Trabalho de Conclusão de Curso
Ciência da Computação

A SEGURANÇA EM SISTEMAS OPERACIONAIS ANDROID

Alunos:

Antônio Augusto Duarte

Leonardo Silva

Orientadores:

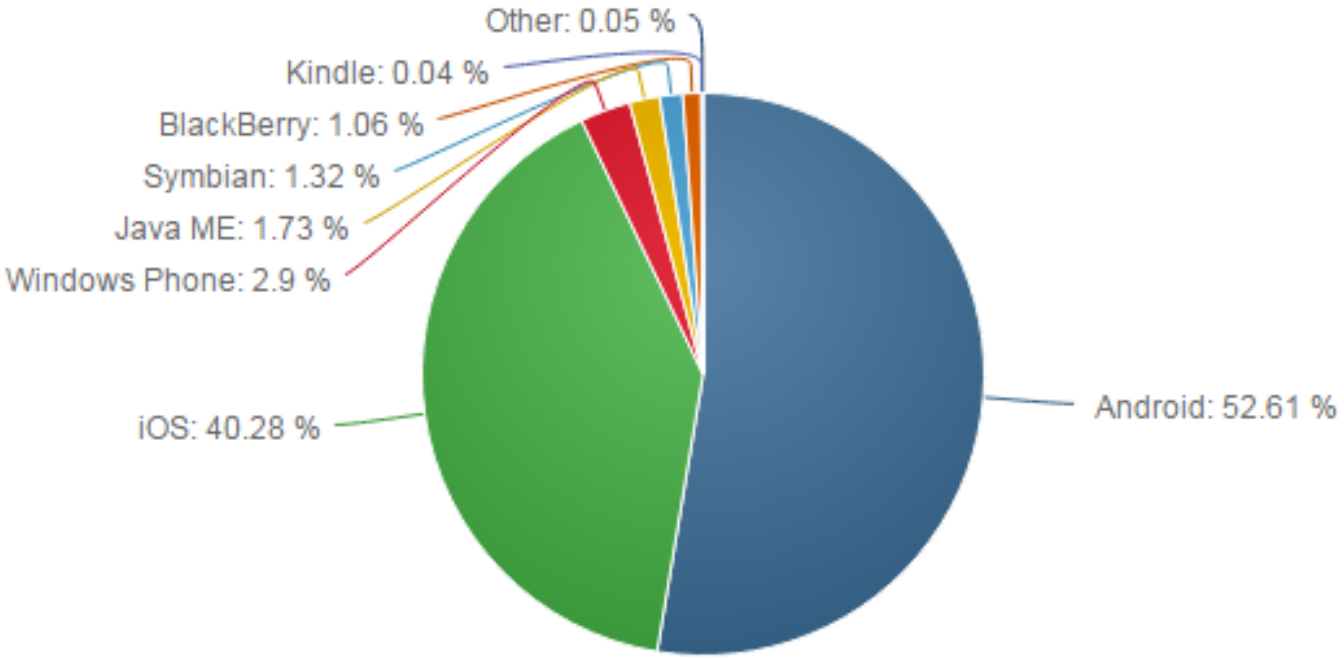
Prof. Humberto Fernandes Villela

Prof. Davis Anderson Figueiredo

INTRODUÇÃO

- Tema do trabalho:
  - A Segurança em Sistemas Operacionais Android.

- Contexto:
  - Aumento no número de usuários de dispositivos móveis;
  - Parcela do mercado que adota o Sistema Android;
  - Aumento de fraudes e vulnerabilidades;
  - Aumento de serviços disponibilizados em dispositivos móveis que requerem segurança como bancos on-line e sites governamentais como a declaração de imposto de renda;



Fonte: NET MARKET SHARE, 2015

PROBLEMA ABORDADO

- Quais as vulnerabilidades mais comuns que foram reportadas no sistema Android e os seus mecanismos para garantir a segurança?

OBJETIVOS

- Objetivo Geral:
  - Este trabalho consiste num estudo sobre as principais vulnerabilidades do sistema operacional Android entre a API 18 e a API 22 (exceto API 20).

OBJETIVOS

- Objetivos Específicos:
  - Avaliar a autenticidade dos aplicativos da Google Play Store;
  - Identificar e compreender o funcionamento das atualizações e correções para os sistemas Android;
  - Identificar, analisar e comparar as versões 4.3, 4.4, 5.0 e 5.1 do Android;
  - Analisar as principais vulnerabilidades reportadas no uso do sistema operacional Android.

JUSTIFICATIVA

- Acadêmica:
  - Avançar na discussão do tema central.
- Empresarial:
  - Discutir suas vulnerabilidades e características técnicas para que as organizações e usuários tenham mais segurança no uso dos dispositivos móveis.
- Quanto aos alunos:
  - O TCC busca avançar além da técnica e possibilitar alinhamento ao mercado de empresarial.

