The Method of Detecting Malware-Infected Hosts Analyzing Firewall and Proxy Logs

Kazunori Kamiya, Kazufumi Aoki, Kensuke Nakata, Toru Sato, Hiroshi Kurakami, Masaki Tanikawa

NTT Secure Platform Laboratories

{kamiya.kazunori, aoki.kazufumi, nakata.kensuke, sato.toru, kurakami.hiroshi, tanikawa.masaki}@lab.ntt.co.jp

I. Introduction

The number of security incidents is increasing and many of them are derived from malware activities. However, recent malware have become so sophisticated that commercial anti-virus software is not capable of detecting 100% of them. NTT Global Threat Intelligence Report shows that more than half of malware are not detected by commercial antivirus software [1]. Nowadays, post-infection countermeasure is important to minimize the damage caused by malware.

SIEM(Security Information and Event Management) is a strong approach which analyzes network and security logs to detect infected hosts. In SIEM approach, analyzing Proxy logs by matching with HTTP-based malicious list is effective to detect infected hosts. In fact, HTTP-based detection method is shown to give high accuracy [2]. However, the problem is that HTTP-based detection does not cover non-HTTP communication of malware activity.

Kato et al. propose detection method analyzing Firewall logs [3]. However they do not target HTTP-based communication of malware activity. Moreover, their detection method is based on heuristics taken from malware samples, which is difficult to scale for evolving malware.

In this paper, we propose the detection method that analyzes Firewall logs as well as Proxy logs. This method detects infected-hosts by using both TCP/IP-based malicious list and HTTP-based malicious list. All of malicious lists are automatically generated by dynamic analysis of malware and training with network traffic logs.

Our evaluation results show that the method is capable of detecting malware-infected hosts which is not detected by HTTP-based malicious list. The method contributes 6% to improve the accuracy compared with sole Proxy-based detection. Thus, we show that multi-layer analysis based on Firewall logs as well as Proxy logs is effective to improve malware detecting capability.

II. Firewall and Proxy Logs in Enterprise Network

To start examining malware activity in enterprise network, we describe typical network structure of enterprise in Figure 1.

Firewall is the point where all the OUTBOUND traffic arrives. Proxy is the point where OUTBOUND HTTP traffic reach. In enterprise, since large part of OUTBOUND traffic is HTTP, most of OUTBOUND traffic would pass through Proxy to reach Firewall. However, a little non-HTTP traffic directly comes to Firewall but they are dropped by Firewall policy. (Firewall only permits direct internet access for servers.)

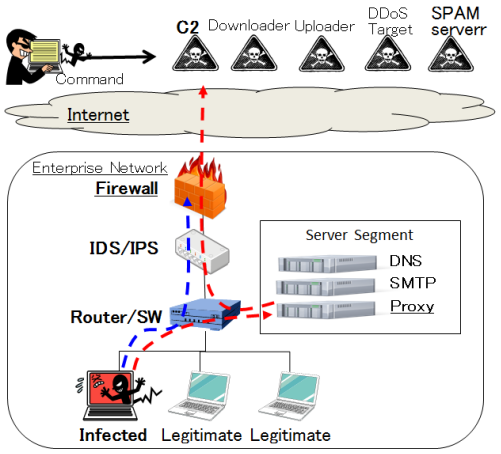

Figure 1 Typical Network Structure of Enterprise

Firewall is enabled to send its ACCEPT/DENY log as syslog. If both ACCEPT and DENY logs are collected, all OUTBOUND traffic from clients is monitored. However the volume of ACCEPT logs tend to be large and it would be preferred that Firewall send only DENY logs. Still in this case, most of OUTBOUND traffic is monitored in combination with Proxy logs since most of OUTBOUND ACCEPT traffic is HTTP.

Table 1 shows typical log field included in either Firewall logs or Proxy logs. In Firewall logs, TCP/IP-based traffic parameters are collected. Proxy logs include HTTP-based parameters in addition to TCP/IP-based parameters.

