# Relatório da Segurança Digital no Brasil

Quarto trimestre - 2017

DFNDR Lab

O segundo relatório divulgado pelo DFNDR Lab apresenta uma estabilidade no volume de ciberataques ocorridos entre o terceiro e o quarto trimestre de 2017. Além disso, observa-se uma mudança de olhar vinda das grandes empresas para a segurança digital. Veja os principais destaques:

## Total de ciberataques

**70** milhões

**66,1** milhões
de ciberataques
via links maliciosos

**3,1** milhões
de ciberataques
via malware

## Crescimento de ciberataques de Phishing via aplicativo de mensagens

**21,3** milhões ▶▶ **44,1** milhões

salto de

**107%**

entre o terceiro e o quarto trimestre

## Links maliciosos foram **17 vezes** mais usados do que malwares

# CONTRA-ATAQUE

O ano de 2017 foi marcado por uma grande guerra cibernética no Brasil. De um lado, cidadãos, empresas e instituições. De outro, cibercriminosos. Ao todo, foram detectados mais de 205 milhões de ciberataques no país.

A segunda edição trimestral do Relatório da Segurança Digital no Brasil do DFNDR Lab apresenta uma estabilidade no volume de ciberataques ocorridos entre o terceiro e o quarto trimestre. Os números permanecem significativos, com uma redução de 1,8% nas detecções totais, e os principais vetores de ciberataques no último trimestre do ano seguem sendo links maliciosos - phishing e golpes diversos - e malwares - classificados como vírus, trojans e worms.

## Ao todo, foram detectados mais de 205 milhões de ciberataques no país

Os dados processados pelo DFNDR Lab apontam que, embora os links maliciosos tenham tido um aumento de apenas 0,6% entre o terceiro e o quarto trimestre, eles foram 17 vezes mais usados em ataques do que malwares. Já o número de detecções de malwares sofreu uma redução de 30,1%, saindo de 5,6 milhões no terceiro trimestre para 3,9 milhões no quarto trimestre. Um indício significativo de que os cibercriminosos estão migrando, gradativamente, os ataques de malwares para links maliciosos devido ao grande potencial de atrair mais vítimas em um curto período de tempo.

## Embora os links maliciosos tenham tido um aumento de apenas 0,6% entre o terceiro e o quarto trimestre, eles foram 17 vezes mais usados

## A PSafe, por exemplo, investiu, em 2017, R$ 3 milhões na expansão da sua infraestrutura de segurança, que cresceu de três para 26 servidores

Além disso, observa-se uma mudança de olhar vinda das grandes empresas para a segurança digital. Isso se confirma com os altos investimentos observados ao longo do ano. A PSafe, por exemplo, investiu, em 2017, R$ 3 milhões na expansão da sua infraestrutura de segurança, que cresceu de três para 26 servidores; e na construção de tecnologias proprietárias de anti-hacking, anti-malware e anti-phishing baseadas em inteligência artificial para aprimorar cada vez mais os métodos de detecção e bloqueio de ciberataques. Além disso, no quarto trimestre de 2017, o DFNDR Lab divulgou dez alertas de segurança junto a grandes veículos de comunicação do país para informar de forma ágil os brasileiros sobre o surgimento de novos golpes.

Outras grandes empresas, como Facebook e WhatsApp, também compraram a briga e se posicionaram a favor da segurança dos seus usuários durante o ano. O Facebook anunciou iniciativas para combater notícias falsas que circulam dentro da rede social. Já o WhatsApp informou que pretende implementar recursos que combatem correntes de spam e golpes compartilhados dentro do app de mensagens.

## Em dezembro de 2017, 1,4 bilhão de informações confidenciais furtadas por vários cibercriminosos ao longo dos últimos três anos foram vazadas na internet

E se por um lado as empresas estão buscando ampliar seus investimentos em segurança, do outro, cibercriminosos seguem desenvolvendo métodos para intimidar e reforçar a suscetibilidade das instituições e cidadãos aos seus métodos de ataque. Em dezembro de 2017, 1,4 bilhão de informações confidenciais furtadas por vários cibercriminosos ao longo dos últimos três anos foram vazadas na internet. Entre elas, haviam credenciais de acesso de domínios do governo brasileiro e dados de diversos cidadãos, que eram comercializados de forma fraudulenta na internet.

