랜섬웨어 유형별 특징분석 및 위협에 대한 연구

Analysis of characteristics and threats by Ransomware type

저자
(Authors)

조성준, 강승용, 노봉남
Sung-Jun Cho, Seung-Yong Kang, Bong-Nam Noh

출처
(Source)

Proceedings of KIIT Summer Conference , 2018.6, 472-475 (4 pages)

발행처
(Publisher)

한국정보기술학회
Korean Institute of Information Technology

URL

http://www.dbpia.co.kr/Article/NODE07467747

APA Style

조성준, 강승용, 노봉남 (2018). 랜섬웨어 유형별 특징분석 및 위협에 대한 연구. Proceedings of KIIT Summer Conference, 472-475.

랜섬웨어 유형별 특징분석 및 위협에 대한 연구

조성준*, 강승용**, 노봉남***

Analysis of characteristics and threats by Ransomware type

Sung-Jun Cho*, Seung-Yong Kang**, and Bong-Nam Noh***

요 약

IT(Information Technology)기술이 발전함에 따라 컴퓨터 저장매체의 대용량화로 인해 문서파일의 저장 수량도 증가하고 있으며, 이에 문서파일 등 디지털 콘텐츠 관리의 중요성도 높아지고 있다. 디지털 콘텐츠 즉 문서, 그림파일 등을 암호화하여 비트코인을 요구하는 악성코드의 일종인 랜섬웨어(Ransomware)에 의한 피해는 점점 증가하고 있다. 즉시 현금화할 수 있는 랜섬웨어는 해커들의 매력적인 사업이 되었으며, 기존 악성코드와 달리 제거 후에도 암호화된 파일은 제작자의 도움없이는 복구하기 어렵다.

본 연구에서는 현재 많은 피해를 주고 있는 랜섬웨어(Ransomware)에 대한 효과적인 방지방법을 연구하기 위해 우선 대표적인 11종의 랜섬웨어를 분석하여 특징을 분류하고 이를 기반으로 위협요소를 정리하였다.

Abstract

With the development of information technology, the storage capacity of computer storage media has been increasing due to the increase in the storage capacity of document files, and the importance of managing digital contents such as document files is increasing. The damage caused by Ransomware, a malicious code that requires bit coin by encrypting digital contents such as documents and picture files, is increasing. Ransomware, which can be instantly cashed, has become an attractive business for hackers, and unlike existing malware, encrypted files are hard to recover without the help of the creator. In this paper, to investigate the effective prevention method of Ransomware, which is currently suffering from a lot of damage, we first classify the ten typical types of Ransomware, classify the features, and classify threats based on them..

Key words

Ransomware type, Characteristics of Ransomware, Threats of Ransomware, Protect of Digital Content

Ⅰ. 서 론

IT(Information Technology)기술이 발전함에 따라 컴퓨터 저장매체의 대용량화로 인해 문서파일의 저

* 전남대학교 정보보안협동과정 박사과정
** 전남대학교 정보보안협동과정 박사과정
*** 전남대학교 전자컴퓨터공학부 교수 (교신저자)

장 수량도 증가하고 있으며, 이에 문서파일 등 디지털 콘텐츠 관리의 중요성도 높아지고 있다. PC에 저장되어 있는 디지털 콘텐츠 즉 문서, 그림파일 등을 암호화하여 비트코인을 요구하는 악성코드의 일종인 랜섬웨어(Ransomware)에 의한 피해는 점점 증가하고 있다. 기존 악성코드와 달리 제거 후에도 암호화된 파일은 제작자의 도움없이는 복구하기 어렵다. 한국인터넷 진흥원이 발표한 '16년 랜섬웨어 동향 및 17년 전망'에 따르면, '16년 국내랜섬웨어 유포는 전년도에 비해 증가하였는데, 한국인터넷진흥원에서 접수한 랜섬웨어 피해신고 현황을 살펴보면 2015년 770건에서 2016년 1,438건으로 전년대비 86.8% 증가하였다[1].

본 연구에서는 현재 많은 피해를 주고 있는 랜섬웨어(Ransomware)에 대한 효과적인 방지방법을 연구하기 위해 우선 대표적인 11종의 랜섬웨어를 분석하여 특징을 분류하고 이를 기반으로 위협을 정리하였다.

II. 본 론

2.1 11종의 랜섬웨어 분석

랜섬웨어(Ransomware)는 이용자의 데이터(시스템 파일, 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[2].

랜섬웨어(Ransomware)는 크게 두 가지 종류가 있다. 사용자의 컴퓨터를 잠그고 컴퓨터를 사용할 수 없게 하는 라커-랜섬웨어(Locker-Ransomware)와 사용자 개인의 파일을 암호화하여 파일을 사용할 수 없게 하는 크립토-랜섬웨어(Crypto-Ransomware)이다. 여기서는 크립토-랜섬웨어(Crypto-Ransomware)를 대상으로 연구하며, Windows, Linux, MacOSX 및 Android 플랫폼에서 동작하는 대표적인 11종의 랜섬웨어(Ransomware)를 분석하고 유형별 특징을 정리하였다. 11종의 랜섬웨어(Ransomware)의 공격대상 운영체제를 분류하면 표 1에서 분류하였다.

