Relatório da Segurança Digital no Brasil

Terceiro trimestre - 2017

DFNDR Lab

O primeiro relatório apresentado pelo DFNDR Lab, referente ao terceiro trimestre do ano, traz informações sobre a evolução e a sofisticação dos ataques que utilizam, cada vez mais, metodologias de engenharia social para ganhar escala. Veja os principais destaques:

Os ciberataques totais cresceram

44%

entre o segundo e terceiro trimestre de 2017

Crescimento de ciberataques via malware

3,7 milhões → **5,5** milhões

salto acima de

49%

entre os dois trimestres

Crescimento de ciberataques via links maliciosos

45,7 milhões → **65,7** milhões

um salto de quase

44%

entre os dois trimestres

Os dados mostram que links maliciosos já são 12 vezes mais usados em ataques do que malwares

GUERRA EPIDÊMICA

O objetivo do Relatório da Segurança Digital no Brasil é fornecer à sociedade — cidadãos, empresas e instituições — uma fotografia do status da guerra cibernética no país.
Em sua primeira edição trimestral, o DFNDR Lab identificou um preocupante crescimento de aproximadamente 44% no volume de ciberataques ocorridos entre o segundo e terceiro trimestres de 2017. Mais que apenas números, os ciberataques têm evoluído em sofisticação, alvos e metodologias, dando ao cenário contornos epidêmicos.

O DFNDR Lab identificou um preocupante crescimento de 44% no volume de ciberataques ocorridos entre o segundo e terceiro trimestres de 2017

Historicamente, hackers mantiveram empresas privadas e órgãos públicos como alvos preferenciais. E há lógica nesta seleção, já que empresas privadas podem proporcionar maiores lucros com ciberataques pontuais, e órgãos públicos detêm informações confidenciais que podem desestabilizar a ordem institucional, gerando conflitos, enfraquecendo esforços diplomáticos e influenciando mercados. Contudo, empresas privadas e os órgãos públicos em geral possuem melhores mecanismos de defesas que usuários comuns da internet, o que para os hackers aumenta o risco de exposição e eventual prisão. Ao mirarem em pessoas, esse risco diminui muito.

O DFNDR Lab foi capaz de detectar um ciberataque via malware por segundo — num total de mais de 2 milhões de vítimas

No segundo trimestre de 2017, o número de detecções de links maliciosos foi de 45,72 milhões. O mesmo número saltou para 65,78 milhões no terceiro trimestre

Porém, para que ciberataques a usuários comuns sejam lucrativos, é preciso quantidade e escala. E é aí que os métodos de engenharia social e o aperfeiçoamento dos códigos computacionais aplicados cumprem um papel importante na lógica da expansão do lucro. Esses métodos fazem com que as vítimas compartilhem o código malicioso com sua família e amigos. Um simples link falso prometendo descontos na compra de um produto, por exemplo, se espalha em redes sociais e em aplicativos de conversa com velocidade viral. Para ser vítima, basta um toque. Hackers sabem disso e estão explorando a confiança que pessoas têm umas nas outras dentro de seus círculos sociais.

Vetores de ataque e infecção

De acordo com os 14.4 terabytes de dados processados pelo DFNDR Lab no terceiro trimestre de 2017, há dois vetores de ciberataques em destaque no Brasil. De um lado, malwares classificados como vírus, trojans e worms. De outro, links maliciosos, phishing e golpes diversos. Embora os malwares tenham crescido em proporções maiores, em números absolutos foram os links maliciosos que mais escalaram.

Do segundo para o terceiro trimestre, a exposição a malwares aumentou 49%, subindo de 3,74 milhões para 5,58 milhões de detecções. Ao longo de julho, agosto e setembro, o DFNDR Lab foi capaz de detectar um ciberataque via malware por segundo — num total de mais de 2 milhões de vítimas.

Mas é a viralização de links maliciosos que torna o quadro brasileiro ainda mais crítico. Eles somam mais de 12 vezes a quantidade total de infecções de malware no país. No segundo trimestre de 2017, o número de detecções de links maliciosos foi de 45,72 milhões. O mesmo número saltou para 65,78 milhões no terceiro trimestre, um avanço de 43,86% em apenas três meses.

A análise cruzada desses números com os hábitos de consumo de conteúdo digital no país demonstra que o usuário brasileiro é muito suscetível aos ciberataques de engenharia social. De acordo com o relatório anual *We Are Social* de 2017, produzido pelo Hootsuite, os brasileiros estão na segunda posição mundial tanto em tempo de uso de internet em telefones celulares (3 horas e 56 minutos por dia), como em tempo de acesso a redes sociais (3 horas e 43 minutos por dia). É exatamente o alto engajamento do usuário brasileiro em curtidas, comentários e compartilhamentos em redes sociais como Facebook, Twitter e em apps de comunicação como WhatsApp e Facebook Messenger que torna os ataques de engenharia social tão virais no país.

