An evaluation of method for zero-day malicious email detection using email header information analysis (EHIA) and deep-learning approach

Sanouphab Phomkeona and Koji Okamura
Graduate School of Information Science and Electrical Engineering, Kyushu University, Japan

九州大学
KYUSHU UNIVERSITY

Introduction

CIS Center for Internet Security®

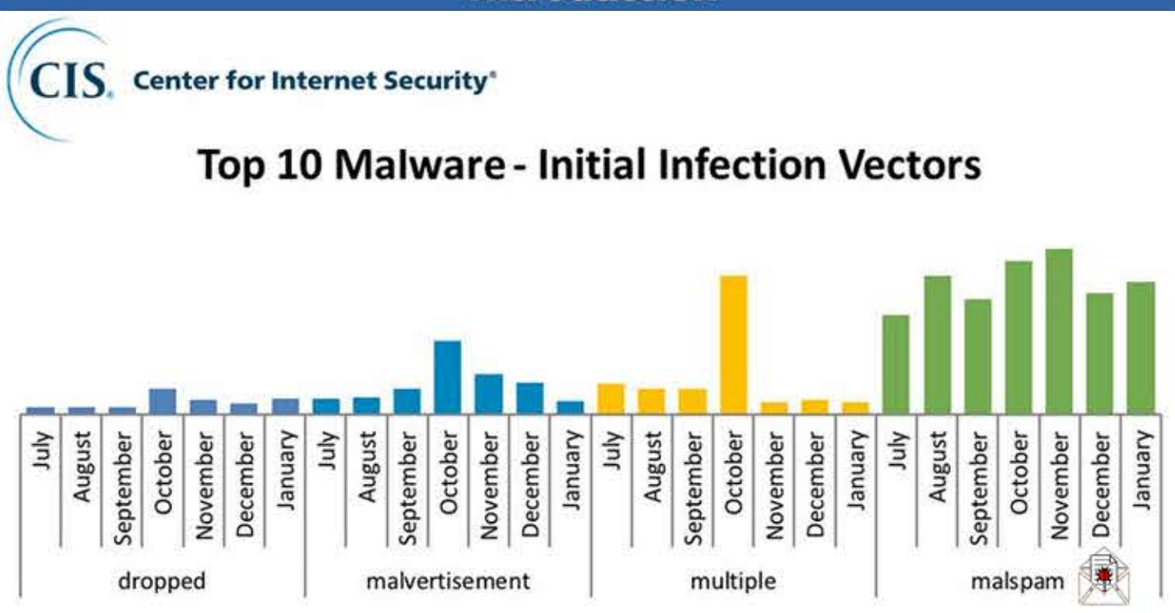


Fig. 1 CIS Cybersecurity report on malware infection vector

1. Email is the most common entry point of targeted attacks
2. About half of all email traffic is malspam, it means about 14.5 billion malspam are sent every single day in Q1 2018
3. Currently, the majority of security systems are unable to detect and stop today's advanced email threats that are specifically designed to fool the security systems

Related Works

Table 1.
Email header features considered by different machine learning malspam filtering techniques

Sheu, 2009 [11]	Ye et al., 2008 [12]	Wu, 2009 [13]	Hu et al., 2010 [14]	Wang & Chen, 2007 [15]	Al-Jarrah et al., 2012 [10]	Our approach
Length of sender field , Sender field, Title (more than one category), Time, Size of email	Received field (domain add., IP add., relay servers, date, time), From field, To field, Date field, Message-ID, X-Mailer	Comparing header fields with syslog	Originator fields, Destination fields, XMailer field, Sender IP, Email subject	Sender address validity, Receiver address (To, CC, BCC), Mail User Agent, Message-ID	Received field # of hops, Span Time, Domain add. Legality, Date & Time Legality, IP add. Legality, sender add. legality, # of Receivers (To, CC, BCC), Mail User Agent, Message-ID, Email subject Date of reception	Span Time, Domain add. Legality, Domain Zone, Date & Time Legality, IP add. Legality, IP Zone, Email Subject, Subject Language Detect, Subject Language Zone, Machine Translate Detect

[10] Omar Al-Jarrah, Ismail Khaterz and Basheer Al-Duwairi, "Identifying Potentially Useful Email Header Features for Email Spam Filtering", ICDS 2012 : The Sixth International Conference on Digital Society.

