Original Article

Analysis of Prediction and Detection of Spyware for User Applications.

Mahesh V
Bachelor of Computer Applications
Jain University, Bangalor-560067, India
v.mahesh@jainuniversity.ac.in

Dr. Sumatra Devi K.A
GSSS Institute of Engineering & Technology for Women
Mysore-570 016, India
sumithraka@gmail.com

ABSTRACT

Nowadays web applications are essential part of our daily life. Vulnerabilities of web applications have become more in the recent years as a major threat to computer systems data security. Meanwhile, the attacks using web application weaknesses and the damage caused by them are increasing day by day. Spyware is such type of threat which steals the user data without the user awareness or acknowledgement. This paper talks about different methods available in preventing fundamental and advanced types of personal information leakage through internet spyware with the idea of “Do not send the individual data to a dangerous recipient”.

Keywords: Spyware, Antispyware Limitations.

I. INTRODUCTION

The word “spyware” was first experienced by the news group of the Microsoft in 1995 for the first time. Main body of the spyware involves two parts. First part is what presents the appearance of the spyware that is different from such program’s main idea and is visible by the user. Second part is responsible for collecting, monitoring and transforming user’s data to the constructor of spyware. This part is implemented in the background. Based on the developers purpose, these software perform different operations, they are also deployed via different methods. Most of the spywares are implemented for marketing and financial purposes [7].

Nowadays hackers would have embedded their spywares in the freely available software’s in the app store. In this way they will install these software’s on the user’s PCs using hack methods which include methods for collecting personal information, monitoring user operations, spoofing files on the hard disk, installing hidden programs and putting them in the startup menu, measuring system resources to exploit in transforming data, capturing snapshots of screen and recording voice by use of user’s microphone [12].

The leaked personal information may violate the person’s privacy. Some data such as user ids and passwords can be used in impersonation. Contact information like as e-mail address and telephone number can causes many spam mail or spam phone call. Credit card numbers, pin code or bank account number may be used in a crime. The spyware, software that is installed secretly in a user’s personal computer steals the personal information stored in the PC or captures user’s keyboard input. The spyware sends the information to the malicious person who installed the same and the eavesdropping of a network line between user PC and application server is another way of the leakage [1].

The most important major threats for information stored on a smartphone is Applications that the user installs. While many users are heavily used to extend the uses of the phone capability and make it more usable or efficient, while many other applications may be malicious and only interested in stealing information [9].

Symantec's Website Vulnerability Assessment Services found that 77% of sites which are existing at present contained vulnerabilities and among them 16% were classified as risky vulnerabilities that may allow attackers to access sensitive information and may alter the website content, or compromise visitor system said by Internet Security Threat Report 2014[8].

II. LITERATURE SURVEY

Due to the increase in the number of Internet users initially spyware was not considered explicitly illegal, which made difficult to removal of malware and resulted in the formation of a legal grey zone as brand. A commonly used technique for identifying malware was to blacklist those applications through the use of signatures, and the idea of dividing between legitimate and malicious software. However, this idea requires a copy of the same malware to be taken on the Internet activity to create a unique signature database and then being distributed to all customers of the anti-virus tool developers. The main drawback of this technique is the fact that the anti-virus tools were one step lagging behind the creators of malwares [2].

There are different security threats that are affecting the mobile devices. Mobile threats are divided into various categories like Application-based threats, Web-based threats, Network-based threats and Physical threats [7]. Trust assessment of Apps is necessary and important since smartphones are becoming the new information hubs for public and companies but the security of their devices are generally lacking (rooting is common, malware and spyware widely distributed) such that, one can say that there is no assurance that user information is safe. In addition, even App stores (Google Play, Apple App store) often contain unsafe Apps [9]. To provide secure application, it is very difficult to wait until attack take place. Hence, it is healthier to keep on avoiding attack patterns with help of data validations and input sanitization is only the best solution to introduce secure web applications [10].

Once the attacker influences a victim to click on a URL that contains of malicious HTML/JavaScript code, then the user browser will then display the HTML and execute JavaScript, this event can results in robbery of that particular browser cookies and other sensitive information related to the user activity. SQL Injection vulnerability on the other side, results from the user uses the applications input in constructing database statements. The important observation is that all these vulnerabilities are caused by incorrect string manipulations. Programs that transmit and use malicious user inputs without sanitization or with improper sanitization are vulnerable to these well-known above stated attacks [11]. Massachusetts Institute of Technology (MIT) of researchers, Harvard, and Carnegie-Mellon universities suggested that apps on Apple and Android smartphones leak lots of user's information to third parties, they found that 73% of the android applications shared user's email addresses and 47% of the iOS apps shared location data. The study named as who knows about me? A Survey conducted to find behind the scenes personal Data Sharing to Third Parties by Mobile Apps by testing 55 of the most popular android apps and the same number of iOS apps. The researchers recorded the HTTP and HTTPS traffic that takes place while using the different apps and looked for transmissions that consists of personally identifiable information, behavioral data such as search patterns and location data.

