

랜섬웨어 대응 가이드라인

2019. 5



연세대학교
학술정보원 정보보안팀

※ 본 가이드는 한국인터넷진흥원(KISA)의 [랜섬웨어 대응 가이드라인]을 인용하였음.

목 차

1. 랜섬웨어란?

- 가. 랜섬웨어란 무엇인가?
- 나. 랜섬웨어 감염 경로와 증상
- 다. 주요 랜섬웨어

2. 랜섬웨어 사전 예방

3. 랜섬웨어 감염 시 대응절차

- 가. 증상 확인하기
- 나. 피해 최소화를 위한 긴급 조치
- 다. 신고하기
- 라. 데이터 복구하기

1. 랜섬웨어란?

가. 랜섬웨어란 무엇인가?

1) 랜섬웨어(Ransomware)는 이용자의 데이터(시스템파일 문서 이미지 동영상 등)를 암호화하고 복구를 위한 금전을 요구하는 악성코드임

※ 랜섬웨어는 악성코드의 일종이나, 다른 악성코드와 달리 감염된 시스템을 암호화시키는 특성을 가짐

몸값(Ransom)과 소프트웨어(Software)의 합성어로 시스템을 사용 불가능한 상태로 변경하거나 데이터를 암호화해 사용할 수 없도록 하고 이를 인질로 금전을 요구하는 악성 프로그램

※ 감염 후, 랜섬웨어는 공유 폴더 및 기타 접근 가능한 시스템(클라우드 서버, USB, 외장 하드 등)으로 확산을 시도

< 일반 악성코드와 랜섬웨어의 차이점 >

구분	일반 악성코드	랜섬웨어
유포	웹사이트, 이메일, 네트워크 취약점 등 유포방식 동일	
감염	SW 취약점 또는 피해자의 실행으로 악성코드 감염 동일	
동작	정보 및 파일 유출, DDoS 공격 등	문서, 사진, MBR 등 데이터 암호화
치료	백신 등을 통해 악성코드 치료	백신 등을 통해 악성코드 치료 → 암호화된 파일은 복구 어려움
피해	개인, 금융 정보 유출 및 이를 이용한 2차 공격으로 피해 발생	암호화된 파일에 대한 복호화를 빌미로 가상통화(비트코인 등)로 금전을 요구

2) 랜섬웨어 공격 절차

- 감염 경로에 접속 → PC로 랜섬웨어 다운로드 및 랜섬웨어 실행 → 암호화 대상 (문서 파일, 이미지 등) 검색 및 암호화 → 복호화 대가 요구



나. 랜섬웨어 감염 경로와 증상

- 1) 홈페이지 이메일을 통해 유포되던 방식에서 불특정 다수를 감염시키는 웹 형태와 해킹을 통해 감염시키는 타깃형 공격으로 진화
- 2) **감염방식**: 보안이 취약한 웹사이트 악용, 사회공학적 기법(이메일, SNS, 첨부파일실행, 파일공유사이트 등) 활용, 보안설정이 미흡한 유·무선 네트워크 악용 해킹을 통해 직접 침투/실행 등

- **이메일**: 랜섬웨어를 유포하는 파일이 첨부되어 있거나 다운로드 할 수 있는 URL 링크를 포함
 - ※ 메일이 스팸인지 구별되지 않을 만큼 정교한 경우가 대부분이며, 신뢰할만한 기관이나 대상을 사칭하기도 함. 첨부파일이 실행파일, 그림파일 등인 경우가 많음
- **취약점 악용**: 보안이 취약한 웹사이트 커뮤니티에 접속 시 PC내 운영체제 응용프로그램의 취약점을 이용하여 랜섬웨어를 다운로드하고 실행하도록 함
 - ※ 플래시플레이어, 아크로뱃 리더, 인터넷 익스플로러, 실버라이트, 자바 등
- **파일공유사이트**: 파일공유 사이트에는 랜섬웨어를 포함한 위장 파일(영화 사진 프로그램 등)이 존재하며 이러한 파일을 다운로드하여 실행하면 감염
- **네트워크전파**: 유 무선 네트워크 설정 미흡으로 인해 랜섬웨어 확산 및 감염

· 윈도우즈 운영체제 로그인 계정 비밀번호가 단순하거나 예측이 가능한 경우 암호 사전대입공격 방식으로 감염(예: 배드래빗(Bad Rabbit) 랜섬웨어)

· 최신 보안 패치가 적용되지 않은 윈도우즈 운영체제의 SMB 원격코드 실행 취약점을 악용하여 감염(예: 워너크라이(WannaCry) 랜섬웨어)

※ SMB(Server Message Block): 도스나 윈도우즈에서 파일이나 디렉토리 및 주변장치들을 공유하는데 사용되는 메시지 형식

· 공유기나 네트워크 스위치로 업무망을 구성한 경우, 업무망 내 공유기·스위치·시스템 등에 설정한 사용자 계정에 동일한 비밀번호를 사용하면 이를 악용하여 원격 접속 및 랜섬웨어 감염 발생

