Detection of Novel-Type Brute Force Attacks Used Ephemeral Springboard IPs as Camouflage

Satomi Honda, Yuki Unno, Koji Maruhashi, Masahiko Takenaka, and Satoru Torii

***Abstract*—In recent years, the way of brute force attacks has become more tactical and tricky to avoid being detected by intrusion detection or prevention systems (IDS/IPS). In this paper, we show that we have detected three organized or systematic brute force attack instances from actual network monitoring logs by visualization focused on source IPs and detection time. One of the instances shows that specific terminals have been attacked used innumerable IPs for a long time. These IPs were like ephemeral because they had appeared almost only one time. We also propose a new system, DEMITASSE, for detecting such terminals in the earlier phase and mitigating the damage caused by brute force attacks used ephemeral IPs. We conduct feasibility studies with our logs and evaluate DEMITASSE can detect and mitigate that kind of attacks effectively.**

***Index Terms*—Log analysis, brute force attacks, network monitoring, network security.**

I. Introduction

Brute force attacks are one of the most famous attacks to obtain pairs of user names and passwords to login some network services illegally. Attackers often refer to dictionaries to find available pairs in a less trial than trying for all existing words. Default settings like "admin" as user name or "0000" as password also give them a benefit [1]. Furthermore, they come to use more effective dictionaries, called password lists [2]. Once attackers get pairs of user names and passwords list used one network service, they try to login other network services with that list. The reports on these kinds of brute force attacks are increasing in recent years.

The way of brute force attacks has become more tactical and tricky like this. In April 2013, a contents management system "WordPress" has been attacked. It is said that the attack had considered more than 1,000,000 attacks and that more than 90,000 servers had been used for that. Accounts using user names "admin" was the main target [3], [4]. In November of the same year, a source code management system "GitHub" has also been attacked. GitHub was attacked with long term from about 40,000 IP addresses. It is said that the attacked passwords were weak or shared with other services [5]. In both attacks attackers targeted weak passwords to obtain pairs of user names and passwords effectively. And they used innumerable IP addresses to avoid being detected by intrusion detection or prevention systems (IDS/IPS).

Several institutes also report these trends. IBM SOC report has said some brute force attacks on Secure Shell (SSH) or File Transfer Protocol (FTP) are from multiple IP addresses (IPs) a day and that the number of times for login trials had been about from 10 to 30 from one IP [6]. The blog entries from SANS Internet Storm Center and Dragon Research Group have said some brute force attacks on SSH by much unique IPs have occurred and that PCs with those IPs were infected by botnets [7], [8]. It is difficult to find this kind of brute force attack only by analyzing network monitoring logs form one server or network service.

In this paper we analyze large-scale network monitoring logs from multi network services to discover and extract unknown security threats or criminal techniques. We focus on our network monitoring log down to network IDS logs. In our IDS logs, attacks from one terminal to the other are detected as IP addresses (source IP and destination IP) that are allocated to each terminals. We have visualized our IDS logs from 2011 to 2012 focused on source IPs and detection time. As a result, we have detected three organized or systematic brute force attack instances on SSH. I) One source IP have attacked to several destination IPs for a long time. II) One source IP have attacked to several destination IPs repeatedly at almost the same time every day. III) Specific destination IPs have been attacked used ephemeral IPs for a long time. That is, one source IP has attacked to several destination IPs for a specific term, and the other IPs have attacked to the same destination IPs after a brief interval. The term range is from only one minute to several hours. The source IP has tried to login tens of times per minute and destination IPs have attacked almost at the same time.

Especially, attack instance III has never reported as long as we know. We named attack instance III "Ephemeral BFs." One Ephemeral BF attack is defined as that one source IP attacks on several destination IPs for a specific term. We call Ephemeral BFs as a set of several Ephemeral BF attacks. In Ephemeral BFs, the number of times for login trials is small and source IPs are like ephemeral. Because of the fact that different IPs had appeared in each attacks, we guess that these IPs are prepared as springboard to camouflage brute force attacks. With these behaviors, it is difficult to detect Ephemeral BFs by only collecting or analyzing IDS logs from one network service. Furthermore it is ineffective to shut down the traffic from IPs which has been detected as Ephemeral BFs.

To counter Ephemeral BFs, we propose a new system called DEMITASSE for detecting and mitigating Ephemeral BFs. DEMITASSE works for detecting destination IPs and mitigating the damage caused by Ephemeral BFs. This system extracts destination IPs from IDS logs earlier than collecting a

Manuscript received January 25, 2013; revised April 20, 2014.

The authors are with the Fujitsu Laboratories LTD., 4-1-1, Kamikodanaka, Nakahara-ku, Kawasaki, Kanagawa, 211-8588, Japan (e-mail: honda.satomi@ jp.fujitsu.com).

DOI: 10.7763/JACN.2014.V2.126

large amount of IDS logs using characteristics among source IPs, detection time and the number of times for login trials. And it mitigates the damage by detecting the beginning of Ephemeral BFs and shuts down the traffic from IPs corresponding to the attack promptly.

Our contributions are as follows:

1) We detect novel-type brute force attacks (Ephemeral BFs) by visualization focused on destination IPs and detection time.
2) We propose a new system for detecting and mitigating the damage caused by Ephemeral BFs.
3) We evaluate that DEMITASSE can mitigate the damage by Ephemeral BFs effectively.

