Colóquio Técnico de Incidentes de Redes

Desafios de segurança em Plataforma móveis

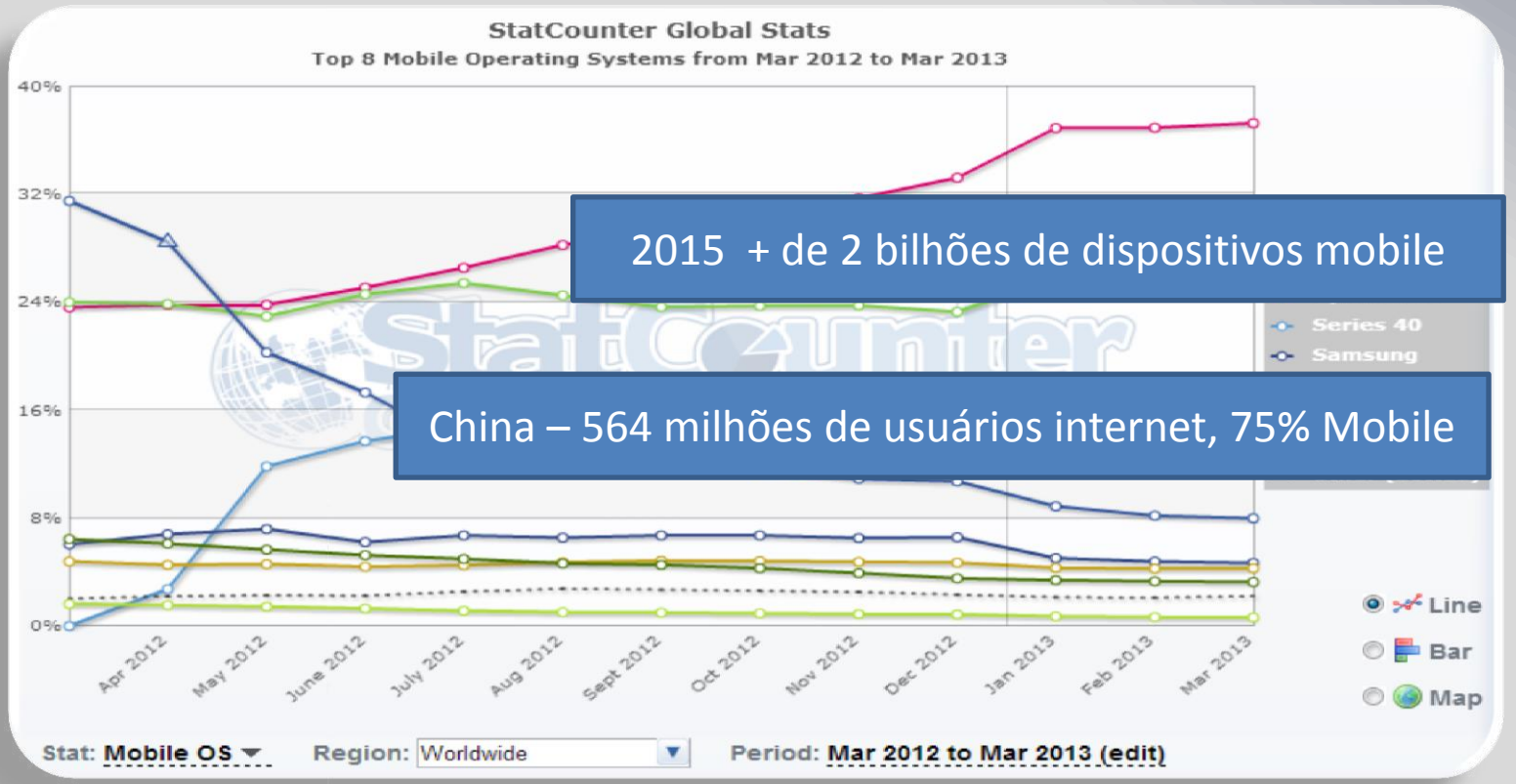
Ricardo Leocádio
ricardo.leocadio@mercantil.com.br

Agenda

- Market Share Mobile OS
- Entendimento básico do mundo mobile
- Uma visão sobre os Malwares Android
  - Análise de reports da Mcafee
    - Android Atack Main-the-middle and remote controlled
    - Android Bank Trojan
  - Infecção By-Driver Mobile
- Notícias de outros mundos mobile
- Lições aprendidas

Market Share Mobile OS

World

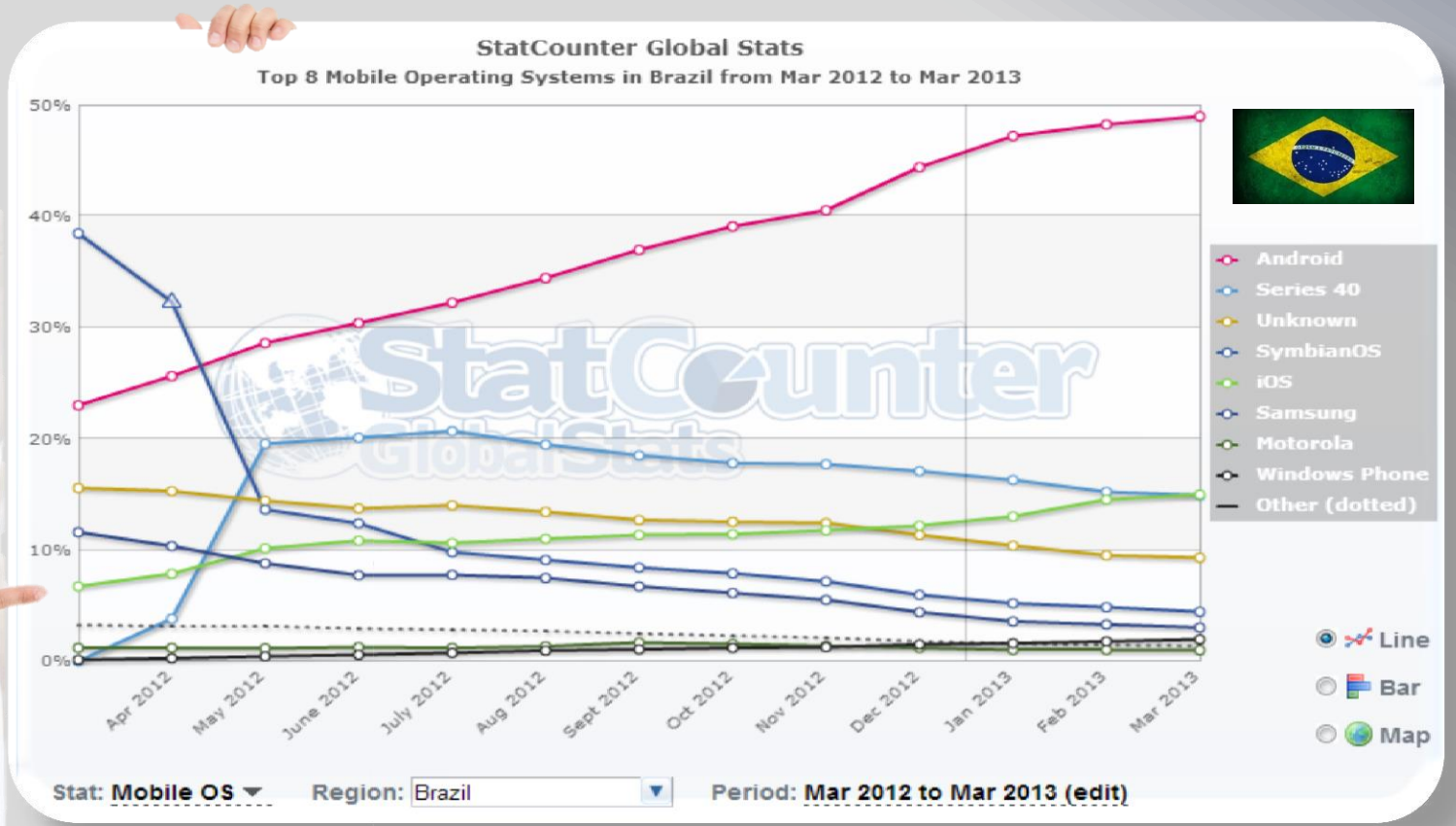


2015 + de 2 bilhões de dispositivos mobile

China – 564 milhões de usuários internet, 75% Mobile

MERCANTIL DO BRASIL

Market Share Mobile OS



MERCANTIL DO BRASIL

Mobile Threats & the Underground Marketplace

APWG White Paper

Figure 1 Countries at Most Risk

Fonte: APWG

Onde estamos

- Market Share Mobile OS
- Entendimento básico do mundo mobile
- Uma visão sobre os Malwares Android
  - Análise de reports da Mcafee
    - Android Atack Main-the-middle and remote controlled
    - Android Bank Trojan
  - Infecção By-Driver Mobile
- Notícias de outros mundos mobile
- Lições aprendidas

