JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 21, No. 8 : 1581~1588 Aug. 2017

랜섬웨어 분석 및 탐지패턴 자동화 모델에 관한 연구

이후기[1] · 성종혁[2] · 김유천[3] · 김종배[4] · 김광용[5*]

The Automation Model of Ransomware Analysis and Detection Pattern

Hoo-Ki Lee[1] · Jong-Hyuk Seong[2] · Yu-Cheon Kim[3] · Jong-Bae Kim[4] · Gwang-Yong Gim[5*]

[1]Department of IT Policy and Management, Soongsil University, Seoul 06978, Korea
[2]Department of Information Security Systems, Kyonggi University, Seoul 03746, Korea
[3]Department of Information Security, Dongguk University, Seoul, 04620, Korea
[4]Professor, Graduate School of Software, Soongsil University, Seoul, 06978, Korea
[5*]Professor, Dept. of Business Administration, Soongsil University, Seoul, 06978, Korea

요 약

최근 광범위하게 유포되고 있는 랜섬웨어는 단순 파일 암호화 후 금전을 요구하는 기존 방식의 공격에서 벗어나 신·변종 유포, 사회공학적 공격 방법을 이용한 표적형 유포, 광고 서버를 해킹해 랜섬웨어를 대량으로 유포하는 멀버타이징 형태의 유포, RaaS 등을 통해 더욱 고도화, 지능화되고 있다. 특히, 보안솔루션을 우회하거나 파일암호화를 통해 파라미터 확인을 불가능하게 하고, APT 공격을 접목한 타겟형 랜섬웨어 공격 등으로 공격자에 대한 추적을 어렵게 하고 있다. 이와 같은 랜섬웨어의 위협에서 벗어나기 위해 다양한 탐지기법이 개발되고 있지만 새롭게 출몰하는 랜섬웨어에 대응하기에는 힘든 상황이다. 이에 본 논문에서는 시그니처 기반의 탐지 패턴 제작 및 그 문제점에 대해 알아보고, 랜섬웨어에 보다 더 능동적으로 대처하기 위해 일련의 과정을 자동으로 진행하는 랜섬웨어 감염 탐지 패턴 자동화 모델을 제시한다. 본 모델은 기업이나 공공 보안관제센터에서 다양한 응용이 가능할 것으로 기대된다.

ABSTRACT

Recently, circulating ransomware is becoming intelligent and sophisticated through a spreading new viruses and variants, targeted spreading using social engineering attack, malvertising that circulate a large quantity of ransomware by hacking advertising server, or RaaS(Ransomware-as-a- Service), from the existing attack way that encrypt the files and demand money. In particular, it makes it difficult to track down attackers by bypassing security solutions, disabling parameter checking via file encryption, and attacking target-based ransomware with APT(Advanced Persistent Threat) attacks. For remove the threat of ransomware, various detection techniques are developed, but, it is very hard to respond to new and varietal ransomware. Accordingly, in this paper, find out a making Signature-based Detection Patterns and problems, and present a pattern automation model of ransomware detecting for responding to ransomware more actively. This study is expected to be applicable to various forms in enterprise or public security control center.

키워드 : 랜섬웨어, 멀버타이징, 서비스 형태의 랜섬웨어, 시그니처 기반 탐지, 패턴 자동화

Key word : Ransomware, Malvertising, RaaS, Signature-based Detection, Pattern Automation

Received 14 April 2017, **Revised** 25 April 2017, **Accepted** 19 May 2017

* **Corresponding Author** Gwang-Yong Gim(E-mail:gygim@ssu.ac.kr, Tel:+82-2-828-7071)
Dept. of Business Administration, Soongsil University, Seoul 06978, Korea

Open Access https://doi.org/10.6109/jkiice.2017.21.8.1581 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

2016년 한해 뉴스 등 언론을 통해 가장 많이 등장한 보안용어는 바로 '랜섬웨어(Ransomware)'일 것이다. 랜섬웨어는 이용자의 데이터(시스템파일, 문서, 이미지 등)를 암호화하는 악성코드로, 몸값(Ransom)과 소프트웨어(Software)의 합성어로, 시스템을 잠그거나 데이터를 암호화해 사용할 수 없도록 한 뒤 이를 인질로 삼아 금전을 요구하는 악성 프로그램을 말한다[1]. 원래 랜섬웨어는 미국을 중심으로 활동하는 악성코드였으나 컴퓨터 및 사용자 증가를 통해 전 세계적으로 급속하게 유포되었으며 2015년 4월에는 국내에서도 출현하게 되었다[2].

