Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.2, Apr. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.2.251

MacOS에서 파일확장자 관리를 통한 랜섬웨어 탐지 및 차단 방법*

윤 정 무,† 류 재 철‡
충남대학교

How to Detect and Block Ransomware with File Extension Management in MacOS*

Jung-moo Youn,† Jae-cheol Ryu‡
Chung-Nam National University

요 약

랜섬웨어를 비롯한 대부분의 악성코드들은 Windows 운영체제를 대상으로 제작된다. 점유율이 높은 운영체제를 목표로 삼아야 그만큼 피해가 더 커지기 때문이다. 하지만 최근 몇 년 전부터 MacOS의 운영체제의 점유율이 꾸준히 증가하고 있다. 사람들에게 점점 많이 사용되기 시작하면서 MacOS운영체제에서 동작하는 악성코드의 수도 점점 늘어나고 있는 상황이다. 랜섬웨어는 2015년부터 우리나라에 많이 알려지기 시작했으며 점차 피해사례도 증가하고 있다. 2016년 3월에 MacOS용 랜섬웨어가 발견되는 등 더 이상 MacOS도 랜섬웨어로부터 자유롭지 않은 상황이다. 앞으로 계속 발생 할 랜섬웨어에 대처하기 위해서 본 논문은 랜섬웨어를 탐지하기 위한 방법으로 랜섬웨어가 암호화 한 파일의 확장자를 변경하는 것을 이용하였다. 사용자에 의해 확장자가 변경되는 것과 랜섬웨어 프로세스에 의해 확장자가 변경되는 것을 구분함으로써 랜섬웨어 프로세스를 탐지하고 차단하는 방법을 연구했다.

ABSTRACT

Most malware, including Ransomware, is built for the Windows operating system. This is because it is more harmful to target an operating system with a high share. But in recent years, MacOS's operating system share has steadily increased. As people become more and more used, the number of malicious code running on the MacOS operating system is increasing. Ransomware has been known to Korea since 2015, and damage cases are gradually increasing. MacOS is no longer free from Ransomware, as Ransomware for MacOS was discovered in March 2016. In order to cope with future Ransomware, this paper used Ransomware's modified file extension to detect Ransomware. We have studied how to detect and block Ransomware processes by distinguishing between extensions changed by the user and extensions changed by the Ransomware process.

Keywords: Ransomware, File extension, Detection, Block

I. 서 론

컴퓨터를 사용하는 사람이 증가하면서 컴퓨터가 제공하는 편의기능들은 계속 증가해왔다. 최근에는 개인정보를 이용한 전자결제시스템이나 전자투표 등 민감한 정보를 다루는 기능들도 제공한다. 동시에 타인의 컴퓨터에 무단으로 접속하고 개인정보를 탈취하고 심각한 악성행위를 하는 악성코드들도 증가하고

Received(01. 31. 2017), Modified(03. 07. 2017), Accepted(03. 07. 2017)
* 이 논문은 2015년도 미래창조과학부 및 정보통신기술진흥센터의 SW컴퓨팅산업원천기술개발사업[R0190-16-2009, 화이트리스트와 상황인지 기술을 이용한 엔드포인트 보호기술 개발]의 일환으로 수행하였습니다.
† 주저자, jmstar1@cnu.ac.kr
‡ 교신저자, jcryou@home.cnu.ac.kr(Corresponding author)

있다[1]. 초기의 악성코드들은 단순히 재미를 위해서 제작되었거나 자신의 지식을 자랑하기 위해서 제작된 것에 반해 최근의 악성코드들은 그렇지 않다. 특정 대상을 목표로 고의적으로 피해를 입히는 용도로도 사용되며 개인정보를 유출하고 불법으로 타인에게 판매해서 수익을 챙기는 악성코드도 있다. 최근 유행하는 악성코드인 랜섬웨어의 경우도 마찬가지다. 랜섬웨어는 타인의 컴퓨터에 무단으로 침입하고 사용자 몰래 중요한 파일들을 암호화 한다. 암호화 된 파일들은 사용자가 정상적으로 사용 할 수 없게 되므로 해커는 암호화된 파일들을 인질로 삼고 돈을 요구한다[2]. 이렇듯 악성코드는 점차 목표가 명확해지고, 단순히 재미가 아닌 체계적이고 더 심각한 악영향을 미치도록 진화하고 있다. 악성코드는 최대한 많은 피해를 입히기 위해서 현재 가장 많이 사용 중인 Windows운영체제의 PC를 대상으로 악성코드가 가장 많이 제작되었고 유포되었다. 두 번째로 높았던 Linux계열의 운영체제 또한 많은 악성코드가 존재한다. 세 번째로 높은 MacOS의 경우, 2013년까지만 해도 악성코드는 불과 수천 개에 불과했지만 현재는 상황이 달라졌다. MacOS는 Linux보다 더 사용량이 많아졌으며, 악성코드 또한 급증했다[3].

