AXUR

RELATÓRIO

Atividade criminosa online no Brasil

3º trimestre / 2020

São Paulo, 28 de outubro de 2020

Principais números deste relatório

Clique no número de página após o dado para ir à seção correspondente.

289,1 mi

de **credenciais** vazadas foram expostas — página 11

72,4%

dos **cartões expostos** identificados são **brasileiros** — página 14

90,4%

foi o aumento dos **cartões de crédito e débito** vazados expostos — página 15

- **9,87%** foi o aumento dos **casos de phishing** em um trimestre — página 4
- **54%** dos casos de phishing são voltados a **e-commerce** — página 5
- **63%** dos ataques de phishing são feitos **sem menção a marcas no domínio** — página 7
- **38 arquivos de malware** detectados, mesmo número do trimestre anterior — página 8
- **Amazon AWS** é a infraestrutura mais escolhida para hospedagem de arquivos de malware — página 10
- **7,5 caracteres** é o tamanho médio das **senhas vazadas** detectadas — página 13
- **51,8%** é o total de casos de **pirataria** dentro de usos de marca — página 16

A última seção deste relatório, sobre a atividade criminosa 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

Quando a segurança digital não é só trabalho de um grupo

Fazer um relatório para refletir trimestralmente sobre o impacto do crime digital no ambiente brasileiro é daquelas tarefas que assustam bastante e, ao mesmo tempo, dão motivação para poder agir (e reagir) com base em dados e fatos.

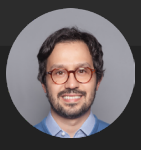
Na Axur fazemos isso todos os dias, é claro, mas com dados como os que você vai ver nas próximas páginas é que conseguimos mostrar com exatidão o porquê da segurança digital estar tão em alta (alô, LGPD), e isto é algo que repito ao longo dos tempos: os cibercriminosos evoluem na mesma medida - ou até mais rápido - que a sociedade.

São muitas novidades espalhadas por muitos períodos, de problemas com fraudes e vazamentos de dados surgidos com a pandemia do novo coronavírus aos novos golpes que já estão surgindo com as transações instantâneas e carteiras do PIX. Por isso, queremos reforçar algo que pode soar meio clichê, mas muito verdade: a segurança digital é responsabilidade de todos os setores, de todas as empresas.

Pensando nisso, temos nesta edição um glossário com os principais riscos digitais e termos usados neste relatório. Recomendo que essas páginas sejam usadas como consulta de cabeceira a todo o momento. Afinal, como disse acima, os crimes do futuro são os digitais.

Também já avisamos de antemão que o quarto trimestre iniciou a todo o vapor e em breve teremos informações e dados importantes sobre o PIX - e que devem sair antes da próxima edição deste relatório que você está lendo agora.

Por enquanto, tenha uma boa leitura e não deixe de acompanhar nossos conteúdos! Só o conhecimento permite avanços.



Fábio Ramos, CEO da Axur

Phishing

10.517 é o número de casos de phishing identificados no terceiro trimestre de 2020.

Isso significa um **crescimento de 9,87%** em comparação com os 9.572 casos do segundo trimestre. Em agosto, foi identificado o pico absoluto de detecções, inclusive se comparado a períodos do ano passado.

Em comparação com o mesmo período de 2019, o terceiro trimestre de 2020 também teve um aumento registrado de **53,26%** no número de phishing.

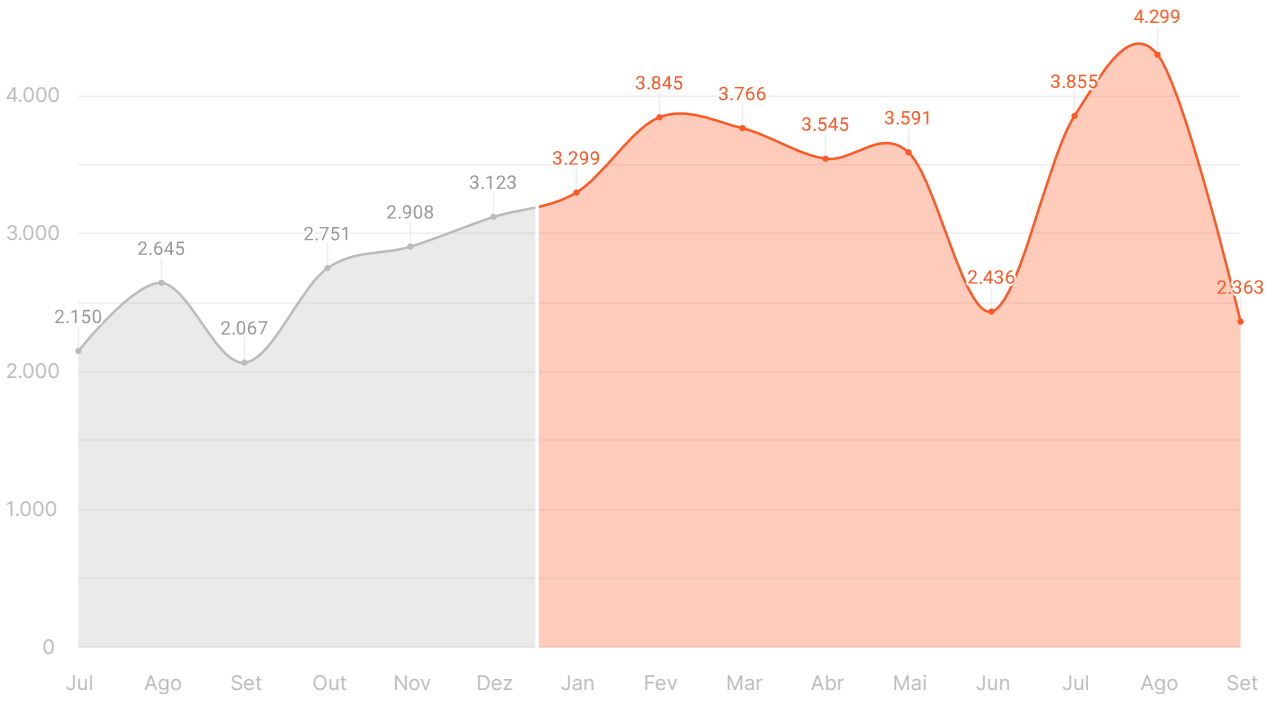


Figura 1. Evolução do número total de casos de phishing detectados no Brasil entre o terceiro trimestre de 2019 e o terceiro de 2020.

O maior destaque do crescimento de phishing do trimestre é no **setor de e-commerce,** que foi líder no número de ataques entre julho e setembro (Figura 2) e contabilizou, no total do trimestre, **54%** do volume de phishing.

