A Proposal of Malware Distinction Method Based on Scan Patterns Using Spectrum Analysis

Masashi Eto[1], Kotaro Sonoda[1], Daisuke Inoue[1], Katsunari Yoshioka[2], and Koji Nakao[1]

[1] National Institute of Information and Communications Technology
4-2-1, Nukui-Kitamachi, Koganei, Tokyo 184-8795, Japan
[2] Yokohama National University
79-7 Tokiwadai, Hodogaya-ku, Yokohama 240-8501, Japan

Abstract. Network monitoring systems that detect and analyze malicious activities as well as counter them, are becoming increasingly important. As malwares, such as worms, viruses, and bots, can inflict significant damages on both the infrastructure and the end user, technologies for identifying such propagating malwares are in great demand. In the large-scale darknet monitoring operation, we can see that malwares have various kinds of scan patterns that involves choosing destination IP addresses. With a focus on such scan patterns, this paper proposes a novel concept of malware feature extraction and a distinct analysis method named "*SPectrum Analysis for Distinction and Extraction of malware features* (*SPADE*)."Through several evaluations using real scan traffic, we show that SPADE has the significant advantage of recognizing the similarities and dissimilarities between the same and different types of malwares.

1 Introduction

Malwares are spread all over the Internet and they often lead to serious security incidents that can cause significant damage to both the infrastructure and end users. As countermeasures, a number of ongoing network monitoring projects are already in their operational phase. Many of these projects are concentrating on the event analysis that provides statistical data, such as rapid increase in access on certain port numbers, by using network event monitoring. Particularly, it is becoming popular to monitor a dark address space (darknet), which is a set of globally announced unused IP addresses [1, 2].

In order to identify the root causes of network events observed on darknets, we have started the *Network Incident analysis Center for Tactical Emergency Response (nicter)* project, with the goal of achieving an integrated analysis of security incidents on large networks [3, 4]. Our present focus is particularly on detecting and identifying the propagation of malwares such as worms, viruses, and bots, which can infect remote hosts through fundamental propagation steps,

C.S. Leung, M. Lee, and J.H. Chan (Eds.): ICONIP 2009, Part II, LNCS 5864, pp. 565–572, 2009.

such as *scan → exploit code → malware download*, by exploiting the vulnerabilities of operating systems or server applications of the targeted hosts. One of the purposes of nicter is to reveal certain malware species, which infect attacking hosts, only through their scan patterns. As a first step to realize this purpose, this paper aims at providing a method to distinguish attacking hosts observed on darknets.

Through our large-scale darknet monitoring operation, we have learned that malware uses various kinds of scan patterns, that involves choosing destination IP addresses [5, 6, 7, 8], such as regular increment or random determination of destination IP addresses for each packet. Since these scan patterns resemble a signal waveform, we applied the discrete Fourier Transform (DFT) algorithm to the feature extraction and distinction method.

In this paper, we propose a malware feature extraction and distinction method called *SPectrum Analysis for Distinction and Extraction of malware features* (*SPADE*), which analyzes the scan traffic data from a pair of attacking hosts and derives the correlation coefficient between them.

The rest of this paper is organized as follows: Section 2 introduces the background of this research and related works. The SPADE algorithm is explained in Section 3. Several evaluations with actual darknet traffic are presented in Section 4. Finally, Section 5 presents the conclusions and future work.

2 Background

As a background of this research, we first explain the darknet monitoring and its advantage. Second, we show that malwares have various scan patterns according to our long-term and large-scale darknet monitoring, which can be used to classify the malwares. Third, we mention some related works.

2.1 Darknet Monitoring

A darknet is a set of globally announced unused IP addresses and using it is a good way of monitoring network attacks, such as malwares' scans. A big advantage of darknet monitoring is that there is no legitimate host using these addresses; we can thus consider all incoming traffic to be a consequence of some kind of malicious activity or the result of misconfigurations. As the principal darknet monitoring method, we deployed *black hole sensors*, which quietly monitor incoming packets without ever responding to the opposite hosts. By using these black hole sensors in the darknet IP domains, we could observe emerging network attacks, including malware-initiated network scan, malware infection behavior, and DDoS backscatters.