MacOS에서의 악성코드수가 적은 것은 단순히 점유율 뿐만은 아니다. 기본적으로 Windows, Linux와 달리 폐쇄적인 운영체제며 운영체제 구조 및 동작에 관련된 공개된 자료들이 희박하고, 연구를 하는 사람도 많지 않다. 그리고 Apple사의 제품들은 보안을 중요시하므로 MacOS도 타 운영체제에 비해서 강화된 보안기능을 가지고 있다. 이러한 이유로 2015년 11월까지만 해도 Apple사에서는 MacOS용 랜섬웨어/암호화 바이러스는 절대 없을 것이라고 주장했다. 하지만 주장한 지 몇 달이 채 안 돼서 브라질의 보안 전문가 Rafael Salema Marques가 공개한 시연 비디오에는 MacOS에서도 충분히 랜섬웨어가 제작 될 수 있음을 확인 할 수 있었다. 실제로, 2016년 3월에 MacOS를 대상으로 하는 랜섬웨어인 KeRanger가 발견되었다. 이 랜섬웨어는 개발자서명을 훔쳐서 사용했으며 정상적인 개발자의 서명을 통해 보안 매커니즘을 우회했다. 사용자끼리 파일을 공유하는 프로그램의 설치파일에 악성스크립트를 포함시키고, 설치 시 지정한 서버에서 랜섬웨어 다운로드 및 실행하도록 한 것이다. MacOS에서는 Application을 최초 설치 할 때 관리자 로그인을 하므로 랜섬웨어는 쉽게 관리자 권한을 얻어 파일들을 암호화 할 수 있었다.

랜섬웨어는 자신이 암호화한 파일들을 특정 확장자로 변경해놓는다. 자신이 암호화 한 파일들을 식별하기 위한 용도로 특정 확장자로 변경하는 것이며, 랜섬웨어의 종류마다 다양한 확장자명을 사용한다.

본 논문에서는 MacOS에서 점점 증가할 랜섬웨어로 인한 피해를 줄이고자 랜섬웨어의 공통적인 특징인 파일 확장자변경을 이용한 랜섬웨어 탐지 방법론을 제시하고자 한다. 커널에서는 파일접근 및 제어가 가능하다. 이것을 이용하여 랜섬웨어로 판단된 프로세스를 제어하는 기술을 제시하고자 한다.

II. 관련 연구

2.1 랜섬웨어

2.1.1 Windows에서의 랜섬웨어

대다수의 컴퓨터가 Windows운영체제 시리즈를 탑재하고 있다고 해도 무방할 정도로 Windows는 점유율이 높은 운영체제다. 마찬가지로 악성코드역시 Windows에서 가장 많이 발견되며 특히 랜섬웨어도 가장 많은 피해를 입힐 수 있는 Windows를 대상으로 많이 제작되고 있다[4].

우리나라에서는 랜섬웨어가 2015년 CryptoWall의 등장으로 사람들에게 알려지기 시작했으며 점점 유명세를 떨쳐나갔다. CryptoWall 랜섬웨어는 메일 또는 웹페이지, p2p등을 통해 감염되며 파일 또는 문서파일에 위장하여 배포된다. “.js”확장자를 가진 자바스크립트를 실행하거나 문서파일속에 심어진 실행파일로도 감염된다. 이 랜섬웨어는 문서파일과 이미지파일, 압축파일, 텍스트파일등 70여 가지의 확장자의 파일들을 암호화한다. 암호화가 완료되면 해커에게 비용을 지불할 것을 요구한다.

그 다음으로는 TeslaCrypt 랜섬웨어가 있다. 이 랜섬웨어역시 감염경로는 위와 같으나, 감염파일을 서버에서 다운로드 받아서 실행한다. 문서파일 등 40여 가지의 확장자를 가진 파일을 대상으로 암호화하며 암호화가 완료된 파일들은 확장자가 변경된다. 또한 암호화도중 컴퓨터 성능저하를 우려하여 200MB이상의 파일은 암호화하지 않는다. 비슷한 종류의 랜섬웨어가 계속 유행하는 중 Locky라는 신종 랜섬웨어가 등장한다. 이 랜섬웨어는 메일을 송장 및 결제내역으로 교묘하게 위장하여 첨부파일을 확인

하도록 유도하며, 첨부파일 확인 시 랜섬웨어 감염파일을 서버에서 다운로드받아서 PC를 감염시킨다. 100여 가지의 확장자를 가진 파일을 대상으로 암호화를 수행하며 암호화가 완료된 폴더에 1개의 파일을 신규생성하며 확장자를 locky로 변경한다.

