Cybercrime: The Case of Obfuscated Malware

Mamoun Alazab[1], Sitalakshmi Venkatraman[1], Paul Watters[1],
Moutaz Alazab[2], and Ammar Alazab[2]

[1] Internet Commerce Security Laboratory
School of Science, Information Technology and Engineering
University of Ballarat, Australia
{m.alazab,s.venkatraman,p.watters}@ballarat.edu.au
[2] School of Information Technology
Deakin University, Australia
{malazab,aalazab}@deakin.edu.au

Abstract. Cybercrime has rapidly developed in recent years and malware is one of the major security threats in computer which have been in existence from the very early days. There is a lack of understanding of such malware threats and what mechanisms can be used in implementing security prevention as well as to detect the threat. The main contribution of this paper is a step towards addressing this by investigating the different techniques adopted by obfuscated malware as they are growingly widespread and increasingly sophisticated with zero-day exploits. In particular, by adopting certain effective detection methods our investigations show how cybercriminals make use of file system vulnerabilities to inject hidden malware into the system. The paper also describes the recent trends of Zeus botnets and the importance of anomaly detection to be employed in addressing the new Zeus generation of malware.

Keywords: Cybercrime, Obfuscation, Malware, Intrusion Detection.

1 Introduction

In the context of crime-ware, malicious code is the most valuable resource to perform unauthorized access by cybercriminals [1]. Malicious software (Malware) attackers are taking advantage of our increased reliance on digital systems, available digital resources, and increased connectivity and activity through Internet. On one hand, technology advancements have resulted in home computers featuring 1 Terabyte (TB) of storage that are now available for purchase. On the other hand, sophistication in malware offers a new class of criminal activity that has created new challenges for law and forensic examiners [2]. Current threats [3] posed to organizations by cybercrimes continue to aggressively hunt and develop new techniques to steal money and credential information.

A review of the history of malware and anti-malware reports [2] [3] [4] and predictions [5] show a continuous growth thriven in sophistication over the years, and traditional malware detections appear insufficient to tackle increasingly sophisticated malware. Therefore, the detection of malware is not only of interest

H. Jahankhani et al. (Eds.): ICGS3/e-Democracy 2011, LNICST 99, pp. 204–211, 2012.

to researchers but is also a major concern to the general public. Malwares are designed to perform illegal activities being designed more for financial gains, leading to a huge impact against individuals, organisations and business assets. Recent trends in malware for such malicious and illegal purposes indicate increasing complexity and are evolving rapidly as systems provide more opportunities for more automated activities of late. Hence, the damages caused by malware to individuals and businesses have dramatically increased in 2010 [3], [5].

In this paper we perform investigations on the obfuscated techniques used in the malicious code, and illustrate with recent trends in exploits that use file system vulnerabilities including Zeus botnets.

The remainder of this paper is organized as follows. In Section 2, we discuss the malicious code growth in the wild. We describe the recent trends in cybercrime attacks in Section 3. We discuss and investigate the recent obfuscation techniques that are used in malicious code, in Section 4. We also discuss new threats, in particular feature the Zeus as a case study. Finally, Section 5 provides a summary.

2 Malicious Code Growth

The current situation is that known malware can be recognized by all the popular anti-malware engines. Malware detection usually occurs in an online system and the anti-virus (AV) software forms the primary tool for the defense against malware. However, cybercriminals continually develop new techniques for creating malware that cannot be detected leading to what is known as a 'zero-day-attack'. In other words, once new malicious code is released, the detection engines will have to update their signatures in order to detect and combat the new malicious code. Though the quality of such malware detectors is improving in their techniques from virus signature-based detection towards heuristic-based detection, the malware cybercriminals are one step ahead [1] of the AV engines and anti-forensic methods adopted. The present malware detection systems usually rely on existing malware signatures with limited heuristics and are unable to detect those malware that can hide itself during the scanning process in online systems [8].

