Indian Journal of Science and Technology, Vol 8(19), DOI: 10.17485/ijst/2015/v8i19/80196, August 2015
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Design of Quantification Model for Prevent of Cryptolocker

Donghyun Kim[1], Wooyoung Soh[2] and Seoksoo Kim[1*]

[1]Department of Multimedia, Hannam University, Korea; sskim0123@naver.com
[2]Department of Computer Engineering, Hannam University, Korea

Abstract

The growth of ICT (Information and Communication Technology) within the society has become increasingly digitized, thus, the overall activity has amounted to various researches for protecting any data from malicious threats. Recently, ransomware has been a rapidly propagated subject for social engineering techniques especially the ransomware crypto locker. Users can delete a crypto locker code using an antivirus software code. However, the encrypted data would be impossible to recover. Therefore, crypto locker must be prevented and must have early detection before it infects any data. In this paper, we are proposing a quantification model to prevent and detect any cryptographic operations in the local drive.

Keywords: Cryptolocker, Prevent Model, Quantification, Social Engineering, Warning Technologies

1. Introduction

Recently, the development of ICT (Information Communication Technology) within the society has become increasingly digitized, the national society's overall activity has been closely related to cyberspace as the growth of ubiquitous environment heightens. Then the overall activity has amounted to various researches for protecting any data from malicious threats[1].

Recently, not only technological engineering techniques but also social engineering has been applied to target against attacks such as APT (Advanced Persistent Threat)[2].

Malicious codes are the main cause of cyber-attacks and the main factor of threating networks. They are malicious programs that are installed without users' agreement to threaten users' information or systems[3].

The initial malicious codes were mostly virus-typed ones to destroy systems. With the development of information communication technology, they have continued to evolve. Ransomware like crypto locker, a recent top issue, employs social engineering[2] techniques that are used to trigger users' curiosity and induce users to make approach. Therefore, such malware emerges as a more powerful threat.

Crypto Locker can be detected and deleted by general security programs. But, once infected with the malicious program, it is hard to recover encrypted files[3].

For the reason, in the case of crypto Locker, it is necessary to make pre-detection, rather than post-detection, in order to protect users' critical data.

Therefore, based on a social engineering technique, this paper designs a quantification model to previously detect the data encryption work of crypto locker with which a user's PC is infected.

2. CryptoLocker

CryptoLocker, a sort of Trojan horse virus, targets computers running Microsoft Windows Operating System.

Cypto Locker propagates via email attachments as if it is a normal file. Once activated, the ransomware uses the encryption of a private key saved into its control server and RSA open key to encrypt the files with specific formats in the local network drive[3].

Crypto Locker can be deleted by vaccine programs, but it is impossible to recover the infected computer's files encrypted by the malware.

*Author for correspondence

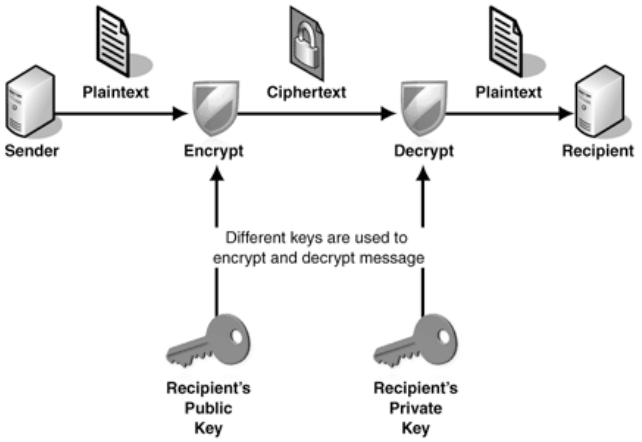

Figure 1. Structure of Crypto Locker.

3. Intrusion Detection System

3.1 File-based Intrusion Detection System

File-based detection method is based on the fact that a malicious code takes the form of a PE (Portable Executable) file in an operation system. It must have a signature of specific format to determine the PE type malicious code. Signature-based detection has the advantage of fast scanning as it examines particular or unique part of a file classified as a malicious code.

