https://doi.org/10.33778/kcsa.2020.20.3.021

A Study on Hacking E-Mail Detection using Indicators of Compromise★

Hoo-Ki, Lee*

ABSTRACT

In recent years, hacking and malware techniques have evolved and become sophisticated and complex, and numerous cyber-attacks are constantly occurring in various fields. Among them, the most widely used route for compromise incidents such as information leakage and system destruction was found to be E-Mails. In particular, it is still difficult to detect and identify E-Mail APT attacks that employ zero-day vulnerabilities and social engineering hacking techniques by detecting signatures and conducting dynamic analysis only. Thus, there has been an increased demand for indicators of compromise (IOC) to identify the causes of malicious activities and quickly respond to similar compromise incidents by sharing the information. In this study, we propose a method of extracting various forensic artifacts required for detecting and investigating Hacking E-Mails, which account for large portion of damages in security incidents. To achieve this, we employed a digital forensic indicator method that was previously utilized to collect information of client-side incidents.

침해지표를 활용한 해킹 이메일 탐지에 관한 연구

이 후 기*

요 약

최근 해킹 및 악성코드는 점검 기법이 매우 정교하고 복잡하게 발전하고 있으며, 다양한 분야에서 침해사고가 지속적으로 발생하고 있다. 그 중 정보유출, 시스템 파괴 등에 활용되는 침해사고의 가장 큰 이용 경로는 이메일을 이용한 것으로 확인되고 있다. 특히, 제로데이 취약점과 사회공학적 해킹 기법을 이용한 이메일 APT공격은 과거의 시그니처, 동적분석 탐지만으로는 식별이 매우 어려운 상황이다. 이에 대한 원인을 식별하고 해당 내용을 공유하여 유사한 침해사고에 대해 빠르게 대응하기 위한 침해지표(IOC, Indicators Of Compromise)의 필요성은 지속적으로 증가하고 있다. 본 논문에서는 기존에 클라이언트단의 침해사고를 수집하기위해 활용되었던 디지털 포렌식 탐지 지표 방식을 활용하여 보안사고의 가장 큰 피해를 유발하는 해킹 메일의 탐지 및 조사 분석 시 필요한 다양한 아티팩트 정보를 효과적으로 추출할 수 있는 방법을 제안한다.

Keywords: Hacking E-Mail , Indicators Of Compromise (IOC), Artifact, Digital Forensic, E-Mail

접수일(2020년 07월 05일), 게재확정일(2020년 09월 29일)

* 건양대학교/사이버보안공학과

★ 본 논문은 2019학년도 건양대학교 학술연구비 지원에 의하여 이루어진 것임

1. Introduction

Among various cyber-attack methods, the distribution of malware through E-Mail (i.e., cyber-attacks through E-Mails) is continuously increasing around the world. Unlike typical virus methods, these attacks have been conducted through E-Mail or network sharing and have also been widely spread through a method of sending E-Mails to huge number of random targets [1].

According to the 2017 Ransomware Infringement Analysis Report by the Korea Computer Emergency Response Team Coordination Center, more than 70 percent of ransomware incidents were infected through phishing E-Mails in the United States and Europe. Further, in Korea, 74 percent of compromise incidents have been linked to Hacking E-Mails [2]. To respond to such cyber-attacks, various digital forensic technologies have been developed, and numerous forensic artifacts that can investigate intrusion traces have been discovered and are in use [3]. In particular, research and use of the digital forensic technologies for investigating and tracking client-side digital system compromise incidents have continuously developed. Processing the information output from the forensic tools has been actively conducted as well. However, although indicators of compromise (IOCs) for web hacking types at the client-side are available to some degree, there is a lack of research and application of IOCs related to Hacking E-Mails, which are considered a popular route for widespread of malicious codes.

