LexisNexis®
RISK SOLUTIONS

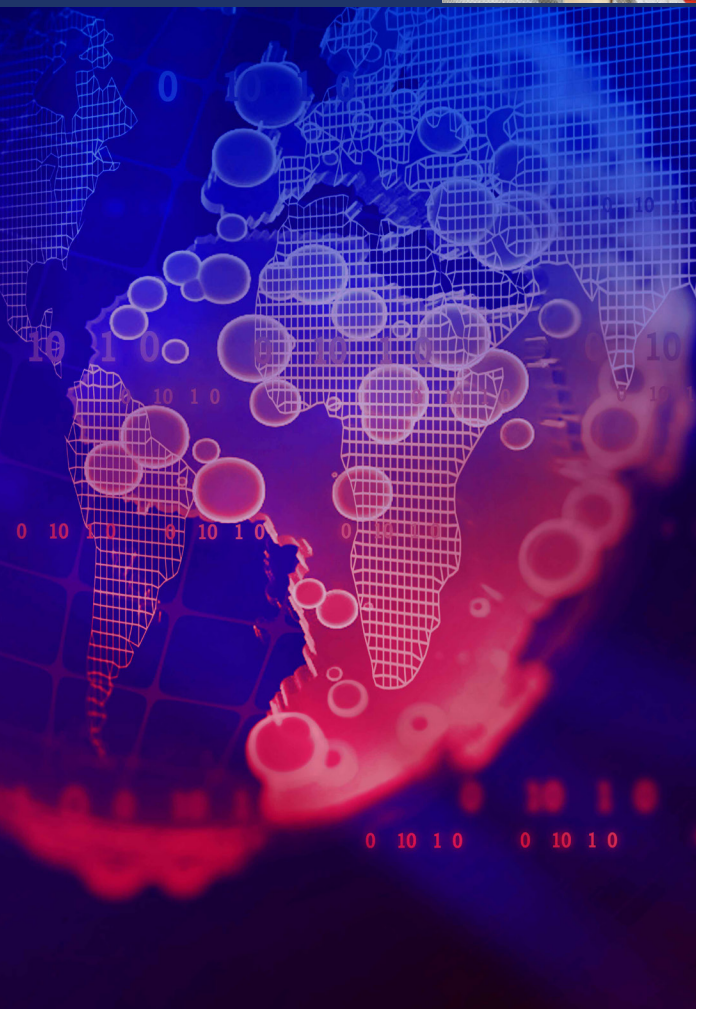
OS CRIMES CIBERNÉTICOS NA AMÉRICA LATINA

A ADAPTAÇÃO A UM MUNDO PÓS PANDEMIA

O Relatório sobre crimes cibernéticos da LexisNexis® Risk Solutions
Janeiro a junho de 2021


INTRODUÇÃO

Rafael Costa
Diretor de Mercados
Planejamento & Estratégia,
LexisNexis® Risk Solutions



INTRODUÇÃO

Com o surgimento da pandemia, pudemos ver em todo o mundo uma aceleração da transformação digital da noite para o dia, os mais diversos ramos de negócios foram forçados a migrar para os canais digitais. Na América Latina, em especial, pudemos ver um avanço rápido da inclusão digital da população. Um exemplo dessa inclusão foi a rápida bancarização de grande parcela da população não bancarizada que, para receber os pacotes de ajuda dos governos regionais abriram pela primeira vez uma conta bancária. E com as agências bancárias fechadas, todas as aberturas foram através de canais digitais.

Se por um lado tivemos o benefício da inclusão digital da população latinoamericana, por outro lado essa rápida digitalização abriu caminho para quadrilhas especializadas direcionarem seus ataques para os benefícios que os governos estavam disponibilizando para a população. Ao analisarmos milhões de transações ao redor do mundo, pudemos constatar que a guerra não é apenas contra um vírus, mas também contra a fraude digital que vitimiza milhares de cidadãos que dependem desse benefício para a sua subsistência.

A pandemia trouxe uma grande mudança no mundo, transformando os hábitos de consumo das pessoas ao redor do mundo, com cada vez mais serviços sendo consumidos através dos canais digitais. Compras, negócios, serviços financeiros e entretenimento são consumidos através de canais online, o que tem atraído a atenção de cibercriminosos.

DESTAQUES GLOBAIS: JANEIRO - JUNHO 2021

O volume de pagamentos digitais continuou disparando à medida que os consumidores migraram, cada vez mais, para o mundo online.

28,7 bi
OPERAÇÕES

+28% ▲
crescimento ano a ano (a.a.) no volume das operações globais:

+30%
crescimento nos serviços financeiros.

+21%
crescimento no comércio eletrônico.

+27%
crescimento em mídia.

236 mi
ATAQUES INICIADOS POR HUMANOS

-29% ▼
queda a.a.

