2017. 01. 26

Analysis Report

최신 랜섬웨어 동향 분석 보고서

2016년 주요 랜섬웨어 상세 분석 및 전망

ASEC대응팀

AhnLab

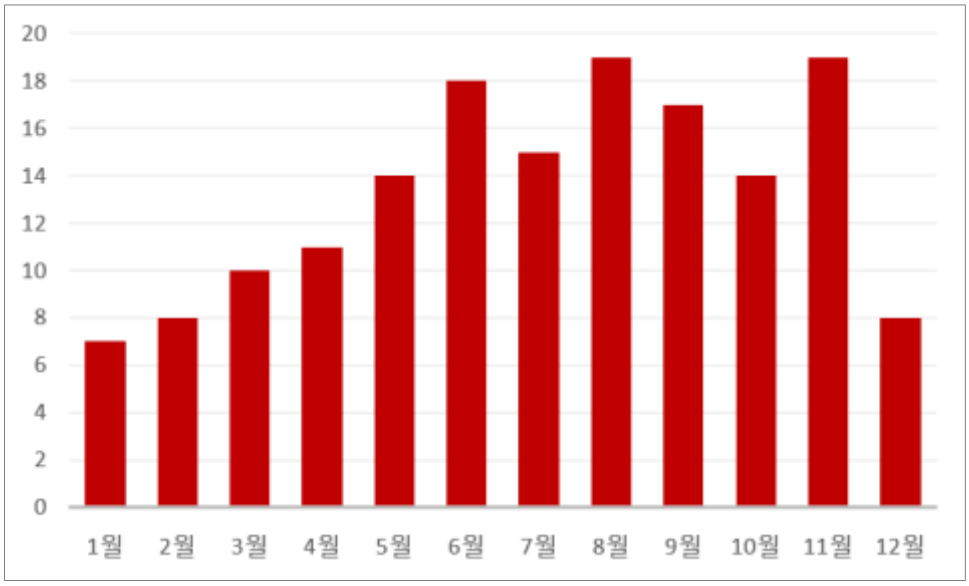
경기도 성남시 분당구 판교역로 220 (우) 13493 | 대표전화 : 031-722-8000 | 팩스 : 031-722-8901 | www.ahnlab.com

목차

도입(Introduction)

랜섬웨어(Ransomware)는 국내외를 막론하고 2015년 전후부터 본격적인 존재감을 드러내기 시작했다. 특히 국내에서는 2015년 4월 유명 커뮤니티사이트를 통한 대규모 랜섬웨어 감염 사태를 분수령으로, 2016년에 들어서며 그 수가 폭발적으로 증가했다.

안랩 시큐리티대응센터(AhnLab Security Emergency response Center, ASEC)의 자체 분석 결과를 기준으로 2013년부터 2015년 사이 10여종에 불과하던 것이 2016년에는 업그레이드된 버전을 포함해 160 여종에 달했다(12월 15일 현재). 최근 1년간 ASEC에서 확인한 신종 랜섬웨어 추이를 살펴보면 가파른 증가세를 보였으며, 하반기에는 매월 15~20여개의 신종 랜섬웨어가 꾸준히 등장했다. 그러나 이는 알려진 랜섬웨어에 한한 것으로, 알려지지 않은 랜섬웨어까지 포함하면 그 수는 훨씬 클 것으로 짐작된다.



