# 파일의 읽기/쓰기 권한 제한을 통한 암호화 랜섬웨어로부터 선택적 파일보호 연구

김재홍*, 나중찬*
*과학기술연합 대학원 대학교
e-mail:jhong3842@ust.ac.kr, njc@etri.re.kr

# A study of restricting read/write permission of the selecitve file from file encryption ransomeware

Jae-hong Kim*, Jung-chan Na*
*Dept of Information Security Enginerring, UNIVERSITY OF SCIENCE AND TECHNOLOGY

요 약

정보화 사회가 도래함에 따라 정보를 가공, 처리 유통하는 활동이 주를 이루고 정보의 가치는 경제적 가치를 창출하는 요소로 연결됐다.. 이와 맞물려 ICT(Information & Communication Technology) 산업이 발전함에 따라 정보를 디지털 데이터 형식으로 저장관리 한다. 이러한 이유로 디지털 정보를 노리는 악성 행위들이 디지털 세상에서 문제가 되고 있다. 그중 사용자의 동의 없이 컴퓨터에 불법으로 설치되어 사용자의 디지털 파일(정보)를 인질로 잡아 금전적인 요구를 하는 악성 프로그램인 랜섬웨어의 피해는 날로 증가하고 있다.[1]. 본 논문에서는 운영체제의 시스템 콜 후킹을 통한 읽기/쓰기 권한을 제한함으로써 다양한 종류의 랜섬웨어 중 파일 암호화 기반 랜섬웨어로부터 사용자가 선택적으로 파일을 보호할 수 있는 방안을 제시하려 한다.

## 1. 서론

랜섬웨어(Ransomware)는 1989년 PC 사이보그사의 에이즈 정보 디스켓을 통한 유포로 시초로 하여 현재까지 꾸준히 발전해 해왔다[2]. 그리고 최근 Tor(익명 네트워크) 기반의 결제 홈페이지와 비트코인으로 결제하는 시스템의 발전으로 수익성이 높아지고 있어 최근 많이 유포되고 있다[1]. 뿐만 아니라 공개와 개인키 방식을 통한 암호화 방식으로 랜섬웨어 제작자가 아니면 파일의 복구는 실질적으로 한계가 있기 때문에 피해는 날로 증가하고 있다. 이러한 랜섬웨어로부터 파일과 컴퓨터를 보호하는 기술, 제품들이 개발되고 있지만 랜섬웨어를 방어하기에는 현재 개발된 기술로는 한계를 가진다. 본 논문에서 제안하는 방식은 랜섬웨어의 근본적인 대안은 아니지만, 보호할 파일을 선택하고 읽기/쓰기 권한을 제한하여 파일암호화 랜섬웨어로부터 파일을 좀 더 효과적으로 보호하는 방안을 제안하려고 한다.

## 2. 관련연구

### 2.1 랜섬웨어

랜섬웨어는 Ransom(몸값)과 Software(소프트웨어)의 합성어이다. 이는 시스템을 잠그거나 데이터를 암호화해서 사용할 수 없도록 한 뒤, 이를 인질로 삼아 금전을 요구하는 악성 프로그램을 뜻한다[1]. 초기 랜섬웨어는 특정 확장자의 파일을 암호가 설정된 압축 파일로 만들어 몸값을 요구하였다. 그 후 세계적으로 랜섬웨어가 유포되었고, 다양한 변종의 랜섬웨어가 출현되고 있다[3]. 랜섬웨어의 종류는 화면 잠금형 랜섬웨어와 파일 암호화형 랜섬웨어로 나눌 수 있다. 화면 잠금형 랜섬웨어는 바탕화면 전체를 사용 불가능하게 만들어 사용자의 불안감을 조성하여 금전을 요구한다[4]. 파일 암호형 랜섬웨어의 경우 비대칭 키 암호화 방식(RSA 2048, AES 256, ECC 알고리즘 등)으로 디지털 기기에 저장되어 있는 각종 문서, 데이터 베이스 등을 암호화 시켜 파일을 복호화하기 위해 금전을 요구한다. 화면 잠금형 랜섬웨어의 경우에는 시스템 복원, MBR 복구 등 복원 가능성이 비교적 높은 편이나 파일 암호형 랜섬웨어는 복구 가능성은 높지 않다.

