랜섬웨어 대응 가이드라인

2018. 2.

과학기술정보통신부

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

목 차

1. 개 요

□ 랜섬웨어로 인한 국내 피해 예방을 위해, 랜섬웨어 감염피해 사전 예방 및 감염 후 대응절차 등의 대국민 안내체계 마련

o **(랜섬웨어 바로알기)** 랜섬웨어의 특징과 감염 증상 등을 안내

- 랜섬웨어가 무엇인지, 감염 경로와 증상, 유형, 피해사례 등을 소개

o **(예방방안 안내)** 랜섬웨어 감염피해 예방을 위한 보안수칙 안내

- 파일 복구가 어려운 랜섬웨어의 특성을 고려한 예방수칙(중요파일 백업, 주요SW 업데이트, 파일 다운로드 실행 주의 등) 안내

o **(대응요령 안내)** 감염된 랜섬웨어 종류·특징 확인, 감염 PC 격리, 신고절차, 해커 협박 시 대응절차 등 랜섬웨어 추가 피해 방지를 위한 대응요령 안내

- 피해자가 감염증상(파일 확장자, 감염메시지, 랜섬노트 등)에 따른 랜섬웨어 종류를 직접 파악 가능하도록 주요 랜섬웨어 특징 안내

- 랜섬웨어 감염으로 인한 파일 암호화, 해커 협박 등 피해 발생 시 사이버침해 대응기관(KISA, 경찰 등) 신고를 통해 복구가능 여부파악, 피해 감소방안 확인 등 신고 절차 안내

- 감염 PC와 연결된 다른 PC나 저장장치에 대한 추가 피해방지를 위한 격리조치 방법 안내

- 파일 복구를 위한 금전 지불에도 복구를 보장받지 못하는 경우를 고려한 해커 협박 대응을 위한 고려사항 등 안내

2. 랜섬웨어란?

가. 랜섬웨어란 무엇인가?

o 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

< 정 의 >

랜섬웨어(Ransomware)란?

Ransom(몸값) + Software(소프트웨어) 의 합성어

시스템을 잠그거나 데이터를 암호화해 사용할 수 없도록 한 뒤, 이를 인질로 삼아 **금전을 요구하는 악성 프로그램**

- 1989년 최초의 랜섬웨어 AIDS를 시작으로 유행하기 시작했으며 국내의 경우 2015년 크립토락커(Cryptolocker) 한글버전이 유포되면서 본격적으로 사회문제가 됨

※ 랜섬웨어 대부분은 윈도우즈 운영체제를 설치한 컴퓨터를 감염시키지만, 안드로이드(Android) 스마트폰이나 맥(Mac) 운영체제가 설치된 시스템에도 감염사례가 발견되기도 함

- 랜섬웨어가 지정한 기간 내에 금전 지불 등 요구사항을 처리하지 않으면 요구 금액이 증가할 수 있고 감염 시스템과 암호화된 데이터는 사용할 수 없거나 삭제될 수 있음

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

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**
대응	악성코드유포지 및 명령조정지(C&C)*서버 주소 차단 ※ C&C : 해커가 악성코드에 감염된 PC에 원격으로 접속하기 위한 서버·PC로 악성코드 감염 시 C&C에 연결되어 해커의 명령을 수행	악성코드유포지 및 명령조정지(C&C)서버 주소 차단 ※ 복호화 키가 저장된 서버(도메인/IP)와의 통신 경로는 미차단
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**

< 일반 악성코드와 랜섬웨어의 차이점 >

o 랜섬웨어 공격 절차

< 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

o 홈페이지, 이메일을 통해 유포되던 방식에서 불특정 다수를 감염시키는 웜 형태와 해킹을 통해 감염시키는 타깃형 공격으로 진화

o **(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 PC內 운영체제·응용프로그램의 취약점을 이용하여 랜섬웨어를 다운로드 하고 실행하도록 함

  ※ 플래시플레이어, 아크로뱃리더, 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 內 공유기·스위치·시스템 등에 설정한 사용자 계정에 동일한 비밀번호를 사용하면 이를 악용하여 원격 접속 및 랜섬웨어 감염 발생

- **(사회관계망)** 유명인 SNS 계정을 해킹하거나 단축 URL 등을 사용하여 랜섬웨어 유포

- **(스미싱)** 스마트폰을 이용(문자, 메일 등)한 랜섬웨어 유포

- **(이동식 저장장치)** 이동식 드라이브(USB) 內 자동실행기능을 악용해서 각 PC에 연결할 때 마다 랜섬웨어 감염

구 분	홈페이지 방문	이메일·SNS 유포	웜(자가전파)	타깃형(APT) 공격
감염방법	랜섬웨어가 유포중인 홈페이지 방문	첨부 파일 다운로드·링크 실행시 감염	컴퓨터 부팅시 자동 감염	서버 침투 및 악성코드 설치
감염원인	운영체제 등 SW 취약점 존재	이용자 주의 부족 (출처가 불분명한 메일의 첨부파일 실행 등)	운영체제, 네트워크 등 SW 취약점 존재	보안관리 수준 취약
감염사례	크립트락커, 케르베르, 크립트XXX 등	올클라이, 록키, 비너스락커 등	워너크라이, 페트야, 배드레빗 등	에레버스 등

< 랜섬웨어 감염 경로 >

o (**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 사용자의 주요 파일을 사용 불능 상태로 변환

- 높은 수준의 암호화 방식(RSA-2048*, AES-256** 등)을 악용하고 있어 복구키가 없는 한 사실상 복구 불가능

* RSA: 큰 수에 대한 소인수 분해의 어려움을 기반으로 한 비대칭키(공개키) 암호화 알고리즘의 하나로, 암호화뿐만 아니라 전자서명이 가능한 알고리즘

** AES: 고급 암호화 표준(Advanced Encryption Standard)의 약자이며 기존에 사용하던 데이터 암호화 표준(DES: Data Encryption Standard)을 보다 더 강력한 암호화 알고리즘으로 대체하기 위해 2001년에 선정 된 대칭키 암호화 알고리즘

- 운영체제 시동·시작을 위한 디스크 영역을 암호화하여 운영체제 시동·시작이 불가능

- 볼륨 섀도 복사본*을 삭제해서 윈도우즈 운영체제에서 제공하는 파일 백업 및 복원 기능을 무력화하기도 함

* 볼륨 섀도 복사본(Volume Shadow Copy) : 윈도우즈 운영체제 복구를 위해 사용되는 특정 시각의 파일 및 폴더, 주요 시스템파일 등의 복사본

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

- 익명성이 보장된 가상통화(비트코인·이더리움 등)와 토르(Tor)* 네트워크를 이용하여 몸값을 요구하고 있어 해커 추적이 매우 어려움

* 가상 회선을 만들고 암호 통신을 적용함으로써 인터넷에서 익명성을 보장하는 소프트웨어

다. 랜섬웨어 유형 (붙임 참조)

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, zzzzz, 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 변경 모든 폴더에 랜섬노트 생성	venusp, venusf
워너크라이 (WannaCry)	공유폴더(SMB) 접속	특정 도메인 접속 성공 시 미동작하는 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(영어/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 네트워크를 통해 전파 MBR 변조를 통해 운영체제 부팅 불가	encrypted
매그니버 (Magniber)	이메일 취약 홈페이지 접근 P2P 다운로드 파일	모든 폴더에 한국어로 작성된 랜섬노트 생성	ihsdj, iupgujqm, kgpvwnr, fprgpk, ymdmf, vbdrj
페트야 (Petya)	이메일 네트워크 전파	MBR 변조로 인한 운영체제 부팅 불가	-

< 주요 랜섬웨어 >

라. 랜섬웨어 피해 사례

< 최근 국내외에 전파된 랜섬웨어 사례 >

☑ 전세계를 강타한 워너크라이(WannaCry) 랜섬웨어('17.5)

o 영국 국립 의료기관, 러시아 내무부, 스페인 통신업체 및 중국 출입국관리소 등 全 세계 150개국 30만대 감염

o MS 윈도우 운영체제의 취약점*을 악용하여 인터넷상에서 **스스로 복제·전파(웜방식)** 됨에 따라 전 세계에 다량 확산

* SMB(Server Message Block) : 파일·장치를 공유하기 위해 사용되는 통신 프로토콜

☑ 국내 호스팅社를 타겟으로한 에레버스(Erebus) 랜섬웨어('17.6)

o 호스팅 업체('인터넷나야나') 내부 서버를 해킹 한 후 랜섬웨어를 감염시켜 150여대 서버(5,000여개 홈페이지)에서 피해발생

* 서버 접근권한 탈취 ⇨ 랜섬웨어 감염 ⇨ 백업장치 파괴 ⇨ 파일 암호화

o 기업 내부의 보안허점을 정밀 공격하는 **APT(Advanced Persistent Threat)** 공격기법과 랜섬웨어가 결합된 형태

☑ 우크라이나 정부를 타겟으로한 페트야(Petya) 랜섬웨어('17.6)

o 우크라이나 정부에서 주로 사용하는 회계 SW 메독(Medoc)의 업데이트 서버를 해킹하고 이를 통해 랜섬웨어 전파 ☞ **파일 다운로드 시 감염**

o 메독 업데이트 서버를 통해 유포된 랜섬웨어가 **웜방식**으로 확산되어 러시아, 프랑스, 독일, 미국 등에서 감염 사례 발생

☑ **한국을 타겟으로한 올크라이(AllCry), 마이랜섬 랜섬웨어('17.10)**

o 해킹을 통해 랜섬웨어가 삽입된 국내 웹하드 설치파일 등을 통해 올크라이 유포, 국내 1,600여 PC 피해 ☞ **파일 다운로드 시 감염**

o 인터넷 브라우저 등의 **취약점을 악용**하여 한국어 버전의 운영체제 사용자를 공격하는 변종 **마이랜섬**이 발견

3. 랜섬웨어 사전 예방

가. 랜섬웨어 피해 예방 수칙

< 랜섬웨어 예방 5대수칙 >

o 모든 소프트웨어는 최신 버전으로 업데이트하여 사용(자동 업데이트 설정 권고)

- 보안업데이트가 제공되는 최신 버전의 운영체제 사용 및 매달 발표되는 보안 업데이트 적용

※ 윈도우즈 XP·비스타 등 보안 지원이 중단된 운영체제는 최신 버전으로 교체

- 직접적인 공격수단인 인터넷 익스플로러(Internet Explorer)가 아닌 마이크로소프트 엣지(Microsoft Edge), 구글 크롬(Google Chrome), 모질라 파이어폭스(Mozilla Firefox) 등 다른 브라우저 사용