Referencial Teórico

TÓPICOS ESTUDADOS	AUTORES
Os principais tipos de cibercriminosos	MARTINS (2015)
	RAYMOND (1996)
	RUSSO (2013)
	SANTOS (2010)
	ULBRICH (2004)
Os principais tipos de aplicativos maliciosos	BEAL (2015)
	BORGES (2006)
	GASPAR (2007)
	GRIFFIN (2000)
	INFO WESTER (2013)
	ISHIMI (2005)
	MICROSOFT (2015)
	TECHTERMS (2015)
	UOL (2013)
	XAVIER (2008)
A origem do sistema operacional Android	LECHETA (2015)
	MEYER (2015)
Arquitetura do Android	BORDIN (2012)
	CÁRDENAS (2011)
	GOMES (2012)
	LECHETA (2015)
	MACK (2010)
	PEREIRA JÚNIOR (2014)
Histórico de versões do Android	ANDROID (2015)
	ANDROID DEVELOPERS (2015)
	GOOGLE (2015)
	LECHETA (2015)
	MANN (1998)

METODOLOGIA

- A pesquisa foi desenvolvida de forma qualitativa dissertativa, fazendo o uso de referências bibliográficas, como artigos, livros e notícias sobre as falhas relatadas com maior frequência pelos autores.

Resultados

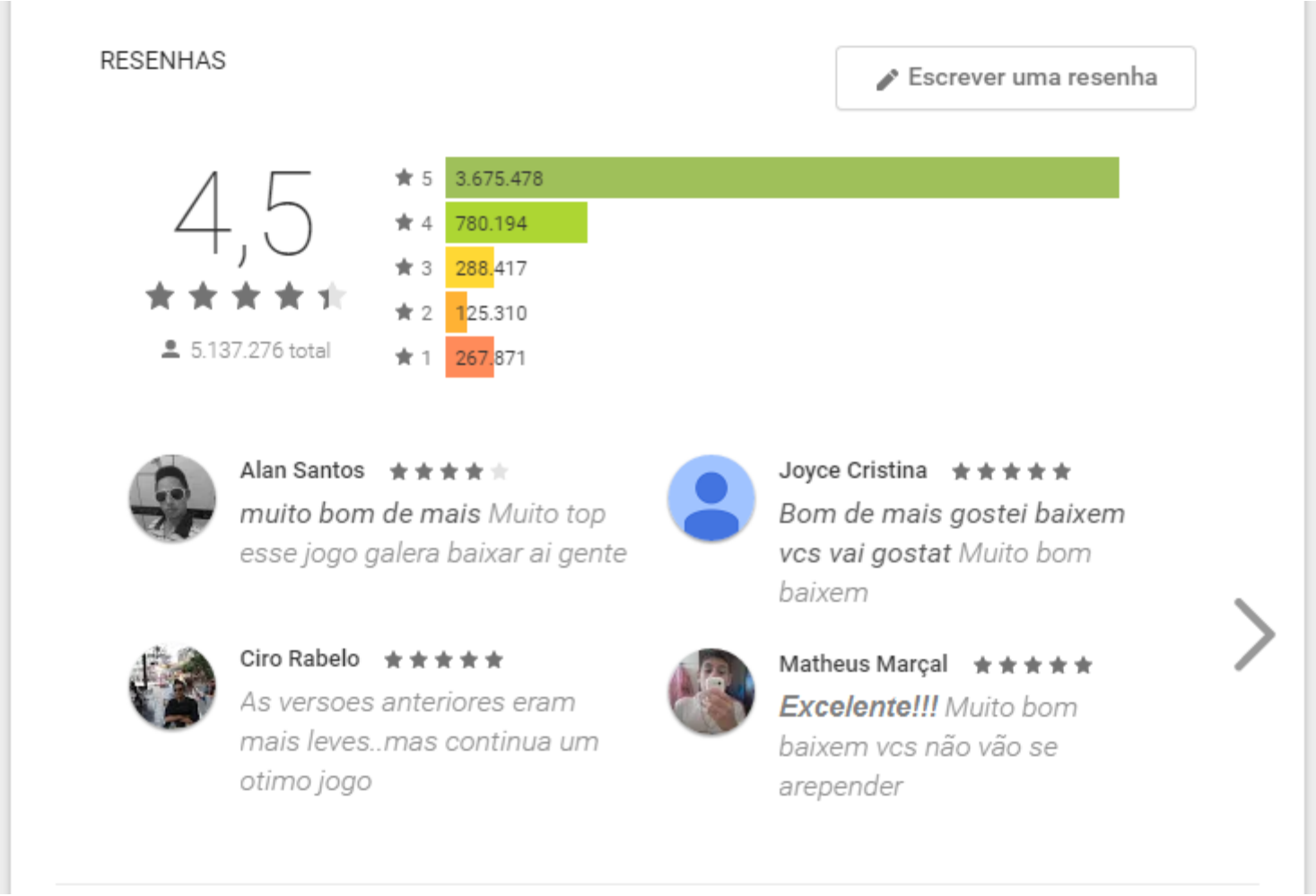
GOOGLE PLAY STORE

- Loja online da Google para distribuição de aplicações, jogos, filmes, música e livros para dispositivos com o sistema Android.

