Detecting Targeted Malicious Email Through Mail Client

Sandhya Rani Barre
Computer science Engineering
UCEK-JNTUK
Kakinada, India
Email: sandhya.2227@gmail.com

SSSN. Usha Devi N
Asst.prof, Computer science Engineering
UCEK-JNTUK
Kakinada, India
Email: usha.jntuk@gmail.com

***Abstract*--**Sharing and storing of data in the web world is with the help of social networks. Messages are exchanged between hosts using the Simple Mail Transfer Protocol (SMTP). While the email messages are transporting between systems, SMTP communicates delivery parameters using a message envelope separate from the message (header and body) itself. A malicious email message is the one which have been deliberately crafted to cause problems on the server or at the client side. This message may contain a virus. A filtering technique is applied on messaging string contents by applying tokenization and then applying naïve bayesian classifier we classify targeted and non targeted malicious email. A network defender encounters different classes of threat actors with varying intents and capabilities. Conventional computer network attacks exploit network-based listening services such as Web servers. Traditional decision-tree classification algorithms split each node using the best split from all available features. With random forests, each node splits from a randomly selected set of features at that node. It is only focus on mail body not on hyperlinks and attachments. Proposed extension is feature extraction to file attachment metadata. Threat actors might inadvertently leave remnants of information such as file paths, time zones, or even author names. In addition, organizations can track features that characterize the types and amounts of email received by a particular email address.

Keywords: *Email, SMTP, Tokenization, Decision –tree, Random Forests*

*****

I. INTRODUCTION

Common uses for mail filters include organizing incoming email and removal of spam and computer viruses. A less common use is to inspect outgoing email at some companies to ensure that employees comply with appropriate laws. Users might also employ a mail filter to prioritize messages, and to sort them into folders based on subject matter or other criteria. Mail filters can be installed by the user, either as separate programs, or as part of their email program (email client). In email programs, users can make personal, "manual" filters that then automatically filter mail according to the chosen criteria. Mail filters can operate on inbound and outbound email traffic. Inbound email filtering involves scanning messages from the Internet addressed to users protected by the filtering system or for lawful interception. Outbound email filtering involves the reverse - scanning email messages from local users before any potentially harmful messages can be delivered to others on the Internet. One method of outbound email filtering that is commonly used by Internet service providers is transparent SMTP proxying, in which email traffic is intercepted and filtered via a transparent proxy within the network. Outbound filtering can also take place in an email server.

II. LITERATURE REVIEW

Social networks [1] are playing an important role in the internet world. Messages are exchanged between hosts using the Simple Mail Transfer Protocol (SMTP) [2]. Network providers are the one which allows all type of emails for communication purpose. While transferring the messages some malicious emails [3] are received by the users this causes many problems either at the server side or at the client side. This type of messages may contain viruses, or it could be due to the message being crafted. A filtering technique [4] is applied on messaging stings contents by applying tokenization [5] and then applying naïve bayesian classifier[4] we classify targeted and non targeted malicious email[3].

A network defender encounters different classes of threat actors with varying intents and capabilities. Conventional computer network attacks exploit network-based listening services such as Web servers, whereas targeted attacks oft en leverage social engineering through vehicles such as email. Traditional decision-tree [6] classification algorithms split each node using the best split from all available features. The best split is that which provides the most separation in the data. With random forests [7], each node splits from a randomly selected set of features at that node. In addition, they create multiple decision trees using bootstrap samples from the dataset. It is only focus on mail body not on hyperlinks and attachments.

Feature extraction is to file attachment metadata. Threat actors might inadvertently leave remnants of information such as file paths, time zones, or even author names. In addition, organizations can track features that characterize the types and amounts of email received by a particular email address. One method of outbound email filtering that is commonly used by Internet service providers is transparent SMTP proxying [8], in which email traffic is intercepted and filtered via a transparent proxy within the network. Outbound filtering can also take place in an email server.