2.2 Scanning Patterns of Malwares

According to our long-term and large-scale darknet monitoring and some previous researches [5, 6, 7, 8], malwares use various kinds of scan patterns. These patterns

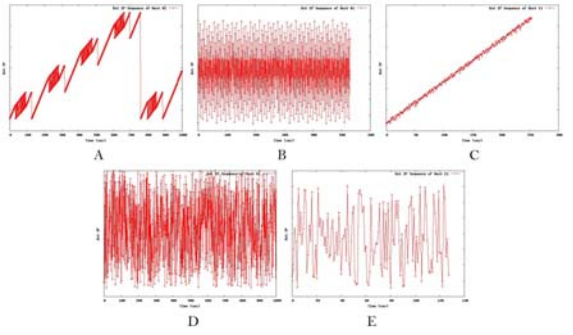

Fig. 1. Examples of Malware Scanning Patterns

can be important clues to classify malwares. Figure 1 shows the examples of typical scan patterns that are observed by nicter's black hole sensors. These graphs represent scan patterns of five individual attacking hosts *A*-*E* that are probably infected by different types of malwares. In each graph, the X axis represents the packet arrival sequence and the Y axis represents the value of the destination IP address of our black hole sensor that monitors a network with /16 subnet mask.

The examples state that there are various scan patterns, such as regular increment pattern (*A*, *C*), random determination pattern (*D*, *E*), and specific rule-based pattern that appears to be a random pattern (*B*). Through these observations, we found that the scan patterns of malwares have their own individual characteristics, and also found that many of the patterns appear to have the natural periodicity, as if they are signal waveforms. Consequently, we apply a spectrum analysis method to the scan traffic in order to extract their characteristics and to classify them.

2.3 Related Works

In the context of spectrum analysis, Mitra et al. [9] proposed an anomaly detection method based on spectrum analysis. They focused on the harmonic structure of the traffic data spectrum obtained by Fourier transform and wavelets so as to detect DDoS and bottleneck traffic. Meanwhile, Yu et al. [10] applied a spectrum analysis method for detecting slow scan worms. The objective of these studies was to detect the presence of anomalous activities in normal traffic on a live network by means of analyzing the fluctuation of traffic volume. In contrast, since our basic tactics involves black hole monitoring, where most of the observed activities are assumed to be anomalous, we aim at establishing a fine-grained distinction method of attacking hosts based on their scan patterns rather than merely determining whether the activities are malicious or not.

3 SPADE: Malware Correlation Method Based on Spectrum Analysis

In this section, the SPADE algorithm is proposed, which is a malware feature extraction and correlation method based on spectrum analysis. SPADE begins

with the application of discrete Fourier transform (DFT) to a series of destination IP addresses and ends at the derivation of a correlation coefficient between two different series of data.

3.1 Algorithm of SPADE

The main processes of SPADE algorithm are as follows.

1. Hamming Window Function for Series Data
   As a preparation of subsequent processes, SPADE applies the *Hamming window function* to the original series data of destination IP addresses in order to emphasize the characteristics of the oscillations. Specifically, where the original series data X has N elements, the following formula is applied to each element $X(n)$;

$$X'(n) = \{0.54 - 0.46\cos(\frac{2\pi n}{N})\}X(n) \quad (1)$$

   It should be noted that the parameters (0.54 and 0.46) were defined as the constant number of Hamming window function [11].
2. Discrete Fourier Transform
   SPADE applies DFT to the series data and derives a spectrum, which represents the characteristics of the original scanning behavior.
3. Removal of High-Frequency Bands
   Minor phenomena such as packet losses and disorders in the packet arrival sequence appear in high-frequency bands. Therefore, in order to avoid these influences, which are the result of the degradation of network conditions, SPADE removes frequency bands higher than the vertical threshold A.
4. Extraction of Maximum Value Indices
   In this step, SPADE extracts the peaks of frequency components, namely, those whose magnitudes are higher than neighboring components, since high-level components in a spectrum are dominant in characterizing the original scanning behavior. Furthermore, with this process, SPADE reduces the number of samples for the subsequent calculations.

