EXHIBITING AND REVEALING OF CAMOUFLAGING WORM

B.V.M.G.KARTHIK, C. JOTHI KUMAR

Abstract : Active worms cause major security threats to the Internet. This is due to the ability of active worms to propagate in an automated fashion as they continuously compromise computers on the Internet. Active worms evolve during their propagation and thus pose great challenges to defend against them. New class of active worms is investigated, referred to as Camouflaging Worm (C-Worm in short). The C-Worm is different from traditional worms because of its ability to intelligently manipulate its scan traffic volume over time. Thereby, the C-Worm camouflages its propagation from existing worm detection systems based on analyzing the propagation traffic generated by worms. Novel spectrum-based scheme can be used to detect the C-Worm. Power Spectral Density (PSD) distribution of the scan traffic volume and its corresponding Spectral Flatness Measure (SFM) can be used to distinguish the C-Worm traffic from background traffic. I determine the performance evaluation metrics and it is used to analyze the system.

Introduction : An active worm refers to a malicious software program that propagates itself on the Internet to infect other computers. The propagation of the worm is based on exploiting vulnerabilities of computers on the Internet. Many real-world worms have caused notable damage on the Internet. These worms include "Code-Red" worm in 2001, "Slammer" worm in 2003, and "Witty"/"Sasser" worms in 2004. Many active worms are used to infect a large number of computers and recruit them as bots or zombies, which are networked together to form botnets. These botnets can be used to: (a) launch massive Distributed Denial-of-Service (DDoS) attacks that disrupt the Internet utilities, (b) access confidential information that can be misused through large scale traffic sniffing, key logging, identity theft etc, (c) destroy data that has a high monetary value, and (d) distribute large-scale unsolicited advertisement emails (as spam) or software (as malware). There is evidence showing that infected computers are being rented out as "Botnets" for creating an entire black-market industry for renting, trading, and managing "owned" computers, leading to economic incentives for attackers. Researchers also showed possibility of "super-botnets," networks of independent botnets that can be coordinated for Due to the substantial damage caused by worms in the past years, there have been significant efforts on developing detection and defense mechanisms against worms.

Active worms are similar to biological viruses in terms of their infectous and self-propagating nature. They identify vulnerable computers, infect them and the worm-infected computers propagate the infection further to other vulnerable computers. In order to understand worm behavior, I first need to model it. With this understanding, effective detection and defense schemes could be developed to mitigate the impact of the worms. For this reason, tremendous research effort has focused on this area. Active worms use various scan mechanisms to propagate themselves efficiently. The basic form of active worms can be categorized as having the Pure Random Scan (PRS) nature. In the PRS form, a worm-infected computer continuously scans a set of random Internet IP addresses to find new vulnerable computers. Other worms propagate themselves more effectively than PRS worms using various methods, e.g., network port scanning, email, file sharing, Peer-to-Peer (P2P) networks, and Instant Messaging (IM). In addition, worms use different scan strategies during different stages of propagation. In order to increase propagation efficiency, they use a local network or hit list to infect previously identified vulnerable computers at the initial stage of propagation. They may also use DNS, network topology and routing information to identify active computers instead of randomly scanning IP addresses. They split the target IP address space during propagation in order to avoid duplicate scans.
A network based worm detection system plays a major role by monitoring, collecting, and analyzing the scan traffic (messages to identify vulnerable computers) generated during worm attacks. I conduct a systematic study on a new class of such smart-worms denoted as Camouflaging Worm (C-Worm in short). The C-Worm is quite different from traditional worms in which it camouflages any noticeable trends in the number of infected computers over time. The camouflage is achieved by manipulating the scan traffic volume of worm-infected computers. I comprehensively analyze the propagation model of the C-Worm and corresponding scan traffic in both time and frequency domains. The above recurring manipulations involve steady increase followed by a decrease in the scan traffic volume, such that the changes do not manifest an any trends in the time domain or such that the scan traffic volume does not cross thresholds that could reveal the C-Worm propagation. Based on the above observation, I adopted frequency domain analysis techniques and develop a detection scheme against wide-spreading of the C-Worm. Particularly, I

develop a novel spectrum-based detection scheme that uses the Power Spectral Density (PSD) distribution of scan traffic volume in the frequency domain and its corresponding Spectral Flatness Measure (SFM) to distinguish the C-Worm traffic from non worm traffic (background traffic).

1.1 OBJECTIVE

The main objective is to Modeling and Detection of Camouflaging Worm (C-Worm)

1. Design a Spectrum Based Scheme to capture the distinct pattern of the C-Worm in the frequency domain .
2. The Power Spectrum Density is used to identify the C-worm propagation in frequency domain. The PSD describe how the power of time series is distributed in the frequency domain .
3. The spectral Flatness Measure is defined as ratio of geometric mean to arithmetic mean of coefficient of PSD

1.2 EXISTING SYSTEM

Existing detection schemes are based on a tacit assumption that each worm-infected computer keeps scanning the Internet and propagates itself at the highest possible speed. Furthermore, it has been shown that the worm scan traffic volume and the number of worm-infected computers exhibit exponentially increasing patterns.

