International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

An Improved Real Time Method for Detection, Blocking and Traceback of Malicious Traffic Over TOR

Rinaj Gafoor[1], Charlse M Varghese[2]

[1]Student of KMP College of Engineering, Perumbavoor, Ernakulam

[2]Assistant Professor at KMP College of Engineering, Perumbavoor, Ernakulam

Abstract: ***Tor is a prominent low-latency anonymous communication system. But it is currently abused in numerous ways. Attackers choose Tor because of its assurance of communication privacy. To gain an insight into such abuse, it is necessary to designed and implemented a novel system, for the discovery and the systematic study of malicious traffic over Tor. In this paper a novel real-time detection method based on fractal and information fusion is proposed. It focuses on the intrinsic macroscopic characteristics of network. It regards network traffic as the signal, and synthetically considers the macroscopic characteristics of network under different time scales with the fractal theory, including the self-similarity and the local singularity, which don't vary with the topology structures, the protocols and the attack types. To facilitate forensic traceback of malicious traffic, we implemented a dual-tone multi-frequency signaling-based approach to correlate botnet traffic at Tor entry routers and that at exit routers.***

Keywords: Tor, Malicious Traffic, Traceback, Intrusion Detection System

1. Introduction

Tor is a popular overlay network that provides anonymous communication over the Internet for TCP applications and helps fight against various Internet censorship [1]. It serves hundreds of thousands of users and carries terabyte of traffic daily. Unfortunately, Tor has been abused in various ways [2]. Copyrighted materials are shared through Tor. The illicit businesses can be deployed through Tor hidden service. Attackers also run botnet Command and Control (C&C) servers and send spam over Tor.

Attackers pick Tor as a result of its protection of communication privacy, which is achieved in the following way. A user uses source routing, selects a few Tor routers, and builds an anonymous route along these Tor routers. Traffic between the user and the destination is relayed along this route. The last hop, called exit router, acts as a "proxy" to directly communicate with the destination. Hence, Tor exit routers often become substitutes and are barraged with copyright act notices and botnet and spam complaints. Since Tor exit routers are mainly hosted by volunteers, these abusing activities prevent potential volunteers from hosting exit routers and hinder the advancement of Tor as a large-scale privacy-enhancing network.

In this work, an Improved Real Time Method for the analysis of Malicious Traffic over Tor, which integrates an Intrusion Detection System (IDS) along with DMFIF at Tor exit routers for Tor malicious traffic detection is suggested. This implements a defence mechanism to block malicious traffic. The IDS is configured to send alerts to a monitoring agent, which retrieves the source IP addresses and ports of the suspicious traffic and sends the tear-down command to the exit router through our modified Tor control protocol. The exit router disconnects the specific connection. The system deploy the IDS with extensive rule sets, which are updated regularly to block as much malicious traffic. The proposed system can be also used to traceback malicious traffic across Tor for forensic purpose.

In this a real-time detection method (DMFIF) based on fractal and information fusion is proposed. It regards network flow as the signal, and focus on the intrinsic characteristics of network, and synthetically takes into account the macroscopic characteristics of network traffic under the different time scales with the fractal theory, including the self-similarity and the local singularity, which don't vary with the topology structures, the protocols. Firstly, the self-similarity and the local singularity are used to describe accurately the characteristics of network traffic, and two detection results are acquired by using the nonparametric CUSUM algorithm to detect the traffic abnormalities of the above characteristics, and the final detection result is acquired by fusing the above two detection results with the Dempster-Shafer evidence theory.

We propose a dual-tone multi-frequency (DTMF) signaling based approach to correlate botnet traffic at Tor entries and that at Tor exits. We use "phantom" IRC messages, which do not interfere with the bot or botmaster, and pack these IRC messages into cells and control the cell transmission frequencies at our exit router. Two frequencies are used to embed secret binary signals into a target circuit. Once the two feature frequencies are detected at our controlled entry routers, the suspect botnet IP address can be identified.

2. Malicious Traffic Detection

In this area, we first present the architecture design to gather and analyse malicious traffic in the live Tor system and afterward expound the detailed framework setup.

