

# Relatório da Segurança Digital no Brasil

Segundo trimestre - 2018

---

**dfndr** lab



# SUMÁRIO

Destaques do trimestre .....	03
Carta do Diretor: A sofisticação do crime cibernético.....	05
Sobre o laboratório .....	07
Total de detecções de links maliciosos no Brasil .....	08
Principais categorias de links maliciosos .....	08
Detecções de links maliciosos por gênero .....	09
Detecções de links maliciosos por região .....	10
Detecções de links maliciosos por estado .....	11
Top 3 categorias de links maliciosos .....	12
Total de detecções de notícias falsas no Brasil .....	13
Detecções de notícias falsas por região .....	14
Top 5 notícias falsas .....	15
Detecções de notícias falsas por assunto .....	16
O papel do dfndr lab na identificação de notícias falsas .....	17
Os bastidores da Copa .....	18
Entrevista: Delegacia de Repressão aos Crimes Informáticos .....	19

# DESTAQUES

# 120,7 milhões

de detecções de links maliciosos no primeiro semestre de 2018

1º Tri 2018

56,9 milhões

2º Tri 2018

63,8 milhões

↑ Aumento de 12%

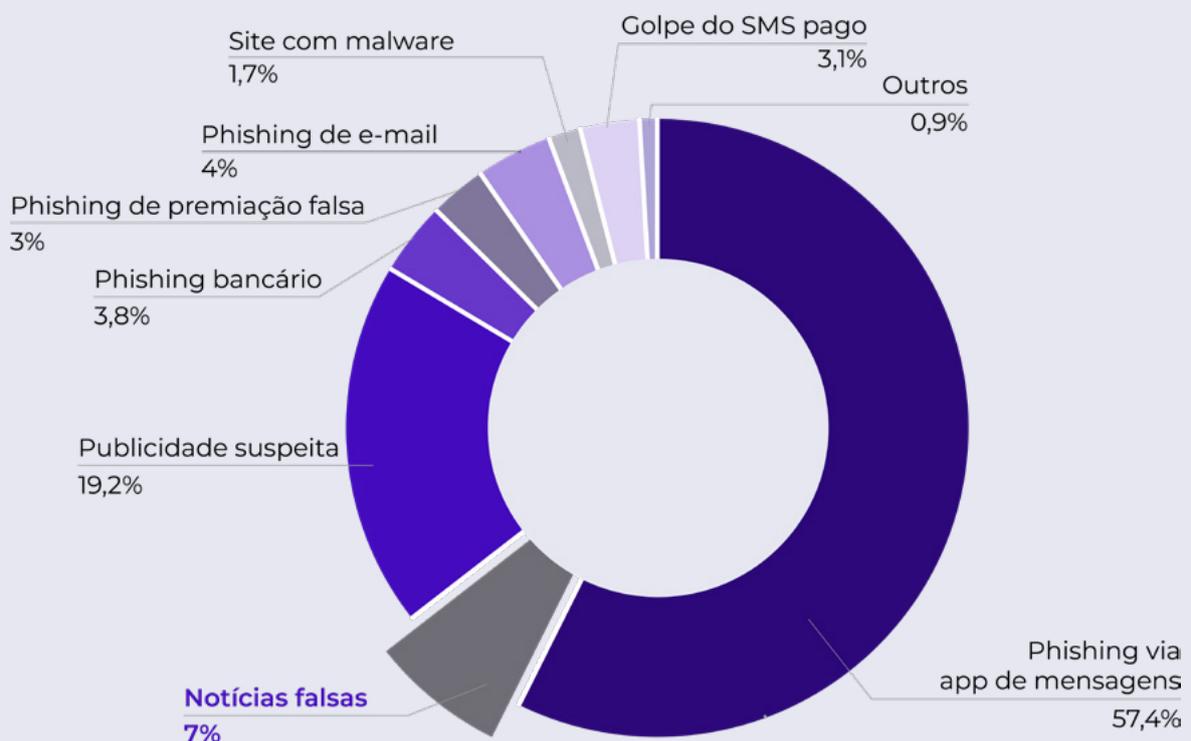
**8** links maliciosos detectados por segundo

Em comparação às mulheres, **homens** acessaram **o dobro de links maliciosos** no 2º trimestre

Aproximadamente

**1 em cada 3** brasileiros foi potencialmente alvo

## Principais categorias detectadas no 2º trimestre



## Notícias falsas



### Top 3 assuntos das Notícias falsas:

1. Dinheiro fácil
2. TV e celebridades
3. Política

## Curiosidade do trimestre

**Hackers** se aproveitam de grandes eventos para intensificar ataques



# A sofisticação do CRIME CIBERNÉTICO

A quarta edição do Relatório de Segurança Digital no Brasil do dfndr lab aponta para um cenário que segue preocupante: mais de 120 milhões de detecções de ciberataques via links maliciosos nos primeiros seis meses de 2018 - número 95,9% maior que o registrado no mesmo período de 2017.

