RELATÓRIO 2021

Atividade Criminosa Online no Brasil

Um relatório completo sobre fraudes digitais e vazamentos de dados no Brasil durante 2021: o ano que especialistas estão chamando de pior ano da história da proteção e privacidade de dados pessoais no país.

São Paulo, Fevereiro de 2022.

O que você vai encontrar neste relatório

Highlights 2021

720 mil

cartões vazados durante o ano, levando o Brasil ao topo no ranking pelo segundo ano consecutivo.

37,7%

das páginas de phishing tiveram empresas do e-commerce como alvo durante o ano de 2021.

123 mil

perfis falsos foram identificados em 2021, o que representa 58% do total de incidentes de marca detectados no ano todo.

- Esses 123 mil perfis falsos detectados em 2021 ultrapassam em **14,21%** os 108 mil identificados em 2020;

- **13 mil aplicativos mobile fraudulentos foram identificados em 2021**, 103,4% a mais do que em 2020. Destes, 23,4% se passaram por marcas do setor financeiro;

- **A Axur detectou 24 vazamentos de dados em 2021**, somando 910 GB de informações sensíveis, como CPF, CNPJ, emails e credenciais completas. Computamos **2,8 bilhões de registros**;

- **273 milhões de credenciais foram detectadas em 2021**, sendo que 98% foram expostas em grandes vazamentos;

- **2,1 bilhões de cartões de crédito e débito foram detectados em 2021** distribuídos em 75 mil BINs diferentes, sendo que 95,9% estavam dentro da data de validade;

- 25 mil páginas de phishing identificadas em 2021, queda de 36,84% em relação a 2020.

PANORAMA DE CIBERSEGURANÇA

O ano que times e profissionais de segurança da informação não esperavam

A cada **8 segundos**, uma tentativa de fraude digital foi realizada contra um consumidor brasileiro na primeira metade de 2021.

É o que diz um levantamento realizado pela Serasa Experian, que concluiu que, pelo menos, **1,9 milhão de fraudes digitais aconteceram no período**. Só o mercado financeiro ocupa 63,1% do total, com pelo menos 1,2 milhão de tentativas de fraudes.

Esses números revelam que não são acontecimentos isolados. De uma década para cá, os cibercriminosos estão cada vez mais engenhosos e evoluindo até mais rápido do que a cibersegurança no Brasil.

E, toda vez que um cliente da sua empresa é vítima de um golpe ou fraude digital envolvendo sua marca, há consequências. E a primeira é imediata: o dano reputacional.

Em um mundo de redes sociais, conectado 24/7, no qual consumidores têm inúmeros canais para contar suas experiências com uma marca, é difícil sair ileso de uma fraude digital. Um estudo da PwC aponta que 60% dos consumidores param de fazer negócios com uma empresa que não protege seus dados pessoais: e isso vale tanto para vazamentos de dados, quanto para fraudes digitais em nome da empresa.

A segunda consequência pode demorar um pouco mais para aparecer: o prejuízo financeiro. O cibercrime custa caro: em 2021 o prejuízo com crimes virtuais chegou aos 6 trilhões de dólares.

Só a título de comparação, em 2020 o PIB do Brasil não ultrapassou a marca de 1,5 trilhão de dólares. Isso quer dizer que a perda global com o cibercrime, só em 2021 foi equivalente a quatro vezes PIB do Brasil em 2020. De acordo com a Cybersecurity Ventures, anualmente, até 2025 o estrago será de 10,5 trilhões de dólares.

Melhor estar preparado.

Fabio Ramos, CEO da Axur

FRAUDES DIGITAIS

Fraude Digital fez história no Brasil

O ano passado deixou uma coisa bem clara para as empresas no Brasil: é impossível crescer e se manter saudável sem monitorar, detectar e remover ameaças digitais da internet.

Tão grande quanto o crescimento do e-commerce, das fintechs e da aceleração digital que a pandemia trouxe de presente inusitado para as empresas, o crescimento cibercriminosos e das fraudes digitais é notável. E, quanto mais sua empresa expande sua presença no ecossistema digital, mais deveria investir no tratamento dos riscos digitais.

Além disso tudo, o sentimento do consumidor ao ser enganado é um bom ponto de partida para entender a necessidade de se prevenir contra fraudes digitais que podem afetar as pessoas que fazem ou querem fazer negócios com sua empresa. De acordo com um estudo realizado pela NortonLifeLock, **52% dos consumidores sentem raiva ao serem alvos de fraudes**, com essa raiva ligada não ao fraudador, mas sim à marca pelo qual o cibercriminoso se passou. A sensação é de que a culpa é da empresa e não do cibercrime. Ao mesmo tempo, 46% se sentem estressados e 41%, vulneráveis.

Outra pesquisa local destaca o sentimento de medo. De acordo com uma pesquisa realizada pela FEBRABAN - Federação Brasileira de Bancos, 86% dos brasileiros têm medo de ser vítima de uma fraude virtual ou de ter seus dados pessoais violados. Quanto aos dados, falaremos a respeito mais adiante.

A ingenuidade, desinformação e a vulnerabilidade humana imperam nesse cenário, pois, de acordo com uma pesquisa da Dinamo Networks, **80% das fraudes digitais estão ligadas à engenharia social**. Ao contrário do que o senso comum acha: o cibercriminoso não necessariamente é um hacker extremamente habilidoso, com técnicas excepcionalmente sofisticadas. Esse número comprova que qualquer pessoa com intuito malicioso pode aplicar golpes na internet.

E o Brasil tem se tornado protagonista internacional nessa trama. Em 2020, em um estudo realizado pela ESET, o **Brasil foi considerado o segundo país com mais detecções de ataques de engenharia social na América Latina, com 18,5% das detecções**.

Com a consolidação da digitalização dos negócios, compras e finanças por conta da pandemia, dá para imaginar quanta gente que é nova nos muitos tipos de tecnologias existentes começou a utilizar serviços digitais, ou comprar pela internet. Essa população é vulnerável às fraudes e aos cibercriminosos e se apresenta digitalmente sob risco.

Além de instruir o seu cliente consumidor a não clicar em links suspeitos em qualquer canal, implementar a autenticação de 2 fatores, verificar a veracidade da mensagem, promoção ou contato por outros meios e outras técnicas de segurança é de extrema importância também que se sua presença digital seja monitorada além da superfície de ataque tradicional por possíveis ameaças e vazamentos.

As marcas têm a responsabilidade de monitorar seus riscos digitais, de proteger seus clientes de serem enganados em golpes e de terem seus dados pessoais expostos, colaborando com a aderência à **Lei Geral de Proteção de Dados** e contribuindo com a confiança pública na economia digital brasileira.

Ramiro Rodrigues, CISO Global da Axur

Phishing

Total de detecções

25.133 foi o número de páginas de phishing que a Axur identificou ao longo de 2021. Isso é **36,4%** menor do que os mais de **39 mil** casos registrados em 2020.

O último trimestre do ano, com **7.010** páginas falsas, não conseguiu ultrapassar o terceiro trimestre, no qual tivemos **7.639,** mas chegou bem perto, impulsionado pelos eventos de final de ano: Black Friday, Cyber Monday e compras natalinas (Figura 1).

Só entre os dias 15 a 30 de novembro, nós identificamos **1.183 páginas de phishing** tentando se passar por grandes marcas varejistas. Isso representa 46,1% do total de páginas identificadas no mês de novembro. Página. 9

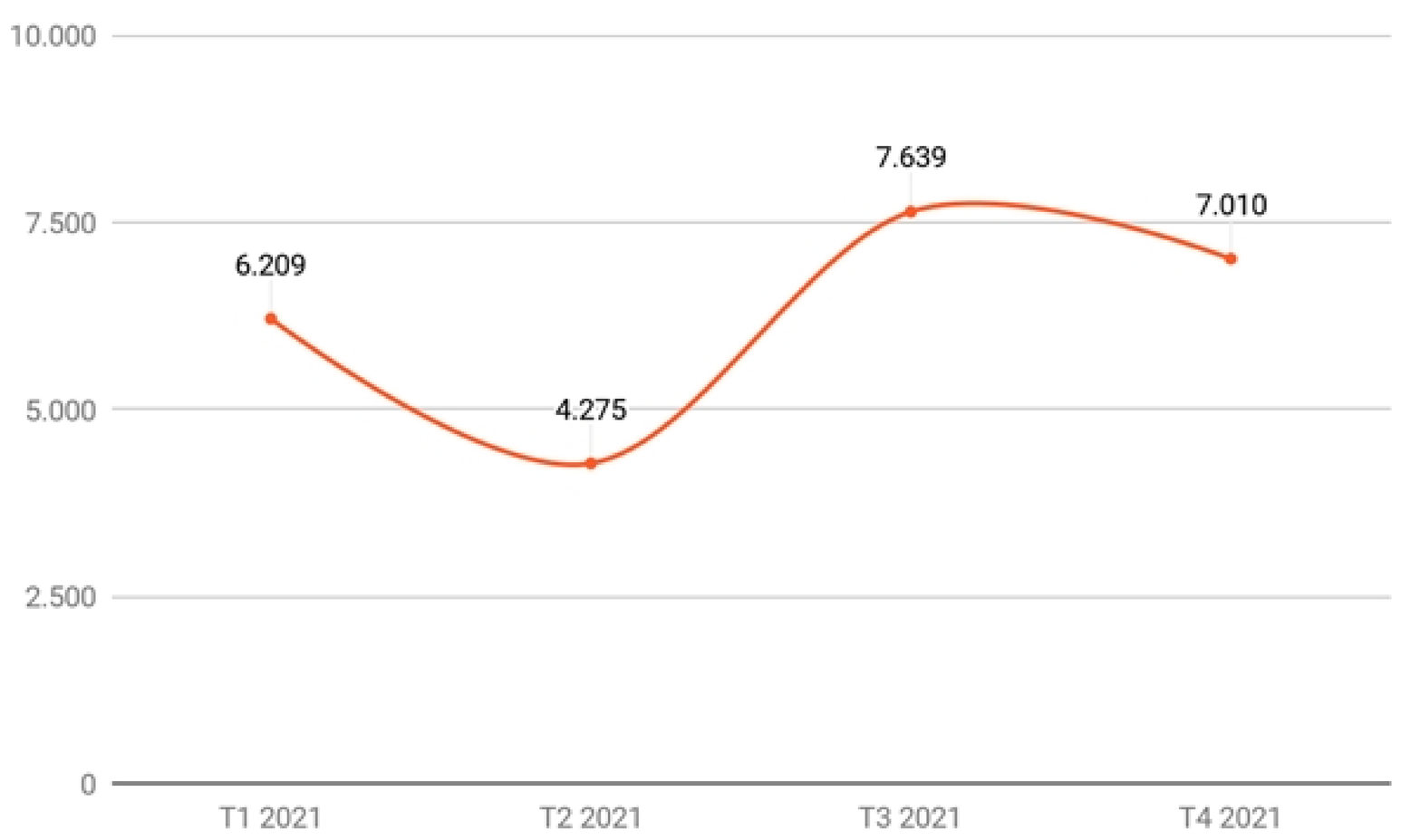


Figura 1. Evolução do número total de casos de phishing detectados no Brasil em 2021.

O segundo semestre de 2021 foi mais intenso do que o primeiro, quando o assunto é detecção de páginas de phishing: tivemos **14.649** casos de julho a dezembro, o que é **36,8%** maior do que os **10.484** casos detectados de janeiro a junho (Figura 2).

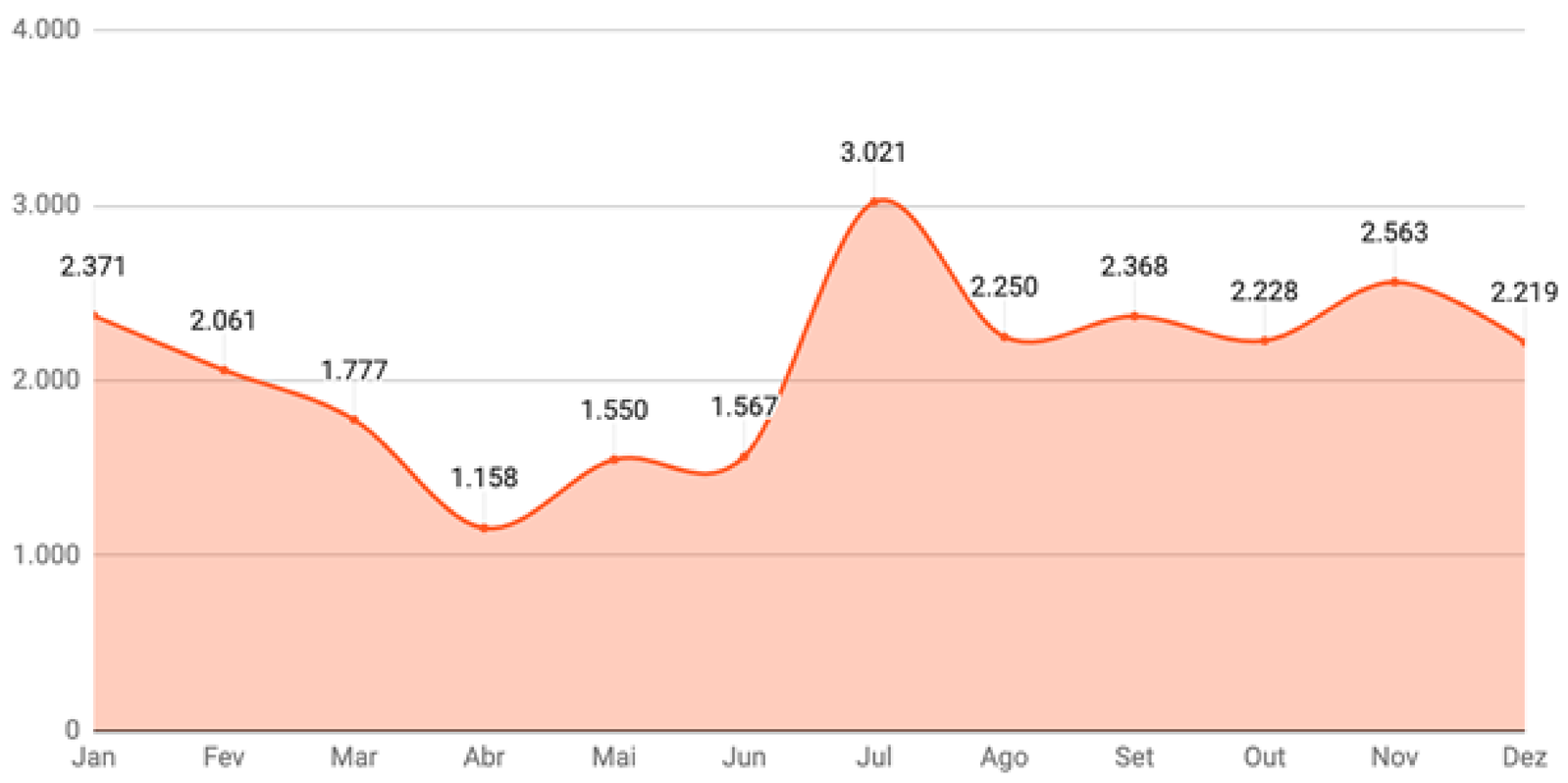


Figura 2. Evolução do número total de casos de phishing detectados no Brasil em 2021.

Se compararmos ao primeiro e segundo semestre de 2020, podemos entender que o primeiro semestre de ambos os anos (2020 e 2021) têm papel fundamental na diminuição de phishing que presenciamos de um ano para o outro.

Em 2020, a Axur detectou **20.482** páginas de phishing só no primeiro semestre. Contra as **10.484** páginas identificadas no primeiro semestre de 2021, temos uma diferença de **48,8%**, isto é, quase metade a menos.

A diferença entre o segundo trimestre de 2020 e de 2021 foi menor: **23,2%**, se considerarmos as **19.086** detecções de julho a dezembro de 2020, contra as **14.649** de 2021 (Figura 3).

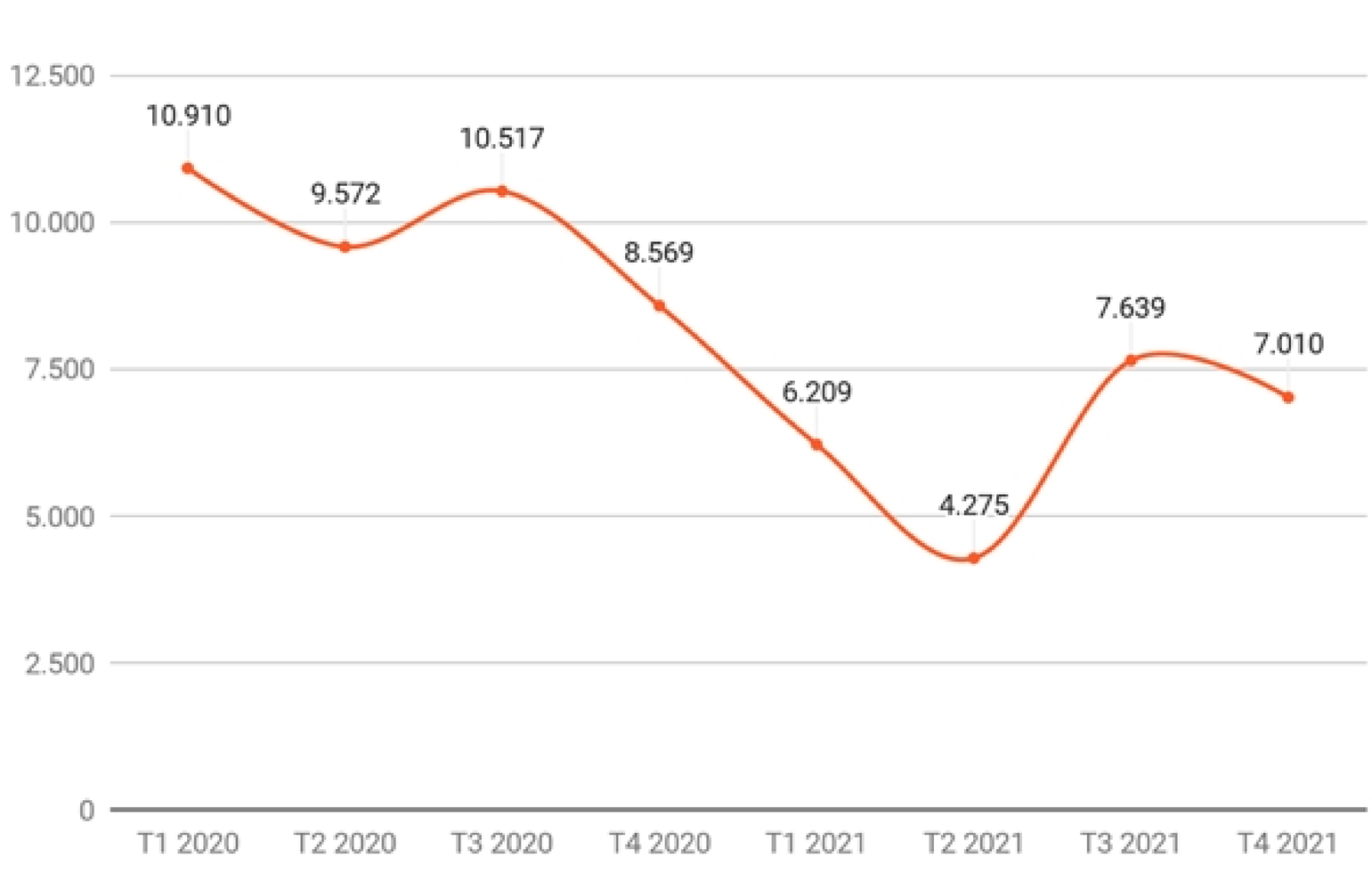


Figura 3. Evolução do número total de casos de phishing detectados no Brasil de 2020 a 2021, separados por trimestre.

