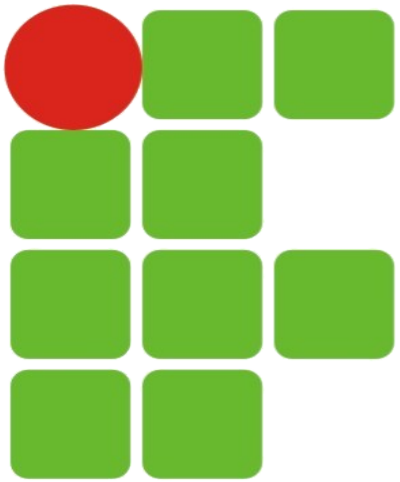
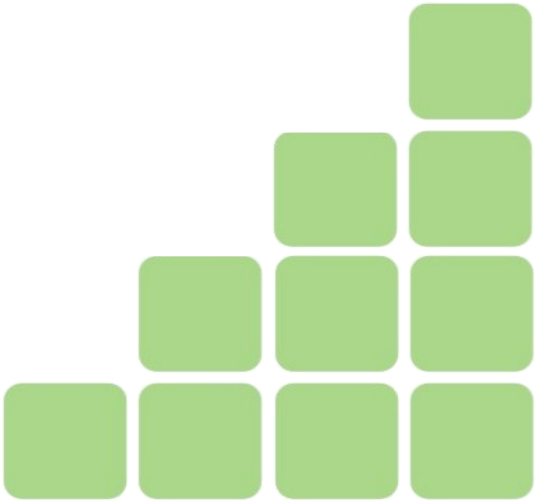


INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

(In)Segurança em Dispositivos Móveis com Android

Ricardo Kléber Martins Galvão
www.ricardokleber.com
ricardo.galvao@ifrn.edu.br
www.twitter.com/ricardokleber



Grupo de Pesquisa no IFRN

Linha Específica

Grupo de Pesquisa em

Segurança da Informação e Software Livre

SEGURANÇA DE REDES

www.segurancaderedes.org

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

O Crescimento no Uso de Celulares

Cenário Mundial (Contextualizando)

- Número de Televisores: **1,5 bilhão**
- Número de pessoas que acessam Internet: **1 bilhão**
- Número de aparelhos celulares em uso: **Mais de 3 bilhões**

(metade da população mundial)

Fonte: OHA (www.openhandsetalliance.com)

Smartphones :: Números

Cenário Mundial

IMS research
excellence in market intelligence

420 Milhões de Aparelhos Vendidos em 2011

As vendas globais de smartphones vão superar a marca de 420 milhões de aparelhos em 2011, aponta levantamento da IMS Research. Sob essa projeção, os dispositivos vão responder por cerca de **28% do mercado mundial de celulares** até o fim do ano.

Segundo a consultoria, com a maior variedade de modelos e preços mais acessíveis, **as vendas anuais vão ultrapassar um bilhão de dispositivos até 2016**, respondendo por um em cada dois celulares vendidos no período.

LG e Nokia apresentam resultados negativos comparados a Apple e Samsung. Um conjunto de fatores explicam o insucesso de alguns fabricantes, como design pobre dos aparelhos, interfaces de usuário insatisfatórias, portfólios que não oferecem recursos diferenciados e **Sistema Operacional escolhido**.

Em outra frente, o estudo ressalta os bons resultados da Apple, mas indica que a empresa de Steve Jobs não estará sozinha nesse cenário. O principal concorrente, segundo a pesquisa, é a Samsung, que ampliou sua participação no mercado de smartphones de 3% no primeiro trimestre de 2010 para mais de 13% no período correspondente em 2011.

Smartphones :: Números

América Latina

http://www1.folha.uol.com.br/mercado/1001933-vendas-de-smartphones-somarao-us-6-bi-na-america-latina-em-2011.shtml

FOLHA.com

04/11/2011 - 20h52

Vendas de smartphones somarão US$ 6 bi na América Latina em 2011

A venda de smartphones na América Latina deve gerar receitas de US$ 6 bilhões em 2011, de acordo com dados da empresa de pesquisa de mercado Pyramid. A expectativa é que sejam vendidas **31 milhões de unidades desse tipo de equipamento no acumulado do ano.**

O crescimento da categoria no "mercado popular" e os esforços das operadoras de telecomunicações para expandir sua base instalada de smartphones devem guiar o crescimento da categoria neste ano, segundo a empresa de pesquisa.

A Pyramid espera que a venda de smartphones na América Latina avance a uma média de 30% ao ano nos próximos cinco anos.

"Esse crescimento vai ser impulsionado pelos esforços das operadoras em aumentar receitas, além da queda no preço dos aparelhos e da necessidade cada vez maior dos consumidores de estarem conectados", disse a analista Juliana Gomez, da Pyramid.

De acordo com a empresa de pesquisa, o mercado de smartphones cresceu 117% na América Latina em 2010, enquanto o segmento de dispositivos móveis como um todo cresceu 17%.

Smartphones :: Android Ganha Força

Apple x Samsung

http://www1.folha.uol.com.br/mercado/998094-samsung-supera-apple-na-venda-de-smartphones-no-3-trimestre.shtml

FOLHA.com

28/10/2011 - 08h36

Samsung supera Apple na venda de smartphones no 3º trimestre

A Samsung Electronics ultrapassou a Apple como **maior fabricante de smartphones** no período de julho a setembro com um salto de 44% nos embarques e prevê fortes vendas no atual trimestre, em um claro alerta para os concorrentes. (...)

"(...)Apple e Samsung continuarão a dominar o mercado no quatro trimestre", disse o gerente de fundos Kim Hyun-joong, da Midas Asset Management, que tem ações da Samsung.

O lucro da divisão de telecomunicações da companhia sul-coreana, anunciado nesta sexta-feira, mais que dobrou em relação a um ano atrás, para o recorde de 2,5 trilhões de wons (US$ 2,2 bilhões) e respondeu por 60% do lucro total da Samsung, além de ter compensado a queda acentuada nos ganhos da divisão de chips de memória.

Os embarques de smartphones subiram 44% em relação ao trimestre anterior, para 27,8 milhões de unidades, quase quatro vezes mais que um ano antes, segundo a consultoria Strategy Analytics.

As vendas da Apple diminuíram em 16%, para 17,1 milhões de unidades no terceiro trimestre. A Samsung tinha 23,8%do mercado global de smartphones no trimestre passado, nove pontos percentuais acima da Apple.

