논문 18-43-04-14 The Journal of Korean Institute of Communications and Information Sciences '18-04 Vol.43 No.04
https://doi.org/10.7840/kics.2018.43.4.715

최신 랜섬웨어 특징 분석

문 기 운◆, 이 종 혁°

Analysis of the Latest Ransomware Features

Kiwoon Moon◆, Jong-Hyouk Lee°

요 약

최근 들어 사용자의 파일 및 시스템을 암호화하고 사용자에게 금전적 피해를 입히는 악성코드인 랜섬웨어의 제작 및 유포가 폭발적으로 증가하고 있다. 최근 랜섬웨어들은 스팸메일에 악성 파일을 첨부하는 방식 뿐만 아니라 멀버타이징 기법을 사용하며, 사용자가 추가적인 행위를 하지 않더라도 인터넷에 연결되어 있다면 감염될 수 있는 형태로 발전하였다. 또한 암호화폐의 지갑정보를 탈취하거나 사용자의 시스템에 암호화폐 채굴 도구를 설치하여 암호화폐를 갈취하는 형태로 발전하고 있다. 본 논문에서는 국내에서 보고된 최신 랜섬웨어들을 분석하고 이들을 특징적 분류를 통해 분석한다. 또한 암호화폐의 출현에 따른 랜섬웨어의 변화 추세를 소개한다.

Key Words : Malware, Ransomware, Malvertising, Cryptocurrency

ABSTRACT

In recent years, the production and dissemination of ransomware, a malicious code that encrypts users' files and systems and causes financial harm to users, has increased explosively. Ransomware uses malvertising techniques as well as attaching malicious files to spam. In addition, if the victim's system is connected to the Internet, it can be infected. The latest ransomware has developed not only to steal cryptocurrency wallet information, but also to install cryptocurrency mining tools to illegally mine cryptocurrencies for attackers. In this paper, we analyze the latest ransomware reported in Korea and analyze them through characteristic classification. In addition, we present a new trend of ransomware with the advent of cryptocurrencies.

Ⅰ. 서 론

최근 몇 년 동안 피해자의 파일 및 시스템을 암호화하여 금전적인 요구를 하는 랜섬웨어의 제작 및 유포가 폭발적으로 증가하였다. 1989년의 PC Cyborg Trojan은 최초의 랜섬웨어로써 우편으로 송부된 디스켓의 랜섬웨어가 실행되면 대상 PC의 하드 디스크의 루트 디렉터리 정보를 암호화하였다. 공격자는 복호화의 조건으로 약 $189 - $378의 금액을 요구하였다[1]. 당시 배포 방식의 비효율성과 제한된 PC의 수로 인하여 널리 유포되지 않았다. 하지만 최근 랜섬웨어로 인한 피해가 급증한 배경으로는 IT기술의 발전과 디지털 자산의 가치의 증가를 예로 들 수 있다. 더불어 암호화폐인 비트코인의 등장으로 온라인상에서 추적이 불가능한 거래가 가능하다는 점이 있다[2]. 기존의 악성코드 제작자들은 해킹으로 취득한 정보들을 판매하는 방식을 취하였다. 하지만 비트코인의 거래 추적이 어렵다는 특성을 악용하여 피해자들의 파일 및 시스

※ 본 논문은 2017년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. NRF-2017R1A1A1A05001405)
◆ First Author : (ORCID:0000-0003-4364-8782)Dept. of Software, Sangmyung University, kiwoon@pel.smuc.ac.kr, 학생회원
° Corresponding Author : (ORCID:0000-0002-1753-1284)Dept. of Software, Sangmyung University, jonghyouk@pel.smuc.ac.kr, 종신회원
논문번호 : KICS2018-01-028, Received January 27, 2018; Revised March 22, 2018; Accepted April 18, 2018

템을 인질로 삼아 금전적인 요구를 하고 있다. 제작 시간 대비 고수익을 얻을 수 있는 장점으로 인하여 랜섬웨어의 공격은 계속적으로 증가하고 있다.

세계적으로 많은 피해를 일으키며 이슈화되고 있는 랜섬웨어는 몸값(Ransom)을 의미하는 단어와 소프트웨어(Software)의 합성어이다. 랜섬웨어는 악성코드의 한 종류이며, 여타 다른 악성코드와는 다르게 피해자의 시스템이나 파일들을 인질로 잡고 피해자들에게 금전적인 요구를 하는 악성 소프트웨어이다. 랜섬웨어는 백신을 통하여 치료를 수행하더라도 실제적으로 암호화된 데이터들은 복구하지 못하므로 공격자들은 피해자에게 직접적으로 금전적인 이득을 취할 수 있다. 랜섬웨어는 사회공학기법을 사용하거나 주요 기관을 사칭하여 시스템 자체를 잠그는 락커(Locker) 계열과 특정한 파일이나 전체 파일을 암호화하는 크립토(Crypto) 계열로 나뉠 수 있다[3]. 하지만 현재 배포되는 랜섬웨어들은 계열을 통한 구분이 모호해지고 있는 실정이다. 암호화폐의 가치가 증가하고 사용자들의 관심도가 높아짐에 따라 암호화폐를 대상으로 하는 악성코드들이 등장하였다. 이러한 악성코드의 행위들을 차용하여 랜섬웨어들은 점차 진화하고 있다.