2.1 System Architecture for malicious traffic collection

Tor traffic can be classified as inbound and outbound traffic. Inbound Tor traffic is encrypted and transmitted between OR and OR or between OP and OR. Outbound Tor traffic is decrypted by the Tor exit router and forwarded to an application server. An exit router behaves as a proxy for a Tor client and communicates with the application server.

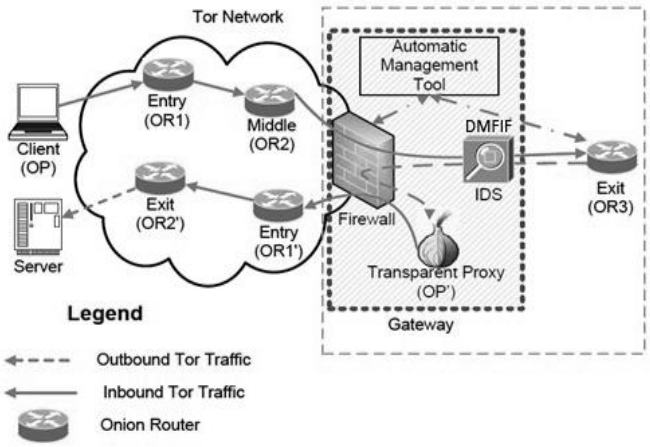

Figure 1: System Architecture for malicious traffic collection

The system consists of four logical components: a firewall, an IDS using DMFIF, a transparent proxy, and a Tor exit router. Port forwarding is enabled at the firewall to enable communication between the exit router and middle routers in the public network. To attract other Tor clients to select our exit router, our exit router is set to accept all traffic and has a relatively large average bandwidth.

3. Blocking of Malicious Traffic

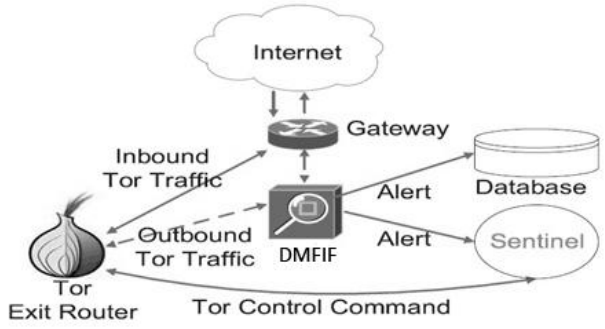

Figure 2: Blocking Malicious Traffic

The intrusion detection alerts from IDS based on the analysis of DMFIF and make a decision of either disconnecting or keeping the corresponding outbound traffic through our custom Tor control protocol. Fig.2 illustrates the structure of the system for this purpose.

In this defense system, there are four components: a Tor exit router, an IDS based on DMFIF, a sentinel, and a database. The IDS monitors traffic passing through the exit router and sends alerts to the sentinel for real-time processing and to the database for offline analysis. The sentinel retrieves the destination of a suspect connection from the alerts and sends our customized disconnection command to the Tor exit router through the Tor control protocol. The Tor exit router obtains the IP address and port, and then searches its connection list. Once the suspect connection is found, the corresponding connection will be terminated.