Smartphones :: Android Ganha Força

Apple x Samsung

http://tecnologia.terra.com.br/noticias/0,,OI5471818-EI15606,00-Android+detem+do+mercado+de+smartphones+diz+pesquisa.html

16/11/2011 - 09h49

Android detém 52,5% do mercado de smartphones, diz pesquisa

Mais da metade dos smartphones vendidos no mundo no terceiro trimestre do ano são equipados com o sistema operacional Android do Google, disse nesta terça-feira a empresa Gartner, dedicada a pesquisas sobre tecnologia. No terceiro trimestre de 2011, foram vendidos cerca de 60,5 milhões de telefones que funcionam com Android, o que supõe que esse sistema operacional possui 52,5% do mercado, contra 25,3% no mesmo período de 2010, afirmou a Gartner.

A Nokia vendeu 19,5 milhões de smartphones equipados com o sistema operacional Symbian no terceiro trimestre do ano, mas sua fatia parcela de mercado caiu de 36,3% há um ano para 16,9% atualmente. A Apple vendeu 17,3 milhões de iPhones com o sistema operacional iOS. A empresa tem uma fatia de mercado de 15% contra 16,6% um ano atrás.

A BlackBerry foi a marca que teve a maior queda. Apesar de suas vendas terem subido no período para 12,7 milhões de unidades de seu smartphone, sua fatia de mercado caiu de 15,4% há um ano para 11%. "O Android se beneficiou de uma maior oferta de produtos de massa, de uma competição mais fraca e da menor espectativa por novos produtos com sistemas operacionais alternativos", disse a principal analista da Gartner, Roberta Cozza.

Smartphones :: Android Ganha Força

Apple x Samsung

IMS research
excellence in market intelligence

http://macmagazine.com.br/2011/09/22/ims-research-smartphones-com-android-serao-o-futuro-hub-digital-de-conteudo/

MacMagazine.com.br

22/09/2011

Smartphones com Android serão o futuro hub digital de conteúdo

Nem computadores, nem TVs, nem a nuvem, nem iGadgets com AirPlay: para a IMS Research, **o hub digital do futuro para conteúdo digital serão smartphones com Android**. Ou seja, esses gadgets serão capazes de alimentar televisores, consoles de videogame e outros eletrônicos com conteúdo digital de forma similar ao que iPhone, iPads e iPods touch fazem hoje com o Apple TV.

O segredo por trás disso está em quatro letras: DNLA, sigla para Digital Living Network Alliance, um protocolo aberto de compartilhamento de mídia que vem sendo amplamente adotado por fabricantes de Androids. Estima-se que, em 2015, 75% dos aparelhos com DNLA vendidos fora dos Estados Unidos e do Japão serão smartphones.

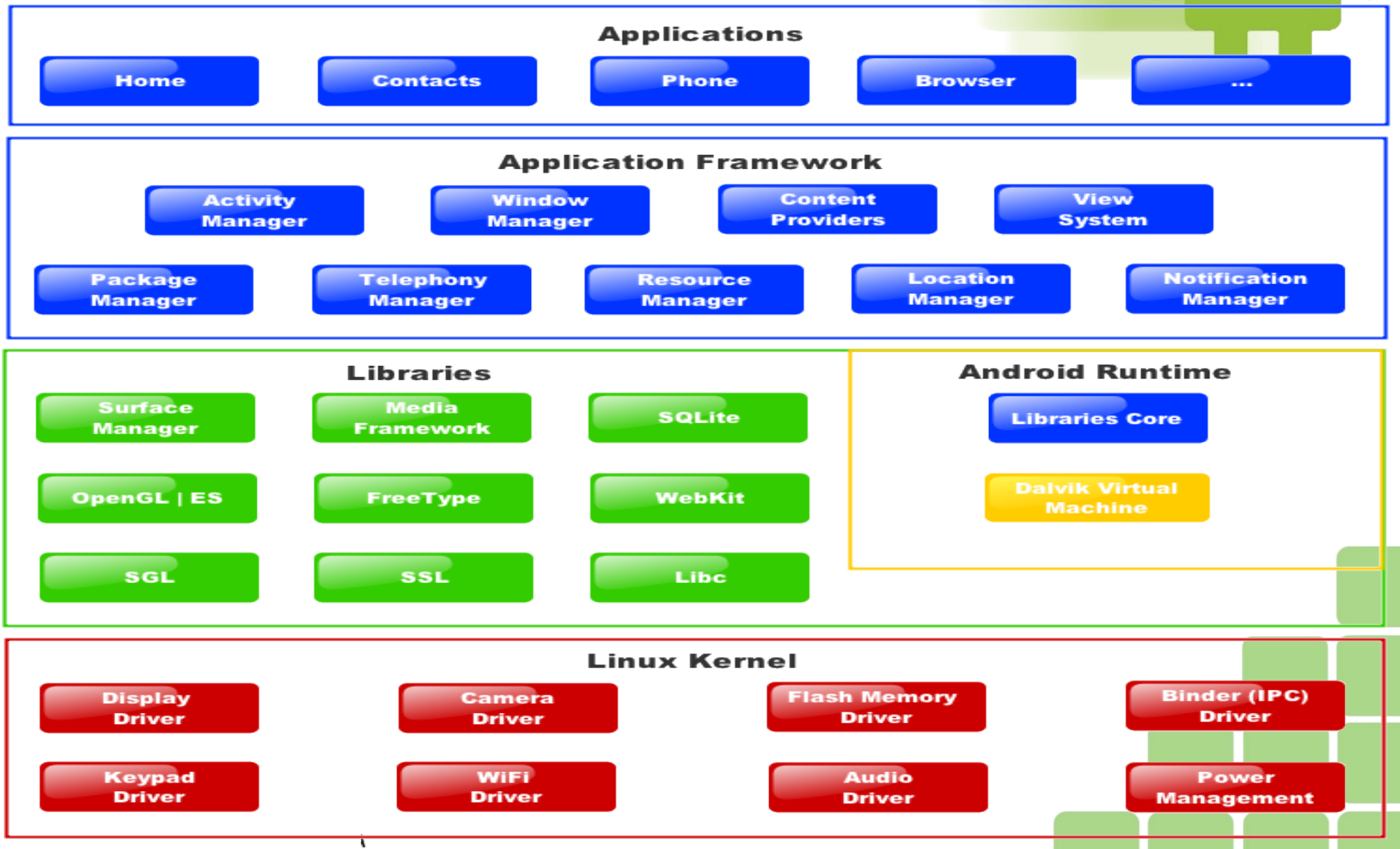
O Sistema Operacional Android

O que é?

