MOBILE MALWARE

This report details the current status of Malware for mobile devices, their security risks, the possible future evolution of Mobile Malware and Future Mitigation Options.

INTRODUCTION

With the penetration of Smartphones now reaching record highs in the UK, at just under 50% owning a Smartphone [(1)]; it comes to no surprise that the risk of malware on mobile devices is also increasing. With the introduction of the iPad and other tablet computers which are built upon the same firmware as Smartphones; malware can be easily written to infect both devices, giving further support for malicious code writers to focus their sights on mobile devices.

CURRENT EXAMPLES OF MOBILE MALWARE

Below are examples of real threats to user equipment on various platforms which exist today. The vast majority of malware discovered works on the android platform as it is possible to install unchecked 3rd party applications, unlike the Apple IOS platform. However it is still possible to install unregistered apps from outside the Apple App store by “jail breaking” the iPhone.

ANDRIOD TROJAN (JIMM ICQ TROJAN CLIENT) is a piece of malware which is distributed by QR codes. A QR code is an image similar to a barcode which is captured by a Smartphone’s camera. It can be used to provide a link to a WebPage in printed publications. To infect their phone the user scans the QR code which directs them to a webpage that downloads a trojanised version of the JIMM ICQ client. This software when installed sends various SMS message to a premium number costing roughly £4 per message. It is possible for the attackers to hijack QR codes found in public places and replace them with their corrupted versions to infect the victim’s phone.

ANDRIOD TROJAN (GOOGLE+ IMITATION APP) creators rely on the fact that users will not pay particular attention to the software they are downloading. They have labelled their software Google++ in the hope to hoodwink their victims. Once installed it captures instant messages, call logs, location, GPS information and other sensitive data.

WALKINWAT TROJAN is a corrupted version of the Walk and Text app which uses the Smartphones’ camera to display the world to the user while they send SMS messages, allowing them to walk and text at the same time. This Trojan identifies itself as a pirated version of the popular walk and text app available for free download.

Once installed the software extracts IMEI information and other sensitive data and uploads it to a central server for retrieval by the attackers. While uploading the information it sends an SMS message to each of the victim's contacts saying:

"Hey, just downloaded a pirated App off the Internet, Walk and Text for Android. Im stupid and cheap, it costed only 1 buck. Don't steal like I did!"

Symantec have claimed that this is first corrupted app discovered which actively scolds the victim for software piracy.

IKEE, IPHONE WORM was the first computer worm discovered for the iPhone during 2009. It only affected users who had "jailbroken" their iPhone; this is when the user gains root access to their phone to install custom firmware to allow for applications not available through the Apple App Store. Through this process of jail breaking, the default installation installs a SSH service with a default username and password. This vulnerability was then exploited by iKee to infiltrate the phone and gain access. This attack vector was then witnessed again by Security Company F-Secure in which another piece of Malware compromised banking transactions on corrupted iPhones.

THE FUTURE OF MALWARE

The future of malware in mobile devices is evolving at an exponential rate. Many researchers are now trying to fully understand the capabilities of malware on a mobile device; as tablet computers become more popular the malware threat will increase.

REGISTER KEYSTROKES OF A KEYBOARD THROUGH A PHONE. Patrick Traynor from Georgia Technology University demonstrated at a conference in Chicago that by using an iPhone's accelerometer they were capable of capturing the keystrokes of a user on a computer to an accuracy of 80%. Patrick outlined that the malware could work by allowing the user to download a seemingly innocent app which will then sense when the phone is placed upon a hard surface near a keyboard. It will then start to listen for keystrokes and send the information to a central server. (2)

IOS APP SECURITY FLAW

This was a flaw studied by Charlie Miller where he was able to bypass Apple's security checks and allow an App listed in their App Store to download a payload and run on the phone. The current security procedure in place at Apple is that all apps are verified before they are available on the App Store. However at the time of the vulnerability, they did not have sufficient measures in place to confirm if the app would try to execute a payload. As Charlie Miller shows in his video, the payload vulnerability allows an attacker to gain near full control of the victim's phone. This includes the ability to download the user's address book, download any file which currently resides on the phone and send SMS messages. At the time of writing there is no patch for this. (3)

ACTIVE RECORDING OF PHONE CONVERSATIONS

Researchers at Total Defence Security have discovered a piece of malware for the

Android Platform which will actively record a user's phone conversation and upload the file to a central server for retrieval. It stores the recording of the telephone conversation in the AMR format and then stores it on the user's MicroSD card before uploading. [4]

WINDOWS 7 PHONE

Currently there are no known security vulnerabilities of the Windows 7 phone operating system. The operating system is fairly new to the Smartphone market so the hackers have had a limited amount of time to find the vulnerabilities.

