Exfiltração de dados em Android: Um estudo de caso

Pedro A. K. Leone, Pedro O. F. Blaudt, Ygor de A. Cardinot, Nilson M. Lazarin

[1]Bacharelado em Sistemas de Informação – Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (Cefet/RJ) – Nova Friburgo, RJ – Brazil

{pedro.akleone,peedrofr,ygor.cardinot,nilsonmori}@gmail.com

Abstract. *Our smartphones contain a lot of private and important data in it, such as family albums, bank information, passwords, documents, among others. This paper presents a survey with smartphone users, about your behavior and sense of security. Moreover, an analysis of the Android security system and were try some antivirus apps available on Google Play Store against a malware developed to steal pictures of user gallery.*

Resumo. *Os smartphones contêm muitos dados privados e importantes, como álbuns de família, informações bancárias, senhas, documentos, entre outros. Este trabalho apresenta uma pesquisa com usuários de smartphones, sobre seu comportamento e sensação de segurança. Além disso, foi realizada uma análise do sistema de segurança do Android e foram testados alguns aplicativos antivírus disponíveis na Google Play Store contra um malware desenvolvido para exfiltrar imagens da galeria do usuário.*

1. Introdução

Nos últimos anos houve um crescimento no uso de aparelhos smartphone no Brasil, chegando a registrar mais de 234 milhões de acessos de telefonia móvel em dezembro de 2020 [Silva et al. 2021]. Ademais, a pandemia da COVID-19 influenciou a rotina dos internautas, fazendo com que mais da metade destes estejam conectados mais de 8 horas por dia [Guilherme et al. 2021]. Nesses aparelhos estão armazenadas diversas informações pessoais e profissionais de seus usuários, além de localização, dados bancários, senhas e consumo.

Um dos fatores de segurança do sistema Android é a sua loja de aplicativos. Entretanto, existem aplicativos maliciosos, mesmo em lojas oficiais, que buscam capturar dados sensíveis, tanto para vendê-las, usar de maneira ilícita ou até sequestrar os dados [Mas'ud et al. 2014]. Brechas de segurança sejam elas causadas por uma aplicação maliciosa ou uma conexão insegura na internet apresentam um grande risco ao usuário [Omer et al. 2021].

Este trabalho apresenta uma pesquisa com usuários de smartphones, realizada por redes sociais. Buscou-se compreender quais as medidas de segurança comumente utilizadas e se eles já sofreram algum problema de segurança. Além disso, é apresentada uma análise sobre o funcionamento de softwares antivírus. Para isso, um trojan foi desenvolvido com a intenção de exfiltrar imagens da galeria do usuário para um servidor através do protocolo HTTP. Os experimentos foram realizados pelos autores em VM (máquinas virtuais) executando o sistema Android. Nessas foram instalados aplicativos antivírus disponíveis na loja de aplicativos. Por fim, o Trojan foi instalado em cada VM e o comportamento do software antivírus e do trojan foram analisados.

2. Pesquisa com usuários

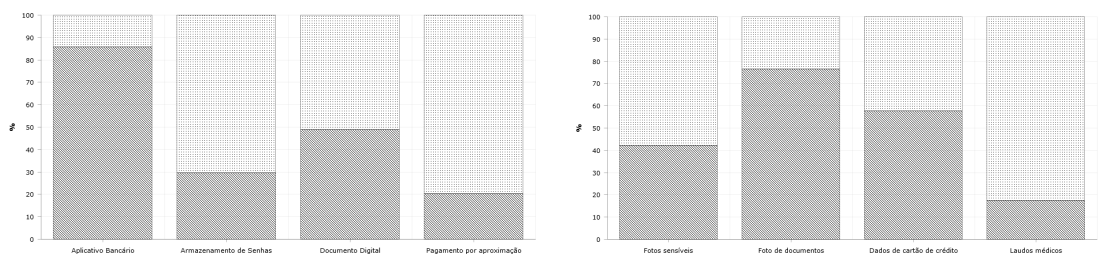
Foi realizada uma pesquisa via formulário online, com usuários de smartphone, por redes sociais. Foram obtidas 102 respostas. Buscou-se compreender quais as medidas de segurança comumente utilizadas e se eles já sofreram algum problema de segurança, além disso, os respondentes foram questionados sobre o sistema operacional e categorias de aplicativos utilizados no aparelho, por fim, foram questionados sobre que categoria de dado sensível estão armazenados no aparelho. Foram obtidos os seguintes resultados:

- **Sistema Operacional:** 91.2% afirmaram usar Android e 8.8% iOS.
- **Incidentes de Segurança:** 14.7% declaram que já tiveram o celular roubado, 2% já tiveram o celular clonado, 3.9% já tiveram o celular invadido, 3,9% tiveram dados roubados e nenhum participante informou que teve dados sequestrados.
- **Sensação de segurança:** os participantes consideram seus smartphones: Muito seguro (9.8%); Seguro (37.25%); Razoável (40.20%); Inseguro (11.76%); e Muito inseguro (0.98%).
- **Controle de acesso:** 4.9% informaram não utilizar nenhuma segurança para o desbloqueio do aparelho, 36.3% informaram utilizar senha de desenho, 34.3% informaram utilizar PIN (senha numérica).
- **Uso de biometria:** para o controle de acesso, 16.38% informaram não utilizar biometria, 68.97% informaram utilizar a digital e 14.66% informaram utilizar reconhecimento facial ou de íris.

Os participantes ainda foram questionados sobre o uso de aplicativos não oficiais (obtidos fora da loja de aplicativo padrão do sistema), 46.1% afirmaram já ter instalado algum aplicativo não oficial. Sobre o uso de software antivírus, 75.5% dos participantes afirmaram não utilizar nenhum software antivírus em seu smartphone.

Sobre o uso de aplicativos sensíveis, conforme Figura 1(a), 85.7% dos participantes declararam utilizar algum aplicativo bancário, 29.6% declararam utilizar aplicativos para armazenamento de senha, 49% declararam utilizar algum aplicativo de documento digital (RG, CPF, Título de Eleitor) e 20.4% declararam utilizar algum aplicativo de pagamento por aproximação.

Sobre o armazenamento de dados sensíveis, conforme Figura 1(b), 42.4% dos participantes declararam armazenar fotos consideradas sensíveis, 76.5% declararam armazenar fotos ou digitalização de documentos pessoais, 57.6% declararam armazenar fotos ou digitalização de cartão de crédito e 17.6% declararam armazenar laudos ou exames médicos.



(a) Aplicativos sensíveis instalados (b) Dados sensíveis armazenados

Figura 1. Aplicativos e dados sensíveis no smartphone.

3. Experimentos com software antivírus

Aplicativos antivírus são incapazes de mitigar ou detectar exfiltração de dados [Ramachandran et al. 2012]. Os experimentos apresentados nesta seção buscam analisar esta afirmação. Para execução dos experimentos, foi preparado um ambiente de virtualização em uma rede isolada, contendo uma máquina virtual com Debian Buster (para armazenamento das imagens capturadas) e cinco máquinas virtuais com o Android-x86 8.1 oreo-x86[1] (para instalação dos softwares antivírus e execução do trojan).

Para a execução dos testes, em cada máquina virtual Android foi instalado um software antivírus através da Google Play Store. Foram selecionados os cinco aplicativos antivírus, melhor colocados no Mobile Security Review 2021[2] da AV Comparatives, todos com 100% de taxa de detecção. Sendo eles: Avira Security Antivirus & VPN; Bitdefender Mobile Security & Antivirus; G DATA Mobile Security Light; Kaspersky Antivirus: AppLock; Trend Micro Mobile Security & Antivirus.

Para analisar o funcionamento dos antivírus foi desenvolvido um Trojan[3], cuja função era exfiltrar as cinco últimas imagens armazenadas na galeria para um servidor remoto. O malware foi criado utilizando o Framework Flutter e a linguagem Dart.

Também foi necessária a criação de um servidor para onde pudessem ser enviadas as requisições HTTP do malware e assim as imagens pudessem ser convertidas e armazenadas. O servidor foi criado utilizando Node.js.

Posteriormente, em cada máquina virtual o navegador foi aberto e realizou-se o download do arquivo .APK do trojan. Através do aplicativo Files do Google, foi realizada a instalação do .APK. Após a instalação o aplicativo malicioso foi executado e o usuário recebe uma notificação do sistema que o aplicativo deseja acessar fotos, mídias e arquivos do dispositivo. Caso o usuário aceite o pedido, as imagens da galeria são codificadas em Base64 e enviados via JSON para o servidor na rede.

