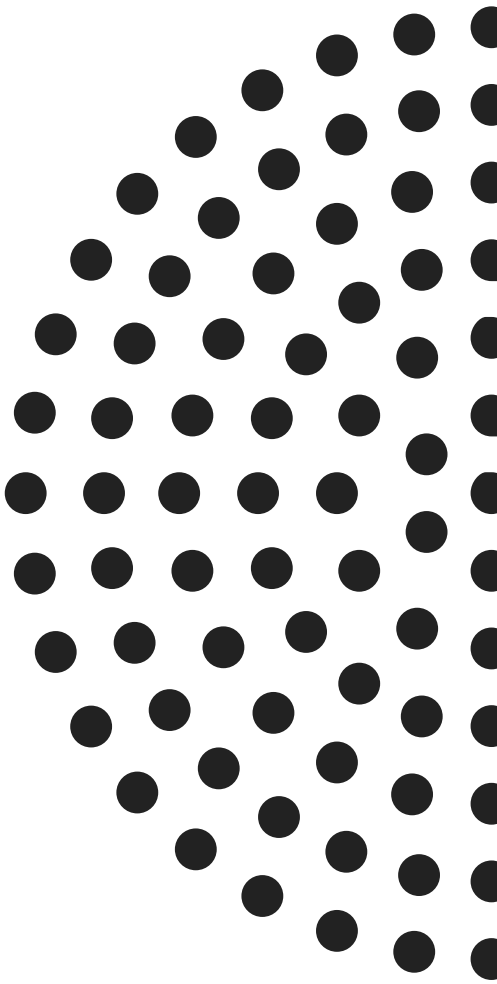
RELATÓRIO

Atividade criminosa on-line no Brasil

4º trimestre / 2019

+ year-in-review



São Paulo, 31 de janeiro de 2020

Principais dados

Os destaques do relatório *Atividade criminosa on-line no Brasil* do último trimestre de 2019 + year-in-review são:

+231,5%
foi o crescimento dos ataques de phishing entre fevereiro e dezembro

26,7%
dos cartões de crédito e débito vazados on-line são brasileiros

37,6 mi
de vazamentos da senha *123456* foram detectados em 2019

- Ataques de phishing, páginas falsas que capturam dados de consumidores, atingiram o recorde trimestral de **8.762 casos**
- O volume mensal de phishing cresceu **231,5%** entre fevereiro (menor registro) e dezembro (pico anual)
- **38** instituições financeiras diferentes foram afetadas por um mesmo malware, software para captura de dados sensíveis. Esse é o maior número já identificado
- **Pirataria**, vendas não autorizadas e **perfis falsos** em redes sociais tiveram os maiores crescimentos em usos de marca on-line
- Com **26,7%** de todos os vazamentos de cartões de crédito e débito detectados, o Brasil é o segundo país com mais dados desse tipo expostos on-line
- **23,6 milhões** de senhas vazadas de organizações com domínios .br foram identificadas em 2019
- 123456 continua sendo a senha mais comum em vazamentos de dados no mundo, e contabilizou **37,65 milhões** de detecções em 2019

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

Carta do CEO

O ano das fraudes digitais

O ano de 2019 foi único para observarmos como o crime digital evolui na mesma medida (ou mais rápido) que o acesso à internet: em dezembro, atingimos o pico de detecção de phishing, as páginas falsas que capturam dados de consumidores.

Também comprovamos em números que perfis falsos em redes sociais e nomes de domínios similares estão conectados ao furto de dados em páginas falsas de phishing, por exemplo.

Com tantos dados sendo capturados (e expostos), veio nossa primeira grande meta em 2019: tornar pública a verificação de senhas vazadas a partir de nossa base, que tem hoje mais de 9 bilhões de credenciais já expostas em web superficial, deep e dark web. O resultado está no **MinhaSenha.com**.

Em meio a esse cenário, também a partir de agosto de 2020 a LGPD (Lei Geral de Proteção de Dados, nº 13.709/2018) está prevista para entrar em vigor no Brasil, e o cuidado com dados de consumidores deve ser redobrado. Mas, para além de multas milionárias, a preocupação em entender os perigos digitais deve ser uma responsabilidade básica de qualquer empresa.

Uma segunda meta surgiu então em nossos debates: tornar públicas as análises do cenário brasileiro on-line. Agora, você vê na quarta edição de nosso relatório os dados do último trimestre de 2019 e também do ano inteiro – que, juntos, mostram a evolução das ameaças digitais e seus picos nos últimos meses do ano.

Esperamos que este material seja de grande valia.
Boa leitura!

Fabio Ramos
CEO da Axur

Phishing

Páginas falsas que capturam dados de consumidores

De 1º de outubro a 31 de dezembro de 2019 foram identificados **8.782** casos de phishing. Esse número corresponde a **35,25%** do total de 2019 (24.161 casos) e é o recorde de detecções do ano, superando sozinho os 8.517 casos vistos em todo o primeiro semestre.

Os volumes de detecções em cada mês superam também todos os outros volumes mensais dos outros três trimestres de 2019:

2.751	2.908	3.123
Outubro	Novembro	Dezembro

Se comparado com o registro de 942 casos em fevereiro (o menor do ano), o número de dezembro mostra que **o nível mensal de phishing no Brasil cresceu expressivos 231,5% em apenas dez meses**.

Os casos mensais de phishing no Brasil separados segmento de indústria afetado estão dispostos na Figura 1. Apesar das diferentes variações entre os segmentos, o crescimento dos ataques durante 2019 na linha de tendência do gráfico é também visto nos recentes **dados mundiais** da APWG (Anti-Phishing Working Group).

O maior destaque em crescimento dos números no último trimestre do ano é no setor de bancos e financeiras, que atingiu seu volume máximo em dezembro e registrou **1.007** ataques únicos – equivalendo a um crescimento de 205,15% em três meses. Um comportamento semelhante a esse só foi observado antes entre março e maio, quando houve um crescimento de 265,7%.

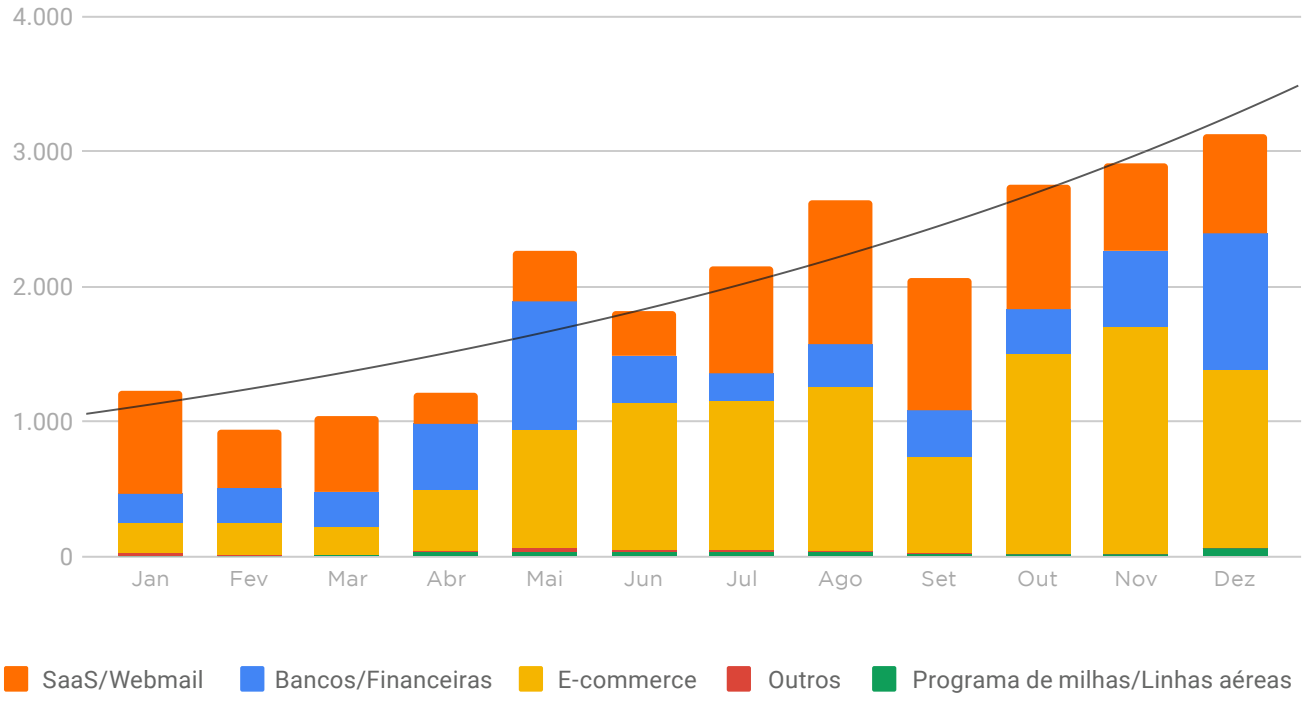


Figura 1. Quantidade mensal de casos únicos de phishing detectados entre janeiro e dezembro de 2019 no Brasil, por setor atingido.