In general, countermeasures such as AV engines must perform 3 main tasks to provide protection to systems: Scanning, Detection, and Removal. As shown in the *equation* below a Malware detector MD is defined as a function to determine if an executable program (file) is malicious or benign MD: p ? malicious, benign. Modern and traditional anti-malwares scan the files in a system for a byte sequence or malware signature(s) that are stored in the database engine. Current live malware detection tools such as anti- malware software are able to identify known malware, therefore, cybercriminals are continually developing new techniques for creating malware that are not detectable by AV engines. Once new malware is released, the AV engines will reactively update their signatures to combat the new malware. However, recent methods adopted by computer intruders, cybercriminals and malware are to target hidden and deleted data so that they could evade from virus scanners. As a result, some malware adopt

circumvention techniques such as polymorphic and metamorphic obfuscations so that they cannot be detected through current live analysis techniques.

$$MD(P) = \begin{cases} Malware & if S \in p \\ Benign & otherwise \end{cases} \quad (1)$$

Creating and producing malicious code is not done only by malware writers, but there are also in the market, malicious software kit vendors [9] such as Zeus, exploit kits, Flesta, MyPolySploit, Limbo2 and SpyEye, snd these kits are used to create highly effective malware. These kits serving as new offsprings of malware have caused serious threats and major problems. The new market for malware creation software on-sale is widely available on the internet and can be found easily using Google and other search engines. Apart from purchasing these kits, one could also buy the updates for the kit to ensure and guarantee it is a reliable business. Likewise, cybercriminals are being purchased in underground markets with even after sales services and guaranteed effectiveness of evading security countermeasures offered. As a result, cybercriminals update the construction kits to suit the needs of their client base to stay ahead of their contenders. Malicious software kit vendors or 'crime ware' is being offered for sale on underground trading forums and IM for negotiation.

> "Full ZeuS Souurce code of last v2.0.8.9 (includes everything). Requires MSVC++ 2010. You can create your own HWID licenses and much more."

According to the Internet Crime Complaint Center $(IC3)^2$ in 2010 malicious codes are evolving rapidly. For instance, a study conducted by University of Maryland?shows?that on an average, a?computer?connected to?the?Internet? may experience an attack every 39 seconds [10]. Equally important in the first quarter of 2010, another experiment conducted by the San Diego Supercomputer Center (SDSC) shows that an average of 27,000 hacking attempts were made per day. Similarly, when PSINet Europe purposely built an unprotected server and connected it to the internet their results were staggering: in the first 24 hours and the server was maliciously attacked 467 times [11]. More recently, these figures have grown exponentially [3], [5].

Types of malware such as worms, rootkits viruses, script viruses, trojans, macro viruses, backdoors, spyware, key loggers, etc. are being recycled [12] to produce new variants of old malware. In 2006, BitDefender Antivirus [12] published that it had over 270 thousand malware signatures in its database. Symantec Internet Security threat published report in 2010 [13] announced that malicious code activity continues to grow at a record pace, and there are over 2.8 million new malicious code signatures, mostly developed in 2009. Other sources show the infection rates through experiments performed by Kaspersky Labs that identified almost 120 million servers in the first quarter of 2010 of which 0.64% was malicious [9]. Recently, McAfee Labs [5] identified almost 60,000 new pieces of malware per day and this shows the sophistication in malware is getting more

difficult to detect and that cybercriminals are engaging in a growing number of targeted attacks.

3 Cybercrime

In many ways, cybercrime is no different than traditional crime [6]. Both crimes are involved in identifying targets, using surveillance and psychological profiling. The major difference is that the perpetrators of cybercrime are increasingly remote to the scene of the crime [7]. The traditional idea of a criminal gang loses its meaning as members can now reside on different continents without ever having to actually meet.