Destes 120 milhões, 63,8 milhões foram detectados somente no segundo trimestre do ano, montante 12,2% maior que os 56,9 milhões do primeiro trimestre. Os números são alarmantes, pois, se comparados ao total da população brasileira, segundo dados do Instituto Brasileiro de Geografia e Estatística (IBGE), projeta-se que um em cada três brasileiros pode ter sido vítima de cibercriminosos somente entre os meses de abril, maio e junho de 2018. Somado a isso, nossa análise nos mostra que, a cada segundo, no último trimestre, foram detectados oito links maliciosos. Foram mais de 28 mil detecções por hora.



**Emílio Simoni**  
Diretor do dfndr lab

---

**63,8 MILHÕES** de ciberataques foram detectados somente no segundo trimestre do ano. Isto significa que foram detectados 8 links maliciosos por segundo. Mais de 28 mil por hora.

---

Entre os ataques detectados no segundo trimestre, três categorias seguem se destacando: Phishing via app de mensagem (36,6 milhões de detecções); Publicidade suspeita (12,2 milhões de detecções); e Notícias falsas (4,4 milhões de detecções). Estes dois últimos, no entanto, demandam especial atenção a partir do momento em que apresentaram um aumento de mais de 50% entre o primeiro e o segundo trimestre e mantêm como principal objetivo do ataque o lucro indevido a partir de visualizações, acessos e cliques.

Também confundida, em muitos casos, com alertas de erros e problemas no smartphone, a Publicidade suspeita tem crescido, principalmente, devido a uma diversificação das fontes de ataque, que antes ficavam mais concentradas em sites duvidosos ou de conteúdo adulto. Nos últimos meses, no entanto, foi possível notar que os cibercriminosos estavam usando cada vez mais sites confiáveis para propagar Publicidade suspeita - representando 41,6% de todas as fontes de origem destes alertas falsos. Já as Notícias falsas têm crescido devido a uma maior sofisticação de conteúdo, muitas vezes mais críveis e ligados a situações cotidianas.

Outro importante destaque do período foi a confirmação de uma tendência que notamos no último trimestre de 2017: uso massivo de estratégias para convencer o usuário a aceitar uma permissão de envio de notificações de celular. Com isso, os cibercriminosos vêm construindo uma base de pessoas para as quais enviam golpes diretamente por meio de notificações e, depois disso, ainda convencem as vítimas a compartilhar e disseminar os links maliciosos por aplicativos de mensagem.

Nos três últimos meses do semestre, o dfndr lab registrou, também, que os grandes eventos se mantêm como um chamariz para cibercriminosos. Ao todo, foram 69 ciberataques focados na Copa e mais de 6 milhões de detecções.

---

Neste segundo trimestre, uma forte tendência se confirmou: criminosos se utilizaram de **notificações de celular** para iniciar diversos golpes via links maliciosos.

---

Para saber mais sobre o cenário da segurança digital no Brasil nos últimos meses, confira na íntegra o nosso relatório, nas próximas páginas.

# Sobre o

# LABORATÓRIO

O dfndr lab é um time global de especialistas em segurança digital com vasta experiência e conhecimento técnico. Sua missão é combater a disseminação de links maliciosos e notícias falsas e contribuir para que todos possam navegar com liberdade e segurança. O laboratório conta com tecnologias proprietárias, e utiliza técnicas de Inteligência Artificial e Machine Learning - capacidade programada para que computadores aprendam sozinhos a melhorar o desempenho de suas funções - nos seus métodos de detecção e prevenção contra ciberataques. Cerca de 200 milhões de arquivos digitais são processados, analisados e indexados diariamente pelos sistemas do dfndr lab.

O Relatório da Segurança Digital no Brasil, do dfndr lab, é baseado nos dados de detecções de ciberataques aos celulares Android dos mais de 21 milhões de usuários dos aplicativos dfndr. Para inferir dados de volumes e percentuais demográficos, os algoritmos utilizam inúmeros critérios de comportamento. A análise foi realizada entre 01 de abril e 30 de junho de 2018.

## Total de detecções de links maliciosos no Brasil

1º trimestre de 2018  
**56,9** milhões

2º trimestre de 2018  
**63,8** milhões

↑ Aumento de **12,2%**

O percentual de aumento no segundo trimestre de 2018 está diretamente relacionado a datas comemorativas e grandes eventos que marcaram o período, como a Copa do Mundo e Dia dos Namorados. Quando comparado ao trimestre anterior, com temporada de férias escolares e carnaval, os meses de abril, maio e junho foram muito mais propícios a tentativas de ciberataques mais sofisticados e diversificados.