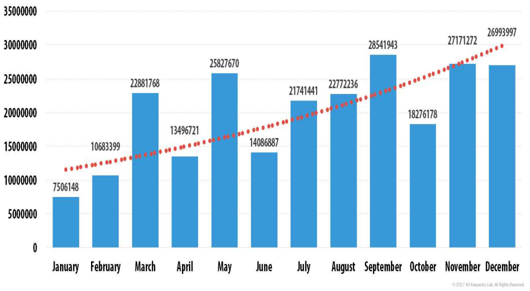
Accordingly, this study is aimed at proposing a system that can thoroughly analyze E-Mail structures and collect elements that can contribute to detecting Hacking E-Mails. In addition, we intend to propose an effective Hacking E-Mail response method by deriving the Hacking E-Mail detection indicators using forensic IOC and verifying with actual data.

2. Related research

2.1 Hacking E-Mail Distribution Status

Many attackers still use E-Mails as a way to distribute ransomware, plant bitcoin mining malware, carry out advanced persistent threats, and perform phishing. Although various countermeasures, such as malicious E-Mail response training, response equipment establishment, commercial E-Mail access denial, security training, and separation of workplace network and Internet network, have been established, it is still impossible to perfectly respond to the attacks due to the attacks becoming more sophisticated and intelligent. According to the Spam and Phishing Reports by Kaspersky Lab, the anti-phishing system was triggered 239,979,660 times on the computers of Kaspersky Lab users in 2016. This number denotes more than the quadrupled number over the previous year's [Figure 1]. Currently, cybercriminals can easily rent botnets and send E-Mails with malware, which simply means that an attacker can perform Hacking E-Mails in various types without the knowledge of coding and without requiring to be a professional hacker in the traditional sense.

Among various forms of Hacking E-Mails such as E-Mails having malware and phishing links attached, spear phishing, which is a personalized phishing by applying social engineering techniques, is a universal and easy attack method that attackers can use to achieve high success rate in performing APT attacks. Accordingly, it is essential to increase the security awareness of E-Mail account owners in order to effectively respond to such Hacking E-Mails. When E-Mail users can get into the habit of not opening suspicious E-Mails and reporting such E-Mails to a security personnel, safer cyberspace can be established, and security risks can be minimized.



(Fig. 1) Quantity of malicious E-Mails in spam[4]

2.2 Digital Forensics and Indicators Of Comp romis(IOC)

2.2.1 Digital Forensics

Digital forensics can be simply defined as procedures and methods for identifying and verifying in a court, the facts of a specific act caused by a digital device as a medium based on the evidence of digital data. Further, digital forensics can be defined as procedures and methods used as information security tools or as risk management and policy related tools in companies. In other words, the definitions may slightly vary depending on the subject and purpose of use [5]. Digital forensics can be mainly divided into two types depending on the purpose and target of analysis. Thus far, digital forensics have been focused on the field of securing data generated by individuals on a computer hard drive as evidence. However, in recent years, the expertise of digital forensics has become intensified due to the development of IT-related technologies and digital devices as more information is found in various places such as networks, Internet, databases, mobile devices, and memory modules. In addition, numerous evidence collection methods are required depending on the hardware type and operating system type [6].

In order to investigate the compromised system, a number of forensic artifacts must be collected and analyzed from the compromised system [7]. There are various types of forensic artifacts such as shellbags and user's web browser history, and with the increased use of IT devices, the amount of information stored in artifacts is also increasing. Accordingly, a standardized data processing method is required to handle and analyze a large amount of data. XML, which stands for eXtensible Markup Language, is a markup language developed to clearly express data by suppressing confusion in recording and sharing various data types. Digital Forensics XML (DFXML), developed by Garfinkel in 2009, is an XML language specialized for displaying raw data stored in a storage device [8]. DFXML is designed not only to accurately represent even the offset unit of a file by analyzing the storage device collected from the suspected compromised system, but also to describe the location of deleted data in the storage device.