   It is to be noted that in the following steps, SPADE treats a collective set of indexes I (and not power levels) of the components that are selected in this step.
5. Removal of Fundamental Frequency
   The purpose of this step is to adjust the number of cycles of oscillations among different attacking hosts. Even if some attacking hosts have the same scanning behavior, the packet counts from them may differ widely because of the differences in the conditions of each network sensor. To resolve this, SPADE removes the fundamental frequency from the spectrum while maintaining its harmonic structure. The normalized index values (N_i) are derived by dividing each index value (I_i) by the index value of the fundamental frequency (I_p) that has the highest power level in the spectrum, as shown by formula (2).

$$N_i = \frac{I_i}{I_p} \tag{2}$$

6. Standardization of Harmonic Structure
   In this step, SPADE standardizes the weight of each value in the normalized index values N and derives a series of deviation values S. As mentioned in the previous step, the number of observed packets is dependent on the environmental conditions of the sensor. To neutralize the differences in environmental conditions, SPADE computes a series of deviation values (S) of N. For a series of index values N that has n samples, the standard deviation SD_N is derived by formula (3).

$$SD_N = \sqrt{\sum_{i=1}^{n} \frac{(N_i - M)^2}{n}} \tag{3}$$

   Here, M is the average of the all index values. The deviation value of each index value (S_i) is computed from the standard deviation (SD_N) by formula (4).

$$S_i = \frac{N_i - M}{SD_N} \tag{4}$$

7. Synchronization and Alignment of Two Series of Data
   As the last step of the preparation process, we must synchronize two independent series of data and adjust their lengths. In this step, SPADE aligns two series based on the index values of their base frequencies. The missing space resulting from the differences in the series lengths is padded with zeros. Thus, the two series of data are synchronized and aligned, ready to be compared with each other.
8. Derivation of Correlation Coefficient
   Finally, SPADE computes the correlation coefficient between two independent series of data. The correlation coefficient $C_{\alpha\beta}$ between series S_α and S_β is derived by formula (5).

$$C_{\alpha\beta} = \frac{1}{n} \sum_{i=1}^{n} S_{\alpha i} \times S_{\beta i} \tag{5}$$

   The correlation coefficient ranges from -1 to 1. An absolute value of coefficient approaches 1 with increasing similarity between the original scan data, and approaches 0 with decreasing similarity.

A sample result of the SPADE algorithm is shown in Figure 2, where two attacking hosts A_1 and A_4 are analyzed. As shown in Figure 2-(1) and (2), these hosts have similar scan patterns that oscillate destination IP addresses based on a specific rule although it appears to be determined randomly. Figure 2-(3) shows that the picked up maximum values (indicated by $\times$ and $+$) in each spectrum overlap on six points. Figure 2-(4) shows that the correlation coefficient between these hosts is 0.80.

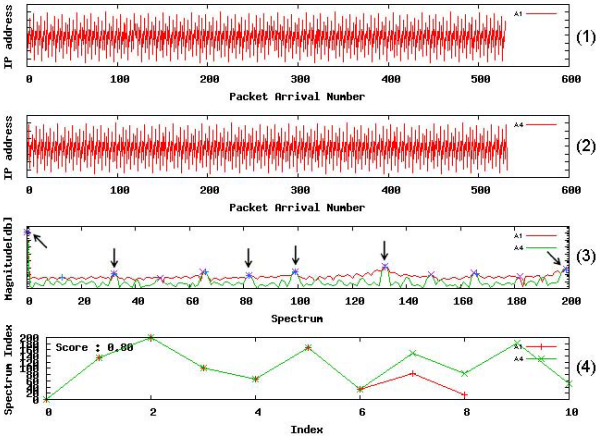

Fig. 2. Result of Correlation between A_1 and A_4

4 Evaluation

The purpose of SPADE is to extract the features of scan patterns from individual attacking hosts and derive the similarities or dissimilarities among them. Consequently, this section provides some evaluations using practical traffic data observed by nicter's black hole sensors in December 2008. High correlation coefficients are expected among hosts infected by the same type of bot, while low correlation coefficients are derived among hosts infected by different types of bots.

4.1 Analyses among Same Bots

At first, SPADE analyzed five attacking hosts (A_1 - A_5) in the same botnet, which sophisticatedly fluctuated destination IP addresses, and derived the correlation coefficients in all combinations (Table 1). There were six combinations whose coefficients were over 0.70, among the ten combinations excluding self-comparison, and the coefficient average of those ten combinations was 0.73.

Table 1. Correlation Results among Hosts in the Same Botnet (1)

	A_1	A_2	A_3	A_4	A_5
A_1	1.00	0.74	0.61	0.80	0.59
A_2	–	1.00	0.71	0.92	0.60
A_3	–	–	1.00	0.77	0.94
A_4	–	–	–	1.00	0.65
A_5	–	–	–	–	1.00

As a result, we found that most of the correlation coefficients among hosts in the same botnet were higher than at least 0.70. This signifies that SPADE can recognize hosts infected by the same type of bot.