본 논문의 2장에서는 랜섬웨어의 현황 및 피해 규모에 대하여 파악하고, 3장에서는 국내에서 유행한 주요 랜섬웨어들에 대하여 알아본다. 4장에서는 변종을 포함한 26개의 랜섬웨어들을 7가지 특징으로 분류하여 동향을 분석하고, 5장에서는 최신 랜섬웨어의 변화 추세에 대하여 소개한다. 마지막으로 6장에서 결론을 맺는다.

Ⅱ. 랜섬웨어의 현황 및 피해 규모

2.1 랜섬웨어의 현황

표 1과 같이 한국인터넷진흥원에 접수된 랜섬웨어 피해신고 현황에 따르면 2015년 770건에서 2016년 1,438건으로 86.8% 증가하였다. 2017년에 보고된 피해신고 건수는 5,825건으로써 전년 대비 305% 증가하였다[4]. 이와 같이 랜섬웨어의 피해는 지속적으로 늘어나는 추세이다.

표 2와 같이 한국인터넷진흥원에서 수집, 분석한

표 1. 랜섬웨어 피해 신고 현황
Table 1. Receipted ransomware damage complaints

	2015'	2016'	2017'
Complaints received	770	1,438	5,825

표 2. 악성코드 분석 통계
Table 2. Malware Analysis Statistics

Malware Type	Collection count	Rate
Ransomware	1,340	62.1%
Information Capture	336	15.6%
Remote Control	295	13.6%
Pharming	90	4.2%
Downloader	16	0.8%
Adware	15	0.7%
Injector	12	0.6%
DDoS	8	0.3%
etc.	46	2.1%
	2,158	100%

2017년 4분기의 악성코드 분석 통계에 따르면 가장 많이 확인된 악성코드 유형은 랜섬웨어로 나타났다. 수집된 2,158개의 악성코드 중 랜섬웨어는 1,340개로써, 그 비중이 62.1%를 차지하고 있다[4].

2.2 랜섬웨어 피해 규모

표 3은 국내 랜섬웨어 피해 규모를 나타낸다. 국내에서는 2015년도에는 약 53,000명이 감염되어 약 1,090억원의 피해를 입었으며, 약 30억원 정도의 금액이 해커에게 지급된 것으로 추정되었다. 2016년에는 약 13만명이 감염되었으며, 피해 금액으로는 약 3,000억원 정도의 피해가 발생하였다. 약 13만명의 피해자 중 13,000명이 약 100억원 이상의 비트코인을 지불한 것으로 추정되고 있다[3].

표 3. 랜섬웨어 피해 규모
Table 3. Damage scale of ransomware

	Number of damages caused by Ransomware	Amount of damage
2015	53,000	About 100 billion
2016	130,000	About 300 billion

Ⅲ. 주요 랜섬웨어

한국랜섬웨어침해대응센터에서 발행한 2017년 랜섬웨어 침해분석 보고서[3]에 따르면 2016년에 국내에서 유행한 랜섬웨어와 침해 비율은 다음 표 4와 같다.

2016년에는 Locky 랜섬웨어의 다양한 변종들이 등장 하였으며, 하반기에 등장한 신종 CERBER 랜섬웨

표 4. 랜섬웨어 감염 비율 (2016년)
Table 4. Ransomware Infection Ratio (2016')

Ransomware	Infection Ratio
CERBER(.random)	60.81
CERBER3	8.11
Locky(.thor)	6.61
Locky(.ordin)	6.46
Locky(.zepto)	5.71
Locky(.zzzzz)	3.00
Locky(.aesir)	3.00
CryptXXX	1.35
etc.	4.95

어의 공격이 확대되었다. Locky 랜섬웨어와 CERBER 랜섬웨어의 공격은 전체의 80%이상을 차지한다[3]. 또한 한국인터넷진흥원에서 발행한 2017년 1분기 사이버 위협 동향 보고서에 따르면 랜섬웨어와 관련한 공격들은 지속적으로 발생하였으며, CryptoSheld 변종, Sage와 같은 랜섬웨어들이 등장하였다고 보고하였다[5]. 본 장에서는 국내에서 널리 퍼진 랜섬웨어 8종에 대하여 자세히 알아본다.