In Section II, we describe brute force attacks reports and related works. We describe our large-scale network monitoring logs analysis and show three types of brute force attack instances in Section III. In Section IV, we propose a new system for detecting destination IPs and mitigating the damage by Ephemeral BFs, DEMITASSE. We conduct feasibility studies DEMITASSE in Section V. Finally, we conclude in Section VI.

Here src-IP means source IP address and dst-IP means destination IP address. One brute force attack has occurred means a src-IP brute force attacked to a dst-IP. We deal with the number of times for login trials following the IDS we are using.

II. Related Works

Many kinds of brute force attacks are reported from universities, companies and institutes. Spreotto *et al*. have reported brute force attacks which consist of three phase, scanning, brute-force and die-off. They have also proposed the detection method based on Hidden Markov Model [9]. Vykopal *et al*. have classified brute force attacks into three patterns according to the number of src-IPs and dst-IPs: 1:1, 1:N and N:1. And they have investigated and taken statistics of each patterns about their university network traffic [10]. They have also shown several methods for detecting brute force attack and discussed shortcomings of flow-based detection [11]. In 2010 IBM SOC report has said that some brute force attacks on Secure Shell (SSH) or File Transfer Protocol (FTP) had tended to be from multiple IP addresses (IPs) per day [6]. They have shown that a lot of unique src-IPs had appeared for a few days with the line chart. It has also said the number of times for login trials had been about from 10 to 30 from one IP. In 2010 and 2011 the blog entries from SANS Internet Storm Center and Dragon Research Group have also said that a lot of unique src-IPs had detected as origins of brute force attacks on SSH and that those IPs were infected by botnets [7], [8]. SANS have shown a part of their logs and unique IPs however we can't see full IP address. In 2013 IBM SOC report have raised up the topic about brute force attack again [12]. Like those reports or entries, there have been some brute force attacks used innumerable IPs.

As described in introduction, the damage by brute force attacks used much unique IPs are increasing. In 2013, contents management system like WordPress and GitHub have become victims with brute force attacks [1], [4], [5]. Both attacks were from multiple IP addresses and have taken a long time on order to success attacks stealthily.

There are many proposed and existing network monitoring systems. Takenaka *et al*. have analyzed actual network monitoring log and report random or super-slow port scans used multi IPs have occurred [13]. Nicter presented by NICT or TSUBAME by JP-CERT/CC are monitoring darknet traffic and publish annual reports about their analysis [14], [15]. Many papers have proposed systems for detecting malicious activities by monitoring network traffic [16]-[18]. As described in [19], Jelena *et al.* has shown many papers had proposed systems for detecting distributed denial-of-service (DDoS). DDoS is related to Ephemeral BFs in attack source is multiple IPs.

In general, IDS/IPS contains the function to evaluate IP addresses. That evaluates IP addresses monitoring result, country code and etc [20], [21]. Anomaly detection technologies are also effective for detecting or preventing from brute force attacks. Feily *et al*. has classified the botnet detection into four categories, Signature-based, Anomaly-based, DNS-based and Mining-based. Anomaly-based and Mining-based detection are equal to Anoaly detection [22]. Lazarevic *et al*. have introduced Point Anomalies, Contextual Anomalies and Collective Anomalies and show examples of applying anomaly detections to IDS [23]. Those anomaly detection technologies can detect sudden increase of login trials or long-term access. Collaborative intrusion detection systems (CIDSs) are also many proposed. CIDSs combine evidences analyzed from multiple networks simultaneously to detect coordinated attacks ex.DDoS. Chenfeng *et al*. have surveyed coordinated attacks like worm activities or DDoS and classified existing CIDs [24]. According to that, CIDs have been classified into three categories in their system architectures, Centralized, Hierarchical and Distributed. In this paper, we show that the concept of CIDs is effective in detection of brute force attacks with several instances.

III. Extracting Novel-Type Brute Force Attacks

There exists trends of network services or attackers' wills in the sea of some network traffic logs. We can discover these trends by analyzing network monitoring logs carefully. We are analyzing large-scale network monitoring logs form multi network services to discover and extract unknown security threats or criminal techniques. Most existing analyses emphasize on logs received from only one server. However, they can't analyze deeply other servers' attacked situations. For example, many servers were attacked or not, at the same time, from the same src-IPs and so on.

A. Visualization Focused on Dst-IPs and Detection Time

We have applied our logs to visualization focused on dst-IPs and detection time. As a result, we have detected three organized or systematic brute force attack instances on SSH. One of the most advantages of our visualization is that we can figure out easily how attacks have occurred among different servers. Our visualization shows network IDS logs as a scatter chart. The horizontal axis, the vertical axis and the marker indicate detection time, unique dst-IPs and src-IPs. The shape of the marker varies according to src-IPs.