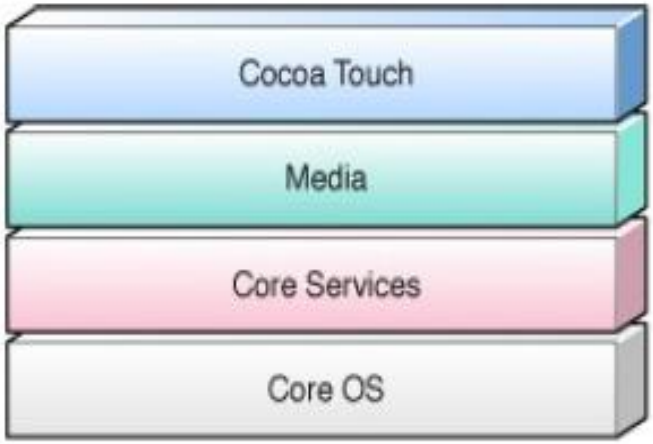
Entendimento básico do mundo Mobile

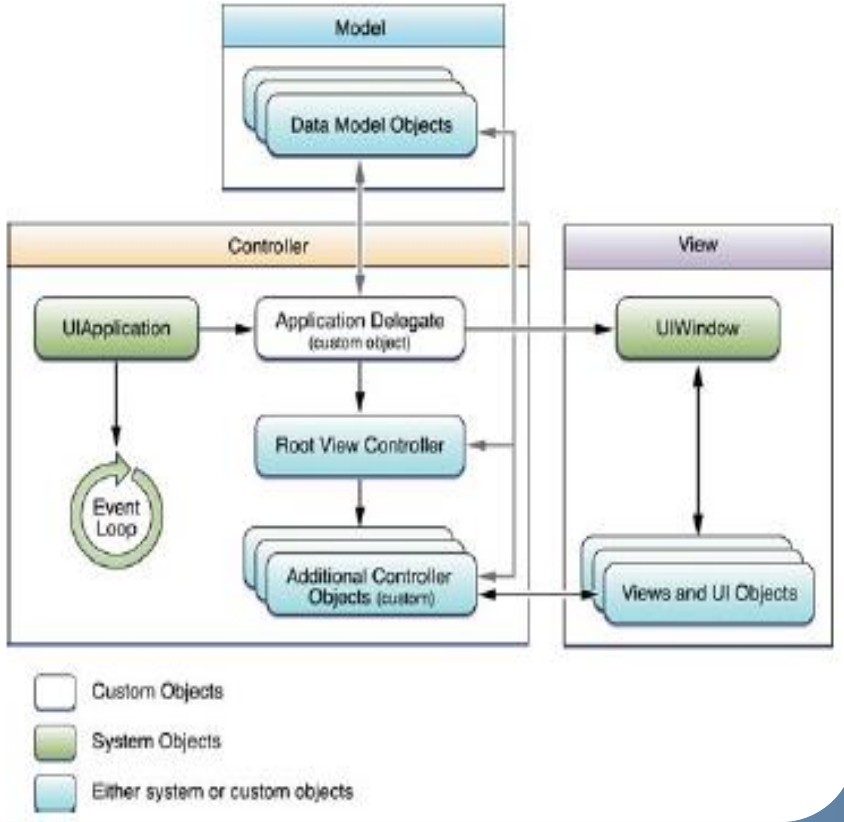
Componentes

COCOA TOUCH	ACTIVITY (Broadcast Receiver / Intent)
MEDIA	SERVICES
CORE SERVICES	Dalvik VM + Libraries
CORE OS	LINUX KERNEL

