RELATÓRIO

Atividade criminosa online no Brasil

1º trimestre / 2020

São Paulo, 23 de abril de 2020

Principais dados

Covid-19

tornou-se o foco de fraudes digitais já em março, antes do auxílio emergencial do governo ser oficializado, em abril

308,17%

foi o maior aumento já registrado do volume mensal de **phishing** em um ano (comparando-se fev/2019 e fev/2020)

3,46 mi

de senhas vazadas de e-mails de organizações com **domínios .br** foram identificadas

- **10.910 ataques de phishing**, páginas falsas que capturam dados de consumidores, foram detectados. Esse é o novo recorde trimestral.
- 35,9% dos casos de phishing afetam **bancos e financeiras**. Pela primeira vez, esse é o setor mais atingido.
- 62% dos casos de phishing utilizam **domínios genéricos**, sem nome de marcas.
- **43 instituições financeiras** diferentes foram atingidas por um único malware, em março. Esse número supera o recorde anterior de 38 instituições atingidas, registrado em dezembro de 2019.
- 123456 continua sendo **a senha mais comum em vazamentos de dados** no mundo, e contabilizou 383.765 detecções.
- 20,7% é o total de **cartões vazados** no mundo que são **brasileiros**. O Brasil cresceu 8 pontos percentuais e segue sendo o segundo país com mais dados desse tipo expostos online.
- 41,6% foi o **aumento de perfis falsos em redes sociais** no total de usos de marca. Eles são os principais vetores para phishing, que também cresceu no período.

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.

Conteúdo

Em uma pandemia, atenção às fraudes digitais

Quando casos como o da Cambridge Analytica começaram a aparecer e as discussões pela regulamentação da proteção de dados pessoais tomaram conta dos debates, diversas empresas deram início a seus setores de compliance e/ou começaram a entender como se adequar às novas legislações – nessa época, nascia a GDPR (General Data Protection Regulation).

No Brasil, cerca de 85% das empresas não atendem às novas normas[1] de privacidade e proteção de dados. Essas empresas vão ter mais um ano para a adaptação. Antes prevista para entrar em vigor em agosto de 2020, a nossa LGPD (Lei Geral de Proteção de Dados) foi adiada para o mesmo mês de 2021. O motivo da mudança tem nome e sobrenome: a pandemia do novo coronavírus.

Apesar das novidades, nesse cenário o que infelizmente permanece é o aumento das táticas, técnicas e procedimentos sofisticados usados pelos cibercriminosos. Só em março, último mês analisado neste relatório e também quando o estado de pandemia foi decretado, detectamos fraudes digitais que personificavam o governo e até mesmo a OMS (Organização Mundial da Saúde), capturando dados e instalando programas maliciosos com o objetivo de transformar o smartphone em um aparelho "zumbi".

Mesmo com esse cenário novo, o que continua espantando é o número de casos de phishing, que continua crescendo e atingindo níveis recorde no Brasil. Além de também se pautarem pelo coronavírus e atingirem tanto órgãos oficiais quanto pequenas e grandes empresas, os fraudadores estão investindo em novas técnicas de engenharia social, como os domínios com chamadas apelativas ("oferta", "promo", "queima estoque") – que não usam nomes de marcas e estão sendo bem mais utilizados, como você vai ver nas próximas páginas.

Com tantas preocupações e novidades, é importante lembrarmos que boa parte de nós se preocupa em tomar as melhores medidas para passar por um momento de incertezas como o atual. Por isso, esperamos que este material seja útil e colabore para que tenhamos uma internet cada vez mais segura. Boa leitura!

Fabio Ramos, CEO da Axur

[1]Segundo pesquisa da Serasa Experian

Phishing

Páginas falsas que capturam dados de consumidores

De 1º de janeiro a 31 de março de 2020 foram identificados **10.910** casos de phishing. Esse número representa um aumento de 24,23% em comparação com o trimestre anterior, quando foram detectados 8.782 casos. O registro deste trimestre também representa um aumento de **238,82%** se comparado com o mesmo período de 2019, quando foram detectados 3.220 casos.

Os volumes de detecções em cada mês do primeiro trimestre de 2020 também superam todos os níveis de 2019 - quando o pico de 3.123 casos foi registrado em dezembro, como aponta a Figura 1.

Figura 1. Evolução do número total de casos de phishing detectados no Brasil entre janeiro de 2019 e março de 2020.

O aumento das fraudes é ainda mais expressivo quando observados os níveis mensais: com o pico de 3.845 páginas registrado em fevereiro deste ano, a comparação com o volume de fevereiro do ano passado (942 casos) mostra que **o nível mensal de phishing triplicou no período de um ano, registrando crescimento de 308,17%**.

Os casos mensais de phishing no Brasil, separados por segmento de indústria afetado, estão dispostos na Figura 2. Para fins de comparação, os dados do trimestre anterior também estão apresentados no gráfico.