Por isso, é necessário que todos estejam cada vez mais atentos aos seus hábitos de consumo no mundo digital. Os usuários comuns, e não apenas as instituições, continuam sendo os alvos preferenciais dos cibercriminosos e estão expostas não só a golpes aplicados por meio de links maliciosos ou malwares, mas também ao furto, vazamento e comercialização das suas informações.

**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) — nos seus métodos 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.

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. Para apresentar dados demográficos como gênero, os algoritmos empregados na análise usam inúmeros critérios de comportamento para inferir volumes e percentuais. A análise foi realizada entre os dias 01 de outubro de 2017 e 31 de dezembro de 2017.


# Total de acessos a links maliciosos NO BRASIL em 2017

**3º trimestre:**

**65,7**

milhões

**4º trimestre:**

**66,1**

milhões

Crescimento de **0,6%**

**Brasileiros** acessaram, em média, **8 links maliciosos por segundo** no **4º trimestre**

# Links MALICIOSOS
## detectados no Brasil em 2017

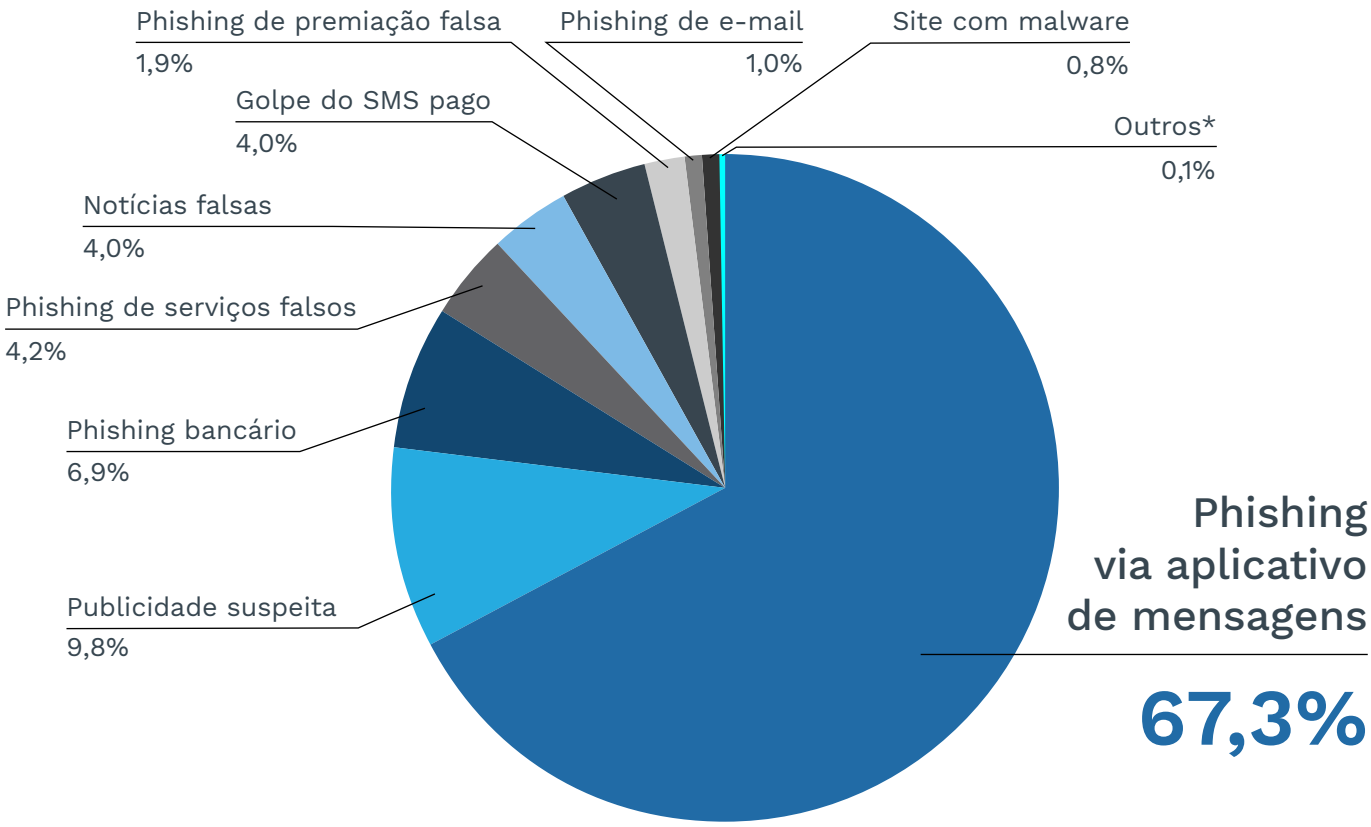
### Total de links maliciosos

**OUTUBRO**
**27.248.972**

**NOVEMBRO**
**23.499.211**

**DEZEMBRO**
**15.403.543**

## Principais tipos de links maliciosos

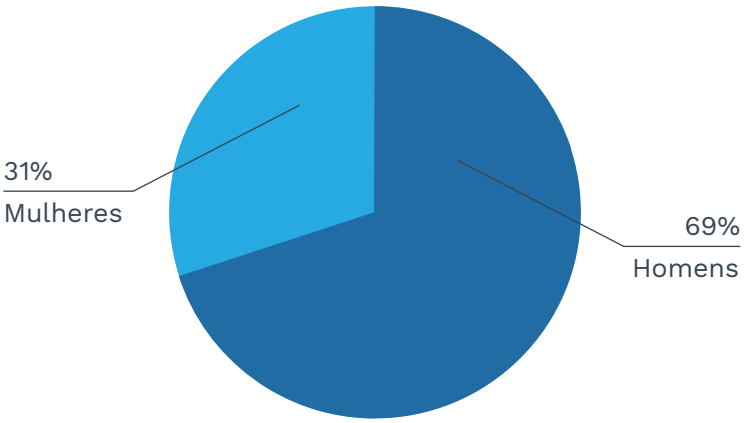



*Phishing genérico; Phishing de redes sociais; Phishing de perfil falso

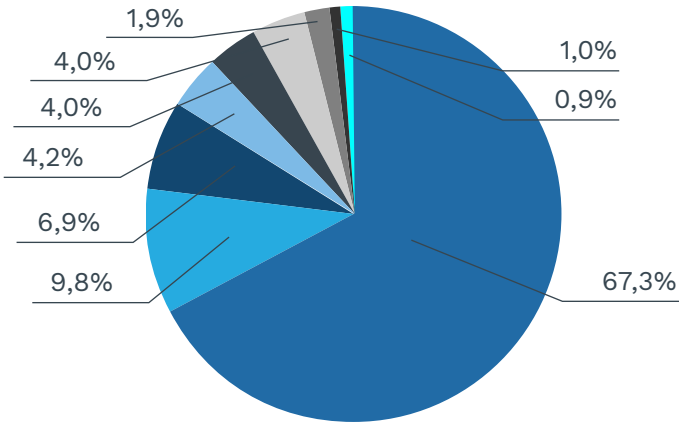
# Homens
acessam mais links maliciosos que mulheres

Assim como no trimestre anterior, a maior parte dos acessos (69%) do quarto trimestre de 2017 foram realizados por homens, enquanto 31% foram realizados por mulheres. Por outro lado, os dois sexos responderam de forma parecida aos diferentes tipos de ataque.