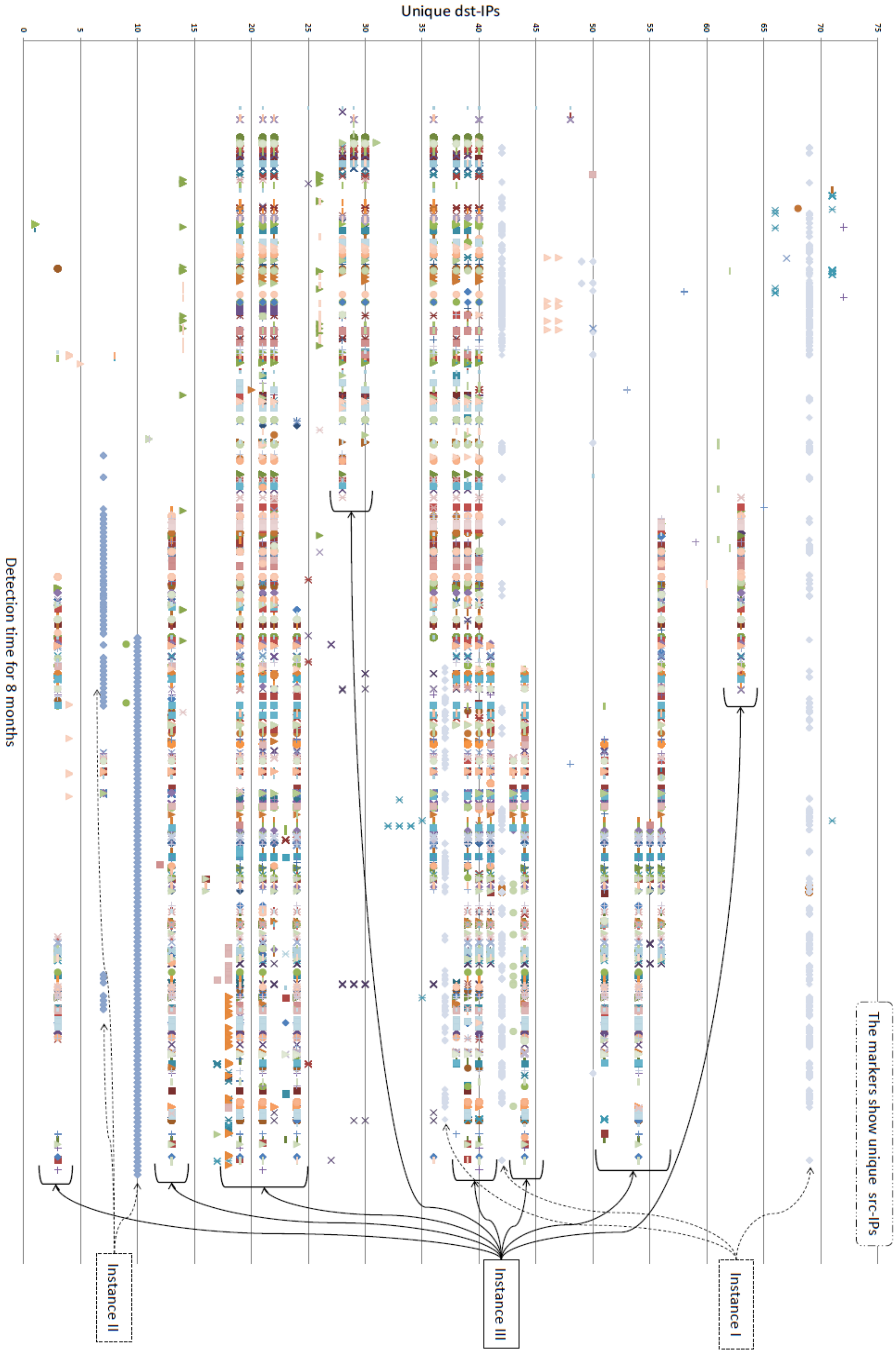


Fig. 1. Our visualization result.

We extracted records in eight months from 2011 to 2012 detected as SSH login brute force attacks from our IDS logs. We show the result of our visualization applied the eight-month records in Fig. 1. At the next subsection, we describe brute force attack instances we have detected in detail.

A. Detected Brute Force Attack Instances

We describe three brute force attack instances. I) One src-IP has attacked to several dst-IPs for a long time. II) One src-IP has attacked to several dst-IPs for a long time only at specific time every day. III) Specific dst-IPs has been attacked used ephemeral src-IPs for a long time. This instance has never been reported as long as we know.

1) Attack instance I

One src-IP has attacked on several dst-IPs. This instance is well-known as one of the typical brute force attack models. However the number of times for login trials was around about 20 to 30 times. We suspect attackers tried to avoid being detected by IDS/IPS as [6]-[8] reported.

2) Attack instance II

One src-IP has attacked to several dst-IPs only at specific time every day. This instance is similar to attack instance I. In addition to that, this instance has periodicity for time. However, most IDS can detect this kind of brute force attack.

3) Attack instance III

We named this instance "Ephemeral BFs." Specific dst-IPs has been attacked used ephemeral src-IPs. One src-IP has been attacked on several dst-IPs for a specific term. The attacked term varied from only one minute to several hours. The src-IP has tried to login tens of times per minute and dst-IPs have attacked almost the same time. For example, a src-IP H_1 attacked to dst-IPs V_1, V_2, …, V_n at time t_1. At the next time t_2, another src-IP H_2 attacked to the same dst-IPs V_1, V_2, …, V_n.