2016년 랜섬웨어의 동향을 살펴보면 기존의 단순 파일 암호화 후 금전을 요구하는 방식에서 벗어나 변화와 소멸을 거듭하며 결과적으로 진화하는 양상을 보인다. 2015년 악명을 떨쳤던 테슬라크립트(TeslaCrypt)나 크립트XXX(CryptXXX)의 경우 2016년 7월 이후 잠잠해진 반면, 스팸메일을 통해 유포되는 록키(Locky)나 음성으로 감염사실을 알려주는 케르베르(Cerber)가 절반이상을 차지하였으며[3], 파일뿐만 아니라 MBR (Master Boot Record)까지 암호화해 PC 사용 자체를 방해하는 랜섬웨어도 등장했다.

보안 솔루션 전문 기업인 소닉월에 따르면, 그림 1과 같이 2016년 랜섬웨어는 전년대비 167배 증가하였으며, 이를 통해 악성이메일공격 및 익스플로잇 킷의 페이로드로 활용되고 있다. 랜섬웨어 공격은 2015년 380만건에서 2016년 6억3800만건으로 폭발적으로 증가하였으며, 특히 4분기에는 2억6650만건을 기록하였다. 특히 서비스형 랜섬웨어(ransomware-as-a-Service, RaaS)의 등장과 함께 랜섬웨어는 쉽게 접근할 수 있고 저렴하며 배포가 편리하고 적발 시 상대적으로 낮은 처벌을 받는다는 인식을 바탕으로 급성장하였다[4].

한편, 그림 2와 같이 전 세계적으로 가장 기승을 떨친 랜섬웨어 종류로는 록키가 5억건 이상으로 가장 많이 유포되었다. 또한 악성링크에 연관된 대표적인 키워드들은 랜섬웨어, 드라이브 바이 다운로드, 앵글러, Cerber, Locky, 카이신, 파밍, Flash 등으로 랜섬웨어와 관련된 키워드들이 가장 많았다[5].

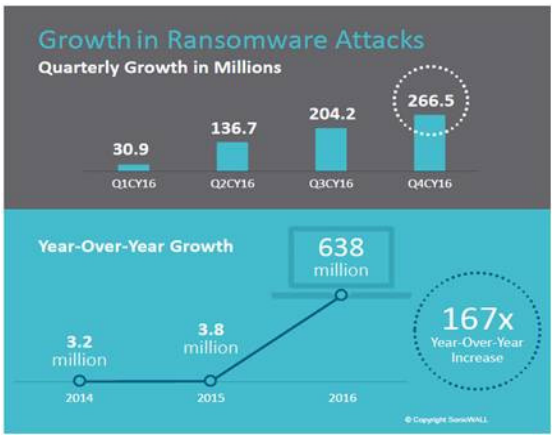


Fig. 1 Growth in Ransomware(SonicWall)

국내에서도 랜섬웨어에 대한 피해사례는 기하급수적으로 증가하였다. 한국랜섬웨어침해대응센터에 의하면 2016년 랜섬웨어 피해자는 13만명, 피해규모는 3000억원에 달한 것으로 집계되어진다. 이는 2015년 피해자 5만3000명, 피해 규모 1090억원과 비교해 약 3배 가량 증가한 수치다. 2016년 상반기에는 위장이메일 방식으로 새롭게 등장하여 수천개의 기업과 공공기관을 공격한 록키가 가장 큰 피해를 입혔고, 하반기에는 록키 변종과 신종 케르베르 공격이 확대되어 전체 피해의 80%를 차지하였다[6].

