An Exploratory Analysis in Android Malware Trends

Full paper

Chelsea Hicks
University of Texas at San Antonio
chelsea.hicks@utsa.edu

Glenn Dietrich
University of Texas at San Antonio
glenn.dietrich@utsa.edu

Abstract

As smartphones become increasingly integral to our daily lives, so too is the prevalence of malware for smartphones. This is because while mobile phones used to only function as portable phones, today's mobile phones are now miniature computers. This means that risks that used to only be for computers are now risks for our smartphones as well. As a result, a research stream dedicated to understanding what's unique about smartphone malware has emerged. In this study, we analyze malware characteristics from a non-technical view, unlike previous studies. Previous studies analyze the actual code and execution of malware, while we take advantage of anti-virus companies analysis of malware already conducted, and instead analyze these analyses. We do this to discover trends that are emerging in smartphone malware, such that anti-virus companies can give these trends greater priority to researching and discovering these malware.

Keywords

mobile malware, android malware, malware trends.

Introduction

One of the never ending problems that both users and organizations have is malware. Malware is a term used to describe malicious software on computers that can steal data, delete files, or otherwise harm an individual. Malware has been around since at least 1988, where the first Internet Worm was created (i.e. the Morris Worm). Since then, it has been only a growing problem for two primary reasons: the first being that malware continues to become more harmful (such as locking a user out of their computer unless they pay a ransom), and that it is getting harder to catch all malware due to the reliance of using signatures to detect malware. As a result, malware continues to become more prevalent. In this paper, we concentrate on one example of this – malware now being on smartphones. Malware on smartphones is increasing at an alarming rate. Between December 2012 and December 2013, there was an increase of malware on smartphones of 197% (McAfee 2014). In this study, we only concentrate on Android smartphones, as they are the most targeted smartphones for malware and they have the most market-share at 75% (Faruki et al. 2015; Kelly 2014).

Previous literature for smartphone malware has focused on various aspects. From a technical standpoint, one of the most popular topics is to study the characteristics of smartphone malware in order to improve anti-virus software for smartphones (Arabo and Pranggono 2013; Ho and Heng 2009; Zhou and Jiang 2012). Similarly, there are studies that concentrate on improving detection of malware on third-party app stores, surveying the status of malware on different markets, identifying trends of anti-virus companies, or simply listing the challenges that currently exist in the smartphone malware literature (Arabo and Pranggono 2013; Shaerpour and Dehghantanha 2013; Zhou et al. 2012). Finally, research has focused on analyzing Android malware from an aspect on how to best analyze the malware – dynamically or statically, and proposing new solutions to help malware investigators better discover and analyze malware (Allix et al. 2014; Karlsson and Glisson 2014; Linger et al. 2011; Smith and Pridgen 2012). From a behavioral standpoint, literature has concentrated on the need for better training, studying whether users have become desensitized to their mobile application requests, and security concerns for small and medium enterprises (Brookshire et al. 2015; Harris et al. 2012, 2013).

In this study, we take a different approach. While we are studying characteristics of mobile malware, we are studying different characteristics than previously studied. Previous characteristics that have been studied are very technical and relate to the code of the malware itself (Arabo and Pranggono 2013; Ho and Heng 2009; Zhou and Jiang 2012). In this study, we study characteristics relating to the infection channels (i.e. the way in which malware is delivered to a smartphone), and mobile malware characteristics that the anti-virus companies assign each malware. The primary research question in this paper is to discover what factors influence mobile malware to be more successful on different infection channels, so companies can defend against mobile malware from a behavioral aspect rather than a technical aspect. We believe that the characteristics in this paper are critical to understand. This is because technical features, which are what previous research has primarily concentrated on, often require a technical background in order to fully understand. Additionally, once a characteristic is understood about a malware, it is limited in scope – this characteristic will most likely only be found in that malware and any of it's variants (i.e. how it infects a phone, how it steals data, etcetera). These types of characteristics are well suited for improving anti-virus software, but they do not help studying malware from a behavioral point of view. The characteristics we study in this paper are easier to obtain than actual malware, as it requires collecting data from anti-virus vendors. Additionally, experts in malware (i.e. the anti-virus vendors) have made the classifications used in this dataset, which allows us to utilize their knowledge in an inexpensive manner. One of the biggest advantages our characteristics have is that we can obtain insights from a higher level, such as the trend of malware in a given time period, in a time efficient manner since we do not have to examine the malware manually. Using this insight, organizations and individuals can make more informed decisions on how to defend against malware. For example, if we find that app stores are more susceptible to malware that is spyware, then app stores can try to inspect their apps more carefully for spyware until the trend is over. Additionally, organizations could provide targeted training of specific malware that is the most popular to protect against these trends.