[그림 1] 2016년 월별 신종 랜섬웨어 추이

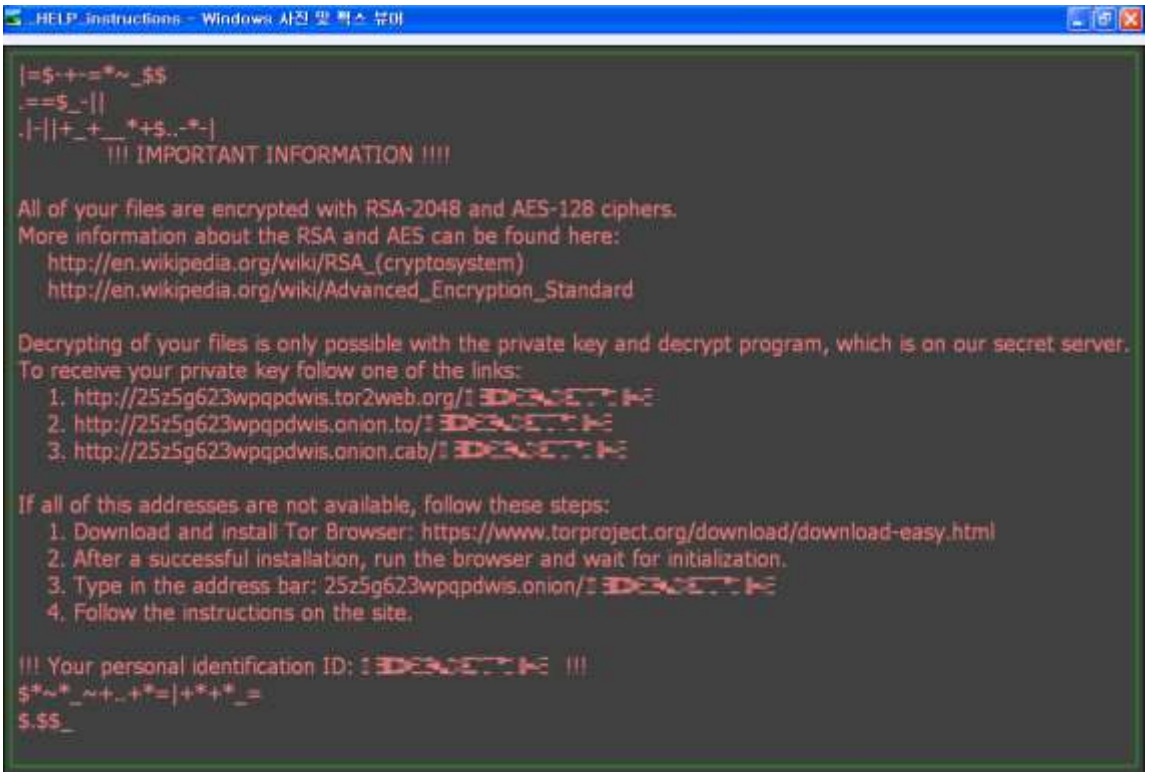
랜섬웨어가 폭발적으로 증가한 원인은 바로 "돈"이다. 공격자의 관점에서 랜섬웨어는 단기간에 즉각적인 수익을 창출하는 수단으로 입증됐기 때문이다. 2017년에도 랜섬웨어 증가 추세는 계속될 전망이다.

이 보고서에서는 지난 2016년 하반기 주요 랜섬웨어를 중심으로 최신 랜섬웨어 동향과 향후 전망을 살펴본다.

2016년 주요 랜섬웨어 상세 분석

전세계를 휩쓴 록키(Locky)

2016년을 대표하는 랜섬웨어로 꼽히는 록키(Locky) 랜섬웨어는 전세계적으로 광범위한 피해를 입혔다. 지난 1년 간 유포 방법 및 감염 방식의 변화를 통해 세를 확장해왔다. 주로 스팸 메일을 통해 유포되었는데, 특히 지난 1년 간 상상을 초월하는 양의 스팸 메일을 유포하며 악명을 떨쳤다.

