



KOREAN SOCIETY FOR INTERNET INFORMATION

The 15th Asia Pacific International Conference on Information Science and Technology (APIC-IST 2020)

July 5-7, 2020, Sheraton Seoul Palace Gangnam Hotel, Korea

<http://www.apicist.org/2020>

Proceedings of APIC-IST 2020

| Organized by |

**Korean Society for Internet Information (KSII)
The University of Queensland (Australia)**

| Sponsored by |



Contents



2-3	A study on the genetic algorithm for solving the job shop scheduling problem Fuladi Shubhendu, Chang Soo Kim (Pukyong National Univ., ROK)	44-46
2-4	Implementation of Subjective Visual Vertical Testing System with Virtual Reality Hongly Va, Sungjin Lee (Soonchunhyang Univ., ROK), Soo Kyun Kim (Jeju National Univ., ROK), Min Hong (Soonchunhyang Univ., ROK)	47-49
2-5	VR based random dot kinematogram for Mild cognitive impairment Jun Ma, Eek-Sung Lee, Min Hong (Soonchunhyang Univ., ROK)	50-52
2-6	TestHub - Towards An Ecosystem for software and hardware testing using AI and ML Tahir Hussain, Mir Hassan Qazi, Zahoor Ahmad, Isma Farah Siddiqui (Mehran Univ. of Engineering & Technology, Pakistan)	53-61
3-1	A Detection of Webtoon Infringement Site Using Page Source Analysis Eui-Jin Kim, Seul-Ki Choi, Jin Kwak (Ajou Univ., ROK)	62-65
3-2	Drive-by Download Detection Method with Traffic Analysis Hee-Seung Lee, Jin Kwak (Ajou Univ., ROK)	66-69
3-3	Video Steganography-based Botnet Communication in Telegram Messenger Minkyung Kwak, Youngho Cho (Korea National Defense Univ., ROK)	70-73
3-4	Research on Cyber Intelligence Preparation of the Battlefield Visualization Plan using BGP Archive Data Jaepil Youn (Sejong Univ., ROK), Oh Haengrok (Agency for Defense Development, ROK), Jiwon Kang, Dongkyoo Shin (Sejong Univ., ROK)	74-80

Drive-by Download Detection Method with Traffic Analysis

Hee-Seung Lee¹ and Jin Kwak²

¹ISAA Lab., Department of Computer Engineering, Ajou University
Suwon, Republic of Korea

²Department of Cyber Security, Ajou University
Suwon, Republic of Korea

[e-mail: hslee.isaa@gmail.com, security@ajou.ac.kr]

*Corresponding author: Jin Kwak

Abstract

Drive-by Download has been cited as one of the serious threats in recent is a method of distributing malicious code through vulnerabilities such as websites and applications. In the past while the procedure of distribution had been reading E-mail or USB by users, Drive-by Download has been an attack that infects malicious code just by accessing websites has malicious code. Drive-by Download has a characteristic make web pages access via several pages distribute and execute malicious code. In this paper, we analyzes behaviors of Drive-by Download raises HTTP packets based on TCP protocol and configures them with a single flow. We proposed method for detecting Drive-by Download with correlation analysis between first request packet and final response packet and analysis of number of webpage redirection.

Keywords: Detection, Drive-by Download, Traffic Analysis, Web based Attack

1. Introduction

With IT techniques getting more and more advanced, it is giving convenience to life. But as technology pushes on, it evolves attack method. Accordingly, the importance of security has come up. In particular, the performance of a portable device has become like a desktop PC recently. It affected the portable device that the attack method targeted at desktop PC [1]. In addition, financial crime and leakage of personal information had increased than they used to be. For these reasons, analysis and research are being vigorously pushed forward about the security of a portable device, that some security companies develop anti-virus for a portable device.

Accordingly, this paper proposed a Drive-by Download detection method used in the portable

device and desktop PC through traffic characteristics analysis. The proposed method is an analysis of the gap between normal sites and sites infected by Drive-by Download. This study aimed at the dynamic analysis of the Drive-by Download from the websites

This paper composition is as follows. Chapter 2 is explained the Drive-by Download overview and operation process. and Chapter 3 proposes the analysis of traffic characteristics and detection methods of Drive-by Download. And the conclusion is in Chapter 4.