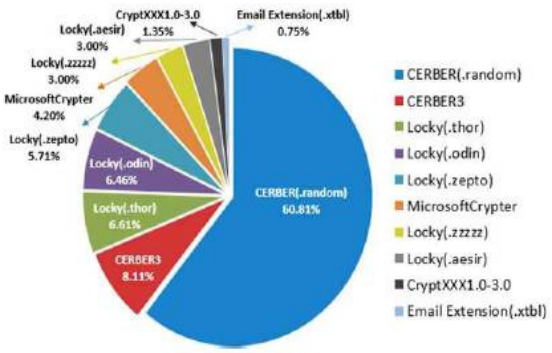


Fig. 2 Types of Ransomware(SonicWall)

또한 한국인터넷진흥원에서 접수한 랜섬웨어 피해신고 현황을 살펴보면 표 1과 같이, 2015년 770건에서 2016년 1,438건으로 전년대비 86.8% 증가한 것을 확인할 수 있다.

Table. 1 '15-'16 Ransomware Damage Complaint Receipt Statistics(KISA)

Division	2015					2016				
Number of Complaints	Q1	Q2	Q3	Q4	Total	Q1	Q2	Q3	Q4	Total
	0	127	58	585	770	176	353	197	712	1,438

랜섬웨어의 종류별 비율도 상반기에는 록키 랜섬웨어가 높은 비율(79%)을 보였으나, 하반기에는 케르베르 랜섬웨어가 높은 비율(52%)로 유포되었음이 확인되었다. 하반기에 케르베르 랜섬웨어가 증가한 것은 서비스형 랜섬웨어의 대표적인 예로 지속적인 업데이트를 통해 지속 관리되고 있기 때문인 것으로 추정된다[7].

이와 같이 2016년 한해는 랜섬웨어에 대한 위협이 매우 심각한 수준으로 발전하였다. 비트코인을 이용하여 공격자의 추적을 불가능하게 하거나, Drive-By-Download 방식을 통해 사이트에 접속만 해도 감염이 되는 형태를 취하고 있으며[8, 9], 현재까지 적절한 치료방법이나 대응책이 없어 감염이 되면 돈을 지불하거나 해당 시스템을 포맷 후 재사용을 하여야 하는 상황이며 돈을 지불하여도 복호화에 대한 보장도 없는 상태이다.

감염되었을 시 막대한 피해를 유발하는 랜섬웨어에 대한 탐지에 현재까지는 시그니처 기반 탐지 기법이 적용되고 있다. 그러나, 이 기법은 신·변종 랜섬웨어에 대한 대응이 어렵고, 분석가에 따른 차이로 시스템 성능 저하 및 오탐을 야기할 수 있다는 단점이 있다. 이에 본 연구에서는 이를 개선한 탐지 패턴의 자동화 모델을 제시하고자 한다.

Ⅱ. 본 론

2.1. 랜섬웨어 유포방식

2016년 나타난 랜섬웨어 유포방식은 먼저 사회공학적 공격 방법을 이용한 표적형 스팸메일을 통한 랜섬웨어 유포 및 광고 서버를 해킹해 랜섬웨어를 대량으로 유포하는 멀버타이징(Malvertising) 형태의 랜섬웨어 유포 사례가 대량 발견되었다. 주로 홈페이지 취약점을 악용하거나, 파일공유 사이트를 통해 유포되던 기존 방식에서 한 단계 진화한 모습이다. 특히 랜섬웨어 악성코드 분석을 지연시키거나 백신 등 보안솔루션 우회를 위한 지능화 방법이 적용되고 있다. 예를 들면, 스크립트 및 PE(Program Execution) 파일 암호화를 통해 특정 파라미터 확인 불가 유도, 네트워크 연결 없이 파일을 암호화하여 분석 근거 확보 불가 유도 등 분석 방해 기법을 적용하고 있다. 또한, Tor 네트워크와 비트코인을 이용하고 있어 공격자에 대한 추적이 어렵다는 한계를 악용하고 있다[7].

랜섬웨어 공격 그룹이 체계적으로 분업을 시작한 것도 2016년 특징 중의 하나이다. 랜섬웨어 공격 그룹은 크게 개발자와 유포자로 구분되는데, 유포자가 전면에 나서고 개발자는 노출을 최소화 하는 구조로 운영된다. 수익 분배는 통상 개발자 40%, 유포자 60%의 비율로 이뤄진다고 알려져 있다.

취약점을 이용한 악성코드를 대량으로 유포하는 툴인 익스플로잇킷(Exploit Kit)을 제작/판매하는 랜섬웨어 암시장이 활성화되면서 랜섬웨어 유포는 더욱 활개를 치고 있다. 이와 함께 익스플로잇킷의 치열한 경쟁과 지각 변동이 나타났다.