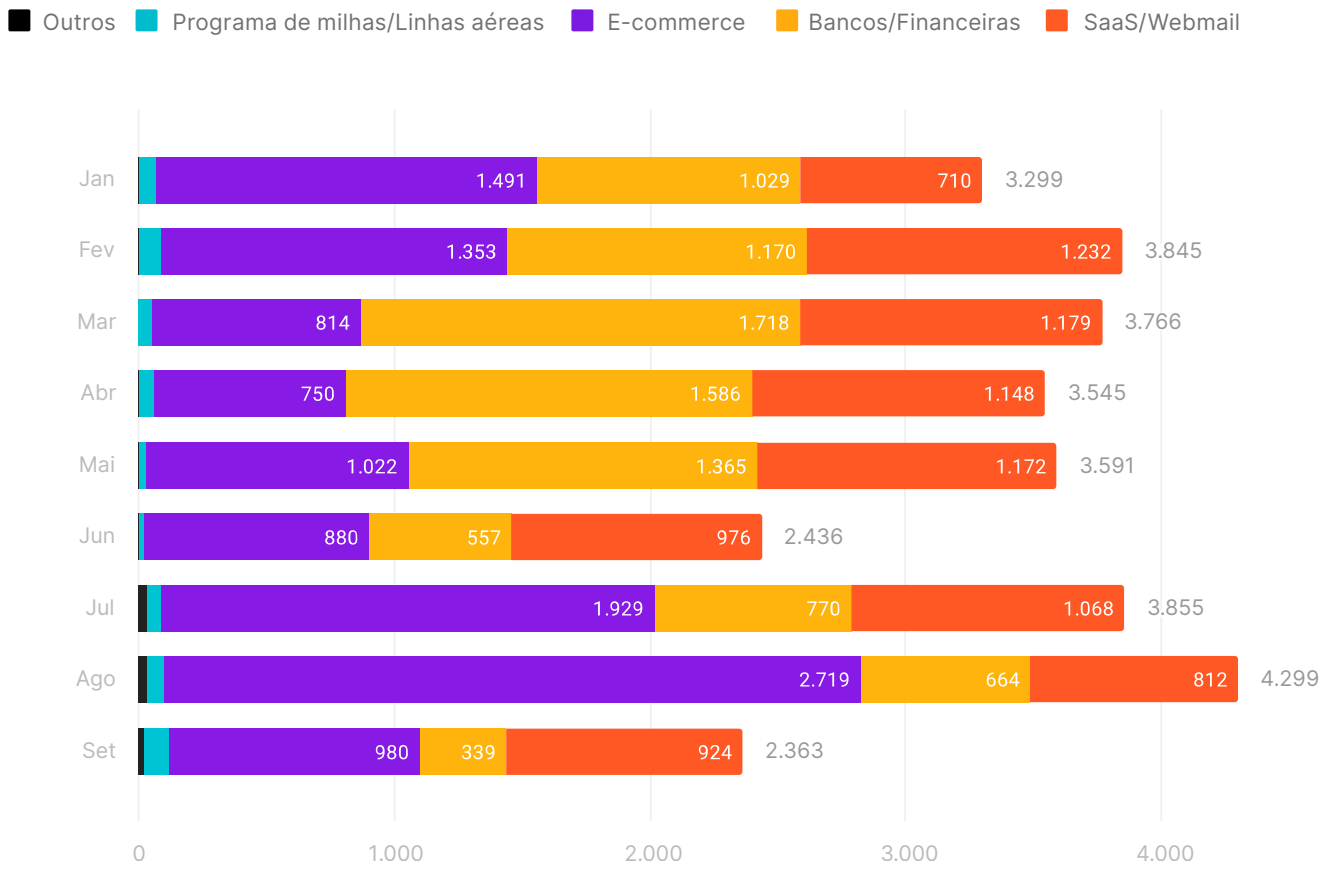


Figura 2. Casos de phishing detectados por mês em 2020, separados por setor atingido.

Esse valor mostra um crescimento acentuado em comparação com a fatia de 27,7% ocupada no trimestre anterior, que foi liderado pelos ataques ao setor financeiro (Figura 3).