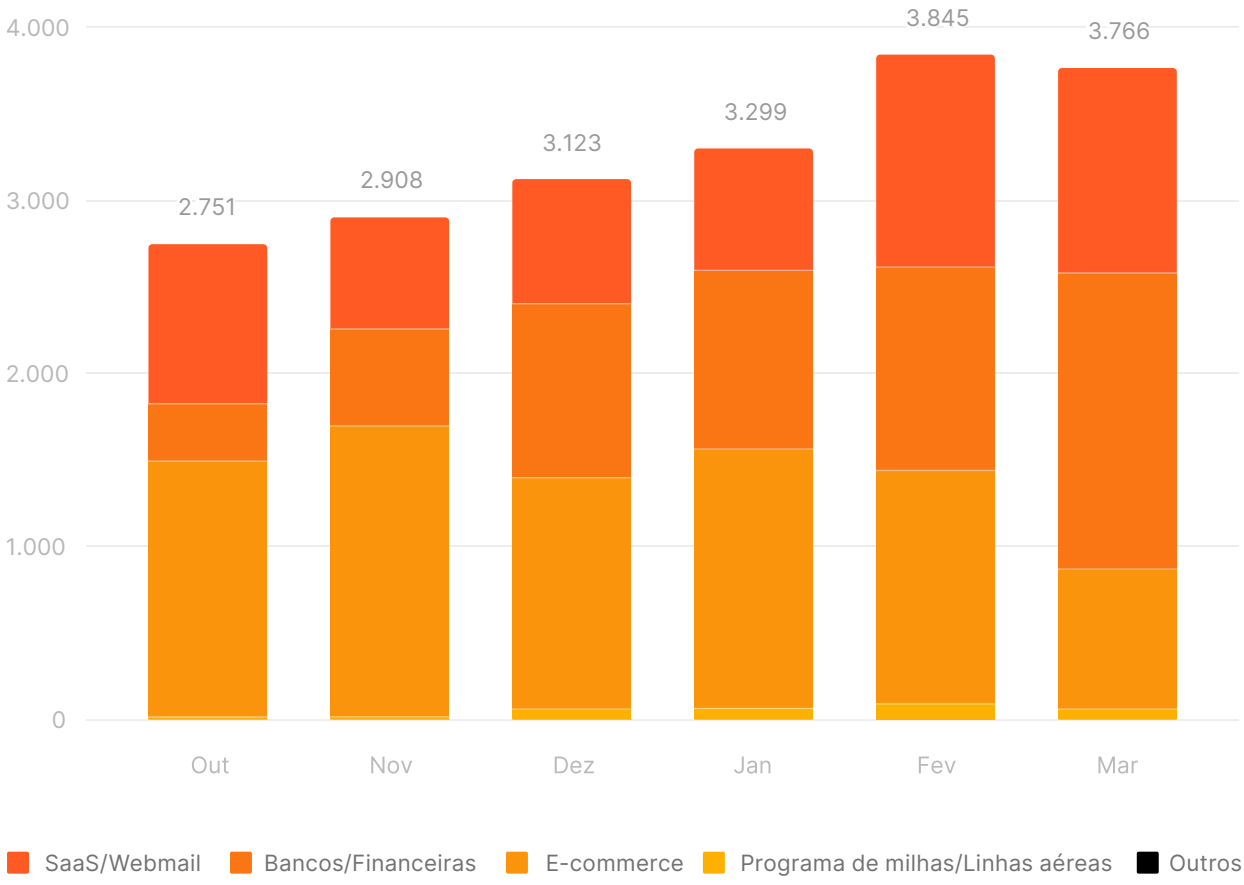

Figura 2. Quantidade mensal de casos únicos de phishing detectados entre outubro de 2019 e março de 2020 no Brasil, por setor atingido.

Brasil: o país do phishing

O phishing no Brasil tem mostrado comportamento diferente do visto mundialmente. Os dados do último relatório feito pela APWG (Anti-Phishing Working Group) mostraram redução significativa nos últimos meses de 2019 no nível mundial de phishing – enquanto no Brasil novos picos de detecção continuam acontecendo ao longo dos últimos meses.

Pela primeira vez no Brasil, **bancos e financeiras são o setor mais afetado, somando 35,9% do total no trimestre** e ultrapassando os níveis de e-commerce. Esse valor agora se assemelha à disposição mundial: no relatório da APWG, os setores de pagamentos e bancos correspondem a 39,2% dos casos de phishing. A disposição total da porcentagem de phishing por setor no primeiro trimestre de 2020 no Brasil está apresentada na Figura 3.

A segunda principal peculiaridade do phishing no Brasil são os ataques ao setor de e-commerce, também visíveis na Figura 3. Não tão comuns a nível global e representando apenas 5,4% das detecções mundiais, no Brasil as fraudes personificando marcas de e-commerce contabilizaram **33,5%** do total.

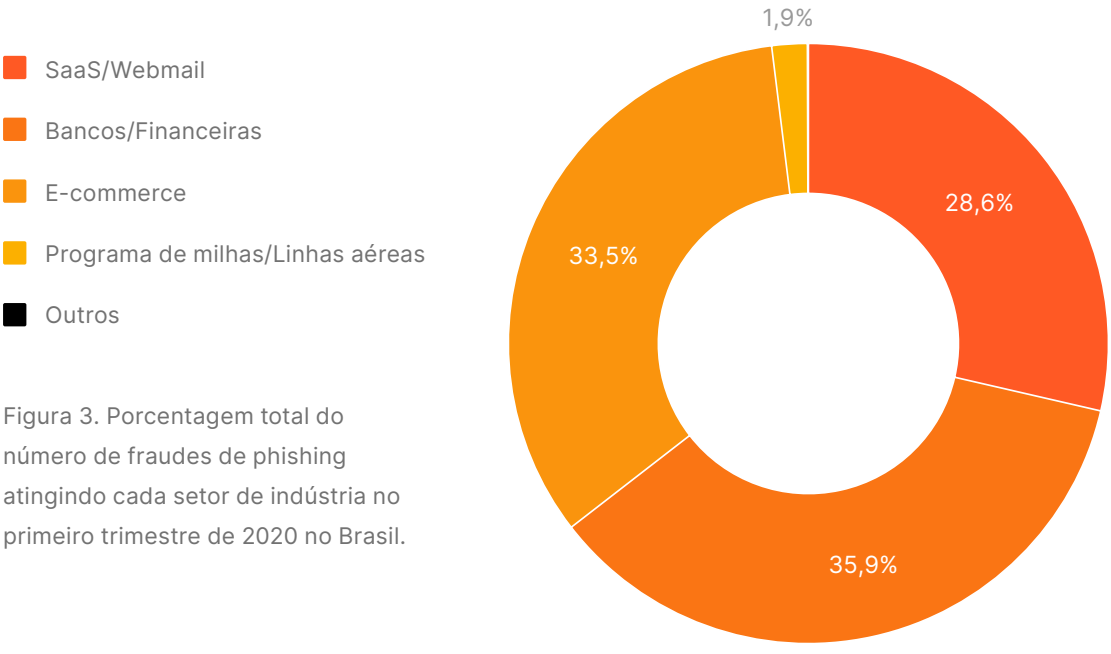

Figura 3. Porcentagem total do número de fraudes de phishing atingindo cada setor de indústria no primeiro trimestre de 2020 no Brasil.

Domínios genéricos em ascensão

Na Figura 4, estão dispostas as porcentagens de uso de domínios genéricos ou domínios similares a marcas na atividade de phishing em três períodos distintos: no ano inteiro de 2019; no último trimestre de 2019 e no primeiro trimestre de 2020.