- 브라우저, 자바, 플래시 플레이어, 아크로뱃리더 등 사용하고 있는 소프트웨어를 항상 최신 버전으로 유지

- 그 외 응용소프트웨어에서 업데이트를 제공하는 경우 즉시 적용

- 사용하지 않는 불필요한 소프트웨어는 삭제

- 국내 주요 백신 소프트웨어에서 제공하는 'SW 원클릭 안심 서비스' 활용

※ 사용자 PC에 설치되어 있는 ActiveX의 버전을 확인하여 최신 업데이트를 권고하는 서비스

※ 확인 가능한 소프트웨어(14종): JAVA, Flash Player, Adobe ODF, Chrome, Firefox, Opera, 한컴오피스, 곰플레이어, 팟플레이어, KM플레이어, 알툴즈, Internet Explorer, Microsoft Office, ActiveX

o 백신 소프트웨어를 설치하고, 최신 버전으로 업데이트

- 최신 업데이트를 유지하고 실시간 감시 이용기능 활성화 등 백신 소프트웨어가 정상적으로 동작하도록 설정

- 주기적으로 PC 악성코드 검사 수행

o 출처가 불명확한 이메일과 웹사이트 주소(URL)는 실행하지 않기

- 수상한 이메일 열람과 첨부파일 실행, URL 클릭을 자제

- 이메일에 첨부되어 있는 MS오피스(DOC, XLS 등) 파일의 매크로 기능 허용하지 않음

- 이메일에 첨부되어 있는 스크립트(JS, JAVA 등)나 실행파일(EXE, SCR, VBS 등)은 실행하지 않음

o 파일 공유 사이트 등에서 파일 다운로드 및 실행에 주의

※ 공짜 사이트는 악성코드의 온상임을 기억

o PC內 중요 자료는 정기적으로 백업

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

※ 보안백업 SW는 정상적인 이용자 인증을 수행해야 특정 폴더 및 파일에 접속 가능

나. 기업환경을 고려한 예방수칙

o 보안사고 대응 및 비즈니스 연속성 계획 마련

- 기업 내부의 랜섬웨어 위협을 격리 및 제거하고 데이터 복구와 시스템 정상 동작을 복원하기 위한 비즈니스 연속성 계획을 마련

※ 신·변종 랜섬웨어 동향 파악, 대응책 마련 및 적용 등

- 조직은 백업 계획, 재해 복구 계획 및 비즈니스 연속성 절차를 유지하고 정기적으로 테스트해야 함

※ 백업망은 별도 구축하고 망구성 및 접근통제 설정이 잘못되는 경우 잠재적 위협에 노출될 수 있으므로 주기적 점검 실시 등

- 망 분리를 적용한 기업의 경우, 인터넷PC에서 인터넷으로부터 다운로드하는 데이터(모든 종류의 프로그램, 파일 등)의 저장을 금지하기 위한 기술적·관리적 방안을 강구해야 함

※ 인터넷과 업무망을 분리 구축하고 망연계 접점의 접근통제를 강화, 인터넷 감염을 통한 업무망 피해 확산 차단 등

o 랜섬웨어 감염을 최소화하는 예방법 안내

- **(시스템 보호환경 구축)** 서버 백신·접근통제SW 등 서버 보안제품을 도입, 악성코드 감염 및 데이터 위·변조 행위 차단
- **(취약점 관리 및 패치)** 운영체제, 웹브라우저, 브라우저 플러그인 및 응용 프로그램의 소프트웨어 취약점에 대해 패치하는 것이 중요

- **(실행코드 제어)** 허가되지 않은 코드(워드파일의 매크로 실행 등)의 실행 방지 및 관리자 승인 없이 사용자가 SW설치 금지 등

- **(웹 브라우저 트래픽 필터링)** 보안정보(사용자가 많이 방문하는 사이트 분류정보, 평판 정보 등)를 활용하여 불명확한 사이트 접근차단 등 필터링

- **(이동식 매체 접근 통제)** 이동식 매체의 사용 제한, 공식적인 이동식 매체 발급, 이동식 매체에 대한 악성코드 검사 및 자동실행 기능 비활성화 등

※ 기업內 조직(부서) 단위로 백업전용 이동식 저장매체를 최소화하여 지정·운용하되 반드시 이동식 저장매체 관리대장(또는 관리시스템)에 등록하고 관리

- **(스팸메일 차단)** 메일 보안 솔루션 도입 등을 통해 악성코드가 첨부 된 스팸메일의 내부 유입 차단

o **랜섬웨어 공격 제한 방법**

- **(접근통제)** 관리자의 경우 이메일 및 웹 브라우저 사용을 주의하고 랜섬웨어 감염 시 확산되지 않도록 공유 네트워크 드라이브에 대한 사용권한을 정기적으로 재평가 할 것

- **(데이터백업)** 정기적인 데이터 백업에 대한 지침 제공

※ 백업 자료에 대해 정기적으로 실전 복구 테스트를 반드시 실시, 자료 정상복구 여부를 확인

o **랜섬웨어 피해 예방을 위한 자가 체크리스트(점검 목록)**

① **(데이터백업)** 모든 중요 정보를 별도의 저장장치에 백업하는가? 랜섬웨어 감염시 백업된 자료로 복구할 준비가 되어 있는가?

①-1. **(복원지점생성)** 운영체제 복원지점을 주기적으로 생성하고 있는가?

①-2. **(권한설정)** 사용자에게 파일 쓰기 권한 등 불필요한 권한이 해제 되어 있는가?

② **(위험 분석)** 조직의 사이버 보안 위험 분석을 수행 했는가?

③ **(직원 교육)** 사이버 보안 우수 사례에 대한 직원 교육을 받았는가?

※ 랜섬웨어 감염예방 대책 및 감염의심시 행동요령 등 보안대책을 수립하고 교육 등을 통해 전직원이 숙지토록 조치

④ **(취약점패치)** 알려진 취약점에 대한 적절한 패치를 했는가?

⑤ **(화이트리스트)** 승인된 프로그램만 네트워크에서 실행할 수 있는가?

⑤-1. **(네트워크 설정)** 무선 인터넷 암호 설정, 네트워크 공유 폴더 설정 등을 알맞게 설정했는가?

※ 공유폴더 삭제 및 SMB 포트(UDP/137·138, TCP/139·445) 차단 등

⑥ **(사고 대응)** 침해사고 대응 계획이 있고 그렇게 실행 하는가?

⑦ **(비즈니스 연속성)** 특정 시스템 없이 비즈니스를 운영할 수 있는가? 얼마나 오랫동안 이것을 테스트 하는가?

⑧ **(침투테스트)** 해커의 공격을 방어하는 능력을 점검하는 모의 침투 테스트를 계획하고 실행하는가?

다. 중요한 데이터 백업하기

o 중요 파일에 대한 백업을 통해 랜섬웨어 감염 피해를 최소화해야 함

- 백업에 사용하는 장비는 매체 백업 시에만 연결
- 필요시에는 한번만 저장 가능한 DVD 등의 매체를 이용
- 백업에 대한 정확성은 정기적으로 확인
- 운영체제에서 제공하는 백업 기능 등을 사용

o 데이터 백업 시 주의사항

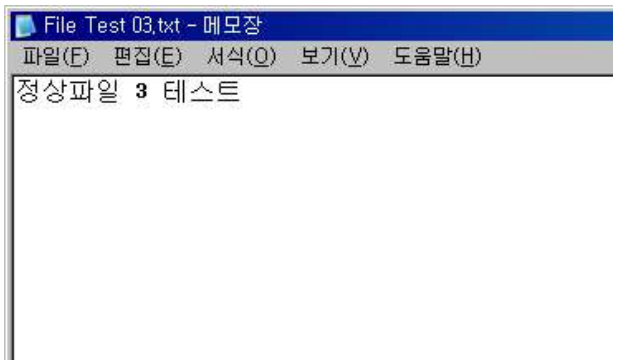
- 지속적으로 연결하는 장치와 생성하는 파일들을 암호화하기 때문에 악성코드 제거 후 데이터 백업 진행
- 무분별한 자동 백업 구성은 암호화된 파일(확장자 변경이 없는 파일)로 백업이 진행되어 주의 필요

4. 랜섬웨어 감염 시 대응절차

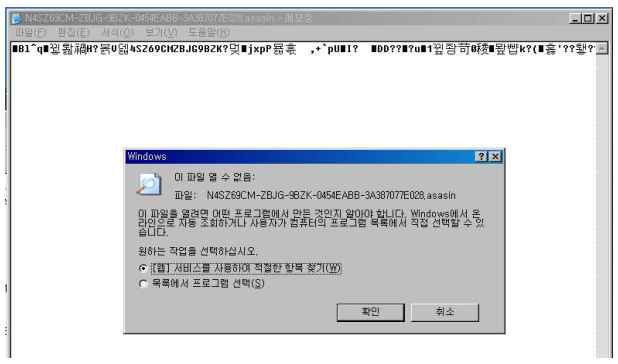
가. 증상 확인하기

o 랜섬웨어에 감염되면 일반적으로 다음과 같은 증상이 나타남

① **(파일 사용불가)** 평소 문제없이 열렸던 문서, 사진, 그림, 음악, 동영상, 파일들 중 일부 혹은 전체가 읽을 수 없게 되거나 열리지 않는 현상이 발생



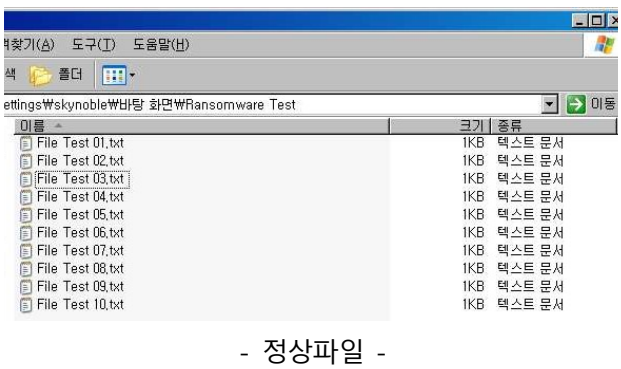
- 정상파일 -



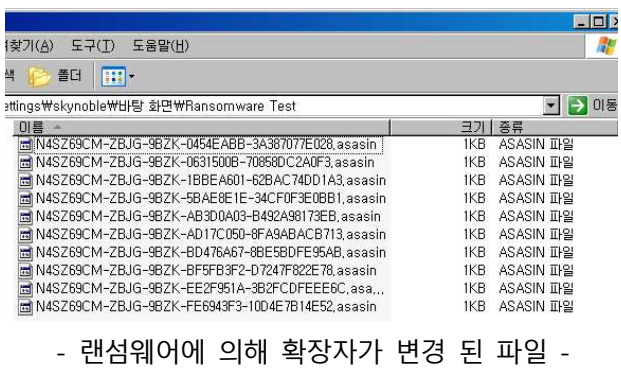
- 랜섬웨어에 의해 암호화 된 파일 -

< 파일 사용불가 >

② **(파일 확장자 변경)** 평소 아무 문제없이 사용하던 파일의 이름과 확장자가 바뀌거나 파일 확장자 뒤에 특정 확장자가 추가된 것을 볼 수 있음



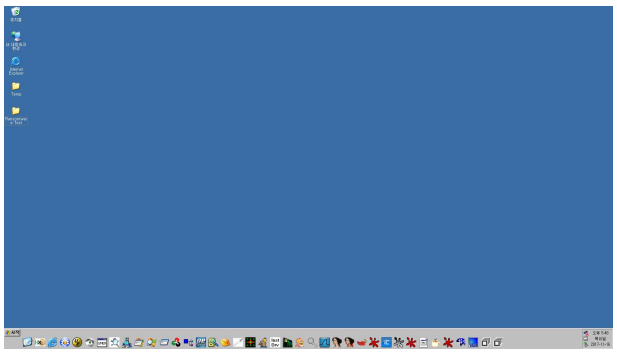
- 정상파일 -



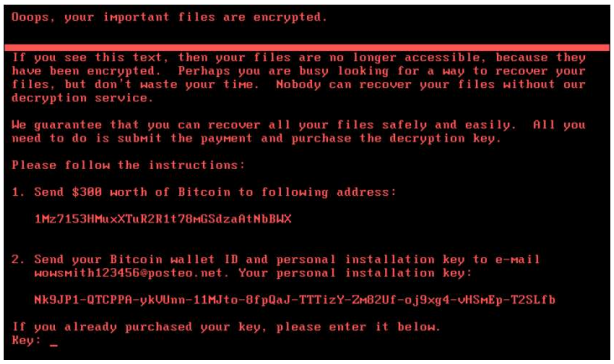
- 랜섬웨어에 의해 확장자가 변경 된 파일 -

< 파일 확장자 변경 >

③ **(부팅 불가능)** 평소 사용하던 운영체제로 부팅이 되지 않고 랜섬웨어 감염 사실 및 금전요구 화면을 볼 수 있음



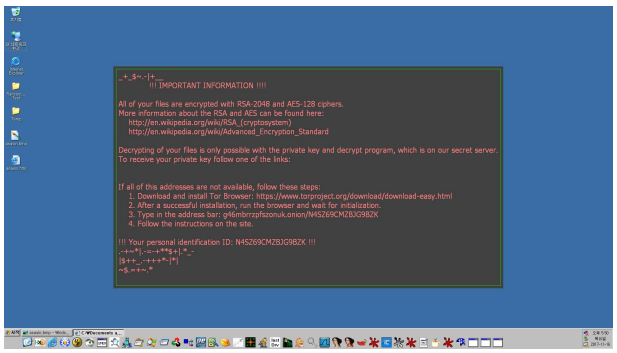
- 정상 운영체제 -



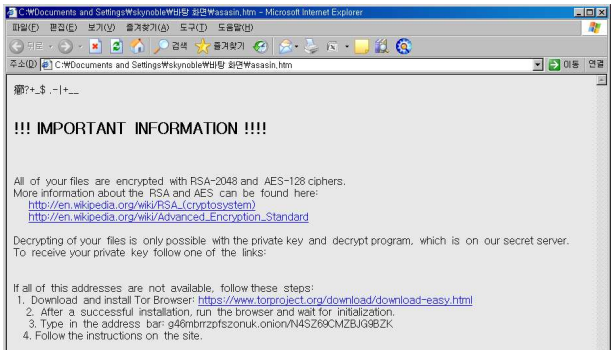
- 랜섬웨어에 의해 부팅이 불가능한 상태 -

< 부팅 불가능 >

④ **(바탕화면 변경 및 감염 알림 창)** 사용자의 파일이 암호화되었음을 알리고 이를 해제하기 위한 비용과 지불할 방법을 보여주는 안내 창을 볼 수 있음