As long as we know, we have first detected this kind of brute force attack instance. This instance seems to be similar to the cases that IBM SOC, SANS and Dragon Research Group have reported as [6]-[8], [12]. In addition to these reports, we have grasped the fact that several dst-IPs had attacked simultaneously. As these institutes have said, it is difficult for existing detection technologies to detect or prevent from this Ephemeral BFs. Here one Ephemeral BF attack is one src-IP attacks brute force attack to dst-IPs for a specific term. We call Ephemeral BFs as a set of Ephemeral BF attacks. We describe the characteristics of Ephemeral BFs in detail and guess the attackers' wills at the next subsection.

B. Characteristics of Ephemeral BFs

Ephemeral BFs has four characteristics in point of src-IPs, dst-IPs, the number of times for login trials and detection time. We extracted 378 src-IPs and 450 Ephemeral BF attacks from our logs.

1) Characteristics in src-IPs

At first, most src-IPs attacked only once per Ephemeral BF attack. This is the reason why we named "Ephemeral." Table I and II show detected dates and country codes about src-IPs corresponding to Ephemeral BFs. The figures of brackets in Table I shows the number of src-IP which was detected for continuous days. Table I indicates that about 80% of all src-IPs appeared only a day. According to Table II, major code was CN (China) but various codes were also there. From that information, it is ineffective to shut down the traffic from IP addresses that have attacked as Ephemeral BFs once or twice before, or whose country is said to have much records about attacks somewhere.

TABLE I: DETECTED DATES OF SRC-IPS CORRESPONDING TO EPHEMERAL BFS.

Detected Dates	src-IPs
1	304(0)
2	53(14)
3	15(1)
4	4(3)
5	1(0)
8	1(0)

TABLE II: COUNTRY CODE (TOP 10).

Country Code	CN	US	KR	RU	IN
src-IPs	167	38	15	11	9
Country Code	BR	CA	TR	NL	DE
src-IPs	9	9	8	7	7

2) Characteristics in dst-IPs

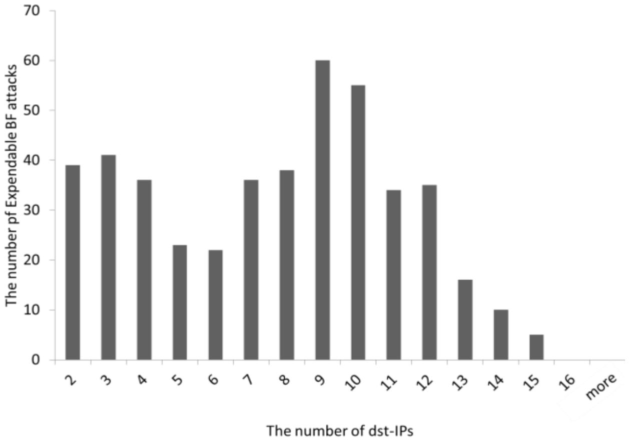


Fig. 2. Histogram about dst-IPs per ephemeral BF attack.

Second, specific dst-IPs has been attacked for a long time. However, some dst-IPs has not been attacked by several Ephemeral BF attacks. Fig. 2 shows the histogram about the number of dst-IPs per Ephemeral BF attack. The attack objects vary by each Ephemeral BF attacks. The group of Dst-IPs that has been attacked can't be found by observing only one server.

3) Characteristics in detection time

Forth, one Ephemeral BF attack occurred at the same time. We can see the same shape markers are plotted straight in lengh at Fig. 1. We extract 304 src-IPs that attacked for a day and plot each detection times as line at Fig. 3. How Ephemeral BF attacks lasted was different from each other.

As described above, strong correlation in detection time can't be found without observing multiple servers. Furthermore, all Ephemeral BFs can't be detected from the length of attacked term because the lengths are different from each other.

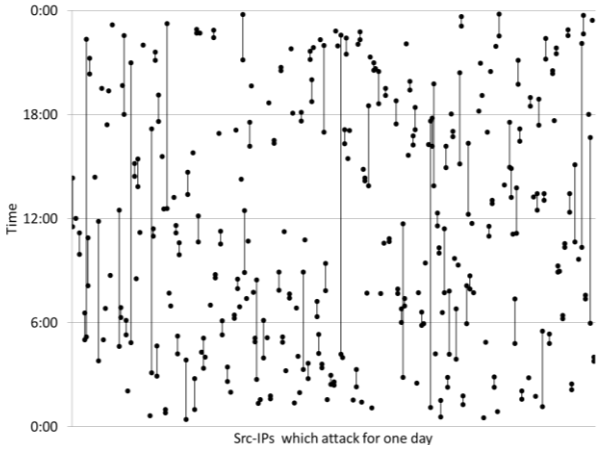


Fig. 3. How an ephemeral BF attack lasted.

4) Characteristics in the number of time for login trials

Third, the number of time for login trials was small. The average of the number of times for login trials from our all IDS logs was about 72.18. On the other hand, the average of the number of times for login trials in Ephemeral BFs was about 17.6. We show the maximum, minimum and averages of all Ephemeral BF attacks at Fig. 4. The upper side of line shows the maximum, lower side shows the minimum and the triangle marker shows the average of each Ephemeral BF attacks. Fig. 4 describes the number of times for login trials were smaller than common brute force attacks in most Ephemeral BFs. Common anomaly detection technologies can't always detect Ephemeral BFs because the number of time to login are small and feature points won't be appeared.