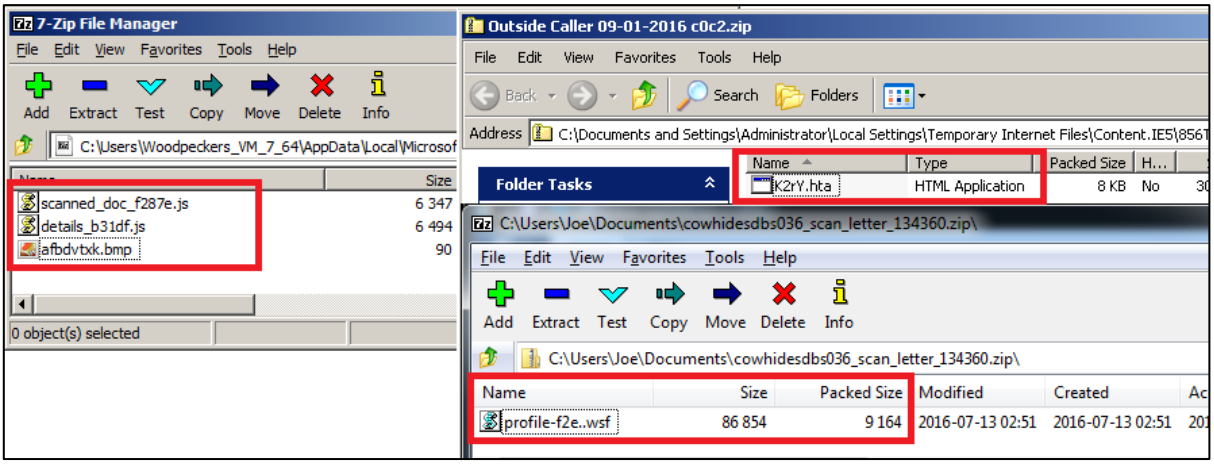


[그림 2] 록키 랜섬웨어 감염 화면

1. 록키 랜섬웨어 유포 방식

록키 랜섬웨어가 처음 등장한 것은 지난 2016년 2월로, 스팸 메일 유포로 유명한 드라이덱스(Dridex) 봇넷을 통해 이메일에 문서 파일(doc)을 첨부한 형태로 유포됐다. 2016년 3월 이후부터는 첨부파일을 스크립트 파일이 내장된 압축파일(zip)로 변경했는데, 이후 록키 랜섬웨어 유포 메일의 특징적인 방식으로 자리잡았다. 압축파일에 내장 스크립트 파일의 종류는 지속적으로 변화했는데, 3월에는 JS(Java Script), 5월에는 HTA(HTML Application), 7월에는 WSF(Windows Script File) 등을 사용하였다. 이는 스팸 필터 솔루션

이나 안티바이러스 프로그램의 탐지를 우회하기 위한 전략으로 추정된다.



[그림 3] 록키 랜섬웨어 유포에 사용된 다양한 첨부 파일

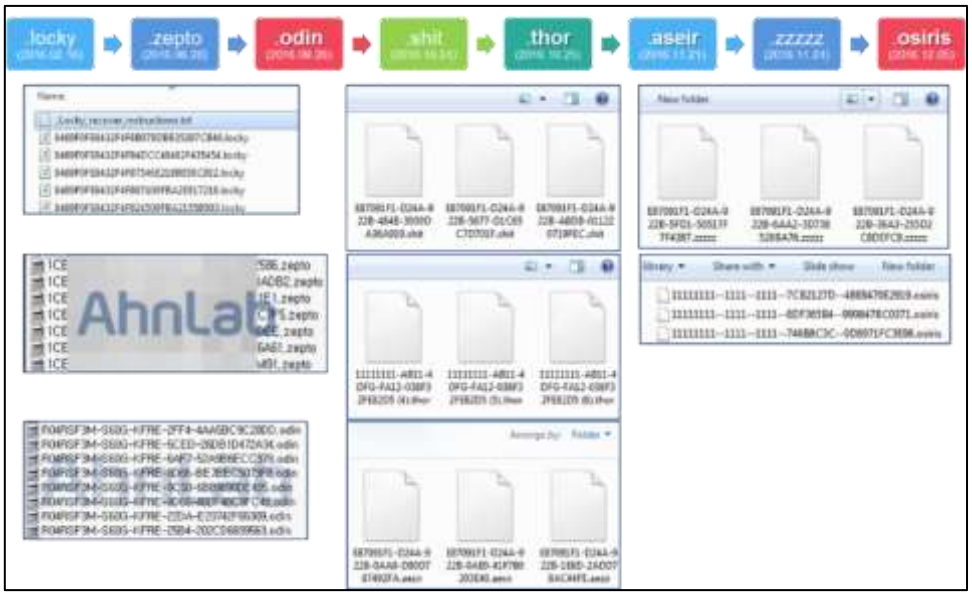
첨부파일 실행 시 다운로드되는 파일의 형태 또한 2016년 8월을 기점으로 EXE 파일(실행 파일)에서 DLL 파일(자가 실행 불가, rundll32.exe를 통해 실행)로 변경되었다. 또 2016년 11월 말부터는 DLL 파일의 확장자명을 아래 예시 같이 무작위의 3글자로 변경하여 다운로드하는 방식을 혼용하기 시작했다.

