LexisNexis®
RISK SOLUTIONS

O NOVO CENÁRIO DOS CRIMES CIBERNÉTICOS

RISCOS GLOBAIS, TENDÊNCIAS REGIONAIS, OPORTUNIDADES DOS SETORES

O Relatório sobre crimes cibernéticos da LexisNexis® Risk Solutions
Julho a dezembro de 2020

01 INTRODUÇÃO:

ÍNDICE

01 **INTRODUÇÃO:** 2

A mudança global sem precedentes criou novas oportunidades para os criminosos cibernéticos 3

2020: Retrospectiva completa do ano 5

O CENÁRIO DOS CRIMES CIBERNÉTICOS: ANÁLISE DE JULHO A DEZEMBRO DE 2020

02 Riscos globais 6

03 A jornada do cliente 21

04 Tendências regionais 26

05 Oportunidades dos setores 37

06 **OS CRIMES CIBERNÉTICOS EM UMA PANDEMIA:** 45

Tendências dos clientes e tipologias de fraudes 46

Risco de fraude por idade 48

07 **CONCLUSÃO:** 50

Previsões para o próximo ano: As oportunidades para os negócios digitais 51

08 **GLOSSÁRIO, METODOLOGIA, INFORMAÇÕES PARA CONTATO** 52

A MUDANÇA GLOBAL SEM PRECEDENTES CRIOU NOVAS OPORTUNIDADES PARA OS CRIMINOSOS CIBERNÉTICOS

Em um ano de mudanças irreversíveis, os criminosos cibernéticos mantiveram-se consistentes buscando novas oportunidades, isolando os alvos que proporcionam os maiores ganhos e colocando pressão adicional sobre empresas globais, que foram forçadas a se adaptar e evoluir diante de uma demanda sem precedentes.

Diversas novas linhas de crédito sofreram ataques. Os fraudadores também se aproveitaram do nervosismo dos clientes dando golpes relacionados à pandemia, oferecendo produtos e serviços com alta procura ou baixa oferta. A Pymnts.com, por exemplo, afirmou que as taxas de fraudes aumentaram 55% desde o começo da pandemia*, enquanto no Reino Unido, a Experian relatou alta de 33% durante o primeiro lockdown da Covid-19 em abril**.

Entretanto, esse crescimento não foi registrado em todos os negócios digitais. Muitas plataformas consolidadas apresentaram queda no volume de ataques durante 2020. Foi o caso das organizações que fazem parte do LexisNexis® Digital Identity Network®, que vivenciaram redução significativa no número de ataques em comparação ao ano anterior. Defesas antifraudes bem consolidadas e em camadas representaram uma grande barreira aos criminosos cibernéticos que, por sua vez, parecem ter voltado a atenção para as novas oportunidades criadas pela pandemia global.

Apesar da queda registrada pelas empresas do Digital Identity Network® nas taxas de ataques, vetores perigosos ainda persistiram:

- Ataques de *bots* automatizados continuaram bastante comuns, registrados em todas as regiões globais e atingindo uma grande variedade de setores e casos de uso, com o objetivo de testar credenciais de identidade em massa, oferecendo uma forma de ataque inicial barata, rápida e eficaz aos fraudadores.
- Da mesma forma, criações de novas contas continuam sofrendo altos índices de ataques, representando um ponto de entrada importante para fraudadores em busca de lucros a partir de credenciais coletadas de violações de dados.

A pandemia aumentou o número de usuários online. Uma nova análise neste relatório mostra que a faixa etária mais jovem, menos de 25 anos, é a mais vulnerável a ataques de fraudes, enquanto a mais velha é a que apresenta as maiores perdas. Esse grande risco nas extremidades do espectro coloca a necessidade de proteger os clientes novos e vulneráveis no topo da lista de prioridades de todos os negócios digitais globais.

** https://www.pymnts.com/fraud-prevention/2021/swap-data-analytics-holiday-fraud/*
*** https://www.experianplc.com/media/news/2020/fraud-rate-rises-33-during-covid-19-lockdown/*

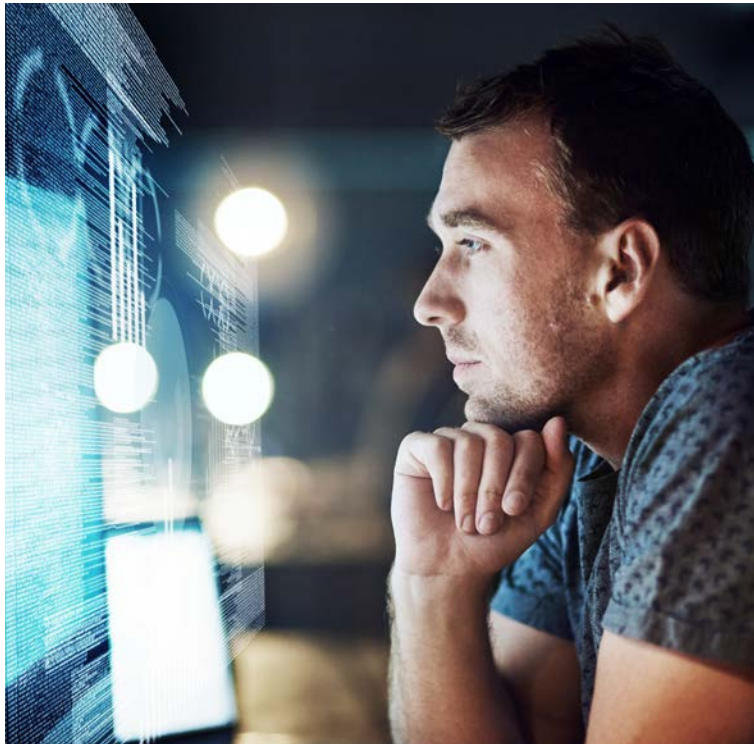
A MUDANÇA GLOBAL SEM PRECEDENTES CRIOU NOVAS OPORTUNIDADES PARA OS CRIMINOSOS CIBERNÉTICOS

Independente das muitas incertezas que as empresas enfrentarão em 2021, elas podem ter a convicção de que seus usuários finais continuarão exigindo acesso a produtos e serviços onde e quando quiserem:

- Empresas de comércio eletrônico, por exemplo, devem tentar priorizar experiências do cliente holísticas e omnicanais. Os caminhos de compra estão convergindo cada vez mais, à medida que as experiências na loja física são substituídas ou combinadas às ofertas digitais. Reconhecer o cliente em toda essa jornada se tornou mais importante do que nunca.
- De maneira semelhante, a diversificação das soluções de pagamento digital, que evoluem para atender à crescente demanda dos consumidores, coloca o ônus em métodos de autenticação confiáveis, que consigam identificar o uso de credenciais roubadas e falsificadas.

Nesse cenário dinâmico, a inteligência de identidade digital surge como um dos ativos mais preciosos, tanto para os clientes como para as empresas. Identidades digitais online podem adaptar-se e evoluir de acordo com as operações realizadas por consumidores individuais na internet, construindo uma pegada digital do comportamento, histórico e inteligência de dispositivo.

Quando essa inteligência é colaborativa entre as empresas digitais globais e atualizada em tempo quase real, ela oferece uma visão incomparável de confiança e risco. Para os consumidores, isso significa uma experiência online sem atrito, já que as empresas conseguem reconhecer melhor os seus clientes recorrentes e confiáveis e, ao mesmo tempo, identificar comportamentos não compatíveis a estes. Quando combinada a identidade física, soluções de autenticação e dados de biometria comportamental, essa abordagem pode fornecer uma forte estratégia de combate a fraudes preparada para o futuro.



2020: RETROSPECTIVA COMPLETA DO ANO

Um resumo das operações e ataques de janeiro a dezembro de 2020

A mudança que forçou os consumidores a migrarem aos canais digitais gerou um rápido crescimento nas operações confiáveis, com um declínio geral de ataques a empresas no Digital Identity Network. As economias em crescimento contribuíram com a maior alta no volume de ataques. A avaliação abaixo representa um resumo dos padrões de operação e ataques no ano.

OPERAÇÕES PROCESSADAS

47.1 bi — 35.5 bi em 2019

Penetração de operações móveis:

67% — 65% em 2019

ATAQUES INICIADOS POR HUMANOS

495 mi — 679 mi em 2019

Taxa de ataques originados em dispositivos móveis:

56% — 55% em 2019

Maiores atacantes por volume:

Estados Unidos

Maior crescimento de ataques:

1. Guatemala
2. Barém
3. Zimbábue

ATAQUES DE *BOTS* AUTOMATIZADOS

2.1 bi — 2.0 bi em 2019

Maiores atacantes por volume:

Estados Unidos

Maior crescimento de ataques:

1. Ilha de Man
2. Emirados Árabes
3. Nigéria

SPOOFING DE IDENTIDADE

Vetor de ataque mais prevalente

02

O CENÁRIO DOS CRIMES CIBERNÉTICOS:
JULHO-DEZEMBRO DE 2020
RISCOS GLOBAIS

DESTAQUES GLOBAIS: JULHO-DEZEMBRO DE 2020

OPERAÇÕES

+29% ▲

Crescimento ano a ano (a.a.) no volume das operações globais:

- **+29%** ▲ **Crescimento** nas operações de serviços financeiros.
- **+38%** ▲ **Crescimento** nas operações de comércio eletrônico.
- **+9%** ▲ **Crescimento** nas operações de mídia.

ATAQUES INICIADOS POR HUMANOS

-58% ▼

Redução a.a. na taxa de ataques iniciados por humanos:

- **-58%** ▼ **Redução** na taxa de ataques a serviços financeiros.
- **-58%** ▼ **Redução** na taxa de ataques ao comércio eletrônico.
- **-54%** ▼ **Redução** na taxa de ataques à mídia.

ATAQUES DE *BOTS* AUTOMATIZADOS

-2% ▼

Redução a.a. nos ataques de *bots* automatizados:

- **-8%** ▼ **Redução** no volume de *bots* nos serviços financeiros.
- **+32%** ▲ **Crescimento** no volume de *bots* no comércio eletrônico.
- **+10%** ▲ **Crescimento** no volume de *bots* na mídia.

AS TENDÊNCIAS DAS OPERAÇÕES GLOBAIS EM NÚMEROS

A Covid-19 criou novas oportunidades para negócios digitais e levou mais clientes para a internet

OPERAÇÕES

Nos últimos seis meses de 2020, o volume de operações manteve forte crescimento no Digital Identity Network, à medida que empresas e clientes continuaram migrando para a internet.

Entretanto, o número de criação de novas contas caiu em comparação ao ano anterior, o que se deu principalmente por conta do grande volume de ataques a criação de novas contas tendo os serviços financeiros como alvo no final de 2019.

Os dispositivos móveis continuaram facilitando o amplo acesso a bens e serviços, originando quase 7 de cada 10 operações.

As empresas precisarão priorizar progressivamente não apenas a estratégia *digital-first* como também a *mobile-first* para atender aos consumidores que raramente usam ou não têm acesso a um dispositivo desktop.

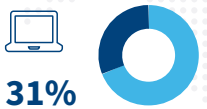
OPERAÇÕES PROCESSADAS JULHO-DEZEMBRO DE 2020

24.6 bi

Crescimento a.a.
+29% ▲

OPERAÇÕES CLASSIFICADAS POR CANAL

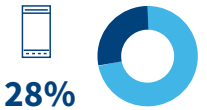
Desktop / Mobile



31% **69%**

Crescimento a.a.
+2% ▲

Navegadores / **aplicativos móveis**



28% **72%**

OPERAÇÕES CLASSIFICADAS POR CASO DE USO*

	Crescimento/ Queda a.a.
Criação de novas contas	495 mi — **-43% ▼**
Logins	17 bi — **+26% ▲**
Pagamentos	4.3 bi — **+34% ▲**

O volume restante das operações é composto de casos de uso não essenciais como redefinição de senha e alteração de dados.

AS TENDÊNCIAS DOS ATAQUES GLOBAIS EM NÚMEROS

O volume de ataques continuou caindo no Digital Identity Network®

ATAQUES

ATAQUES INICIADOS POR HUMANOS

Apesar dos inúmeros riscos de fraudes publicados na mídia, as organizações no Digital Identity Network apresentaram queda no volume de ataques sofridos entre julho e dezembro de 2020.

As operações realizadas nos navegadores para dispositivos móveis continuaram sendo o maior alvo de ataques, enquanto as em aplicativos para dispositivos móveis o menor.

VOLUME DE ATAQUES

235 mi — Queda a.a. **-42% ▼**

Ataques classificados por desktop / dispositivos móveis

44% 56%

A taxa de ataques originados em dispositivos móveis tem caído ano a ano

-16% ▼

TAXA DE ATAQUES

		Queda a.a.
Geral	1,1%	-58% ▼
Desktop	1,6%	-41% ▼
Navegadores móveis	2,3%	-45% ▼
Aplicativos móveis	0,4%	-79% ▼

ATAQUES DE *BOTS* AUTOMATIZADOS

Os setores de comércio eletrônico e de mídia apresentaram crescimento no volume de *bots* automatizados entre julho e dezembro de 2020.

Embora as organizações de serviços financeiros tenham observado um declínio geral nos *bots*, o volume absoluto tendo como alvo outros setores permaneceu extremamente alto.