- **사회관계망**: 유명인 계정을 해킹하거나 단축 URL 등을 사용하여 랜섬웨어 유포
- **스미싱**: 스마트폰을 이용 문자 메일 등 한 랜섬웨어 유포
- **이동식 저장장치**: 이동식 드라이브(USB) 자동실행기능을 악용해서 PC에 연결할 때 마다 랜섬웨어 감염

- 3) **감염증상**: 파일 암호화(문서, 이미지, 서버파일, DB 등), 화면 잠금(PC 또는 스마트폰 잠금), 부트영역 암호화(PC 재부팅 불가) 등

- 기존 악성코드와 감염 방법 및 유포 경로는 동일하나, 암호화 기능을 통해 사용

자의 주요 파일을 사용 불능 상태로 변환

- 높은 수준의 암호화 방식(RSA-2048, AES-256 등)을 악용하고 있어 복구키가 없는 한 사실상 복구 불가능
- 운영체제 시동·시작을 위한 디스크 영역을 암호화하여 운영체제 시작이 불가능
- 윈도우즈 운영체제에서 제공하는 파일 백업 및 복원 기능을 무력화하기도 함

4) **금전요구:** 개인 및 기업의 중요한 파일을 암호화한 후 파일 복구를 빌미로 비트코인 등 금전을 요구

다. 주요 랜섬웨어

종류	감염경로	특징	감염파일 확장자
로키 (Locky)	이메일 취약 홈페이지 접근 P2P다운로드 위장 파일	사용자가 인지하지 못하는 네트워크 경로를 찾아 데이터를 암호화	locky, lukitus, diablo6, osiris, zzzzzz, aesir, shit, thor, odin
테슬라크립트 (TeslaCrypt)	이메일 취약 홈페이지 접근	200MB이상의 파일은 손상시키지 않음 키를 공개하여 복호화 가능	ecc, ezz, exx, aaa, abc, ccc, micro, mp3
케르베르 (Cerber)	이메일 취약 홈페이지 접근	음성을 통해 암호화 사실을 전달	cerber 랜덤 4자리 문자
비너스락커 (Venus Locker)	이메일	감염사실을 알리기 위해 바탕화면 변 경 모든 폴더에 랜섬노트 생성	venusp, venusf
워너크라이 (WannaCry)	공유폴더(SMB) 접속	특정 도메인 접속 성공 시 미동작하 는 킬스위치 기능 보유	WNCRYT, WNCRY
에레버스 (Erebus)	이메일	감염사실을 알리기 위해 모든 폴더에 랜섬노트 생성	ecrypt
크립토락커 (CryptoLocker)	이메일 취약 홈페이지 접근	시스템 자체 백업본 삭제 후 동작	encrypted
크립토월 (Cryptowall)	이메일 취약 홈페이지 접근	감염 확장자 변조 없음 파일의 고유 서명 값 위변조	-
올크라이 (AllCry)	웹하드 설치 프로그램	네트워크 연결 시 악성행위 동작 감염 정보를 알리기 위해 다국어(영 어/중국어/한국어) 지원	allcry
크립트XXX (CryptXXX)	이메일	브라우저, 메일, 쿠키, ftp 계정 등 사용자 정보 탈취	crypt
배드래빗 (Bad Rabbit)	공유폴더(SMB) 접속	Windows SMB 취약점에 의해 네트 워크를 통해 전파 MBR 변조를 통해 운영체제 부팅 불가	encrypted

종류	감염경로	특징	감염파일 확장자
매그니버 (Magniber)	이메일 취약 홈페이지 접근 P2P 다운로드 파일	모든 폴더에 한국어로 작성된 랜섬노 트 생성	ihsdj, iupguiqm, kgpvwnr, fprgpk, ymdmf, vbdrj
페트야 (Petya)	이메일 네트워크 전파	MBR 변조로 인한 운영체제 부팅 불가	-

2. 랜섬웨어 사전 예방

- 가. 모든 소프트웨어는 최신 버전으로 업데이트하여 사용(자동 업데이트 설정 권고)
- 1) 보안업데이트가 제공되는 최신 버전의 운영체제 사용 및 매달 발표되는 보안 업데이트 적용
 - 2) 직접적인 공격수단인 인터넷 익스플로러(Internet Explorer)가 아닌 마이크로소프트 엣지(Edge), 구글 크롬(Chrome), 모질라 파이어폭스(Firefox) 등 다른 브라우저 사용
 - 3) 브라우저, 자바, 플래시 플레이어, 아크로뱃리더 등 사용하고 있는 소프트웨어를 항상 최신 버전으로 유지
 - 4) 그 외 응용소프트웨어에서 업데이트를 제공하는 경우 즉시 적용
 - 5) 사용하지 않는 불필요한 소프트웨어는 삭제