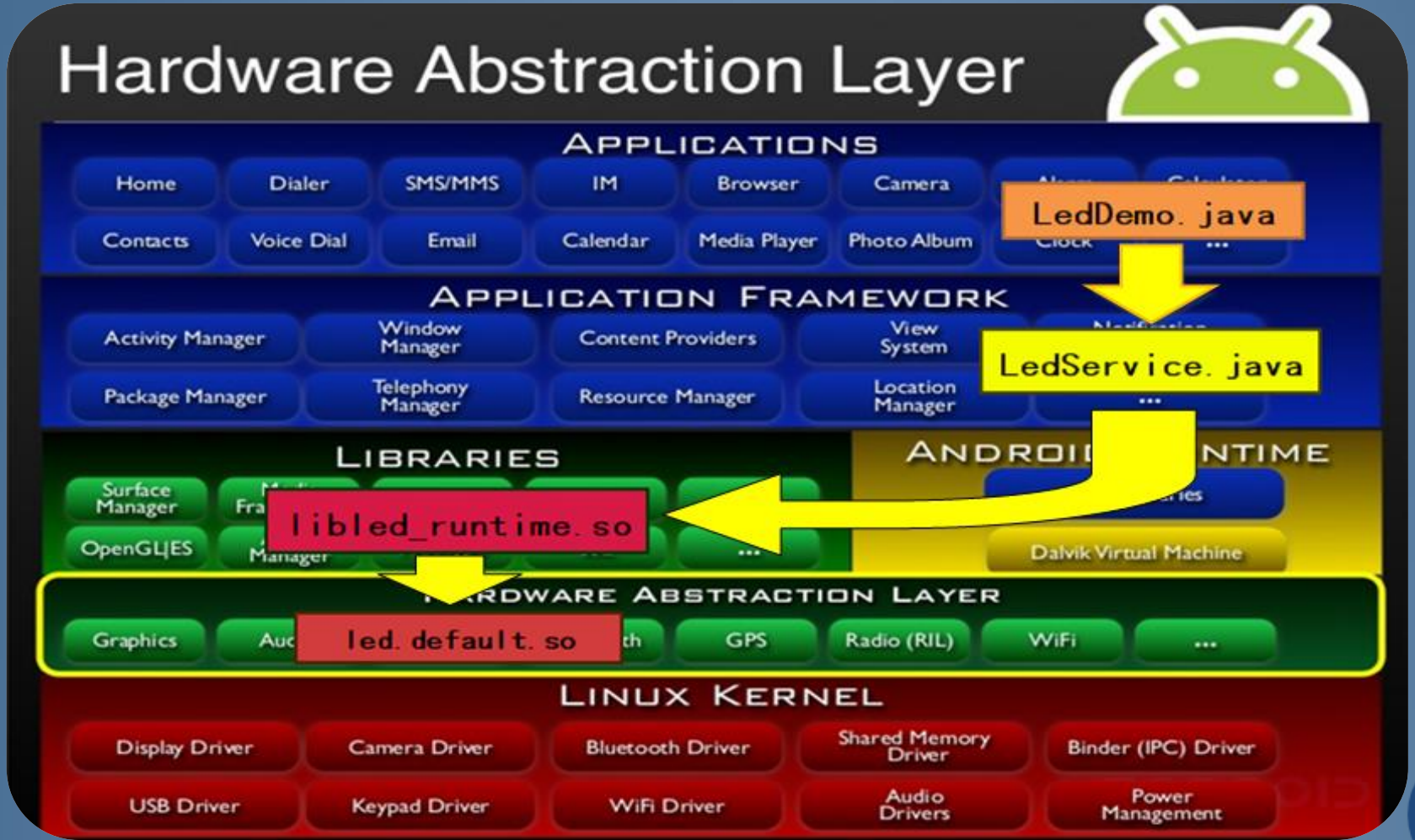
Entendimento básico do mundo Mobile

Arquitetura





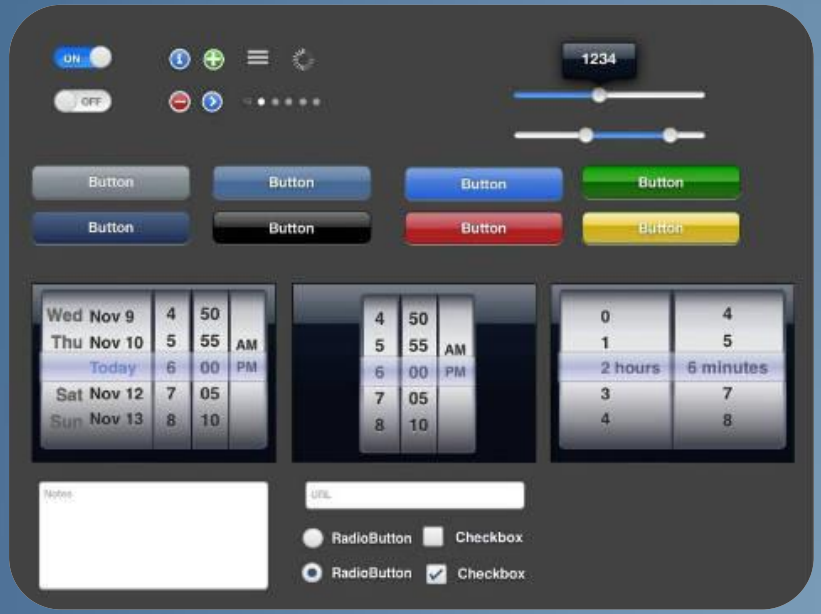
Entendimento básico do mundo Mobile



Entendimento básico do mundo Mobile

Construção de um APP

Native screen



Funcionamento on-line/off-line

WEBVIEW

Funcionamento somente on-line

GUI: HTML

Entendimento básico do mundo Mobile

- Segurança

Não permite acesso ao File System (APP confinado)

Ambos possuem segurança no sistema de arquivos baseada em User/Group/Others
(**R**- read, **W** – write, **X** – executable)

Permite acesso ao File System para USER e entre APP's

Um APP só é executado no contexto de um usuário. Não compartilha dados ou memória.

- Aceita execução como ROOT
- Pode compartilhar se alterar permissão

Um APP antes de executar verifica sua assinatura digital

Manifest.PLIST

Um APP antes de executar verifica seu "Manifesto"

Manifest.XML

Entendimento básico do mundo Mobile

Instalação de fontes alternativas

Black Market

RISCO

Entendimento básico do mundo Mobile

Exemplo de arquivo AndroidManifest.xml

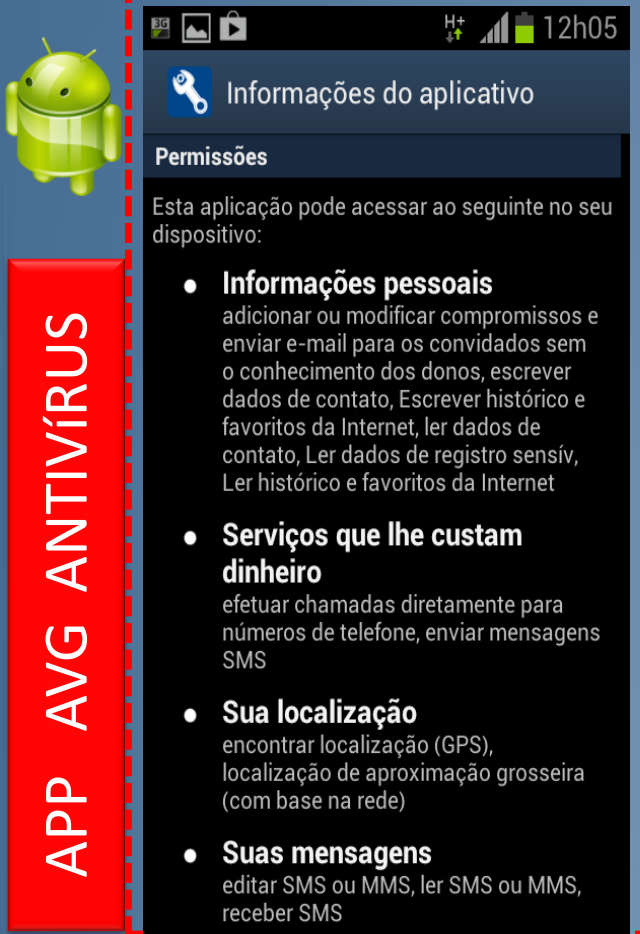
```
<?xml version="1.0" encoding="utf-8"?>
  <manifest xmlns:android="http://schemas.android.com/apk/res/android"
   package="br.com.exemplo.oimundo"
   android:versionCode="1"   android:versionName="1.0">
    <application android:icon="@drawable/icon" android:label="@string/app_nam
      <activity android:name=".OiMundo"
       android:label="@string/app_name">
        <intent-filter>
          <action android:name="android.intent.action.MAIN" />
          <category android:name="android.intent.category.LAUNCHER" />
        </intent-filter>
      </activity>
    </application>
  </manifest>
```

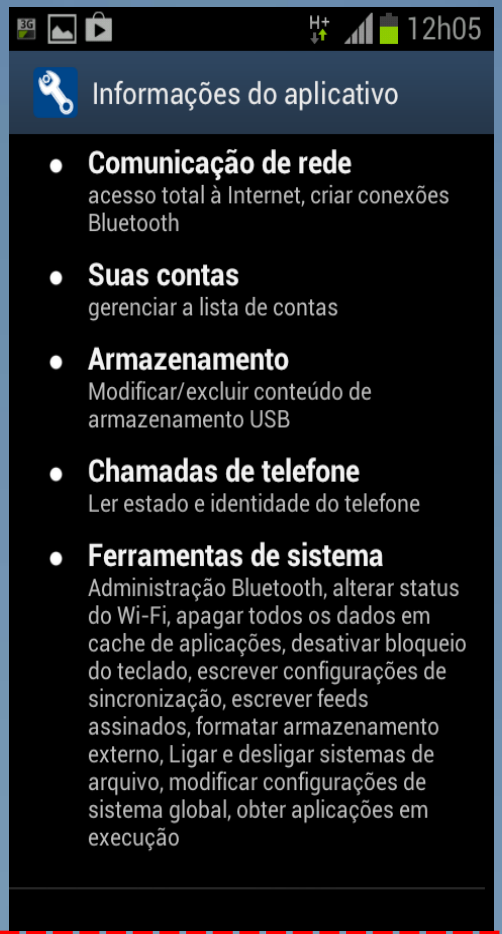
É obrigatório que cada elemento do projeto esteja declarado no arquivo de manifesto, caso contrário não é possível utilizá-lo.

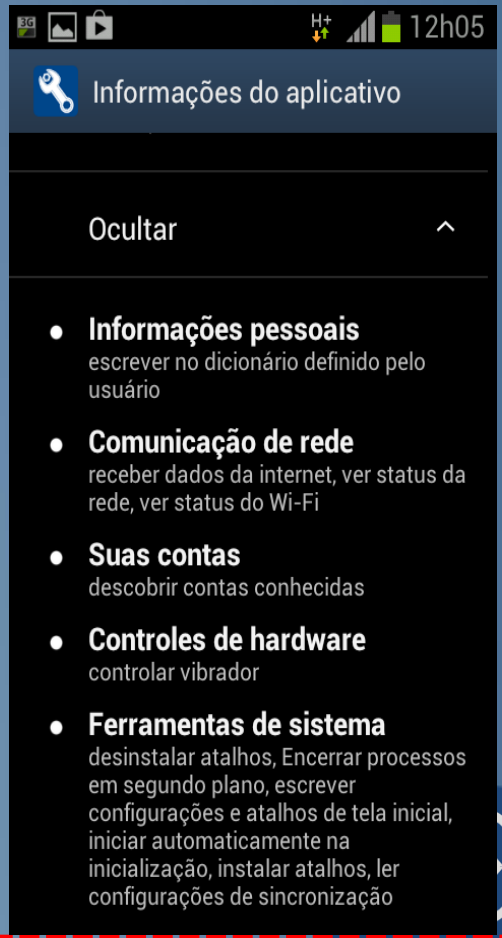
Entendimento básico do mundo Mobile

Ações declaradas em um manifesto.

