International Journal of Advanced Computational Engineering and Networking, ISSN(p): 2320-2106, ISSN(e): 2321-2063
Volume-7, Issue-3, Mar.-2019, http://iraj.in

CASE STUDY ON STEGANOGRAPHY AND MALWARE

KI-HYUN JUNG

[1]Department of Cyber Security, Kyungil University, Republic of Korea
E-mail: khanny.jung@gmail.com

Abstract- Malware is any malicious software to cause damage to computer systems. Steganography is a technique to embed the secret information without any notice. Recently, malware using steganography technique is used to evade detection. In this paper, various cyber attacks are explained and malwares using steganography are described. These attacks are not only difficult to detect but also increased the damage because of various forms and combination with each other.

Keywords- Steganography, Malicious Code, Malware, Information Hiding.

I. INTRODUCTION

Cybersecurity issues are becoming everyday struggle in the world. In the U.S. economy, malicious cyber security activity was estimated between $57 billion and $109 billion in 2016 [1-2].

Malware describes any malicious program or code whose purpose is designed to cause harmful damage to a computer. Malware takes many forms of software that may be deployed on desktops, servers, mobile devices, printers and programmable electronic devices. There are many different types of malware such as virus, worms, Trojan, backdoors, rootkits, bots, spyware, ransomware, adware, and scareware [3-4].

Steganography is one kind of information security to communicate with secret by hiding the existence of the secret data itself [5-6]. Digital contents such as image, video, text, audio, network protocol and DNA are used as communication mediums. Steganography can be divided into spatial/frequency domain based techniquesor technical/linguistic based techniques as shown in Fig. 1.

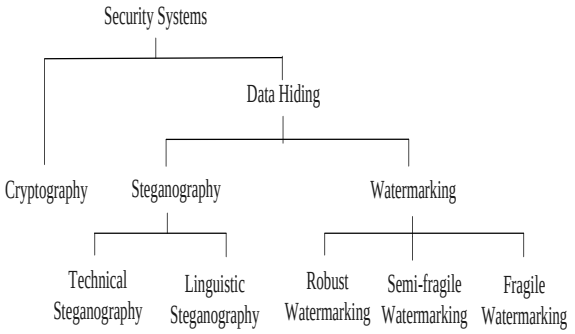

Fig. 1. Techniques in security system.

Recently, malware using steganography techniques was found to hinder detection [7-9]. The malicious code can be carried as hidden messages in image, voice, audio/video and even electrocardiogram data. Hackers use steganography to evade detection by conventional security tools when infiltrate computer systems.

In this article, some malwares using steganography technique are described and damage caused by malware is shown to get interests and research in the field.

II. MALWARE AND STEGANOGRAPHY

2.1. Cyber and Malware Attacks

Common types of cyber attacks are shown inFig. 2. [10-11]. TCP SYN flood attack, teardrop attack, smurf attack, ping of death attack and botnets attacks are common types of DoS/DDoS attack. Session hijacking, IP spoofing and Replay attacks are common types of MITM attack. Drive-by download attack is used generally to spread malware, where hackers plant a malicious script into HTTP or PHP code for insecure websites. For password attack, brute-force and dictionary attacks are often used. The birthday attack try to find two random messages that generate the same message digest by hash algorithms.

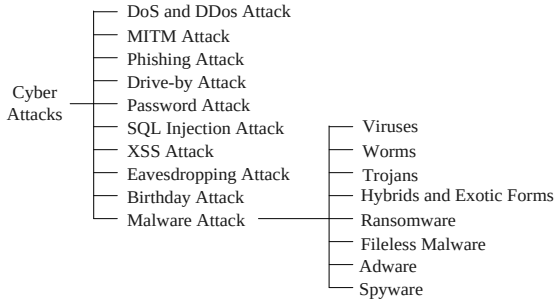

Fig. 2. Types of cyber attacks.

Malware can be described as unwanted software that is installed without consent. Common types of malware are viruses, worms, Trojans, hybrids, ransomware, adware, spyware and so on. Viruses are the only type of malware that can infect other files. Worms have ability to replicate itself and to spread without end user action. Trojans hiding in a useful program contain malicious instructions that can establish a back door and exploit by attackers. Recently, most of malware programs are considered rootkits or stealth programs.

2.2. Malware Examples

An attacker uses steganography to embed securely a piece of malicious code. In smartphone apps,

steganography malware contains three basic components: stego-text, stego-key, and steganography extracting algorithm [8]

There are some cases of malware using steganography [13-14]. Lurk malware was documented in 2014, which is used to download additional malware on infected computers. Lurk downloads firstly an image which embeds a download URL by least significant bit replacement. The GoziNeverquest malware can inject malicious code into browsers to retrieve URLs, where it could download the configuration file from decrypted a URL from image pixel. Stegoloader is a modular information stealer to check whether it is an analysis computer and then to download an image file from a legitimate website.

