مجلة جامعة بابل / العلوم الصرفة والتطبيقية / العدد (٣) / المجلد (٢٠) : ٢٠١٢

Host-Based Detection of P2P Active Worm Through Extensive Packet Matching

Ausama A. Majeed
College of Science / Thi-Qar University

Abstract:

Active worms continue to pose major threats to the security of today’s Internet. This is due to the ability of active worms to automatically propagate themselves and compromise hosts in the Internet. Due to the recent surge of peer-to-peer (P2P) network with large numbers of users and rich connectivity, active P2P worm has a non-scanning feature and can use of neighbor routing table of P2P network as hit-list to launch an attack. It avoids blind scanning which is the shortcoming of traditional Internet worms. Also, it generates a low failure rate of the network connection and spreads faster. To improve the security of P2P network, this paper undertake this issue by analyzing active worm propagation on P2P network and proposed an effective detection strategy within P2P network based on the rules “packets with similar payload (data) are sent to many hosts in a very short time using the same protocol and destination port is attempting to carry out worm propagation”. The implementation shows that a P2P active worm can detect anomaly with less false positive alarm message as possible.

Keywords: P2P network; Active worm attacks, Network security.

الخلاصة

يستمر هذه الأيام الـ P2P Worm النشط بتهديد امن الانترنت بسبب إمكانيته على تكرار نفسه بشكل تلقائي و فضحه للجهاز المضيف. و قد أظهرت الدراسات الأخيرة على شبكه الند- للند بأنه ذو طبيعة غير بحثيه (non-scanning) وله القدرة على استخدام جدول المسارات (routing table) الخاص بالاجهزه المجاورة لتكوين قائمه بالا جهزه المرشحة للهجوم. فهو بهذا يتجنب البحث الأعمى عن الاجهزه الضحية مع نسبه خطأ قليله و سرعه بالانتشار.

و من اجل تعزيز حماية شبكه الند- للند تم اقتراح طريقه اكتشاف فعاله تعتمد على مبداء " كل حزمه بيانات (packet) تحوي نفس البيانات و مرسله إلى عده أجهزه ضمن مده زمنيه قليله جدا باستخدام نفس بروتوكول النقل و المنفذ " هي محاوله لنشر الـ Worm . و قد أظهرت النتائج كفائه هذه الطريقة باكتشاف الـ P2P Worm النشط بدون الحاجة إلى قاعدة بيانات تحوي معلومات تفصيلية عن هذا الـ Worm مع اقل عدد ممكن من رسائل الاكتشاف الخاطئة.

I. Introduction

There is no guarantee that the software and the system running the software have not security vulnerability in the process and management because the used P2P software in Internet lack of unified norms and have strong randomness and diversity at present. P2P worms discover system vulnerabilities and spread automatically by using the interactive nature of peer-to-peer network. This is the major threat to the Internet and P2P users. So, it is necessary to make a study and exploration on P2P worm detection (Zhou et al., 2005).

P2P network is kind of self-organizing system composed of autonomic nodes, and it has been becoming an active platform for Internet-scale resource sharing and cooperation (Yang, Shen, Chang, & Yao, 2010). Currently there are two kinds of P2P network topology model called unstructured P2P network and structured P2P network (Chunyan & Zhiyu, 2009). Unstructured P2P network has no relationship with the location of resources. Resources search the nodes each other to achieve transfer of information. In this environment, P2P worms use the neighbor nodes for spreading between inter-nodes. On the other hand, structured P2P network has a close relationship with the location of resources.

According to scanning strategies, P2P Worms can be classified into two classes. One is called as scanning worms, and the other non-scanning worms (Fahimian, Movahed, & Kharrazi, 2010). Many notorious Internet worms employ a random scanning strategy to find the potential victims. P2P worms tend to use neighbor list to find the potential victims instead of scanning, so P2P worms are non-scanning. According to different attacking ways, non-scanning worms in P2P networks can be classify into three types passive, reactive, and active. *Passive* worms are hiding themselves in malicious files and trick users into downloading and opening them. *Reactive* worms are only propagating with legitimate network activities. *Active* worms are automatically connected to and infect known peers using topological information. Note that the reactive and active worms are similar to contagion and topological worms (Feng, Qin, Cuthbet, & Tokarchuk, 2008).