APP AVG ANTIVíRUS







Onde estamos

- Market Share Mobile OS
- Entendimento básico do mundo mobile
- Uma visão sobre os Malwares Android
  - Análise de reports da Mcafee
    - Android Atack Main-the-middle and remote controlled
    - Android Bank Trojan
  - Infecção By-Driver Mobile
- Notícias de outros mundos mobile
- Lições aprendidas

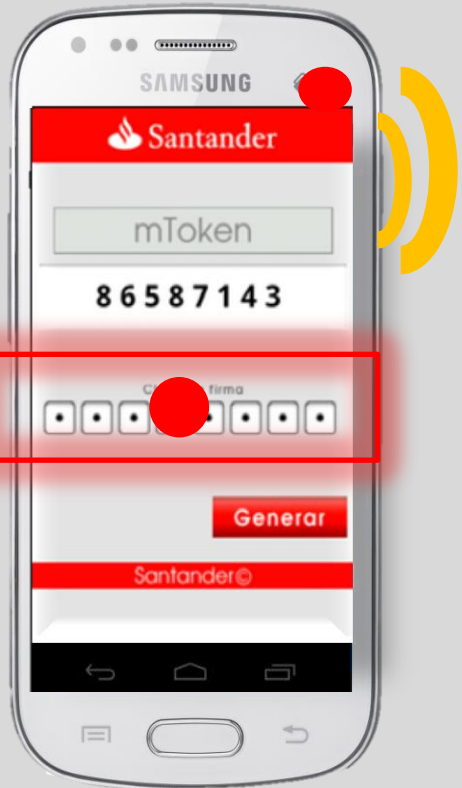
As ameaças apresentam-se

- Arquitetura e Infraestrutura → Mobile DNS, monitoramento de tráfego e comunicaçoes (Wi-fi, 3G, SMS, Bluetooth, NFC)

- Hardware → Sensores, GPS, Câmeras, Teclado
- Software → Sistema operacional, APP e lojas (black Market)
- Permissão do sistema → Compartilhamento de informações

Você conhece o Flexispy?

Android Man-in-the-Middle com o Remote-Controlled Trojan Bancário



MERCANTIL DO BRASIL

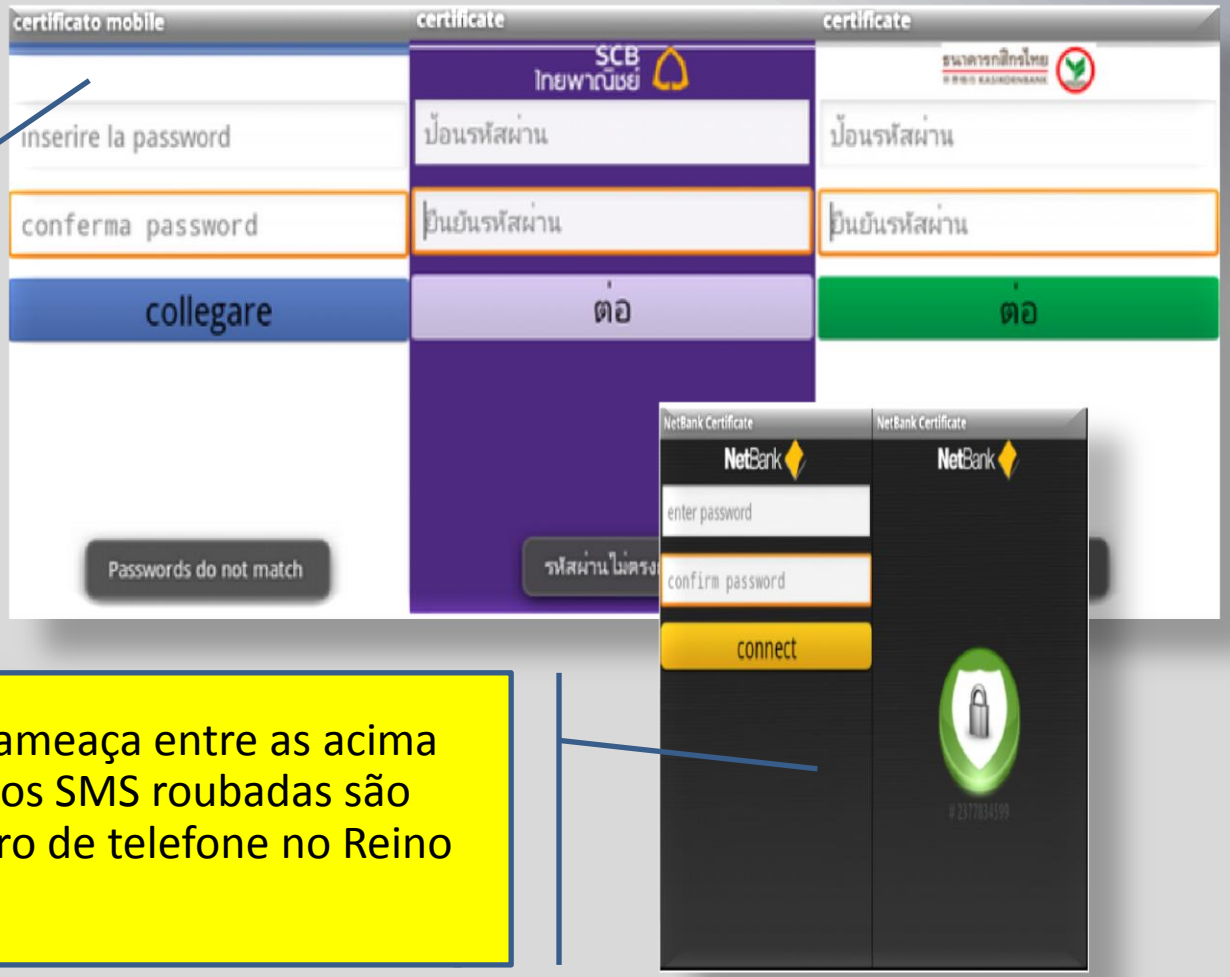
Comercialização

Sample Toolkits & Service	Price (US$) - March 2013	Example Descriptions
Mobile intrusion (keyloggers)	Open Source - 400	Java & Python Keyloggers, Mobistealth,
Mobile Intrusion (surveillance)	500 – 5,000	Re-engineered Finfisher, Finfisher Lite & FlexiSpy extended copies
Mobile malware for banking theft	10,000 – 30,000	Eurograbber, ZitMo, Tinba Trojan, DroidCleaner, Citadel (inc. PtH capabilities)
Mobile botnet (rental)	50 - 400	Hourly rates
Mobile botnets (operational & tailored source code)	4,000 - 30,000	Mobile ISP service, SMS, & Drive by
Mobile malware for black SEO and underground partnership programs	5,000 – 10,000	Used to traffic redirects, J2ME midlets, or standard applications for the popular platforms.
Mobile traffic by targeted country	10 – 30 per 1,000 hosts	Can be bought through special underground services (by area, by country)
Mobile SMS spam service	2-8 cents per 1 SMS	Mobile spamming
Mobile SMS spamming tool	30-50	SMS spamer by klychev v0.3
Mobile flooder (Skype or SIP)	30-80	Skype Flooder