AUTENTICIDADE DE APPS DA LOJA

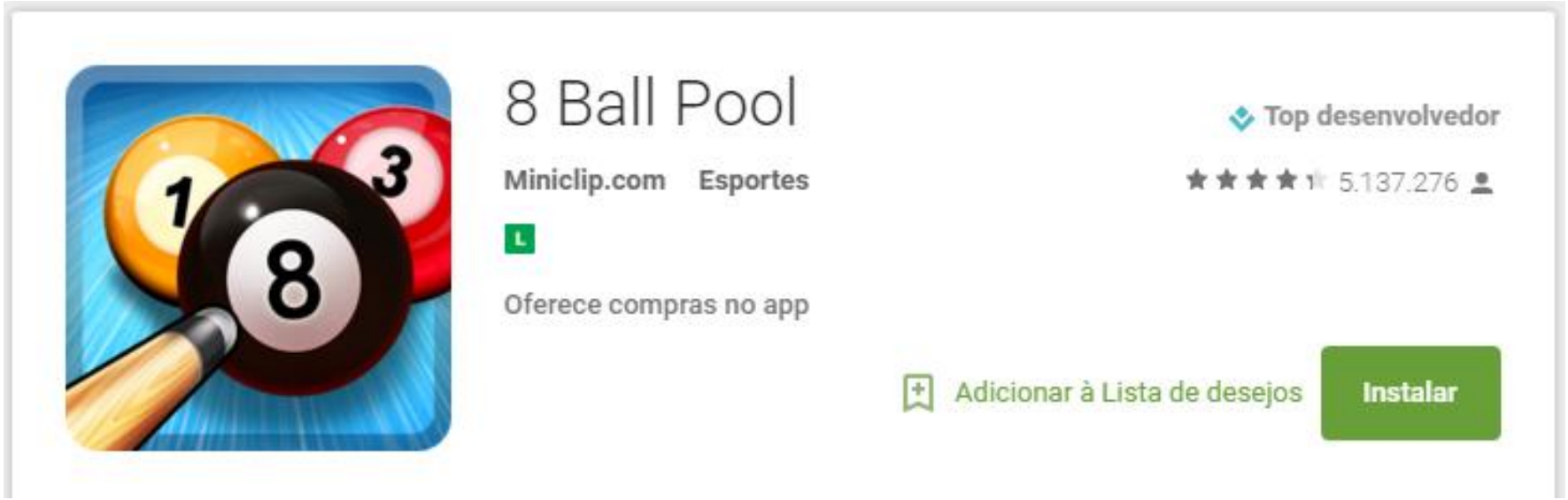
- Como identificar se tal aplicativo da loja é realmente confiável?

- Quadro de resenhas na página do app “8 Ball Pool” da Google Play Store.



