A Study on Various Proximity Malware Detection Techniques

Nithya.K[1], Dr.A.Malathi[2]
[1]*M.Phil Scholar, Government Arts College, Coimbatore.*
[2]*Assistant Professor of Computer Science*
Government Arts College, Coimbatore.

***Abstract*—In modern network the malware is one of the serious issues where it can be identified by many roles such as email spam, Denial of service and Trojan like viruses. This paper focused on various malware proximity nodes for accurate misbehavior identification. It also explains about general behavioral characterization of proximity malware, which captures the normal and abnormal behavior of data and its functional differences. This paper presents a detailed study on various malware detection techniques such as anomaly detection and signature based detection that identifies the imperfect nature in order to detect proximity malware.**

Index Terms—Malware; proximity malware; Anomaly based; signature based.

I. INTRODUCTION

Malware is a piece of malicious code which disrupts the host node's functionality and duplicates and propagates itself to other nodes via contact opportunities. Malware is a very big threat in today's computing world.
Malware has become the major impediment in the development of networks. Any new type of network that provides promising applications always becomes the main target of new malware. Among the recent viruses and worms, those propagating in a distributed manner and without central control are the hardest to defend against. In the last year, the rapid outbreak of the Conflicted worm, which propagates updates in a distributed peer-to-peer way, clearly indicates the difficulty and importance of coping with distributed malware.

Millions of compromised website launch drive- by download exploits against vulnerable hosts [1].Botnets [2] used miscreants to launch denial of service attack send spam,E-Mails, host scam pages. Measure the size of botnet [3], infestation executable with spyware [4].

II. TYPES OF MALWARE

There are various types of malware is generated .some of the malware are

2.1 VIRUS:

The computer virus is code and replicates inserting into other program. The virus is promulgating injecting into another program called host program. Virus can affect your system .virus attached to executable file and exist the system until and unless host program is executed [5], virus damage or obliterate data on your computer even expunge everything your hard disk.

2.2 WORM:

Worm is self-replicating. Worm use computer system to transfer the malicious code to another system. Worm is stand-alone software program. Computer worm replicates own code independent of other program. Primary distinction between virus and worm in that worm does not need host to cause harm. Another distinction is virus and worm is propagation model [6].

2.3 TROJAN:

Malware embedded in designer an application or system. Application or systems perform some useful function and some unauthorized action. Embedded malware also be time bomb [7], Drive-by downloads or installing online games, song or movies by internet driven application order to reach target computer.

2.4 SPYWARE:

Without knowledge of user spyware can collect any type of data including user personal information such as bank account number, credit card number.

ISSN: 2278 – 1323

2.5 BACKDOOR:

Backdoor is a hacker / attacker access the system without using username, password, enter into system that act front door. The name suggests software allows system from backdoor bypassing the user authentication scheme. The hacker installs backdoor program helps them access the system without entering username and password into login screen.

Christo dorsum and jha [8], and McGraw and Morisot [9], provide various type of malware. Obfuscation and behavior addition and modification order to circumvent malware detectors. The widespread use aforementioned technic and malware codes mention by researchers reused code is major component development of new malware.

2.6 PROXIMITY MALWARE:

Proximity malware and existing schemes' number of studies demonstrate the severe threat of proximity malware propagation. Collected Bluetooth scanner traces used simulation malware effectively propagate via Bluetooth [10].Sophisticated malware containment capability, such as patching or self-healing [.11]. Yan et al Developed malware model [12].malware use both SMS/MMS and Bluetooth propagate faster by messaging alone [13].Proximity malware and mitigation schemes has been proposed which helps to collect Bluetooth traces and demonstrated that malware could effectively propagate via Bluetooth with simulations.

Some existing developed Bluetooth malware model, which showed that Bluetooth can enhance malware, propagation rate over SMS/MMS. Malware attack move from large scale internet growing popular mobile network [14].mobile malware instance more than 350 reported early 2007.mobile malware propagate 2 different dominate approach.1st one address book and 2nd one proximity malware .content based signature malware many node possible at [15],[16].