Programas de milhas e linhas aéreas também tiveram destaque em dezembro: foram 58 casos detectados, ultrapassando os 39 registrados em agosto.

Historicamente, os criminosos aumentam a frequência e a amplitude dos ataques no período de festas e recessos de final de ano, voltando-se ao setor aéreo para a captura de dados. Da mesma forma, os pagamentos de décimo terceiro salário no Brasil são indicativos do aumento da movimentação bancária e financeira que podem atrair ataques a consumidores.

Phishing no e-commerce: o fenômeno Black Friday

O grande destaque em 2019 é o pico de detecção de páginas falsas de e-commerce em novembro: foram **1.685** casos únicos no Brasil. Esse é o maior número do ano, e deve-se principalmente a golpes envolvendo a Black Friday.

Na Figura 2 estão dispostos os incidentes de phishing dos clientes de e-commerce e varejo da Axur em 2019, separados em períodos semanais. Essa separação mostra o **pico absoluto de detecções na semana da Black Friday**, entre 24 (domingo) e 30 de novembro (sábado).

O segundo maior pico semanal, em maio, deve-se ao do Dia dos Namorados (como apontado em relatório anterior). Entretanto, novembro segue como o mês campeão: registrou 3 dos 4 maiores picos semanais do ano – e o quarto trimestre possui **31,94%** mais ocorrências que o segundo.

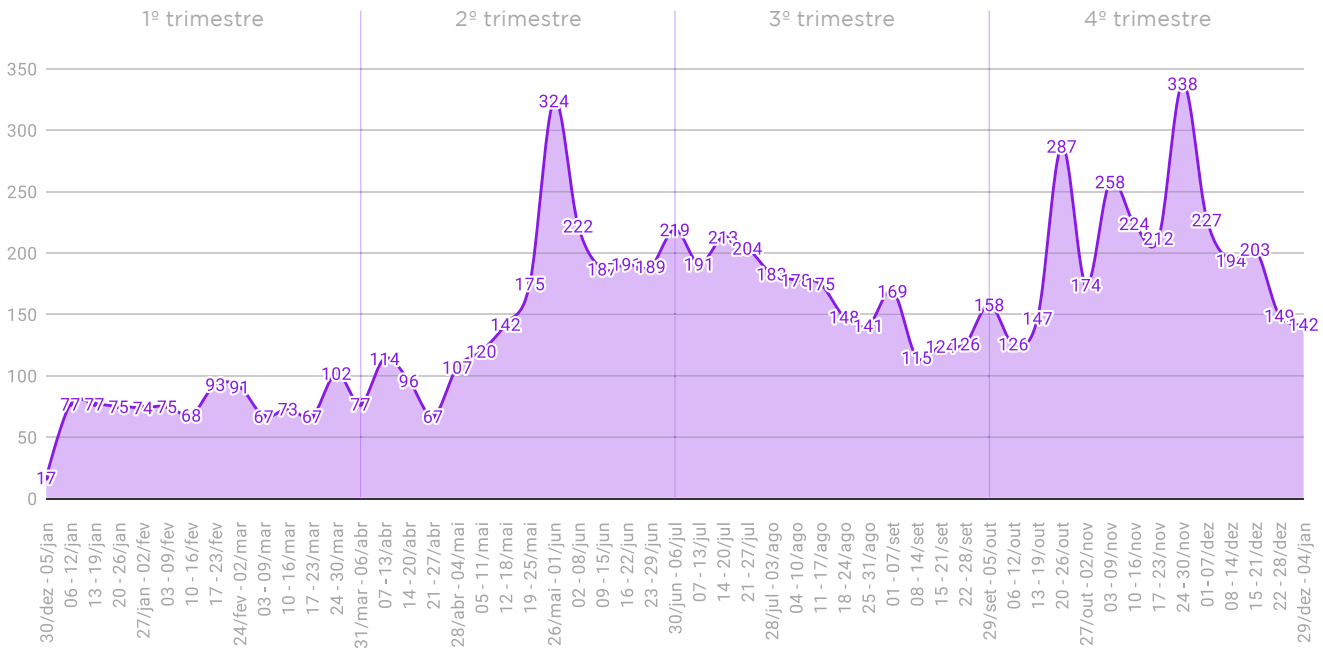


Figura 2. Quantidade semanal de incidentes de phishing afetando os clientes de e-commerce da Axur entre janeiro e dezembro de 2019.

Domínios usados para phishing

A hospedagem dos golpes de phishing acontece, em geral, a partir da criação de um novo nome de domínio para hospedagem do conteúdo malicioso. Existem duas principais formas de classificação de um domínio usado para phishing:

- **Domínios genéricos**

  Possuem, em geral, nomes com ganchos para datas comemorativas ou com frases e chamadas apelativas. Não fazem menção a marcas, como no exemplo detectado na Figura 3.

- **Domínios similares**

  Feitos com uso de marca em seu nome. Para criar ilusões de semelhança, são utilizadas técnicas como o *cybersquatting* – que é a troca, remoção ou adição de algum caractere com propósito de enganar. Na seção sobre infrações em uso de marca (página 13) estão descritos os setores mais atingidos por domínios similares.

A porcentagem total de cada um dos tipos de domínios verificados nas detecções de phishing do 4º trimestre está no gráfico da Figura 4. Na Figura 5 estão os resultados de 2019 - que mostraram ser maiores em domínios similares do que no período específico pesquisado.

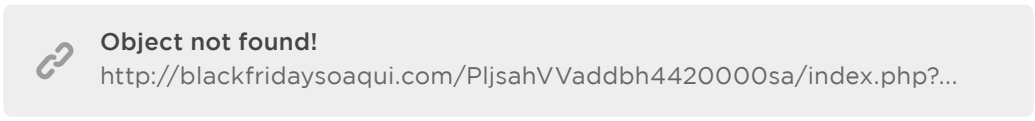


Figura 3. Exemplo de domínio genérico com chamada para a Black Friday e que hospedou um ataque de phishing.