특히 한글을 이용한 국내 타겟형 랜섬웨어도 발견되고 있다[2]. 이와 같은 랜섬웨어는 주로 러시아와 그 주변국에서 개발되었고, 유포는 중국에서 이루어졌을 것으로 추정된다. 설문지 문서파일로 위장한 국내 맞춤형 랜섬웨어인 '비너스락커'의 경우 기존 버전에 없었던 '.hwp' 확장자를 갖는 한글문서들을 암호화하는 것으로 알려져 있다[10, 11].

2.2. 랜섬웨어 향후 전망

2016년 한 해 동안 가파른 성장세를 보였던 랜섬웨어는 공격자 관점에서 즉각적으로 금전적 이득을 취할 수 있는 유용한 범죄 수단으로 자리 잡았다. 특히 기업의 경우, 비즈니스 중단이나 고객 정보와 같은 중요 데이터를 잃을 수 있다는 부담 때문에 결국 몸값(ransom)을 지불하는 사례가 적지 않다. 여기에 랜섬웨어 제작 및 유포의 서비스화(RaaS) 등 랜섬웨어 자체가 수요자와 공급자가 유기적으로 활동하는 하나의 시장을 형성[7, 12]하기에 이르러, 랜섬웨어의 위협은 더욱 고도화되고 공격범위도 확장되고 있다.

2016년 하반기 크게 확산되었던 RaaS를 이용한 랜섬웨어 공격과 Exploit Kit을 이용한 공격도 더욱 증가되리라 예상되어지며, 수익성을 극대화하기 위해 지능

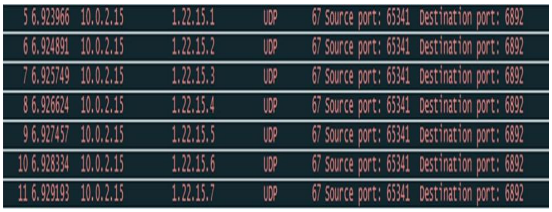
형 지속위협(APT)공격을 접목한 타겟형 랜섬웨어 공격 시도가 증가할 것으로 전망된다. SNS 계정탈취 등 모바일을 통한 유포 및 사회적 이슈를 다룬 게시물을 가장하여 랜섬웨어 유포용 가짜 페이지로 이동시켜 감염을 유도하는 공격방식도 예상되어진다[7, 13].

랜섬웨어의 위협은 올해 더욱 고도화되고 공격 범위도 확장될 전망이다. 지금까지 금전적인 피해를 야기하는 사이버 범죄는 가짜 홈페이지를 통해 사용자 정보를 탈취하는 피싱과 파밍이 주도했지만 이제 랜섬웨어가 그 중심에 있다 해도 과언이 아니다.

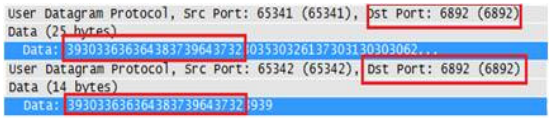
Ⅲ. 랜섬웨어 감염 탐지 기법

3.1. 시그니처 기반 탐지 패턴 제작 과정

랜섬웨어에 효과적으로 대응하기 위해서는 주요 데이터 백업, 보안 업데이트 철저, 취약한 사이트 방문 제한과 같은 사전 준비와 더불어 랜섬웨어 감염 시 이에 대한 신속한 인지를 통하여 감염경로 차단과 같은 피해 확산 조치가 중요하다. 이를 위해서는 네트워크 트래픽 내에서 랜섬웨어 감염 시 발생하는 고유한 신호를 탐지하는 방법이 현재 가장 많이 활용되고 있다.



(a)



(b)

alert any any -> any 6892 (content:"| 39 30 33 63 63 64 38 47 39 64 37 32|"; offset:0; depth:12;)

(c)

Fig. 3 Example of Signature-based Detection Pattern (a) Example of Malicious Code Infected Signal (b) Example of Common Signature Analysis through Packet Comparison

(c) Example of Snort Detection Pattern

실제 랜섬웨어를 이용하여 시그니처 기반 탐지 패턴 제작 과정을 분석해보면, 랜섬웨어 샘플 실행 시 그림 3의 (a)와 같이 외부에 6892 포트로 UDP 트래픽이 대량 발생하는 것을 확인 할 수 있다.

