An Analysis of Mobile Malware Evolution

Author:

Tommy Tianyu Zhu

Tianyu.zhu@tufts.edu

An Analysis of Mobile Malware Evolution

Abstract

People used to think of malicious software - or more commonly known as malware - as mainly a threat to desktop or laptop computers. As the use of smartphones becomes increasingly integrated into daily lives, the amount of mobile malware attacks is also growing rapidly. Smartphones have become a common device for storing personal information and sensitive data, which made them perfect targets for malware. Although the largest mobile companies like Apple and Google have taken tremendous measures to protect their users, malware keeps evolving and continue to find new ways onto smartphone systems. This paper will discuss the evolution of mobile malware in recent years. We will investigate the history of mobile malware, survey the emergence of new attack philosophies and way of distribution, evaluate the current situation, and discuss the future of mobile malware.

Introduction

Nowadays, most smartphone users store private information such as messages, photos, emails, and even banking information on their mobile devices. While more and more people consider a smartphone as an essential part of their daily lives, they are often not aware of or not concerned enough with the potential security vulnerabilities of their devices. Smartphones grow "smarter" each year into sophisticated pocket computers that not only store huge amount of personal data, but also contain sensors such as GPS, camera, and fingerprint, which has made smartphones the perfect targets of information and identity theft and a great platform for spyware. As a result, malware that specifically targets mobile phones began to appear.

To the Community

This paper is aimed at everyday smartphone users. I wanted to focus on the evolution of mobile malware because this would help raise people's awareness on the importance of mobile security, and help people understand why we should also be on high alert when it comes to mobile malware. Smartphones keep getting more sophisticated, while mobile malware also continues to evolve, making themselves more powerful, harder to detect, and harder to get rid of. Even though companies like Google and Apple keep improving on their security measures, we as smartphone users should learn to be proactive in educating ourselves and help spreading cyber security awareness. As I will show in this paper, mobile malware has grown into a global phenomenon since its beginning in 2004, and will most likely to keep involving in the near future. In the age of smartphones, let us always be aware of the danger that awaits us.

The Beginning of Mobile Malware - 2004

The first ever mobile malware Cabir was discovered by researchers from Kaspersky Lab in 2004. It was designed to target Symbian OS, the most popular mobile operating system at the time, and spread via Bluetooth (Millard, 2004). Once a phone was infected by Cabir, the word "Caribe" would be displayed. Cabir would try to infect other devices if Bluetooth was enabled on the infected phone and prompting users to download it. In nature, Cabir was not malicious, but the concept of it was later expanded upon by other hackers to achieve more mischievous attacks.

A year later, a new malware called Commwarrior used the basic concept of Cabir and took it further. When a phone was infected, Commwarrior would constantly send out text messages to everyone in the address book. Back in 2005, each text messages cost money, so the victim would be left with an ugly phone bill. On the receiving end of these messages, if the message was opened by an unsuspecting user, then the malware would install itself on this new phone. Commwarrior didn't generate money for its creator in any way, but it was the first mobile malware that had a financial impact on its victims (Wueest, 2014). Then in 2006, RedBrowser extended Commwarrior's functionalities and would run on Java 2 Micro Edition as the first trojan that could infect multiple mobile platforms. It would send messages with actions, such as claiming to be a Wireless Application Protocol browser but was, in fact, sending text messages to premium-rate numbers abroad, resulting in financial losses for the victim (A History of Mobile Malware from Cabir to SMS Thief, 2016).

The Emergence of Spyware and iPhone Malware - 2007

As the smartphone industry moved on to 'smarter smartphones', the malware capabilities kept pace. Within a few years, mobile devices began to deal with malware that is similar to the

established malware found on desktop computers, and the rise of spyware also caught up to mobile phones.

Spyware is a type of malware that enables the attacker to secretly obtain private information from the victim's device. FlexiSpy was one of the earliest forms of mobile spyware introduced in 2007 and was very successful at extracting data like text messages, phonebook, and recordings from compromised mobile devices. It was also commercialized, advertising itself as the perfect solution for people to spy on their spouses (Wueest, 2014).

2007 was also the year when the 1st gen iPhone was released, and hackers caught up quickly. In 2009, an iOS worm IKee was created to target jailbroken Apple devices that had OpenSSH. IKee was not a complicated malware, it only affected people who hadn't bothered to change the default password – "alpine". This once again proves how ignorant people could be when it comes to protecting their devices, as a simple password change could have saved them from IKee. However, IKee did not cause any serious damage. In fact, it was more hilarious than malicious, as it simply changed the infected iPhone's wallpaper to either a photo of the malware author or the singer Rick Astley who sang "Never Gonna Give You Up" (A History of Mobile Malware from Cabir to SMS Thief, 2016). While IKee was relatively harmless, it reminded people that iPhone security was just as important as Android malware protection.