The paper is organized as follows. The next section outlines the related work of our study. The following section introduces our methodology for data collection and analysis. Then, we highlight the findings of the study and discuss the results. Finally, we conclude the paper and provide highlight potential future work.

Related Work

Malware can be defined as applications that gain access to a device for the purpose of stealing data, damaging the device, annoying the user, etcetera (Felt et al. 2011; Ho and Heng 2009). In order for malware to get on the smartphone, the malware must convince the user to download it. This can be done in various ways, such as by being downloaded when a user accidentally clicks a malicious link, or when the user downloads an application that seems safe when it is not. Then, once the application is on the smartphone, it uses an exploit or excessive privileges on the smartphone to gain access and achieve its goals, such as stealing data (Felt et al. 2011; Ho and Heng 2009). Malware is a broad term, and includes specific types such as Trojans, worms, botnets, and viruses (Felt et al. 2011).

In 2011, there was an increase in mobile malware of 155 percent increase from 2010 (Arabo and Pranggono 2013). Malware targeting Android smartphones experienced the largest increase, as in 2011 there was a 3325 percent increase (Arabo and Pranggono 2013; Zhou and Jiang 2012). The reason that Android smartphones are targeted so much is that Android, the operating system of the smartphone, is open source. What this means is that anyone can look at the technical details of the operating system and discover exploits much easier than normal. Additionally, Android smartphones are the best selling smartphones in the market. This leads to Android smartphones being the most targeted smartphones for malware. Google tried to prevent this by making applications declare permissions that they required on the smartphone, and the user could approve the access (Shaerpour and Dehghantanha 2013).

However, it has been shown that users don't understand the warnings and as a result, disregard the warnings (Bal 2014; Shaerpour and Dehghantanha 2013). As a result, researchers have done tests to see much malware exists on the official Android marketplace, and how much exists in alternative markets (Zhou et al. 2012). Alternative markets are places where users can buy and download applications that aren't supported by Google, such as Amazon's app store. These alternative markets are generally not as strictly regulated as the application store from the manufacturer, and research supports this. It was found in 2012 that the Android market had a 0.02% infection rate, while alternative markets had 0.20-0.47% infection rate (Zhou et al. 2012). While this rate is very low and may make users think that they shouldn't worry about mobile malware, this is incorrect. When a new malware called DroidDream was released, it took 48 hours for Google to remove the malware from the Android market and infected more than 260,000 users (Zhou et al. 2012). This is enough time for malware to cause serious harm to these users, whether it may be damaging their phone or stealing sensitive data.

As emphasized throughout this literature review, most of the previous literature has been setting the stage for future research. This has included defining mobile malware, which is an important step in a new domain. They then moved onto studying characteristics of mobile malware to improve detection, trends in malware detection to find short comings, and improvements on detecting mobile malware. In this study, we are studying characteristics of malware to help understand how to better detect and prevent malware in the future.

Methodology

To collect data, we manually gathered data using Trend Micro's database of threats (TrendMicro 2016). While data collection began November 24, 2015, we went back as far as January 1, 2012 to collect data. This continued until December 15, 2016. This resulted in 155 unique malware's characteristics being obtained. We obtained the following information for each malware: name, date the malware's information as published, threat sub-type, threat type, damage potential, distribution potential, and infection channel.