Essa variação semestral revela padrões de comportamentos tanto dos cibercriminosos quanto do mercado, incluindo de nossos clientes. Em 2021, esse tipo de golpe completou 25 anos de história, com uma vasta lista de inovações e melhorias por parte dos criminosos.

Nós sabemos que os estelionatários digitais são motivados pelos ganhos financeiros, que podem ser maiores ou menores dependendo da marca que eles escolhem fraudar e construir uma campanha de phishing, por exemplo.

Da nossa experiência, comprovamos que após o início do monitoramento e da remoção de ameaças digitais, entre elas o phishing, o criminoso tende a identificar quais marcas estão derrubando suas tentativas de fraudes e abandonam esses alvos.

Fraudar uma marca que monitora seu perímetro digital custa caro, ainda mais se for uma modalidade de golpe que exige certo nível de esforço, como é o caso do phishing.

Além disso, movimentos como Open Banking, a onda de grandes vazamentos de dados no Brasil e a instauração completa da LGPD, levaram as empresas a olhar com mais cuidado para o que chamamos de *digital footprint*.

Ao perceber que têm a responsabilidade legal de manter protegidos os seus digital assets, essas empresas adotam práticas para mitigar os riscos cibernéticos, tais como: política interna de cibersegurança, parceiros especializados em pentest, invasões, monitoramento e remoção de ameaças digitais (do phishing ao vazamento de dados).

Segmentos mais atingidos

Mês a mês durante o ano todo de 2021, podemos ver três grupos de empresas que marcaram presença nas páginas de phishing dos cibercriminosos: setor financeiro, varejo online e empresas SaaS, que oferecem serviços baseados em aplicações digitais.

Foi-se o tempo em que programas de milhas e passagens aéreas eram foco dos fraudadores. Pelo gráfico abaixo dá pra ver a discrepância desses três primeiros setores em relação ao resto das detecções.

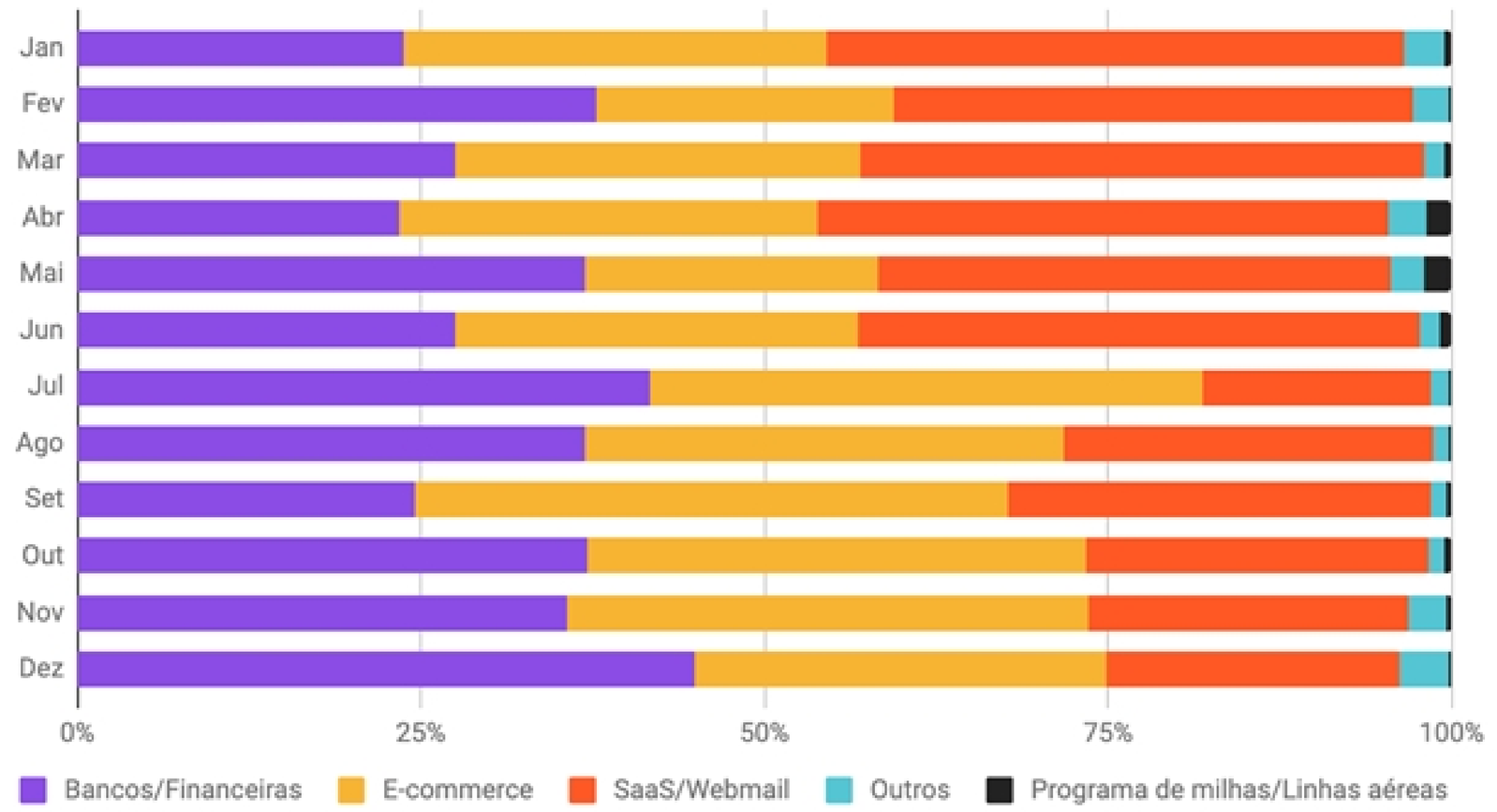


Figura 4. Percentual que cada setor representa do total de casos de phishing identificados mês a mês em 2021.

Em primeiro lugar, as empresas do setor financeiro, como bancos, cooperativas e, principalmente, as fintechs, detém **34,4% do total de páginas de phishing** identificadas em 2021. Isso soma **7.957** páginas que tentaram vender algum tipo de serviço financeiro para os clientes.

Isso pode ser explicado por dois motivos: **financeiro e comportamental.** Primeiro, financeiramente falando, as fintechs demonstraram um crescimento invejável no Brasil e 2021 foi um ano tremendo para empresas desse tipo.

Também é preciso levar em consideração o aumento da adesão pelos serviços digitais, impulsionada pela covid-19, principalmente, se olharmos os segmentos de bancos, fintechs e e-commerces. Cada vez mais consumidores estão deixando de ir às agências bancárias para realizar transações, bem como estão deixando de ir às lojas para fazer compras.

De março de 2020 a outubro de 2021, mais de 2 mil agências bancárias espalhadas pelo Brasil todo fecharam. Outro dado revela que, desde o início da pandemia, **89 cidades perderam agências bancárias**, indicando que 43% das cidades brasileiras não têm mais esse serviço de atendimento presencial.

Esse dado demonstra a adesão pelos serviços digitais, por meio de smartphones, tablets e computadores. No e-commerce, isso não é diferente. Em 2020, **75 mil lojas fecharam as portas por conta da pandemia e pela adesão das compras online**, diz um levantamento realizado pela Confederação Nacional do Comércio. De acordo com um estudo realizado pela FGV, as vendas online representam 21,2% do faturamento do varejo no Brasil.

Voltando para o mercado financeiro, no início do ano, era esperado que as fusões e aquisições entre fintechs crescessem pelo menos **50%**. Além disso, **20%** de todo capital de risco investido em 2021 foi destinado às fintechs: **130 milhões de dólares**. Por si só, esses dados já são uma imensa propaganda para o setor. E os cibercriminosos também estão atentos às notícias.

Além disso, uma coisa foi acentuada no comportamento do consumidor digital em 2021: o endividamento. De acordo com a CNC, Confederação Nacional do Comércio, na Pesquisa de Endividamento e Inadimplência do Consumidor 2021, **70,9% das famílias brasileiras estão com algum tipo de dívida**.

Como forma de se aproveitar disso, os golpistas investem em páginas de phishing que prometem dinheiro fácil, renegociações ou a contratação de prazos mais longos.

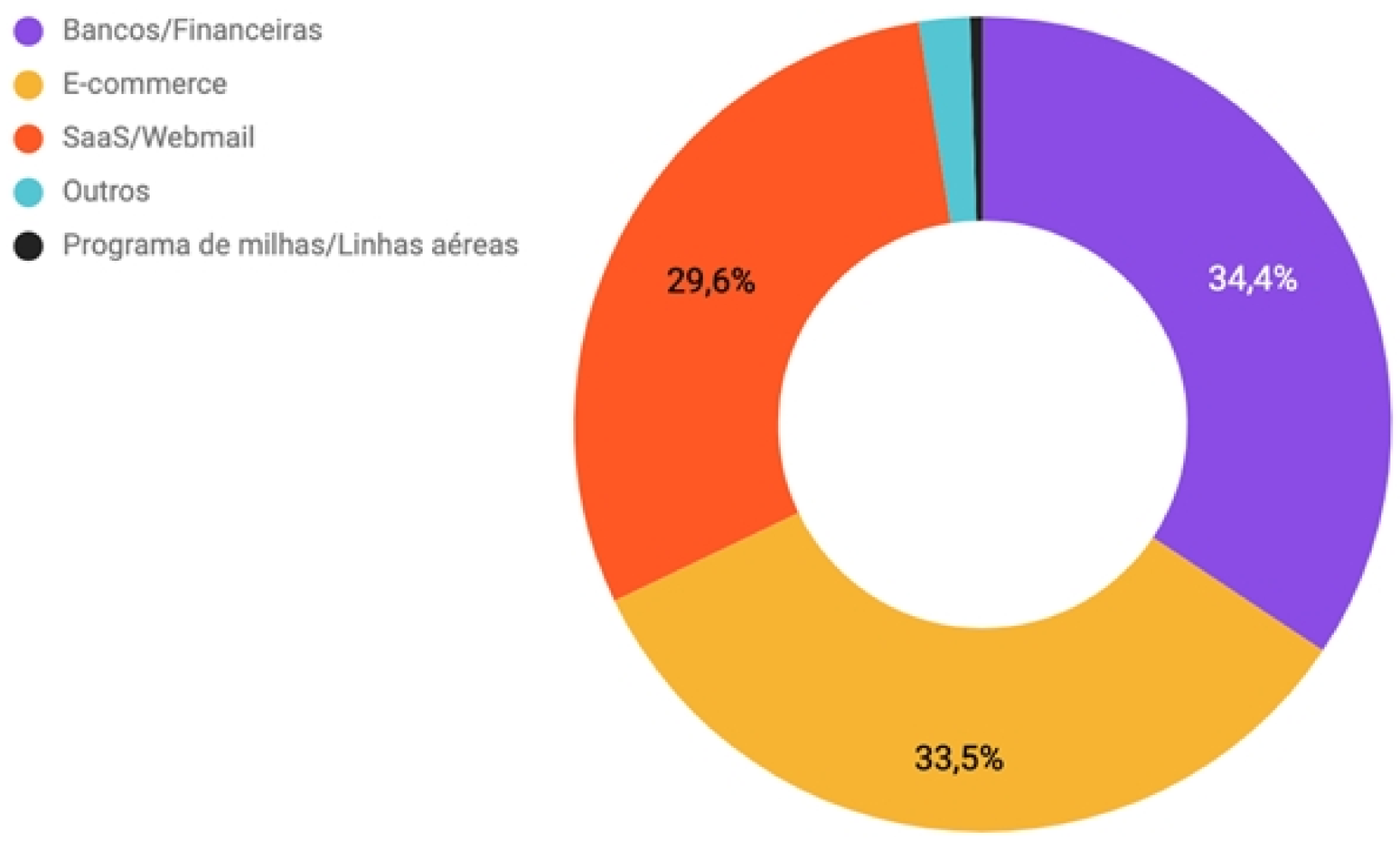


Figura 5. Percentual que cada setor detém das páginas de phishing identificadas em 2021

Em segundo lugar está o e-commerce e lojas físicas que implementaram as vendas digitais, com **33,5%**, isto é, **7.755 páginas de phishing detectadas em 2021**.

A mesma Confederação Nacional do Comércio também indica que as recentes mudanças no comportamento do consumidor brasileiro, impulsionado pela pandemia de covid-19, são responsáveis por um crescimento de **38%** do e-commerce nacional, que **fecharia o ano de 2021 com o faturamento de 304 bilhões de reais para o setor.**

Além disso, de acordo com a Receita Federal, o consumidor brasileiro deve manter vivo o hábito de comprar online, comodidade que se comprovou útil na pandemia: uma pesquisa realizada em sete capitais brasileiras revela que **59,4%** compraram dessa maneira durante o ano e que **44%** dos entrevistados devem seguir comprando online no próximo ano.

Em terceiro lugar, estão empresas que se configuram como provedores de serviços digitais para consumidores e outras empresas. Com a pandemia, muitas empresas foram obrigadas a digitalizar suas operações e, com isso, contrataram mais e mais serviços digitais: provedores de nuvem, ferramentas de gestão financeira, de equipes, bem como ferramentas de comunicação, como de mensagens instantâneas e de videoconferência.

De acordo com o IDC, em 2020, durante o início da pandemia, **o mercado de tecnologia da informação recebeu investimentos de 200 milhões de reais**, e cresceu 22,9%.

Servidores de hospedagem e Top-Level Domains

No último trimestre de 2021, a Axur identificou sites de phishing espalhados por **178 servidores**. Abaixo você pode ver os 10 servidores mais utilizados pelos criminosos:

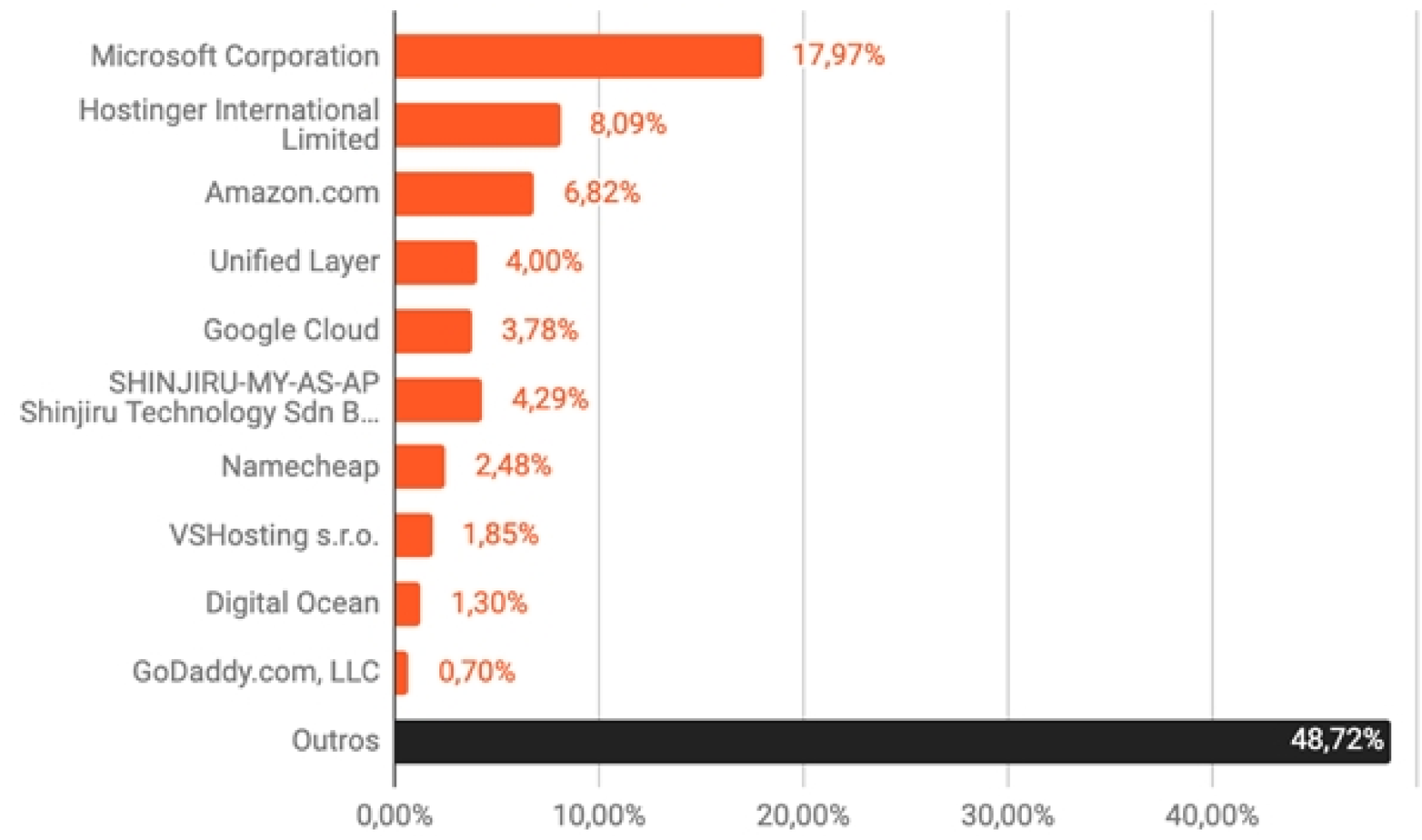
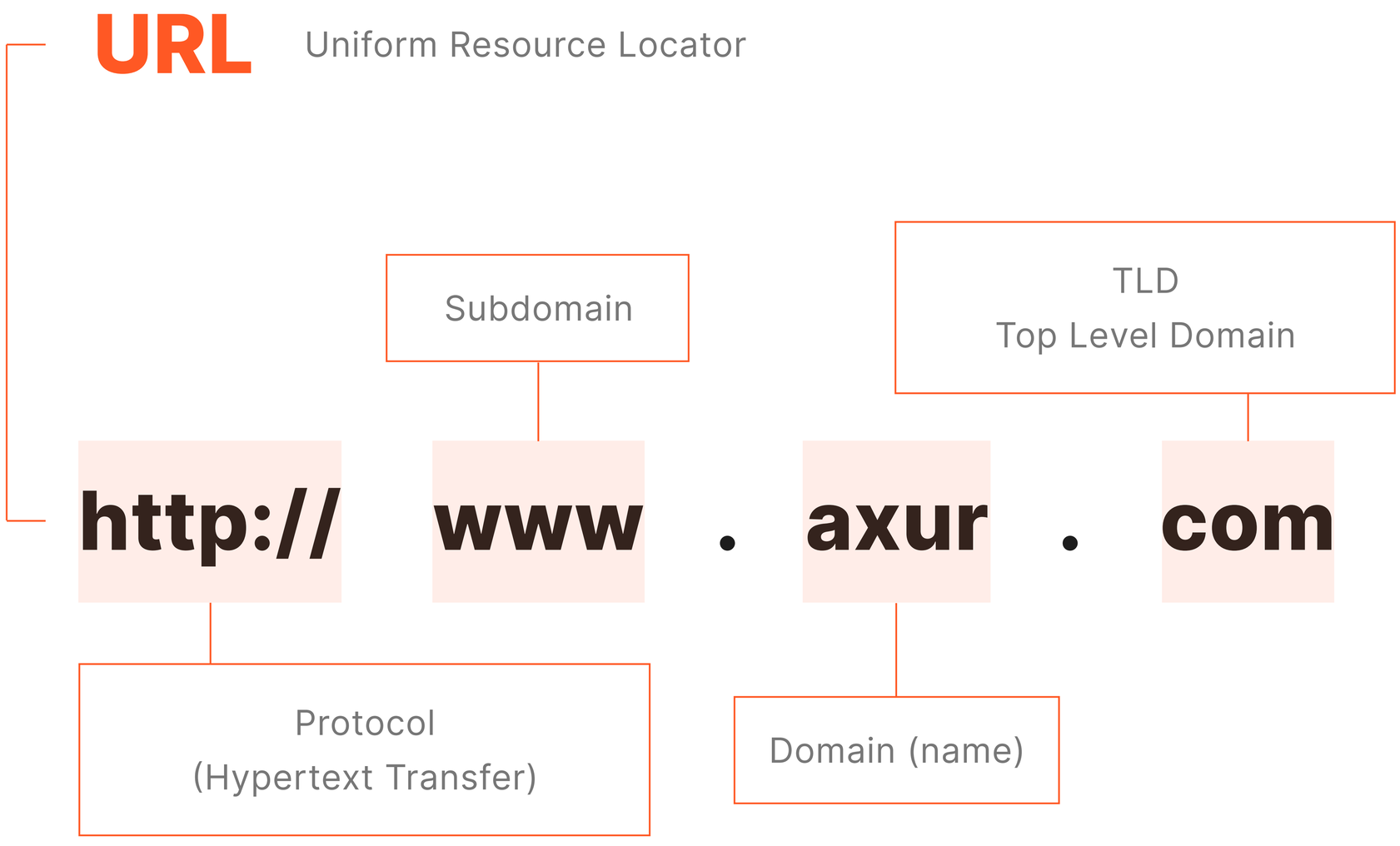


