Middle-East Journal of Scientific Research 19 (9): 1142-1145, 2014
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2014.19.9.1263

Monitoring and Early Detection of Internet Worms

N. Priya

Department of Computer Science,
Bharath University Chennai, Tamil Nadu, India

Abstract: After many Internet-scale worm incidents in recent years, it is clear that a simple self-propagating worm can quickly spread across the Internet and cause severe damage to our society. Facing this great security threat, we need to build an early detection system that can detect the presence of a worm in the Internet as quickly as possible in order to give people accurate early warning information and possible reaction time for counteractions. Then, based on the idea of "detecting the trend, not the burst" of monitored illegitimate traffic, we present a "trend detection" methodology to detect a worm at its early propagation stage by using Kalman filter estimation, which is robust to background noise in the monitored data.

Key words: Internet and Cause · Counteractions · Detecting the Trend · Propagation Stage

INTRODUCTION

Since the Morris worm in 1988, the security threat posed by worms has steadily increased, especially in the last several years. Code Red appeared on July 19, 2001 which began the new wave of Internet-scale worm attacks. After that, Code Red II, Nimda, Slammer, Blaster, Sasser and Witty have repeatedly attacked the Internet and caused great damage to our society. When they observe abnormal network activities, their security experts immediately analyze these incidents.

Anomaly intrusion-detection systems usually concentrate on detecting attacks initiated by hackers. In the case of Internet worm detection, we find that we can take advantage of the difference between a worm's propagation and a hacker's intrusion attack. A worm code exhibits simple attack behaviors; all computers infected by a worm send out infection traffic that has similar statistical characteristics. Moreover, a worm's propagation in the Internet usually follows some dynamic models because of its large-scale distributed infection. On the other hand, a hacker's intrusion attack, which is more complicated, usually targets one or a set of specific computers and does not follow any well-defined dynamic model in most cases. Based on this observation, we present a new detection methodology, "*trend detection*," by using the principle "detecting monitored traffic *trend*, not *burst*". Our "trend detection" system attempts to detect the dynamic *trend* of monitored traffic based on the fact that, at the early stage, a worm propagates exponentially with a *constant*, *positive* exponential rate. The "trend" we try to detect is the exponential growth trend of monitored traffic. Based on worm propagation dynamic models, we detect the presence of a worm in its early propagation stage by using the *Kalman filter* estimation algorithm, which is robust to background noise existing in the monitored data. The Kalman filter is activated when the monitoring system encounters a surge of illegitimate scan activities. If the infection rate estimated by the Kalman filter, which is also the exponential growth rate of a worm's propagation at its early stage, *stabilizes* and *oscillates* slightly around a *constant positive* value, we claim that the illegitimate scan activities are mainly caused by a worm, even if the estimated worm infection rate is still not well converged. If the monitored traffic is caused by nonworm noise, the traffic will not have the exponential growth trend and the estimated value of the infection rate would converge to zero or oscillate around zero. In other words, the Kalman filter is used to detect the presence of a worm by detecting the *trend*, not the *burst*, of the observed illegitimate traffic. In this way, the noisy illegitimate traffic in the Internet we observe everyday will not cause too many false alarms in our detection system. We also present a formula to correct the bias in the number of infected hosts observed by a monitoring system. But neither of them has presented methods to correct it.

Corrseponding Author: N. Priya, Department of Computer Science, Bharath University Chennai, Tamil Nadu, India.

System Analysis

Problems with Existing Technologies: In recent years, people have paid attention to the necessity of monitoring the Internet for malicious activities. Symantec Corporation has an "enterprise early warning solution", which collects IDS and firewall attack data from the security systems of thousands of partners to keep track of the latest attack incidents. Internet Storm Center, which could gather the log data from participants' intrusion detection sensors distributed around the world. Our contribution in this context is to point out the infrastructure specifically for worm monitoring and what data should be collected for early detection of worms [1]. Early Bird detect and block worm spreading through identifying the common characteristics, such as a common bit-string, among all infection network traffic of a worm. Counter-based detection algorithm that tracks the increased rate of new infected hosts. Our early detection system tries to detect the presence of a worm in the global Internet. GrIDS, which can detect worm-infected hosts in a local network through building the worm's infection graph. The Counter Malice quarantine device also tries to detect infected hosts in local enterprise networks.