한편, 록키 랜섬웨어가 암호화하는 파일 형식에 한글 워드문서 HWP도 포함되어 있어 록키 랜섬웨어가 한국어 사용자도 노리고 있음이 확인되었다.

DLL 파일 확장자명 변경 예시
ransom.dll => ransom.zvk

2. 록키 랜섬웨어의 확장자명 변화

초기에는 파일 암호화 후 '.locky'라는 확장자명을 추가하는 형태였다. 그러나 2016년 6월부터 확장자명 변경이 시작되어 6월 말에 '.zepto', 9월 말에 '.odin', 10월 말에는 '.shit'과 '.thor'가 동시에 사용되었다. 11월 말에는 '.aesir'와 '.zzzzz'가 등장한데 이어 12월 초에 '.osiris'가 추가되는 형태도 나타났다.



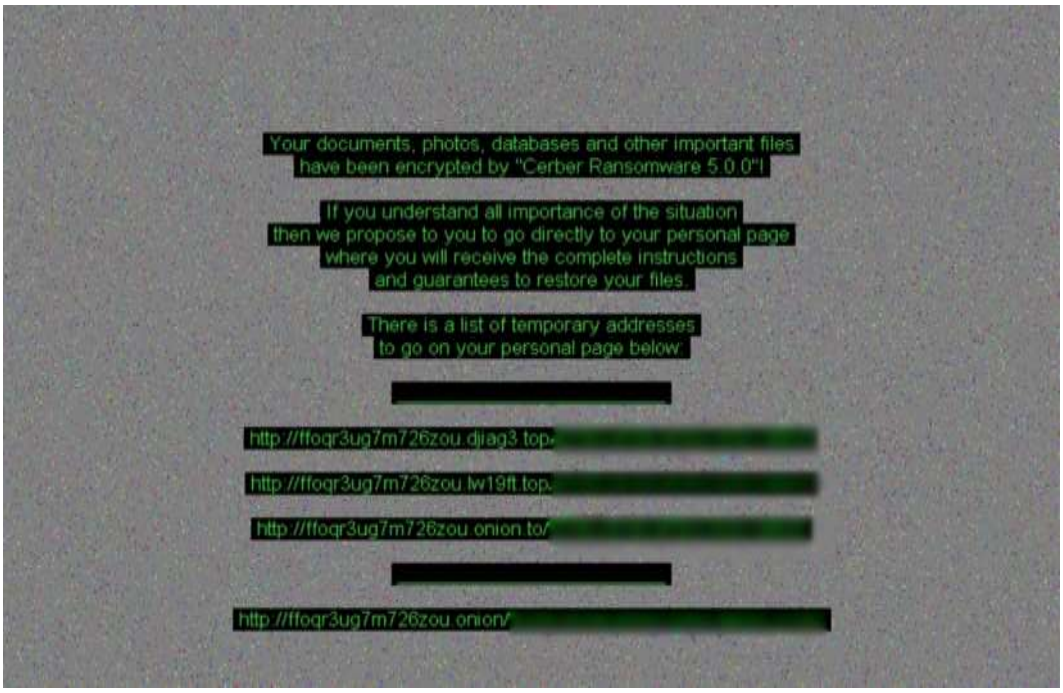
[그림 4] 록키 랜섬웨어의 감염 시 확장자명 변화

여기서 주목해야 할 점은, 우선 2016년 하반기에 들어서면서 록키 랜섬웨어의 확장자명 변경 주기가 짧아졌다는 것이다. 또 오딘(Odin), 토르(Thor), 에시르(Aesir)는 북유럽 신화에 등장하는 신들의 이름을 차용한 것이고 오시리스(Osiris)는 이집트 신화에서 차용한 이름인 반면, '.shit', '.zzzzz' 등의 확장자명은 궤를 달리하고 있다. 록키 랜섬웨어 제작 그룹이 최소 2개 이상으로 분리되어 활동하고 있는 것으로 추정되는 이유다.