- 바탕화면 변경 -



- 감염 알림 창 -

< 바탕화면 변경 및 감염 알림 창 >

o 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

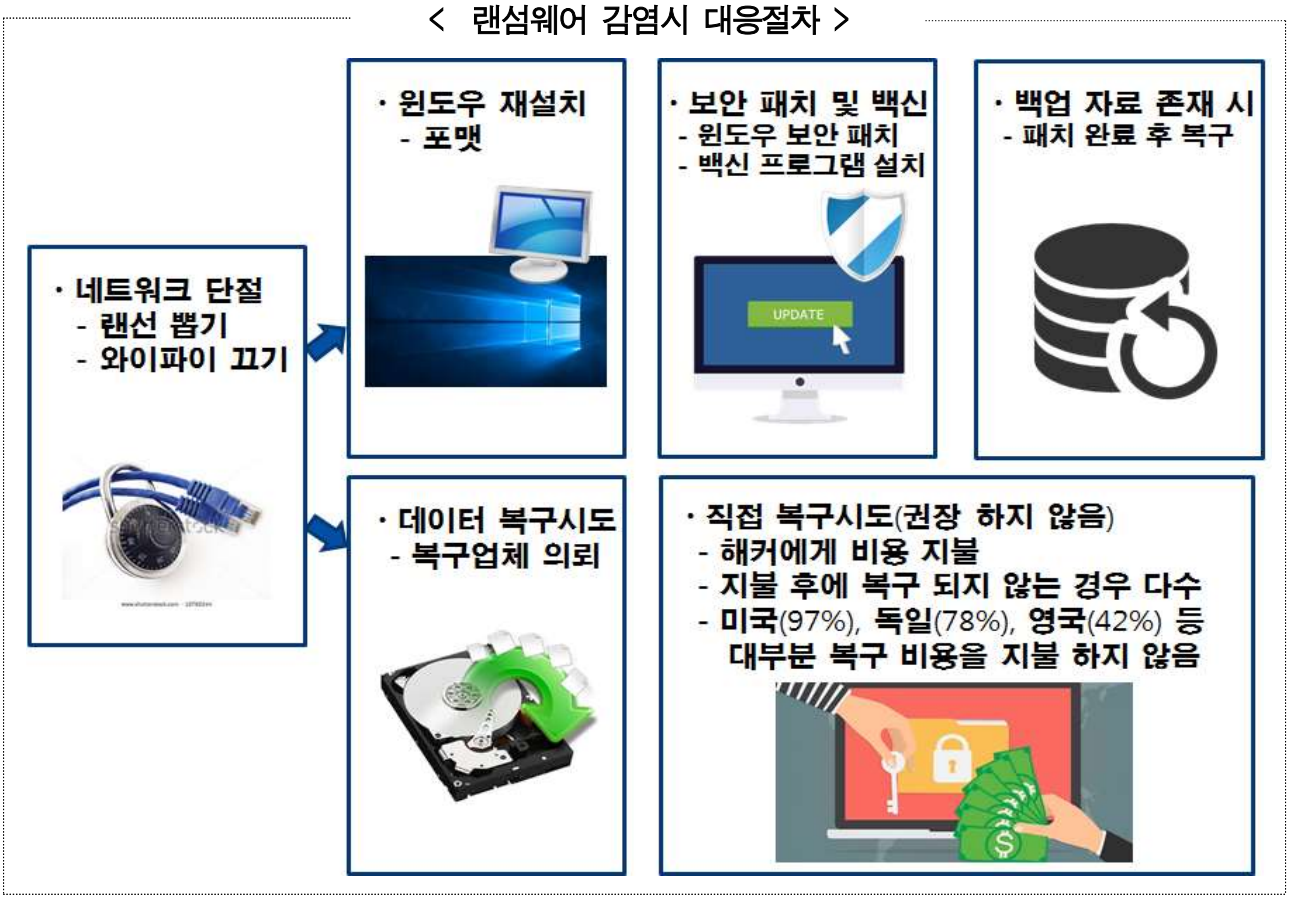
※ 워너크라이 랜섬웨어와 같이 내부망 전파도 될 수 있으니 외부 저장장치뿐만 아니라 네트워크 연결도 해제해야 함

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

< 랜섬웨어 감염시 대응절차 >



나. 신고하기

o **(증거 남기기)** 감염 알림창과 암호화 된 파일이 생성된 화면 캡쳐 및 저장

o **(신고하기)** 신고기관*에 해당 사항을 신고하고 남겨놓은 증거물(캡쳐 파일)을 제출

※ 한국인터넷진흥원(KISA)에서는 비용을 지불하지 말고 관련기관에 신고할 것을 권장

* 관련기관 : 한국인터넷진흥원 사이버민원센터(☎118, boho.or.kr)
경찰청 사이버안전국(☎02-3150-2659, cyber.go.kr)

다. 데이터 복구하기

o 랜섬웨어에 의해 암호화되지 않은 PC 또는 이동식 저장장치(USB)에 데이터 백업하기

o PC 포맷 및 운영체제 재설치, SW 최신 보안 업데이트 적용

o 기존 백업매체 연결 및 데이터 복구

o 랜섬웨어 복구도구 활용

- 보안업체나 노모어랜섬(No More Ransom) 홈페이지* 등에서 일부 랜섬웨어에 대한 복구도구를 제공하지만, 모든 파일 또는 암호화 키에 대한 복구가 아닌 부분적인 복구를 지원

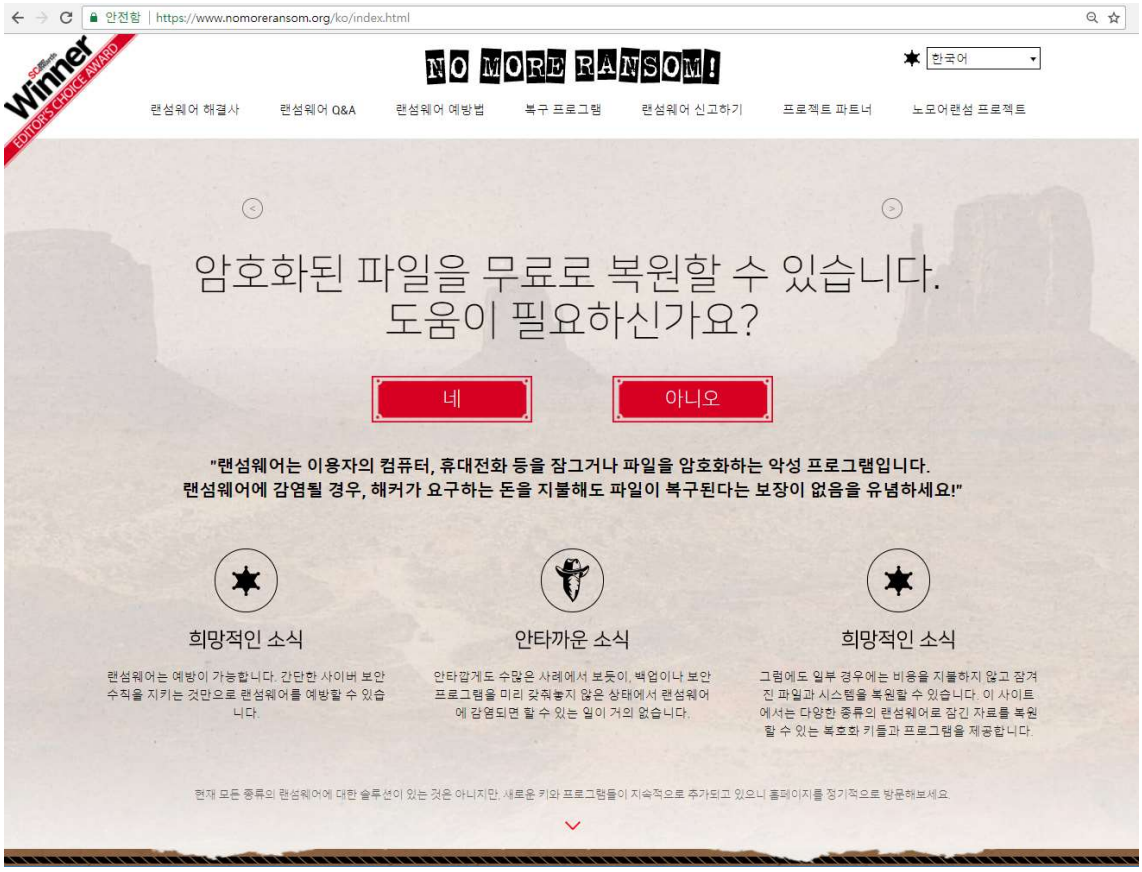
* 노모어랜섬 홈페이지 : http://www.nomoreransom.org