Figura 6. Top 10 servidores de hospedagem utilizados para hospedar páginas de phishing no último trimestre de 2021.

28,4% dos domínios de phishing identificados no trimestre estavam atrelados ao Cloudflare, serviço de CDN que visa melhorar a velocidade de carregamento da página e resposta do servidor, geralmente utilizados para para provedores que não têm serviço no Brasil, como GoDaddy, Hostgator, Hostinger e outros.

Isso é uma tentativa dos cibercriminosos de mascarar o verdadeiro servidor utilizado na fraude, dificultando o takedown, isto é, a derrubada do conteúdo infrator.

Outro aspecto a ser analisado que nos dá pistas sobre o comportamento cibercriminosos é a utilização das TLD ou Top-Level Domains que nada mais são o que chamamos de sufixo de domínio, ou seja, aquilo que está depois do nome do domínio. **Como no infográfico abaixo:**



Em muitos casos, o TLD serve para identificar o propósito do site em questão. Sabemos que os sites **.com** tem um propósito comercial e que os sites **.com.br** provavelmente são de negócios situados no Brasil.

Ao diversificar o uso das TLDs, os criminosos estão tornando a detecção do domínio mais difícil e, consequentemente, tentando escapar do takedown.

Vejamos abaixo os 10 mais utilizados:

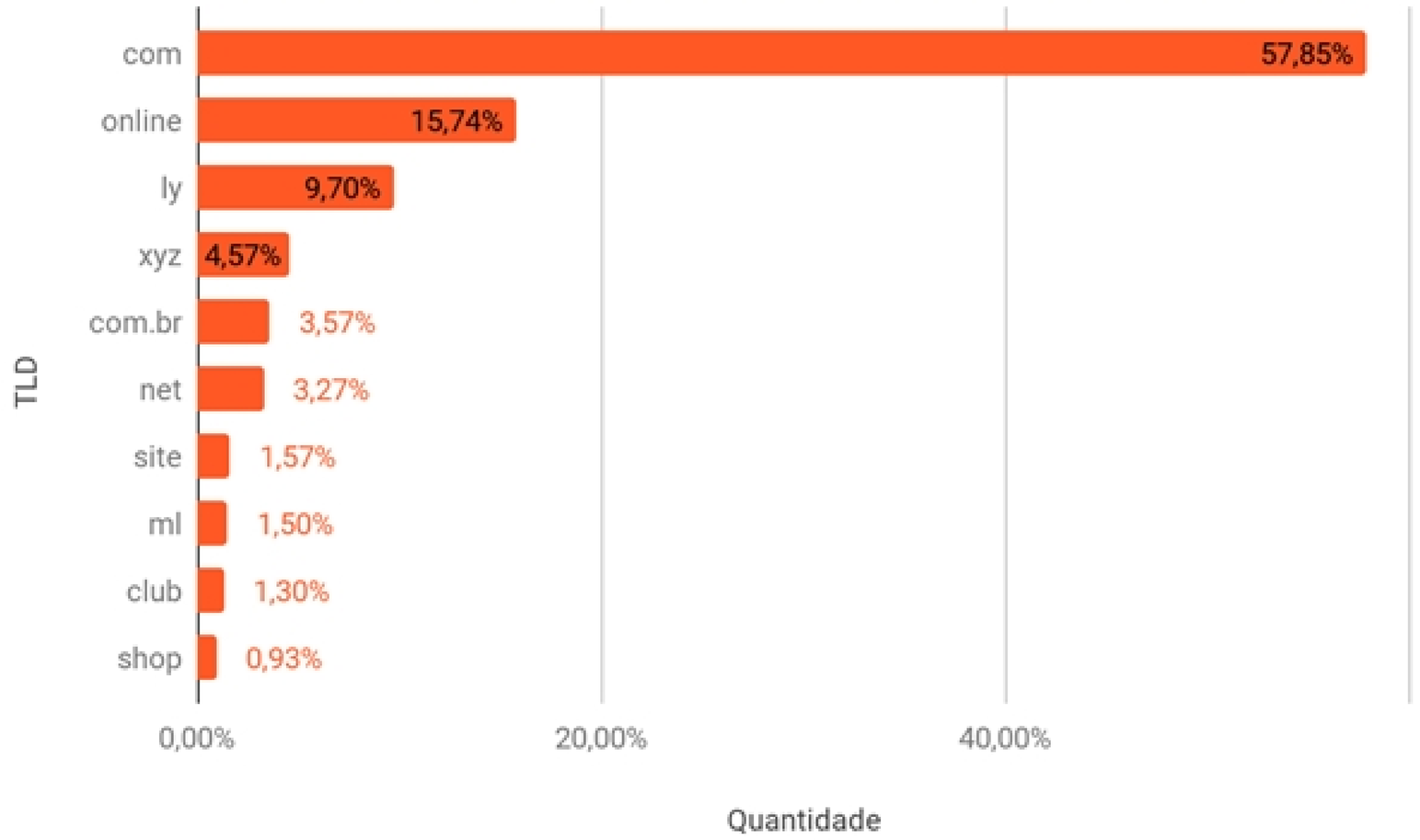


Figura 7. Top TLDs mais utilizadas pelos cibercriminosos nas páginas de phishing detectadas no quarto trimestre de 2021.

Ao analisarmos o gráfico, notamos que 58,85% dos domínios identificados pela Axur no trimestre estão com um domínio genérico comercial. "online", "net", "xyz" são exemplos de TLDs bastante comuns, o que chamamos de Generic Top-Level Domains, ou gTLD.

Os criminosos usam esses domínios para criar sites clonados com diferentes terminações, todos com páginas de phishing prontas para roubar as informações pessoais das vítimas que não se atentam à terminação da URL.

É como se você procurasse por **axur.com** e encontrasse um anúncio ou um resultado de pesquisa com **axur.net**. Como é um domínio de sintaxe genérica, é provável que você clique, pensando que estaria prestes a acessar o site original da empresa.

Incidentes em uso indevido de marca

Total de detecções no trimestre

Em 2021, nós detectamos **210.906 incidentes que faziam uso indevido das marcas** monitoradas pela Axur. Isso é 14,7% menor do que registramos em 2020, quando registramos mais de 247 mil incidentes.

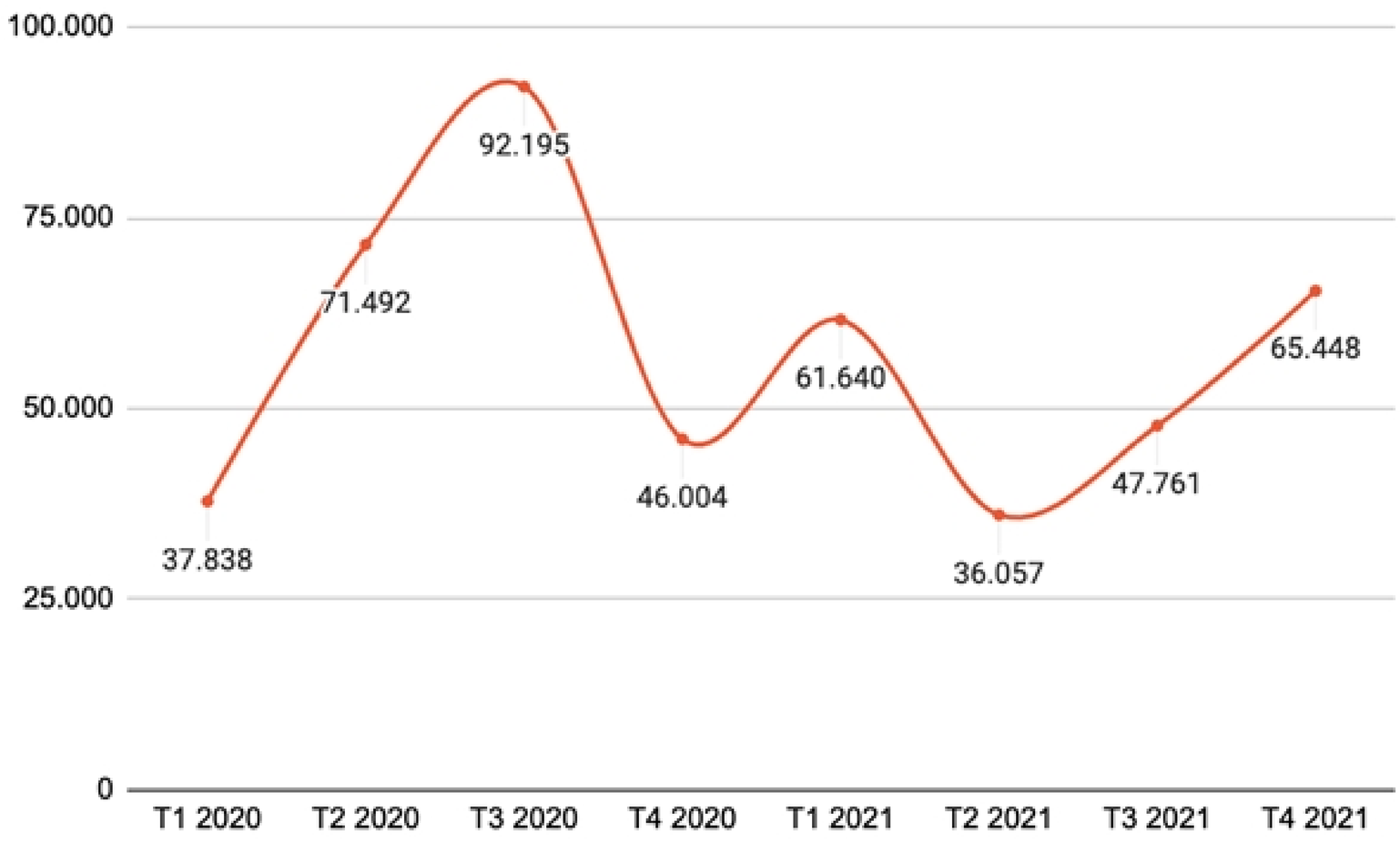


Figura 8. Oscilação trimestral na quantidade de incidentes de marca entre 2020 e 2021, separados por trimestre.

Assim como o phishing, é importante mencionar que as infrações de uso de marca seguem a mesma tendência já mencionada neste relatório: quanto maior o poder de monitoramento e remoção de ameaças virtuais uma marca tem, menor é o número de tentativas fraudulentas envolvendo essa marca entre os cibercriminosos.

Isso explica a queda de 14,7% de 2020 para 2021, que consideramos quase inexpressiva, dado o volume total de fraudes que continuam a envolver marcas famosas. Nós queremos pontuar aqui os novos padrões de comportamentos envolvendo essas fraudes. Veja o gráfico abaixo:

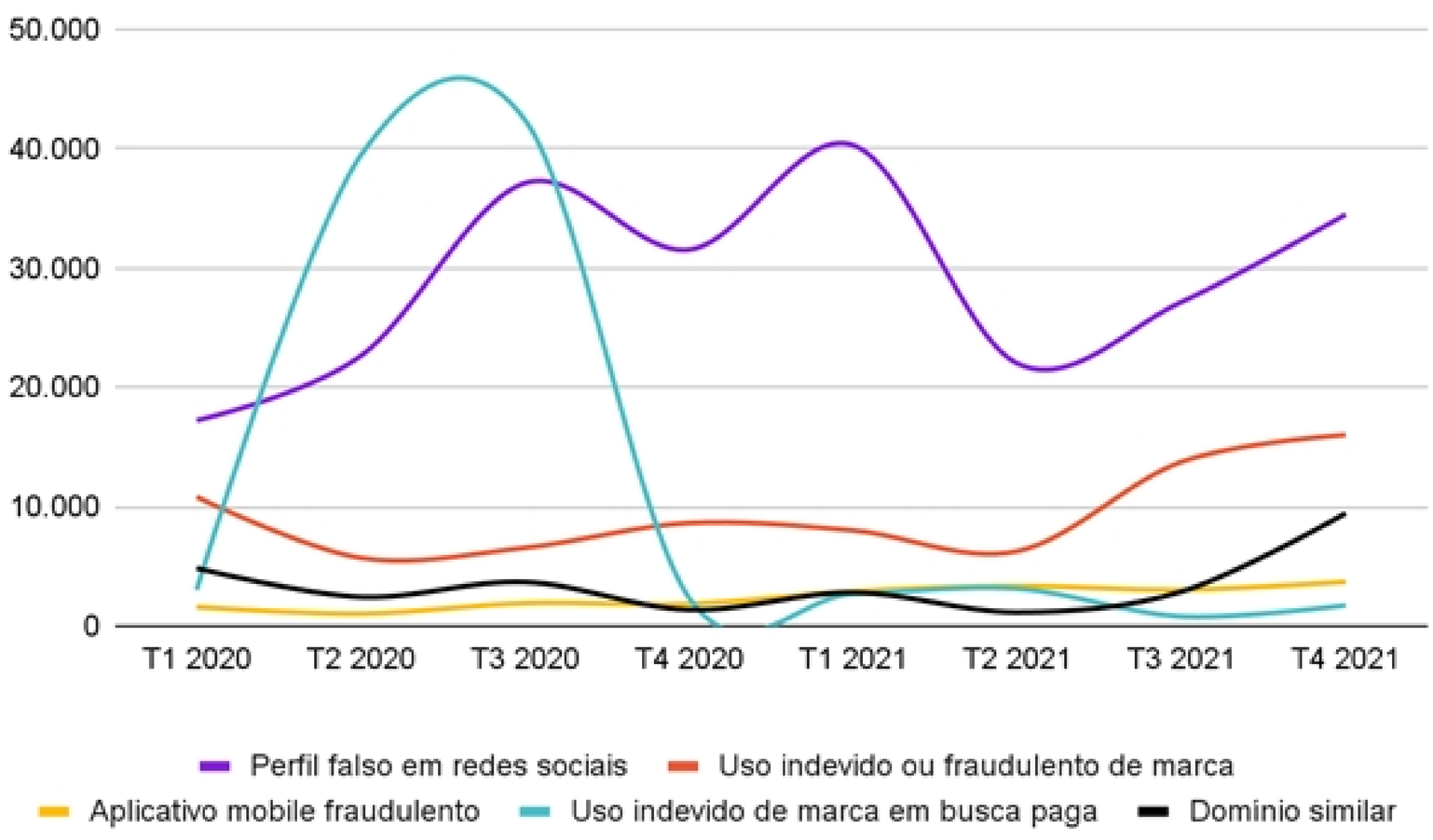


Figura 9. Oscilação dos tipos de infração de uso de marca entre os anos de 2020 e 2021.

É notória a queda pelo interesse dos cibercriminosos por anúncios falsos envolvendo o nome das marcas, que se provou ser uma tática mais fácil de detectar e remover junto ao ISP oficial, que é o Google.

Na Figura 8 podemos notar a adesão de três técnicas pelo cibercrime: os perfis falsos em redes sociais, o uso indevido ou fraudulento de marca e os aplicativos mobile fraudulentos.