Table 1 Fields taken from Firewall and Proxy logs

	Firewall	Proxy
timestamp	OK	OK
ip_proto	OK	Limited (TCP only)
src_ip	OK	OK
dst_ip	OK	Limited (HTTP only)
dst_port	OK	Limited (HTTP only)
http_url	NG	OK

III. The Method of Detecting Malare-Infected Hosts

We propose the method of detecting compromised hosts based on Firewall logs and Proxy logs. The method consists of 2 phases:

phase1) generate malicious lists from malware traffic logs and network traffic logs

phase2) detect infected hosts by matching traffic with malicious lists

A. The method of extracting malicious lists

Figure 2 shows the process of extracting malicious lists from malware samples and network logs.

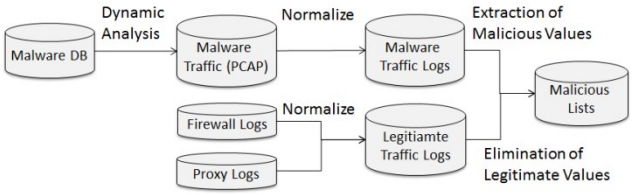

Figure 2 Process of malicious list extraction

The first step is collecting malware traffic logs by dynamic analysis of malware. Dynamic analysis should be run to control OUTBOUND traffic not to give damage to real network [4].

Dynamic analysis gives malware traffic in PCAP format. Now, it is transformed into session stream and TCP/IP parameters are decoded. If protocol is HTTP, HTTP parameters are also decoded. After these processes, malware traffic logs are acquired in normalized format that include TCP/IP-based fields and HTTP-based fields shown in Table 1.

Second step is collecting legitimate traffic logs from real network devices. Now Firewall logs and Proxy logs are collected in the period of no incident occurrence. Then, both Firewall logs and Proxy logs are transformed into normalized format that include fields shown in Table 1.

Final step is creating malicious lists from malicious traffic logs and legitimate traffic logs. This is done by extracting popular values in malware traffic logs as well as eliminating frequently used values of legitimate traffic logs. This step is formulated as below.

Suppose we have malware sets M and legitimate host sets L. Now when we have value k in field α of malware traffic logs filtered by condition β, the occurrence rate of value k for malware traffic logs : $PM_{\alpha,\beta}(k)$ and that of legitimate logs $PL_{\alpha,\beta}(k)$ is calculated as follows.

$$PM_{\alpha,\beta}(k) = \frac{n\left(m_{\alpha,\beta}(k)\right)}{n(M)}$$

$$PL_{\alpha,\beta}(k) = \frac{n(l_{\alpha,\beta}(k))}{n(L)}$$

where $m_{\alpha,\beta}(k) \in M$ is set of malware that have value k in the field α of malicious traffic logs filtered by condition β, and $l_{\alpha,\beta}(k) \in L$ is that of legitimate traffic logs.

Malicious list of field α with filtering condition β is extracted to meet following conditions.

$$\Phi_{\alpha,\beta} = \{k \mid PM_{\alpha,\beta}(k) > tm, PL_{\alpha,\beta}(k) < tl\}$$

To lower the false positive, tl value should be small enough.

B. The method of detecting malware-infected host

We define two types of detection method. The one is frequency-based method which triggers detection if host traffic matches single value of malicious list for more than specified times. The other is sort-based method which detect if host traffic matches more than specified number of values from malicious list. Each of method is formulated as below.

For $k \in \Phi_{\alpha,\beta}$, $w_{\alpha,\beta}(k)$ is defined as the number of times k occurs, and $s(k)$ is defined as follows.

$$s_{\alpha,\beta}(k) = \begin{cases} 0, & w_{\alpha,\beta}(k) = 0 \\ 1, & w_{\alpha,\beta}(k) > 0 \end{cases}$$

Then, $w_{\alpha,\beta}$: the number of logs that match single value in malicious list, $s_{\alpha,\beta}$: the unique number of value that match malicious list are defined as follows.

$$w_{\alpha,\beta} = \max_k w_{\alpha,\beta}(k) \quad s_{\alpha,\beta} = \sum_k s_{\alpha,\beta}(k)$$

By using threshold $tw_{\alpha,\beta}$, frequncy-based detection triggers when $w_{\alpha,\beta} > tw_{\alpha,\beta}$. Same way, using threshold $ts_{\alpha,\beta}$, sort-based detection triggers when $s_{\alpha,\beta} > ts_{\alpha,\beta}$.