3.1 CERBER 랜섬웨어

CERBER 랜섬웨어는 파일을 암호화한 후 음성으로 감염 사실을 알려주는 특징을 가지고 있다. 스팸메일이나 익스플로잇 킷(Exploit Toolkit)을 이용하여 유포되었다. 기존에는 DOC와 같은 확장자 파일을 통하여 배포되었지만 최근에는 VBS(Visual Basic Script), HTA(HTML Application)와 같은 확장자 파일로 구성되어 유포되는 사례가 발견되고 있다. CERBER 랜섬웨어는 대상 파일을 암호화 한 후 파일의 확장자를 .cerber로 바꾼다[6]. 버전에 따라 확장자명을 .cerber2, .cerber3와 같이 변경하기도 하며, 최근에 유포된 버전에서는 확장자명을 무작위로 변경하는 사례도 발견되고 있다. 최근에는 PC에서 접근이 가능한 모든 저장소(Cloud Drive, Local Disk, USB Drive, NetWork Drive)의 파일들을 암호화하는 형태로 발전하였다.

3.2 Locky 랜섬웨어

Locky 랜섬웨어는 파일들을 암호화 한 후 대상 파일의 확장자를 .locky로 바꾼다. 주로 악성 매크로가 포함된 워드 문서를 이메일에 첨부하여 유포한다[6]. 최근에는 JS파일로 위장하여 유포되는 경우도 보고되고 있다. 첨부 파일 실행 시 다운로드 되는 파일의 형태는 EXE 파일에서 DLL파일로 변경되었으며, DLL 파일의 확장자도 무작위로 바꾸어 다운로드하는 형태로 진화하였다[7]. 최근에 발견되는 Locky 랜섬웨어들은 웹사이트에 게시된 광고 배너를 통해서도 감염되는 사례가 보고되고 있다. 또한 바탕화면의 변조를 수행하지 않아 감염 초기에 쉽게 대응하지 못하도록 한다.

3.3 CryptXXX 랜섬웨어

CryptXXX 랜섬웨어는 국내 스마트폰 관련 커뮤니티에서 멀버타이징(Malvertising) 기법에 의한 광고 배너를 통하여 유포되었다. 멀버타이징은 악성코드(Malware)와 광고(Advertising)의 합성어로써 온라인 광고를 통해 악성코드를 유포시키는 행위를 말한다. 정상적인 온라인 광고 네트워크나 웹사이트에 악성코드가 탑재된 광고를 삽입하여 악성코드를 유포시킨다[8]. 또한 스팸 메일 뿐만 아니라 드라이브 바이 다운로드(Drive-by-download) 방식을 이용하여 유포되었으며, 메모리에서만 동작하는 DLL 파일을 생성하고 암호화를 수행하는 방식을 사용한다. 암호화 대상 파일 확장자에는 한글 워드 문서(.hwp)도 포함되어있다[6].

3.4 WannaCry 랜섬웨어

2017년 4월 해킹집단인 쉐도우브로커스(Shadow Brokers)는 미국 국가안보국(NSA, National Security Agency)가 이용한 해킹 도구들을 공개하였다. 공개된 취약점 중 하나인 Server Message Block(SMB) 취약점(MS17-010)은 Windows SMBv1 서버에 조작된 메시지를 전송하여 원격 코드 실행이 가능한 취약점이다. 해당 취약점을 활용하여 WannaCry 랜섬웨어가 제작되었다. WannaCry 랜섬웨어는 2017년 5월에 첫 감염 사례가 보고되었으며, 피해 규모는 전 세계 150개국, 20만대 이상의 PC를 감염시킨 것으로 추산되었다. 기존의 랜섬웨어는 사회공학기법을 활용하거나 취약한 웹사이트에서 다운로드받은 파일을 실행시킴으로써 감염되었다. 하지만 WannaCry 랜섬웨어는 네트워크를 통해 보안 패치가 이루어지지 않은 취약한 PC에 접근한 후, SMB 취약점(MS-010)을 이용하여 사용자가 별도의 악성코드 파일을 실행하지 않더라도 감염된다는 특징이 있다[9]. WannaCry 랜섬웨어는 감염 후 3일 이내의 기간에는 $300에 해당하는 비트코인을 요구하며, 7일이 경과하면 $600에 해당하는 비트코인을 요구하기도 한다.

3.5 PETYA 랜섬웨어

PETYA 랜섬웨어는 기존의 랜섬웨어와는 달리 MBR(Master Boot Record) 영역을 암호화한다. 시스템의 파티션 정보가 담겨 있는 MBR 영역과 윈도우의 NTFS(New Technology File System)에서 사용하는 파일에 관한 모든 정보(파일 크기, 작성 일자, 사용 권한, 데이터의 내용 등)가 담긴 MFT(Master File Table) 영역을 암호화하여 PC의 사용을 불가능하게 만든다.