Money, Money, Money - 2010

In 2010, mobile hackers started to form organizations across the globe and focused on generating money together. From then on, a lot of them could make a living by exploiting vulnerabilities on phones, as reports indicate some present-day mobile hackers make about 7500 dollars a month (Szoldra, 2016).

Zitmo was an example of mobile malware that generated tremendous income for its creators. Zitmo is short for Zeus-in-the-mobile, as it originated from its desktop counterpart Zeus. Zitmo was a trojan that could migrate from PC to mobile device and back again. It targeted internet banking to steal transaction authorization numbers and caused massive losses to those who preferred to do online banking. Zitmo was so successful that mobile malware targeting online banking services began to appear on all major mobile platforms including Android, Blackberry, Windows Mobile, and Symbian (Wueest, 2014).

Rise of Android Malware – 2011

As the Android platform continued to dominate the mobile marketplace and became the biggest mobile phone platform in 2011, hackers began to take notice (Wueest, 2014). Attackers often disguise their malware as a useful app to make them more palatable for potential victims to download.

In 2011, the Trojan DroidDream plagued the Google Play Store. It infected more than 50 apps, each with tens of thousands of downloads. This malware sent sensitive user information from infected devices to remote servers and silently installed other apps (Ramos, 2011). To minimize the damages, Google soon removed the infected apps from Google Play Store.

Another Trojan called Boxer was created in 2012 to attack Android devices. Its behavior was similar to Commwarrior, which sent premium-rate text messages from infected phones. Boxer was discovered in 63 countries, where it took advantage of mobile country codes and mobile network codes from infected phones. It was distributed via text messages and once users who received the messages downloaded the app with the provided link, it would automatically

download a modified version of a legitimate application that would send messages to premium numbers.

A year later, the first ransomware designed to target Android surfaced. The malware, called FakeDefender, would display bogus security alerts and prompted users to buy a security app that did not exist under the false promise to eliminate a non-existent malware (A History of Mobile Malware from Cabir to SMS Thief, 2016). Once the user agreed to install it, it would display a picture of an animal peering out of the letters “OZ” with a subhead of “Android Defender”.

Escalating Situation – 2014 and Beyond

After 2014, Mobile malware attacks continued to escalate, and are expected to increase even further in years to come. According to the 2016 report by Nokia Threat Intelligence, mobile malware attacks on smartphones rose by 95 percent from January to April 2016 alone (Nokia Security Center Berlin, 2016).

Modern day mobile malware has also become more sophisticated. A good example of this is SMS Thief that appeared in 2016, a malware that disguised itself as an uninstaller utility but would actually steal stored text messages. It ran silently in the background while it quietly intercepted, copied, and forwarded all messages from the infected phone. The concept of SMS Thief is nothing new, but it is very tricky to uninstall and is largely hidden from the user (A History of Mobile Malware from Cabir to SMS Thief, 2016).

Malware has also become more aggressive in making financial threats, gained increasing stealth, and incorporated new attack methods. Also in 2016, researchers discovered 22 Android apps that belonged to a new Trojan type called “Xbot”. Xbot is a ransomware that was regularly

updated and capable of multiple malicious behaviors (Zheng, Xiao, & Xu, 2016). First, it would try to steal banking credentials and credit card info from the infected phones via phishing pages specifically created to look like Google Play's payment interface and the login pages of multiple bank apps. Secondly, it could also steal SMS messages and contact information, and parse mobile transaction authentication messages from banks. Most importantly, it could remotely lock infected Android devices and encrypt user's files displaying a page that is unable to be closed, asking for a 100-dollar PayPal cash card as ransom. So far, Xbot doesn't seem to be widespread, but the author of this malware appears to be constantly updating it and making this Trojan more complex and harder to detect (Zheng, Xiao, & Xu, 2016).

The distribution of mobile malware has also evolved. Typically, mobile malware relies on tricking victims into downloading a malicious app from an app marketplace. However, increased security screening has made it difficult for attackers to put their malware onto the marketplace. As a result, hackers began to use desktop computers as a jump pad onto Android devices. A recent malware called Droidpak first appeared on Windows PC, but it would eventually download a malicious Android application package file on to the infected PC. If any Android device is connected to the compromised computer, then Droidpak would try to install the Android malware called Fakebank on the Android device. Once installed, Fakebank would try to convince users to install malicious versions of bank apps (O'Brien, 2014).

Defenses

With a few simple rules, you could protect your mobile devices against common mobile malware:

1. Install a security app. There are many great security apps out there, both on Android and iOS. Find a trustworthy developer, and regularly scan your phone for potential security vulnerabilities or malware.
2. Do not download apps from untrusted developers or marketplace! If you receive a link that let you download an app outside of Apple's App Store or the Google Play Store, don't click on it. Even though Google Play Store is not 100% safe from malicious apps, it is still safer to download apps from official channels.
3. Keep your mobile OS up to date. Developers would usually fix some security vulnerabilities when they roll out a new OS version, or release a quick fix when a security issue is discovered.