## Cliques por gênero

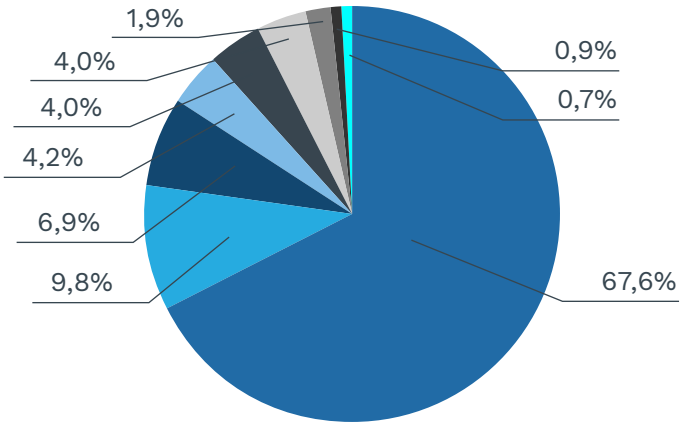



## Tipos de links acessados - Mulheres




- Phishing via aplicativo de mensagens
- Publicidade suspeita
- Phishing bancário
- Phishing de serviços falsos
- Notícias falsas
- Golpe do SMS pago
- Phishing de premiação falsa
- Phishing de e-mail
- Outros (Site com malware; Phishing genérico; Phishing de perfil falso; Phishing de redes sociais)

## Tipos de links acessados - Homens

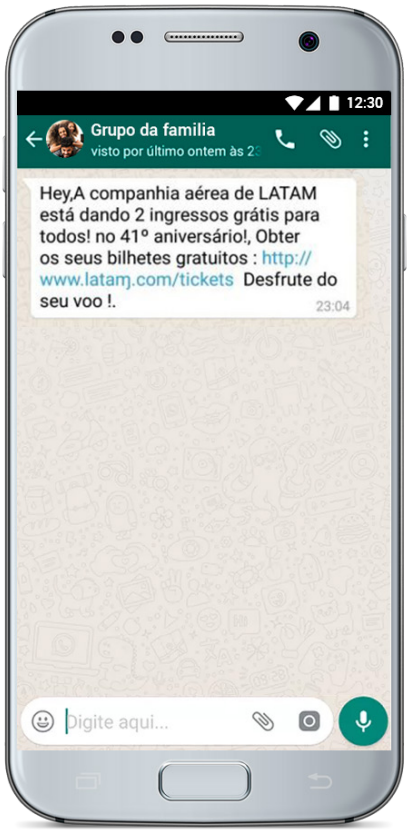



- Phishing via aplicativo de mensagens
- Publicidade suspeita
- Phishing bancário
- Phishing de serviços falsos
- Notícias falsas
- Golpe do SMS pago
- Phishing de premiação falsa
- Site com malware
- Outros (Phishing de e-mail; Phishing genérico; Phishing de perfil falso; Phishing de redes sociais)

# 1 Phishing via aplicativo de mensagens

## 44,1 milhões
de ataques

Compartilhamento de links maliciosos via aplicativos de mensagens foi o principal meio de disseminação de golpes no último trimestre de 2017. O número de detecções saltou de 21,3 milhões para 44,1 milhões entre o terceiro e o quarto trimestre do ano, totalizando um crescimento de 107%. O WhatsApp é o meio preferido para espalhar ataques, correspondendo a 66% do total de registros realizados pelo DFNDR Lab.

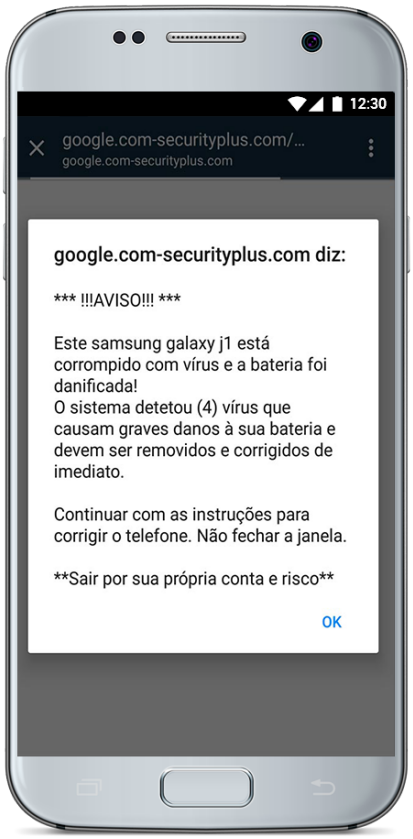



Os cibercriminosos utilizam iscas, geralmente com nomes de marcas e pessoas famosas, anunciando grandes promoções ou oferecendo brindes e vales-presente. A vítima, então, é induzida a responder perguntas, compartilhar o link falso com os seus contatos e, por fim, fornecer dados pessoais. Além de não receber a oferta prometida, ela pode ser levada a baixar aplicativos falsos, que poderão danificar e infectar seu celular com vírus ou ser cadastrada em serviços de SMS pago pelos quais, a cada assinatura, os hackers recebem dinheiro em troca.