		Crescimento/ Queda a.a.
Criações de novas contas	490 mi	-10% ▼
Logins	20,5 bi	+25% ▲
Pagamentos	4,8 bi	+41% ▲

Maiores contribuições a ataques cibernéticos iniciados por humanos:

1. EUA
2. CANADÁ
3. BRASIL
4. MÉXICO
5. REINO UNIDO

1,2 bi
ATAQUES DE BOTS AUTOMATIZADOS

+41% ▲
crescimento a.a

		Crescimento/ Queda a.a.
Serviços financeiros	683 mi	+28% ▲
Comércio eletrônico	189 mi	-9% ▼
Mídia	351 mi	+174% ▲

Maiores origens de ataques de bots:

1. EUA
2. REINO UNIDO
3. JAPÃO
4. CANADÁ
5. ESPANHA

© 2022 LEXISNEXIS RISK SOLUTIONS

LexisNexis® RISK SOLUTIONS


CENÁRIO NA
AMÉRICA LATINA

OPERAÇÕES E PADRÕES DE ATAQUE NA LATAM

AS 5 MAIORES ORIGENS DE ATAQUES

1. Brasil
2. México
3. Colômbia
4. Peru
5. Argentina

OS 5 MAIORES DESTINOS DOS ATAQUES

1. Brasil
2. EUA
3. Chile
4. Reino Unido
5. México

OPERAÇÕES

OPERAÇÕES PROCESSADAS

1,2 bi

Crescimento a.a.
+57% ▲

OPERAÇÕES CLASSIFICADAS POR CANAL

Desktop / Móvel

22% 78%

Navegadores móveis / **aplicativos móveis**

25% 75%

ATAQUES

VOLUME DE ATAQUES DE BOTS AUTOMATIZADOS

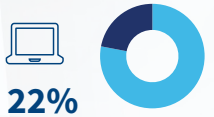
Crescimento a.a.
+84% ▲

VOLUME DE ATAQUES INICIADOS POR HUMANOS

Queda a.a
-1% ▼

ATAQUES INICIADOS POR HUMANOS CLASSIFICADOS POR CANAL

Desktop / Móvel



22% 78%

A taxa de ataques originados em dispositivos móveis tem **crescido ano a ano**
+8% ▲

© 2022 LEXISNEXIS RISK SOLUTIONS

LexisNexis® RISK SOLUTIONS

A POSIÇÃO DA LATAM EM COMPARAÇÃO AOS NÚMEROS GLOBAIS

Pequena queda dos ataques iniciados por humanos, acompanhado de forte crescimento de bots.

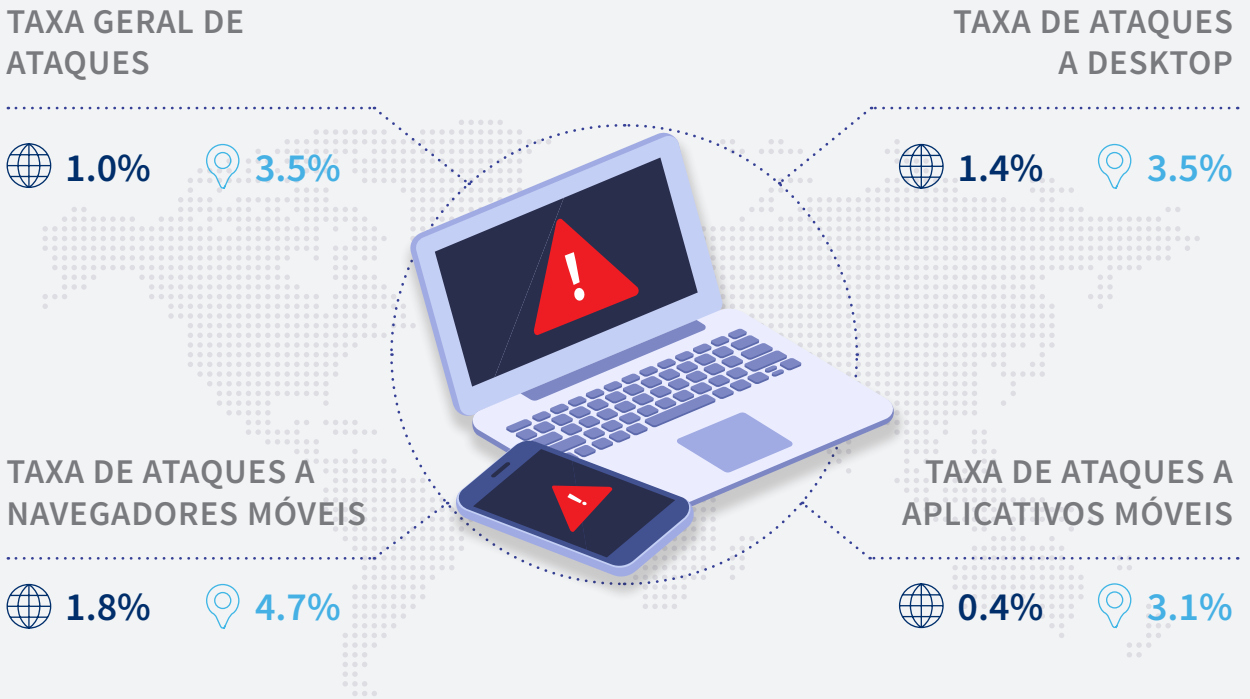
GLOBAL **LATAM**

As ocorrências de ataques na LATAM permaneceram as mais altas de todas as regiões do mundo, entre todos os casos de uso.