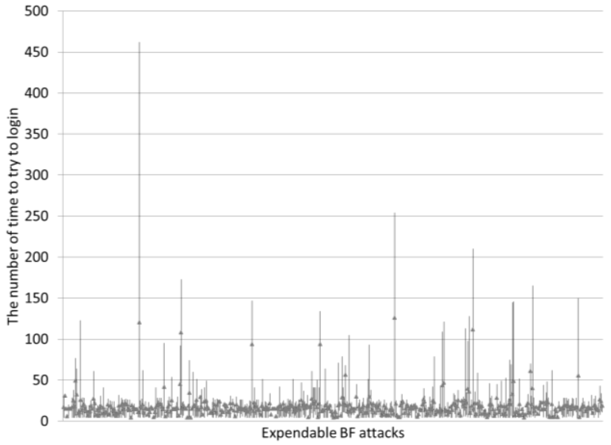


Fig. 4. The maximum, minimum and averages of all Ephemeral BF attacks.

C. Consideration about Ephemeral BFs

From these statistical results, we guess the following three topics about the background of Ephemeral BFs: There exists attackers who intend to try brute force attacks and prepare for innumerable IPs. Attackers use those IPs as springboard to camouflage their attacks with the small number of times for login trials in order to avoid being detected by IDS/IPS. They target several dst-IPs and keep on attacking persistently.

On the other hand, dst-IPs side doesn't notice easily they have been attacked.

As described at each subsections, it is ineffective to detect Ephemeral BFs by collecting IDS logs from only one server and applying existing detection methods. For example, creating blacklist about src-IPs to shut down their traffics is not effective because src-IPs are ephemeral and used like springboard as camouflage.

IV. Detecting and Mitigating System against Ephemeral BFs (DEMITASSE)

In this section, we propose a new system DEMITASSE, detecting and mitigating system against Ephemeral BFs, a system for detecting and mitigating the damage caused by Ephemeral BFs. As described in previous section, it is difficult to detect Ephemeral BFs for existing or well-known detection technologies. System whole architecture shows in Fig. 5. DEMITASSE consists of two phases, the first phase is detecting dst-IPs from IDS logs earlier than collecting a large amount of IDS logs by using characteristics among src-IPs, detection time and the number of times for login trials. The second phase is mitigating the damage by shutting down the traffic from IPs corresponding to Ephemeral BFs.

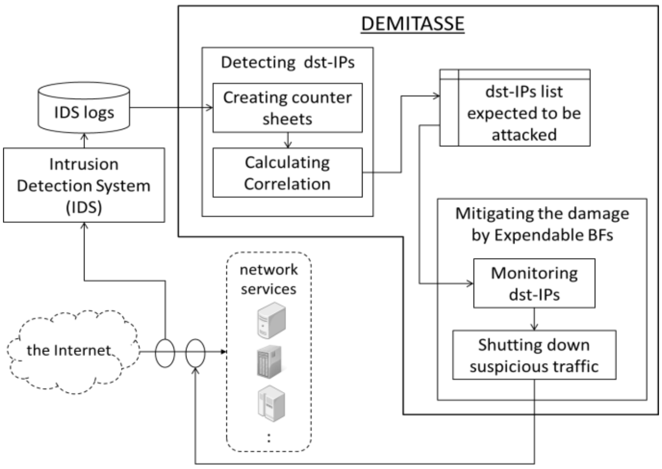

DEMITASSE
Detecting dst-IPs
IDS logs
Creating counter sheets
Calculating Correlation
dst-IPs list expected to be attacked
Intrusion Detection System (IDS)
Mitigating the damage by Expendable BFs
Monitoring dst-IPs
Shutting down suspicious traffic
network services
the Internet

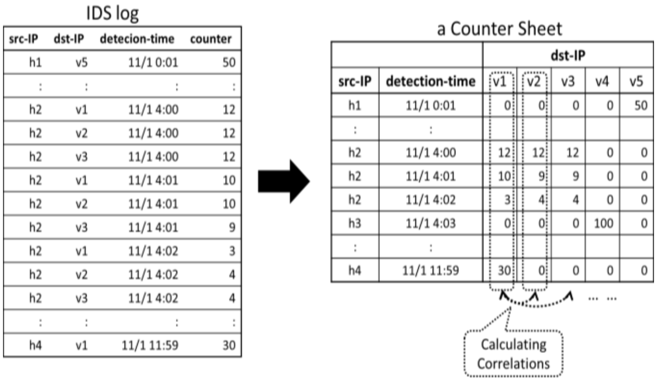
Fig. 5. The whole architecture of DEMITASSE.

A. Phase 1: Detecting dst-IPs from IDS Logs

We focus on characteristics that one set of Ephemeral BF attack has. At one set, a src-IP brute force to several dst-IPs at the same time. The numbers of times for login trials are also the same among dst-IPs. Therefore we can extract dst-IPs which received one set of Ephemeral BF attack without collecting a large amount of IDS logs and visualizing them. From the behaviors of Ephemeral BFs, extracted dst-IPs are expected to be attacked again near the future.