III. MALWARE DETECTION TECHNIQUES

Techniques used for detecting malware can be categorized broadly into two categories:

- anomaly-based detection
- signature-based detection

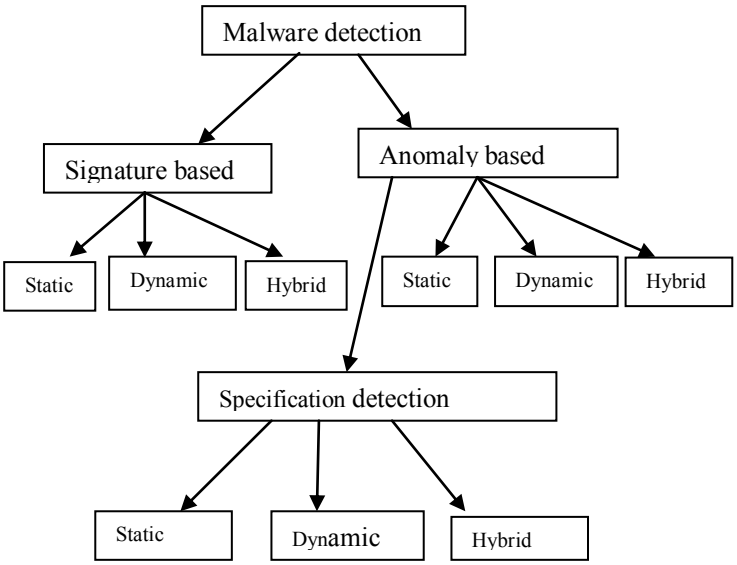
ANOMALY-BASED DETECTION TECHNIQUE:

Anomaly-based detection is Occurs 2 phases. 1st one is training phases and 2nd one is detection phases. The training phases are detector attempt to learn normal behavior. Anomaly-based detection technique uses its knowledge of what constitutes normal behavior to decide the maliciousness of a program under inspection. A special type of anomaly-based detection is referred to as specification-based detection. Specification-based techniques leverage some specification or rule set of what is valid behavior in order to decide the maliciousness of a program under inspection. Programs violating the specification are considered anomalous and usually, malicious. Key advantages of anomaly based detection ability to detect zero-day attack. Sekar et al[17],create finite state automata(FSA)based to anomaly detection.

SIGNATURE-BASED DETECTION TECHNIQUE:

The Signature-based malware detection is based on bit patterns a malware contains. These types of technique to detect the virus or other threats to look for signature in file that under scanning process. Signature is basically sequence of bytes that define malware. Signature-based detection uses its characterization of what is known to be malicious to decide the maliciousness of a program under inspection. As one may imagine this characterization or signature of the malicious behavior is the key to a signature-based detection method's effectiveness. Spike [18], framework designed to user monitor behavior of application with goal of finding malicious behavior.

key to a signature-based detection method's effectiveness. Spike [18], framework designed to user monitor behavior of application with goal of finding malicious behavior.



1. Classification of malware detection techniques

The hybrid techniques combine 2 approaches, static and dynamic information used to detect malware. Ellis et al[19],the signature based worm detection base malicious behavior .Lo et al[20],propose tool malicious code

filter(MCF)this tools analyze and executable. Cross-view diff-based approach detects the type of malware. This approach scanning 2 ways.1st one is inside the box approach and 2nd one is outside the box approach. Inside the box is comparisons of high-level and low level result within same machine. Outside the box is low-level access without target host's knowledge. High-level scan of target host is compare to low-level scan from clean host.

SPECIFICATION BASED DETECTION:

Specification-based detection is a type of anomaly-based detection. Specification-based detection method attempt approximate the implement application or system. The training phase is attainment of some rule set and valid behavior system being protected program under inspection. The main limitation of difficult to specify completely and accurately entire set of valid behavior system exhibitor. et al[21], propose specification-based method for detecting maliciousness in a distributed environment.

COMPARISON OF MALWARE DETECTION METHOD

Techniques	**Advantage**	**Disadvantage**
Signature based	1.Model Well known attacks 2.Use these known pattern to detect intrusion 3.Accurate and generate much fewer false alarm 4. supervised learning	1. Cannot detect new, unknown intrusion detection. 2.No signature is available for such attack.
Anomaly based	1.Trained using normal behavior of the system 2.Try to flag the deviation from normal pattern as intrusion 3.Is able to detect unknown attacks based on audit 4. Unsupervised learning	1. It need update the data describing the users' behavior and statistics in normal usage. 2. High false positive-alarm and limited by training data

Table1. Comparison of malware detection method

IV. CONCLUSION

The security is the primary concern in every field of computer network from the malware detection. This paper provides a depth study on various type of malware. The two major category in detection technique such as anomaly and signature based malware has also been compared. The paper also analyzed the imperfect of proximity malware.