3.1 Overview of DMFIF

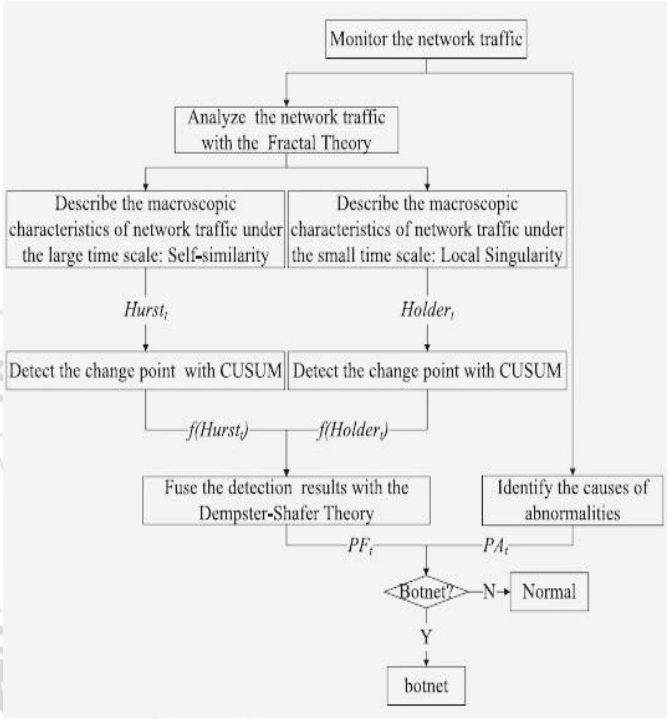

Figure 3: The process of DMFIF

The detection method proposed in the paper focuses on the intrinsic characteristics of network, which reflects not the "unique" abnormalities of P2P botnet but the "common" abnormalities of them. It regards network traffic as the signal, and synthetically considers the characteristics of network under different time scales with the fractal theory, including the self-similarity and the local singularity, which don't vary with the topology structures, the protocols and the attack types of P2P botnet [30]. Firstly, the self-similarity and the local singularity are used to describe accurately the characteristics of network, and two detection results are acquired by using the nonparametric CUSUM algorithm to detect the traffic abnormalities of the above characteristics, and the final detection result is acquired by fusing the above detection results with the Dempster-Shafer evidence theory.

3.1.1 Fractal Theory

Fractal refers to a rough or fragmented geometric shape which is able to split into parts, each of which is (at least approximately) a reduced-size copy of the whole shape. Network traffic exhibits the characteristics of the signal, and it can be regarded as the signal. The studies showed that network traffic exhibits an inherent characteristic fractal, including the self-similarity (Single fractal) under the large time scale and the local singularity (Multi-fractal) under the small time scale. The botnet will make the number of IP packets increase, which leads to the change of the self-similarity and the local singularity of network traffic, so P2P

botnet can be detected with the help of the above characteristics.

Self-similarity: Studies have demonstrated that the self-similarity process is able to better describe the characteristics of network traffic than the traditional short-term correlation model. Self-similarity refers to that there is a certain degree of consistency between the local structure and the overall structure.

Local singularity: For many non-uniform fractal processes, one dimension is not able to describe all the characteristics of it. After in-depth studies on TCP flow, found that the self-similarity is only one aspect of the fractal of network traffic under the large time scale. The network traffic exhibits self-similarity under the large time scale, but it behaves differently under the small time scale. Compared with the constant scale parameter under the large time scale, signals under the small time scale possess an irregular changing exponent, so these signals have been called multi-fractal. Generally speaking, self-similarity focus on the global characteristics of a process, and the self-similarity describes how the whole process changes from one scale to another. In other word, it characterizes the characteristic of a process under the large time scale. On the contrary, multi-fractal cares more about the local singularity of a process, which means the characteristic of a process under the small time scale. Multi-fractal is the extension and refinement of self-similarity, and is able to flexibly describe the irregular phenomenon under the local time scale that has little connection to the self-similarity of the network traffic under the large time scale.

3.1.2 Nonparametric CUSUM algorithm

Non-parametric CUSUM (Cumulative Sum) algorithm is able to detect the changes of the mean of a statistical process. It cumulates the small offset so as to achieve the effect of amplifying the offset. And it is typically used for monitoring change detection, and it is a sequential analysis technique, and it satisfies the requirements of detecting P2P botnets. The Hurst exponent $Hurst_t$ of the self-similarity and the Holder exponent $Holder_t$ of the local singularity are separately input into CUSUM to detect the abnormalities.

3.1.3 Dempster-shafer evidence theory

Since the characteristics of P2P botnet are complex and changeable, using a single network characteristic to describe the details of the network changes to detect botnet can lead to high false negative rate and false positive rate, so the information fusion method of decision level is adopted to solve the problem. There are many information fusion methods of decision level, include the Bayesian theory and the Dempster-Shafer evidence theory. The Bayesian theory requires the priori probability and the conditional probability for each question of interest, and requires that all the hypotheses are mutually independent and that all the hypotheses construct a complete set. The Dempster-Shafer evidence theory is a generalization of the Bayesian theory of subjective probability and it doesn't require the priori probability and conditional probability, and it is able to reduce the hypothesis set by combining the evidences gradually.