한편, 지난 2016년 11월 말에는 페이스북이, 링크드인과 같은 소셜미디어 사이트의 메신저를 통해 그림 파일을 보내는 것으로 위장하여 록키 랜섬웨어를 유포한 사례도 발견됐다.

음성 지원 랜섬웨어: 케르베르(Cerber)

케르베르(Cerber) 랜섬웨어는 파일을 암호화한 후 이 사실을 음성으로 알려주는 독특한 특징을 갖고 있다. 2016년 3월 초에 발견되었으며 2016년 하반기에 더욱 활발하게 활동했다. 케르베르 랜섬웨어는 록키 랜섬웨어와 달리 변경될 때마다 새롭게 버전을 부여하는 점이 특징인데, 최근 확인된 버전은 5.0.1이다.



[그림 5] 케르배르 v5.0의 랜섬노트

1. 케르베르 랜섬웨어 유포 방식

케르베르는 록키 랜섬웨어와 마찬가지로 대표적인 악성코드 유포 방식인 스팸 메일이나 익스플로잇킷(Exploit Toolkit, 이하 EK)을 이용하여 유포되었다. 초기에는 DOCX, DOC 등의 첨부파일을 이용했지만 DOCM(Word Open XML Macro-Enabled Document file), HTA(HTML Application), VBS(Visual Basic Script) 등으로 확대했다.

익스플로잇킷은 취약한 웹사이트나 광고 모듈을 악용하는 멀버타이징(Malvertising)에 주로 사용되는 방식으로, 과거 파밍이나 온라인게임핵 악성코드 유포에 악용된 전례가 있다. 케르베르 버전 1~2는 주로 뉴클리어(Nuclear) EK, 앵글러(Angler) KE, 뉴트리노(Neutrino) EK를 통해 유포되었다. 그러나 2016년 상반기에 뉴클리어 EK와 앵글러 EK가 활동을 종료함에 따라 케르베르 버전 3는 주로 RIG, 매그니튜드(Magnitude) EK를 통해 유포되었다. 케르베르 버전 4부터는 대부분 RIG(RIG-E, RIG-V 포함), 뉴트리노 EK,

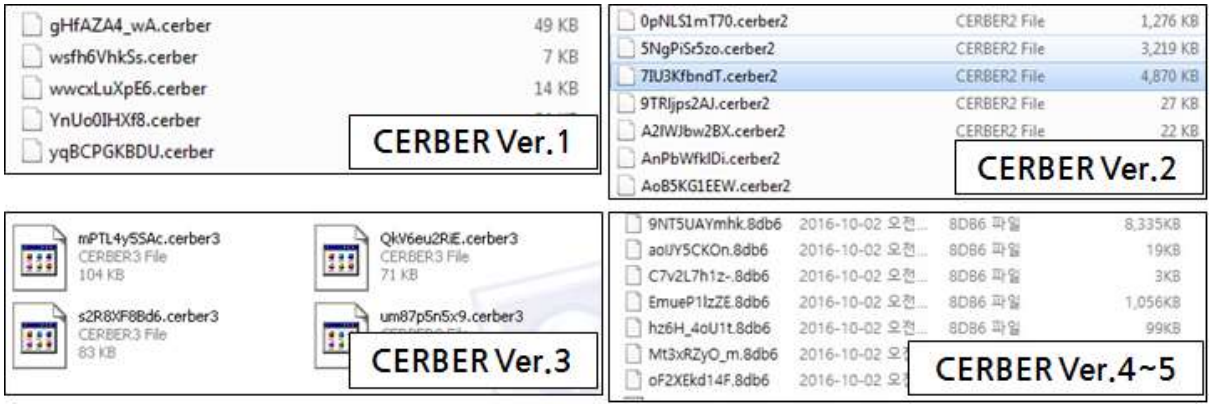
매그니튜드 EK를 통해 유포되고 있다.