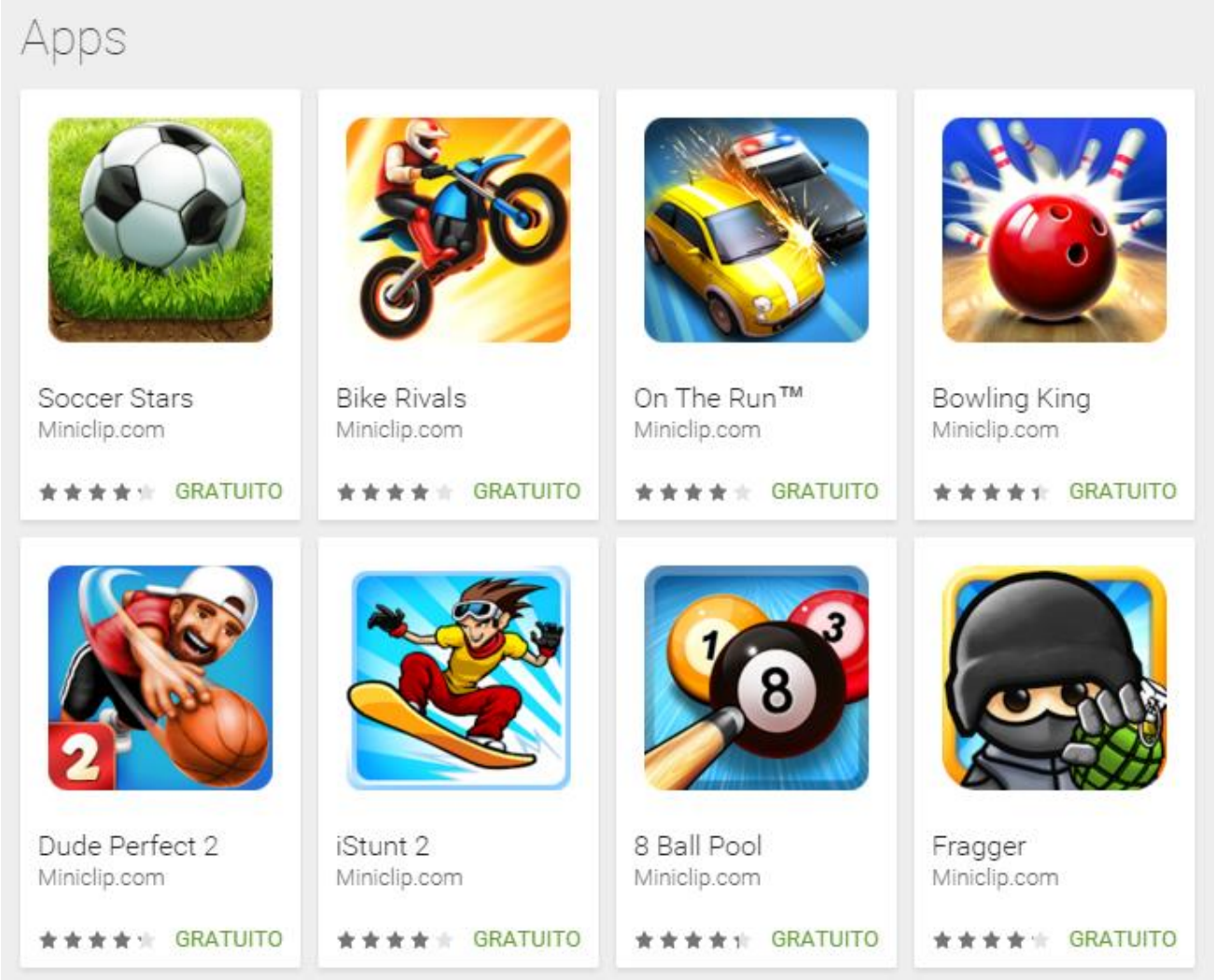
Fonte: GOOGLE PLAY STORE, 2015

- Informações principais da página do app “8 Ball Pool” na Google Play Store.



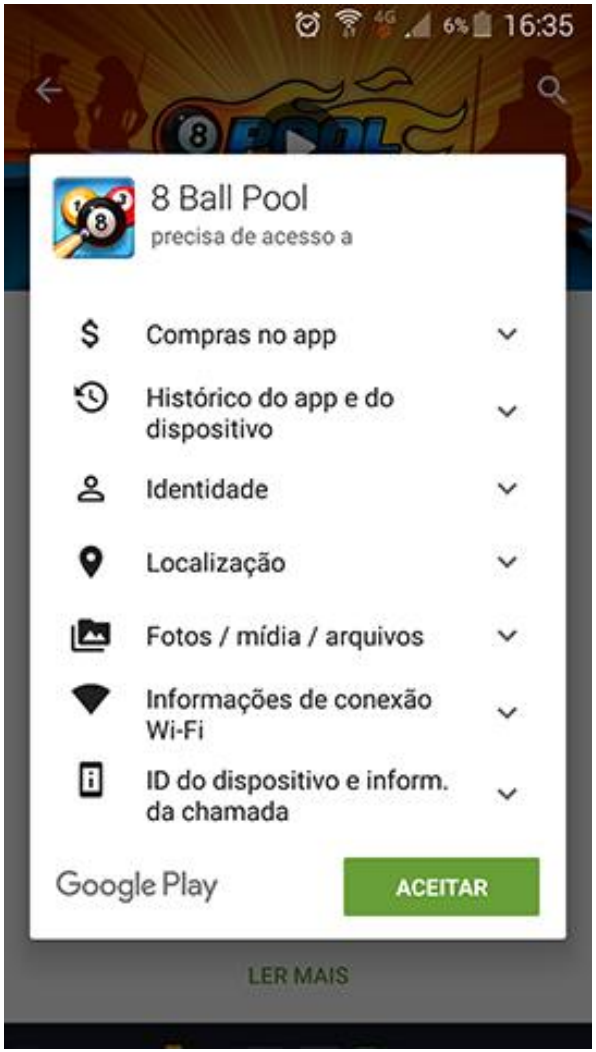
Fonte: GOOGLE PLAY STORE, 2015

- Alguns aplicativos postados pelo *Miniclip.com* na Google Play Store.