They also found that android apps were likely to share more personal information such as user name (49% of the apps) and address (25%) than the iOS apps, where 18% shared names and 16% shared email addresses [12].

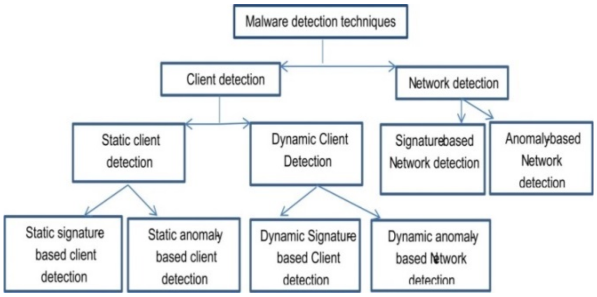

Malware detection techniques
Client detection
Network detection
Static client detection
Dynamic Client Detection
Signaturebased Network detection
Anomalybased Network detection
Static signature based client detection
Static anomaly based client detection
Dynamic Signature based Client detection
Dynamic anomaly based Network detection

Fig 2. Classification of Mobile Malware Detection Techniques[11].

Above diagram shows that all the mobile malware identifying techniques are either signature-based or anomaly-based. With signature-based techniques, the malicious behaviors of known malware are captured as their signatures. The malware is detected when one of its signatures is identified. With anomaly-based techniques, the normal system behavior is modeled first. Then the malware is detected whenever the system behavior differs from the modeled normal behavior.

From the perspective of where malware detection is executed, malware detection methods are classified as two domains, client detection and network detection. Generally, techniques for client detection could be either host-based or cloud-based. Most of the malware detection tools for mobile devices use signature-based detection techniques. The efficiency of techniques depends upon the availability of an up-to-date signature database. Often it requires the device to store a huge signature database for static scanning. One possible way to reduce the database size is to usage of same stored signature for all deviations of the same malware. In any case, susceptibility to obfuscation is a main disadvantage of signature-based detection techniques.

In static analysis, codes or apps are analyzed without being executed. It consists of three steps: unpacking, disassembling, and analyzing. It is generally fast and simple. Dynamic analysis means that the behavior of apps is continuously monitored in an isolated environment. This technique collects and investigates runtime information of an app, e.g. events and system calls. Static analysis techniques focus on what is being accessed, while dynamic analysis focuses on why certain suspicious operations are performed and how often they are performed.

Kaspersky found that personal computers in almost 30 countries infected with spying programs, in which most of the infections seen in Iran, followed by Russia, Afghanistan, Pakistan China, Yemen, Syria and Algeria. The targets consist of government and energy companies, military institutions, banks, telecommunication companies, nuclear researchers and Islamic activists [13].

Following approaches are used and marks confirm that user might be infected with Spyware [14]:

- Reduced performance: They use system resources, CPU cycles, memory, disk space, bandwidth and it also makes your system slower.
- System instability: Most of the spywares not well tested or debugged and no way to report bugs or obtain technical support. This outcome leads to system crashes, hangs or other strange behavior.
- Deception: They typically use Trojan horse tactics to infiltrate user computer. It offers to synchronize user PC's clock or keep track of forms, but it will also do some other unseen things while user browsing.
- Browser hijacking: If user default home page has changed, it most likely is due to the spyware.
- Privacy Loss: Spyware can track the web sites user visits and send the same date back to the spyware developer.

- Popup Advertising: Even though user installed a popup blocker or run a web browser with popup blocking and still if he gets pop-ups, then those pops up may not be coming from the web site, they undoubtedly coming from spyware.
- Stolen advertising: Instead of showing the ads that should appear on a web site, some spyware replaces its own ads which can rob a web site of revenue.
- Broken web sites: Spyware sometimes changes the actual content on a web page and breaks the page. The page may not appear correct, or user may get JavaScript errors.
- Security risks: hey have a built-in update feature that allows the spyware maker download and install new code to user system without his\her knowledge or acknowledgement.
- Redirection: They may cause the results of user Internet search or web site selection to be redirected to another web site which not intended. Many spyware programs collect information such as a Text Messages, Call History, Contact List, Web History, Wi-Fi Networks, Emails, Calendar, Notes, Tasks and GPS Location [15].

III. SPYWARE AFFECTED COUNTRIES.

TABLE 1. Encounter rate trends for the locations with computers reporting spyware and unwanted software [17].