A rápida transformação digital favoreceu um ambiente de ataques voláteis, onde o volume de investidas por bots apresentou uma trajetória de alta e as taxas de ataques diários alcançaram diversos picos fortes durante o período.

Os canais móveis na região foram particularmente suscetíveis a ataques, com altos índices sendo registrados em operações tanto em navegadores como em aplicativos móveis. Todas as outras regiões globais registraram taxas de ataques bem inferiores em operações em aplicativos móveis.

Isso foi provavelmente impulsionado pelo celular ter facilitado a inclusão financeira sendo assim, um alvo mais atacado do que desktops em alguns casos de uso. A taxa de ataques aos canais móveis tem crescido 8% ano a ano.



© 2022 LEXISNEXIS RISK SOLUTIONS

A LATAM SOFREU MAIOR AUMENTO NA TAXA DE ATAQUES MÓVEIS EM COMPARAÇÃO A OUTRAS REGIÕES

A digitalização e a modernização da infraestrutura resultou em aumento nas operações realizadas em dispositivos móveis.

Internet banking e soluções de pagamento mais baratas e fáceis de usar estão mudando o padrão bancário na América Latina

A LATAM continuou surfando a onda da transformação digital, com o crescimento acelerado dessas plataformas, internet banking, diferentes formas de pagamento e ofertas de comércio eletrônico. Embora muitas economias da região sejam altamente digitais, grandes parcelas da população ainda acessam os serviços online somente através de um dispositivo móvel, o que significa que bancos somente digitais e virtuais podem ajudar a facilitar a inclusão financeira da população não bancarizada ou que conta com acesso limitado a esses serviços por meio de serviços bancários móveis.

Essa rápida digitalização e modernização da infraestrutura contribuiu para a LATAM continuar sofrendo o maior volume diário de ataques no mundo, com grande destaque ao crescimento de investidas de bots automatizados. Na primeira metade do ano, três diferentes picos de ocorrências de ataques foram alcançados em janeiro, abril e maio.

Além disso, os governos sul-americanos lançaram pacotes de estímulo para fornecer assistência por conta da Covid, o que resultou em um grande número de pessoas abrindo contas bancárias digitais pela primeira vez. Isso levou a um aumento no volume das operações de internet banking e também expôs essa grande parcela da população novata ao mundo digital a fraudes e golpes em potencial.

Para muitos desses novos bancos digitais e organizações de pagamento, o acolhimento digital simplificado facilitou o rápido fluxo de novos clientes. Entretanto, esses mesmos processos simplificados de *onboarding* costumam ser bastante atacados por fraudadores, especialmente em países onde as verificações de KYC ainda não estão maduras e não há um padrão nacional de documentação de identidade. Um grande facilitador para esse tipo de fraude foi o celular da vítima. A região registrou alto volume de roubos de celulares, que são usados pelos fraudadores para interceptar as credenciais de uso de internet banking.

DESTAQUE DOS ATAQUES NA REGIÃO DA LATAM JAN - JUNHO 2021

- Grande tentativa de criações de novas contas por ataques de bots, com origem no México, em instituições financeiras.
- Ataques de bots automatizados também tentaram invadir contas tendo como alvo organizações de mídia por streaming. Elas tiveram origem predominantemente no Brasil, na Argentina e na Colômbia e testavam endereços de e-mail roubados.

© 2022 LEXISNEXIS RISK SOLUTIONS

ÍNDICE DE ABUSO DE IDENTIDADE POR REGIÃO

As regiões LATAM e APAC continuaram sofrendo as taxas de ataques mais voláteis, com picos diários significativos por todo o ano de 2021.