마지막으로 2015년도부터 꾸준히 피해를 입혀온 CryptoLocker랜섬웨어가 있다. 이 랜섬웨어는 발신지가 명확하지 않은 메일의 첨부파일을 실행하면 감염되며 서버로부터 랜섬웨어 감염파일을 다운받아 실행한다. 약 40여 가지의 확장자를 가진 파일을 대상으로 암호화를 수행하며 완료된 파일들은 확장자가 ".encrypted"로 변경된다. 또한 백업을 하지 못하도록 시스템보호기능의 백업 본을 삭제하는 치밀함까지 보였다. 특이사항으로는 tmp폴더에 저장된 파일에 대해서는 암호화를 수행하지 않는다.

지금까지 설명한 랜섬웨어들을 살펴보면 공통적으로 랜섬웨어에 의해 암호화된 파일들은 특정 확장자로 확장자가 변경된다는 것이다[5]. 물론 파일을 암호화 한 후 폴더내에 자신만 식별 할 수 있는 신규파일도 생성하지만 파일의 확장자변경을 통해 자신이 암호화 한 파일이 어떤 것들이 있는지 확인한다. 이는, 파일들을 다시 복구하기 위해 복호화를 시도할 때, 대상파일을 지정하기 위한 것이다. 바꿔 말하면 랜섬웨어 중 파일의 확장자를 변경하지 않는 랜섬웨어가 있다면 이 랜섬웨어는 단순히 돈만 요구하고 복구는 하지 않는 랜섬웨어일 가능성이 있다[6].

2.1.2 MacOS에서의 랜섬웨어

MacOS운영체제에서는 악성코드가 Windows에 비해 상대적으로 적다. 랜섬웨어또한 2013년 7월에 FBI 랜섬웨어라는 이름으로 처음 등장했다. 이 랜섬웨어는 무료로 제공되는 영화나 TV프로그램을 검색하는 과정에서 링크를 잘못 클릭한 경우 감염된다. 자바스크립트로 제작되었으며 맨 처음에 FBI를 사칭하는 웹페이지를 띄우고 FBI가 사용자가 불법으로 영화나 TV프로그램을 시청하는 것을 적발했고, 이를 해결하기 위해서는 일정금액을 지불 할 것을 요구한다. 요구를 받아들이지 않고 웹페이지를 닫기 위해 종료버튼을 클릭하면 당신의 브라우저가 잠겼다는 경고창이 나타나고 확인을 클릭해도 무한히 경고창이 발생한다. 시스템에서 강제종료를 해도 다시 브라우저를 실행하면 FBI경고창이 뜬다. 이 랜섬웨어는 MacOS에서 기본적으로 사용하는 웹 브라우저인 Safari에서 사용되는 자바스크립트의 취약점을 이용했다. Safari의 기본설정을 FBI경고페이지로 시작페이지를 설정하고, 닫기 버튼을 눌려도 계속 경고창이 발생하도록 코드를 수정했다. 이를 해결하기 위해서는 단순히 Safari의 설정을 초기설정으로 되돌리기만 하면 된다. 이 랜섬웨어는 특정 파일을 암호화하는 것이 아닌 웹브라우저의 설정변경을 통해 웹브라우저를 인질로 삼고 돈을 요구했다. 하지만 단순히 설정을 변경한 것이므로 감염되었다 하더라도 쉽게 치료가 가능했다[7].

Windows의 경우 2015년부터 우리나라에서는 더욱 활발하게 랜섬웨어에 감염되는 사례가 많았으나 MacOS는 그렇지 않았다. 게이트키퍼라는 보안매커니즘에 의해 Windows보다 더욱 까다로운 보안설정을 했으며 배포하는 프로그램은 무조건 개발자 서명을 해야만 했다. 그렇기 때문에 쉽게 랜섬웨어를 제작하지 못했으며, Apple사에서도 MacOS는 랜섬웨어로부터 안전하다고 주장했다.