VOLUME DE ATAQUES

1.2 bi — Queda a.a. **-2% ▼**

		Crescimento/Queda a.a.
Serviços Financeiros	812 mi	-8% ▼
Comércio Eletrônico	207 mi	+32% ▲
Mídia	170 mi	+10% ▲

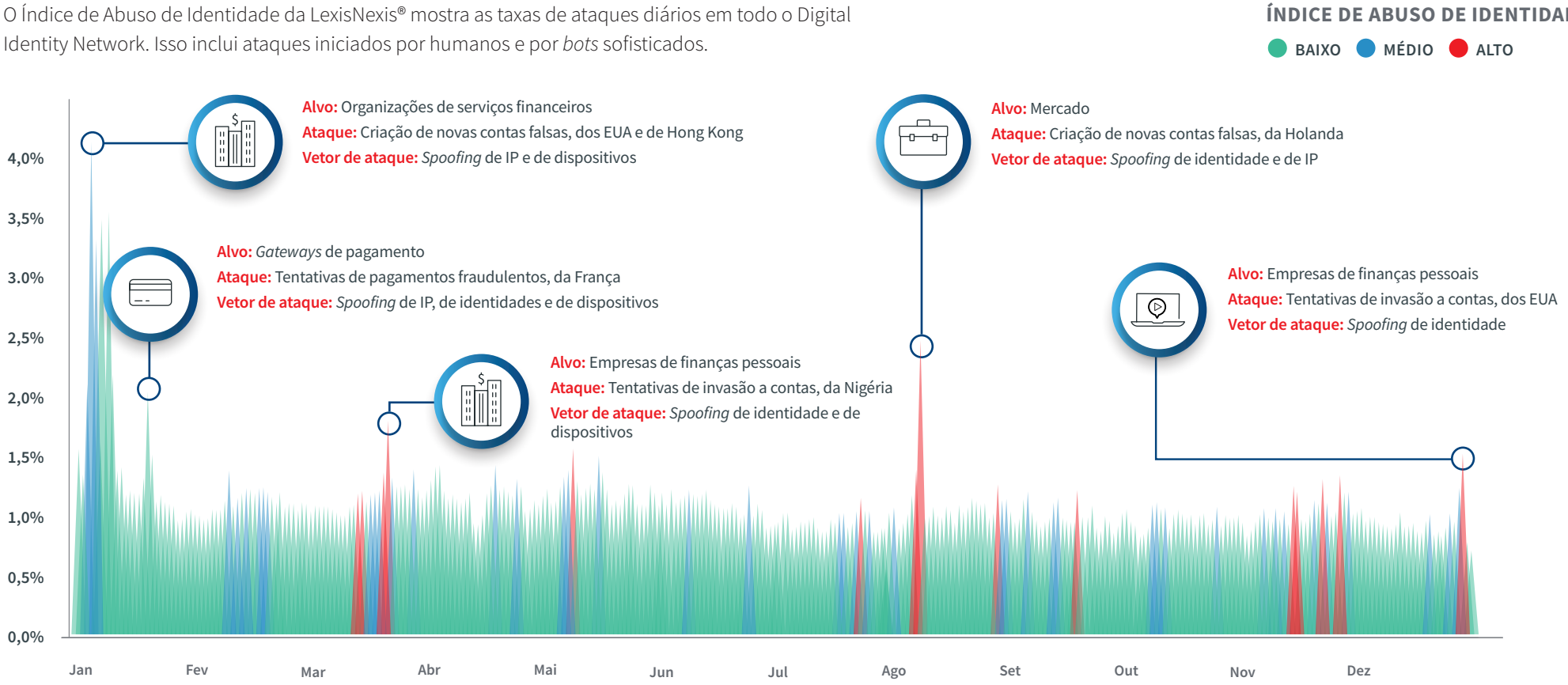
Os ataques no Digital Identity Network® são classificados em ataques iniciados por humanos, que costumam resultar em dados completos de definição de perfis de identidade digital relacionados a ocorrências individuais, e ataques de bots automatizados em alta velocidade.

LexisNexis® RISK SOLUTIONS

O ÍNDICE DE ABUSO DE IDENTIDADE

Os *bots* continuaram sendo o método usado nos testes de identidade em todo o espectro de casos de uso

O Índice de Abuso de Identidade da LexisNexis® mostra as taxas de ataques diários em todo o Digital Identity Network. Isso inclui ataques iniciados por humanos e por *bots* sofisticados.



Um nível alto no Índice de Abuso de Identidade (em vermelho) representa uma taxa de ataque de dois desvios padrões da tendência média.

OS MAIORES CONTRIBUIDORES DE ATAQUES INICIADOS POR HUMANOS, POR VOLUME

A Arábia Saudita entrou para a lista dos 10 maiores atacantes por país de região

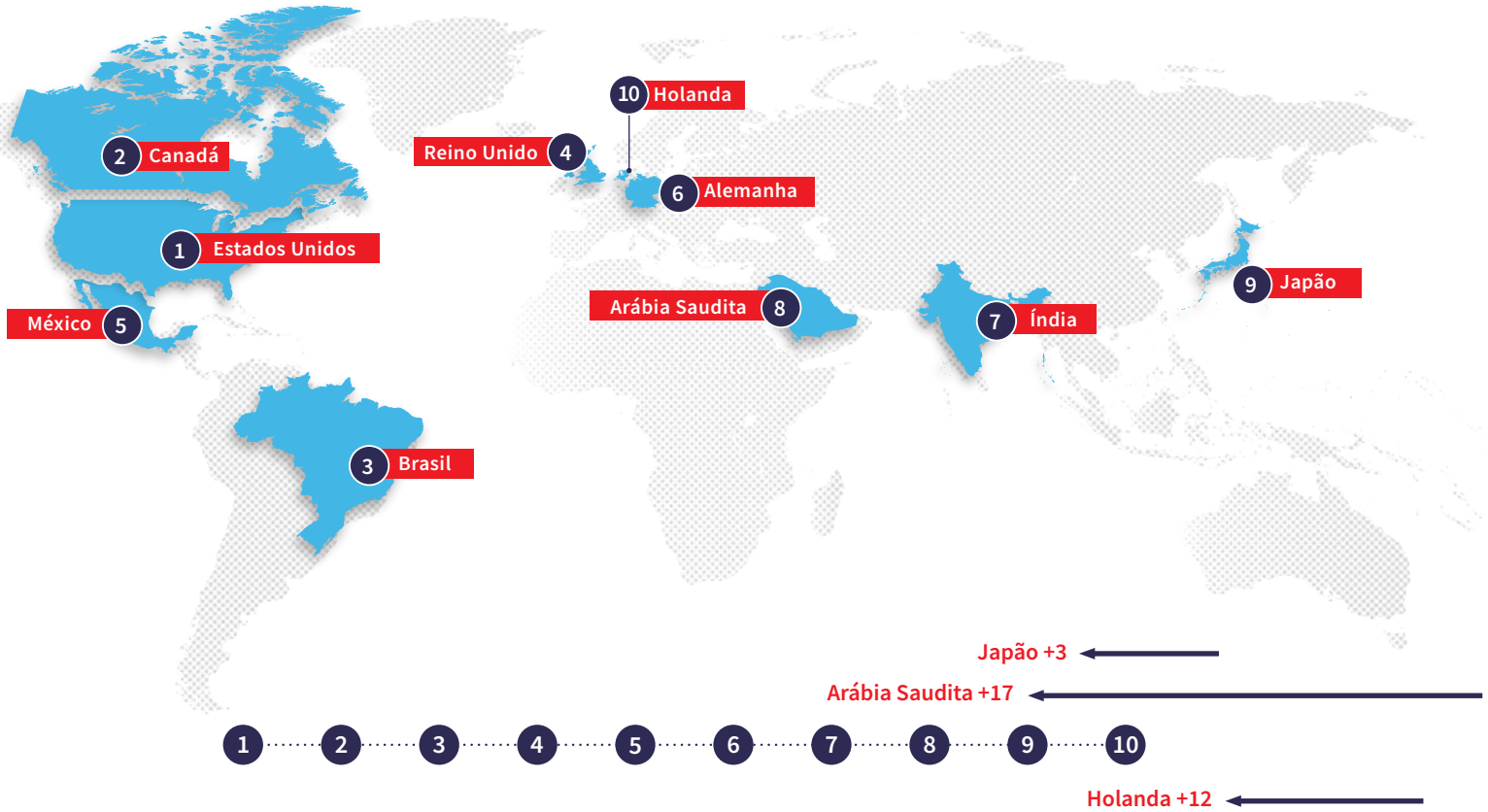
Ataques iniciados por humanos

Os EUA, Canadá e Reino Unido têm sido os atacantes mais consistentes entre os 5 principais nos últimos anos e continuam acompanhados de diversas economias menores em crescimento e novas potências regionais.

O Brasil e o México permaneceram entre os 5 principais atacantes globais por país de região. O México estreou na lista em 2019, consolidando a LATAM como uma região geradora de um alto volume de ataques cibernéticos.

Em comparação ao mesmo período do ano anterior:

- A Arábia Saudita subiu 17 posições na lista.
- A Holanda subiu 12 posições na lista.
- O Japão subiu 3 posições na lista.



AS MAIORES ORIGENS DE ATAQUES DE *BOTS* AUTOMATIZADOS, POR VOLUME

A Irlanda, Austrália e Holanda registraram aumento significativo na geração de ataques de *bots* em comparação ao ano anterior

Ataques de *bots* automatizados

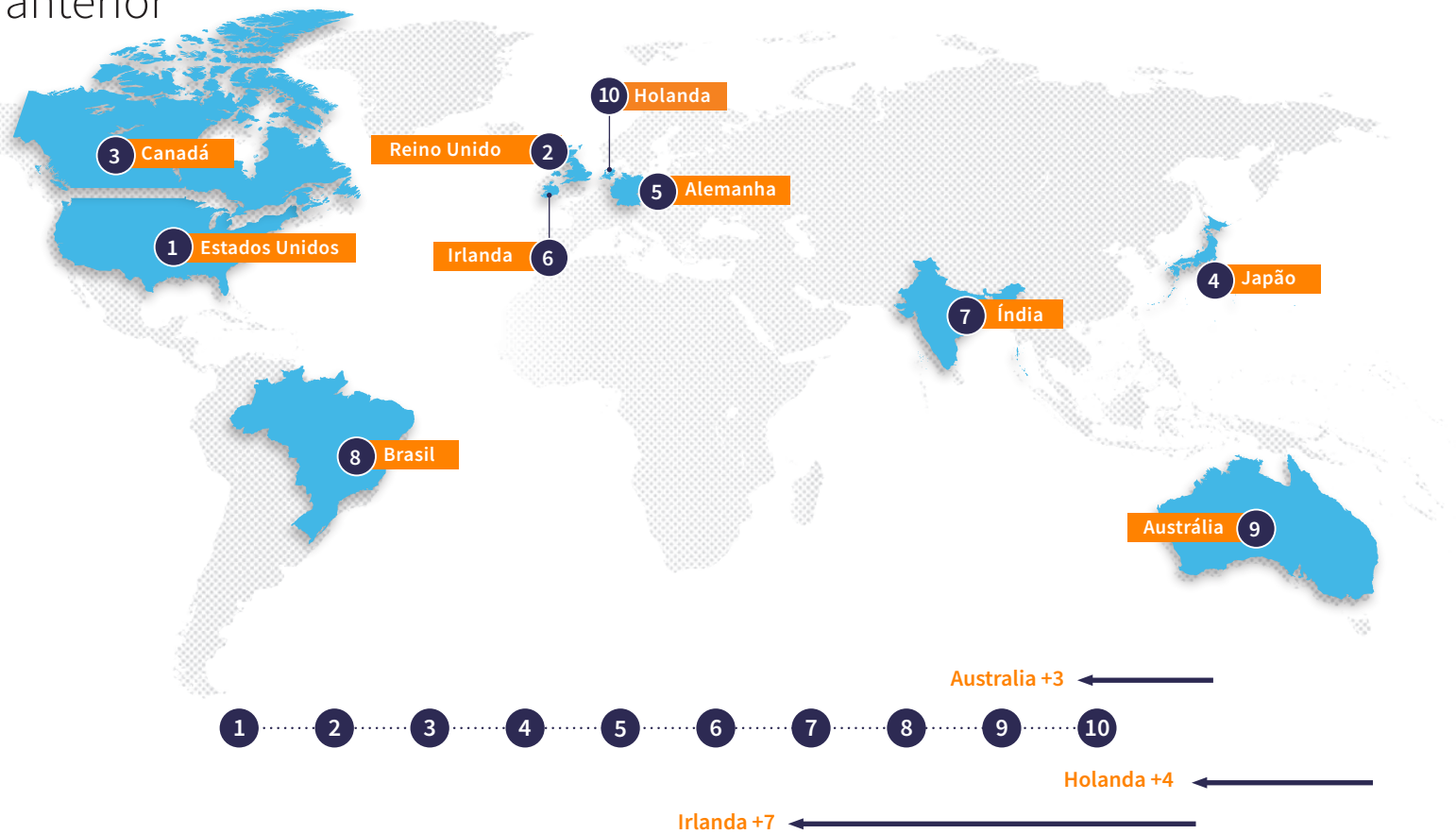
O Brasil voltou à lista dos 10 principais países de onde ataques de *bots* têm origem, depois de ficar ausente na primeira metade de 2020.

O reaparecimento do país como um importante local de procedência desse tipo de ataque significa que as quatro regiões globais voltaram a ser representadas entre os 10 principais.

APAC, LATAM e América do Norte registraram aumento no volume de *bots* entre julho e dezembro de 2020, em comparação à primeira metade do ano.

