IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

nCORETech 2017

LBS College of Engineering, Kasaragod

Vol. 6, Special Issue 3, March 2017

A Survey on Malwares, and detection Techniques

Ujwala Vijayan [1], Midhun T P[2]

PG Student, Computer Science & Engineering, Vimal Jyothi Engineering College, Kannur, India [1]

Assistant Professor, Computer Science & Engineering, Vimal Jyothi Engineering College, Kannur, India[2]

Abstract: Malware or malicious software refers to software programs designed to damage or do other unwanted actions on a computer system which includes disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising. Smartphones and mobile tablets are rapidly becoming indispensable in daily life. Given their large distribution, and also their capabilities, in the last two years mobile devices have become the main target for attackers . Android, the open source OS introduced by Google, has currently the largest market share, which is greater than 80%.Due to the openness and popularity, Android is the main target of attacks against mobile devices (98.5%), with more than 1 million of malicious apps currently available in the wild . Equipped withthe knowledge of malware's capabilities, the detection of malware is an area of major concern not only to the research community but also to the general public. This paper focuses on the survey on different categories of malwares, its features and detection techniques.

Keywords: Malwares, Static Analysis, Dynamic Analysis, Security, Android.

I. INTRODUCTION

Malware or malicious software refers to software programs designed to damage or do other unwanted actions on a computer system which includes disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising. In Spanish, ”mal” is a prefix that means ”bad,” making the term ”badware,” which is a good way to remember it.

Malware' is an umbrella term used to refer to different forms of hostile orintrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and othermalicious programs. It can take the form of executable code, scripts, active content, and other software. Malware is oftendisguised as, or embedded in, non-malicious files.

The amount of malware threats has increased in volume andevolve in complexity during the past few years. As more andmore organizations try to address this problem, the number ofwebsites distributing malwares are increased at an alarmingrate. Most of the malware enters the system while downloadingfiles over Internet. Once the malicious software finds its wayinto the system, it scans for vulnerabilities of operating systemand perform unintended actions on the system finally slowing down the performance of the system.[5]

II. CATEGORIES OF MALWARES

Malwares has increased in types and complexities day by day. Some of the common forms of malwares are as follows:[1]

A. Adware

Adware is the short for advertising-supported software. It automatically plays, displays, or downloads advertisements to a computer after malicious software is installed or application is used. This piece of code is generally embedded into free software. Most of the adwares which are authored by the advertisers serves as a revenue generating toolwhile some of them are only desigened to deliver adds.Exaples of adwares include free games, peer-to-peer clients like KaZaa, BearShare etc.

B. Bots

Bots are software programs created to done some specific operations while some of them are harmless like video gaming etc. It can be used in collection of remotely controlled computers called botnets for DDos attacks as spambots that render advertisements on websites, as web spiders that scrape server data, and for distributing malware disguised as popular search items on download sites. Websites can guard against bots with CAPTCHA tests that verify users as human.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
nCORETech 2017
LBS College of Engineering, Kasaragod
Vol. 6, Special Issue 3, March 2017

C. Bugs

A bug is flaw that produces an undesired outcome. These flaws are usually the result of human error and typically exist in the source code or compilers of a program. Minor bugs only slightly affect a programs behavior and as a consequence can go for long periods of time before being discovered.

More significant bugs can cause crashing or freezing. Security bugs are the most severe type of bugs and can allow attackers to bypass user authentication, override access privileges, or steal data. Bugs can be prevented with developer education, quality control, and code analysis tools.

D. Ransomware

Ransomware is a form of malware that essentially holds a computer system locked up while demanding a deal (ransom). The malware restricts user accessto the computer either by encrypting files on the hard drive or locking down the system and displaying messages that are intentional to force the user to pay the malware creator to remove the restrictions and regain access to their computer. Ransomware typically spreads like a normal computer worm ending up on a computer via a downloaded file or through some other vulnerability in a network service.

E. Rootkit

A rootkit is a type of malicious software designed to remotely access or control a computer without being detected by users or security programs. Once a rootkit has been installed it is probable for the malicious party behind the rootkit to remotely execute files, access/steal information, modify system configurations, alter software (especially any security software that could detect the rootkit), install concealed malware, or control the computer as part of a botnet. Rootkit prevention, detection, and removal can be difficult due to their stealthy operation.

Because a rootkit frequently hides its presence, typical security products are not effective in detecting and removing rootkits. As a result, rootkit detection relies on manual methods such as monitoring computer behavior for irregular activity, signature scanning, and storage dump analysis. Organizations and users can defend themselves from rootkits by regularly repairing vulnerabilities in software, applications, and operating systems, updating virus definitions, avoiding suspicious downloads, and performing static analysis scans.