2017년 6월에는 우크라이나에서 발전된 형태의 PETYA 랜섬웨어 감염 사례가 보고되었다. WannaCry 랜섬웨어와 마찬가지로 SMB 취약점을 악용하여 감염되는 형태이며, 네트워크 전파기능 또한 추가되었다. 최근 등장하고 있는 변종 랜섬웨어들은 MBR 영역의 암호화 뿐만 아니라 일부 특정 확장자 파일들을 암호화하기도 한다[10].

3.6 Erebus 랜섬웨어

Erebus는 2016년에 처음 발견되었다. Windows Event Viewer의 사용자 계정 제어(UAC)의 보안 기능을 우회하는 기법을 사용한다. UAC의 보안 기능을 우회하기 위하여 레지스트리를 수정하여 .msc 확장명에 대한 연결을 하이재킹하게 된다. 이후 상승된 Windows Event Viewer의 권한을 통하여 Erebus 랜섬웨어가 실행되어 암호화를 수행한다. Erebus 랜섬웨어에 감염되면 스스로 익명(Tor) 브라우저 클라이언트를 설치하고, 사용자의 홈 디렉토리를 대상으로 암호화를 수행한다.[11].

2017년 6월에는 국내의 인터넷호스팅 업체가 Erebus 랜섬웨어에 감염되는 사례가 보고되었다. 이 랜섬웨어는 Linux 운영체제를 대상으로 공격을 수행하는 변종 랜섬웨어로써, 해당 인터넷호스팅 업체에서 관리하는 153대의 Linux 서버를 대상으로 공격을 수행하였다. 그 결과 약 3000여개의 홈페이지가 마비되는 사태가 발생하였다. 이 업체의 대표는 복호화키를 전달받기 위하여 약 13억원에 해당하는 금액을 지불하기도 하였다[12].

3.7 Sage 랜섬웨어

Sage 랜섬웨어는 Sage 2.0이란 이름으로 2016년 처음 등장하였다. 기본적으로 이메일을 통하여 유포되는 형태를 가지고 있으며, 첨부되어 있는 파일을 실행하면 암호화 동작을 수행하는 파일을 자동으로 생성하여 암호화를 수행한다[13]. 또한 발전된 형태의 Sage 랜섬웨어는 익스플로잇 킷을 사용하여 유포하는 형태로 발전하였다. 피해자가 데이터를 암호화하기 이전 시점으로 되돌리는 것을 막기 위하여 기존에 생성된 볼륨 섀도 카피를 모두 삭제한다. 기존과 다르게 발전된 형태의 Sage 2.2는 금전적인 요구와 감염 사실을 알리는 안내문에 한국어를 추가하고, 암호화 대상파일에 한글 워드 문서(.hwp)를 추가하여 국내 사용자를 노리고 있다는 사실을 알 수 있다[14].

3.8 CryptoShield 랜섬웨어

CryptoShield 랜섬웨어는 주로 멀버타이징 기법을 사용하여 유포되는 형태를 가지고 있다. 익스플로잇 킷을 사용하여 웹사이트 상의 광고 배너에 악의적인 자바스크립트 코드를 삽입하고, 해당 웹사이트를 방문한 사용자의 PC 환경에 삽입된 자바스크립트 코드를 이용하여 CryptoShield 랜섬웨어를 다운로드하고 실행하는 형태를 가진다. CryptoShield 랜섬웨어는 영어 알파벳을 13글자씩 밀어내는 방식으로 문자들을 치환하는 ROT13 방식[15]을 사용하여 원본 파일 명을 변조한 뒤, 원본 파일의 확장자를 .CRYPTOSHIELD로 변경한다. 또한 사용자 PC의 볼륨 섀도 카피를 삭제하여 암호화 이전 상태로 복구하는 것을 방지한다[16].

Ⅳ. 주요 랜섬웨어의 특징

이 장에서는 국내에서 유행한 랜섬웨어들을 아래 표 5와 같이 총 27개의 랜섬웨어를 선정하였다. 선정된 랜섬웨어를 대상으로 다음과 같이 7가지 특징으로 분류하여 최신 동향을 파악한다.

