Estudo sobre spywares. Uma Proposta de Solução para o Controle de Dispositivos Móveis

Camila de Matos Alonso, Luana Vieira Martinez, Fernanda Acosta dos Santos, Leticia Cunha, Érico Marcelo Hoff do Amaral

Unipampa – Universidade Federal Pampa
Bagé – RS – Brasil
{camilamalonso, luanavmartinez, nanda.acosta.31, leticia.cunha1988, ericohoffamaral}@gmail.com

Abstract. *With the rapid expansiveness of the Android mobile platform, there was great interest not only of user and developers, as well as attackers, resulting in a wide spread of malware. The focus of this research is to make the analysis of spies malicious softwares, and from this point to integrate this type of application so that it is possible to separate them by type and provide solutions to control device wholesale.*
Keywords: *Android, Spyware, Keylogger, Security.*

1.Introdução

O Android é a plataforma móvel mais instalada e de maior crescimento, está instalada em centenas de milhões de dispositivos móveis em mais de 190 países ao redor do mundo. Segundo o site oficial Android, a Google Play é principal loja de distribuição de aplicativos e jogos para Android, dela é feito o download de mais de 1,5 milhões por mês (ANDROID, 2003). Nesta linha, Zhou *et. al.* (2012) acredita que a popularidade e adoção de dispositivos móveis têm estimulado muito a propagação de *malware* móvel, especialmente nesta plataforma.

Atualmente existem muitos aplicativos espiões para android, que podem ser encontrados facilmente na internet. Um aplicativo espião de *smartphones* é um *software* que permite que você rastreie a atividade de um dispositivo móvel alvo, com ou sem o conhecimento do usuário. Com esse software é possível armazenar vários tipos de informações relacionadas com a atividade do dispositivo, para que a pessoa que instalou o *spyware* possa monitorá-lo de forma discreta e à distância (Mohsen, 2013). Esta pesquisa tem como objetivo mostrar os principais tipos de aplicativos espiões, a fim de caracterizar o funcionamento dos mesmos, indicando o que pode ser roubado por ele e por fim disponibilizar soluções ao controle do aplicativo atacado.

2. A informação e Aplicativos Espiões

Com o avanço na área das tecnologias de informação e comunicação, uma vasta escala de problemas virtuais surgiu e cresceu gradativamente de acordo com Isoni at al (2008). Segundo o autor a grande parte dos problemas gira em torno de fraudes, tentativa de extorsão, falsificação de dados, roubo de informações pessoais e profissionais, roubo de identidade, invasão de privacidade, tais como acesso a fotos e muitos outro crimes que se encontram em crescente desenvolvimento e vêm aumentando a preocupação dos usuários dessa "*informarion highway*", como o próprio autor se refere.

Alguns ataques a dispositivos móveis envolvem danos aos usuários e aos próprios dispositivos. Os atacantes desenvolvem aplicações Android que permitem

monitorar usuários com a finalidade de coletar dados. Dessa maneira é possível exportar todas as mensagens SMS, e-mails, logs de chamadas, locais de GPS, ou ouvir mensagens de voz, segundo Chien (2003). Um tipo de aplicativo espião a ser citado são os *keyloggers*, eles podem ser parte de um *spyware* ou de um aplicativo de teclado legítimo. Um *keylogger* pode ser definido por sua vez como parte de um pacote de *spyware* baixado para algum *smartphone* sem o conhecimento do usuário. Grande parte desses aplicativos permitem capturar dados através do teclado, podendo o dado ser armazenado em um armazenamento local, ou então ser automaticamente transmitido da rede para um computador ou servidor remoto (Nasaka, 2011).

3. Metodologia e Solução Proposta

Este estudo vislumbra, a partir de uma relevante pesquisa sobre os tipos de aplicativos espiões com o objetivo de após ser concluído o estudo ser possível identificar possíveis soluções para esse problema. Um conjunto de etapas previamente estabelecidas foi criado para o desenvolvimento desta pesquisa, como segue na Figura 01.

O desenvolvimento da pesquisa seguirá um conjunto de 4 momentos, pontualmente definidos: **Informações coletadas por spyware:** Nesta primeira etapa será realizado um estudo para identificar quais as informações podem ser roubadas a partir de aplicativos espiões; **Análise dos tipos de aplicativos espiões:** A segunda etapa consiste em analisar quais os tipos de aplicativos espiões, identificando quais as suas funções e quais as diferenças de um aplicativo para o outro; **Funcionamento e acessos dos aplicativos:** Na terceira etapa iremos mostrar o funcionamento de um aplicativo espião, mostrando os passos necessários para utilizar essa ferramenta, e por fim; **Solução anti-spyware:** A partir das informações coletadas iremos buscar soluções para evitar e controlar o dispositivo contra esse tipo de aplicativo.

Figura 01: passos a serem adotados na metodologia

4. Considerações Parciais

O estudo está em fase de desenvolvimento, contudo apresenta alguns resultados preliminares. Após a conclusão da primeira etapa da pesquisa, é possível elencar os principais tipos de informações que podem ser espionadas em dispositivos móveis. Os próximos momentos buscam identificar aplicativos espiões e, a partir deste levantamento, propor um modelo integrado que sirva como solução para o controle e monitoramento deste tipo de dispositivo.

Referências

ANDROID. **Projeto Oficial**, 2003. Disponível em: <http://developer.android.com/distribute/googleplay/index.html>. Acesso em: 10 out. 2014.

CHIEN, Eric. Motivations of Recent Android Malware. **Symantec Security Response**, 2003.

ISONI, Miguel Maurício *et. al.* **E-crime em ambientes digitais informacionais da Internet**. PBCIB, v. 2, n. 2, 2008

MOHSEN, Fadi; SHEHAB, Mohammed. Android keylogging threat. In:**Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom), 2013 9th International Conference Conference on**. IEEE, 2013. p. 545-552.

NASAKA, Kohei et al. A keystroke logger detection using keyboard-input-related API monitoring. In: **Network-Based Information Systems (NBiS), 2011 14th International Conference on**. IEEE, 2011. p. 651-656.

ZHOU, Yajin; JIANG, Xuxian. Dissecting android malware: Characterization and evolution. In: **Security and Privacy (SP), 2012 IEEE Symposium on**. IEEE, 2012.