### 2.2 랜섬웨어로인한 피해량[5][6]

16년 한 해에만 62개의 신종 랜섬웨어가 개발 유포되었고 많은 피해가 발생하였다[5][6]. 국내에서는 '15년에는 2,678건, '16년에는 3,255건으로 랜섬웨어 피해 신고가 증하였다. FBI가 조사한 결과에 따르면 세계적으로 2016년

1~3월 동안 비트코인을 통해 랜섬웨어 복구 지급 금액만 8억 달러, '16년 한 해에는 지급액은 10억 달러 정도로 추정하고 있다. 국내의 랜섬웨어로 인한 피해 규모는 '15년에는 1,090억 원, '16년에는 3,000억 원 정도 피해가 발생한 것으로 추정하고 있다. 그리고 올해('17년)에는 랜섬웨어로 인한 피해는 증가할 것이라고 예상하고 있다.

### 2.3 기존 파일 암호화 랜섬웨어 방어 기술과 한계

#### 2.3.1 시그니처 기반 탐지

기존의 백신에서 일반적으로 사용되는 방법으로 알려진 랜섬웨어의 시그니처(YARA, Pattern matching)을 토대로 랜섬웨어를 판별하는 방법을 사용한다. 하지만 시그니처 기반 탐지는 새로운 유형의 랜섬웨어일 경우 막지 못할 확률이 높다.

#### 2.3.2 행위차단 기법

랜섬웨어의 주요 유포 방법은 인터넷을 통해 유포되는 DBD(Drive By Download)와 이메일 첨부파일, p2p를 통한 방법이 있다[4]. 이를 통해 인터넷 브라우저와 같은 프로세스가 새로운 프로세스를 생성하거나, 파일을 암호화하는 행동을 감시하여 프로세스를 차단하는 행위를 통해서 랜섬웨어를 방지한다. 또한 랜섬웨어의 동작 과정 중 비정상적으로 I/O 행위가 발생하기 때문에 I/O Interval을 확인하여 프로세스를 차단하는 방법도 있다[7]. 그러나 오탐(False Positive)으로 인해 빈번하게 프로세스를 차단하게 되면 오히려 사용자에게 많은 불편을 줄 수 있는 단점이 있다.

#### 2.3.3 자동 백업 시스템

실시간 데이터 백업 기술을 이용해서 MS Office, HWP, PDF, 이미지 파일을 실시간으로 자동 백업하는 방법이다[8]. 이를 통해 랜섬웨어에 감염되더라도 다시 복구하는 방식의 방어 방법이 존재한다. 위와 같은 방법의 경우에는 대용량 데이터도 위와 같은 방식으로 백업하기 때문에 자원의 낭비가 발생하는 문제점이 존재한다.

## 3. 제안하는 선택적 파일의 읽기/쓰기 권한 연구

### 3.1 설계

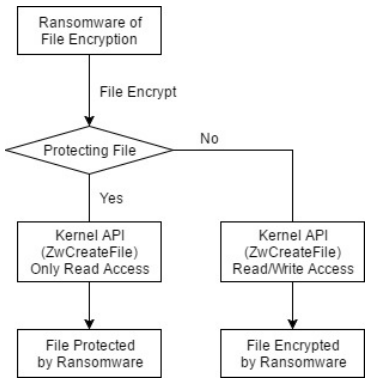
현재까지 다양한 랜섬웨어 방지를 위한 연구가 진행되고 있지만 아직까지 근본적인 대책은 부재한다. 이로 인해 지속적으로 많은 피해가 발생하고 있다. 본 논문에서 제안하는 방식은 모든 파일을 보호하기 어렵다면 중요한 파일만 선택적으로 효율적으로 보호하는 것이다. 선택된 파일의 읽기/쓰기 권한을 제한함으로써 해당 파일을 보호 할 수 있다. 선택된 파일의 경우에 쓰기 권한만 제한하기 때문에 문서를 보거나 재생에 있어서는 불편함이 없다. 만약 문서의 수정이 필요할 경우 해당 제한을 풀고 수정 후 다시 제한하면 된다. 읽기/쓰기 권한 제한을 위해서 운영체제의 파일과 폴더의 Handle을 획득하는 Kernel Mode API(System Call)를 후킹(hooking) 함으로써 구현한다. Kernel Mode API를 후킹 하는 이유는 User Mode에서 Handle을 획득하는 API는 다양하게 존재하기 때문에 관련 API를 모두 후킹하는 작업은 비효율적이다. 또한 읽기/쓰기 권한을 제한하기 어렵기에 Kernel Mode API를 후킹 방법을 사용한다.