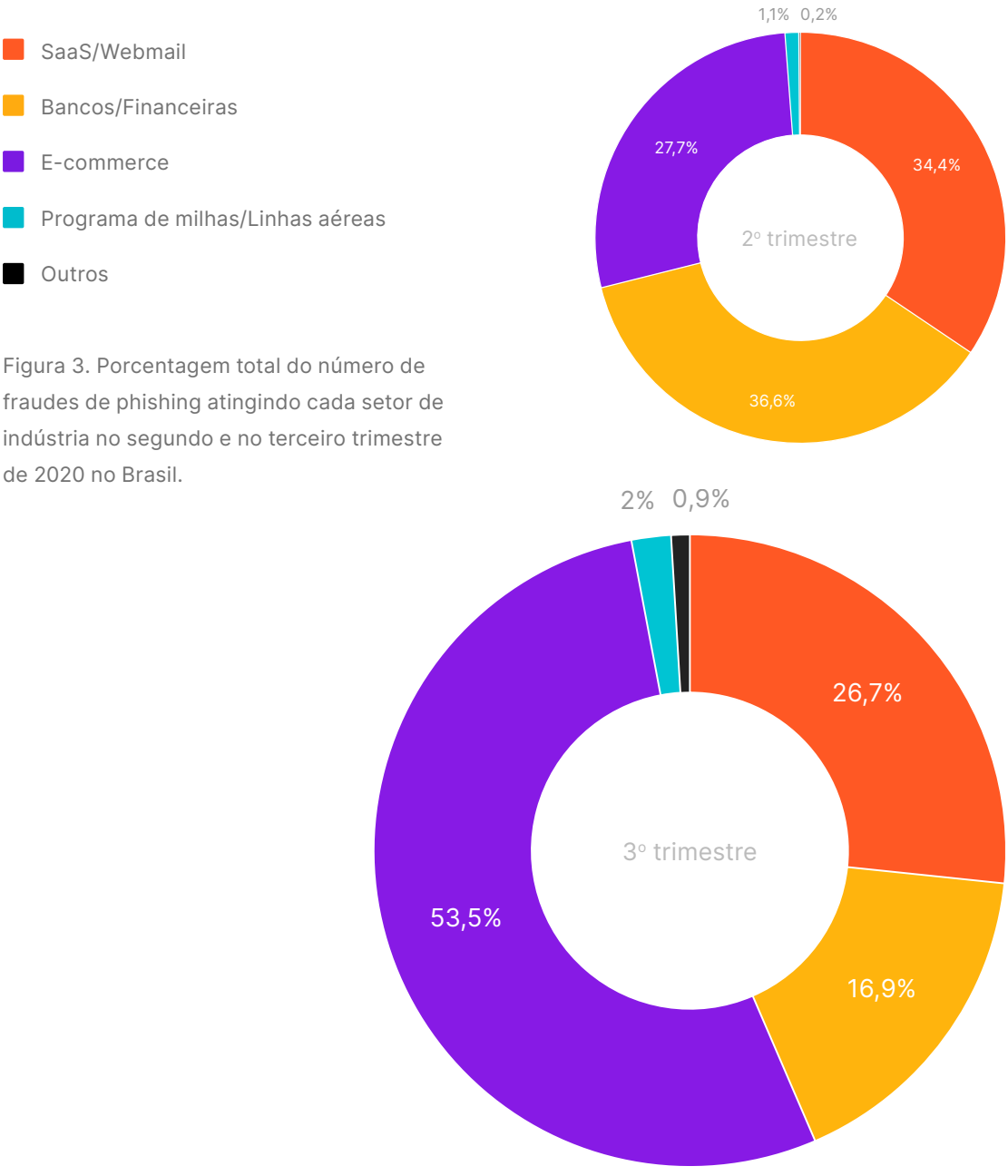


Figura 3. Porcentagem total do número de fraudes de phishing atingindo cada setor de indústria no segundo e no terceiro trimestre de 2020 no Brasil.

Quanto aos nomes de domínio usados para phishing também existem novidades. O terceiro trimestre registrou **recorde do total de casos com nomes de domínios genéricos,** sem menção a marcas e que visam dificultar detecções.

Nesses casos, são usadas palavras como “atualize”, “aproveite”, “ofertas” e outros termos que também podem fisgar mais vítimas. O comparativo entre 2019 e os outros períodos de 2020 está na Figura 4.

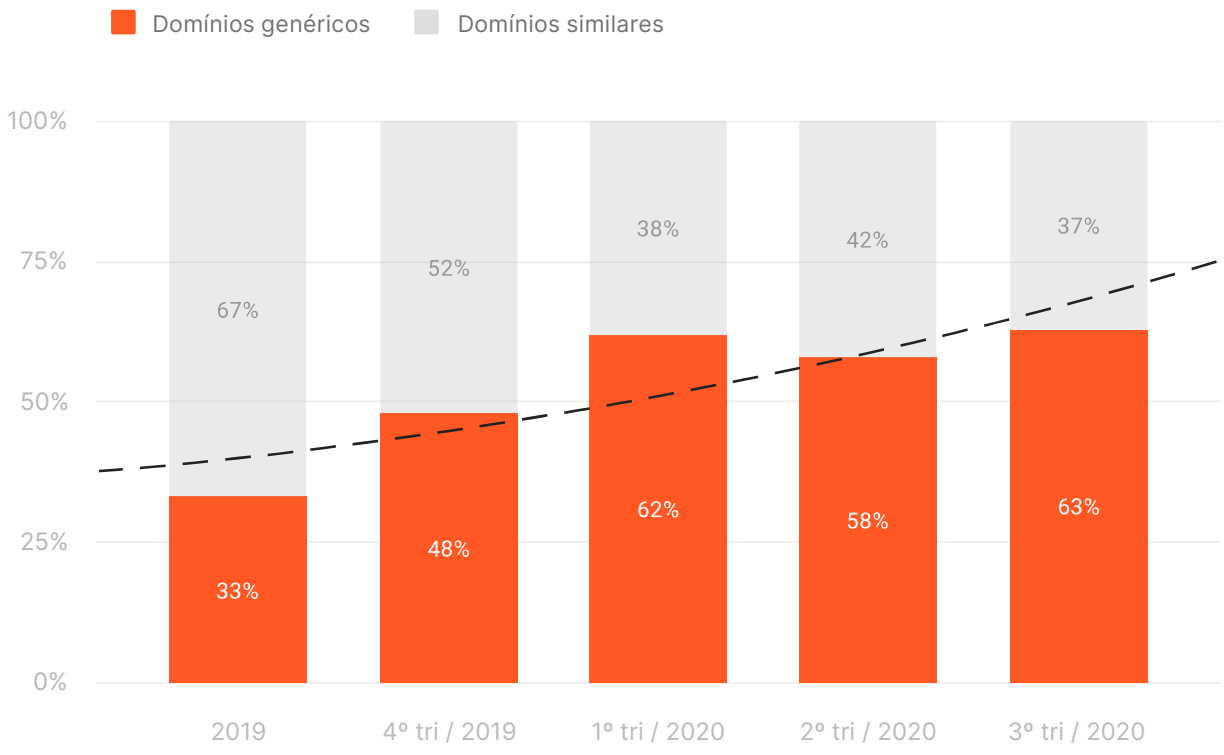


Figura 4. Porcentagem dos ataques de phishing com uso de domínios similares a marcas ou uso de domínios genéricos entre 2019 e o terceiro trimestre de 2020.

Malware e vírus

38 é o número de arquivos únicos de malware afetando diferentes instituições financeiras foram identificados no terceiro trimestre de 2020.[1]

O volume bruto de artefatos de malware tem estado **em diminuição em 2020,** que permanece em nível semelhante desde o segundo trimestre, quando também foram identificados 38 arquivos (Figura 5).

