A Mobile Threat Landscape in Cyber Forensics

Narayan Bhosale[1], S.G. Gupta[2,] Ramesh Manza[3]

[1] Assistant Professor, Govt. Institute of Forensic Science, Aurangabad-01.

[2] Director, Govt. Institute of Forensic Science, Aurangabad-01.

[3] Assistant Processor, Dept of Computer Science and IT, Dr.B.A.M.U., Aurangabad-01.

narayanbhosale@gmail.com,gifsa2009@gmail.com,manzaramesh@gmail.com

Abstract

This paper addresses the various threats among the recent mobile operating system which will always cause risk in cyber forensic view. The security could compromises with backdoors, vulnerabilities, malicious (malware), Botnet, threats can effect on Mobile device at wide. So, the mobile will become victim tool via hackers. Computer system, mobile would be compromised through back door entities means risk at security linkage become more common in cyber worlds but our deepth study on issues which addresses various aspect of Mobile and Computer threats. Therefore, in this paper we are discussing that all threats and providing precaution major list as rescue point view.

Keywords- *Threat, Malware, Mobile Forensic, Cyber Crime and Malnet.*

Introduction

From large enterprises and government agencies to small businesses and consumers, the use of smartphones and other mobile devices to manage professional and personal interactions is now ubiquitous. Mobile devices have become the new personal computer, storing as much data as a PC but providing greater flexibility and portability. Online banking, commerce, and other business applications put daily business and financial transactions at users' fingertips. And, at every turn, users are implored to download productivity and entertainment applications to further increase the value of their mobile devices.

While smart phones and tablet devices now perform the same functions as a PC, one critical feature is missing—security. Whereas most PCs come equipped with antivirus and other endpoint security software, the vast majority of mobile devices are devoid of any security protection, leaving both the data and applications on these mobile devices at risk of exploitation or misuse.

A mobile malware and exploitation techniques have reached the complexity and capabilities of their counterparts in wired networks. Malware developers are capable of researching, uncovering, and leveraging weaknesses in mobile platform security models, as well as inherent weaknesses in app stores and open ecosystems.

A lack of oversight, coupled with an exploding number of new consumers who lack security awareness or are disinterested in the mundane aspects of mobile security with access to a plethora of new apps for their mobile devices, is creating a recipe ripe for a catastrophic malware disaster. As mobile device usage increases, the absence of installed mobile security products is playing an enabling role in the vulnerability of mobile devices and the exploitation of Sensitive data and personal identifying information (PII).

Literature Review

According to Juniper Networks report, [2012], The threats to mobile devices are real and reach far beyond simple viruses to include malware, loss and theft, data communication interception, exploitation and misconduct, and direct attacks[1].

"In the Symantec survey,80% of responders said that they did not expect a cybercriminal to get caught"[2].

Researchers at the University of California, Los Angeles (UCLA) [31 July 2013], IBM Research, and the University of Texas at Austin have developed a system to encrypt software so that it only allows someone to use a program as intended while preventing any deciphering of the code behind it. "The real challenge and the great mystery in the field was: can you actually take a piece of software and encrypt it but still have it be runnable, executable, and fully functional," says UCLA professor Amit Sahai. He says the system makes it impossible for a cybercriminal to reverse-engineer the software without solving mathematical problems that take hundreds of years to work out on today's computers. The researchers say their mathematical obfuscation method can be used to protect intellectual property by preventing the theft of new algorithms and by hiding the vulnerability that a software patch is designed to repair when the patch is distributed. Through this mechanism, attempts to determine why and how the software works will be stopped by a nonsensical jumble of numbers. Sahai notes that their method for software obfuscation has lead to the development of functional encryption, which offers a much more secure way to protect information. "Through functional encryption, you only get the specific answer, you don't learn anything else," [3].

Malwares

Definition-short for malicious software used or programmed by attackers to disrupt computer operation, gather sensitive information, gain access on private computer.

Threat: A possible danger that might exploit vulnerability.

Malnet (malware networks) are distributed infrastructures within the internet that are built, managed and maintained by cybercriminals for the purpose of launching ongoing attacks against users over extended period of time.

Fig-1- Leading Mobile threats

Botnet

Botnets are often the focal point for collecting the confidential information, launching Denial of Service attacks and distributing SPAM. A ***bot,*** short for *ro**bot***, is an automated software program that can execute certain commands. A ***botnet,*** short for *ro**bot** **net**work,* is an aggregation of computers compromised by bots that are connected to a central "controller." Botnet controllers are often controlled from chat rooms and can be linked together to form even larger botnets. Botnets controlling tens of thousands of compromised hosts are common.

