IEICE TRANS. COMMUN., VOL.E93–B, NO.8 AUGUST 2010

LETTER

Identifying IP Blocks with Spamming Bots by Spatial Distribution

Sangki YUN[†], **Byungseung KIM**[††], ***Nonmembers***, **Saewoong BAHK**[†††], ***and*** **Hyogon KIM**[†a)], ***Members***

SUMMARY In this letter, we develop a behavioral metric with which spamming botnets can be quickly identified with respect to their residing IP blocks. Our method aims at line-speed operation without deep inspection, so only TCP/IP header fields of the passing packets are examined. However, the proposed metric yields a high-quality receiver operating characteristics (ROC), with high detection rates and low false positive rates.

key words: *botnet, spamming, identification, detection, false positive*

1. Motivation

Botnets are analogous to multi-utility tools — they can serve as the platform from which to launch various illegitimate operations such as spamming, distributed denial-of-service (DDoS) attacks, incrementing click counters, and worm propagation. Today, there is an increasingly pressing need to develop methods to identify them in various circumstances to prevent them from wreaking havoc on the Internet services. One of the most difficult aspects of botnet identification is that individual bots keep a low profile by staying dormant most of the time and even when active, generating little traffic [1]. Therefore, monitoring the traffic behavior in terms of individual IP addresses is likely to fail to grasp the collective behavior of botnets. In this letter, we attempt to overcome this difficulty by monitoring blocks of IP addresses and develop a metric to tell whether a given block harbors a bot with high precision. We take the case of spamming bots in this letter, and show how to identify the likely residing locales of botnets in the Internet address space by "shallow" packet inspection of the Internet traffic.

2. IP Blocks Formation

In order to identify bot habitats in terms of IP address blocks, we first start with the /16 prefix for the block size since the recent prefix allocations are very conservative. For instance, the Asia-Pacific Network Information Center (APNIC) allocates smaller blocks such as /24 or /19 to ISPs [2]. Then for further refinement of the blocks, we use the hop distances of the email senders in a given block, measured from the given vantage point. Specifically, we extract the TTL value from the IP header and compute the hop distance by subtracting the TTL value from one of the typically used initial values. Most operating systems today use either 32, 64, 128, or 255 for the initial TTL. We pick the closest initial TTL to estimate the hop distance of the spammer. For instance, if the TTL from the IP header is 25, we choose 32 for the initial TTL and 7 for the hop distance to the spammer. Our assumption is that within a block, the bot nodes in the same botnet will be placed in the comparable hop distances. But in order to account for the hop distance differences among bot nodes in the same IP block, we split out a new block only if the difference exceeds 3. Figure 1 shows an example of the blocking. In the 163.152/16 network, there are two instances where the adjacent mail sender addresses differ by more than 3 hops. Although we started with a single block of size /16, we refine it into three blocks. For instance, we ran the blocking algorithm against a spam database containing 200,000 spams collected by the Korea Information Security Agency (KISA) over a three day period in September 2009. We obtained 8,604 blocks, which excludes the /16 blocks from which no spam mails were received.

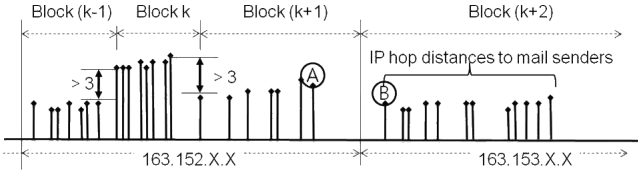

Fig. 1 Block demarkation by hop distances to mail senders.

3. Metrics

Once the block formation is done, we can compute metrics for each block to tell if a given block harbors bots. In our previous work based on two large SMTP traces from 2006 and 2007 [3], we developed two metrics. First, the *density of sources* (DS) is given as the ratio of the number of distinct sources in the block to the number of distinct sizes of mails. The higher DS is, the more likely the block is botnet-compromised. The rationale is that there will be relatively large number of bots in the botnet harboring block that will send mails with the same contents (i.e., a single spamming campaign). The second metric is the *dispersion of destinations* (DD), as defined by the Kullback-Leibler (KL) divergence between the mail destination distribution and uniform random distribution. The lower the value is, the more likely

Manuscript received January 16, 2010.
Manuscript revised April 7, 2010.
[†]The authors are with Korea University, Korea.
[††]The author is with Samsung Electronics, Korea.
[†††]The author is with Seoul National University, Korea.
a) E-mail: hyogon@korea.ac.kr
DOI: 10.1587/transcom.E93.B.2188

Table 1 A single bot transmitting various emails.

Time	Size in bytes	Subject
00:33:31	17169	Prove to your...
00:33:31	17185	Prove to your...
00:33:31	17175	Prove to your...
00:37:37	2302	=?koi8-r?B?Q2...
00:37:37	2308	=?koi8-r?B?Q2...
00:37:37	2324	=?koi8-r?B?Q2...
00:37:37	2286	Get a diploma...
00:37:37	2288	Get a diploma...
00:37:37	2288	Get a diploma...
00:37:37	2288	Get a diploma...
00:37:37	2284	Get a diploma...
03:24:50	6099	Create more b...
03:24:50	6101	Create more b...
04:41:09	6097	Your super-ab...
04:41:09	6099	Your super-ab...
04:41:09	6049	Magnet for fe...
04:41:09	6045	Magnet for fe...
04:41:10	6116	Wanna look un...
04:41:10	6116	Wanna look un...
04:41:10	6108	Wanna look un...
04:41:10	6114	Wanna look un...
04:41:10	6110	Wanna look un...
04:41:10	6110	Wanna look un...
05:15:32	16036	Got free time...
05:30:43	15957	Got free time...

the block is botnet-compromised. It assumes that the spammers randomly choose mail destinations, unlike normal mail servers whose mail destinations should have a certain bias. These two metrics, however, have drawbacks. First, in case a single bot almost simultaneously participates in multiple spam campaigns, the DS metric can be seriously distorted, which would lead to a high false negative rate. Indeed, we find some evidence of such behavior by spamming bots in the more recent KISA spam captures. Table 1 shows that a single bot transmits spam mails of various sizes in a relatively short duration of time.