Emílio Simoni
Diretor do DFNDR Lab

Sobre o LABORATÓRIO

O DFNDR Lab é um time global de *white hat hackers* com vasta experiência e conhecimento técnico em segurança digital. Sua missão é contribuir para que todos possam se conectar, expressar, compartilhar e navegar com liberdade e segurança. O laboratório conta com tecnologias proprietárias baseadas em inteligência artificial e *machine learning* (capacidade programada para que computadores aprendam sozinhos a melhorar o desempenho de suas funções) — nas suas funções de detecção, análise, previsão e prevenção contra ataques cibernéticos. Cerca de 200 milhões de arquivos digitais são processados, analisados e indexados diariamente pelos sistemas do DFNDR Lab e estão a serviço de todos de maneira gratuita.

O Relatório da Segurança Digital no Brasil, do DFNDR Lab, é baseado na coleta de dados sobre detecções e bloqueios de ciberataques aos celulares Android dos mais de 21 milhões de usuários dos aplicativos de segurança DFNDR. A análise foi realizada entre os dias 01 de julho de 2017 e 30 de setembro de 2017.

Total de acessos a links maliciosos NO BRASIL

2º trimestre:

45,72

milhões

3º trimestre:

65,78

milhões

Crescimento de

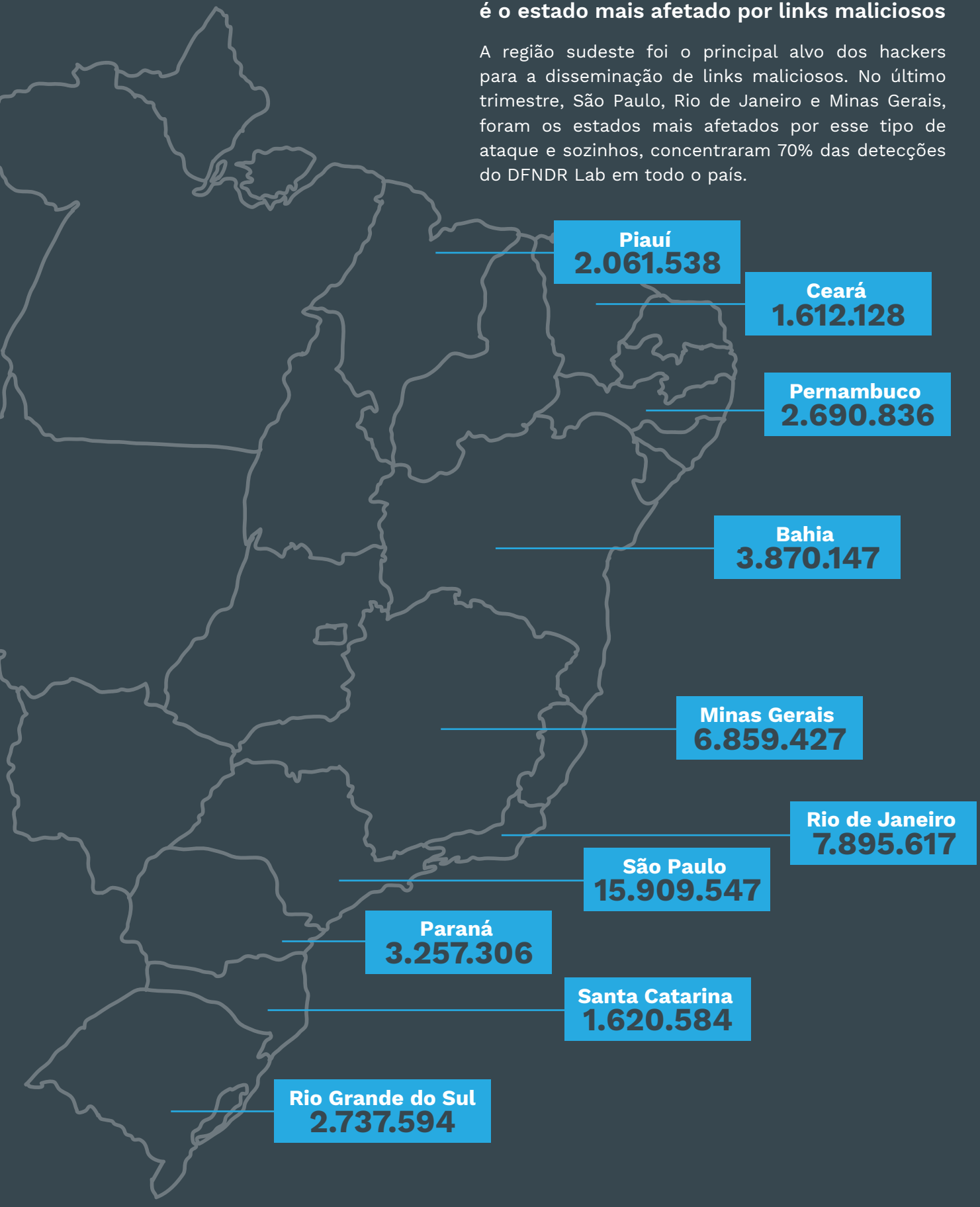
43,86%

Brasileiros acessaram, em média, 9,6 links maliciosos por segundo no 3º trimestre

SÃO PAULO

é o estado mais afetado por links maliciosos

A região sudeste foi o principal alvo dos hackers para a disseminação de links maliciosos. No último trimestre, São Paulo, Rio de Janeiro e Minas Gerais, foram os estados mais afetados por esse tipo de ataque e sozinhos, concentraram 70% das detecções do DFNDR Lab em todo o país.