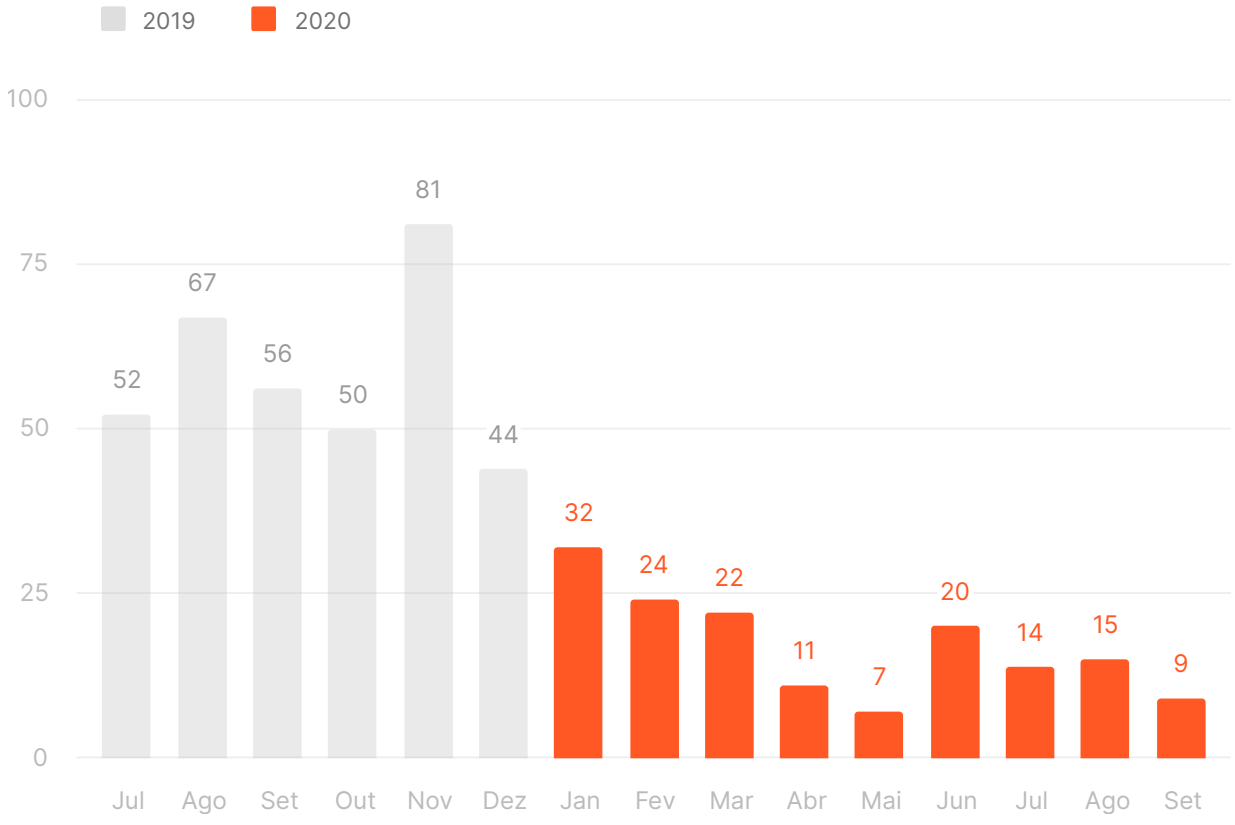


Figura 5. Volume mensal de casos únicos de malware detectados entre o terceiro trimestre de 2019 e o terceiro de 2020.

[1]Todos os malwares identificados são do tipo *trojan banker*, ou seja, nesta análise não foram computados ransomwares e outros tipos de artefatos.

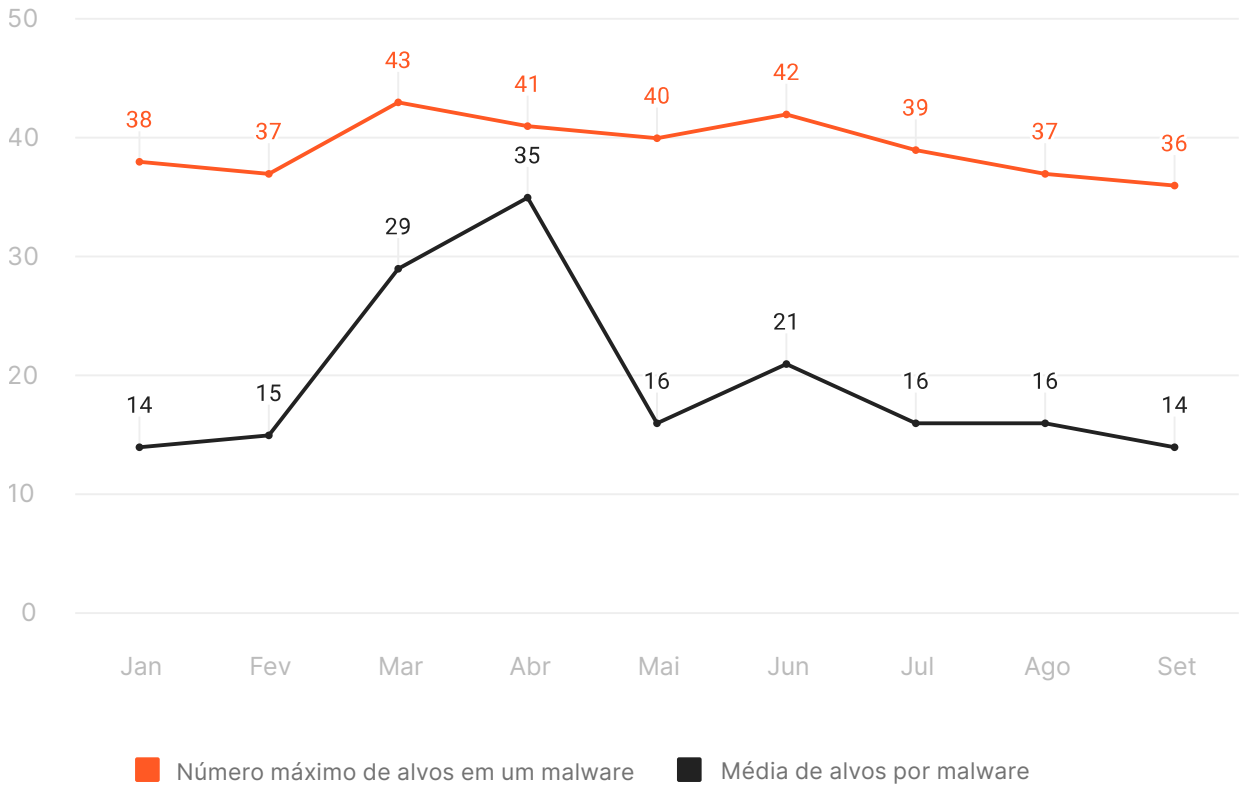


Figura 6. Média e número máximo mensal de bancos e instituições financeiras afetados por malware entre janeiro e setembro de 2020.

Os números médio e máximo de bancos e instituições financeiras detectadas por arquivo estão diminuindo (Figura 6), sem nenhum recorde registrado como no trimestre anterior.

A qualificação dos arquivos, porém, apresenta novidades. A maioria dos artefatos de malware detectada foi encontrada em servidores Amazon AWS (Figura 7).