A cada segundo, **8 links maliciosos** foram detectados no Brasil

ABRIL

**19.451.958**

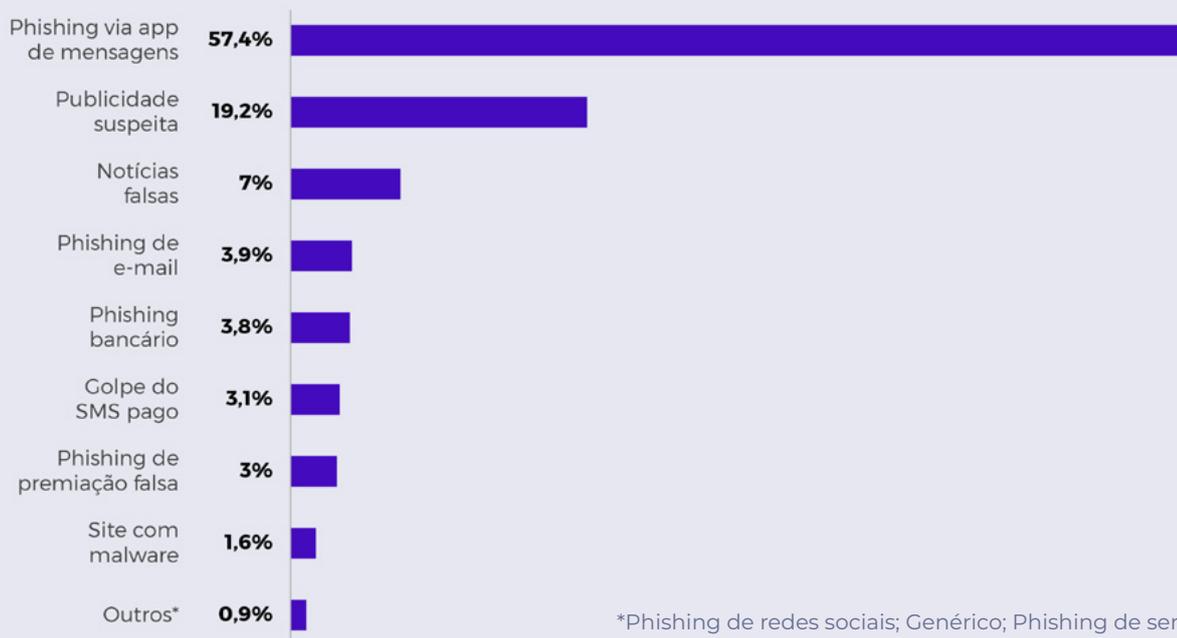
MAIO

**22.911.396**

JUNHO

**21.523.322**

## Principais categorias de links maliciosos

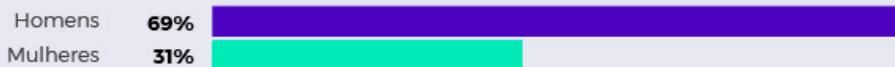


\*Phishing de redes sociais; Genérico; Phishing de serviços falsos