2. Related Work

2.1 Overview of the Drive-by Download

Drive-by Download is one of the serious threats recently because it distributes malicious code through vulnerabilities of websites or

applications [3]. Drive-by Download infected malicious code by behavior accessing the websites, Contrary to the past method, that distribution E-mail or USB by used the user [3].

Drive-by Download has the number of characteristics, it induces to access several websites and distributes or execute malicious code in the distribution area [2].

2.2 Drive-by Download Operating Proces

The attacker used Drive-by Download for infecting about websites, and it has the operation process as follows [2,3,4].

Step 1. Infecting of Website

Attacker inserts malicious code in the websites with vulnerabilities by using SQL injection or XSS, etc.

Step 2. Accessing Users to Infected Websites

User access to the infected website without awareness.

Step 3. Analyzing Vulnerabilities in User Devices

Malicious code analyzes vulnerabilities about browsers or applications on the accessing device.

Step 4. Inducing Users into a Distribution Area

Malicious code induced the user to the distribution area by using found vulnerabilities.

Step 5. Downloading Malicious Code

Malicious code induces users to the distribution areas and then make it download another malicious code.

Step 6. Execution of Malicious Code in a Distribution Site

Malicious code executes without user recognition.

3. The Proposed Scheme

3.1 Analysis of Drive-by Download Traffic Characteristics

The traffic of the Drive-by Download has some characteristics, first, it induces several websites to access. Second, users transmit access to requests, it changed to another response like file download.

Table 1. Comparison of Characteristics of Normal and Infected Sites

	Normal site	Infected site
Redirection	Use	Use
Multiple Redirection	Optional Use	Use (2 times or more)
Response of Request	Request and result match	Request and result do not match
Execute File	Requests must be made manually by the user	Automatically execute files from malicious code
Download File	Requests must be made manually by the user	Automatically download files from malicious code

Table 1 is such as characteristics of traffic with normal sites and infected sites through the Drive-by Download. In this paper, we proposed the Drive-by Download detection method by using these characteristics.

3.2 Drive-by Download Detection Process

The proposal detection process is the same Fig. 1, based on Table 1 of section 3.1 by characteristics of traffic analysis.

Step 1. Analysis of Redirection Times

In this proposal we set the lower bound of redirection times as twice. Because when we analyze the characteristics by using the sample of Drive-by Download execute at least twice.

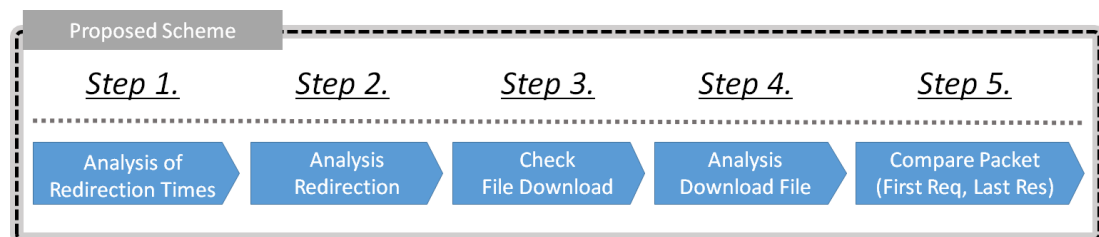


Fig. 1. Drive-by Download detection process with traffic analysis

Step 2. Analysis Redirection

When access to a website, it checks the redirection was performed and analyzes data of the packets.

TCP protocol has a rule that sends a Sequence Number of Request, that is Acknowledgment Number of Response as the Fig. 2. And HTTP protocol has a target address in the data of the packet. We consider one's phase and track response of request by using these characteristics of TCP protocol and HTTP protocol.



