Relatório da Segurança Digital no Brasil

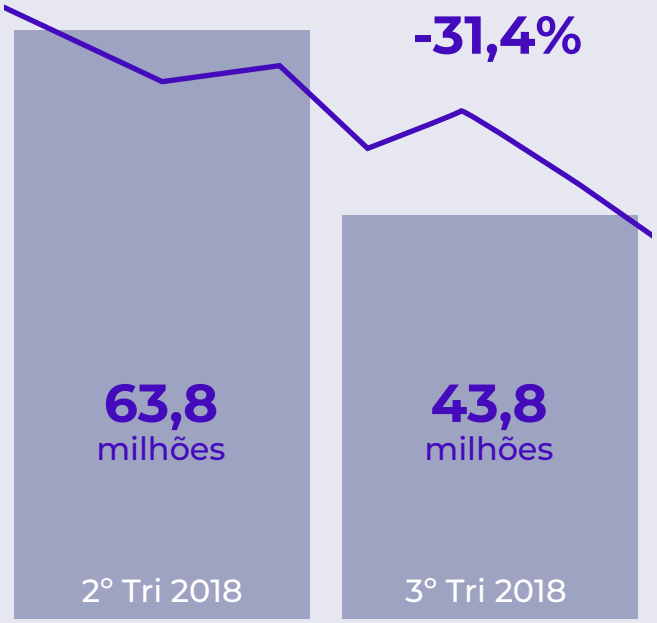
Terceiro trimestre - 2018

dfndr lab

SUMÁRIO

DESTAQUES

Terceiro trimestre tem queda de ciberataques e crescimento de fake news.



5 **links maliciosos**
detectados por segundo

Aproximadamente
1 em cada 5
brasileiros foi potencialmente alvo

Top 3 categorias detectadas no 3° trimestre

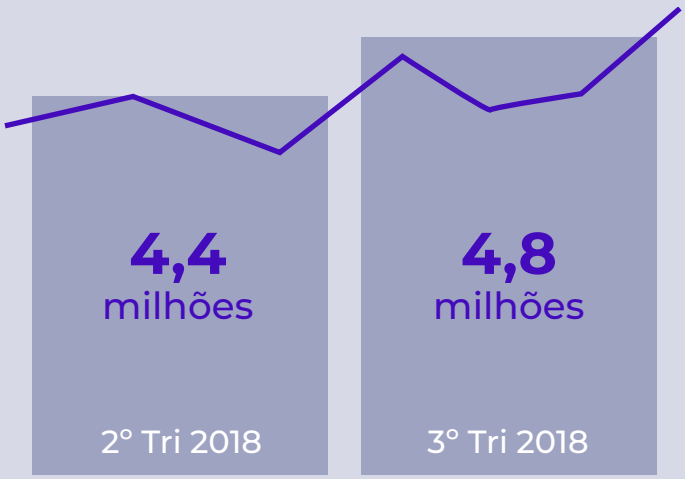
Phishing via app de mensagem

Publicidade suspeita

Notícias falsas

NOTÍCIAS FALSAS

aumento de **7%**



Top 3 assuntos das Notícias falsas

Política

Saúde

Dinheiro Fácil

Top 3 fontes de Notícias falsas

WhatsApp

Navegador

Facebook

Pesquisa realizada com mais de

35 mil brasileiros

mostrou que

85%

recebem correntes por WhatsApp ou Facebook Messenger

64,6%

foram impactados por informações falsas nessas correntes

Fake news em **debate**

Queda nos ciberataques via Phishing de app de mensagem (golpes via WhatsApp, em sua maioria) e crescimento de Notícias falsas (*fake news*). Este é o cenário do terceiro trimestre de 2018, retratado pela quinta edição do Relatório da Segurança Digital no Brasil, produzido pelo dfndr lab. Ao todo, foram 43,8 milhões de detecções de crimes cibernéticos no período de julho a setembro, sendo 4,8 milhões somente de *fake news*.

Apesar da sensível queda percebida entre os trimestres (31%), não podemos olhar para essa informação de forma simples e genérica. Os ciberataques não estão diminuindo. O que vimos, neste trimestre, foi uma combinação de fatores que englobam a redução do foco em grandes eventos que envolvam questões público-financeiras, como FGTS e PIS/Pasep, e de datas comemorativas de alta relevância para o varejo, além de uma intensificação de controle por parte de grandes empresas. Em alguns casos, vimos páginas de golpes serem construídas e retiradas do ar em questão de minutos.

Emilio Simoni
Diretor do dfndr lab

Um dos grandes vilões do ano, as **Notícias falsas** representaram mais de 10% de todas as detecções ciberataques do trimestre. **Ao todo foram quase 5 milhões,** o que equivale a 36 detecções por minuto.