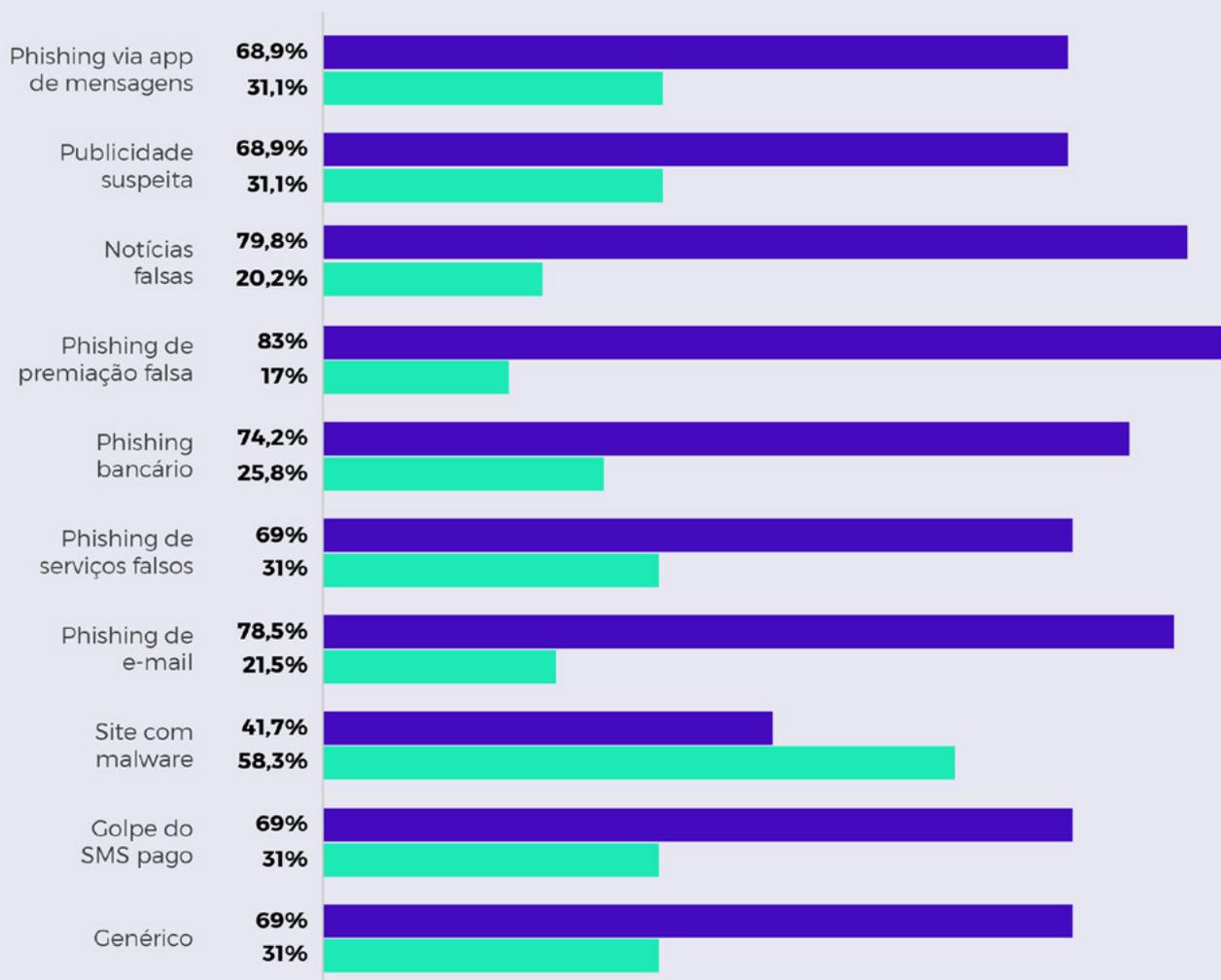
Número de deteções entre o **público masculino** corresponde **ao dobro** do **público feminino**

De acordo com o dfndr lab, **69%** das deteções de links maliciosos do segundo trimestre de 2018 foram registradas a partir de acessos masculinos, enquanto **31%** foram femininos.