### 3.2 동작원리

윈도우 환경에서 ZwCreateFile(Kernel Mode API)의 호출을 통해서 파일에 접근한다. 해당 함수의 원형[그림1]을 확인해본다. 본 연구와 관련된 매개변수를 확인해보면 DesiredAccess 인자의 경우 파일의 접근 권한을 설정하는데 사용된다. 그리고 ObjectAttributes 인자의 경우에는 파일의 이름을 포함하고 있는 객체로서 보호할 파일을 선택할 때 사용된다. 위의 매개변수들을 확인하여 읽기/쓰기 권한과 파일 선택 기능을 구현함으로써 [그림2]와 같은 전체적인 도식화를 그려 볼 수 있다. [그림3]의 경우 후킹한 ZwCreateFile 함수에서 보호하는 파일을 확인하고 읽기/쓰기 권한을 제한하는 부분이다.

```
NTSTATUS ZwCreateFile(
_Out_    PHANDLE            FileHandle,
// A pointer handle of the file
_In_     ACCESS_MASK        DesiredAccess,
// Determines the requested access to the object
_In_     POBJECT_ATTRIBUTES ObjectAttributes,
// Structure of object name
_Out_    PIO_STATUS_BLOCK   IoStatusBlock,
_In_opt_ PLARGE_INTEGER     AllocationSize,
_In_     ULONG              FileAttributes,
_In_     ULONG              ShareAccess,
_In_     ULONG              CreateDisposition,
_In_     ULONG              CreateOptions,
_In_opt_ PVOID              EaBuffer,
_In_     ULONG              EaLength
);
```

[그림1] ZwCreateFile 원형[9]




[그림2] 파일보호 시스템 도식화

```
//Verify the protecting file
if (RtlCompareUnicodeString(ObjectAttributes->ObjectName,
          &ProtectingFile, TRUE) == NULL){
    //If protecting file Access option is write ,
      Change option to Only Read
    if (!(DesiredAccess & GENERIC_WRITE))
    {
        DesiredAccess = FILE_GENERIC_READ | FILE_GENERIC_EXECUTE;
        //CALL Original ZWCREATEFILE
        return ((ZWCREATEFILE)(OrigZwCreateFile))

                                    …
```

[그림3] 후킹한 ZwCreateFile 함수 내부

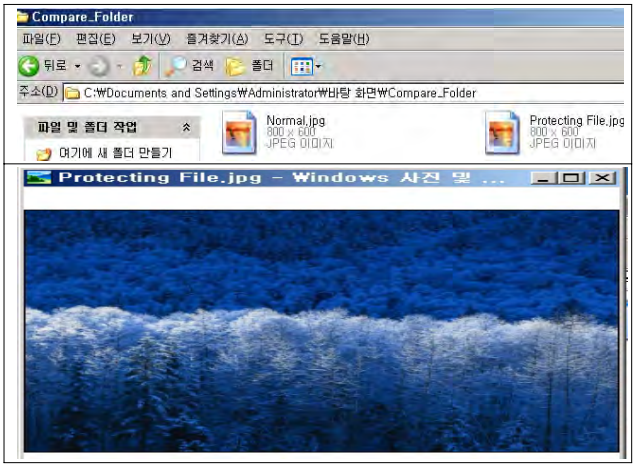
4.3 실험결과

본 실험에서 실제 많이 유포되고 있는 랜섬웨어인 CERBER를 감염, 파일의 감염 유무를 확인하였다. 실험 환경은 [표1]과 같이 구성하였다. Compare_Folder 아래 [표2]와 같이 같은 내용의 이미지를 Normal.jpg (보호되지 않는 파일)과 Protecting File.jpg(보호 중인 파일)구성, CERVER 랜섬웨어를 감염 시켰다. 그 결과 [표3]과 같이 보호되지 않는 파일은 파일 이름과 확장자가 변경되고, 내용 또한 같이 변경되었다. 반면 보호 중인 파일의 경우 이름, 확장자, 내용 모두 랜섬웨어로부터 보호 되었다.