No entanto, apesar destes fatores, os números seguem assustadores. E a criatividade dos cibercriminosos brasileiros faz com que, mesmo com um controle maior, os golpes na internet mantenham registros alarmantes. Ao compararmos o total da população brasileira, segundo os dados do Instituto Brasileiro de Geografia e Estatística (IBGE), projeta-se que um a cada cinco brasileiros possa ter sido vítima de um ciberataque. Por minuto, foram mais de 330 detecções de ataques.

Já entre as Notícias falsas, não é surpresa que o tópico política seja destaque. Entre todas as detecções realizadas no período, 46,3% estão relacionadas a este assunto. As eleições brasileiras, por sua vez, foram um dos temas que mais contribuíram para o aumento das divulgações de Notícias falsas no terceiro trimestre do ano. Foram mais de 2,2 milhões de detecções de fake news sobre o tema.

Outro importante destaque do trimestre fica por conta do alto índice de disseminação de conteúdos falsos entre os brasileiros. Uma pesquisa realizada pelo nosso aplicativo dfndr security com mais de 35 mil respondentes ao redor do Brasil mostra que quase 65% das pessoas já receberam correntes com conteúdo falso em aplicativos mensageiros, como WhatsApp e Facebook Messenger. Por terem temas alarmantes ou altamente atrativos para o público, estes conteúdos se espalham rapidamente através de amigos, familiares e conhecidos, inclusive porque solicitam o compartilhamento.

Diante de todos estes dados, uma dica importante: fique alerta! Golpes pela internet, conteúdos maliciosos e/ou tendenciosos continuam se espalhando em grandes proporções e ficam cada vez mais críveis.

Quer saber mais sobre o cenário de cibersegurança no Brasil nos últimos três meses? Confira nosso relatório na íntegra.

Sobre o RELATÓRIO

O Relatório da Segurança Digital no Brasil é produzido pelo dfndr lab, laboratório de cibersegurança da PSafe, que utiliza técnicas de inteligência artificial e *machine learning* e conta com um time de especialistas em segurança digital. Os dados do relatório são gerados pelas detecções de ciberataques aos smartphones Android dos mais de 21 milhões de usuários do aplicativo de segurança dfndr security. Por meio de uma aplicação pioneira da tecnologia anti hacking, o app é capaz de checar links maliciosos em aplicativos de mensagens e redes sociais e identificar se pode ser golpe ou *fake news*. Atualmente, o dfndr security é o principal aplicativo de segurança para smartphones que alerta sobre notícias falsas, sendo também o único meio de gerar dados sobre a circulação deste tipo de conteúdo em aplicativos de mensagens.

Todos os dados de volumes e percentuais demográficos contidos no relatório são inferidos por algoritmos do dfndr lab, que utilizam inúmeros critérios de comportamento dos usuários, protegendo a sua privacidade. Quanto às *fake news*, qualquer conteúdo identificado como suspeito é analisado previamente pela equipe de especialistas do dfndr lab e por agências de *fact-checking* parceiras. A análise contida no relatório foi realizada entre 01 de julho e 30 de setembro de 2018.