Em comparação ao mesmo período do ano anterior:

- Irlanda subiu 7 posições na lista.
- Holanda subiu 4 posições na lista.
- Austrália subiu 3 posições na lista.



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

As redes hiperconectadas continuaram atacando diversos setores e organizações

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

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.

Os dispositivos associados a ocorrências confirmadas de fraudes devem estar ligados aos mesmos indivíduos ou organizações de fraudadores, já que o hardware não é compartilhado da mesmo forma que dados roubados.

A análise neste relatório inclui:

- As principais ligações entre dispositivos e dados de identidade roubados, inclusive endereços de e-mail e números de telefone.
- O volume de operações que compõem as redes fraudulentas, ilustrando o tamanho e a escala do comportamento fraudulento.
- A atribuição de valores monetários à toda rede de fraude com base em valores conhecidos de operações de pagamento.

O Digital Identity Network permite que as organizações compartilhem inteligência relacionada a ocorrências de fraudes para que uma entidade marcada como sendo de alto risco ou fraudulenta por uma instituição possa ser revisada pelas outras antes que mais operações sejam processadas.

GRANDES REDES DE SERVIÇOS FINANCEIROS NORTE-AMERICANAS CARREGAM MARCAS DE ATIVIDADES “MULAS”

A próxima página mostra a movimentação de uma rede de fraudes atacando o setor de serviços financeiros, operando em diversas organizações nos EUA e Canadá.

Cada flecha ilustra uma entidade associada a uma ocorrência confirmada de fraude em uma organização passando para outra no Digital Identity Network.

Entidades analisadas como parte dessa rede incluem dispositivos, endereços de e-mail e números de telefone. Entretanto, houve um forte padrão de fraudes ligadas a dispositivos, o que sugere o mesmo fraudador ou organização fraudulenta operando em diversos bancos, carteiras digitais e organizações credoras.

Esse padrão de fraudes é característico de comportamento de “mula”, já que os “pastores” movimentam dinheiro entre diversas contas para evitar serem detectados.

A REDE EM NÚMEROS

+100.000

Ocorrências associadas para confirmar fraudes registradas em uma organização de origem.

Pelo menos US $1.5 mi

Fraudes bloqueadas.

+500.000

Ocorrências registradas em outras organizações no Digital Identity Network associadas a um dispositivo, endereço de e-mail e/ou número de telefone envolvidos nesses eventos fraudulentos nas organizações de origem.

Pelo menos US$ 8.7 mi

Exposição monetária a fraudes em toda a rede. Algumas dessas operações podem ter sido bloqueadas por organizações na rede que não compartilham dados sobre fraudes.

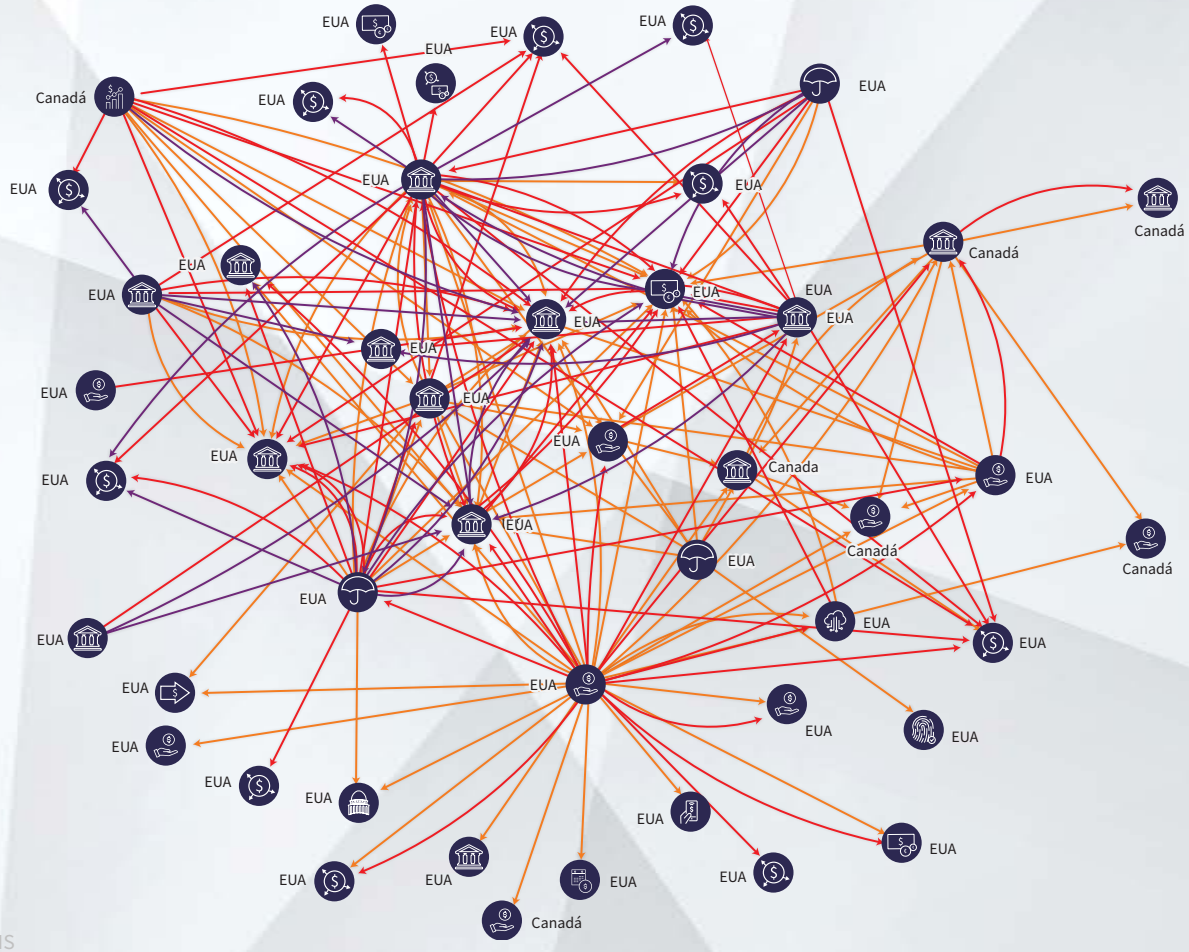
Veja a rede de fraudes na próxima página.

América do Norte inclui EUA e Canadá. México faz parte da região da LATAM.

A REDE DE FRAUDES NORTE-AMERICANA EXIBIU FORTE PADRÃO DE FRAUDES INTERORGANIZACIONAIS COM BASE EM DISPOSITIVO

ENTIDADES:

- **DISPOSITIVO**
- **E-MAIL**
- **TELEFONE**



SERVIÇOS FINANCEIROS

- GATEWAYS DE PAGAMENTO
- FINANÇAS PESSOAIS
- GOVERNO
- EMPRÉSTIMOS
- CORRETORA DE BOLSA DE VALORES
- SEGUROS
- CARTEIRA DIGITAL
- BANCOS
- VERIFICAÇÃO DE IDENTIDADE
- REMESSA
- FOLHA DE PAGAMENTO

Menos de 100 sobreposições de entidades entre empresas foram excluídas.

América do Norte inclui EUA e Canadá. México faz parte da região de LATAM.

A REDE DE FRAUDES DE PAGAMENTO REGISTRADA EM DIVERSAS ORGANIZAÇÕES DE COMÉRCIO ELETRÔNICO NA EMEA

A próxima página mostra a movimentação de uma rede de fraudes atacando o setor de comércio eletrônico, operando em:

- Varejistas, um mercado e gateway de pagamento na Alemanha
- Um varejista e um agente de viagens na França
- Um varejista na Holanda
- Um mercado na Espanha
- Um programa de fidelidade nos Emirados Árabes
- Um varejista na Letônia
- Um varejista na Itália

Como na rede anterior, cada flecha ilustra uma entidade associada a uma ocorrência confirmada de fraude em uma organização passando para outra no Digital Identity Network. Entretanto, essa rede de fraudes sofre uma maior proliferação de ocorrência de fraudes conectadas por endereços de e-mail.

Isso mostra grupos de fraudadores trabalhando juntos para atacar diversos varejistas, usando credenciais roubadas compartilhadas.

A REDE EM NÚMEROS

+2.000

Ocorrências associadas para confirmar fraudes registradas em uma organização de origem.

+3.000

Ocorrências registradas em outras organizações no Digital Identity Network associadas a um dispositivo, endereço de e-mail e/ou número de telefone envolvidos nessas ocorrências nas organizações de origem.

Pelo menos US$ 750 mil

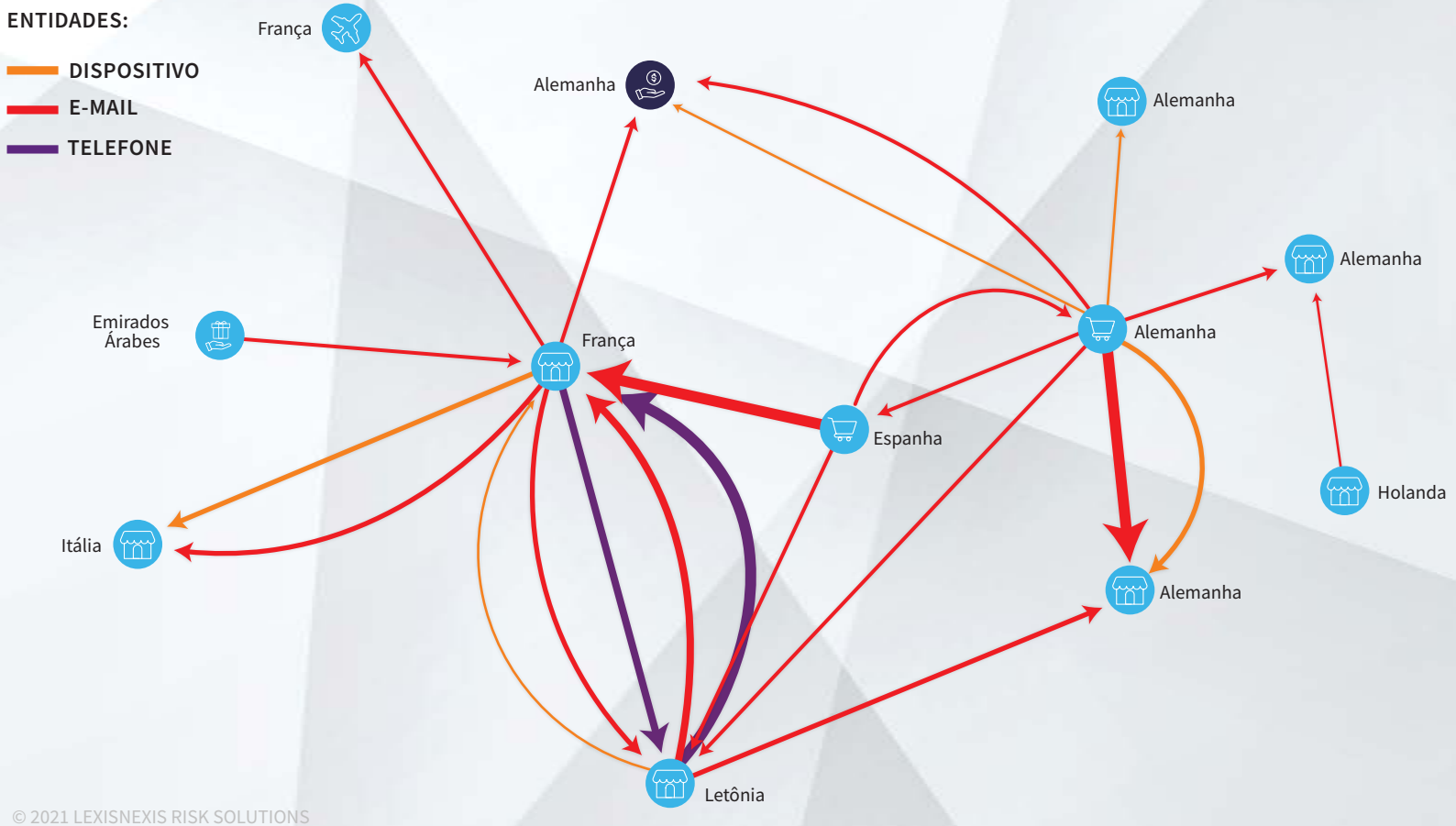
Fraudes bloqueadas.

Pelo menos US$ 250 mil

Exposição monetária a fraudes em toda a rede. Algumas dessas operações podem ter sido bloqueadas por organizações na rede que não compartilham dados sobre fraudes.

Veja a rede de fraudes na próxima página.

CREDENCIAIS ROUBADAS COMPARTILHADAS USADAS POR GRUPOS DE CRIMINOSOS CIBERNÉTICOS PARA INVASÃO A CONTAS E PAGAMENTOS FRAUDULENTOS



SERVIÇOS FINANCEIROS

- GATEWAY DE PAGAMENTO

COMÉRCIO ELETRÔNICO

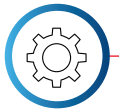
- MERCADO
- PROGRAMA DE FIDELIDAE
- VAREJISTA
- VIAGEM

Essa rede de fraudes só mostra conexões de mais de 10 entidades.
As linhas mais grossas representam um volume maior de fraudes.