## Detecções de links por gênero

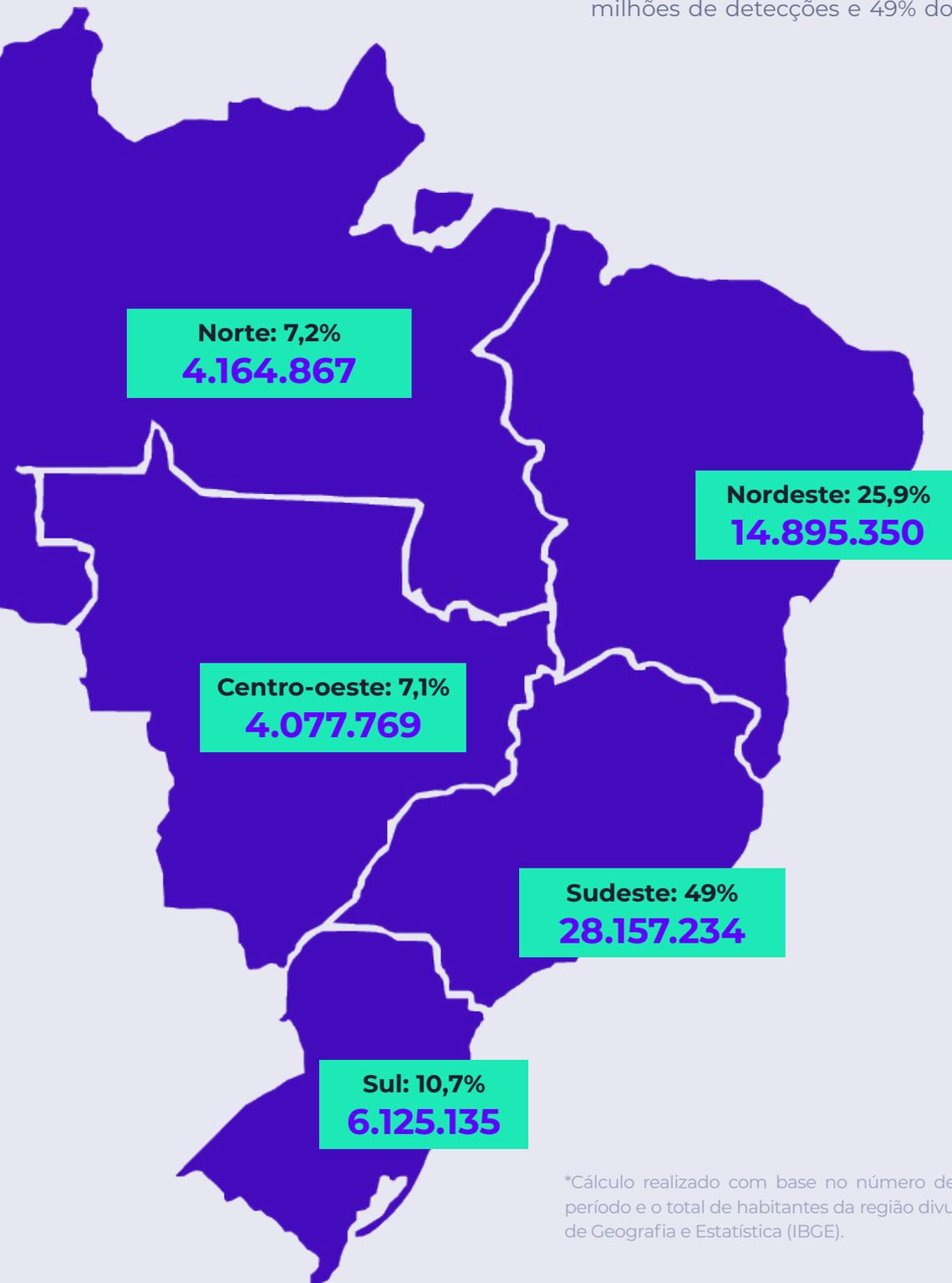


## Categorias de links detectados



## Norte se destaca no trimestre chegando a **1 detecção para cada 3 habitantes\***

Nos meses de abril, maio e junho, Centro-oeste, Norte e Sudeste foram as regiões com o maior número de detecções de links maliciosos por habitante. Ao todo, foram 4,1 milhões de detecções na região Norte que, pela primeira vez, atingiu a proporção de 1 detecção para cada 3 habitantes. Em números absolutos, a região Sudeste segue como o principal alvo, com 28 milhões de detecções e 49% dos registros no período.



\*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).

# Detecções

## POR ESTADO

### Norte

Acre	112.471
Amapá	244.775
Amazonas	1.215.653
Pará	1.948.468
Rondônia	335.072
Roraima	982
Tocantins	307.446

### Nordeste

Alagoas	723.120
Bahia	4.235.528
Ceará	2.700.679
Maranhão	1.209.357
Paraíba	964.951
Pernambuco	2.758.204
Piauí	680.731
Rio Grande do Norte	898.163
Sergipe	724.617

### Centro-Oeste

Distrito Federal	1.224.026
Goiás	1.554.287
Mato Grosso	748.076
Mato Grosso do Sul	551.380

### Sudeste

Espírito Santo	817.830
Minas Gerais	6.335.574
Rio de Janeiro	6.306.142
São Paulo	14.654.436

### Sul

Paraná	2.374.477
Rio Grande do Sul	2.399.043
Santa Catarina	1.351.615

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

## 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.

**36,6** MILHÕES DE DETECÇÕES

O Phishing via app de mensagens segue liderando o ranking de categorias como principal meio de disseminação de ciberataques. Com uma redução mínima de 1,6% quando comparado ao primeiro trimestre de 2018, a categoria concentrou 57,4% do total de detecções realizadas pelo dfndr lab no período, com uma média de 12,2 milhões de registros por mês.

Assuntos relacionados a futebol foram os mais usados como iscas em Phishing via app de mensagens. Ao todo, 33,4% de detecções da categoria prometiam desde camisas oficiais da Seleção Brasileira até temas de times de futebol para personalizar o WhatsApp.



## 2 PUBLICIDADE SUSPEITA

Páginas ou notificações com avisos falsos sobre o funcionamento do celular, induzindo o usuário a instalar um aplicativo ou redirecionando a outro link malicioso.

**12,2** MILHÕES DE DETECÇÕES

Quando comparada com o primeiro trimestre de 2018, a Publicidade suspeita teve um aumento de 50,4% nas detecções, saltando de 8,1 milhões para 12,2 milhões no segundo trimestre. Os registros apontam que 41,7% do total foi veiculado em sites de conteúdo adulto; 41,6% em sites confiáveis de e-commerce, jornalismo online e entretenimento (sem o consentimento das empresas proprietárias); e 16,8% em sites de download de música e filme e fake news.