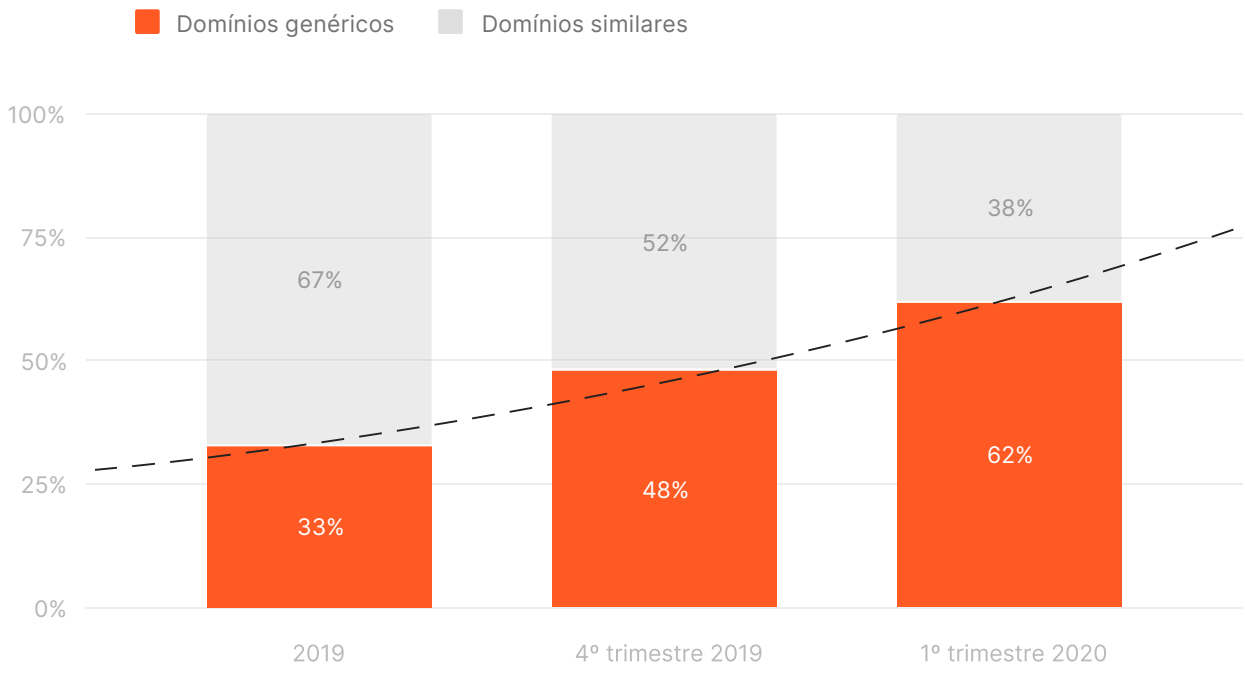

Figura 4. Porcentagem de casos de phishing utilizando domínios similares ou domínios genéricos no ano inteiro e no quarto trimestre de 2019 e no primeiro trimestre de 2020.

O gráfico mostra importante variação no total de casos de phishing que utilizaram domínios genéricos, que foram de 33% do total em 2019 para **62%** no primeiro trimestre de 2020. Esses domínios diminuem a probabilidade de uma fraude ser encontrada, visto que não mencionam as marcas atingidas e usam chamadas apelativas como “promo”, “oferta” e outras.

O novo coronavírus e as fraudes digitais

No dia 11 de março, a Organização Mundial da Saúde decretou estado de pandemia do novo coronavírus (Covid-19), que então levou, alguns dias depois, a um estado de isolamento social também no Brasil.

As detecções de fraudes digitais envolvendo a pandemia e o momento de preocupação generalizada só aumentaram desde então. A Figura 5 mostra um caso de phishing com a venda de álcool em gel, produto que esgotou em muitas farmácias e supermercados.

Assim como o uso de domínios genéricos, esse tipo de caso também reflete uma estratégia dos cibercriminosos: a utilização de um produto que seja o foco do momento ou que esteja com preço muito abaixo do comum, aumentando a eficácia e o volume da captura de dados.

Figura 5. Ataque de phishing de e-commerce falsificando a venda de álcool em gel.

Em março, também foram detectados domínios genéricos com “corona” ou “covid” e que continham fraudes. Muitos dos sites hospedados sob estes domínios são informativos ou sequer possuem conteúdo, porém, exemplos com termos genéricos como o da Figura 6 já estão sendo detectados com ataques de phishing.

É importante notar que, por serem muito recentes, essas fraudes ainda tendem a aumentar e demonstrar novos comportamentos no decorrer do segundo trimestre do ano. Ainda assim, mesmo em março outros golpes surgiram com foco em fisgar vítimas a partir das primeiras suposições sobre o auxílio emergencial do governo federal brasileiro (que só foi disponibilizado oficialmente em abril).

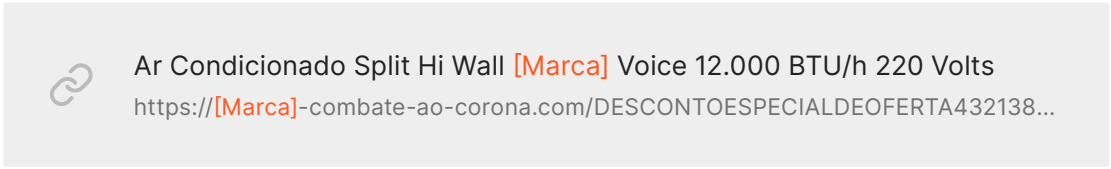

Figura 6. Exemplo de domínio com uso de marca (ocultado) e termo genérico utilizando a palavra “corona” que hospedou um ataque de phishing, detectado em março de 2020.

Na Figura 7, um exemplo de site falso veiculado via WhatsApp que criava uma rede de compartilhamentos de um mecanismo para a veiculação massiva de propagandas em dispositivos móveis. Alegando ser o cadastro oficial para saque imediato de contas do FGTS (Fundo de Garantia do Tempo de Serviço), essa fraude também utilizava um domínio genérico: **auxiliocorona.online**.

Quarentena sem fraudes

Considerando a possibilidade de disseminação extensiva de golpes personificando entidades governamentais e até a OMS (Organização Mundial da Saúde), ainda em março a Axur lançou a iniciativa voluntária #QuarentenaSemFraudes.

No site, toda denúncia de páginas desse tipo é então analisada e, se confirmada a fraude, o conteúdo é removido e/ou a página é retirada do ar a partir de esforços de notificação. O exemplo da Figura 7 é uma das fraudes já removidas.

Figura 7. Fraude registrada no domínio auxiliocorona.online e que solicitava compartilhamentos via WhatsApp, visando à veiculação massiva de propagandas em dispositivos móveis.

Malware

Softwares maliciosos que capturam dados de consumidores

A atividade de malware no Brasil continua com muitas variações, mas pela primeira vez registra importante declínio no volume de artefatos detectados em quatro meses consecutivos, de dezembro de 2019 a março de 2020. Para observar este novo comportamento em comparação com meses anteriores, a Figura 8 apresenta o volume de detecções mensais a partir de janeiro de 2019.

