RELATÓRIO TRIMESTRAL

Vazamentos de Dados no Brasil

2º trimestre / 2021

São Paulo, 11 de agosto de 2021

O que você vai encontrar neste relatório

Principais números deste relatório

645 mi

de registros ficaram expostos no segundo trimestre deste ano

460 mi

de CPFs foram identificados em grandes vazamentos de Abril a Junho

181,5 mi

de credenciais foram expostas em grandes vazamentos no trimestre passado

- **31 milhões** são corporativas e **160 mil** são do governo brasileiro
- A Axur identificou **420 mil** cartões expostos. Só no Brasil, foram **249 mil** números de cartões de crédito foram vazados

A seção sobre atividades criminosas em deep e dark web é de **acesso exclusivo a clientes da Axur**. Por listarem canais, tipos de infração e setores que são alvos dos cibercriminosos, esses dados são sensíveis e centrais em estratégias de segurança digital.

PANORAMA

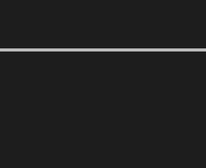
Com menos força, mesma consistência

O primeiro trimestre de 2021 foi um divisor de águas no Brasil. Se você leu nosso relatório no trimestre passado, está lembrado que os megavazamentos que vimos de janeiro a março deste ano foram responsáveis por um aumento de 785% na exposição de credenciais, isso sem falar na exposição de cartões de crédito e débito, que registramos 420 mil expostos na surface, deep e dark web.

No segundo trimestre, trazemos a boa notícia: não foram tantos vazamentos quanto no anterior. Tivemos, sim, um número alto de detecções, mas nada que supere o que passamos nos três primeiros meses do ano.

Nas próximas páginas, você vai encontrar diferentes tipos de dados que a Axur detectou durante o trimestre, desde os grandes vazamentos que registramos até a exposição de credenciais, cartões de crédito e débito.

Boa leitura.



Fabio Ramos, CEO da Axur

Grandes Vazamentos

TOTAL DE DETECÇÕES

Neste segundo trimestre de 2021, identificamos 435, 5 milhões de registros expostos em 5 bases de dados diferentes, tanto de empresas privadas quanto de órgãos governamentais.

Isso representa uma redução de 87,6% em relação ao trimestre anterior, que encontramos 3,75 milhões de registros. O principal motivo foi o COMB21, base gigantesca vazada em fevereiro que, sozinha, tinha 2,2 bilhões de credenciais (Figura 2).

Desses 435,5 milhões de registros, tivemos diferenças em relação aos tipos de dados que ficaram expostos. CPFs representam 82,9% do total, acumulando um crescimento de 89% em relação ao trimestre anterior.

Mas foi o vazamento de passaportes que mais chamou a atenção, que cresceu de pouco mais de 21 mil no trimestre passado para quase 317 mil neste trimestre, representando um ganho de 1392,5%.

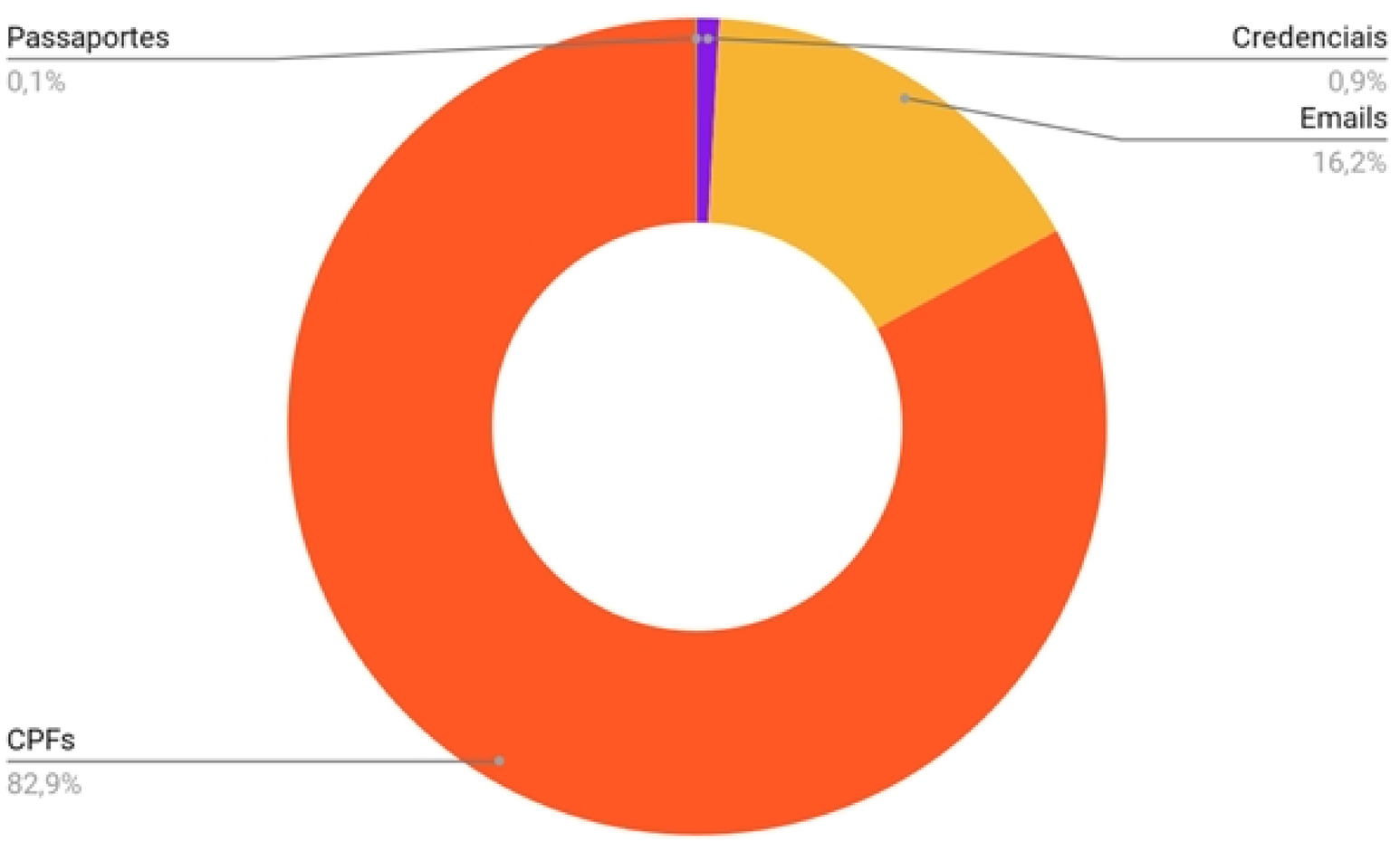


Figura 1. Percentual que cada tipo de dado representa no total de dados vazados no segundo trimestre de 2021.

A exposição de emails foi a que menos teve expressão, com um crescimento de 6% apenas. Confira na tabela abaixo os números exatos.

Credenciais	Emails	CPFs	Passaportes
4,8 milhões	**89,8 milhões**	**460,1 milhões**	**321 mil**