2.3. Malware Inspection Scenarios

Malware installation to target systems is complex, but two main steps are required. First, initial decryption and installation of the malware is needed. Second, download of the inspected image and use of the hidden secret information are required to establish covert communication further actions.A possible scenarios malware using steganography is shown in Fig. 3.

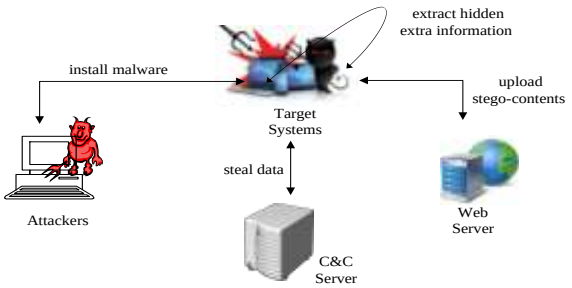

Fig. 3. Attack scenarios.

III. FUTURES AND DISCUSSION

3.1. Malware Statistics

According to AV-TEST statistics, over 350,000 new malware and potentially unwanted applications are registered [15].

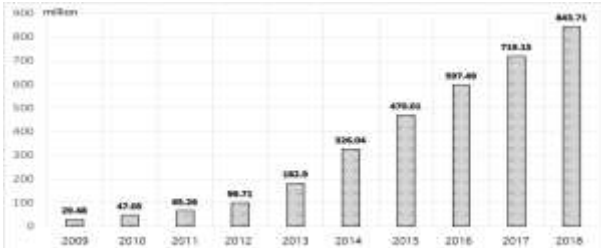

Fig. 4. Malware statistics.

3.2. Steganography in Malware

Malware using steganography can be extremely difficult to detect and scanning performance for every files on small and non-impacting anomalies are huge. Nowadays, more intrusion cases are being found as criminals.

CONCLUSIONS

Steganography has been used for evading detection in malware. Malware attacks are very difficult to detect because of various forms and combination. As results, the damage from malware attacks will increasing. Interests of security and research in the field are mandatory in the future.

ACKNOWLEDGMENTS

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(NRF-2018R1D1A1A09081842),Ministry of Culture, Sports and Tourism(MCST) and from Korea Copyright Commission in 2018(2018-f_drm-9500), and Brain Pool program funded by the Ministry of Science and ICT through the National Research Foundation of Korea(No. 2018H1D3A2065993).

REFERENCES

[1] A.P. Namanya, A. Cullen, and J.P. Disso, “The world of malware: an overview”, IEEE 6th International Conference on Future Internet of Things and Cloud, pp. 420-427, 2018.
[2] The Council of Economic Advisers, “The cost of malicious cyber activity to the U.S. economy”, February 2018.
[3] Malware, https://en.wikipedia.org/wiki/Malware.
[4] A. Makandar, A. Patrot, “Overview of malware analysis and detection”, International Journal of Computer Applications, pp. 35-40, 2015.
[5] M.S. Subhedar, V.H. Makar, “Current status and key issues in image steganography: a survey”, Computer Science Review, pp. 95-113, 214.
[6] M. Hussain, A.W.A. Wahab, Y.I.B. Idris, T.S. Ho, and K.H. Jung, “Image steganography in spatial domain: a survey”, Signal Processing: Image Communication, pp. 46-66, 2018.
[7] L.J. Young, “The dark side of steganography”, https://spectrum.ieee.org, 2015.
[8] S.T. Guillermo, E.T. Juan, and P.L. Pedro, “Stegomalware: playing hide and seek with malicious components in smartphone apps”, International Conference on Information Security and Cryptology, pp. 496-515, 2014.
[9] L. Mosuela, “How it works: steganography hides malware in image files”, https://www.virusbulletin.com, 2016.
[10] J. Melnick, “Top 10 most common types of cyber attacks”, http://blog.netwrix.com, 2018.
[11] R.A. Grimes, “8 types of malware and how to recognize them”, httpd://www.csoonline.com, 2018.
[12] P.M. Bureau, C. Dietrich, “Hiding in plain sight”, Black Hat, 2015.
[13] F. Wu, H. Narang, and D. Clarke, “An overview of mobile malware and solutions”, Journal of Computer and Communications, pp. 8-17, 2014.
[14] K. Cabaj, L. Caviglione, W. Mazurczyk, S. Wendzel, A. Woodward, and S. Zander, “The new threats of information hiding: the road ahead”, IT Professional, pp. 31-39, 2018.
[15] Total Malware, https://www.av-test.org/en/statistics/malware/.

★★★