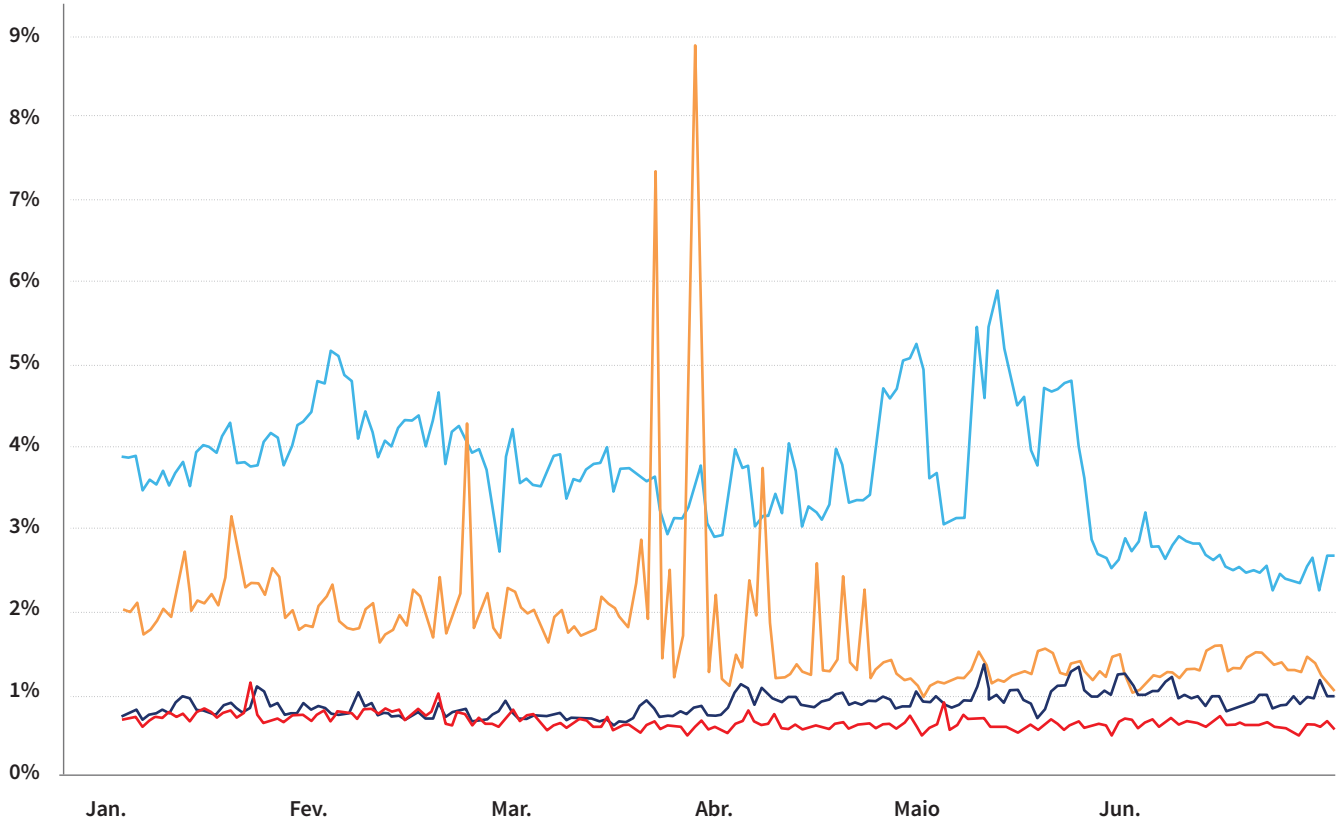
APAC EMEA LATAM AMÉRICA DO NORTE

A LATAM continuou registrando as taxas mais elevadas de ataques diários entre todas as regiões, com diversos picos observados durante 2021.

A APAC registrou diversos picos extremamente altos de ataques de bots, apesar da clara tendência de queda nas investidas diárias entre março e junho de 2021.

A América do Norte registrou taxas crescentes de ataques diários entre março e junho de 2021, ultrapassando, claramente as ocorrências da EMEA, tendência anormal aos períodos anteriores.

A EMEA continuou registrando taxas gerais de ataques mais baixas do que qualquer outra região, com atividades de bots especialmente baixas durante esse período.



© 2022 LEXISNEXIS RISK SOLUTIONS

LexisNexis® RISK SOLUTIONS

OS FRAUDADORES SE APROVEITARAM DO PODER DAS REDES PARA FACILITAR OS ATAQUES

Redes hiperconectadas continuaram atacando diversos setores e organizações.

O Digital Identity Network continuou registrando um forte padrão de fraudes interorganizacionais, intersetoriais e até mesmo inter-regionais.

É provável que cada rede inclua vários grupos de fraudadores usando as mesmas listas de dados de identidade roubados, que são explorados nas regiões e setores.

Golpes

O volume e a complexidade dos golpes explodiram e estão rapidamente se tornando um transtorno para os serviços financeiros e para as empresas de comércio eletrônico. Por exemplo, golpes perfeitos de engenharia social convencem um cliente desavisado a divulgar os seus dados pessoais ou realizar um pagamento autorizado a um beneficiário de escolha do fraudador, sob o pretexto de proteger a sua conta ou aumentar ativos. Diferentemente das tentativas tradicionais de golpes, que utilizam o dispositivo do fraudador ou credenciais roubadas para realizar o ataque, quando o cliente é cúmplice do golpe sem saber, os métodos padrões de detecção, como anomalias de dispositivo, localização ou credenciais são ineficazes.

O Digital Identity Network também observou diversos exemplos de golpes sofisticados com a seguinte tipologia de ataque:

A APRESENTAÇÃO DO GOLPE

O cliente responde a uma mensagem *phishing* ou smishing. Em seguida, o fraudador costuma entrar em contato com o cliente, usando engenharia social para induzi-lo a acreditar que estão executando uma oferta ou operação genuína. Isso pode ser corroborado por um aplicativo ou website falso.

METODOLOGIA

Os fraudadores exploram a preocupação ou o senso de urgência da vítima, o que pode dificultar a interrupção de uma operação de pagamento. O pagamento é feito pelo titular legítimo da conta, como parte de uma sessão de internet banking totalmente autenticada. Como alternativa, o cliente pode concluir uma verificação de AFC durante uma de CNP iniciada pelo fraudador.

ATAQUE

Os protocolos de pagamento em tempo real significam que o dinheiro pode sair da conta da vítima imediatamente, sendo muito difícil de ser rastreado ou recuperado, especialmente se o valor for dividido e movimentado por uma série de contas mula.