하지만, 2016년 3월 KeRanger라는 랜섬웨어가 등장했다[8]. 이 랜섬웨어는 MacOS용 사용자 공유 프로그램인 BitTorrent의 클라이언트 설치 프로그램에 포함되어 유포되었다. 이 랜섬웨어는 개발자 서명이 되어있었기 때문에 보안매커니즘인 게이트키퍼로부터 간섭받지 않았다. 사용자가 해당 설치파일을 실행하면 시스템에서 랜섬웨어가 동작한다. 또한, 3일간의 대기시간을 가진 후 제어서버에 연결하고, 특정 문서파일 및 데이터파일을 암호화하기 시작했다. 암호화 한 파일들은 확장자를 ".encrypted"로 변경하였으며 암호화 과정이 완료되고 난 후 KeRanger는 피해자에게 특정주소로 가상화폐로 입금할 것을 요구했다. 피해자가 백업데이터를 통해 복구하지 못하도록 Time Machine 백업 파일까지 암호화를 시도했다. 서버를 통해 얻은 RSA키를 이용하여 랜덤넘버를 생성하며, 이 랜덤넘버를 이용하여 AES암호화 알고리즘으로 대상 파일들을 암호화 하였다. 실제로 파일들을 암호화하고 서버와 통신하여 키를 생성함으로써 피해자 스스로 파일을 복호화하지 못하도록 하는 MacOS에서의 제대로 만들어진 최초의 랜섬웨어인 것이다.

비록 MacOS가 타 운영체제보다 보안적인 측면에서 더 안전하다 할지라도 인증된 개발자의 서명하나로 보안매커니즘을 우회하여 쉽게 랜섬웨어가 유포될 수 있다는 가능성을 충분히 알 수 있었다[9].

III. 제안 연구 방법

대부분의 랜섬웨어는 자신이 타겟으로 삼은 파일을 암호화하고 난 후 확장자를 기존에 지정해놓은 확장자로 변경한다. 이 과정은 결국 랜섬웨어가 특정 파일의 정보에 접근하고 변경하는 것이므로 커널에서는 충분히 확인가능하다. 또한 확장자명을 변경한다는 것은 결국 파일명을 변경하는 것과 마찬가지다. 본 논문에서 제안하는 방법은 기존의 랜섬웨어들이 변경하는 확장자명들을 블랙리스트로 등록하여 랜섬웨어를 탐지하고 차단한다. 또, 커널에서는 파일의 이름이 변경될 때 사용자에 의해서 변경된 것인지 랜섬웨어에 의해 변경된 것인지 구분하여 랜섬웨어를 탐지하고 차단한다.

3.1 확장자 블랙리스트를 이용한 랜섬웨어 탐지

기존에 발견된 랜섬웨어들이 변경하는 확장자명을 수집하여 블랙리스트로 등록 한 후 변경되는 파일의 확장자가 블랙리스트에 등록된 확장자일 경우 해당 작업을 수행하는 프로세스를 랜섬웨어의 프로세스로 간주한다. 일련의 과정들은 유저레벨에서 수행 할 경우 타 프로세스에 의해 쉽게 간섭 및 변조가 가능하므로 관리자 권한에서 동작해야한다. 또한, 프로세스의 동작을 제어하기 때문에 결과적으로 커널영역에서 위와 같은 탐지과정을 수행한다. 일단 랜섬웨어 프로세스로 판단이 되면 커널에서는 해당 프로세스가 파일을 접근하지 못하도록 권한을 뺏음으로써 프로세스의 활동을 차단 할 수 있다.

총 19개의 랜섬웨어를 조사한 결과 Table 1과 같이 확장자를 변경하는 것을 알 수 있다. 31개의 랜섬웨어에 대한 변경확장자는 총 33개로 이를 활용하여 블랙리스트를 만들었다. 하지만 경우에 따라서 아예 확장자를 변경하지 않는 랜섬웨어도 있었고 어떤 랜섬웨어는 랜덤한 문자열로 바꾸는 경우도 있었다. 확장자를 변경하지 않는 랜섬웨어로는 CryptoWall3.0, MicrosoftCrypter, Spora등이 있었으며 이 랜섬웨어는 확장자 블랙리스트를 통해서 탐지할 수 없다. 즉, 확장자 블랙리스트를 만들어서 랜섬웨어를 탐지하는 것은 기존에 알려져 있는 랜섬웨어 중 확장자를 변경하는 랜섬웨어의 경우에만 모두 탐지 및 차단이 가능하며, 앞으로 발생할 랜섬웨어에 대해서는 탐지를 하지 못 할 수 있다.