BASES DE DADOS EXPOSTAS

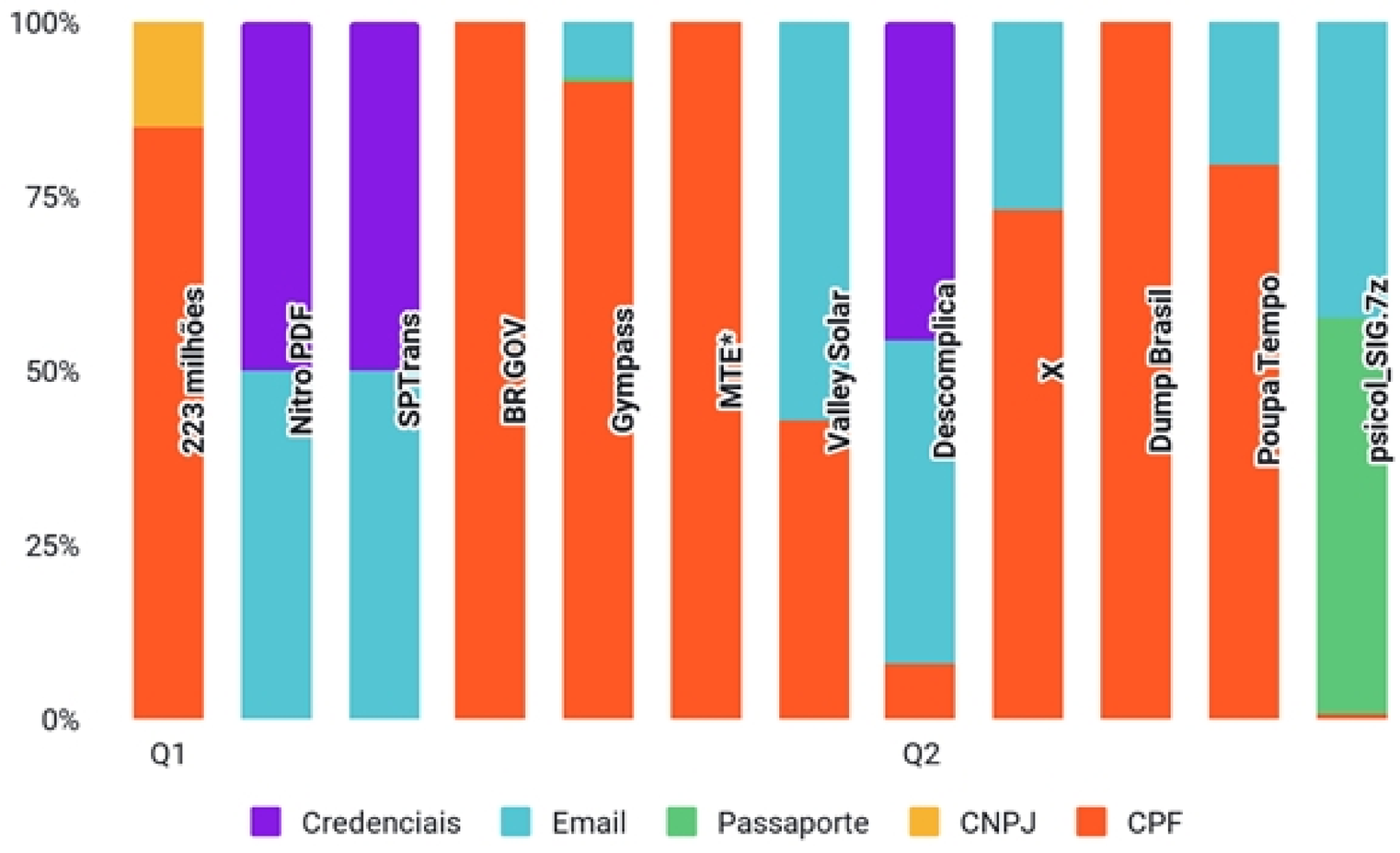


Figura 2. Tipo de dados vazados primeiro semestre de 2021, atribuídos a cada base de dados analisada pela Axur (sem a base "Compilado 2021", que, sozinha, expôs 2,2 bilhões de credenciais).

Olhando mais de perto fica claro o motivo do crescimento na exposição de CPFs, já que três das cinco bases computadas (Figura 3) apresentam muito mais CPFs do que qualquer outro tipo de dado.

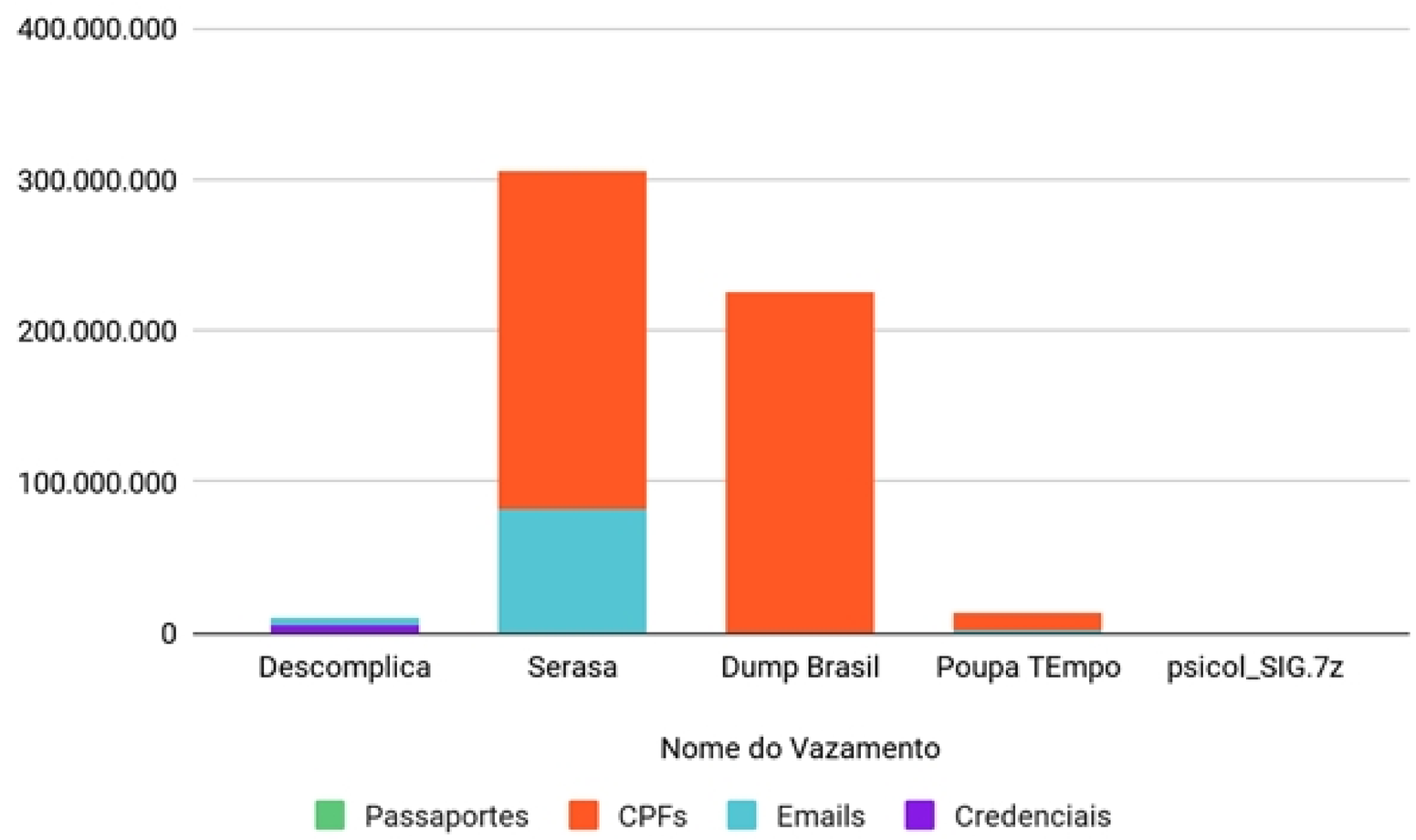


Figura 3. Quantidade de dados comprometidos por bases expostas de abril a junho de 2021.

O suposto vazamento do Serasa (no gráfico está como X) e Dump Brasil somam quase 450 mil CPFs sozinhas (Figura 3). A única base que teve vazamento de credenciais foi a da Descomplica, que ficou exposta em abril deste ano. Confira também na tabela abaixo os números exatos de dados vazados dessas cinco bases:

	Credenciais	Emails	CPFs	Passaportes
Descomplica	**4.800.000**	**4.909.086**	**828.252**	**-**
Serasa	**-**	**82.103.268**	**223.798.881**	**-**
Dump Brasil	**-**	**-**	**225.556.870**	**-**
Poupatempo	**-**	**2.547.850**	**10.000.000**	**-**
Piscolo_SIG.7z	**-**	**241.776**	**4.584**	**321.618**