2.2.2 Indicator Of Compromise(IOC)

Indicators of compromise (IOC) can be defined as "forensic artifacts that can identify system compromises or malware infections". In general, IOCs include various types of information such as IP address, MD5 hashes of malware, host and Internet explorer information, and cache files. These information pieces can be used to detect execution traces of malware discovered during initial analysis conducted using static and dynamic analysis information of malware [9].

In 2008, MANDIANT released an open source based OpenIOC IOC developed for generating and analyzing IOCs in order to effectively utilize IOCs (e.g., applying to other systems, sharing information intuitively, and distributing data in common format).

OpenIOC is an XML-based (Extensible Markup Language) threat intelligence describing framework, which allows organizing forensic artifacts in a logical group format. Since the OpenIOC uses the concept of "lessons learned", it has the advantage of securing reliability and flexibility of IOCs. In addition, since the IOCs are written in XML format, OpenIOC also has the advantage of being both machine and human readable when distributing IOCs, thus securing readability. Lastly, it secures the portability as it can easily be implemented on signature-based security devices such as intrusion prevention system (IPS) and intrusion detection system (IDS) [10]. [Table 1] illustrates 33 E-Mail IOC artifacts defined in RFC2822 (Internet Message Format) [12].

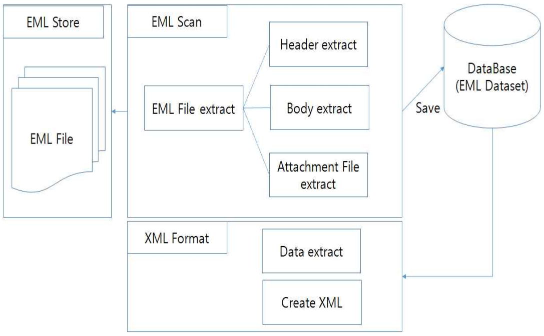
<Table. 1> E-Mail IOC Artifact

No.	Title
1	E-Mail Attachment Content
2	E-Mail Attachment MIME Type
3	E-Mail Attachment Name
4	E-Mail Attachment Size
5	E-Mail Attachment Count
6	E-Mail BCC Recipients(s)
7	E-Mail Body Text
8	E-Mail CC Recipients(s)
9	E-Mail Content-Type
10	E-Mail Date (Sent)
11	E-Mail Sender
12	E-Mail In-Reply-To
13	E-Mail MIME-Version
14	E-Mail Received Date
15	E-Mail Received From Host
16	E-Mail Received From IP
17	E-Mail References
18	E-Mail Return Path
19	E-Mail Subject
20	E-Mail Thread-Index
21	E-Mail Thread-Topic
22	E-Mail Recipients
23	E-Mail X-MS-Has-Attach
24	E-Mail X-filenames
25	E-Mail X-filesizes
26	E-Mail X-filetypes
27	E-Mail X-Original-SENDERIP
28	E-Mail X-Original-E-MailFROM
29	E-Mail X-Original-RCPTTO
30	E-Mail X-Originating-IP
31	E-Mail Content-Transfer-Encoding
32	E-Mail X-E-Mailer
33	E-Mail X-Client IP

3. Proposed Model

3.1 EML Extraction System

[Figure 2] shows a diagram of the constructed EML extract system designed to automatically extract artifacts for Hacking E-Mail detection by applying IOCs. In the proposed system, EML Scan is executed in the EML Store where the EML file is stored to extract the unique data of the artifact files from the E-Mail header, body, and attachments. The results are then stored into the database to be saved in the EML Dataset. Subsequently, the data stored in the database are extracted in the form of an XML file to support usability.



(Fig. 2) EML Extraction System

[Figure 3] illustrates the source code of the EML extract system designed to extract E-Mail content data and attachments from the EML file. Once the database is generated through the extracted data, the data are re-extracted from the database to create an XML file as shown in [Figure 4].