Key Mobile Malware Findings

Mobile device and OS marketshare and mobile malware infection rates are linked

- Mobile malware uses the same techniques as PC malware to infect mobile devices.
- The greatest mobile malware risk comes from rapid proliferation of applications from app stores.
- RIM BlackBerry, Google Android, and Apple iOS operating systems suffer predominantly from spyware applications

Threats

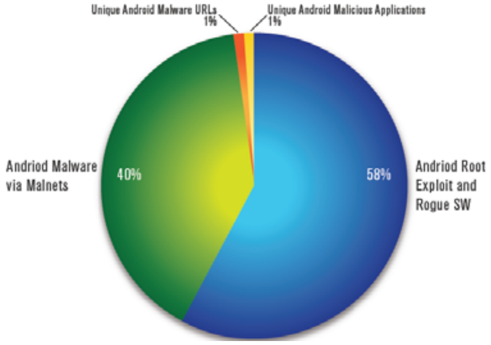

Fig-2- Android Malware Blocked by WebPulse in 2012

The growth in requests to malnets from mobile devices was driven by eight unique malnets in 2012. Three of the malnets, Narid, Devox and Criban, targeted mobile devices exclusively while the others simply expanded their malicious activities to include mobile devices. Narid and Devox are no longer active malnets. Criban continues to show a low level of activity with 83 new hosts over the past year. The maximum number of hosts used in a given day was 3.

Fig-3- Leading Malnets Exclusively Targeting Mobile Devices

Other Mobility Issues:

App Use and Privacy

App use has become the cornerstone for smartphone ownership. A Nielsen study showed that the number of apps U.S. smartphone users install increased from 32 in 2011 to 41 in 2012.25 Research from Flurry revealed that the average amount of time spent on apps grew 35% in 2012[17-18].But while apps continue to rise in popularity, users may not be aware that they can put personal data at risk [19]. Apps like "Angry Birds" and "Angry Birds Space" can access data like a phone's IMEI number and a user's location.

Potential risk Findings

Cybercrime organizations spent 2012 tuning malnets to require low investment and deliver high impact results. This same strategy is now being extended to mobile devices for further financial gain. This is a significant shift that will rapidly increase attacks on mobile devices [1].

Fascination with the technical side of cybercrime can blind users to the classic weaknesses that are being exploited [2].

Yet, the information security community needs to get a grip on this issue because crime that utilities Internet connectivity is increasing, not decreasing. Social networking sites are rich hunting grounds for scammers and those wanting to harvest credit card details. All it takes is a convincing free offer and many will willingly divulge their personal data. If they succumb in a moment of weakness, they are unlikely to tell the story to those around them and so build up the community understanding of the hazard. This kind of awareness needs to be built into the security culture otherwise what can result is a weakness of the organization as well as the individual [3-5].

Android seems to be repeating history by way of Windows. The platform's growing dominance in the mobile landscape echoes that of Windows in the desktop and laptop space [6]. And much like Windows, Android's popularity is making it a prime target for cybercriminals and attackers, albeit at a much faster pace.

In 2012, we detected 350,000 malicious and high-risk Android app samples, showing a significant increase from the 1,000 samples seen in 2011. It took less than three years for malicious and high-risk Android apps to reach this number—a feat that took Windows malware 14 years [7].

Just as Windows malware varied, so did Android malware—around 605 new malicious families were detected in 2012. Premium service abusers, which charge users for sending text messages to a premium-rate number, comprised the top mobile threat type, with transactions typically costing users US$9.99 a month [8]. And victims of mobile threats didn't just lose money, they also lost their privacy. The issue of data leakage continued to grow as more ad networks accessed and gathered personal information via aggressive adware.

Aggressive adware in mobile devices are now similar to the notorious spyware, adware, and click-fraud malware rampant in the early days of the PC malware era. They, like PC malware, generate profit by selling user data. PC malware took advantage of loopholes in legitimate ads and affiliate networks; while today's aggressive adware can cause data leakages that aren't always limited to malicious apps. Even popular and legitimate apps can disclose data [9].