Bases de dados expostas

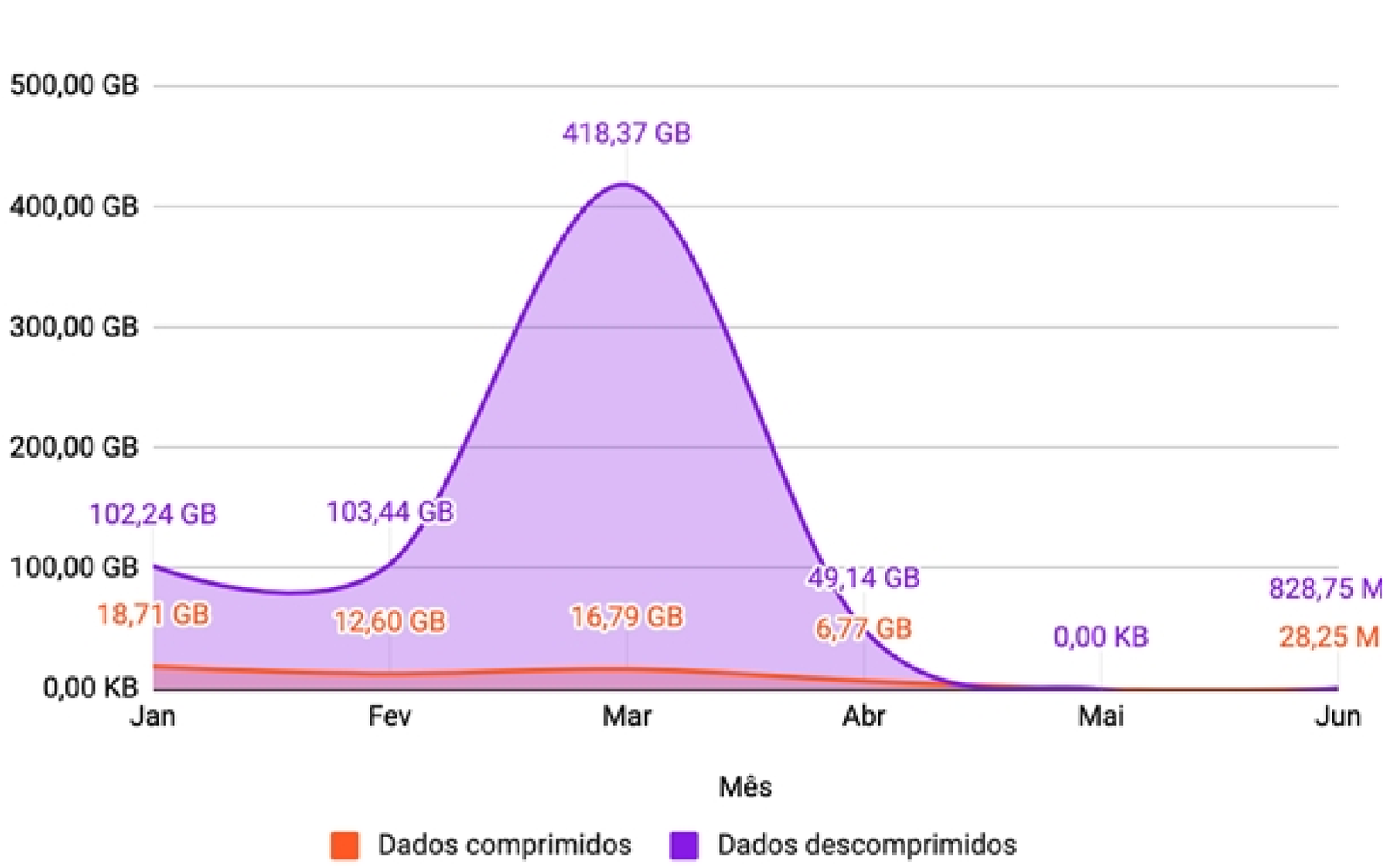


Figura 4. Volume de dados comprimidos vs. volume de dados descomprimidos do total de dados expostos no primeiro semestre de 2021.

Em relação ao trimestre anterior, as bases de dados que encontramos foram bem menores em relação ao tamanho dos arquivos. Ao todo, as cinco bases somam 50GB descomprimidos, número muito inferior aos 624 GB do trimestre anterior.

Vazamento ou exposição de credenciais

TOTAL DE DETECÇÕES

Nossa plataforma detectou **181,5 milhões** credenciais expostas (incluindo as 4,8 milhões do vazamento da Descomplica) entre os meses de abril a junho deste ano.

Se desconsiderarmos o vazamento do COMB21 (que foi a junção de vários vazamentos de credenciais desde 2014 e foi um evento singular), a exposição de credenciais vem crescendo mês a mês desde o começo do ano.

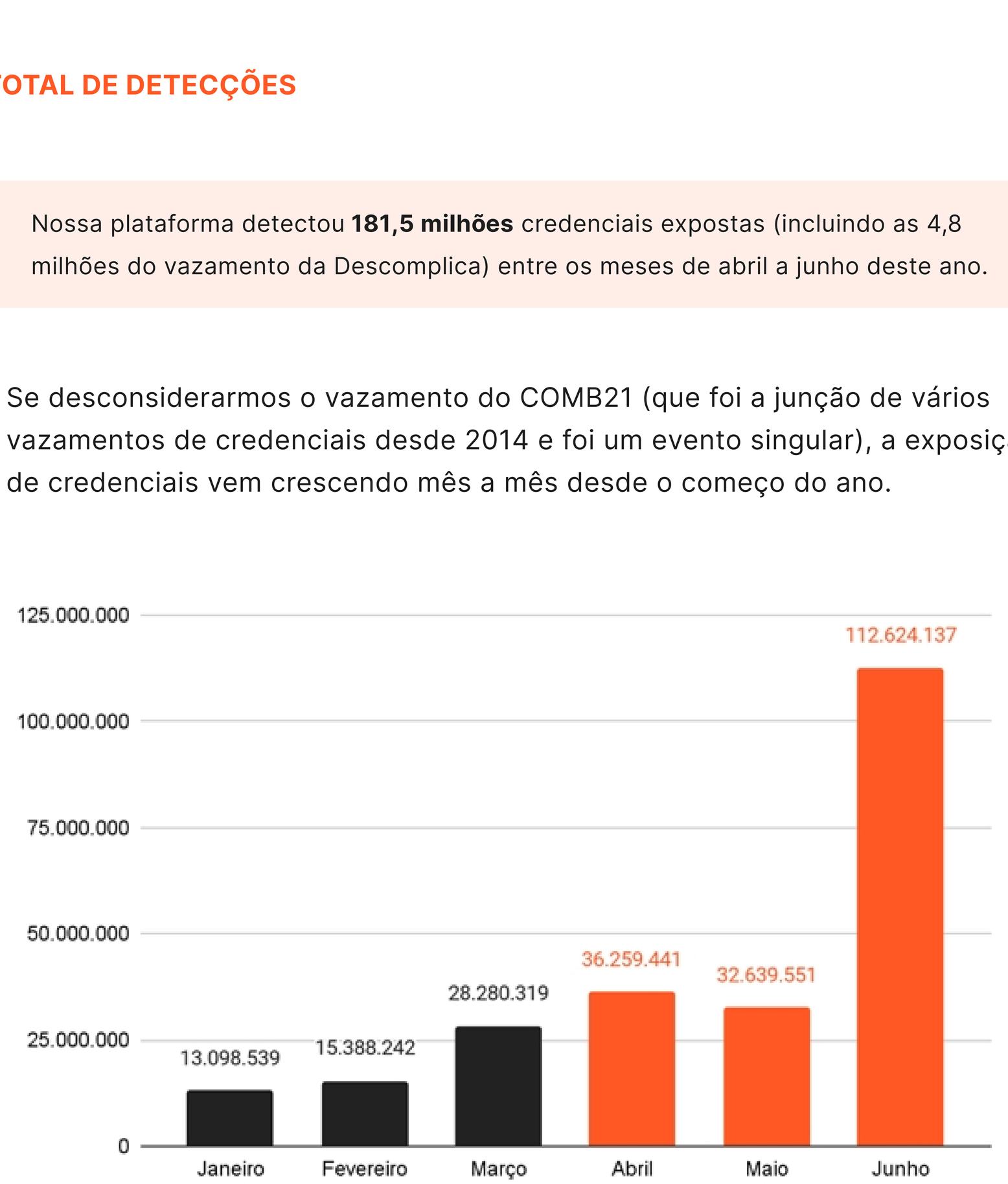


Figura 5. Volume mensal de credenciais expostas detectadas pela Axur no primeiro semestre de 2021.

CREDENCIAIS BRASILEIRAS

- No segundo trimestre foram encontradas:
  31 milhões de credenciais de domínios corporativos[1] (17,1% do total), distribuídas entre 4,26 milhões de empresas distintas (total mundial)[2].