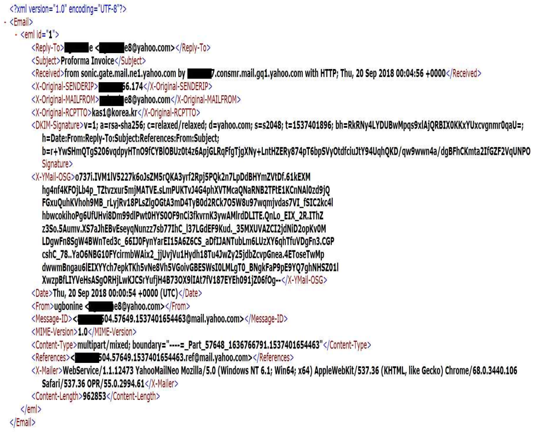
```
public static ArrayList<String> dataExtr(File emlFile) throws Exceptio
n{              InputStream source;
                source = new FileInputStream(emlFile);
                Properties props = System.getProperties();
                props.put("E-Mail.host", "smtp.dummydomain.com");
                props.put("E-Mail.transport.protocol", "smtp");
                Session E-MailSession =
 Session.getDefaultInstance(props, null);
                MimeMessage message = new
MimeMessage(E-MailSession, source);
                List<String> dataLists = new ArrayList<String>();
                message.getAllHeaderLines();
                for (Enumeration<Header> e =
message.getAllHeaders(); e.hasMoreElements();) {
                        Header h = e.nextElement();
                        h.getName();
                        h.getValue();
                        dataLists.add(h.getName() + "||" + h.getValue());
                        //System.out.println("name : " + h.getName() );
                        //System.out.println("value : " + h.getValue() );    }
                return (ArrayList<String>) dataLists;
}
```

Extract content data from within EML files

```
public static ArrayList<String> attachFileExtr(File emlFile) throws Ex
ception{
                InputStream source;
                source = new FileInputStream(emlFile);
                Properties props = System.getProperties();
                props.put("E-Mail.host", "smtp.dummydomain.com");
                props.put("E-Mail.transport.protocol", "smtp");
                Session E-MailSession =
Session.getDefaultInstance(props, null);
                MimeMessage message = new
MimeMessage(E-MailSession, source);
                List<String> fileLists = new ArrayList<String>();
                Multipart multipart = (Multipart) message.getContent();
                for (int x = 0; x < multipart.getCount(); x++) {
                       BodyPart bodyPart = multipart.getBodyPart(x);
                       String disposition = bodyPart.getDisposition();
                       if (disposition != null   &&
(disposition.equals(BodyPart.ATTACHMENT))) {
                              DataHandler handler =
bodyPart.getDataHandler();
                              fileLists.add(handler.getName() + "|" + handler.ge
tContentType() ); //System.out.println(handler.get);
                       }
                }               return  (ArrayList<String>) fileLists;
```