Nevertheless, the attackers are crafting attack strategies that intend to defeat existing worm detection systems. In particular, 'stealth' is one attack strategy used by a recently-discovered active worm called "Attack" worm and the "self-stopping" worm circumvent detection by hibernating (i.e., stop propagating) with a pre-determined period. Worm might also use the evasive scan and traffic morphing technique to hide the detection.

Limitations of Existing System:

The issues in existing system are Existing worm detection schemes will not be able to detect such scan traffic patterns, it is very important to understand such smart-worms and develop new countermeasures to defend against them.

1.3 Proposed System

Proposed Worm detection schemes that are based on the global scan traffic monitor by detecting traffic anomalous behavior, there are other worm detection and defense schemes such as sequential hypothesis testing for detecting worm-infected computers, payload-based worm signature detection.

In presented both theoretical modeling and experimental results on a collaborative worm signature generation system that employs distributed fingerprint filtering and aggregation and multiple edge networks.

In presented a state-space feedback control model that detects and control the spread of these viruses or worms by measuring the velocity of the number of new connections an infected computer makes. Despite the different approaches described above, I believe that detecting widely scanning anomaly behavior continues to be a useful weapon against worms, and that in practice multifaceted defense has advantages.

Advantages of Proposed System:

Worm detection schemes that are based on the global scan traffic monitor by detecting traffic anomalous behavior, there are other worm detection and defense schemes such as sequential hypothesis testing for detecting worm-infected computers, payload-based worm signature detection. I believe that detecting widely scanning anomaly behavior continues to be a useful weapon against worms, and that in practice multifaceted defense has advantages.

Literature Survey

2.1 Modeling the Spread of Active Worms

- When an active worm is fired into the Internet, it simultaneously scans many machines in an attempt to find a vulnerable machine to infect. When it finally finds its prey, it sends out a probe to infect the target. If successful, a copy of this worm is transferred to this new host.
- This new host then begins running the worm and tries to infect other machines. When an invulnerable machine or an unused IP address is reached, the worm poses no threat.
- A patch, which repairs the security hole of the machines, is used to defend against worms. When an infected or vulnerable machine is patched, it becomes an invulnerable machine.
- To speed up the spread of active worms, I presented the "hitlist" idea. It uses these infected machines as "stepping stones" to search for other vulnerable machines.
- The Analytical Active Worm Propagation (AAWP) model, which captures the characteristics of the spread of active worms and explains the aforementioned "mystery" to some extent.
- The AAWP model can be used to simulate the Code Red v2 worm with the following parameters: 500,000 vulnerable machines, starting on a single machine, a scanning rate of 2 scans/second, a death rate of 0.00002 /second, a patching rate of 0.000002 /second, and a time period of 1 second to complete infection.
- An address space of more than 218 unused IP addresses is needed by LaBrea to defend against the Code Red v2 like worm effectively. This model to understand the spread of active worms using local subnet scanning.

2.2 Traffic Morphing: An Efficient Defense Against Statistical Traffic Analysis

- The identities of web pages can be inferred by examining the sizes of packets within an encrypted HTTP connection.
- Packet lengths of encrypted Voice over IP (VoIP) calls can leak information about the languages being spoken.
- Through the use of convex optimization techniques, I show how to optimally modify packets in real-time to reduce the accuracy of a variety of traffic classifiers
- Here I are padding the packets to uniform sizes and to send packets at fixed timing intervals
- The goal of traffic morphing is to provide users who encrypt their network data with an efficient method of preventing information leakage that induces less overhead than deterministic padding.
- This morphing method just reduces the accuracy of the VoIP classifier and the web page classifier.

2.3 Monitoring and Early Detection for Internet Worms

- A simple self-propagating worm can quickly spread across the Internet and cause severe damage to our society.
- Facing this great security threat, I must build an early detection system to detect the presence of a worm as quickly as possible in order to give people enough time for counteractions.
- I present a non-threshold based "**trend detection -not the burst**" methodology to detect a worm at its early stage by using **Kalman filter estimation**.
- I can effectively predict the overall vulnerable population size, and estimate accurately how many computers are really infected in the global Internet based on the biased monitored data.
- Traditional threshold-based anomaly detection meth-ods try to detect a worm by detecting either the long-term or the short-term burst of monitored traffic. Thus traditional threshold-based detections usually will generate excessive false alarms.

Functional Specification

3.2 Module 1 (Pure Random Scan (Prs))

C-Worm can be extended to defeat other newly developed detection schemes, such as destination distribution-based detection. In the following, Recall that the attack target distribution based schemes analyze the distribution of attack targets (the scanned destination IP addresses) as basic detection data to capture the fundamental features of worm propagation, i.e., they continuously scan different targets

Active worms use various scan mechanisms to propagate themselves efficiently. The basic form of active worms can be categorized as having the Pure Random Scan (PRS) nature. In the PRS form, a worm-infected computer continuously scans a set of random Internet IP addresses to find new vulnerable computers.