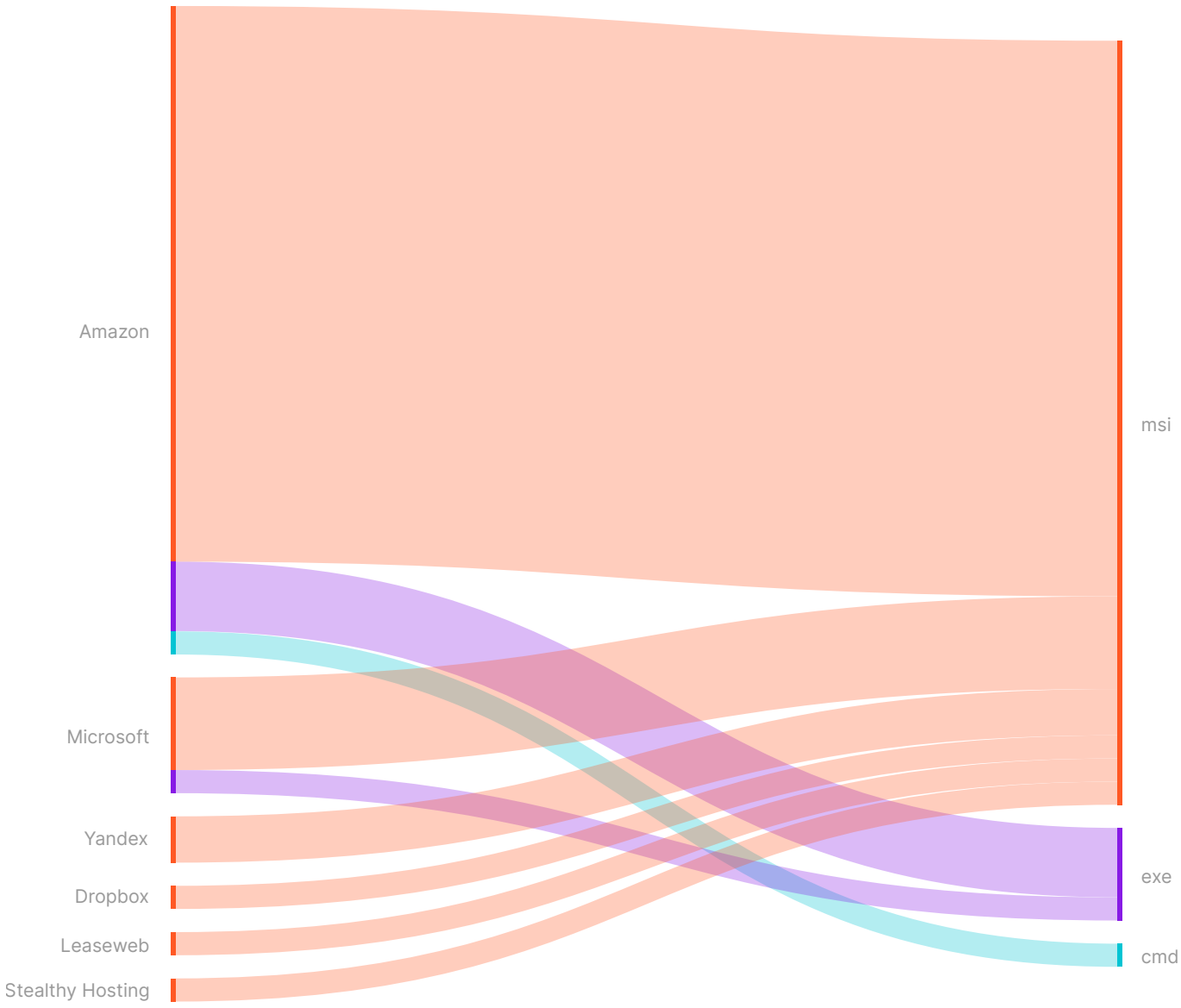


Figura 7. Classificação por ISP de hospedagem e por formato dos arquivos de malware do terceiro trimestre de 2020 detectados no Brasil.

Vazamento de credenciais

289,1 milhões é o número de credenciais expostas que foram detectadas pela Axur no terceiro trimestre de 2020.

Este número é comparativamente maior do que os 9,16 milhões de credenciais encontrados no trimestre anterior, e é majoritariamente composto por **grandes vazamentos em bases únicas** detectadas no período, que sozinhas contêm milhões de dados (Figura 8).

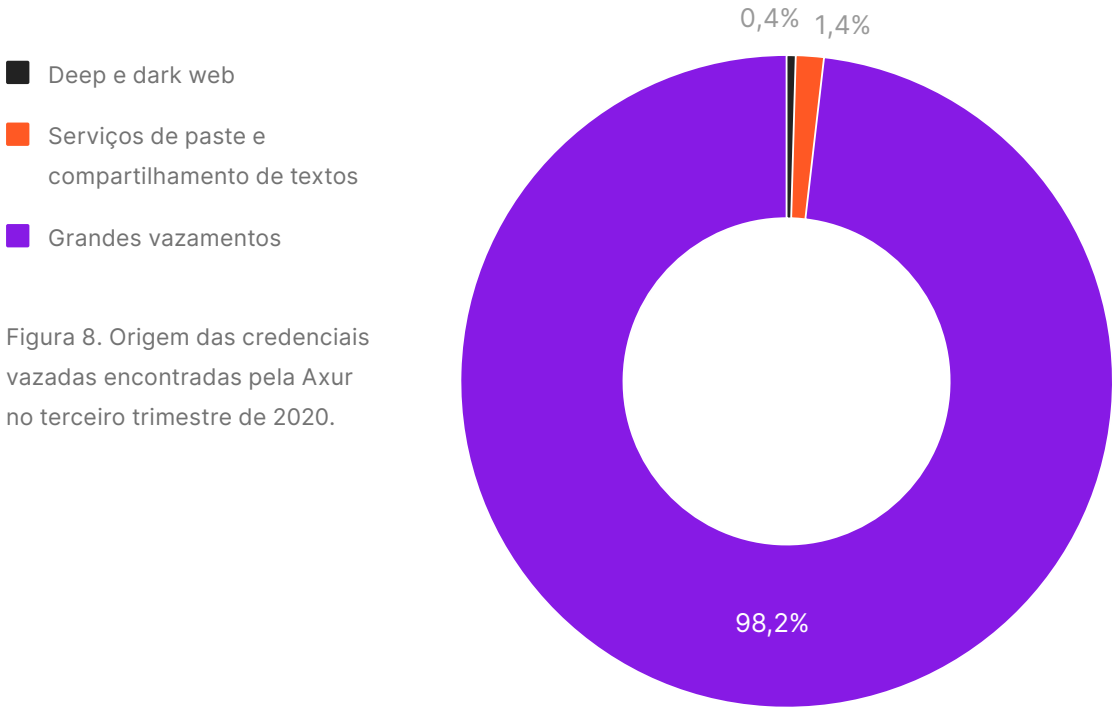


Figura 8. Origem das credenciais vazadas encontradas pela Axur no terceiro trimestre de 2020.