- 494.329 credenciais .br, distribuídas entre 309.613 domínios distintos[2].
  Dessas, foram:

  - 149.044 credenciais de domínios corporativos (30,1% do total brasileiro) e 160.569 de domínios gov.br (32,4%).

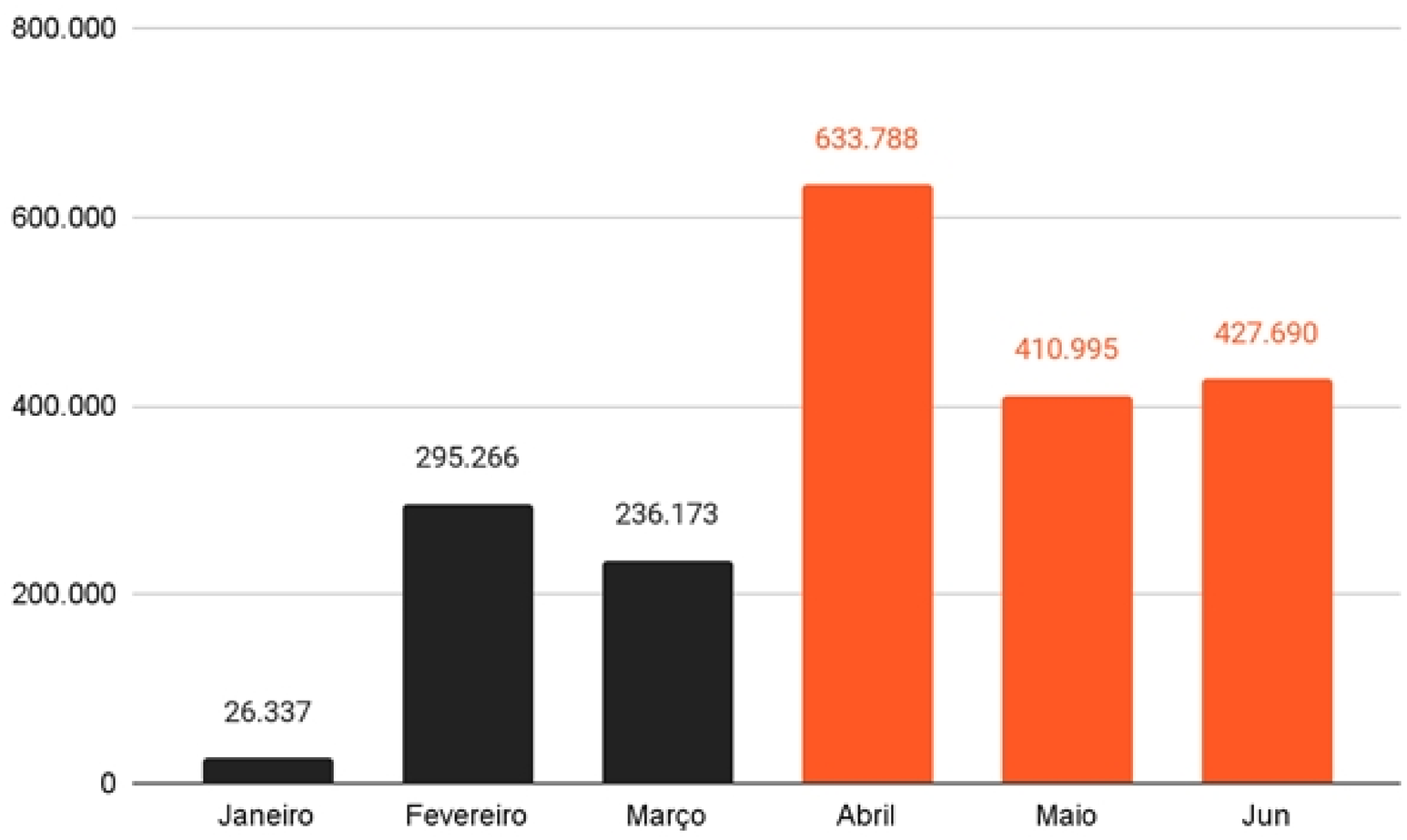


Figura 6. Crescimento mensal das credenciais expostas encontradas pela Axur somente no Brasil durante o primeiro trimestre de 2021.

[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.

Credenciais corporativas e gov.br

Na figura 7, logo abaixo, você poderá ver a distribuição de credenciais corporativas e governamentais ao longo dos últimos seis meses, que também denotam um crescimento acelerado após o mês de fevereiro. Em relação ao trimestre anterior, tivemos um aumento de 815% para credenciais corporativas brasileiras, e de 530% para credenciais gov.br.

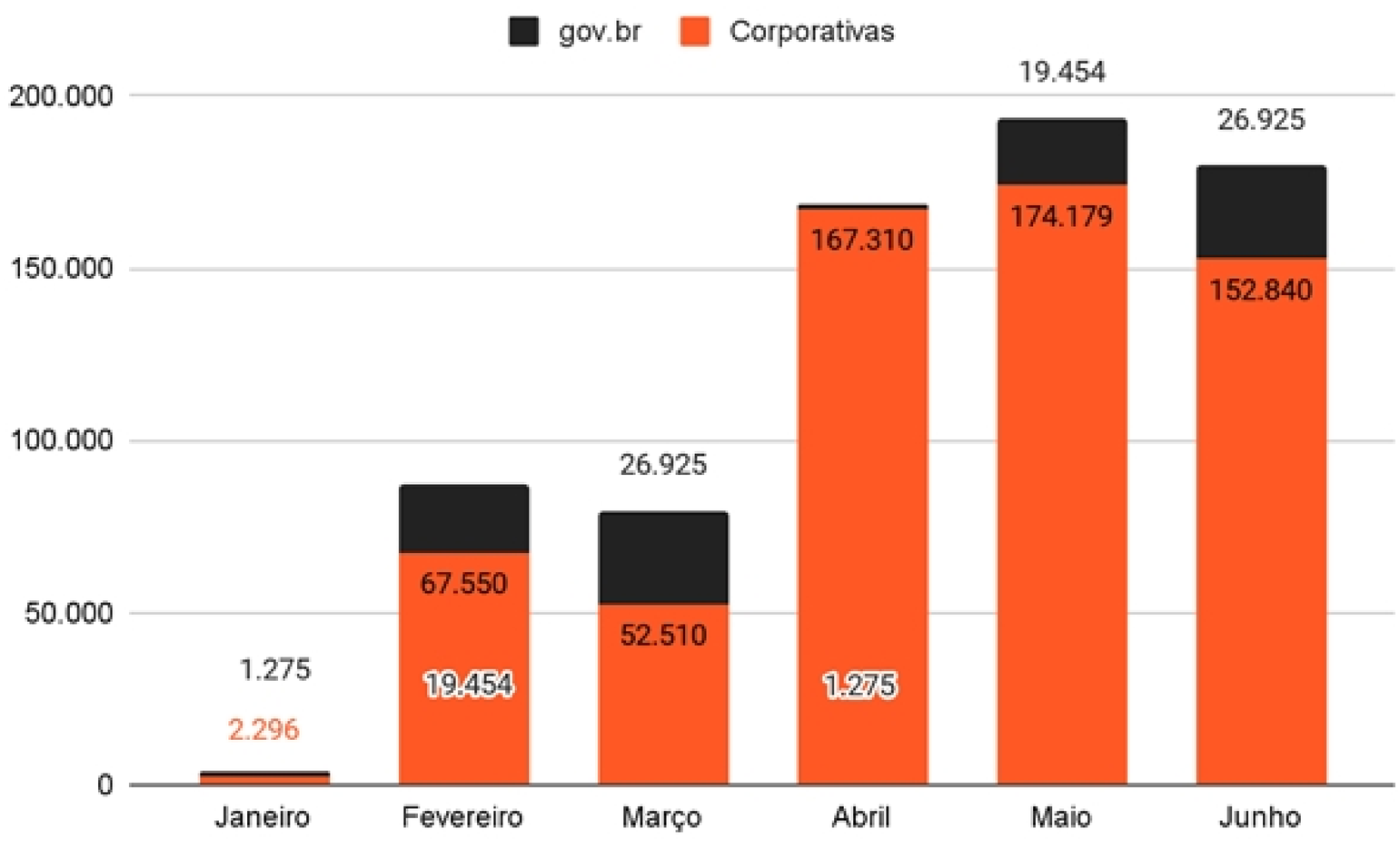


Figura 7. Volume de credenciais corporativas e de órgãos públicos detectadas pela Axur no quarto trimestre de 2020 e no primeiro de 2021.