- Mais que um sistema operacional, o Android é...
- ...uma nova plataforma de desenvolvimento para **aplicativos móveis**, tendo por base (kernel) o sistema operacional **Linux**, associado a diversas aplicações, ambiente de desenvolvimento otimizado baseado na linguagem Java e flexibilidade para adequação às mais diversas plataformas e necessidades.

O Sistema Operacional Android

Arquitetura (Diagrama)



O Sistema Operacional Android
Projeto e Manutenção

- Projeto (e manutenção) do sistema liderado pela empresa **Google** `(www.google.com)`
- Juntamente com outras grandes empresas líderes do mercado de:
  - telefonia (como a Motorola, LG, Samsung, HTC, Sony Ericsson Telefónica, Telecom Italia, Sprint Nextel e Vodafone, ...);
  - hardware (como a Toshiba, Intel ASUS, Acer, Sharp, Nec e companhias chinesas)
- criaram e/ou mantém a **OHA (Open Handset Alliance)**...
- ... com a *"intenção de padronizar uma plataforma de código aberto e livre para celulares que pudesse atender a todas as expectativas e tendências do mercado atual"*.

`Fonte: OHA (www.openhandsetalliance.com)`

A OHA conta, atualmente, com mais de 80 empresas entre operadoras de telefonia móvel, fabricantes de dispositivos móveis, fabricantes de semicondutores e empresas de desenvolvimento de software, comércio e serviços

O Sistema Operacional Android

Licença de Uso e Comercialização

- Plataforma livre e de código aberto
- Gratuito e disponibilizado com licença flexível possibilitando aos fabricantes de dispositivos móveis a realização de alterações em seu código-fonte e a customização de seus produtos
- Sem a necessidade/obrigação do compartilhamento dessas alterações.
- Possibilidade/abertura a contribuições (em seu código-fonte) por parte de desenvolvedores de todo o mundo, adicionando funcionalidades e/ou corrigindo falhas.

Aplicações para o Android

- API disponibilizada para desenvolvedores construírem aplicações para execução em Máquina Virtual Java Otimizada (Dalvik)
- Aplicações (arquivos jar) empacotados em arquivos .apk
- Aplicações são instaladas pelo usuário (baixando e instalando pacotes .apk ou usando um App Store)
- AndroidManifest.xml (arquivo embutido em cada .apk com "regras" de funcionamento do pacote)

(In) Segurança no S.O. Android

Ok... Mas vamos lá...

E sobre a (In) Segurança no Android ???

(In) Segurança no S.O. Android

Dois Enfoques...

- **Velhos problemas = sempre problemas!**
- **Novos recursos = novos problemas**

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

(In) Segurança no S.O. Android

Velhos problemas = sempre problemas

Cavalos de Tróia / Malwares no Android !!??

(In) Segurança no S.O. Android

Velhos problemas = sempre problemas

http://idgnow.uol.com.br/seguranca/2011/07/15/cavalo-de-troia-que-ja-invadiu-symbian-blackberry-e-wp7-chega-ao-android/

IDG NOW! tecnologia em primeiro lugar

15/07/2011 - 13h40

Cavalo de Troia que já invadiu Symbian, BlackBerry e WP7 chega ao Android

Praga finge ser aplicativo de Mobile Banking, mas, uma vez instalada, copia dados bancários e os envia a um servidor remoto.

Um cavalo de Tróia que já contaminou as plataformas Symbian, BlackBerry e Windows Phone chega agora ao Android. Conhecido como **Zitmo**, a praga vem sendo usada pelo grupo criminoso ZeuS a fim de roubar dados bancários de dispositivos móveis.

A nova invasão foi confirmada pela companhia de segurança Fortinet na semana passada. O trojan finge ser um aplicativo de Mobile Banking, mas, uma vez instalado, encaminha as mensagens que o usuário recebe para outro endereço. Assim, **obtém as senhas de autenticação (mTan) utilizadas em transações**.

A praga é muito eficiente no que se propõe a fazer, vencendo a autenticação dupla que instituições financeiras promovem por questões de segurança. Primeiro, a gangue infesta o smartphone com um malware, responsável por identificar o login e a senha da vítima. Depois, dizendo ser o próprio banco, envia um SMS a ela, oferecendo o download de um aplicativo, que roubará as informações necessárias para completar o roubo.

"Funcionando em segundo plano, ele intercepta as mensagens e as encaminha para um servidor remoto". Apesar de simples, é o bastante para que a gangue consiga os mTans.

(...)

(In) Segurança no S.O. Android

Velhos problemas = sempre problemas

http://idgnow.uol.com.br/seguranca/2011/08/23/trojan-letal-ameaca-usuarios-de-android/

23/08/2011 - 11h14

IDG NOW! tecnologia em primeiro lugar

Trojan letal ameaça usuários de Android

Malware pode ganhar acesso root e roubar dados pessoais, incluindo o IMEI do aparelho.

De acordo com uma equipe da Universidade Estadual da Carolina do Norte (EUA), que analisou o malware com apoio da empresa chinesa de segurança móvel NetQin, o '**GingerMaster**' carrega várias das características da crescente família de Trojans Android que atualmente circulam em sites de terceiros na China, mas com algumas inovações tão interessantes quanto perigosas.

Embutido em um app aparentemente legítimo feito para mostrar fotos de mulheres, o GingerMaster captura o máximo de dados pessoais do usuário - incluindo o número do celular e seu IMEI - e os envia para um servidor remoto. Em seguida, o servidor começará a baixar discretamente o malware, que explora o hack GingerBreak e que, **uma vez instalado, tomará completamente o controle do smartphone**.

Como é do tipo root, este hack será capaz de burlar o sistema do Android que controla as permissões de apps - e é isso que revela o poder destrutivo deste ataque. Diante de um acesso tão profundo ao sistema, os programas de segurança do Android serão incapazes de barrar a invasão e, **para se livrar da praga, muitos usuários terão de apagar completamente o conteúdo do aparelho e voltar às configurações de fábrica.**

(...)