Links MALICIOSOS

2° trimestre de 2018

63,8 milhões

3° trimestre de 2018

43,8 milhões

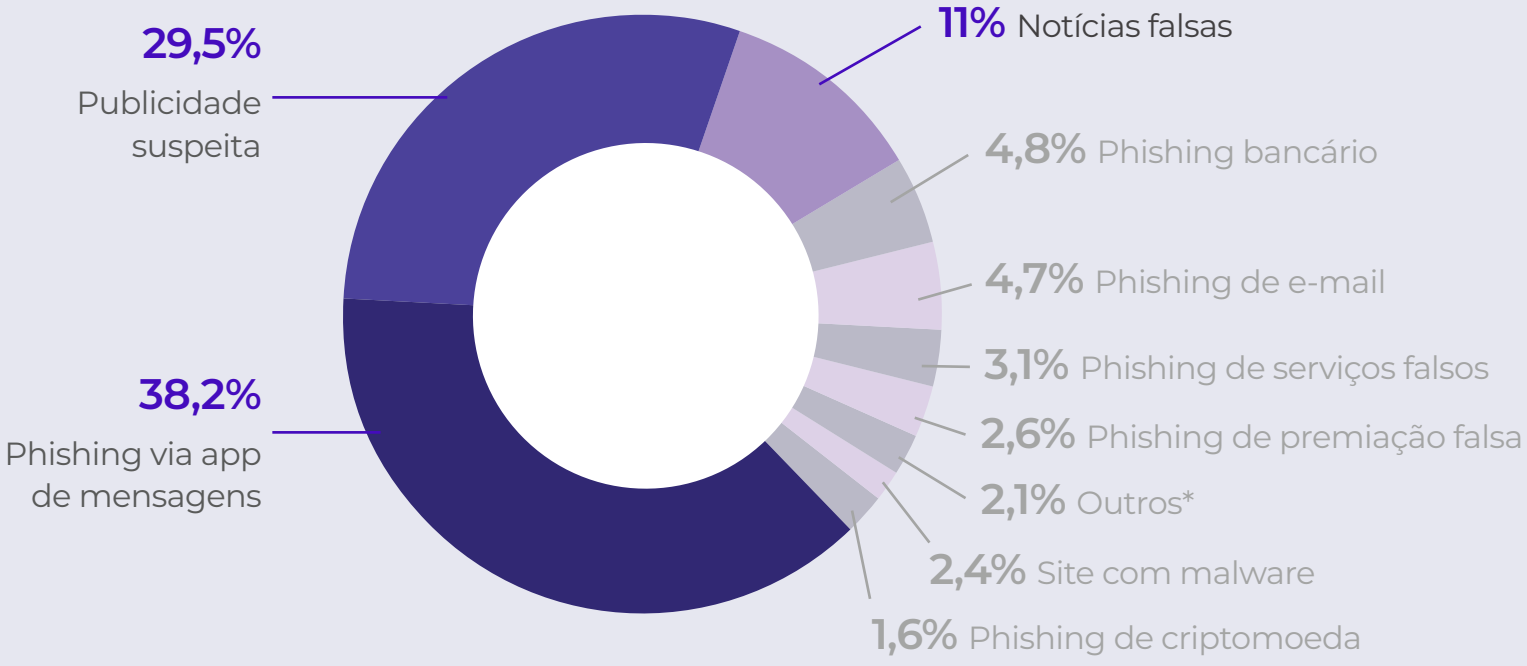
Redução de **31,4%**

O período foi marcado pela redução do foco em grandes eventos que envolvam questões público-financeiras e de datas comemorativas de alta relevância para o varejo, além da intensificação na proteção e controle por marcas promovidas indevidamente em links maliciosos.

JULHO	AGOSTO	SETEMBRO
15.609.179	**13.256.500**	**14.962.191**

19,8 mil / HORA **331** / MINUTO

Principais categorias de links maliciosos



*Golpe do SMS pago; Phishing de perfil falso; Genérico; Phishing de redes sociais;