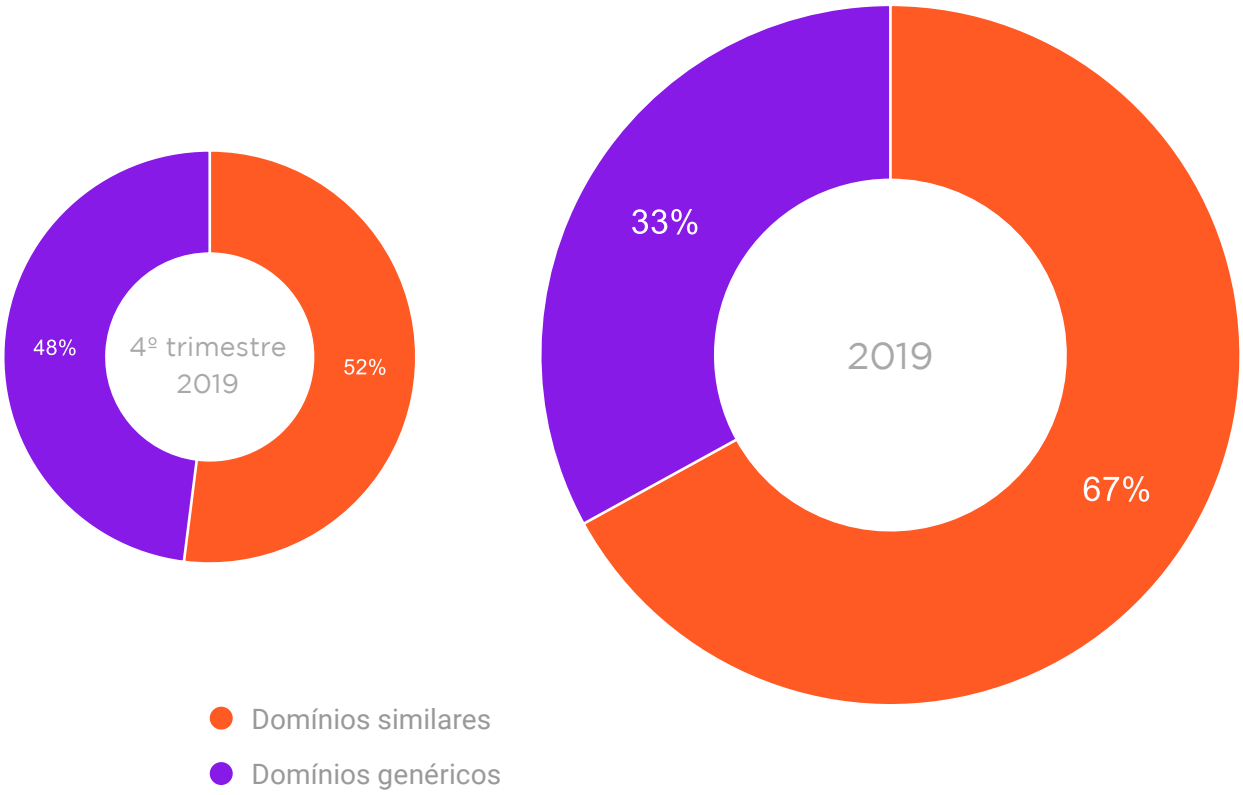


Figura 4. À esquerda, porcentagem de domínios similares e domínios genéricos utilizados para phishing no quarto trimestre de 2019 no Brasil.

Figura 5. À direita, porcentagem de domínios similares e domínios genéricos utilizados para phishing de janeiro a dezembro de 2019 no Brasil.

O número maior de casos de phishing com uso de domínio similar a marcas no período total do ano indica a utilização de técnicas para personificar uma marca – visando aumentar os níveis de persuasão e sucesso dos golpes.

Malware

Softwares maliciosos que capturam dados de consumidores

Os números mensais dos ataques de malware mostraram mudanças no volume de detecções ao longo de 2019 que não são bruscas, a não ser pela maior taxa de detecção em novembro – quando foram encontrados 81 artefatos diferentes (Fig. 6).

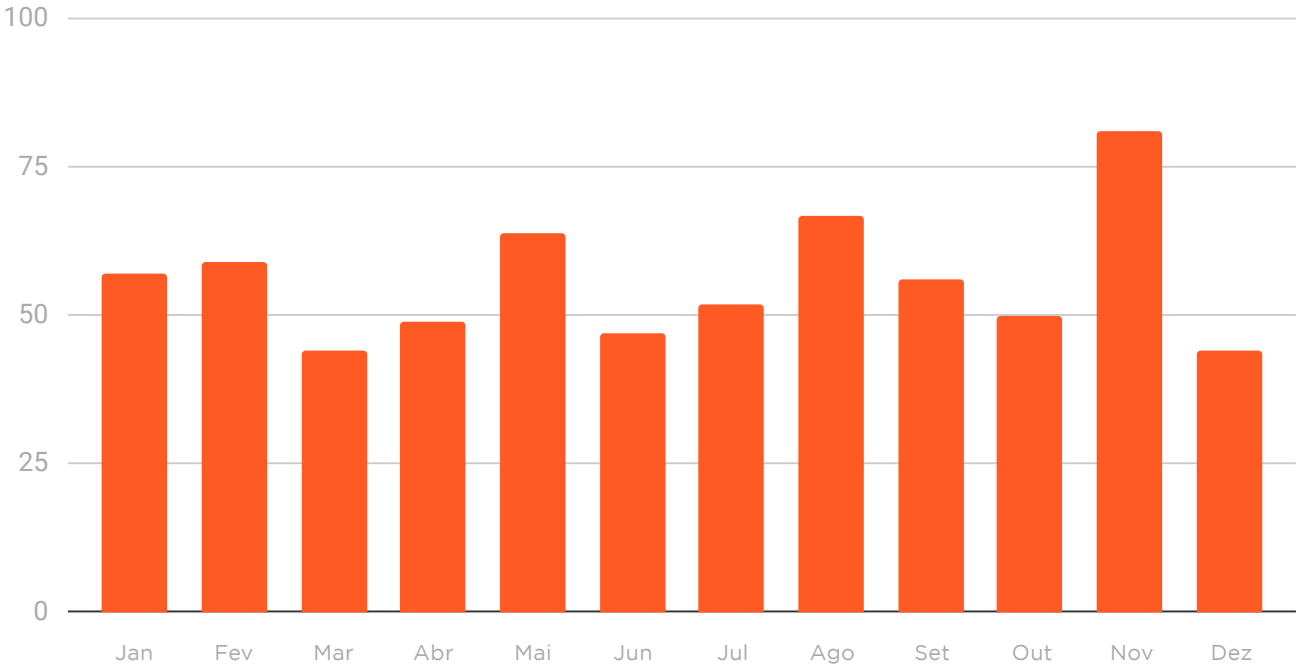


Figura 6. Quantidade mensal de casos únicos de malware detectados entre janeiro e dezembro de 2019 no Brasil.

No quarto trimestre, **175** arquivos diferentes de malware foram detectados. Esse número corresponde a 26,11% do total anual: em 2019, **670** artefatos foram encontrados.

O maior destaque das detecções é na quantidade de instituições financeiras atingidas por artefato. A média desse número cresceu de forma leve durante 2019, mas o número máximo de alvos teve crescimento expressivo no quarto trimestre: foram **38** instituições financeiras brasileiras afetadas em um mesmo malware (Fig. 7).

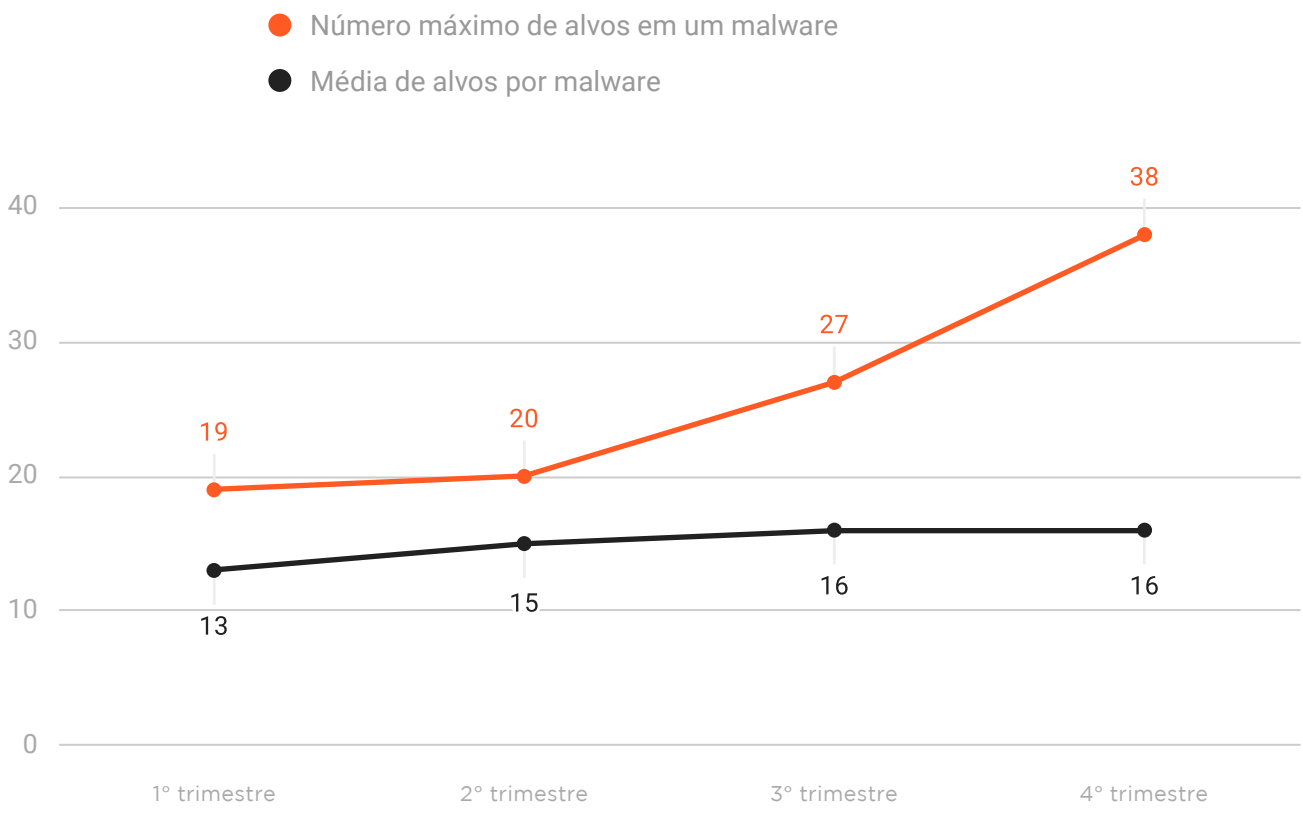


Figura 7. Média e número máximo de instituições financeiras afetadas em um malware em 2019