In the detecting phase, dst-IPs suspect to receiving Ephemeral BFs is extracted from IDS logs. IDS logs have following data structures: IP address which was detected as origin of brute force attacks (src-IP), IP address which was detected as being received brute force attacks (dst-IP), time when brute force attacks detected (detection-time), and the number of time to try to login (counter).

The detecting procedure is as follows. First, the counter is mapped from IDS logs to a counter sheet. An example of creating a counter sheet from IDS log in Fig. 6. The sheet has two dimensions, one is dst-IP and the other is a combination of detection-time and src-IP. Next, dst-IPs is extracted by calculating correlations and collecting dst-IPs with high correlations each other. One of methods for collecting dst-IPs with high correlations is to apply enumeration maximal cliques. Dst-IP pairs with high correlation are outputted by calculating correlations. Enumeration maximal cliques is applied by considering Dst-IP to node and one dst-IP pair to edge connected with each dst-IPs. The nodes set as maximal clique is equal to dst-IPs with high correlations each other. Therefore, these dst-IPs are outputted as they are expected to be attacked again near the future.



IDS log

src-IP	dst-IP	detecion-time	counter
h1	v5	11/1 0:01	50
:	:	:	:
h2	v1	11/1 4:00	12
h2	v2	11/1 4:00	12
h2	v3	11/1 4:00	12
h2	v1	11/1 4:01	10
h2	v2	11/1 4:01	10
h2	v3	11/1 4:01	9
h2	v1	11/1 4:02	3
h2	v2	11/1 4:02	4
h2	v3	11/1 4:02	4
:	:	:	:
h4	v1	11/1 11:59	30

a Counter Sheet

		dst-IP				
src-IP	detection-time	v1	v2	v3	v4	v5
h1	11/1 0:01	0	0	0	0	50
:	:					
h2	11/1 4:00	12	12	12	0	0
h2	11/1 4:01	10	9	9	0	0
h2	11/1 4:02	3	4	4	0	0
h3	11/1 4:03	0	0	0	100	0
:	:					
h4	11/1 11:59	30	0	0	0	0

Fig. 6. Example of creating counter sheets from IDS logs.

B. Phase 2: Mitigating the Damage Caused by Ephemeral BFs

The damage caused by next sets of Ephemeral BF attacks can be mitigated by monitoring dst-IPs extracted in previous phase. If a part of dst-IPs is detected as brute force by unknown src-IP, other dst-IPs are expected to be attacked by the src-IP as one Ephemeral BF. Hence DEMITASSE shuts down the traffic from the src-IP for a certain period. Due to this process, the damage to dst-IPs caused by Ephemeral BFs can be mitigated. For example, V_1, $V2$ and V_3 are extracted in the detecting phase. An unknown src-IP H_2 try to attack to V_1, V_2, V_3. DEMITASSE shut down the traffic from H_2 after detecting that H_2 attacked V_1, V_2 for a few minutes.

V. Feasibility Studies

In this section, we conduct feasibility studies that DEMITASSE can detect correct dst-IPs which are received Ephemeral BFs and mitigate the damage caused by Ephemeral BFs effectively.

A. Phase 1 (Detecting Phase)

In the detection phase, we can tune detection-time and threshold of correlation. Creating the counter sheet, detection-time can be tuned every second or minute according to characteristics of IDS. Threshold of correlation is necessary for calculating end determining dst-IP pairs with high correlations. We apply our IDS logs with various settings and evaluate extracted dst-IPs.

We apply our 1061 divided IDS logs to the detecting phase in DEMITASSE with various settings. We divided our IDS logs by dates. After that, we compare dst-IPs in false positive (FP) and false negative (FN). Detection-time varies every 1, 2, 3, 5 and 10 minutes. Threshold of correlation varies 0.8, 0.6 and 0.4. Note that we calculate correlation based on Pearson product-moment correlation coefficient and we use MACE in order to apply enumeration maximal cliques [25].

Fig. 7 shows FP and FN of extracted dst-IPs at each settings. FP rate was minimum at about 13% when detection-time was every minute and threshold of correlation was 0.8. FN rate was minimum at about 9% when detection-time was every minute and threshold of correlation was 0.4 or detection-time was every 2 minutes and threshold of correlation was 0.6. The amount of counter sheets increased by about 7.7 times at every 10 minutes compared with every minute. As two kinds of graphs show, there is trade-off between the accuracy and the amount of processing in extracting dst-IPs.

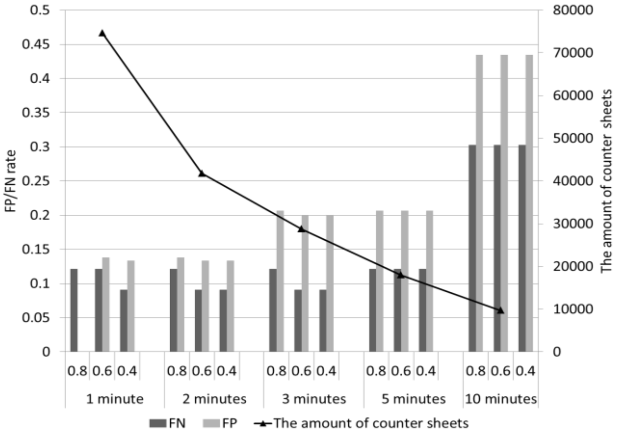


Fig. 7. FP and FN rates at each setting.