O período foi marcado pela confirmação da tendência prevista pelo dfndr lab no último trimestre de 2017: o uso massivo de estratégias para convencer o usuário a permitir o recebimento de notificações. Só no segundo trimestre de 2018, foram detectados 4,6 milhões de Publicidades suspeitas que solicitam essa permissão, com um aumento expressivo de 958% entre maio e junho.



# 3 NOTÍCIAS FALSAS

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

## 4,4 MILHÕES DE DETECÇÕES

A categoria Notícias falsas segue como o terceiro meio de disseminação de links maliciosos. Quando comparado ao trimestre anterior, as chamadas fake news tiveram um aumento de 50,6% no número de registros realizados pelo dfndr lab, saltando de 2,9 milhões para 4,4 milhões entre o primeiro e segundo trimestre de 2018.

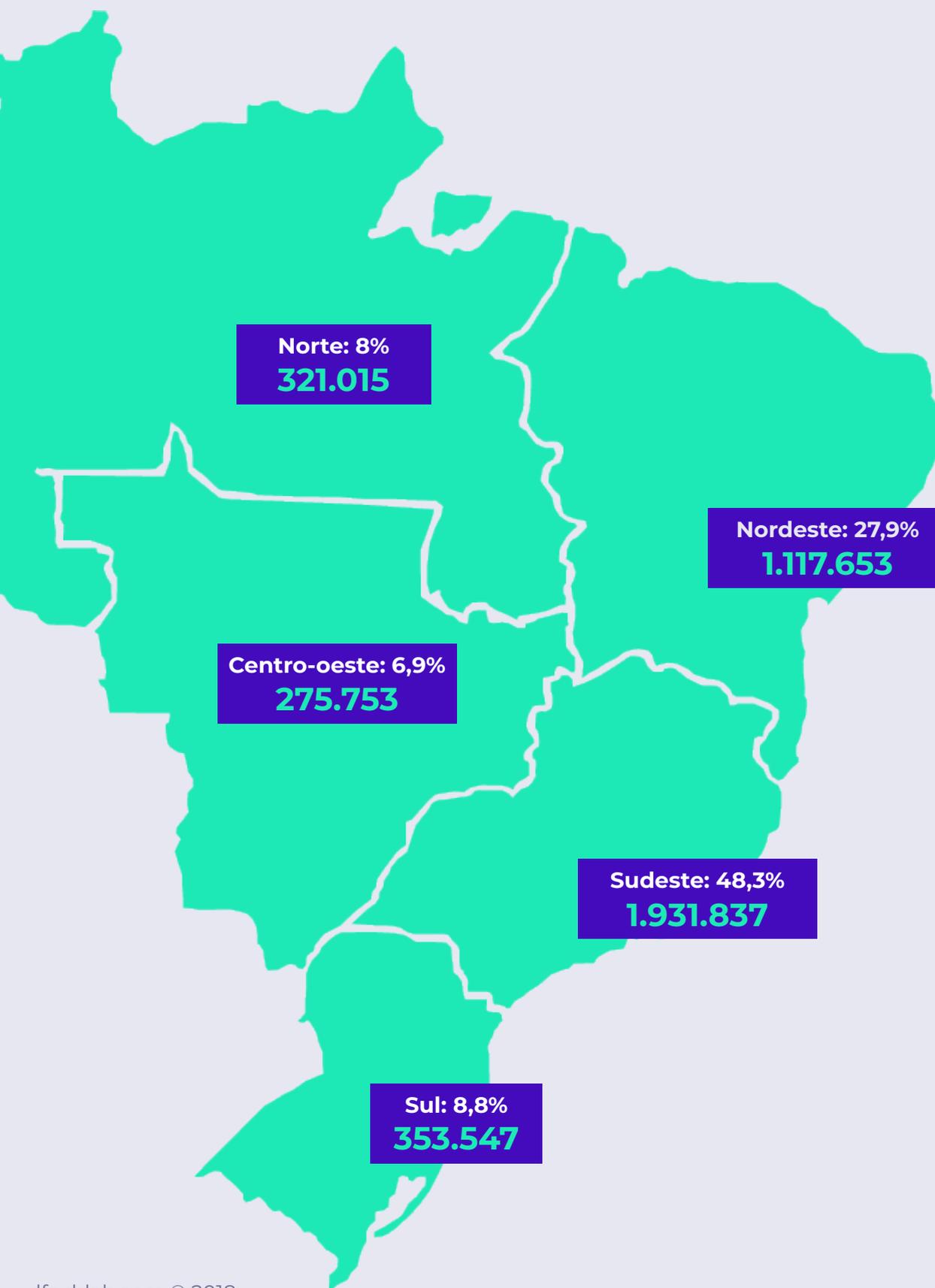


### Notícias falsas

#### Total de detecções de Notícias falsas no Brasil



**Região Sudeste** foi responsável por **48%** do total de detecções de **Notícias falsas** no trimestre



# TOP 5

## NOTÍCIAS FALSAS



# 1

### SOLICITE SEU CARTÃO ONLINE

Os conteúdos mais compartilhados no período prometiam crédito facilitado e livre de burocracias ou pagamento de anuidade.