Era esperado que o antivírus instalado impedisse a instalação ou execução do malware. Adicionalmente foram realizadas varreduras à procura de malware. Na tabela abaixo encontram-se os resultados de cada antivírus testado e sua respectiva versão. Destaca-se que o Kaspersky não funcionou no Android x86, exibindo mensagem de erro ao ser executado. Em todas as execuções dos antivírus que puderam ser executados, nenhum conseguiu relatar algum problema durante o download, durante a instalação, durante a execução ou durante a varredura.

Antivírus	Versão	Instalação	Execução	Impediu o download	Impediu a instalação	Localizou na varredura
Avira	7.10.1	OK	OK	NÃO	NÃO	NÃO
Bitdefender	3.3.159.1907	OK	OK	NÃO	NÃO	NÃO
G DATA	27.4.4.2130ad	OK	OK	NÃO	NÃO	NÃO
Kaspersky	11.79.4.6841	OK	ERRO	NÃO	NÃO	ERRO
Trend Micro	12.10.0	OK	OK	NÃO	NÃO	NÃO

Tabela 1. Resultados dos experimentos.

[1] https://www.android-x86.org/releases/releasenote-8-1-r6.html
[2] https://www.av-comparatives.org/tests/mobile-security-review-2021/
[3] https://github.com/LabRedesCefetNF/android-exfiltracao

4. Considerações finais

Neste trabalho foi apresentada uma pesquisa, onde se constatou que quase a metade dos participantes afirmaram já ter instalado algum aplicativo não oficial em seu smartphone, confirmando o apontado em Guilherme *et al*. (2021) de que o usuário tem a tendência de baixar aplicativos, programas ou arquivos de origem duvidosa e compartilhar o smartphone com outras pessoas.

Também, foi possível constatar que mais da metade dos participantes afirmaram armazenar fotos ou digitalização de cartão de crédito, ou de documentos pessoais em seu smartphone. Este comportamento do usuário de smartphone é preocupante, pois como demonstrado, um aplicativo mal-intencionado pode burlar a segurança nativa do sistema Android, enganando o usuário e facilmente capturar as imagens armazenadas na galeria.

Os aplicativos antivírus analisados não conseguiram mitigar a exfiltração de dados, conforme apontado por Ramachandran *et al*. (2012). O trojan desenvolvido, após enganar o usuário para ter acesso à galeria de imagens, converteu os arquivos em base64 e os enviou por requisições HTTP, direcionadas a um servidor na rede. Os aplicativos antivírus, mesmo aqueles que apresentam módulo de segurança web, não impediram o download do arquivo .APK, não impediram a instalação do aplicativo de fonte desconhecida, não impediram a execução do mesmo e também não conseguiram interceptar a comunicação de rede.

Trabalhos futuros podem analisar outros softwares antivírus ou levantar e analisar outras ferramentas que possam conseguir mitigar a exfiltração de dados em dispositivos mobile.

Referências

Guilherme, L., Ferreira, M., da Fonseca, G., and Lazarin, N. (2021). Uma breve noção sobre o comportamento dos internautas em relação à segurança na rede. In *Anais da VII Escola Regional de Sistemas de Informação do Rio de Janeiro*, pages 1–7, Porto Alegre, RS, Brasil. SBC.

Mas'ud, M. Z., Sahib, S., Abdollah, M. F., Selamat, S. R., and Yusof, R. (2014). Android Malware Detection System Classification. *Research Journal of Information Technology*, 6(4):325–341.

Omer, M. A., Zeebaree, S. R. M., Sadeeq, M. A. M., Salim, B. W., Mohsin, S. x., Rashid, Z. N., and Haji, L. M. (2021). Efficiency of Malware Detection in Android System: A Survey. *Asian Journal of Research in Computer Science*, pages 59–69.

Ramachandran, R., Oh, T., and Stackpole, W. (2012). Android anti-virus analysis. In *Annual symposium on information assurance & secure knowledge management*, pages 35–40, NY, USA. Citeseer.

Silva, H. B. P., Simas, H., Moura, P. R. d., Griese, P. B., Rampaso, R. C., and Macedo, S. A. C. (2021). RELATÓRIO DE ACOMPANHAMENTO DO SETOR DE TELECOMUNICAÇÕES: Telefonia Móvel 2º semestre de 2020. Technical report, ANATEL, Brasília.