Análise dos arquivos de malware

O ISP (Internet Service Provider) de hospedagem e o tipo de arquivo de malware das detecções do quarto trimestre de 2019 estão descritos na Figura 8. Essas duas classificações mostram a predominância dos arquivos do tipo .msi, que são instaladores para o sistema Microsoft Windows.

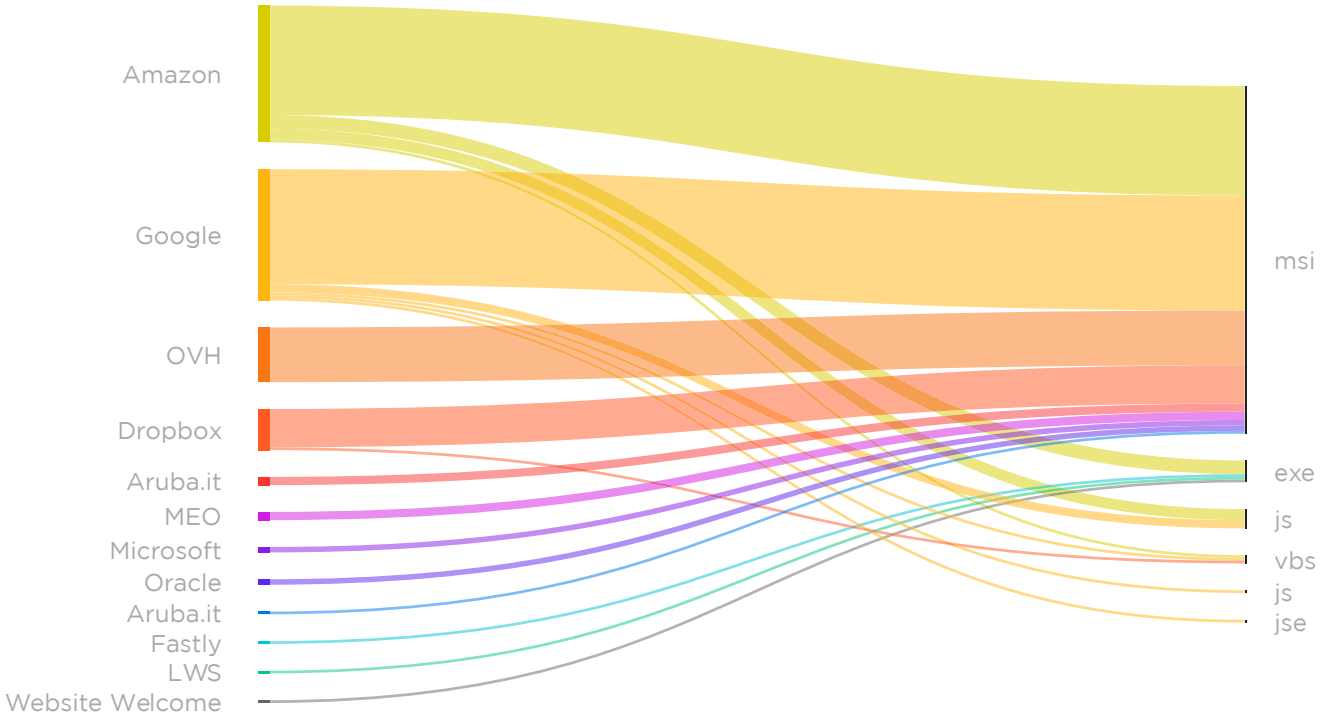
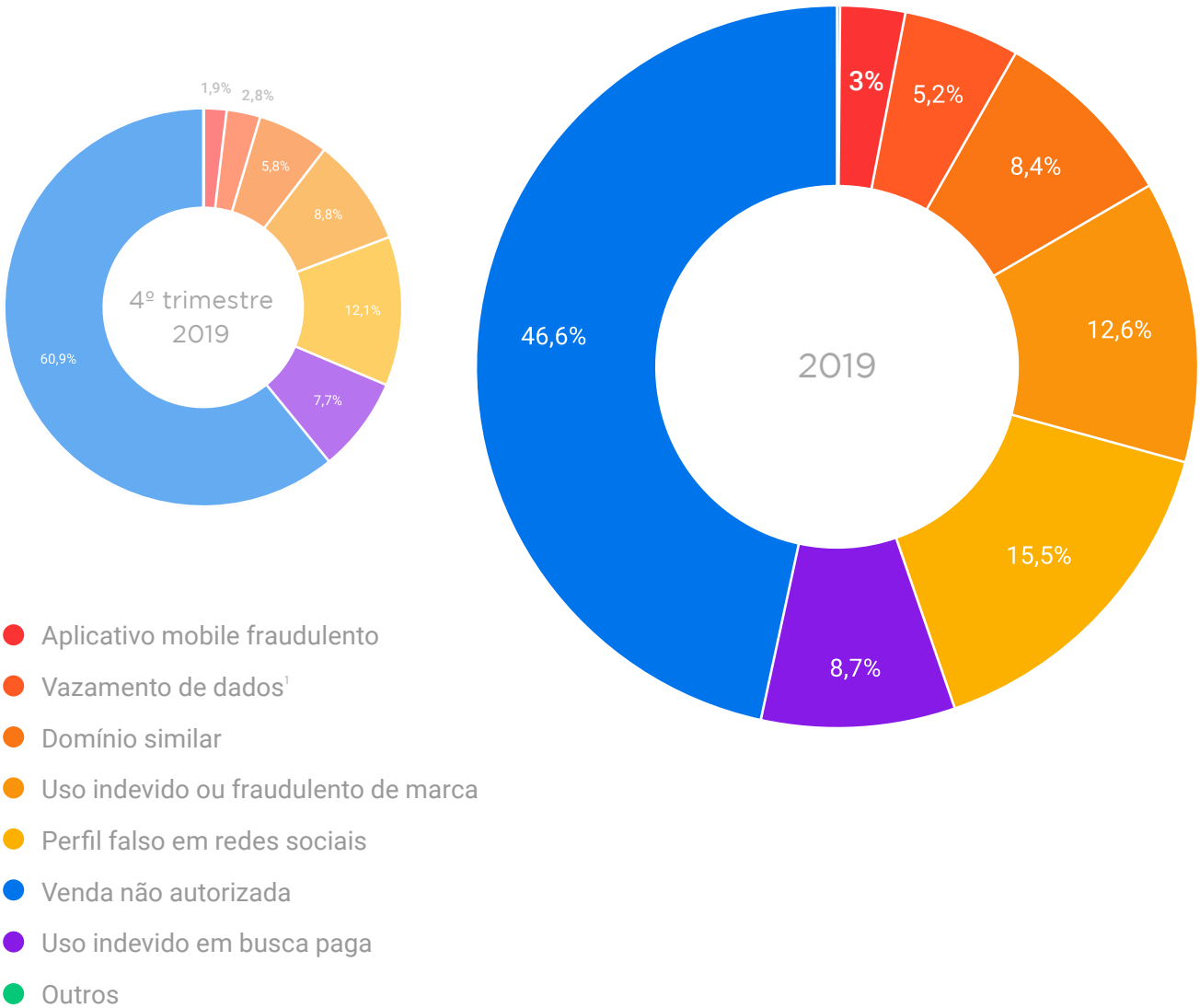


Figura 8. Classificação por ISP de hospedagem e por formato dos arquivos de malware do quarto trimestre de 2019 detectados no Brasil.