## 1,1 MILHÃO DE DETECÇÕES



# 2

### STJ AUTORIZA CANCELAMENTO DE CNH EM CASO DE IPVA ATRASADO

Para impedir o avanço desta suposta medida, o texto pedia que os leitores assinassem uma falsa petição e compartilhassem o link.

## 830,9 MIL DETECÇÕES



# 3

### NOVO DIPIRONA IMPORTADO DA VENEZUELA PARA O BRASIL CONTÉM VÍRUS

Em tom alarmista, o conteúdo citava o nome do vírus e o número do lote do remédio que estaria contaminado, com objetivo de gerar medo na população.

## 612,5 MIL DETECÇÕES

4

## PABLO VITTAR GANHA PROGRAMA INFANTIL NA GLOBO

A falsa matéria anunciava Pablo Vittar apresentando uma nova atração infantil, supostamente intitulada “TV Criança Gay”, nas manhãs da emissora.

442,4 MIL DETECÇÕES



5

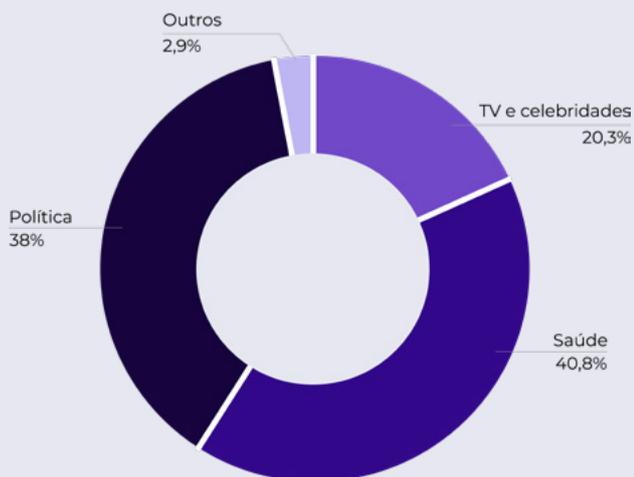
## NOVA NOVELA DA GLOBO TERÁ CASAMENTO ENTRE AVÔ E NETA

Utilizando-se da popularidade do ator José de Abreu, a notícia falsa dava como certa sua participação na suposta trama que retrataria a pedofilia.

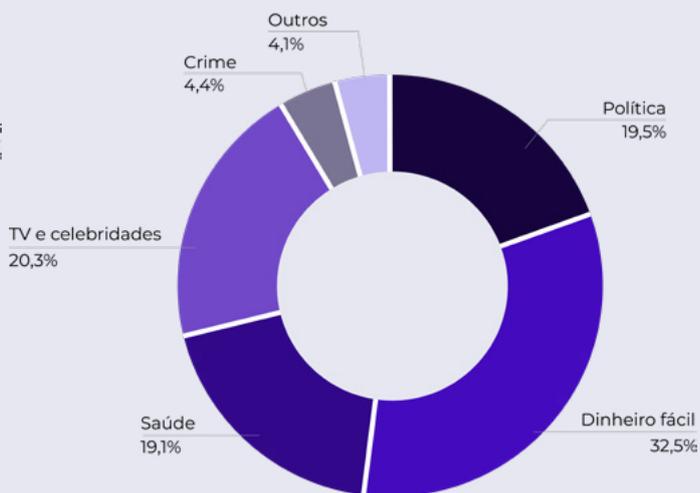
316,1 MIL DETECÇÕES

**Dinheiro fácil** foi o assunto que gerou mais detecções no 2º trimestre

1º trimestre de 2018



2º trimestre de 2018



# O papel do dfndr lab na identificação de notícias falsas

O dfndr lab tem investido em tecnologias proprietárias, baseadas em inteligência artificial e humana, para aumentar sua capacidade de alertar sobre notícias falsas. Os computadores 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 segunda 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, acessível ao público no site do dfndr lab, todo link submetido passa pelo processo de análise do conteúdo, primeiramente pelos computadores do laboratório, e em seguida pela equipe de especialistas.

## 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, mais probabilidade há de que atinja um alto número de acessos e compartilhamentos na rede.