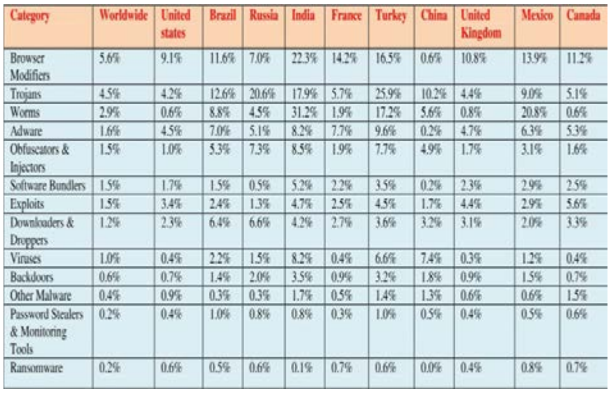
Country/Region	3Q14	4Q14	1Q15	2Q15
United States	15.4%	11.6%	11.0%	9.8%
Brazil	32.9%	21.7%	20.5%	20.2%
Russia	27.3%	24.1%	22.8%	17.7%
India	38.2%	32.0%	34.9%	31.3%
France	22.8%	13.0%	15.8%	13.2%
Turkey	35.1%	27.9%	32.0%	28.1%
China	18.1%	15.2%	13.1%	13.7%
United Kingdom	17.2%	11.4%	12.7%	11.7%
Mexico	30.0%	21.7%	22.6%	21.2%
Canada	18.1%	12.5%	14.0%	12.5%

According to the above table, Encounter rate is defined as the percentage of computers running Microsoft real-time security products that reports or affected by a malware encounter. The worldwide encounter rate increased slightly in 1Q15 before decreasing again in 2Q15, and this pattern is reflected in several of the locations as well. India, France, Turkey, the United Kingdom, Mexico, and Canada all had small encounter rate increases in the beginning of the first quarter of 2015. In general, however, encounter rates endured largely stable through the first half of 2015 in all of these locations, without any remarkably large increases or decreases.

IV. RESULT ANALYSIS

As observed from the above sections that, even though many spywares developed for protection, but still these are not capable enough in providing complete protection. So, it is essentials to have anti-spyware or malware software which protects from all categories of spywares present in the world now and in the future [16].

TABLE 2. Shows the occurrence of different types of malware in several locations around the world in 2Q15 [17].



Category	Worldwide	United states	Brazil	Russia	India	France	Turkey	China	United Kingdom	Mexico	Canada
Browser Modifiers	5.6%	9.1%	11.6%	7.0%	22.3%	14.2%	16.5%	0.6%	10.8%	13.9%	11.2%
Trojans	4.5%	4.2%	12.6%	20.6%	17.9%	5.7%	25.9%	10.2%	4.4%	9.0%	5.1%
Worms	2.9%	0.6%	8.8%	4.5%	31.2%	1.9%	17.2%	5.6%	0.8%	20.8%	0.6%
Adware	1.6%	4.5%	7.0%	5.1%	8.2%	7.7%	9.6%	0.2%	4.7%	6.3%	5.3%
Obfuscators & Injectors	1.5%	1.0%	5.3%	7.3%	8.5%	1.9%	7.7%	4.9%	1.7%	3.1%	1.6%
Software Bundlers	1.5%	1.7%	1.5%	0.5%	5.2%	2.2%	3.5%	0.2%	2.3%	2.9%	2.5%
Exploits	1.5%	3.4%	2.4%	1.3%	4.7%	2.5%	4.5%	1.7%	4.4%	2.9%	5.6%
Downloaders & Droppers	1.2%	2.3%	6.4%	6.6%	4.2%	2.7%	3.6%	3.2%	3.1%	2.0%	3.3%
Viruses	1.0%	0.4%	2.2%	1.5%	8.2%	0.4%	6.6%	7.4%	0.3%	1.2%	0.4%
Backdoors	0.6%	0.7%	1.4%	2.0%	3.5%	0.9%	3.2%	1.8%	0.9%	1.5%	0.7%
Other Malware	0.4%	0.9%	0.3%	0.3%	1.7%	0.5%	1.4%	1.3%	0.6%	0.6%	1.5%
Password Stealers & Monitoring Tools	0.2%	0.4%	1.0%	0.8%	0.8%	0.3%	1.0%	0.5%	0.4%	0.5%	0.6%
Ransomware	0.2%	0.6%	0.5%	0.6%	0.1%	0.7%	0.6%	0.0%	0.4%	0.8%	0.7%

Above table shows the significant differences exist in the types of threats that affect users in different parts of the world. The spread of malware can be highly reliant on language and socioeconomic factors as well as the methods used for circulation. Some threats spread using techniques that target people who use online services that are local to a specific geographic region. Other threats mainly targets vulnerabilities or operating system configurations and applications that are unevenly distributed around the world. India experienced higher encounter rates for Backdoors, Browser Modifiers, Obfuscators, Malware, and Injectors, Software Bundlers, Viruses, and Worms than the other locations.