O primeiro trimestre de 2020 registrou **78** artefatos de malware diferentes, que correspondem a somente **11,6%** do total registrado em 2019 (670 artefatos). Esse número também representa uma diminuição de 51,25% se comparado ao registro feito no mesmo período de 2019 (janeiro a março), quando foram detectados 160 arquivos de malware.

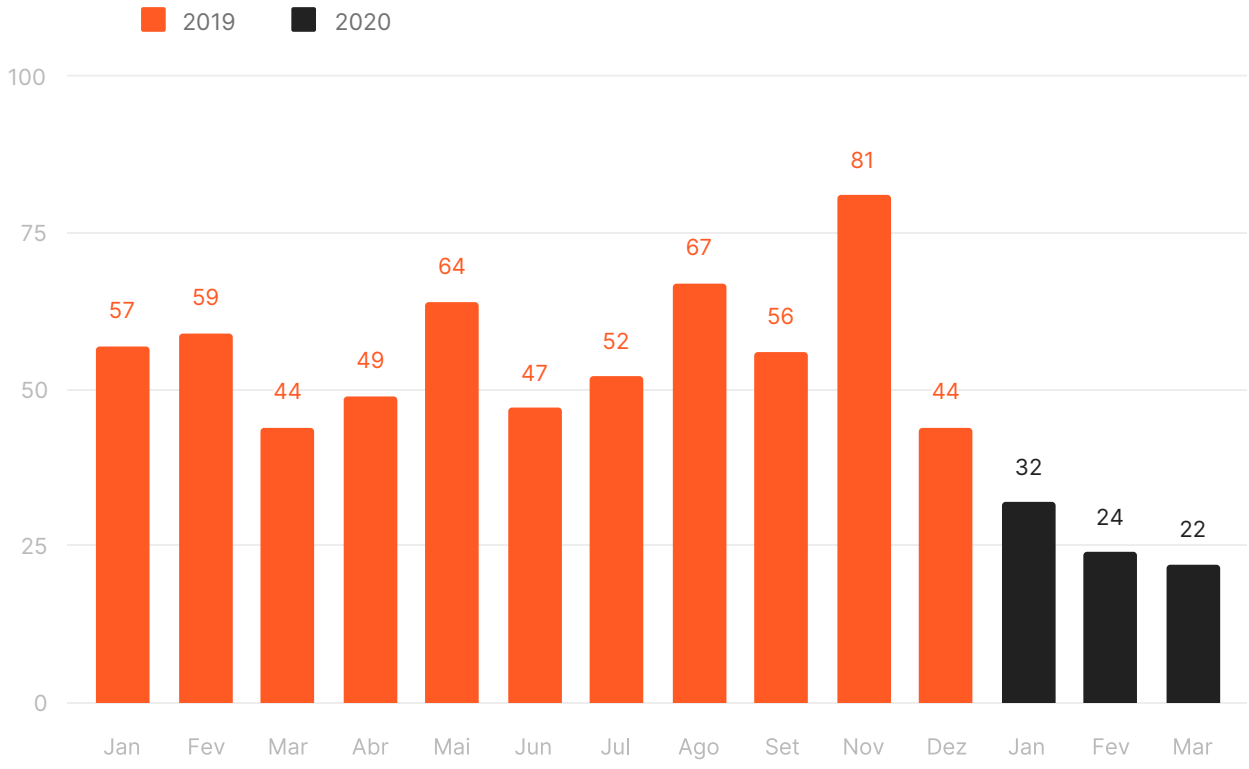

Figura 8. Quantidade mensal de casos únicos de malware detectados entre janeiro de 2019 e março de 2020 no Brasil.

Apesar do menor volume, os arquivos de malware encontrados em 2020 possuem novidades importantes: estão mirando muito mais instituições financeiras e seus clientes do que qualquer registro feito em 2019, quando foram em média 15 empresas atingidas. O número máximo de alvos foi 38, em um arquivo de dezembro.

No mês de março, 43 marcas de diferentes empresas foram encontradas em um único malware enviado para consumidores. Esse é o maior número já registrado. No mesmo mês, a média de 29 alvos nos 22 arquivos detectados também é recorde de todos os dados de detecções.

A Figura 9 mostra a variação da média e do número máximo de alvos dos arquivos de malware encontrados mensalmente entre o último trimestre de 2019 e o primeiro trimestre de 2020.

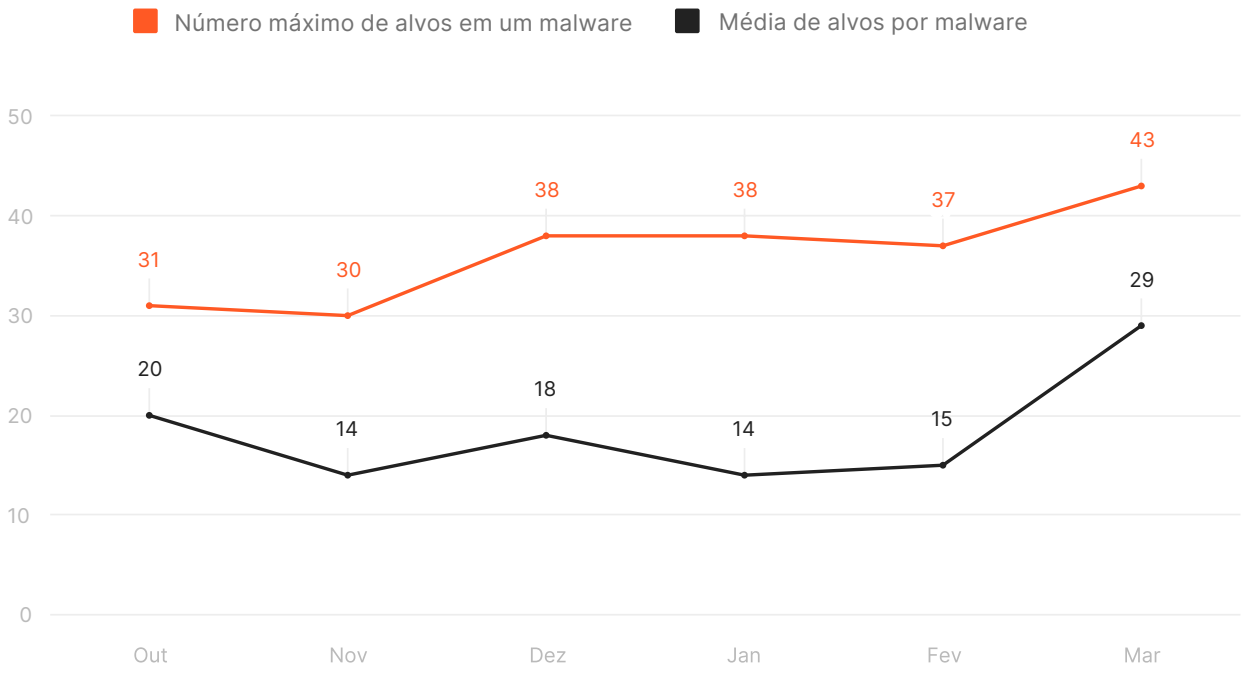

Figura 9. Média e número máximo de instituições financeiras afetadas em um malware por mês, entre outubro de 2019 e março de 2020.