Threat sub-type represents what Trend Micro classified the actual malware to do. Threat sub-type consists of seven unique categories. These categories were: Click Fraud, Hacking Tool, Information Stealer, Malicious Downloader, Premium Service Abuser, Rooting Tool, and Spying Tool. The threat type was the type of malware that was classified, where there were six different types: adware, backdoor, cracking application, hacking tool, spyware, and Trojan. Damage potential is how much potential the malware has to damage a smartphone or it's user, which from low to critical. Damage potential was simply classified as low, medium, high, or critical. In this dataset no high damage potential malware was found, so the only categories ended up being low, medium, or critical. Distribution potential is how much potential a malware has to spread rapidly, and it was simply classified as low, medium, high, or critical. In this dataset no high distribution was found. Infection channel is how the malware gets put onto the phone, and there were six categories, which were app store (which includes both Google Play and other third party app stores), downloaded from the Internet, dropped by other malware, manually installed, SMS messages, and visiting malicious websites.

The collected data was analyzing using the IBM SPSS Statistics 22 software (IBM 2015). The statistical significance and strength of interactions between the different malware characteristics were analyzed through contingency tables, the Pearson's $\chi 2$ tests of independence, and the Cramer's V coefficients. We considered only results that had a p-value that was below 0.05. We chose to use contingency tables as our method of analysis as we are doing an exploratory study, we wanted a statistical analysis method that was flexible and allowed us to find unique interactions. More traditional methods were not chosen, such as ANOVAs, as most of our data was categorical, which greatly limits what methods of analysis we can use.

While using contingency tables are uncommon, we are not the only ones who have done so. Contingency table has been used for varying purposes, including but not limited to: discovering what favors influenced people to adopt exercise games, test what characteristics contribute to the differentiation of crowdfunding intermediaries, uncover conjunctions between mobile enterprise application characteristics, to discover the extent of reviews differing among open source projects, and to analyze the interaction between user skill level, travel product, and online shopping motivation (Asundi and Jayant 2007; Beldona et al. 2005; Giessmann et al. 2012; Haas et al. 2014; Kari 2015).

Results

As shown in Table 1, we analyze the interaction of dates and threat subtype. When looking through this contingency table, some interesting trends emerge. While some threat subtypes such as click fraud, and hacking tools have stayed around the same throughout the years, the other threat subtypes have more interesting results. For example, when analyzing information stealer, we can see that this type of threat subtype was extremely common in 2012, but as the years progressed it dwindled down to a negligible amount of malware. This trend continues for the premium service abuser and spying tool as well. This is a strange trend, as this would argue that the overall amount of malware is decreasing over time, as well as threat subtypes. This seems counterintuitive, as many people argue that malware is continuing to grow at an exponential pace (PRNewswire 2012).

Threat Subtype							
Date	Click Fraud	Hacking Tool	Information Stealer	Malicious Downloader	Premium Service Abuser	Rooting Tool	Spying Tool
2012	1	2	35	4	20	8	8
2013	3	1	18	0	4	2	0
2014	5	3	9	1	3	3	0
2015	3	0	6	1	1	6	2

Table 1. Threat Subtype by Date

Analyzing Table 2, more counterintuitive findings emerge. While the trend of malware decreasing over the years has emerged, as discovered previously, a more interesting trend emerges in this contingency table. Over the years, the amount of low damaging malware has gone to zero, the amount of medium damaging malware has stayed about the same, and the amount of critically damaging malware has decreased dramatically over the years. If news reports and academia are to be believed, this should not be the case – the amount of malware and the damage potential should be at least maintaining, if not increasing.

Damage Potential			
Date	Low	Medium	Critical
2012	14	15	49
2013	2	4	22
2014	3	16	5
2015	0	12	7

Table 2. Damage Potential by Date

From Table 3, we can see that the trends that emerge from this contingency table are not as interesting as previous discovered. The overall trend is that the distribution potential of all malware is decreasing to a low distribution potential, and the amount of malware has decreased over the years. Is this trend due to better warnings and awareness to the end user, or are smartphone manufacturers better securing exploits? No one agrees that either of these are the cases, in fact they argue the opposite (Faruki et al. 2015; Linger et al. 2011; Zhou et al. 2012, 2012). Therefore, this is another interesting trend that has emerged.