MD5	511F33AC0F421A484C94C637F8C96457
Detection Pattern	
alert tcp any any -> any any (content:"GET"; pcre:"/[a-zA-Z0-9]{4}-[a-zA-Z0-9]{4}-[a-zA-Z0-9]{4}-[a-zA-Z0-9]{4}-[a-zA-Z0-9]{4}\?iframe";)	
Infection Signal Detection	
GET /C93A-0600-3A97-05C5-7617?iframe&_=1498656461298 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; .NET4.0E) Host: p27dokhpz2n7nvgr.14zwws.top Connection: Keep-Alive	

(a)

MD5	8C413E31F39a54ABF78C3585444051F7
Detection Pattern	
alert tcp any any -> any 80 (content:"GET|20|/";content:"Host|3A20|microsoftinformation.html";)	
Infection Signal Detection	
GET /microsoftinformation.html HTTP/1.1 User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0) Host: 195.154.105.247 Cache-Control: no-cache	

(b)

MD5	F00D9B4F41C473E7EB15EBFA8504396A
Detection Pattern	
alert tcp any any -> any 80 (pcre:"/^(GET|POST)/"; offset:0; content:"/checkupdate"; nocase; within:18; pcre:"/Host\x3A\x20[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\x0d\x0a/i";)	
Infection Signal Detection	
POST /checkupdate HTTP/1.1 Accept: */* Accept-Language: en-us Referer: http://91.237.247.24/ x-requested-with: XMLHttpRequest Content-Type: application/x-www-form-urlencoded Accept-Encoding: gzip, deflate Cache-Control: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; .NET4.0E) Host: 91.237.247.24 Content-Length: 1148 Connection: Keep-Alive	

(c)

Fig. 4 Ransomware Detection Pattern and Example of Real Detection (a) Cerber Ransomware (b) Cryptomix Ransomware (c) Locky Ransomware

각각의 UDP 트래픽을 확인 한 결과, 그림 3의 (b)와 같이 공통된 포트 정보 이외에도 payload 내에 공통된 문자열(39 30 33 63 63 64 38 37 39 64 37 32)이 포함된 것을 확인 할 수 있다.

확인된 문자열을 통하여 snort 패턴을 작성하기 위하여 'content' 옵션에 탐지하고자 하는 문자열을 등록하고 패턴의 정합성을 높이기 위하여 'offset', 'depth' 옵션으로 위치를 지정하면 그림 3의 (c)와 같은 탐지 규칙이 생성된다.

이와 같은 방법으로 실제 시그니처 기반 랜섬웨어 감염을 탐지한 결과 그림 4와 같은 결과값을 확인 할 수 있다.

하지만 시그니처 기반 탐지 기법은 신·변종 랜섬웨어가 등장할 경우, 이에 대한 분석이 완료될 때까지 대응할 수 없는 단점이 있다. 또한 분석가 역량에 따라 생성되는 시그니처 품질에 차이가 발생하고, 이로 인하여 일회성 시그니처 증가로 탐지 시스템 성능 저하 및 오탐을 야기할 수 있는 문제점이 발생할 수 있다.

3.2. 탐지 패턴 자동화 모델

변종 랜섬웨어의 빈번한 등장으로 보안 담당자가 전통적인 시그니처 기반 탐지 방법으로는 적절한 대책 수립이 매우 어려워짐에 따라, 그림 5와 같이 파일 수집, 행위분석, 감염 신호 분류, 탐지패턴 생성, 네트워크 탐지 시스템 적용까지 일련의 과정을 자동으로 진행하는 대응 모델을 제안한다.

파일 수집 단계에서는 외부에서 유입되는 트래픽에서 랜섬웨어 유포에 활용되는 메일 첨부파일, 문서 및 실행 파일을 추출한 후 행위분석 단계로 넘긴다.