Análise dos arquivos de malware

A Figura 10 apresenta a classificação dos artefatos de malware detectados no primeiro trimestre de 2020 conforme seu ISP (Internet Service Provider) de hospedagem e o tipo de arquivo encontrado. Assim como no quarto trimestre de 2019, **Amazon** e **Google** continuam sendo os locais de hospedagem com maior volume.

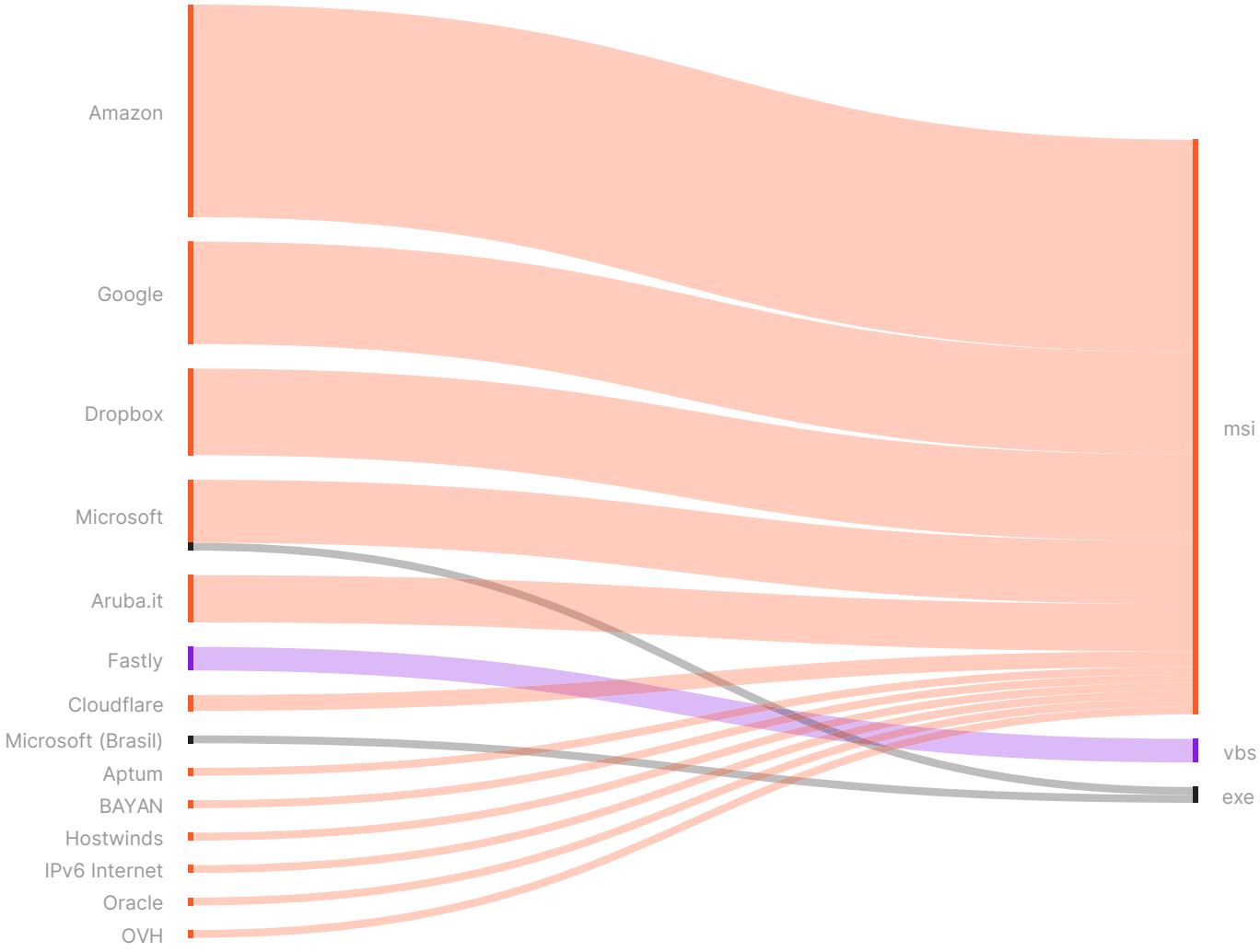

Figura 10. Classificação por ISP de hospedagem e por formato dos arquivos de malware do primeiro trimestre de 2020 detectados no Brasil.

O primeiro trimestre de 2020 apresenta mudanças importantes, entretanto: Dropbox e Microsoft tiveram maior volume, aproximando-se do nível visto em servidores do Google.

Mudanças importantes no comportamento dos arquivos também são **a predominância e o aumento dos arquivos .msi**, que são instaladores para o sistema operacional Windows.

Um arquivo .msi é caracterizado por fazer o download de outros arquivos adicionais, que são executados e dão continuidade na infecção/ataque. Esse comportamento é comum e tem como objetivo **burlar mecanismos de defesa**, como filtros de spam e antivírus – nesse caso, o .msi não é um malware, mas sim um downloader que é a fonte de um malware.

A maior tendência de migração para os arquivos .msi é também perceptível na quantidade de tipos de formatos detectados: se no último trimestre de 2019 foram cinco (.msi, .vbs, .exe, .js e .jse), no primeiro trimestre de 2020 foram apenas três.

Vazamento de credenciais

Exposição de e-mails com senha ou hash

Entre 1º de janeiro de 31 de março de 2020, foram detectadas e inseridas **86,67 milhões** de credenciais únicas na base de dados da Axur. Esse número é **11,6 vezes maior** que a detecção feita no último trimestre de 2019, quando foram registradas 7,44 milhões de credenciais vazadas.

Assim como o terceiro trimestre de 2019 registrou um nível ainda maior que o atual, 167,17 milhões de credenciais, é importante observar que variações entre períodos são também devidas à detecção de bases que, sozinhas, somam milhões de credenciais em um único vazamento.