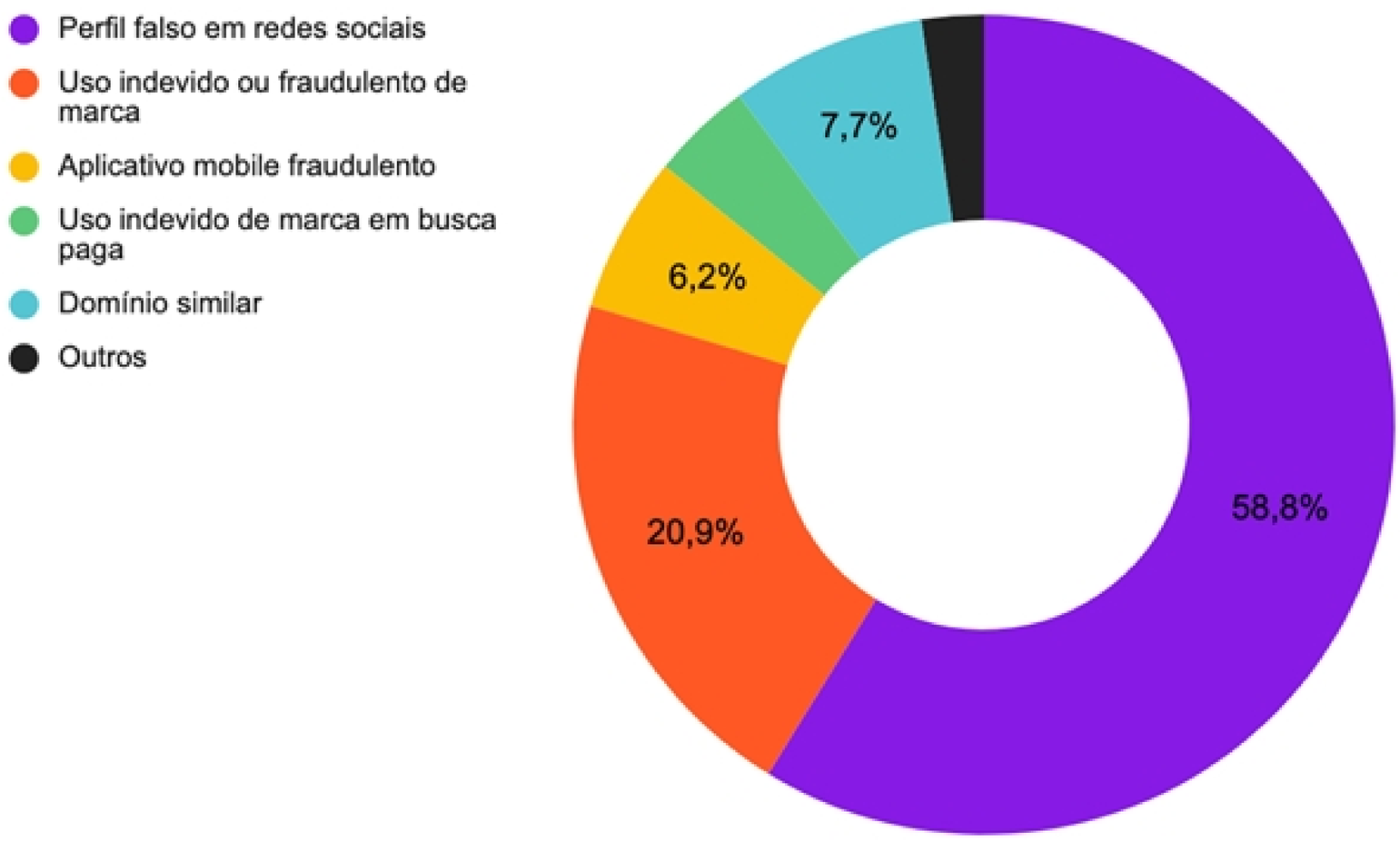


Figura 10. Porcentagem total de incidentes de uso de marca no terceiro trimestre de 2021.

Fica clara a preferência pela utilização dos perfis falsos em redes sociais entre os estelionatários digitais. Em 2021, 58,8% dos incidentes que fizeram uso indevido das marcas monitoradas foram perfis falsos, totalizando **123.982 perfis fraudulentos identificados pela Axur**.

Outra oscilação digna de nota foi o crescimento na criação de apps falsos: **foram identificados 13.032 aplicativos fraudulentos para smartphones em 2021**, 103,4% a mais do que em 2020, consolidando a prática entre os criminosos virtuais.

Vamos nos aprofundar mais nessas práticas abaixo.

Fake Social Profile

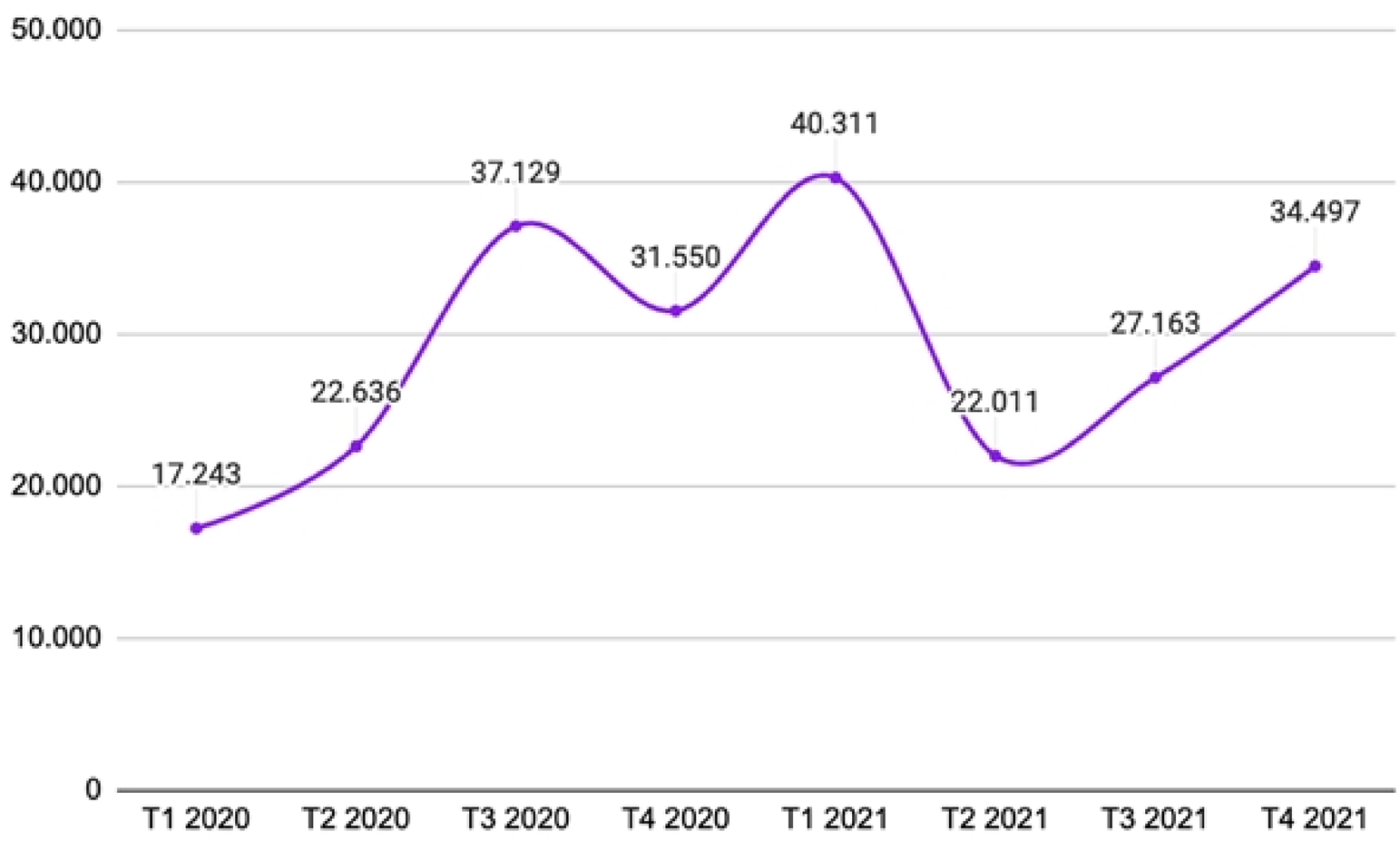


Figura 11. Oscilação trimestral no volume de detecção de perfis falsos entre 2020 e 2021.

O crescimento na utilização de perfis falsos entre os cibercriminosos está ligado à praticidade e muito por conta do custo reduzido desse tipo de golpe, se comparado com uma campanha de phishing, por exemplo.

Também notamos diferenças na popularidade desses perfis falsos no momento da detecção. 78,3% dos perfis falsos não seguiam ninguém. E 57,6% não tinham nenhum seguidor.

Isso quer dizer que 56,1% dos perfis identificados pela Axur não seguiam ninguém e não tinham nenhum seguidor no momento da detecção.

Também trouxemos os termos mais utilizados no trimestre em textos e nomes destes perfis falsos:

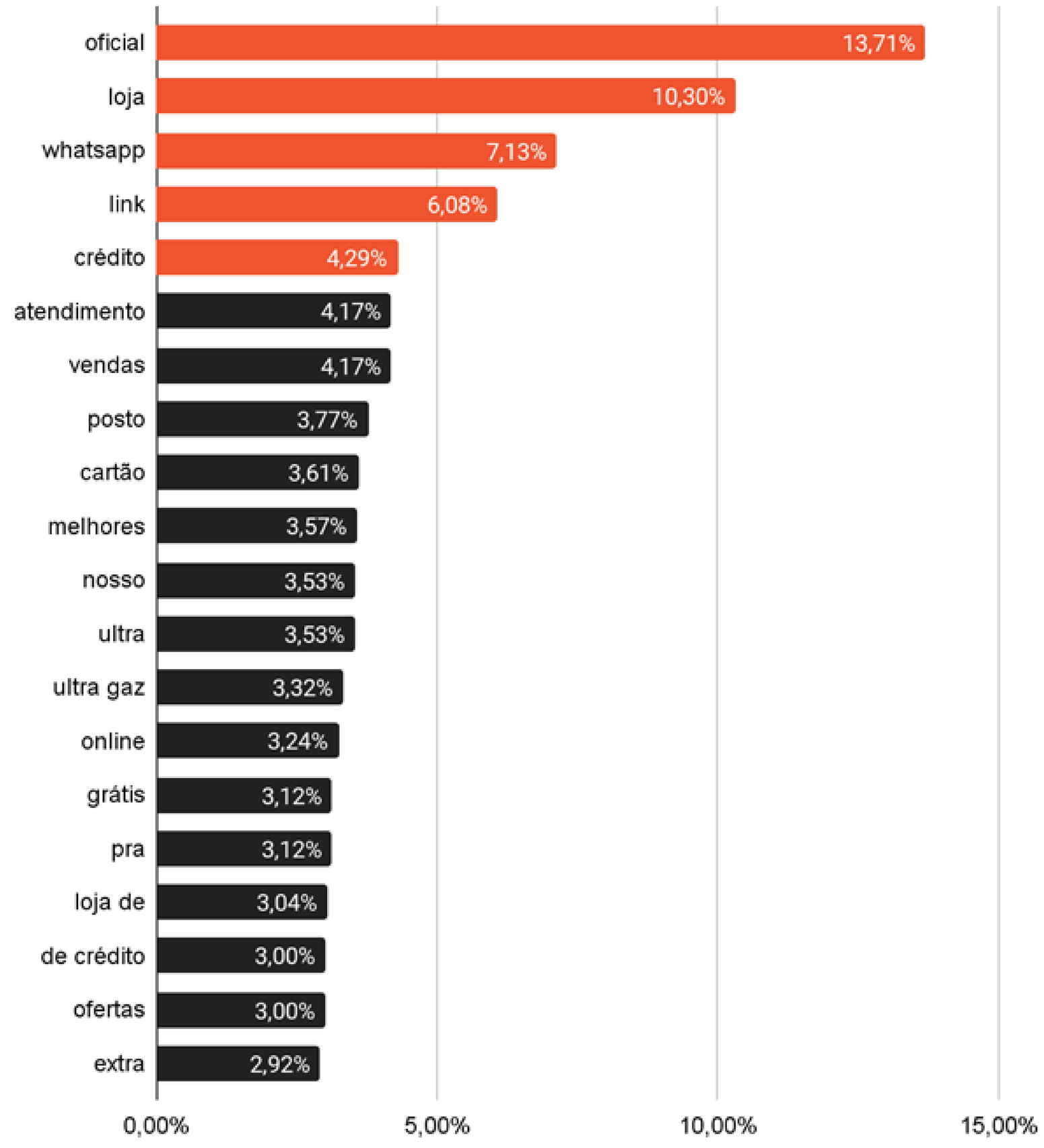


Figura 12. Ranking das 30 palavras mais utilizadas em perfis falsos em redes sociais detectadas em 2021.

Termos relacionados a websites continuam a ocupar as primeiras posições das listas, o que confirma a hipótese que estes perfis são utilizados para pulverizar links de phishing. Mas é interessante notar que as palavras "whatsapp", "suporte", "atendimento", "oficial" e "online" continuam nessa lista, isso porque os cibercriminosos entendem que a utilização desses termos ajuda a gerar maior credibilidade para o perfil falso.

Além disso, neste trimestre, identificamos termos relacionados a serviços financeiros, como "consórcio", "cartão", "crédito" e "empréstimos", indicando que os cibercriminosos também se utilizam da necessidade e, muitas vezes, do desespero de pessoas endividadas para aplicar golpes.

Aplicativo mobile fraudulento

A tendência de crescimento que vemos no gráfico abaixo é quase que linear. E isso estabelece um novo tipo de fraude que vamos ver muito em 2022: **os aplicativos mobile fraudulentos.**

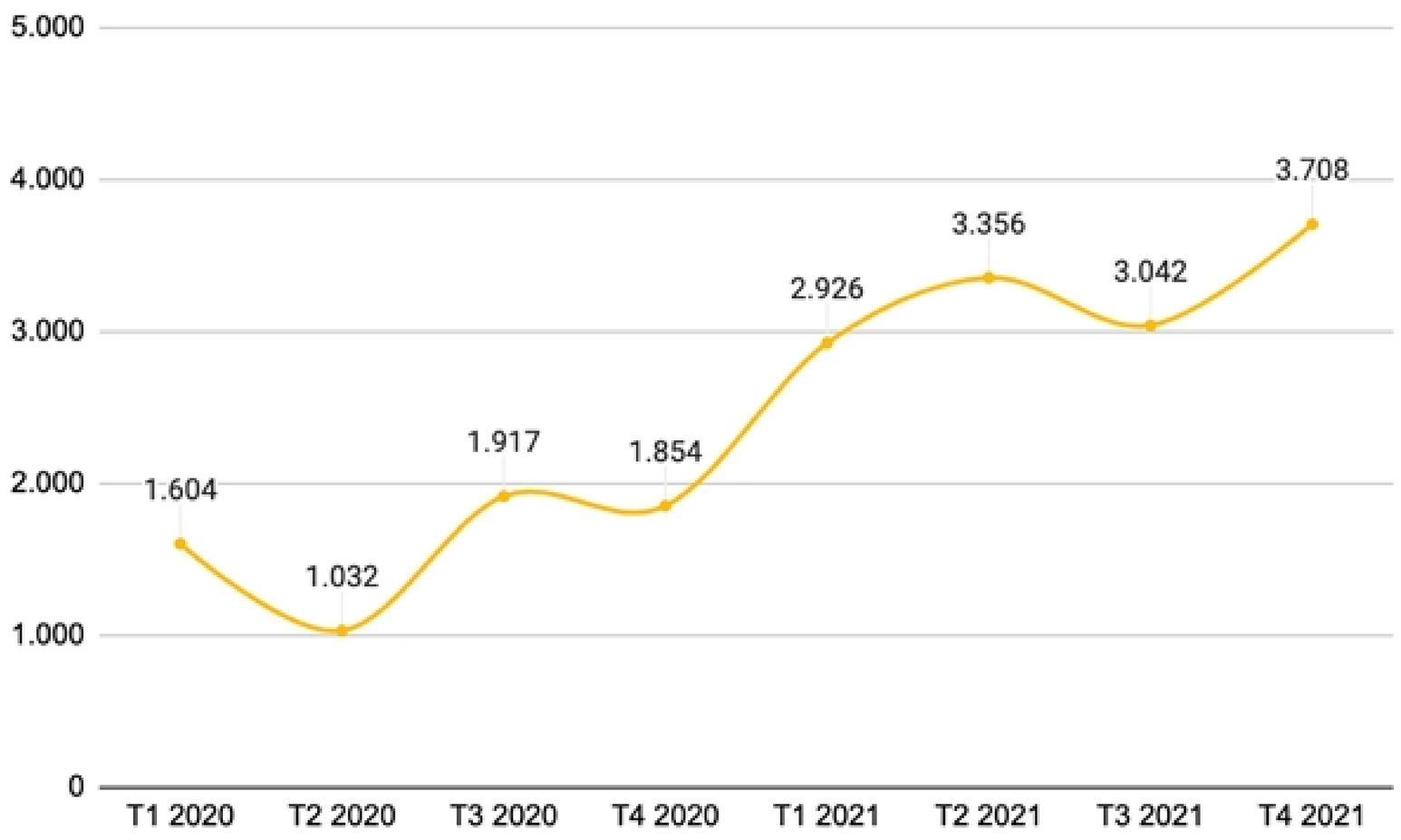


Figura 13. Oscilação trimestral no volume de detecção de aplicativos mobile fraudulentos entre 2020 e 2021.

Assim como o phishing e os perfis falsos, esses aplicativos tomam conta da identidade visual e features das marcas para enganar os consumidores. Além disso, apps que prometem features inovadoras e pouco prováveis também são grandes chamarizes dos cibercriminosos.

Se lembra da versão rosa do WhatsApp, ou da versão dourada? Essa é só mais uma forma de enganar os consumidores desavisados. Da mesma forma, vestindo o logo, cores, produtos de marcas famosas, os cibercriminosos prometem promoções, preços e condições imperdíveis de pagamento para roubar informações dos usuários.

Esses apps podem funcionar tanto como malwares, que se apoderam do dispositivo e armazenam tudo o que é digitado, inclusive com a possibilidade de gravar ligações e tirar fotos.

Ou ainda como plataformas móveis de phishing, que fornecem formulários para os usuários preencherem informações sensíveis direto para as mãos dos cibercriminosos.