3.3 Module 2 (Modeling Of The Code-Red Worm)

"Code Red Worm", also known as I-Worm Bady and W32/Bady worm. It is a self-replicating malicious code that exploits a known vulnerability in IIS servers. Once it has infected a system, it multiplies itself and it begins scanning random IP addresses at TCP port 80 looking for other IIS servers to infect. At the same time, the home page of infected machines will also be defaced.

The AAWP model can be used to simulate the Code Red v2 worm with the following parameters: 500,000 vulnerable machines, starting on a single machine, a scanning rate of 2 scans/second, a death rate of 0.00002 /second, a patching rate of 0.000002 /second, and a time period of 1 second to complete infection.

3.4 Module 3 (Propagation Model Of The C-Worm)

The Epidemic Dynamic model is used for analyzing propagation of C-Worm. I modified the original Epidemic dynamic formula to model the propagation of the C-Worm by introducing the P(t) the attack probability that a worm-infected computer participates in worm propagation at time 't'. Spectrum based scheme captures the distinct patterns of c-worm in the frequency domain.

$$\frac{dM(t)}{dt} = \beta \cdot M(t) \cdot P(t) \cdot [N - M(t)]..$$

That P(t) =MC/M(t) , M (t) is the estimation of M(t) at time t, and assuming that.

M (t) = (1+e) ・M(t), where 'e' is the estimation error.

Worm scan traffic volume in the open-loop control system will expose a much higher probability to show an increasing trend with the progress of worm propagation. As more and more computers get infected, they in turn take part in scanning other computers. Hence, I consider the Cworm as a worst case attacking scenario that uses a closed loop control for regulating the propagation speed based on the feedback propagation status.

3.4 Module 4 (C-Worm Detection)

I develop a novel spectrum-based detection scheme. That the C-Worm goes undetected by detection schemes that try to determine the worm propagation only in the time domain. Our detection scheme captures the distinct pattern of the C-Worm in the frequency domain, and thereby has the potential of effectively detecting the C-Worm propagation. To identify the C-Worm propagation in the frequency

domain, I use the distribution of PSD (power spectral density) and SFM (spectral flatness measure) are used to detecting the c-worm. PSD used to identify the c-worm propagation in frequency domain. SFM is defined as the ratio of geometric mean to arithmetic mean of coefficient of PSD.

Particularly, PSD describes how the power of a time series is distributed in the frequency domain. Mathematically, it is defined as the Fourier transform of the auto-correlation of a time series. The SFM of PSD is defined as the ratio of geometric mean to arithmetic mean of the coefficients of PSD. The range of SFM values is [0, 1] and a larger SFM value implies flatter PSD distribution and vice versa. **DESIGN**

References

1. Moore, C. Shannon, and J. Brown, "Code-red: a case study on the spread and victims of an internet worm," in Proceedings of the 2-th Internet Measurement Workshop (IMW), Marseille, France, November 2002.
2. Moore, V. Paxson, and S. Savage, "Inside the slammer worm," in IEEE Magazine of Security and Privacy, July 2003.
3. S. Staniford, V. Paxson, and N.Weaver, "How to own the internet in your spare time," in Proceedings of the 11-th USENIX Security Symposium (SECURITY), San Francisco, CA, August 2002.
4. Z. S. Chen, L.X. Gao, and K. Kwiat, "Modeling the spread of active worms," in Proceedings of the IEEE Conference on Computer Communications (INFOCOM), San Francisco, CA, March 2003.
5. M. Garetto, W. B. Gong, and D. Towsley, "Modeling malware spreading dynamics," in Proceedings of the IEEE Conference on Computer Communications (INFOCOM), San Francisco, CA, March 2003.
6. C. Zou, W. Gong, and D. Towsley, "Code-red worm propagation modeling and analysis," in Proceedings of the 9-th ACM Conference on Computer and Communication Security (CCS), Washington DC, November 2002.
7. J. Ma, G. M. Voelker, and S. Savage, "Self-stopping worms," in Proceedings of the ACM Workshop on Rapid Malcode (WORM), Washington D.C, November 2005.
8. Min Gyyng Kang, Juan Caballero, and Dawn Song, "Distributed evasive scan techniques and countermeasuress," in Proceedings of International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA), Lucerne, Switzerland, July 2007.
9. Charles Wright, Scott Coull, and Fabian Monrose, "Traffic morphing: An efficient defense against statistical traffic analysis," in Proceedings of the 15th IEEE Network and Distributed System Security Symposium (NDSS), San Diego, CA, Febrary 2008.
10. Zou, W. B. Gong, D. Towsley, and L. X. Gao, "Monitoring and early detection for internet worms," in Proceedings of the 10- th ACM Conference on Computer and Communication Security (CCS), Washington DC, October 2003.

***

Department of Computer Science & Engineering, SRM UNIVERSITY
SRM Nagar, Kattankulathur – 603 203, Kancheepuram District