표 1. 11종 랜섬웨어의 공격대상 운영체제분류

공격대상운영체제	랜섬웨어 이름
Windows	VaultCrypt, TeslaCrypt, WannaCry, Petya, Cerber, Spora, Serpent
Linux	Linux.Cryptor
Android	Simplelocker
MacOSX	OSX/KeRanger-A

2.1.1 배포방법

11종의 랜샘웨어 배포방법은 표 2에서 분류하였다.

표 2. 11종 랜섬웨어의 배포방법

배포방법	랜섬웨어 이름
스피어 피싱(Spear Phishing), 드라이브 바이 다운로드(Drive-by-Download)	VaultCrypt, TeslaCrypt, OSX/KeRanger-A, Cerber, Spora, Serpent, GandCrab
Magento 플랫폼의 취약점을 악용하여 웹 서버 공격하여 유포	Linux.Cryptor
비공식 앱스토어에서 악성앱 배포	Simplelocker
EternalBlue exploit	WannaCry
CVE-2017-0199 exploit	Petya

랜섬웨어(Ransomware)에서 악용되고 있는 스피어 피싱(Spear Phishing)은 '창으로 찌르다'는 스피어(Spear)와 '사용자를 속이기'를 의미하는 피싱(Phishing)의 합성어이며, 신뢰할 수 있는 내용으로 위장한 악성 이메일을 관련자들에게 전송하여 메일 수신자가 해당 메일을 열람하거나 첨부파일을 열면 악성코드에 감염된다[3]. 드라이브 바이 다운로드(Drive-by-Download)는 웹사이트 접속만으로 사용자의 동의 없이 악성코드에 감염되게 하는 악성코드 유포 기법을 말한다. 이 기법은 웹사이트에 존재하는 응용프로그램의 취약점을 공격함으로 악성코드 유포가 이루어지게 된다. 인터넷 익스플로러, 자바, 플래시 플레이어 등의 응용 프로그램 취약점을 악용하는 익스플로잇 킷(Exploit Kit)을 이용해 유포된다[4]. 익스플로잇 킷(Exploit Kit)이란 응용프로그램의 취약점을 공격하는 취약점 코드를 가지고 있으

며, 해당 도구를 이용하여 자동으로 웹사이트 취약점을 공격하게 된다. 이러한 익스플로잇 킷은 매우 정교하고 자동화되어 사이버 범죄자들이 이용하기 쉬우며, 블랙마켓을 통해 구하기도 간편하여 악성코드 유포시 많이 사용된다[5].

2.1.2 파일 암호화 방법

11종 랜섬웨어의 파일 암호화 방법을 살펴보면 RSA, AES, RC4 등 다양하며 표3에서 분류하였다. 랜섬웨어 제작자의 공개키로 파일을 암호화하여 암호화된 파일을 복호화를 하기 위해서는 랜섬웨어 제작자의 개인키가 필요하며, 랜섬웨어 제작자의 C&C 서버에서 전달받은 공개키에 대한 개인키를 알지 못하면 파일의 복구는 불가능하다.

표 3. 11종 랜섬웨어의 파일 암호화 방법

파일 암호화 방법	랜섬웨어 이름
RSA-1024	VaultCrypt
AES-128-CBC	Linux.Cryptor, Simplelocker, WannaCry
AES-256-CBC	TeslaCrypt, OSX / KeRanger-A, Spora, Serpent, GandCrab
Salsa20-256	Petya
RC4-128	Cerber

2.1.3 백업파일 무력화

표 4. 11종 랜섬웨어의 백업파일 삭제

백업파일 무력화	랜섬웨어 이름
vssadmin.exe를 사용하여 볼륨섀도카피를 삭제	TeslaCrypt, WannaCry, Spora
WMIC.exe를 사용하여 볼륨섀도카피를 삭제	Serpent
Time Machine 백업 파일을 암호화	OSX / KeRanger-A
해당 없음	VaultCrypt, Linux.Cryptor, Simplelocker, Petya, Cerber, GandCrab

11종 랜섬웨어의 백업파일 무력화는 표 4에서 분류하였다. 랜섬웨어가 파일시스템의 다른 영역에 암호화된 파일을 저장하고 원본파일을 삭제하는 경우 Windows의 VSC(Volume Shadow Copy) 기능을 통해 암호화된 파일 중 일부 파일을 복구가 가능하나 원본파일을 덮어쓰기 방식으로 암호화하는 경우 복원이 어렵다. 최신 랜섬웨어는 볼륨 섀도 카피(VSC:Volume Shadow Copy)를 삭제하여 복원할 수 없다.