Attachment File Extract

(Fig. 3) EML Extract Program



```
  <?xml version="1.0" encoding="UTF-8"?>
- <Email>
  - <eml id="1">
      <Reply-To>[redacted]e <[redacted]e8@yahoo.com></Reply-To>
      <Subject>Proforma Invoice</Subject>
      <Received>from sonic.gate.mail.ne1.yahoo.com by [redacted]7.consmr.mail.gq1.yahoo.com with HTTP; Thu, 20 Sep 2018 00:04:56 +0000</Received>
      <X-Original-SENDERIP>[redacted]66.174</X-Original-SENDERIP>
      <X-Original-MAILFROM>[redacted]e8@yahoo.com</X-Original-MAILFROM>
      <X-Original-RCPTTO>kas1@korea.kr</X-Original-RCPTTO>
      <DKIM-Signature>v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1537401896; bh=RkRNy4LYDUBwMpqs9xlAjQRBIX0KKxYUxcvgnmr0qaU=;
        h=Date:From:Reply-To:Subject:References:From:Subject;
        b=r+YwSHmQTgS206vqdpyHTnO9fCYBlOBUz0t4z6ApjGLRqFfgTjgXNy+LntHZERy874pT6bpSVyOtdfciuJtY94UqhQKD/qw9wwn4a/dgBFhCKmta2IfGZF2VqUNPO
        Signature>
      <X-YMail-OSG>o737i.IVM1lV5227k6oJsZM5rQKA3yrf2Rpj5PQk2n7LpDdBHYmZVtDf.61kEXM
        hg4nf4KFOjLb4p_TZtvzxur5mjMATVE.sLmPUKTvJ4G4phXVTMcaQNaRNB2TFtE1KCnNAl0zd9jQ
        FGxuQuhKVhoh9MB_rLyjRv18PLsZlgOGtA3mD4TyB0d2RCk7O5W8u97wqmjvdas7VI_fSIC2kc4l
        hbwcokihoPg6UfUHvi8Dm99dlPwt0HYS0OF9nCi3fkvrnK3ywAMlrdDLITE.QnLo_EIX_2R.IThZ
        z3So.5Aumv.XS7aJhEBvEseyqNunzz7sb77IhC_l37LGdEF9Kud._35MXUVAZCI2jdNiD2opKv0M
        LDgwFn8SgW4BWnTed3c_66IJ0FynYarEI15A6Z6CS_aDfIJANTubLm6LUzXY6qhTfuVDgFn3.CGP
        cshC_78..YaO6NBG10FYcirmbWAix2_jjUvjVu1Hydh18Tu4JwZy25jdbZcvpGnea.4EToseTwMp
        dwwmBngau6lEIXYYch7epkTKh5vNe8Vh5VGoivGBESWsI0LMLgT0_BNgkFaP9pE9YQ7ghNHSZ01l
        XwzpBfLIYVeHsASgORHjLwKJCSrYufjH4B73OX9lIAt7fV187EYEh091jZ06fOg--</X-YMail-OSG>
      <Date>Thu, 20 Sep 2018 00:00:54 +0000 (UTC)</Date>
      <From>ugbonine <[redacted]e8@yahoo.com></From>
      <Message-ID><[redacted]504.57649.1537401654463@mail.yahoo.com></Message-ID>
      <MIME-Version>1.0</MIME-Version>
      <Content-Type>multipart/mixed; boundary="----=_Part_57648_1636766791.1537401654463"</Content-Type>
      <References><[redacted]504.57649.1537401654463.ref@mail.yahoo.com></References>
      <X-Mailer>WebService/1.1.12473 YahooMailNeo Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106
        Safari/537.36 OPR/55.0.2994.61</X-Mailer>
      <Content-Length>962853</Content-Length>
    </eml>
  </Email>
```

(Fig. 4) XML Format

3.2 Construction of Hacking E-Mail IOC

As shown in [Table 2], in this study, a total of 21 forensic artifacts were selected from 33 E-Mail forensic IOC artifacts in order to configure necessary indicators for Hacking E-Mail detection. Once the 21 indicators are analyzed for the header, body, and attachments extracted through the EML extract system introduced in Section 3.1, the IOCs for malicious E-Mails are configured by constructing the indicators of the actual Hacking E-Mails and the weight and logical combination of each indicator to be preserved. Each set of indicator and content data is matched with the existing malicious E-Mail information and then categorized into conditions of same, inclusion, or below setting. Further, each set is weighted from 0.1 to 1.0, where the weighted value represents the degree of suspicion for the given malicious E-Mail data. Although the key analysis elements are execution records or logs when detecting and identifying a compromise incident at the client-side, such as a server or PC, the scope of E-Mail data is much more broad and the verification factors are extremely limited, thus the key analysis element for E-Mails is the comparative analysis of uniformity with previously traced harmful data.