B. Phase 2 (Mitigating Phase)

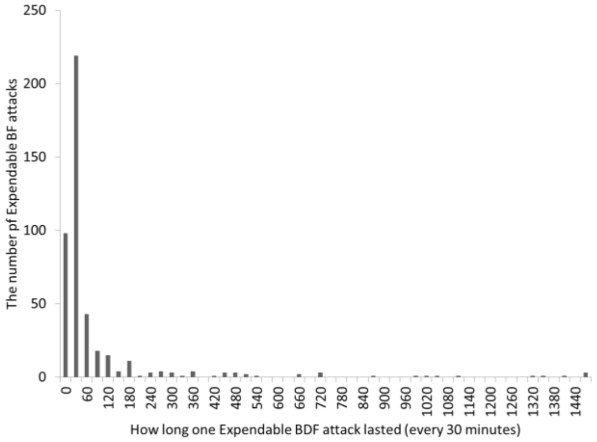


Fig. 8. Histogram with data range every 30 minutes.

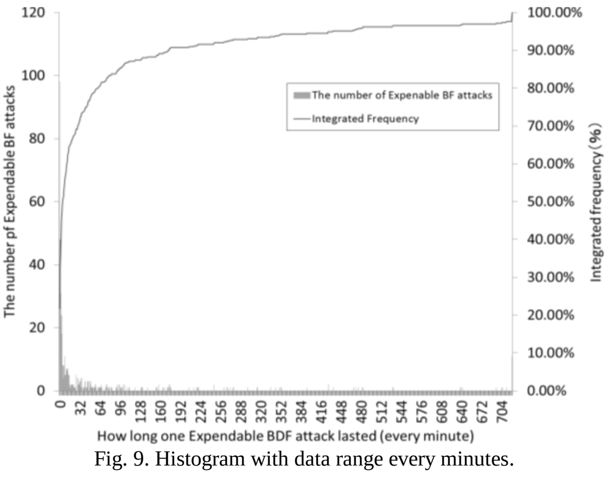


Fig. 9. Histogram with data range every minutes.

In the mitigation phase, we can tune two kinds of periods, one is how long the traffic shut down and another is from the first detection of unknown src-IPs to start shutting down the traffic. We create a histogram with data range every 30 minutes from 0 to 1440 minutes (Fig. 8). The peak of this histogram biased left side. Most of Ephemeral BF attacks can be shut down within about 720 minutes. To observe their relations in detail, we also create a histogram with data range every minute from 0 to 720 minutes (Fig. 9). The line shows integrated frequency. About 64% of Ephemeral BF attacks can be prevented by detecting traffic suspect of Ephemeral Bf attacks until 1 minute and shutting down this traffic for 10 hours.

VI. Conclusion

We have extracted a novel-type brute force attack, which we have named Ephemeral BFs, by observing multi servers and visualizing focused on dst-IPs and detection time. Though some cases similar to this kind of attack had been reported by several institutes in recent years, we have first grasped the fact that several dst-IPs had attacked simultaneously as long as we know. As a result of statistics about Ephemeral BFs, it is ineffective to detect Ephemeral BFs by collecting IDS logs from only one server and applying existing detection methods. To counter Ephemeral BFs, we have proposed a new system DEMITASSE for detecting and mitigating the damage caused by Ephemeral BFs. DEMITASSE detects dst-IPs using the correlation among src-IPs, detection time and the number of times for login trials from a certain amount of IDS logs. After that, it mitigates the damage by shutting down the traffic from src-IPs that are suspected to next Ephemeral BF attacks. We have shown that DEMITASSE can effectively mitigate the damage and protect dst-IPs by feasibility studies with our IDS logs.

Our future work will compare some kinds of logs output by different IDSs and consider which is the most suitable for DEMITASSE. It is also important to expand the monitoring range and examine Ephemeral BFs are appeared in other situations.

References

[1] US-CERT. Risks of Default Passwords on the Internet. [Online]. Available: http://www.us-cert.gov/ncas/alerts/TA13-175A

[2] Ars Technica. Mass-login attack on Nintendo fan site hijacks 24,000 account. [Online]. Available: http://arstechnica.com/security/2013/07/mass-login-attack-on-nintendn-fan-site-hijacks-24000-accounts/

[3] SUCRI Blog. Mass WordPress Brute Force Attacks? Myth or Reality. [Online]. Available: http://blog.sucuri.net/2013/04/mass-wordpress-brute-force-attacks-myth-or-reality.html

[4] SUCRI Blog. The Wordpress brute force attack timeline. [Online]. Available: http://blog.sucuri.net/2013/04/the-wordpress-brute-force-attack-timeline.html

[5] PCWorld. GitHub bans weak passwords after brute-force attack results in compromised accounts. [Online]. Available: http://www.pcworld.com/article/2065340/github-bans-weak-passwords-after-bruteforce-attack-results-in-compromised-accounts.html

[6] IBM. Tokyo SOC Report 2010, latter half of the year. [Online]. Available: https://www-304.ibm.com/connections/blogs/tokyo-soc/

[7] SANS Internet Storm Center. ISC Diary | Distributed SSH Brute Force Attempts on the rise again. [Online]. Available: https://isc.sans.edu/diary/Distributed+SSH+Brute+Force+Attempts+on+the+rise+again/9031

[8] Dragon Research Group. (April 29, 2011). SSH brute force attack source insight. [Online]. Available: http://www.dragonresearchgroup.org/2011/04/29/.