(In) Segurança no S.O. Android

Velhos problemas = sempre problemas

http://exame.abril.com.br/tecnologia/android/noticias/android-e-o-alvo-preferido-de-virus-e-malwares-em-dispositivos-moveis

26/11/2011 - 16h46

EXAME.COM

Android é o alvo preferido de vírus e malwares em dispositivos móveis, diz McAffee

Plataforma do google para dispositivos móveis sofreu aumento de 37% no número de vírus e malwares em apenas 3 meses

O mais recente relatório da **McAfee** liga o alerta de segurança para os usuários de Android. A pesquisa mostra que a plataforma é o alvo preferido dos aplicativos maliciosos (também conhecidos como malwares) para dispositivos móveis. **No terceiro trimestre deste ano, praticamente só foram criados malwares para atingir a plataforma desenvolvida pelo Google**.

O estudo revela aumento no volume de malwares no sistema operacional móvel do Google em 37% em relação ao trimestre anterior. O vice-presidente sênior do McAfee Labs, Vincent Weafer, disse em comunicado divulgado à imprensa que o cenário de ameaças de agora inclui ataques de "alto nível de sofisticação".

Entre os destaques estão os vírus que forçam o envio de SMS sem que o dono do aparelho saiba. O smartphone passa a mandar mensagens de texto com informações sobre o proprietário do celular para o criador do malware, que pode usar tais dados para roubar dinheiro da pessoa.

Diante da proliferação de programas maliciosos neste ano, a empresa aumentou sua previsão de 70 milhões de malwares no fim de 2011 para **75 milhões de malwares**, o maior volume da história dos softwares produzidos com a intenção de causar prejuízos aos usuários.

(In) Segurança no S.O. Android

Combatendo a Infecção por Malwares

Como garantir que não há Malware em um App?

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

(In) Segurança no S.O. Android

Combatendo a Infecção por Malwares

Como garantir que não há Malware em um App?

Usando o Android Market !!??

- Base pública e centralizada de Apps p/Android
- Possibilidade de análise (comentários) de outros usuários da aplicação
- Apps testados (!?) pelo Google

(In) Segurança no S.O. Android

Combatendo a Infecção por Malwares

O Android Market **diminui o risco** mas **não garante** que todos os Apps da base estão imunes a Malwares

- *"Tudo que você precisa é ter uma conta de desenvolvedor, que pode facilmente ser anônima, pagar US$ 25 e postar seus aplicativos"* (Juniper Networks)

- Sem processo de revisão do software ou verificação do usuário, o aplicativo malicioso só é removido da Android Market após denúncias.

- Até que isso aconteça, milhares de downloads são feitos e donos de smartphones Android prejudicados.

- Notificações de remoção de Apps do Android Market crescem a cada dia.

(In) Segurança no S.O. Android

Remoção de Apps com Malware do Android Market

http://www.blogdoandroid.com/2011/03/google-remove-21-apps-do-android-market-por-conter-malware-trojan-root-kit/

02/03/2011 - 10h10

Google remove 21 apps do Android Market por conter malware – trojan root kit

Após uma denúncia do Blog Android Police, juntamente com um usuário do serviço Reddit.com, ao Google, **foram retirados 21 aplicativos do Android Market**, infectados com um Trojan backdoor rootkit.

Segundo a Google, os aplicativos eram de fato malware, que após ganhar acesso root, juntavam informações variadas, como IMEI, MSI, ID do produto, modelo, parceiro, língua, país, ID do usuário. O Malware podia também baixar mais instruções para então fazer outras tarefas.

Embora a Google tenha removido rapidamente, assim que foi avisada, do Android Market, os aplicativos infectados foram baixados por pelo menos 50 mil usuários. A estratégia do cracker foi bem simples, ele copiava jogos famosos, injetava o código malicioso e republicava os jogos no Market com um nome ligeiramente diferente.

Todos os apps foram publicados pelo mesmo desenvolvedor. Eles utilizam a falha do sistema rageagainstthecage para ganhar acesso root ao sistema (acesso de administrador).

(In) Segurança no S.O. Android

Remoção de Apps com Malware do Android Market

http://news.cnet.com/8301-27080_3-20067505-245.html

CNET | News

31/03/2011 - 07h20

Malicious apps removed from Android Market

Between 30,000 and 120,000 Android devices may have been affected, Lookout said.

"This weekend, multiple applications available in the official Android Market were found to contain malware that can compromise a significant amount of personal data," the company said in a blog post late last night. "Likely created by the same developers who brought DroidDream to market back in March, more than 25 applications were found to be infected with a stripped down version of DroidDream we're calling **'Droid Dream Light' (DDLight)."**

Google removed 58 malicious apps from the market in March and remotely removed the apps from the devices they'd been downloaded to.

The problem was **reported to Lookout** by a developer who found that modified versions of his app and another developer's app were being distributed in the Android Market. Lookout confirmed that malicious code was inserted into the apps and identified markers that linked the code with DroidDream samples.

"We discovered **24 additional apps re-packaged and re-distributed with the malicious payload** across a total of 4 different developer accounts," Lookout said.

(In) Segurança no S.O. Android

O DroidDream

Pior Trojan Instalado Via App (Android Market ou Malware de Fonte Externa)

- Codinome: Android.Rootcager
- Primeiro registro em 03/01/2011
- Desbloqueia automaticamente o acesso "root" do equipamento, usando o exploit "rageagainstthecage"
- Em seguida, captura várias informações contidas no aparelho como IMEI, ID do produto, modelo, fornecedor de serviços, língua, país e userID.
- Possibilidade de conseguir fazer download de código adicional e expandir-se automaticamente.
- Ação registrada em 4 dias: 200 mil downloads de Apps infectados.
- Google lançou o App "Android Market Security Tool" e instalou automaticamente em aparelhos que foram infectados.
- Em março, o DroidDream voltou disfarçado de vacina, um .APK com o nome de "Android Market Security Tool March 2011"

(In) Segurança no S.O. Android

Detalhes sobre o "DDLight"

http://g1.globo.com/tecnologia/noticia/2011/06/virus-para-android-se-executa-quando-usuario-recebe-chamada.html

01/06/2011 - 17h27

Vírus para Android se executa quando usuário recebe chamada

Praga estava sendo distribuída no Market. Apps contendo o código já foram removidos.