No trimestre, foram identificadas:

- **17,36 milhões de credenciais de domínios corporativos**[2] (6% do total), distribuídas entre 1,21 milhão de empresas distintas afetadas (no total mundial).[3]
- **11,52 milhões de credenciais .br**, distribuídas em 224.276 domínios distintos.[4] Dessas, foram:
  - 3,8 milhões de credenciais de domínios corporativos (33% do total brasileiro, percentual 5 vezes maior que os 6% do total mundial), em 276.454 empresas distintas afetadas.
  - 33.911 credenciais .gov.br distribuídas em 2.446 domínios distintos.

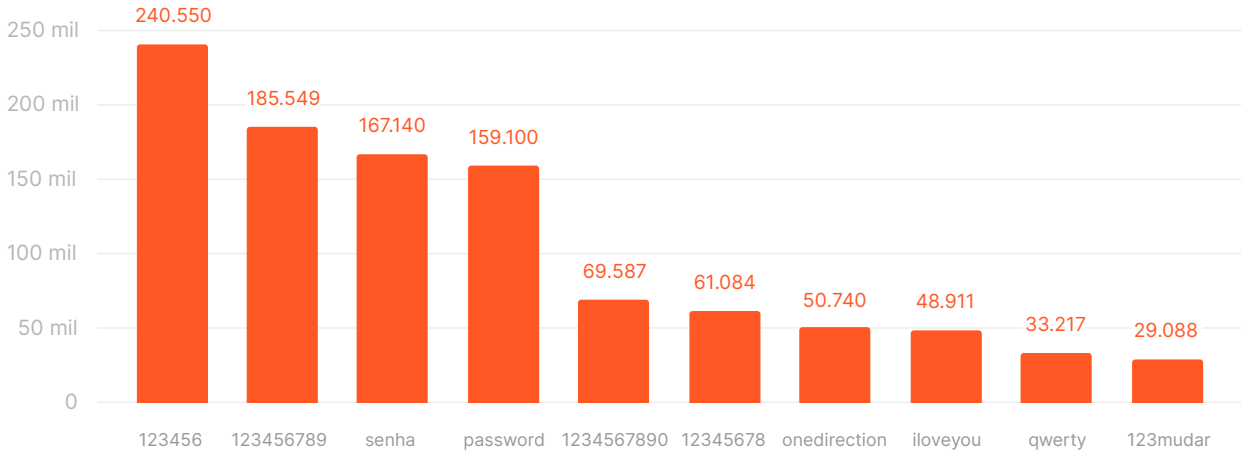


Figura 9. Ranking global de exposição de senhas detectadas pela Axur no terceiro trimestre de 2020.

[2]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. Ainda assim, é importante perceber que essas credenciais representam risco devido à prática de utilizar o mesmo par de e-mail e senha em vários sites.
[3]O número de domínios distintos de empresas é obtido a partir da remoção de todos os domínios considerados públicos (como gmail.com, yahoo.com e outros).
[4]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.

Graças aos grandes vazamentos registrados, existe grande disparidade no ranking e nos tipos de caracteres utilizados nas senhas detectadas. A campeã em vazamentos continua sendo 123456, sequência numérica mais comum (Figura 9).

O tamanho médio de todas as senhas detectadas no período é de **7,5 caracteres,** abaixo dos 8,3 do trimestre anterior.

Desta vez, o tipo campeão de senha com maior volume de vazamentos é o de **senhas com caracteres/símbolos especiais,** que ocupa 55,1% do total. Para fins de comparação, o trimestre anterior registrou 75,06% de senhas formadas somente por letras minúsculas (Figura 10).

De qualquer forma, o tipo de senha composta somente por letras minúsculas continua ocupando uma parcela considerável dos vazamentos e registrou 37,2% do total do trimestre.

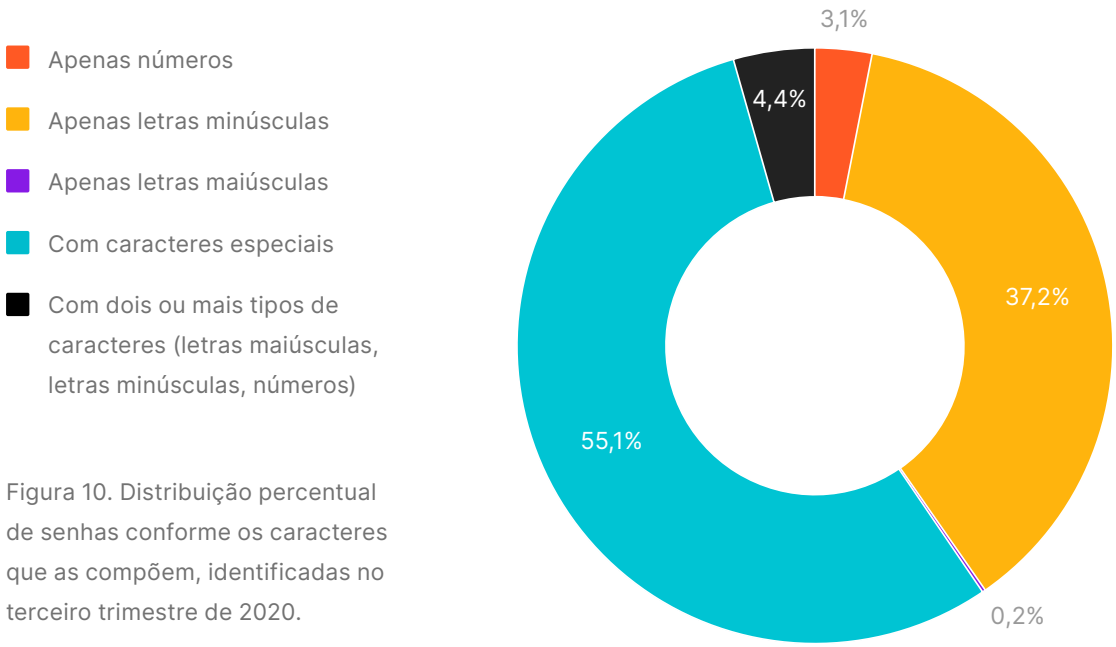


Figura 10. Distribuição percentual de senhas conforme os caracteres que as compõem, identificadas no terceiro trimestre de 2020.

Vazamento de cartões de crédito e débito

No terceiro trimestre de 2020, **986.063 cartões** de crédito e débito com dados completos foram identificados pela Axur, expostos da web superficial à deep e dark web e distribuídos entre 61.104 BINs distintas.

Destes, **96,9%** (956.201 cartões) estavam dentro da data de validade no momento da detecção.

