International Journal of Electrical and Computer Engineering (IJECE)
Vol. 6, No. 4, August 2016, pp. 1681~1684
ISSN: 2088-8708, DOI: 10.11591/ijece.v6i4.10320

Analysis of Brute Force Attacks with Ylmf-pc Signature

Anton Valeryevich Arzhakov, Dmitry Sergeevich Silnov
Department of Information Systems and Technologies, National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, Russia

Article Info

Article history:

Received Jan 18, 2016
Revised Mar 14, 2016
Accepted Mar 29, 2016

Keyword:

Brute force
Mail spam
Scanning
Ylmf-pc

ABSTRACT

Brute force techniques used in many fields of authentication process. Ftp servers, web servers and mail servers very often got threatened by attackers. Old technique for mail service brute force still working and it can be easily detected by special signature. Main sources of attacks were detected and separated by countries and time of the day. Bursts of attacks detected depending on weekdays.

Corresponding Author:

Dmitry Sergeevich Silnov,
Department of Information Systems and Technologies,
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe sh. 31, Moscow, Russian Federation.
Email: ds@silnov.pro

1. INTRODUCTION

In today's world, information security has become a very crucial issue like never before. With unauthorized access to certain services, an attacker can cause significant financial damage to the victim. Any modern information resource [1],[2] may be subject to attack. So, the various seemingly minor attacks should not be overlooked. Such attacks include brute force attack with Ylmf-pc signature [3] against a mail server.

2. ANALYZING THE PROBLEM

With time, many mail server owners are faced with a situation where the server log file (an example is shown in Figure 1 is filled with lots of records about attempts to connect to the server from the user ylmf-pc.

As can be seen in the Figure 1, the server blocks connection from ylmf-pc, which sends wrong smtp ehlo/helo command [4]. Ylmf-pc is the name used during authentication on the server. Upon receipt of this command, the server checks whether the name sent matches with the IP address from where the command came, and if they don't match, then it is most likely that person is an unscrupulous user. The server terminates or doesn't terminate such connection depending on the server settings. The attack is aimed at obtaining the authentication password of an e-mail server via a brute force attack. If authentication is successful, the attacker gains access to the mail server account from where spam will be subsequently sent. It is widely believed that servers, whose security was breached using ylmf-pc queries, are one of the largest Cutwail/Pushdo botnets [5]. However, there is no reliable information that the attacking computers or compromised computers are part of this botnet [6].

```
00:01:29 H=(ylmf-pc) rejected EHLO or HELO ylmf-pc: HELO/EHLO - ylmf-pc blocked
00:01:41 H=(ylmf-pc) rejected EHLO or HELO ylmf-pc: HELO/EHLO - ylmf-pc blocked
00:01:50 H=(ylmf-pc) rejected EHLO or HELO ylmf-pc: HELO/EHLO - ylmf-pc blocked
00:02:01 H=(ylmf-pc) rejected EHLO or HELO ylmf-pc: HELO/EHLO - ylmf-pc blocked
00:02:15 H=(ylmf-pc) rejected EHLO or HELO ylmf-pc: HELO/EHLO - ylmf-pc blocked
00:02:28 H=(ylmf-pc) rejected EHLO or HELO ylmf-pc: HELO/EHLO - ylmf-pc blocked
00:02:39 H=(ylmf-pc) rejected EHLO or HELO ylmf-pc: HELO/EHLO - ylmf-pc blocked
00:02:50 H=(ylmf-pc) rejected EHLO or HELO ylmf-pc: HELO/EHLO - ylmf-pc blocked
00:03:00 H=(ylmf-pc) rejected EHLO or HELO ylmf-pc: HELO/EHLO - ylmf-pc blocked
00:03:13 H=(ylmf-pc) rejected EHLO or HELO ylmf-pc: HELO/EHLO - ylmf-pc blocked
00:03:26 H=(ylmf-pc) rejected EHLO or HELO ylmf-pc: HELO/EHLO - ylmf-pc blocked
00:03:37 H=(ylmf-pc) rejected EHLO or HELO ylmf-pc: HELO/EHLO - ylmf-pc blocked
00:03:52 H=(ylmf-pc) rejected EHLO or HELO ylmf-pc: HELO/EHLO - ylmf-pc blocked
00:04:02 H=(ylmf-pc) rejected EHLO or HELO ylmf-pc: HELO/EHLO - ylmf-pc blocked
00:04:12 H=(ylmf-pc) rejected EHLO or HELO ylmf-pc: HELO/EHLO - ylmf-pc blocked
00:04:26 H=(ylmf-pc) rejected EHLO or HELO ylmf-pc: HELO/EHLO - ylmf-pc blocked
```

Figure 1. An example of the log-file

As can be seen from Figure 2, there is no cyclic pattern of queries, but it should be noted that activity peaks on weekends. At the same time, it should be remembered that the time of the attacker and not of the victim should be taken into account. These observations coincide with the patterns derived in [7]. On weekdays, when servers are busy sending out spam emails, less resources are allocated to the botnet for its hacking attempts on new servers. But during weekends when the spam effectiveness falls, the servers deploy the bonnet to expand.

