SiDi

Vulnerabilidades de Software em Dispositivos Móveis_

Palestrantes:

Danilo Rodrigues

Analista de segurança de software
Unicamper
Defensor de privacidade cibernética
FLOSS <3

Fábio Sartorato

Análista de segurança de software
Ex-Unicamper
Foco em segurança de plataformas móveis

Especialistas em solucionar problemas

ICT (Instituição Científica e Tecnológica) localizada em Campinas (SP)

Nascemos em 2004 sob os incentivos da Lei da Informática atuando em P&D

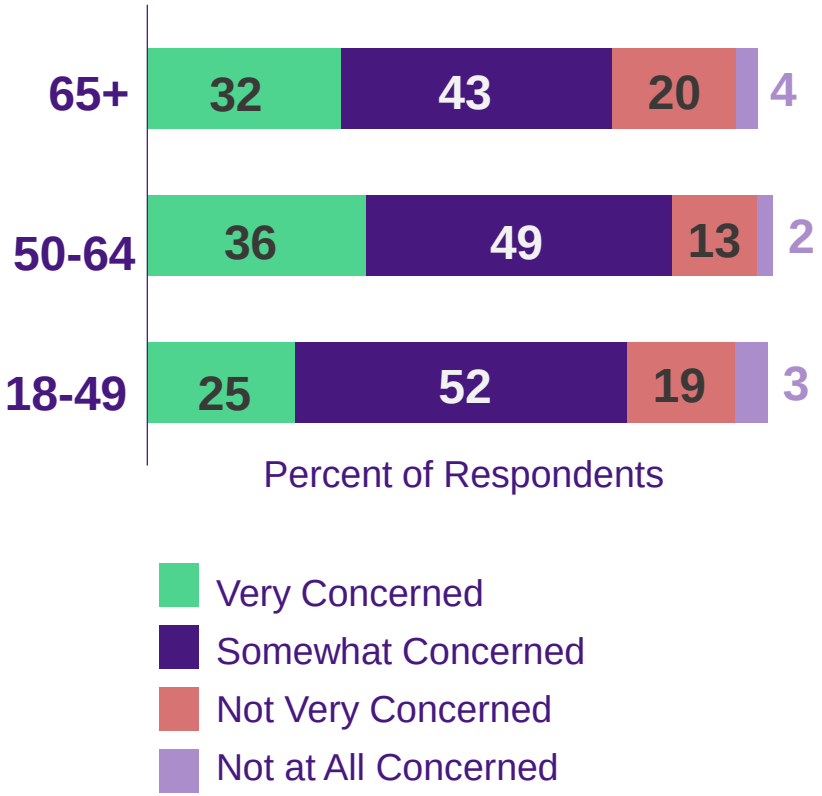
Nosso time conta com mais de 300 SiDiers

Análise de segurança

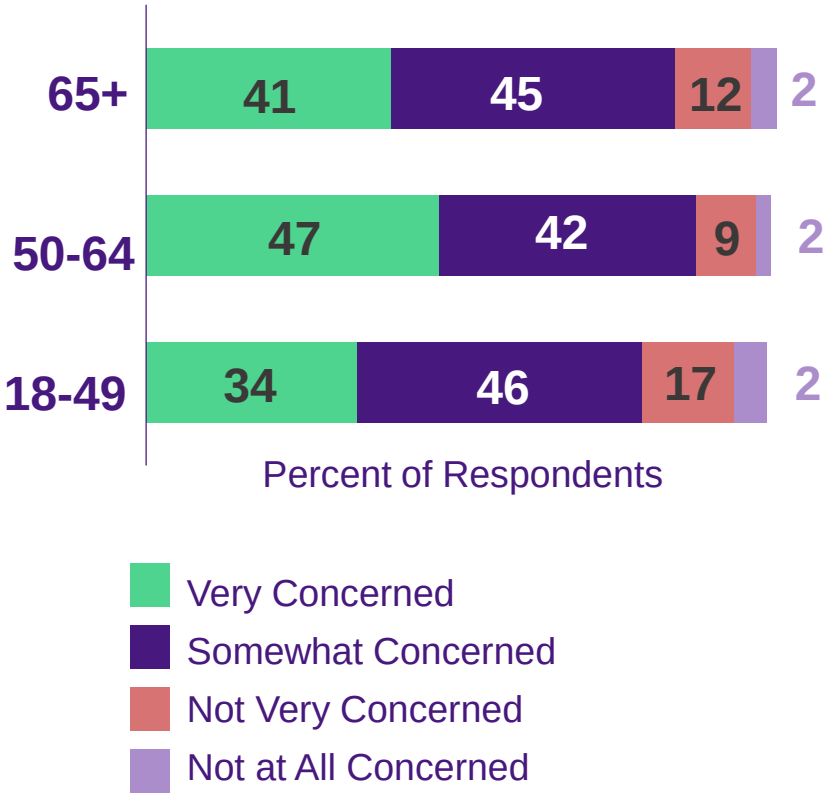
Por que se preocupar com segurança cibernética?

Usuários se preocupam!

O quanto você se preocupa com privacidade quando você está conectado digitalmente?



O quanto você se preocupa sobre seus dados serem *hackeados* ou roubados?



[Aarp 2017]

Segurança impacta a confiabilidade.

26/04/2011 18h03 - Atualizado em 26/04/2011 19h59

Dados pessoais de usuários da PSN foram roubados, admite Sony

Empresa não descarta roubo de informações de cartões de crédito. PlayStation Network está fora do ar há seis dias.

