April - June © 2015 Transactions; 2(6): 275-277

International Journal of Research and Applications

ISSN (online): 2349-0020 ISSN (print): 2394-4544 http://www.ijraonline.com/

Research Article

Bot Net Detection by Using SSL Encryption

D. Jyothi [1] and Dr. G. Narsimha [2]

Corresponding Author:
damallajyothii@gmail.com

DOI:
http://dx.doi.org/
10.17812/IJRA.2.6(49)2015

Manuscript:
Received: 22nd April, 2015
Accepted: 15th May, 2015
Published: 15th June, 2015

Publisher:
Global Science Publishing Group, USA
http://www.globalsciencepg.org/

ABSTRACT

Botnets spread throw Distributed Denial of service. When a large number of computers act under the control of a single attacker it is called a botnet. The Upatre attachment comes in the form of a zip file. Its purpose is to download a payload from elsewhere, detonate it, and disappear. The authors propose checking SSL traffic resource and a set of SSL features that can be used to detect malicious connections.

Keywords: Botnet, bot, Upatre, zip, p2p.

[1] Research Scholar (JNTU), [2] Professor,
[1 2] Department of Computer Science and Engineering,
[2] JNTUH, kondagattu, Karimnager, Telangana, India.

IJRA - Year of 2015 Transactions:
Month: April - June
Volume – 2, Issue – 6, Page No's:275-277
Subject Stream: Computers

Paper Communication: Author Direct

Paper Reference Id: IJRA-2015: 2(6)275-277

DOI: 10.17812/IJRA.2.6(49)2015

International Journal of Research and Applications
Apr-Jun © 2015 Transactions 2(6): 275-277

eISSN : 2349 - 0020
pISSN : 2394 - 4544

COMPUTERS RESEARCH ARTICLE

Bot Net Detection by Using SSL Encryption

D. Jyothi [1] and Dr. G. Narsimha [2]
[1] Research Scholar(JNTU), [2] Professor
[1 2] Department of Computer Science and Engineering,
[2] JNTUH, kondagattu, Karimnager, Telangana, India.
[1] damallajyothii@gmail.com, [2] narsimha06@gmail.com

ABSTRACT

Botnets spread throw Distributed Denial of service. When a large number of computers act under the control of a single attacker it is called a botnet. The Upatre attachment comes in the form of a zip file. Its purpose is to download a payload from elsewhere, detonate it, and disappear. The authors propose checking SSL traffic resource and a set of SSL features that can be used to detect malicious connections.

Keywords: Botnet, bot, Upatre, zip, p2p.

I. INTRODUCTION

A botnet is a network which consists of a group of computers and is controlled by a single person. Usually, the user does not find out the existence of a bot (malicious program). Botnets are now recognized as one of the most serious security threats, such as DDos, spam, click fraud, etc. Botnets often use some common protocols, such as P2P, HTTP, IRC, etc. This makes the detection of botnet a challenging problem, especially the P2P botnet. The P2P (peer to peer) botnet is a distributed malicious software network; it is more difficult to detect this bot.

Comparison to previous malware, botnets have their unique characteristics. For example, in order to implement group attack, a bot has to communicate with another bot; communication characteristic is distinguishable between a bot and a common single malware. Therefore, for p2p detection, we only consider the communication program in the local machine. We proposed a new general p2p botnet detection framework. This mechanism not only can successfully detect known P2P botnet with a high detection rate but also can detect some unknown P2P malware.

Botnet was composed of the virus-infected computers severely threaten the security of internet. Hackers, firstly, implanted virus in targeted computers, which were then commanded and controlled by them via the internet to operate distributed denial of services (DDoS), steal confidential information, and distribute junk mails [1] and other malicious acts.

By imitating P2P software, P2P botnet used multiple main controllers to avoid single point of failure, and failed various misuse detecting technologies together with encryption technologies. Differentiating from the normal network behavior, P2P botnet sets up numerous sessions without consuming bandwidth substantially, causing itself exposed to the anomaly detection technology. The data mining scheme was tested in real internet to prove its capability of discovering the host of P2P botnet.

II. P2P BOTNET FRAME WORK

A. Detected system

We define private computer system as a detected system. For detected system, the first thing we have to do is to distinguish a communication

program from a single program. The single program is a program that can only run in local machine and not connect with the outside world. Communication program is a program that needs to communicate with another computer.

B. Filtering

The main objective of filtering is to reduce the traffic workload and make the rest of system perform more efficiently.

Extract features from P2P data

There are two kinds of data sources: one is host data, another is network data

- Improving the performance of the machine learning algorithms.
- Data understanding, gaining knowledge about the process and perhaps helping to visualize it.
- Data reduction, limiting storage requirements and perhaps helping in reducing costs.
- Simplicity, possibility of using simpler models and gaining speed.

Botnet detection

According to data sources, the detection methods fall into two categories Host-based detection [2], Network based detection.

III. PROCESS OF P2P BOT DETECTION

Botnet was composed of the virus-infected computers severely threaten the security of internet. Hackers, firstly, implanted virus in targeted computers, which were then commanded and controlled by them via the internet to operate distributed denial of services (DDoS), steal confidential information [11], and distribute junk mails [6] and other malicious acts.