Raio-X das senhas

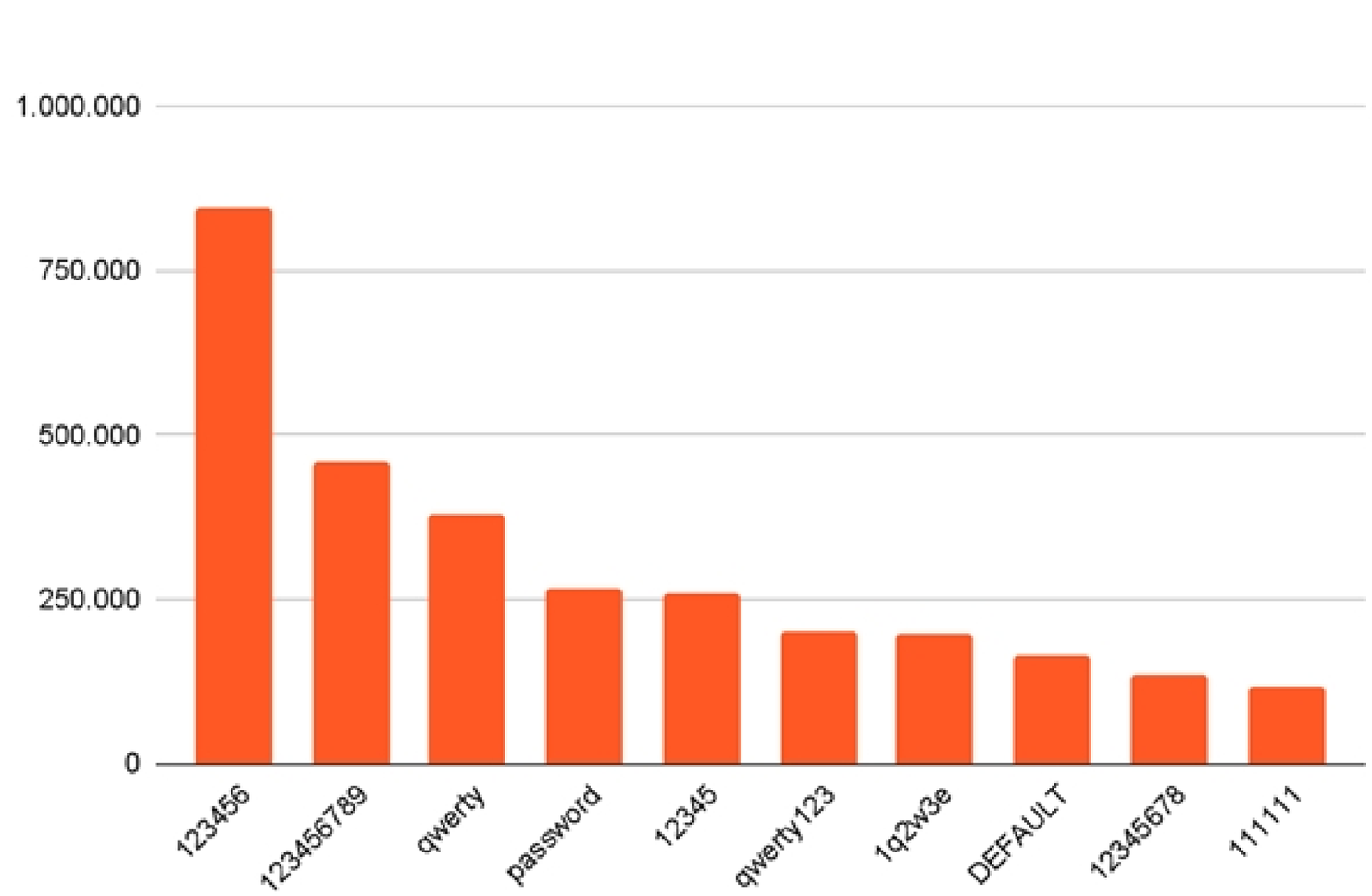


Figura 8. Volume das senhas mais expostas no segundo trimestre de 2021.

Como temos visto já há 1 ano, a sequência numérica "123456" continua sendo a senha mais utilizada (Figura 8). Neste trimestre, entre as credenciais expostas, 845.399 pessoas optaram por utilizar a senha mais querida dos cibercriminosos.

Também vemos outras sequências numéricas como "123456789", "12345", "12345678"e "111111"entre as 10 mais utilizadas. 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.

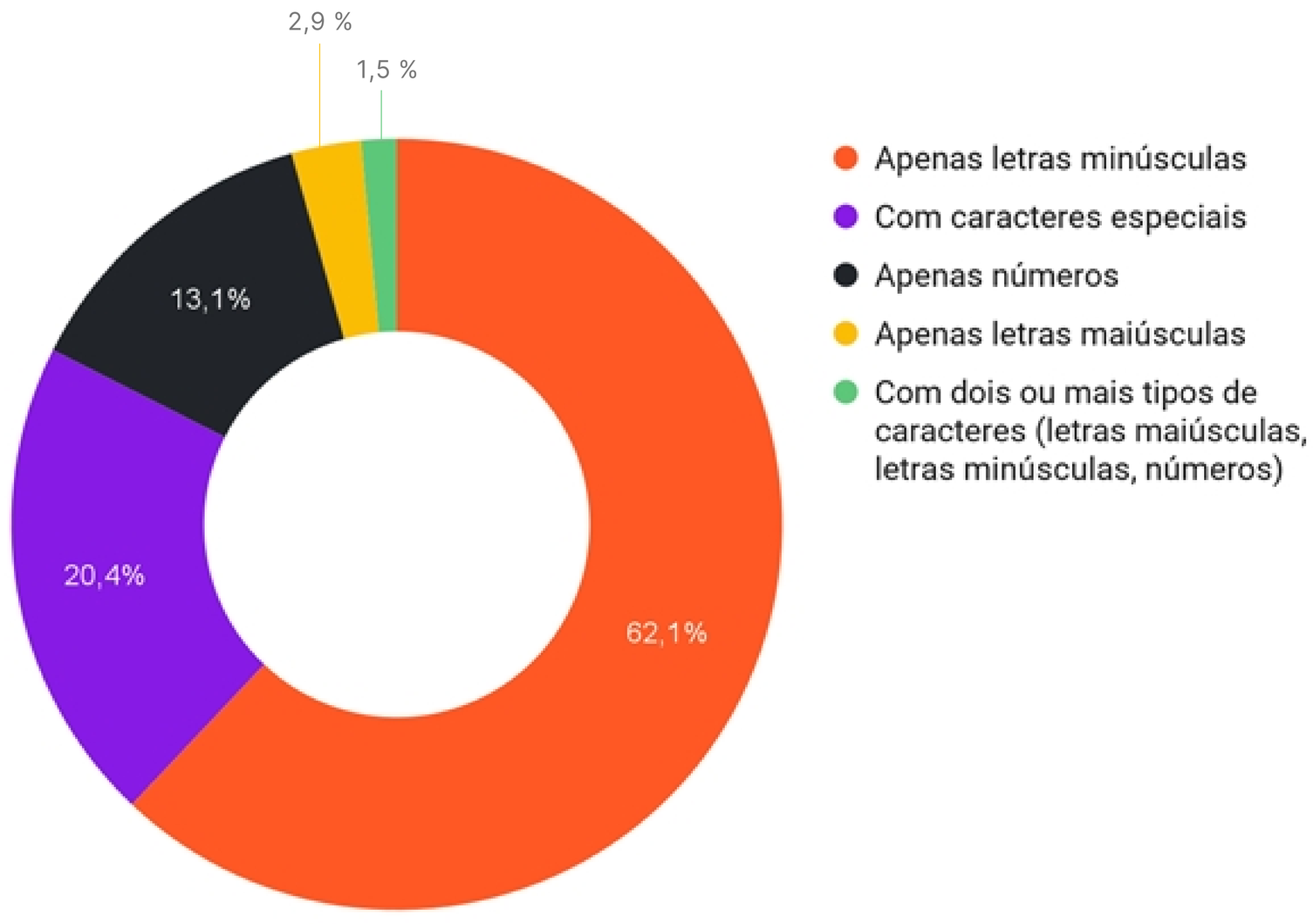


Figura 9. Distribuição percentual de senhas conforme os caracteres que as compõem, identificadas no segundo trimestre de 2021.

