma única fonte. Já no DDoS, múltiplas máquinas são mobilizadas ao mesmo tempo, elevando drasticamente o volume de requisições e dificultando as defesas. O impacto pode ser severo, afetando diretamente a disponibilidade de serviços essenciais.

[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/

Ameaças de Injeção de Código: Técnicas que exploram brechas em aplicações ou sistemas para introduzir comandos maliciosos. As consequências podem variar desde extração de dados até controle completo da aplicação.[248]

Entre os vetores mais frequentes:

- **Injeção SQL:** Manipulação de instruções SQL para acessar dados restritos ou executar ações não autorizadas diretamente no banco de dados.
- **Injeção de Comandos:** Execução direta de comandos no sistema operacional, usando entradas mal validadas.
- **XSS (Cross-Site Scripting):** Inserção de scripts em sites confiáveis, capazes de capturar informações de usuários ou interferir em sessões legítimas.[249]
- **Injeção XML:** Exploração de falhas na interpretação de dados XML para inserir código malicioso.
- **Injeção LDAP:** Utilização de comandos maliciosos para manipular diretórios corporativos, podendo resultar em acessos indevidos a dados e permissões.

7.3 Panorama de Vulnerabilidades e Indicadores de Comprometimento no Setor Financeiro

As vulnerabilidades mais recorrentes mapeadas em instituições financeiras foram analisadas com base em seu nível de ameaça. A gestão de riscos e falhas de segurança é fundamental para esse setor, dada a criticidade das informações que ele manipula. Abaixo, estão alguns dos glossários e estruturas mais utilizados para classificar vulnerabilidades e indicadores de comprometimento (IoCs).

Common Vulnerabilities and Exposures (CVE):

- Lista padronizada de vulnerabilidades cibernéticas de conhecimento público.
- Cada item CVE possui um número de identificação, uma descrição e referências a boletins de segurança relacionados.
- Utilizado por instituições financeiras para monitorar e avaliar falhas em seus sistemas.

Common Vulnerability Scoring System (CVSS):

- Modelo de avaliação que classifica o grau de severidade das vulnerabilidades.[250]
- Atribui uma pontuação com base no potencial de exploração e impacto, ajudando a definir prioridades de resposta.

National Vulnerability Database (NVD):

- Repositório oficial dos EUA que reúne dados sobre vulnerabilidades, incluindo CVEs, pontuações CVSS e metadados complementares.
- Amplamente utilizado no setor financeiro para análise e gestão de riscos.

Financial Services Information Sharing and Analysis Center (FS-ISAC):[251]

- Fornece inteligência de ameaças e informações sobre vulnerabilidades voltadas especificamente ao setor financeiro.
- Compartilha indicadores de comprometimento e alertas para apoiar a prevenção e a proteção institucional.

MITRE ATT&CK Framework:

- Base de conhecimento com táticas e técnicas adversárias documentadas a partir de casos reais.[252]
- Auxilia instituições financeiras na identificação e contenção de métodos de ataque sofisticados.

7.4 Indicadores de Comprometimento (IOCs)

- Hash de Arquivos: Valores únicos que representam arquivos específicos e podem ser utilizados para identificar atividades maliciosas.
- Endereços IP: Endereços associados a comportamentos maliciosos conhecidos.
- URLs/Domínios: Usados por invasores para controlar malwares ou extrair dados de forma não autorizada.
- Endereços de E-mail: Utilizados em ataques de phishing ou outras fraudes baseadas em e-mail.

