Publication of Little Lion Scientific R&D, Islamabad PAKISTAN
Journal of Theoretical and Applied Information Technology
31st July 2011. Vol. 29 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MALWARE THREATS AND MITIGATION STRATEGIES: A SURVEY

RIZWAN REHMAN[1], DR. G.C. HAZARIKA[2], GUNADEEP CHETIA[3]

[1] Assistant Professor, Centre for Computer Studies, Dibrugarh University, Dibrugarh

[2] Director i/c, Centre for Computer Studies, Dibrugarh University, Dibrugarh

[3] Lecturer, Centre for Computer Studies, Dibrugarh University, Dibrugarh

ABSTRACT

Malicious software is one of the major threats faced by the internet today. Basically the program is designed to disrupt the operation, collect information which can be used for unauthorized access and other targeted behavior. Malwares from their early designs which were just for propagation have now developed into more advanced form, stealing sensitive and private information. Apart from these their can even be some targeted worms to victimize an organization and even identity theft. In this paper, we are addressing different trends and techniques used for developing malware and a survey on how these can be handled in an efficient manner. Finally we discuss trends in malware designs and latest attack models and also the latest mitigation strategies.

Keywords: *Malicious Software, Security, Performance, Mitigation Strategy, Threats*

1. INTRODUCTION

Malware is a malicious code that propagates over the network. It can be considered as the one to which new features can be easily added to enhance its attack. It can also be powerful so as to take full control of infected host and network connection disabling all the firewalls and installed ant viruses. The problem is cumulating with the use of internet as most of the web pages have been infected with various types of malware downloads which are delivered by just opening the web page. According to statistics by Google , 70% of the malware comes from popular sites.

According to Osterman Research [1] survey 11 million malware variants were discovered by 2008 and 90% of the malware comes from hidden downloads, pointers in trusted and popular websites. These threats can be delivered in many different variant modes often called blended threats which contain multiple components such as fishing attempts, spams, viruses, worms and Trojan.

The current picture can be seen as follows:

Table 1

Types	Layer
Viruses / Worms /Spyware	Applications
Trojan Horses	System Software
OS Rootkits	Operating System and Drivers
VMM Rootkits	Virtual Machines
Bios Rootkits	Firmware

The intent behind recent malware attack has shifted the focus into invasion of privacy, financial gain and identity thefts using spams, fishing attack, spyware, adware, root kits and keystroke loggers to capture password as well as other sensitive information's. The new form of malware conceals themselves in order to hide their existence from personal firewalls, antivirus programs, anti spyware software and the OS itself [1][2]. Detections of these threats is very difficult job and data may be sent out of internal network which may be sensitive making it very risky not only to government organization but also to the general users.

Publication of Little Lion Scientific R&D, Islamabad PAKISTAN
Journal of Theoretical and Applied Information Technology
31st July 2011. Vol. 29 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 2
Perceived Risks of Various Security Problems
(% Responding a Serious or Very Serious Risk)

Risk	%
Your users visiting Web sites that could introduce malware into your network	51%
A new virus, worm or Trojan that enters via email harming your network, data, etc.	41%
A new virus, worm or Trojan that enters via a mobile device harming your network, data, etc.	39%
A new virus, worm or Trojan that enters via instant messaging harming your network, data, etc.	29%

2. BEHAVIOR AND STRUCTURAL PROPERTIES OF MALICIOUS CODE

Malicious codes at present are detected primarily by syntactic signature [3]. These are basically byte sequences that are characteristics of a particular malware instance. This technique requires frequent updates of the signature database when some previously unknown sample is found this makes the technique quite vulnerable. The metamorphic nature of the malware enables the malware code to mutate while spreading across the network making the detection using signature completely ineffective.

A rootkit may be considered as a collection of tools often used by a attacker after gaining administrative privileges on host. Rootkit focuses on background program and tools to hide the attacker from system administrator. The latest in this category of rootkit are the ones which are implemented as loadable kernel module (LKMs). These loadable kernel modules are part of the operating system which can be loaded and unloaded at runtime. These kernel rootkit takes over the entries in the system call table and provide modified implementation of corresponding system call function [4][5]. These modified system call often perform checks and can easily hide information about files and processes. The `adore-ng` rootkit [6][7] do not modify the system call table, but it takes over routines used by virtual file system and hence able to intercept calls that access files in both the /proc file system and root file system.

On the other hand polymorphic code has the ability to change its binary representation as a part of replication process. This is achieved by self-encryption techniques. As a result, copies of polymorphic malware often no longer share a common substring which can be used for detecting signature.