III. PROPOSED APPROACH

A. *Background*

Targeted attacks

These are highly customized threats directed at a specific user or group of users typically for intellectual property theft. These attacks are very low in volume and can be disguised by either known entities with unwitting compromised accounts or anonymity in specialized botnet distribution

channels. Targeted attacks generally employ some form of malware – and often use zero day exploits – in order to gain initial entry to the system and to harvest desired data over a period of time. With these attacks, criminals often use multiple methods to reach the victim. Targeted attacks are difficult to protect against and have the potential to deliver the most potent negative impact to victims. While potentially similar in structure, the major differentiator of targeted attacks relative to spear phishing attacks is the focus on the victim. A targeted attack is directed toward a specific user or group of users whereas a spear phishing attack is usually directed toward a group of people with a commonality, such as being customers of the same bank. Targeted attackers often build a dossier of sorts on intended victims – gleaning information from social networks, press releases, and public company correspondence. While spear phishing attacks may contain some personalized information, a targeted attack may contain a great deal of information which is highly personalized and generally of unique interest to the intended target.

Attributes	Targeted Attacks	Spearphishing Attacks
Intent	Intellectual Property Theft	Financial Gain
Malware	Yes, often with zero-day exploits	Possibly
Target Reconnaissance	Yes	No
Level of Personalization	Very High	Some

Figure 1: Comparison between Targeted and Spear phishing Attack

Impact of Targeted Attacks

The malicious nature of targeted attacks causes them to be very expensive to society in general and to individual organizations specifically. The cybercriminal benefit from a targeted attack, while substantial, is not easy to estimate because it is highly variable, based on the specific victim and intellectual property compromised. However, the cybercriminal benefit is a subset of the overall cost to the victim organization, which also depends heavily on the organization's reputation and status.

Email Header processing

What is an email header?

The email header is the information that travels with every email, containing details about the sender, route and receiver. It is like a flight ticket: it can tell you who booked it (who sent the email), the departure information (when the email was sent), and the route (from where it was sent and how did it arrive to you) and arrival details (who is the receiver and when it was received). As when you would book a flight ticket with a false identity, the same goes for emails: the sender can partially fake these details, pretending that the email was sent from a different account.

Generally email header contains following information

*From***:** It specifies source of the email sender. But it doesn't specify the actually source because it can be easily counterfeit and unreliable.

*Subject***:** This is like title or abstract contains objective of the mail body and for which it is intended to.

*Date***:** Specifies the composition date and time of email.

*To***:** Destination mail id to which the message was addressed.

*Return-Path***:** Similar to Reply-To and specifies return mail address.

*Envelope-To***:** Describes address of mailbox to specified email id in "To"

*Delivery Date***:** Specifies date and time of delivery of email to intended client or service.

*Received***:** It specifies the stack trace address mechanism. I.e. it is the mail received path in hop by hop fashion. The oldest or first address is placed in the last part of the path and final address received is place in the first part of the path. It is most useful part of email header for email forensics.

Message-id: This is a non-repeatable string or unique id assigned to a new message at the time of creation by the mail system. But this is unreliable due possibility of tampering.

*Content-Type***:** Specifies the MIME type such as html, plain text or image etc.

*Content-Length***:** Size of the mail message

X-Spam-Status: Specifies Probability of the current mail as spam.

*Message Body***:** Actual content prepared by the sender in the email.

Among these fields proposed system utilizes Subject, Date, To, Delivery Date, Message Id, Received, Content type, Content length and Message Body fields for email statistics and analysis.

B. Email header

Where the spam starts?

Here is the starting part of the header of a junk email (spam), which includes information about the transfer of the email between the sender and the receiver:

Let's analyze the red highlighted lines:

*Return-path***:** the header tells that if you reply to this email message, the reply will be sent to ydcdd...@yahoo.com.

Would you use such an email address for real?