Malicious lists are generated with every set of field α and condition β, and detection is executed respectively.

IV. Evaluation

A. Data Sets

Malware traffic logs are extracted from about 10 thousands of malware which are acquired from VirusTotal [5] in a week. Dynamic analysis is executed for 5 minutes for each malware. We confirm that the SHA1 hash value are all different and malware family names are well diversified.

Legitimate traffic logs are collected from Firewall and Proxy of enterprise network for 1 week. The number of hosts are in thousands order.

We generate training data sets and evaluation data sets by dividing both malicious traffic logs and legitimate traffic logs by 7 so that we execute 7-fold cross validation.

B. Evaluation Criteria

TPR(True Positive Rate) and FPR(False Positive Rate) for single set of field α and condition β is defined as follows.

$$\text{TPR} = \frac{n(md_{\alpha,\beta})}{n(M)} \quad \text{FPR} = \frac{n(ld_{\alpha,\beta})}{n(M)}$$

where $md_{\alpha,\beta}$ is set of detected hosts of malicious traffic logs and $ld_{\alpha,\beta}$ is that of legitimate traffic logs. When we have multiple sets of field and condition, total TPR, total FPR is defined as follows.

$$\text{Total TPR} = \frac{n(\cup_{\alpha,\beta} md_{\alpha,\beta})}{n(M)} \quad \text{Total FPR} = \frac{n(\cup_{\alpha,\beta} ld_{\alpha,\beta})}{n(L)}$$

C. Evaluation

We select 4 following sets of field and condition.

a)dst_port(ip_proto=TCP)

b)dst_port(ip_proto=UDP)

c)dst_ip(ip_proto=TCP, dst_port=80)

d)http_url(none)

Namely, from a) to c) are sets for evaluating Firewall-based detection. d) is for evaluating Proxy-based detection. Frequency-based method is applied for a) to c). Sort-based method is applied for d).

Table 2 shows the result of single field evaluation. We measured 2 types of TPR/FPR with threshold $T_{selected}$ and $T_{\max\_tpr}$. $T_{selected}$ is optimized threshold($tw_{\alpha,\beta}$ or $ts_{\alpha,\beta}$) that gives the highest TPR by satisfying FPR < 0.005. $T_{\max\_tpr}$ equals 1 such that TPR is the highest but FPR tends to be large. We measured $T_{\max\_tpr}$ to see the sensitivity of threshold.

Table 2 Single Field Evaluation

Field α (Condition β)	$T_{selected}$		$T_{\max\_tpr}$	
	TPR	FPR	TPR	FPR
dst_port(ip_proto=TCP)	0.056	0.0036	0.071	0.0060
dst_port(ip_proto=UDP)	0.025	0.0025	0.025	0.0025
dst_ip (dst_port=80)	0.16	0.0042	0.82	0.063
http_url (none)	0.72	0.0011	0.72	0.0011

Table 3 shows the result of multiple field evaluation which select 1 Firewall field and 1 Proxy field(http_url), then calculate total TPR, total FPR and TPR contribution of Firewall fields.

Table 3 Multiple Field Evaluation with http_url

Field α (Condition β)	Total TPR	Total FPR	FW Field Contribution
dst_port(ip_proto=TCP)	0.75	0.0046	0.035
dst_port(ip_proto=UDP)	0.73	0.0036	0.015
dst_ip (dst_port=80)	0.73	0.0050	0.017

1) Consideration on dst_port malicious list

In Table 2, TPR of dst_port is small such as 0.056 for TCP, 0.025 for UDP. The reason is that most of malware uses dst_port=80(HTTP access) and comparably a little malware use other ports than 80(non-HTTP access).