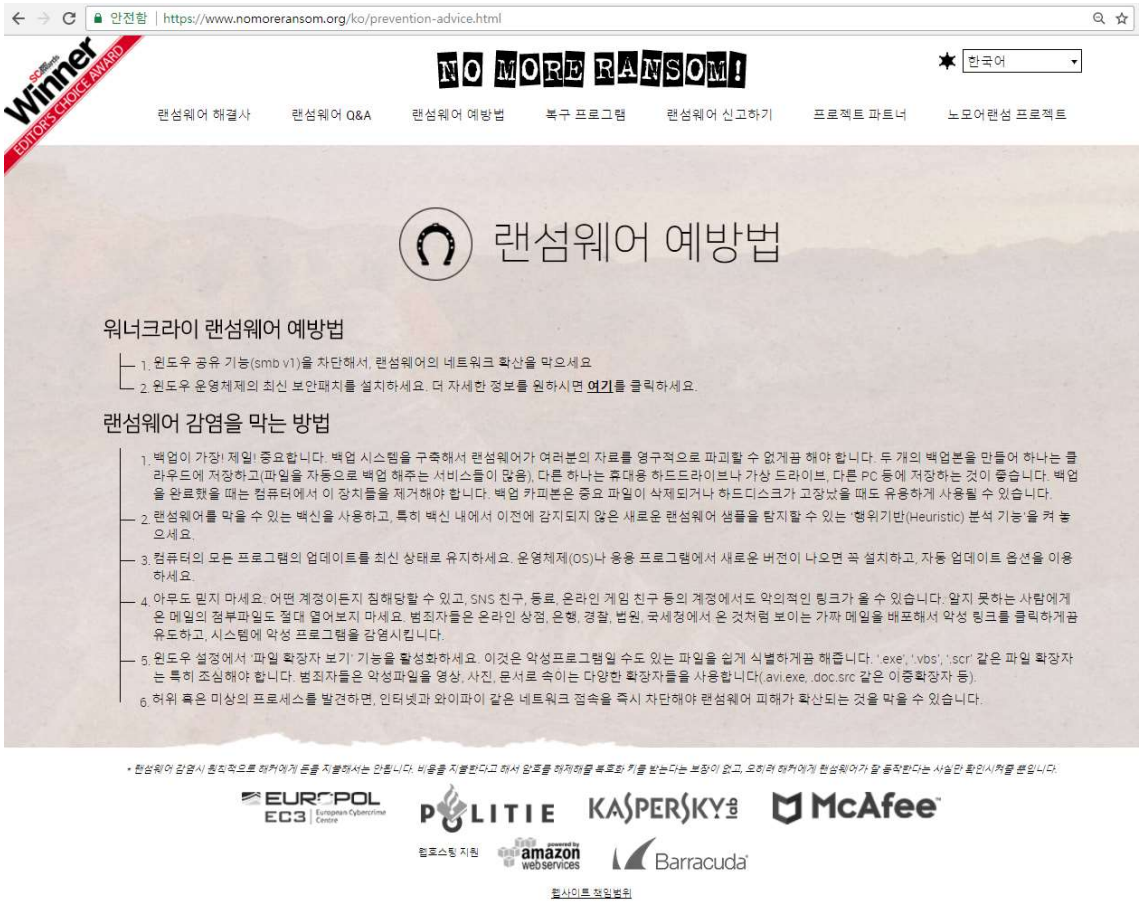
※ 랜섬웨어의 역사, 종류, 랜섬웨어 감염 후 조치방법 등 해당 사이트에서 제공하는 서비스 설명 지원

< 암호화된 데이터를 보관해야하는 이유 >

☞ 추후 암호화된 파일 및 시스템을 복구할 수 있는 도구가 제공될 경우를 대비하여 감염 된 랜섬웨어의 정확한 유형과 감염된 디스크 및 저장장치를 보관하고 있어야 복구 확률을 높일 수 있음

< 노모어 랜섬(No More Ransom) >





라. 공격자(해커)와의 협상 시 고려사항

o **(주의사항)** 돈을 받은 공격자가 파일 복구에 필요한 복호화 키(Decryption key)를 제공한다고 보장할 수 없고, 합법적 거래가 아니기 때문에 법적 보호를 받을 수 없음

- 한번 돈을 지불한 피해자는 공격자에게 손쉬운 대상으로 인식되어 암호를 풀 수 있는 복호화 키를 제공받더라도 이후 또 다른 범죄행위를 위한 대상이 될 수 있음
- 이에, 한국인터넷진흥원뿐만 아니라 전 세계적으로도 랜섬웨어 감염시 공격자에게 복호화 비용을 지불하지 않도록 권장

o **(고려사항)** 기업이 기능을 수행 할 수 없는 상황에 직면할 경우 임원은 주주, 직원 및 고객을 보호하기 위한 모든 상황을 검토해야함

- 복호화 비용을 지불한다고 해서 조직의 데이터 재사용을 보장하는 것은 아님
- 일부 개인이나 조직은 복호화비용을 지불 한 후에도 암호 해독키를 제공받지 못한 사례도 있음
- 비용을 지불한 일부 조직이 다시 공격 대상이 되는 경우도 확인됨
- 처음 요구된 비용을 지불 한 후에, 일부 피해자는 약속한 복호화 비용보다 더 많은 금액의 지불을 요구하는 경우도 확인됨
- 복호화 비용을 지불하면 범죄 비즈니스 모델을 장려하는 효과 발생

[붙임1] 랜섬웨어 관련 FAQ

Q1) 랜섬웨어란 무엇인가?

o 몸값(Ransom)과 소프트웨어(Software)의 합성어로

o 이용자의 PC를 **악성코드로 감염시켜, PC內 문서·파일 등을 암호화**하고 **복구를 대가로 금전을 요구**하는 **해킹 기법**입니다.

Q2) 랜섬웨어는 어떻게 감염된 건가요? (감염 경로)

o 대부분 신뢰할 수 없는 메일(URL, 첨부파일) 또는 보안이 취약한 웹사이트 방문, 파일 공유(토렌트 등) 사이트 등을 통해 감염됩니다.

* 금번 워너크라이 랜섬웨어는 MS社 윈도우즈 운영체제의 SMB 취약점을 악용하여 기관 내·외부 PC를 무작위로 추가 감염시키는 웜(worm) 형태로 자동전파

Q3) 어떤 경우 랜섬웨어에 감염되나요? (감염 원인)

o 운영체제 및 주요 프로그램(어도비社 플래시 플레이어, 리더, 자바 등)의 최신 보안 업데이트가 적용되지 않거나,

o 최신 백신 소프트웨어가 미설치된 시스템이 감염됩니다.

Q4) 제가 현재 감염된 랜섬웨어의 종류가 뭔가요 ?

o 일반적으로 랜섬웨어에 의해 암호화되어 열어 볼 수 없는 **파일의 확장자**로 구분이 가능합니다.

※ SAGE 랜섬웨어(.sage), CERBER 랜섬웨어(.cerber), Crysis(.crypted, .CrySiS, .wallet,) Crypto Locker(.cryptolocker, .encryptred), CTB-Locker(ctb2) 등

o 또한 랜섬웨어에 감염된 화면에 명시되어 있는 경우도 있습니다.

Q5) 랜섬웨어에 다시 감염되지 않기 위해서는 어떻게 해야 하나요?

o KISA 랜섬웨어 피해 예방 5대 수칙을 꼭 지켜주시기 바랍니다.

① 모든 소프트웨어는 최신 버전으로 업데이트하여 사용합니다.

② 백신 소프트웨어를 설치하고, 최신 버전으로 업데이트 합니다.

③ 출처가 불명확한 이메일과 URL 링크는 실행하지 않습니다.

④ 파일 공유 사이트 등에서 파일 다운로드 및 실행에 주의합니다.

⑤ 중요 자료는 정기적으로 별도의 매체(USB, 클라우드 등)에 백업합니다.

Q6) 해커의 말대로 비트코인을 지불하면 복구가 가능한 건가요?

o 비용 지불 후에도 복구되지 않는 경우가 있어 권장하지 않으며, 국외에서도 대부분 복구비용을 지불하지 않는다는 조사결과도 있습니다.

※ 국외 : 미국(97%), 독일(78%), 영국(42%) 등

Q7) 외부에서 일부 랜섬웨어는 복구툴이 있어 복구가 가능하다고 하는데 정말 인가요?

o 대부분의 랜섬웨어의 경우 공격자를 검거하여, 공격자 서버에 저장된 감염자들의 복호화 키(암호를 풀 수 있는)를 획득하여야만 복구가 가능하나,

o 극히 일부의 랜섬웨어만 복구가 가능하며, 아래 링크를 참고하시기 바랍니다.

※ 랜섬웨어 복구 도구 링크 참고(보호나라-www.boho.or.kr/ransomware/recovery.do, 노모어랜섬-www.nomoreransom.org)

[붙임2] 랜섬웨어 종류 및 특징

▣ AllCry 랜섬웨어

▣ CERBER 랜섬웨어

▣ DMA Locker 랜섬웨어

▣ Erebus 랜섬웨어

▣ GlobeImposter 랜섬웨어

▣ Jigsaw 랜섬웨어

▣ Kamil 랜섬웨어

▣ Locky(diablo6) 랜섬웨어

▣ Locky(asasin) 랜섬웨어

▣ Matrix 랜섬웨어

▣ Magniber(MyRansom) 랜섬웨어

▣ Spora 랜섬웨어

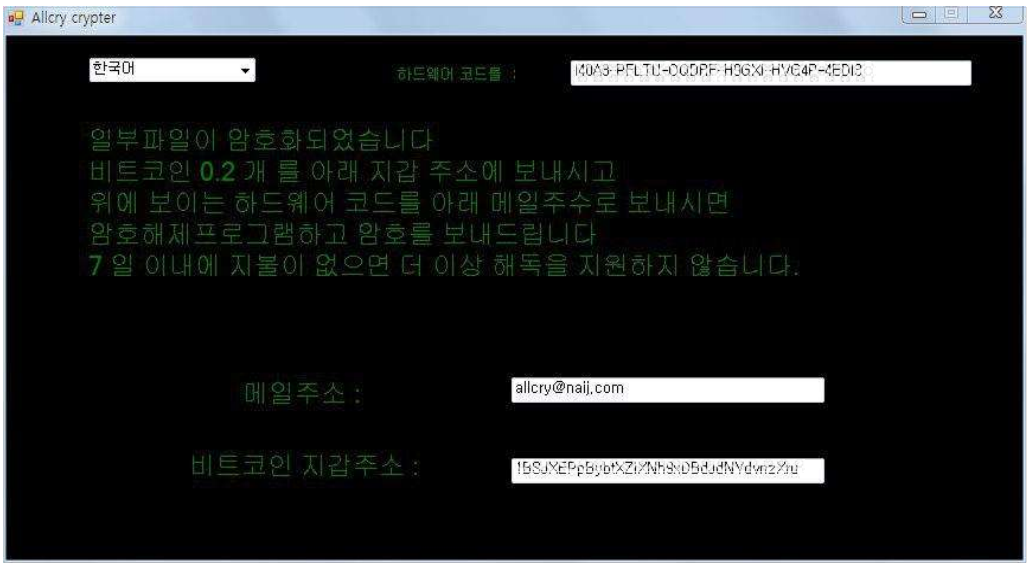
▣ SyncCrypt 랜섬웨어

▣ TechSupportScam 랜섬웨어

▣ VenusLocker 랜섬웨어

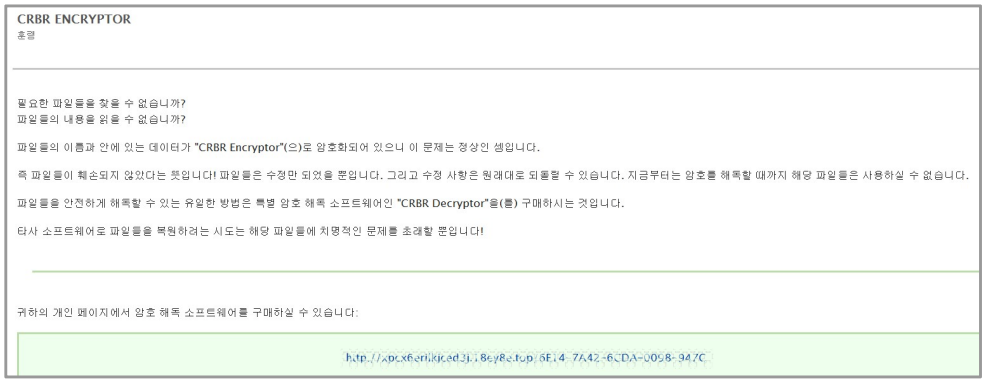
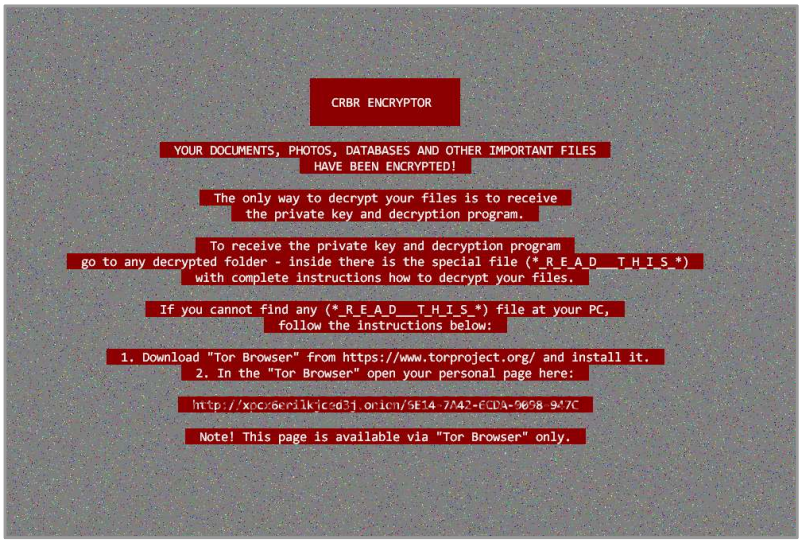
▣ WannaCry 랜섬웨어

□ AllCry 랜섬웨어

구분	내용
랜섬노트	  • 지갑주소를 명시하여 **가상통화(약 0.2Bitcoin)를 지불**하도록 유도하는 랜섬노트 • '**allcry@naij.com, allcry@alquds.com**' 메일정보 포함 • 영어, 한국어, 중국어로 작성된 랜섬노트
피해범위	• PC에 존재하는 파일 (jpg, xls, doc, ppt, zip, hwp, exe 외 200개의 확장자) • Local Disk
특징	• '**.allcry**'로 **파일 확장자를 변경** • 바탕화면 폴더에 "**readme.txt**" 랜섬노트 파일 생성 • 특정 홈페이지에서 유포 or 웹하드 프로그램에 포함되어 유포

※ 신규 또는 변종 랜섬웨어에 따라 위 내용과 다를 수 있습니다.