*Received tags***:** as on web blogs, read them from the bottom to top. The header says the email was originally sent from 206.85... and it was sent to 217.225... (which is the name/IP of the first mail server that got involved into transporting this message). Then suddenly, the next Received tag says the message was received from root@localhost, by mailv.fx.ro. You can also notice that so far, the Received tags do not contain any information about how the email was transmitted (the "with" tag is missing: this tag tells the protocol used to send the email). In reality, this is the common case of a spammer pretending to be the root user of mailv.fx.ro and sending the email from 206.85..., through 217.225... and telling 217.225... to act as the root user of mailv.fx.ro, in order to use the SMTP server of mailv.fx.ro to send the email. Since more and more mail servers are not allowing open-relay connections, the spammer can only use the mail server of the receiver, in order to send the message. If the spammer will try to send the email to support@emailaddressmanager.com, through exactly the same route as above, it wouldn't work,

ISSN: 2321-8169
2261 – 2264

because support@emailaddressmanager.com is not a network user of mailv.fx.ro. This is the reason why you may have received spam emails appearing to be sent through an email address of your own ISP.

Going deeper with the analysis, you can use an IP tracing tool, like Visual Route, in order to see to whom the IP belongs to. As in most of the spamming cases, the starting IP (206.85...) is unreachable, which means that the spammer could have routed the real IP or he could have used a dynamic IP (a normal case for dial-up users). However, by tracing 217.225..., you will get to the ISP used by the spammer, a German provider. The ISP has nothing to do with the spam itself, but it was simply used by the spammer to connect to the Internet.

Let's look further into the email header:

```
Message-ID: <VHUCXEYVIXPEUNUKOJEW@hotmail.com>
From: "Julianne Lloyd" <ydcddlhanqz@yahoo.com>
Reply-To: "Julianne Lloyd" <ydcddlhanqz@yahoo.com>
To: boby_con@fx.ro
Cc: bodistvan@fx.ro, bogdan.micu@fx.ro, bogdan@fx.ro, bogdans@fx.ro
Subject: Get viagra over night - no prescription needed
Date: Wed, 24 Mar 2004 08:31:16 -0200
X-Mailer: AOL 9.0 for Windows US sub 740
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="--0591734046654782085l"
X-Priority: 3
X-MSMail-Priority: Normal
X-IP: 162.238.92.104
X-RAV-Bulk: RAV AntiVirus classifies this e-mail as spam (accuracy medium)
X-RAV-Signature: 250F0FB03547C3C93609D82815AB3746
X-RAVMilter-Version: 8.4.3(snapshot 20030212) (mail)
X-UIDL: l+/"!l-H"![JK!!^U"!
```

The *Message-ID* field is a unique identifier of each email message. It is like the tracing ID of an express postal mail. The rule says the ID is composed by the name of the server that assigned the ID and a unique string (for example, QESADJHO@emailaddressmanager.com). Hmm, this is strange, because on our case, the ID belongs to hotmail.com, while the sender appears to belong to yahoo.com. In fact, this difference mainly shows that the sender is forged (fake address or someone pretending to own that email address).

The *X-IP tag* (also named X-Originating-IP) is probably the most important one and it should give precise information about the sender (from where the email was actually sent). Unfortunately, this tag is optional for email protocols, so some spam messages will not include it. As you can see, the originating IP is not even close to the sender's IP, from the Received tags.

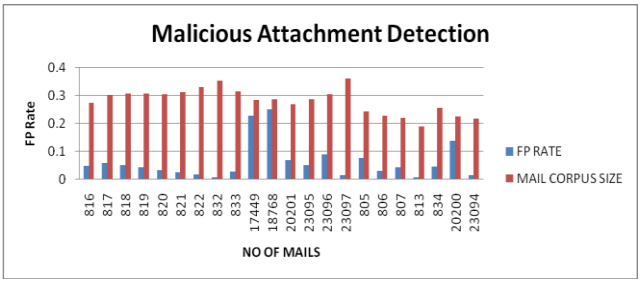
The *X-UIDL tag* is another unique ID, but this one is used by the POP3 protocol when your email client is receiving the email. This is an optional email tag, but the rule of thumb says spammers love to include it.