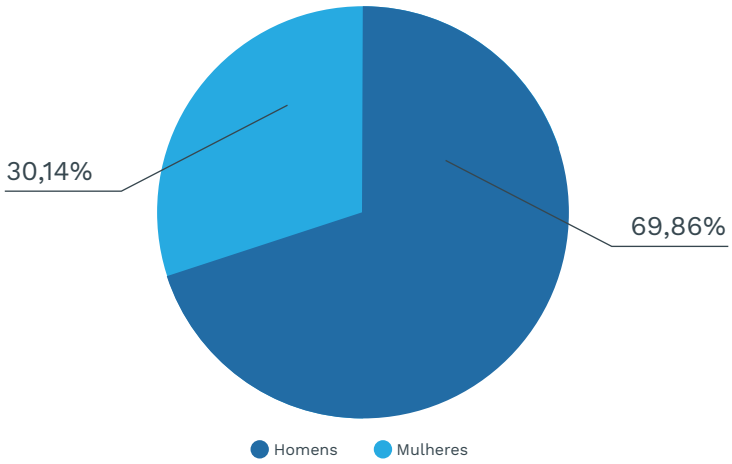


Homens

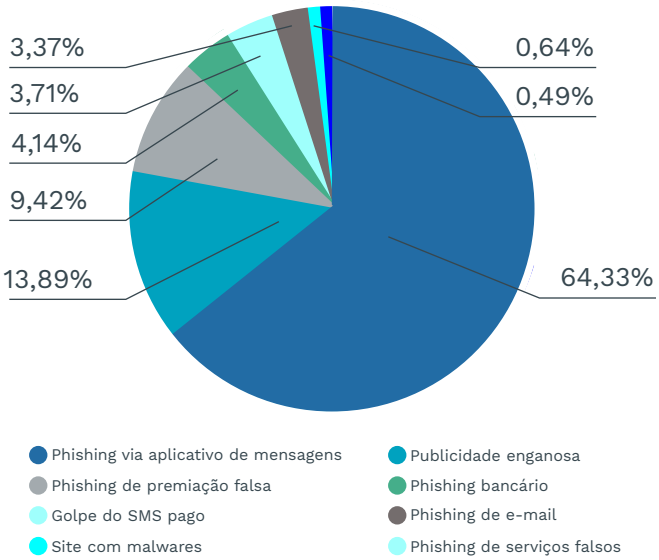
clicam mais em links maliciosos que mulheres

No último trimestre, 69,86% dos acessos a links maliciosos foram realizados por homens contra 30,14% por mulheres. Por outro lado, os dois sexos responderam da mesma forma aos diferentes tipos de ataque. Phishing via aplicativos de mensagens ainda é o principal responsável por atrair vítimas.