Do total de vazamentos detectados no primeiro trimestre de 2020, foram identificados:

- **12,66 milhões** de credenciais de domínios corporativos
- **2,74 milhões** de domínios corporativos distintos[2]
- **3,46 milhões** de credenciais de **domínios .br**[3]
- **48.729** credenciais de **domínios .gov.br**
- **9,06 milhões** de senhas formadas somente por números

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

[2]As credenciais de domínios corporativos que foram detectadas não necessariamente dão acesso a sistemas internos de empresas, pois podem apenas ter sido vazadas a partir de cadastros feitos em outros locais e que utilizaram e-mails corporativos.
[3]A separação das senhas de domínios .br é apenas uma amostra para análise do cenário brasileiro, já que muitos usuários e empresas do Brasil utilizam domínios terminados em .com ou outros.

Das senhas detectadas no primeiro trimestre, predominam novamente aquelas formadas somente por números, como aponta o ranking de detecções da Figura 11. A senha 123456, sozinha, foi detectada 383.765 vezes em e-mails distintos e segue sendo a senha mais vazada em todo o mundo.

Mais uma vez, além de os números serem predominantes (ocupando 6 das 10 primeiras posições com mais vazamentos), eles são principalmente utilizados na forma de sequências simples, como também apresenta a Figura 11.

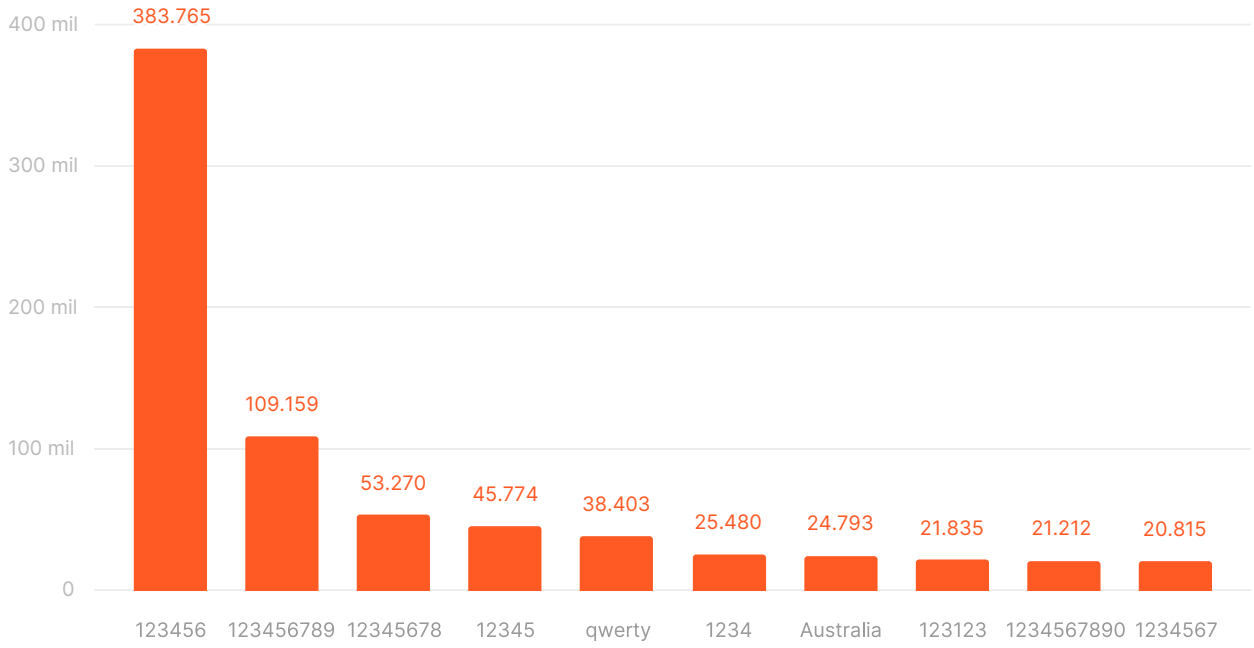

Figura 11. Ranking global de exposições de senhas detectadas pela Axur no primeiro trimestre de 2020.

Vazamento de cartões de crédito e débito

Exposição de dados completos de cartões

No primeiro trimestre de 2020, **1,009 milhão** de cartões de crédito e débito expostos em web superficial, deep e dark web foram inseridos na base de dados da Axur. Esse número representa um **aumento de 10,45% nos vazamentos**, se comparado com os 914.137 cartões encontrados no quarto trimestre de 2019.

Para analisar as BINs com mais vazamentos de dados no período, foram selecionadas aquelas que tiveram 100 ou mais cartões expostos. Elas totalizam 778.680 cartões distribuídos em 904 BINs e 85,2% do total detectado no trimestre.

Desse total, 239 BINs são de instituições brasileiras (26,43%), que somam **160.977 cartões (20,7%) expostos no período**. Assim como no último trimestre e nos dados totais do ano de 2019, **o Brasil continua sendo o segundo país com mais vazamentos de cartões de crédito e débito registrados**.

BINs (Bank Identification Numbers)
Os seis primeiros dígitos de um cartão de crédito ou débito, que identificam a instituição financeira emissora e o tipo de cartão.

O ranking dos países com mais vazamentos está apresentado na Figura 12. Cabe observar que o campeão Estados Unidos teve diminuição na porcentagem de seus cartões expostos mundialmente entre o último trimestre de 2019 e o primeiro de 2020, passando de 69,2% para 42,4%.

O Brasil apresenta aumento deste percentual, entretanto: no quarto trimestre também ocupava a segunda posição, mas com 12,7% do total de cartões expostos. Se comparado com os atuais 20,7% registrados, o Brasil teve um **aumento de 63% ou 8 pontos percentuais** em sua presença na extensão do vazamento de cartões de crédito e débito a nível mundial.