Distribution Potential			
Date	Low	Medium	Critical
2012	71	7	0
2013	25	3	0
2014	15	7	1
2015	16	2	0

Table 3. Distribution Potential by Date

Table 4 shows the contingency table for infection channel by date. While some infection channels, such as SMS messages and the app store have maintained a similar trend throughout the years, the rest of the infection channels have shown a drastic decrease. For example, visiting malicious websites has dropped to zero in 2015, while it was the second largest infection channel in 2012. While not as drastic, this is also the case for downloaded from the internet and manually installed. We again wonder why this counterintuitive result has emerged – both academia and practitioners agree that mobile malware is a continuing issue, not one that is solving itself. This concludes the discussion of any of the malware characteristics and dates.

			Infection Channel			
Date	App Store	Downloaded From Internet	Dropped by Other Malware	Manually Installed	SMS Messages	Visiting Malicious Websites
2012	9	12	8	28	1	20
2013	7	0	2	7	2	10
2014	10	2	2	8	1	1
2015	6	3	0	9	1	0

Table 4. Infection Channel by Date

Starting in this section, we start analyzing the different malware characteristics when compared to the threat subtype of the malware. Table 5 shows the contingency table for damage potential by threat subtype. We see that spying tools are never a low damage risk – they are only medium or critical. This makes sense as spying tools are always gathering private information about a user that they would not want leaked – such as their login credentials, their contacts list, and their private messages. All of the results in Table 5 are intuitive and help confirm that the current understanding of threat subtypes is correct.

	Damage Potential		
Threat Subtype	Low	Medium	Critical
Click Fraud	2	9	1
Hacking Tool	1	2	3
Information Stealer	3	14	51
Malicious Downloader	1	4	1
Premium Service Abuser	7	13	8
Rooting Tool	5	1	13
Spying Tool	0	4	6

Table 5. Damage Potential by Threat Subtype

Table 6 shows the contingency table for threat type by threat subtype. One of the most obvious results is that Trojans are the most common type of smartphone malware, which supports existing literature (Faruki et al. 2015; Shaerpour and Dehghantanha 2013). We can additionally confirm that our definitions for threat type makes sense by using the threat subtypes. For example, spyware only has the the subtypes of information stealers and spying tool, which makes intuitive sense. Spyware, as discussed earlier, is spying on the user and stealing their information – which is what spying tools and information stealers do respectively. Click Fraud only makes up Adware and Trojans, which again make sense. Adware shows annoying ads that may charge users, while Trojan may pretend to be an app that it is not – such a game with in-app purchases. Hacking tools are only hacking tools and Trojans, the surprising one out of these two is the fact that Trojans can be hacking tools. However, this is most likely due to the fact a user may want a hacking tool, but the official app store may not want this listed – therefore the app will pretend to be something else. Information stealer can be adware, backdoor, spyware, and Trojans which makes intuitive sense. Malicious downloaders can only be found in Trojans – which could be surprising that backdoors are not included in this. However, the fact Trojans can be malicious downloaders make sense – if a Trojan is doing something malicious, it may need to download additional tasks without the user knowing, which can constitute as a malicious downloader. Premium service abusers were found to only be backdoors and Trojans. Rooting tools were found to be in backdoors, hacking tools, and Trojans. Again, this is not surprising.

Threat Type					
Threat Subtype	Adware	Backdoor	Hacking Tool	Spyware	Trojan
Click Fraud	1	0	0	0	11
Hacking Tool	0	0	4	0	2
Information Stealer	4	19	0	6	39
Malicious Downloader	0	0	0	0	6
Premium Service Abuser	0	2	0	0	26
Rooting Tool	0	2	15	0	2
Spying Tool	0	1	0	6	3

Table 6. Threat Type by Threat Subtype

From Table 7, we can see that manual installation, app store, and visiting malicious websites are the most common way to obtain smartphone malware. This is not surprising, and is intuitive. What is more interesting is how information stealer, malicious downloader, and premium service abusers are the type of malware that gets dropped by other malware. Additionally, click fraud, information stealer, and premium service abusers are the type of malware that gets installed via SMS messages. The rest of the results are intuitive and are not discussed further.