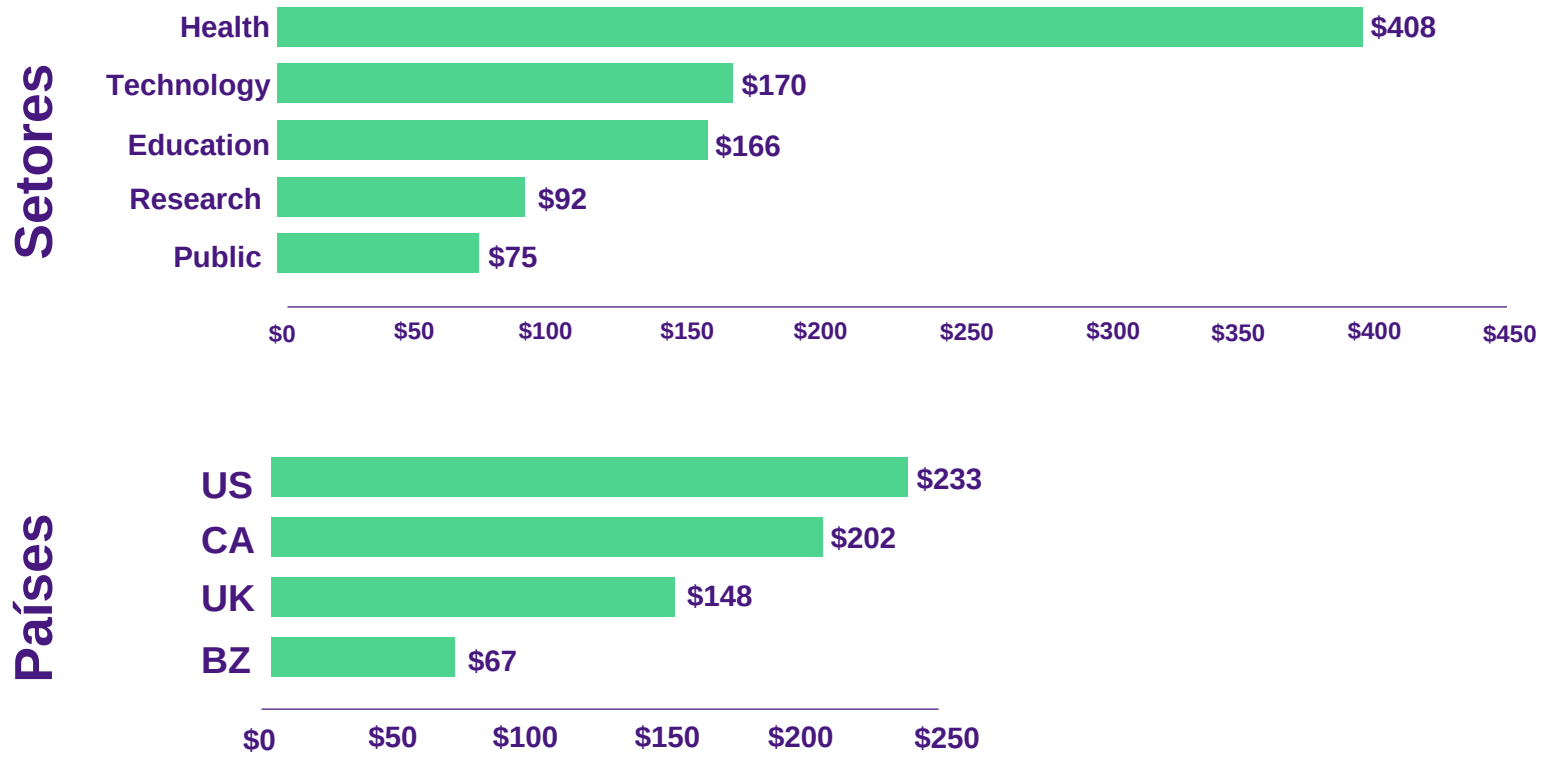
04/09/2012 21h48 - Atualizado em 04/09/2012 21h48

Hackers publicam 1 milhão de IDs de dispositivos da Apple

Equifax, empresa de crédito dos EUA, sofre ataque hacker e dados de 143 milhões de pessoas são expostos

Empresa sofreu ataque no fim de julho e admitiu nesta quinta-feira vazamentos de informações dos usuários.

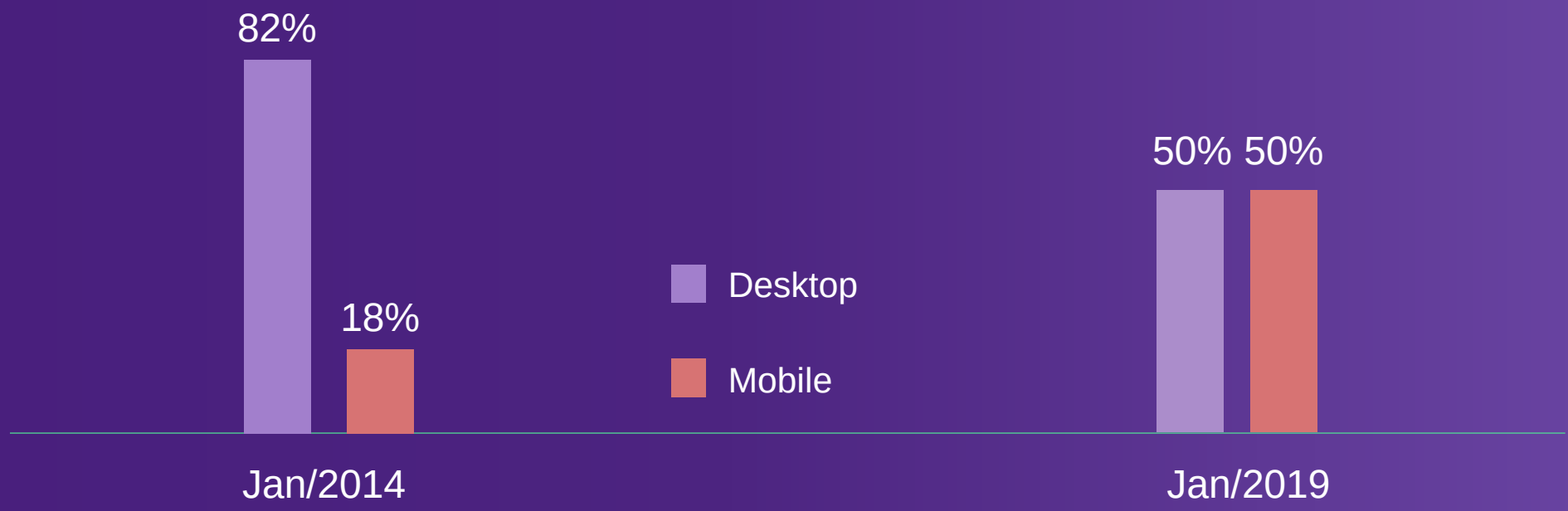
Custo médio per capta de vazamentos de dados:



[Ponemon Institute]

E segurança em dispositivos móveis?

Smartphones estão nas mãos de todo mundo!



StartCounter Global Stats – Desktop vs Mobile Market Share Worldwide

Quase 40% das transações bancárias em 2018 foram feitas pelo celular [Febraban]

Total de
R$ 35.600.000.000,00
R$ 500.000.000,00 Mobile

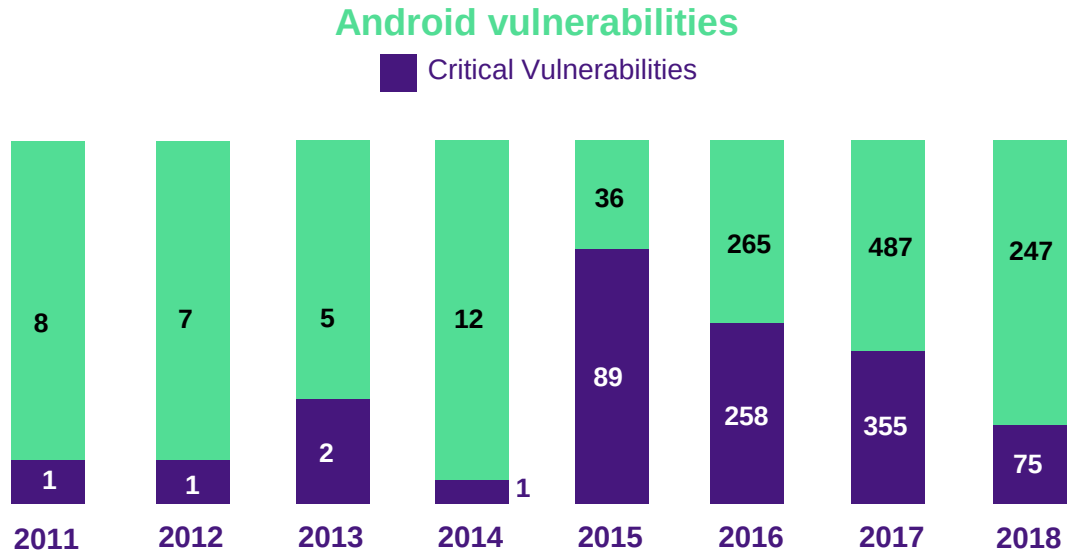
2012

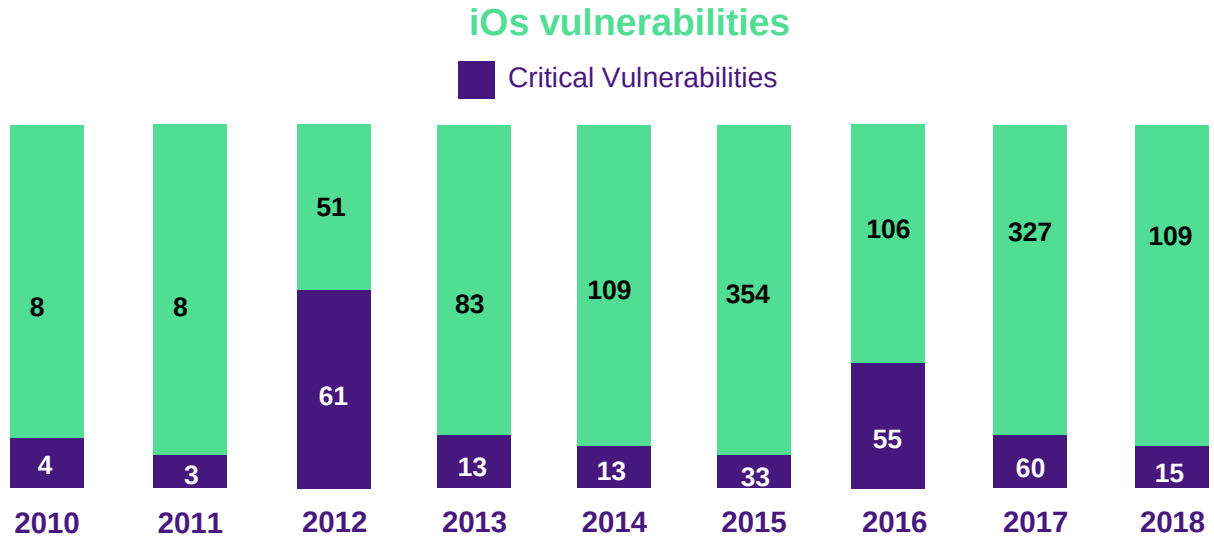
Total de
R$ 78.900.000.000,00
R$ 31.300.000.000,00 Mobile

2018

Estamos seguros?