If the set of indicator and content data is deemed to be malicious E-Mail with a certainty, a weight value of 1.0 is assigned, and this was applied to the case of file hash values of E-Mail attachment file category. As a way of detecting suspicious E-Mail senders and receivers, IP X-Original-SENDERIP, X-Original-E-MailFROM, and X-Original-RCPTTO indicators from Header, and HyperText LINK indicator from Body are given a weight of 0.5 each. Further, as for the score indicators, subject, from, and X-E-Mailer indicators from Header, and Filename and Contents-Type indicators from Attachment File are given a weight of 0.25 each. Additionally, the rest 12 indicators are option values and E-Mail forensic IOCs that can be used as prospective referencing indicators when a malicious E-Mail is detected, and they are given a weight of 0.1 each.

<Table. 2> Hacking E-Mail IOC

item	Indicator	Composition	Content	condition	weight
HEADER	Subject	AND	Suspicious Subject	Inclusion	0.25
	From	AND	Suspicious E-Mail Address	sameness	0.25
	message	AND	Suspicious message	sameness	0.1
	Received	AND	Suspicious Domain Name	sameness	0.1
	X-Original-SENDERIP	AND	Suspicious IP Address	sameness	0.5
	X-Original-E-MailFROM	AND	Suspicious E-Mail Address	sameness	0.5
	X-Original-RCPTTO	AND	Suspicious E-Mail Address	sameness	0.5
	DKIM-Signature	AND	Suspicious DKIM-Signature	sameness	0.1
	Received	AND	Suspicious IP Address	sameness	0.1
	Date	AND	Date	sameness	0.1
	Reply-To	AND	Suspicious Reply-To	sameness	0.1
	Message-ID	AND	Suspicious Message-ID	sameness	0.1
	MIME-Version	AND	Suspicious MIME-Version	sameness	0.1
	Content-Type	AND	Suspicious Content-Type	sameness	0.1
	References	AND	Suspicious References	sameness	0.1
	X-E-Mailer	AND	Suspicious Client Program Name	sameness	0.25
	Content-Length	AND	Content-Length	setting or less	0.1
BODY	HyperText LINK	AND	Suspicious URL	sameness	0.5
	Body Text	AND	Suspicious Body Text	Inclusion	0.1
Attachment File	filename	AND	Suspicious filename	Inclusion	0.25
	Contents-Type	AND	Suspicious Contents-Type	sameness	0.25
	File Hash	OR	Suspicious Hash(SHA1)	sameness	1.0

In the above table, composition is categorized into logical operations of AND and OR. The AND logical operation is expressed as the sum of weights corresponding to the indicators, where the maximum sum of weights cannot exceed 1. As for OR logical operations, the result is expressed as an indicator function, meaning that if the E-Mail attachment file corresponds to the file hash indicator, the weight is expressed by 1, otherwise the weight is expressed by 0. Accordingly, the total weight is the maximum value from logical operations of AND and OR. Equation (1) below describes the weight calculation formula according to logical operation.

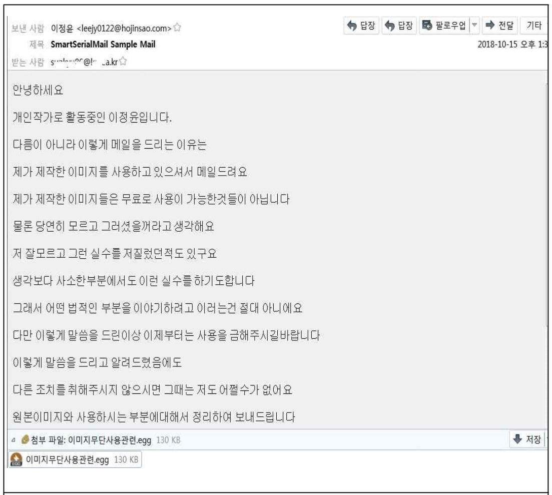
$$ight = Max[(\quad Matched\,Content\ Weight), I\ (x)], \tag{1}$$

$$x) = \begin{matrix} 1 \text{ for } x = file\ hash \\ 0 \text{ for } x \quad file\ hash \end{matrix}$$