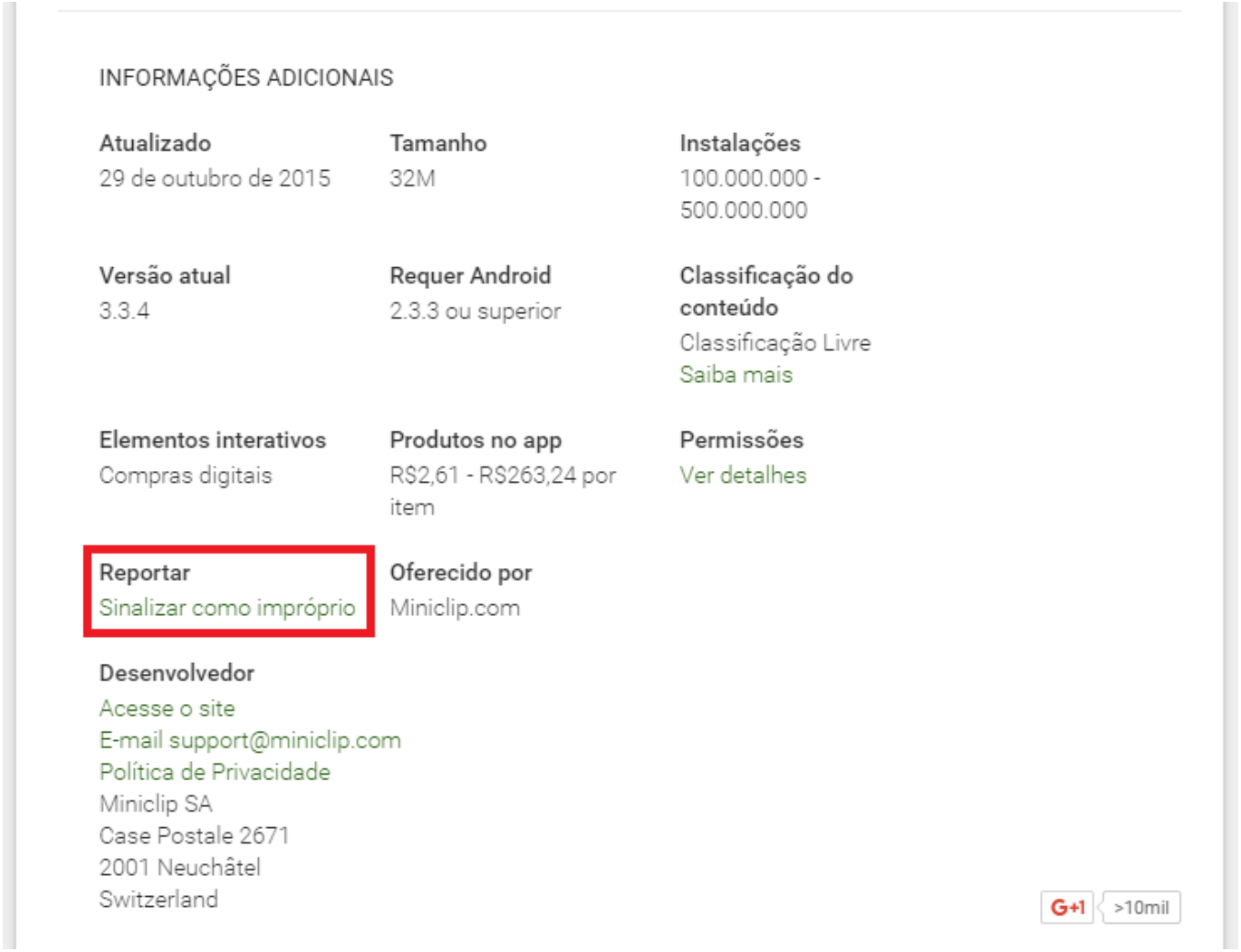
Fonte: GOOGLE PLAY STORE, 2015

- Permissões de acesso ao aparelho do aplicativo “8 Ball Pool”.



Fonte: GOOGLE PLAY STORE, 2015

- Opção de reportar aplicativo na Google Play Store.