In this 21st Century, a bank robber does not require a gun, a mask, a note, or a getaway car. Data has become more valuable than money. Hence, accessing bank data gives cybercriminals repeated access to the money. Research studies relating to credit card fraud detection has steadily increased over the recent years [5] [10] [11] [12] [13] [14]. Moreover, use of botnets, VOIP and mobile SMS in attacks are expected to rise. Globally, 30,000 phishing attacks are reported each month and at least 3% of phishing attempts are successful. Although phishing alone is not directly responsible for all online banking fraud, Singh (2007)'s statistics indicates that 900 online bank accounts get compromised each month from phishing alone. In general, online banking fraud includes all unauthorized transactions conducted without the legitimate account holder's knowledge and (usually) resulting in loss of funds from the account.

4 Obfuscated Malicious Code Types

Criminals today have sophisticated service providers and high-tech expertise to fully take advantage of their current targets. Furthermore, the exploit servers used can be changed to avoid detection and countermeasures.

4.1 Polymorphic Malware

Anti-malware vendors are confronting a serious problem of defeating the complexity of malwares. Polymorphic malware uses encryption and data appending/ data pre-pending in order to change the body of the malware, and further, it changes decryption routines from infection to infection as long as the encryption keys change, making it very difficult to create antivirus signatures to block infections. Crime-ware tool kits such as CRUM Cryptor Polymorphic, PoisonIvy Polymorphic Online Builder and Mariposa, use polymorphic code and obfuscation techniques to avoid detection, and are available on black-market for a price range $50-10000$ depending on the features included. As result, this will lead to anti-malware experts to develop different scanning techniques from simple byte sequence matching to combine of the difficulty of antivirus engines to block it and its numerous propagation techniques. In early 2011, Symantec Internet Security

Threat Report stated that detecting polymorphic malware such as w32.Polip and w32.Detnat is much more difficult and complex than any other type of Malware. The use of simple virus scanners has made this type of obfuscation prolific and continues to pose a major threat [14].

4.2 Metamorphic Malware

Metamorphic malware changes the code itself without the need of using encryption. In general, there are four techniques commonly used for metamorphic obfuscation. These are, i) Dead-code Insertion which is meant to do nothing such as a sequence of NOPs (No Operation Performed), ii) Code Transposition that changes the instructions such as using JMP instructions so that the order of instructions is different from the original one, iii) Register Reassignment such as replacing push ebx with push eax to exchange register names, and iv) Instruction Substitution which replaces the instructions with different instructions that have the same result, and some authors use a database dictionary of equivalent instruction sequences to make the replacement easier and faster.

4.3 Packer

Packers are commonly used today for code obfuscation or compression. Packers are software programs that could be used to compress and encrypt the PE in secondary memory and to restore the original executable image when loaded into main memory (RAM). Cybercriminals do not need to change several lines of code to change the malware signature mainly because, changing any byte sequence in the PE results in a new different byte sequence in the newly produced packed PE. For instance, Themida (`www.oreans.com`), Obsidium (www.obsidium.de), ASPack (`http://www.aspack.com`) and Armadillo (`www.siliconrealms.com`) are all commonly used packers and malicious code authors are using such packers to produced new codes. Packers have the essential features of reducing the size of malware, making malware easier to transfer, and thereby producing malware more resistant to static analysis. Hence, packers being able to bypass detection engines have become the most favorite toolkits.

4.4 File System Vulnerabilities

Cybercriminals make use of file system vulnerabilities in order to infect more computers and guarantee effectiveness of evading security countermeasures. For instance, keeping the last modified date of an infected file unchanged to make it seem like it was uninfected was one of the first early techniques cybercriminals had adopted to thwart detection. Cybercriminals target a hidden area on the system structure to hide the malware. Since NTFS is predominantly used in most computer systems, and malware cybercriminals take advantage of NTFS weaknesses to hide malware, more computers get infected without being detected by commercial detection engines. They are capitalizing on the vulnerabilities of

NTFS to hide the malware from AV engines and further exploit the weaknesses of the present digital forensic techniques from being detected. From a preliminary investigation we had conducted on the hidden data of the $Boot file [2], we observe that a variety of tools and utilities have to be adopted along with manual inspections to identify unseen malware. It takes an enormous amount of time to analyse the data derived with such tools and most of the existing tools are complex and not easy to use. Moreover, not all computer infections are detected by forensic tools, especially intrusions that are in the form of hidden data in the $Boot file go unchecked. Hence, our study reveals that the existing forensic tools are not comprehensive and effective in identifying the recent computer threats that use obfuscated malware.