However, it causes false negative that disables detection if the file size changes even by a few hundred bytes, which only enables response to codes detected in advance and not unknown codes with a new format[4].

The scanning engine checks files using key generation and other commands in a particular registry a specific folder from malicious codes. By comparison with heuristic signature, it determines the level of similarity with generally known malicious codes and detects lesser-known malicious codes.

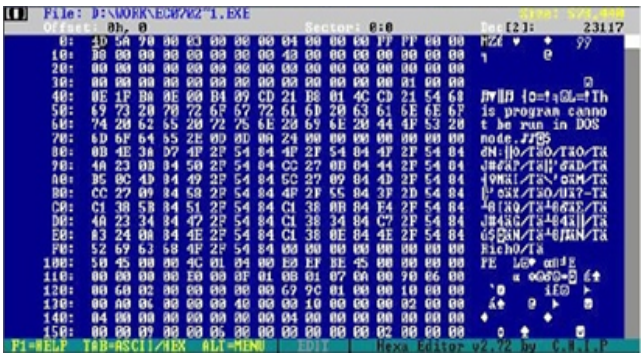

Figure 2. Malicious code of PE (Portable Executable) type.

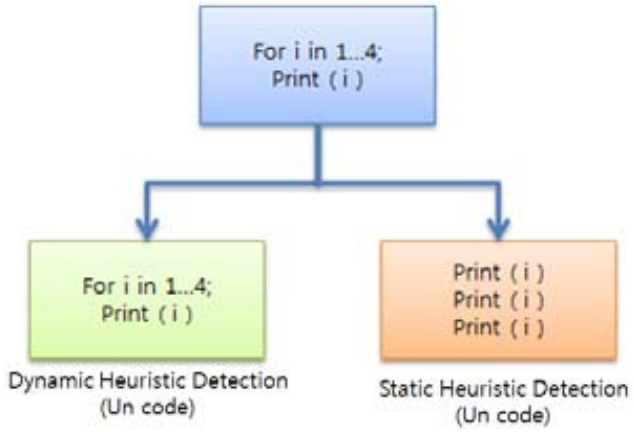

Figure 3. Dynamic and static heuristic detection code.

Depending on what form the scanning engine takes while heuristic analysis for the subjected files, it is classified as dynamic heuristic detection and static heuristic detection.

Although it can detect both known and unknown malicious codes, there is a possibility of misdiagnosing normal files as malicious codes and, especially given the characteristics of anti-virus software that deletes and fixes files, high rate of misdiagnosis can lead to considerable problems to the computer system itself[5].

3.2 IP Trace back Algorithm

Features an IP verification function that checks the source IP or destination port that is fed into the router through Standard or Extend Access-list, and improve the router performance with filtering, which allows it to prevent changing sender address. However, it should be applied to all routers and cannot efficiently track back large packets like DoS (Denial of Service) attack[6].

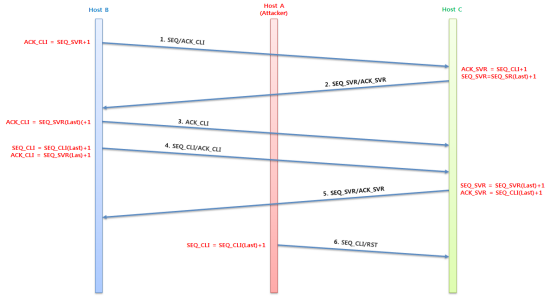

Figure 4. Track back large packet in DoS.

In the routers that compose a network, it checks the connected links and whether the traffic packet sent from a DoS attack. However, it does not provide automated track back and directly combines and determines the packet path, which causes overhead in network management[7].

After recording characteristic of packets transmitted from a router, it applies deduction system such as data mining to detect the source of attack. However, a large quantity of information must be stored and managed and the amount of data processing is substantial, which makes it less efficient[8].