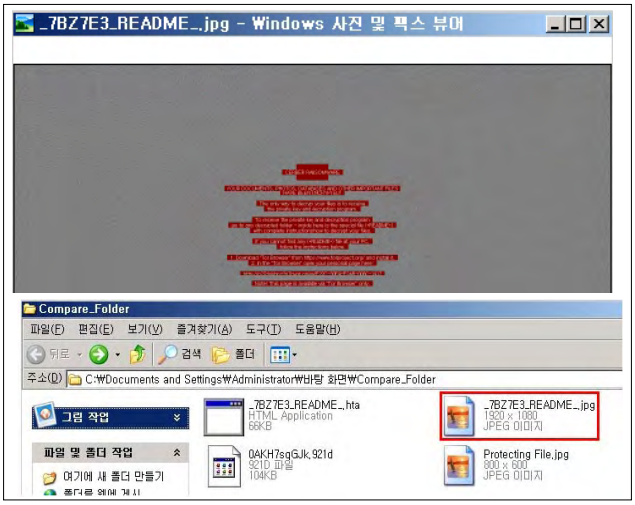
[표1] 실험 환경

| 실험 환경 | |
|---|---|
| OS | Windows XP 32bit |
| 랜섬웨어 파일 | CERBER Ransomware[10] |
| 보호할 파일 | Protecting File.jpg |

[표2] 랜섬웨어 감염전




[표3] 랜섬웨어 감염 후




## 5. 결론

랜섬웨어로 인한 피해는 최근 급속히 증가하였다. 그리고 앞으로도 많은 피해가 발생할 것이라는 의견이 지배적이다. 이러한 위협에 대응하고자 선택적으로 파일의 읽기/쓰기 권한 제한을 통한 대응책을 제시하였다. 이를 통해 랜섬웨어로부터 선택된 파일의 보호할 수 있음을 증명하였다. 하지만 보호 파일을 선택하고 수정할 때 사용자의 번거로움의 문제점이 예상된다. Kernel Mode API를 후킹하였기 때문에 백신과의 충돌이 발생하는 문제점도 예상된다. 앞으로의 연구에서는 위와 같은 문제점을 개선하는 방식으로 진행되어야 한다.

## 참고문헌

[1] 나무위키, 랜섬웨어
https://namu.wiki/w/%EB%9E%9C%EC%84%AC%EC%9B%A8%EC%96%B4

[2] KISA, 국내 타깃 랜섬웨어의 현황 및 대응방법
http://www.cisokorea.org/data_file/board/%EA%B5%AD%EB%82%B4%20%ED%83%80%EA%B9%83%20%EB%9E%9C%EC%84%AC%EC%9B%A8%EC%96%B4%EC%9D%98%20%ED%98%84%ED%99%A9%20%EB%B0%8F%20%EB%8C%80%EC%9D%91%EB%B0%A9%EC%95%88.pdf, 2015. 05

[3] TREND MICRO, 랜섬웨어 정의 및 종류
http://www.trendmicro.co.kr/kr/security-intelligence/ransomware/definition/index.html

[4] HAURI, [보안정보] 알기쉬운 랜섬웨어
http://www.hauri.co.kr/information/notice_view.html?intS

eq=179, 2015. 11
[5] 한국랜섬웨어침해대응센터, 2017 랜섬웨어 침해분석 보고서
http://img.innotium.com/newsletter/rans_201702/rancert_analysis_report_1702.pdf, 2017. 02

[6] KISA, '16년 랜섬웨어 동향 및 '17년 전망
https://www.krcert.or.kr/filedownload.do?attach_file_seq=979&attach_file_id=EpF979.pdf, 2017. 01

[7] 윤정무 (2016). "파일 I/O Interval을 이용한 랜섬웨어 공격 차단 방법론" 한국정보보호학회 제26권 제3호, pp 649-650.

[8] 한국랜섬웨어침해대응센터. 랜섬웨어 방어 솔루션
https://www.rancert.com/barzakook.php

[9] MSDN, ZwCreateFile routine
https://msdn.microsoft.com/en-us/library/windows/hardware/ff566424(v=vs.85).aspx

[10] MALWARE-TRAFFIC-ANALYSIS, CERVER RANSOMWARE
http://malware-traffic-analysis.net/2016/12/29/index.html, 2016, 12

[Acknowledgement]
이 논문은 2017년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2016 M2A8A4952280).