LINKS MALICIOSOS
por gênero

NÚMERO DE DETECÇÕES ENTRE **HOMENS** É **3,3 vezes maior** QUE ENTRE AS **MULHERES**

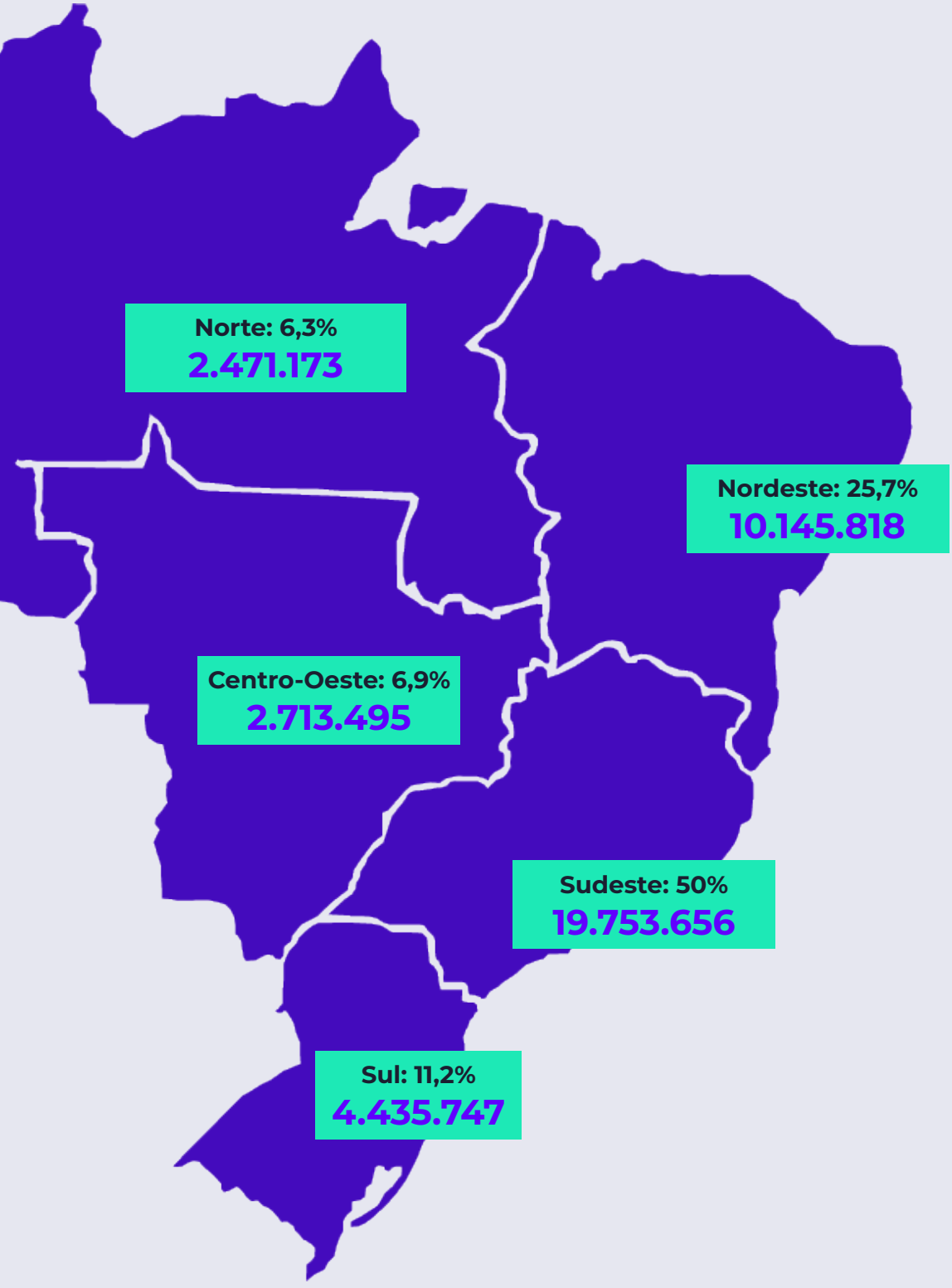
76,9%

23,1%

76,8%	PUBLICIDADE SUSPEITA	**23,2%**
73,4%	PHISHING BANCÁRIO	**26,6%**
76,3%	PHISHING DE CRIPTOMOEDA	**23,7%**
84,8%	NOTÍCIAS FALSAS	**15,2%**
77,5%	PHISHING DE PREMIAÇÃO FALSA	**22,5%**
76,1%	PHISHING VIA APP DE MENSAGENS	**23,9%**
67,4%	PHISHING DE SERVIÇOS FALSOS	**32,6%**
75,7%	PHISHING DE E-MAIL	**24,3%**
76,6%	SITE COM MALWARE	**23,4%**
78,8%	GOLPE DO SMS PAGO	**21,2%**
65,7%	GENÉRICO	**34,3%**
82,9%	PHISHING DE PERFIL FALSO	**17,1%**
69,0%	PHISHING DE REDES SOCIAIS	**31,0%**

LINKS MALICIOSOS
por região

1 em cada 4 pessoas do Sudeste foi potencialmente **vítima de ciberataques***



*Cálculo realizado com base no número de detecções do dfndr lab no período e o total de habitantes da região divulgado pelo Instituto Brasileiro de Geografia e Estatística (IBGE).

LINKS MALICIOSOS
por estado

Norte	
Acre	74.850
Amapá	152.112
Amazonas	778.411
Pará	1.063.031
Rondônia	214.166
Roraima	441
Tocantins	188.162

Nordeste	
Alagoas	484.632
Bahia	2.871.842
Ceará	1.863.293
Maranhão	804.781
Paraíba	674.603
Pernambuco	1.936.969
Piauí	443.875
Rio Grande do Norte	636.663
Sergipe	429.160

Centro-Oeste	
Distrito Federal	836.856
Goiás	1.002.335
Mato Grosso	446.324
Mato Grosso do Sul	427.980

Sudeste	
Espírito Santo	575.890
Minas Gerais	4.063.991
Rio de Janeiro	4.650.561
São Paulo	10.463.214

Sul	
Paraná	1.702.242
Rio Grande do Sul	1.744.947
Santa Catarina	988.558

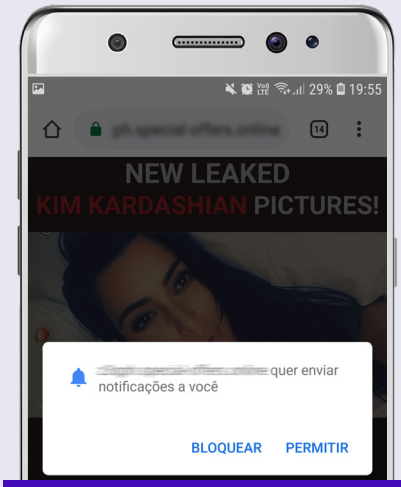
Cerca de 10% do total de ataques não possui região identificada

TOP 3
LINKS MALICIOSOS

1 PHISHING VIA APP DE MENSAGEM

Link para uma página web de uma oferta falsa, que induz o usuário a fornecer seus dados pessoais e/ou compartilhar um link com seus contatos em troca de alguma vantagem.

2º trimestre	3º trimestre	Variação de
36,6 MILHÕES DE DETECÇÕES	**16,7** MILHÕES DE DETECÇÕES	**-54,2%**



2 PUBLICIDADE SUSPEITA

Páginas ou notificações com avisos falsos sobre o funcionamento do celular, induzindo o usuário a instalar um aplicativo, conceder permissão para envio de notificação ou redirecionando a outro link malicioso.