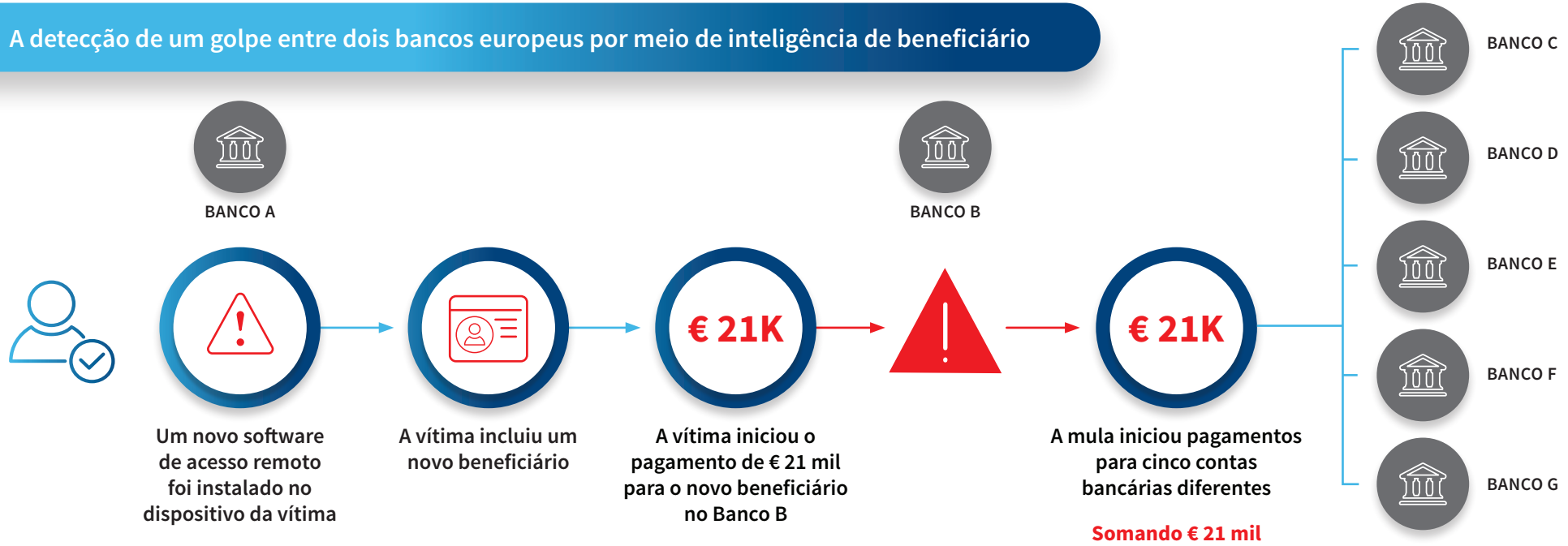
© 2022 LEXISNEXIS RISK SOLUTIONS

DETECÇÃO DE FRAUDES EM REDE EM TODO O AMBIENTE DE INTERNET BANKING

Caça às mulas nos pagamentos globais: monitoramento de operações do pagador para o beneficiário.

A detecção de redes de mulas também depende da capacidade de monitoramento dos pagamentos desde o pagador até o beneficiário, o que pode ser especialmente desafiador quando o pagamento é executado pelo próprio cliente, coagido por meio de um golpe ou fraude de engenharia social. Detectar atividades incomuns através do beneficiário pode ajudar a proteger os bons clientes que fizerem pagamentos para contas associadas a redes mulas conhecidas.

A detecção de um golpe entre dois bancos europeus por meio de inteligência de beneficiário



© 2022 LEXISNEXIS RISK SOLUTIONS

LexisNexis® RISK SOLUTIONS

DESTAQUES DO BRASIL

OPERAÇÕES

OPERAÇÕES PROCESSADAS

Crescimento a.a.

+28% ▲

OPERAÇÕES CLASSIFICADAS POR CANAL

Desktop / Móvel

Navegadores móveis / **aplicativos móveis**

ATAQUES

VOLUME DE ATAQUES DE BOTS AUTOMATIZADOS

Crescimento a.a.

+141% ▲

VOLUME DE ATAQUES INICIADOS POR HUMANOS

Queda a.a.

-44% ▼

ATAQUES INICIADOS POR HUMANOS CLASSIFICADOS POR CANAL

Desktop / Móvel

A taxa de ataques originados em dispositivos móveis tem **crescido ano a ano**

+5% ▲

© 2022 LEXISNEXIS RISK SOLUTIONS

DESTAQUES DO MÉXICO

OPERAÇÕES

OPERAÇÕES PROCESSADAS

Crescimento a.a.

+185%▲

OPERAÇÕES CLASSIFICADAS POR CANAL

Desktop / Móvel

Navegadores móveis / **aplicativos móveis**

ATAQUES

VOLUME DE ATAQUES DE BOTS AUTOMATIZADOS

Crescimento a.a.

+162%▲

VOLUME DE ATAQUES INICIADOS POR HUMANOS

Queda a.a.