On the other hand, the metric DD requires that the observer's (i.e. destination's) IP address space is considerable enough to hold a large number of legitimate mail servers to have a general distribution. This practically limits the usefulness of the metric for an observer's network with a small address space.

Based on the observations above, we propose a new metric called the *source spread* (SS). We still account for the number of spam senders n_{src} in the given IP block, but do not couple it with the number of distinct mail sizes. Instead, we use only the n_{src} as the main component of the new metric. In order to enhance the accuracy, we additionally consider the distribution of these spammers in the given IP block. Then we compute the KL divergence between the distribution and the uniform distribution. It measures how randomly the mail sources are dispersed in the given IP block. Now, the metric SS is defined to be

$$SS = \left(1 - \sum_{k=1}^{N} p(s_k) \log \frac{p(s_k)}{1/N}\right) \cdot n_{src} \quad (1)$$

where N is the number of IP addresses in the given IP block, $p(s_k)$ is the pmf of the sender address distribution, and n_{src} is the number of distinct spammer addresses. The larger the metric, the higher the likelihood that the given block harbors bot-based spammers.

In order to validate the usefulness of the newly developed metric, we test it against the KISA spam database. For comparison, we manually classified the 8,604 IP blocks from the IP blocking algorithm in Sect. 2. Our rule for manual classification is that if there are three or more distinct IP addresses in the given block that transmitted the same mail contents then the block is considered botnet-compromised. Next, we measure the SS for each block and compare it against a threshold. If the measured SS for a block is higher than the detection threshold, we regard the block as a spamming botnet block. Once we get the classification according to the SS metric, we compute the detection rate and the false positive rate against the manual classification. Figure 2 shows the two rates for various threshold values. Figure 3 summarizes the relation between the two rates in the Receiver Operating Curve (ROC) of SS metric and compares it with DS and DD. The figure shows that the false positive rate can be controlled relatively low for most detection rates. For instance at 90% target detection rate, the false positive remains just over 10%. On the other hand, both DS and DD have much higher false positive rates to achieve such a detection rate. Finally, this metric can be used in combination with other network-oriented metrics, some of which are easily found in the literature [1], [4], in order to further improve the ROC.

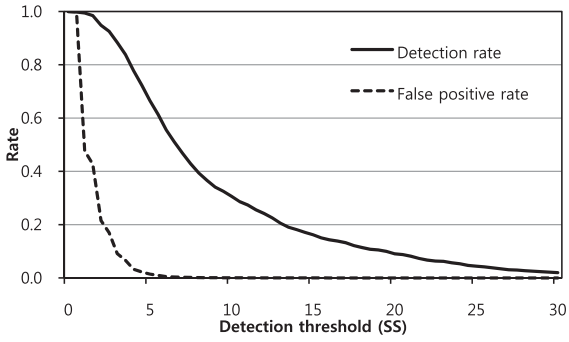

Fig. 2 False positive and detection rate of the Source Spread as a function of detection threshold.

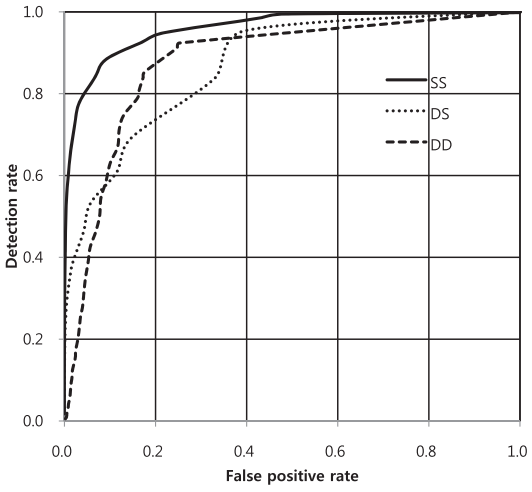

Fig. 3 ROC of the detection metrics.

4. Conclusion

Changing bot behaviors require redesign of existing botnet detection methods. In this letter, we develop a new spam botnet detection metric from our observations of recent spam campaigns. Computed for a given set of spams, the metric can classify a group of mail senders situated in proximity in terms of the IP addresses and the hop distances from the mail receiver whether they are bot-compromised. The receiver operating curve (ROC) of the metric shows that high detection rates are achievable for low false positive rates. Designed to inspect only the transport header of the packet, it can be easily used inside the network.

Acknowledgement

This work was supported by the IT R&D program of MKE/KEIT (KI001863), The Development of Active Detection and Response Technology against Botnet.

References

[1] A. Ranmachandran and N. Feamaster, "Understanding the network-level behavior of spammers," Proc. ACM SIGCOMM, 2006.
[2] Asia-Pacific Network Information Center (APNIC), Policies for IPv4 address space management in the Asia Pacific region, Feb. 2009. Available at: http://www.apnic.net/policy/add-manage-policy
[3] B. Kim, H. Kim, and S. Bahk, "NSF: Network-based spam filtering based on on-line blacklisting against spamming botnets," Proc. IEEE Globecom, 2009.
[4] L.H. Gomes, C. Cazita, and W. Meira, "Characterizing a spam traffic," Proc. Internet Measurement Conference (IMC), 2004.