Fonte: GOOGLE PLAY STORE, 2015

ATUALIZAÇÕES DO ANDROID

PASSO	DESCRIÇÃO
1	Vulnerabilidade é descoberta
2	Vulnerabilidade é reportada via NDA (*Non-Disclosure Agreement* - Acordo de Não Divulgação)
3	Se a vulnerabilidade for proveniente do código fonte do sistema, o erro é corrigido pela equipe de desenvolvimento do Android
4	Fabricantes recebem o código fonte concertado e adequam as suas personalizações
5	Operadoras de telefonia também se adequam ao código e as suas personalizações
6	Os usuários recebem a atualização via OTA (*Over The Air* - “Pelo Ar”) e instalam o patch de segurança

ATUALIZAÇÕES DO ANDROID

- A complexidade da atualização é grande, devido à inúmera quantidade de fabricantes, dispositivos Android e operadoras diferentes;
- Muitos aparelhos datados como ultrapassados não chegam a receber tais melhorias. A alternativa para esses usuários é a técnica de *flashing*;
- A empresa CyanogenMod fornece versões oficiais customizadas do sistema Android.

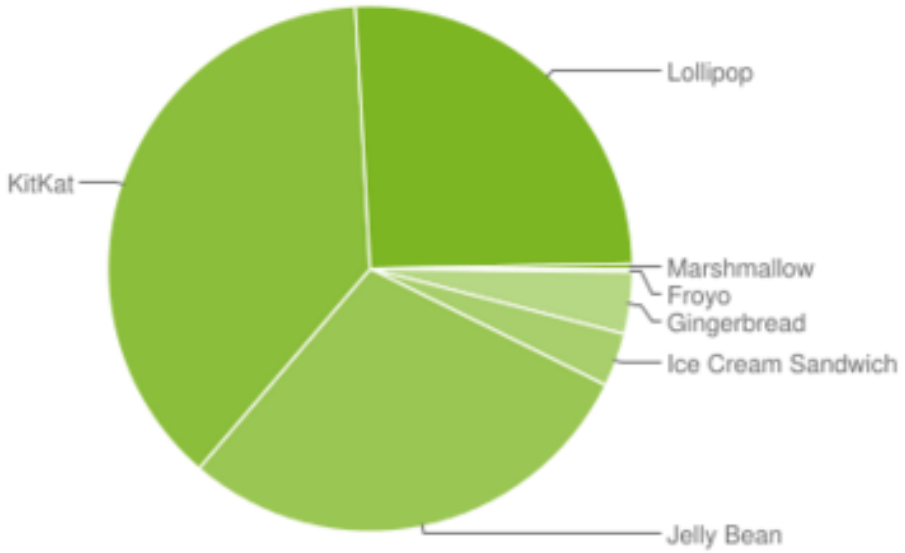
ATUALIZAÇÕES DO ANDROID

- Em janeiro de 2015, a Google decidiu parar de lançar atualizações de segurança para a versão Android 4.3 e anteriores;

- Cerca de 930 milhões de usuários foram prejudicados;

- A causa principal da decisão: o módulo *WebView*. a partir da versão 4.4, ele foi substituído pelo plug-in derivado do “Chromium Project”.

Versão	Codinome	API	Distribuição
2.2	Froyo	8	0.2%
2.3.3 - 2.3.7	Gingerbread	10	3.8%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	3.3%
4.1.x	Jelly Bean	16	11.0%
4.2.x		17	13.9%
4.3		18	4.1%
4.4	KitKat	19	37.8%
5.0	Lollipop	21	15.5%
5.1		22	10.1%
6.0	Marshmallow	23	0.3%



- Dados coletados em Novembro de 2015.
- Quaisquer versões com distribuição inferior a 0,1% não são mostradas.

Fonte: ANDROID DEVELOPERS, 2015 (tradução nossa)

ANDROID 4.3 *Jelly Bean*

(API 18)

- Lançamento: julho de 2013;
- Perfis restritos (controle de pais);
- Suporte a “Bluetooth Smart”;
- Compatível com OpenGL ES 3.0;
- Melhoria do algoritmo do teclado;
- Atualizações descontinuadas em janeiro de 2015.

ANDROID 4.4 *KitKat*

(API 19)

- Lançamento: outubro de 2013;
- Compatível com dispositivos que possuem até 512 MB de RAM;
- Mudanças marcantes no Design;
- Modos de tela cheia *Lean Back* e *Immersive*;
- Novos gestos do usuário com o dispositivo;
- *WebView* substituído pelo plug-in derivado do “Chromium Project”.

ANDROID 5.0 *Lollipop*

(API 21)

- Lançamento: novembro de 2014;
- Criação do "Material Design" um guia completo sobre como implementar o visual, animações e interação entre componentes de um layout;
- Melhoria das notificações (*Lock Screen* e *head-up notifications*);
- Tela de aplicativos recentes (*Overview Screen*) renovado;
- Compatível com OpenGL ES 3.1.