The operating system has strong security preventions in place if a piece of malware were to be installed. All applications that are run on the phone must be developed in Microsoft's Silverlight development platform. Each application cannot access the system files of the phone, so it is "sandboxed" from the rest of the phone. The inherent security of Silverlight is also present in the phone, the customer sensitive data must be accessed through a series of APIs which launch and collect the data required. This provides a level of security as applications cannot have direct access to the data. [5]

SECURITY PRACTICES TO MITIGATE MALWARE

With the given rise of malware, the rate of Smartphone anti-virus software has also increased. There are two options available to a user who wishes to mitigate the threat of malware. They can choose to implement a local application which will periodically scan their phone for any signs of malicious application behaviour; or they could implement a cloud security based system. The local application approach is already available from various vendors including Kaspersky and F-Secure. These products can be configured to actively scan any file which is downloaded onto the handset providing a level of security to the user.

The second approach is the cloud security based systems such as the recent partnership between Allot and AdaptiveMobile [6]. This system, which is currently unavailable, will work on the service provider level as a chargeable opt-in feature. From here the service provider can stop the malware from even reaching the user's handset providing a higher level of protection.

CONCLUSION

With higher usage of Smartphones, the pool of victims for Malware creators is increasing at an exponential rate. Today's Smartphone is also fast becoming a honey pot of personal information; with many users now using their phones for bank transactions, calendar appointments as well as storing detailed contact information of their associates.

This makes any of the malware presented in this report of high risk to users and their data. Any of these malicious programs could cause high levels of damage to the users should their data fall into the hands of the wrong people. It is clear that the average Smartphone user should take greater care about the level of information they hold on their phones, which applications they allow to install and the level of permissions it holds upon the phone. Perhaps, some might even consider mitigating some risks through the use of security software.

BIBLIOGRAPHY

1. Arthur, Charles. Half of UK Population own a Smartphone. The Guardian. [Online] 31 October 2011. [Cited: 14 11 2011.] http://www.guardian.co.uk/technology/2011/oct/31/half-uk-population-owns-smartphone.
2. PhysOrg. Turning iPhone into spiPhone: Smartphones' accelerometer can track strokes on nearby keyboards. PhysOrg. [Online] 18 Oct 2011. [Cited: 5 December 2011.] http://www.physorg.com/news/2011-10-iphone-spiphone-smartphones-accelerometer-track.html.
3. Greenberg, Andy. iPhone Security Bug Lets Innocent-Looking Apps Go Bad. Forbes. [Online] 7 Nov 2011. [Cited: 5 Dec 2011.] http://www.forbes.com/sites/andygreenberg/2011/11/07/iphone-security-bug-lets-innocent-looking-apps-go-bad/.
4. Venkatesan, Dinesh. A Trojan spying on your conversations. Total Defense Blog. [Online] 1 Aug 2011. [Cited: 5 Dec 2011.] http://www.totaldefense.com/securityblog/2011/08/26/A-Trojan-spying-on-your-conversations.aspx.
5. Shinder, Deb. Windows Phone 7 Security Implications. Windows Security. [Online] 12 Jan 2011. [Cited: 5 Dec 2011.] http://www.windowsecurity.com/articles/Windows-Phone-7-Security-Implications.html.
6. Allot. Allot and AdaptiveMobile Partner to Enable Carriers to Deliver Personalized Cloud Security . Allot Press Releases. [Online] 4 Oct 2011. [Cited: 5 Dec 2011.] http://www.allot.com/index.aspx?id=3797&itemID=70861.