World Journal of Engineering and Technology, 2015, 3, 203-207
Published Online October 2015 in SciRes. http://www.scirp.org/journal/wjet
http://dx.doi.org/10.4236/wjet.2015.33C030

Design of Quantification Model for Ransom Ware Prevent

Donghyun Kim, Seoksoo Kim

Department of Multimedia, Hannam Universiciy, Daejeon, Korea
Email: donghyunk1986@gmail.com, sskim0123@naver.com

Received 9 September 2015; accepted 16 October 2015; published 23 October 2015

Abstract

The growth of ICT 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. Users can delete a ransomeware code using an antivirus software code. However, the encrypted data would be impossible to recover. Therefore, ransomware 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

Ransom Ware, Quantification Model, Prevent, Cryptolocker

1. Introduction

With the progress of digital society, the traditional society's activity has been closely related to cyberspace the growth of ubiquitous technology.

Most of Society activity on cyberspace protecting data from malicious threats as being society has become increasingly digital [1].

Malicious codes are the major threat of cyber-attacks, the malicious programs are installed without users agreement at same time break user system's protection to control user system secretly [2].

The initial malicious codes are virus-typed to destroy systems. With the development of computer engineering and algorithm theory, the malicious codes also evolved.

With the risk increase of malicious code, the anti-malware's design and develop are necessary. It is not only Traditional software engineering techniques but also social engineering has been applied to target against attacks such as APT (Advanced Persistent Threat) [3].

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

For that reason, in the case of protect system from ramsomware, it is effective to make pre-detection, rather than postdetection, in order to protect user's critical data.

However, ransomware is recent top issue, employs social engineering techniques that are used to trigger users curiosity and induce users to make approach. Therefore, such malware emerges as a more powerful threat [4].

How to cite this paper: Kim, D. and Kim, S. (2015) Design of Quantification Model for Ransom Ware Prevent. *World Journal of Engineering and Technology*, **3**, 203-207. http://dx.doi.org/10.4236/wjet.2015.33C030

Therefore, in this paper we provide a techniques for detect ransomware with social engineering, in this design include a quantitative model, which can be use to detecting.

2. Related Works

2.1. Ransomware

Ramsomware, a sort of Trojan virus, It is targets are which computers running on Microsoft Windows Operating System. Ramsomware propagates via email attachments using social engineering 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 [4].

In the case of fish infected with ransomware delete the ransomware through the vaccine program, it is possible to prevent the diffusion. However, if the infected computer or file to ransomware, and it is not be repaired (**Figure 1**).

2.2. File-Based Intrusion Detection Method

In the this case of ransomwares are use the Microsoft Windows Operating System's flaw base on that we ransomwares infect system core files [5].

Therefore in order to detect ransomware, use the file-based detection techniques, the provided file-based pre-detection approach is as follows.

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 [6].

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.

Depending on what form the scanning engine takes while heuristic analysis for the subjected files, it is classified as dynamic heuristic detection [7] and static heuristic detection (**Figure 2**).

2.3. IP Trace Back Algorithm

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

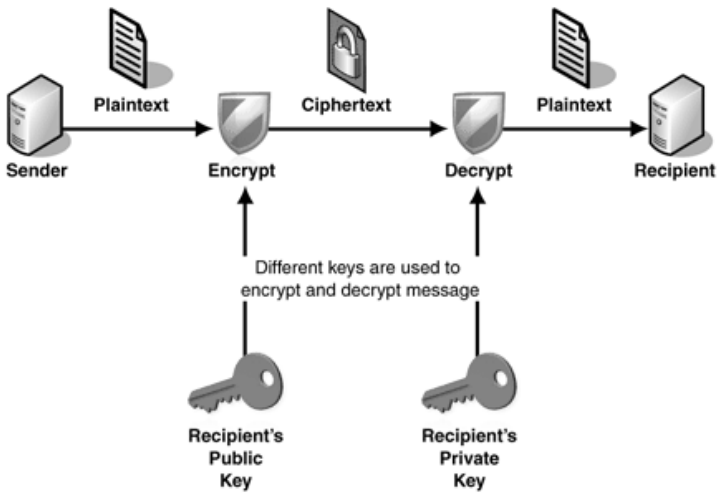

Figure 1. Structure of ransomware [4].

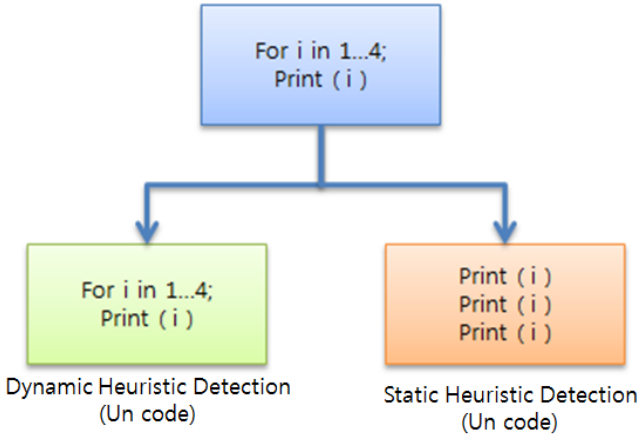

Figure 2. Dynamic and static heuristic detection code [7].

operation. DGA collects and manages IP header data, which is hash value of packet message from relevant routers, and 8 byte 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. When there is a hacking attack, IPSec connection is formed between the network router and the attacked system [8] [9].

In this paper, we provided a quantification model based on hash algorithm to against social engineering based malicious attacks. It's include social engineering threat-analysis, ransomware infection path dynamic detection and matching engine.