An active worm attack is the most common threats in the Internet and is not new. There have always been worm propagations on the Internet since the Morris worm appeared in 1988. The security threat posed by active worms has regularly increased, especially in the last several years (Fan & Xiang, 2010; Liu & Zhang, 2008; Yu, Chellappan, Wang, & Xuan, 2008). One well-known instance is Code-Red version 2 worms that were able to infect over more than 350,000 IIS web servers in less than 14 hours on July 2001. MyDoom worm compromised about 20,000 hosts in total within 2 hours after it was first discovered. On September 2001, Nimda achieved very successful attack damage due to improved contagion schemes. On January 2003, the Slammer worm presented a new attack record – it infected nearly 75,000 MS-SQL server in less than 10 min. These worms identify new victims simply by following P2P neighbor information on the cash of infected nodes. They are different from the currently popular scanning worms which employ a random scanning strategy to find the potential victims. In other words, active worms do not randomly select targets from IP space. Thus it is not possible to detect them by capturing their scans directly. Moreover they do not cause abnormal network activities which could be passively observed for detection. Instead, these worms propagate using legitimate network activities or network topology information and hide behind normal network traffic (Saadat, Yousefi, & Fathy, 2009).

This paper aim to study the behavior of active worm in peer-2-peer network and its strategies for spreading attacks and propose a new method with which active worm could be detected. The main idea of the detection algorithm relies on P2P active worm transmitting behavior.

The rest of paper is structured as follows. Section II define active P2P worm and explain its attack strategies. Section III describes the proposed detection algorithm by this paper. Also, the assumptions and implementation of the proposed algorithm are presented. The conclusion finished this paper in section IV.

II. Active P2p Worm Attacks Models

An active worm is a program that propagates across hosts in a network by exploiting their security flaws. Active worms are similar to biological viruses in their self-replicating and propagating behavior. In general, there are two stages in an active worm attack: (1) scanning the network to select victim hosts; (2) infecting the victim after discovering its vulnerability (Antonatos, Akritidis, Markatos, & Anagnostakis, 2007; Yu, Chellappan, Wang, & Xuan, 2008). Infected hosts further propagate the worm to other vulnerable victims and so on. Therefore, the worm detection and identification is one of the most important researches, mainly related to the new worm infected with the goal find and its effectiveness. As the P2P worms have obvious distinction with a traditional, the defense used to the traditional worms such as the Intrusion Detection, content filtering, address blacklist is no longer applicable to P2P worms, we need a new strategy (Chunyan & Zhiyu, 2009). The P2P worms will not cause abnormal flow and it is a non-scanning network worm.

P2P worm attack spreading mainly used three types of strategies which are:

A. Pure Random Scanning Strategy (PRS)

In this strategy, assuming the host which has been infected does not have any prior vulnerability knowledge or active/inactive information of other hosts, then the host will select an IP address randomly. The new host was infected through the same method to continue to attack the system (Chunyan & Zhiyu, 2009; Yu, Chellappan, Wang, & Xuan, 2008).

B. Off-line P2P-based Hit-List Scan Strategy (OPHLS)

In this strategy, assuming the host which has been infected has gathered the whole system off-line host IP address information as the hit-list of attacks. Obtaining the hit-list can be achieved by various methods, such as using P2P-based Crawler tools. In this attack model, there are two phases: in the first phase (called the P2P system attack phase), all newly infected hosts continuously attack the hit-list until all hosts in the hit-list have been scanned. In the second phase, all infected hosts continue to attack the Internet via PRS (Chunyan & Zhiyu, 2009; Yu, Chellappan, Wang, & Xuan, 2008).

C. On-line P2P Scanning strategy (OPS)

In this strategy, the rich connectivity of P2P systems will be utilized by worms during propagation. After a worm infected host joins the P2P system, the host immediately launches the attack on its P2P neighbours as a high priority. In addition, if there are additional forces available to attack, the host will attack other hosts through *PRS* system (Chunyan & Zhiyu, 2009; Yu, Chellappan, Wang, & Xuan, 2008).

Active worms exploit connectivity in a network to self-propagate. P2P systems in the Internet have large number of users, rich connectivity, and host vulnerability. In P2P-based attack models, worms exploit these effectively. This translates to rapid worm propagation which highlighting the threats caused by P2P system-based worm attacks.