행위 분석 단계에서는 가상 머신에서 수집한 파일을 직접 실행시킨다. 가상 머신 내에는 랜섬웨어 행위 탐지를 위하여 사전에 hwp, pdf, doc, jpg와 같은 각종 샘플 파일이 저장되어 있으며, 해당 파일의 상태 변화를 모니터링 하여 랜섬웨어 감염 유무를 확인한다. 또한 랜섬웨어 동작 시 생성되는 네트워크 트래픽을 수집하여 저장하는데, 시그니처 제작에서 가장 중요한 것은 감염 PC 종류에 상관없이 발생하는 공통된 탐지 패턴을 찾는 것이다. 그렇기 때문에 환경 설정을 달리한 2개의 가상 머신에서 랜섬웨어 파일을 각각 실행하여 2개의 감염 신호를 pcap 포맷으로 생성한다.

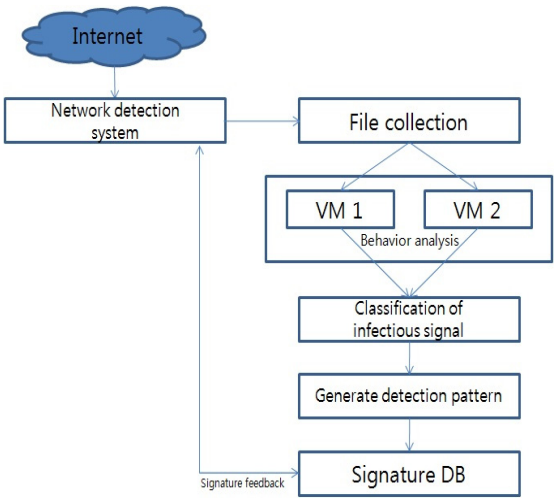


Fig. 5 Automation Model of Ransomware Infection Detection Pattern

감염 신호 분류에서는 그림 6과 같이, 랜섬웨어 실행 시 발생하는 트래픽에서 시그니처 제작에 필요한 패킷을 선별하는 과정이다.

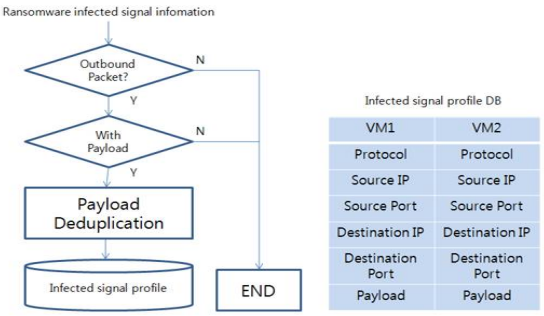


Fig. 6 Classification of Infection Signal

랜섬웨어가 동작 시 명령제어서버로 전송하는 감염 PC 정보나 추가 파일 다운로드를 요청하는 패킷을 대상으로 하기 때문에 방향성을 확인하여 Outbound 트래픽을 추출한다. 또한 생성된 시그니처의 정합성을 높이기 위하여 ip, port 정보 보다는 payload 내에서 고유 패턴을 찾아야 함에 따라 payload가 없는 패킷을 제외한다. 또한 복수의 C&C로 동시에 감염 신호를 보내는 랜섬웨어도 존재하는데, 이럴 경우 패턴 제작 시 시스템에 부하를 주기 때문에 payload에 대한 중복 제거 후 감염 신호 프로파일 DB에 저장한다.

탐지패턴 생성 단계에서는 VM1, VM2에서 생성된 감염 신호 프로파일 DB에서 동일 목적지 IP로 향하는 패킷을 선택하여 그림 7과 같이 매칭시킨다.

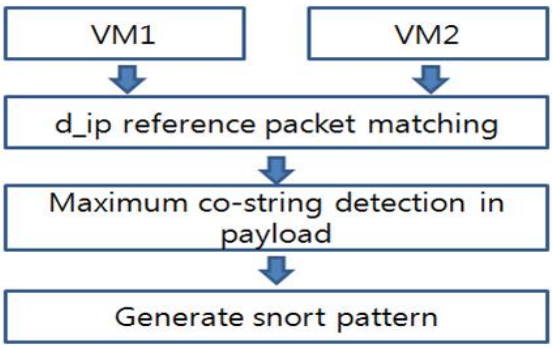


Fig. 7 Generation of detection pattern

매칭된 패킷을 대상으로 payload 내에서 연속된 최대 공동 문자열을 검출해야 하는데, 본 연구에서는 각각의 문자열을 일대일로 비교하여 공동 문자열을 검출하는 프로그램을 그림 8과 그림 9와 같이 작성하였다.