ANDROID 5.1 *Lollipop*

(API 22)

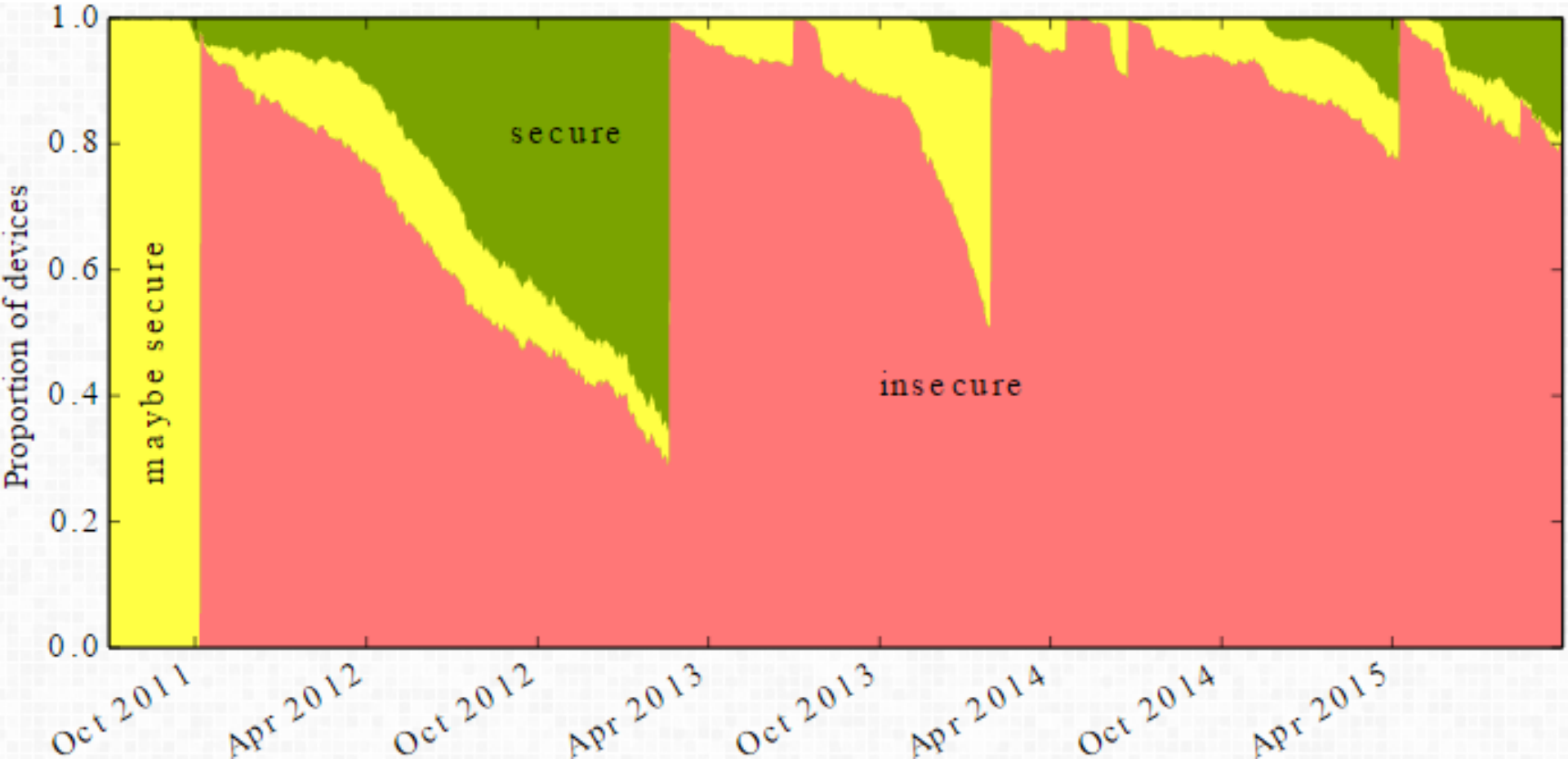
- Lançamento: março de 2015;
- Nova função de segurança, chamada “Proteção de Dispositivos”;
- Recurso de chamada por voz sem ruídos;
- Estabilidade do sistema foi totalmente otimizada e refletiu na drenagem da carga da bateria - como rapidez em conexões sem fio (Wi-Fi, Bluetooth,...).

ANDROID 6.0 *Marshmallow*

(API 23)

- Versão mais recente do Android, lançada em outubro de 2015;
- Melhoria do software leitor de impressão digital;
- Introdução ao “Android Pay”;
- Reformulação do sistema de controle de permissões dos aplicativos;
- Criação de *App Links*;
- Implementações de segurança no *Kernel* (criptografia, backup,...).