# 2 Falsos alertas de vírus e Publicidade suspeita

## 6,3 milhões
de ataques

O quarto trimestre de 2017 foi o período do ano com o menor registro de ciberataques via Publicidade suspeita, totalizando 6,3 milhões de detecções.




Para ganhar dinheiro de forma ilegal, os cibercriminosos promovem serviços de empresas de forma fraudulenta, sem que essas organizações tomem ciência. A Publicidade suspeita, em geral, oferece produtos milagrosos ou afirma que o celular da vítima está infectado ou desatualizado, induzindo-a a baixar apps, contratar serviços ou até mesmo informar dados pessoais.

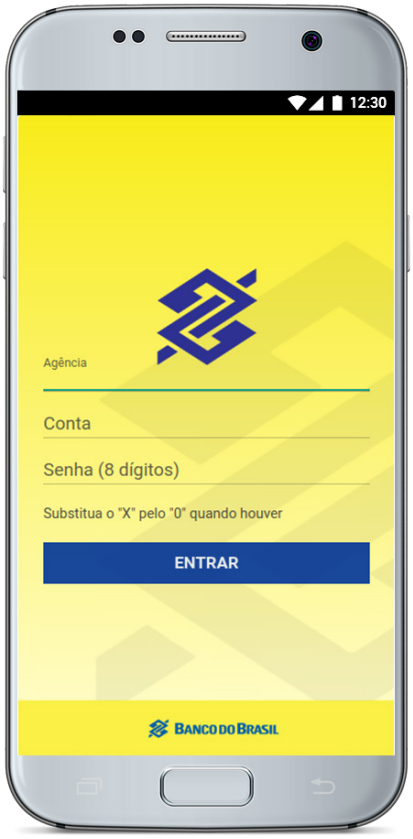
Quando comparado ao trimestre anterior, esta categoria teve uma redução de 73,5% no número de detecções, reflexo das novas políticas de controle de publicidade da Google que trabalham, em parceria com os departamentos de marketing dos aplicativos mais baixados do mundo, para banir práticas fraudulentas do mercado de publicidade mobile.

# 3 Phishing bancário

## 4,5 milhões
de ataques

Ataques de Phishing bancário tiveram um crescimento significativo de 31,7% do terceiro para o quarto trimestre de 2017, totalizando 4,5 milhões de detecções realizadas pelo DFNDR Lab. O largo aumento no período foi influenciado pela grande mobilização econômica que ocorreu no último ano, em que milhares de brasileiros realizaram saques das suas contas inativas do FGTS.

Outro fator que deve ser levado em consideração no crescimento deste tipo de ataque é a migração dos ambientes bancários para dispositivos móveis. No Phishing bancário, cibercriminosos criam sites falsos idênticos às versões oficiais dos bancos e, sem perceber, a vítima acaba fornecendo suas credenciais, como senhas, dados de cartão e número de conta aos criminosos.




* Hackers criam sites falsos idênticos às versões oficiais dos bancos

# ATENÇÃO!

## Golpe do crédito de celular

## 1,7 milhão
de ataques

O maior golpe via Phishing registrado pelo DFNDR Lab no quarto trimestre de 2017 prometia crédito de graça no celular. A isca, disseminada através do WhatsApp, atingiu a marca de 1,7 milhão de detecções em apenas um dia. Com a viralização do Phishing, cibercriminosos criaram mais duas versões do ataque, com 557 mil acessos e 50 mil acessos respectivamente, totalizando 2,3 milhões.

Para ganhar o suposto bônus, a vítima precisava compartilhar o link malicioso com todos os seus contatos, o que contribuiu para a disseminação rápida do golpe. Por fim, além de não receber os créditos prometidos, a vítima era induzida a se cadastrar em um serviço de SMS pago, a ver anúncios abusivos ou a baixar aplicativos.