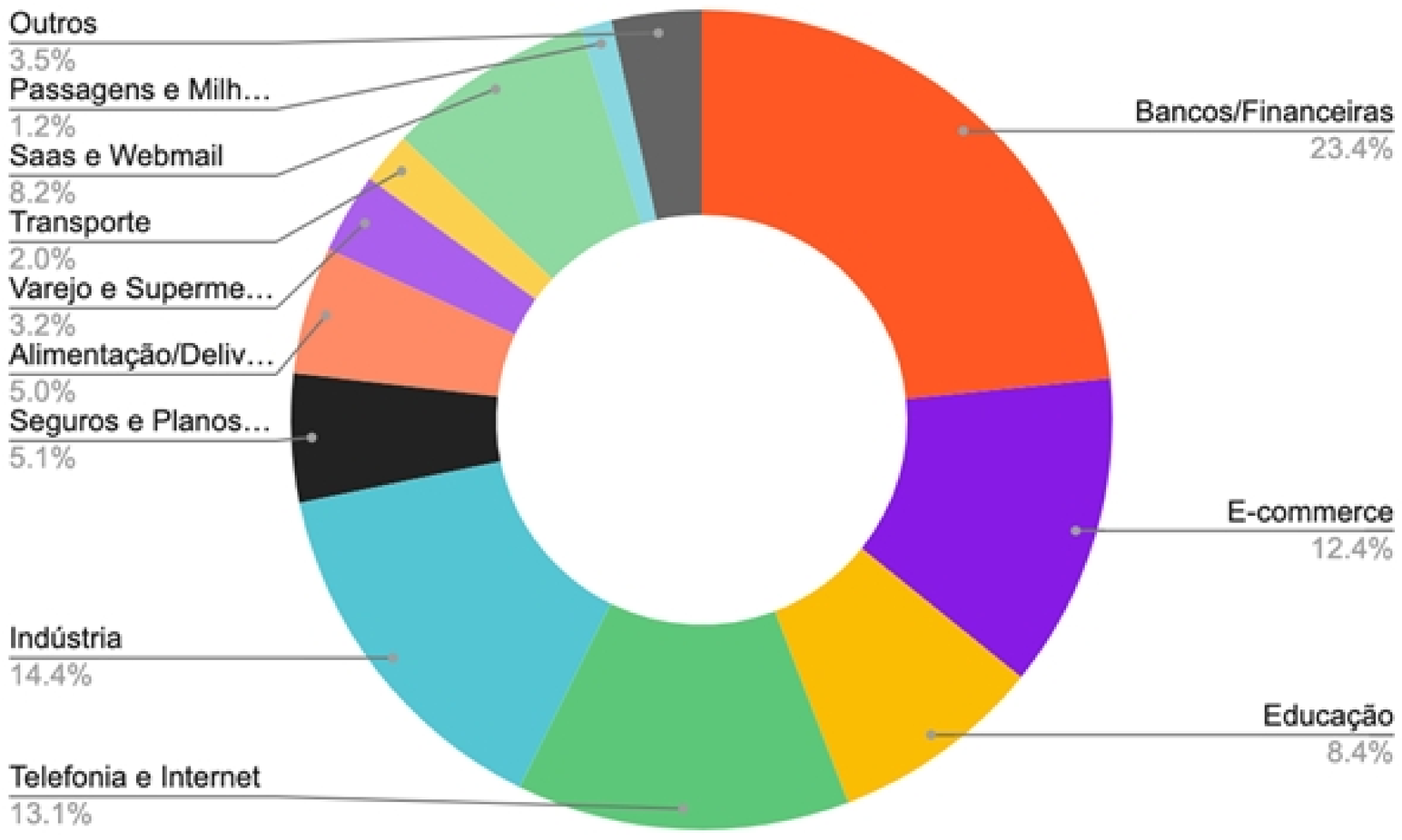


Figura 14. Percentual de aplicativos falsos por setor identificados no terceiro trimestre de 2021.

Outra tendência interessante é que os cibercriminosos têm uma preferência muito clara por fazer o upload dos app falsos em sites que agregam ou fazem review de apps no formato .apk (Figura 14).

97% dos aplicativos mobile fraudulentos identificados no ano são voltados para os usuários Android, enquanto somente 3% dos apps maliciosos estavam em lojas oficiais, como Google Play (1,7%) e Apple Store (1,3%).

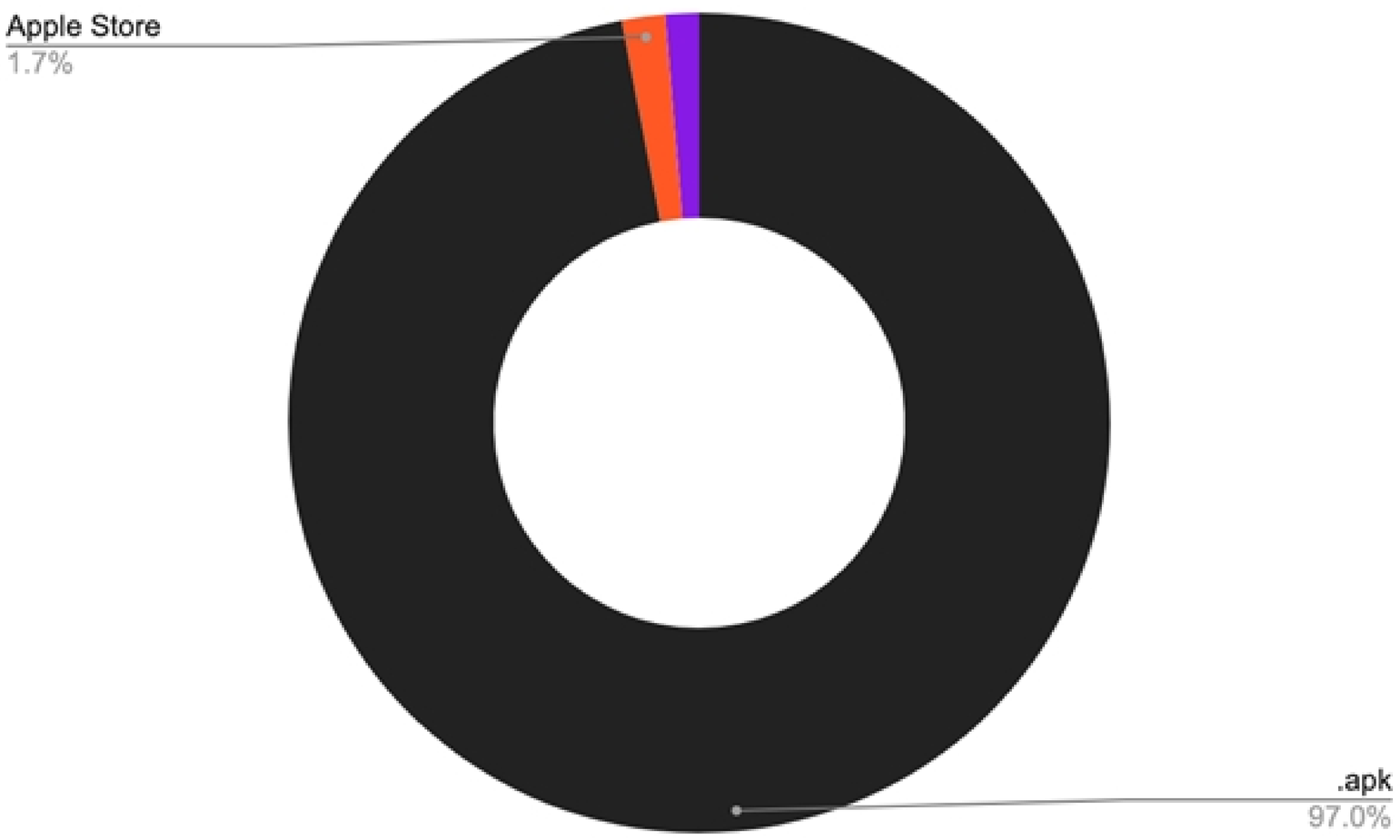


Figura 15. Origem dos aplicativos mobile fraudulentos detectados em 2021.

Isso se dá por dois grande motivos: a dificuldade de aprovação de aplicativos nas lojas oficiais, principalmente na Apple Store, que é conhecida por dificultar a vida dos desenvolvedores ao subir aplicações maliciosas.

A acentuada preferência por arquivos .apk é que o upload desses vetores pode ser feito em qualquer site de review de apps. **Esses arquivos .apk estavam distribuídos em 500 sites diferentes**, tanto nacionais quanto internacionais.

Esse tipo de arquivo permite que o próprio usuário faça a instalação do app malicioso. Ele só precisa fazer o download do arquivo, copiar para o armazenamento e ativar o modo de desenvolvedor do dispositivo.

O método é altamente eficaz em todas as camadas de segurança das lojas de apps e do dispositivo, uma vez que é o próprio usuário quem fica responsável por instalar a ameaça.

Grandes Vazamentos

Total de detecções

Ao longo de 2021, **nós detectamos 24 bases de dados expostas na surface, deep e dark web. Foram 2,8 bilhões de registros identificados.**

2021 foi um ano movimentado no Brasil quando o assunto é vazamento de dados (Figura 16). No segundo trimestre de 2021, todo brasileiro esperava que o pior havia passado: **ledo engano.**

Figura 16. Conteúdo dos 24 vazamentos de 2021, separados por trimestre.

O que é um registro? Nós chamamos de registro tudo o que se refere a um tipo de dado sensível atrelado a uma pessoa.

O primeiro semestre de 2021 se mostrou mais rico no que tange à diversidade de dados. Além disso, também registramos fotos de documentos, como RG, CPF, bem como selfies com documentos, geralmente ligadas a cadastros em serviços financeiros.

No entanto, apesar da diversidade, o primeiro semestre não conseguiu ultrapassar os números do segundo semestre. Com um terceiro trimestre inexpressivo, os três últimos meses de 2021 foram os piores do ano.

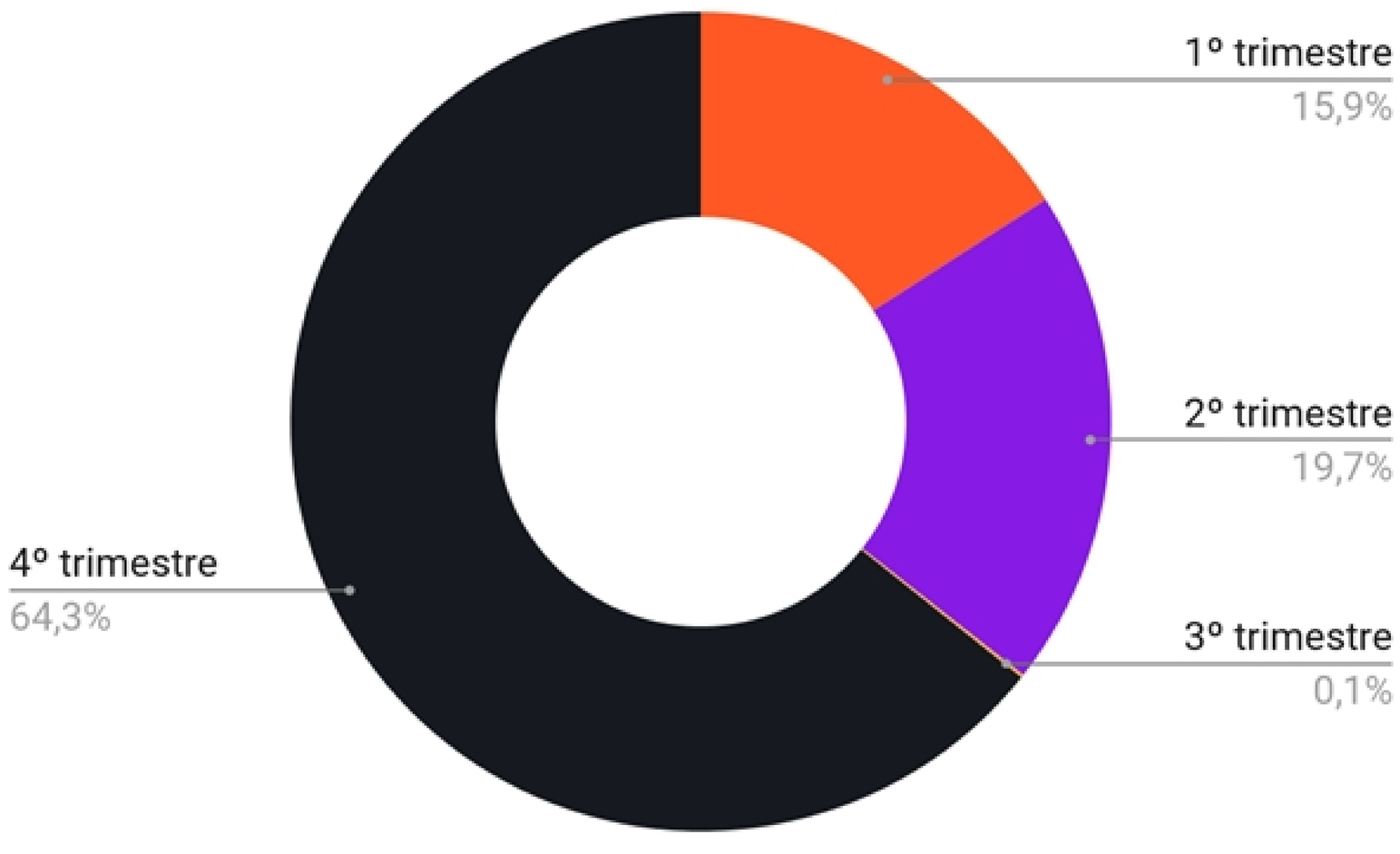


Figura 17. Percentual que cada trimestre representa no total de registros expostos em 2021.

Foram 1,8 bilhão de registros, representando 64,3% do total de registros expostos em 2021, como podemos ver no gráfico acima.

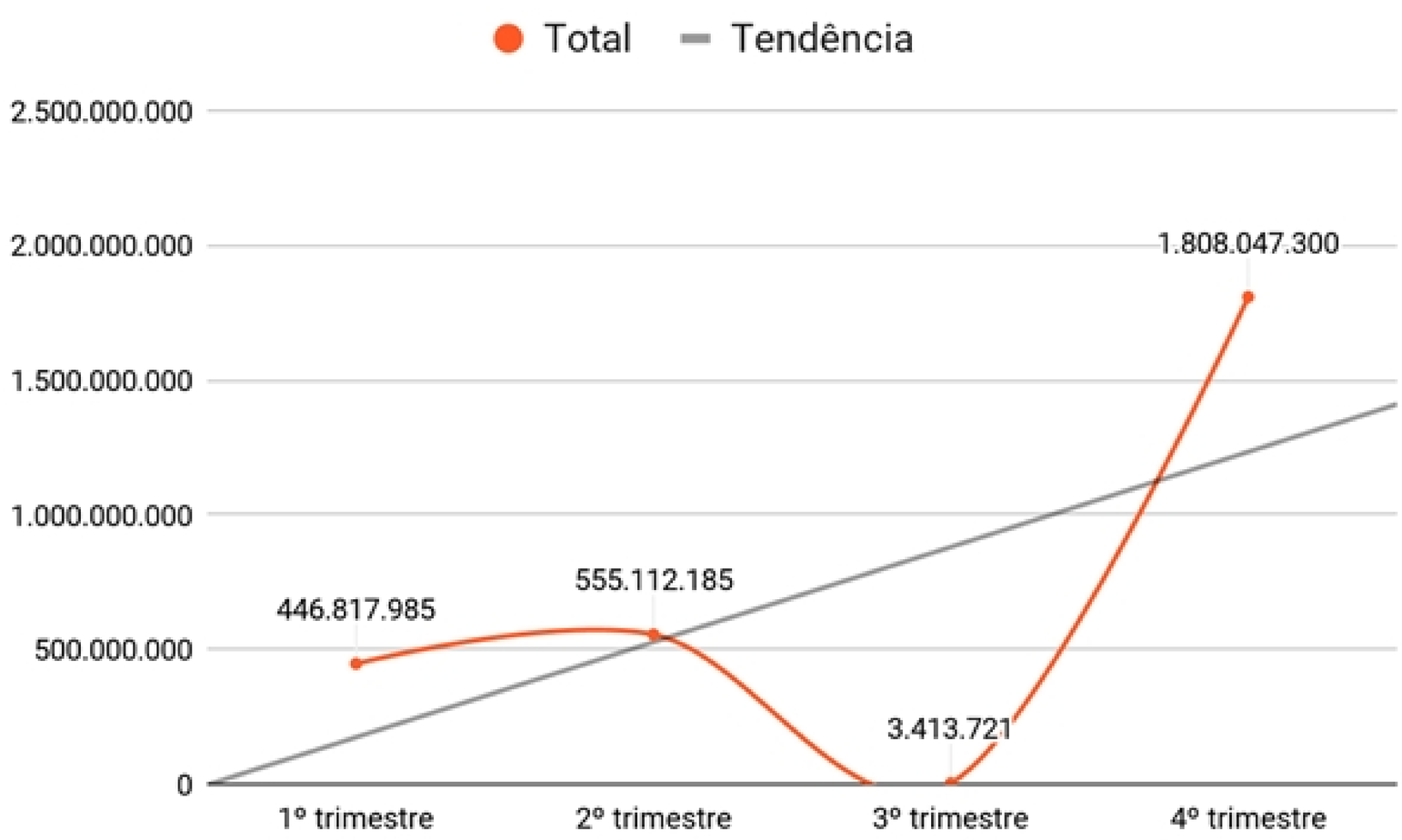


Figura 18. Evolução do volume de registros expostos em 2021, separados por trimestre (considerando CPF, CNPJ, Passaportes, Emails e Credenciais)

Veja os números totais de 2021 abaixo:

Credenciais	Emails	CPFs	CNPJs	Passaportes	Documentos
935 milhões	**1,13 bilhão**	**699 milhões**	**40 milhões**	**343 mil**	**7 mil**

Figura 19. Volume de cada tipo de registro exposto em 2021.

Bases de dados expostas

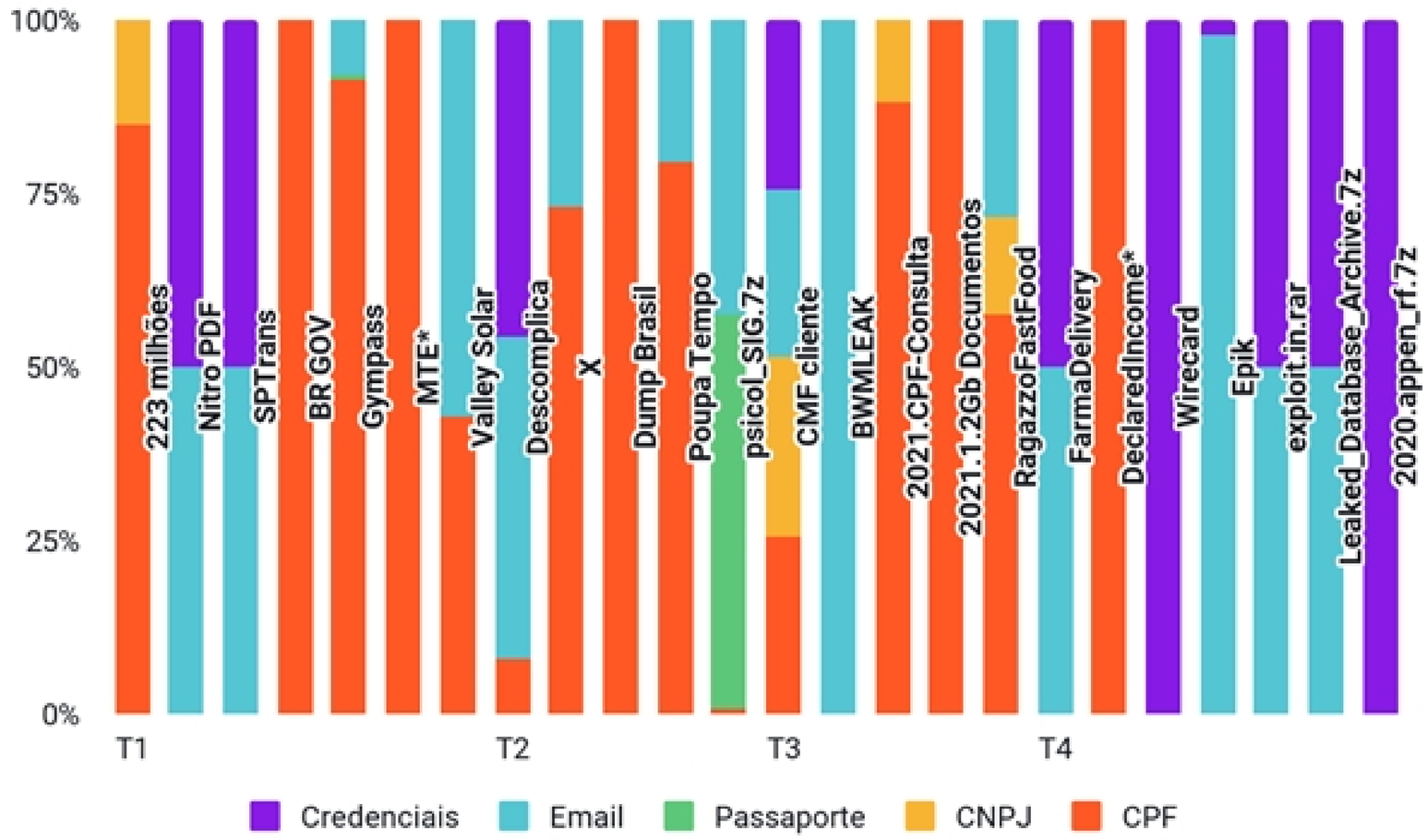


Figura 20. Tipo de dados vazados em 2021, atribuídos a cada base de dados analisada pela Axur.