F. Spyware

Spyware is a collective term for software that functions by spying on user activity without their knowledge. These spying capabilities can include activity monitoring, collecting keystrokes (keys pressed by the user), data harvesting (account information, logins, financial data), and more. Spyware often has additional capabilities as well, ranging from modifying security settings of software or browsers to interfering with network connections.

Spyware spreads by exploiting software vulnerabilities, bundling itself with legitimate software, or in Trojans. It generally enters a system when free or trial software is downloaded. Software, applications, and operating systems, updating virus definitions, avoiding suspicious downloads, and performing static analysis scans.

G. Trojan Horses

A trojan describes the class of malware that appears to perform a desirable function but in fact performs undisclosed malicious functions that allow unauthorized access to the victim computer. It shows the behavior of an authentic program such as login shell and hijacks user password to gain control of system remotely.

H. Viruses

A virus is a software with bad intension which is capable of copying itself and spreading to other computers. Viruses can be mainly of two types: Polymorphic which uses a polymorphic engine to mutate while keeping the original algorithm intact (packer) and metamorphic which change after each infection. A virus may spread from an infected computer to other through network or corrupted media such as floppy disks, USB drives.

I. Worms

A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other nodes and do so without any user involvement.

Worms may cause harm to network by consuming the bandwidth. In contrast to viruses, worms do not need the support of any file. It might delete files, encrypt files in as crypto viral extortion attack or send junk email. Example of worms include Sasser, My Doom, Blaster, Melissa etc.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
nCORETech 2017
LBS College of Engineering, Kasaragod
Vol. 6, Special Issue 3, March 2017

J. Browser Hijacker

When your homepage changes to one that looks similar to those in the imagesinserted next, you may have been infected with one form or another of a Browser Hijacker. This dangerous Malware will redirect your normal search activity and give you theresults the developers want you to see. Its intention is to make money off your web surfing. Using this homepage and not eliminating the Malware lets the source developers capture your surfing interests. This is especially dangerous when banking or shopping online. These homepages can look harmless, but in every case they allow other more infectious.

III.MALWARE DETECTION

There are mainly two approaches in malware security detection[2] that is static analysis and dynamic analysis. Static analysis means troubleshooting programs potential security problems without performing the program. Most static malware detection methods are based on traditional content signatures, such as a list of malware signature definitions, and compare each application against the database of known malware signatures. The disadvantage of this detection method is that users are only protected from malwares, which are known or detected by most recently updated signatures, but can't be protected from the malwares, which are newly designed or derived from originals.[4]

Dynamic analysis means analyzing the program with performing in real or simulated environment. Instead of using static signatures, an effective alternative solution is to use characteristic and behavior-based methods, which try to detect malware by observing the statistic and/or dynamic behavior and features of mobile applications. One of the most popular behavioral methods is malware detection based on static requested permissions, which check what types of resources, such as Wi-Fi network, user location, user contact information and requesting for installation. There is an approach called hybrid techniques which combines both static and dynamicapproaches.Malware detection techniques can be broadly classified into two:[3]

- Signature based detection
- Behavior based detection

A. Signature Based Detection

Looks for signatures within the malware code to declare that the program scanned is malicious in nature. Detection of basic malware is relatively if the signature can be found for the viral code. Polymorphic virus generates new signature for each variantwhich makes signatures based detection difficult.[8] Metamorphic viruses evade the detections from the malware detector since each new variant generated will have different signature. It is impossible to store the signatures of multiple variants of same malware sample. Main problems with the signature baseddetection: Signature extraction and distribution is a complex task The signature generation involves manual intervention and requires strict code analysis. The signatures can be easily bypassed as and when new signatures are created. The size of signature repository keeps on growing at an alarming rate.[6]

B. Behavior Based Detection

Identifies the action performed by the malware rather than the binary pattern .Programs with dissimilar syntax's but having same behavior. are collected. Thus this single behavior signature can identifyvarious samples of malware.Components of behavior detector are as follows:[7]

- Data Collection: This component collects the dynamic /static information's.
- Interpretation: This component converts the raw information collected by data collection module into intermediate representations.
- Matching Algorithm: It is used to compare the representation with the behavior signature.