Hash-based IP trace-back composes SPIE (Source Path Isolation Engine)- based track back server and manages the network based on agent for each subgroup. And, each router features DGA (Data Generation Agent) for operation. DGA collects and manages IP header data, which is hash value of packet message from relevant routers, and 8byte payload and saves them in the bloom filter structure.

When IDS in the receiver system detects cyber-attack, if compares and analyzes data stored in DG router within the group and hacking packet information through SCAR (SPIE Collection and Reduction) agent and SPIE receives the data and reconfigures the transmission path of hacking-related packets. While it can be applied to ISPs in different model environments, SPIE, SCAR agent, and DGA must be built HANCE requires memory to manage the hash value for the packets on a regular basis[9].

When there is a hacking attack, IPSec connection is formed between the network router and the attacked system. When the attack packet is sent through the relevant router from the attacker, the path information is sent to the attacked system though IPSec tunnel and this process is repeated. This enables determination of router on the path through which the packet has been sent during the hacking. The trackback method based on IPSec can find the attack path if there is an IPSec tunnel built between the attacked system and router on the other hand, problems can be found in path reconfiguration for networks that do not support IPSec connection[10].

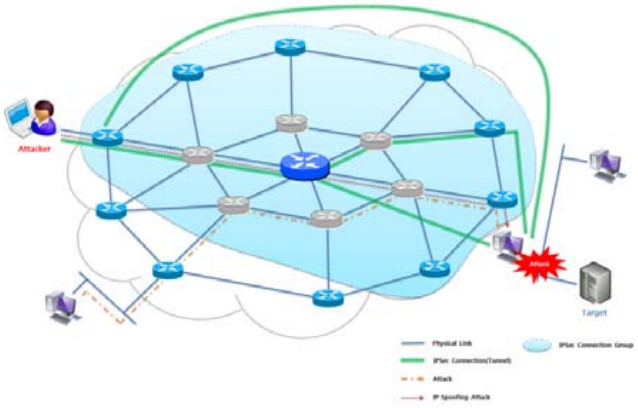

Figure 6. Structure of IPSec dection system.

4. Quantification of Crypto Locker

Conventional qualification techniques are limited to technique security areas in terms of threat factors and thus it is impossible to draw a risk calculation formula for post-quantification.

For pre-quantification of Crypto Locker based on a social engineering technique, it is necessary to apply social-engineering attackers' perception or behavior patterns.

Therefore, in the addition of other social engineering threat[11] factors than the technical threat factors of Crypto

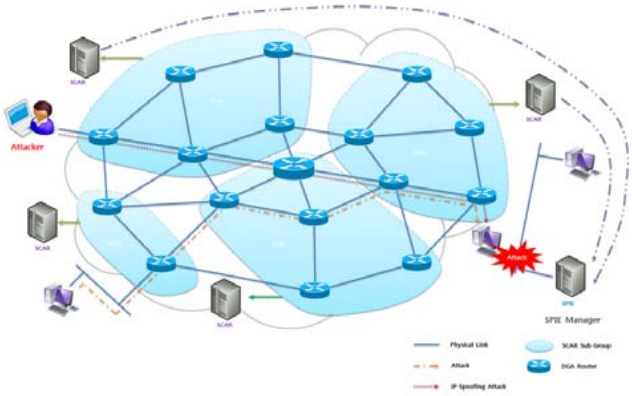

Figure 5. Structure of SPIE.

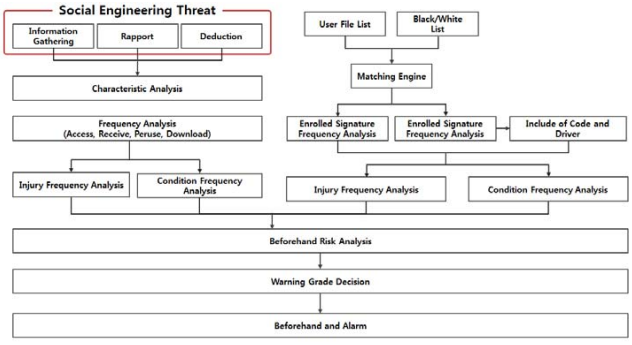

Figure 7. Prevent quantification model for Crypto Locker.