Predominantemente, endereços de emails e credenciais foram o tipo de dado preferido dos cibercriminosos em 2021. Juntos, esses dados representam 73,6%, isto é, de todo volume de dados expostos no ano.

Em alguns vazamentos, inclusive, o número de credenciais é equivalente ao número de endereços de emails expostos. O que comprova o interesse dos cibercriminosos nos dados completos de acesso dos usuários.

Ao conseguir acesso às credenciais, sejam elas pessoais, sejam corporativas, o cibercriminoso pode testá-las em portais diferentes. Você com certeza se lembra da raspagem de dados de 1 bilhão de usuários do LinkedIn em abril de 2021. Em uma ocasião como essa, as credenciais são vendidas a "hackers" menos habilidosos, mas que dispõem de tempo e dedicação para testá-las em outras plataformas.

Com uma credencial de acesso do Linkedin, por exemplo, é possível tentar o login na conta de email. Com a conta de email tomada, existe um universo de possibilidades: descobrir cadastros em e-commerces, bancos e outros serviços. Basta enviar um link de recuperação de senha para este email e pronto. Esse tipo de ataque é chamado de credential stuffing e é bastante comum também no meio corporativo.

E já que estamos falando de credenciais, vamos nos aprofundar um pouco mais em relação ao que foi identificado em 2021.

Vazamento ou exposição de credenciais

⚠ Disclaimer

A Axur tem duas formas de detecção de vazamentos de credenciais: automática e manual.

Total de detecções

Nossa plataforma detectou automaticamente **273 milhões de credenciais expostas ao longo de 2021**. Nossos times de especialistas expandiram essa detecção para **935 milhões de credenciais**.

O segundo trimestre de 2021 foi, sem sombra de dúvidas, o mais movimentado em relação ao assunto. Sozinho, o mês de junho é responsável por **41,2%** de todas as credenciais identificadas em 2021 (Figura 21).

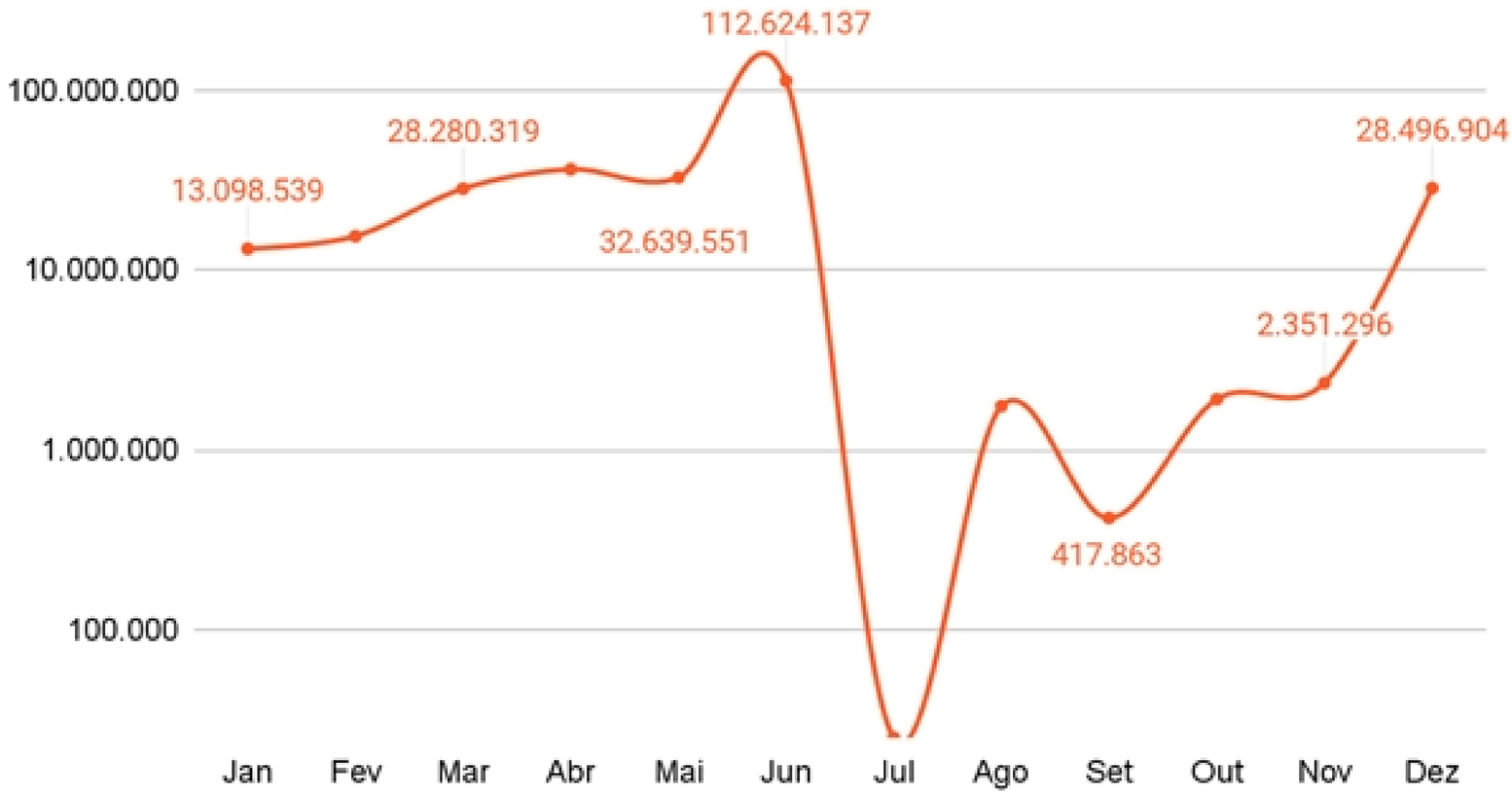


Figura 21. Volume mensal de credenciais expostas detectadas pela Axur em 2021

Por este motivo, o primeiro semestre do ano representa 87,2% do total de credenciais detectadas pela Axur durante o ano todo.

De onde vem essas credenciais?

43,3 milhões são credenciais de domínios corporativos[1] (15,8% do total), **distribuídas entre 17,9 milhões de empresas** distintas afetadas (total mundial)[2].

3,9 milhões de credenciais são de domínios .br (1,45% do total de credenciais), distribuídas entre **557 mil** domínios nacionais distintos . Desse total do universo nacional, temos mais de 1 milhão de credenciais de domínios corporativos brasileiros (26,2%% do total brasileiro) e 227 mil de domínios **gov.br** (5,7%).

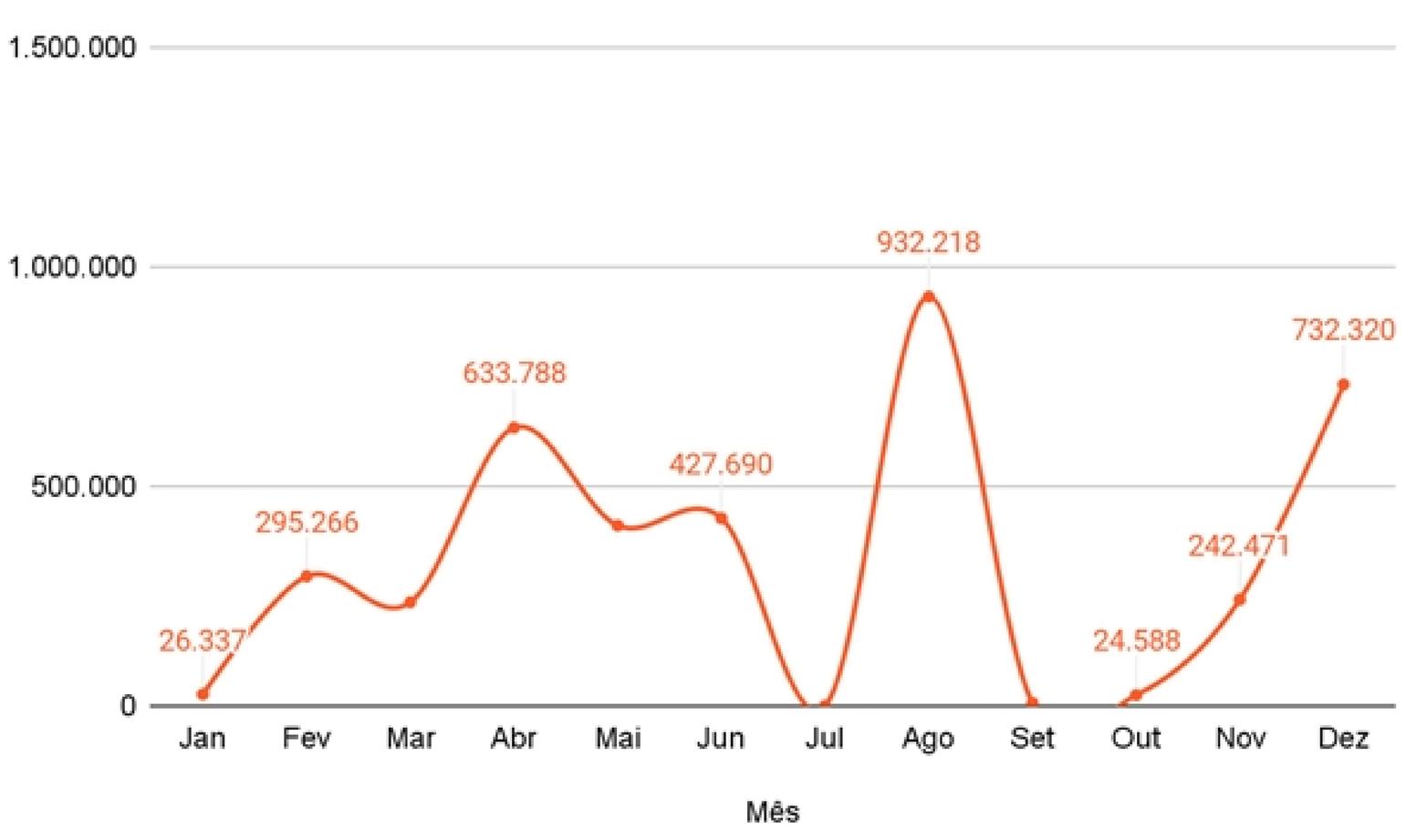


Figura 22. Volume mensal de credenciais brasileiras expostas detectadas pelas Axur em 2021.

[1]As credenciais corporativas detectadas não necessariamente dão acesso aos sistemas e bases internos das empresas, pois podem apenas ter sido vazadas a partir de cadastros feitos em outros sites com e-mails dessas empresas.

[2]As credenciais .br são apenas uma amostra para análise do cenário brasileiro, já que muitos usuários e empresas do Brasil utilizam domínios .com ou outros.

É interessante notar a discrepância entre as Figuras 21 e 22. A primeira denota os vazamentos de credenciais internacionais, tendo uma forte crescente no início do ano, um ápice de detecções em junho e dezembro.

Enquanto isso, quase o inverso acontece no âmbito nacional: há um movimento ascendente nos primeiros meses do ano, mas totalmente desligado da cena internacional. Temos em agosto o pico de detecções nacional.

Isso nos diz que **os vazamentos nacionais estão alheios aos internacionais**, indicando que existem *threat actors* nacionais distintos dos internacionais. Esse fato nos dá indícios que uma estratégia de segurança da informação focada somente no movimento internacional, por exemplo, pode dar grandes brechas para criminosos brasileiros.

Raio-X das senhas

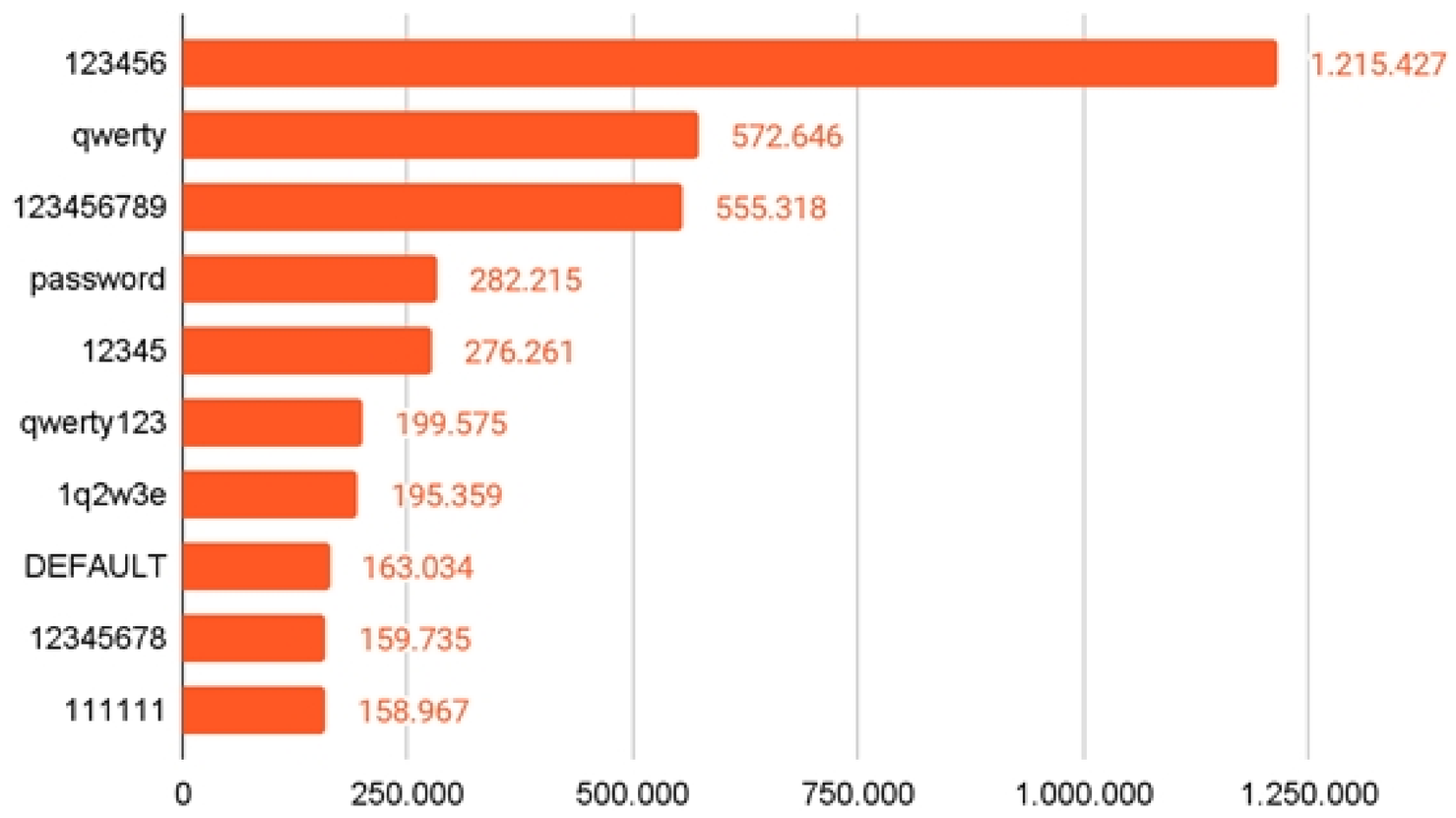


Figura 23. Volume das senhas mais expostas em 2021.

Pelo segundo ano consecutivo, **a sequência numérica "123456" é o padrão que mais se repete nas detecções** da Axur (Figura 23). Sozinha, essa senha ocupa 0,44% do total de credenciais detectadas durante o ano todo.

Outras quatro sequências numéricas, como "123456789", "12345", "12345678" e "111111" permanecem no ranking. Isso nos diz mais sobre o comportamento do usuário ao configurar a senha do que do próprio cibercriminoso.

Lembrando que estamos falando de credenciais tanto pessoais quanto corporativas. Nesse sentido, instruir leads, clientes e colaboradores a adotarem senhas seguras na hora de se cadastrar no seu ambiente digital é imprescindível para barrar os criminosos.

É importante ressaltar que em um ataque de Brute Force, essas senhas numéricas de até 9 dígitos seriam facilmente descobertas em menos de 1 minuto.