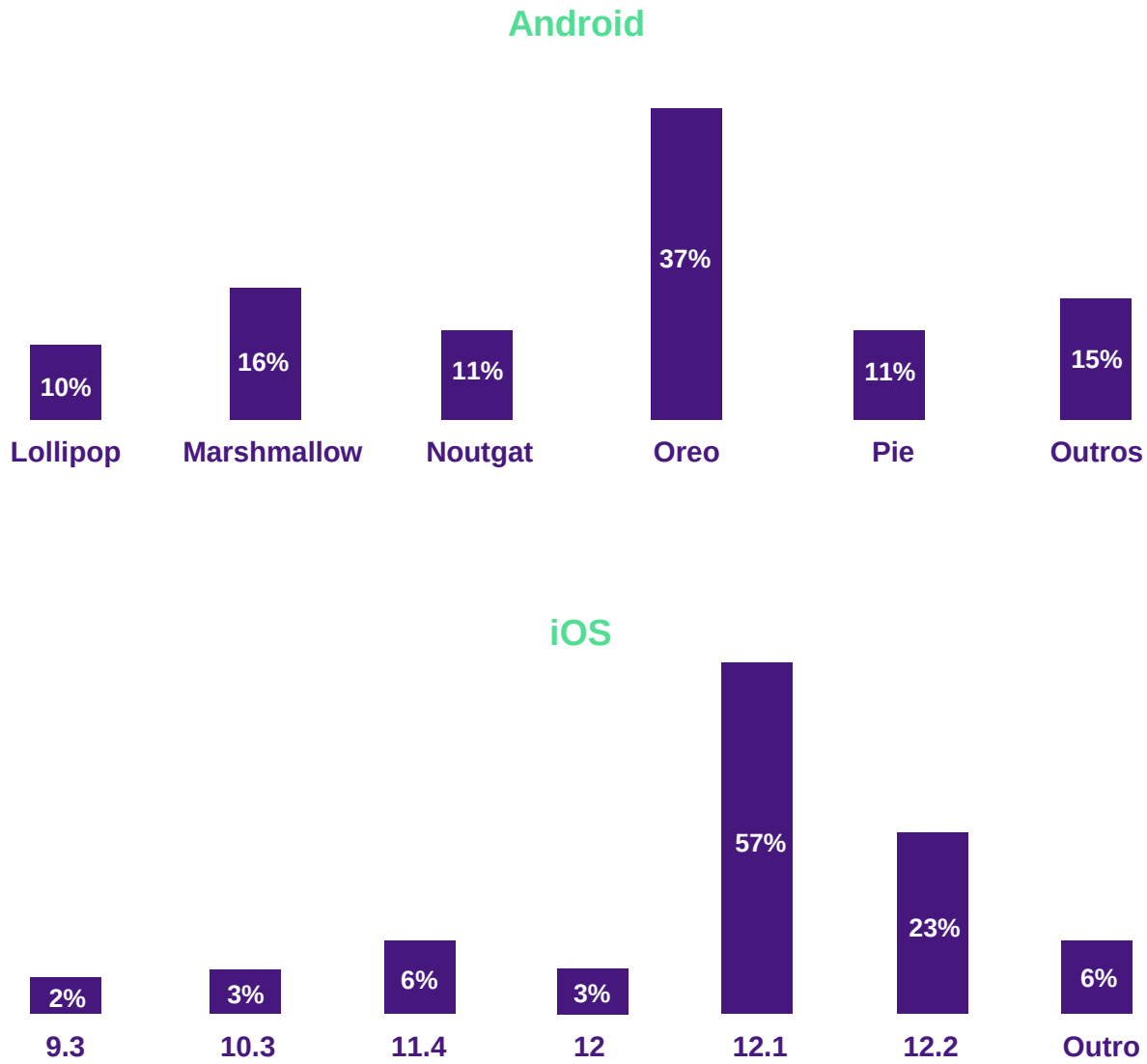
Vulnerabilidades por plataforma_





[CVEDetails]

Fragmentação de versões_



[Statcounter, abril 2019]

Modelos de ataque_

Usuário atacando o próprio telefone

Aplicação maliciosa atacando o sistema

Ataque físico

Aplicação maliciosa atacando outras aplicações

Ataque remoto

Aplicação maliciosa atacando o sistema

First Android-Rooting Trojan With Code Injection Ability Found On Google Play Store

June 08, 2017 Mohit Kumar

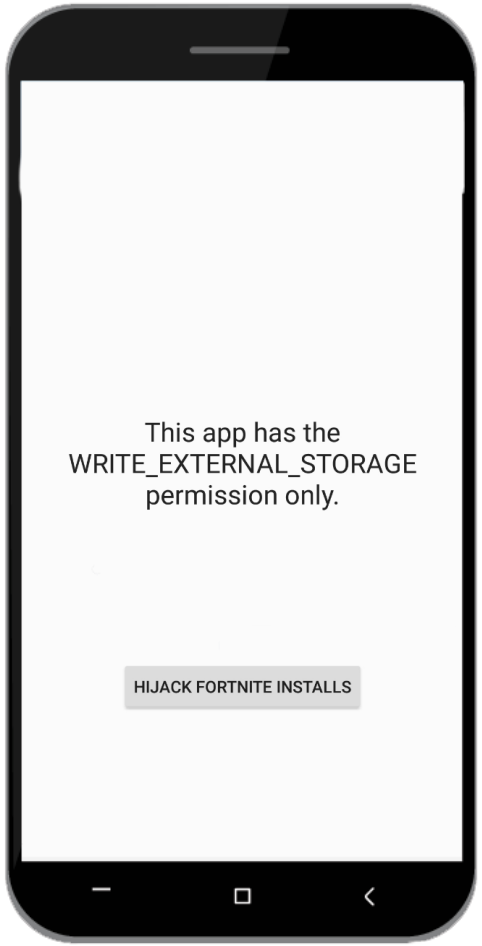
This New Android Malware Can Physically Damage Your Phone

