Tendências do mercado nacional:

PROCURANDO MALWARE EM APLICAÇÕES ANDROID

Muriel Mazzetto

Lojas de aplicativos

- As lojas de aplicativos são o meio utilizado para a aquisição de um aplicativo para os dispositivos móveis.
- Além das lojas oficiais de cada dispositivo, existem lojas paralelas.
  - Disponibilidade de aplicativos piratas;
  - Aplicativos de outras plataformas (emuladores, Android no Windows);
- As medidas de segurança variam para cada loja, deixando passar aplicativos maliciosos que podem prejudicar clientes e outros vendedores.
  - Aplicativos que utilizam dados pessoais;
  - Desestabilizar método de propagandas de lojas oficiais;

Malware

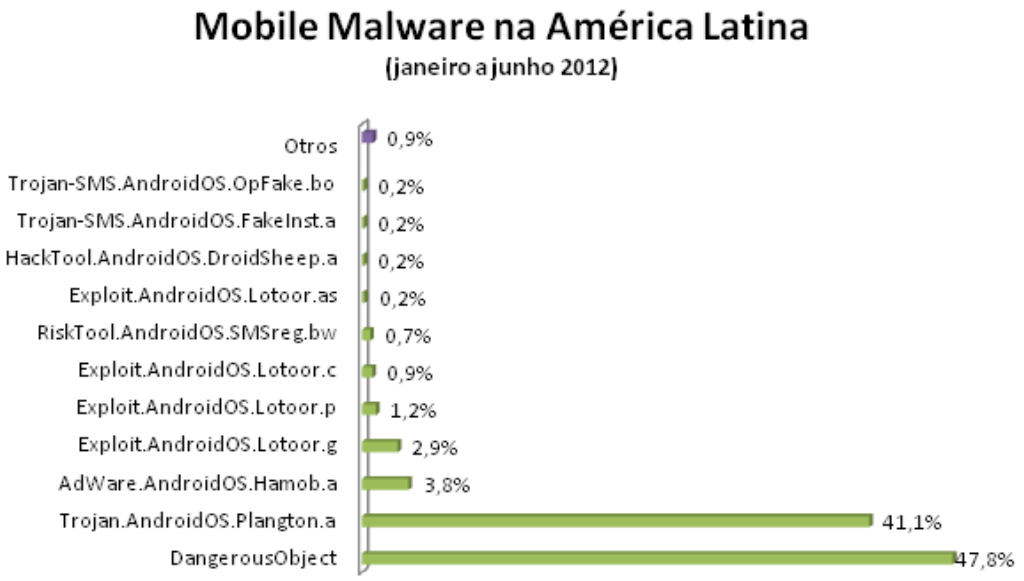
- Aplicativos costumam estar “mascarados” com uma proposta, porém utilizam acesso para outras funcionalidades com o intuito de conseguir informações pessoais, transformar em botnet, extorquir pagamentos, entre outros objetivos.
- Utilizam troca de bibliotecas e inserção de códigos.
- Um estudo de 2012, analisando duas lojas americanas e duas lojas chinesas, comparando com a loja oficial do Google, mostrou que:
  - 0.02% dos aplicativos testados estavam infectados na loja oficial;
  - Nas alternativas varia de 0.2% a 0.47%.

Parcela de mercado em 2012

Sistema Operacionais	Market Share
Android	56,10%
iPhone OS	22,90%
Symbian	8,60%
RIM	6,90%
Bada	2,70%
Windows Phone/ Mobile	1,90%
Outros SOs	0,90%
Total	100,00%