Email Header Information Analysis

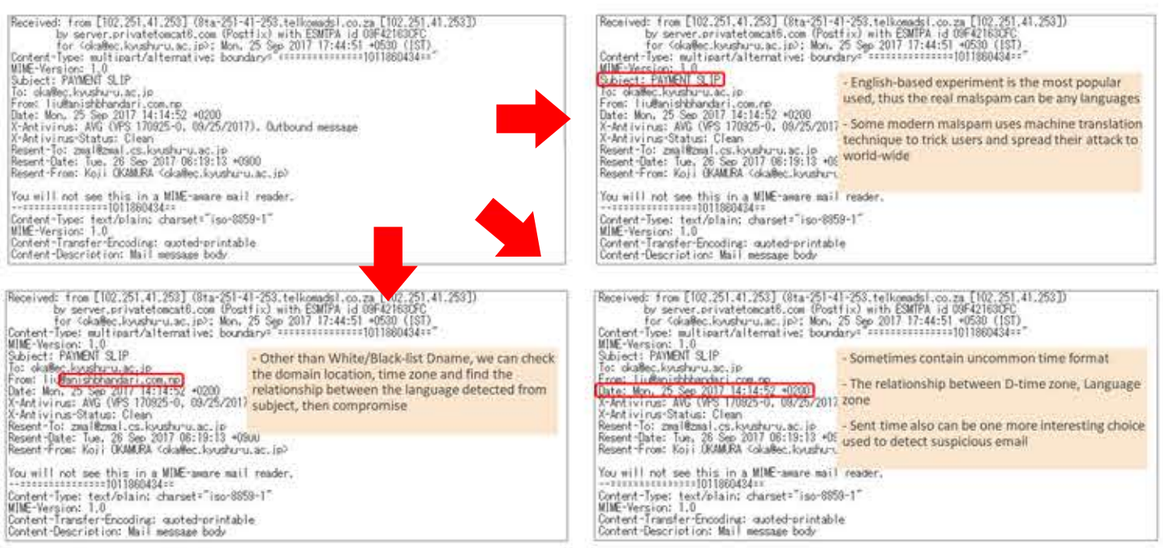


Fig. 2 Example how human being analyze email header

Unlike machine, cybersecurity experts also take consider in email header where suspicious data and their relationship among them are provided. For example:

- A relationship between domain zone and language
- A relationship between time zone and time sent
- Email was written by machine translation detection

Fig. 3 Differnetial of email spawn time between normal email, work email and malspam

From 436 work mails (Green), 4251 normal mails (Blue), and 277 malspam (Red) We can see that most of normal and work mails were sent on work time (8AM-8PM), but the malspam's sent time were varied

Purposed method

Our research focus on developing a new algorithms by using email header information analysis for malspam filtering and also to increase a possibility of zero-day malicious email detection