2º trimestre	3º trimestre	Variação de
12,2 MILHÕES DE DETECÇÕES	**12,9** MILHÕES DE DETECÇÕES	**+6%**

3 NOTÍCIAS FALSAS

São conteúdos falsos produzidos e compartilhados como verdadeiros com o objetivo de manipular a opinião pública e gerar visualização de anúncios.

2º trimestre	3º trimestre	Variação de
4,4 MILHÕES DE DETECÇÕES	**4,8** MILHÕES DE DETECÇÕES	**+7,2%**

Detecções de NOTÍCIAS FALSAS

O dfndr lab tem investido em tecnologias proprietárias, baseadas em inteligência artificial e humana, para aumentar sua capacidade de detectar e alertar sobre notícias falsas. Os sistemas do laboratório são programados para analisar links que apresentem comportamentos maliciosos ou que tentem imitar domínios confiáveis. Quando localizados, esses links são enviados a uma base de dados e, logo após, submetidos a uma análise de conteúdo pela equipe de especialistas do dfndr lab.

Para complementar a efetividade do combate às *fake news*, todos os dias os especialistas do dfndr lab buscam pessoalmente por notícias falsas que viralizam nas redes sociais. Com apoio da ferramenta de Análise de Links, disponível ao público no site do dfndr lab, todo link submetido passa pelo processo de análise do conteúdo, primeiramente pelos sistemas do laboratório e em seguida pela equipe de especialistas.

JULHO	AGOSTO	SETEMBRO
2.304.221	**1.127.877**	**1.388.853**

52,4 mil / DIA | **2,1 mil** / HORA

2° trimestre de 2018

32,5% Dinheiro fácil
20,3% TV e Celebridades
19,5% Política
19,1% Saúde
8,5% Outros

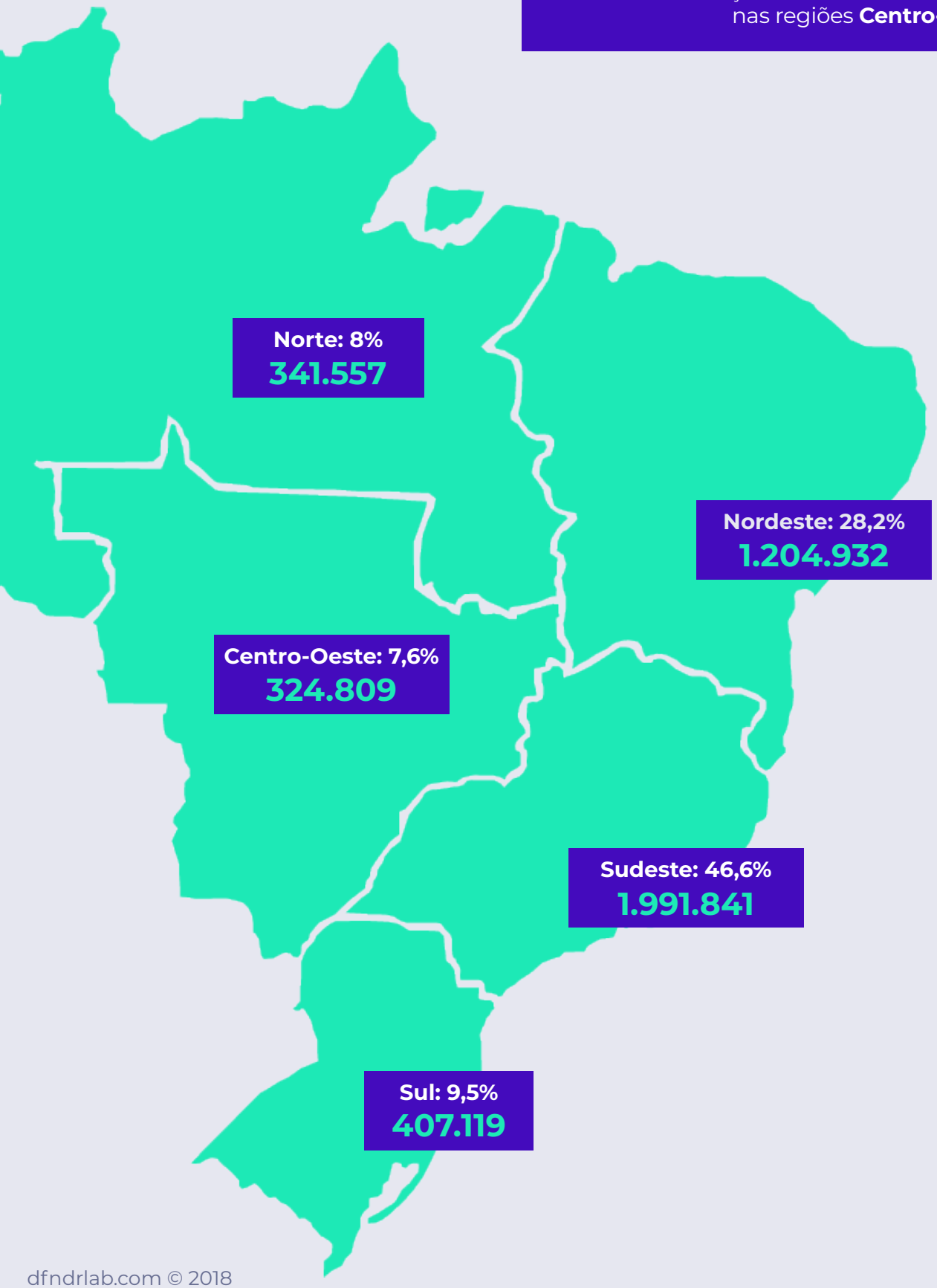
NOS ÚLTIMOS SEIS MESES, O TEMA **POLÍTICA** REPRESENTOU MAIS DE **3 MILHÕES** DE DETECÇÕES

