



ICONI



KOREAN SOCIETY FOR INTERNET INFORMATION

The 11th International Conference on Internet

(ICONI 2019)

Dec. 15-18, 2019, Lotte Hotels & Resorts Hanoi, Vietnam

<http://www.iconi.org>

Proceedings of ICONI 2019

| Organized by |

Korean Society for Internet Information (KSII)

| Sponsored by |

Korea Electronics Technology Institute (KETI)

Contents



12-5	Recent Progress on Parallel Processing Techniques for Computational Engineering Minseong Kim, Woonchan Lee (Incheon National Univ., ROK), Moonseong Kim (Seoul Theological Univ., ROK), Jaeyoung Park (KIST, ROK)	364-365
12-6	Characteristics Analysis of Sodinokibi and GANDCRAB Young-Woong You, Ju-Seong Ko, Jin Kwak (Ajou Univ., ROK)	366-367
12-7	A Development of Digitalized Raw Materials Location by Connection of the Energy Monitoring System Hyunsuk Hwang, YoungWon Seo, Taeyeon Kim (New Communication Infotech Co., Ltd. ROK)	368-370
12-8	Blockchain-based value record preservation platform Minsung Son, Namgi Kim, Heeyoul Kim (Kyonggi Univ., ROK)	371-372
12-9	Study on IoT Service Server for Smart Contents Jiyong Lim, Sanghyun Park, Hyosang Lee, Hochul Kim, Amsuk Oh (Tongmyong Univ., ROK)	373-374
12-10	Ethernet Ring Protection Method for Fronthaul Links in 5G Cloud Radio Access Networks Muhammad Waqar, Ajung Kim (Sejong Univ., ROK)	375-378
12-11	Analysis of interval-based and fuzzy-based granular models based on knowledge-based rules Chan-Uk Yeom, Keun-Chang Kwak (Chosun Univ., ROK)	379-380
12-12	Integrating Structure of Multiple Levels using Meta Learning in Task Configuration Joo-Chang Kim, Sung-Soo Park (Kyonggi Univ., ROK), Roy C. Park (Sangji Univ., ROK), Namgi Kim, Kyungyong Chung (Kyonggi Univ., ROK)	381-383
12-13	Deep Learning Model Validation Method based on the Shared Memory in Distributed High Performance Computing Eun-Ji Lim, Shin-Young Ahn, Wan Choi (ETRI, ROK)	384-385
12-14	Development of early-childhood education platform for immersive interaction-based block play employing smart devices EUN HO KIM (Korea Institute of Industrial Technology, ROK)	386-387

Characteristics Analysis of Sodinokibi and GANDCRAB

Young-Woong You¹, Ju-Seong Ko² and Jin Kwak³

^{1,3}Department of Cyber Security, Ajou University
Suwon, South Korea

²ISAA Lab., Department of Computer Engineering, Ajou University
Suwon, South Korea

[e-mail: youngwoong2596@ajou.ac.kr, jsko.isaa@gmail.com, security@ajou.ac.kr]

*Corresponding author: Jin Kwak

Abstract

Recently, many users download and use digital content that is not allowed to be distributed without permission through the Internet. However, users are not aware that downloading such files could include malicious data, leading to several cases where many of their files are infected by malicious codes such as ransomware. The Sodinokibi, which had spread since April 2019, was an advance from the existing GANDCRAB and attacked by encrypting the victims' data and demanding the cost for the restoration. In this paper, for a prompt response to these ransomware attacks, we compare the dissemination, encryption, and operation of the two ransomware and describe the changes in the ransomware.

Keywords: Ransomware, Characteristic Analysis

1. Introduction

The size of the paid digital content market is expected to grow gradually[1]. However, about 30% of digital content users illegally download and use content[2], which causes many damages by the use of such illegal contents. Typically, there are cases where Sodinokibi Ransomware disguised as video downloader utility was distributed through phishing sites and others[3]. Various ransomware that was distributed with Sodinokibi caused damage[4]. Several studies have been conducted to counter this[5]. Therefore, in this paper, we would like to compare and analyze GANDCRAB and his variant, Sodinokibi, for the detection of new/modified ransomware. In this paper, each Ransomware is described in Chapter 2, compared and analyzed in Chapter 3, and finally concluded.