These behavior and structural properties are important to analyze as it can be effectively used to detect and abort loading and execution of these rootkit. In case of kernel modules, malicious behavior is defined as write to forbidden regions in the kernel each of the kernel modules is statically analyzed using symbolic execution so that when an illegal write is detected it is identified as kernel rootkit module and hence loading aborted.
In case of polymorphic worms, graph isomorphic test can be performed which enables to identify identical structure that appears in different executables. If same structure is identified in connection from multiple source hosts to multiple destinations, this structure is considered to be a worm.

3. MALWARE DESIGN TRENDS

It is very important to anticipate in prior how these malware are going to be more destructive in different forms in near future in order to develop mechanism to tackle then in prior. Nazario et al. [8] identifies two categories of evolution of malware: improved protection and organization between nodes. Improved protection includes the usage of techniques such as rootkit or covert channels. Whereas for organized behavior of the nodes, author describes different organizational groupings of infected systems to increase their co-ordination and reduce their chance of being discovered and stopped by network administrator. Zou et al [9] describes new kind of malware that use routing table information to only scan the internet routing table information to scan the internet routing address space.

The scope of improvement of the malware can be categorize into first use of better malware strategy i.e. the agents which are more target specific and secondly better malware codes which can have the capability of decision making using artificial

Publication of Little Lion Scientific R&D, Islamabad PAKISTAN
Journal of Theoretical and Applied Information Technology
31st July 2011. Vol. 29 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

intelligence , data mining or machine learning. However the perfect breeding ground of such malware is still the internet. Internet is already being attacked by a variety of malware and hackers that generates high volumes of malicious traffic. So, it would be relatively easy for the malware creator to hide the whole optimization process. Thus malware can be created which can study the firewall or IDS system for kind of check up they make and then to modulate itself in a manner untraceable by such firewall or IDS.

Thus to tackle such variants of malware a perfect strategy development of the defense mechanism would be necessary which can always be one step ahead of the malware variations and detect them at the earliest and block all its possible different forms. The secure flow analysis has the potential to guarantee strong security properties in computer software. The possible future forms of the malware can be intelligent worms, modular and upgrading worms, Warhol and flash worm, polymorphic worm and jumping executable worms.

4. LATEST ATTACK MODELS

Today's malwares can be characterized as more powerful and destructive than ever. They take full control over infected host and network connection, blocks known firewalls, eliminates rival malware, encrypts host data and asks for ransom and generates revenue for its authors. They are no more just for fun or intellectual exploration; they are now monetized. Latest malware attacks can be of following categories:

Social Networks Malware:

With the increasing popularity of social networking sites like Facebook, Orkut etc. a lot of attacks are going through them. For example a message containing a link can be sent to a Facebook or Orkut user. After clicking on the link the user is taken to a website that is similar to YouTube and he will be prompted to download the latest version of Flash Player to view the video. The user clicks to install the update, but actually installs a piece of malware on the machine. The authors of this malware are likely to generate revenue from installations or purchases of these products.

Botnets:

"Compared with viruses and spam, botnets are growing at a Faster rate", said Wenke Lee [10], a leading botnet researcher. Lee cites three primary factors that are spurring botnet growth:

- Infection can occur even through legitimate websites.
- Bot malware delivery mechanisms are gaining sophistication and better obfuscation techniques.
- Users no need to do anything to become infected; simply rendering a webpage can launch a botnet exploit.

Once installed, bots actually become bot armies that engage in a variety of malicious activities like data theft, Denial of service attacks, spam delivery, DNS server spoofing etc.

VOIP attacks:

Another trend in malware attack is through VOIP technologies. The cell phone is becoming a common tool for accessing Internet and cyber criminals are paying close attention to it. Attackers are using them to engage in voice fraud, data theft and other scams similar to the problems e-mail has experienced in the past.

Pay-Per-Click-Hijacking [11] :

Pay-Per-Click-Hijacking is a fully realistic practice these days. For example, an SDBOT variant [12] detected by Eric at the MalwareBlog.com, is a suitable example of how malware is able to automatically generate revenue, vote, or count as a visit.

5. LATEST MITIGATION STRATEGIES

Broadly the mitigation strategies can be divided in following categories depending upon the type of malware attack and its variation:

Signature based Detection

Signature-based detection is primarily based on pattern matching. A dictionary of known fingerprints is used and run across a set of input. This dictionary typically contains a list of known bad signatures, such as malicious network payloads or the file contents of a worm executable. This database of signatures is the key to the strength of

Publication of Little Lion Scientific R&D, Islamabad PAKISTAN
Journal of Theoretical and Applied Information Technology
31st July 2011. Vol. 29 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the detection system, and its prowess is a direct result of its speed. Three main types of signature analysis for worm detection are network payload signatures, as is used in network intrusion detection systems second type of signature matching is based on logfile analysis. The third type of signature detection is the most popular method, file signatures. File payloads of worms and their executables are typically monitored using host-level antivirus products.