Conclusion

As smartphones integrate into our daily lives, they also introduce many security concerns. One of the main goals of this paper is to help reduce the lack of knowledge about mobile malware because it is crucial for smartphone users to understand how vulnerable their mobile devices can be. While mobile phones become more advanced, they have also brought along more sophisticated malware. The fight between malware creators and mobile security measures will never stop, and the landscape of mobile security is unpredictable as it is evolving at an unprecedented rate. As a result, it is essential for people to educate themselves about mobile device security and learn the simple ways to reduce the possibility of becoming a victim of mobile malware. As mobile malware continues to be on the rise, the best way to defend against them is through raising the awareness of smartphone security, and we all have a responsibility to spread the word.

References

A History of Mobile Malware from Cabir to SMS Thief. (2016, November 1). Retrieved from We Live Security: https://www.welivesecurity.com/2016/11/01/history-mobile-malware-cabir-sms-thief/

Millard, E. (2004, June 16). *Cabir: World's First Wireless Worm*. Retrieved from Tech News World: https://www.technewsworld.com/story/34542.html

Nokia Security Center Berlin. (2016). *Nokia Threat Intelligence Report.* Berlin: Nokia Threat Intelligence Laboratories. Retrieved from https://resources.ext.nokia.com/asset/200492

O'Brien, L. (2014, February 23). *The Future of Mobile Malware*. Retrieved from Symantec: https://www.symantec.com/connect/blogs/future-mobile-malware

Ramos, P. (2011, March 9). *Google vs. DroidDream*. Retrieved from We Live Security: https://www.welivesecurity.com/la-es/2011/03/09/google-vs-droiddream/

Sager, I. (2012, June 29). *Before IPhone and Android Came Simon, the First Smartphone*. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2012-06-29/before-iphone-and-android-came-simon-the-first-smartphone

Szoldra, P. (2016, June 2). *Flashpoint Report Ransomware*. Retrieved from Tech Insider: http://www.businessinsider.com/flashpoint-report-ransomware-2016-6

Wueest, C. (2014, February 25). *The Tenth Anniversary of Mobile Malware*. Retrieved from Symantec: https://www.symantec.com/connect/blogs/tenth-anniversary-mobile-malware

Zheng, C., Xiao, C., & Xu, Z. (2016, February 18). *New Android Trojan "Xbot" Phishes Credit Cards and Bank Accounts, Encrypts Devices for Ransom*. Retrieved from Palo Alto Networks: https://researchcenter.paloaltonetworks.com/2016/02/new-android-trojan-xbot-phishes-credit-cards-and-bank-accounts-encrypts-devices-for-ransom/

Evolution of Android Malware: Analysis and Detection Techniques 76:5. just as the sophisticated Cabir worm targeted Symbian when it was the most popular. in 2004, the Trojan Obad, considered one of the most sophisticated mobile Trojans. today, was discovered in 2013 and targets Android [Unuchek 2013]. In general, nearly. half of all mobile malware as of 2014 are Trojans and are being tailored to target. speciï¬c demographics. Together, Russia, India, and Vietnam account for over 50%. Sophisticated mobile malware, particularly Android malware, acquire or utilize such data without user consent. It is therefore essential to devise effective techniques to analyze and detect these threats. This article presents a comprehensive survey on leading Android malware analysis and detection techniques, and their effectiveness against evolving malware. Thisâ€¦ CONTINUE READING. In 2005, Shevchenko [6] presented evolution of mobile malware which is considered to be first comprehensive study. In 2011, Becher et al. [7] continued the evolution from 2005 and explained about specifics of mobile security. The aforementioned study focused on different security classes, however, in this paper we focus primarily on software centric attacks. In 2011, Felt et al.Â 4.1 History of Mobile Malware. The first malicious software aimed at smartphones hit in 2004. The first virus for mobile phones was written by a group known as 29A in June 2004. An article written by Shevchenko [6], gives a detailed overview of mobile malware history.Â Analysis of code or application without executing the program is called Static Analysis. It is a fast and simple approach. Chandramohan et al. Evolution of Android Malware: Analysis and Detection Techniques. 00:3. 2. BACKGROUND. Prior to discussing current approaches to analyze Android malware, this article begins with this background section on the evolution of mobile malware. This concludes with a more in-depth sec-tion on the Android operating system (OS), which is the focus of this article. 2.1. Evolution of Mobile Malware. Initially, when computing systems were primarily understood by a few experts, malware develop-ment was a test of oneâ€™s technical skill and knowledge. For example, the PC Internet worm known as Creeper displaye 2009. Mobile malware evolution: An overview. Retrieved from http://www.viruslist.com/en/analysis?pubid=204792080.Google Scholar. Michael Grace, Yajin Zhou, Qiang Zhang, Shihong Zou, and Xuxian Jiang.Â 2013. Analysis of Android malware detection performance using machine learning classifiers. In Cybercrime and Trustworthy Computing (CTC). Google Scholar.