Fonte: APWG

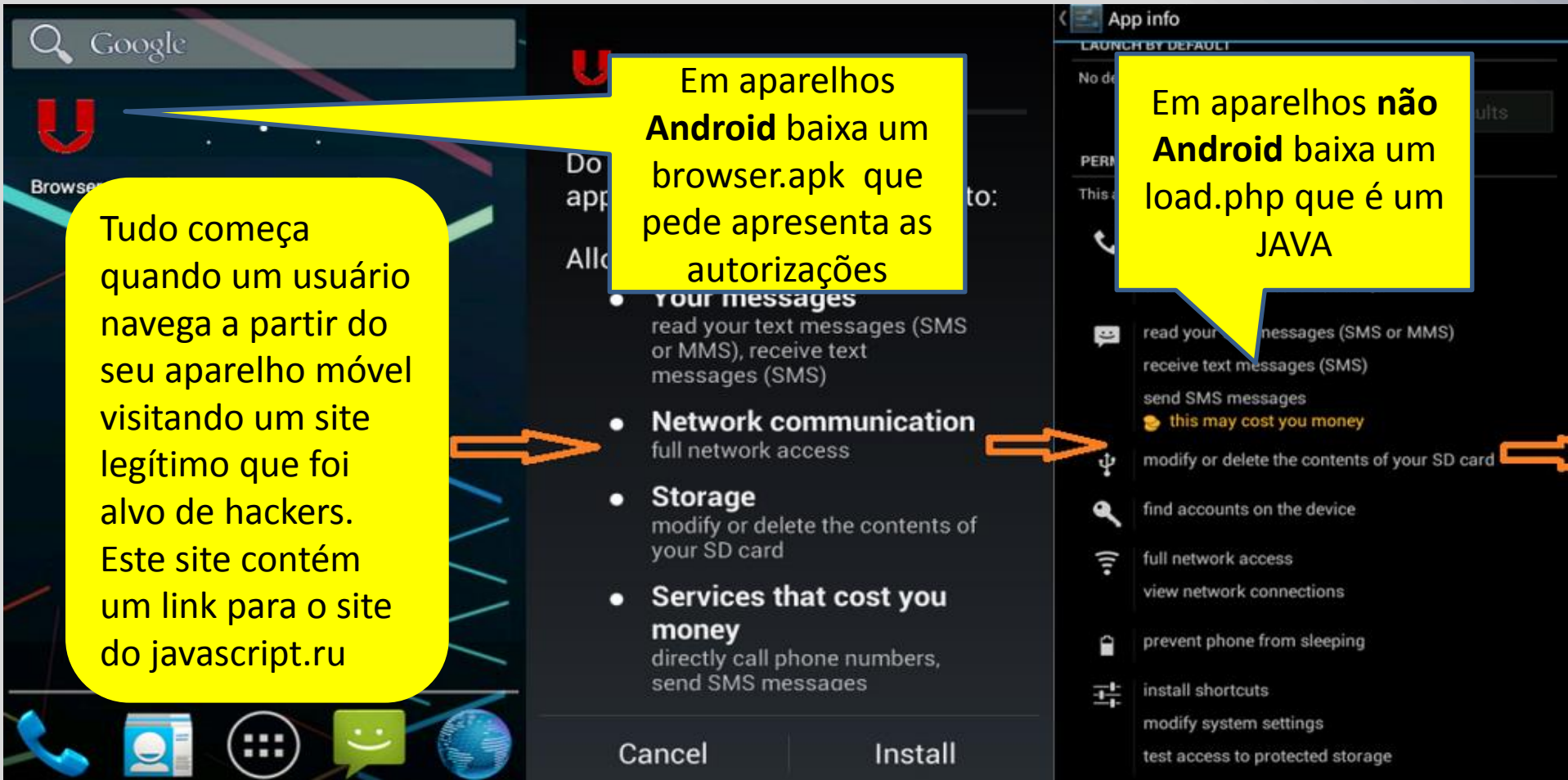
Android Banking Trojans alvo Itália e Tailândia

Este malware identificado pela MCAFEE engana o usuário e envia a senha para o atacante via Internet ou SMS na Rússia.



A única diferença desta ameaça entre as acima que descrevemos é que os SMS roubadas são enviadas para um número de telefone no Reino Unido.

Infecção por Driver-By Mobile



BadNews Android

Como funciona

"BadNews" - Vírus para Android teve mais de 9 milhões de downloads

"BadNews" – Vírus para Android teve mais de 9 milhões de downloads

Postado por Wagner Junior em abr 22, 2013 no Aplicativos, Mobile, Quick News | Sem comentários ainda

Este novo tipo de vírus foi descoberto em ao menos 32 aplicativos e jogos disponíveis para download no Google Play.

O vírus foi descoberto pela empresa de segurança Lookout Mobile Security, que publicou a novidade em seu blog, na última sexta-feira. Logo após a publicação, o Google removeu todos os programas que estavam disponíveis em sua loja virtual e que continham o malware. A novidade desta inclusão de vírus, mesmo no Google Play, é que aparentemente os apps haviam sido aprovados pelo Google e o vírus foi inserido após isso, como forma de atualização dos apps.

1º APP disponível é legítimo e fica um bom tempo até ganhar score +

Google play

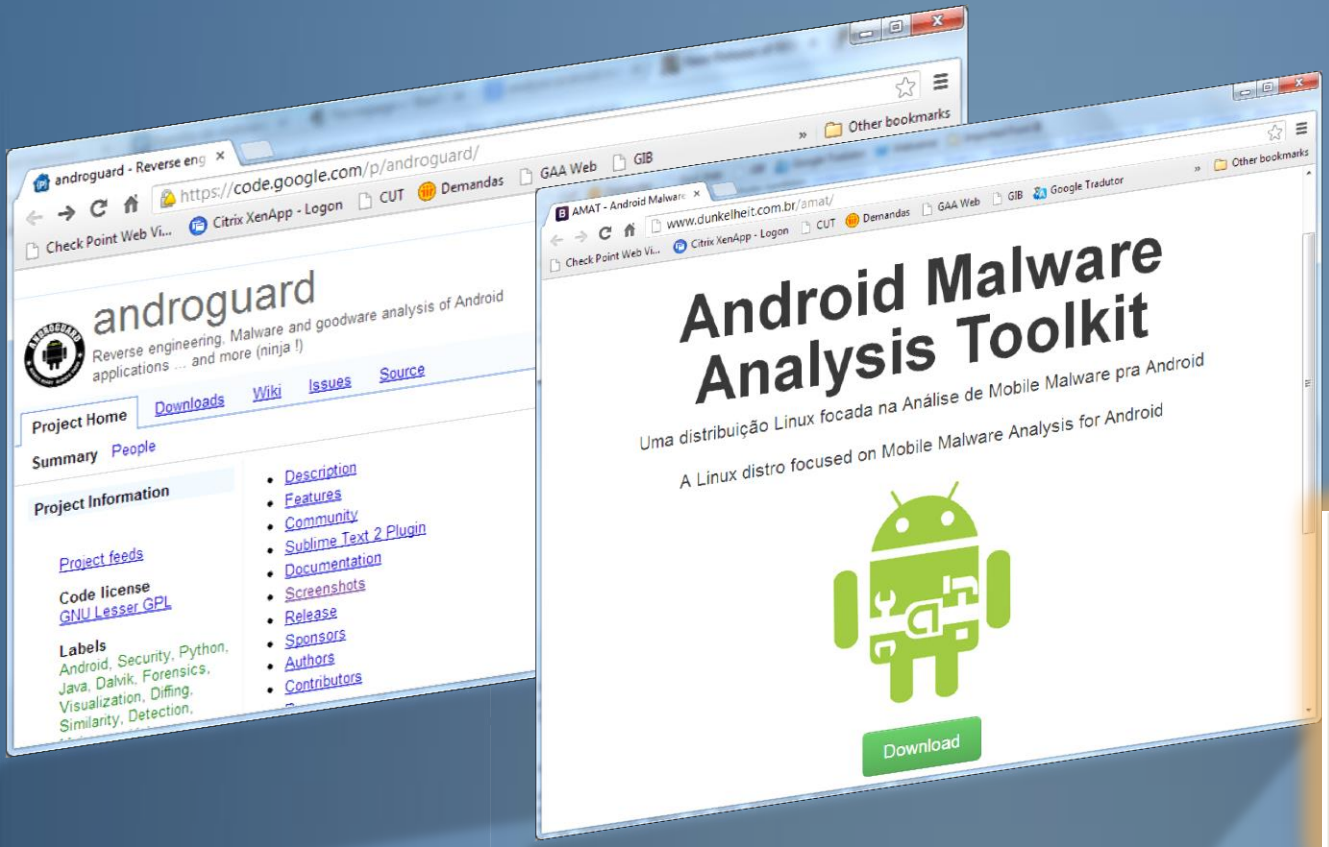
Ao receber atualização o malware entra em ação enviando dados do usuário para o fraudados

Google play

MERCANTIL DO BRASIL

Ferramentas de análise

- Começam a surgir as primeiras ferramentas de análise automatizado de mobile malware.