DESTAQUE: ANÁLISE DO IMPACTO DE ENDEREÇOS DE E-MAILS VIOLADOS NO DIGITAL IDENTITY NETWORK

FRAUDE:
Ataques de teste de identidade em várias organizações do Digital Identity Network usando endereços de e-mail aparentemente roubados. A maioria dos domínios dos e-mails é genuína (gmail.com, hotmail.com, yahoo.com), o que indica que esses endereços foram provavelmente roubados de clientes reais em vez de terem sido criados sinteticamente.

ALVO:
Um operador de jogos eletrônicos e de azar, um varejista e uma companhia aérea.



MÉTODO:
Grande volume de ataques de *bots* testando diversos endereços de e-mail em ataques curtos e constantes.

ATAQUE:

- Companhia aérea 13 mil tentativas de invasão a contas associadas a 3.200 e-mails roubados.
- Operador de jogos eletrônicos e de azar Mais de 2.500 tentativas de invasão a contas associadas a 10 e-mails roubados também registrados nos ataques à companhia aérea.
- Varejista 1.150 tentativas de invasão a contas associadas a mais de 800 e-mails roubados, um dos quais também visto no ataque à companhia aérea.
- Os e-mails continuam sendo utilizados por consumidores genuínos nas organizações do Digital Identity Network.

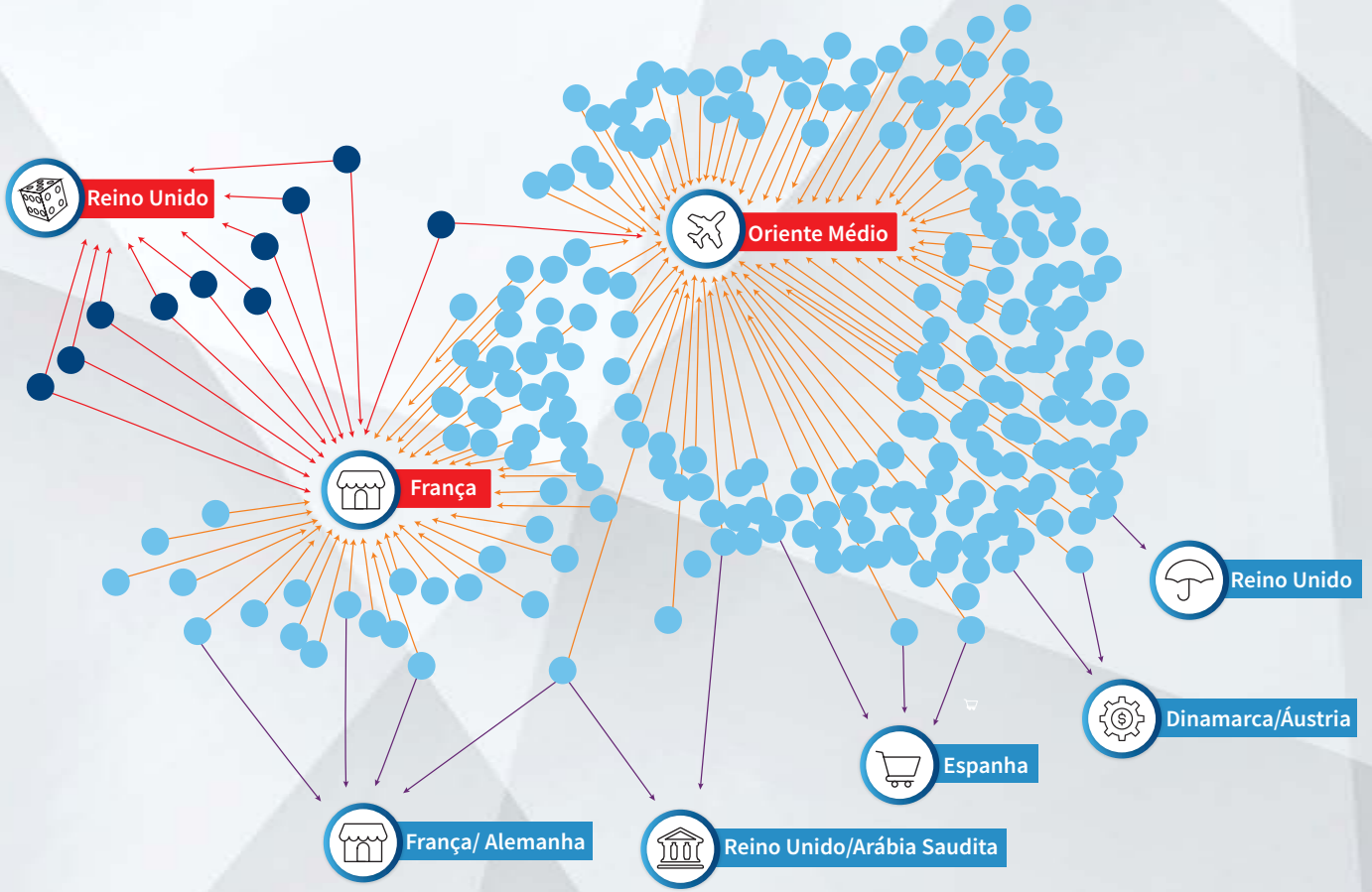
DETECÇÃO:
A avaliação de risco de e-mail do Digital Identity Network faz distinção entre uso legítimo e fraudulento de endereços de e-mail.

O USO DE ENDEREÇOS DE E-MAIL ROUBADOS NAS ORGANIZAÇÕES REFORÇA A IMPORTÂNCIA DE UMA AVALIAÇÃO ROBUSTA SOBRE OS RISCOS DE E-MAIL

Endereços de e-mail roubados usados em **ataques a organizações**

Endereços de e-mail roubados usados em ataques **a uma organização**

Endereço de e-mail usado por cliente genuíno em **outras organizações**



OPERADOR DE JOGOS ELETRÔNICOS E DE AZAR
COMPANHIA AÉREA
VAREJISTA
BANCO
MERCADO
FINTECH
SEGUROS

LexisNexis® RISK SOLUTIONS

DESTAQUE: ANÁLISE DE ATAQUES DE FRAUDES EM REDE ASSOCIADOS A DIFERENTES PARTES DE DADOS DE IDENTIDADE DIGITAL

A união de todos os elementos de dados de identidade digital revelou conexões de alto risco nunca vistas antes

Ataque de fraudes

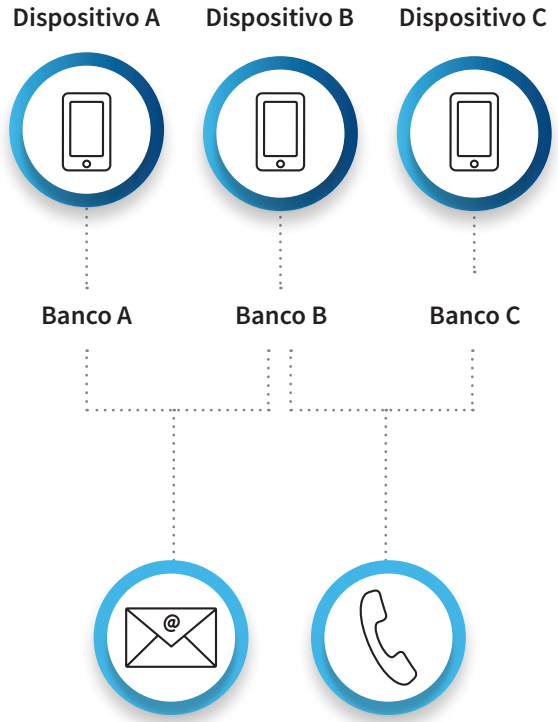
Fraudadores usando 3 dispositivos diferentes em 3 bancos diferentes.

3 operações fraudulentas não podem ser associadas pois não há um identificador comum.

Adicionando dados adicionais

Associação dos Dispositivos A e B por um endereço de e-mail.

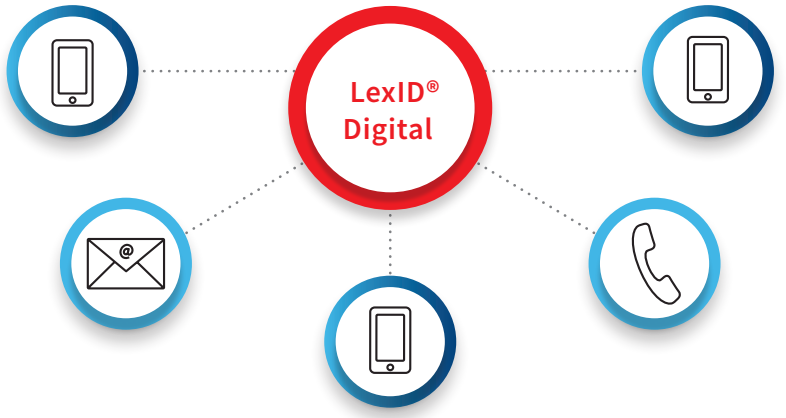
Associação dos Dispositivos A e B por número de telefone.



Construindo esta identidade digital no Digital Identity Network

É possível construir uma identidade digital online no Digital Identity Network associando as 3 operações fraudulentas através do endereço de e-mail e do número de telefone.

Quando qualquer uma dessas entidades for vista em uma nova operação, pode-se verificar se há fraudes no histórico da identidade digital.



03

O CENÁRIO DOS CRIMES CIBERNÉTICOS:

JULHO-DEZEMBRO DE 2020

A JORNADA DO CLIENTE

DESTAQUE DA JORANDA DO CLIENTE: JULHO-DEZEMBRO DE 2020

CRIAÇÃO DE NOVAS CONTAS

- A maior taxa de ataques de todos os casos de uso.
- 1 em cada 10 operações no Digital Identity Network é uma tentativa de ataque.

LOGINS

- Baixo índice geral de ataques.
- Crescimento de 9% ano a ano na taxa de ataques móveis.

PAGAMENTOS

- Crescimento significativo ano a ano no volume de operações de pagamento, à medida que os clientes dependem cada vez mais de formas digitais de pagamento.
- O maior volume de tentativas de ataques a operações de pagamento do que qualquer outro caso de uso.

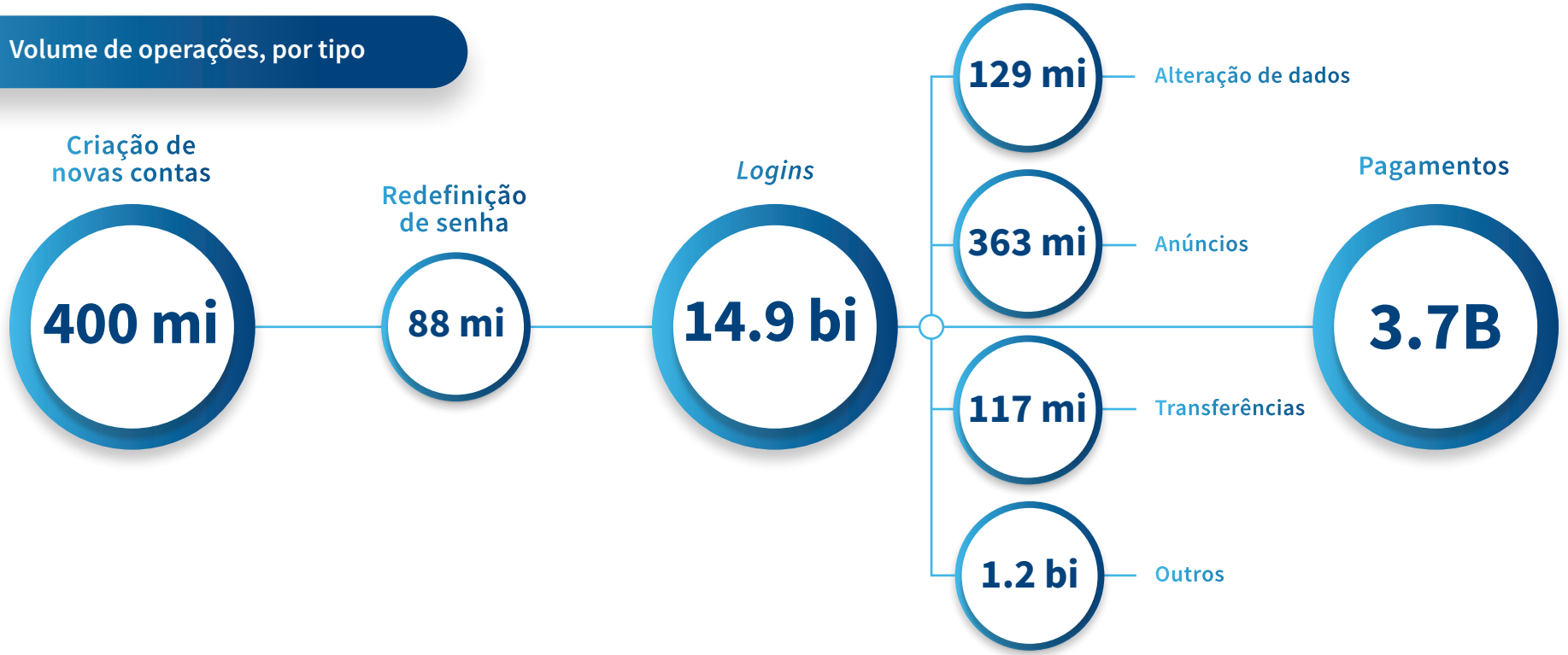
ALTERAÇÃO DE DADOS

- Dos casos de uso não essenciais, as operações de alteração de dados apresentaram a maior taxa de ataque, 2,2%.