-28%▼

ATAQUES INICIADOS POR HUMANOS CLASSIFICADOS POR CANAL

Desktop / Móvel

A taxa de ataques originados em dispositivos móveis tem **crescido ano a ano**

+5%▲

© 2022 LEXISNEXIS RISK SOLUTIONS

OPORTUNIDADES DO SETOR

PANORAMA DO SETOR: TENDÊNCIAS E PADRÕES DE ATAQUE NA LATAM

As organizações de mídia continuam suportando o peso dos ataques de testes de identidade.

PANORAMA DO SETOR	RESUMO DE TODOS OS SETORES	SERVIÇOS FINANCEIROS	COMÉRCIO ELETRÔNICO	MÍDIA
TENDÊNCIAS DE RISCO	De todos os canais, as operações em desktop continuaram sendo as que sofrem a maior taxa de ataques.	Apesar do alto volume de ataques, as taxas gerais foram extremamente baixas, impulsionadas pelo grande número de operações repetidas e de confiança. As operações de pagamento foram exceção, pois continuaram sendo atacadas com maior frequência do que os outros setores.	As taxas de ataques no comércio eletrônico permaneceram relativamente baixas e continuam caindo. Uma queda modesta no volume de bots automatizados.	Criações de novas contas e logins atacados com mais frequência do que em qualquer outro setor. Forte crescimento no volume de bots automatizados atacando plataformas de mídias sociais, sites de streaming e operações de jogos eletrônicos e de azar.
TAXA DE ATAQUES				
GERAL	3,5%	3,1%	3,4%	6,0%
DESKTOP	**3,52%**	2,9%	**3,9%**	**6,2%**
MÓVEL	3,5%	**3,14%**	3,2%	5,9%

© 2022 LEXISNEXIS RISK SOLUTIONS

SERVIÇOS FINANCEIROS NA LATAM: PANORAMA DAS TENDÊNCIAS E PADRÕES DE ATAQUE

As operações de pagamento de serviços financeiros continuaram registrando a taxa mais alta de ataques entre todos os setores.

PANORAMA DOS SERVIÇOS FINANCEIROS	CRIAÇÃO DE NOVAS CONTAS	LOGINS	PAGAMENTOS
TENDÊNCIAS DE RISCO	Queda significativa no volume/ocorrências de ataques em aplicativos móveis devido ao grande número de investidas de bots a criações de novas contas em aplicativos móveis em janeiro de 2020, o que levou a um enorme pico nesse período. No entanto, foi registrado crescimento nas taxas de ataques em operações em navegadores para desktops e dispositivos móveis.	A taxa geral de ataques a operações de acesso permaneceu baixa graças ao alto volume de operações regulares de clientes confiáveis. Continuou sendo muito mais seguro acessar uma conta de serviços financeiros de um aplicativo móvel do que de um desktop.	Embora as operações de pagamento de serviços financeiros tenham sofrido uma taxa maior de ataques do que os outros setores, esse número continuou em queda em todos os outros. As operações em navegadores para desktops e dispositivos móveis foram atacadas com mais frequência do que as realizadas em aplicativos móveis, com pagamentos fraudulentos representando uma oportunidade importante para os fraudadores ganharem ou movimentarem dinheiro entre contas mulas no ambiente dos serviços financeiros.
TAXA DE ATAQUES			
GERAL	4,5%	2,0%	7,9%
DESKTOP	**6,6%**	1,8%	6,9%
NAVEGADORES MÓVEIS	5,7%	0,7%	4,6%
APLICATIVOS MÓVEIS	2,7%	**2,1%**	**12,4%**

© 2022 LEXISNEXIS RISK SOLUTIONS

A ASCENSÃO DOS BANCOS DIGITAIS

Análise da mudança do comportamento do consumidor nos bancos tradicionais e digitais.

Os bancos digitais oferecem todos os produtos e serviços online e não possuem rede de agências.

Por vezes, são submarcas de bancos tradicionais, mas costumam operar de forma totalmente independente do modelo bancário tradicional.

Cada vez mais, eles ajudam a facilitar a inclusão financeira das populações não bancarizadas e com acesso limitado aos serviços bancários em economias em crescimento, já que muitos priorizam os aplicativos móveis em detrimento às operações realizadas em navegadores.

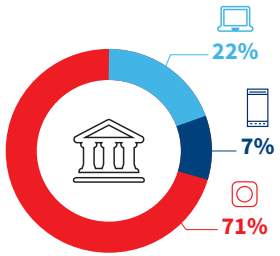
CRESCIMENTO ANO A ANO NO VOLUME DE OPERAÇÕES

37%
Bancos tradicionais

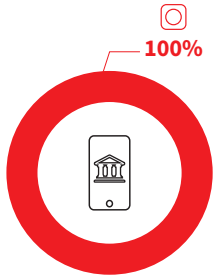
68%
Bancos digitais

PREFERÊNCIA DE CANAL

APLICATIVOS MÓVEIS · DESKTOP · NAVEGADORES MÓVEIS



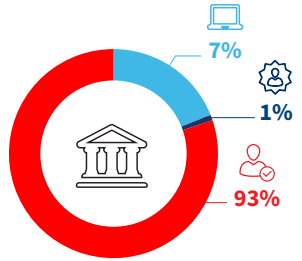
Bancos tradicionais
Combinação de operações em desktop e móveis