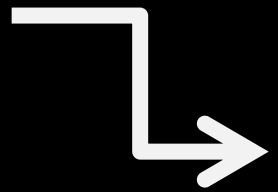
O Processo consiste em:

- Descompactar o arquivo
- Examinar os arquivos ".class" utilizando as ferramentas disponíveis na web;
- Encontrar partes do código que envolvam as ações do malware.

Exemplo.: 'sms :/ /'

```
01. /0SIF|6XI8ULE|YNLD5QDA6WM|YJ90RL/
02. while 7375/88600168904|7202/65510
    1283|8385/88600168904|
03. 1 16
04. 2 33
05. 3 49
06. 4 66
07. 7375 88600168904 //sms://7375
08. 7202 65510006691 //sms://7202
09. 1899 fteme 1283 //sms://1899
10. 8385 88600168904 //sms://8385
11. decoded
```

Onde estamos



- Market Share Mobile OS
- Entendimento básico do mundo mobile
- Uma visão sobre os Malwares Android
  - Análise de reports da Mcafee
    - Android Atack Main-the-middle and remote controlled
    - Android Bank Trojan
  - Infecção By-Driver Mobile
- Notícias de outros mundos mobile
- Lições aprendidas

Notícias do Mundo Mobile

Primeiro cavalo de troia para iPhone, iPad e iPod

Publicado em 8 de julho de 2012 por Kadu Soares

Após longo tempo sem histórico de Malwares, a Apple sofre sua primeira ameaça com um aplicativo capaz de enviar dados dos aparelhores para uso indevido.

Especialista em segurança da Kaspersky afirma ter identificado um cavalo de troia criado para dispositivos móveis da Apple – iPhone, iPad e iPod, disfarçado como um aplicativo chamado "Find and Call", que também teria uma versão para aparelhos Android. A Apple já tomou providência e retirou o aplicativo da App Store.

Em um post, Denis Maslennikov, especialista do laboratório da Kaspersky, explica que ao instalar o cavalo de troia (programa malicioso que abre brechas de segurança no dispositivo onde está instalado), o aplicativo envia a lista de contatos dos dispositivos para um servidor remoto. Os dados são usados posteriormente nesse servidor remoto para envio de spams via SMS. O alvo principal são usuários da Rússia.

Maslennikov disse ter entrado em contato com a Apple e Google para informar sobre o aplicativo malicioso, mas ainda

29/11/2012 17h41 - Atualizado em 29/11/2012 18h20

Windows Phone 8 ganha primeiro malware pelas mãos de adolescente

Aline Jesus
Para o TechTudo

12 comentários

Tweet

O **Windows Phone 8** pode ter um grande problema pela frente: um malware supostamente criado por um indiano de apenas 16 anos. Shantanu Gawde garantiu que conseguiu quebrar o código do novo sistema operacional da **Microsoft**, demonstrando como fez o *hack* em um evento chamado MalCon Security Conference, em um evento nesta última semana, em Nova Deli.

O novo sistema operacional móvel da Microsoft teve seu primeiro malware desenvolvido (Foto: Divulgação)

Notícias do Mundo Mobile

categoria : softwares | 08.02.2013 / 17h14 | comentários : 7

TAMANHO DO TEXTO -A +A

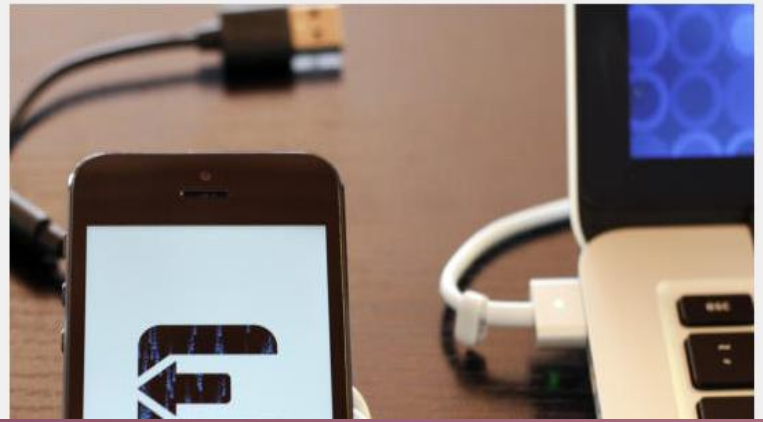
Com 7 milhões de usuários, Evasi0n é o jailbreak mais popular já feito

autor: risastoider

A mais nova ferramenta de jailbreak para o **iOS**, o **Evasi0n**, foi responsável pelo desbloqueio de mais de 7 milhões de dispositivos desde seu lançamento há quatro dias. Isso o torna o jailbreak mais popular já criado para o sistema.

Os dados, conforme o Slashgear, foram cedidos por Jay Freeman, o homem por trás da app store alternativa Cydia. Ele detectou todo esse número de usuários na sua loja, afirmando que o Evasi0n trouxe a ela "um novo tráfego insano".

Assine a tag evasi0n para ser avisado sempre que novos conteúdos marcados pela tag forem publicados



Andy Greenberg, Forbes Staff

Covering the worlds of data security, privacy and hacker culture.

+ Follow (800)

SECURITY | 2/08/2013 @ 8:00AM | 56.288 views

Evasion Is The Most Popular Jailbreak Ever: Nearly Seven Million iOS Devices Hacked In Four Days

15 comments, 10 called-out + Comment Now + Follow Comments

Over the last half a week, Apple has been hit with the largest mass-hacking incident in its history. And the perpetrators were the company's own users.

Nearly seven million iPhone, iPad and

Notícias do Mundo Mobile

O **Jailbreak** poderá ser considerado crime no Brasil. | iPod School
ipodschool.com/.../o-**jailbreak**-podera-ser-considerado-crime-no-brasil/
Parece que até os fãs de **jailbreak** estão correndo perigo de cadeia com essa lei em vigor, ela pode fazer com que os **usuários** do método peguem até 1 ano de ...

Reddit faz uma pesquisa para tenta identificar a - **Jailbreak** Space
www.**jailbreak**-space.com/2013/.../reddit-faz-uma-pesquisa-para-tenta.ht...
19/03/2013 – Dentro do Reddit, existe uma enorme comunidade **Jailbreak** com pessoas em busca de informação, e ainda tem os **usuários** mais experientes ...

12/04/2012 – Obs: Infelizmente, grande parte dos **usuários** que conheço e **usam** o **jailbreak**, o fazem para instalar apps pirateados. Se você é um desses, ...

Cinco razões para você NÃO fazer **jailbreak** no seu iPhone (ou ...
www.techtudo.com.br/.../cinco-razoes-para-voce-nao-fazer-**jailbreak**-no-...
26/05/2011 – 1 - Boa parte dos **usuários** simplesmente não precisam do **jailbreak** ... por você, mas **porque** não fazem muita questão de estudarem esses recursos. ... computacionais que os **usuários** que só **usam** o computador para ver ...

Blog do **Jailbreak** » dicas - Macworld - Uol
macworldbrasil.uol.com.br/blog/**jailbreak**/category/dicas/
15/08/2012 – Vídeo: Como fazer **jailbreak** sem problemas no iOS 5.1.1 .... Se você ainda não fez **jailbreak porque** não sabe usar, então aqui vai a dica ... por conta de alguns **usuários** mal-intencionados, que **usam** a liberdade oferecida ...