December 19, 2017 Mohit Kumar

Watch Out! New Cryptocurrency-Mining Android Malware is Spreading Rapidly

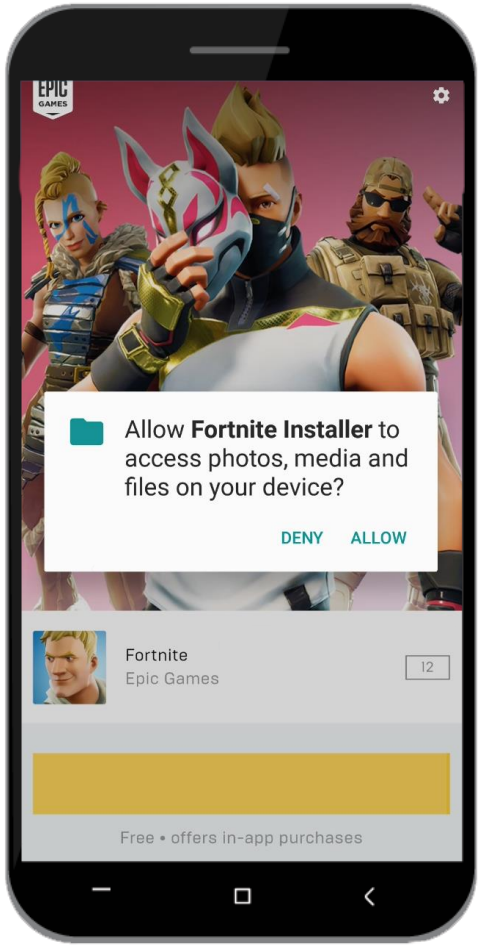
February 06, 2018 Mohit Kumar

Aplicação maliciosa atacando outras aplicações



1. Aplicação maliciosa pede permissão para escrita em armazenamento externo

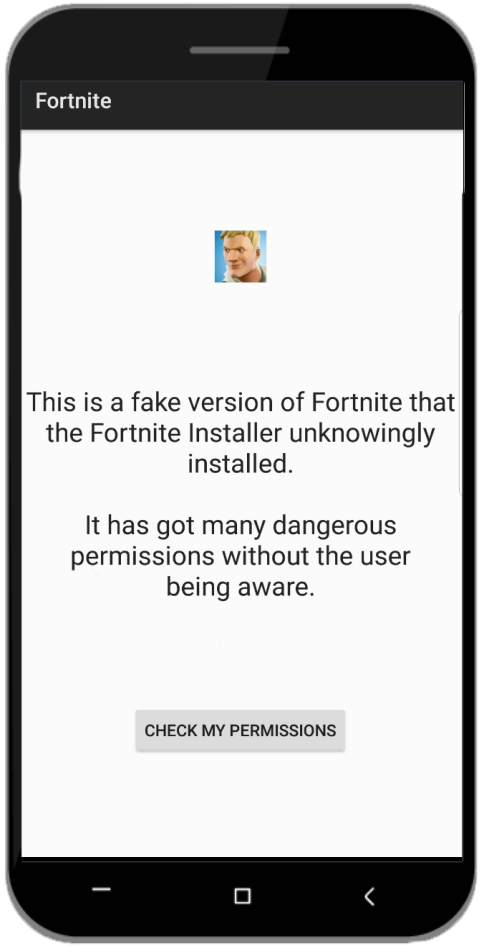
Aplicação maliciosa atacando outras aplicações



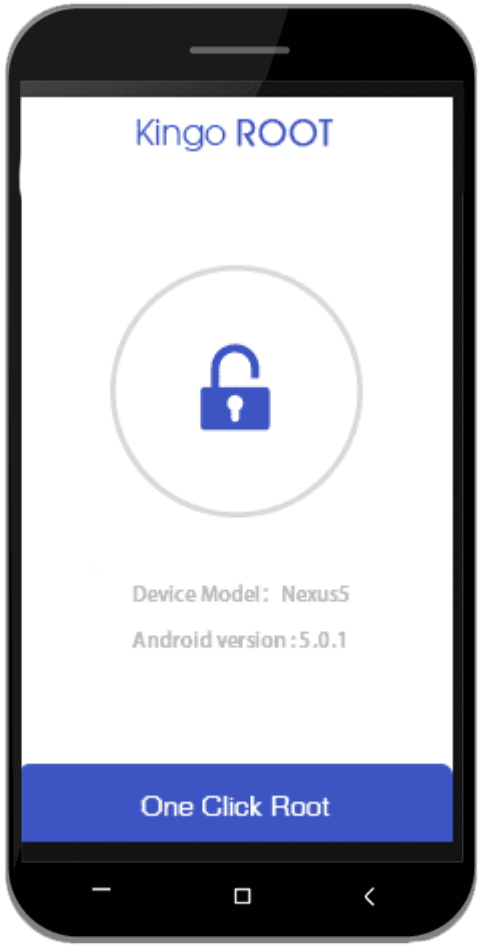
1. Aplicação maliciosa pede permissão para escrita em armazenamento externo