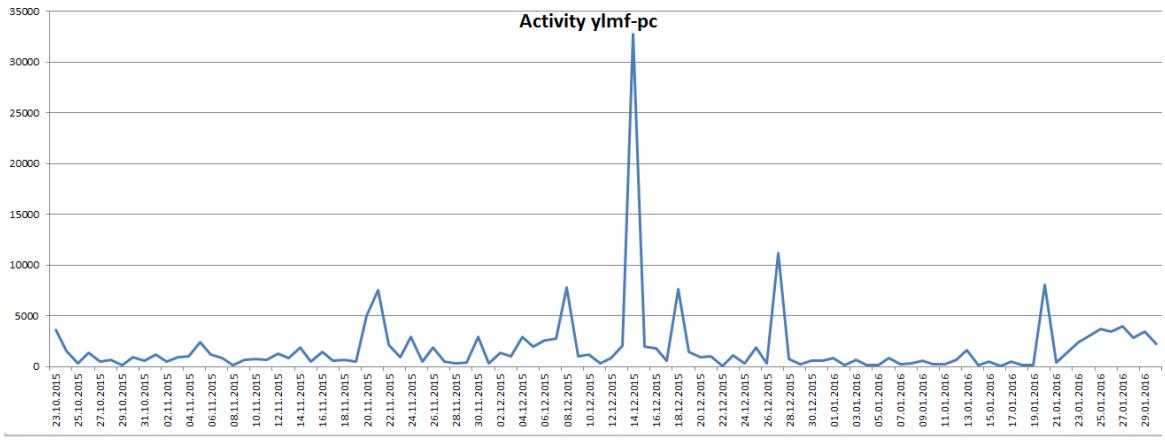


Figure 2. Activity query from ylmf-pc

There are various IP addresses from which ylmf-pc brute-force attack is carried out. Therefore, blocking connections by IP address will not fetch the proper result. Since IP addresses rarely change country, one can see which countries have the highest activity of ylmf-pc queries. Collected statistics showed that IP addresses from the United States, the Netherlands and France account for over half of the queries. The full picture of the percentage distribution of the number of queries from different countries is shown in Figure 3.

The statistics was gathered over 100 days. A total of 192,858 queries from clients with ylmf-pc signature were recorded. The top 5 countries that sent the highest number of queries are presented in the Table 1.

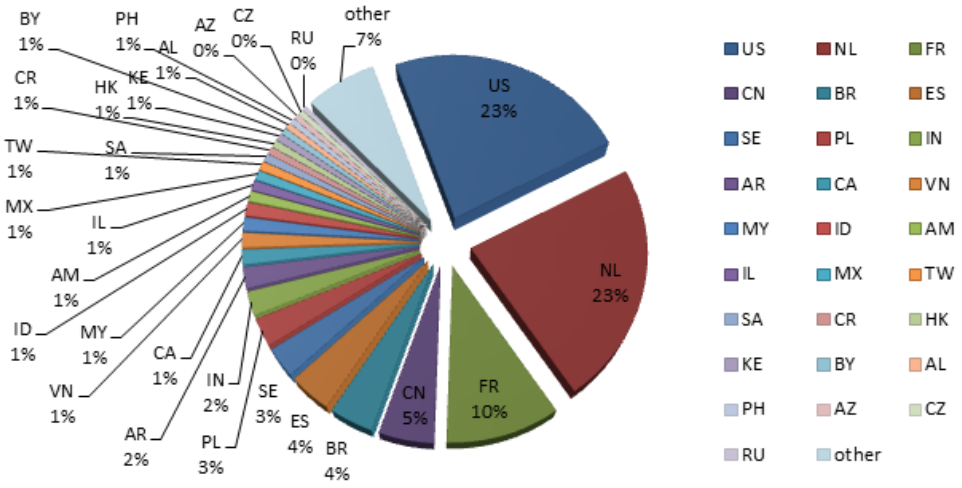


Figure 3. Distribution of queries by country

Table 1. Statistical results of attacker ip addresses

IP address (country of location)	Number of queries (percentage of the total number of queries)
37.59.87.23(NL)	43,895 (22%)
62.210.188.27(FR)	15,926 (8%)
198.251.79.135(US)	8,155 (4%)
212.225.165.70(ES)	7,237 (3%)
46.29.254.244(US)	6,413 (3%)

There were 599 unique IP addresses from which attacks were made. There was an average of 1928.58 queries, and about 80 queries per hour. That is, an average of 1.3 queries per minute. Daytime queries (9:00 to 21:00) account for 59%, while night queries (21:00 to 09:00) take up the remaining 41%. At the same time, this distribution for each country does not match. Figure 4 shows the distribution for the top 3 countries by number of queries and averaged statistics.