Table 1. Ransomware's changing Extensions

Ransomware name	Changing Extensions
7ev3n-HONE$T	.R5A
AlphaCrypt	.ecc, .ezz, .exx
CERBER	.cerber
CERBER2	.cerber2
CERBER3	.cerber3
CERBER4	random value
CERBER5	random value
CERBER6	random value
Crypted	.crypted
CryptoLocker	.encrypted
CryptoMix	.rdmk
CryptoShield	.cryptoshield
CryptoWall3.0	None
CryptoWall4.0	random value
CryptXXX	.crypt
CryptXXX2.0	.crypt
CryptXXX3.0	.crypt
CTB-Locker	random value
Locky	.locky, .odin, .shit, .thor, .aesir, .zzzzz, .osiris
MicrosoftCrypter	None
NK_	None
Sage	.sage
Spora	None
TeslaCrypt	.ecc, .ezz, .exx
TeslaCrypt2.0	.aaa, .abc, .ccc, .vvv
TeslaCrypt3.0	.xxx, .ttt, .micro, .mp3
TeslaCrypt4.0	None
TeslaCrypt4.1	None
UltraCrypter	.cryp1, .crypz, random value
VenusLocker	.venusf, .venusp
VO_	None

3.1.1 파일 이름변경 이벤트 수집

MacOS의 커널은 Kernel Extension이라는 부가기능이 있다. 이 기능을 활용하면 커널에서 특정프로세스가 파일에 접근하여 수행하는 일련의 작업들에 대한 이벤트를 확인 할 수 있다. 이 기능은 주로 백신이 프로세스를 모니터링할 때 사용되도록 고안되었으며, 단순히 수집을 위한 File Operation기능과 프로세스를 제어 할 수 있는 Vnode기능으로 구분된다. 여기에서는 파일의 이름이 변경되는 이벤트를 수집하기 위해서 File Operation기능을 사용했다.

파일의 Rename에 대한 이벤트가 발생 할 경우를 탐지할 수 있다. 커널에서는 파일명과 파일확장자를 구분하지 않고 단순히 파일이름에 대한 변경이 발생할 경우만을 알려주기 때문에 이벤트를 받고 필터기능을 부가적으로 구현해 확장자 검사를 수행한다.

3.1.2 파일 접근이벤트 필터

위의 과정은 단순히 이벤트만을 수집하는 것이다. 그러므로 수집하는 동안에도 랜섬웨어에 의한 파일의 암호화는 계속 진행되므로 각 이벤트 한 개를 수집할 때 마다 확장자 검사를 실시간으로 수행해야 한다. File Operation에서는 단순히 파일명이 변경되는 것을 확인만하기 때문에 파일의 이름이 변경되었는지 파일의 확장자가 변경되었는지는 구별하지 못한다. 그러므로 이벤트 필터를 구현하여 파일의 이름과 확장자를 온점(.)으로 구분한다. 파일명 끝에서부터 온점이 나올 때 까지 검색하고 온점 이전까지를 확장자명으로 인식하도록 한다. 우선적으로 파일명이 파일이름만 바뀐 것인지 확장자까지 바뀐 것인지를 확인하고, 확장자가 바뀌었을 경우 블랙리스트에 있는 확장자로 바뀐 것인지를 확인한다.

즉, 실시간으로 프로세스의 파일명 변경 행위를 탐지하고, 블랙리스트와 비교하여 프로세스가 랜섬웨어 프로세스로 판단 된 경우 프로세스의 파일에 대한 접근권한을 뺏는다. 커널의 File Operation에 의해 파일명 변경 이벤트를 수집했을 때, 아무 이상이 없다면 수집만 하고 넘어가지만, 랜섬웨어 프로세스를 탐지하였을 경우 해당 프로세스의 파일접근권한을 우선 차단하기 때문에 수집한 파일명 변경 이벤트부터 프로세스는 정상적으로 작업을 수행할 수 없다. 하지만, 랜섬웨어가 파일명을 변경하는 시점은 파일을 암호화 한 후에 진행되므로 위와 같은 방법으로 랜섬웨어를 차단했을 경우 최초 파일 1개의 암호화는 막을 수 없다.

3.2 커널에서 확장자 변경 탐지 및 차단

3.2.1 랜섬웨어에 의한 확장자 변경 탐지

확장자 블랙리스트를 통한 랜섬웨어 탐지의 경우 새로운 랜섬웨어가 파일들을 암호화 한 후 어떤 확장자로 변경 할지 알 수 없기 때문에 기존에 발견된 랜섬웨어들을 탐지하기엔 적합하지만 앞으로 발생할 랜섬웨어를 탐지하기에는 부적합하다.