# Malware

**3º trimestre:**

**5,6**

milhões

**4º trimestre:**

**3,9**

milhões

Redução de

**30,1%**

O DFNDR Lab detectou, em média,
30 malwares por minuto no 4º trimestre

# MALWARES
## detectados no Brasil em 2017

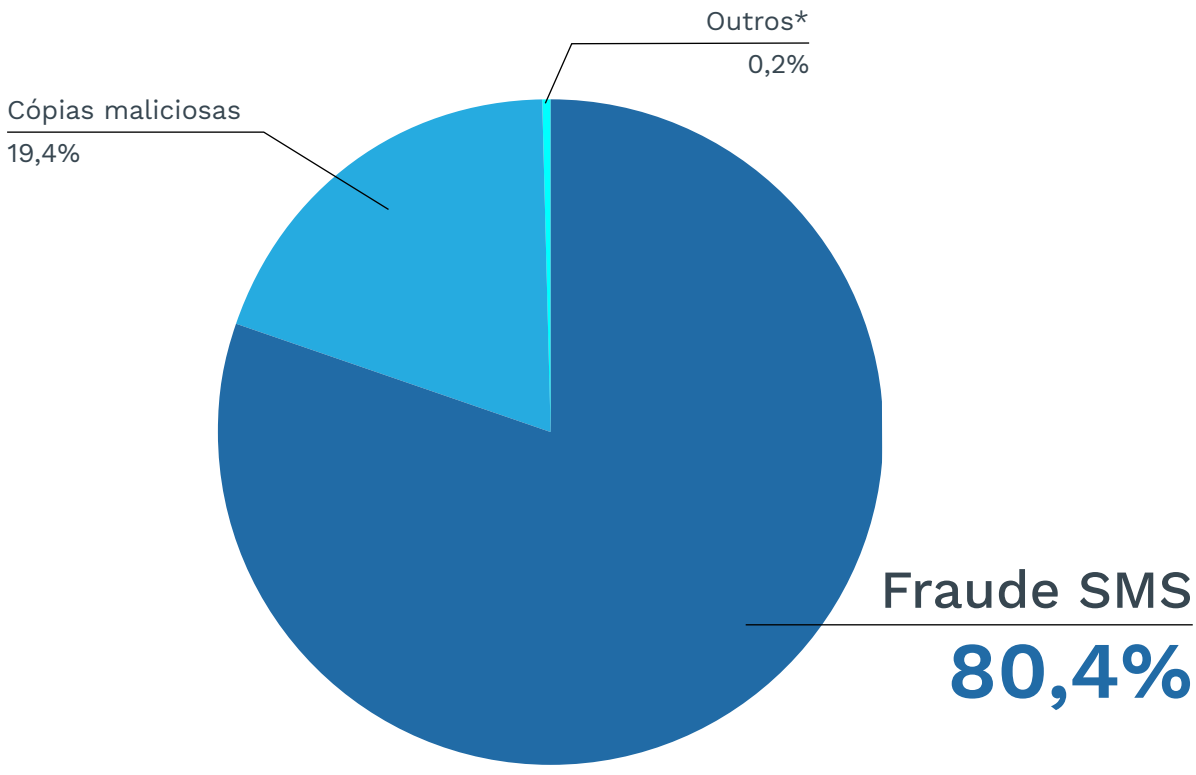
### Total de malwares

**OUTUBRO**
**1.549.100**

**NOVEMBRO**
**1.326.656**

**DEZEMBRO**
**1.027.141**

### Principais tipos de malwares




*Ataque bancário; Ransomware

# 1 Fraude SMS

**3,1 milhões**
de ataques

O principal objetivo deste tipo de malware é cadastrar o número de telefone da vítima em serviços pagos de SMS. Tanto o terceiro quanto o quarto trimestre de 2017 registraram, em média, 1 milhão de detecções por mês desta categoria.