Host based defenses

Host-based firewalls may be considered as an appropriate solution for defending a set of hosts. Host-level firewalls are available in two major types. The first is a traditional firewall with statically configured rules. The second type of popular host-based firewall is one that dynamically adapts to the user's network use. Often called the personal firewall, these systems query the user to determine what applications are in use on the system

Firewall and malware defenses

Firewalls are devices that enforce a network security policy. This policy can be the authorization to establish communications between two endpoints, controlled by the ports, applications, and protocols in use. The firewall evaluates connection requests against its rule base and applies a decision to the requested action [13]. Most firewalling devices are of two basic types. The first is a packet filter, which performs policy enforcement at the packet level [14]. A second type of firewalling device, a network proxy, performs its decision at the application layer. These devices have additional potentials for security applications.

Proxy based defences

Proxy server is a yet another kind of firewall. Proxy servers, or application gateways, provide their services by being an intermediate system for a network connection. A listening agent on the proxy server receives a request for a network action and, on behalf of the client, fulfils the request. The biggest benefit for the detection and prevention of network-based attacks is the role application gateways play in network architecture.

However, these known threat detection mechanisms have become less effective with the advent of the "Commercial" malware market. For instance Botnet worm infections can occur even when the impacted organization has the very latest antivirus (AV) signatures and is automatically pushing out OS and application patches. [15].

Today's malware uses multiple methods to hide and disguise itself making detection and mitigation very difficult. Protection from these growing threats requires multiple layers of defenses. One approach to combat malware is to use a virtual environment within a network device or host agent [16]. This can enable the security device to determine the behavior of malware that is plucked off the network once it is allowed to run in this safe environment. Based on the captured malware's behavior, the source IP address is then added to a known "bad-actor" database.

Another approach to mitigate malware attack is to work with companies that offer malware threat intelligence services. These services may be building and maintaining databases of suspicious IP addresses and identifying active agents in malware organizations.

6. CONCLUSION

The Internet as a growing force shaping our ways of thinking and living is as useful, as easy to exploit as well. The clear growth in E-commerce, today's opensource nature of malware, the growing penetration of the Internet in respect to insecure connected PCs, are among the main driving factors of the scene. Organizations should adopt a multi-layered Web defense strategy that can protect their users and networks from increasingly sophisticated threats. Key elements of this strategy include community-watch monitoring of Web traffic using a cloud-based service, protection of remote clients, and real-time inputs from Web gateways and clients for background analysis to detect malware, rate reputations and analyze Web content. In this paper we have discussed about different issues related to malware starting first from the structural properties of the malware and its behavior which is necessary for analysis so as to able to defend them. Then we have taken up the most important issue regarding the latest design trend and how the attack model of the malware has evolved. The different attack models of the malware have been discussed so as to find out best mitigation strategy depending on the type of attack. At the end we have discussed about the latest mitigation strategies which can detect the malware, we have talked about the latest techniques which are being used for the mitigation.

Publication of Little Lion Scientific R&D, Islamabad PAKISTAN
Journal of Theoretical and Applied Information Technology
31st July 2011. Vol. 29 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFERENCES:

[1] Malware threats and mitigation strategies: US-CERT informational whitepaper.

[2] Protecting against the new wave of malware: An osterman research white paper.

[3] Mihai Christodorescu, Somesh Jha, Douglas Maughan, Dawn Song, Cliff Wang: Malware Detection,Springer.

[4] T.Miller. Analysis of the KNARK Rootkit. http://www.ossec.net/rootkits/studies/knark.txt, 2004

[5] Stealth, adore, http://spider.scorpions.net/~stealth, 2001.

[6] Stealth. Kernel Rootkit Experiences and the Future.*Phrack Magazine, ll{()\),August* 2003.

[7] Stealth, adore-ng. http://stealth.7350.org/rootkits/, 2004.

[8] J. Nazario, J. Anderson, R. Walsh, and C. Connelly.The future of Internet worms. Technical report, Crimelabs Research, July 2001.

[9] C. C. Zou, D. Towsley, W. Gong, and S. Cai. Routing worm: A fast, selective attack worm based on IP address information. In Proc. IEEE Work. on Princ. Adv. and Dist. Simul. (PADS), pages 199–206, 2005.

[10] Georgia Tech Information Security Centre, "Emerging Cyber Threats".

[11] http://www.lurhq.com/ppc-hijack.html

[12] http://www.malwareblog.com/?p=164

[13] Wack, J., K. Cutler, and J. Pole, "Guidelines on Firewalls and Firewall Policy: Recommendations of the National Institute Of Standards and Technology," 2001.

.

[14] Chapman, D. B., "Network (In)Security Through IP Packet Filtering," *Proc. UNIX Security Symposium III*, Baltimore, MD, 1992, pp. 63–76.

[15] Malware Threats and Mitigation Strategies (US-CERT informational Whitepaper)

[16] http://insight.accuvant.com – Malware Mitigation Trends