O VOLUME DE OPERAÇÕES POR CASO DE USO EM TODA A JORNADA ONLINE

Monitoramento de todos os pontos de contato do cliente para uma tomada de decisão de risco melhorada

Volume de operações, por tipo



"Outras" operações incluem: cadastro de dispositivo novo, download digital, saldo em conta, aceitação de empréstimos, leilões, entre outros.

RISCOS DE ATAQUES EM PONTOS DE CONTATO IMPORTANTES

Queda nas taxas de ataques em todos os casos de uso de julho a dezembro de 2020

	CRIAÇÃO DE NOVAS CONTAS	*LOGINS*	PAGAMENTOS
TENDÊNCIAS DE RISCO	O volume de ataques têm caído de maneira significativa ano a ano. Isso se deve a um ataque enorme de *bots* a criações de novas contas em serviços financeiros entre dezembro 2019 e janeiro 2020, o que aumentou bastante o número que, em comparação, foi baixo durante o 2H2020.	As operações de *logins* continuaram sofrendo baixas taxas de ataques no geral, graças ao alto volume de operações de clientes recorrentes e confiáveis. Entretanto, o número absoluto de ataques foi significativo, ilustrando o risco que as contas dos bons usuários correm.	As operações de pagamento sofreram o maior volume de ataques de todos os casos de uso, com as em navegadores para dispositivos móveis sendo o alvo mais constante.
VOLUME DE ATAQUES	39 mi	62 mi	108 mi
TAXA DE ATAQUES			
GERAL	9,8%	0,4%	2,9%
DESKTOP	**13,9%**	**0,8%**	3,3%
NAVEGADORES MÓVEIS	9,1%	0,7%	**3,4%**
APLICATIVOS MÓVEIS	5,4%	0,1%	1,7%

2H refere-se ao período entre julho e dezembro.

RISCOS DE ATAQUE EM PONTOS DE CONTATO ADICIONAIS DE ALTO RISCO

Operações de alteração de dados podem ser percursores de alto risco a ataques futuros

	REDEFINIÇÃO DE SENHA	ALTERAÇÃO DE DADOS	ANÚNCIOS	TRANSFERÊNCIAS	OUTROS
TENDÊNCIAS DE RISCO	A redefinição de senha possibilita que fraudadores invadam contas online, geralmente usando credenciais roubadas. O acesso à conta possibilita, então, que fraudadores iniciem ações futuras, como pagamentos.	Alterações dos dados da conta possibilitam que fraudadores modifiquem informações importantes. Por exemplo, a mudança do número de telefone significa que eventos subsequentes, como uma mensagem de texto de uso único (OTP) para verificação de autenticação, serão enviados ao fraudador. Grandes investidas contra operações de alteração de dados em organizações de serviços financeiros contribuíram para as altas taxas de ataques a aplicativos móveis durante este período.	Anúncios possibilitam que fraudadores controlem a venda e a promoção de bens e serviços, podendo oferecer uma maneira de monetizar bens roubados, postagens de anúncios falsos de propriedades ou serviços ou comentários forjados para melhorar as vendas.	As transferências possibilitam que dinheiro seja movimentado para contas diferentes dentro do perfil de um mesmo cliente. Por vezes, esse tipo de ação pode preceder uma ocorrência fraudulenta de pagamento após a invasão de uma conta.	Inclui diversos outros pontos de contato de alto risco como registros em um novo canal, autorização para débito automático, débito direto e alterações de beneficiários.
VOLUME DE ATAQUES	0.7 mi	2.9 mi	1.8 mi	1.1 mi	19.3 mi
TAXA DE ATAQUES					
GERAL	0,8%	2,2%	0,5%	0,9%	1,6%
DESKTOP	**0,9%**	1,2%	0,5%	**1,8%**	**2,2%**
NAVEGADORES MÓVEIS	**0,9%**	1,3%	**1,5%**	1,2%	1,2%
APLICATIVOS MÓVEIS	0,2%	**3,8%**	0,4%	0,6%	1,2%

04

O CENÁRIO DE CRIMES CIBERNÉTICOS: **JULHO-DEZEMBRO DE 2020**

TENDÊNCIAS REGIONAIS

DESTAQUES REGIONAIS: JULHO-DEZEMBRO DE 2020

APAC

+24%
Crescimento a.a. no volume de operações.

-42%
Redução a.a. nos ataques iniciados por humanos.

-2%
Redução Redução a.a. no volume de *bots*.

EMEA

+23%
Crescimento a.a. no volume de operações.

-54%
Redução a.a. nos ataques iniciados por humanos.

-6%
Redução a.a. no volume de *bots*.

LATAM

+18%
Crescimento a.a. no volume de operações, com aumento de 16% na penetração de operações móveis - a maior de todas as regiões.

-26%
Redução a.a. nos ataques iniciados por humanos.

-20%
Redução a.a. no volume de *bots*.

AMÉRICA DO NORTE

+37%
Crescimento a.a. no volume de operações.

-37%
Redução a.a nos ataques iniciados por humanos.

+1%
Crescimento a.a. no volume de *bots*.

América do Norte inclui EUA e Canadá. México faz parte da análise da região da LATAM.

ÍNDICE DE ABUSO DE IDENTIDADE POR REGIÃO

LATAM e APAC sofrem o maior número de ataques voláteis

APAC EMEA LATAM **AMÉRICA DO NORTE**

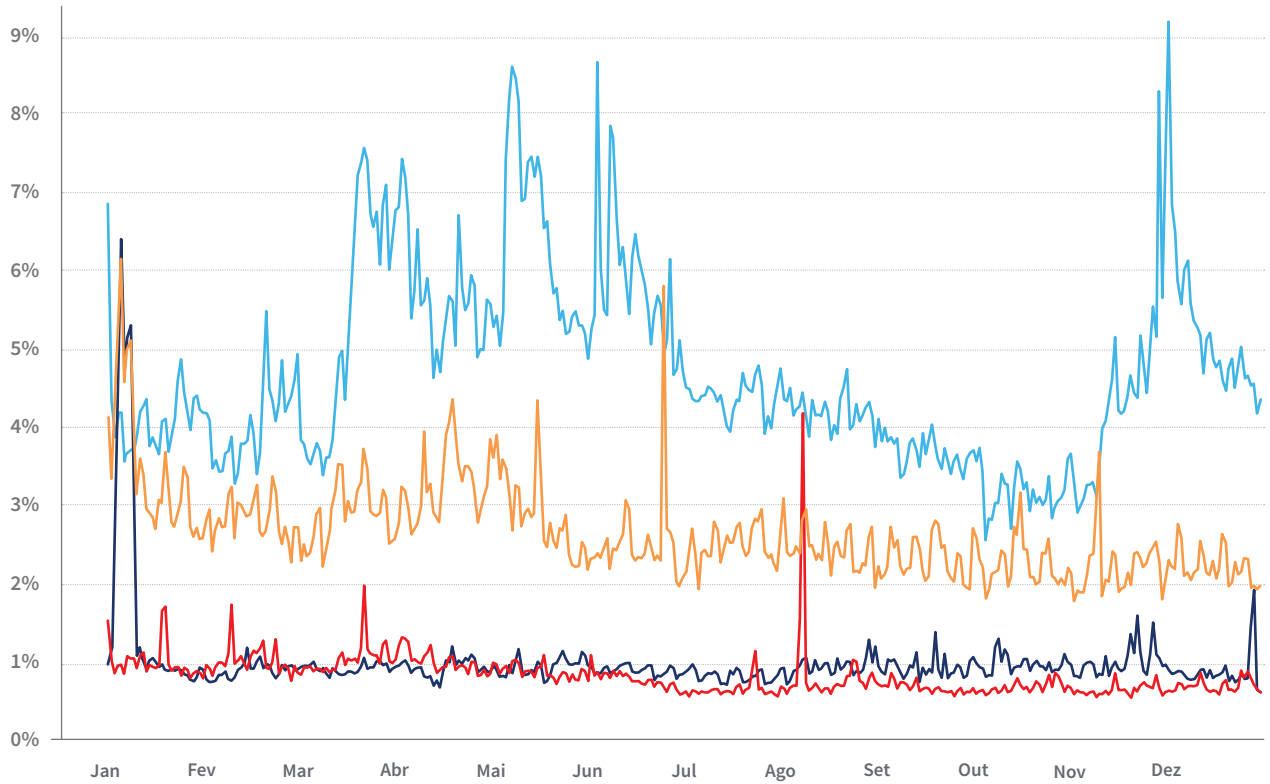
A LATAM continuou registrando a maior taxa de ataques diários entre todas as regiões, com diversos picos observados durante o ano.

Uma grande investida a serviços financeiros em dezembro aumentou a taxa geral de ataques para mais de 9% de todas as operações diárias.

A região da **APAC** registrou uma tendência consistente de baixa na taxa de ataques diários durante o segundo semestre de 2020, apesar do volume significativo de atividades de *bots* em novembro, procedente da Índia, com o objetivo de invadir contas em um grande varejista norte-americano.

América do Norte e **EMEA** continuaram registrando baixas taxas gerais de ataques com o decorrer do tempo, em comparação às outras regiões do mundo.

Mesmo assim, em agosto, houve um grande ataque de *bots*, originado na Holanda, a um mercado online, que registrou um aumento de mais de 4% na taxa geral de ataques de todas as operações na EMEA.



LexisNexis® RISK SOLUTIONS

OPERAÇÕES E PADRÕES DE ATAQUES DA REGIÃO DA APAC

APAC

OS 5 MAIORES ATACANTES

1. Índia
2. Japão
3. Bangladesh
4. Filipinas
5. Malásia

OS 5 MAIORES DESTINOS DOS ATAQUES

1. EUA
2. Reino Unido
3. Austrália
4. Japão
5. Malásia

OPERAÇÕES

OPERAÇÕES PROCESSADAS

1.7 bi

Crescimento a.a.
+24% ▲

OPERAÇÕES CLASSIFICADAS POR CANAL

Desktop / Móvel

Navegadores / aplicativos móveis

ATAQUES

VOLUME DE ATAQUES INICIADOS POR HUMANOS

33 mi

Queda a.a.
-42% ▼

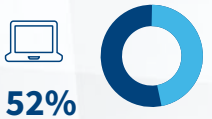
VOLUME DE ATAQUES DE *BOTS* AUTOMATIZADOS

142 mi

Queda a.a.
-2% ▼

ATAQUES CLASSIFICADOS POR CANAL

Desktop / Móvel



A taxa de ataques originados em dispositivos móveis **tem caído a.a.**

-15% ▼

A POSIÇÃO DA APAC EM COMPARAÇÃO AOS NÚMEROS GLOBAIS

APAC

A APAC registrou maior taxa de ataques em todos os canais em comparação aos números globais

GLOBAL **APAC**

As taxas de ataques na região Ásia-Pacífico (APAC) permaneceram mais altas do que a média global, embora continuem apresentando queda ano a ano em todos os canais.

A região continuou contribuindo amplamente aos ataques de *bots* no mundo, com Japão, Índia e Austrália na lista de locais de maior procedência.

O volume de ataques de *bots* automatizados originados na região da APAC é bastante consistente ano a ano.