2. Instalador legítimo baixa a aplicação e a coloca no armazenamento externo

Aplicação maliciosa atacando outras aplicações

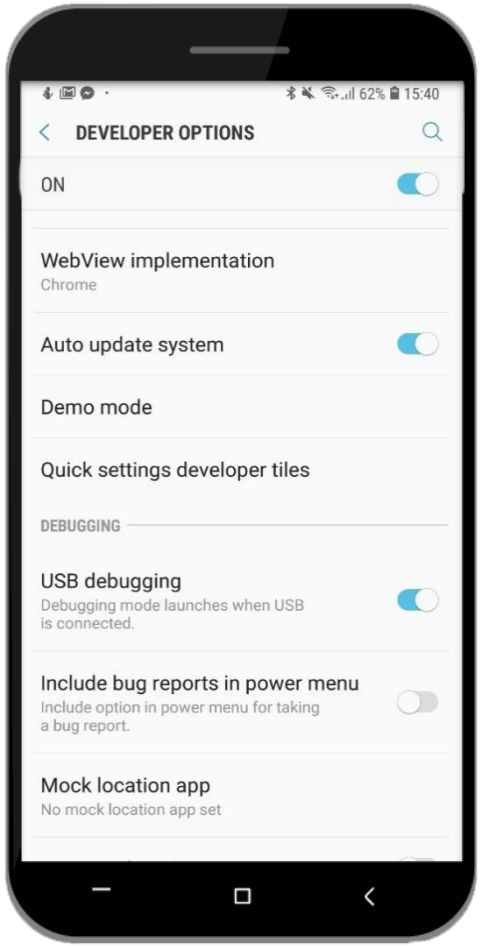


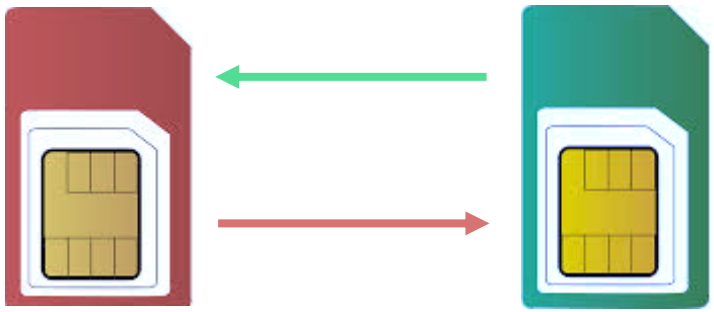
1. Aplicação maliciosa pede permissão para escrita em armazenamento externo
2. Instalador legítimo baixa a aplicação e a coloca no armazenamento externo
3. Aplicação maliciosa substitui o APK legítimo por uma versão falsa, que é instalada.