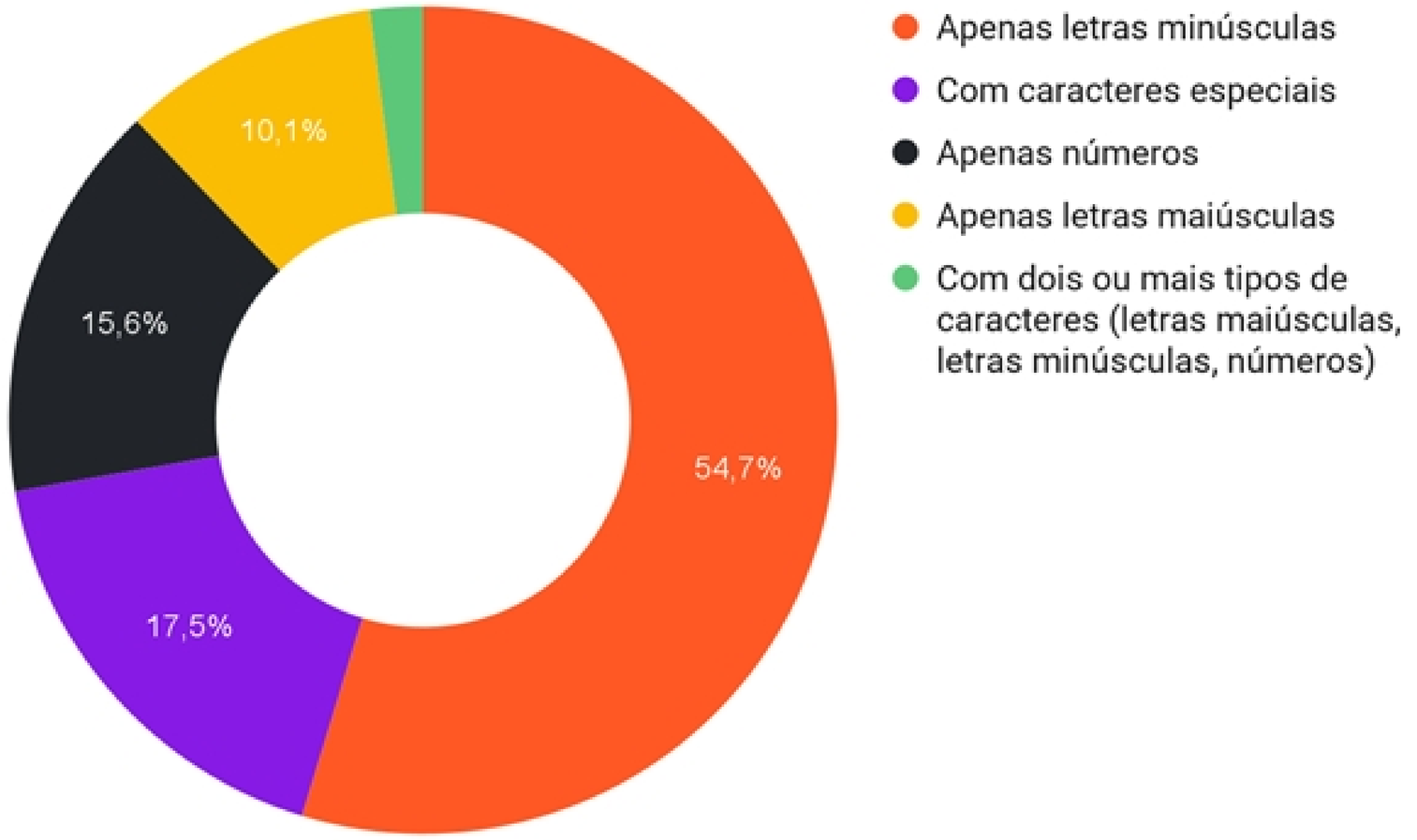


Figura 24. Distribuição percentual de senhas conforme os caracteres que as compõem, identificadas em 2021.

Outro aspecto a ser analisado, quanto ao comportamento na hora de criar senhas, é em relação aos caracteres que ela utiliza. Por exemplo, **134,1 milhões de senhas detectadas pela Axur continham somente letras minúsculas**, que representam 54,7% do total.

Senhas com apenas letras minúsculas (10,1%) e somente com números (15,6%) somam 62,9 milhões. Isso quer dizer **que as senhas com somente um tipo de caracter totalizam 80,4% de todas as credenciais identificadas**.

Restando somente 19,6% que fazem a combinação de dois ou mais tipos de caracteres, **senhas estas que são consideradas as mais seguras**.

De novo, é importante ressaltar a importância de adotar medidas que façam com que o usuário se conscientize em relação ao uso e formulação das senhas, bem como medidas que o ajudem a formar senhas mais seguras, como por exemplo, **exigir na hora do cadastro** que a senha contenha um número, uma letra maiúscula, um carácter especial e mais de 8 dígitos.

Origem dos vazamentos

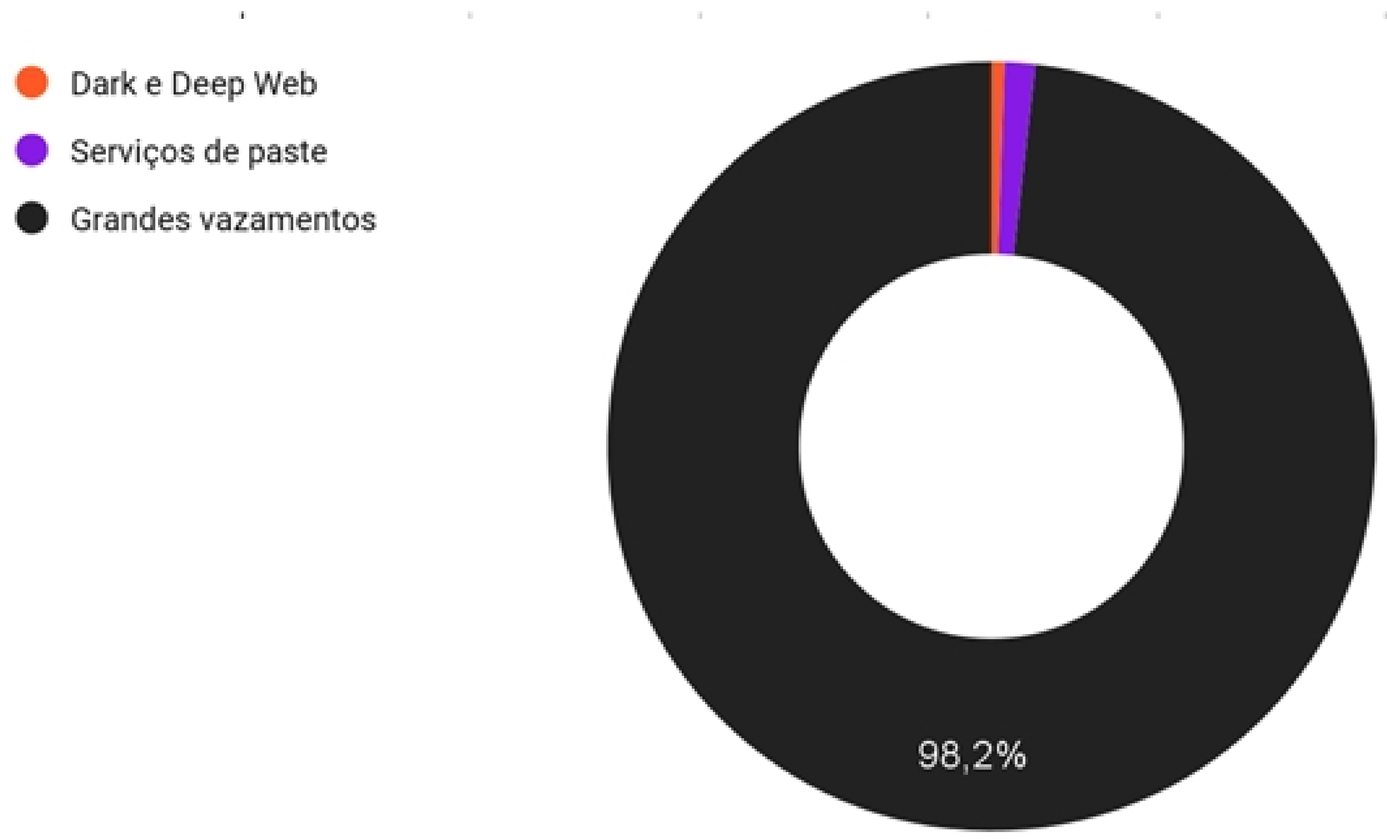


Figura 25. Origem das credenciais expostas encontradas pela Axur em 2021.

Quando se trata do vazamento de credenciais, a esmagadora maioria dos 268,2 milhões estavam presentes em grandes vazamentos na surface web.

A título de comparação, temos os 3,5 milhões em serviços de paste e compartilhamento de texto e 1,4 milhões distribuídas por fóruns restritos na dark web e em aplicativos de mensagens entre criminosos.

Se analisarmos as detecções manuais do time de especialistas da Axur, podemos somar mais 660 milhões de credenciais aos vazamentos que aconteceram em 2021.

Vazamento ou exposição de cartões de crédito e débito

Outro dado de extremo valor para os cibercriminosos são os cartões de crédito e débito. Todos os cartões que a Axur detectou estão com o CVV, indicando que poderiam ser utilizados pelos estelionatários digitais. **Veja os dados:**

Total de detecções

Em 2021, **nós detectamos 2,17 milhões de cartões de crédito e débito expostos** na web superficial, deep e dark web. Página. 39

O último trimestre de 2021 foi o menos tumultuado no vazamento de cartões de crédito, tendo 90,3% a menos do que no trimestre anterior (Figura 25). Ao compararmos os dois semestres de 2021, vemos um aumento expressivo de 115,9% do primeiro para o segundo semestre.

É preciso lembrar que em agosto do ano passado, o *threat actor* conhecido como **AW_cards** publicou uma base com pouco mais de **1 milhão de cartões de crédito e débito em diversos fóruns da Dark Web**. A base foi compartilhada gratuitamente, a fim de gerar mais credibilidade ao autor do vazamento.

Esse comportamento denota o interesse dos cibercriminosos em obter o máximo de informações sensíveis e financeiras possível e que apenas um vazamento pode ser responsável por mudar os números de um ano inteiro.

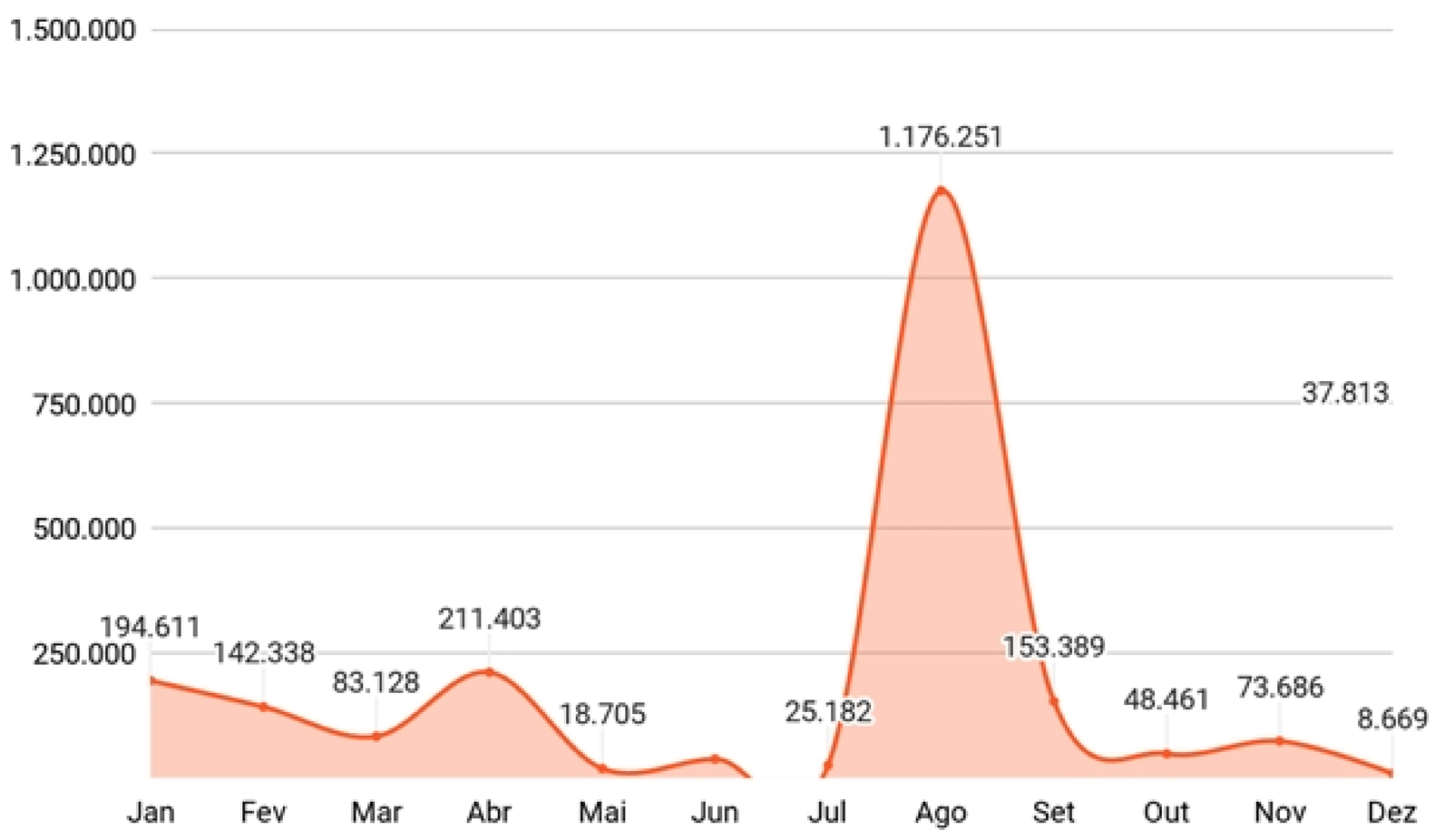


Figura 26. Quantidade de cartões de crédito e débito expostos por mês em 2021.

No ranking dos Top 10 países, pelo segundo ano consecutivo, o **Brasil segue como campeão dos vazamentos de cartões de crédito e débito com 720.643 cartões expostos** (Figura 26) e representam sozinho 33,2% do total de cartões expostos no mundo todo.

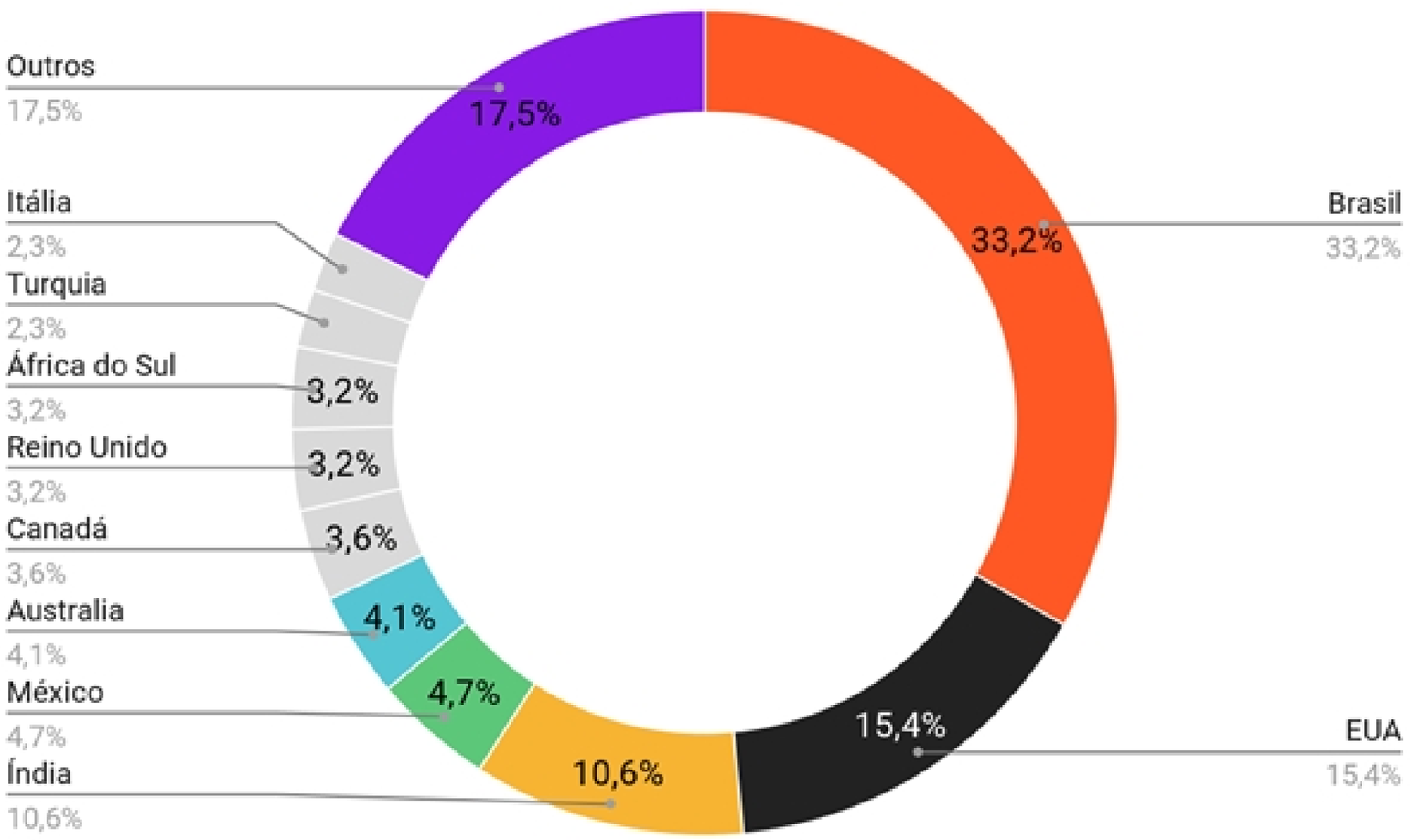


Figura 27. Porcentagem total dos países com mais cartões de crédito e débito vazados online e detectados pela Axur em 2021.

Isso é 116% a mais do que os EUA, segundo colocado no nosso ranking com 333 mil cartões de crédito e débito expostos durante o ano. A menção honrosa de terceiro lugar ficou com a Índia, detentora de 10,6% de todos os cartões expostos no ano.

É interessante notar uma troca de posições nessas três primeiras colocações do ranking mundial de países que tiveram mais cartões expostos.

Nos relatórios anteriores, registramos um interesse muito presente na América como um todo, com Brasil, EUA e México como protagonistas da exposição de cartões no mundo.

Exposição de BINs

BINs ou **Bank Identification Number** é um número composto pelos seis primeiros dígitos de um cartão de crédito ou débito, a fim de identificar o próprio cartão, bem como a empresa emissora.