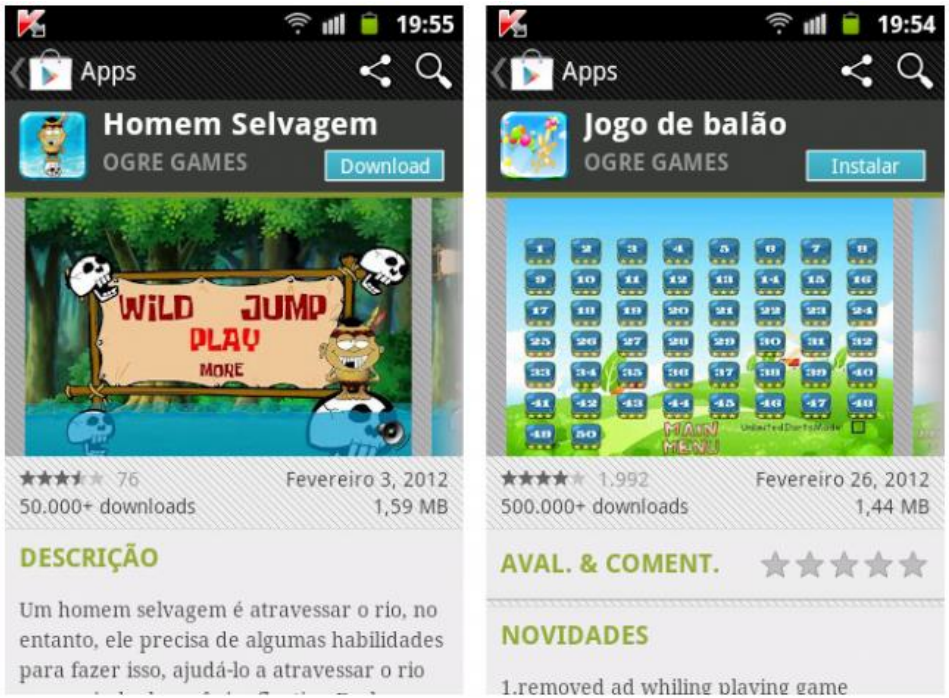
- Os ataques são dirigidos por nicho, quanto maior o uso, mais ataques terá.
- Usuários possuem a visão de "*só ocorre no computador*".

Malwares mais comuns em 2012



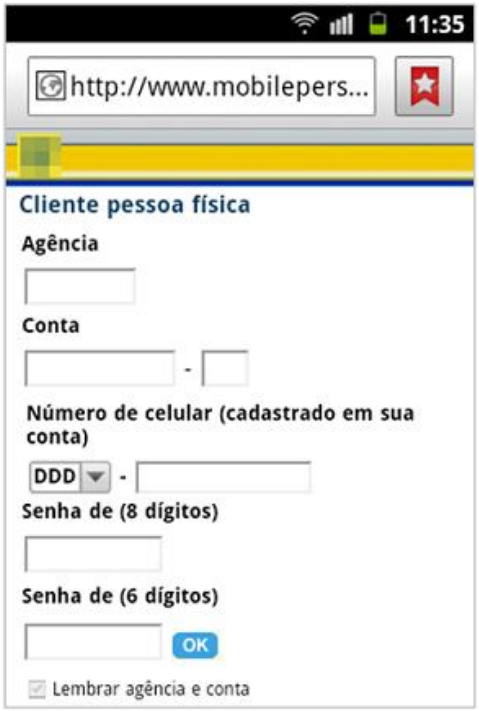
- **Dangerous Object:** ligados a atividade de *phishing* durante a navegação.
- **Plangton.a:** em aplicativos, que quando instalados acessam informações pessoais e executam serviços em background.
- **Lotoor:** aplicações para habilitar o root do aparelho, para executar aplicativos pagos de forma gratuita. Fica aberto a vulnerabilidade de terceiros.

Plangton



- Desinstalação de atalhos, alteração da tela inicial, acesso as configurações do aparelho e às chamadas de telefone, acesso total a internet.
- Esses aplicativos também costumam alterar a pagina inicial do navegador e coletam os favoritos gravados.
- Atuam como um verdadeiro spyware, coletando o número de identificação do aparelho (IMEI), a lista de permissões dadas ao aplicativo malicioso, etc.
- Os dados são enviados ao desenvolvedor, que poderá controlar remotamente o aparelho da vítima.

Phishing



- Clone de páginas bancárias.
- Aplicativos falsos de bancos.