4.1 유입 방식

국내에서 유행한 랜섬웨어들의 주로 스팸메일을 통하여 유포되고 있다. 최근에 발견되는 발전된 형태의 랜섬웨어들은 취약한 웹사이트나 광고 모듈을 악용하는 멀버타이징 방식을 사용하기도 한다. 멀버타이징 기법을 악용하는 공격자는 우선적으로 보안이 취약한 광고 서버를 해킹하여 온라인 광고에 악성코드를 삽입한다. 이 방식은 취약한 응용 프로그램(웹브라우저, 플래시 플레이어, Java 등)을 사용하는 사용자가 해당 웹사이트를 방문할 경우 사전에 삽입된 악성코드를 통하여 랜섬웨어 파일을 다운로드하여 유포하는 방식이다. 멀버타이징 기법을 통하여 공격자들은 불특정 다수를 대상으로 랜섬웨어를 감염시킬 수 있다. 또한 유포지를 찾거나 차단하기도 어렵다는 특성으로 인하여 멀버타이징 기법에 의한 감염 사례가 늘어나고 있다. 더불어 2017년 SMB 취약점을 이용하여 제작된

표 5. 랜섬웨어의 특징적 분류
Table 5. Characteristic Classification of Ransomware

Ransomware	Inflow Method	Spread Time	Target OS	File extension of Attack target	Encryption algorithm	File extensions created after encryption	Payment request amount (BTC)
Locky	Spam	2016. 2	Windows	About 100 (.hwp)	AES-128, RSA-2048	.locky	0.5~5.1
Locky(.zepto)		2016. 6		About 350 (.hwp)		.zepto	2.0~3.0
Locky(.odin)		2016. 9				.odin	2.5~3.0
Locky(.shit)		2016. 10				.shit	0.8
Locky(.thor)		2016. 10				.thor	0.8~3.0
Locky(.aesir)		2016. 11				.aesir	3.0
Locky(.zzzzz)		2016. 11				.zzzzz	3.0
Locky(.osiris)		2016.12, 2017. 4				.osiris	2.5~3.0
Locky(.loptr)	Spam, Malvertising	2017. 5		About 400 (.hwp)		.loptr	0.5
Locky(.diablo6)		2017. 8				.diablo6	0.5
Locky(.lukitus)		2017. 8				.lukitus	0.5
CERBER		2016. 3		About 450		.cerber	1.1~1.25
CERBER2		2016. 8				.cerber2	0.7~1.2
CERBER3		2016. 9				.cerber3	1.0
CERBER4		2016. 9				Random	1.0
CERBER5		2016. 11				Random	0.7~1.0
CERBER6		2016. 12				Random	0.25
CryptXXX2.0		2016. 5		About 200 (.hwp)	RSA modify	.crypt .crypt1	1.2
CryptXXX3.0		2016. 5		About 200 (.hwp)	RSA modify	Random	1~1.5
PETYA	Spam	2016. 4		MBR modulation	SALSA20	-	2.0
NotPETYA (2017)	Using SMB Vulnerabilities	2017. 6		MBR modulation	AES-128, RSA-2048	-	$ 300
WannaCry		2017. 6		About 175 (.hwp 포함)	AES-128, RSA-2048	.WNCRY	$ 300
Erebus	APT	2017. 6	Linux	About 430	AES-256, RSA-2048	.ecrypt	5.4~10.8
Sage 2.0	Spam, Malvertising	2016. 12	Windows	About 400	chacha20	.sage	3.22
Sage 2.2		2017. 2		About 400	chacha20	.sage	$ 2000
CryptoShield		2017. 1		About 450	AES-256, RSA-2048, ROT-13	.cryptoshield	0.5~2.0
CryptoShield 2.0		2017. 3		About 1200		.cryptoshield	0.5~2.0

WannaCry 랜섬웨어와 PETYA 랜섬웨어의 경우 인터넷이 연결되어 있는 상태에서 피해자가 별도의 악성 파일을 실행하지 않더라도 감염된다는 특징을 나타낸다.

4.2 유입 시기

Locky 랜섬웨어는 2016년 2월 처음 국내에 등장한 이후 다양한 변종 랜섬웨어들이 유행하였다. Locky(.osiris)의 경우 2016년 12월 등장 후, 2017년

4월에 재유포 되기도 하였으며, 2017년 상반기에는 멀버타이징 기법을 사용한 Locky(.loptr), Locky (.diablo6), Locky(.lukitus)와 같은 변종들이 등장하였다. CERBER는 2016년 3월 처음 등장하여 2016년 하반기까지 다양한 변종들이 출현하여 CERBER6 버전까지 등장하였다. 2017년 5월 해킹집단인 쉐도우브로커스(Shadow Brokers)에 의하여 SMB 취약점을 이용한 해킹 도구들을 공개된 후, 동일한 취약점을 사용하여 공격을 수행하는 WannaCry, NotPETYA와 같은 랜섬웨어들이 등장하였다. 2015년 6월에는 국내 인터넷 호스팅 업체의 Linux 서버를 대상으로 공격을 수행한 Erebus 랜섬웨어가 등장하였다. 2017년 상반기에는 기존에 유행했던 랜섬웨어의 변종인 Sage 2.2, CryptoShield 2.0가 국내에 등장하여 지속적으로 공격을 수행하고 있다.