Infection Channel						
Threat Subtype	App Store	Download From Internet	Dropped by Other Malware	Manually Installed	SMS Messages	Visiting Malicious Websites
Click Fraud	6	1	0	3	1	1
Hacking Tool	2	1	0	3	0	0
Information Stealer	11	7	8	19	3	20
Malicious	2	1	1	2	0	0

Downloader						
Premium Service Abuser	6	4	3	6	1	8
Rooting Tool	2	0	0	16	0	1
Spying Tool	3	3	0	3	0	1

Table 7. Infection Channel by Threat Subtype

Table 8 allows us to see which types of threat types are the most damaging. Unsurprisingly, Trojans, backdoors, and hacking tools are the most critically damaging smartphone malware. What is a bit surprising being that adware has been critical damaging according to TrendMicro, which contradicts the normal understanding of adware – which is typically just annoying and may obtain minor information about a user.

Threat Type					
Damage Potential	Adware	Backdoor	Hacking Tool	Spyware	Trojan
Low	0	1	5	0	13
Medium	1	3	2	2	39
Critical	5	24	19	12	89

Table 8. Threat Type by Damage Potential

Table 9 shows us to how malware is obtained. Not surprisingly, Trojans can be obtained in all infection channels, and it is the only type of malware that can do so. It is also not surprising that hacking tools and backdoors are most commonly manually installed. Most of these results are intuitive and make sense.

Infection Channel						
Threat Type	App Store	Downloaded From Internet	Dropped by Other Malware	Manually Installed	SMS Messages	Visiting Malicious Websites
Adware	2	1	0	0	0	2
Backdoor	3	0	1	12	1	7
Hacking Tool	1	0	0	17	0	1
Spyware	3	2	0	3	0	4
Trojan	23	14	11	20	4	17

Table 9. Infection Channel by Threat Type

Table 10 shows the statistical significance of all the contingency tables discussed so far. All of the contingency tables meet our p-value requirement of being less than 0.05, as otherwise they were not included in our discussion. We are primarily interested in Cramer's V, as Cramer's V is used to measure the strength of the association between variables, and allows variables to have more than 2 categories. We interpret Cramer's V as follows: anything below 0.15 is unacceptable, 0.15 to 0.20 is weak, 0.20 to 0.25 is moderate, 0.25 to 0.30 is moderately strong, 0.30 to 0.35 is strong, 0.35 to 0.40 is very strong, 0.40 to 0.50 indicates either an extremely good relationship or two variables measuring the same concept. Anything above 0.50 indicates that both variables are probably measuring the same concept. Analyzing Table 10, distribution potential by date is the only one that has a moderate relationship. We have no relationships that are weak. Threat subtype by date, infection channel by date, infection channel by threat subtype, threat type by damage potential, and infection channel by threat type all have a moderately strong relationship. Damage potential by date and damage potential by threat subtype have a strong relationship. Finally, threat type by threat subtype is our only worrisome result with a Cramer's V of 0.533, which means that they may be measuring the same concept. This is unsurprising, as threat subtype can easily be seen as a subset of threat type. Therefore, we do not consider this relationship any further.

Contingency Table Results			
	Pearson χ2	Cramer's V	p-value
Threat Subtype by Date	37.512	.290	.004
Damage Potential by Date	36.356	.349	.000
Distribution Potential by Date	18.161	.202	.033
Infection Channel by Date	31.168	.264	.008
Damage Potential by Threat Subtype	45.127	.389	.000
Threat Type by Threat Subtype	169.089	0.533	.000
Infection Channel by Threat Subtype	47.556	.253	.022
Threat Type by Damage Potential	26.105	.296	.001
Infection Channel by Threat Type	47.589	.283	.000

Table 10. Contingency Table Results

As we found earlier, the following relationships are significant: distribution potential by date, threat subtype by date, infection channel by date, infection channel by threat sub type, threat type by damage potential, infection channel by threat type, damage potential by date and damage potential by threat subtype. It is important to understand these characteristics since they are significant. Out of these relationships, date is the most reoccurring characteristic. This is unsurprising as we are investigating trends, and the trends change over time which make them significant. However, what is more interesting is how often threat type and threat sub type are significant. Therefore, we argue that these two characteristics are the most critical of this study, as their definitions are not necessarily intuitive or easily agreed upon. For example, threat type in this study is defined as adware, backdoors, hacking tools, spyware, or Trojans. If any of these specific characteristics, such as Trojans, are chosen to be further studied, we could help detect and preempt malware. For example, we can see trend wise that Trojans have continued to become more popular throughout the years. This is unsurprising as malware can pretend to be games to guarantee a large amount of downloads. Therefore, a further analysis conducted only on

Trojans could help detect and prevent Trojans. From our analysis alone, we know that Trojans are most commonly downloaded form the App store or manually installed, that they are in varying damage potential (although they are primarily very damaging), and that they are primarily information stealers. This means that future research should concentrate on how to mitigate this information stealing so that sensitive data is not stolen from the user, and this should be kept in mind when further developing the Android operating system.