5 razões para fazer **jailbreak** no iPhone ou iPad - Macworld - Uol
macworldbrasil.uol.com.br › Home › Aplicativos
30/01/2012 – Como você já deve saber, o **jailbreak** libera acesso a aplicativos não ... por conta de alguns **usuários** mal-intencionados, que **usam** a liberdade oferecida ....
Isso eh uma merda **pq** pelo aplicativo do facebook vc pode marcar

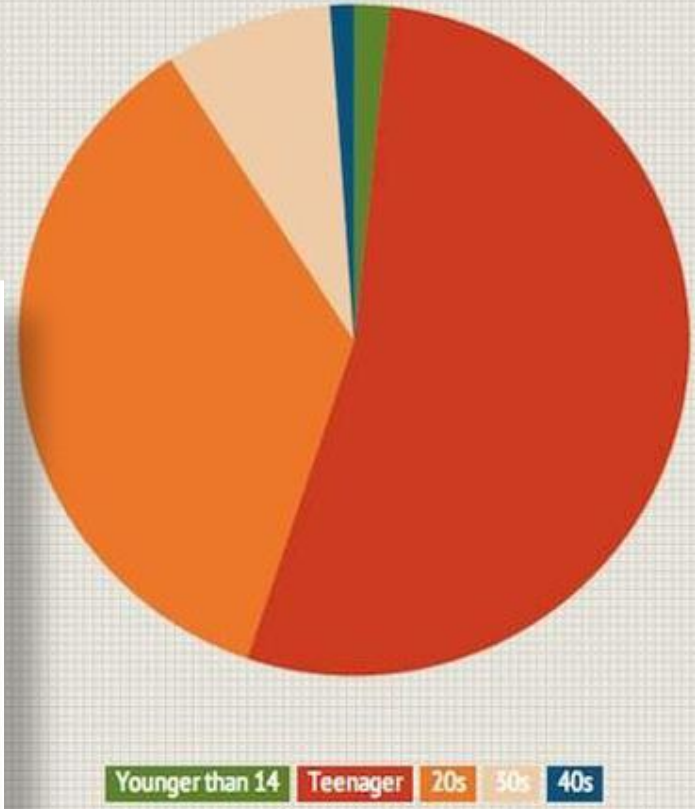
Perfil Jailbreak

/R/JAILBREAK SURVEY

THANKS TO THE 360+ PEOPLE WHO PARTICIPATED!

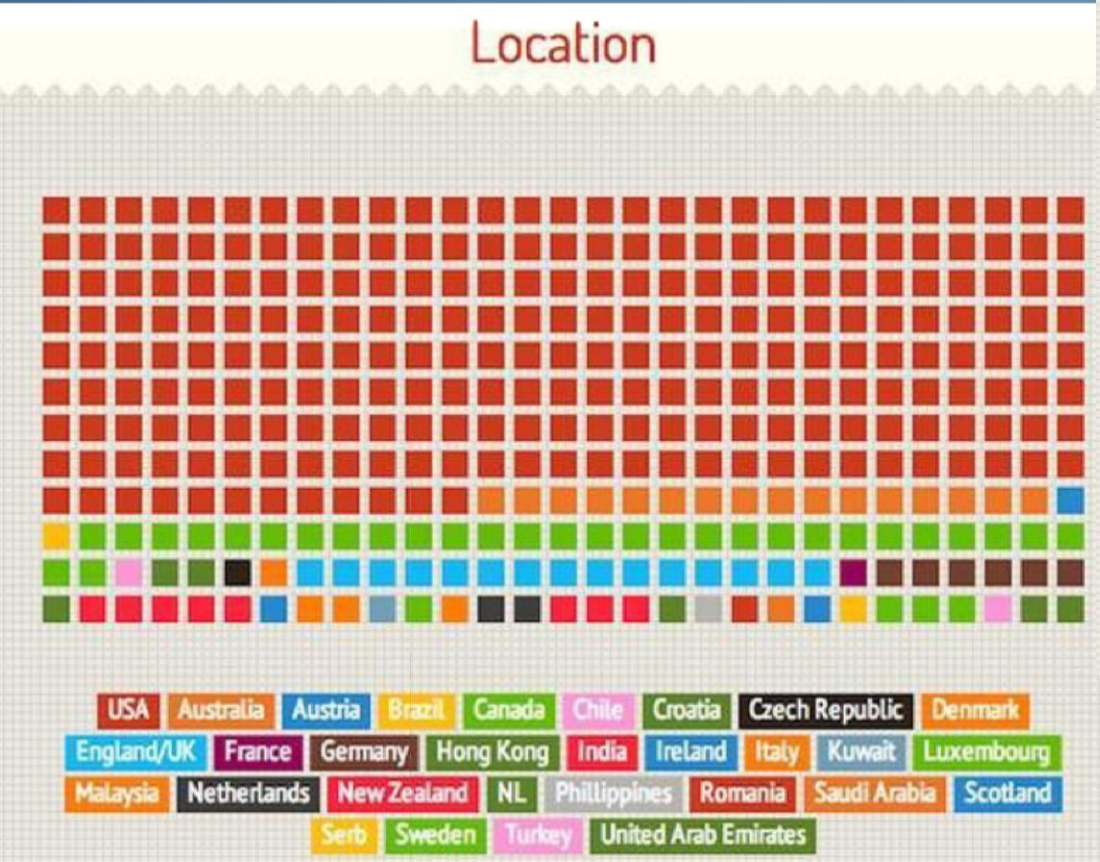
HOSTED BY: /U/SPICEMAN54J

Gender and Age



Fonte: Reddit

Perfil Jailbreak



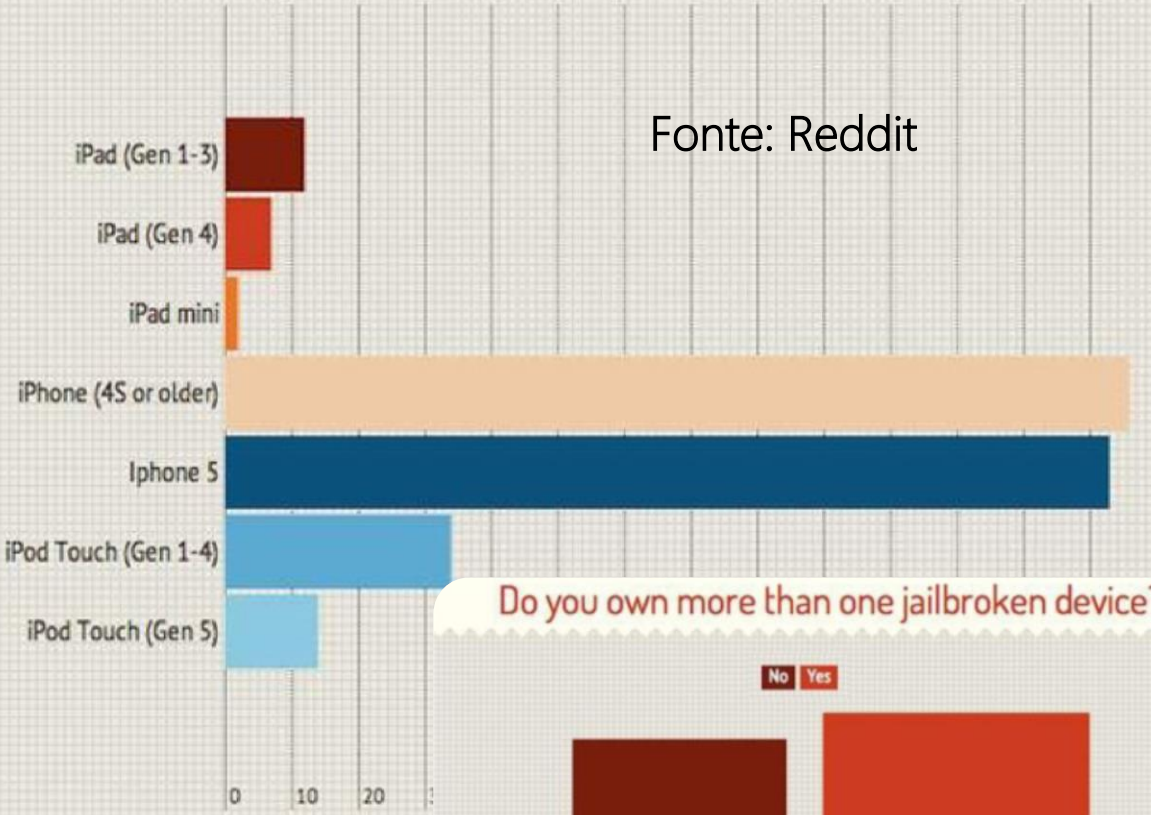
Fonte: Reddit

Perfil Jailbreak

What iOS version are you on?