Nota-se também que os arquivos .exe não aparecem hospedados no ISP Google LLC. Os outros formatos indicados (js, vbs, js e jse) são arquivos de texto que levam à instalação do arquivo malicioso a partir de um "comando". Eles tendem a ser mais raros e dispersos entre vários ISPs, e por isso registraram menor número de detecções.

Infrações em uso de marca

Personificação e violação de propriedade intelectual em web superficial



[1] Em web superficial.

Figura 9. Porcentagem total de incidentes de uso de marca no quarto trimestre e no ano inteiro de 2019.

Dos 7 principais tipos de usos de marca em web superficial, o quarto trimestre de 2019 teve número expressivo de detecção de incidentes do tipo Venda não autorizada (Fig. 9). Isso indica um crescimento acentuado na distribuição on-line de produtos falsos (pirataria) e/ou que são vendidos sem autorização do detentor da marca.

De forma a observar outros comportamentos de um mesmo uso de marca on-line no ano, a Figura 10 apresenta os percentuais de detecção de cada um dos 7 principais tipos de incidentes em cada trimestre de 2019.

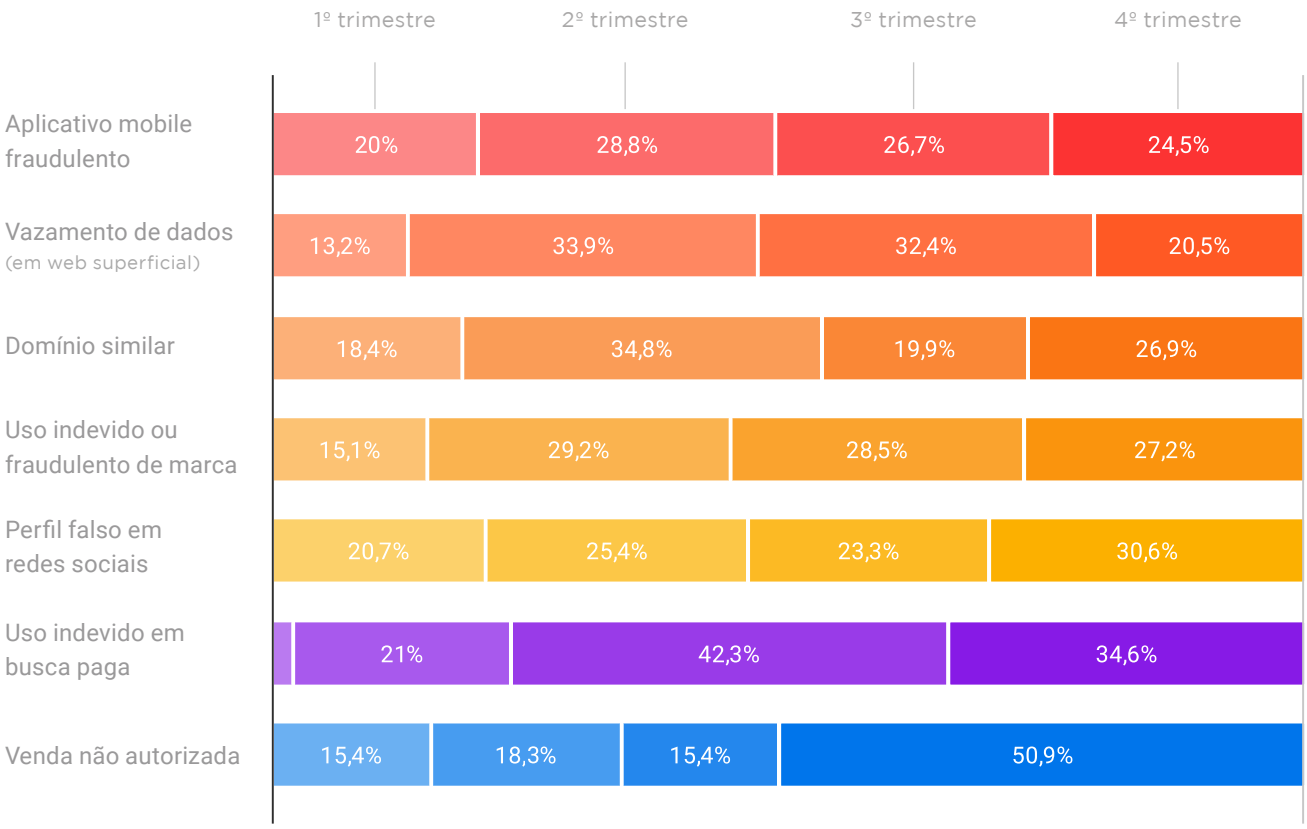


Figura 10. Porcentagem trimestral de cada infração em uso de marca em 2019 no Brasil. Os valores iniciam à esquerda, com o primeiro trimestre.

Perfil falso em redes sociais

A Figura 10 também mostra as maiores taxas do ano acontecendo neste período para perfil falso em redes sociais.

Como mostram as detecções recentes, esse tipo de risco digital com uso de marca tende a veicular fraudes e golpes para furto ou captura de dados de consumidores. Assim como o phishing (página 7), seu crescimento no quarto trimestre pode estar ligado a datas como a Black Friday e as festas de final de ano.

A Figura 11 aponta um exemplo de perfil falso personificando um e-commerce e veiculando uma página de phishing no Facebook. Em geral, esse tipo de fraude também acontece em anúncios impulsionados. As menções a marcas foram ocultadas para preservar a imagem das empresas.

Figura 11. Exemplo de perfil falso de marca em rede social com chamada para dezembro e divulgação de phishing.

Domínios similares

Usos de marca em nomes de domínio similares são problemas comuns e que podem levar à hospedagem de golpes e fraudes como sites de phishing (como apontado na página 8) ou ataques de spear phishing (feitos via e-mail).

A Figura 10 mostra que o segundo trimestre de 2019 teve a maior taxa de hospedagem de domínios similares, contabilizando mais de um terço do ano ao registrar 34,8% do total. Esse problema diminuiu no terceiro trimestre, que registrou 19,9% do total anual, mas voltou a um nível maior no quarto trimestre, registrando 26,9%.

Os incidentes de domínios similares de 2019 estão separados por setor no gráfico da Figura 12. Assim como no phishing, os dois principais setores atingidos por esse uso de marca são o financeiro e o de varejo/e-commerce.

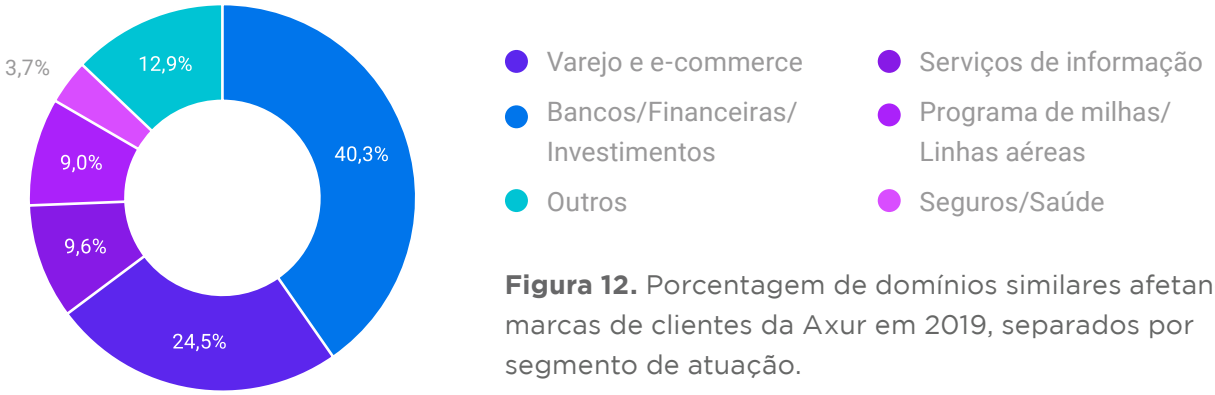


Figura 12. Porcentagem de domínios similares afetando marcas de clientes da Axur em 2019, separados por segmento de atuação.