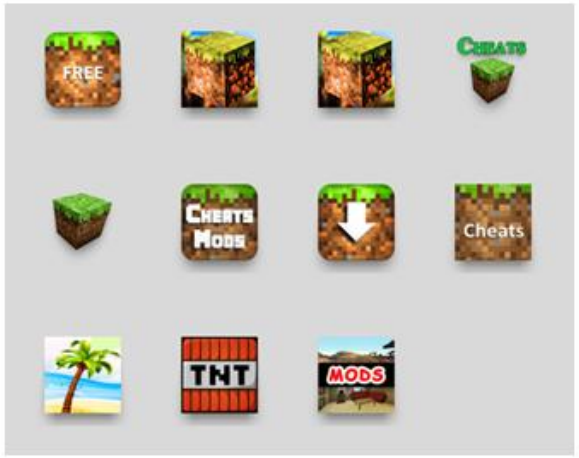
Scareware

- Aplicativos que dizem ter um propósito porém, quando instalados, começam a exibir telas com avisos de que o usuário está infectado.
- Dão opção de “remover” a infecção através de um pagamento.
- Por não possuir permissão para enviar SMS por si, usa engenharia social para ludibriar usuários à solicitarem a compra do aplicativo “antivírus”.
- Após a solicitação enganosa, costumam cobrar taxas semanais do usuário.

Scareware

A ESET revelou hoje que, ao longo dos últimos nove meses, se estima que entre 600.000 e 2,8 de utilizadores descarregaram através da Google Play mais de 30 aplicações maliciosas que na sua grande maioria se fazem passar por “cheats” ou “mods” do popular jogo Minecraft.

De acordo com os investigadores da ESET, todas estas apps eram falsas, no sentido de que não só não continham qualquer da funcionalidade anunciada, como tudo o que faziam era exibir ecrãs com avisos assustadores (daí a designação de “scareware”) que levavam os utilizadores a crer que os seus dispositivos Android tinham sido infetados com um “vírus perigoso”.



Os utilizadores eram então persuadidos a “remover” os falsos vírus ativando uma subscrição premium através de SMS que lhes custava 4,80 euros por semana.

am a

para

o.

Scareware

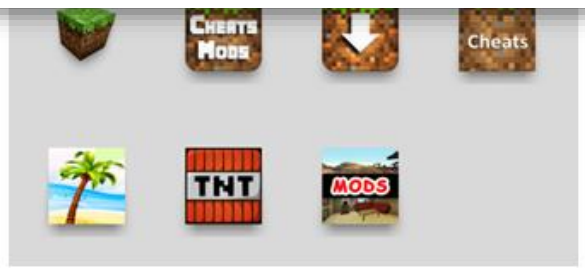
A ESET revelou hoje que, ao longo dos últimos nove meses, se estima que entre 600.000 e 2,8 de utilizadores descarregaram através da Google Play mais de 30 aplicações maliciosas que na sua grande maioria se fazem passar por “cheats” ou “mods” do popular jogo Minecraft.

am a

De acordo com os investigadores da ESET, todas estas apps eram falsas, no sentido de que não só não continham qualquer da funcionalidade anunciada, como tudo o que faziam era exibir ecrãs com avisos assustadores (daí a designação de “scareware”) que levavam os utilizadores a crer que os seus dispositivos Android tinham sido infetados

para

As primeiras aplicações scareware foram colocadas na loja em Agosto passado. Durante o tempo que estiveram online, todas receberam más classificações e comentários negativos por parte dos utilizadores. Contudo, de acordo com dados públicos disponibilizados pela própria Google Play, isto não impediu que muitas dessas apps tenham sido instaladas entre 100.000 e 500.000 vezes, com o número total estimado de instalações das 33 apps scareware descobertas entre 660.00 e 2,8 milhões.



Os utilizadores eram então persuadidos a “remover” os falsos vírus ativando uma subscrição premium através de SMS que lhes custava 4,80 euros por semana.

Scareware


22:53
Odstráňte ho teraz!
Start
Options
Bol nájdený vírus?
Bol nájdený vírus?
Exit
Bol nájdený vírus?
Bol nájdený vírus?
Bol nájdený vírus?
Bol nájdený vírus?
16:02
Bol nájdený vírus?
Odstráňte ho teraz!
Loading Please Wait !

Andrubis

- Ferramenta para monitorar aplicativos e identificar atividades maliciosas em ambiente Android. Baseado em Droidbox.
- Monitoramento dinâmico:
  - Hashes for the analyzed package
  - Incoming/outgoing network data
  - File read and write operations
  - Started services and loaded classes through DexClassLoader
  - Information leaks via the network, file and SMS
  - Circumvented permissions
  - Cryptography operations performed using Android API
  - Listing broadcast receivers
  - Sent SMS and phone calls
- Monitoramento estático:
  - Observa os componentes solicitados para funcionamento do aplicativo, buscando vazamento de informação indevida através deles.