A principal novidade do "DDLight" é a **capacidade de se executar automaticamente quando o usuário recebe uma chamada**, mesmo que o app não tenha sido acessado pelo usuário depois de instalado. Em outras palavras, ele não é capaz de se instalar sozinho a partir de uma chamada, apenas de se executar caso ele já esteja instalado pelo Market.

Em contrapartida, o vírus **não consegue** instalar outros componentes maliciosos no telefone sem a autorização do usuário, como a versão anterior conseguia. O DDLight, quando executado, **transmite dados de telefone como o IMEI (identificador do celular), o IMSI (identificador do chip), o modelo e a lista de programas instalados**. Não se se sabe ainda o que os criadores do vírus querem fazer com essas informações.

Para disseminar o vírus, os criminosos infectaram programas legítimos e reenviam para o Market com nomes simples, como "Tetris". A Lookout estima que entre 30 e 120 mil usuários tenham baixado alguns dos softwares infectados pelo Market.

A Lookout acredita que os responsáveis pelo novo ataque são os mesmos que infectaram 50 apps do Android Market em março.

(In) Segurança no S.O. Android

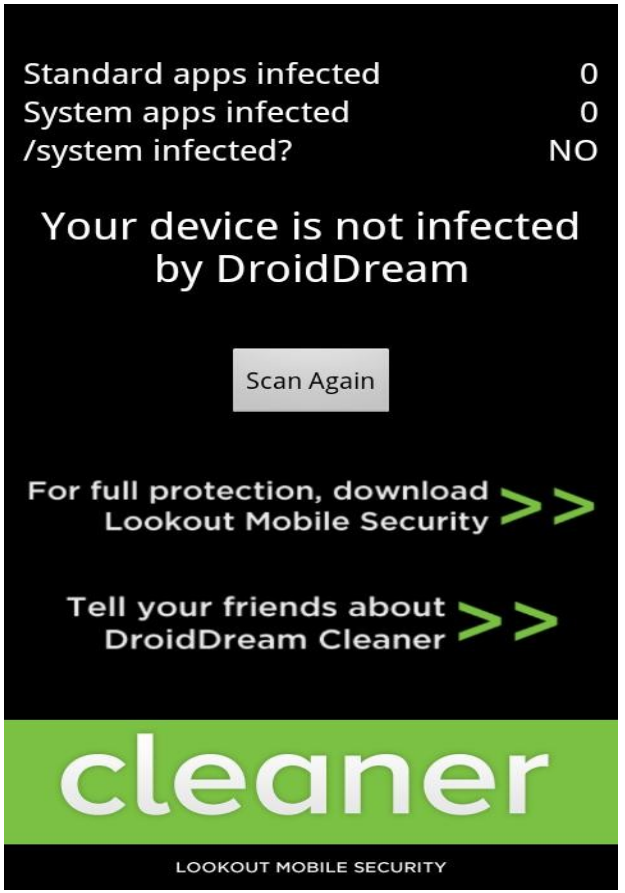
Detectando e Removendo o DroidDream

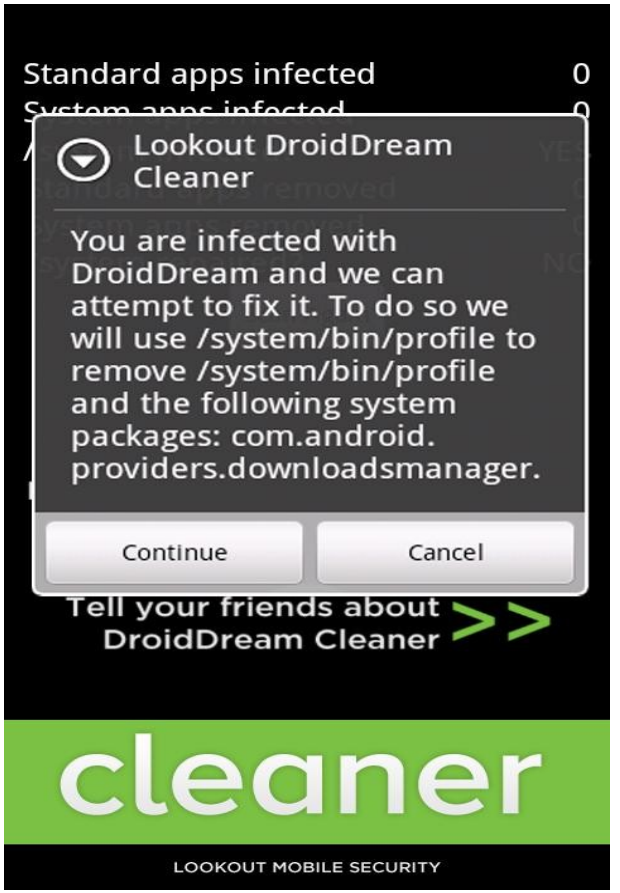
http://pt.appbrain.com/app/droiddream-cleaner/com.lookout.cleaner.droiddream

DroidDream Cleaner

AppBrain

Diagnose & repair phones infected with DroidDream Malware





INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

(In) Segurança no S.O. Android

Kill Switch :: O **"Botão Vermelho"** do Google/OHA

- Quando as coisas "saem do controle" o Google pode utilizar um recurso chamado **Kill Switch** e desinstalar Apps remotamente
- Este recurso, apesar de intrusivo, é utilizado, por exemplo, quando Apps maliciosas são disponibilizadas no Android Market e instaladas por usuários
- O objetivo é utilizá-lo somente quando "a segurança do Sistema Operacional e/ou do usuário estiver comprometida"

BACKDOOR ???

(In) Segurança no S.O. Android

Upgrade Attack (infecção na atualização do App)

• Neste tipo de ataque ao Android o problema **não está na instalação de um App** (que instala sem problemas e sem qualquer malware embutido)

• **Está na Atualização de versão do App**

• **Situação 01:** Usuário recebe notificação de que existe uma nova versão de um App instalado... **Mas não é o desenvolvedor do App quem enviou esta notificação**

• **Situação 02:** Usuário recebe notificação de que existe uma nova versão de um App instalado... Desenvolvedor, **após ganhar confiança dos usuários com seu App original**, envia uma nova versão com malware.