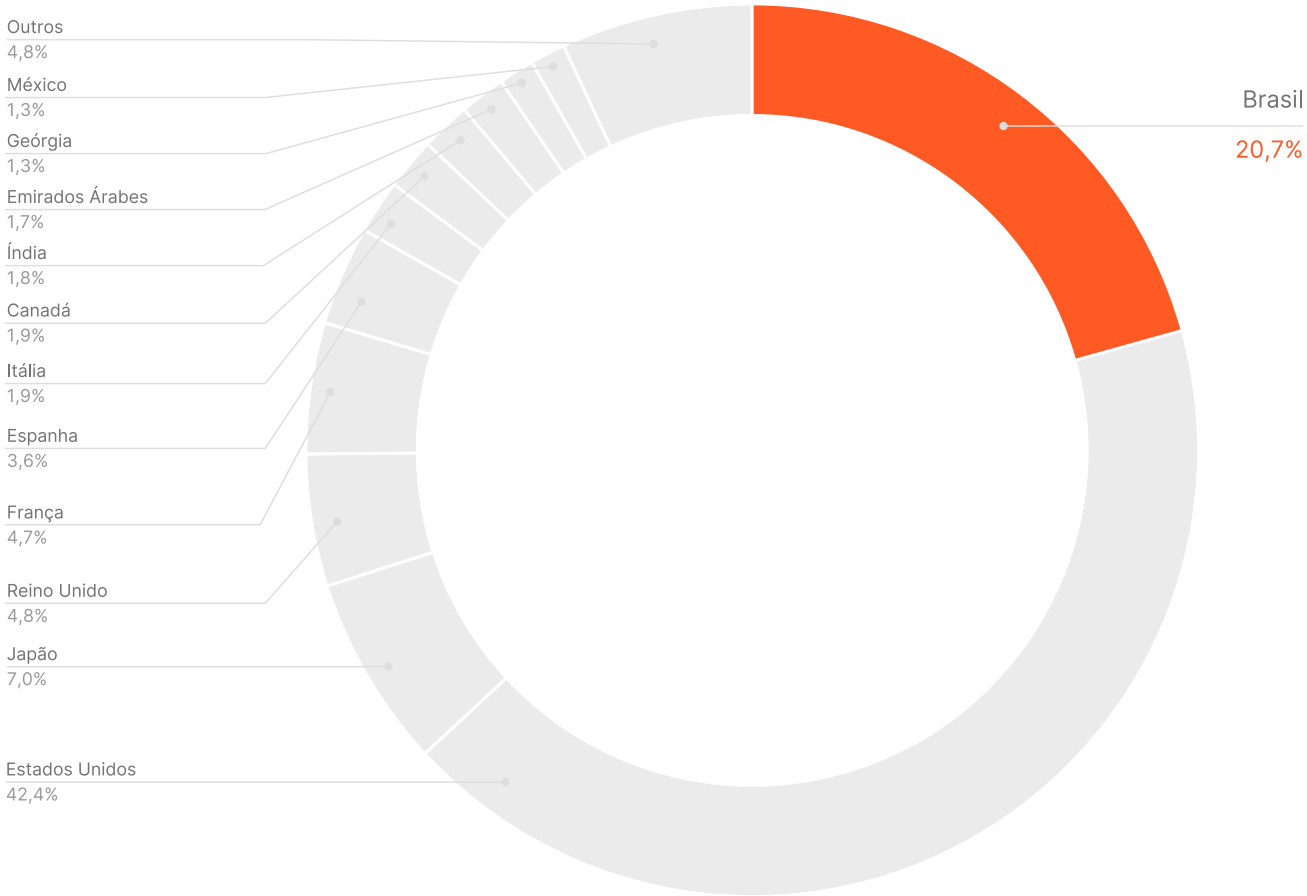

Figura 12. Porcentagem total dos países com mais cartões de crédito e débito vazados online e detectados pela Axur no primeiro trimestre de 2020.

O ranking da Figura 13 aponta que **o Brasil está bem próximo aos líderes globais em BINs com mais vazamentos registrados**, com uma uma BIN que teve **18.973** detecções de cartões distintos no primeiro trimestre de 2020.

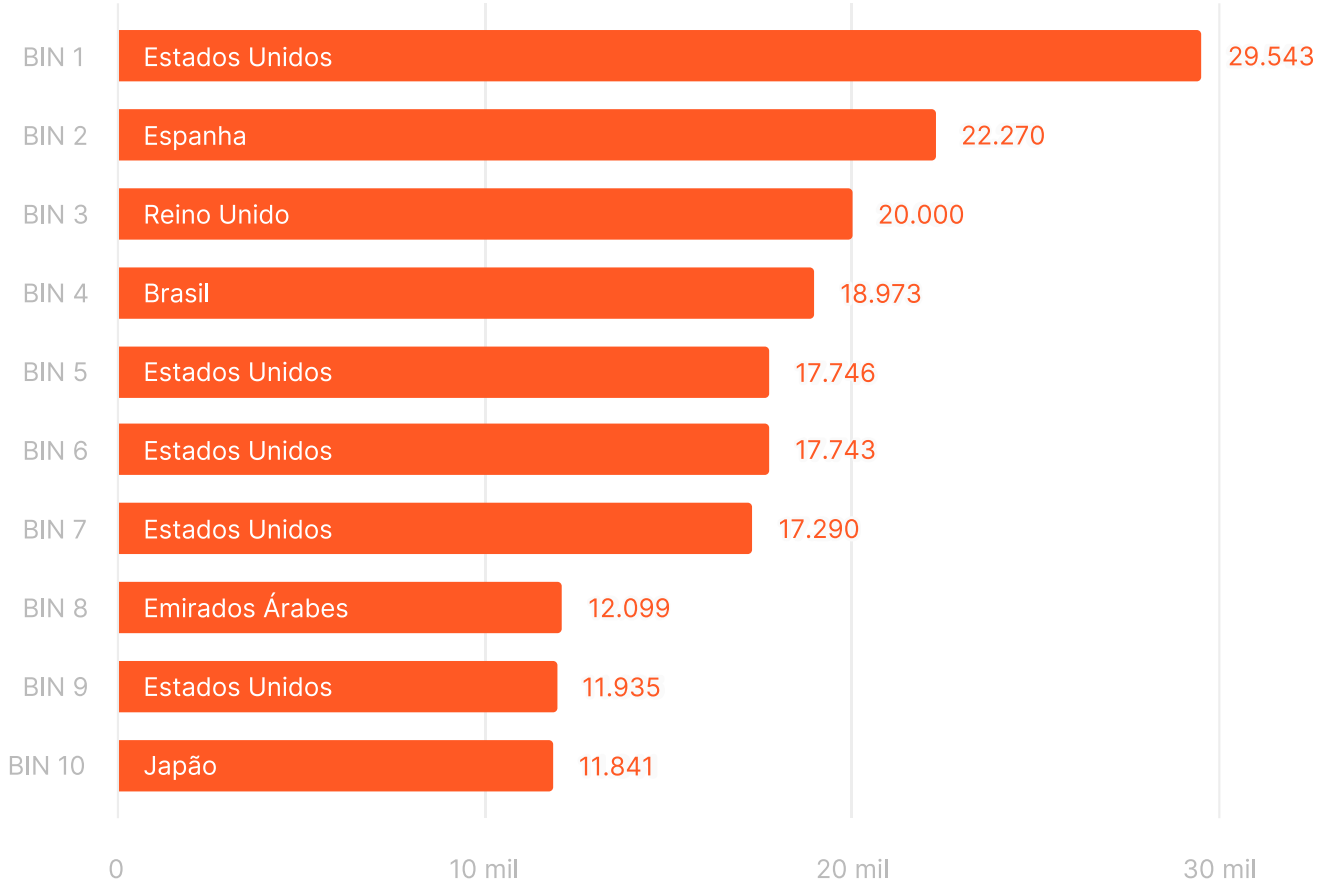

Figura 13. Ranking mundial do total de cartões de crédito e débito expostos online das 10 BINs com mais vazamentos registrados no primeiro trimestre de 2020, identificadas por país.