Behavior based detection can be again classified into:[10]

- Anomaly Based Detection: Anomaly based detection uses the knowledge of what is considered as normal to find out what actually is malicious. It approximates the requirements of application or system instead of implementation. While anomaly based detection has the following two shortcoming 1) It is susceptible to false positives and 2) It is susceptible to mimicry attacks.[10]
- Specification based detection:Specification based detection makes use of signature-based detection to some extent. All events from the program to the operating system are mediated by a specification or policy. The policy specifies what action should be taken for a sequence of events. Programs violating the rule set are considered as malicious program.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

nCORETech 2017

LBS College of Engineering, Kasaragod

Vol. 6, Special Issue 3, March 2017

TABLE I COMPARISON OF DETECTION TECHNIQUES PROPOSED BY DIFFERENT AUTHORS

Paper	Author	Approach	Accuracy & remarks
Kernel-based Behavior Analysis for Android Malware Detection	Takamasa Isohara et.al.	Behavior based	Can be applied for security inspections for Android application markets.
Android Malware Detection Based On Permission And Behavior Analysis	Zhongyuan Qin et.al	Behavior based	Advantage of detecting unknown malware, compared with signature-based detection method. Defines the actual malicious behaviors more accurately than anomaly-based detection method

TABLE II COMPARISON OF DETECTION TECHNIQUES PROPOSED BY DIFFERENT AUTHORS

Paper	Author	Approach	Accuracy & remarks
A Hybrid Approach of Mobile Malware Detection in Android	Fei Tong et.al.	Behavior based	Detection accuracy can be furtherimproved since the pattern sets can be automatically optimized through self-learning.
Effective detection of android malware based on the usage of data flow APIs and machine learning	Songyang Wu et.al	Behavior based	97.66%
Droid Chain: A novel Android malware detection method based on behavior chains	Zhaoguo Wang et.al	Behavior based	Accuracy 73%–93%, precision 71%–99%, recall 42%–92%,
Apposcopy: Semantics-Based Detection of Android Malware through Static Analysis	Yu Feng et.al.	Signature based	Not invincible. Unfit for scenarios that require instant detection of malware.

TABLE IIII COMPARISON OF DETECTION TECHNIQUES PROPOSED BY DIFFERENT AUTHORS

Paper	Author	Approach	Accuracy & remarks
A Probabilistic Discriminative Model for Android Malware Detection Using Decompiled Source code	Lei Cen et.al.	Signature based	Limits in detecting zero-day malicious applications.
Structural Detection of Android Malware using Embedded Call Graphs	Hugo Gascon	Signature based	89%
MADAM: Effective and Efficient Behavior-basedAndroid Malware Detection and Prevention	Andrea Saracino et.al	Behavior based	96%

IV. CONCLUSION

With the growing volume and sophistication of cyber-attacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security. Increasing Number of Mobile Devices and Mobile Traffic makes android security to be treated carefully. From this survey it is identified that specification based detection is the good detection technique for malware. Disadvantages of signature based detection is that there are no known techniques for accurately representing the set of software's via signatures and also human involvement/expertise is usually needed to develop the signatures. Since Anomaly-based detection is an approximation, valid behavior might be flagged as malicious under anomaly-based detection methods.

REFERENCES

[1] Isohara, Takamasa, Keisuke Takemori, and Ayumu Kubota. "Kernel-based behavior analysis for android malware detection." Computational Intelligence and Security (CIS), 2011 Seventh International Conference on. IEEE, 2011.

[2] Qin, Zhongyuan, et al. "Android malware detection based on permission and behavior analysis." Cyberspace Technology (CCT 2014), International CoSaracino, Andrea, et al.

[3] "Madam: Effective and efficient behavior-based android malware detection and prevention." (2016).conference on. IET, 2014.
[4] Zhu, Jiawei, et al. "API Sequences Based Malware Detection for Android." Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom), 2015 IEEE 12th Intl Conf on. IEEE, 2015.
[5] Arp, Daniel, et al. "DREBIN: Effective and Explainable Detection of Android Malware in Your Pocket." NDSS. 2014.
[6] Cen, Lei, et al. "A probabilistic discriminative model for android malware detection with decompiled source code." IEEE Transactions on Dependable and Secure Computing 12.4 (2015): 400-412.
[7] Wu, Songyang, et al. "Effective detection of android malware based on the usage of data flow APIs and machine learning." Information and Software Technology 75 (2016): 17-25.
[8] Sedano, Javier, et al. "On the Selection of Key Features for Android Malware Characterization." International Joint Conference. Springer International Publishing, 2015.
[9] Yuan, Zhenlong, Yongqiang Lu, and YiboXue. "Droiddetector: android malware characterization and detection using deep learning." Tsinghua Science and Technology 21.1 (2016): 114-123.
[10] Vinod, P., et al. "Survey on malware detection methods." Proceedings of the 3rd Hackers' Workshop on computer and internet security (IITKHACK'09). 2009.