하지만 신규 랜섬웨어가 파일들을 암호화 한 후 확장자를 변경한다면 탐지할 방법이 있다. 기존의 파일 접근이벤트 필터를 통해 파일이름 중 확장자 이름이 변경 될 경우를 이용한다. 특정 확장자를 지정하는 것이 아닌, 확장자를 변경하는 행위 자체를 이용하는 것이다. 사람에 의해 파일의 확장자가 변경 될 수 있고 랜섬웨어의 프로세스에 의해 확장자가 변경될 수 있다고 가정한다면, 사람의 경우 파일을 클릭하고 이름변경을 클릭해서 자신이 원하는 파일명과 확장자로 변경해야한다. 즉, 사람의 경우 파일의 확장자변경에 일정시간 이상이 소모된다. 그러므로 1개의 파일의 확장자가 변경되는 것은 구별할 수 없지만 2개 이상의 파일에 대해 확장자변경이 일어난 경우 사람에 의한 변경인지 랜섬웨어 프로세스에 의한 변경인지 알 수 있다. 랜섬웨어의 특성상 사용자 모르게 최대한 빨리 파일들을 암호화하기 때문에 잠복기는 존재한다고 해도 시간간격을 두고 암호화를 하진 않는다. 그러므로 파일이 암호화 된 후 파일의 확장자가 변경될 때 짧은 시간 내에 여러 파일의 확장자가 변경된다. 또한, MacOS의 특성상 Windows에 비해 확장자에 따른 기능이 더 명확하게 구분되기 때문에 사용자입장에서는 파일의 이름을 바꿀 때 확장자를 변경하는 경우는 드물다. 그러므로 제안하는 방법은 파일의 확장자 변경이 짧은 시간 내에 두 번 이상 발생 할 경우, 바뀐 후 확장자가 동일하다면 랜섬웨어로 간주한다.

3.2.2 사용자 입력확인을 통한 랜섬웨어 판단

위와 같이 짧은 시간 내에 두 번 이상 파일의 확장자변경 이벤트가 수집되었을 때, 조건에 따라 해당 프로세스를 랜섬웨어 프로세스로 간주한다. 하지만 첫 번째 파일은 암호화가 되고 난 후에 랜섬웨어를 탐지하는 것이므로 최초에 암호화된 파일 한 개는 암호화를 막지 못한다. 이를 해결하기 위해서는 파일의 확장자가 변경되었을 때 사용자 입력이 있는지 확인하면 된다. 사용자가 파일의 확장자를 변경하는 방법은 해당 파일을 마우스로 클릭한 후 이름변경하기를 클릭하고 파일이름 및 확장자를 변경한 후 엔터를 타이핑한다. 또 다른 방법으로는 터미널에서 mv명령어를 통해 파일이름 및 확장자를 수정하고 엔터를 타이핑하는 경우다. 즉, 사용자가 파일의 확장자를 변경하는 이벤트는 사용자의 키보드입력 이벤트를 동반

한다. 특히 엔터키입력 이벤트는 반드시 생긴다.

커널에서 최초 파일이름변경 이벤트를 수집하고 파일 이름이 아닌 확장자가 변경되었을 경우, 키보드의 엔터 이벤트가 발생되었는지를 확인한다. 만약 키보드의 입력이벤트 없이 확장자 변경이 일어났다면 사용자에 의한 변경이 아니기 때문에 랜섬웨어 프로세스로 간주한다.

요약하면, 커널에서 파일의 이름변경 이벤트를 수집 한 경우 확장자가 변경되었는지를 우선 확인한다. 확장자가 변경되었을 경우 확장자 블랙리스트에 있는 확장자로 변경되었는지를 확인한다. 확장자가 블랙리스트에 없는 경우, 확장자를 변경하는 시점에 키보드 엔터키의 입력이벤트가 발생했는지를 확인한다. 사용자입력이 없다면 랜섬웨어로 간주한다. 사용자의 입력이 있더라도 짧은 시간동안 다수의 확장자 변경이벤트가 수집된다면 랜섬웨어 프로세스인지 의심해야 한다. 왜냐하면 랜섬웨어 프로세스에 의해 파일의 확장자가 변경되고 있는 와중에도 사용자는 이를 인지하지 못하고 PC를 계속 사용하고 있기 때문에 충분히 키보드 혹은 마우스 이벤트가 발생할 가능성이 있기 때문이다.

IV. 실 험

MacOS 가상머신환경에서 제안한 방법을 실험했다. 운영체제 버전은 OS X 10.10.5 Yosemite이며, 2.67Ghz의 CPU, 2GB의 메모리를 사용했다.

MacOS에서 기본으로 제공하는 Xcode라는 개발도구를 이용하여 Kernel Extension을 구현하였다. Kernel Extension의 세부기능인 File Operation에서는 기본적으로 파일에 대한 이벤트를 탐지할 수 있는 라이브러리를 제공하고 있기 때문에 이것을 활용하여 파일의 Rename이벤트를 수집했다. 파일의 Rename이벤트는 파일이름과 확장자를 구분하지 않고 파일명이 변경되면 발생하기 때문에 Rename이벤트에서 파싱을 통해 확장자가 변경되었는지 확인한다. 또한, Table 1의 확장자리스트를 저장할 배열을 생성해서 블랙리스트를 등록했다. 블랙리스트는 상황에 따라 추가되거나 제거될 수 있으나 실험목적상 Table 1의 확장자 목록만을 이용하였다.