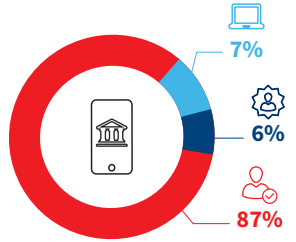
Bancos digitais
Todas as operações em aplicativos móveis

PERFIL DAS OPERAÇÕES

ACESSO À CONTA · PAGAMENTOS · ABERTURA DE NOVAS CONTAS



Bancos tradicionais
Baixa taxa de criação de novas contas



Bancos digitais
Maior volume de abertura de novas contas à medida que os consumidores migram para um modelo exclusivamente digital

© 2022 LEXISNEXIS RISK SOLUTIONS

LexisNexis® RISK SOLUTIONS

O COMÉRCIO ELETRÔNICO NA LATAM: PANORAMA DAS TENDÊNCIAS E PADRÕES DE ATAQUE

As taxas de ataques continuaram em queda conforme os comerciantes reforçaram os controles.

PANORAMA DO COMÉRCIO ELETRÔNICO	CRIAÇÃO DE NOVAS CONTAS	LOGINS	PAGAMENTOS
TENDÊNCIAS DE RISCO	A criação de novas contas em desktop continuaram sendo atacadas a uma frequência maior do que qualquer outro caso de uso, com mais de uma em cada 10 operações identificadas como um ataque em potencial. Embora a taxa geral de ataque tenha permanecido baixa, houve um aumento significativo ano a ano nas investidas de bots na criação de novas contas.	Embora o setor de comércio eletrônico tenha sofrido um volume maior de tentativas de invasão a contas em comparação aos serviços financeiros, as taxas gerais de ataques permaneceram relativamente baixas e estão diminuindo em todos os canais ano a ano.	As operações de pagamento na jornada do cliente de comércio eletrônico representaram uma oportunidade para os fraudadores monetizarem com credenciais roubadas. Entretanto, a taxa geral de ataques tem apresentado queda, o que indica que os comerciantes estão implementando autenticação e estratégias de autorização robustas para avaliar o risco de operações de pagamento.
TAXA DE ATAQUES			
GERAL	9,5%	3,7%	3,2%
DESKTOP	**15,1%**	**7,2%**	1,7%
NAVEGADORES MÓVEIS	8,9%	3,6%	2,3%
APLICATIVOS MÓVEIS	0,7%	0,9%	**4,2%**

© 2022 LEXISNEXIS RISK SOLUTIONS

MÍDIA: PANORAMA DAS TENDÊNCIAS E PADRÕES DE ATAQUE

Organizações de mídia atingidas por onda de ataques de bots testando as credenciais roubadas.