Our futuristic plan will be implementing the Hybrid approach detect the spyware using Artificial Neural Networks which is capable of detecting all the above mentioned types of spywares and adaptable to all the different categories of platforms and user.

V. CONCLUSION

Many people in the world are unaware of the impact of the spyware. This paper discusses about the possible spyware threats to user's and also the limitations of existing antispyware. The literature survey of the previous research concludes that there exists a race between a spyware and antispyware. Finally this is a responsibility of each individual's, or company or authority to ensure that certain level of Security, which provides to maintain the information security and privacy with the knowledge of what and how personal data should be retain, manage and share?

All the limitations mentioned about the spyware in this paper will be our future work to improvise existing research or methodology.

REFERENCES

[1]. Shukla, H., et el "Enhance operating system security by restricting privileges of vulnerable application," in Consumer Electronics (GCCE), 2013 IEEE 2nd Global Conference on, vol, no, pp.207-211, 1-4 Oct. 2013 doi: 10.1109/GCCE.2013.6664800.

[2]. Gangula, A., et el "Survey on Mobile Computing Security," in Modelling Symposium (EMS), 2013 European, vol, no, pp.536-542, 20-22 Nov. 2013 doi: 10.1109/EMS.2013.89.

[3]. Suteva, N., et el "Computer forensic analisys of some web attacks," in Internet Security (WorldCIS), 2014 World Congress on , vol., no., pp.42-47, 8-10 Dec. 2014 doi: 10.1109/WorldCIS.2014.7028164.

[4]. Kuehnhausen, M.; Frost, V.S., "Trusting smartphone Apps? To install or not to install, that is the question," in Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), 2013 IEEE International Multi-Disciplinary Conference on , vol, no, pp.30-37, 25-28 Feb. 2013 doi: 10.1109/CogSIMA.2013.6523820.

[5]. Kumar, A; Reddy, K., "Constructing secure web applications with proper data validations," in Recent Advances and Innovations in Engineering (ICRAIE), 2014 , vol., no., pp.1-5, 9-11 May 2014 doi: 10.1109/ICRAIE.2014.6909304.

[6]. Fang Yu., et el "An Online Service for Detecting, Viewing and Patching Web Application Vulnerabilities," in System Sciences (HICSS), 2014 47th Hawaii

International Conference on , vol., no., pp.4878-4886, 6-9 Jan. 2014 doi: 10.1109/HICSS.2014.598.

[7]. Arastouie, N., et el "Hunter: An Anti-Spyware for windows Operating System," in Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. IIIInternational Conference on , vol., no., pp.1-5, 7-11 April 2008 doi: 0.1109/ICTTA.2008.4530281.

[8]. Parmjit Kaur., et el “Spyware Detection in Android Using Hybridization of Description Analysis, Permission Mapping and Interface Analysis, Procedia Computer Science”, Volume 46, 2015, Pages 794-803, ISSN 1877-0509, http://dx.doi.org/10.1016/ j.procs.2015.02.148.

[9]. Hui Xu., et el "Spyware: Investigating the privacy leakage signatures in app execution traces," in Software Reliability Engineering (ISSRE), 2015 IEEE 26th International Symposium on , vol., no., pp.348-358, 2-5 Nov. 2015 doi: 10.1109/ISSRE.2015.7381828.

[10]. Tyagi, G., et el "A novel framework for password securing system from key-logger spyware," in Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on , vol., no., pp.70-74, 7-8 Feb. 2014 doi: 10.1109/ICICICT.2014.6781255.z

[11]. Daojing He., et el "Mobile application security: malware threats and defenses," in Wireless Communications, IEEE , vol.22, no.1, pp.138-144, February 2015 doi: 10.1109/MWC.2015.7054729.

[12]. www.bbc.com/news/technology-34732514, Report finds apps regularly spy on users, accessed on 30th November 2015.

[13]. www.telegraph.co.uk/news/worldnews/northamerica/usa/11416985/Millions-of-computers-may-be-compromised-by-US-spyware-report.html, Millions of computers may be compromised by US spyware – report, accessed on 10 Feb 2016.

[14]. www.windowsecurity.com/whitepapers/Network_Security/Spyware-etwork.html, Spyware Clogging Network Arteries by Jeff McDermott, accessed on 15 Feb 2016.

[15]. www.blackhat.com/docs/us-15/materials/us-15-Dalman-Commercial-Spyware-Detecting-The-Undetectable.pdf, Fidelis Cyber security, accessed on Dec 2015.

[16]. KKhan., et el "An advanced algorithm for Malware Detection," in Electrical, Electronics, Signals, Communication and Optimization (EESCO), 2015 International Conference on, vol, no, pp.1-3, 24-25 Jan. 2015 doi: 10.1109/EESCO.2015.7253988.

[17]. Microsoft Security Intelligence Report Volume 19, January through June, 2015.