Primeiro Caso Real: DroidKungFu

(In) Segurança no S.O. Android

Outras "Pragas" instaladas via App

- **Zitmo**
  - *Programado para roubar dados bancários dos usuários.*
  - *Arquivo APK possui 19 KB de tamanho.*
  - *App se passa por uma ferramenta de segurança do desenvolvedor Trusteer.*
  - *Cria um ícone com o nome "Trusteer Rapport" no menu principal.*
- **SoundMiner**
  - Capaz de registar números de cartão de crédito, digitados no teclado ou ditos por voz, e de os enviar para o criador da aplicação, (sem acesso à rede de dados).
  - Faz/fazia uso de uma segunda aplicação, Deliverer (com acesso à rede de dados), para fazer o envio.
- **GGTracker**
  - *Disponível (junho/2011) em página semelhante ao Android Market*
  - *Disponibilizava um aplicativo de Economia de Bateria do Smartphone*
  - *Enviava mensagens SMS Premium (US$ 40 dólares por mensagem)*

(In) Segurança no S.O. Android

Outras "Pragas" instaladas via App

- **Android.PjappsM**
  - *Primeiro registro no início de 2010*
  - *Injetado em programas legítimos (baixados do Android Market) e redistribuídos (versão com o malware embutido) em "marketplaces terceirizados".*
  - *Symantec aponta como principais objetivos o roubo de informações e montagem de uma botnet.*

- **AndroidOS.FakePlayer**
  - *App se disfarça de aplicativo Media Player*
  - *Envia mensagens SMS (sem a autorização/intervenção do usuário) par a números da Rússia (versão descoberta pela Symantec)*

(In) Segurança no S.O. Android

Novos Recursos = Novos problemas

Autenticação de Serviços Google

(In) Segurança no S.O. Android

Novos Recursos = Novos problemas

http://www.uni-ulm.de/en/in/mi/staff/koenings/catching-authtokens.html

Google AuthTokens é Seguro?

ulm university universität ulm

- Falha descoberta em versões do Android anteriores a 2.3.3
- Ulm University Institute of Media Informatics (Alemanha)
- Uso do protocolos sem criptografia (como HTTP) para transmitir AuthTokens em aplicativos como Google calendar, Google contact list, Google Picasa, além de outros serviços Google acessados por dispositivos com Android.
- Ataque "**Sidejacking**": Interceptação desses dados dão/dariam acesso a informações de usuários armazenadas na "nuvem" do Google.
- Em Maio/2011 noticiou-se (ZDNet) que 99,7% dos Smartphones com Android estavam vulneráveis a este tipo de ameaça.

ZDNet

http://www.zdnet.com/blog/hardware/997-of-all-android-smartphones-vulnerable-to-serious-data-leakage/12831

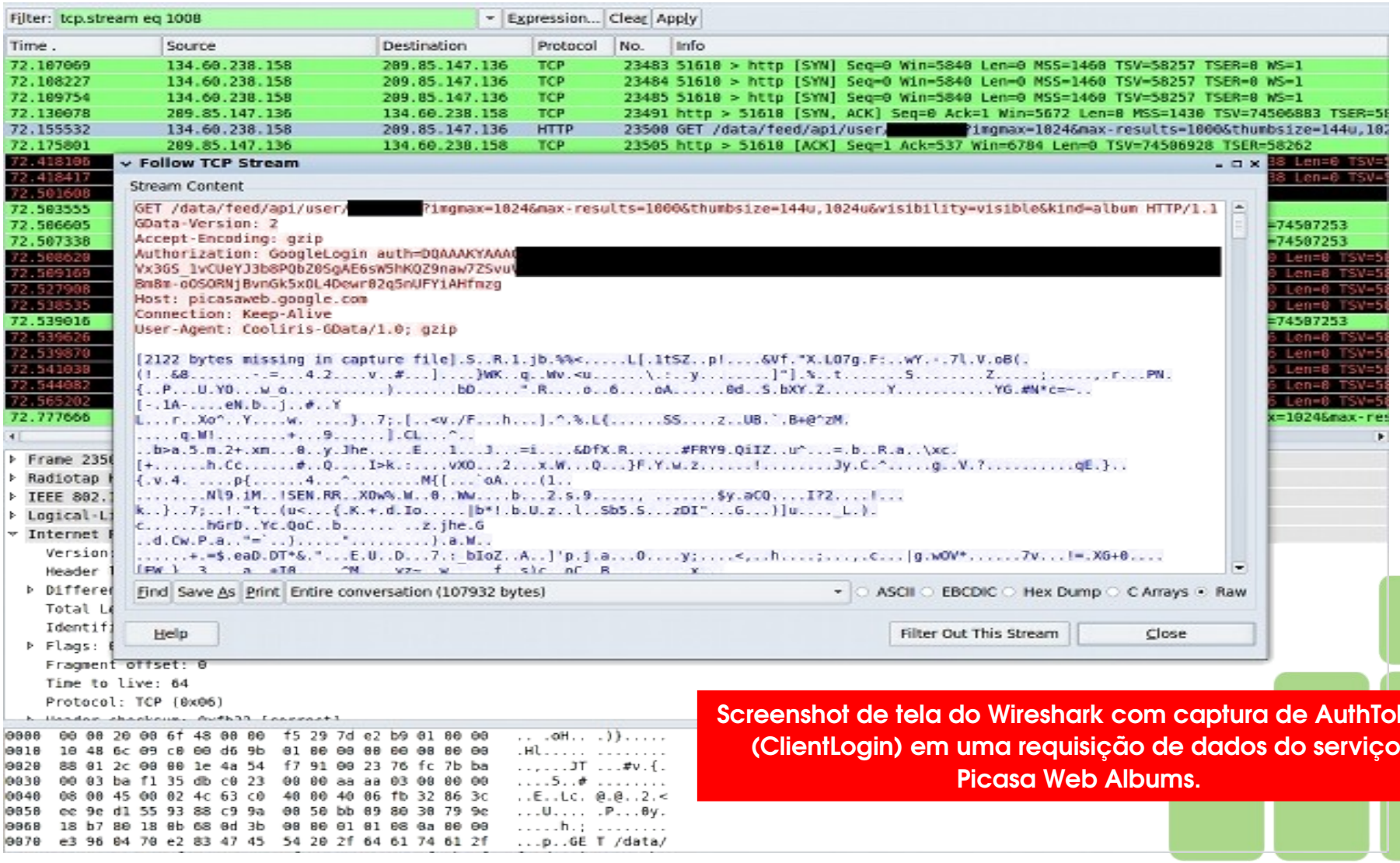
(In) Segurança no S.O. Android

Novos Recursos = Novos problemas

http://www.uni-ulm.de/en/in/mi/staff/koenings/catching-authtokens.html

Google AuthTokens é Seguro?

ulm university universität ulm



Screenshot de tela do Wireshark com captura de AuthToken (ClientLogin) em uma requisição de dados do serviço Picasa Web Albums.