However, Table 3 shows that dst_port contributes effectively for TPR improvements by 0.035(62.5% of single field TPR) for TCP and 0.015(60% of single field TPR) for UDP. It means about 5% of malare use only specific dst_port for communication rather than HTTP connection.

Contributed dst_ports are shown in Figure 3. TCP139, TCP445 and UDP137 traffic are Windows-related protocol which is considered to scan or infect other hosts in Internet. UDP78 and UDP9000 are for host scanning. TCP25 seems spam traffic. Other dst_ports traffic are unknown but may be used as C2 communication.

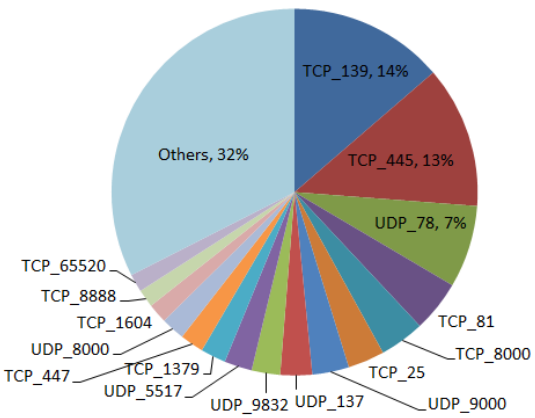

Figure 3 Contributed dst_port

Threshold is easily tuned to achieve low FPR since TPR of $T_{selected}$ is quite near from or the same as TPR of $T_{\max\_tpr}$.

2) Consideration on dst_ip malicious list

Table 2 shows that TPR for $T_{\max\_tpr}$ is high(0.82), but TPR for $T_{selected}$ decreases a lot. This indicates that threshold tuning for field dst_ip is not easy. The reason of TPR decrease with $T_{selected}$ is that many malicious URLs are hosted in same IP address with legitimate web site. This is often the case for hosting service providers, CDN service providers, and file download site.

Still, Table 3 shows that dst_ip malicious list a little(1.7%) contribute to TPR improvement. We confirm that malicisous dst_ips that contribute have following characteristics. 1) Traffic that uses dst_port=80 but is not HTTP, 2) Traffic which uses HTTP protocol but http_url is not listed in malicious list.

3) Total Contribution of Firewall Fields

Figure 4 shows total contribution of all evaluated Firewall fields. Firewall fields, such as dst_port (TCP/UDP) and dst_ip(dst_port=80), contributes 6% to improve TPR.

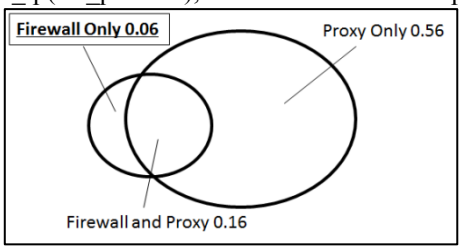

Figure 4 TPR Contribution of Firewall Fields

V. Conclusion and Future Work

We propose the method of detecting malare-infected hosts by analyzing both Firewall logs and Proxy logs. We show that the method is capable of detecting malware-infected hosts which is not detected by HTTP-based malicious list. The method contributes 6% to improve the accuracy compared with sole Proxy-based detection. Thus, we show that multi-layer analysis is effective to improve malware detecting capability.

Future work will evaluate the method with different data sets such as malware collected in longer period of time. We also plan to expand the method for other log sources such as IDS/IPS logs and DNS/SMTP server logs.

REFERENCES

[1] NTT Global Threat Intelligence Report, http://www.nttgroupsecurity.com/
[2] T.Nelms, R.Perdisci and M.Ahamad, ExecScent: Mining for New C&C Domains in Live Networks, UseNix Security, 2013
[3] J.Kato, M.Hatada, F.Takeuchi, T.Kadota, Detection method of malware activity based on the Firewall log, IWSEC, 2009.
[4] K. Aoki, T.Yagi, M. Iwamura, and M. Itoh, Controlling Malware HTTP Communications in Dynamic Analysis System Using Search Engine, CSS, 2011
[5] VirusTotal, https://www.virustotal.com/