블랙리스트에 있는 확장자와 동일한 확장자로 파일이 변경된다면 랜섬웨어로 간주하고 해당 프로세스를 차단하는지 실험하기 위해서 실제로 악성행위를 하는 악성스크립트를 제작했다. 파이썬 언어를 이용하여 MacOS의 특정 폴더에서 ".pdf"확장자를 가진 파일만 검색해서 AES암호화 알고리즘으로 암호화 하였다. 암호화가 완료된 파일의 확장자는 ".ecc"로 변경하였고, 실험목적상 복호화가 가능하도록 키를 보관했다. 실제 랜섬웨어의 경우 모든 폴더를 대상으로 타겟파일을 검색하지만 실험목적상 악성스크립트는 구체적인 타겟을 정해서 진행했다. Table 2는 악성스크립트로 ".pdf"확장자를 가진 파일들을 암호화 했을 때 걸린 시간을 나타낸 것이다.

실험에 사용한 ".pdf" 확장자를 가진 파일 1700개는 실제로 사용 중인 파일들이며 크기는 1KB에서 105MB까지 다양하다. 이 파일들을 대상으로 악성스크립트로 암호화를 수행하면 암호화 및 파일 확장자변경에 걸리는 시간은 평균 0.1108초가 소모된다. 가장 늦게 수행되는 시간은 4.6507초가 소모되었다. 그러므로 같은 확장자의 파일이 동일한 확장자로 변경하는 이벤트가 두 번째 발생했을 경우 첫 번째와 두 번째 이벤트의 시간차이가 4.6507초 이하라면 랜섬웨어 프로세스로 의심할 수 있다. 하지만 4.6507초의 시간차이는 사람에 의해서도 충분히 발생할 수 있는 시간이고, 제안하고자 하는 방법은 pdf파일 뿐만 아니라 모든 파일에 대해서 적용 가능해야하기 때문에 단순히 105MB크기의 파일을 암호화 하는데 걸린 시간인 4.6507초를 기준으로 삼기에는 부적절하다. 실제로 문서파일이 100MB가 넘을 경우도 흔하지 않다. 일반적인 경우로 적용하기 위해서 1700개 파일의 암호화 및 확장자변경 소모시간의 평균을 이용했다. 즉, 첫 번째 이벤트와 두 번째 이벤트의 시간차이가 0.1108초 이하일 경우 랜섬웨어 프로세스로 간주하고 차단하도록 했다.

Table 2. Experiment of malicious script file encryption

Target file	pdf
Number of files	1700
Total file encryption time	188.46s
Total file encryption average time to complete	0.1108s
Single file encryption minimum time	0.0033s
Single file encryption maximum time	4.6507s
Minimum file size	1KB
Maximum file size	105.0MB

커널에서의 Rename이벤트 수집뿐만 아니라 유저레벨에서 사용자 입력 이벤트수집도 동시에 진행했다. 사용자입력 이벤트는 커널에서 수집하지 못하기 때문에 유저레벨의 어플리케이션과 소켓통신을 하였다. 사용자가 직접 파일의 확장자를 변경하는 경우 결국 엔터키를 타이핑해야하기 때문에 유저레벨의 어플리케이션에서는 엔터키의 입력이 있는지만 확인했다. 하지만 키보드에서 특정키의 입력이 있는지 확인은 불가능했고 대신 키보드 전체키 중에서 입력이 있는지 없는지와 마우스 좌 클릭, 우 클릭여부만 구별가능했다.

제안한 방법은 유저레벨 어플리케이션에서는 계속 엔터키입력을 확인하고 메시지를 보내서 커널에서 확인하는 것이지만 엔터키만 식별하는 것이 불가능했다. 키보드 전체 키의 입력을 기록하고 커널과 소켓통신을 하기에는 커널에 부담을 주기 때문에 Rename이벤트를 수집한 경우에만 키보드입력이벤트도 수집하도록 했다. 즉, 커널에서 Rename 이벤트가 최초 수집되었을 때 파싱을 통해서 확장자만 변경된 것인지를 먼저 확인한다. 만약 확장자만 변경되었다면 유저레벨의 어플리케이션에 지금부터 0.1108초 동안 키보드 입력여부를 확인하고 그 결과를 소켓통신으로 메시지를 보내도록 한다. Rename이벤트가 한 번 더 수집되고, 확장자만 변경되고, 첫 번째 이벤트와 동일한 확장자로 변경되었다면 시간차이가 0.1108초 이하면서 키보드입력이 없으면 랜섬웨어로 간주하고 해당 프로세스의 파일 접근권한을 차단했다. 프로세스의 파일접근권한을 차단하는 것은 Kernel Extension의 Vnode를 이용했다.