(In) Segurança no S.O. Android

Novos Recursos = Novos problemas

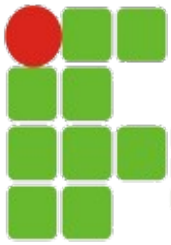
http://www.uni-ulm.de/en/in/mi/staff/koenings/catching-authtokens.html

Google AuthTokens é Seguro?

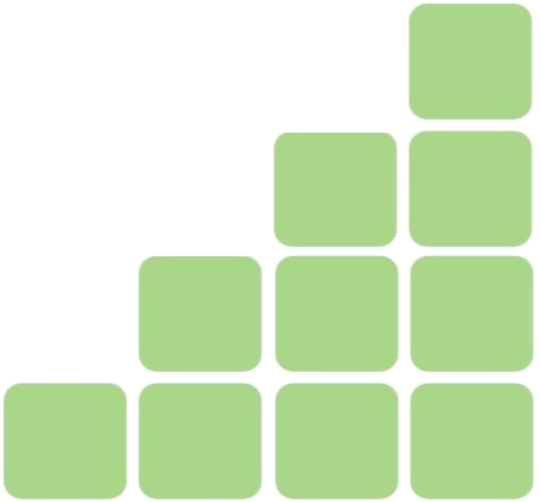
ulm university universität ulm

Android version	Calendar Sync	Contacts Sync	Picasa Sync (Gallery)
3.0	yes	yes	?
2.3.4	yes	yes	no
2.3.3	no	no	no
2.2.1	no	no	n/a
2.2	no	no	n/a
2.1	no	no	n/a

Uso de HTTPS em Apps Android Google



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE



(In) Segurança no S.O. Android

Novos Recursos = Novos problemas

http://www.uni-ulm.de/en/in/mi/staff/koenings/catching-authtokens.html

Google AuthTokens é Seguro?

ulm university universität ulm

- Google AuthTokens geralmente são válidos por longos períodos
  - Tokens do Google Calendar, por exemplo, são válidos por 14 dias.

- **Solução !? Atualização do Android**

  - Android 2.3.4 passou a oferecer transferência de AuthTokens utilizando HTTPS para a autenticação e sincronização de Apps em serviços Google.

- Outras dicas/sugestões:
  - Diminuir o tempo de vida dos AuthTokens !!!
  - Forçar o uso de HTTPS (Google)
  - Desabilitar a sincronização de dados em redes Wi-Fi públicas e abertas.
  - Evitar utilizar Apps que requerem autenticação em redes Wifi públicas e abertas

Só Wi-Fi ???
Isso é um problema do Android ou de Serviços Google?

(In) Segurança no S.O. Android

Gerência Segura de Tokens :: Mercado Corporativo

http://www.item.com.br/2011/01/novas-ferramentas-de-seguranca-da-rsa-tornam-a-plataforma-google-android%E2%84%A2-mais-amigavel-para-as-empresas-e-o-comercio-eletronico/

BEDFORD, MA, EUA, 04 de janeiro de 2011

A Divisão de Segurança da EMC expande a opção de autenticadores RSA SecurID® para aplicativos e dispositivos móveis baseados no Android™ como um componente conveniente para a segurança corporativa

- A RSA (divisão de segurança da EMC) anuncia a disponibilidade do RSA SecurID® Software Token para Android™
- Desenvolvido para possibilitar que um dispositivo baseado no Android seja usado como um autenticador RSA SecurID, proporcionando autenticação em dois fatores conveniente e eficaz em termos de custos para aplicativos e recursos corporativos.
- A RSA também está liberando um novo **Software Development Kit (SDK) para a plataforma Android**.
- Permite aos desenvolvedores integrar autenticação em dois fatores RSA SecurID diretamente em aplicativos Android e obter vantagem competitiva ao oferecer esta camada adicional de segurança.
- O SDK é distribuído gratuitamente para todos os parceiros RSA Secured®.
- O RSA SecurID Software Token para Android **gera uma senha dinâmica que muda a cada 60 segundos**, possibilitando acesso seguro a recursos corporativos.
- O token pode ser instalado diretamente em dispositivos baseados no Android, sem custo, por meio de um simples download no Android Market™.

(In) Segurança no S.O. Android

Gerência Segura de Tokens :: Mercado Corporativo

http://www.item.com.br/2011/01/novas-ferramentas-de-seguranca-da-rsa-tornam-a-plataforma-google-android%E2%84%A2-mais-amigavel-para-as-empresas-e-o-comercio-eletronico/

BEDFORD, MA, EUA, 04 de janeiro de 2011

A Divisão de Segurança da EMC expande a opção de autenticadores RSA SecurID® para aplicativos e dispositivos móveis baseados no Android™ como um componente conveniente para a segurança corporativa

- Com ajuda mínima do departamento de TI, os usuários podem habilitar o aplicativo com um software token seed exclusivo, criando um autenticador RSA SecurID conveniente, seguro e eficaz em termos de custos.
- "Ao capacitar dispositivos móveis baseados na plataforma Android a implementar a tecnologia RSA SecurID, proporcionamos aos nossos usuários a **entrega transparente de autenticação em dois fatores em aplicativos na nuvem ou nas dependências dos clientes**."

  (Tom Corn, Chief Strategy Officer da RSA, a Divisão de Segurança da EMC)
- The RSA SecurID Software Token para a plataforma móvel Android está **disponível para download gratuitamente desde o dia 22 de dezembro de 2010 no Android Market**.
- Ele é habilitado para usuários com um software token seed exclusivo adquirido pelas organizações de TI que utilizam o RSA® Authentication Manager.

E o que mais?

Android Botnets !!??