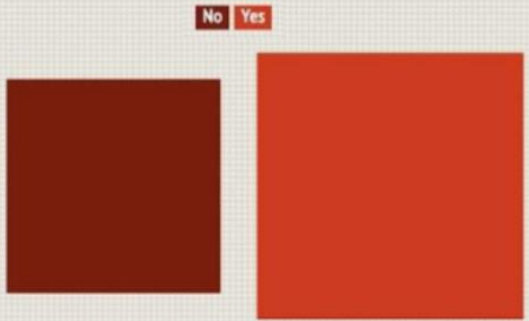
iOS 4.x.x | iOS 5.x.x | iOS 6.0 | iOS 6.0.1 | iOS 6.1 | iOS 6.1.x

What iDevice do you use most often?



Fonte: Reddit

Do you own more than one jailbroken device?



Notícias do Mundo Mobile

...are
...one – O smartphone mais hackeado…

iPhone – O smartphone mais hackeado...

2013-03-31 02:00:58

Conheças quem são os mais vulneráveis dos últimos de 25 anos

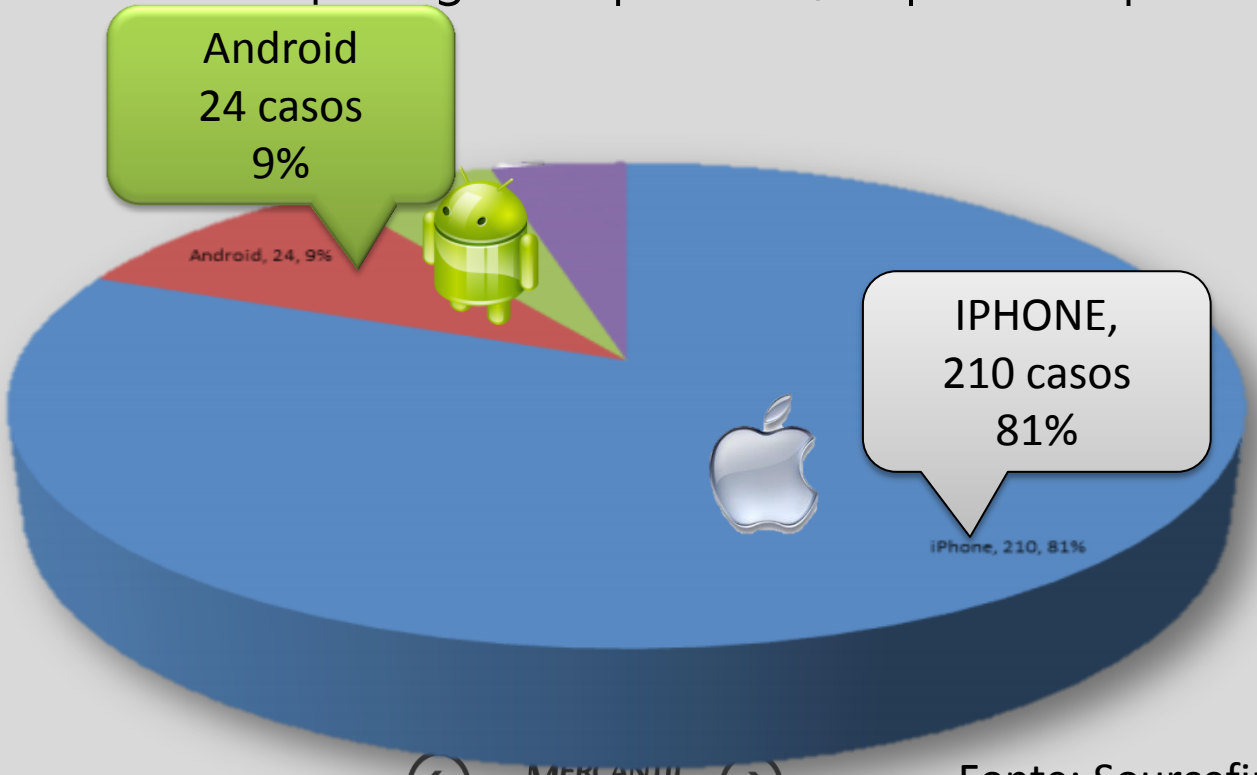
As vulnerabilidades estão presentes na maioria dos sistemas. A empresa de segurança SourceFire, disponibilizou recentemente um relatório intitulado "25 Years of Vulnerabilities " (em português – 25 anos de vulnerabilidades), onde se podem consultar os resultados,interessantíssimos, sobre as CVE (Critical Vulnerabilities and Exposures) dos últimos anos, presentes em vários sofwares e dispositivos móveis.

Fonte: www.pplware.com

MERCANTIL DO BRASIL

Notícias do Mundo Mobile

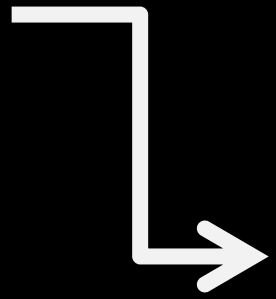
- Total 210 vulnerabilidades no IPHONE, que corresponde a cerca de 81%, seguido pela plataforma Android que registou apenas 24, o que corresponde a 9%.



Fonte: Sourcefire

Entenda as informações ao ler

Onde estamos



- Market Share Mobile OS
- Entendimento básico do mundo mobile
- Uma visão sobre os Malwares Android
  - Análise de reports da Mcafee
    - Android Atack Main-the-middle and remote controlled
    - Android Bank Trojan
  - Infecção By-Driver Mobile
- Notícias de outros mundos mobile
- Lições aprendidas

Isso é igual em outro sistema operacional

Minha percepção sobre o mundo mobile

MERCANTIL DO BRASIL

Dificuldades encontradas

- Usuários preparados e conscientes;
- Diversidade de sistemas operacionais para dispositivos móveis;
- Pouca oferta no mercado de ferramentas forense para dispositivos móveis;
- Pouca literatura e profissionais de segurança para dispositivos móveis;
- Diversidade de operadoras, aparelhos e conectores;

Minha percepção sobre o mundo mobile

Lições aprendidas

- Em geral, os aplicativos maliciosos Mobile não são complexos em comparação com ameaças mais sofisticadas de PC.
- As principais vulnerabilidades se apresentam no mundo Android devido a criação do APP, já no mundo IOS as principais vulnerabilidades estão no sistema operacional.
- O rigor da publicação de um APP pode melhorar significativamente o risco/exposição do usuário.
- Tentativa de portar modalidades de malware do mundo Windows para o mobile continuam a ser testadas.
- A falta de suporte do fabricante pode favorecer lojas virtuais como o Jailbreak.
- Programas de antivírus continuam a ser reativos as ameaças de mobile malware.


MERCANTIL DO BRASIL
Obrigado!
Ricardo Leocádio
prof.ricardoleocadio@gmail.com

Referências utilizadas

- http://www.apwg.org
  Acessado em 15/05/2013
- http://blogs.mcafee.com/mcafee-labs/android-malware-pairs-man-in-the-middle-with-remote-controlled-banking-trojan
  Acessado em 18/03/2013
- http://blogs.mcafee.com/mcafee-labs/android-banking-trojans-target-italy-and-thailand
  Acessado em 21/03/2013
- http://jornalterceiravia.com.br/blog/kadusoares/primeiro-cavalo-de-troia-para-iphone-ipad-e-ipod
  Acessado em 21/03/2013
- http://www.techtudo.com.br/noticias/noticia/2012/11/windows-phone-8-ganha-primeiro-malware-pelas-maos-de-adolescente.html
  Acessado em 21/03/2013
- http://blog.avast.com/pt-br/2013/03/28/mobile-drive-by-malware-example-2/
  Acessado em 10/04/2013
- http://community.qualys.fr/servlet/JiveServlet/previewBody/1541-102-1-1535/Sourcefire%2025%20Years%20of%20Vulnerabilities%20Research%20Report-%20A4%20(1)%20-%20copie.pdf
  Acessado em 02/04/2012
- http://www.jailbreak-space.com/2013/03/reddit-faz-uma-pesquisa-para-tenta.html
  Acessado em 26/04/2012