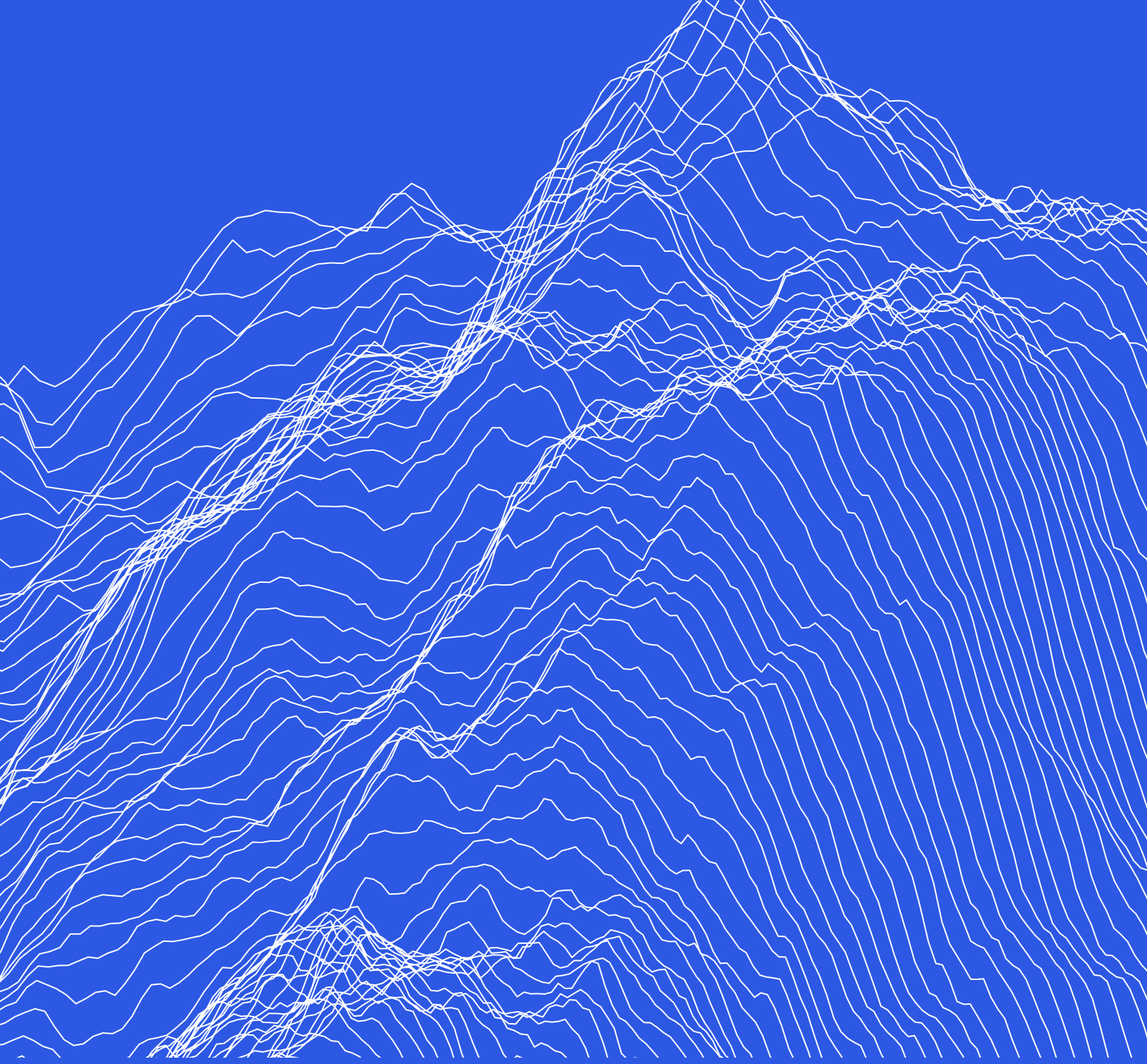
Essas ferramentas e estruturas auxiliam instituições financeiras a gerenciar e mitigar ameaças cibernéticas de forma eficaz, protegendo seus dados sensíveis.

7.5 Provas Forenses

As três evidências forenses mais relevantes para detectar possíveis intrusões em sistemas ou redes de instituições financeiras.[253]

- Escalonamento de privilégios: Situação em que o agente malicioso obtém permissões superiores às inicialmente acessadas, aumentando o potencial de impacto dentro do sistema.
- Movimentação lateral: Ações que demonstram que o invasor conseguiu transitar entre diferentes pontos da infraestrutura, o que pode facilitar o alcance de dados críticos ou a propagação de códigos maliciosos.
- Exfiltração de dados: A mais grave das evidências, pois confirma que houve vazamento de informações sensíveis, muitas vezes com repercussões legais, reputacionais e financeiras.

[248] https://www.securityjourney.com/post/owasp-top-10-injection-attacks-explained
[249] https://datapacket.net/website-security/
[250] https://hadrian.io/blog/tag/security-solutions
[251] https://www.ibm.com/reports/threat-intelligence
[252] https://nsarchive.gwu.edu/media/29421/ocr
[253] https://core.ac.uk/download/346450152.pdf



DIGI
AMERICAS