Infrações em uso de marca

Personificação e violação de propriedade intelectual

Como aponta a Figura 14, o uso de marca mais numeroso continua sendo aquele do tipo Venda não autorizada, com **61,1%** dos incidentes registrados no primeiro trimestre de 2020. Comportamento semelhante foi observado no último trimestre de 2019, quando este tipo somou 62,6% das detecções.

A predominância de vendas não autorizadas e pirataria teve início nos últimos meses do último ano, conforme observado no relatório do quarto trimestre de 2019. As detecções feitas entre outubro e novembro somaram, sozinhas, 50,9% do total de 2019 desse tipo de infração.

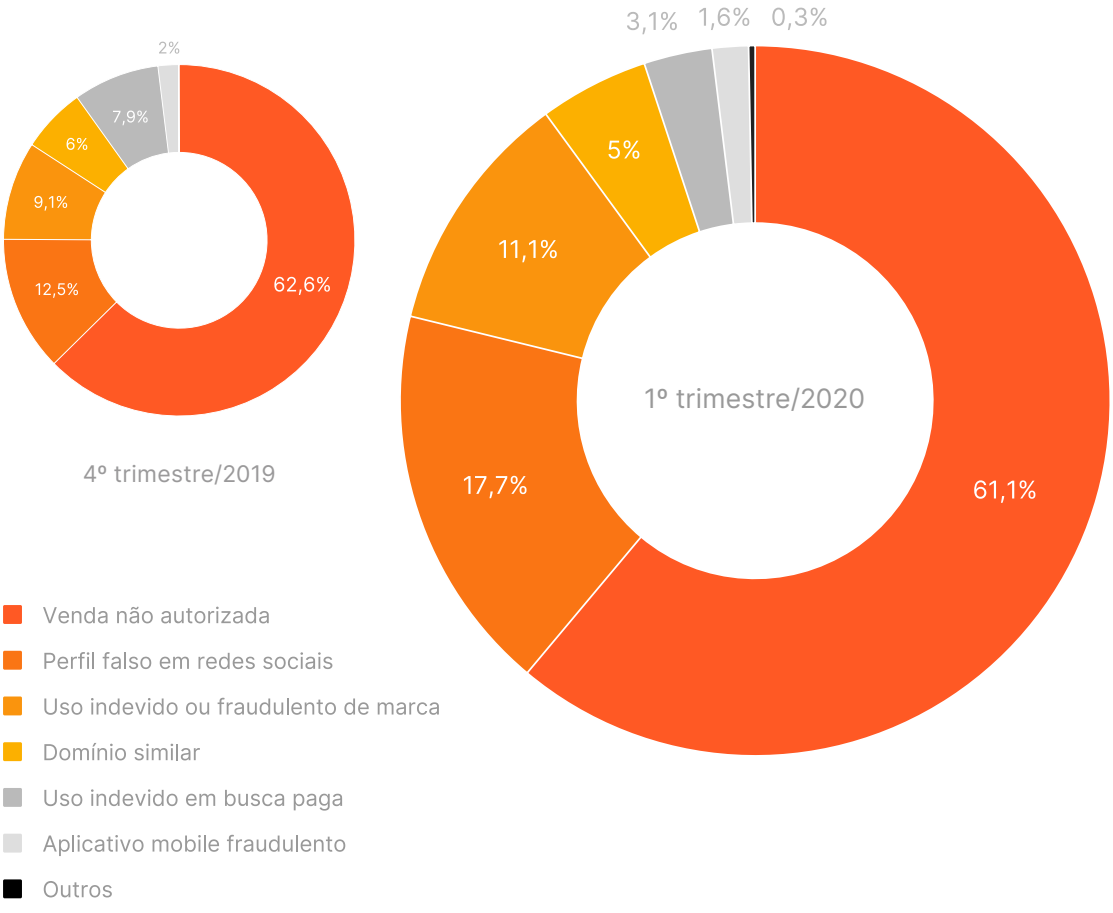

Figura 14. Porcentagem total de incidentes de uso de marca no primeiro trimestre de 2020.

Perfis falsos em redes sociais aumentam, domínios similares diminuem

Também predominantes nos últimos meses de 2019 (período da Black Friday e das festas de final de ano), os perfis falsos em redes sociais continuam com alto índice de detecção no primeiro trimestre de 2019: agora, somaram **17,7%** do total de usos de marca e ultrapassando os 12,5% registrados entre outubro e dezembro do ano passado. Da mesma forma, domínios que foram registrados com uso de marca tiveram diminuição neste trimestre em comparação com o anterior, **variando de 4 para 5%** do total das detecções.

Considerando o aumento da atividade de phishing (p. 5) e também o aumento dos casos de fraudes que utilizam domínios com chamadas e nomes genéricos (p. 8), é possível observar que a atividade criminosa tende a se disseminar de forma mais estratégica, evitando detecções de nomes da marca e aumentando o volume de perfis falsos em rede sociais.

Como observado em relatórios anteriores, perfis falsos em redes sociais são fortes vetores para phishing e também contêm chamadas apelativas, como as utilizadas em domínios genéricos. Um exemplo de perfil falso de e-commerce que veiculou phishing com chamadas genéricas (para o carnaval e para o início do ano) está apresentado na Figura 15.

Figura 15. Perfil falso no Facebook que veiculou phishing com chamadas genéricas para o carnaval e para a época de início de ano.

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, objetivando a identificação de padrões que são ensinados e testados – possibilitando os mais elevados níveis de acertos.

Essas técnicas permitem à Axur entregar resultados com precisão, fazendo com que seja possível visualizar ameaças em potencial e incidentes de forma prática e clara. Todas as detecções acontecem no Axur One, plataforma onde é também possível realizar as ações de tratamento.

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

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

Denise Claudino
+55 51 3012 2987
press@axur.com

Endereços

US
535 Mission St.
San Francisco, CA 94105

Singapore
109 North Bridge Road
Cityhall District, 179097

São Paulo
Alameda Santos, 2326
9º andar, conjunto 95

Axur OneAxur AxurOne