A instalação do malware no celular do usuário pode ocorrer por meio de falsos aplicativos baixados em lojas não-oficiais ou via Publicidade suspeita. Uma vez instalado, o atalho do app pode ficar invisível na tela inicial do aparelho ou apresentar problemas no funcionamento. A partir daí, o cibercriminoso passa a enviar SMS sem permissão e a vítima sofre prejuízo financeiro, uma vez que os custos são descontados do seu saldo de créditos ou da fatura mensal do celular. Na maior parte das vezes, a pessoa não se dá conta que isso foi ocasionado por um malware e, por conta disso, continua sofrendo com a fraude por algum tempo.

# 2 Cópias maliciosas

**755 mil**

ataques

Apesar de estar na lista dos malwares com maior número de detecções, a categoria de Cópia maliciosa não causa, necessariamente, danos financeiros aos cidadãos. O principal intuito do cibercriminoso com isso é ganhar, de forma fraudulenta, dinheiro de empresas por meio da exibição ilegal de anúncios em seus nomes. Este tipo de malware se instala no celular do usuário por meio de um aplicativo falso que, muitas vezes oferece supostas atualizações e funcionalidades exclusivas usando o nome de outros apps conhecidos. Sem conseguir identificar qual é a origem, o usuário passa a receber anúncios, notificações e pop-ups de propaganda no seu aparelho de forma indiscriminada.


# 3 Ataque bancário

**6 mil**

ataques

Os malwares de Ataque bancário, assim como os de Fraude SMS, são instalados no celular do usuário por meio de falsos aplicativos baixados em lojas não-oficiais ou via Publicidade suspeita. Após concluir a instalação, o atalho do app fica disponível por algum tempo na tela inicial do aparelho e logo em seguida desaparece, ficando praticamente invisível. Dessa forma, o cibercriminoso consegue monitorar as atividades que a vítima faz em aplicativos bancários e sobrepor telas falsas exatamente como a original para furtar dados financeiros, como números de cartão de crédito ou credenciais bancárias.

No último trimestre de 2017, o DFNDR Lab registrou uma redução de 51,2% nas detecções deste tipo de malware. Em contrapartida, houve um aumento de 31,7% no número de Phishing bancário, um método mais simples de furtar dados financeiros sem depender de instalações de apps para se infiltrar no celular das vítimas.

# Um golpe a cada notificação

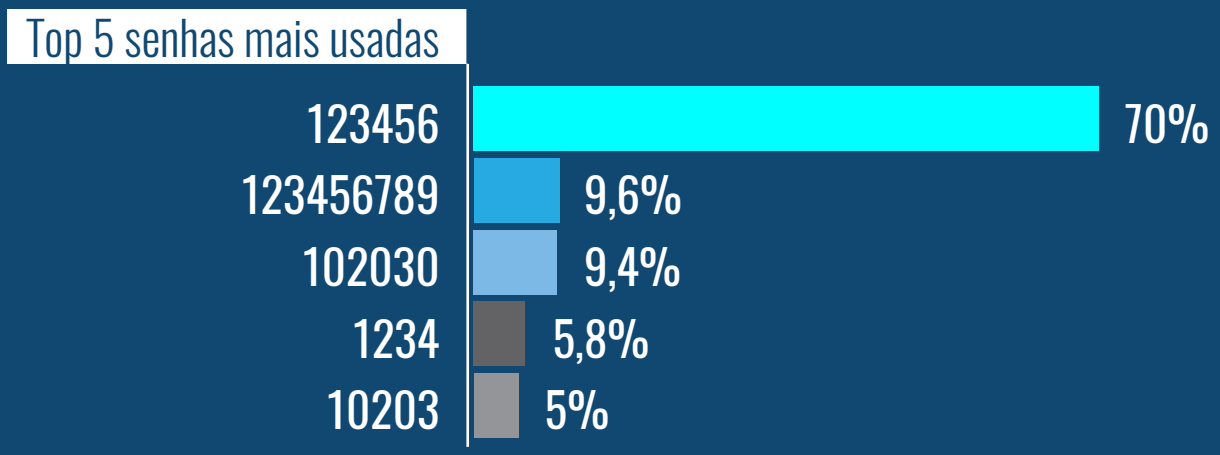
O DFNDR Lab identificou uma nova técnica utilizada para aplicar golpes através do recurso de push notification - notificações personalizadas. Ao tocar em um Phishing via aplicativo de mensagem, em grande parte no WhatsApp, a vítima é levada a uma página falsa para responder algumas perguntas. Durante esse processo, o cibercriminoso solicita uma permissão para enviar notificações para o celular da vítima e disseminar de forma mais ágil outros golpes no futuro. Na maior parte das vezes, a pessoa nem se dá conta que está fornecendo essa permissão, pois os cibercriminosos mascaram a solicitação com perguntas como “Deseja marcar sua entrevista para a vaga de emprego?”.