NTFS, Windows NT's native file system, is designed to be more robust and secure than other Microsoft file systems. The key feature to note in NTFS disk structure is that the Master File Table (MFT) contains details of every file and folder on the volume and allocates two sectors for every MFT entry. Since the Windows operating system does not zero the slack space, cybercriminals make use of MFT to hide malicious code without raising any suspicion. Our investigations have revealed that such limitations in NTFS have led to cybercriminals using different techniques such as disguising file names, hiding attributes and deleting files to intrude the system.

5 Case Study: The Zeus Botnet

The Zeus Trojan, a financial malware Zeus botnet, is a well-known banking Trojan also called Zbot, NTOS, WSNPOEM, or PRG, and forms the king of financial malware 'in wild', both in terms of infection size and effectiveness. Furthermore, it is the biggest and most sophisticated threat to internet security and to most of the detection engines such as Symantec and McAfee. The Zeus Trojan estimated to be responsible for about 90% of banking fraud worldwide [5] and found guilty in 44% of the banking malware infections [15]. Symantec Corporation describes it as "*Zeus, King of the Underground Crimeware Toolkits*".

The Zeus Trojan software with a friendly interface toolkit that is available in underground online forums for $1,500-20{,}000$US is causing a serious problem because it enables cybercriminals to configure and create malicious software to affect user systems, allowing them to take control of a compromised computer, harming the data, logging keystrokes, and executing unauthorized transactions in online banking. The name Zeus has created a panic in the world of computers and security experts today. Reports and studies [5] [12] [13] [14] show that since last year Zeus has been found embroiled in more than half of the banking malware infections in the world.

The Zeus Trojan carries a very light footprint and is designed to steal sensitive data stored on computers or transmitted through web browsers and protected storage. Once infected, the computer sends the stolen data to a bot command and control (C&C) server via encrypted HTTP POST requests, where the data is stored. Also, it allows cybercriminals to inject content into a bank's web page

as it is displayed in the infected computer browser in real time. It is setup such that the stolen data is sent to a "drop server" controlled by an attacker called a botmaster and it allows cybercriminals to control the infected systems remotely. Moreover, Zeus is highly dynamic and applies obfuscation methods such as polymorphic encryption and metamorphic in a network of bots. In each infection, it re-encrypts itself automatically to create a new signature to defeat signature-based detection. Thus, Zeus poses a threat as it can successfully evade commercial detection engines and is able to hide malicious features such as string and API function calls. Zeus is still evolving with new plugin releases that can infect even latest operating systems such as Windows 7.

According to numerous research labs and hacker forums, the ZeuS botnet recently has combined [5] [16] [17] with the new release of 2010 'SpyEye Trojan' source codes to create more sophisticated bots and takes the new threat to a new level. This new toolkit is being reported that it is currently available for purchase in the underground market and version 1.4.1 has been published on January 11, 2011 [17]. The new version of the combination has two versions of a control panel used for committing fraud and managing compromised systems. These trends indicate that self-learning and self-updating by observing system anomalies and behavior patterns is much warranted in malware detection systems of the future [18].

6 Summary

Overall observation is that malicious code authors are producing unique threats using different obfuscation methods, and signature-based detection is of little defense to our present computing environments and such traditional anti-virus techniques are rapidly becoming obsolete. Therefore, Anomaly Detection (AD) should be more explored and used than signature-based detection since it has many limitation and proven inability against the new threats. Also, we believe that anamoly-based detection methods are required to be adopted to detect Zeus botnets and malicious activities that are increasing exponentially since the start of this year.