In the paper the Dempster-Shafer evidence theory is used to fuse the above two detection results, which allows one to combine evidences from different sources and arrive at a degree of belief that takes into account all the available evidences. Often used to fuse the information of sensor, the Dempster-Shafer evidence theory is based on two ideas: obtaining degrees of belief for one question from subjective probabilities for a related question, and Dempster's rule for combining such degrees of belief when they are based on independent items of evidence.

3.1.4 Process of DMFIF

Let t denote the current time, the process of DMFIF is:

(a) Capture network data from monitoring device, and get the number of IP packets. Meantime, get PA_t of TCP flow to identify that whether the abnormalities of network traffic are caused by P2P botnet or P2P application programs, so as to weaken the side effect on detecting the P2P botnet which the P2P application programs generate.

(b) Detect the abnormities of traffic flow under different time scale with the fractal theory.

Detect the abnormities of traffic flow under the large time scale Calculate the Hurst exponent with the method based on the sliding window, and then get the parameter $Hust_t$ to describe the self-similarity of network traffic under the large time scale, and finally get the output $f(Hust_t)$ after input $Hust_t$ into the nonparametric CUSUM algorithm.

Detect the abnormities of traffic flow under the small time scale Calculate the $Holder_t$ exponent to describe the local singularity of network traffic under the small time scale, and get the output $f(Holder_t)$ after input $Holder_t$ into the nonparametric CUSUM algorithm.

(c) Get the fused detection result PF_t with the Dempster-Shafer evidence theory.

(d) Synthesize the outputs and make the decision.

4. Dual-Tone Multi-Frequency Signaling Based Traceback

The goal of traceback is to correlate botnet traffic at an exit router and that at an entry router across Tor. For this purpose, adopt the dual-tone multi-frequency (DTMF) signaling approach [32], which has been used for telecommunication signaling over analog telephone lines in the voice frequency band between telephone handsets, other communications devices and the switching center. In DTMF, to send a single key such as "9", we select a low frequency and a high frequency, and send a sinusoidal tone of the two frequencies. The tone is decoded by the switching center to determine the key that was transmitted. The original DTMF adopts 8 frequencies to represent $4 \times 4 = 16$ keys. Here introduced a DTMF signaling based approach to tracing the botmaster or bots over Tor. In the following, represent the basic idea and the workflow,

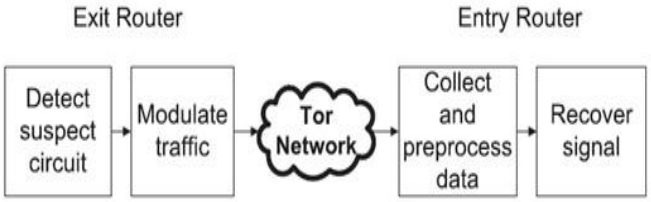

Figure 4: Workflow of the DTMF signaling

The basic idea of tracing botnet traffic is that at the controlled exit router, first inject extra cells at alternating frequencies that represents a signal into the suspect circuit and then attempt to confirm the signal at our controlled entry routers. If one entry detects the signal, this entry will be used to identify the IP addresses of botnet hosts, which actually create the suspect circuit. The DTMF signaling uses two different frequencies to represent bit 0 and bit 1, respectively.

Step 1 (Detecting Suspect Circuit): With the help of an IDS using DMFIF, the exit router can find the suspect connection and corresponding circuit, which transmits the IRC bot traffic. The IP address and port are obtained accordingly.

Step 2 (Modulating Traffic): Once a suspect circuit is detected, inject artificial cells into the circuit and start the traceback procedure. For an IRC channel, messages in the injected cells should not be displayed. Two distinct frequencies for transmitting cells, denoted as feature frequencies, are selected to represent 0 and 1, respectively, and modulate a signal into the injected traffic.

Step 3 (Collecting and Pre-Processing Data): At our controlled entry routers, record cells for each circuit in order to derive the feature frequency embedded in cells and recover a signal.

Step 4 (Recovering Signal): In this step, we apply the Fourier transform. If a circuit indeed carries the botnet traffic, strong amplitudes will be observed at feature frequencies. The IP address that creates the suspect circuit will disclose the suspect botnet.