4. Verification and Conclusions

4.1 Verification and Utilization of Hacking E-Mail detection indicator

To verify the effectiveness of the indicators, a total of 300 malicious E-Mails were extracted through the proposed system and the results were examined. As a result, a total of 47 E-Mails, which account for 15.7 percent of E-Mails, had the maximum weight value of 1.0. Among these E-Mails, 20 E-Mails were detected due to the matching File Hash indicator, and 27 E-Mails were detected based on the indicator combinations through AND operation. In all E-Mails, a weight value of 0.5 or higher was observed. [Figure 5] is an Hacking E-Mail that included a malicious attachment of GandCrab ransomware distributed on October 15, 2018. As shown in the figure, in Case 1 with AND logical operation combination, total sum of weights exceeded the maximum value of 1.0 due to the four detected indicators. In Case 2 with OR condition, the hash value of the attachment was matched, thus the weight value of 1.0 is assigned.



보낸 사람 이정윤 <leejy0122@hojinsao.com>
제목 SmartSerialMail Sample Mail
2018-10-15 오후 1:3
받는 사람 s[redacted]a.kr

안녕하세요

개인작가로 활동중인 이정윤입니다.

다름이 아니라 이렇게 메일을 드리는 이유는

제가 제작한 이미지를 사용하고 있으셔서 메일드려요

제가 제작한 이미지들은 무료로 사용이 가능한것들이 아닙니다

물론 당연히 모르고 그러셨을꺼라고 생각해요

저 잘모르고 그런 실수를 저질렀던적도 있구요

생각보다 사소한부분에서도 이런 실수를 하기도합니다

그래서 어떤 법적인 부분을 이야기하려고 이러는건 절대 아니에요

다만 이렇게 말씀을 드린이상 이제부터는 사용을 금해주시길바랍니다

이렇게 말씀을 드리고 알려드렸음에도

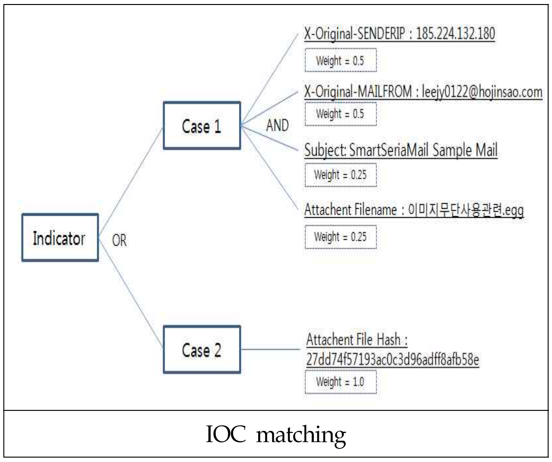
다른 조치를 취해주시지 않으시면 그때는 저도 어쩔수가 없어요

원본이미지와 사용하시는 부분에대해서 정리하여 보내드립니다

첨부 파일: 이미지무단사용관련.egg 130 KB

이미지무단사용관련.egg 130 KB

Hacking E-mail body and attachment file


Indicator
OR
Case 1
AND
X-Original-SENDERIP : 185.224.132.180
Weight = 0.5
X-Original-MAILFROM : leejy0122@hojinsao.com
Weight = 0.5
Subject: SmartSeriaMail Sample Mail
Weight = 0.25
Attachent Filename : 이미지무단사용관련.egg
Weight = 0.25
Case 2
Attachent File Hash : 27dd74f57193ac0c3d96adff8afb58e
Weight = 1.0