Vazamento de dados

O volume de exposição de dados em web superficial contendo uso de marca e/ou violação de propriedade intelectual diminuiu no quarto trimestre de 2019. Como apontado no relatório anterior, no terceiro trimestre foram destaque as exposições de dados desse tipo em repositórios de códigos-fonte, como GitHub, GitLab e Bitbucket.

Nas seções seguintes, que elencam dados sobre vazamentos de credenciais e cartões de crédito e débito, veja detalhes sobre detecções também em deep e dark web, além da web superficial.

Vazamento de credenciais

Exposição de e-mails com senha ou hash em web superficial, deep e dark web

Entre 1º de outubro e 31 de dezembro de 2019, foram detectadas e inseridas **7,44 milhões** de credenciais únicas na base da dados da Axur. Esse número é expressivamente menor se comparado às **167,17 milhões** de credenciais detectadas no terceiro trimestre. A diferença entre os períodos se deve à inserção de bases grandes que somaram mais de 160 milhões de dados em setembro.

Do total de vazamentos detectados no quarto trimestre, foram identificadas:

198.281
credenciais de domínios **.br**

641
credenciais de domínios **.gov.br**

Das senhas detectadas no quarto trimestre, predominam novamente as sequências de números. O ranking da Figura 13 aponta que o primeiro lugar global é ocupado pela senha *123456*. Essa sequência é também a campeã das credenciais expostas de domínios .br, como apontado no ranking da Figura 14 – em que também predominam as sequências de números.

556.130 senhas identificadas no quarto trimestre são compostas somente por números, e **37.068** dessas senhas são de credenciais de domínios .br.

Credencial:
E-mail com senha ou hash, tipo de senha criptografada.

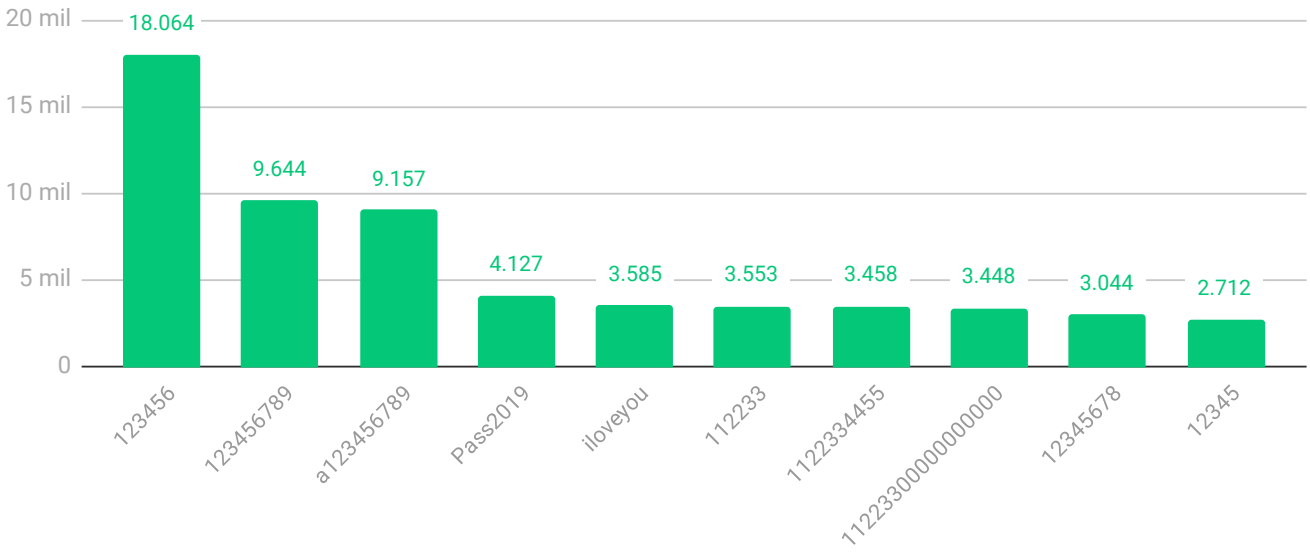


Figura 13. Ranking global de exposições de senhas detectadas pela Axur no quarto trimestre de 2019.

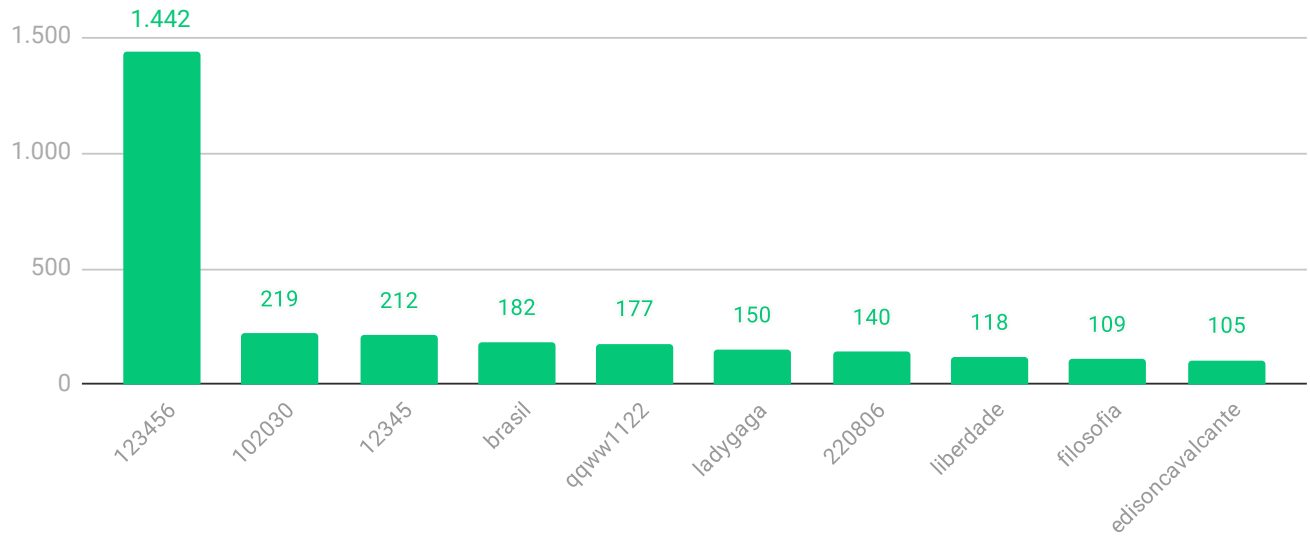


Figura 14. Ranking de exposições de senhas de domínios .br detectadas pela Axur no quarto trimestre de 2019.

2019: 5,7 bilhões de detecções

No período entre janeiro e dezembro de 2019, **5,703 bilhões** de credenciais únicas foram detectadas e inseridas na base de dados da Axur. Esse número vem das novas tecnologias implementadas para detecção e da reformulação do site **MinhaSenha.com**, plataforma gratuita de verificação de credenciais vazadas.

Do total de vazamentos detectados em 2019, foram identificadas:

23,6 milhões
de credenciais
de domínios **.br**

224.532
credenciais de
domínios **.gov.br**

As Figuras 15 e 16 mostram os rankings de senhas armazenadas em texto simples detectadas em 2019 a nível global e de domínios .br, respectivamente. *123456* é a senha com maior recorrência nos dois casos, com 37,65 milhões de aparições no ano.

Em 2019, foram identificadas **803,54 milhões** de senhas compostas somente por números, e **4,57 milhões** dessas senhas são de credenciais de domínios .br.

Nota: 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.