나. 백신 소프트웨어를 설치하고, 최신 버전으로 업데이트

- 1) 최신 업데이트를 유지하고 실시간 감시 이용기능 활성화 등 백신 소프트웨어가 정상적으로 동작하도록 설정
- 2) 주기적으로 PC 악성코드 검사 수행

다. 출처가 불명확한 이메일과 웹사이트 주소(URL)는 실행하지 않기

- 1) 수상한 이메일 열람과 첨부파일 실행
- 2) 이메일에 첨부되어 있는 MS오피스 파일의 매크로 기능 허용하지 않음
- 3) 이메일에 첨부되어 있는 스크립트(JS, JAVA 등)나 실행파일(EXE, SCR, VBS 등)은 실행하지 않음
- 4) 파일 공유 사이트 등에서 파일 다운로드 및 실행에 주의

라. PC내 중요 자료는 정기적으로 백업

- 1) 업무 및 기밀문서 각종 이미지 등 중요파일은 주기적으로 백업
- 2) 특히 중요 파일은 PC외에 외부 저장장치 등을 이용한 2차 백업을 하거나 보안백업 SW 등을 통해 쉽게 접근하기 어렵도록 설정

3. 랜섬웨어 감염 시 대응절차

가. 증상 확인하기

- 1) **파일 사용불가**: 평소 문제없이 열렸던 문서, 사진, 그림, 음악, 동영상 파일들 중 일부 혹은 전체가 읽을 수 없게 되거나 열리지 않는 현상이 발생
- 2) **파일 확장자 변경**: 평소 아무 문제없이 사용하던 파일의 이름과 확장자가 바뀌거나 파일 확장자 뒤에 특정 확장자가 추가된 것을 볼 수 있음
- 3) **부팅 불가능**: 평소 사용하던 운영체제로 부팅이 되지 않고, 랜섬웨어 감염 사실 및 금전요구 화면을 볼 수 있음
- 4) **바탕화면 변경 및 감염 알림 창**: 사용자의 파일이 암호화되었음을 알리고 이를 해제하기 위한 비용과 지불할 방법을 보여주는 안내창을 볼 수 있음

나. 피해 최소화를 위한 긴급 조치

- 1) **외부 저장장치 연결 해제**: 랜섬웨어는 공유폴더, PC에 연결되어 있는 이동식 저장장치(USB)나 외장하드 등에 저장되어 있는 파일에도 접근해서 암호화할 수 있기 때문에 기존에 백업해둔 파일까지 암호화 될 수 있음
※ 랜섬웨어에 따라 내부망 전파도 될 수 있으니 외부 저장장치뿐만 아니라 네트워크 연결도 해제해야 함
- 2) **PC 전원 유지**: 경우에 따라 PC가 종료된 경우 부팅까지 불가능하게 되는 경우도 있으므로 PC의 전원은 끄지 말 것
- 3) **네트워크 차단**: 네트워크를 통해 랜섬웨어가 확산 될 가능성이 있으므로, 감염 사실 확인 즉시 네트워크 차단
- 4) **복구 방법 확인**: 랜섬웨어의 유형 파악(감염 알림 창, 암호화된 파일 등) 후, 백신소프트웨어 제조사 홈페이지 등을 통해 제공하는 복구 툴이 있는지 확인

다. 신고하기

- 1) **증거 남기기**: 감염 알림창과 암호화 된 파일이 생성된 화면 캡처 및 저장
- 2) **신고하기**: 학술정보원 정보보안팀(내선 6476) 및 관련기관에 해당 사항을 신고하고 남겨놓은 증거물(캡처파일)을 제출

* 관련기관: 한국인터넷진흥원 사이버민원센터(☎118, boho.or.kr)

경찰청 사이버안전국(☎02-3150-2659, cyber.go.kr)

라. 데이터 복구하기

- 1) 랜섬웨어에 의해 암호화되지 않은 PC 또는 이동식 저장장치(USB)에 데이터 백업하기
- 2) PC 포맷 및 운영체제 재설치, SW 최신 보안 업데이트 적용
- 3) 기존 백업매체 연결 및 데이터 복구
- 4) 랜섬웨어 복구도구 활용
 - 보안업체나 노모어랜섬(www.nomoreransom.org) 홈페이지 등에서 일부 랜섬웨어에 대한 복구도구를 제공하지만 모든 파일 또는 암호화키에 대한 복구가 아닌 부분적인 복구를 지원
- 5) 추후 암호화된 파일 및 시스템을 복구할 수 있는 도구가 제공될 경우를 대비하여 감염된 랜섬웨어의 정확한 유형과 감염된 디스크 및 저장장치를 보관하고 있어야 복구 확률을 높일 수 있음