Usuário atacando o próprio telefone

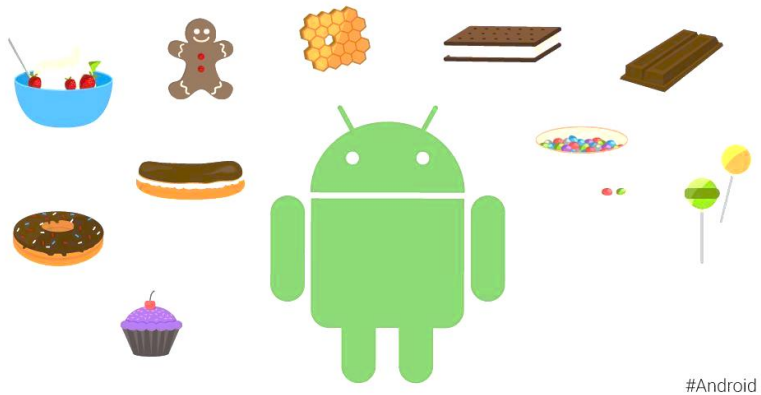
Ataque físico





Ataque remoto

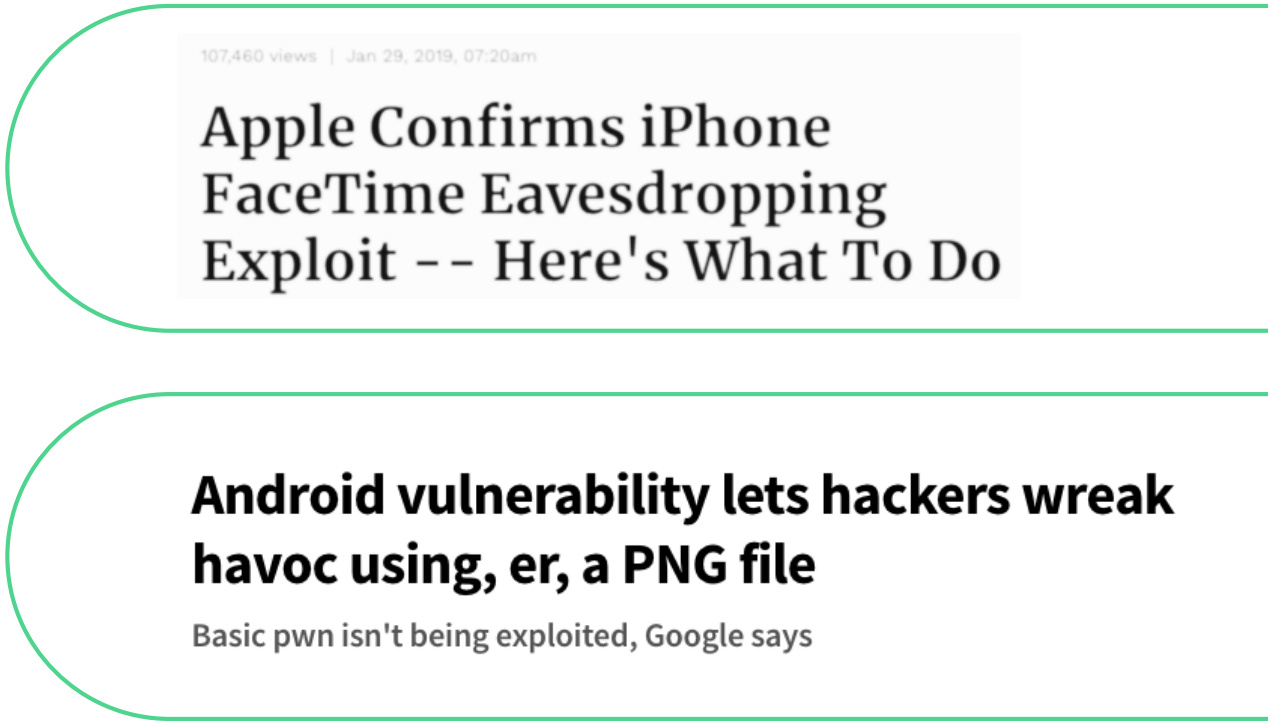
Duas visões bem diferentes_



#Android

Window Package
Managers Content Providers
ANDROID FRAMEWORK
Camadas controladas pelo carrier Resourse
Location Activity View System
Notification Telephony

Tanto Google quanto Apple lançam atualizações de seguranças recorrentes para corrigir erros reportados_



THIS IS MY SURPRISED FACE —

Fortnite's Android vulnerability leads to Google/Epic Games spat

Fortnite on Samsung phones was vulnerable to a man-in-the-disk attack.

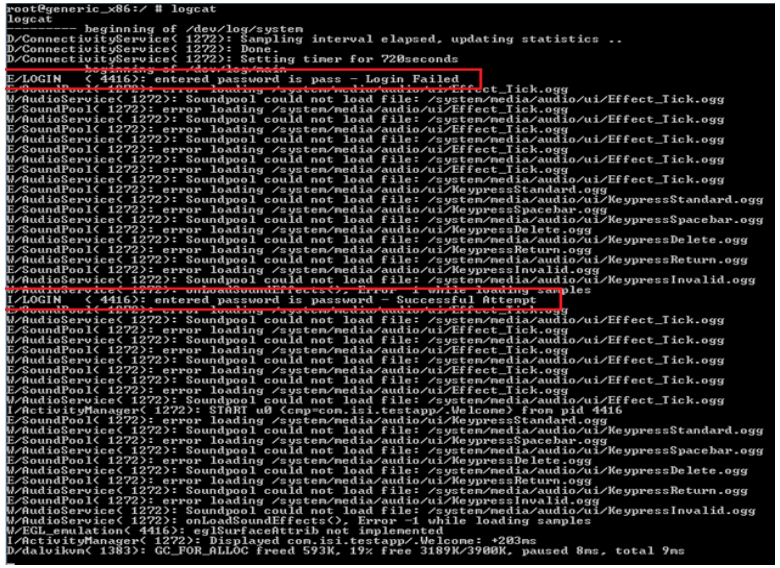
Almost 150 million users impacted by new SimBad Android adware

SimBad adware found in 210 Android apps available on the official Google Play Store.

De malware à problemas de implementação, o usuário fica vulnerável de vários métodos a partir de aplicações_

Falhas de Desenvolvimento_

Vazamento de dados sensíveis_



Através do log

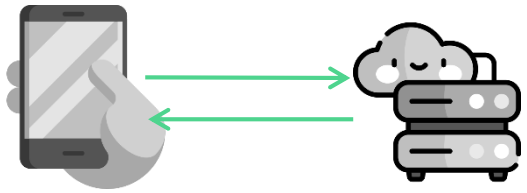
```
package com.august.util;

import android.content.SharedPreferences;

public class Settings
{
  private static final String ENC_KEY = "A[redacted]";
  private static final LogUtil LOG = LogUtil.getLogger(Settings.class);
  public static final String SIZE_SUFFIX = "*size*";
  public static final String STR_ACCESS_TOKEN = "API_ACCESS_TOKEN";
  public static final String STR_DEBUG_SETTINGS = "DEBUG_SETTINGS";
  public static final String STR_INSTALL_TOKEN = "API_INSTALL_TOKEN";
  public static final String STR_PUSH_ALERTS = "PUSH_ALERTS";
  public static final String VERSION_SUFFIX = "_v1";
  static Settings _instance = null;
  DebugSettings _debugSettings = new DebugSettings();
  Properties _encryptedProps = null;

  public static Settings init()
  {
    if (_instance == null) {
      _instance = new Settings();
```

Hardcoded keys



Transmissão insegura de dados

Armazenamento inseguro

Funcionalidades maliciosas_

Monitoramento de atividades e coleta de dados

Chamadas não autorizadas, SMS e pagamentos

Conectividade de rede não autorizada

Falsa interface de usuário

Modificações no sistema

Como o usuário é impactado?