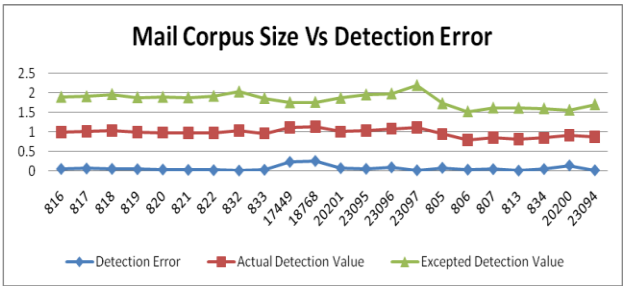
C. Attachment Processing

Last but not least is attachment classification. In this case attachments may have virus information. Already Gmail like mail systems don't allow files with extension exe, bat, sh etc. But it only considers the extension. i.e if the file is renamed or placed in a Winrar it cannot be traced out and it can be uploaded. To overcome this limitation, first two bytes of every attachment has to be extracted and verify the file type. Because most of the cases first two bytes represent unique magic numbers belongs to the file type. If those two bytes are belongs to any not allowed case then either attachment has to be stopped or mail can't be forwarded to the actual client system. In case of archive files this process should be applied after extracting only.

IV. SIMULATION RESULTS

CORPUS SIZE	EXCEPTED	ACTUAL	ERROR
816	0.049491	0.948406	0.898915
817	0.059319	0.956271	0.896951
818	0.050986	0.983909	0.932922
819	0.042654	0.943515	0.900862
820	0.034321	0.947553	0.913232
821	0.025989	0.940475	0.914487
822	0.017656	0.959974	0.942318
832	0.008424	1.017861	1.009438
833	0.027207	0.933144	0.905937
17449	0.227812	0.878114	0.650301
18768	0.250189	0.882401	0.632212
20201	0.068137	0.934979	0.866842
23095	0.052001	0.979138	0.927137
23096	0.089294	0.991645	0.902351
23097	0.014957	1.098797	1.08384
805	0.076916	0.866085	0.789169
806	0.031442	0.760893	0.729451
807	0.043305	0.80891	0.765605
813	0.00698	0.807025	0.800044
834	0.04599	0.799635	0.753646
20200	0.138656	0.781269	0.642614
23094	0.014708	0.852975	0.838267





V. CONCLUSION

This project did feature extraction to file attachment metadata. Threat actors might inadvertently leave remnants of information such as file paths, time zones, or even author names. In addition, organizations can track features that characterize the types and amounts of email received by a particular email address. It also shows the statistics of mail corpus received till now and accordingly display false positive and false negative rates.

Future work

Future extension could be attachment filter based on semantic search and natural language processing to analyze the internal content of emails.

REFERENCES

[1] The Risks of Social Networking,Candid Wuest, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_risks_of_social_networking.pdf

[2] Simple Mail Transfer Protocol, http://www.facweb.iitkgp.ernet.in/~agupta/IWT/SMTP-POP3_4.pdf

[3] Rohan Mahesh Amin**,** Detecting Targeted Malicious Email Through Supervised Classification of Persistent Threat and Recepient Oriented. http://pqdtopen.proquest.com/pqdtopen/doc/817552431.html?FMT=ABS Uffe B. Kjærulff, Anders L. Madsen, Probabilistic Networks — an Introduction to Bayesian Networks and Influence Diagrams, 10 May 2005.

[4] http://people.cs.aau.dk/~uk/papers/pgm-book-I-05.pdf

[5] C. Apte and S. Weiss. Data mining with decision trees and decision rules. Future Generation Computer Systems, 13, 1997. http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=1D71172A1A7E294510D75DCF269F21B9?doi=10.1.1.46.5128&rep=rep1&type=pdf

[6] Leo Breiman, http://www.stat.berkeley.edu/~breiman/RandomForests

[7] RANDOM FORESTS ,Leo Breiman Statistics Department University of California Berkeley, CA 94720 January2001 http://oz.berkeley.edu/~breiman/randomforest2001.pdf

[8] SMTP PROXYING, http://en.wikipedia.org/wiki/SMTP_proxy