□ CERBER 랜섬웨어

구분	내용
랜섬노트	  • URL주소를 명시하여 **복호화도구를 구매**하도록 유도하는 랜섬노트 • "**CRBR ENCRYPTOR**"이 명시된 **바탕화면 이미지**
피해범위	• PC에 존재하는 파일 (jpg, xls, pdf, ppt, zip, avi, wmv 외 300개의 확장자) • Local Disk, USB Drive, Network Drive, Cloud Drive
특징	• 4자리의 '**임의의 숫자 or 영문자**'로 **파일 확장자를 변경 (PC마다 확장자가 다름)** • **음성**으로 암호화 사실을 전달 • 암호화된 폴더에 **3개의 랜섬노트를 생성** - (**_R_E_A_D__T_H_I_S__[영문+숫자].hta**) - (**_R_E_A_D__T_H_I_S__[영문+숫자].txt**) - (**_R_E_A_D__T_H_I_S__[영문+숫자].png**) • 자동실행으로 등록하여 재부팅 하더라도 랜섬노트 실행 • 시스템복원이 불가능하도록 **볼륨 쉐도우(Volume Shadow) 삭제** • 낮은 버전의 CERBER(Ver.1)의 경우 **복호화 도구가 존재** (No More Ransom)

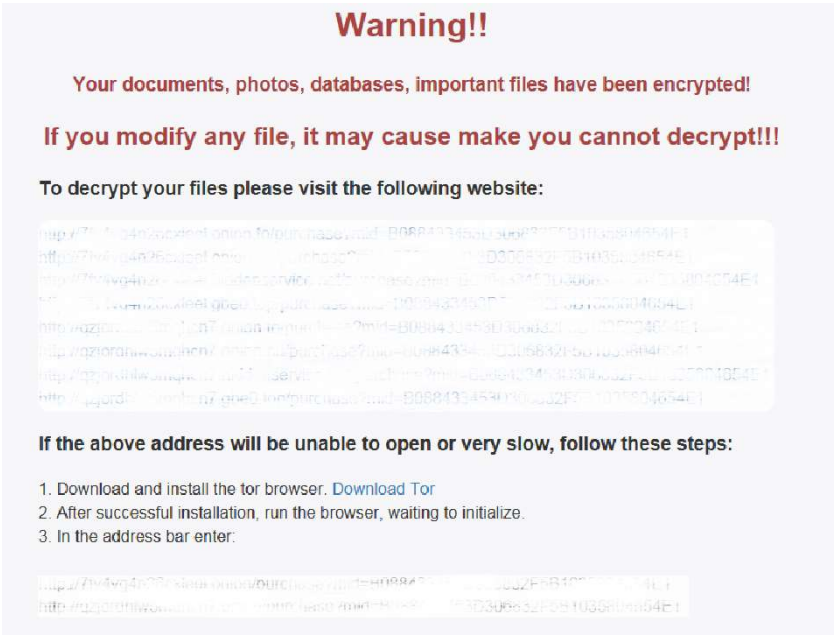
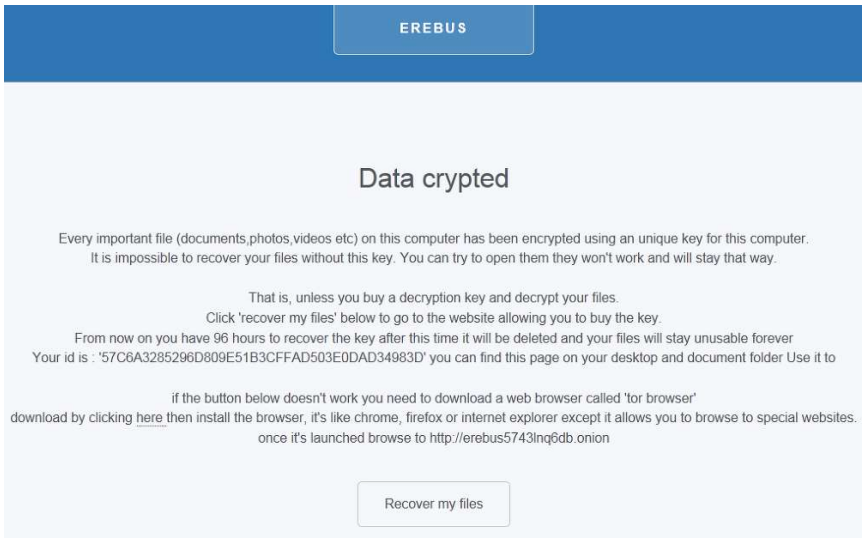
※ 신규 또는 변종 랜섬웨어에 따라 위 내용과 다를 수 있습니다.

□ DMA Locker 랜섬웨어

구분	내용
랜섬노트	 • 지갑주소를 명시하여 **가상통화(3Bitcoin)**를 지불하도록 유도하는 랜섬노트 • '**DMA Locker 3.0**' 이름의 프로그램 실행 • 시간(96h)이 지나면 복호화 비용 증가 • '**week4004@fastmail.com**' 메일정보 포함
피해범위	• PC에 존재하는 파일 (블랙리스트 기반*의 파일 암호화 대상 선정) * 시스템 동작을 위한 파일 등 특정 파일 확장자를 제외한 파일을 선정하여 암호화 시도 • Local Disk, USB Disk
특징	• **파일 확장자 변경이 없음** • 자동 실행으로 등록되어 재시작시 **랜섬노트(프로그램, 텍스트 파일) 실행**

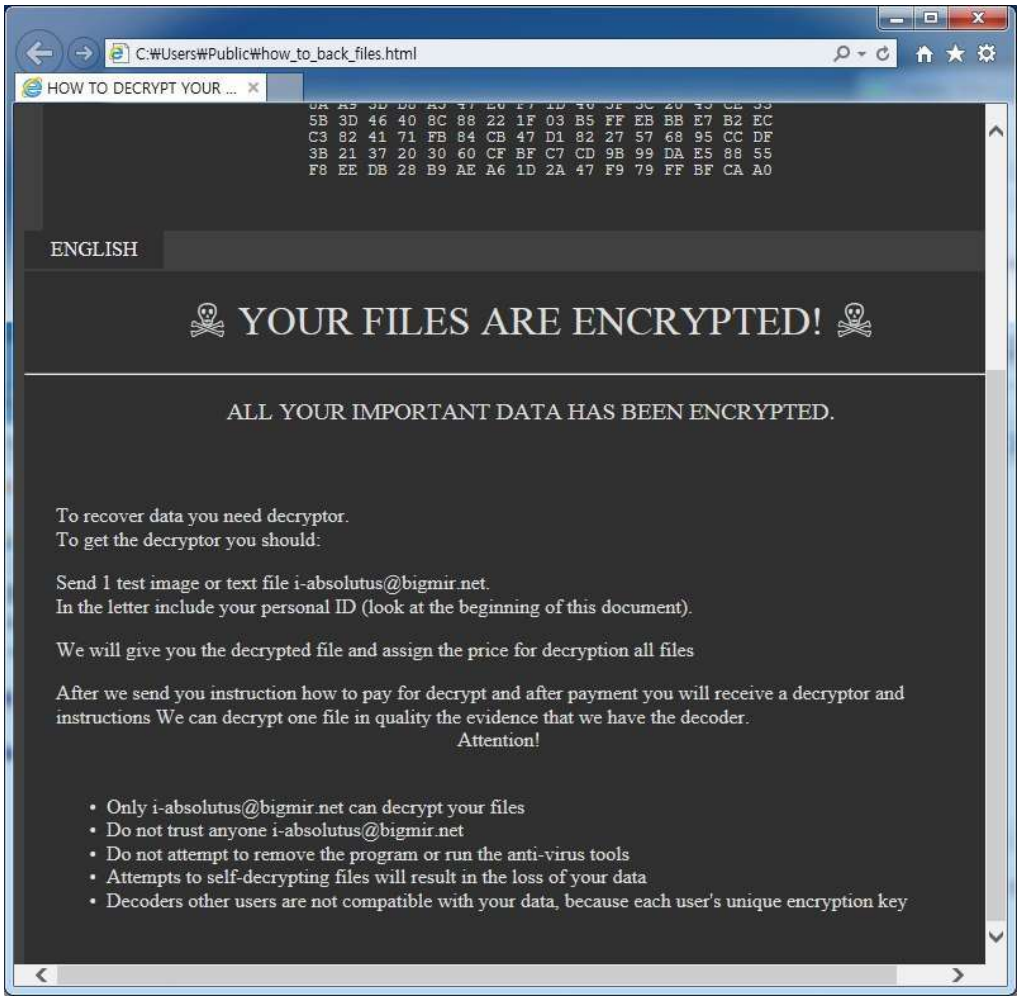
※ 신규 또는 변종 랜섬웨어에 따라 위 내용과 다를 수 있습니다.