5. Conclusion

In this work, a novel system for the discovery, blocking, and traceback of malicious traffic over Tor is introduced. The proposed system inspects the passing traffic through an IDS using DMIFIF at a Tor exit router. To block malicious traffic at an exit router, deployed IDS to forward alerts to a sentinel agent of proposed system, which can dynamically disrupt malicious traffic through our Tor control protocol. An effective real-time detection method (DMFIF) based on the fractal and information fusion theory is suggested to improve the existing methods. It synthetically considered the characteristics of network under different time scales with the fractal theory, including the self-similarity and the local singularity, which reflect the intrinsic characteristics of network and don't vary with the topology structures. To facilitate forensic analysis, we designed an effective dual-tone multi-frequency (DTMF) signaling based approach to tracing malicious traffic across Tor.

References

[1] Z. Ling, J. Luo, K. Wu, W. Yu, and X. Fu, "TorWard: Discovery, Blocking and Traceback of malicious traffic over Tor," IEEE Trans. Inf. Forensics Security, vol.10, no. 12, pp. 2515–2530, Dec. 2015.
[2] N. Christin, "Traveling the silk road: A measurement analysis of a large anonymous online marketplace," in Proc. 22nd Int. World Wide Web Conf. (WWW), 2013, pp. 213–224.
[3] Z. Ling, J. Luo, K. Wu, and X. Fu, "Protocol-level hidden server discovery," in Proc. 32nd IEEE Int. Conf. Comput. Commun. (INFOCOM), Apr. 2013, pp. 1043–1051.
[4] D. Storm. (2011). Fingered by IP: Does It Take Chutzpah to Run a Tor Exit Relay? [Online]. Available: http://blogs.computerworld.com/18892/ fingered by ip does it take chutzpah to run a tor exit relay.
[5] D. McCoy, K. Bauer, D. Grunwald, T. Kohno, and D. Sicker, "Shining light in dark places: Understanding the Tor network," in Proc. 8th Int. Symp. Privacy Enhancing Technol. (PETS), 2008, pp. 63–76.
[6] A. Chaabane, P. Manils, and M. A. Kaafar, "Digging into anonymous traffic: A deep analysis of the Tor anonymizing network," in Proc. 4th Int. Conf. Netw. Syst. Secur. (NSS), 2010, pp. 167–174.
[7] Z. Ling, J. Luo, K. Wu, W. Yu, and X. Fu, "TorWard: Discovery of malicious traffic over Tor," in Proc. 33th IEEE Int. Conf. Comput. Commun. (INFOCOM), Apr./May 2014, pp. 1402–1410.
[8] D. Brown. (2010). Resilient Botnet Command and Control With Tor. [Online]. Available: https://www.defcon.org/ images/defcon-18/dc-18-presentations/D.Brown/DEFCON-18-Brown-Tor CnC.pdf
[9] (2015). Tor2web: Visit Anonymous Websites. [Online]. Available: http://tor2web.org/
[10] Anonymous. (2012). IAmA a Malware Coder and Botnet Operator, AMA. [Online]. Available: http://www.reddit.com/r/IAmA/comments/sq7cy/
[11] C. Guarnieri. (2012). Skynet, a Tor-Powered Botnet Straight From Reddit. [Online]. Available: https://community.rapid7. com/community / infosec /blog/2012/12/06/Skynet-a-tor-powered botnet-straight-from-reddit
[12] (2012). Dec. 2012 Skynet Tor Botnet/Trojan.Tbot Samples. [Online]. Available: http://contagiodump.blogspot.ca/2012/12/dec2012-skynettor- botnet-trojantbot.html
[13] (2015). Freenet. [Online]. Available: https://freenetproject.org/
[14] A. Matrosov. (2013). The Rise of TOR-Based Botnets. [Online]. Available: http://www.welivesec-urity.com/2013/07/24/therise-of-tor-based-botnets/
[15] L. Øverlier and P. Syverson, "Locating hidden servers," in Proc. IEEE Secur. Privacy Symp. (S&P), May 2006, pp. 100–114.
[16] D. Danchev. (2013). Cybercriminals Experiment With Tor-Based C&C, Ring-3-Rootkit Empowered, SPDY Form Grabbing Malware Bot. [Online]. Available: http://blog.webroot.com/2013/07/02/ cybercriminals-