Fig. 2. Sequence Number and Acknowledgement Number of TCP Protocol

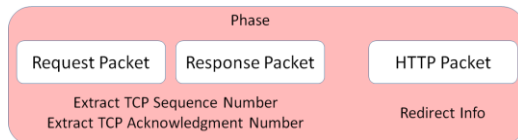


Fig. 3. Extracted Information from each Phase

Step 3. Check File Download

After redirection, it checks whether the file was downloaded or not. When the file is downloaded, the next step proceeds.

Step 4. Analysis Download File Types and Configuration the Flow

Drive-by Download analyzes file type if it is executable because it needs to download the malicious code and execute it. In addition, it configures a flow by connecting the phases in order to figure out the whole flow.

Step 5. Comparison Packet(First Request, Last Response)

Finally, it compares the first request packet that the user transmitted access request with the final response packet of configured flow. In the flow, we figure out the first request packet by the user transmitted access request and compare the first request packet, final response packet on the configuration flow.

Drive-by Download makes the access request download malicious code. It classifies the site normal and infected by using the characteristic that access request(first request packet) which is

changed to be downloading request(final response packet).

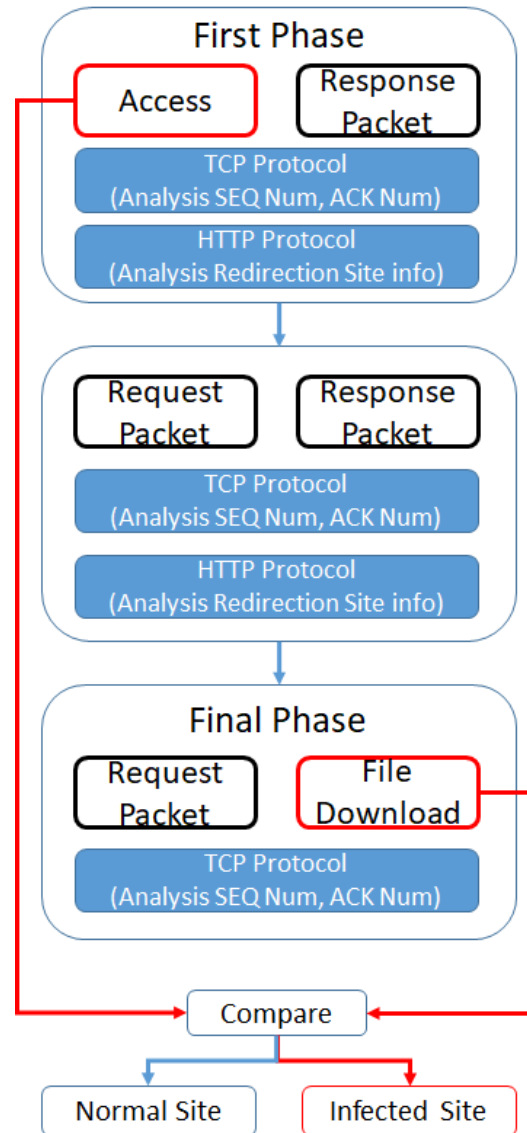


Fig. 4. Analysis Process of Step 5

4. Conclusions

In this paper, we proposed the Drive-by Download detection method using traffic analysis. The difference of Drive-by Download and normal site is redirection times and the behavior which is changed to anomaly response. This paper has the proposed Drive-by Download detection method based on the characteristics of Drive-by Download. In the future, a study on

encrypted HTTP protocol detection and implemented Drive-by Download detection method.

References

- [1] Y. Zhou, X. Jiang, "Dissecting Android Malware: Characterization and Evolution", *IEEE Symposium on Security and Privacy*, pp. 95-109, Jul. 2012.
- [2] R. Kiire, S. Goto, "Detecting Drive-by-Download Attacks based on HTTP Context-Types", *Asia Pacific Advanced Network*, pp. 1-7, Aug. 2016.
- [3] C. Choe, "Malicious program response strategies distributed over the Internet", *The Institute of Electronics and Information Engineers*, pp. 31-39, Apr. 2014.
- [4] H. Kim, I. Kim, "A Study on Characteristic Analysis and Countermeasure of Malicious Web Site", *Korea Institute of Information Security and Cryptology*, Vol. 29, No. 1, pp. 93-103, Feb. 2019.