□ Erebus 랜섬웨어

구분	내용
랜섬노트	  • URL주소(Tor)를 명시하여 **가상통화**를 지불하도록 유도하는 랜섬노트
피해범위	• PC에 존재하는 파일 (jpg, xls, doc, ppt, zip 외 400개의 확장자) • Local Disk, USB Drive, Network Drive
특징	• '**.ecrypt**'로 **파일 확장자를 변경** • 바탕화면을 포함한 모든 폴더에 랜섬 노트 생성 - '**_DECRYPT_FILES.html**, **_DECRYPT_FILES.txt**' • 윈도우즈, 리눅스 계열의 운영체제에서 발견된 랜섬웨어 • 공격자는 서버 복호화를 위해 많은 금액을 요구(2000만원~4000만원)

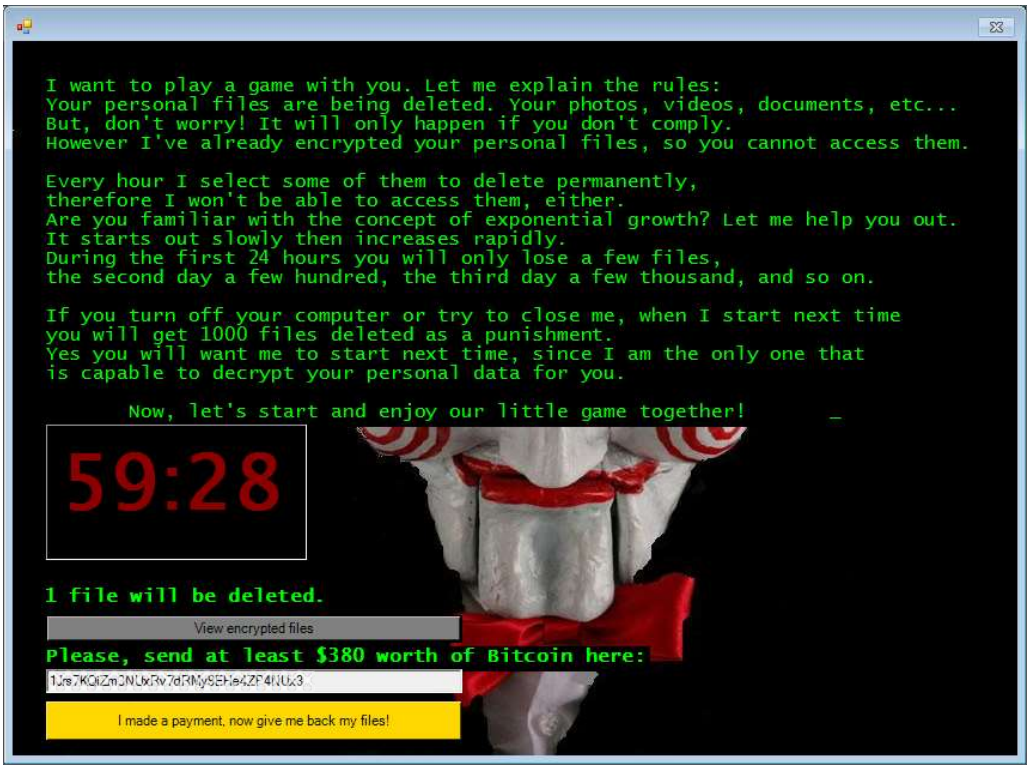
※ 신규 또는 변종 랜섬웨어에 따라 위 내용과 다를 수 있습니다.

□ GlobeImposter 랜섬웨어

구분	내용
랜섬노트	 • **E-Mail 주소(i-absolutus@bigmir.net)로 연락**하도록 유도 • '**how_to_back_Files.html**' 파일명을 가지고 있는 **랜섬노트**
피해범위	• PC에 존재하는 파일 (xls, xlsx, pdf, ppt, pptx, hwp 외 200개의 확장자) • Local Disk, USB Drive, Network Drive
특징	• '**[i-absolutus@bigmir.net].rose**'로 파일 확장자를 변경 • 암호화된 폴더에 "**how_to_back_files.html**" 랜섬노트 생성 • **'EXE' 파일 암호화** 진행 (PC재부팅 시 오류 발생 가능성 존재) • E-Mail을 통해 배포 • 디지털 서명을 포함한 변종 GlobeImposter 랜섬웨어

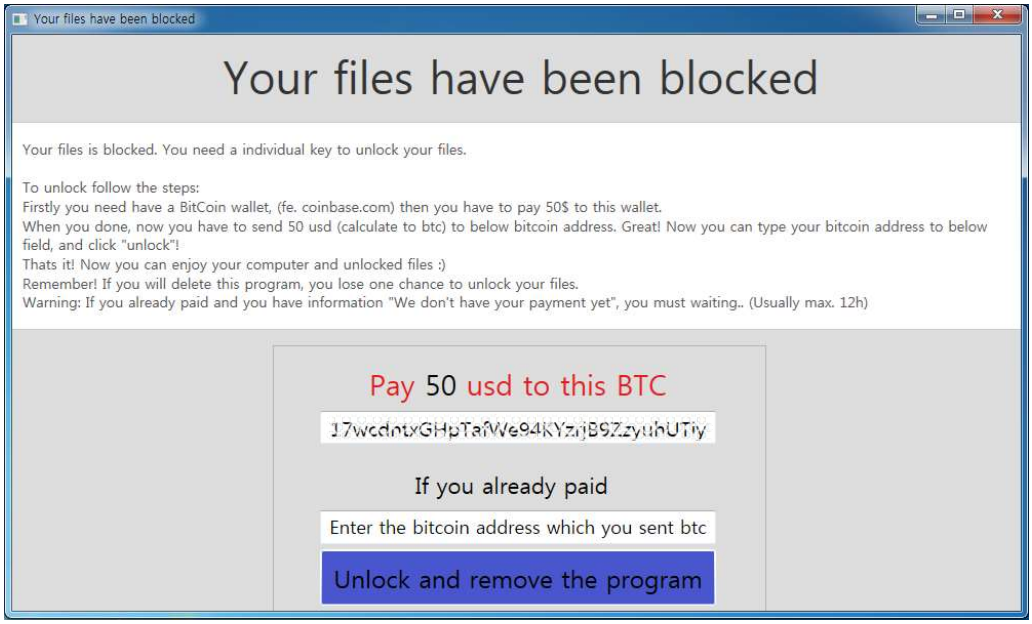
※ 신규 또는 변종 랜섬웨어에 따라 위 내용과 다를 수 있습니다.

□ Jigsaw 랜섬웨어

구분	내용
랜섬노트	 • 지갑주소를 명시하여 **가상통화(Bitcoin)를 지불하도록 유도** • 영화 **'Jigsaw' 이미지**가 나타나는 **랜섬노트**
피해범위	• PC에 존재하는 파일 (jpg, xls, pdf, ppt, zip, db 외 120개의 확장자) • Local Disk, USB Drive, Network Drive
특징	• **'.lost, .fun, .kkk, .btc, .gws'**로 파일 확장자를 변경 • **플래시 업데이트 파일로 위장** • 시간이 지날 때마다 **암호화된 파일을 삭제** • 자동실행으로 등록하여 재부팅 하더라도 랜섬노트 실행 • **복호화 도구가 존재** (No More Ransom)

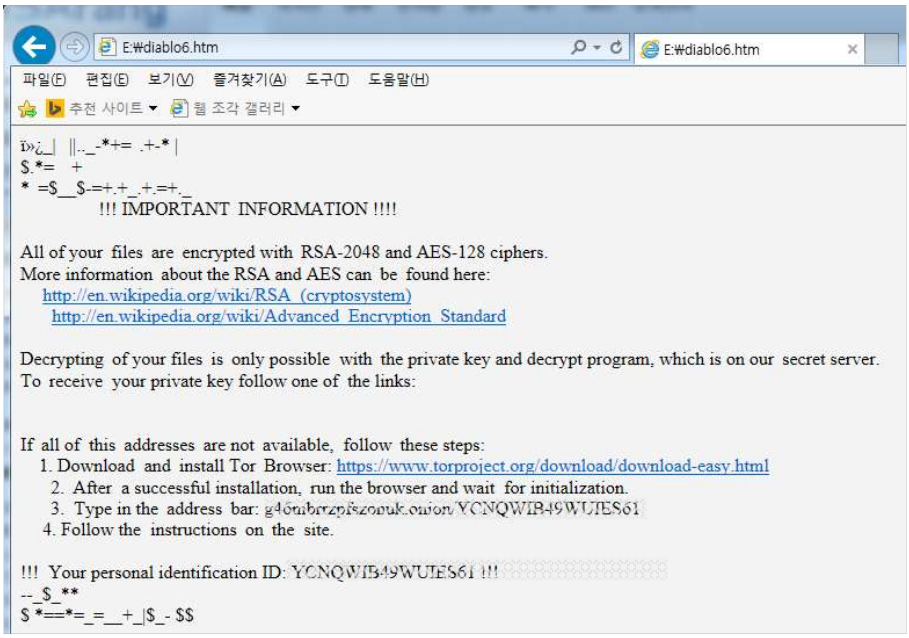
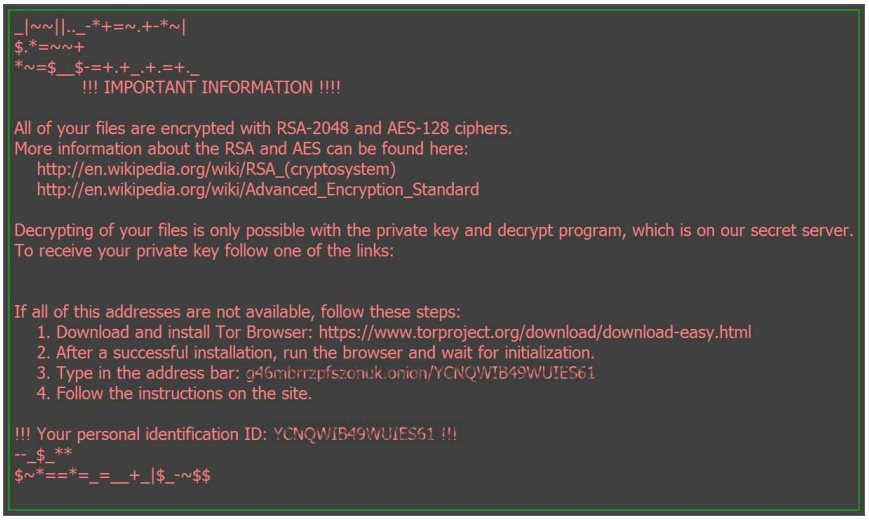
※ 신규 또는 변종 랜섬웨어에 따라 위 내용과 다를 수 있습니다.

□ Kamil 랜섬웨어

구분	내용
랜섬노트	 • 지갑주소를 명시하여 **가상통화(약50$)**를 지불하도록 유도하는 랜섬노트 • "**Your files have been blocked**" 타이틀명을 가지는 프로그램 실행
피해범위	• PC에 존재하는 파일 (exe, lnk 파일 확장자를 제외한 특정 디렉터리의 모든 파일) - **CommonProgramFilesX86** - **CommonProgramFiles** - **DesktopDirectory** • Local Disk
특징	• 일부 파일은 '**.lock**'로 **파일 확장자를 변경** • 대부분의 암호화 파일은 **파일 확장자 변경이 없음**

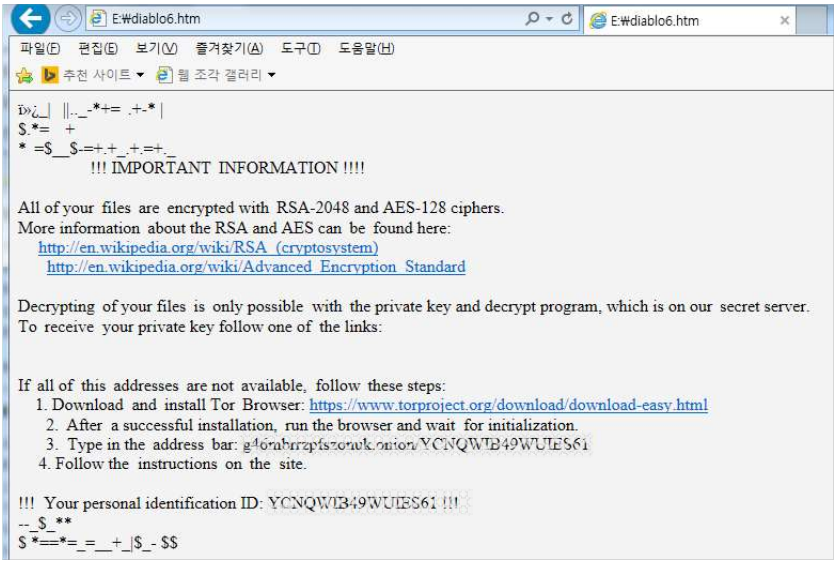
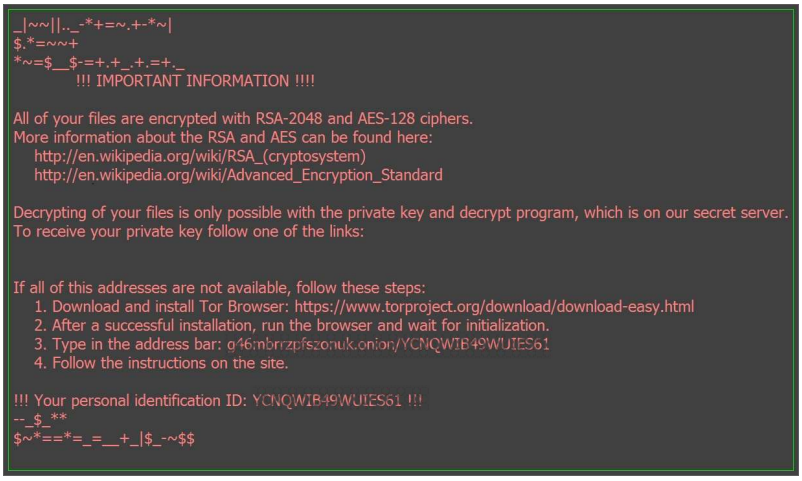
※ 신규 또는 변종 랜섬웨어에 따라 위 내용과 다를 수 있습니다.