2. Related Works

2.1 Ransomware

Ransomware is malicious software that, along with its execution, requires costs to disable and restore a computer function[6].

2.2 GANDCRAB

GANDCRAB is a ransomware that has spread since January 2018. As shown in Fig. 1. below, The ransomware was distributed through e-mail, web servers, seized web pages, and malvertising and users' files were not available through encryption using various methods[7].

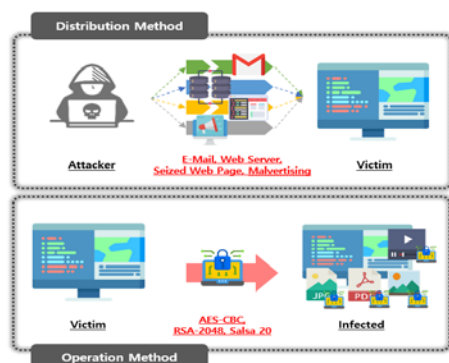


Fig. 1. Distribution and operation of GANDCRAB ransomware

2.3 Sodinokibi

Sodinokibi is a ransomware which first began to spread in April 2019, and is one of the ransomware that is currently causing a lot of damage at home and abroad. Also, the Ransomware infected PCs using managed services[8] through vulnerability attacks such as CVE, and the privilege escalation vulnerability attacks disabled and deleted anti-virus programs in the target environment to enable the attack to be carried out[9].

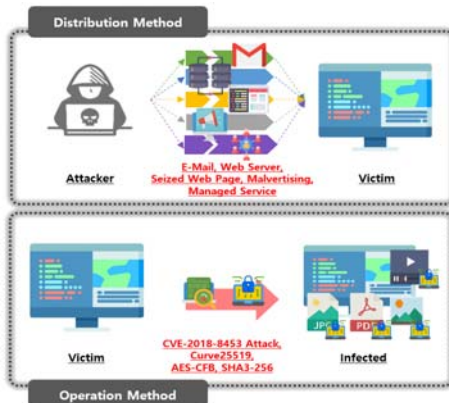


Fig. 2. Distribution and operation of Sodinokibi ransomware

3. Comparative Analysis

Table 1. specific features of each ransomware

	GANDCRAB	Sodinokibi
Dissemination	E-mail Web Server Web page Malvertising	E-mail Web Server Web page Malvertising Managed Service

Operation	File encryption	File encryption, CVE
Encryption	AES-CBC, RSA-2048, Salsa20	Curve25519, SHA3-256, AES-CFB

The characteristics between GANDCRAB and Sodinokibi can be seen in **Table 1** above. The above comparison shows that the distribution using the managed service, the vulnerability attack using CVE, the encryption using Curve25519, an asymmetric elliptic curve cipher was carried out.

4. Conclusions

In this paper, the characteristics of GANDCRAB and Sodinokibi and the methods of dissemination, operation, and encryption were compared and analyzed. This has led to changes in the process of the emergence of new ransomware.

In the future, we will research detection methods through the extraction of features of new/modified ransomware.

References

- [1] KOCCA, "Content Industry Closeout 2018 and Forecast Report for 2019," Jan. 2019.
- [2] KCOPA, "Investigation of illegal copying product recognition and content usage behavior," Feb. 2019.
- [3] Ahnlab, " Ransomware installed when caught in the video utility, Caution!," Sep. 2019.
- [4] Boannews, "Damage to Ransomware in 2018 is expected to be worth \$1.05 trillion.," Nov. 2018
- [5] D. Y. Huang, D.McCoy, M. M. Aliapoulos, V. G. Li, L. Invernizzi, E. Bursztein, K. McRoberts, J. Levin, K. Levchenko, and A. C. Snoeren, "Tracking Ransomware End-to-end," in *Proc. of IEEE Symposium on Security and Privacy*, pp. 618-631, May. 2018.
- [6] Gavin O'Gorman and Geoff McDonald, "Ransomware: A Growing Menace," Nov. 2012.
- [7] KISA, "Report on malicious code analysis of GANDCRAB ransomware," Feb 2019.
- [8] CA Technologies, "Introduction to Managed Services," Sep. 2012.
- [9] Kaspersky, "Sodin ransomware exploits Windows vulnerability and processor architecture," Jul. 2019.