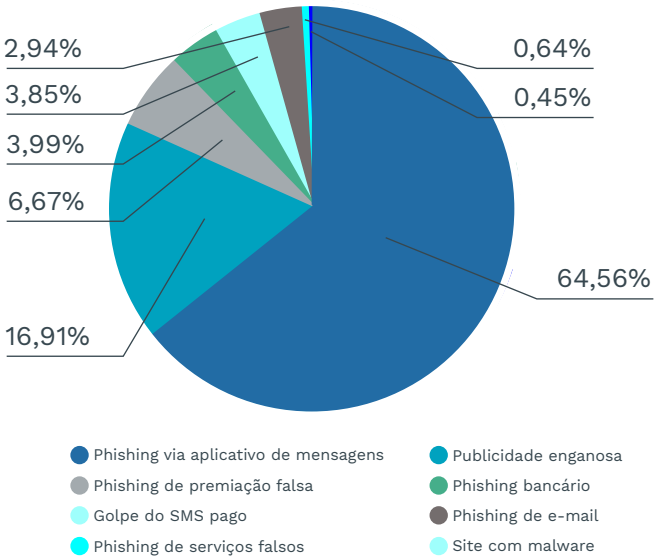
Cliques por gênero



Tipos de links acessados - Mulheres



Tipos de links acessados - Homens



Links MALICIOSOS
detectados no Brasil

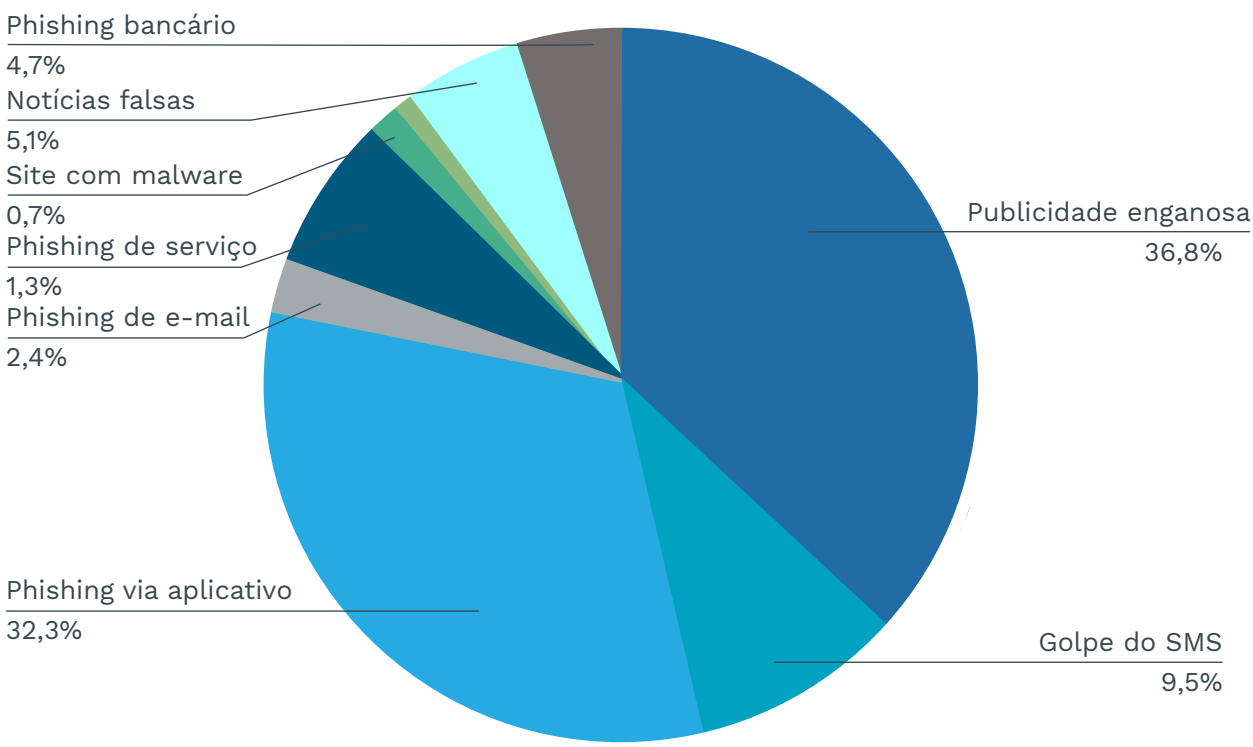
Total de links maliciosos

JULHO
14.092.026

AGOSTO
24.306.873

SETEMBRO
27.342.028

Principais tipos de links maliciosos



1 Falsos alertas de vírus e propaganda enganosa

24,19 milhões
de ataques

Um dos principais problemas do mercado de publicidade mobile, as propagandas enganosas representaram, no terceiro trimestre, mais de 35% de todos os ataques de links maliciosos no Brasil. Buscando ganhar dinheiro de empresas de forma fraudulenta, os hackers criam anúncios fingindo ser propagandas reais de aplicativos e forçam as vítimas a instalarem esses aplicativos. Com isso, os cibercriminosos recebem dinheiro pelas instalações, sem que as empresas tomem ciência.

Apesar de ainda ser o principal meio de golpe por links maliciosos, os falsos alertas de vírus e propagandas enganosas apresentaram, no terceiro trimestre do ano, uma redução de 7,44% em relação ao período anterior, resultado das novas políticas de controle de publicidade do Google em conjunto com os departamentos de marketing dos aplicativos mais baixados do mundo, que trabalham em parceria para banir essa prática fraudulenta do mercado.

2 Phishing via aplicativo de mensagens

21,24 milhões
de ataques

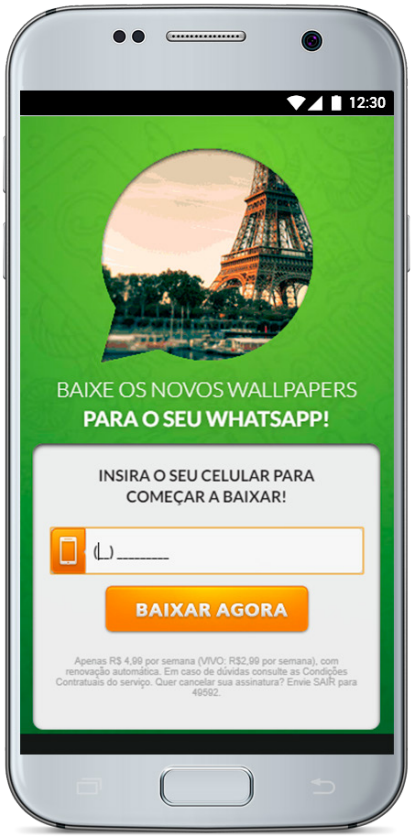
No segundo trimestre deste ano, o DFNDR Lab registrou 2,06 milhões de detecções de golpes que envolvem compartilhamentos via aplicativos de mensagens, como o WhatsApp. No último trimestre, este número saltou para 21,24 milhões, o que representa um expressivo crescimento de 830%.