TAXA GERAL DE ATAQUES

1,1% **2,3%**

TAXA DE ATAQUES A DESKTOP

1,6% **2,8%**

TAXA DE ATAQUES A NAVEGADORES MÓVEIS

2,3% **3,0%**

TAXA DE ATAQUES A APLICATIVOS MÓVEIS

0,4% **1,3%**

OPERAÇÕES E PADRÕES DE ATAQUES DA REGIÃO DA EMEA

EMEA

OS 5 MAIORES ATACANTES

1. Reino Unido
2. Alemanha
3. Arábia Saudita
4. Holanda
5. Rússia

OS 5 MAIORES DESTINOS DOS ATAQUES

1. EUA
2. Reino Unido
3. Canadá
4. Rússia
5. Suécia

OPERAÇÕES

OPERAÇÕES PROCESSADAS

8.7 bi

Crescimento a.a.
+23% ▲

OPERAÇÕES CLASSIFICADAS POR CANAL

Desktop / Móvel

Navegadores / aplicativos móveis

ATAQUES

VOLUME DE ATAQUES INICIADOS POR HUMANOS

60 mi

Queda a.a.
-54% ▼

VOLUME DE ATAQUES DE *BOTS* AUTOMATIZADOS

256 mi

Queda a.a.
-6% ▼

ATAQUES CLASSIFICADOS POR CANAL

Desktop / Móvel

A taxa de ataques originados em dispositivos móveis **tem caído a.a.**

-13% ▼

A POSIÇÃO DA EMEA EM COMPARAÇÃO AOS NÚMEROS GLOBAIS

EMEA

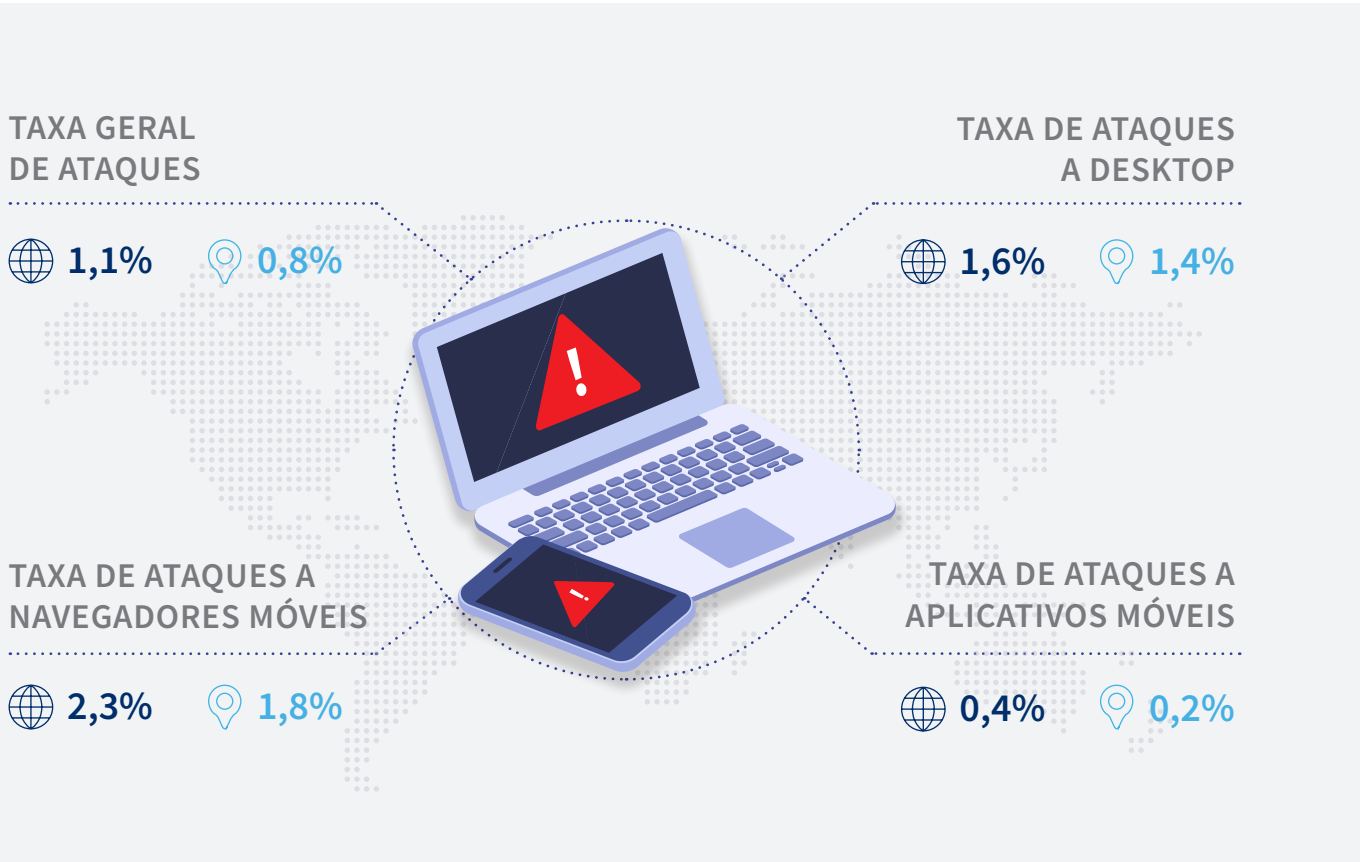
A EMEA apresentou a maior penetração de operações em aplicativos móveis entre todas as regiões no mundo

GLOBAL EMEA

A região Europa, Oriente Médio e África (EMEA) continuou sofrendo baixas taxas gerais de ataques em comparação às médias globais, impulsionadas por um grande volume de operações confiáveis em aplicativos para dispositivos móveis.

A região apresentou a maior queda de ataques iniciados por humanos em comparação às outras regiões.

Apesar disso, diversos países da EMEA aparecem na lista dos maiores contribuidores de ataques de *bots* e iniciados por humanos, por volume.



OPERAÇÕES E PADRÕES DE ATAQUES LATAM

LATAM

OS 5 MAIORES ATACANTES

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

OS 5 MAIORES DESTINOS DOS ATAQUES

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

OPERAÇÕES

OPERAÇÕES PROCESSADAS

875 mi

Crescimento a.a.
+18% ▲

OPERAÇÕES CLASSIFICADAS POR CANAL

Desktop / Móvel

Navegadores / aplicativos móveis

ATAQUES

VOLUME DE ATAQUES INICIADOS POR HUMANOS

33 mi

Queda a.a.
-26% ▼

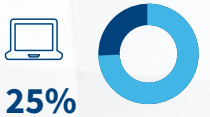
VOLUME DE ATAQUES DE *BOTS* AUTOMATIZADOS

44 mi

Queda a.a.
-20% ▼

ATAQUES CLASSIFICADOS POR CANAL

Desktop / Móvel



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

+2% ▲

A POSIÇÃO DE LATAM EM COMPARAÇÃO AOS NÚMEROS GLOBAIS

LATAM

As mais altas taxas de ataques em todos os canais do que qualquer região

GLOBAL **LATAM**

Apesar da taxa geral de ataques ter caído na LATAM em comparação ao ano anterior, elas permaneceram as mais altas de todas as regiões do mundo, especialmente para as operações em aplicativos para dispositivos móveis.

O volume de ataques de *bots* automatizados também diminuiu 20% em comparação ao ano anterior. O Brasil é o único país da LATAM na lista de principais procedências de *bots*.

O percentual de operações móveis cresceu 16% a.a. na LATAM, o que sugere que os dispositivos móveis possam estar facilitando a inclusão financeira na região, que passou a EMEA como tendo a maior penetração de operações realizadas em dispositivos móveis, com quase 4 em cada 5.

OPERAÇÕES E PADRÕES DE ATAQUES DA AMÉRICA DO NORTE

AMÉRICA DO NORTE

OS MAIORES ATACANTES

1. EUA
2. Canadá

OS 5 MAIORES DESTINOS DOS ATAQUES

1. EUA
2. Canadá
3. Austrália
4. Reino Unido
5. Brasil

OPERAÇÕES

OPERAÇÕES PROCESSADAS

12.6 bi

Crescimento a.a.
+37% ▲

OPERAÇÕES CLASSIFICADAS POR CANAL

Desktop / Móvel

Navegadores / aplicativos móveis

ATAQUES

VOLUME DE ATAQUES INICIADOS POR HUMANOS

105 mi

Queda a.a.
-37% ▼

VOLUME DE ATAQUES DE *BOTS* AUTOMATIZADOS

747 mi

Crescimento a.a.
+1% ▲

ATAQUES CLASSIFICADOS POR CANAL

Desktop / Móvel

A taxa de ataques originados em dispositivos móveis **tem caído a.a.**
-24% ▼

América do Norte inclui EUA e Canadá. México faz parte da análise da região da LATAM.

A POSIÇÃO DA AMÉRICA DO NORTE EM COMPARAÇÃO AOS NÚMEROS GLOBAIS

AMÉRICA DO NORTE

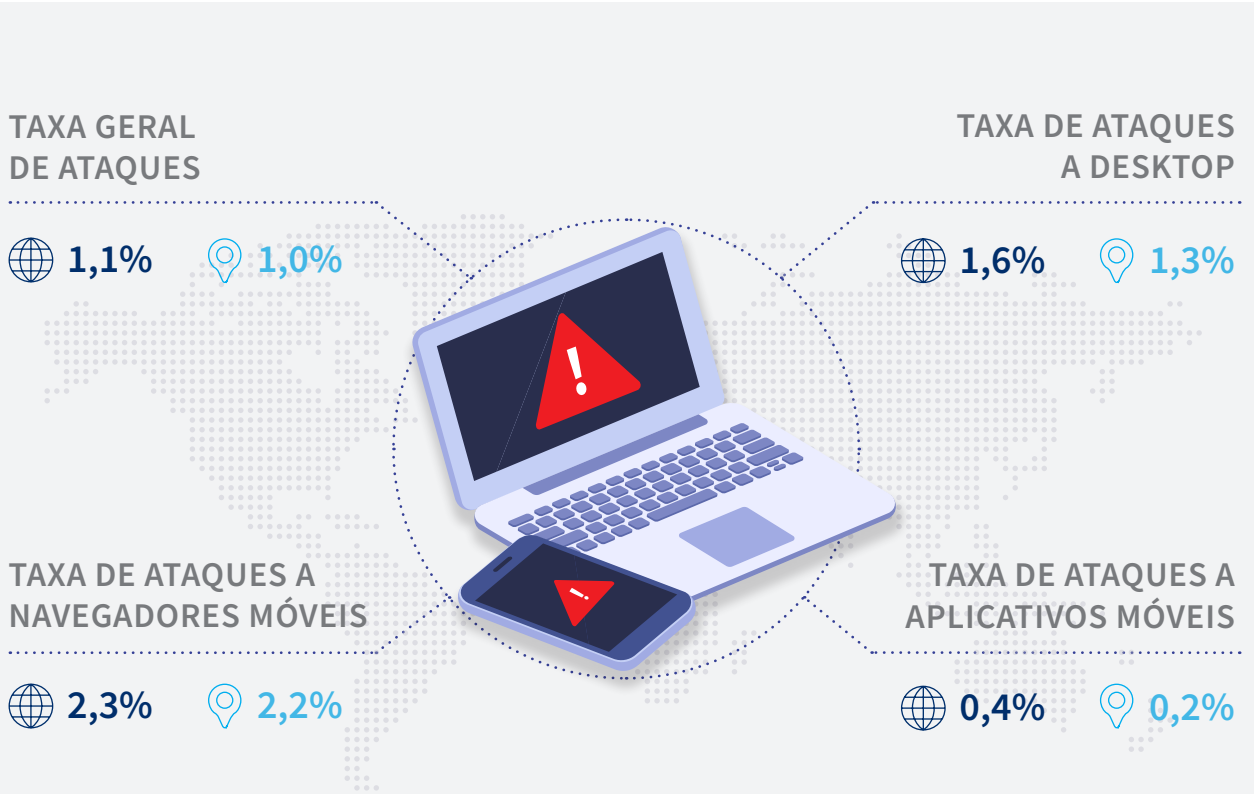
Forte crescimento no volume de *bots* automatizados entre julho e dezembro de 2020

GLOBAL **AMÉRICA DO NORTE**

A América do Norte continuou apresentando baixas taxas gerais de ataques em comparação às médias globais, seguindo um padrão semelhante ao da região da EMEA.

A taxa de ataques iniciados por humanos também encolheu na região, enquanto o volume de ataques de *bots* permaneceu consistente, com aumento registrado de 1% a.a.

Entretanto, os EUA são os maiores originadores, por volume, de ataques de *bots* e iniciados por humanos, com o Canadá permanecendo na 3a posição.



05

O CENÁRIO DOS CRIMES CIBERNÉTICOS:
JULHO-DEZEMBRO DE 2020

OPORTUNIDADES DOS SETORES

DESTAQUES DO SETOR: JULHO-DEZEMBRO DE 2020

SERVIÇOS FINANCEIROS

- Baixas taxas gerais de ataque, impulsionadas por um alto volume de operações de *login* repetidos realizados por clientes confiáveis.
- A exceção ficou por conta das operações de pagamento, que sofreram mais ataques do que em qualquer outro setor, apresentando uma ótima oportunidade de lucro para os fraudadores.
- Crescimento dos ataques a criações de novas contas em navegadores para desktops e dispositivos móveis.

COMÉRCIO ELETRÔNICO

- O comércio eletrônico apresentou o maior crescimento no volume de *bots* em comparação a outros setores, apesar da retração nas taxas de ataques iniciados por humanos.
- A taxa de ataques a pagamentos para o comércio eletrônico realizados em aplicativos para dispositivos móveis é a mais alta entre os setores, representando um ponto de risco em potencial.

MÍDIA

- Criações de novas contas atacadas com mais frequência do que qualquer outro setor, com os fraudadores usando organizações de mídia para testar dados de identidades roubados.
- Crescimento nas taxas de ataques a criações de novas contas em navegadores para desktops e dispositivos móveis, bem como operações de *login* em navegadores e aplicativos para dispositivos móveis.

PANORAMA DA INDÚSTRIA: TENDÊNCIAS E PADRÕES DE ATAQUES

O setor de mídia sofreu as taxas mais altas de ataques de todos os casos de uso, enquanto as operações em desktop foram as mais atacadas entre todos os canais

PANORAMA DA INDÚSTRIA	RESUMO DE TODOS OS SETORES	SERVIÇOS FINANCEIROS	COMÉRCIO ELETRÔNICO	MÍDIA
TENDÊNCIAS DE RISCO	De todos os canais, as operações em desktop foram as mais atacadas.	Apesar do alto volume de ataques, as taxas gerais são as mais baixas entre todos os setores, impulsionadas pelo grande número de operações repetidas e de confiança.	A taxa de ataques a dispositivos móveis (um subgrupo da taxa de ataques móveis) em operações de pagamento foi mais alta para o comércio eletrônico do que para os outros setores.	Criações de novas contas representaram o maior risco na jornada do cliente de mídia, tanto em termos de volume como de taxas de ataques.
VOLUME DE ATAQUES	235 mi	123 mi	65 mi	46 mi
TAXA DE ATAQUES				
GERAL	1,1%	0,8%	1,4%	**4,5%**
DESKTOP	**1,6%**	**1,3%**	**1,8%**	**4,2%**
MÓVEL	0,9%	0,7%	1,1%	**4,7%**

SERVIÇOS FINANCEIROS: PANORAMA DAS TENDÊNCIAS E PADRÕES DE ATAQUES

As operações de serviços financeiros registraram 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/taxa de ataque a aplicativos móveis devido ao grande número de ataques de *bots* a criações de novas contas em aplicativos móveis em dezembro de 2019/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 *login* permaneceu baixa devido ao alto volume de operações regulares de clientes confiáveis. No entanto, as 36 milhões de tentativas de invasão a contas representaram um risco significativo às contas dos bons clientes. As operações em navegadores para desktops e dispositivos móveis foram as mais atacadas, embora essas taxas tenham caído em comparação ao ano anterior.	À medida que o volume de operações de pagamento aumentou ano a ano, o volume de ataques também apresentou crescimento. No entanto, o crescimento do volume de ataques foi menos pronunciado do que o de operações, levando a um declínio geral nas taxas de ataque.
VOLUME DE ATAQUES	5 mi (94 mi)	36 mi (48 mi)	69 mi (58 mi)
TAXA DE ATAQUES			
GERAL	4,1% (18,3%)	0,3% (0,5%)	3,6% (4,5%)
DESKTOP	**7,1%** (5,0%)	**0,7% (1,2%)**	4,1% (4,2%)
NAVEGADORES MÓVEIS	3,4% (3,1%)	**0,7%** (1,0%)	**4,9% (6,3%)**
APLICATIVOS MÓVEIS	2,3% **(20,8%)**	0,1% (0,2%)	1,0% (2,2%)

Os números entre parênteses são referentes ao 2H 2019.