□ Locky(diablo6) 랜섬웨어

구분	내용
랜섬노트	 • URL주소(Tor)를 명시하여 가상통화(비트코인)를 지불하도록 유도하는 랜섬노트 • **바탕화면 이미지** 변경 
피해범위	• PC에 존재하는 파일 (jpg, xls, pdf, ppt, zip, avi, wmv 외 200개의 확장자) • Local Disk, USB Drive, Network Drive, Cloud Drive
특징	• **'diablo6'로 파일 확장자를 변경** • 암호화된 폴더에 **랜섬노트(diablo6_[3자리].htm) 생성** • 시스템복원이 불가능하도록 **볼륨 쉐도우(Volume Shadow) 삭제** • E-mail로 유포 (제목과 첨부파일은 '**E 2017-08-09 (숫자).[확장자]**' 형태)

※ 신규 또는 변종 랜섬웨어에 따라 위 내용과 다를 수 있습니다.

□ Locky(asasin) 랜섬웨어

구분	내용
랜섬노트	 • URL주소(Tor)를 명시하여 **가상통화(약0.5비트코인)**를 지불하도록 유도하는 랜섬노트 • **바탕화면 이미지** 변경 
피해범위	• PC에 존재하는 파일 (jpg, xls, pdf, ppt, zip, avi, wmv 외 300개의 확장자) • Local Disk, USB Drive, Network Drive, Cloud Drive
특징	• **'asasin'로 파일 확장자를 변경** • 암호화된 폴더에 **랜섬노트(asasin_[4자리].htm) 생성** • 시스템복원이 불가능하도록 **볼륨 쉐도우(Volume Shadow) 삭제** • E-mail로 유포 (송장 및 결제내역으로 메일을 교묘하게 위장) • **Locky 랜섬웨어 변형 과정** - locky→zepto→odin→shit→thor→aesir→zzzzz→osiris→loptr→diablo6→lukitus→asasin

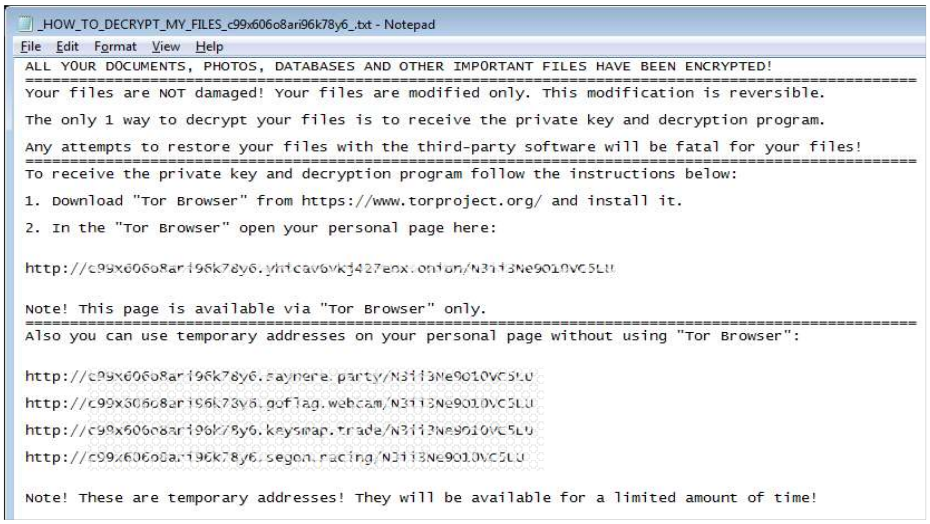
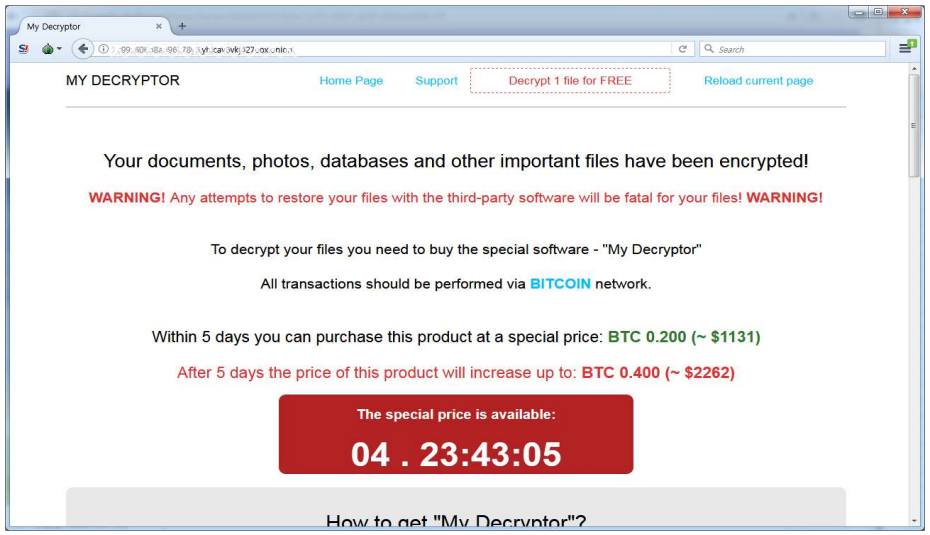
※ 신규 또는 변종 랜섬웨어에 따라 위 내용과 다를 수 있습니다.

□ Matrix 랜섬웨어

구분	내용
랜섬노트	 • 시간(12h)이 지나면 복호화 비용 증가 • 시간(96h)이 지나면 복호화키를 삭제하여 복호화 불가 • '**mshta.exe**' 이름을 가지고 있는 프로그램 실행 (랜섬노트) • '**decodedecode@tutanota.com**, **restoreassistant@yandex.com**' 메일 주소를 통해 복호화 비용을 지불(가상통화)하도록 유도
피해범위	• PC에 존재하는 파일 (xls, xlsx, pdf, ppt, pptx, hwp 외 200개의 확장자) • Local Disk, USB Drive, Network Drive
특징	• '**.matrix**, **.b10ckedl**'으로 파일 확장자를 변경 • 최근에는 **파일확장자를 변경하지 않고** 암호화를 진행 • 암호화된 폴더에 "**!WhatHappenedWithMyFiles!_rtf**" 파일(랜섬노트) 생성 • E-Mail을 통해 배포

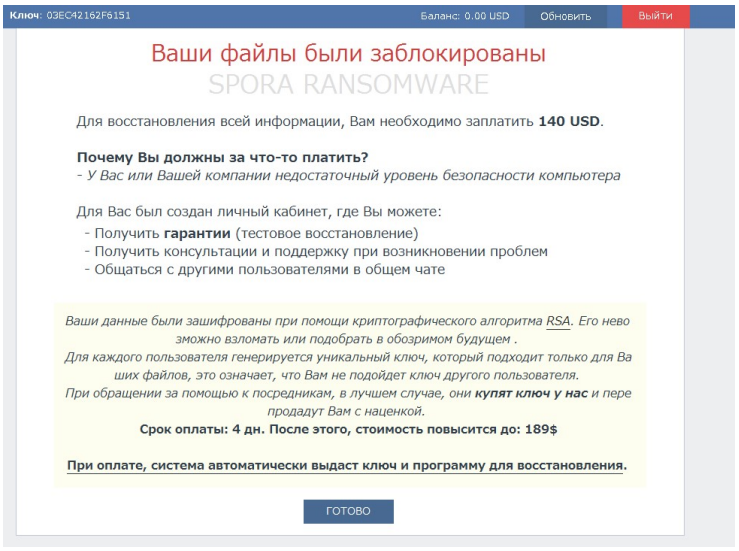
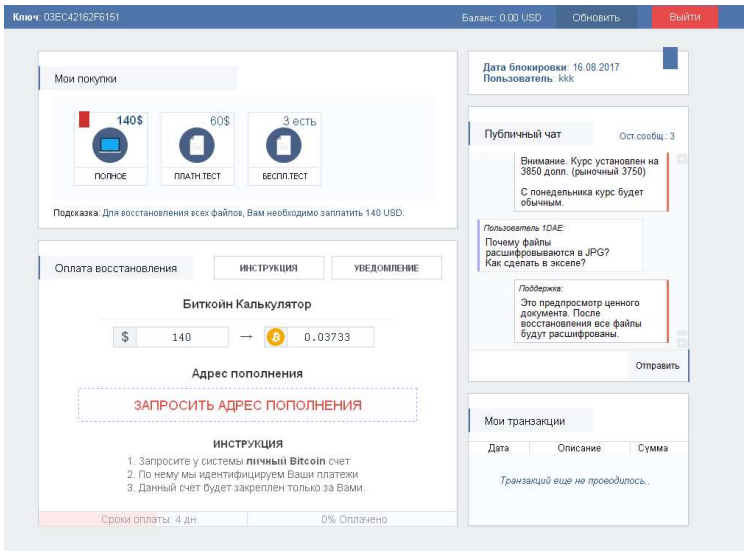
※ 신규 또는 변종 랜섬웨어에 따라 위 내용과 다를 수 있습니다.

□ Magniber(MyRansom) 랜섬웨어

구분	내용
랜섬노트	  • URL주소(Tor)를 명시하여 **가상통화(2Bitcoin)**를 지불하도록 유도하는 랜섬노트 • 일정 시간이 지나면 추가 **가상통화(4Bitcoin) 요구**
피해범위	• PC에 존재하는 파일 (jpg, xls, doc, ppt, zip, hwp 외 300개의 확장자) • Local Disk, USB Drive, Network Drive, Cloud Drive
특징	• '**.kgpvwnr, .ihsdj**'로 **파일 확장자를 변경** • 바탕화면 폴더를 포함한 모든 폴더에 랜섬노트 파일 생성 - '**READ_ME_FOR_DECRYPTOR_[ID].txt**', '**_HOW_TO_DECRYPT_MY_FILES_[ID]_.txt**' • 스케줄러에 등록하여 **15분마다 암호화를 하고 랜섬노트 실행** • 멀버타이징(Malvertising)* 방식으로 유포 (**취약한 홈페이지에 접근**하는 것만으로 **감염**) * 취약한 온라인 광고를 통해 악성코드를 감염시키고 유포하는 방식