Cybercriminals are leveraging innovation at a pace to target many organizations that ecurity vendors cannot possibly match. Effective deterrents to cybercrime are not known, available, or accessible to many practitioners, many of whom underestimate the scope and severity of the problem. In our view the key for fast speed in malware growth is the lack of understanding of the various types of hidden malware and their capabilities to exploit file system vulnerabilities. Security breaches are increasing in frequency and sophistication. Through a preliminary investigation conducted in this research work, we have illustrated the abovementioned attacking trend with a view to identify the various behavior of hidden malicious code that could be categorized as distinct malware types. This paper has also identified and described Zeus botnet as the start of a new generation of malware and has highlighted the importance of anomaly detection to combat Zeus.

References

1. Herrera-Flanigan, J.R., Ghosh, S.: Criminal Regulations. In: Ghosh, S., Turrini, E. (eds.) Cybercrimes: A Multidisciplinary Analysis, pp. 265–308. Springer, Heidelberg (2010)
2. Alazab, M., Venkataraman, S., Watters, P.: Effective digital forensic analysis of the NTFS disk image. Ubiquitous Computing and Communication Journal 4, 551–558 (2009)
3. RSA: The Current State of Cybercrime and What to Expect in 2011. RSA 2011 cybercrime trends report (2011)
4. Venkatraman, S.: Autonomic Context-Dependent Architecture for Malware Detection. In: Proceedings of International Conference on e-Technology, International Business Academics Consortium, Singapore, pp. 2927–2947 (2009)
5. Alperovitch, D., Dirro, T., Greve, P., Kashyap, R., Marcus, D., Masiello, S., Paget, F., Schmugar, C.: McAfee Labs - 2011 Threats Predictions. McAfee, Inc. (2011)
6. Jahankhani, H., Al-Nemrat, A.: Global E-Security. Communications in Computer and Information Science. In: Jahankhani, H., Revett, K., Palmer-Brown, D. (eds.) ICGeS 2008. CCIS, vol. 12, pp. 3–9. Springer, Heidelberg (1974)
7. Jahankhani, H., Al-Nemrat, A.: Examination of Cyber-criminal Behaviour. International Journal of Information Science and Management, 41–48 (2010)
8. Alazab, M., Venkataraman, S., Watters, P.: Towards Understanding Malware Behaviour by the Extraction of API Calls. In: Second Cybercrime and Trustworthy Computing Workshop, pp. 52–59. IEEE Computer Society, Victoria (2010)
9. Komisarczuk, P.: Web Attack: WHO ARE WE FIGHTING? Dealing with threats is one thing, finding them is another. The manazine of the BSC security forum, ISNOW (Autumn 2010)
10. Cukier, M.: Study Documents Rate, Nature of Hacker Attacks. IT Pro. (2007)
11. Daniel, J.: Internet Security - the Threats Are Very Real. Educators' eZine (2007)
12. BitDefender Antivirus Technology, white paper (2010), `http://www.bitdefender.com/files-/Main/file/BitDefender_Antivirus_Technology.pdf`
13. Symantec Enterprise Security: Symantec Global Internet Security, Security Threat Report, Trend for 2009, vol. XV (2010)
14. Symantec Enterprise Security: Symantec Report on Attack Kits and Malicious Websites. White paper (2011)
15. Banking malware zeus sucessfully bypasses anti-virus detection (2011), `http://ecommerce-journal.com/news/18221_zeus_increasingly_avoids_pcs_detection`
16. SPAMfighter News: Seculert Finds Fresh Malware Combining Zeus And SpyEye (2011), `http://www.spamfighter.com/Seculert-Finds-Fresh-Malware-Combining-Zeus-And-SpyEye-15773-News.htm`
17. SPAMfighter News: Alliance of ZeuS-SpyEye Resulting in the Publication of First Toolkit in the Underground Market (2011), `http://www.spamfighter.com`
18. Venkatraman, S.: Self-Learning Framework for Intrusion Detection. In: Proceedings of The 2010 International Congress on Computer Applications and Computational Science (CACS 2010), Singapore, pp. 517–520 (2010)