III. Detection Method & Implementation

A. The Proposed Detection Algorithm

An active P2P worm replicates itself and produces large amount of worm messages with same or similar content in the P2P network within a very short period of time. In this paper, a detection method is proposed against active P2P worms based on comparing the characteristics of the packets that wear captured in very short time interval. The detection rules are: packets with similar payload (data) are sent to many hosts in a very short time using same protocol and destination port. If the source host satisfies these rules it is attempting to carry out worm propagation and need to send alert to the system administrator to inform him that this host was infected and starting attacks other hosts. This approach dose not has a permanent worm signature database, thus a P2P active worm can detect anomaly. Since incoming data is very high in volume, the program need to run packets eliminator to dump all data after cretin time unit for better memory size maintains.

According to the fact "each normal traffic signature is unique" it is guarantees there is no false positive detection as stated by Yu and his group.

The detection algorithm can be derived according to the detection rules stated above. Packet characteristics that are required to perform the proposed detection algorithm are: a captured timestamp (*ctime*); source IP address (*src_ip*); destination IP address (*dst-ip*); destination port no. (*dst_port*); protocol (*proto*); and payload (*data*). Algorithm 1 describes the Extensive Packet Matching (EPM) algorithm which proposed by this paper.

Algorithm 1: ***EPM -Extensive Packet Matching Algorithm***

Require: A host *h* capture all traffic in a traffic set *T* which contains a packets, *T= {P1, P2, P3,…}* sorted ascending by *ctime*, where each packet contains *Pi = < ctime; src_ip; dst_ip; dst_port; proto; data >*

```
While T is not empty Do
    $\forall Pi, Pj \in T$
    If $Pj.ctime - Pi.ctime \leq Time\_unit$ Then
        If $Pj.data == Pi.data$ Then
            If $(Pj.proto == Pi.proto) \cap (Pj.dst\_ip \neq Pi.dst\_ip) \cap (Pj.dst\_port == Pi.dst\_port)$
            Then Generate worm detection alert
    Packets Eliminator (Pi)
End While
```

The main idea of EPM is comparing between each packets captured in a specified time interval (time-unit). In other words, when two packets (Pi, Pj) carrying same data (*Pj.data == Pi.data*) and using same transport protocol (*Pj.proto == Pi.proto*) and same destination port number (*Pj.dst_port == Pi. dst_port*) with different destination IP-address (*Pj.dst_ip ≠ Pi.dst_ip*). When all these conditions are satisfy, it is guarantee carrying P2P active worm and worm detection alarm must be generate to inform the network manager that this host was infected and staring spreading attack to other hosts in range.

B. Assumption

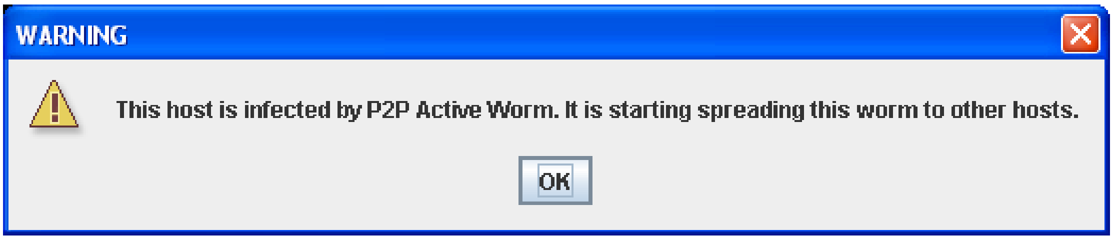
Extensive Packet Matching was implemented under the following assumptions:

1. P2P messages can only be sent to online nodes.
2. All nodes can send multicast messages to their online neighbors.
3. Once node *i* responds to a received worm message, it will be infected and worm multicast messages are immediately sent to all or part online neighbors of node *i*.

C. System Implementation

To evaluate the proposed system, some network traffic needs to be run through the detection system. Explicitly, this traffic, operation of the detection system in a live environment, should be tested in a live environment. Since our concern focus on P2P network, the traffic is applicable to be obtained and adapt some traffic characteristics into P2P network characteristics as an example of being used in environment test.

A laboratory with two computers is required to assist application of the proposed detection method. The main computer loaded with Windows XP (SP2) as platform from one side. On other side, for the purpose of gathered traffic characteristics to be process later by a proposed detection system, Snort 2.8.5 employed in a packet logger mode and WinPcap 4.0.2 software (a Windows version of the UNIX LibPcap API). Snort sends packet info. in MySQL database that log details of a packet (including TCP/IP options and the payload). Java programming language is used to develop the proposed worm detection algorithm. This system read a packets logged database and analyzes its content to detect a worm. Once the rules matches some traffic, a worm alert message is generated to the system administrator or the user to inform him that this node (host) is infected by active P2P worm and starting spreading attacks to other nodes as shown in figure 1 . Colasoft Packet Player software is used to read pre-captured traffic and send it again on specified network interface.