4.3 공격 대상 운영체제

국내에서 유행한 랜섬웨어들은 대부분 Windows 운영체제를 대상으로 제작되고 있다. 2017년 발견된 Erebus 랜섬웨어의 경우 Linux 운영체제를 대상으로 제작되었다. 2017년 5월에 WannaCry 랜섬웨어가 발견된 이후, 모바일 환경을 대상으로 한 WannaCry 랜섬웨어의 변종이 중국에서 발견되기도 하였다. 랜섬웨어 제작자들은 특정 운영체제에 국한되지 않고 공격을 수행할 수 있으며, 주요 기반 시설이나 IoT환경을 대상으로 한 랜섬웨어들도 제작될 우려가 있다.

4.4 공격 대상 파일 확장자

국내에서 유행한 랜섬웨어들은 100~450여개의 확장자를 대상으로 암호화를 수행한다. 2017년 3월 등장한 CryptoShield 2.0는 약 1200여개의 확장자를 대상으로 암호화를 수행한다. Locky 랜섬웨어, CryptXXX 랜섬웨어, WannaCry 랜섬웨어는 대상 파일 확장자에 한글 워드 문서(.hwp)를 포함하고 있는 것으로 보아 우리나라를 직접적인 타겟으로 삼고 있다는 것을 확인할 수 있다.

4.5 사용 암호화 알고리즘

국내에서 발견된 랜섬웨어들은 주로 AES 알고리즘과 RSA 알고리즘을 사용한다. 최근에 발견되는 랜섬웨어들은 AES-256, RSA-2048과 같은 보다 강력한 알고리즘을 채택하고 있다. 또한 ROT13, SALSA20와 같은 부수적인 알고리즘[17]을 사용하여, MFT에 대한 암호화를 수행하거나 파일명에 대한 암호화를 수행하기도 한다. Sage 랜섬웨어의 경우 기존의 랜섬웨어들과는 다르게 파일 암호화 및 통신데이터 암호화를 수행하기 위하여 chacha20 알고리즘[18]을 사용한다.

4.6 암호화 후 생성된 파일 확장자

랜섬웨어들은 암호화 후 변조되는 파일 확장자에 따라 그 이름이 명명되는 경우가 많다. 예를 들어 CERBER 랜섬웨어의 경우 대상 파일을 암호화한 후 .cerber의 확장자를 부여한다. Locky 랜섬웨어의 경우 북유럽 신화 속에 등장하는 신들의 이름을 사용하는 특징을 가지기도 한다. 하지만 최근에 발견되는 랜섬웨어들의 경우 원본 파일의 확장자를 무작위로 변조한다.

4.7 요구 금액

2008년 나카모토 사토시(Nakamoto Satoshi)라는 필명을 사용하는 사용자 혹은 단체에 의해 비트코인이라는 암호화폐가 등장하였다. 블록체인 기술을 이용해 이전 암호화폐들이 해결하지 못한 이중지불 문제를 해결한 비트코인은 중앙 서버의 개입 없이 개인 간 거래를 가능케 한다[19]. 임의의 공개키를 활용해 거래 주소를 생성하기 때문에 거래 당사자에 대한 정보와 직접적인 상관관계를 분석하기 쉽지 않다. 이러한 특징을 악용하여 랜섬웨어 제작자들은 피해자들에게 비트코인을 요구하고 있다. 요구 금액은 랜섬웨어 제작자가 대상 폴더마다 남겨놓은 텍스트 파일을 열어 그 안에 적혀 있는 주소로 접속하면 확인할 수 있다. 특정 랜섬웨어들은 특정 시간이 지나면 요구 금액을 높이는 수법을 사용하기도 한다. 국내에서 널리 퍼진 랜섬웨어들은 0.5 BTC~10.8 BTC를 요구하고 있다[20]. 2017년 1월에 이르러 비트코인은 1BTC당 약 1,300만원 이상에 거래되고 있으며[21], 비트코인의 가치가 증가함에 따라 랜섬웨어 제작자들의 공격은 더욱 증가할 것으로 예상된다.