As notícias falsas também apresentam construções de texto similares, com pontos-chave que podem comprovar que o seu conteúdo é irreal. Desta forma, verificar a existência desses pontos-chave pode ajudar a não cair nas “Fake News”.

# Os bastidores da Copa

Faltando poucos dias para o início da Copa do Mundo, os primeiros ciberataques relacionados ao evento começaram a surgir. Este comportamento já era previsto pelo time do dfndr lab, uma vez que os hackers costumam se aproveitar de eventos de grandes proporções, como os Jogos Olímpicos e outras datas comemorativas, para promover golpes.

Durante a Copa, no entanto, um novo fato chamou a atenção: muitos sites falsos identificados eram, rapidamente, tirados do ar. Para driblar a situação, os criminosos utilizaram diversos links para divulgar os mesmos ataques. Foram mais de 6 milhões de detecções em 69 links maliciosos diferentes.

Dentre os assuntos mais detectados pela equipe do dfndr lab estiveram os falsos sorteios de camisas da Seleção, responsáveis por 98,1% das mais de 6 milhões de detecções; falsos sorteios usando nomes de patrocinadores da Copa; e links de falsos sites de e-commerce prometendo produtos com descontos. Em todos os casos, os homens foram os principais alvos dos hackers.

**6.005.492**

Detecções de golpes  
relacionados a Copa

Quantidade de golpes  
relacionados a Copa

**69**

## Detecções por assunto

Sorteio de camisa da Seleção

**5,8** milhões

**113,3** mil

Sorteios usando nome  
de patrocinador

Produtos com desconto

**872**

## Detecções por gênero

**Homens** **Mulheres**

**71.5%**

**28.5%**



## DELEGADO MARCO ANTÔNIO ARRUDA GUNS

*Delegacia de Repressão aos Crimes Informáticos  
Polícia Civil do Estado do Rio Grande do Sul  
Departamento Estadual de Investigações Criminais*

**“Vítimas devem sempre procurar as delegacias de Polícia Civil”**

### **1) Quais os principais tipos de queixas cibernéticas que vocês recebem?**

Os crimes cibernéticos estão divididos em duas modalidades: próprios e impróprios. Os próprios são aqueles que decorrem da atividade cibernética diretamente, tais como ransomware, malware, entre outros. Os impróprios são os que utilizam das plataformas digitais para cometer crimes, como estelionato, difamação, compra fraudulenta em falsos sites de venda, boletos falsificados, divulgação de fotos íntimas, entre outros. Hoje, aqui na delegacia, praticamente 99% dos casos que atendemos são de crimes cibernéticos impróprios. A baixa quantidade de notícias de crimes cibernéticos próprios acontece porque, na maioria dos casos, as vítimas preferem buscar ajuda técnica para solucionar o problema. Além disso, como muitas vítimas são empresas/instituições, há uma tentativa de preservação da marca e, por isso, não são registrados os fatos em boletim de ocorrência policial.

### **2) Quais as estratégias mais comuns utilizadas por cibercriminosos para enganar as vítimas?**

No caso dos crimes impróprios, os infratores se escondem, muitas vezes, atrás de perfis falsos para difamar e ludibriar suas vítimas. Já no caso de crimes próprios, os criminosos em geral se valem de vulnerabilidades existentes para invadir sistemas de empresas, bancos, instituições e até mesmo de usuários finais.

### **3) Como as pessoas devem se prevenir para não cair em golpes na internet?**

Algumas dicas seriam:

- Cuidado com a exposição excessiva. É importante que as pessoas saibam que quanto mais elas expõem suas vidas e rotinas na internet, mais suas informações ficam expostas também para criminosos;
- Desconfie das coisas. Não é normal que uma TV que custa R\$ 1.000,00 seja vendida por R\$ 200,00;
- Não seja ingênuo. Empresas, bancos e instituições sempre avisam quais são os canais por onde se comunicam com os clientes. Não acredite que uma comunicação via e-mail, telefone ou SMS é verdadeira sem antes checar;
- Tenha sempre a melhor proteção de segurança que puder. Se prevenir, reduzindo ao máximo as vulnerabilidades, é sempre a melhor arma.

#### **4) O que um usuário deve fazer, caso tenha caído em algum golpe na internet?**

As vítimas devem sempre procurar as delegacias de Polícia Civil e registrar em ocorrência policial o crime, para que seja aberta uma investigação para buscar os criminosos envolvidos.

#### **5) Vocês costumam receber queixas específicas ligadas a grandes eventos?**

Sim. Quando há shows locais importantes, vemos muitos casos de aplicativos e sites atacados por criminosos para fraudar senhas, gerar boletos falsos e, assim, enganar as vítimas.

**dfndr lab**  
dfndrlab.com