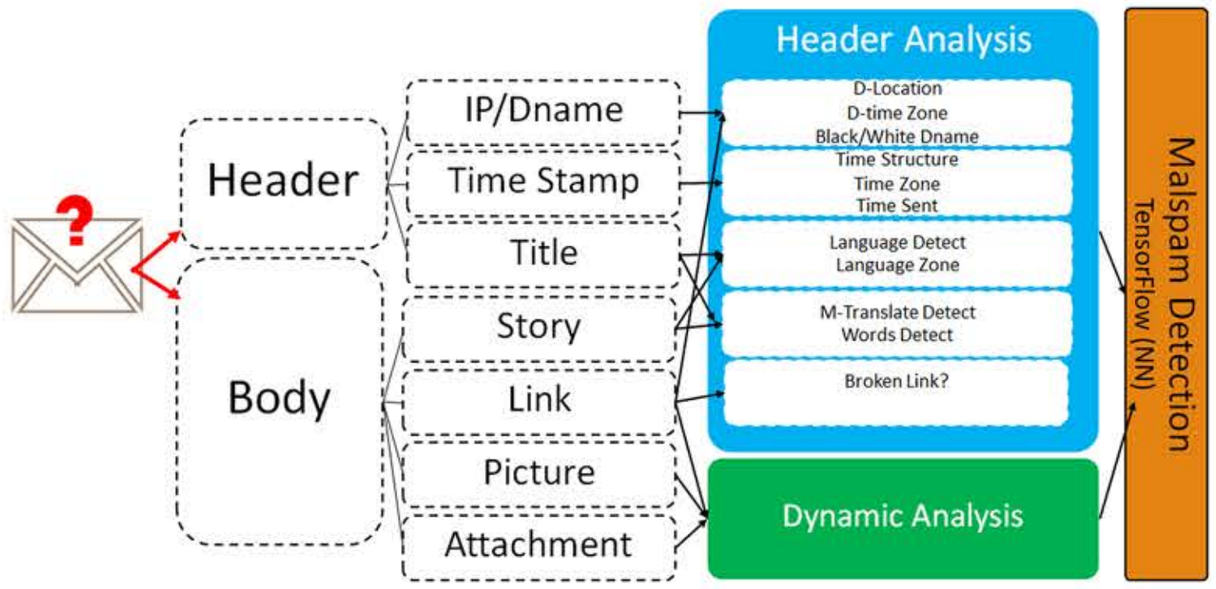


Fig. 4 Design Method for EHIA and Deep-Learning

Email Header Features Extraction

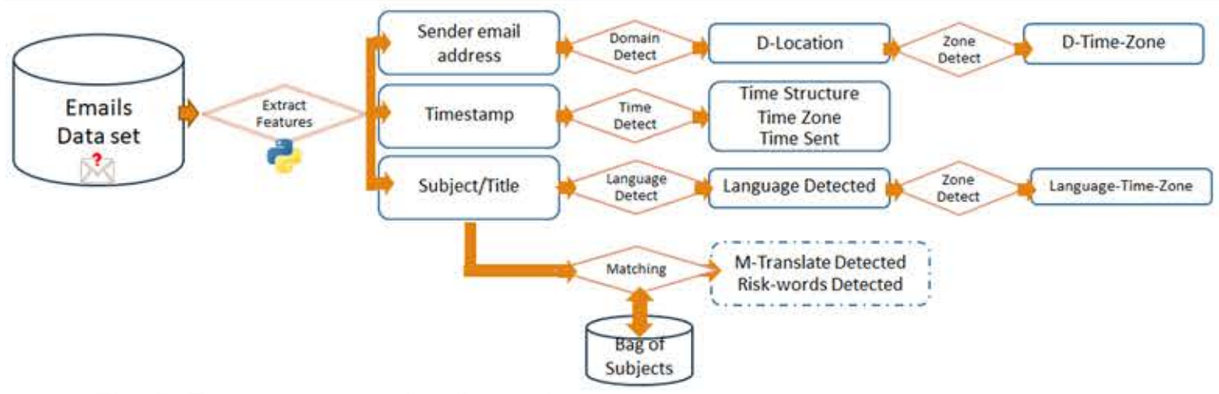


Fig. 5 Features extraction flows chart

From email dataset we first extract 3 features: source address, timestamp and subject

Then we can extract more features from those 3 to get other features in order.

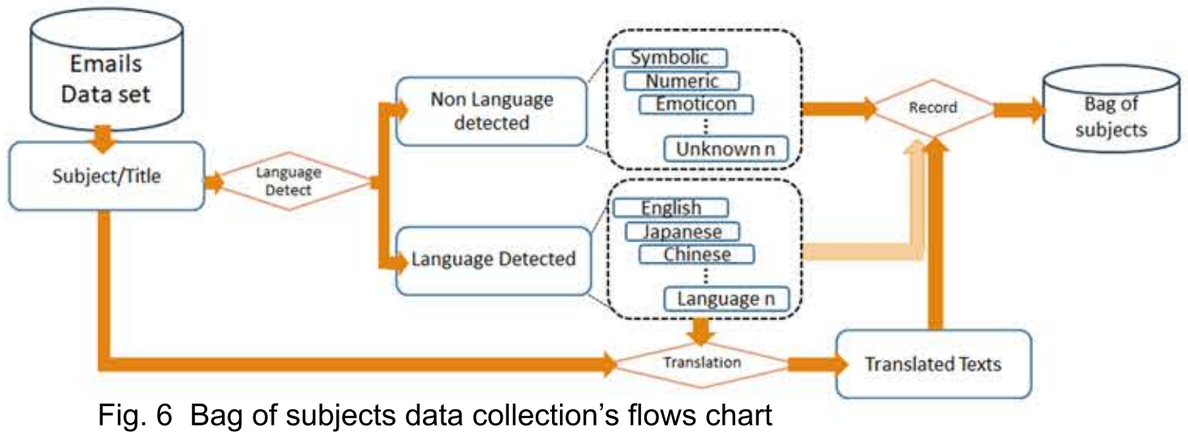
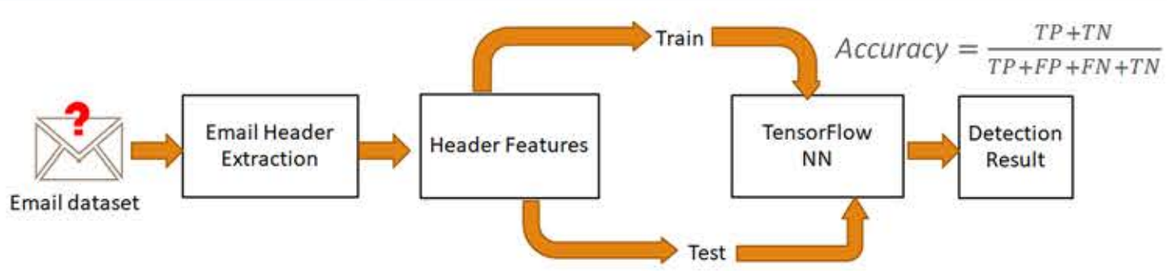


Fig. 6 Bag of subjects data collection's flows chart

Email subject database are created for matching propose and receive M-translate detected, and risk-words detected features

Experiments and Results



Normal Email		Spam Email		Total used	Features		Result
Train	Test	Train	Test				
2350	600	2350	600	5900	1.Sender address 3.D-Zone 5.Time Zone 7.Lang Detected 9.Title	2.D-Location 4.Time structure 6.Time sent 8.Lang Zone	0.7866667

- Normal emails : more than 500,000 (from enron_mail_2015-05, etc.)
- Spam/malspam: more than 500,000 (from http://untroubled.org/spam/ & Cybersecurity Center, Kyushu Univ.)

On progress

Conclusion

In this research, we proposed a method by using new features extracted from email headers and deep-learning approach to detect malspam. From the current experiments, we have not used all the features yet, but we got the best detection result at 78.66% accuracy. Thus, we keep doing more experimentation and improving the method technique to evaluate the detection result

Email: 3IE17305G@s.kyushu-u.ac.jp