Para viralizar esses ataques, hackers geralmente se aproveitam de nomes de celebridades ou marcas famosas para atrair a vítima, que é levada a fornecer dados e, em seguida, a compartilhar o link malicioso com seus contatos. Na maior parte das vezes, ela é cadastrada indevidamente em um serviço de SMS pago e, a cada assinatura, criminosos recebem dinheiro. Em setembro, hackers usaram o nome da marca O Boticário para promover um vale-presente falso de R$ 150 reais. O potencial de viralização foi tão alto que o link atingiu mais de 1 milhão de acessos em menos de 24 horas. Ao todo, foram mais de 1,4 milhão de acessos à fraude.

3 Golpe do SMS Pago

6,24 milhões
de ataques

O terceiro tipo de link malicioso mais acessado pelos brasileiros ocorre, geralmente, ao final de outros ataques, como o phishing via aplicativo de mensagem. O hacker vincula-se a um serviço legítimo de SMS pago - por exemplo, que oferece papéis de parede para customizar o celular ou mensageiros - e o criminoso ganha dinheiro a cada assinatura. O golpe causa grande prejuízo às vítimas pelo fato que, muitas vezes, os valores desses serviços são abusivos e o cadastro pode ocorrer de forma automática a qualquer pessoa que acessar o link.



ATENÇÃO!

Notícias falsas

3,35
milhões de ataques

Diferente da maioria dos golpes, o dano ao usuário neste caso não é financeiro. A intenção dos links maliciosos com notícias falsas é, em sua maioria, aumentar o número de acesso a determinada página para gerar visibilidade aos anúncios ali publicados. Assim como os falsos alertas de vírus e propaganda enganosa, neste caso os anunciantes são as grandes vítimas. A forma utilizada para atração das pessoas é a disseminação de manchetes sensacionalistas e absurdas, que não entregam nenhum conteúdo verdadeiro ao leitor.

Notícias falsas com maior número de detecção

Melhor do que Viagra? Chega ao Brasil o Fênomeno em Vendas nos EUA que Está Dando o Que Falar

Dois doutores vencedores do prêmio Nobel desenvolvem um suplemento que recupera a ereção de mais de 5 mil pessoas

1.184.318 bloqueios

brasilia-esta-para-ser-tomada-congresso-sera-ocupado-leiam-aqui

por João Guilherme
29 de julho de 2017, 15:01
2.1k Views

117.419 bloqueios

IMPORTANTE! Novo dipirona importado da Venezuela para o Brasil contêm vírus!

Rádio Nacional de Venezuela: AVISO URGENTE!