Proposed System: Our contribution in this context is to point out the infrastructure specifically for worm monitoring and what data should be collected for early detection of worms [2]. We also emphasize the functionality of egress monitors, which has been overlooked in previous research. Worm monitors can be set up as ingress and egress filters on routers, which cover more IP space and gather more comprehensive information than the log data collected from intrusion detection sensors or firewalls for current monitoring systems [3].

System Architecture: There are two kinds of monitors: ingress scan monitors and egress scan monitors. Ingress scan monitors are located on gateways or border routers of local networks. They can be the ingress filters on border routers of the local networks, or separated passive network monitors. The goal of an ingress scan monitor is to monitor scan traffic coming into a local network by logging incoming traffic to unused local IP addresses. For management reasons, local network administrators know how addresses inside their networks are allocated; it is relatively easy for them to set up the ingress scan monitor on routers in their local networks. For example, during the Code Red incident on July 19, 2002, a "/8" network at UCSD and two "/16" networks at Lawrence Berkeley Laboratory were used to collect Code Red scan traffic. All port 80 TCP SYN packets coming in to nonexistent IP addresses in these networks were considered to be Code Red scans. The goal of an egress scan monitor is to monitor the outgoing traffic from a network to infer the scan behavior of a potential worm. Ingress scan monitors listen to the global traffic in the Internet; they are sensors for global worm incidents [4]. On the other hand, if a computer inside a local network is infected, the egress scan monitor on this network's routers can observe most of the scans sent out by the compromised computer. Therefore, an egress scan monitor is good at observing a worm's scan rate and scan distribution, e.g., uniform scan (such as Code Red), or subnet scan (such as Code Red II and Sasser), or sequential scan (such as Blaster).

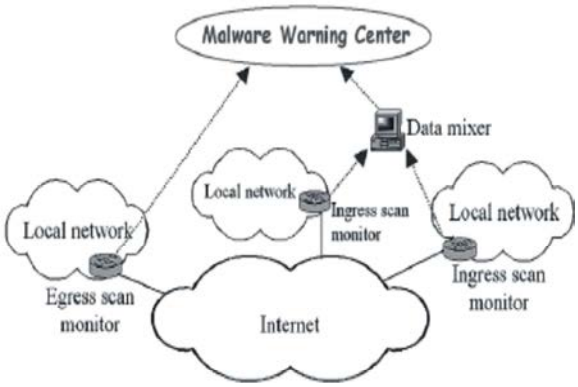

Fig. 1: Generic worm monitoring system

Location for Distributed Monitors: Ingress scan monitors on a local network may need to be put on several routers instead of only on the border router because the border router may not know the usage of all IP addresses of this local network. In addition, since worms might choose different destination addresses by using different preferences, such as subnet scanning, we need to use distributed address spaces with different sizes and characteristics to ensure proper coverage [5]. Later on, we show that for monitoring nonuniform scan worms such as Blaster, the IP space covered by a monitoring system should be as distributed as possible. For egress scan monitors, worms on different infected computers may exhibit different scan behaviors. For example, Slammer's scan rate is constrained by an infected computer's bandwidth [6-9]. Therefore, we need to set up distributed egress filters to record the scan behaviors of many infected hosts at different locations and in

different network environments. In this way, the monitoring system could obtain a comprehensive view of the behaviors of a worm. For example, it can get a better observation of the average number of scans an infected host sends out per unit of time.