Em relação ao tipo de senha, temos 62,1% das senhas expostas neste trimestre que utilizam somente letras minúsculas, que perdeu pouco espaço (3,1%) desde o trimestre anterior. O mais interessante deste trimestre é o aumento da preferência pela utilização de senhas com caracteres especiais, que dificulta muito mais a vida dos cibercriminosos (20,4%).

Figura 10. Origem das credenciais expostas encontradas pela Axur no segundo trimestre de 2021.

Aqui sim tivemos muitas mudanças. O crescimento de credenciais expostas em grandes vazamentos toma conta de quase todas as credenciais que identificamos (99,1%), que representam o crescimento de 92,8% da preferência dos cibercriminosos pela deep e dark web na hora de monetizar suas ações com a venda de credenciais.

Vazamento ou exposição de cartões de crédito e débito

TOTAL DE DETECÇÕES

Neste trimestre, a Axur identificou **267.921 cartões expostos** na web superficial e na deep e dark web. Destes, 248.758 (92,8%) estavam na data de validade no momento da detecção.

Do trimestre passado para este, tivemos uma diminuição de 36,2% na detecção de cartões de crédito e débito, ou seja, 152.156 cartões a menos do que no trimestre anterior.

No entanto, tivemos, em abril deste ano, o maior pico detectado até agora, com 211.403 cartões (Figura 10), que bateu, inclusive nosso maior pico de janeiro (194.611 cartões), que representa um crescimento de 8,63%.

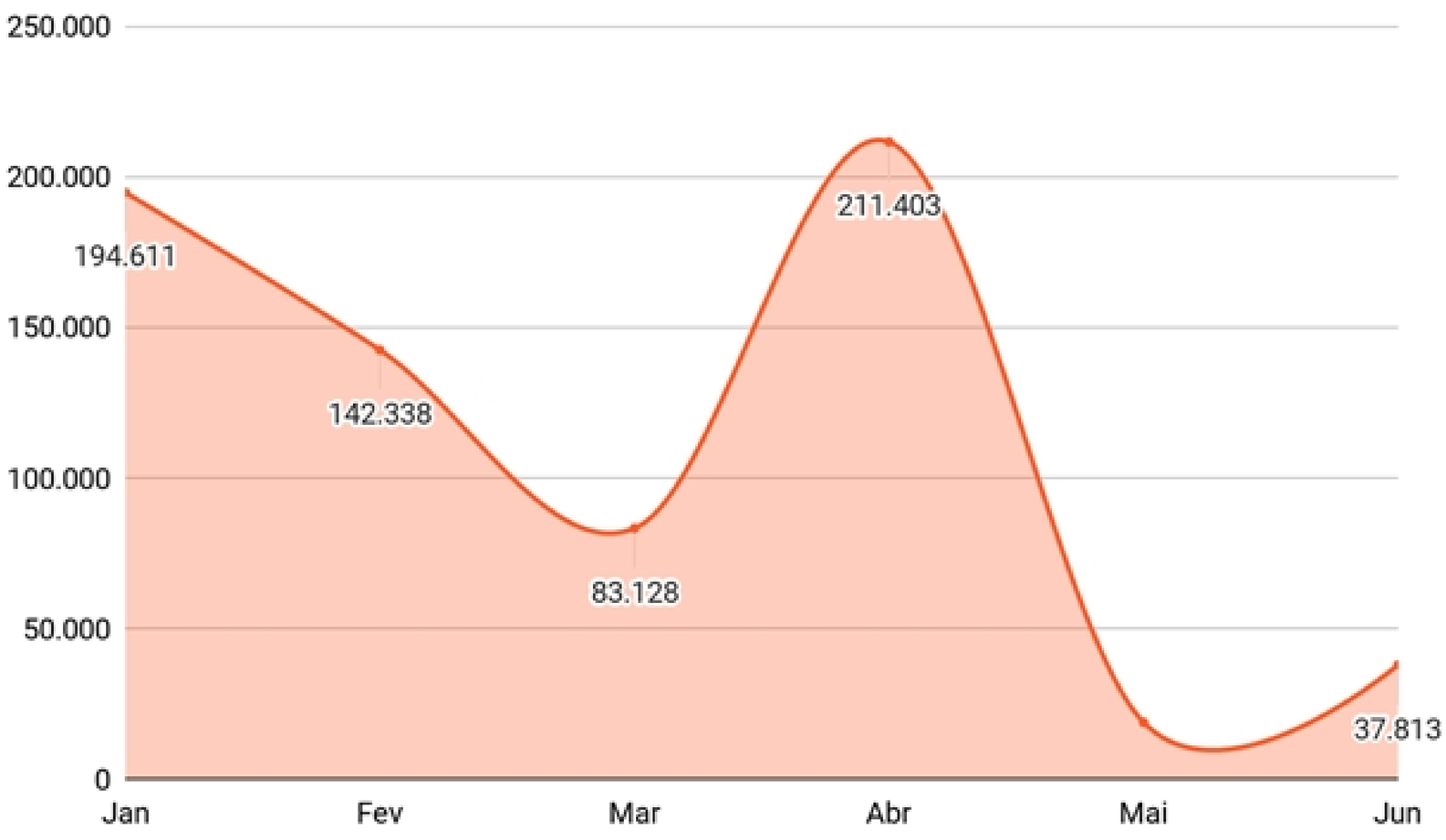


Figura 11. Quantidade de cartões de crédito e débito expostos por mês, comparando os dois primeiros trimestres de 2021.

O Brasil mantém sua posição como campeão de vazamentos de cartões de crédito e débito, com **137.483 cartões identificados** pela Axur

Isso é 44,3% a mais do que o segundo colocado, os EUA, com 60.939 cartões. No entanto, apesar de manter a posição no ranking, registramos uma queda de 8,1% na incidência de cartões brasileiros entre os expostos.

Isso se dá, muito por conta do aumento da participação de outros países, como Colômbia, Canadá, Espanha, Georgia, Bélgica e Turquia, bem como os outros países não mencionados que juntos detém 20,4% dos cartões expostos (4,7% a mais do que no trimestre anterior).