Em um dos testes realizados pelos especialistas em segurança do DFNDR Lab, algumas horas após o acesso a um link de golpe específico, o cibercriminoso enviou uma nova isca, via notificação direta, para o aparelho dos especialistas.

# Vazamento maciço de dados

Apesar de fazerem parte da lista dos principais ciberataques do ano, os golpes via links maliciosos e malwares estão longe de serem os únicos tipos de cibercrimes praticados. Em dezembro de 2017, um cibercriminoso realizou um dos maiores vazamentos de dados da história. Ele reuniu e divulgou todas as informações furtadas por outros cibercriminosos nos anos de 2015, 2016 e 2017. Ao todo, foram vazados 1,4 bilhão de dados - um número sete vezes maior que a população brasileira. É como se cada habitante do Brasil tivesse as senhas de sete serviços online furtadas.

De acordo com a análise dos especialistas do DFNDR Lab, no documento divulgado pelo cibercriminoso haviam dados de acesso de mais de 37 domínios brasileiros de bancos, imprensa e até do governo, como Senado, Câmara dos Deputados e Previdência Social. Dentre as senhas mais usadas para acessar esses domínios, 85,6% são exclusivamente numéricas e sequenciais, como 0123.




Boa parte dessas invasões à base de dados ocorre a partir de brechas de segurança no código dos sites e plataformas digitais ou por descuido das próprias vítimas, ao escolherem senhas de fácil dedução e repeti-las em diversos serviços. Por isso, é importante evitar o uso de números sequenciais, datas de nascimento ou casamento e números de telefone devido à facilidade de serem adivinhados. O ideal é criar senhas longas e diferentes para cada conta, com pelo menos 10 caracteres que combine letras minúsculas, maiúsculas, caracteres especiais e números, além de alterá-las periodicamente, de preferência a cada três meses.

Apesar do grande vazamento de dados em dezembro, o foco dessas invasões ainda são bases de dados que contenham senhas e números de cartões de crédito, uma vez que essas informações podem ser facilmente vendidas para outros cibercriminosos na Dark web, uma rede invisível para os sistemas e mecanismos de busca. Uma vez que os dados são comercializados dentro dessa rede, os riscos à segurança das vítimas se multiplicam. Além da venda ser feita para mais de um cibercriminoso e os dados serem usados para aplicar novos golpes, o compartilhamento e a divulgação das informações se mantém por anos.

# NOVA TENDÊNCIA

## Dois phishings, um único golpe

De acordo com os dados do DFNDR Lab, houve um aumento de 107% no número de detecções de Phishing via aplicativo de mensagem e de 31,7% de Phishing bancário entre o terceiro e o quarto trimestre de 2017. A integração entre esses dois tipos de phishing em um único golpe é uma grande tendência, pois enquanto o Phishing via aplicativo de mensagem tem um enorme potencial de viralização, o Phishing bancário fornece um maior ganho financeiro aos cibercriminosos.


A principal estratégia para disseminar o ataque é o compartilhamento, inconsciente, de links maliciosos por meio de mensagens. Usando o golpe do FGTS, que ocorreu em outubro do ano passado, como exemplo, essa modalidade teria a mesma sequência de ações: a vítima clica no link, responde a perguntas e precisa compartilhar a notícia com outros amigos para ganhar o benefício oferecido. O diferencial estaria na etapa final, onde a vítima poderia ser encaminhada para uma página falsa de banco que solicita dados de acesso, como número do CPF, NIS, PIS/PASEP, credenciais bancárias e senhas para acessar o benefício.

DFNDR Lab

DFNDRlab.com