Ⅴ. 랜섬웨어의 발전 추세

최근 들어 다양한 암호화폐들이 등장하였다. 그에 따라 최근의 악성코드들은 암호화폐를 대상으로 하는 공격들을 수행하고 있다. 2017년 하반기에는 피해자들의 PC 자원을 이용해 암호화폐를 채굴하는 채굴형 악성코드의 유포가 증가하였다. 대표적으로 Digmine과 KJU와 같은 악성코드들이 채굴형 악성코드에 해당한다[22,23]. 또한 암호화폐 채굴형 악성코드와는 다르게 암호화폐의 지갑정보를 탈취하는 지갑 탈취형

악성코드도 등장하였다. 대표적으로 KimChenIn과 Cyptoshuffler는 피해자가 암호화폐를 송금하기 위하여 수신자의 지갑주소를 입력할 때, 해당 주소를 공격자 자신의 지갑주소로 바꿔치기한다[24,25]. 이때 공격자는 약 1만개의 지갑주소를 악성코드에 심어 놓았으며, 피해자가 입력하는 송신자의 지갑주소와 가장 유사한 것을 선택하여 바꿔치기한다. 결과적으로 피해자가 송금하는 암호화폐는 공격자에게 전달된다.

이러한 암호화폐를 대상으로 하는 악성코드가 등장함에 따라 랜섬웨어들도 진화하고 있다. VenusLocker 랜섬웨어는 기존의 랜섬웨어의 행위와 더불어 모네로 코인의 채굴 도구를 피해자의 PC 환경에 설치하고 암호화폐를 채굴하여 공격자에게 전송하는 행위가 추가되었다[26]. 또한 Cerber 랜섬웨어는 기존의 랜섬웨어의 행위 뿐만 아니라 암호화폐의 지갑정보를 탈취한 후, 피해자의 암호화폐를 갈취한다[27].

스프라이트 코인은 암호화폐를 가장한 랜섬웨어이다. 암호화폐와 관련된 커뮤니티나 포럼 등에 자신들의 코인의 우수성을 홍보하여 홈페이지 접속을 유도하고, 악성 스프라이트 코인 도구를 설치하도록 한다. 피해자가 악성코드가 탑재된 도구를 실행하면 암호화를 진행한다. 스프라이트 코인은 암호화 뿐만 아니라 피해자의 크롬과 파이어폭스의 보안 크리덴셜까지 수집한다. 수집된 정보들은 익명(Tor) 네트워크를 통하여 공격자에게 전송된다[28]. 이와 같이 암호화폐의 종류가 다양해지고 사용자들의 관심도가 높아짐에 따라 랜섬웨어는 지속적으로 발전하고 있다.

Ⅵ. 결 론

최근 들어 사용자의 파일 및 시스템을 암호화하여 피해자에게 금전적인 피해를 입히는 랜섬웨어의 현황 및 국내외 피해 규모를 알아보고, 주요 랜섬웨어를 소개하였다. 또한 최신 랜섬웨어를 특징에 따라 분류하여 동향을 분석하였다.

기존 랜섬웨어들은 스팸메일에 악성 파일을 첨부하는 방식을 주로 이용했지만, 최근에는 취약한 응용 프로그램을 사용하는 사용자가 해당 웹사이트를 방문할 경우에도 감염되는 형태의 멀버타이징 기법을 사용하는 형태로 발전하였으며, WannaCry와 NotPETYA와 같이 인터넷이 연결되어 있는 상태에서 피해자가 별도의 악성 파일을 실행하지 않더라도 감염되는 랜섬웨어들도 등장하였다. 대부분의 Windows 운영체제를 대상으로 공격을 수행하고 있지만 최근에는 Linux 운영체제와 모바일 환경을 대상으로 하는 랜섬웨어도 등장하였다. 향후 등장할 랜섬웨어들은 특정 운영체제 환경에 국한되지 않고, 주요 기반 시설이나 IoT 환경을 대상으로 제작될 우려가 있다. 변종 랜섬웨어들은 공격 대상 파일의 확장자 수를 증가시키고 있으며, 많게는 1200여개의 파일 확장자를 대상으로 공격을 수행하기도 한다. 또한 한글 워드 문서(.hwp)를 공격 대상으로 포함하고 있는 것으로 보아 우리나라를 주요한 공격 대상으로 삼고 있다는 것을 알 수 있다.

암호화폐의 대중화에 따라 최근 들어 주요 랜섬웨어들은 사용자로 하여금 지불방법으로 암호화폐를(예를 들어, 0.5 BTC ~ 10.8 BTC를 요구)채택하고 있다. 암호화폐 종류가 다양해지고 사용자의 관심이 증가함에 따라 암호화폐의 지갑정보를 탈취하거나 암호화폐의 채굴 도구를 직접 설치하여 암호화폐 자체를 채굴하는 행위를 수행하고 있기도 한다.

사용자들은 랜섬웨어로 부터 피해를 예방하기 위하여 중요한 자료는 백업하여 데이터를 보존하며, 바이러스 백신 소프트웨어 및 애플리케이션의 최신 보안 패치를 업데이트하여 유지하여야한다. 또한 출처가 불분명한 이메일과 URL 링크를 실행하는 것을 지양해야한다.