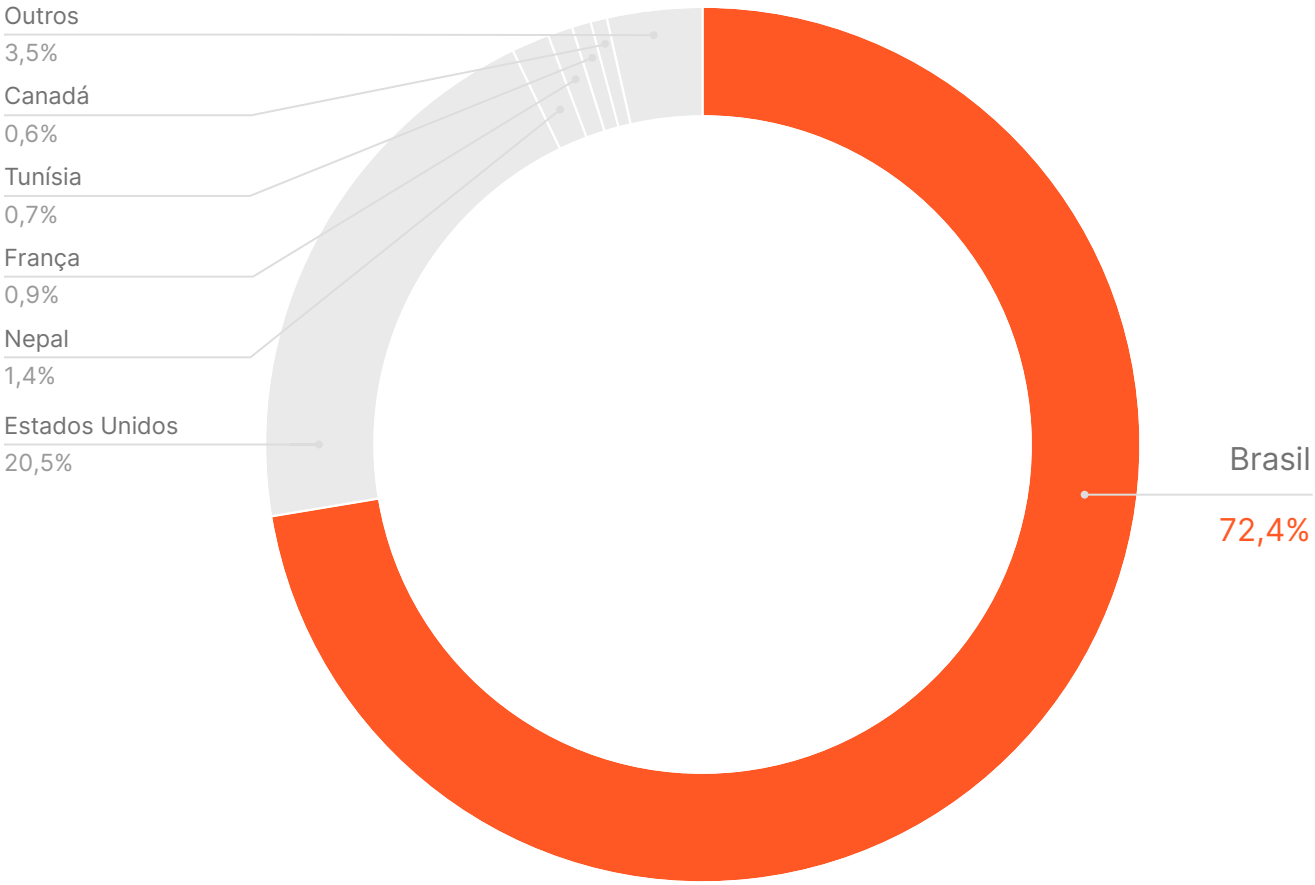


Figura 11. Porcentagem total dos países com mais cartões de crédito e débito vazados online e detectados pela Axur no terceiro trimestre de 2020.

O número total de cartões detectados representa um **aumento de 90,4%** em comparação com o segundo trimestre de 2020, quando foram detectados 517.670 cartões vazados.

É também fato inédito que, como campeão mundial no número total de vazamentos (da amostra das 500 BINs com mais vazamentos, Figura 11), **o Brasil segue na liderança com o maior número de cartões expostos e ainda ocupa o primeiro lugar no ranking de BINs com mais exposições** (além de 8 das 10 primeiras posições, como mostra a Figura 12).

