Tendências do mercado nacional: procurando malware em aplicações Android

Vitor M. Afonso[1], André R. A. Grégio[1], Eduardo Ellery[1], Glauco B. Junquera[2], Guilherme A. K. Schick[2], Ricardo Dahab[1], Paulo Lício de Geus[1]

[1]Universidade Estadual de Campinas (UNICAMP)

[2]Samsung Instituto de Desenvolvimento para a Informática

Abstract. *Mobile devices rely on marketplaces (or app stores) to intermediate applications' downloading. Android devices can use the official marketplace, Google Play, or alternative ones, which may not restrict or evaluate available applications in an adequate way. The lack of rigorous control and the increase of mobile malware make it easier to the user to be a victim of a marketplace malicious application. In this article, we analyze over 5 thousand applications that affect Brazilian users to search for Android malware.*

Resumo. *Dispositivos móveis dependem de "lojas" para intermediar a obtenção de suas aplicações. Dispositivos Android contam com a loja oficial, Google Play, ou com lojas alternativas, as quais podem não restringir ou avaliar adequadamente as aplicações disponibilizadas. O controle menos rigoroso somado ao crescimento na quantidade de malware voltado para dispositivos móveis torna os usuários passíveis de infecção por malware presentes nas lojas. Neste artigo é feita a análise de mais de 5 mil aplicações de lojas que atendem o público brasileiro em busca de malware de Android entre elas.*

1. Introdução

Grande parte dos ataques atuais contra dispositivos computacionais e seus usuários envolve algum programa malicioso (*malware*). Muitos ataques mais genéricos (baseados no comprometimento de quaisquer dispositivos vulneráveis encontrados) podem ser dirigidos a nichos—tipos de usuários, linguagem do sistema, existência de certa aplicação ou biblioteca. Dessa forma, mesmo que os ataques ocorram em escala global, é importante que se tenha uma visão local que possibilite perceber as tendências encontradas no contexto em que os alvos se encontram.

Plataformas móveis em geral fazem com que o usuário se autentique em uma loja de aplicações para obter e instalar novos programas em seu dispositivo. Tal limitação é uma forma de tentar proteger os usuários e minimizar o problema dos ataques ocasionados por *malware*. No caso da plataforma Android, as aplicações também podem ser instaladas de lojas alternativas, potencialmente menos seguras. Porém, pode-se encontrar aplicações maliciosas inclusive na loja oficial (Google Play) [Grace et al. 2012, Zhou et al. 2012b].

A grande penetração do sistema operacional Android no mercado o torna um alvo interessante para ataques por *malware* [Gartner 2012]. Há trabalhos na literatura que investigaram a existência de aplicações maliciosas em lojas alternativas (foco na Ásia e Europa) e na loja oficial [Grace et al. 2012, Zhou et al. 2012b, Zhou et al. 2012a,

Enck et al. 2011]. Neste trabalho, são investigadas aplicações populares disponíveis para usuários brasileiros visando encontrar *malware*. Os resultados dessa investigação delineiam parte do cenário atual dos ataques por *malware* contra dispositivos móveis em atividade no Brasil.

2. Trabalhos Relacionados

De acordo com relatório da empresa Kaspersky, as ameaças a dispositivos móveis mais comumente encontrados na América Latina no primeiro semestre de 2012 são relacionadas a ataques por *malware*. Segundo o autor, os tipos de *malware* mais comuns são *DangerousObject*, *Trojan.AndroidOS.Plangton.a* e *Exploit.AndroidOS.Lotoor* [KasperskyLab 2012].

Um tipo de ataque por *malware* comum em países como Rússia e China é aquele que faz o envio de mensagens SMS que geram custos para o usuário e ganhos financeiros para o atacante. A empresa ESET descobriu 22 aplicações maliciosas na Google Play que enviavam mensagens SMS para números *premium* e que possuíam números de telefone válidos suficientes para funcionar em 63 países, incluindo o Brasil [Eset 2012].

Em [Zhou et al. 2012a], os autores coletaram aplicações de seis lojas alternativas (duas dos EUA, duas da China e duas da Europa) e da loja oficial do Google. Eles descobriram que a quantidade de aplicações modificadas (troca/modificação de bibliotecas de propaganda e injeção de códigos) varia de 5 a 13%. Em [Zhou et al. 2012b], os autores obtiveram aplicações da loja oficial e de quatro lojas alternativas (três chinesas e uma indisponível atualmente) e identificaram que 0,02% das aplicações obtidas da loja oficial eram maliciosas. Nas alternativas, a taxa de detecção variou entre 0,20% e 0,47%.

3. Resultados Obtidos

Foram obtidas as 300 aplicações gratuitas mais populares de cada categoria da loja AndroidPIT[1], totalizando 4.916 aplicações diferentes. De forma semelhante, foram listadas as 400 aplicações gratuitas mais populares de cada categoria da Google Play e obtidas 939 aplicações nacionais. No total, foram coletadas 5.855 aplicações.

As aplicações coletadas foram submetidas ao Andrubis[2]. Do total, 646 aplicações não puderam ser analisadas por restrições de tamanho do sistema ou por algum problema durante sua execução. Andrubis é um sistema de análise dinâmica de *malware* de Android baseado no Droidbox[3] (ferramenta mantida pelo Honeynet Project), que por sua vez é baseado no Taintdroid [Enck et al. 2010]. Além das capacidades herdadas de ambos os sistemas, o Andrubis é capaz de detectar quando uma aplicação subverte uma permissão. A seguir são apresentados os comportamentos observados.

