Digital Investigation 13 (2015) 72–79

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Covert communication by means of email spam: A challenge for digital investigation

Szde Yu*

1845 Fairmount Box 135, Criminal Justice, Wichita State University, Wichita, KS 67260, USA

ARTICLE INFO

Article history:
Received 23 October 2014
Received in revised form 10 April 2015
Accepted 14 April 2015
Available online 16 May 2015

Keywords:
Email
Spam
Encryption
Forensics
Content analysis
Evidence
Incriminating information

ABSTRACT

In digital investigations the investigator typically has to deal with thousands of digital artifacts. Among them, email has long been one of the many focuses that potentially can generate useful information. However, in our training we notice a tendency to overlook or downplay the importance of analyzing spam emails as they are generally assumed to be irrelevant junk emails. In this article we thus illustrate how these seemingly irrelevant messages might play a crucial role in digital investigations. Five scenarios are introduced in which the investigator tends to overlook crucial incriminating information that has been disguised as spam. The methods used by criminals in these cases are discussed. In light of these covert criminal communications, we call for more attention from the digital forensics community to realize how email spam may assist in criminal activities.

Introduction

Email is one of the most pervasive forms of computer-mediated communication (Heisler and Crabill, 2006). It allows for instant and free communication between people at long distance. However, because email features convenience and low cost, it has been involved in a variety of criminal activities. Email could be used as a communication tool among criminals or it could be used to store digital evidence (Maras, 2012; Yu, 2011). Accordingly, email has become one of the focal points in digital forensics (Orebaugh and Allnutt, 2009; Garfinkel, 2006; Shields et al., 2011). Nevertheless, current literature on digital forensics rarely, if ever, pays attention to one email source that could harbor crucial intelligence about criminal activities, that is, email spam.

In USA, the CAN-SPAM Act defines email spam as unsolicited commercial electronic mail that includes any commercial emails addressed to a recipient with whom the sender has no existing business or personal relationship and not sent with the consent of the recipient, and commercial electronic mail is defined as any electronic mail message the primary purpose of which is commercial advertisement or promotion of products or service (Rogers, 2006). Unsolicited commercial emails that fail to comply with the CAN-SPAM regulations would be declared criminal. The punishment could be a fine up to $16,000 for each separate email in violation of the CAN-SPAM Act (Federal Trade Commission, 2009), or it could be imprisonment (Yeargain et al., 2004). However, research has found these potential penalties do not really deter spammers (Yu, 2011). This suggests that spammers do not believe law enforcement would prioritize email spam cases. The lack of law enforcement might be due to the limited resources as well as jurisdictional issues, but it could also indicate an attitude that sees email spam as a trivial problem that results in minimal to no harm.

This downplayed significance of email spam could work in the criminal's favor if digital investigators and researchers share such a perception. Current research on

* Tel.: +1 316 978 6492.
E-mail address: szdeyu@gmail.com.

http://dx.doi.org/10.1016/j.diin.2015.04.003
1742-2876/

email spam mostly focuses on the technical issues, such as spam filtering methods (Blanzieri and Bryl, 2008; Zhou et al., 2010; Liu and Wang, 2012; Zhou et al., 2014), or the methods spammers use (Wang et al., 2013; Lumezanu and Feamster, 2012). These discussions are generally irrelevant to digital forensics as researchers in the field of email spam are more concerned about detecting email spam while reducing false positives, rather than extracting useful leads from spam emails. Hence, email spam becomes a viable medium for criminals to convey incriminating messages. To illustrate, in this article we introduce five scenarios where digital forensics practitioners tend to overlook crucial information hidden in spam emails.

Scenarios

The following five scenarios are based on real investigations involving email forensics. The investigators in each case all initially overlooked crucial information about the case as such information was hidden in email spam.

Computer-aided encryption

It is conceivable that criminals might attempt to conceal their communications by means of encryption. However, if the encryption is too obvious, it will inevitably arouse suspicion. Sophisticated criminals would prefer their encrypted messages to be unnoticed. To this end, email spam offers an ingenious camouflage, because most people, including well-trained digital investigators, probably do not normally pay much attention to emails that are seemingly irrelevant to the case, especially when there could be dozens of spam emails in presence.

In a murder investigation, a housewife was shot to death. The killer did not leave behind much physical evidence to work with and seemed to be familiar with the house. The husband naturally became the prime suspect, but he had an alibi. Despite the alibi, the investigators were convinced that the husband had hired someone else to commit the crime. While searching for evidence of communication between the husband and the killer, the investigation soon turned to the digital world including the suspect's three email accounts. Using keyword searches provided by modern computer forensics tools resulted in no solid clues. The investigators started to peruse all the email messages found in the suspect's email accounts. The conclusion was the same. None of the emails were deemed relevant. However, the investigators did not know they had made a mistake when they automatically dismissed the messages in the spam folders. To be fair, even if they had read those spam emails one by one, they probably would have missed it anyway.