IOC matching

(Fig. 5) Hacking E-Mail IOC Detection

The proposed indicators should be implemented as a method of extracting and indexing the unique forensic artifacts of Hacking E-Mails when storing and converting the malicious E-Mails collected through various paths into a database. As described earlier, the key elements in detecting suspicious E-Mails are aggregating and securing many databases composed of malicious E-Mails and then conducting comparative analysis to identify the attacks. In general, even if a system that can conduct dynamic analysis on E-Mail attachments is established, conducting an accurate detection of malicious E-Mails in which hyperlinks or graphic files are enclosed in the E-Mail body instead of attachments is difficult. Such E-Mails can typically be detected by matching with previously established databases having malicious information. Thus, the proposed EML extract system should be utilized by configuring it into a database mirroring environment to enable extracting EML files from SMTP servers so that malicious E-Mail data can be identified by comparing them with the continuously aggregated databases having Hacking E-Mail data. In addition, the system should be utilized to continuously scale up the Hacking E-Mail indicators over the long term.

4.2. Conclusion and Suggestions

In this study, Hacking E-Mail indicators were configured by applying the forensic IOC artifacts of E-Mails, and a system that can extract related data was proposed and evaluated. In order for a security team of company or institution to implement our proposed indicators, it should be noted that a system for continuously aggregating and managing data should be established for a reliable data comparison between the existing and suspected malicious data. As the data verification of this study was conducted with limited number of samples, we plan to improve the results by accumulating actual operating system data over the long term. Further, in this study, a limited number of static data was used to extract and compare the hash values, file names, content types of the E-Mail attachments. For further research, we plan to expand the data and study additional items.

References

[1] Tae-Kyung Kim, "The study of detection methods for malicious code", Journal of Security Engineering, vol 9, no 5, pp.387-400, 2012.

[2] Yoon-Jae Park, Myung-Sin Chae, "A Research on the Effectiveness of the Vulnerability Detection Against Leakage of Proprietary Informatio Using Digital Forensic Methods", Journal of the Korea Academia-Industrial Cooperation Society, vol 18, no 9, pp.462-472, 2017.

[3] Lee Min Wook, Yoon Jong Seong, Lee Sang Jin, "Digital Forensic Indicators of Compromise Format(DFIOC) and It's Application, KIPS Transactions on Computer and Communication Systems", vol 5, no 4, pp.95-102, 2016.

[4]https://securelist.com/kaspersky-security-bulletin-spam-and-phishing-in-2016/77483/, Feb 20 2017.

[5] Jun-Hyung Lee, Jung-Won Cho, 'The World of Digital Forensic', InfoTheBooks, 2014.

[6] Sang-Duk Jeong, Dong-Sook Hong, Ki-Jun Han, "Technology Trends and Prospects of Digital Forensic", National Information Society Agency, 2006.

[7] Stephen Larson, "Book Review: The Basics of Digital Forensics: The Primer For Getting Started in Digital Forensics", Journal of Digital Forensics, Security and Law, Vol.9, No.1, pp.83-85, 2014.

[8] Simson Garfinkel, "Digital forensics XML and the DFXML toolset". Vol.8. pp.161-174, 2012.

[9] Seong-Ho Kim, "A method to indicator compromise utilization for the effective infringement accident analysis", May 2015.

[10] Chris Alberts, Audrey Dorofee, Georgia Killcrece, Robin Ruefle, Mark Zajicek, "Defining Incident Management Processes for CSIRTs : A Workin Progress", CMU SEI(Carnegie Mellon University Software Engineering Institute), Oct 2004.

[11] Karen Scarfone, Tim Grance, Kelly Masone, "Special Publication 800-61 Revision 1 Computer Security Incident Handling Guide(Recommendations of the National Institute of Standards and Technology)", Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Mar 2008.

[12] https:/www.rfc-editor.org/rfc/rfc2822.txt, Apr 2001.

〔저자소개〕

이 후 기 (Hoo-Ki Lee)
2010년 2월 동국대학교 정보보호 석사
2018년 2월 숭실대학교 일반대학원 IT정책학 공학박사
현재 : 건양대학교 사이버보안공학과 교수
관심분야 : Security Threat Analysis, Security Engineering for High-Assurance Systems, Digital Forensic
email : hk0038@konyang.ac.kr