Hosts acessados. Das aplicações analisadas pelo Andrubis, pelo menos 29,18% (1.520) acessaram um *host* relacionado com propaganda. Além disso, 13,32% (694) acessaram *host* relacionado com o monitoramento do usuário na Internet e 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.

[1] `http://www.androidpit.com.br`
[2] `http://anubis.iseclab.org/`
[3] `https://code.google.com/p/droidbox/`

Vazamento de informações. 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. Neste trabalho focou-se apenas nos vazamentos pela rede e por SMS, por indicarem 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 delas conseguiram subverter a permissão *android.permission.INTERNET*, que permite acesso à Internet, e uma delas 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.

4. Discussão

A análise com o sistema Andrubis revelou que pelo menos 29,18% das aplicações acessaram URLs relacionadas à distribuição de propaganda, pelo menos 13,32% das aplicações acessaram URLs relacionadas ao monitoramento de usuários na Internet e 13,88% evadiram informações do usuário pela rede. Considera-se estes comportamentos suspeitos, mas sem uma análise mais profunda 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.

Os comportamentos mais nocivos identificados são: acesso a uma URL relacionada ao *malware* "plankton" feito por pelo menos 1,79% das aplicações; subversão de permissões, feito por 0,67% das aplicações; envio de SMS ou realização de ligação, feitos por 0,46% das aplicações. Estes comportamentos corresponderam a 152 aplicações diferentes, 2,92% das analisadas pelo sistema Andrubis. De forma semelhante aos trabalhos relacionados discutidos anteriormente, pode-se ver que neste caso também há mau uso das informações dos usuários. Considerando as aplicações que acessaram o *host* relacionado ao *malware* "plankton" como maliciosas, tem-se uma taxa de aplicações maliciosas superior às reportadas pelos trabalhos relacionados, que não chegaram a 1% em [Zhou et al. 2012b] e [Grace et al. 2012]. Portanto, a análise de aplicações gratuitas mais populares acessadas no Brasil, tanto na loja oficial quanto em uma loja alternativa, indica que é necessário que haja um controle maior das aplicações disponibilizadas, assim como métodos de proteção efetivos para os usuários de dispositivos móveis.

5. Conclusão

Neste artigo, mostrou-se que há uma taxa considerável de aplicações maliciosas disponíveis aos usuários do mercado nacional. Essa taxa foi maior do que as obtidas em trabalhos relacionados, porém nota-se que os tipos de *malware* e comportamentos suspeitos identificados são semelhantes.

6. Agradecimentos

Os autores gostariam de agradecer aos pesquisadores do Seclab/UCSB que permitiram a sumissão de uma grande quantidade de aplicações ao Andrubis. Parte dos resultados apresentados neste trabalho foram obtidos por meio do Projeto intitulado "Avaliação e prevenção de vulnerabilidades de segurança, em plataformas smartphone e tablet", financiado pela Samsung Eletrônica da Amazônia Ltda., no âmbito da Lei no. 8.248/91.

Referências

Enck, W., Gilbert, P., Chun, B., Cox, L., Jung, J., McDaniel, P., and Sheth, A. (2010). Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones. In *Proceedings of the 9th USENIX conference on Operating systems design and implementation*, pages 1–6. USENIX Association.

Enck, W., Octeau, D., McDaniel, P., and Chaudhuri, S. (2011). A study of android application security. In *Proceedings of the 20th USENIX security symposium*.

Eset (2012). Boxer: Primer troyano para android que envia sms premium de 63 países, entre ellos españoles, desde los teléfonos de los usuarios sin su conocimiento. Disponível em `http://blogs.protegerse.com/laboratorio/2012/11/08/boxer-primer-troyano-sms-para-android-que-suscribe-a-usuarios-espanoles-y-de-otros-63-paises-a-servicios-premium-sin-su-conocimiento/`. Acessado em 07 de julho de 2013.

Gartner (2012). Gartner says worldwide sales of mobile phones declined 3 percent in third quarter of 2012; smartphone sales increased 47 percent. Disponível em `http://www.gartner.com/newsroom/id/2237315`. Acessado em 07 de julho de 2013.

Grace, M., Zhou, Y., Zhang, Q., Zou, S., and Jiang, X. (2012). Riskranker: scalable and accurate zero-day android malware detection. In *Proceedings of the 10th international conference on Mobile systems, applications, and services*, pages 281–294. ACM.

KasperskyLab (2012). Malware para dispositivos móveis: perspectiva latino americana. Disponível em `http://brazil.kaspersky.com/sobre-a-kaspersky/centro-de-imprensa/blog-da-kaspersky/malware-mobile-latam`. Acessado em 07 de julho de 2013.

Zhou, W., Zhou, Y., Jiang, X., and Ning, P. (2012a). Detecting repackaged smartphone applications in third-party android marketplaces. In *Proceedings of the second ACM conference on Data and Application Security and Privacy*, pages 317–326. ACM.

Zhou, Y., Wang, Z., Zhou, W., and Jiang, X. (2012b). Hey, you, get off of my market: Detecting malicious apps in official and alternative android markets. In *Proceedings of the 19th Annual Network and Distributed System Security Symposium*.