3. Quantification Model for Ramsomware Prevent

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.

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

In this paper, in the addition of other social engineering threat factors than the technical threat factors of ransomware, this paper designed a quantification model based on threat factor frequency. **Figure 3** shows a structure of quantification model for ransomware prevent.

In the case of malicious attacker to use social engineering techniques, information gathering in order to improve the reliability of the attack target, Vitrac formation, in order to expand the ransomware by applying the gastrointestinal technology, the user receives a ransomware code it has been able to be situation (access, receive, peruse, download) for analyzes social engineering threat [10] factors including information collection, rapport, and disguise and ramsomware existing characteristics. Based on the analyzed information.

The model use Hash-based IP trace-back, it is analyzes possibility and situational frequency by conducting frequency analysis on users' access, receipt, opening, downloading and execution as **Figure 4**.

With the use of Dynamic and Static Heuristic Detection Code 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.

$$R = \sum_{l=1}^{k} A_l + \sum_{l=1}^{\gamma} B_l \tag{1}$$

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.

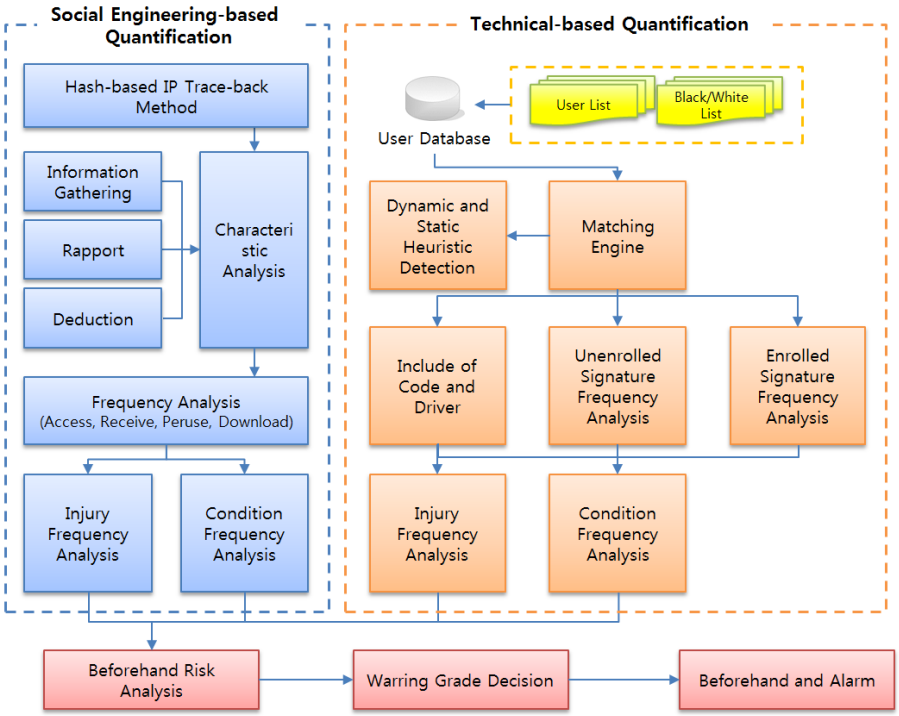

Figure 3. Structure of quantification model.

$K_R \leftarrow$ 16-bit random number $M_R \leftarrow K_R$ XOR $h(A)$
For each Packet p
{
If p.ID = 0 Then p.ID $\leftarrow M_R$
else
{
$M_{old} \leftarrow p$.ID
$M_{new} \leftarrow M_R$ XOR $SRC(M_{old})$
p.ID $\leftarrow M_{new}$
}
}

Figure 4. Pauedo code for frequencty user access.

4. Conclusions

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

In the case of ramsomware, 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.

Acknowledgements

The present research has been supported by a research grant of the Asan Foundation.

References

[1] Han, B.J., Choi, Y.H. and Bae, B.C. (2013) Generating Malware DNA to Classify the Similar Malwares. *Journal of the Korea Institute of Information Security & Cryptology*, **23**, 679-694. http://dx.doi.org/10.13089/JKIISC.2013.23.4.679

[2] Gazet, A. (2010) Comparative Analysis of Various Ransomware Virii. *Journal in Computer Virology*, **6**, 77-90. http://dx.doi.org/10.1007/s11416-008-0092-2

[3] Dell Secure Works (2012) Anatomy of an Advanced Persistent Threat (APT).

[4] Smith, B. (2013) Cryptoviral Extortion.

[5] Shin, D., Kim, Y., Byun, K. and Lee, S. (2008) Data Hiding in Windows Executable Files. *Australian Digital Forensics Conference*, **51**.

[6] Feguson, P. (2000) Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing. Ferguson 2000 Network.

[7] Nachenberg, C.S. (2012) Dynamic Heuristic Method for Detecting Computer Viruses Using Decryption Exploration and Evaluation Phases. U.S. Patent No. 6,357,008.

[8] Savage, S., Wetherall, D., Karlin, A. and Anderson, T. (2000) Practical Network Support for IP Traceback. *ACM SIGCOMM Computer Communication Review*, **30**, 295-306. http://dx.doi.org/10.1145/347057.347560

[9] Aljifri, H. (2003) IP Traceback: A New Denial-of-Service Deterrent. *IEEE Security & Privacy*, **1**, 24-31. http://dx.doi.org/10.1109/MSECP.2003.1203219

[10] Park, K. and Lee, H. (2001) On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack. *Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies*, **1**, 338-347.