Conclusion

This research heavily relies on TrendMicro's dataset, which greatly limits our generalizability to all smartphone malware. If this dataset could be combined with other anti-virus vendors, such as Symantec and Virus Total, then we may get a larger dataset that as a result could be a better representation of smartphone malware as a whole. Additionally, we may be able to obtain other characteristics that may not be categorical, which could open additional statistical method analysis. We also rely on the fact that the anti-virus software has to detect the malware, then analyze it and report it online (Allix et al. 2014). This is an obvious limitation, as there are many malware that aren't found yet. Additionally, it takes quite a while for anti-virus companies to release data on the malware they find, especially detailed analysis like we require for this study. Additionally, we do not have sound theory on why the interactions discovered in this study were found significant as this was an exploratory research. Discovering why these interactions were found significant, and if they hold up to different datasets, is left to future research. Finally, we did not fully investigate the what, how, and why of the malware characteristics studied in this paper which should be further investigated.

This study examined the different relationships between various smartphone malware characteristics, including threat type, infection channel, damage potential, and distribution potential. We discovered that threat subtype by date, damage potential by date, distribution potential by date, infection channel by date, damage potential by threat subtype, infection channel by threat subtype, threat type by damage potential, and infection channel by threat type were all significant interactions. This means that for both end-users and anti-virus companies, these are the interactions that should be examined to discover smartphone malware trends in order to improve better detection and avoiding download these malware in the first place. We have studied malware characteristics that do not require technical expertise, or to download the malware ourselves. This should inspire future studies to take a similar approach, that way research can be conducted more safely and quicker.

Acknowledgements

The authors would like to thank Dr. Raydell Tullous from The University of Texas at San Antonio for their help throughout this paper for the statistical analysis. Additionally, the authors would like to thank Emmanuel Ayaburi for his feedback throughout the paper's development

REFERENCES

Allix, K., Jerome, Q., Bissyande, T. F., Klein, J., State, R., and Traon, Y. L. 2014. "A Forensic Analysis of Android Malware -- How is Malware Written and How it Could Be Detected?," IEEE, July, pp. 384–393 (doi: 10.1109/COMPSAC.2014.61).

Arabo, A., and Pranggono, B. 2013. "Mobile Malware and Smart Device Security: Trends, Challenges and Solutions," IEEE, May, pp. 526–531 (doi: 10.1109/CSCS.2013.27).

Asundi, J., and Jayant, R. 2007. "Patch review processes in open source software development communities: A comparative case study," in *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, IEEE, p. 166c–166c (available at http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4076712).

Bal, G. 2014. "Explicitness of Consequence Information in Privacy Warnings: Experimentally Investigating the Effects on Perceived Risk, Trust, and Privacy Information Quality," (available at http://aisel.aisnet.org/icis2014/proceedings/ISSecurity/27/).

Beldona, S., Morrison, A. M., and O'Leary, J. 2005. "Online shopping motivations and pleasure travel products: a correspondence analysis," *Tourism Management* (26:4), pp. 561–570 (doi: 10.1016/j.tourman.2004.03.008).

Brookshire, R., Harris, M., Patten, K., and Regan, E. 2015. "Mobile Application Installation Influences: Have Mobile Device Users Become Desensitized to Excessive Permission Requests?," (available at http://aisel.aisnet.org/amcis2015/ISSecurity/GeneralPresentations/4/).

Faruki, P., Bharmal, A., Laxmi, V., Ganmoor, V., Gaur, M. S., Conti, M., and Rajarajan, M. 2015. "Android Security: A Survey of Issues, Malware Penetration, and Defenses," *IEEE Communications Surveys & Tutorials* (17:2), pp. 998–1022 (doi: 10.1109/COMST.2014.2386139).