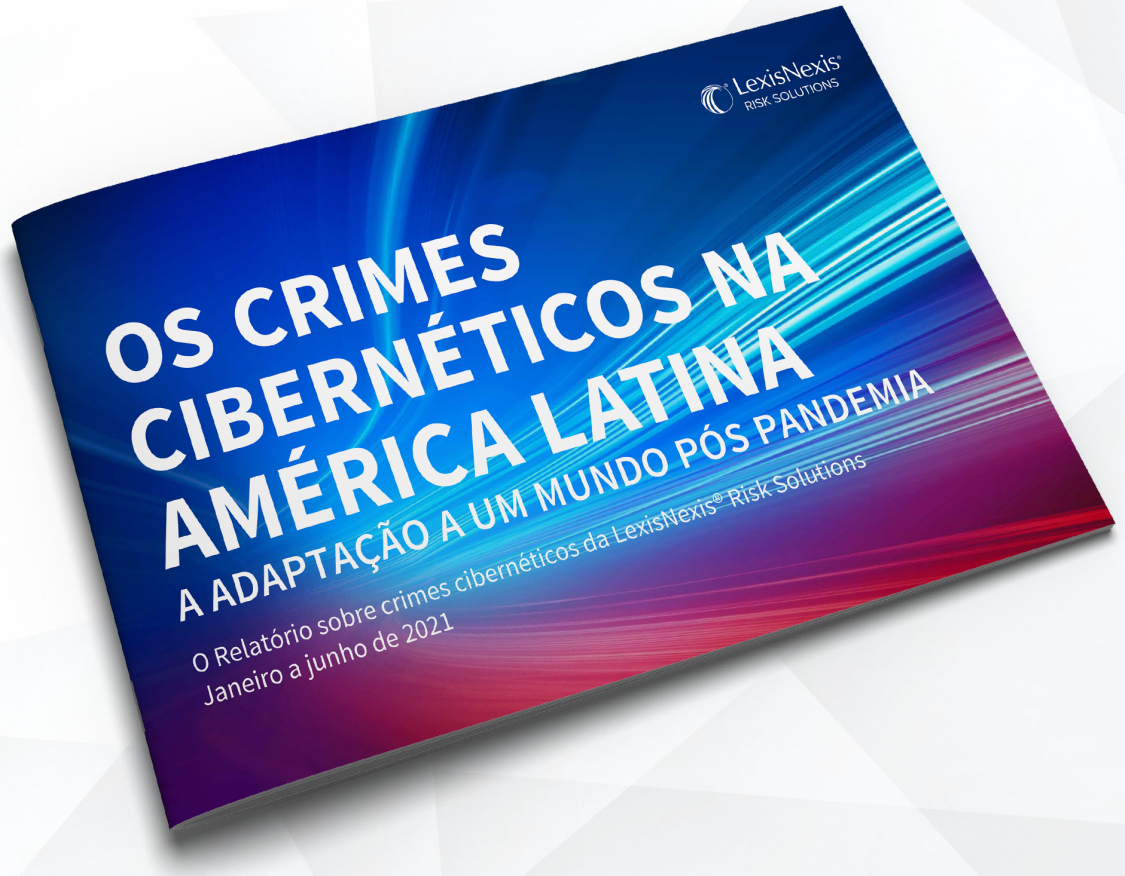
PANORAMA DE MÍDIA	CRIAÇÃO DE NOVAS CONTAS	LOGINS	PAGAMENTOS
TENDÊNCIAS DE RISCO	Embora as ocorrências de ataques para a criação de novas contas tenha caído, elas permaneceram mais altas para organizações de mídia do que qualquer outro setor. É provável que muitas dessas tentativas de criação de novas contas tenha sido realizada por fraudadores testando dados de identidades roubados em empresas que costumam apresentar menos barreiras de entrada. Tentativas são feitas para obter vantagens do bônus para novos clientes ou para revender períodos de teste com o intuito de obter ganhos financeiros.	A taxa geral de ataques é um pouco maior para as organizações de mídia do que para outros setores, embora também tenha apresentado queda. Entretanto, a taxa de ataques a aplicativos móveis permaneceu alta, representando um ponto de risco chave para invasão a contas de mídia. A maioria dos volumes de ataques de bots a mídia tiveram como alvo operações de login, para testar credenciais roubadas.	As taxas de ataque a pagamentos de mídia foram mais baixas do que em outros setores, provavelmente porque representam menos oportunidade de lucros em comparação aos pagamentos de comércio eletrônico ou de serviços financeiros.
TAXA DE ATAQUES			
GERAL	14,0%	0,5%	11,2%
DESKTOP	**17,7%**	0,4%	10,8%
NAVEGADORES MÓVEIS	13,6%	0,1%	**11,7%**
APLICATIVOS MÓVEIS	4,3%	**1,3%**	2,5%

© 2022 LEXISNEXIS RISK SOLUTIONS

BAIXE O RELATÓRIO GLOBAL COMPLETO

O Relatório sobre Crimes Cibernéticos LATAM é um suplemento ao Relatório Global sobre Crimes Cibernéticos da LexisNexis® Risk Solutions, que tem como base os ataques de crimes cibernéticos detectados pelo LexisNexis Digital Identity Network, de janeiro a junho de 2021. Desde os riscos globais e as oportunidades do setor até a análise do cenário dos crimes cibernéticos numa pandemia, o Relatório Global sobre Crimes Cibernéticos irá ajudá-lo a enfrentar as fraudes e conquistar a confiança de clientes genuínos.

Baixe grátis aqui:
risk.lexisnexis.com.br/insights-resources/research/cybercrime-report



© 2022 LEXISNEXIS RISK SOLUTIONS

LexisNexis®
RISK SOLUTIONS

PARA MAIS INFORMAÇÕES:

risk.lexisnexis.com/fraudes

risk.lexisnexis.com.br/insights-resources/research/cybercrime-report

risk.lexisnexis.com.br/products/threatmetrix

Sobre a LexisNexis® Risk Solutions

A LexisNexis® Risk Solutions utiliza o poder dos dados e das análises avançadas para fornecer informações que ajudam empresas e governos a reduzir risco e melhorar a tomada de decisões, beneficiando pessoas no mundo todo. Fornecemos soluções de dados e de tecnologia para uma grande variedade de setores, inclusive de seguros, serviços financeiros, assistência médica e governos. Com sede na área metropolitana de Atlanta, Georgia, EUA, contamos com escritórios por todo o planeta e fazemos parte do RELX (LSE: REL/NYSE:RELX), fornecedor global de análises baseadas em informações e ferramentas de tomada de decisão para clientes profissionais e empresas.

Este documento tem somente fins educativos e não garante a funcionalidade e os recursos dos produtos identificados da LexisNexis. A LexisNexis® não garante que este documento esteja completo e sem erros. Se escrito por terceiros, as opiniões podem não refletir as da LexisNexis® Risk Solutions.

LexisNexis, a logomarca Knowledge Burst e LexID são marcas comerciais registradas da RELX Inc. ThreatMetrix e Digital Identity Network são marcas comerciais registradas da ThreatMetrix, Inc. Emailage é uma marca comercial registrada da Emailage Corp. Outros produtos e serviços podem ser marcas comerciais ou marcas comerciais registradas de suas respectivas empresas. Copyright © 2022 LexisNexis Risk Solutions Group. NXR15337-00-0122-PT

Para mais informações, acesse risk.lexisnexis.com, and relx.com