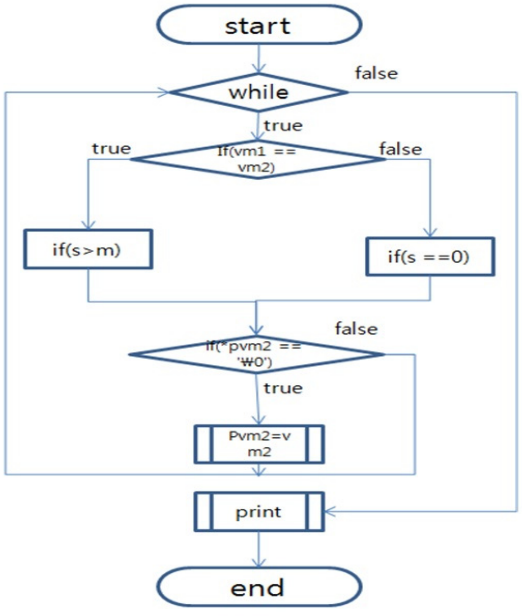


Fig. 8 Algorithm of Longest Continuous Common String Detection Module

```
#include <stdio.h>
int main(){
   char* vm1 = "abcddef";
   char* vm2 = "cbcddea";
   char tmp[2000] = "";
   char* pvm1 = vm1;
   char* pvm2 = vm2;
   char* bm = pvm1;

   int s = 0;
   int m = 0;

   while(*pvm1 != '₩0') {
      if(*pvm1 == *pvm2){
         pvm1++; pvm2++; s++;
         if(s > m){
            m = s;
            for(int i=0;i<s;i++){
               tmp[i] = *(bm + i);
            }
            tmp[s] = '₩0';
         }
      }else{
         pvm1 = bm;
         if(s == 0){
            pvm2++;
         }
         s = 0;
      }
      if(*pvm2 == '₩0'){
         pvm2 = vm2;
         pvm1 = ++bm;
      }
   }
   printf("%d₩n%s₩n", m, tmp);
}
```

Fig. 9 Source Code of Longest Continuous Common String Detection Program

'abcddef' 와 'cbcddea' 임의의 두 문자열을 대상으로 연속된 공통 문자열 검출 결과 그림 10과 같이 정상 동작함을 확인할 수 있다. 이를 이용하여 확보된 공통 문자열을 탐지 패턴으로 삼아서 데이터베이스에 저장 후 탐지 센서에 적용하면 시그니처 자동 생성을 위한 하나의 사이클이 완료된다.

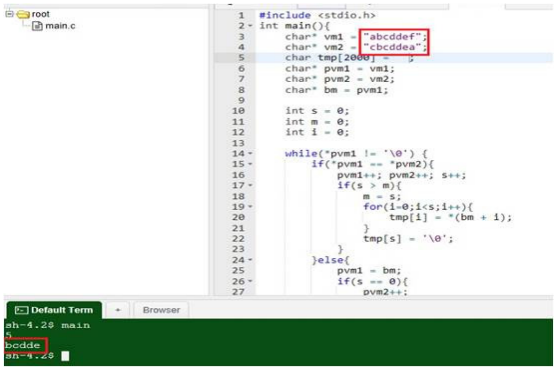


Fig. 10 Result of Verification

Ⅳ. 결 론

본 연구에서는 날로 늘어나고 있는 랜섬웨어 등의 악성코드 자동분석 모델을 제시하였다. 제시한 모델은 악성코드의 파일수집부터 시스템 적용까지의 일련의 과정을 자동으로 생성할 수 있다. 본 연구의 모델은 기업이나 공공의 보안관제센터에서 구비된 시스템에 맞게 응용하여 활용이 가능할 것으로 기대된다.

단, 본 연구에서의 실험은 일부 샘플에 한정되어 진행되었기 때문에 향후 연구에는 실제 운영계 데이터를 축척하여 다양한 시뮬레이션 환경과 확장된 샘플의 실험을 통해 신·변종 악성코드를 대응할 수 있도록 결과를 개선할 것이다.