Steps to Detect Worms: MWC collects and aggregates reports of worm scans from all distributed monitors once in every monitoring interval in real-time. For each TCP or UDP port, MWC has an alarm threshold for monitored illegitimate scan traffic. The observed number of scans, which contains nonworm noise, is below this threshold when there is no global spreading worm. This threshold can be chosen based on observations on normal days when no wide-spreading worm exists in the Internet. If the monitored scan traffic is over the alarm threshold for several consecutive monitoring intervals, e.g., is over the threshold for three consecutive times, the Kalman filter will be activated. Then MWC begins to record and calculates the average worm scan rate from the reports of egress scan monitors. Because is a cumulative observation data that could cumulate all nonworm noise, MWC begins to record data only after the Kalman filter is activated. The Kalman filter can either use or to estimate all the parameters of a worm at discrete time. The recursive estimation will continue until the estimated value of shows a trend: if the estimate stabilizes and oscillates slightly around a positive constant value, we have detected the presence of a worm; if the estimate converges to or oscillates around zero, we believe the surge of illegitimate monitored traffic is caused by nonworm noise.

CONCLUSION

We have proposed a monitoring and early detection system for Internet worms to provide an accurate triggering signal for mitigation mechanisms in the early stage of a future worm. Such a system is needed in view of the propagation scale and the speed of the past worms. We have been lucky that the previous worms have not been very malicious; the same cannot be said for future worms. Based on the idea of "detecting the trend, not the burst" of monitored illegitimate scan traffic, we present a "trend detection" methodology to detect the presence of a worm in its early propagation stage by using the Kalman filter and worm propagation models. Our analysis and simulation studies indicate that such a system is feasible and the trend detection methodology poses many interesting research issues [10-14].

Future Work: The worm detection method presented here assumes that only worm scans can cause exponentially increased traffic to monitors, while other background scan noise cannot. We believe this is a reasonable assumption. If we want to further improve the detection accuracy, however, we can add some other rule sets in the detection system. For example, in order to distinguish a worm attack from a DDoS attack, we can exploit the differences between them: a DDoS attack has one or several targets while a worm's propagation has no specific target.

REFERENCES

1. Anderson, B.D.O. and J. Moore, 1979. Optimal Filtering. Englewood Cliffs, NJ: Prentice Hall.
2. Eye Digital Security: Blaster Worm Analysis, 2003. [Online].Available:http://www.eeye.com/html/Research/Advisories/AL20030811.html.
3. Kumaravel, A., 2013. Routing algorithm over semi-regular tessellations, Xplore, pp: 1180-1184.
4. Kumaravel, A., 2013. Introducing an efficient programming paradigm for object-oriented distributed systems, Indian Journal of Science and Technology, 6(5S): 4597-4603.
5. Kumaravel, A., 2013. Application of non-uniform cellular efficient cryptography automata, Indian Journal of Science and Technology, 6(5S): 4561-4566.
6. Symantec Corp.: Symantec Early Warning Solutions [Online]. Available: http://enterprisesecurity. symantec.com/SecurityServices.
7. Eye Digital Security: ida Code Red, Worm 2001. [Online].
8. Kumaravel, A., 2013. An application of non-uniform cellular automata for efficient cryptography, Xplore, pp: 1200-1205.
9. Kumaravel, A., 2013. Algorithm for automaton specification for exploring dynamic labyrinths, Indian Journal of Science and Technology, 6(5).
10. Shafaq Sherazi and Habib Ahmad, 2014. Volatility of Stock Market and Capital Flow Middle-East Journal of Scientific Research, 19(5): 688-692.
11. Kishwar Sultana, Najm ul Hassan Khan and Khadija Shahid, 2013. Efficient Solvent Free Synthesis and X Ray Crystal Structure of Some Cyclic Moieties Containing N-Aryl Imide and Amide ,Middle-East Journal of Scientific Research, 18(4): 438-443.
12. Pattanayak, Monalisa. and P.L. Nayak, 2013. Green Synthesis of Gold Nanoparticles Using Elettaria cardamomum (ELAICHI) Aqueous Extract World Journal of Nano Science & Technology, 2(1): 01-05.

13. Chahataray, Rajashree. and P.L. Nayak, 2013. Synthesis and Characterization of Conducting Polymers Multi Walled Carbon Nanotube-Chitosan Composites Coupled with Poly (P-Aminophenol) World Journal of Nano Science and Technology, 2(1): 18-25.
14. Parida, Umesh Kumar, S.K. Biswal, P.L. Nayak and B.K. Bindhani, 2013. Gold Nano Particles for Biomedical Applications World Journal of Nano Science and Technology, 2(1): 47-57.