By imitating P2P software, P2P botnet used multiple main controllers to avoid single point of failure, and failed various misuse detecting technologies together with encryption technologies. Differentiating from the normal network behavior, P2P botnet sets up numerous sessions without consuming bandwidth substantially, causing itself exposed to the anomaly detection technology. The data mining scheme was tested in real internet to prove its capability of discovering the host of P2P botnet.

The second-stage malware the Botnet attackers deployed was remote access Trojan (RAT) [3] produces easily identifiable network traffic, which started with a header.

IDS rules to detect Bot RAT have been in existence since at least 2008 and continue to be widely used.7 In fact, the payload of a recent attack that delivered a Java exploit (i.e., CVE-2012-0507) through strategic website compromises, including human rights sites, was Bot RAT.8 While this attack maintained the signature "Bot" header, other attacks leveraged a modified Bot RAT.

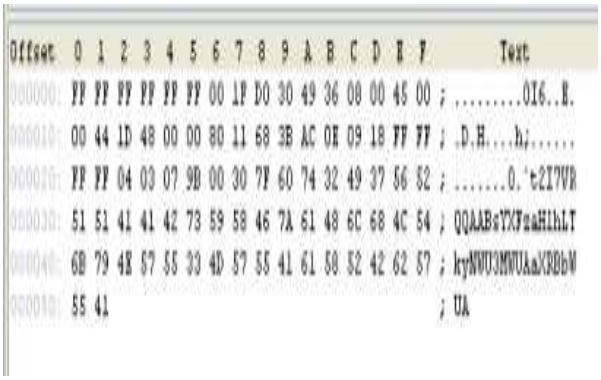

Fig: Malicious SSL Encryption

Apriori algorithm :

Techniques for data mining and knowledge discovery in databases. Developed by Agrawal and Srikant 1994. Items that occur often together can be associated to each other These together occuring items form a frequent itemset.

Conclusions based on the frequent itemsets form association rules[6].

For ex. {milk, cocoa powder} can bring a rule *cocoa powder* ➔ *milk*

Innovative way to find association rules on large scale, allowing implication outcomes that consist of more than one item Based on minimum support threshold. Apriori algorithm used to identify next system attacked by the botnet.

Apriori algorithm :

L_1= {frequent items};
for (k= 2; L_{k-1} !=∅; k++) do begin
C_k= candidates generated from L_{k-1}
for each transaction t in database do
increment the count of all candidates in C_k that are contained in t
L_k = candidates in C_k with *min_sup*
end
return $\cup_k L_k$;

IV. CONCLUSION

In This work, we presented a novel detection system that is able to detect malicious connections over SSL.

Fig: Malicious connections over SSL

V. FUTURE SCOPE

We have shown that Athtek Netwalk can reliably and efficiently detect malware traffic. In future we want to implement a graphical user frame work for detecting next likely system to be infected in the network by using a data mining tool.

VI. REFERENCES

[1] W. Lu, et al., "Clustering botnet communication traffic based on n-gram feature Selection," Computer Communications, 2010.

[2] D. Dittrich and S. Dietrich, "P2P as botnet command and control: a deeper insight," 2008, pp. 41-48.

[3] P. Wang, et al., "An advanced hybrid peer-to-peer botnet," IEEE Transactions on Dependable and Secure Computing, pp. 113-127, 2008.

[4] R. Schoof and R. Koning, "Detecting peer-to-peer botnets," University of Amsterdam, 2007.

[5] M. Feily, et al., "A survey of botnet and botnet detection," 2009, pp. 268-273.

[6] W. Strayer, et al., "Botnet detection based on network behavior," Botnet Detection, pp. 1-24, 2008.

[7] H. R. Zeidanloo, et al., "Botnet detection based on common network behaviors by Utilizing Artificial Immune System (AIS)," 2010, pp. V1-21--25.

[8] B. Saha and A, Gairola, "Botnet: An overview," *CERT-In White PaperCIWP-2005.*

[9] M. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, "A multifaceted approach to understanding the botnet phenomenon," in *Proc. 6th ACM SIGCOMM Conference on Internet Measurement (IMC'06)*, 2006, pp.41–52.

[10] N. Ianelli, A. Hackworth, "Botnets as a vehicle for online crime," *CERT Request for Comments (RFC) 1700*, December 2005.

[11] Honey net Project and Research Alliance. Know your enemy: Tracking Botnets, March 2005. See http://www. honeynet.org/papers/bots/.

[12] G. Schaffer, "Worms and Viruses and Botnets, Oh My!: Rational Responses to Emerging Internet Threats", *IEEE Security & Privacy*,.

Authors

Dr.G.Narsimha is a Professor in Computer Science and Information Technology Department at JNTUH, kondagattu, karimnagar. His research interests include Computer Networks, Adhoc Networks, Network Security, Data mining and warehousing and Cloud computing.

D.Jyothi is a Ph.D candidate in computer science and engineering at the JNTUH hyderabad, Associate Professor at Laqshya institute of science and Technology She's a member of the ISTE. Her research interests include malware analysis and malware defense and data mining and warehousing.