PRINCIPAIS VULNERABILIDADES



Fonte: ANDROID VULNERABILITIES, 2015

PRINCIPAIS VULNERABILIDADES

NOME DA VULNERABILIDADE	DATA DA DESCOBERTA
KillingInTheNameOf psneuter ashmem	13 jul. 2010
exploid udev	15 jul. 2010
levitator	10 mar. 2011
Gingerbreak	18 abr. 2011
zergRush	06 out. 2011
APK duplicate file	18 fev. 2013
APK unchecked name	30 jun. 2013
APK unsigned shorts	03 jul. 2013
Fake ID	17 abr. 2014
TowelRoot	03 mai. 2014
ObjectInputStream deserializable	22 jun. 2014
Stagefright	08 abr. 2015
Stagefright2	15 ago. 2015

Fonte: ANDROID VULNERABILITIES, 2015

PRINCIPAIS VULNERABILIDADES

- Stagefright 1.0:
  - Afeta 95% dos dispositivos Android;
  - Ataques via MMS.

- Stagefright 2.0:
  - Bibliotecas *libutils* (desde a versão 1.0 até 5.0) e *libstagefright* (5.0 e superiores)
  - Ataques por arquivos MP3 (áudio) e MP4 (vídeo) “falsos”

PRINCIPAIS VULNERABILIDADES

- Fake ID:
  - Identificação falsa de um aplicativo;
  - Permite que aplicativos maliciosos representem aplicativos confiáveis.

- Towelroot:
  - Ativa o acesso ilegal do *root* no sistema Android.

CONCLUSÃO

- A hipótese inicial foi confirmada e que a pesquisa atendeu ao seu objetivo principal;
- Apesar de apontar algumas vulnerabilidades, o sistema Android pode ser considerado plataforma eficiente e sua interface atrai usuários técnicos e leigos;
- Esta pesquisa se mostrou como uma grande oportunidade para aumentar os conhecimentos da equipe;
- Estudo futuro: analisar a usabilidade nos diferentes dispositivos Android, de forma comparativa, e o que isto pode influenciar na segurança do sistema.

REFERÊNCIAS

- ANDROID. **Android**. 2015. Disponível em: <https://www.android.com>. Acesso em: 18 set. 2015.
- ANDROID DEVELOPERS. **Android Developers - Homepage**. 2015. Disponível em: <https://developer.android.com/>. Acesso em: 18 set. 2015.
- ANDROID OPEN SOURCE PROJECT. **Android Open Source Project (AOSP) - Homepage**. 2015. Disponível em: <https://source.android.com/>. Acesso em: 18 set. 2015.
- ANDROID VULNERABILITIES (Cambridge, ING). University of Cambridge. **Android Vulnerabilities**. 2015. Disponível em: <http://www.androidvulnerabilities.org/>. Acesso em: 23 out. 2015.
- CVE DETAILS. **Google Android: List of security vulnerabilities**. 2015. Disponível em: <http://www.cvedetails.com/vulnerability-list/vendor_id-1224/product_id-19997/Google-Android.html>. Acesso em: 23 out. 2015.
- FERREIRA, Ricardo. **Outras maneiras além do Google Play de instalar aplicativos no Android**. 2013. Disponível em: <http://www.superdownloads.com.br/materias/6850-outras-maneiras-alem-do-google-play-de-instalar-aplicativos-no-android.htm>. Acesso em: 01 nov. 2015.
- GOOGLE PLAY STORE. **Google Play - Homepage**. 2015. Disponível em: <https://play.google.com/>. Acesso em: 18 set. 2015.

REFERÊNCIAS

- LECHETA, Ricardo R. **Google Android: Aprenda a criar aplicações para dispositivos móveis com o Android SDK**. 4. ed. São Paulo: Novatec, 2015. 1016 p.
- NET MARKET SHARE. **Market share for mobile, browsers, operating systems and search engines**. 2015. Disponível em: <https://netmarketshare.com/>. Acesso em: 18 set. 2015.
- TECHTUDO. **Seis dicas para identificar se um aplicativo do Google Play é seguro ou não**. 2015. Disponível em: <http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2013/04/seis-dicas-para-identificar-se-um-aplicativo-do-google-play-e-seguro-ou-nao.html>. Acesso em: 01 nov. 2015.
- TREND MICRO. **Masque, FakeID, and Other Notable Mobile Threats of 2H 2014**. 2014. Disponível em: <http://www.trendmicro.com/vinfo/us/security/news/mobile-safety/masque-fakeid-and-other-notable-mobile-threats-of-2h-2014>. Acesso em: 18 set. 2015.

OBRIGADO!

Antônio Augusto Duarte
(aadm.aquino@gmail.com)

Leonardo Silva
(leonardospfalci@gmail.com)