References

[1] *MONTHLY SECURITY NEWS LETTERS*, Jinhyun Security Group, Apr. 2016.

[2] JiranSecurity hompage, Retrieved Aug. 2016, http://mi.jiransecurity.com/589

[3] *2017 Ramsomware Infringement Analysis Report*, RanCERT, February 2017

[4] *Cyber Threat Trend Report for the fourth quarter of 2017*, KISA, Jan. 2018.

[5] *Cyber Threat Trend Report for the first quarter of 2017*, KISA, Apr. 2017.

[6] *Latest Ransomware Trend Analysis Report*, AhnLab, Feb. 2017.

[7] *ASEC REPORT VOL.80*, AhnLab, Aug. 2016.

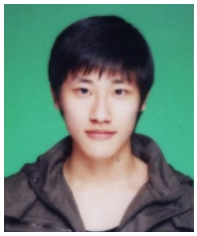
[8] *Security Guide for Distributing Malicious Code with Online Advertising Banner*, KISA, Oct. 2016.

[9] *WannaCry Ransomware Analysis Propagated to Windows SMB Vulnerabilities*, RedAlert, May 2017.

[10] *Petya Ransomware v0.3*, ThaiCERT, Jun. 2017.

[11] *SECURITY MAGAZINE*, ViRobot, Mar. 2017.
[12] ZDNet Korea, Retrieved Jul. 2017, from http://www.zdnet.co.kr/news/news_view.asp?artice_id=20170613100723
[13] *INCA Internet Official Blog*(2017), Retrieved July 2017, from http://erteam.nprotect.com/927
[14] *INCA Internet Official Blog*(2017), Retrieved July 2017, from http://erteam.nprotect.com/1085
[15] C. Swenson, *Modern Cryptanalysis: Techniques for Advanced Code Breaking*, John Wiley&Sons, Mar. 2008.
[16] RenCERT hompage(2017), Retrieved July 2017, from https://www.rancert.com/bbs/bbs.php?bbs_id=case&mode=view&id=64
[17] Daniel J. Bernstein, *Salsa20 design*, Apr. 2005.
[18] Daniel J. Bernstein, "*ChaCha, a variant of Salsa20*," January 2008
[19] B. Lee, Y.-J. Lim, and J.-H. Lee, "Consensus algorithms in blockchain platforms," in *KICS Winter Conf.*, pp. 386-387, Jeongseon, Korea, Jan. 2017.
[20] RenCERT hompage(2016), Retrieved Jul. 2017, from https://www.rancert.com/bbs/bbs.php?mode=view&id=35&bbs_id=case&page=1&part=&keyword=
[21] Chosun Biz hompage, Retrieved Jan. 2018, from http://biz.chosun.com/site/data/html_dir/2018/01/26/2018012601093.html
[22] TrendLabs Security Intelligence Blog, Retrieved January 2018, from https://blog.trendmicro.com/trendlabs-security-intelligence/digmine-cryptocurrency-miner-spreading-via-facebook-messenger/
[23] Anlab Official hompage, Retrieved January 2018, from http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=27098
[24] HAURI Official hompage, Retrieved January 2018, from https://www.hauri.co.kr/security/issue_view.html?intSeq=277&page=6&article_num=218
[25] CoinWire hompage, Retrieved January 2018, from https://www.coinwire.com/be-all-ears-cryptoshuffler-trojan-quietly-alters-wallet-address
[26] Security News hompage, Retrieved January 2018, from http://www.boannews.com/media/view.asp?idx=65688&kind=1&search=title&find=%BA%F1%B3%CA%BD%BA%B6%F4%C4%BF
[27] Trend Micro hompage, Retrieved January 2018, from https://blog.trendmicro.com/trendlabs-security-intelligence/cerber-ransomware-evolves-now-steals-bitcoin-wallets/
[28] FORTINET hompage, Retrieved January 2018, from https://blog.fortinet.com/2018/01/22/spritecoin-another-new-cryptocurrency-or-not

문 기 운 (Kiwoon Moon)



2016년 2월 : 상명대학교 컴퓨터소프트웨어공학과 졸업
2016년 3월~현재 : 상명대학교 소프트웨어학과 석사과정
<관심분야> 네트워크 보안, 악성코드 분석

이 종 혁 (Jong-Hyouk Lee)

2010년 2월 : 성균관대학교 공학박사
2009년 6월~2012년 2월 : 프랑스 INRIA 연구원
2012년 3월~2013년 8월 : 프랑스 그랑제꼴 TELECOM Bretagne 조교수
2013년 9월~현재 : 상명대학교 소프트웨어학과 조교수
<관심분야> 프로토콜 분석, 익스플로잇 개발, 보안