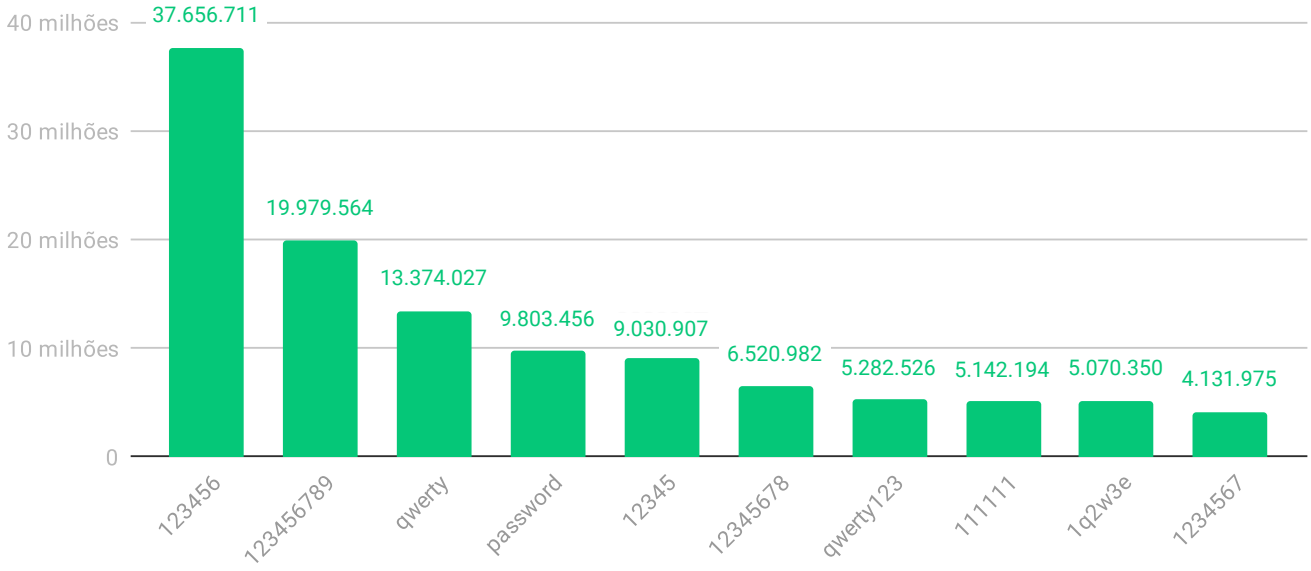


Figura 15. Ranking global de exposições de senhas detectadas pela Axur em 2019.

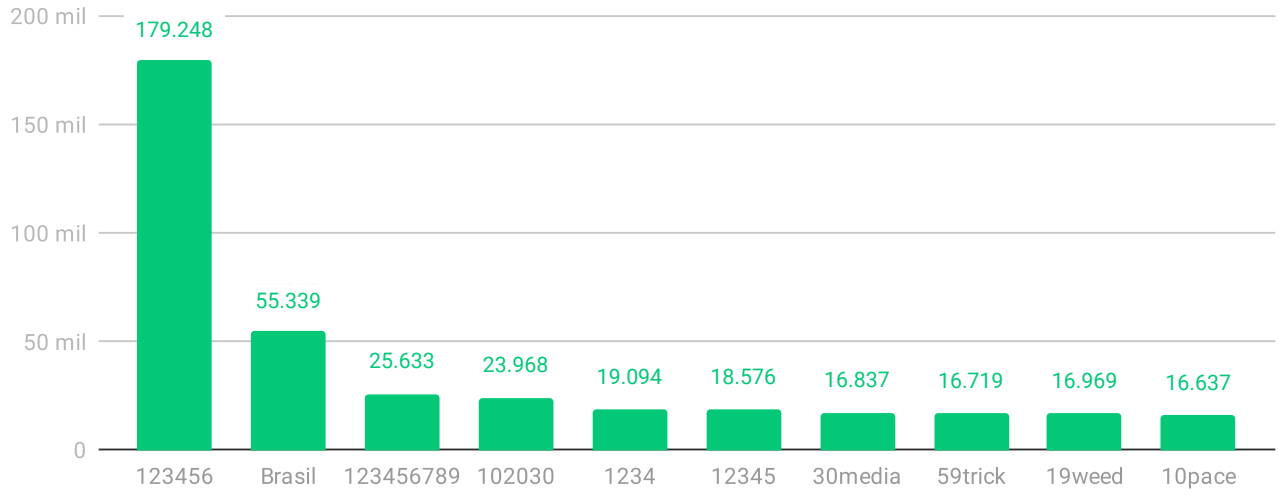


Figura 16. Ranking de exposições de senhas de domínios .br detectadas pela Axur em 2019.

Vazamento de cartões de crédito e débito

Exposição em web superficial, deep e dark web

No último trimestre de 2019, **914.137** 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 global de 69% nos vazamentos**, se comparado com os 540.656 cartões encontrados no terceiro trimestre.

No total anual, **1,6 milhão de cartões expostos** foram detectados em 2019.

Quarto trimestre de 2019

Para analisar as BINs (Bank Identification Numbers) com mais vazamentos de dados no quarto trimestre, foram selecionadas aquelas que tiveram 100 ou mais cartões expostos. Elas totalizam 730.535 cartões distribuídos em 713 diferentes BINs e 79,9% do total detectado no trimestre.

Desse total, 171 BINs são de instituições brasileiras (**23,9%**), que somam **93.093 cartões** (**12,7%**) expostos no período. Os Estados Unidos são o país campeão em vazamentos nesse trimestre, com 284 BINs (39,8%) na lista e que somam 505.982 (69,2%) cartões expostos.

Assim, o quarto trimestre mostra que **o Brasil é hoje o segundo país com mais vazamentos de dados cartões de crédito e débito on-line**, ficando atrás somente dos Estados Unidos. Esse período mostra que o país recuou em vazamentos de dados, já que no terceiro trimestre os cartões brasileiros somavam 49,9% do total vazado a nível mundial.

BIN (Bank Identification Number):
Os seis primeiros dígitos de um cartão de crédito ou débito, que identificam a instituição financeira emitente e o tipo do cartão.

2019

Entre janeiro e dezembro de 2019, foram 1.453 BINs com 100 ou mais cartões expostos, o que equivale a **1,29 milhão de dados vazados** (80,6% do total).

Desse montante, 346.674 cartões são brasileiros - o que equivale a 26,7% do total. Assim como no último trimestre, **em 2019 o Brasil foi o segundo país com mais vazamentos de cartões de crédito e débito on-line**, ficando atrás somente dos Estados Unidos – que registraram 50,9% do total. A Figura 17 apresenta a porcentagem de cada país nos registros analisados.

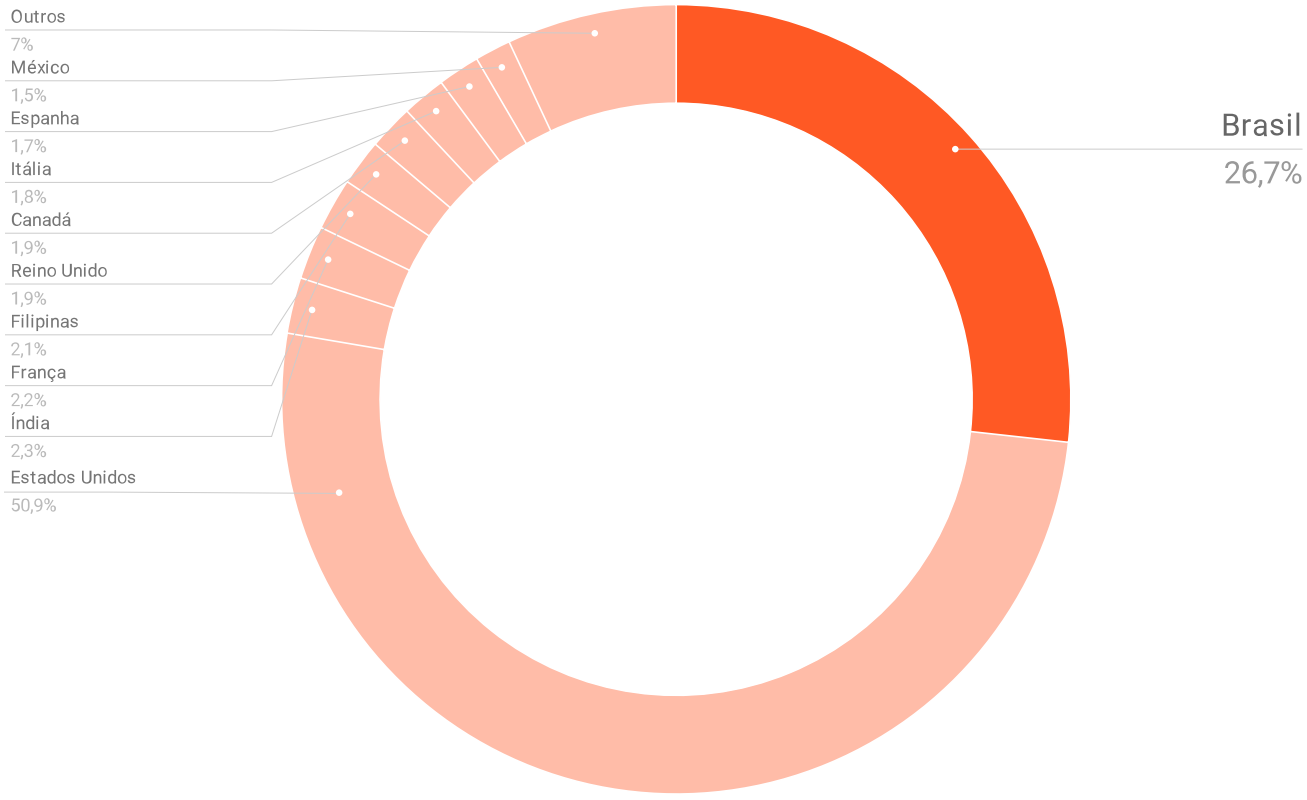


Figura 17. Porcentagem total dos países com mais cartões de crédito e débito vazados on-line e detectados pela Axur em 2019.