experiment-with-tor-based-cc-ring-3-rootkit-empoweredspdy-form-grabbing-malware-bot/
[17] S. J. Murdoch, "Hot or not: Revealing hidden services by their clock skew," in Proc. 13th ACM Conf. Comput. Commun. Secur. (CCS), Nov. 2006, pp. 27–36.
[18] L. Zhang, J. Luo, M. Yang, and G. He, "Application-level attack against Tor's hidden service," in Proc. 6th Int. Conf. Pervasive Comput. Appl., 2011, pp. 509–516.
[19] A. Biryukov, I. Pustogarov, and R.-P. Weinmann, "Trawling for Tor hidden services: Detection, measurement, deanonymization," in Proc. 34th IEEE Symp. Secur. Privacy (S&P), May 2013, pp. 80–94.
[20] G. Tian, Z. Duan, T. Baumeister, and Y. Dong, "A traceback attack on freenet," in Proc. 32th IEEE Int. Conf. Comput. Commun. (INFOCOM), Apr. 2013, pp. 1797–1805.
[21] Y. Xiang, I. Natgunanathan, D. Peng, W. Zhou, and S. Yu, "A dual channel time-spread echo method for audio watermarking," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 383–392, Apr. 2012.
[22] S. Yu, G. Zhao, W. Dou, and S. James, "Predicted packet padding for anonymous Web browsing against traffic analysis attacks," IEEE Trans. Inf. Forensics Security, vol. 7, no. 4, pp. 1381–1393, Aug. 2012.
[23] (2015). Transparently Routing Traffic Through Tor. [Online]. Available: https://trac.torproj-ect.org/projects/tor/wiki/doc/TransparentProxy
[24] Open Information Security Foundation (OISF). (2015). Suricata. [Online]. Available: http://www.openinfosecfoundation.org/
[25] Emerging Threats Pro, LLC. (2015). Emerging Threats. [Online]. Available: http://www.emergingthreats.net/
[26] (2015). Barnyard2. [Online]. Available: http://www.securixlive.com/barnyard2/
[27] (2008). Basic Analysis and Security Engine (BASE) Project. [Online]. Available: http://base.secureideas.net/
[28] Z. Ling, J. Luo, W. Yu, M. Yang, and X. Fu, "Extensive analysis and large-scale empirical evaluation of Tor bridge discovery," in Proc. 31th IEEE Int. Conf. Comput. Commun. (INFOCOM), Mar. 2012, pp. 2381–2389.
[29] S. J. Murdoch and G. Danezis, "Low-cost traffic analysis of Tor," in Proc. IEEE Secur. Privacy Symp. (S&P), May 2006, pp. 183–195.
[30] Song Yuanzhang, "Detecting P2P botnet by analyzing macroscopic characteristics with fractal and information fusion," in China Communications, February 2015, pp.107-117.
[31] K. Bauer, D. McCoy, D. Grunwald, T. Kohno, and D. Sicker, "Low resource routing attacks against anonymous systems," in Proc. ACM Workshop Privacy Electron. Soc. (WPES), Oct. 2007, pp. 11–20
[32] (2015). Dual-Tone Multi-Frequency Signaling. [Online]. Available: http://en.wikipedia.org/ wiki /Dual-tone_multi-frequency_signaling
[33] Z. Ling, J. Luo, W. Yu, X. Fu, D. Xuan, and W. Jia, "A new cell counting-based attack against Tor," in Proc. 16th ACM CCS, Nov. 2009, pp. 578–589.

Author Profile

Rinaj Gafoor received the B.Tech degree in Computer Science and Engineering from Mahatma Gandhi University, Kottayam, Kerala, India in 2011 and currently pursuing final year M.Tech degree in Computer Science and Engineering with specialization in Cyber Security from KMP College of Engineering, Perumbavoor, Ernakulam. His research interests include network security, information/data security, operating system security and digital forensics.

Charlse M Varghese received the B.E degree and M.E degree in Computer Science and Engineering from Anna University, Chennai, Tamilnadu, India in 2013 and 2015 respectively. He is currently an Assistant Professor with Department of Computer Science and Engineering, KMP College of Engineering, Perumbavoor, Ernakulam.