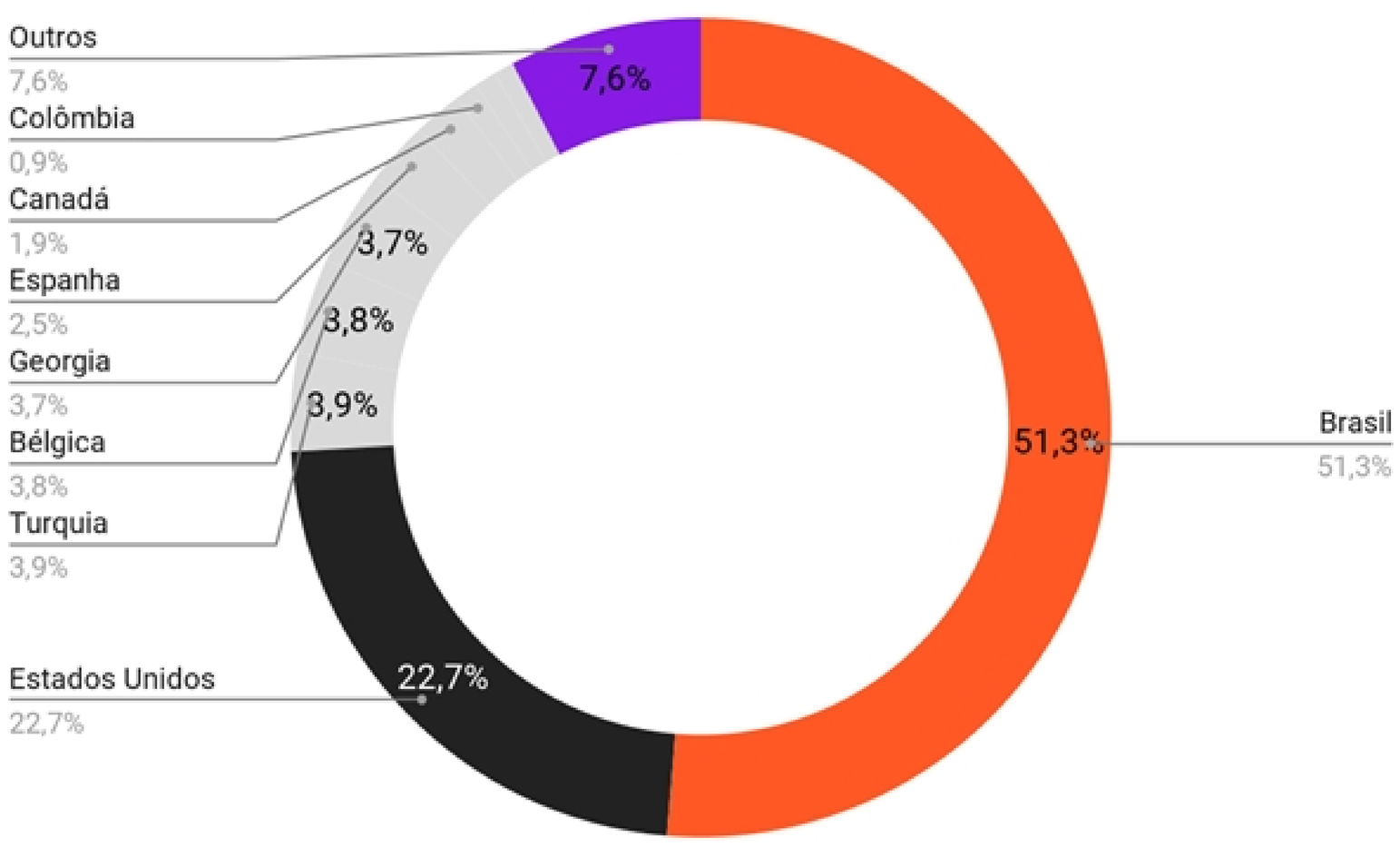


Figura 12. Porcentagem total dos países com mais cartões de crédito e débito vazados online e detectados pela Axur no primeiro trimestre de 2021.

Exposição de BINs

Se no trimestre passado tínhamos identificado uma redução de 15,16% da exposição de BINs únicas, este trimestre é ainda mais animador. Registramos uma queda de 38% em relação ao primeiro trimestre do ano (Figura 13).

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.

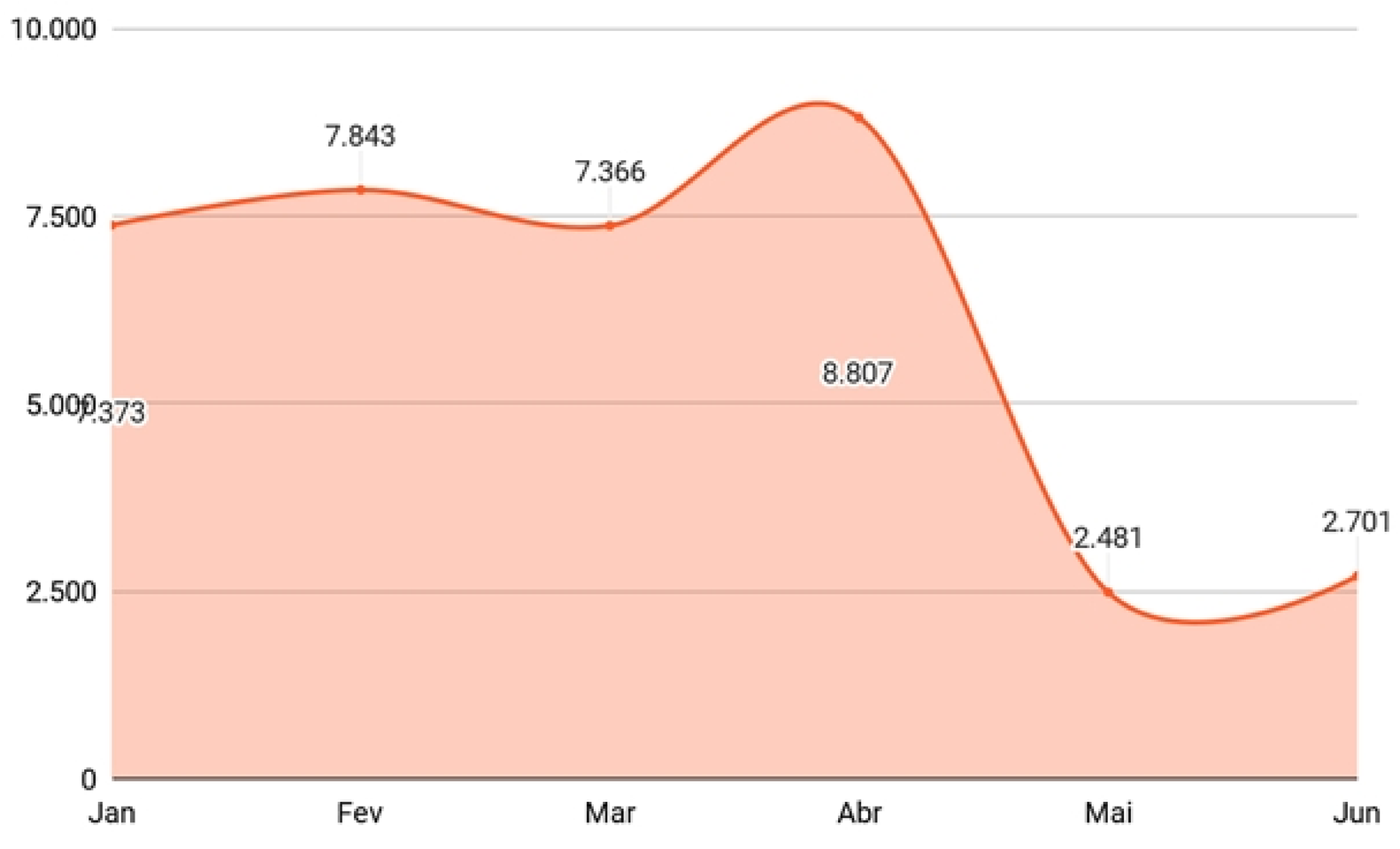


Figura 13. Quantidade de BINs expostas por mês, comparando o último trimestre de 2020 com o primeiro de 2021

Boa notícia para o Brasil. Nós ocupávamos 10 das 15 posições do ranking de países com maior exposição de BINs únicas no trimestre passado. Neste trimestre, ocupamos somente 1, com 1.187 BINs brasileiras vazadas (Figura 14).