3° trimestre de 2018

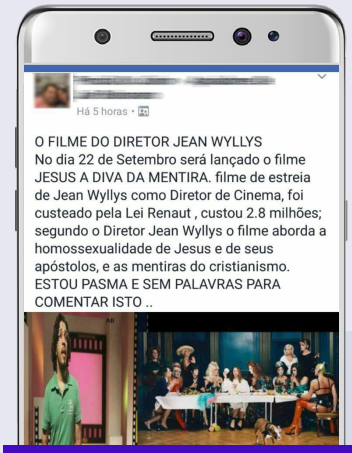
46,3% Política
41,6% Saúde
6,4% Crime
5,0% Religião
0,7% Outros

NOTÍCIAS FALSAS
por região

Detecções de Notícias falsas **crescem** nas regiões **Centro-Oeste** e **Sul**



TOP 5 NOTÍCIAS FALSAS
sobre o tema política



1 JEAN WYLLYS VAI DIRIGIR FILME QUE MOSTRA JESUS COMO HOMOSSEXUAL

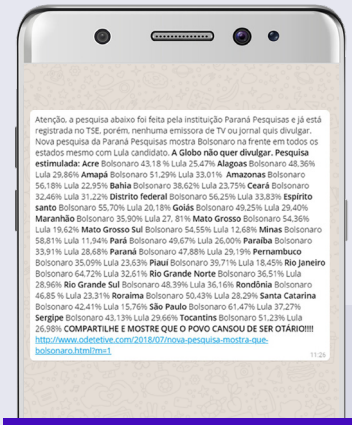
A notícia falsa afirma que o deputado captaria dinheiro público, através da Lei Rouanet, para fazer um filme sobre Jesus Cristo retratado como homossexual.

625 MIL DETECÇÕES

2 STJ AUTORIZA CANCELAMENTO DA CNH EM CASO DE IPVA ATRASADO

A mensagem falsa dizia que, para conter a medida, era preciso compartilhar o link e assinar uma petição que seria enviada ao Congresso Nacional.

577,2 MIL DETECÇÕES



3 NOVA PESQUISA MOSTRA QUE BOLSONARO VENCE LULA EM TODOS OS ESTADOS`

A suposta pesquisa reunia dados de intenção de voto de eleitores de diversos estados do Brasil e era falsamente atribuída a um instituto de pesquisa.

190,6 MIL DETECÇÕES

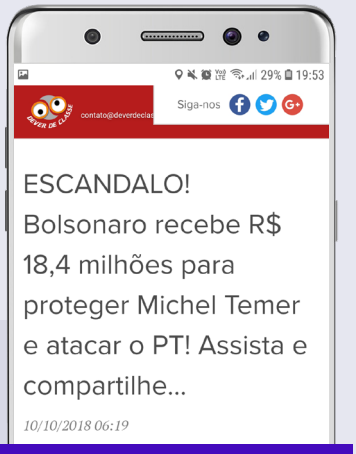
TOP 5 NOTÍCIAS FALSAS
sobre o tema política

4

BOLSONARO RECEBE R$ 18,4 MILHÕES PARA PROTEGER MICHEL TEMER E ATACAR O PT

O falso conteúdo dizia que Bolsonaro teria recebido dinheiro oriundo do governo Michel Temer e usava seus seguidores nas redes sociais para atacar Lula e o PT.

135,5 MIL DETECÇÕES



5

MILITANTE QUE TENTOU ASSASSINAR JAIR BOLSONARO RECEBEU R$ 350 MIL

O boato afirmava que os extratos da transferência de R$ 350 mil para o autor do crime teriam partido do PT e já estariam em posse da Polícia Federal.