Felt, A. P., Finifter, M., Chin, E., Hanna, S., and Wagner, D. 2011. "A survey of mobile malware in the wild," in *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*, ACM, pp. 3–14 (available at http://dl.acm.org/citation.cfm?id=2046618).

Giessmann, A., Stanoevska-Slabeva, K., and de Visser, B. 2012. "Mobile Enterprise Applications--Current State and Future Directions," IEEE, January, pp. 1363–1372 (doi: 10.1109/HICSS.2012.435).

Haas, P., Blohm, I., and Leimeister, J. M. 2014. "An empirical taxonomy of crowdfunding intermediaries," (available at http://aisel.aisnet.org/icis2014/proceedings/SocialMedia/13/).

Harris, M. A., Patten, K., and Regan, E. 2013. "The need for BYOD mobile device security awareness and training," (available at http://aisel.aisnet.org/amcis2013/ISSecurity/GeneralPresentations/14/).

Harris, M., Patten, K., Regan, E., and Fjermestad, J. 2012. "Mobile and Connected Device Security Considerations: A Dilemma for Small and Medium Enterprise Business Mobility?," (available at http://aisel.aisnet.org/amcis2012/proceedings/PerspectivesIS/15/).

Ho, Y. L., and Heng, S.-H. 2009. "Mobile and ubiquitous malware," in *Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia*, ACM, pp. 559–563 (available at http://dl.acm.org/citation.cfm?id=1821856).

IBM. 2015. "IPM SPSS Statistics 22 Documentation," *IPM SPSS Statistics 22 Documetnation*, Product Documentation, (available at http://www-01.ibm.com/support/docview.wss?uid=swg27038407; retrieved December 7, 2015).

Kari, T. 2015. "Explaining the Adoption and Habits of Playing Exergames: The Role of Physical Activity Background and Digital Gaming Frequency," (available at https://jyx.jyu.fi/dspace/handle/123456789/46675).

Karlsson, K.-J., and Glisson, W. B. 2014. "Android Anti-forensics: Modifying CyanogenMod," IEEE, January, pp. 4828–4837 (doi: 10.1109/HICSS.2014.593).

Kelly, G. 2014. "Report: 97% Of Mobile Malware Is On Android. This Is The Easy Way You Stay Safe," *Forbes* (available at http://www.forbes.com/sites/gordonkelly/2014/03/24/report-97-of-mobile-malware-is-on-android-this-is-the-easy-way-you-stay-safe/#889459b7d53d).

Linger, R., Sayre, K., Daly, T., and Pleszkoch, M. 2011. "Function extraction technology: computing the behavior of malware," in *System Sciences (HICSS), 2011 44th Hawaii International Conference on*, IEEE, pp. 1–9 (available at http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5718511).

McAfee. 2014. "Who's Watching You McAfee Mobile Security Report," (available at http://www.mcafee.com/us/resources/reports/rp-mobile-security-consumer-trends.pdf).

PRNewswire. 2012. "ESET 2013 Threat Trends Report," *ESET 2013 Threat Trends Report*, News Agency, , December 20 (available at http://www.prnewswire.com/news-releases/eset-2013-threat-trends-report-184304771.html; retrieved February 29, 2016).

Shaerpour, K., and Dehghantanha, A. 2013. "Trends in android malware detection," *Journal of Digital Forensics, Security and Law* (8:3), p. 21.

Smith, R. W., and Pridgen, A. 2012. "STAAF: Scaling Android Application Analysis with a Modular Framework," IEEE, January, pp. 5432–5440 (doi: 10.1109/HICSS.2012.543).

TrendMicro. 2016. "Malware - Threat Encylopedia," *Malware - Threat Encylopedia - Trend Micro USA*, Encylopedia, (available at http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/page/35; retrieved February 29, 2016).

Zhou, Y., and Jiang, X. 2012. "Dissecting Android Malware: Characterization and Evolution," IEEE, May, pp. 95–109 (doi: 10.1109/SP.2012.16).

Zhou, Y., Wang, Z., Zhou, W., and Jiang, X. 2012. "Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets.," in *NDSS* (available at http://www.csd.uoc.gr/~hy558/papers/mal_apps.pdf).