4.2 Analyses among Different Bots

Secondly, five hosts were analyzed, which belonged to different botnets and had significantly dissimilar scan patterns. As shown in Table 2, there was only one combination whose correlation coefficient was over 0.70 among the ten combinations excluding self-comparison, and the coefficient average of those ten combinations was 0.41. According to this result, we found that SPADE can distinguish hosts that were infected by different types of bots.

Table 2. Correlation Results among Hosts in Different Botnets

	A_1	B_1	C_1	D_1	E_1
A_1	1.00	0.31	0.33	0.87	0.59
B_1	–	1.00	0.28	0.31	-0.01
C_1	–	–	1.00	0.46	0.41
D_1	–	–	–	1.00	0.57
E_1	–	–	–	–	1.00

4.3 Consideration

The evaluation results showed that SPADE derived higher correlation coefficients between each combination within the same botnets, while lower correlation coefficients were derived within different botnets. This signifies that SPADE almost successfully extracted malwares' features and distinguished them. However, in some cases, the results also showed that the correlation coefficients widely varied from 0.59 to 0.98 even though the hosts belonged to the same botnet. Therefore, we need to improve the algorithm in order to extract malwares' feature more efficiently.

5 Conclusion and Future Work

In this paper, by focusing on the oscillations of the destination IP addresses of scan packets, we proposed the concept of malware feature extraction, and implemented and evaluated a distinct analysis method (SPADE) that applied a spectrum analysis methodology. Our contribution is to realize a fundamental technology to grasp the general trend of malwares propagation only from their scan traffic data. In other words, we proposed SPADE algorithm that employed the discrete Fourier transform (DFT). Through several evaluations, we showed that SPADE almost successfully extracted malwares' features and distinguished them.

Although we applied the destination IP addresses of scan packets in our algorithm, we have to further consider other parameterized characteristics such as

the source/destination port numbers and the interval time of packet arrival. As a future work, we shall attempt to establish more multifaceted analysis techniques covering such parameters based on the SPADE algorithm.

References

1. Bailey, M., Cooke, E., Jahanian, F., Nazario, J., Watson, D.: The Internet Motion Sensor: A Distributed Blackhole Monitoring System. In: The 12th Annual Network and Distributed System Security Symposium, NDSS 2005 (2005)
2. Moore, D.: Network Telescopes: Tracking Denial-of-Service Attacks and Internet Worms around the Globe. In: 17th Large Installation Systems Administration Conference, LISA 2003 (2003)
3. Inoue, D., Eto, M., Yoshioka, K., Baba, S., Suzuki, K., Nakazato, J., Ohtaka, K., Nakao, K.: nicter: An Incident Analysis System Toward Binding Network Monitoring with Malware Analysis. In: WOMBAT Workshop on Information Security Threats Data Collection and Sharing, pp. 58–66 (2008)
4. Nakao, K., Yoshioka, K., Inoue, D., Eto, M.: A Novel Concept of Network Incident Analysis based on Multi-layer Observations of Malware Activities. In: The 2nd Joint Workshop on Information Security (JWIS 2007), pp. 267–279 (2007)
5. Filiol, E.: Malware Pattern Scanning Schemes Secure Against Black-box Analysis. Journal in Computer Virology 2, 35–50 (2006)
6. Zou, C., Gong, W., Towsley, D.: Code red worm propagation modeling and analysis. In: 9th ACM conference on Computer and communications security, pp. 138–147 (2002)
7. Chen, Z., Gao, L., Kwiat, K.: Modeling the spread of active worms. In: Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM 2003, vol. 3. IEEE, Los Alamitos (2003)
8. Garetto, M., Gong, W., Towsley, D., di Elettronica, D.: Modeling malware spreading dynamics. In: Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM 2003, vol. 3. IEEE, Los Alamitos (2003)
9. Mitra, U., Ortega, A., Heidemann, J., Papadopoulos, C.: Detecting and Identifying Malware: A New Signal Processing Goal. Signal Processing Magazine 23, 107–111 (2006)
10. Yu, W., Wang, X., Calyam, P., Xuan, D., Zhao, W.: On Detecting Camouflaging Worm. In: 22nd Annual Computer Security Applications Conference (ACSAC 2006), pp. 235–244. IEEE Computer Society. Washington (2006)
11. Harris, F.: On the use of windows for harmonic analysis with the discrete Fourier transform. Proceedings of the IEEE 66, 51–83 (1978)