56,6 MIL DETECÇÕES

Como identificar
Notícias falsas

As famosas *fake news* são, em sua maioria, produzidas a partir de temas polêmicos, apelativos e até sensacionalistas, com grande potencial de viralização. Como todo ciberataque, quanto mais elaborado e próximo da realidade for o conteúdo, maior a probabilidade de atingir um alto número de acessos e compartilhamentos na rede.

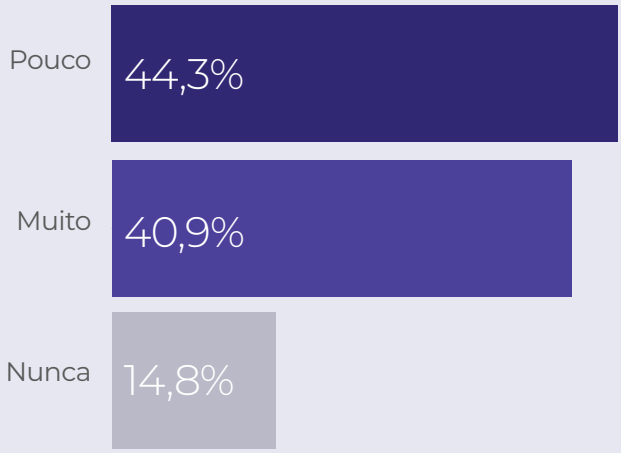
As notícias falsas também apresentam construções de texto similares, com pontos-chave que podem indicar que o seu conteúdo é irreal. Desta forma, verificar a existência desses pontos-chave pode ajudar a identificar as *fake news*.

Pesquisa:

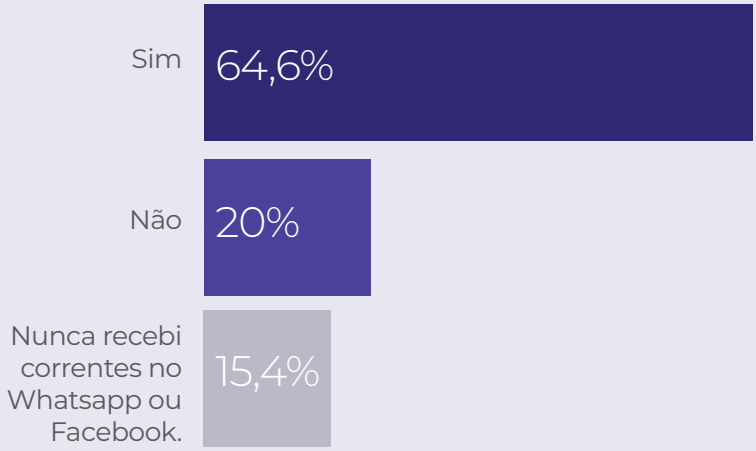
Correntes em apps de mensagem

Pesquisa online conduzida em julho de 2018, pelo dfndr lab, com 35.565 usuários do dfndr security, em dispositivos Android, aponta que mais de 60% das pessoas já receberam conteúdo falso em apps de mensagem, como o WhatsApp e Facebook Messenger.

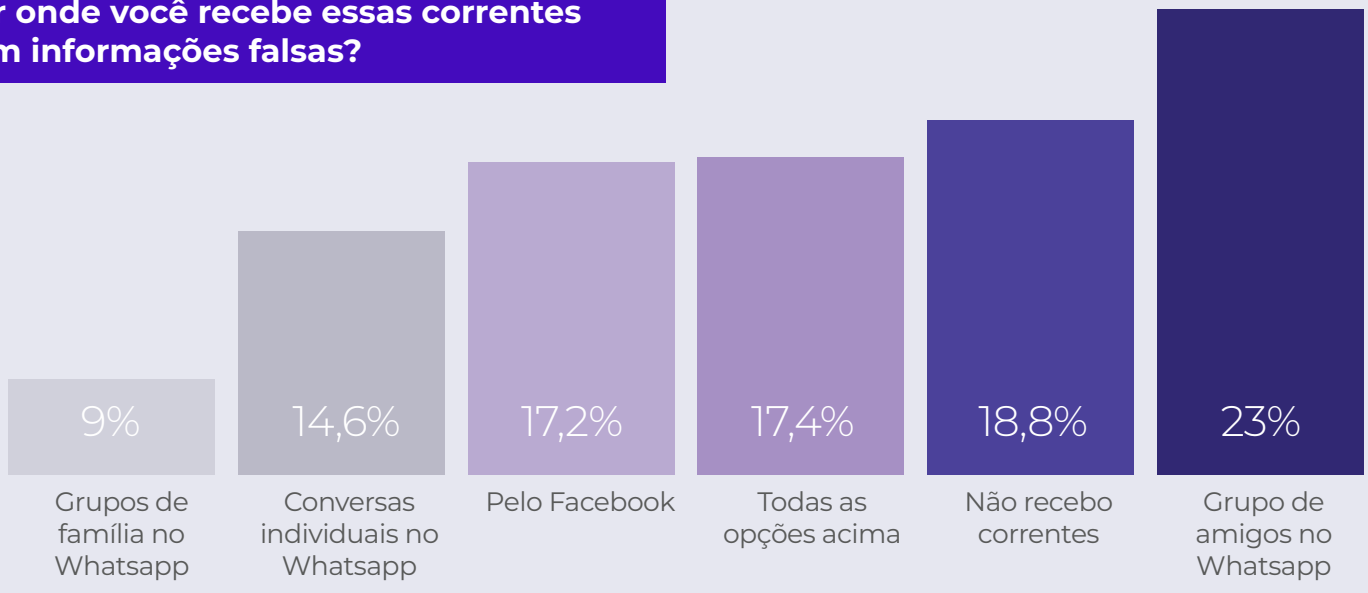
Com que frequência você recebe correntes no Whatsapp ou no Facebook?