REFERENCES

[1] B. J. Kim, W. S. Kim, J. H. Lee, S. H. Yim, S. G. Song, and S. J. Lee, “Design and implementation of a ransomware prevention system using process monitoring on android platform,” *Proceedings of the Korean institute of information scientists and engineers*, pp. 852-853, Dec. 2015.

[2] J. Y. Moon and Y. H. Chang, “Ransomware analysis and method for minimize the damage,” *The Journal of the Convergence on Culture Technology*, vol. 2, no. 1, pp.79-85, Feb. 2016.

[3] Malwarebytes (2017, January). 2017 State of Malware Report[Internet]. Available: https://blog.malwarebytes.com/malwarebytes-news/2017/02/2016-state-of-malware-report/.

[4] SonicWall (2017. February). 2017 SonicWall Annual Threat Report [Internet]. https://www.sonicwall.com/whitepaper/2017-sonicwall-annual-threat-report8121810/.

[5] Badware.info (2016. December), Malicious Link Diffusion Detection System Trend Analysis Report [Internet]. Available: http://www.uproot.im/pdf/badware.pdf.

[6] Korea Ransomware Infringement Response Center (2017. February). 2017 Ransomware Infringement Analysis Report [Internet], Available: https://www.rancert.com/bbs/bbs.php?bbs_id=notice&mode=view&id=52.

[7] KISA (2017. January). 16-year Ransomware trend and 17-year outlook [Internet], Available: http://www.krcert.or.kr/data/reportView.do?bulletin_writing_sequence=24983.

[8] J. M. Youn, J. G. Jo, and J. C. Ryu, “Methodology for intercepting the ransomware attacks using file i/o intervals,” *Journal of The Korea Institute of Information Security & Cryptology*, vol.26, no.3, pp.645-653, Jun. 2016.

[9] G. S. Kim and M. S. Kang, “The next generation of cyber security issues and threats and countermeasures,” *Journal of the Institute of Electronics and Information Engineers*, vol. 41, no. 4, pp. 69-77, Apr. 2014.

[10] Hauri (2017. March). Virobot Security Magazine[Internet], Available: http://www.hauri.co.kr/information/magazine_view.html?intSeq=95&page=1.

[11] Kbench (2017. February). Evolving Korea customized Ransomware. Venus Locker variant disguised as educational schedule discovery in Korea [Internet]. Available: http://www.kbench.com/?q=node/172991.

[12] Symantec (2016. June). An Special report: Ransomware and Business [Internet], Available: https://www.symantec.com/connect/blogs/report-organizations-must-respond-increasing-threat-ransomware.

[13] Trendmicro (2016. July). Why Ransomware is ‘Eaten’ Part 2: Penteration Strategy [Internet]. Available: http://www.trendmicro.co.kr/kr/blog/ransomware-arrival-methods/index.html.

이후기(Hoo-Ki Lee)

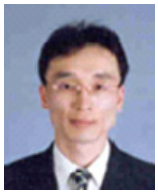
동국대학교 정보보호학 공학석사
숭실대학교 IT정책학과 박사과정
※관심분야 : 사이버보안, 침해사고대응, 보안관제, 전자메일 보안

성종혁(Jong-Hyuk Seong)

영남대학교 컴퓨터공학과 공학석사
경기대학교 산업보안학과 박사과정
※관심분야 : 정보보안, 산업보안, 융합보안

김유천(Yu-Cheon Kim)

동국대학교 정보보호학 석사과정
※관심분야 : 보안관제, 악성코드분석, 융합보안



김종배(Jong-Bae Kim)

2002년 8월 숭실대학교 정보과학대학원 석사
2006년 8월 숭실대학교 대학원 컴퓨터학과 박사
2001년 ~ 2012년 (주)이엔터프라이즈 대표이사
2012년 ~ 현재 숭실대학교 SW특성화대학원 교수
※관심분야 : 소프트웨어공학, 정보보호, 오픈소스소프트웨어

김광용(Gwang-Yong Gim)

1995년 8월 조지아 주립대학교 경영학과 박사
현 IT서비스학회 명예회장
현 숭실대학교 경영학부 교수
현 4차산업혁명포럼 위원장
전 서비스사이언스전국포럼 기획위원장
전 숭실대학교 특임부총장
※관심분야 : 지적재산권, 서비스 CRM, SW산업정책