Roubo de dados

Perda de privacidade

Impacto financeiro

Roubo de dados_

WhatsApp Zero-Day Exploited in Targeted Spyware Attacks

Threatpost

6 hours ago

Advertising Personalization Enabled

Opt-in, the (Default state)

```
Form data:
format:                          json
sdk:                             android
custom_events_file:
[{"_eventName":"origin_selected","_eventName_md5":"b883a259b3e22dcafeb6cd97872e5692","_logTime":1543790183,"_u
i":"unknown","_session_id":"9582dd9a-7d17-4b1e-8f2e-3eb88369c542","origin_city_name":"London","origin_iata":"L
OND","origin name":"London"}]
event:                           CUSTOM APP EVENTS
advertiser id:                   474364c6-e9cf-4971-8dd2-b1dc3c605450
advertiser tracking enabled:     true
installer package:               com.android.vending
anon id:                         XZ91d69838-8980-4d1a-8e41-d6c21362b0b5
application tracking enabled:    true
extinfo:                         ["a2","net.skyscanner.android.main",1811261925,"5.57","8.1.0","Nexus
5","en GB","GMT","",1080,1776,"3.00",4,13,6,"Europe\/London"]
application_package_name:        net.skyscanner.android.main
```

Advertising Personalization Disabled

Opt-out

```
Form data:
format:                          json
sdk:                             android
custom_events_file:
[{" eventName":"origin_selected","_eventName_md5":"b883a259b3e22dcafeb6cd97872e5692","_logTime":1544574571,"
ui":"unknown","_session_id":"7b0174ff-d21f-4877-9a71-64fbda0987e1","origin_city_name":"London","origin_iata":
"LOND","origin_name":"London"},{"_eventName":"destination_selected","_eventName_md5":"cd48f17164b8286eeb6fddd
86eccc8ca","_logTime":1544574580,"_ui":"unknown"," session_id":"7b0174ff-d21f-4877-9a71-64fbda0987e1","destin
ation_city_name":"Tokyo","destination_iata":"TYOA","destination_name":"Tokyo"},{"_eventName":"flight_search",
"_eventName_md5":"d5521a518f2b76694cc27dd453c90120","_logTime":1544574582,"_ui":"unknown","_session_id":"7b01
74ff-d21f-4877-9a71-64fbda0987e1","airport_from_iata_flight_search":"","airport_from_name_flight_search":"","
airport_from_city_name_flight_search":"London","date_to_flight_search":"2018-12-24","origin_iata_flight_searc
h":"LOND","date_from_flight_search":"2018-12-17","airport_to_iata_flight_search":"","airport_to name_flight_s
earch":"","airport_to_city name_flight_search":"Tokyo","destination_iata flight_search":"TYOA"},{"_eventName"
:"Search","_eventName_md5":"13348442cc6a27032d2b4aa28b75a5d3","_logTime":1544574582,"_ui":"unknown","_session
_id":"7b0174ff-d21f-4877-9a71-64fbda0987e1","fb_destination_airport":"TYOA","fb_returning departure_date":"20
18-12-24","fb_description":"Flight","fb_content_type":"flight","fb_origin_airport":"LOND","fb_travel_class":"
economy","fb departing departure date":"2018-12-17","fb_num_adults":"1"}]
event:                           CUSTOM APP EVENTS
advertiser id:                   474364c6-e9cf-4971-8dd2-b1dc3c605450
advertiser tracking enabled:     false
installer package:               com.android.vending
anon id:                         XZ2625c992-f7b7-4568-a4ab-6201af500733
application tracking enabled:    true
extinfo:                         ["a2","net.skyscanner.android.main",1811261925,"5.57","8.1.0","Nexus
5","en GB","GMT","",1080,1776,"3.00",4,13,5,"Europe\/London"]
application_package_name:        net.skyscanner.android.main
```

Perda de Privacidade

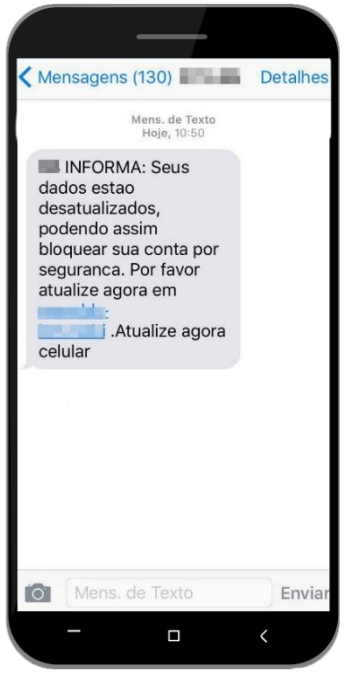
Muitas vezes, aplicativos abusam de permissões dadas pelo usuário para conseguir metadados que podem ferir a privacidade

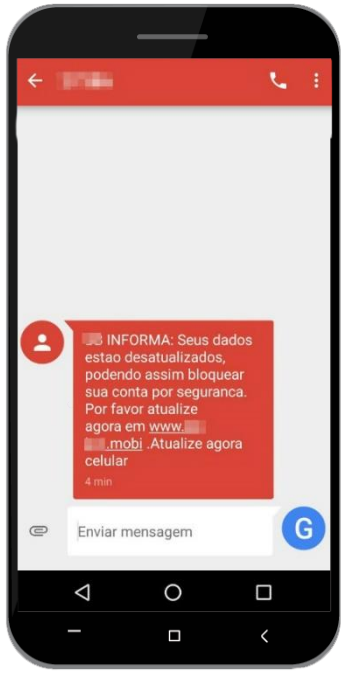
Mobile accounts for nearly half of all banking transactions in Brazil

The number of transactions soars as consumer confidence in the channel increases, according to the Brazilian Banking Federation.

Impacto finaceiro

Engenharia social ainda é a forma mais fácil de conseguir enganhar uma vítima a passar dados bancários ou realizar transferências_





O que pode ser feito pra se prevenir - Usuários

Tente manter o dispositivo sempre atualizado, com os últimos patches de segurança

Sempre baixe aplicativos de repositórios oficiais

O que pode ser feito pra se prevenir - Desenvolvedores

Sempre desenvolva com a mentalidade de least priviledge

#Obrigado_

SiDi