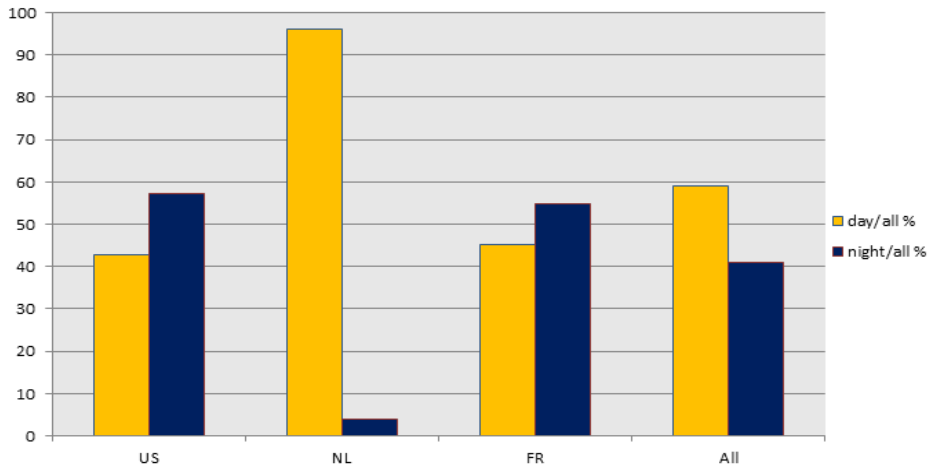


Figure 4. Distribution of queries (day/night)

There are several approaches when it comes to protecting against this type of attack. One option is to block an IP address after several unsuccessful helo/ehlo authentication attempts. With this approach, you must not forget that connection attempts originate from multiple, dynamically allocated IP addresses, and that a blocked address may, after some time, be given to an innocent user. So the optimum ban duration should be chosen. Another option is to interrupt the query session while in the helo/ehlo query field of the ylmf-pc

signature. This option is more preferable because the server, in this case, doesn't process the query, but rather gives a response that the query is incorrect, and immediately terminates the connection, thereby not informing the attacker about whether the data (username and password) sent by him were correct or not. Before establishing a connection, you may also want to check whether the IP address is in the list of infected IP addresses, for example, fail2ban. Another way to protect against this type of attack is to reconfigure the mail server to another port –ylmf-pc executes attack on standard SMTP port. More and more various ways of protection have been emerging over time, and they are moving from one area of use to another [8].

3. CONCLUSION

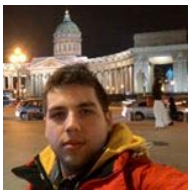
To summarize it all, it should be noted that despite the seeming harmlessness of ylmf-pc queries, loss of control over a mail server account, for example, an educational system [9] or even any functioning mail server, can lead to tragic consequences: your server will become part of the botnet due to sending of various kinds of spam from it [10] and later the IP address will be included by services in the list of spam addresses (DNSBL).

The issue of password guessing is massive in nature. Despite the simplicity of this attack and methods of protection against it, ylmf-pc brute-force attack appears to be producing results, as this attack has been used for over five years now. This implies that its use has been successful on some servers. During the period under review, the top IP addresses in terms of number of attack attempts are IP addresses from the Netherlands and the United States. Both countries shared the first position with 44,000 ylmf-pc queries each (23% of the total).

REFERENCES

[1] D. Devjatykh, *et al.*, "Sleep Apnea Detection Based on Dynamic Neural Networks," *Communications in Computer and Information Science*, vol. 466, pp. 556-567, 2014.
[2] O. G. Berestneva, *et al.*, "Multidimensional medical data visualization methods based on generalized graphic images," *World Applied Sciences Journal*, vol/issue: 24(24), pp. 18-23, 2013.
[3] Sullivan B., "Preventing a Brute Force or Dictionary Attack: How to Keep the Brutes Away from your Loot," 2007. http://h71028. www7. hp. com/ERC/cache/568358-0-0-0-121. html/ (accessed on 21 February 2010).
[4] Klensin J., "RFC 5321—Simple mail transfer protocol (SMTP)," RFC 5321, 2008.
[5] Decker A., *et al.*, "Pushdo/cutwail botnet," 2009.
[6] Zhuang L., *et al.*, "Characterizing Botnets from Email Spam Records," LEET, pp. T. 8. – C. 1-9, 2008.
[7] D. S. Silnov, "An Analysis of Modern Approaches to the Delivery of Unwanted Emails (Spam)," *Indian Journal of Science and Technology*, vol/issue: 9(4), 2016. DOI: 10.17485/ijst/2016/v9i4/84803.
[8] Belashenkova N. N., *et al.*, "Protection Methods of Assessment Procedures Used in e-Learning," *13th International Conference on Emerging eLearning Technologies and Applications,* pp. 27-32, 2015.

BIOGRAPHIES OF AUTHORS



Undergraduate at Department of Information Systems and Technologies, National Research Nuclear University MEPhI (Moscow Engineering Physics Institute). Doing researches in the field of information secutiry.

Assosiated Professor at Department of Information Systems and Technologies, National Research Nuclear University MEPhI (Moscow Engineering Physics Institute). Doing researches in the field of information secutiry.