825.071 bloqueios

Malware

2º trimestre:
3,74
milhões

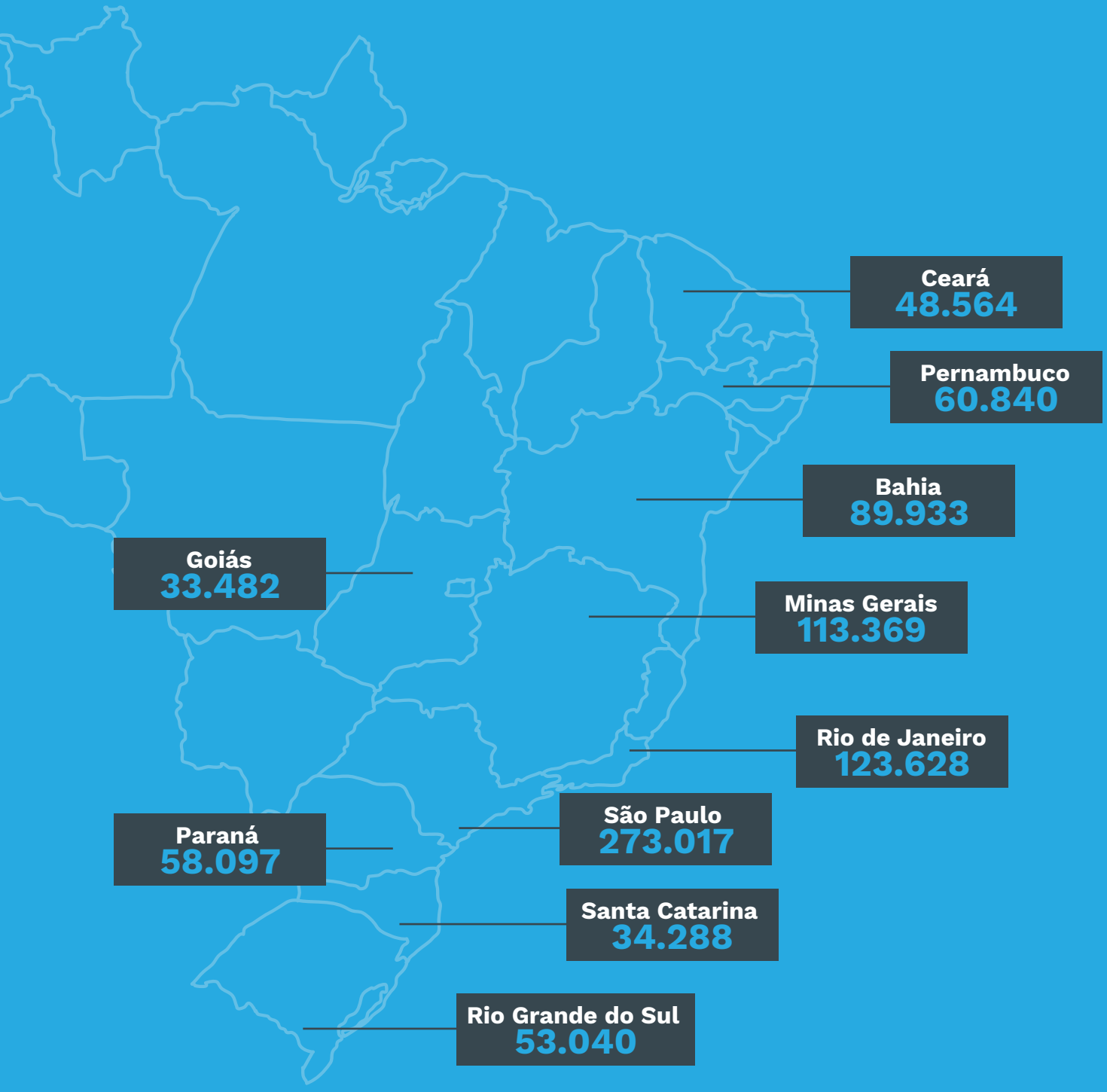
3º trimestre:
5,58
milhões

Crescimento de
49,01%

**O DFNDR Lab detectou, em média,
um malware por segundo no 3º trimestre**

Região Sudeste é a mais afetada

Região com a maior concentração de smartphones do país, o Sudeste é, também, o principal alvo dos ataques de malwares, com mais de 510 mil casos. O estado mais afetado foi São Paulo, com 273.017. Logo atrás do Sudeste, a Região Nordeste aparece representada pelos estados da Bahia (83.933) e Pernambuco (60.840).