Nessas correntes, já circularam falsas promessas de emprego, falsos brindes ou falsos benefícios do governo?



Por onde você recebe essas correntes com informações falsas?



Glossário

Carder
Aquele que compra e vende na internet dados de cartão de crédito roubados através de golpes de phishing ou de ataques a sites de varejo.

Ciberataque
Qualquer atividade ilícita realizada na internet ou por meio de um dispositivo eletrônico. Tais atividades incluem fraude, roubo de identidade, phishing etc.

Crimeware
Qualquer software criado para praticar crimes digitais e, assim, obter ganho financeiro.

Engenharia Social
Método usado por hackers para espalhar links maliciosos e realizar ataques de maneira indireta, em geral por meio de pessoas de confiança da vítima, como familiares e amigos. A vítima fica mais inclinada a aceitar e clicar em links se eles vierem de quem ela confia.

Ferramenta de Hacking
Software ou instrumento usado por um hacker para realizar ações ilegais ou sem autorização.

Golpe do SMS pago
Sites que cadastram automaticamente ou induzem o usuário a se cadastrar em um serviço pago de SMS.

Hacker
Aquele que acessa um dispositivo, software ou rede de computadores de forma ilegal ou sem autorização.

Link malicioso
Links para sites criados com propósito malicioso, como enganar o usuário ou roubar informações. Contemplam golpes de phishing, publicidade suspeita, notícias falsas, sites com malware etc.

Malware
Todos os softwares que contêm um código malicioso, como vírus, trojan ou worm.

Notícias falsas
Conteúdos escritos e publicados de maneira a se parecerem com notícias reais com a intenção de enganar o usuário para obter vantagens diversas.

Phishing
Armadilhas criadas para induzir o usuário a compartilhar seus dados pessoais ou financeiros, como senhas, número de celular e dados do cartão de crédito.

Phishing bancário
Sites falsos iguais às páginas de instituições bancárias criados para enganar usuários e roubar suas credenciais do banco, como tokens, senha, número da conta, dados de cartão de crédito etc.

Phishing de criptomoeda
Sites falsos de negociação de criptomoedas.

Phishing de premiação falsa
Tipo de golpe que diz que o usuário ganhou um prêmio. Normalmente, depois do clique, ele é obrigado a baixar um app, fornecer dados pessoais ou se inscrever em um serviço pago.

Phishing de perfil falso
Perfis falsos criados em redes sociais para persuadir ou redirecionar usuários para outros ataques que podem acarretar no roubo de seus dados pessoais e financeiros.

Phishing de redes sociais
Ataques criados para roubar credenciais das redes sociais a fim de invadir a conta do usuário e usá-la com propósito malicioso.

Phishing de serviços falsos
Página que oferece um serviço em que o usuário é obrigado a fornecer seus dados, instalar algum app ou se inscrever em outro serviço pago para usufruir da oferta, mas ao final não recebe o prometido.

Phishing via aplicativo de mensagens
Tipo de página falsa que obriga o usuário a fornecer dados pessoais e compartilhar um link com seus contatos em mensageiros como WhatsApp.

Publicidade suspeita
Páginas ou pop-ups com mensagens que enganam o usuário, por exemplo, afirmando que o celular tem vírus, para forçá-lo a assinar serviços ou instalar aplicativos.

Scammer
Alguém que finge ser um usuário legítimo de uma plataforma para convencer outras pessoas a enviar dinheiro, informações pessoais ou financeiras e a instalar arquivos maliciosos.

Site com malware
Link enganoso criado para induzir o usuário a instalar um malware que pode danificar seu dispositivo ou roubar dados pessoais.

Spammer
Aquele que é responsável por desenvolver um software ou por enviar um enorme número de e-mails com propósito malicioso, como golpes de phishing ou malware.

Vulnerabilidade
Uma falha ou erro em um software ou sistema que pode permitir a ação de um hacker com propósito malicioso.

dfndr lab