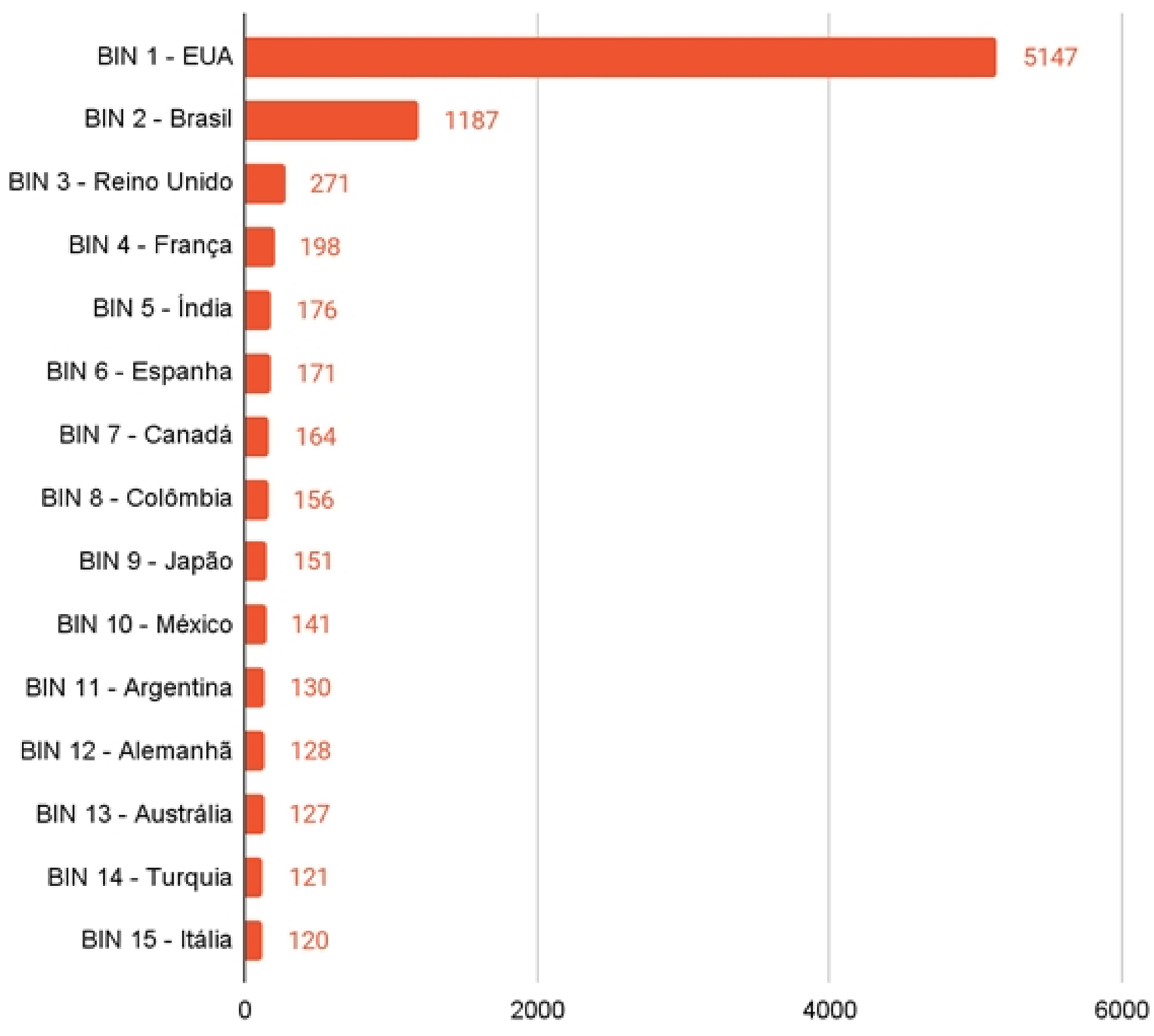


Figura 14. Ranking mundial das 15 BINs com mais exposição de dados de cartões de crédito e débito registrados no primeiro trimestre de 2021, identificadas por país.

Neste trimestre, 52,2% dos cartões identificados pela Axur estavam dentro da data de validade no momento da detecção, 1,8% a mais do que no trimestre anterior (Figura 15).

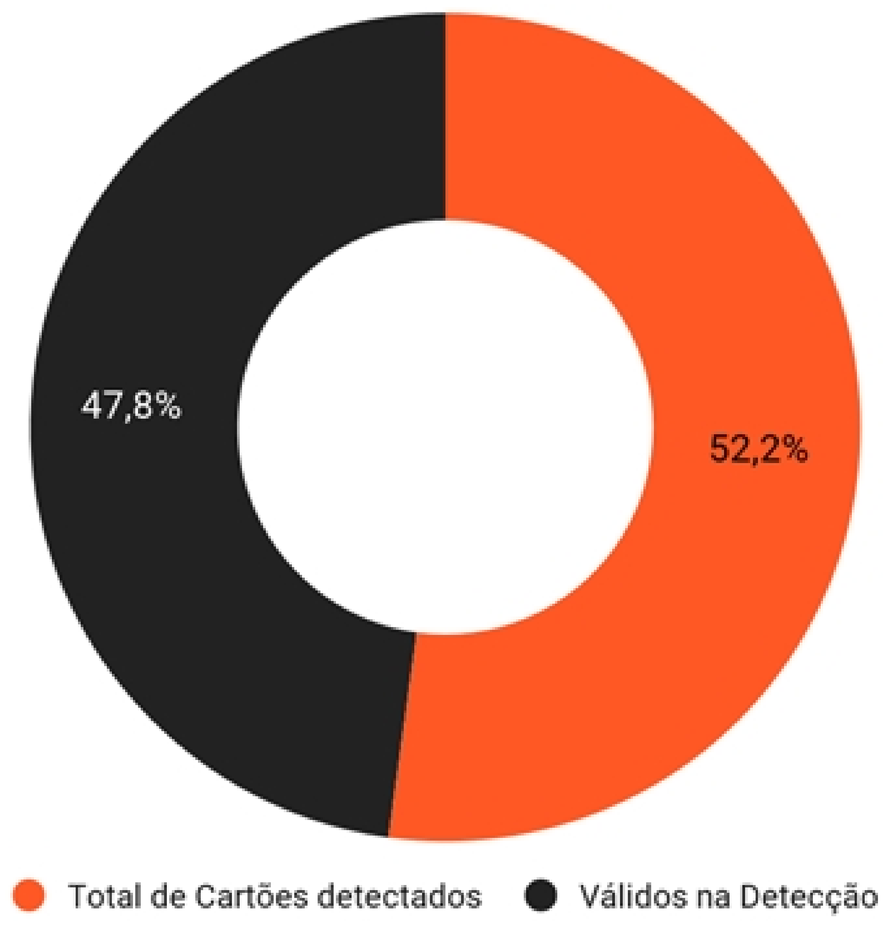


Figura 15. Percentual de cartões expostos vs. cartões válidos na data de coleta no segundo trimestre de 2021.

Glossário

- **Deep web**
  É a web não acessível via mecanismos de busca e indexação (como o Google).

- **Dark web**
  A web acessada somente por navegadores específicos, como a rede TOR.

- **Phishing**
  site falso e fraudulento enviado com o intuito de capturar dados pessoais, como senhas e números de cartão de crédito.

  - **Spear phishing**
    Forma de envio de phishing direcionada a uma pessoa ou empresa específica.

- **Malware**
  Software malicioso que é instalado em computadores, disseminado por técnicas de engenharia social, e que em geral personificam marcas financeiras para capturar dados sensíveis de consumidores.

- **Risco digital**
  Perigos que geram prejuízos financeiros e estão fora do perímetro de atuação da empresa. Em termos técnicos, tudo o que acontece fora das proteções de firewall.

- **ISP (Internet Service Provider)**
  Do inglês, Provedor de Serviços de Internet, esse termo se refere a empresas que fornecem, por meio de seus serviços, acesso à internet.

Acesse o **dicionário de riscos digitais** em nosso blog e veja mais!

Detecção e procedimentos

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 que os processos sejam automatizados e mais facilmente visíveis na forma de dados:

✓ **Coletores**

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).

✓ **Machine learning**

É usado pela Axur para diminuir exponencialmente os tempos 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, fazendo com que seja possível visualizar ameaças em potencial e incidentes de forma prática e clara. 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**

Veja também

Como reagir quando um vazamento de dados acontece?

Saber como agir no caso de um vazamento, bem como agir com agilidade pode ser crucial para evitar que um vazamento tome proporções catastróficas. Assita agora

O que realmente importa na hora de lidar com dados?

Se preparar para um vazamento de dados começa na prevenção dele, isto é, em todas as ações relacionadas à monitoramento, detecção e plano de resposta a incidentes. Assita agora

9 riscos digitais para ficar de olho esse ano

Phishing, ransomware, violação da privacidade de dados. Você já se atentou para as ameaças que os cibercriminosos representam para sua empresa? Assita agora

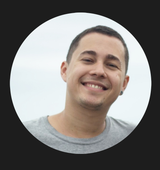
CYBERSEG NEWS

Se inscreva no **AxurCast**, para ouvir os episódios semanais do CyberSeg News, nosso quadro semanal que traz as últimas notícias e comentários do nosso time de especialistas sobre tecnologia e cibersegurança. Ouça agora

Quer conhecer mais sobre o universo da deteção automática de ameaças? Conheça as soluções personalizadas que a Axur oferece.

Monitore sua base de dados | Monitore suas credenciais de acesso | Monitore sua API Open Banking

Hugo Moura, Redação



Patrick Santos, Design

Sobre a Axur

Líder em monitoramento e reação a riscos 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 e vendas não autorizadas.

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

Contato para a imprensa

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

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