MALWARES
detectados no Brasil

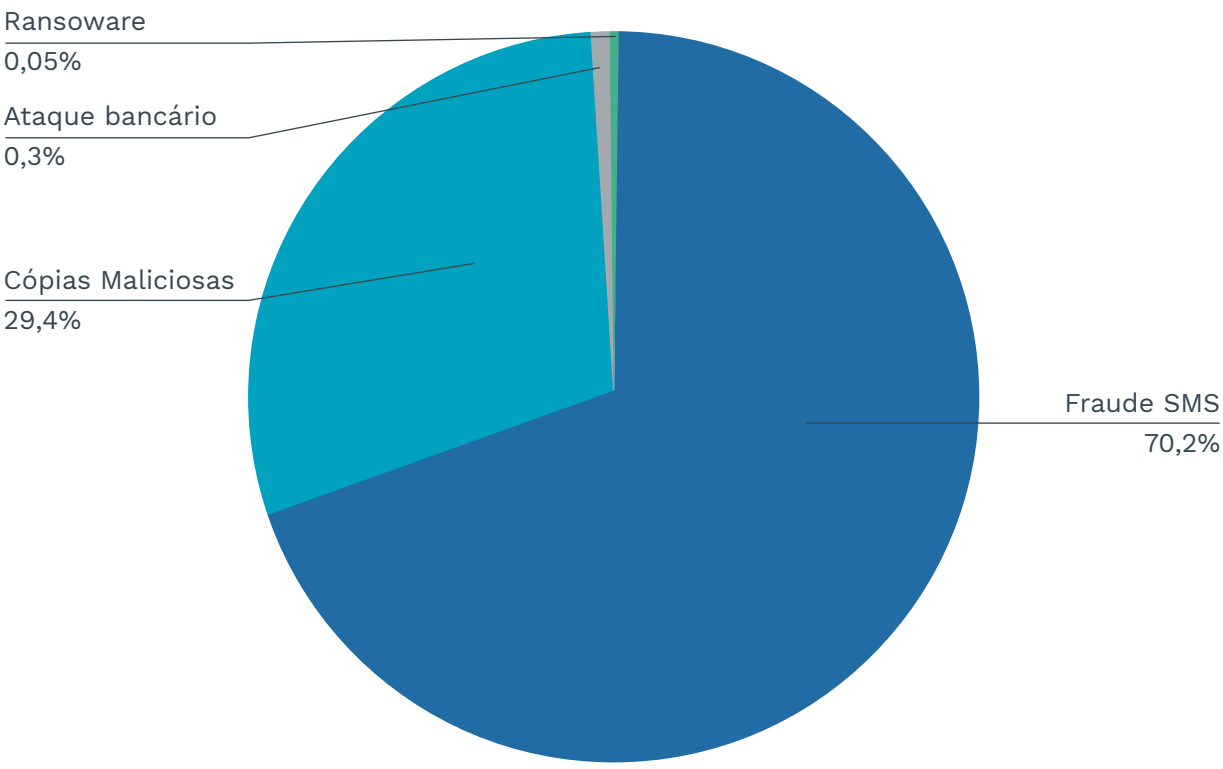
Total de malwares

JULHO
1.633.043

AGOSTO
2.106.341

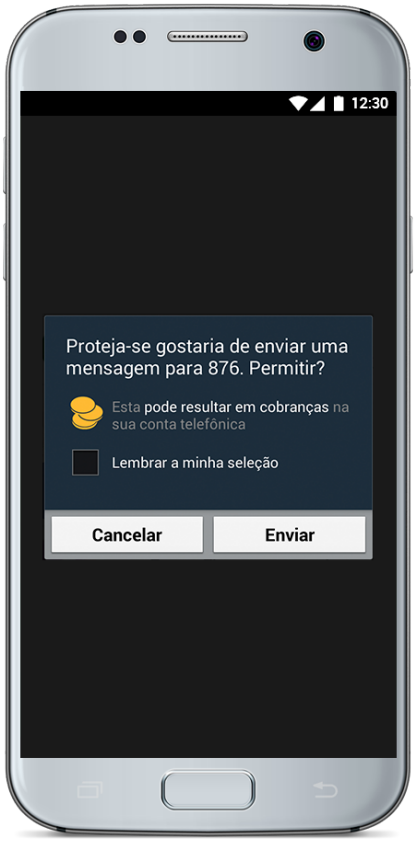
SETEMBRO
1.846.730

Principais tipos de malwares



1 Fraude SMS

3,5 milhões
de ataques

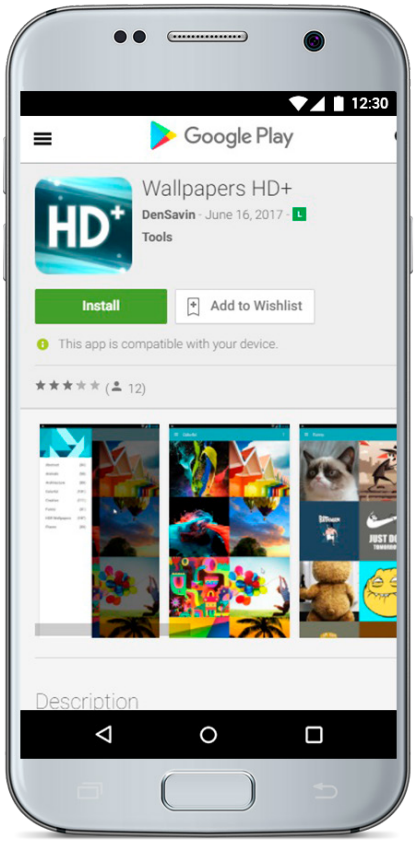


Fácil de ser elaborado e inserido em lojas de apps, este tipo de malware consiste em simular um aplicativo já existente. Quando o usuário finaliza seu download, automaticamente um serviço pago de SMS é ativado e parte do valor é enviado para o hacker. Em um primeiro momento, a vítima pode acreditar que o aplicativo apenas tem algum bug, por não funcionar. O ataque provavelmente só será identificado quando a vítima conferir a fatura mensal do celular pós-pago ou o saldo de créditos do celular pré-pago.

O destaque do último trimestre nesta categoria foi um falso aplicativo chamado Proteja-se, que simulava pertencer a uma operadora de telefonia. Distribuído em lojas não oficiais de download de apps, o malware infectou cerca de 28 mil dispositivos.

2 Cópia Maliciosa

1,47 milhão
de ataques



Diferente da maioria dos malwares, esta categoria não causa, necessariamente, dano ao usuário. Seu principal foco é se passar por um aplicativo real para que, depois de instalado, que mostre propagandas de forma excessiva ao usuário. O principal intuito do hacker com isso é ganhar, de forma fraudulenta, dinheiro de empresas por meio da exibição ilegal de anúncios em seus nomes. Assim como os malwares de Fraudes SMS, as Cópias Maliciosas são mais fáceis de se instalar em lojas o ciais de aplicativos.

Entre os apps falsos identificados pelo DFNDR Lab na Play Store, estão: Call Recorder, HDR Wallpapers, Girls HD, Girls Collection, Wallpapers HD+, SmartRingtones Lite, entre outros.