This host is infected by P2P Active Worm. It is starting spreading this worm to other hosts.

Figure 1. The Alert message

The implementation of a proposed detection algorithm shows ability to detect P2P active worm anomaly in a predefined time unit. Anomaly detection means there is no need to load our system with worm historical behavior as same as applied in (TANG, QI, FANG, & LUO, 2009). For a purpose of this research, time unit used is one second according to fast spreading nature of P2P active worms that infects many thousand on-line nods in a few minutes as presented previously. Also, it accurate detection method because it depends on extensive comparing of packet characteristics using header and payload information of each packet which lead to reduce false positive massages as possible. On the other hand, the packets eliminator procedure used to maintain a database size by removing the tuples from packet database which are acceding to a time unit or not satisfying the detection rules in general.

IV. Conclusion

The widespread use of P2P networks among computer users make them suitable for the worm propagation and also accelerates worm propagation in comparison with other networks. This research contributes to the understanding of the ways with which active worms propagate in P2P networks and presents a new methodology for active worm detection using extensive packet matching. The method proposed in the paper, can effectively detect the worms' attacks even though the attacking traffic is too little. This approach does not require knowledge of worm was predefined, it can automatically detect worm due abnormality packet characteristic. It will be effective way to detect active worm's anomaly making the false positive alarm probability as low as possible.

References

Antonatos, S., Akritidis, P., Markatos, E. P., & Anagnostakis, K. G. (2007). Defending Against Hit-List Worms Using Network Address Space Randomization. *Computer Networks, 51*, 3471–3490.

Chunyan, X., & Zhiyu, Y. (2009). The Research of Worms in P2P Networks. *IEEE Int. Conf. on Computational Intelligence and Natural Computing (CINC 09)*, 389-392, doi 310.1109/CINC.2009.1248.

Fahimian, S., Movahed, A., & Kharrazi, M. (2010). Passive Worm and Malware Detection in Peer-to-Peer Networks. *IEEE/IFIP Int. Conf. on Embedded and Ubiquitous Computing (EUC 10)*, 561-565, doi 510.1109/EUC.2010.1133.

Fan, X., & Xiang, Y. (2010). Defending Against the Propagation of Active Worms. *Supercomput, 51*, 167-200.

Feng, C., Qin, Z., Cuthbet, L., & Tokarchuk, L. (2008). Propagation Model of Active Worms in P2P Networks. *the 9th IEEE Int. Con. for Young Computer Scientists (ICYCS 08)*, 1908-1912, doi 1910.1109/ICYCS.2008.1237.

Liu, T., & Zhang, C. (2008). Approach to Worm Detection, Early Warning Based on Local Victim Behavior. *IEEE Int. Conf. on Computer Science and Software Engineering (CSSE 08)*, 880-884, doi810.1109/CSSE.2008.1823.

Saadat, Z. Z., Yousefi, S., & Fathy, M. (2009). Active Worm Propagation in Hierarchical Peer-to-Peer Network Management Systems. *the 2nd IEEE Int. Conf. on Communication Theory, Reliability, and Quality of Service(CTRQ 09)*, 52-57, doi 10.1109/CTRQ.2009.1122.

TANG, Z., QI, R., FANG, D., & LUO, Y. (2009). W-Aegis: A Propagation Behavior Based Worm Detection Model for Local Networks. *5th IEEE Int. Conf. on Information Assurance and Security (IAS 09)*, 158-162, doi 110.1109/IAS.2009.1293.

Yang, W., Shen, X., Chang, G., & Yao, Y. (2010). A P2P-Based Worm in Next Generation Network. *the 4th IEEE Int. Conf. on Genetic and Evolutionary Computing (ICGEC10)*, 418-421, doi 410.1109/ICGEC.2010.1110.

Yu, W., Chellappan, S., Wang, X., & Xuan, D. (2008). Peer-to-Peer System-Based Active Worm Attacks: Modeling, Analysis and Defense. *Computer Communications, 31*, 4005-4017.

Zhou, L., Zhang, L., McSherry, F., Immorlica, N., Costa, M., & Chien, S. (2005). A First Look at Peer-to-Peer Worms: Threats and Defenses. *The Peer-to-Peer Systems 4th International Workshop*, 24-35.