Table 1. Pauedo code for frequency user access

```
K_R ← 16-bit random number
M_R ← K_R XOR h(A)

For each Packet p
{
        If p.ID = 0 Then
         p.ID ← M_R
        else
        {
                M_old ← p.ID
                M_new ← M_R XOR SRC(M_old)
                p.ID ← M_new
        }
}
```

Locker, this paper designed a quantification model based on threat factor frequency.

The above quantification model first analyzes social engineering threat factors including information collection, rapport, and disguise and Crypto Locker's existing characteristics. Based on the analyzed information, the model analyzes possibility and situational frequency by conducting frequency analysis on users' access, receipt, opening, downloading and execution.

With the use of matching engine for white/black list and user PC's registered file lists, it analyzes the frequencies of registered signatures and unregistered signatures and checks that any codes and drivers are included in unregistered signatures to analyze possibility and situational frequency.

$$R = \sum_{l=1}^{k} A_1 + \sum_{l=1}^{\gamma} B_l \quad (1)$$

With the results of infection possibility and situational frequency, the model analyzes a risk level. If the analyzed risk level exceeds a designated risk level, the model determines an alarm degree and gives a warning to a user in advance.

5. Conclusion

This paper designed a quantification model based on a social engineering technique to prevent Crypto Locker.

In the case of Crypto Locker, it is necessary to make pre-detection, rather than post-detection, in order to protect users' critical data.

Therefore, in this paper necessary to apply social-engineering attackers' perception or behavior patterns. And white/black list and user PC's registered file lists, it analyzes the frequencies of registered signatures and unregistered signatures and checks that any codes and drivers are included in unregistered signatures to analyze possibility and situational frequency.

The quantification model proposed in this paper includes social engineering factors so that it suggested the guidelines of quantification system for objective prevention more than the conventional analysis methods focusing on technical factors.

The future study will apply the technology of detecting the process of receiving a private key in Crypto Locker's control server and thereby design a more systematic quantification model.

6. Acknowledgment

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2013R1A1A2006026).

This paper has been supported by the 2015 Hannam University Research Fund.

7. References

1. Han BJ, Choi YH, Bae BC. Generating Malware DNA to Classify the Similar Malwares. Journal of The Korea Institute of Information Security and Cryptology. 2013; 23(4):679– 94.
2. Dell Secure Works, Anatomy of an Advanced Persistent Threat (APT). 2012.
3. Gu G, Porras PA, Yegneswaran V, Fong MW, Lee W. Bot Hunter: detecting malware infection through IDS-driven dialog correlation. USENIX Security. 2007; 7:1–16.
4. Merriam - webster [Internet]. Available from: http://www.merriam - webster.com/dictionary/engineering?show = 0&t = 1352683275
5. Smith B. Crypto viral Extortion. 2013.
6. Turner D, Fossl M, Johnson E, Mack T, Blackbird J, Entwisle S, Low MK, McKinney D, Wueest C. Symantec Global Internet Security Threat Report. 2008.
7. Arbor Networks, Worldwide Infrastructure Security Report. 2007.
8. Feguson P. Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing. Ferguson 2000 Network. 2000.
9. Savage S, Wether all D, Karlin A, Anderson T. Practical network support for IP trace back. ACM SIGCOMM Computer Communication Review. 2000; 30(4):295–306.

10. Aljifri H. IP trace back: a new denial-of-service deterrent. IEEE Security and Privacy. 2003; 1(3):24–31.
11. Park K, Lee H. On the effectiveness of probabilistic packet marking for ip traceback under denial of service attack. Proceedings of 20th Annual Joint Conference of the IEEE Computer and Communications Societies; 2001. 1. p. 338–47.
12. Snoeren AC. Hash-based IP traceback. ACM SIGCOMM Computer Communication Review. 2001; 31(4): 3–14.
13. Ansari N, Belenky A. IP traceback with deterministic packet marking. IEEE Communications Letter. 2003 Apr; 7(4):162–4.