(In) Segurança no S.O. Android

Android Botnets

- **Geinimi**
  - *Identificada em Janeiro/2011 no mercado chinês*
  - *Infecção de Smartphones da mesma forma que Pcs Zumbis*
  - *Malware inserido via reempacotamento de Apps (Android Market)*
  - *Também encontrados em ROMs e Games customizados (não oficiais)*
- **Zitmo ("Zeus In The MObile")**
  - *Versões para Android, Windows Mobile, Symbian (09/2010) e BlackBerry*
  - *Detalhes já abordados na análise de infecção por Malwares*
- **Novidades...**
  - *Uso de SMS (canal de comando e controle)*
  - *Exploração do novo universo do 3G*
    - *Largura de Banda cada vez maior*
    - *Mobilidade (dificuldade de localização)*

Vídeo de Demonstração de Funcionamento
Shmoocon 2011 (Georgia Weidman)

Smartphone Botnets over SMS

`http://vimeo.com/19372118`

(In) Segurança no S.O. Android

Como Se Proteger ???

"A única maneira de proteger verdadeiramente um smartphone é **cercar o hardware, os dados e os apps.**

Se os três não forem cobertos, não haverá garantias"

John Dashner (McAfee)

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

(In) Segurança no S.O. Android

Contramedidas (Dicas)

"Empresas norte-americanas e européias perdem, em média, 11 smartphones por ano"

(Forrester Research)

- **Bloqueio do Smartphone**
  - *Proteção (!!??) contra perda e roubo*
  - *Ativar a deleção de dados na falha de n (oito !?) tentativas*
  - *Ativar a funcionalidade de permissão de deleção remota de dados*

Esta recomendação é contestada quando utiliza-se a funcionalidade de localização de aparelho perdido. Nesses casos, o bloqueio pode acelerar o processo de reinstalação de Sistema Operacional no caso de roubo.

(In) Segurança no S.O. Android

Contramedidas (Dicas)

A grande maioria dos malwares infectam o Android através de um cavalo-de-tróia

- **Atenção Redobrada na Instalação de Apps**
  - *Só instalar aplicativos .apk de a fonte realmente for confiável*
  - *Usar o Android Market não é garantia de App sem malware*
    - *Buscar aplicativos "mais populares"*
    - *Verificar comentários de outros usuários antes de baixar*
    - *Verificar permissões solicitadas/necessárias na instalação (analisar coerência)*
- **Atualizar aplicações (sempre que disponíveis)**
  - *Atualizações geralmente corrigem falhas (que podem colocar em risco o aparelho)*
  - *Android disponibiliza correções de Apps instalados "over the air"*
  - *Verificar a fonte da atualização (para não ser vítima de um "Update Attack"*
- **Fazer backups periodicamente**
  - *Dica tradicional, mas cada vez mais atual e válida*
  - *No caso de roubo, o recurso de apagamento remoto pode ser feito sem problemas*
    - *Ex. App MyBackup (Apps, contatos, textos e configurações em servidor remoto)*

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

(In) Segurança no S.O. Android

App Inventor :: Liberdade Controlada

- App Inventor = Ambiente Integrado de Desenvolvimento para criar aplicações web ou para dispositivos que utilizam o sistema operacional Android.
- Ambiente simples para o desenvolvimento rápido e fácil do tipo de aplicativo para o qual ele se destina.
- Não é necessário instalá-lo em um computador (aplicativo funciona online diretamente em uma janela de um navegador)
- Para utilizá-lo, é necessário possuir uma conta de usuário da Google.
- O outro lado (além da popularização de desenvolvimento de Apps)...
  - Limitação e controle na utilização de recursos do S.O. minimizando os riscos de criação de novos malwares
  - Menos restrição (ou ausência dela) para publicação no Android Market de Apps criadas como o App Inventor (!!??)

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

(In) Segurança no S.O. Android

A situação é tão grave como "pintam" ???

21/11/2011 :: Chris DiBona (executivo da Google para projetos de código aberto)
https://plus.google.com/u/0/114765095157367281222/posts/ZqPvFwdDLPv#114765095157367281222/posts/ZqPvFwdDLPv

Alarme sobre crise de insegurança no Android é puro charlatanismo...

"Empresas de vírus estão jogando com os seus medos para conseguirem vender softwares de proteção para o Android, o Blackberry e o iOS. (...) Tratam-se de charlatões e picaretas. Se você trabalha numa dessas empresas que tentam vender esse tipo de apps para Android, Blackberry ou iOS, você deveria tomar vergonha na cara."

(In) Segurança no S.O. Android

A situação é tão grave como "pintam" ???

21/11/2011 :: Chris DiBona (executivo da Google para projetos de código aberto)
https://plus.google.com/u/0/114765095157367281222/posts/ZqPvFwdDLPv#114765095157367281222/posts/ZqPvFwdDLPv

- "Além de não existir, na prática, o aumento das ameaças apontado em tais pesquisas, **os sistemas operacionais móveis**, por peculiaridades do seu funcionamento intrínseco, em nível de kernel, **são menos sucetíveis a esse tipo de ataques do que plataformas como o Windows ou o MacOS.**"

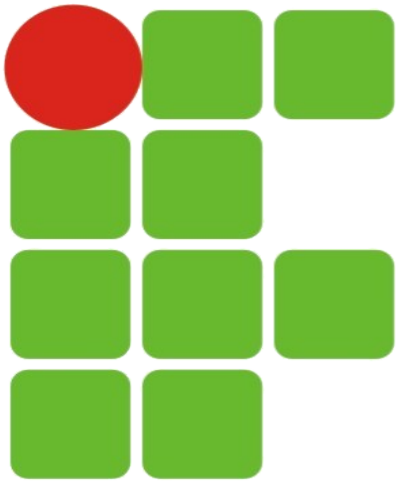
- "Alguns malwares que poderiam potencialmente apresentar riscos de segurança para o Android chegaram, em mais de uma ocasião, a aparecer no próprio Android Market, o que, naquele tempo, pode ter dado ensejo a alarmes. As pragas, no entanto, tinham ação bastante específica e não apresentavam maiores riscos a quem não fosse usuário de certa operadora de telefonia móvel na China."

- "Além dos casos concretos terem praticamente desaparecido de um tempo para cá, **nunca foi observada qualquer ameaça maior**, que oferecesse risco de proliferação ou de causar danos de forma mais abrangente. O mais intrigante é que, justamente quando tais notícias andam bastante raras, os charlatões resolveram berrar seu discurso safado e encontraram em certos veículos um canal de propaganda gratuita."

Link com comentário em www.droider.com.br

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Perguntas



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

(In)Segurança em Dispositivos Móveis com Android

Ricardo Kléber Martins Galvão
www.ricardokleber.com
ricardo.galvao@ifrn.edu.br
www.twitter.com/ricardokleber