The clue did not emerge until a more thorough email forensics analysis was performed. The incriminating message is shown in Fig. 1. It was believed to be an encrypted message that was sent to the husband from the killer asking for a meeting. The original message reads: “first thursday next month walmart on west 9am isle 1”. It means the meeting should take place on the first Thursday next month in the Walmart store on the west side of the town at 9am, and they should meet at aisle 1. This encryption was created by a well-known website “spammimic.com”. This site uses context free grammar to convert an input message into the structure of a spam message. The sender does not need to know how the conversion works exactly and can still easily capitalize on the free web-based service.

To our best knowledge, no existing digital forensics tools can detect such encryption. In the human eye, the message reads nothing more than a common spam message that is aimed to tout a quick-to-fortune scheme. However, a closer examination on the message revealed some warning signs. First, unlike most spam messages, this message did not seem to be sent in bulk when we looked into this message's header. Second, spam messages of this kind normally would come with a link to a website where people can sign up, but the link is missing in this particular message. Therefore, this message stood out. Although by the time this message was discovered the meeting had taken place, this message eventually led the investigators to the killer's location. Luckily this murderer did not hide his IP address well and further evidence was found in his place to incriminate both him and the husband.

It remains unclear as to how the offenders in this case became familiar with this method. Neither the killer nor the husband had an advanced background in computer-related fields, but they did use the Internet on a daily

Dear Professional ; Especially for you - this cutting-edge intelligence . We will comply with all removal requests . This mail is being sent in compliance with Senate bill 1627 ; Title 3 , Section 305 . This is NOT unsolicited bulk mail ! Why work for somebody else when you can become rich within 33 days . Have you ever noticed people love convenience plus most everyone has a cellphone . Well, now is your chance to capitalize on this . We will help you deliver goods right to the customer's doorstep and increase customer response by 200% ! You can begin at absolutely no cost to you . But don't believe us . Prof Ames who resides in Delaware tried us and says "I was skeptical but it worked for me" ! This offer is 100% legal ! Because the Internet operates on "Internet time" you must make a commitment soon ! Sign up a friend and you get half off . Thank-you for your serious consideration of our offer ! Dear Sir or Madam , Especially for you - this amazing information . This is a one time mailing there is no need to request removal if you won't want any more ! This mail is being sent in compliance with Senate bill 1626 ; Title 2 ; Section 305 . THIS IS NOT MULTI-LEVEL MARKETING . Why work for somebody else when you can become rich within 98 DAYS . Have you ever noticed nearly every commercial on television has a .com on in it plus most everyone has a cellphone . Well, now is your chance to capitalize on this ! We will help you sell more plus deliver goods right to the customer's doorstep ! You can begin at absolutely no cost to you . But don't believe us ! Mrs Simpson of New York tried us and says "Now I'm rich, Rich, RICH" . We are licensed to operate in all states ! We beseech you - act now ! Sign up a friend and you'll get a discount of 40% ! Thank-you for your serious consideration of our offer ! Dear Web surfer , Thank-you for your interest in our publication ! This is a one time mailing there is no need to request removal if you won't want any more . This mail is being sent in compliance with Senate bill 1621 , Title 3 ; Section 304 . This is not a get rich scheme . Why work for somebody else when you can become rich inside 87 days ! Have you ever noticed how long the line-ups are at bank machines & society seems to be moving faster and faster ! Well, now is your chance to capitalize on this . We will help you SELL MORE plus SELL MORE ! You are guaranteed to succeed because we take all the risk . But don't believe us . Mrs Ames who resides in Georgia tried us and says "Now I'm rich, Rich, RICH" . We are licensed to operate in all states ! So make yourself rich now by ordering immediately . Sign up a friend and your friend will be rich too ! Thanks . Dear olleague , We know you are interested in receiving amazing intelligence . We will comply with all removal requests . This mail is being sent in compliance with Senate bill 1618 , Title 3 ; Section 304 . This is a ligitimate business proposal . Why work for somebody else when you can become rich in 19 DAYS . Have you ever noticed society seems to be moving faster and faster and people ill do almost anything to avoid mailing their bills ! Well, now is your chance to capitalize on this ! We will help you SELL MORE & deliver goods right to the customer's doorstep ! You can begin at absolutely no cost to you ! But don't believe us . Mr Jones who resides in Montana tried us and says "Now I'm rich, Rich, RICH" ! We are a BBB member in good standing ! If not for you then for your loved ones - act now . Sign up a friend and you'll get a discount of 80% . Best regards .

Fig. 1. Example of spam mimic.