3 Ataques Bancários

14 mil ataques

Multifacetado e praticamente invisível, este tipo de malware infecta dispositivos por meio de e-mails, sites maliciosos ou lojas de aplicativo não-oficiais. Ao se instalarem no smartphone da vítima, podem criar telas que se sobrepõem à tela atual de outros apps ou enviar uma solicitação de cadastro para conseguir coletar dados financeiros, como números de cartão de crédito ou credenciais bancárias. Um malware deste tipo é capaz de monitorar e se sobrepor a mais de 200 apps diferentes.

ATENÇÃO!

GOLPE DELIVERY!

Em agosto, o time de especialistas do DFNDR Lab identificou, na Google Play, um malware de ataque bancário que simulava o app James Delivery, popular no segmento de entregas no Sul do país. O golpe, desenvolvido por um hacker brasileiro (pessoa física), levava o usuário a cadastrar seus dados pessoais, assim como informações financeiras para pagamento no app (compras via cartão de crédito). Ao fazer o cadastro, o usuário era redirecionado para uma página de erro. Neste momento, no entanto, o hacker já possuía as informações necessárias para aplicar golpes financeiros. Este mesmo hacker desenvolveu e distribuiu apps - potencialmente maliciosos - que chegavam a custar R$ 500 para o download.

Projeções E TENDÊNCIAS

Ao longo de todo o ano, o quarto trimestre é o mais crítico para a segurança digital. E, mais uma vez, isso se deve ao comportamento social explorado por hackers à exaustão: a escalada do consumo durante a Black Friday e o Natal.

Baseado nas análises de comportamento do público-alvo e nas curvas de tendência ao longo do ano, o DFNDR Lab projeta um aumento de quase 9 vezes (788,58%) em ciberataques com uso de links maliciosos no último trimestre de 2017, quando comparado ao mesmo período de 2016. Quando comparado ao terceiro trimestre deste ano, os mesmos ataques devem praticamente dobrar para 112.05 milhões, a partir dos 65.78 milhões entre julho e setembro últimos.

Ataques com links maliciosos em 2017

Aferidos

Julho	14.10 milhões
Agosto	24.32 milhões
Setembro	27.36 milhões

TOTAL: 65.78 milhões

Projetados

Outubro	31.12 milhões
Novembro	43.57 milhões
Dezembro	37.35 milhões

TOTAL: 112.05 milhões

1 Phishing via aplicativos de mensagem

24,17 milhões

de ataques em 2017

Um dos tipos de links maliciosos mais acessados no último trimestre é também tendência para os próximos meses. Nesse caso, hackers criam ofertas falsas às quais usuários têm acesso somente após informarem dados pessoais. Elas são disseminadas especialmente via WhatsApp e Facebook Messenger e, geralmente, requerem compartilhamento com amigos, induzindo a viralização do golpe. Um método bastante usado é o de exigir o número do celular da vítima para a obtenção do benefício enquanto, na verdade, o que está sendo ativado é um serviço de SMS pago que irá ser debitado da sua conta telefônica ou de seus créditos pré-pagos.

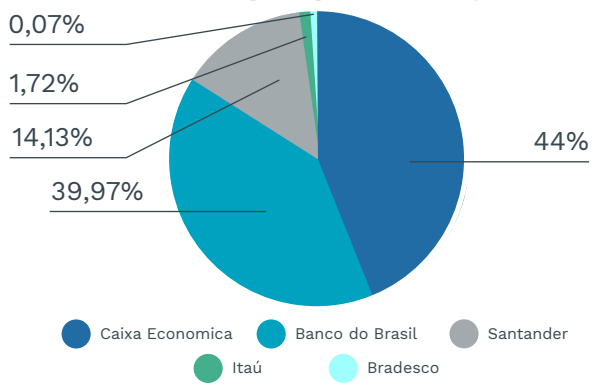
2 Phishing bancário

3,73 milhões

de ataques em 2017

Nesta modalidade, hackers criam websites falsos, iguais às páginas de instituições bancárias. Sem perceber, o correntista acaba digitando suas credenciais como tokens, senhas, números da conta e dados de cartão de crédito. Ao completar o preenchimento, é comum que o website passe a imitar uma condição de baixa velocidade na conexão ou simplesmente de travamento, fazendo com que o correntista recarregue a página sem notar que já foi roubado.

Percentual de ataques por instituição bancária



NOVA TENDÊNCIA

Phishing de perfil falso no Facebook

Para induzir consumidores ao erro e aplicar golpes que causam prejuízos financeiros, hackers estão utilizando a principal rede social do país, o Facebook. Os criminosos criam páginas e perfis falsos de grandes empresas varejistas do mercado (Pontofrio, Casas Bahia, Americanas.com, entre outros), promovendo falsas ofertas atrativas.

Ao clicar no link da falsa oferta, o usuário é encaminhado para realizar a compra em uma página que imita o site oficial da empresa. Uma vez que o usuário tenta realizar o pagamento e insere seus dados na página, o hacker tem acesso a informações pessoais e financeiras da vítima. Para dar ainda mais credibilidade ao perfil falso no Facebook, os cibercriminosos simulam comentários elogiosos à empresa postados na página.

DFNDR Lab

DFNDRlab.com