COMÉRCIO ELETRÔNICO: PANORAMA DAS TENDÊNCIAS E PADRÕES DE ATAQUE

Queda geral nas taxas de ataques, mas pontuada por um crescimento de 32% no volume de *bots* ano a ano

PANORAMA DO COMÉRCIO ELETRÔNICO	CRIAÇÃO DE NOVAS CONTAS	*LOGINS*	PAGAMENTOS
TENDÊNCIAS DE RISCO	As criações de novas contas em desktop continuaram sendo atacadas com frequência maior do que qualquer outro caso de uso, com mais de uma em cada 10 operações identificadas como um ataque em potencial. Apesar disso, as taxas de ataque recuaram em todos os canais.	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 ataque 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 grande oportunidade para os fraudadores lucrarem e monetizarem credenciais roubadas. Embora as taxas de ataques também tenham caído em todos os canais, as contra aplicativos móveis foram maior para o comércio eletrônico do que para qualquer outro setor.
VOLUME DE ATAQUES	6 mi (8 mi)	19 mi (49 mi)	36 mi (44 mi)
TAXA DE ATAQUES			
GERAL	5,2% (11,3%)	1,0% (3,4%)	2,3% (3,8%)
DESKTOP	**10,7% (25,9%)**	**1,3%** (3,3%)	**2,7% (4,7%)**
NAVEGADORES MÓVEIS	2,7% (4,5%)	0,8% (2,9%)	1,6% (2,9%)
APLICATIVOS MÓVEIS	1,3% (4,0%)	0,2% **(4,3%)**	**2,7%** (3,8%)

Os números entre parênteses são referentes ao 2H 2019.

MÍDIA: PANORAMA DAS TENDÊNCIAS E PADRÕES DE ATAQUES

Criações de novas contas de mídia registraram taxas de ataques significativamente mais altas do que qualquer outro setor

PANORAMA DE MÍDIA	CRIAÇÃO DE NOVAS CONTAS	*LOGINS*	PAGAMENTOS
TENDÊNCIAS DE RISCO	Cerca de 1 em cada 6 operações de criação de novas contas foi um ataque em potencial, com um aumento registrado em navegadores para desktops e dispositivos móveis. É provável que muitas dessas tentativas de criação de novas contas tenham sido realizadas por fraudadores testando dados de identidades roubados em empresas que costumam apresentar menos barreiras de entrada. São feitas tentativas para tirar proveito dos bônus para novos clientes ou para revender períodos de teste com o intuito de obter ganhos financeiros.	A taxa geral de ataque a *logins* foi comparável à do comércio eletrônico. No entanto, as organizações de mídia sofreram um crescimento na taxa de ataques a navegadores e aplicativos para dispositivos móveis quando comparado ao ano anterior.	As taxas de ataque a pagamentos de mídia foram mais baixas do que em outros setores, provavelmente porque representam menos oportunidades de lucro em comparação aos pagamentos de comércio eletrônico ou de serviços financeiros. Porém, em comparação ao ano anterior, o setor registrou um crescimento significativo em *bots* realizando operações de pagamento. É provável que tenham sido fraudadores testando dados de cartões de crédito roubados antes de usarem cartões validados em um ataque mais lucrativo em outro lugar.
VOLUME DE ATAQUES	29 mi (30 mi)	7 mi (9 mi)	3 mi (3 mi)
TAXA DE ATAQUES			
GERAL	16,6% (15,5%)	1,1% (1,9%)	1,8% (2,5%)
DESKTOP	**21,9%** (18,3%)	0,7% **(2,8%)**	**2,0% (2,9%)**
NAVEGADORES MÓVEIS	14,9% (12,1%)	0,8% (0,6%)	1,9% (2,8%)
APLICATIVOS MÓVEIS	15,7% **(25,4%)**	**5,1%** (0,8%)	1,1% (1,5%)

Os números entre parênteses são referentes ao 2H 2019.

JOGOS ELETRÔNICOS E DE AZAR (SUBGRUPO DE MÍDIA): PANORAMA DAS TENDÊNCIAS E PADRÕES DE ATAQUES

Oportunidades de ganhar bônus e de invasão a contas atraem os fraudadores aos operadores globais de jogos eletrônicos e de azar

PANORAMA DOS JOGOS ELETRÔNICOS E DE AZAR	CRIAÇÃO DE NOVAS CONTAS	*LOGINS*	PAGAMENTOS
TAXA DE ATAQUES			
GERAL	9,4%	0,9%	0,8%
DESKTOP	**12,6%**	**1,3%**	0,7%
NAVEGADORES MÓVEIS	9,0%	0,9%	**1,0%**
APLICATIVOS MÓVEIS	3,6%	0,1%	0,3%

- Os bônus para novos jogadores tornam os operadores de jogos eletrônicos e de azar suscetíveis a diversas criações de novas contas fraudulentas. Os criminosos costumam explorar oportunidades de jogos grátis em grande escala, aumentando, assim, as chances de ganhar o prêmio.
- Isso explica a alta taxa de ataques a criações de novas contas, especialmente em operações em desktop.
- Embora a taxa de ataques a *logins* em contas tenha permanecido baixa, o volume significativo de tentativas de invasão a contas representa, ao setor, o risco de fraudadores que buscam acessar os saldos das contas de bons usuários ou simplesmente lavar receitas de crimes em diferentes setores e localidades.

TELECOM (SUBGRUPO DE MÍDIA): PANORAMA DAS TENDÊNCIAS E PADRÕES DE ATAQUES

As organizações de telecomunicações correm o risco de grande exposição monetária decorrente de criações de novas contas fraudulentas e invasão a contas

PANORAMA DE TELECOM	CRIAÇÃO DE NOVAS CONTAS	*LOGINS*	PAGAMENTOS
TAXA DE ATAQUES			
GERAL	1,1%	0,2%	1,9%
DESKTOP	1,0%	**0,3%**	1,8%
NAVEGADORES MÓVEIS	**1,1%**	0,1%	**2,0%**

- As organizações de telecomunicações oferecem aos fraudadores oportunidades de lavar hardware de alto valor e registrar contratos de telefonia móvel pré- e pós-pagos para que cometam mais fraudes.
- Com a migração de compras em lojas físicas para operações digitais acelerada por conta dos lockdowns relacionados à Covid, as organizações de telecomunicações foram forçadas a priorizar a sua transformação digital, deixando de lado a venda em pessoa e as verificações de KYC que eram típicos da experiência na loja física.
- Embora as taxas gerais de ataques tenham permanecido baixas, a exposição monetária de criações de novas contas e de invasões a contas individuais pode ser extremamente alta. Isso se deve, em grande parte, ao elevado valor dos aparelhos celulares e à possibilidade de acúmulo rápido de grandes cobranças na conta, especialmente em downloads de conteúdo e streaming de mídia.

Os dados de aplicativos para dispositivos móveis foram excluídos por conta do baixo volume das operações.

06

OS CRIMES CIBERNÉTICOS EM UMA PANDEMIA:

TENDÊNCIAS DE CONSUMO E TIPOLOGIAS DE FRAUDES

RESUMO:

- Embora tipologias específicas de fraudes tenham se proliferado durante a pandemia global, as taxas gerais de ataques caíram no Digital Identity Network.
- Automação e *spoofing* de identidade permaneceram vetores de ataque de destaque em 2020.
- Com muitos clientes novos ao mundo digital acessando-o pela primeira vez, os jovens com menos de 25 anos formaram o grupo mais suscetível a ataques de fraudes.
- A faixa etária mais velha foi o segundo grupo mais atacado, fazendo com que sejam igualmente vulneráveis.
- O prejuízo causado por fraudes aumenta progressivamente com a idade, fazendo com que a população mais velha sofra mais riscos de grandes perdas por fraude.

OS CRIMES CIBERNÉTICOS EM UMA PANDEMIA

Resumo das tendências de consumo e tipologias de fraudes em 2020

TENDÊNCIAS DE CONSUMO

Crescimento de 34% ano a ano em pagamentos online.

Crescimento de 26% ano a ano em operações de *login*.

Crescimento no volume no volume de operações procedentes de novos dispositivos e novas identidades digitais, além dos clientes existentes estarem realizando mais operações.

Queda nas taxas gerais de ataques indica maior volume de operações sendo realizadas por clientes de confiança.

Crescimento no registro de novos clientes de internet banking para os serviços de internet e de celular.

Menos atividades de *login* de clientes que viajaram mais de 1.000 km em uma semana, assim como mudança de logins de áreas metropolitanas para os subúrbios .

TIPOLOGIAS DE FRAUDES

***Spoofing* de identidade** foi o vetor de ataque mais prevalente, visto em 5% de todas as operações globais, seguido por *spoofing* de dispositivo, com 4,2%.

O crescimento dos ataques costuma vir do volume de *bots* automatizados, o que indica que a automação é o método escolhido para os ataques atuais.

Mídia continuou sendo o setor com as maiores taxas gerais de ataques, embora os serviços financeiros tenham sofrido o maior volume de investidas a pagamentos.

Fraudes registradas em pacotes de estímulos de governos em diversos bancos, ex.: ataques ao Bounce Back Loan Scheme no Reino Unido.

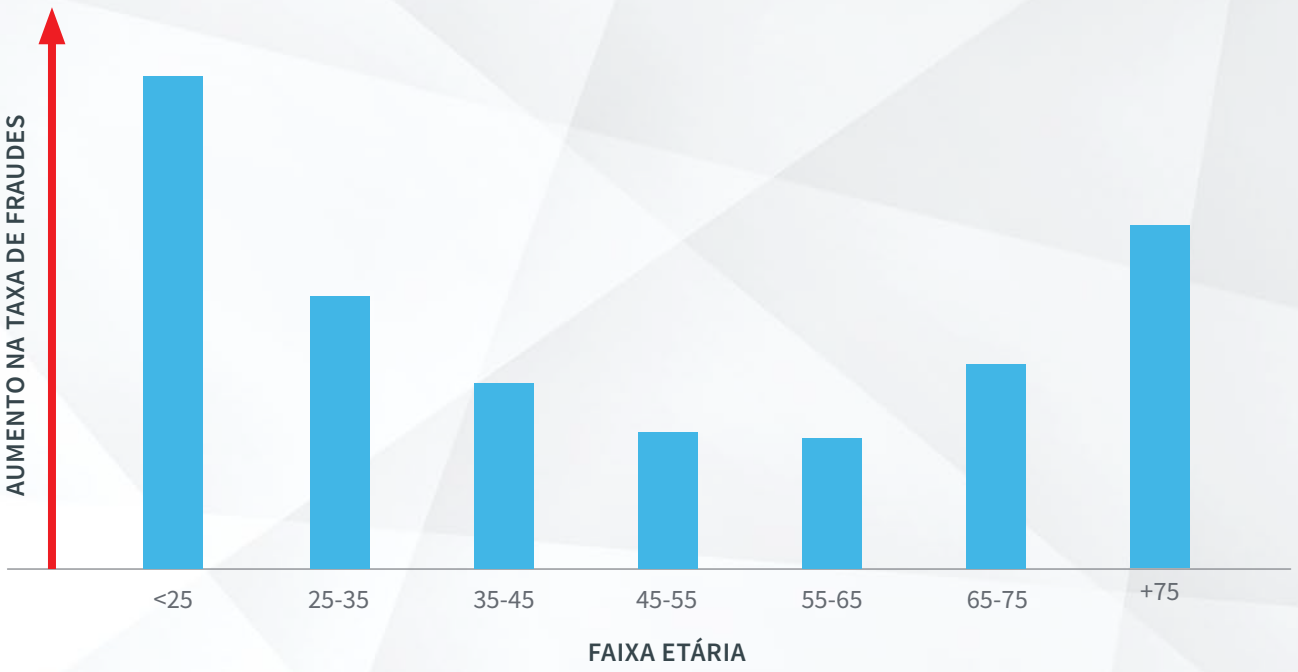
Primeiros sinais de que os consumidores estão sentindo a pressão econômica com o crescimento da taxa de fraudes de estorno inicial no comércio eletrônico.

RISCO DE FRAUDES POR IDADE: QUAIS CLIENTES ESTÃO MAIS VULNERÁVEIS AOS ATAQUES DE FRAUDES?

Os clientes novos ao mundo digital, que chegam à internet em números cada vez maiores, estão correndo grande risco?