O ranking da Figura 18 mostra que **a BIN com mais vazamentos registrados em 2019 é brasileira**, com 26.803 cartões expostos. O Brasil também ocupa a sexta posição desse ranking com uma BIN que contabiliza 19.687 cartões expostos no ano.

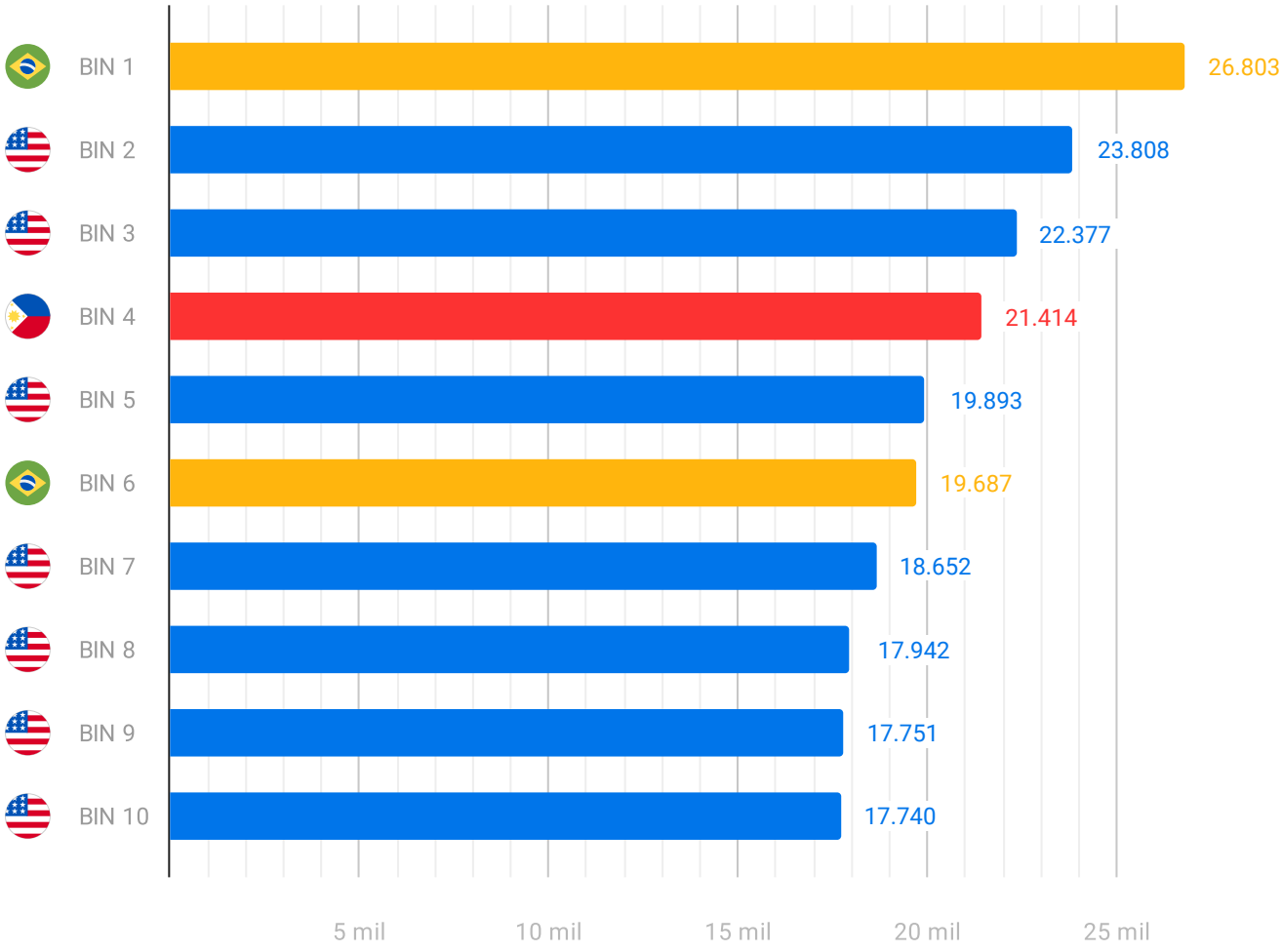


Figura 18. Ranking do número de cartões de crédito e débito expostos on-line das 10 BINs com mais vazamentos registrados mundialmente em 2019, identificadas por país.

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 monitoramento e proteção contra riscos digitais da Axur, **entre em contato conosco**.

INFOGRÁFICO

O crime on-line no Brasil em 2019

1. Uso de marca em golpes digitais

EM TODOS OS LUGARES

Na web superficial, o uso de marca é a principal forma de atrair vítimas para fraudes e golpes. Eles estão em todos os lugares possíveis.

50,9%

dos casos de pirataria e vendas não autorizadas aconteceram nos três últimos meses do ano, quando acontecem datas como a **Black Friday** e as **festas de final de ano**

Só nessa época, a taxa de perfis falsos cresceu **31,3%**

A taxa de domínios com nomes similares a marcas cresceu **35,1%**

Esses são os dois principais usos de marca usados para divulgar e hospedar phishing, a fraude mais comum para a...

2. Captura de dados sensíveis

ARMADILHAS VIRTUAIS

Atraídos os consumidores, as fraudes digitais furtam dados como **senhas e cartões de crédito e débito** ao simularem sites (casos de phishing) ou aplicativos (casos de malware) oficiais.

231,5%

foi o crescimento das páginas falsas de phishing entre fevereiro e dezembro

67%

dos ataques de phishing são feitos com nomes de domínio similares a marcas

A cada **15 minutos**

um ataque de phishing foi detectado no último trimestre

38 instituições financeiras

diferentes (e seus clientes) foram alvo de um mesmo malware, identificado em dezembro

E-commerce

é o setor mais atingido por phishing, com 44% do total

Da mesma forma que invasões de sistemas, essas fraudes geram...

3. Venda e vazamento de dados

UMA CHAVE, MUITAS CÓPIAS

Dados sensíveis são vendidos e expostos em listas **da web superficial à deep e dark web** – e geram prejuízos financeiros para empresas.

5,7 bilhões

de credenciais* expostas foram detectadas em 2019

23,6 milhões

são de domínios .br

37,6 milhões

é o número de vezes que a **senha *123456*** foi detectada em 2019

26,7%

dos cartões de crédito vazados on-line são do Brasil - só ficamos atrás dos Estados Unidos, que têm 50,9% das detecções

*E-mail com senha ou hash (senha criptografada)

axur.com

OneAxur

axur

@axurone

Sobre a Axur

Líder em monitoramento e reação a riscos digitais na América Latina, com foco em criar experiências digitais mais seguras para empresas e seus públicos. Utilizando automações e machine learning, fazemos proteção contra ameaças como uso abusivo de marca, vazamento de dados, phishing, aplicativos mobile fraudulentos e vendas não autorizadas. Para garantir as melhores experiências e jornadas dos consumidores, esse monitoramento é feito da web superficial à deep e dark web. Para mais informações, visite **axur.com** e conheça o blog Deep Space, **blog.axur.com**.

Contato para a imprensa

Denise Claudino
press@axur.com
+55 11 3376 5000

Endereços

US

535 Mission St.
San Francisco, CA 94105

Singapore

109 North Bridge Road
Cityhall District, 179097

São Paulo

Alameda Santos, 2326
9º andar, Conj 95