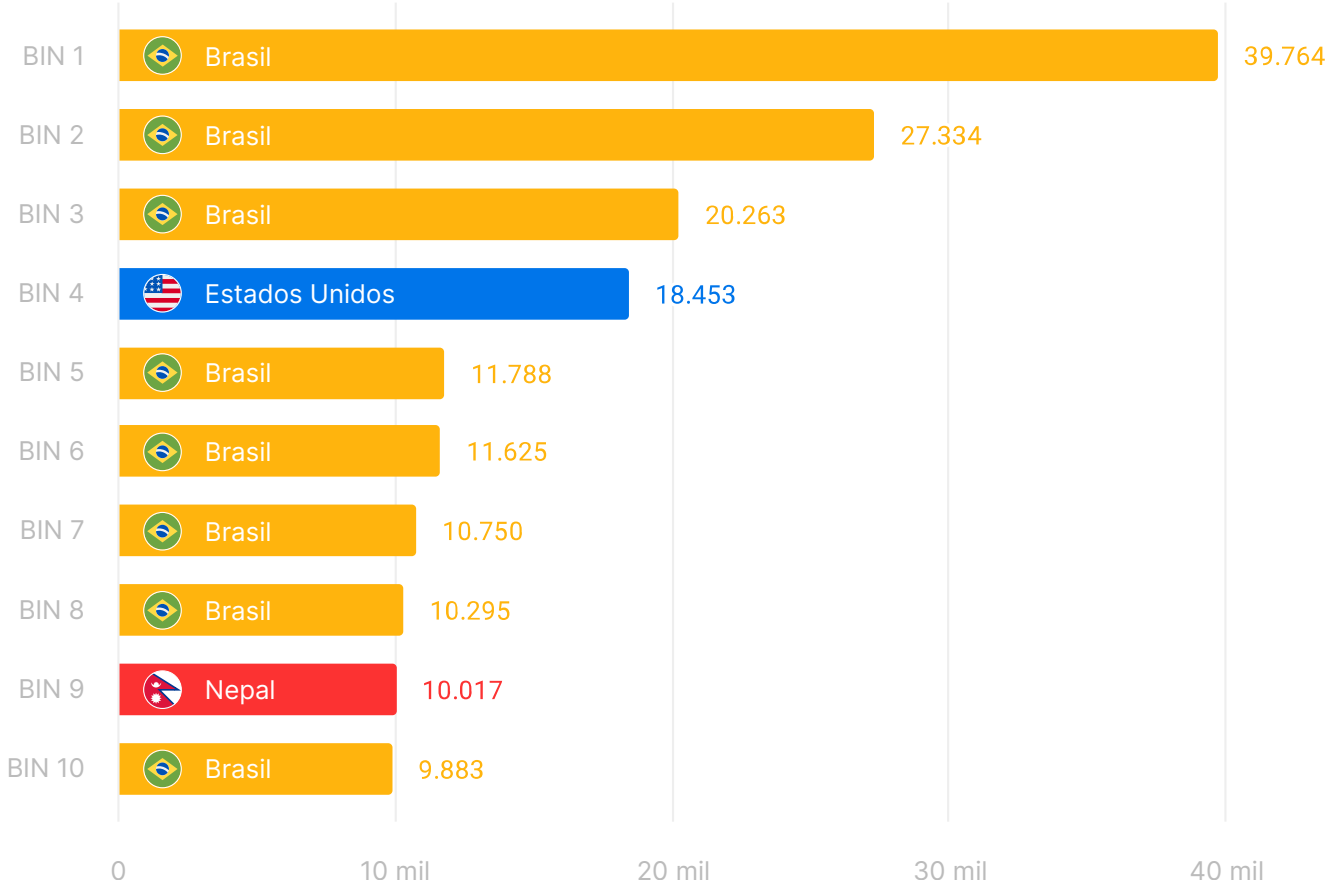


Figura 12. Ranking mundial das 10 BINs com mais vazamentos de cartões de crédito e débito registrados no terceiro trimestre de 2020, identificadas por país.

Infrações em uso de marca

O total de casos atacando marcas indevidamente em web superficial foi marcado no trimestre por maioria de **usos não autorizados para venda ou pirataria** - tipo que ocupa uma fatia de 51,8%. Ainda assim, a distribuição dos casos é bem semelhante à do trimestre anterior, como mostra a Figura 13.

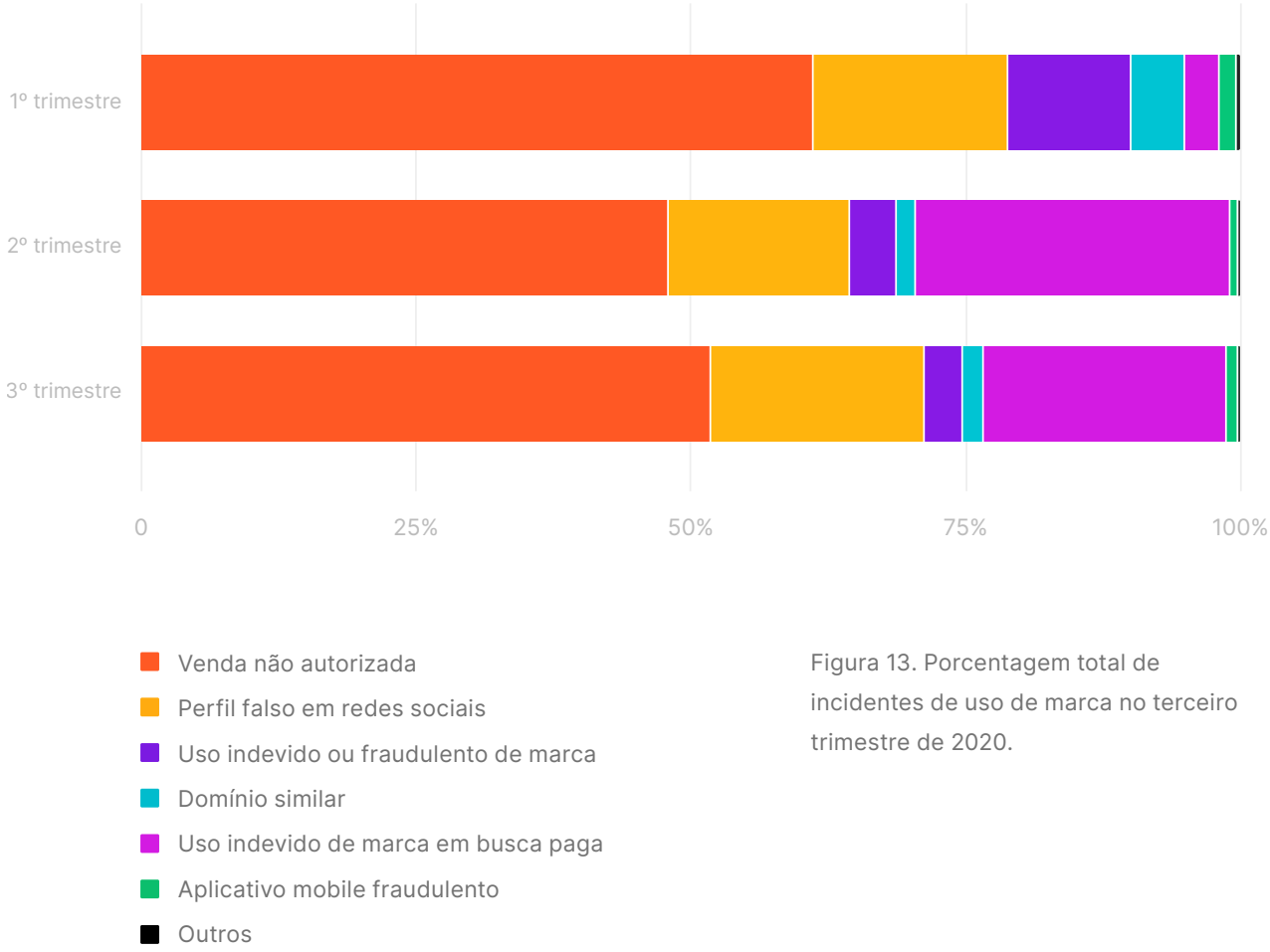


Figura 13. Porcentagem total de incidentes de uso de marca no terceiro trimestre de 2020.

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.

Glossário

- **BIN (Bank Identification Number)**
  Os seis primeiros dígitos de um cartão de crédito ou débito, que identificam a instituição financeira emissora e o tipo de cartão

- **Credencial**
  E-mail com senha ou hash (tipo de senha criptografada)

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

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

- **Hash**
  Resultado da aplicação de uma função matemática em algum conteúdo – como senhas.
  É feito para evitar o armazenamento em texto claro e direto, criptografando-o e garantindo mais segurança. Assim, quando uma senha é inserida em um site que usa esse tipo de sistema, o dado é transformado em hash e comparado com o que já está previamente armazenado.

- **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.

- **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.

- **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.

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

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

Amanda Abed
+55 51 3012 2987
press@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

Axur AxurBrasil AxurBrasil AxurBrasil Axur