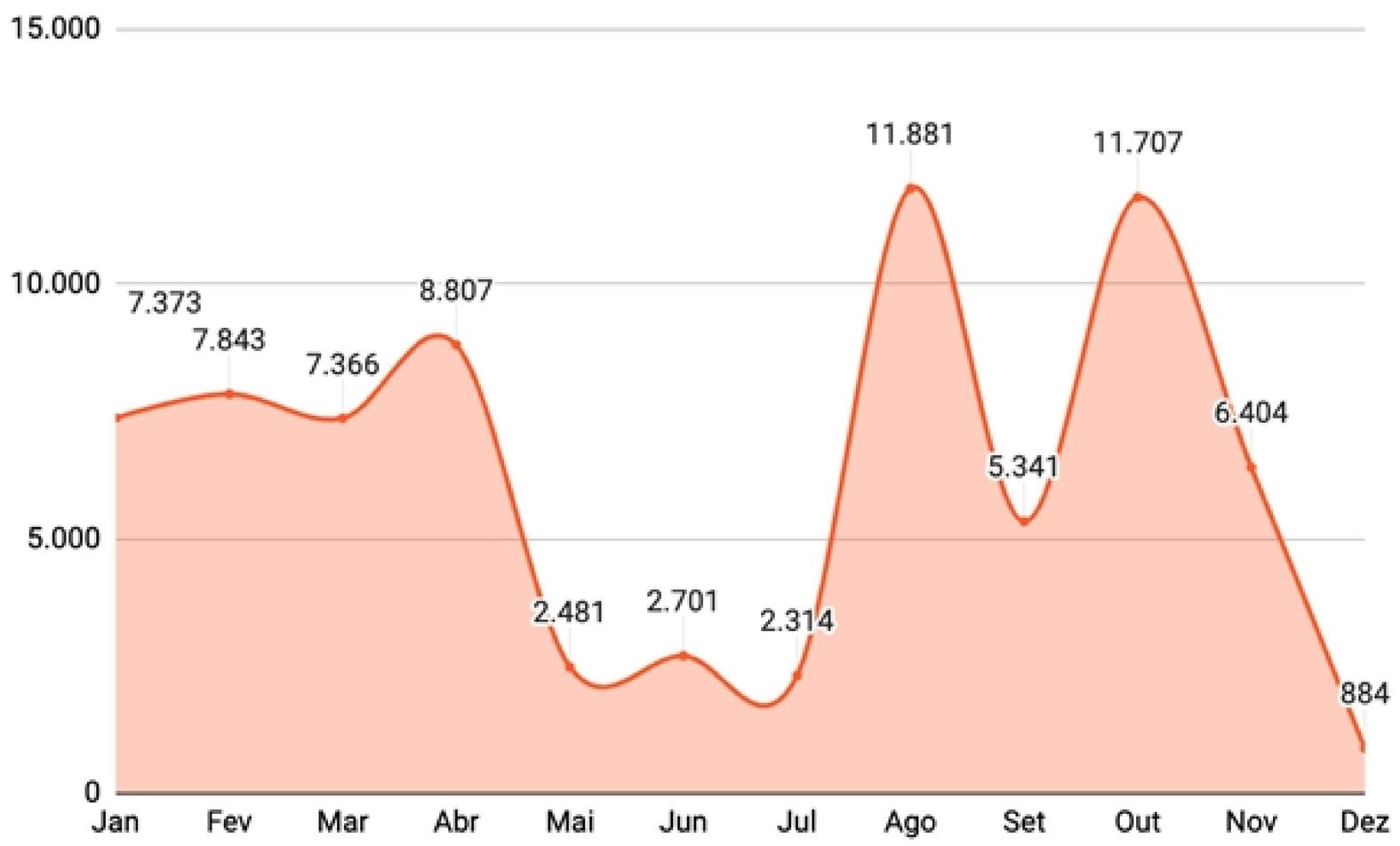


Figura 28. Quantidade de BINs expostas por mês em 2021.

Em 2021, **75.102 BINs ficaram expostas na surface, deep e dark we**b. O segundo semestre foi ligeiramente mais promissor para os cibercriminosos do que o primeiro em apenas 5,3%.

Em relação a de onde são essas BINs, não é de se impressionar que **o Brasil ocupa as 15 primeiras posições do nosso ranking**, como é possível ver no gráfico abaixo (Figura 28). Esse número é um forte indicador de que o Brasil é protagonista entre os cibercriminosos no mundo todo e que isso não vai mudar em 2022.

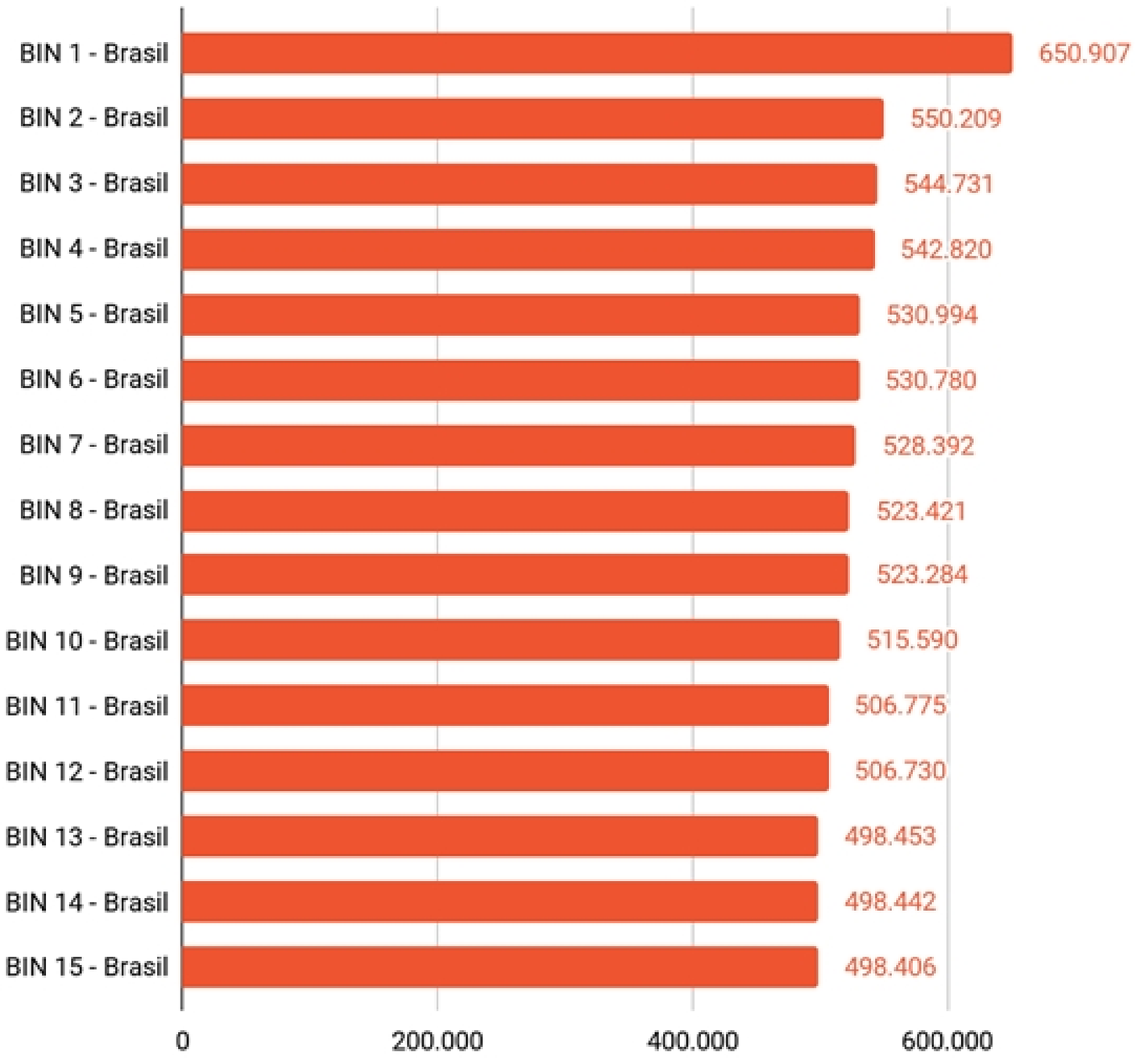


Figura 29. Ranking mundial das 15 BINs com mais exposição de dados de cartões de crédito e débito registrados em 2021, separadas por país.

Além disso, é importante avaliar a validade destes cartões, fator responsável por inutilizar um cartão de crédito exposto na mão de um estelionatário digital.

95,9% dos cartões detectados pela Axur em 2021 estavam dentro do prazo de validade e, portanto, se acompanhados do CVV, estariam disponíveis para compra. Isso nos diz muito sobre a assertividade dos cibercriminosos em coletar esses dados.

Esse número nos diz que quase a totalidade dos cartões podem ter sido utilizados por cibercriminosos na aquisição de domínios para sites de phishing, armazenamento em nuvem e até na compra de produtos pessoais e até ilegais nos marketplaces.

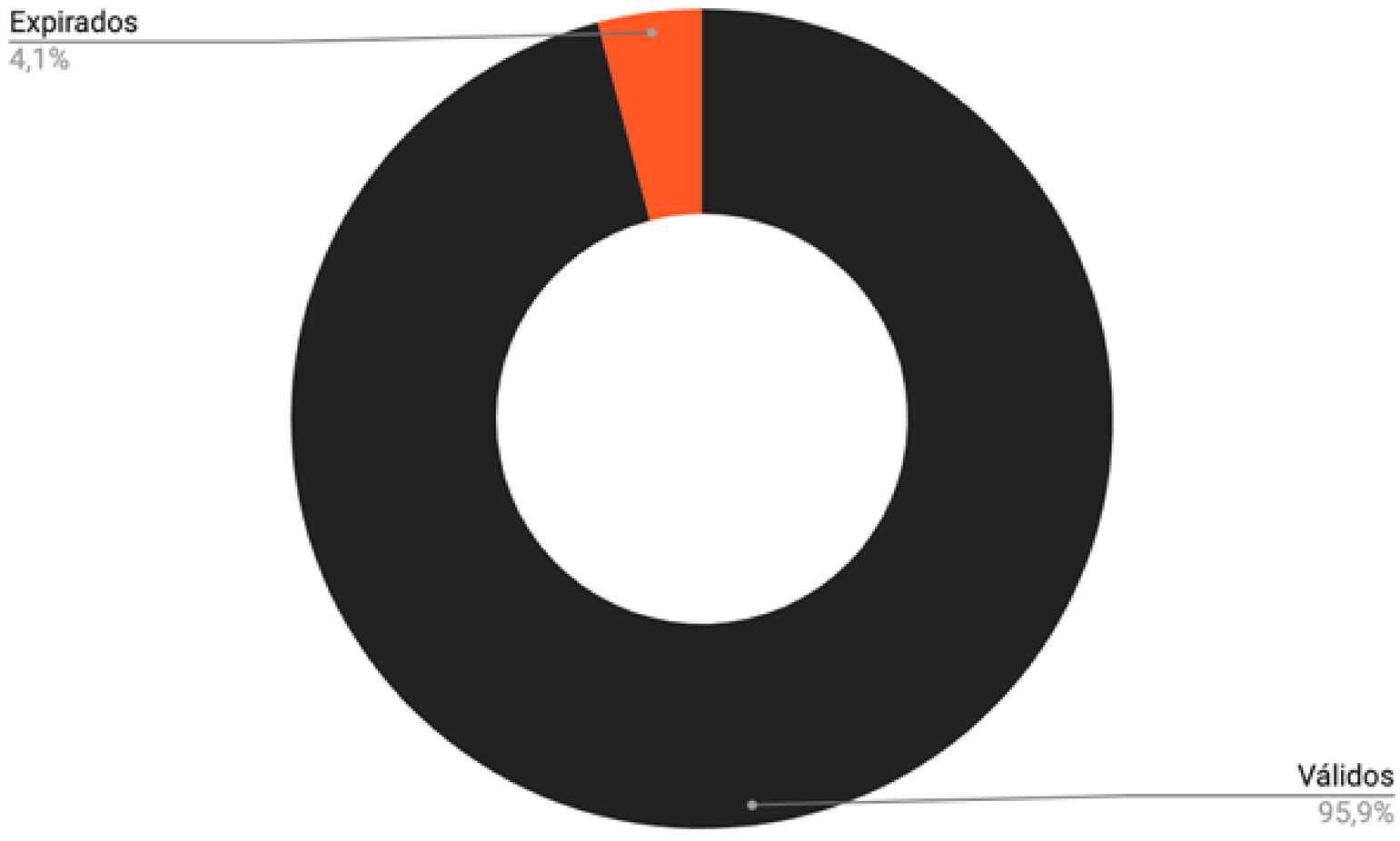


Figura 30. Percentual de cartões válidos vs. cartões expirados na data de coleta em 2021.

Outro aspecto a ser levado em consideração é a origem destes cartões: **58,2% dos cartões detectados em 2021 vieram pela comercialização desses dados na deep e dark web**.

Apesar de ficar em segundo lugar, os serviços de paste, como o Ghostbin e Pastebin, estão com 41,8% dos cartões, o que denota uma expressividade grande e nos diz que os cibercriminosos procuram por esse tipo de dado tanto em fóruns hackers e entre conversas na deep e dark web, quanto em serviços de paste, nos dando a visibilidade que é preciso monitorar tanto um quanto o outro.

Figura 31. Origem dos cartões de crédito e débito expostos detectados pela Axur em 2021.

O que se pode aprender com 2021?

De fato, 2021 foi uma surpresa para os times de segurança do Brasil e do mundo todo. Houve um boom nas fraudes e ataques virtuais, bem como nos vazamentos de dados. Nos últimos meses de 2020 já dava para ter uma noção aproximada de como seria o desenrolar de 2021.

Quem não aproveitou o momento para desenvolver sua macroestratégia de segurança da informação, unindo os times de SI, TI, prevenção a fraudes, jurídico e até o marketing, sofreu as consequências de deixar o perímetro interno e, principalmente o externo, desprotegido.

Ressaltamos a importância de garantir a segurança extra perimetral, o que tem sido um grande desafio. É uma brusca mudança de mindset nas empresas, que se acostumaram a olhar somente para o que acontece dentro de casa: sua infraestrutura de TI, suas redes e por aí vai.

Foram muitas as empresas afetadas por conta disso em 2021, inclusive órgãos governamentais. Várias companhias tiveram prejuízos reputacionais irreparáveis, bem como prejuízos financeiros que vão refletir por alguns anos, ainda. E olha que nem estamos considerando os prejuízos de enfrentar as sanções de uma LGPD que poderão ser aplicadas dependendo da gravidade dos incidentes, inclusive retroativamente.

É necessário observar também que o prejuízo financeiro causado pelas fraudes digitais é quase incalculável. Quantas empresas que quase nem aparecem no mapa, por serem de menor porte, sofreram com criminosos se passando pela sua marca, enganando clientes e causando um ruído no relacionamento dessas empresas com seus consumidores.

Não à toa o Brasil foi o 5º país com mais cibercrimes no mundo, bem como o 6º país no mundo a ter mais dados vazados em 2021. Estamos na mira dos hackers no mundo todo por essa negligência com que muitas empresas encaram suas estratégias de cibersegurança.

Em termos de comparação, vemos o crime cibernético ganhando mais volume do que o próprio crime de rua. **Em São Paulo, estado mais populoso do país, vemos as taxas de homicídios e crimes atingirem a menor taxa em 41 anos**, de acordo com a Secretaria de Segurança Pública, sendo considerada a maior taxa de redução na taxa de criminalidade do país.

Ao contrário, o cibercrime bate recorde atrás de recorde no país. Segundo a CheckPoint Research, **o aumento do número de ataques cibernéticos foi de 62% em comparação a 2020**, enquanto a taxa de crescimento mundial foi de 50%.

Esses dados nos dizem que 2021 tem algo a nos ensinar: essa é a nova realidade do ambiente digital para Brasil e mundo. Diante disso, apesar dos grandes esforços governamentais no combate ao crime apostarem em iniciativas para mitigar os crimes virtuais, a dura verdade é que as empresas são responsáveis por manter a própria segurança, antes de tudo. E a LGPD está aí para comprovar essa relação.

O que esperar para 2022 e como se preparar?

Se 2021 foi um ano desafiador para times de segurança e inteligência de fraudes, nós alertamos que é melhor começar a pensar com clareza na estratégia que sua empresa vai adotar para 2022.

Diante dos muitos dados que esse relatório nos traz, a mudança de mindset que pontuamos logo acima é de extrema necessidade. É preciso olhar para dentro de casa, sim. Cuidar do perímetro interno de cibersegurança é importante. Mas, mais importante, é ampliar essa visão para todos os assets digitais da sua empresa, olhando, principalmente, para a possibilidade de que sua marca pode ser alvo de fraudes e ameaças digitais.

Proteger o perímetro interno é importante para conhecer tudo o que sua empresa tem, digitalmente falando. **Mas olhar para o perímetro externo é entender que sua marca também é um ativo da sua empresa**, distribuída em diversos canais, como sites, redes sociais, marketplaces e por aí vai.

Cuidar da sua marca nesse ambiente virtual que se expande a cada dia é crucial para a saúde e sobrevivência da sua empresa em tempos da multiplicação do crime virtual. Nesse sentido, assumir uma postura proativa e **monitorar ativamente esses canais é o primeiro passo para não ser pego de surpresa em uma fraude ou ataque virtual**.

Como funciona o monitoramento de fraudes digitais da Axur

Todas as informações aqui apresentadas foram obtidas a partir do monitoramento diário de milhões de URLs e artefatos maliciosos realizado pela Axur.

As detecções são feitas em web superficial, deep e dark web, e com o uso de tecnologias que permitem a automação de processos mais visíveis e intuitivos na forma de dados:

Coletores próprios na surface, deep e dark web

A Axur possui uma estrutura de coletores próprios com todas as possíveis fontes de sinais (milhões de e-mails considerados spam são processados diariamente, e cerca de 780 milhões de URLs avaliadas todos os meses).

Detecção aprimorada por machine learning

É usado pela Axur para diminuir exponencialmente o tempo de detecção. O procedimento é feito a partir da análise dos componentes de URLs, de elementos no conteúdo das páginas e do uso de visão computacional, permitindo a identificação de padrões que são ensinados e testados – possibilitando os mais elevados níveis de acertos.

Com essas técnicas, a Axur consegue entregar resultados com precisão, tornando a visualização de ameaças e incidentes em potencial mais prática. Todas as detecções acontecem na plataforma Axur One, onde é também possível realizar as ações de tratamento.

Para saber sobre as detecções de sua marca e/ou conhecer os produtos de proteção contra riscos digitais da Axur, entre em contato conosco.

Sua empresa com o poder de eliminar fraudes

Se quiser saber mais sobre o que sua empresa pode se comportar proativamente junto com a Axur e remover as ameaças digitais que atrapalham suas vendas e colocam em risco os dados dos seus consumidores, veja nossas soluções.

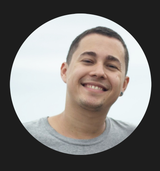
O que mais atrapalha os negócios da sua empresa? A gente derruba pra você!

FAÇA UMA DEMO DA PLATAFORMA

OU

FALE COM NOSSOS ESPECIALISTAS

Hugo Moura, Redação



Patrick Santos, Design

Sobre a Axur

Líder em monitoramento, reação e remoção de riscos e ameaças digitais na internet, com foco em criar experiências digitais mais seguras para empresas e seus consumidores.

Utilizando automações e machine learning, monitoramos a web superficial e a deep e dark web para oferecer proteção contra riscos como uso abusivo de marca, apropriação de identidade, phishing, aplicativos fraudulentos,vendas não autorizadas e vazamento de dados.

Contato para a imprensa

Letícia Olivares
press@axur.com
+55 51 3012 2987

Para mais informações, visite axur.com e conheça o blog Deep Space, blog.axur.com.

Endereços

EUA
535 Mission Street – 14th floor
San Francisco, CA 94105

Singapura
109 North Bridge Road
Cityhall District, 179097

Brasil
Rua Mostardeiro, 322 – 15º andar
Porto Alegre, RS 90430-000

axurbr Axur AxurBrasil AxurBrasil AxurBrasil Axur