REFERENCES

[1] Provos,N.,Mavrommatis,P.,Rajab,M.,Andmonrose,F. Allyouriframespointtous.In17thusenixsecuritysympo-Sium(2008).

[2] Dagon,D.,Gu,G.,Lee,C.,Andlee,W.Ataxonomyofbotn etstructures.Inannual Computer Security Applications Conference(Acsac)(2007).

[3] Rajab,M.,Zarfoss,J.,Monrose,F.,Andterzis,A.Amultif acetedapproachtounderstandingthebotnetphenomenon .Ininternetmeasurementconference(Imc)(2006).

[4] Moshchuk,A.,Bragin,T.,Gribble,S.,Andlevy,H.Acraw lerbasedstudyofspywareontheweb.Innetworkanddistri butedsystemssecuritysymposium(Ndss)(2006).

[5] ArunLakhotia ,AdityaKapoor , Eric Uday, "Are Metamorphic Viruses Really Invincible Part 2" , Virus Bulletin ,January 2005

[6] AbhishekKarnik, SuchandraGoswami and RatanGuha," Detecting Obfuscated Viruses Using Cosine Similarity Analysis", in The Proceeding of IEEE Symposium First International Conference on Modelling& Simulation (ASM '07).

[7] M. Christodorescu and S. Jha.Testing malware detectors. In Proceedings of the International Symposium on Software Testing and Analysis, July 2004.

[8] G. McGraw and G. Morrisett.Attacking malicious code: A report to the infosec research council. IEEE Software, 17(5):33–44, 2000.

[9] J. Su, K. Chan, A. Miklas, K. Po, A. Akhavan, S. Saroiu,E. de Lara, and A. Goel,

[10] "A preliminary investigation of worm infections in a bluetooth environment," in Proc. of the workshop on Rapid malcode (WORM). ACM, 2006.

[11] F. Li, Y. Yang, and J. Wu, "Cpmc: an efficient proximity malware coping scheme in smart phone-based mobile networks," in Proc. of INFOCOM. IEEE, 2010.

[12] G. Yan, H. Flores, L. Cuellar, N. Hengartner, S. Eidenbenz,and V. Vu, "Bluetooth worm propagation: mobility pattern matters!" in Proc. of the Symposium on Information, Com-puter and Communications Security (ASIACCS). ACM,2007.

[13] A. Bose and K. Shin, "On mobile viruses exploiting messagingandbluetoothservices," in Proc. of the ICST Securecomm,2006.

[14] G. Zyba, G. Voelker, M. Liljenstam, A.M´ehes, and P. Johansson,"Defending mobile phones from proximity malware," in Proc. of IEEEINFOCOM, 2009.

[15] "F-Secure Virus Information Pages: Commwarrior," http://www.f-secure.com/v-descs/commwarrior.shtml
[16] N.Weaver, V. Paxon, S. Staniford, and R. Cunningham.A taxonomy of computer worms. In Proceedings of the 2003 ACM Workship on Rapid Malcode, pages 11–18, 2003.
[17] S. Hofmeyr, S. Forrest, and A. Somayaji. Intrusion detection using sequences of system calls. Journal of Computer Security, pages 151 – 180, 1998.
[18] C. Taylor and J. Alves-Foss. Nate – network analysis of anomalous traffic events, a low-cost approach. New Security Paradigms Workshop, 2001.
[19] J. Rabek, R. Khazan, S. Lewandowski, and R. Cunningham.Detection of injected, dynamically generated, and obfuscated malicious code. In Proceedings of the 2003 ACM Workshop on Rapid Malcode, pages 76–82, 2003.
[20] D. Ellis, J. Aiken, K. Attwood, and S. Tenaglia. A behavioral approach to worm detection. In Proceedings of the 2004 ACM Workshop on Rapid Malcode, pages 43–53, 2004.
[21] C. Ko, M. Ruschitzka, and K. Levitt. Execution monitoring of security-critical programs in distributed systems: A specification-based approach. In Proceedings of the 1997 IEEE Symposium on Security and Privacy, 1997