- O maior crescimento de novos clientes chegando ao mundo digital em 2020 foi no grupo de jovens abaixo de 25 anos, registrando 10% em um período de quatro meses.
- As análises mostraram que essa faixa etária também foi a mais vulnerável a ataques de fraudes, seguida de perto pelo grupo com mais de 75 anos.
- As notícias sugerem com frequência que os *millennials* compartilham seus dados online com mais facilidade, tornando-os mais expostos a possíveis violações de dados ou roubo de identidade.
- A faixa etária acima de 75 anos, às vezes chamada de geração silenciosa, costuma ter menos familiaridade com as tecnologias digitais mais recentes e pode, portanto, ficar mais suscetível a golpes e tentativas de *phishing*.

TAXA DE FRAUDES POR IDADE



RISCO DE FRAUDE POR IDADE: QUAIS CLIENTES SOFREM MAIORES PREJUÍZOS EM ATAQUES FRAUDULENTOS?

Como as organizações podem proteger quem corre risco de perder muito?

- Embora os *millennials* e os *zillennials* foram os mais suscetíveis a ataques de fraudes, o prejuízo médio de fraude por cliente aumentou progressivamente com a idade, provavelmente influenciado pela maior renda disponível quando se é mais velho.
- O paradoxo de por que os fraudadores optaram por atacar o grupo dos mais jovem em volume proporcionalmente maior pode ser explicado pelo fato de que maiores taxas de sucesso podem compensar ganhos monetários mais baixos.
- Proteger os mais velhos, grupo potencialmente mais vulnerável, é fundamental para as organizações que priorizam uma estratégia *digital-first*.
- As empresas precisam educar os clientes quanto ao *modus operandi* dos ataques de fraudes, garantindo que a jornada do cliente online esteja protegida, com mensagens online relevantes e oportunas, de acordo com a necessidade.

07 CONCLUSÃO

PREVISÕES PARA O PRÓXIMO ANO: AS OPORTUNIDADES PARA OS NEGÓCIOS DIGITAIS

Grandes oportunidades costumam surgir de mudanças. No entanto, essas oportunidades não se apresentam apenas para empresas digitais com visão de futuro, mas também para os criminosos cibernéticos que podem permanecer um pouco à frente da curva da tecnologia. À medida que as organizações mesclam seus serviços digitais e físicos, inovando para atender a uma base de consumidores cada vez mais diversificada, as estratégias de prevenção a fraudes devem acompanhar essa evolução, transformação e crescimento. Sem uma abordagem robusta e em camadas, as empresas se abrem a novos riscos de fraudes. Os criminosos permanecem mestres do disfarce, escondidos sob um manto de legitimidade, sempre em busca do elo mais fraco.

Inovação líder de mercado continuará acelerada para facilitar este complexo conjunto de oportunidades e mitigar os riscos associados para os negócios digitais globais. Em sua essência, isso deve fornecer às empresas a capacidade de criar camadas de identidade digital e física e soluções de autenticação em uma jornada omnicanal para o cliente.

Esse elo mais fraco pode muito bem ser os novos clientes digitais que migraram para o mundo online durante a pandemia. Os jovens adultos e a população mais velha se mostraram mais suscetíveis a ataques de fraudes. A prevenção se estende não apenas à detecção de spoofing de identidade, ataques de bots automatizados e invasões a contas, mas também à conscientização, educação e mensagens aos clientes, mostrando a todos como melhor identificar possíveis fraudes. É provável que continuemos a ver fraudadores se alimentando do nervosismo relacionado à pandemia, oferecendo investimentos que parecem bons demais para ser verdade ou produtos com alta procura online.

No entanto, não são apenas os novos clientes que devem ser protegidos. Os existentes e de confiança podem se incomodar com etapas adicionais de autenticação, já que o comportamento "de volta ao normal" pode ser potencialmente sinalizado como incomum, após as mudanças sem precedentes que ocorreram no comportamento dos consumidores em 2020. Como as organizações podem se certificar de que prevenção confiável a fraudes não criará atrito desnecessário para os clientes legítimos?

Mudanças regulatórias e incertezas econômicas também irão se fundir a este cenário digital dinâmico:

- As plataformas de sistema financeiro aberto *(open banking)* serão alvo importante para os fraudadores que procuram explorar os dados dos clientes em diferentes contas. O PSD2 na Europa fará com que os criminosos busquem brechas e isenções em defesas contra fraudes mais rígidas. Assim, os clientes legítimos podem sofrer uma mudança nas taxas de aceitação de operações, com a nova faixa de estratégias exigindo duas camadas rígidas de autenticação.
- É provável que, à medida que as economias respondem ao impacto da pandemia, os fraudadores também tentem se beneficiar da crise aumentando o recrutamento de mulas e prometendo, aos consumidores, dinheiro rápido em troca do uso de suas contas bancárias para canalizar os rendimentos procedentes de atividades criminosas através de organizações globais.
- O setor de comércio eletrônico deve sofrer um crescimento nas fraudes primárias, à medida que mais consumidores sentirem a crise econômica.

08

GLOSSÁRIO, METODOLOGIA, INFORMAÇÕES PARA CONTATO

GLOSSÁRIO

Tipos de setor

Serviços Financeiros inclui *mobile banking, internet banking*, transferência online de dinheiro, empréstimos, corretagem, formas alternativas de pagamento e emissão de cartões de créditos.

Comércio eletrônico inclui varejo, companhias aéreas, viagem, mercados, bilhetagem de telecomunicações e empresas de produtos digitais.

Mídia inclui redes sociais, *streaming* de conteúdo, jogos de azar, jogos eletrônicos e sites de namoro.

Ataques comuns

Fraudes de criação de novas contas: uso de identidades roubadas, comprometidas ou sintéticas criando novas contas para acessar serviços online e obter linhas de crédito.

Fraudes de *login* a contas: ataques com o objetivo de invadir contas de usuários usando credenciais roubadas anteriormente e disponíveis ou credenciais compromissadas por ataques de *malwares* ou *Man-in-the-Middle*.

Fraudes de pagamento: uso de credenciais de pagamento roubadas para realizar transferências ilegais de dinheiro ou pagamentos online através de formas alternativas, como depósito bancário.

Porcentagens

As porcentagens de tipo de tipo de operação são baseadas no número de operações (criação de conta, login à conta e pagamentos), a partir de dispositivos móveis e computadores desktops, recebidas e processadas pelo Digital Identity Network.

As porcentagens de ataques são baseadas nas operações identificadas como sendo de alto risco e classificadas como ataques, por caso de uso. Ocorrências identificadas como ataques são geralmente bloqueadas ou rejeitadas automaticamente, em tempo quase real, dependendo dos casos de uso do consumidor.

Desktop x Móvel

Operações em desktops são as originadas a partir de um dispositivo desktop, como computador ou laptop.

Ataques a desktops são os que ocorrem contra operações procedentes de um dispositivo desktop.

Operações móveis são as originadas a partir de um dispositivo móvel portátil, como *tablet* ou aparelho celular, e incluem as realizadas em navegadores e aplicativos para dispositivos móveis.

Ataques móveis são os que investem contra operações procedentes de um dispositivo móvel, sejam elas realizadas em navegador ou em aplicativo.

Explicações sobre os ataques

***Spoofing* de dispositivo:** os fraudadores excluem e alteram as configurações do navegador para mudar a identidade ou a impressão digital do dispositivo ou tentar fazer parecer que foi originada no dispositivo da vítima. A identificação de dispositivo sem cookies patenteada da LexisNexis® ThreatMetrix® consegue detectar usuários recorrentes, mesmo quando os cookies são excluídos ou alterações feitas às configurações do navegador. Para distinguir entre criminosos cibernéticos e clientes legítimos que ocasionalmente limpam cookies, apenas exclusões de cookies de alto risco/alta velocidade (como um grande número de visitas repetidas por hora/dia) são incluídas na análise.

***Spoofing* de identidade:** uso de identidade ou cartão de crédito roubados ou combinação de nome de usuário/senha comprometidos para tentar realizar fraude ou invasão a conta. O *spoofing* de identidade costuma ser detectado com base na alta velocidade de uso da identidade em um determinado dispositivo, identificando quando este acessa várias contas de usuários não relacionados ou ligações e usos incomuns da identidade.

***Spoofing* de endereço de IP:** os criminosos cibernéticos usam proxies para passar por filtros tradicionais de localização geográfica e usam técnicas de *spoofing* de IP para evitar filtros de velocidade e listas negras. O LexisNexis ThreatMetrix® detecta *spoofing* de IP diretamente por navegador ativo e passivo e técnicas de impressão digital de pacotes.

Detecção de *Man-in-the-Browser* (MitB) e *Bots*: os ataques de *Man-In-The-Browser* usam Cavalo de Troia para roubar informações de login e senhas de uso único do navegador do usuário. *Bots* são *scripts* automatizados que tentam ganhar acesso a contas com credenciais roubadas ou criar contas falsas.

LexID® Digital

O LexID® Digital é a tecnologia que da vida ao Digital Identity Intelligence, criando uma identidade digital exclusiva para cada usuário realizando operação. O identificador é construído usando inteligência relacionada a dispositivos, informações sobre identidade, localização, comportamento, detalhes sobre operações e dados de ameaças. O LexID® Digital ajuda empresas a elevarem as tomadas de decisão relacionada a fraudes e a autenticação do nível de dispositivo para o de usuário, além de combinar inteligência de comportamento offline e online.
O LexID® Digital oferece as seguintes vantagens:

- Conecta elementos de dados online e offline para cada usuário realizando operação.
- Vai muito além de simples análises baseadas em dispositivos e agrupamentos de diversas outras entidades com base em associações complexas, formadas entre ocorrências.
- Identifica uma pessoa de forma consistente, independente de mudanças de dispositivos, localização e comportamento. A inteligência do Digital Identity Network ajuda o reconhecimento preciso do mesmo usuário recorrente por trás de diversos dispositivos, endereços de e-mail, endereços físicos e nomes de conta.

METODOLOGIA DE RESUMO

Relatório geral

- O Relatório sobre crimes cibernéticos da LexisNexis® Risk Solutions foi baseado em ataques de crimes cibernéticos detectados pelo LexisNexis Digital Identity Network (o Digital Identity Network) entre julho e dezembro de 2020, durante análises em tempo quase real das interações dos clientes em toda a sua jornada online, desde a criação de novas contas, passando pelo *login*, pagamentos e outras operações não essenciais como redefinição de senha e transferências.
- A legitimidade das operações são verificadas com base em centenas de atributos, inclusive identificação de dispositivo, localização geográfica, histórico e análises comportamentais.
- O Digital Identity Network e a sua ferramenta de política em tempo quase real oferecem informações exclusivas sobre identidades digitais globais em aplicativos, dispositivos e redes.
- Os clientes da LexisNexis Risk Solutions se beneficiam de uma visão global de riscos, aproveitando regras mundiais em políticas sob medida, que são ajustadas para as suas empresas.
- Os ataques mencionados no relatório são baseados em operações de "alto risco" conforme classificação de nossos clientes globais.

Vinculação de rede de fraudes

- Os dados sobre o desempenho de fraudes foram coletados entre julho e dezembro de 2020 com base em dispositivos, endereços de e-mail e números de telefone registrados como fraudulentos no Digital Identity Network.
- Exposição monetária calculada sobre o valor operacional de pagamento observado em risco entre julho e setembro de 2020, com base na identificação de todas as operações associadas àquela ocorrência confirmada fraudulenta (e grupo associado de entidades) durante esse período. Não inclui nenhum valor financeiro em risco de clientes que não forneceram dados operacionais de pagamento.

PROCESSAMENTO E ANÁLISE DE DADOS

O volume geral de operações processadas pelo Digital Identity Network entre julho e dezembro de 2020 foi US$ 28.4 bilhões.

O Relatório sobre crimes cibernéticos da LexisNexis analisa um subgrupo dessas operações que excluem ocorrências não baseadas em operações (como dados de *feedback* e operações teste), assim como movimentações de organizações que são consideradas ponto fora da curva por conta das taxas de rejeição extremamente altas ou nulas registradas. Esse subgrupo soma 24.6 bilhões de operações.

O Relatório sobre crimes cibernéticos usa essas 24.6 bilhões de operações para calcular o volume geral de operações global e por região. Há 880 mil operações sem endereço de IP, as quais, portanto, não podem ser atribuídas a nenhuma região. São, na maioria, sessões desconhecidas em que uma organização não envia o endereço IP de entrada.

Esse subconjunto de 24.6 bilhões de operações também é usado para analisar os ataques de *bots* automatizados. Isso inclui sessões conhecidas relacionadas a ocorrências individuais, assim como sessões desconhecidas que às vezes podem ser um recurso do tráfego de *bot,* visto que a velocidade de ataque não registra todos os dados completos de criação de perfil.

O volume de ataques iniciados por humanos é calculado em um outro subconjunto adicional de 20,9 bilhões de operações, classificadas como “sessões conhecidas” relacionadas a ocorrências individuais.

Esse subconjunto exclui ocorrências que não coletaram dados de inteligência de identidade digital devido a uma criação de perfil malsucedida.

LexisNexis®
RISK SOLUTIONS

PARA MAIS INFORMAÇÕES:

risk.lexisnexis.com/fraudes

risk.lexisnexis.com.br/products/threatmetrix

Sobre a LexisNexis Risk Solutions

A LexisNexis® Risk Solutions aproveita 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, Geórgia, 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.

Para mais informações, acesse www.risk.lexisnexis.com e relx.com