[9] A. Sperotto, R. Sadre, P. T. de Boer, and A. Pras, "Hidden markov model modeling of SSH brute-force attacks," presented at Int. Workshop on Distributed Systems: Operations and Management 2009, Venice, Italy, October 27-28, 2009.

[10] J. Vykopal, "A flow-level taxonomy and prevalence of brute force attacks," in *Proc. American Control Conference 2011(ACC 2011) Part II*, 2011, vol. 191, pp. 666-675.

[11] J. Vykopal, M. Drasar, and P. Winter, "Flow-based brute-force attack detection," *Advances in IT Early Warning*, 2013.

[12] IBM. Tokyo SOC Report 2013, first half of the year. [Online]. Available: https://www-304.ibm.com/connections/blogs/tokyo-soc/

[13] K. Furukawa, S. Shimizu, M. Takenaka, and S. Torii, "On detection for scarcely collided super-slow port scannings in IDSs' log-data," *Journal of Communications*, vol. 8, no. 11, pp. 788-794, November 2013.

[14] D. Inoue, M. Eto, K. Yoshioka, S. Baba, K. Suzuki, J. Nakazato, K. Ohtaka, and K. Nakao, "Nicter: An incident analysis system toward binding network monitoring with malware analysis," presented at WOMBAT Workshop on Information Security Threats Data Collection and Sharing, Amsterdam, Netherlands, April 21-22, 2008.

[15] JPCERT Cordination Center. TSUBAME. [Online]. Available: http://www.jpcert.or.jp/tsubame/

[16] C. C. Zou, L. Gao, W. Gong, and D. Towsley, "Monitoring and early warning for internet worms," in *Proc. 10th ACM Conference on Computer and Communications Security (CCS)*, 2003, pp. 190-199.

[17] V. Yegneswaran, P. Barford, and D. Plonka, "On the design and use of internet sinks for network abuse monitoring," presented at 7th International Symposium on Recent Advances in Intrusion Detection (RAID), Riviera, France, September 15-17, 2004.

[18] M. Bailey, E. Cooke, F. Jahanian, J. Nazario, and D. Watson, "The internet motion sensor: A distributed blackhole monitoring system," presented at Network and Distributed Security Symposium (NDSS), California, USA, Feburary 3-4, 2005.

[19] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39-53, April 2004.

[20] McAfee. McAfee network security platform. [Online]. Available: http://www.mcafee.com/japan/enterprise/nsp/.

[21] Cisco Systems. Cisco IPS. [Online]. Available: http://www.cisco.com/web/JP/product/hs/security/ids4200/index.html

[22] M. Feily, A. Shahrestani, and S. Ramadass, "A survey of botnet and botnet detection," presented at Third International Conference on Emerging Security Information. Systems and Technologies 2009, Athens/Glyfada, Greece, June 18-23, 2009.

[23] A. Lazarevic, A. Banerjee, V. Chandola, V. Kumar, and J. Srivastava, "Data mining for anomaly detection," presented at Tutorial at the European Conference on Principles and Practice of Knowledge Discovery in Databases(PKDD 2008), Antwerp, Belgium, September 15-19, 2008.

[24] C. V. Zhou, C. Leckie, and S. Karunasekera, "A survey of coodinated attacks and collaborative intrusion detection," *Computer & Security on ELSEVIER*, vol. 29, no. 1, pp. 124-140, 2010.

[25] K. Makino and T. Uno, "New algorithms for enumerating all maximal cliques," presented at 9th Scandinavian Workshop on Algorithm Theory, Humlebæk, Denmark, July 8-10, 2004.

Satomi Honda skipped her B.E. degree in 2010 and received her M.E. degree in information science in 2012 from Yokohama National University. Her mater thesis was software protection. Since 2012, she has been engaged in research and development on network security at Fujitsu Laboratories Ltd.

Yuki Unno has been engaged in research and development on application and cyber security at Fujitsu Laboratories Ltd., since 2007. She is a member of IPSJ.

Koji Maruhashi received his Ph.D. in engineering in 2013 from Tsukuba University. Since 1999, he has been engaged in research and development on data mining and big data analysis at Fujitsu Laboratories Ltd.

Masahiko Takenaka received his B.E. and M.E. degrees in electronic engineering in 1990, 1992 respectively from Osaka University. He received his Ph.D. in engineering in 2009 from Tsukuba University. Since 1992, he has been engaged in research and development on cryptography, side channel analysis and network security at Fujitsu Laboratories Ltd. He is currently a research manager. He was awarded Computer Security Symposium (CSS) Paper Prize in 2002 and 2004, and the OHM Technology Award in 2005. He is a member of IEICE.

Satoru Torii received his B.E. degrees in information science in 1985 from Tokyo University of Science. Since 1985, he has been engaged in research and development on network security at Fujitsu Laboratories Ltd. He is currently a research manager. He was awarded Computer Security Symposium (CSS) Paper Prize in 2004. He is a preceding director of IPSJ.

Image Processing and Pattern Recognition