2.1.4 C&C서버와 통신

11종 랜섬웨어의 C&C서버와 통신은 표5에서 분류하였다. 익명의 토르(Tor) 네트워크의 경우 추적을 피하기 위해 사용하는 것으로 보인다.

표 5. 11종 랜섬웨어의 C&C서버와 통신

C&C서버와 통신	랜섬웨어 이름
하드코딩된 URL	VaultCrypt, TeslaCrypt
IP 대역	Cerber
토르(Tor) 네트워크	Simplelocker, Serpent, OSX / KeRanger-A, WannaCry, Spora,
패킷내 host정보(google등)를 위장하고 특정IP로 접속	GandCrab
해당없음	Linux.Cryptor, Petya

2.1.5 보안설정탐지/우회기능

최신 랜섬웨어(Ransomware)들은 가상환경을 탐지하여 자동분석하지 못하도록 하거나 분석도구나 백신의 감시프로세스를 종료하는 등 보안설정 탐지기능이 강화되고 있다. 보안설정탐지/우회기능은 표 6에서 분류하였다.

표 6. 11종 랜섬웨어의 보안설정탐지/우회기능

보안설정탐지/우회기능	랜섬웨어 이름
분석도구 실행여부 탐지	VaultCrypt, TeslaCrypt
백신 실시간 감시프로세스 검사	TeslaCrypt, GandCrab
가상환경 탐지	TeslaCrypt, Cerber, GandCrab
무파일(Fileless)공격	GandCrab
해당없음	WannaCry, Petya, Spora, Serpent, Simplelocker, OSX / KeRanger-A, Linux.Cryptor

갠드크랩(GandCrab)에서 사용된 무파일(Fileless)공격은 인터넷익스플로러(iexplore.exe)에서 취약점 발생시 악성스크립트가 실행되고 해당 스크립트의 코드가 디코딩되면서 악성 DLL파일이 iexplore.exe이 주입되어 실행된다[6].

2.2 위협요소 정리

11종의 랜섬웨어를 분석해 본 결과 여러 위협요소를 확인할 수 있었다. 첫째 스피어 피싱(Spear Phishing)과 같은 사회공학적 기법이나 드라이브 바이 다운로드(Drive-by-Download)와 같이 어플리케이션의 보안 취약점을 이용하여 악성코드를 자동으로 설치한다. 둘째 운영체제의 백업파일을 암호화하거나 삭제하여 문서파일 복구를 무력화하고 RSA, AES, RC4 등 다양한 방식으로 랜섬웨어 제작자의 공개키로 파일을 암호화하여 랜섬웨어 제작자의 공개키에 대한 개인키를 알지 못하면 파일의 복구는 불가능하다. 셋째 C&C서버 추적을 방해하기 위해 패킷 내 HOST정보를 Google 등 정상 데이터로 위장하거나 익명의 토르 네트워크를 이용한다. 넷째 가상환경을 탐지하여 자동분석하지 못하도록 하거나 분석도구나 백신의 감시프로세스를 종료하는 등 보안설정 탐지기능이 강화되고 있으며, 자동분석시스템 및 백신을 우회하는 무파일(Fileless)공격으로 감염시킨다.

III. 결 론

즉시 현금화할 수 있는 랜섬웨어(Ransomware)는 해커들의 매력적인 사업이 되었으며, 랜섬웨어(Ransomware)에 의한 피해는 2016년에 전년 대비하여 86.8%가 증가하였다. 본 연구에서는 많은 피해를 주고 있는 11종의 대표적인 랜섬웨어를 분석하여 특징별로 분류하였고, 이를 기반으로 4가지 위협요소를 정리하였다. 추후 분석을 통해 정리된 위협요소와 현재 랜섬웨어를 탐지하는 기법의 장·단점을 분석하여 보다 효과적인 방지방법에 대한 연구가 필요하다.

참 고 문 헌

[1] 16년 랜섬웨어 동향 및 17년 전망, 한국인터넷진흥원, www.boho.or.kr/filedownload.do?attach_file_seq=979&attach_file_id=EpF979.pdf.

[2] 랜섬웨어의 정의 및 감염경로, 한국인터넷진흥원, https://www.krcert.or.kr/ransomware/information.do.

[3] 구미숙, 이영진, "악성코드의 유입경로 및 지능형 지속 공격에 대한 대응 방안", 중소기업융합학회 논문지, 제5권, 제4호, 2015.12, pages 37-42.

[4] 김종기, "웹사이트를 통해 유포되는 메모리 상주형 악성코드의 탐지에 관한 연구", 순천향대학교, 석사학위논문, 2016.02.

[5] 이재철, 신효정, 김형식, "웹 익스플로잇킷에 의한 감염경로 분석", 보안공학연구 논문지, 제13권 제4호, 2016.8, pages 299-314.

[6] Fileless 형태로 유포되는 GandCrab v2.1, 안랩 ASEC blog, http://asec.ahnlab.com/1130?category=342979.