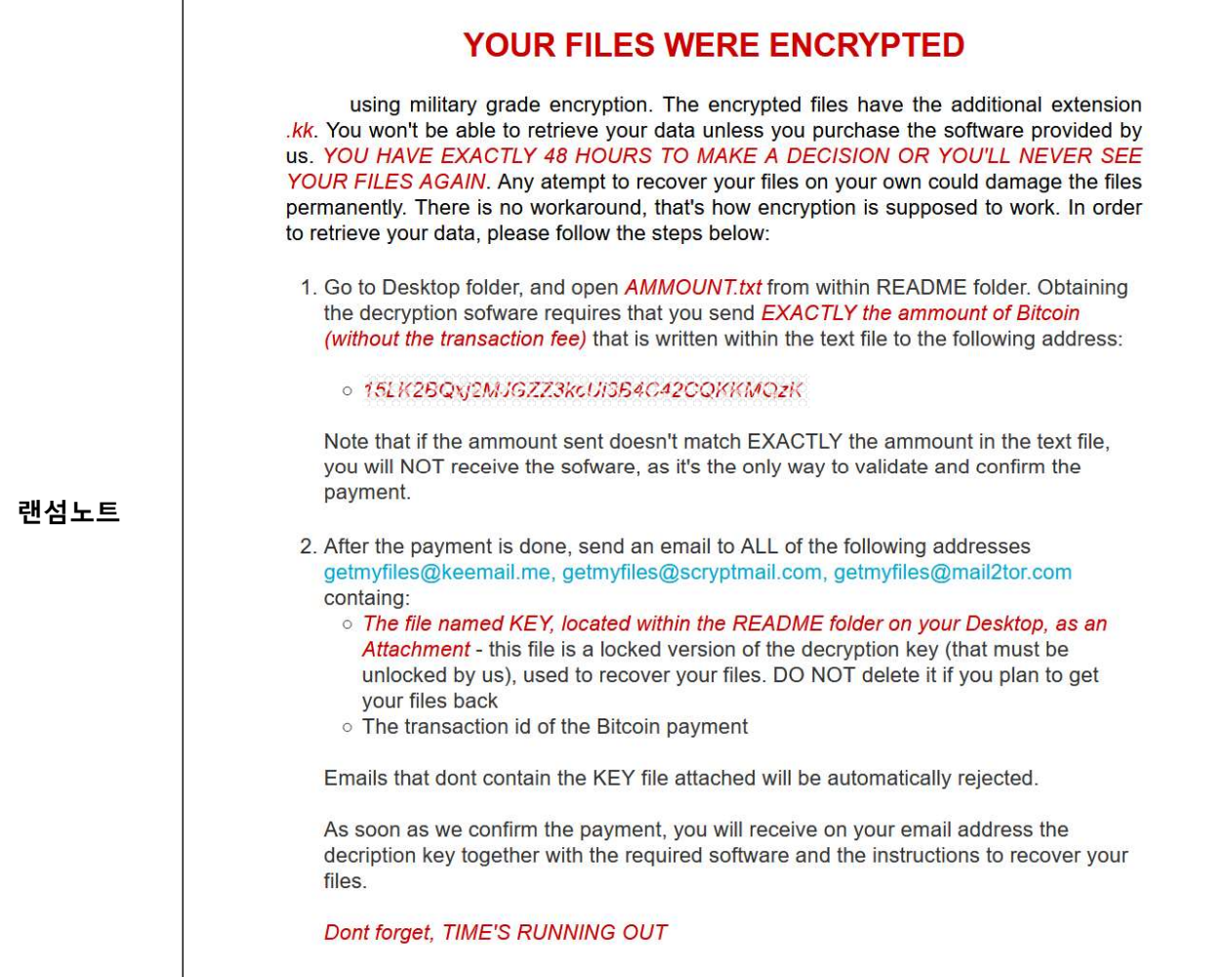
※ 신규 또는 변종 랜섬웨어에 따라 위 내용과 다를 수 있습니다.

□ Spora 랜섬웨어

구분	내용
랜섬노트	  • **가상통화(비트코인)를 지불**하도록 유도하는 랜섬노트 • '**mshta.exe**' 이름을 가지고 있는 프로그램 실행 (랜섬노트)
피해범위	• PC에 존재하는 파일 (jpg, xls, doc, rtf, zip, rar 외 20개의 확장자) • Local Disk, USB Drive, Network Drive
특징	• **파일명, 파일 확장자 변조가 없음** • 암호화된 폴더에 **랜섬노트(README_sTILoTpq.hta) 생성** • 랜섬노트 정보는 네트워크 연결을 통해 전송 비연결시 '**spora.help@gmail,com**' 메일주소를 통해 복호화 방법 문의 요청

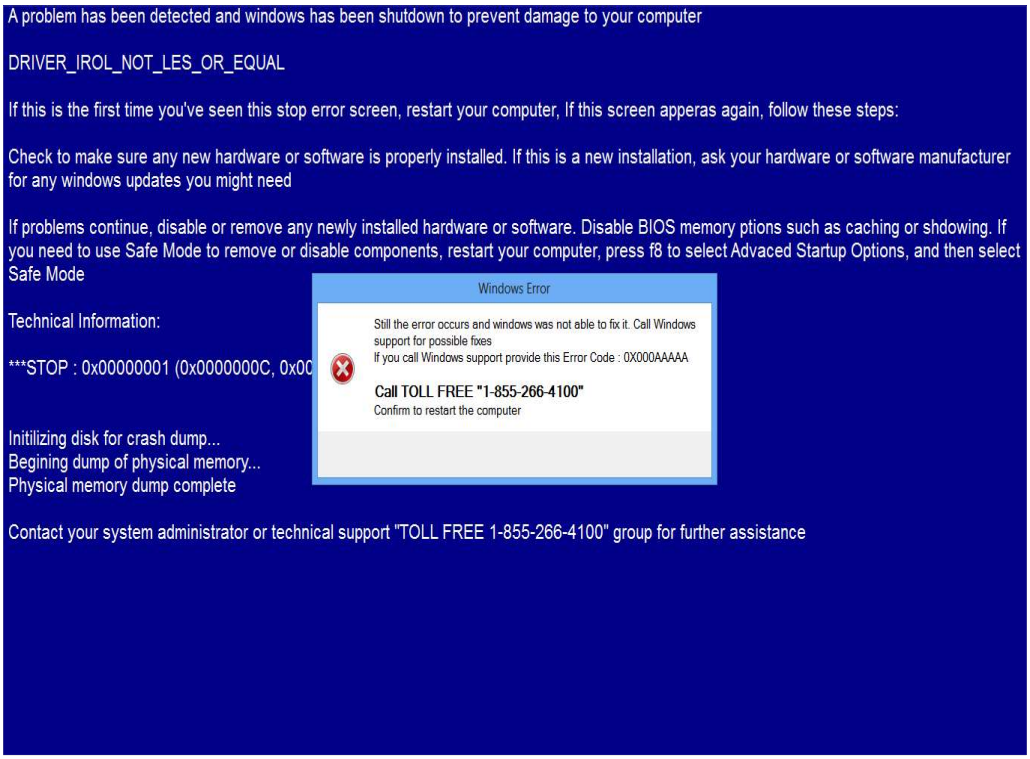
※ 신규 또는 변종 랜섬웨어에 따라 위 내용과 다를 수 있습니다.

□ SyncCrypt 랜섬웨어

구분	내용
랜섬노트	 **YOUR FILES WERE ENCRYPTED** using military grade encryption. The encrypted files have the additional extension *.kk*. You won't be able to retrieve your data unless you purchase the software provided by us. *YOU HAVE EXACTLY 48 HOURS TO MAKE A DECISION OR YOU'LL NEVER SEE YOUR FILES AGAIN*. Any atempt to recover your files on your own could damage the files permanently. There is no workaround, that's how encryption is supposed to work. In order to retrieve your data, please follow the steps below: 1. Go to Desktop folder, and open *AMMOUNT.txt* from within README folder. Obtaining the decryption sofware requires that you send *EXACTLY the ammount of Bitcoin (without the transaction fee)* that is written within the text file to the following address: ○ *15LK2BQvj2MJGZZ3kcUi3B4C42CQKKMQzK* Note that if the ammount sent doesn't match EXACTLY the ammount in the text file, you will NOT receive the sofware, as it's the only way to validate and confirm the payment. 2. After the payment is done, send an email to ALL of the following addresses getmyfiles@keemail.me, getmyfiles@scryptmail.com, getmyfiles@mail2tor.com containg: ○ *The file named KEY, located within the README folder on your Desktop, as an Attachment* - this file is a locked version of the decryption key (that must be unlocked by us), used to recover your files. DO NOT delete it if you plan to get your files back ○ The transaction id of the Bitcoin payment Emails that dont contain the KEY file attached will be automatically rejected. As soon as we confirm the payment, you will receive on your email address the decription key together with the required software and the instructions to recover your files. *Dont forget, TIME'S RUNNING OUT* • 지갑주소를 명시하여 **가상통화(약 0.1Bitcoin)를 지불**하도록 유도하는 랜섬노트 • '**getmyfiles@keemail.me, getmyfiles@scryptmail.com, getmyfiles@mail2rot.com**' 메일정보 포함
피해범위	• PC에 존재하는 파일 (jpg, xls, doc, rtf, zip, hwp 외 200개의 확장자) • Local Disk, USB Drive, Network Drive
특징	• '**.kk**'로 **파일 확장자를 변경** • 바탕화면 "**ReadMe**" 폴더 및 파일 생성(비트코인 가격, 키 파일, 랜섬노트) - "**AMMOUNT.txt**", "**KEY**", "**readme.html**", "**readme.png**" • E-Mail을 통해 배포 (Steganography* 기술을 이용한 이미지 파일 다운로드) * Steganography(스테가노그래피) : 데이터 내부에 또 다른 데이터를 은밀하게 숨기는 기술

※ 신규 또는 변종 랜섬웨어에 따라 위 내용과 다를 수 있습니다.

□ TechSupportScam 랜섬웨어

구분	내용
랜섬노트	 • **심각한 윈도우즈 오류가 나타난 것처럼 위장** • '1-855-266-4100' 연락처 정보가 명시되어 있음
피해범위	• 최상위 화면을 방해하여 정상적인 사용을 방해하며, 그 외 악성행위는 없음
특징	• 숨겨진 프로세스를 실행하여 지속적으로 화면을 방해 • 재부팅 후 PC 정상적으로 사용 가능 • 연구용 또는 장난으로 만든 프로그램으로 추정

※ 신규 또는 변종 랜섬웨어에 따라 위 내용과 다를 수 있습니다.

□ VenusLocker 랜섬웨어

구분	내용
랜섬노트	 • 지갑주소를 명시하여 **가상통화(1Bitcoin)를 지불하도록 유도** • '**VenusLocker**' 이름을 가지고 있는 프로그램 실행 (랜섬노트) • '**venuslockerteam@protonmail.com**' 메일정보 포함 • 바탕화면 이미지가 변경 
피해범위	• PC에 존재하는 파일 (xls, xlsx, pdf, ppt, pptx, hwp 외 200개의 확장자) • Local Disk, USB Drive, Network Drive
특징	• '**.venus, .venusLfS, .venusLf**' 등 "venus" 문자열이 포함된 파일 확장자로 변경 • 언어별 랜섬노트를 포함하고 있음 (**한글 랜섬노트** 존재) • 바탕화면에 "**ReadMe.txt**" 랜섬노트 생성 • E-Mail을 통해 배포

※ 신규 또는 변종 랜섬웨어에 따라 위 내용과 다를 수 있습니다.

□ WannaCry 랜섬웨어

구분	내용
랜섬노트	 • 가상통화 지갑주소를 명시하여 **가상통화($300)**를 지불하도록 유도하는 랜섬노트 • 일정 시간이 지나면 **가상통화 비용이 증가하며, 추가 시간 이후에는 복구 불가능** • 바탕화면 이미지를 변경 • 랜섬노트는 28개의 언어를 지원
피해범위	• PC에 존재하는 파일 (jpg, xls, doc, ppt, zip, hwp 외 175개의 확장자) • Local Disk, USB Drive, Network Drive, Cloud Drive • 내·외부 네트워크망에 연결된 모든 기기
특징	• '**.WNCRYT, .WNCRY**'로 **파일 확장자를 변경** • 바탕화면 폴더에 '**@Plwase Read Me@.txt**' 랜섬 노트 생성 • 킬스위치*가 존재하여 도메인에 접속이 성공하면 랜섬웨어 동작 중지 * 원격으로 기기, 소프트웨어 등을 중지시킬 수 있는 것 • SMB취약점**을 이용하여 랜섬웨어 배포 및 동작 ** MS17-010 취약점을 이용하여 웜형태로 감염 확산

※ 신규 또는 변종 랜섬웨어에 따라 위 내용과 다를 수 있습니다.