Testes

- Obtidas em média 300 aplicações **gratuitas mais populares** de cada categoria da loja virtual AndroidPIT, totalizando 4916 aplicativos da loja.
- Obtidas 939 aplicações **gratuitas mais populares nacionais**, dentre uma lista das 400 mais populares de cada categoria, na loja virtual da Google Play.
- 646 aplicações mostraram erro ao rodar sobre o Andrubis.
- Consiste em analisar as seguintes características:
  - Hosts acessados
  - Vazamento de informações
  - Permissão subvertida
  - Mensagens e ligações

Hosts acessados

- Consiste em verificar quais os hosts que o aplicativo acessa pelo aparelho em background.
- Das aplicacões analisadas pelo Andrubis, pelo menos 29,18% (1.520) acessaram um host relacionado com propaganda.
- 13,32% (694) acessaram host relacionado com o monitoramento do usuário na Internet.
- 1,79% (93) das aplicações acessaram www.apperhand.com, uma URL conhecida por ser usada por exemplares de malware da família Plankton (ou sua variação Counterclank) para envio de informações do usuário.

Vazamento de informação

- A detecção de vazamento de informações pode demonstrar mais claramente aplicações suspeitas que estejam evadindo determinadas informações do usuário.
- O sistema Andrubis é capaz de detectar que certas informações pessoais foram escritas em um arquivo, em uma mensagem SMS, ou passadas pela rede.
- Através dos vazamentos pela rede e por SMS se indica que a informação de fato saiu do sistema.
- Das aplicações analisadas, 13,88% (723) evadiram informação pela rede e nenhuma o fez por SMS. As informações vazadas por mais aplicações foram IMEI (12,88% das aplicações) e número de telefone (5,24% das aplicações).

Permissões subvertidas

- A análise com o sistema Andrubis apontou que 0,67% (35) das aplicações subverteram alguma permissão;
- 34 conseguiram subverter a permissão android.permission.INTERNET, que permite acesso à Internet.
- Uma subverteu a permissão android.permission.READ PHONE STATE, que permite acesso a algumas informações do dispositivo.

Mensagens e ligações

- Mensagens e ligações podem ser feitas automaticamente por aplicações maliciosas para gerar gastos ao usuário infectado e ganhos para o atacante.
- Das aplicações analisadas pelo Andrubis, 0,13% (7) enviaram mensagens SMS e 0,33% (17) fizeram ligações, sendo que nenhuma fez ambos.
- Das aplicações que enviaram SMS, duas o fizeram para contatos cadastrados no sistema de análise.
- No caso das ligações, quatro aplicações as efetuaram para contatos cadastrados. Não foi possível identificar se os números utilizados para envio de SMS e ligação são válidos no Brasil.

Análise

- 29,18% das aplicações acessaram URLs relacionadas à distribuição de propaganda.
- 13,32% das aplicações acessaram URLs relacionadas ao monitoramento de usuários na Internet.
- 13,88% evadiram informações do usuário pela rede.
- Apesar de serem comportamentos suspeitos, não é possível afirmar se estas aplicações são realmente maliciosas. Porém, tais comportamentos apontam para **a tendência de se identificar o usuário de dispositivos móveis e seus hábitos**, seja para realizar campanhas de marketing especializado e rastrear interesses, seja para roubar dados sensíveis ou personificar a identidade.

Prevenção

- Utilizar lojas oficiais para downloads de aplicativos.
- Verificar comentários e avaliações do aplicativo.
- Verificar se é de uma desenvolvedora certificada e conhecida.
- Se infectado, realizar restauração de fábrica do disposivito.

Referências

- http://blog.eset.pt/2015/05/eset-descobre-mais-de-30-apps-scareware-na-loja-google-play-disfarcadas-de-mods-e-cheats-para-minecraft/
- http://brazil.kaspersky.com/sobre-a-kaspersky/centro-de-imprensa/blog-da-kaspersky/2012/malware-mobile-latam
- https://blog.iseclab.org/2012/06/04/andrubis-a-tool-for-analyzing-unknown-android-applications-2/
- https://code.google.com/archive/p/droidbox/