Protecting Your Mobile Devices:

With the constant changes in the mobile threat landscape, smartphone owners should secure their devices. Here are some steps to protect devices against mobile threats:

1. **Use your device's built-in security features.** Opt for phones that have security features and use them. Built-in security features like password, pattern, or PIN lock options prevent outsiders from accessing your data should your phone get misplaced or stolen.
2. **Do research on apps before downloading them even from trusted sources.** Cybercriminals often disguise malware by spoofing popular apps. Familiarize yourself with details of popular apps (e.g., the name of the developer) to ensure that you download the legitimate version. It is advisable to download from reputable app stores like Google Play than third-party ones.
3. **Read permissions before installing apps.** Malicious apps usually seek access to various kinds of data stored in a mobile device. Read permissions to check what type of actions an app will perform once installed. Be wary of apps that require more permissions than necessary (e.g., a calendar app that seeks access to your call logs).
4. **Regularly check for software updates.** Software updates are usually released to address issues like vulnerabilities or improve software performance.
5. **Invest in a security app.** Security apps can inform you if an app has malicious or suspicious behaviors. Some apps even protect data with features like remote wipe or privacy scanner.
6. **Set BYOD** [Bring your Own Devices] **policies at work.** Organizations should decide which employees will only be allowed to bring devices and what types of devices they will support. Set up procedures to take if a device is stolen, lost, or damaged.

Mobile users represent a complex and growing constituency for organizations today. Those that can securely manage mobile devices can gain a competitive advantage by enabling their employees to be more productive. As businesses increasingly open their networks to mobile devices, cybercriminals will be knocking at the door.

As we have seen in this report, they are already arming themselves for an attack.

Extending an enterprise-class web security solution to include mobile devices is a good first step towards protecting your employees. By closing the mobile security gap and enabling access to corporate assets with appropriate policy controls, businesses can proactively protect themselves against this evolving mobile threat landscape while capitalizing on the innovation and productivity of a mobile workforce.

Conclusion

This technical review which spread awareness among the peoples how threat and Malware can make harm in our device. So need be built into the security essential tool with updating and upgradation, otherwise it causes a weakness of the organization as well as the individual. The rate of risk would be increased therefore keep your mobiles operating system upgrade.

References

[1] "Malicious Mobile Threats Report 2010/2011", *Juniper Networks*, Inc. 2012.

[2] Wendy Goucher, Idrach, "Being a cybercrime victim", *Computer Fraud & Security*, October 2010.

[3] Computer Scientists Develop, "Mathematical Jigsaw Puzzles" Encrypt Software UCLA Newsroom (CA) Matthew Chin, 29 July, 2013.

[4]Symantec "Norton Cybercrime Report:The Human Impact",September 2010. http://www.norton.com/cybercrimereport.

[5] Alexander, Harriet, "British victim of 'romance fraud" tells of ordeal'.The Daily Telegraph, 2 May2010.http://www.telegraph.co.uk/news/worldnews/africaandindianocean/ghana/7664240/British-victim-ofrom ance- fraud-tells-of-ordeal.html

[6]http://www.businesswire.com/news/home/20121101006891/en/Android-Marks-Fourth-Anniversary-Launch- 75.0-Market

[7] http://www.av-test.org

[8]http://news.cnet.com/8301-27080_3-20048132-245.html

[9] http://blog.trendmicro.com/trendlabs-security-intelligence/do-you-know-what-data-your-mobile-app-discloses/

[10]http://about-threats.trendmicro.com/us/mobilehub/mobilereview/rpt_mothly_mobile_review_201209_the_growing_problem_of_mobile_adware.pdf

[11] http://blog.trendmicro.com/trendlabs-security-intelligence/malicious-developers-released-rogue-bad-piggies-versions/

[12] http://blog.trendmicro.com/trendlabs-security-intelligence/rogue-instagram-and-angry-birds-space-for-android-spotted/

[13]http://blog.trendmicro.com/trendlabs-security-intelligence/1730-malicious-apps-still-available-on-popular-android-app-providers/

[14] http://blog.trendmicro.com/trendlabs-security-intelligence/rogue-instagram-and-angry-birds-space-for-android-spotted/

[15]http://blog.trendmicro.com/trendlabs-security-intelligence/malicious-developers-released-rogue-bad-piggies-versions/

[16]http://blog.trendmicro.com/trendlabs-security-intelligence/android-malware-family-downloads-paid-media-and-apps/

[17] http://blog.nielsen.com/nielsenwire/?p=31891

[18] http://blog.flurry.com/bid/92105/Mobile-Apps-We-Interrupt-This-Broadcast

[19] http://blog.trendmicro.com/trendlabs-security-intelligence/do-you-know-what-data-your-mobile-app-discloses/