V. 결 론

커널에서 확장자관리를 통해서 충분히 랜섬웨어를 탐지하고 차단 할 수 있음을 확인했다. 하지만 이 방법은 랜섬웨어가 파일을 암호화 한 후 파일의 확장자를 변경한다는 전제하에 가능하다. 해커는 자신의 랜섬웨어가 어떤 파일들을 암호화했는지를 식별하기 위해서 암호화한 파일이 있는 폴더에 추가적으로 파일을 생성함과 동시에 암호화 한 파일들의 확장자를 변경한다. 하지만 작업속도가 더 느려지더라도 암호화된 파일을 식별할 수 있는 파일을 따로 생성하고 파일의 확장자를 바꾸지 않을 수도 있다. 이런 경우는 랜섬웨어가 파일을 암호화 할 때 발생하는 파일 입/출력신호를 이용해서 탐지해야 한다.

또한, 랜섬웨어가 최대한 빠른 시간 내에 자신이 목표로 삼은 확장자의 파일들을 암호화 하지 않고 천천히 암호화를 수행하는 경우에도 위의 방법을 적용하는데 한계가 있다. 하지만 랜섬웨어의 특성상 천천히 파일을 암호화하는 일은 거의 없을 것이다.

파일의 확장자 변경시점을 기준으로 랜섬웨어인지 판단하기 때문에 최초 파일 한 개는 암호화를 막을 수 없다. 대신 커널에서 Rename이벤트를 수집할 때마다 특정 폴더로 자동 백업을 함으로써 암호화가 되더라도 원본으로 대체할 수 있다.

비교적 안전하다고 생각했고, 제조사인 Apple사 또한 안전하다고 주장해왔던 MacOS에서의 랜섬웨어의 등장으로 인해 더 이상 MacOS도 랜섬웨어로부터 안전하지 않다는 것을 알 수 있다. 이러한 상황에서 본 논문에서 제안하는 방법을 이용한다면 앞으로 발생할 랜섬웨어에 대한 위협으로부터 능동적으로 대처가능하다.

References

[1] Jae-yeon Moon, Young-hyun Chang, "Ransomware Analysis and Method for Minimize the Damage", The Journal of the Convergence on Culture Technology pp.79-85, February, 2016

[2] Hyo-mi Nam, Jung-sook Jang, Yong-hee Jeon,, "A Study on the Attack Mechanism Analysis and Countermeasure of Ransomware", Korean Society For Internet Information pp. 283-284, April, 2016

[3] Cabaj, Krzysztof, Piotr, Grochowski, Konrad, Osojca, Dawid, "Network activity analysis of CryptoWall ransomware", PRZEGLAD ELEKTROTECHNICZNY pp.201-204, November, 2015

[4] Ji-yo Park, "A Study on Malicious Behavior Detection of Ransomware in Windows", Department of Information Security, Graduate School of Infromation and Communications, Konkuk University, 2016

[5] Gyeong-sin Kim, Moon-sik Kang, "Next Generation Cyber Security Issues,

Threats and Countermeasures," *The institute of electronics engineers of korea* pp. 69-77, April, 2014

〔6〕 Byng-tae Park, "Security Threat and Response Measures by Ransomware", Department of Electronics and Computer Engineering, Graduate School of Industry, Chonnam National University, 2016

〔7〕 Ji-young Lee, "A Study on Extraction of Ransomware Evidence by Using Forensic Method", Department of Information Security, Graduate School of Dongguk University, 2016

〔8〕 "New OS X Ransomware KeRanger Infected Transmission BitTorrent Client Installer", http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/

〔9〕 "A study on the behavior monitoring ",http://www.riss.kr/search/detail/DetailView.do?p_mat_type=be54d9b8bc7cdb09&control_no=4c2519a94d07172bffe0bdc3ef48d419

〈저자소개〉

윤 정 무 (Jung-moo Youn) 학생회원
2013년 2월: 충남대학교 컴퓨터공학과 졸업
2015년 8월~현재: 충남대학교 컴퓨터공학과 석사과정
〈관심분야〉 정보보호, 시스템보안

류 재 철 (Jae-cheol Ryou) 종신회원
1985년 2월: 한양대학교 산업공학과 졸업
1988년 5월: Iowa State University 전산학 석사
1990년 12월: Northwestern University 전산학 박사
1991년 2월~현재: 충남대학교 컴퓨터공학과 교수
〈관심분야〉 정보보호, 네트워크보안, 암호학, 보안프로토콜