이처럼 유포 시 이용하는 EK의 변경이 잦은 이유는 EK의 종류가 다양하고 활동의 부침이 심한 편이기 때문에 특정 EK에 고정되지 않고 다양한 EK를 활용하는 것으로 보인다. 또한 랜섬웨어 제작 조직이 랜섬웨어 유포 시에는 별도의 조직이 운영하는 악성코드 유포 네트워크를 활용하는 것으로 추정된다. 케르베르는 초기 버전부터 러시아의 블랙마켓에서 판매되는 것으로 확인되었다. 한편, 케르베르 랜섬웨어의 암호화 대상에는 HWP 확장자명이 포함되어 있지는 않다는 점으로 보아 한국은 집중 표적에 포함되지 않은 것으로 짐작된다.

2. 케르베르 랜섬웨어의 확장자명 변화

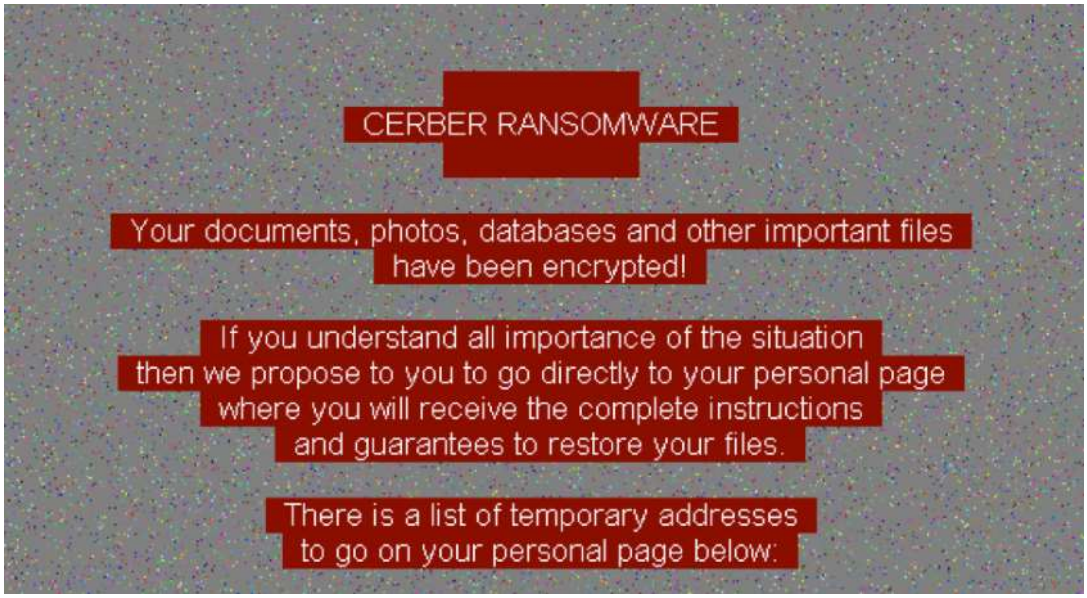
케르베르는 버전이 변경될 때마다 고유한 확장자명을 부여해왔다. 케르베르 버전 1~3까지는 '.cerber', '.cerber2', .'cerber3' 등과 같이 순차적으로 버전에 따라 확장자명이 부여됐다. 케르베르 버전 1은 지난 2016년 3월 초에, 버전 2는 8월 초, 또 버전 3는 8월 말에 발견되었다.

2016년 10월 초에 발견된 케르베르 버전 4부터는 무작위의 파일명과 4자리 확장자명으로 변경되었다. 뒤이어 11월 말에 발견된 버전 5.0도 버전 4와 동일한 확장자명을 유지하고 있다. 이때 추가되는 4자리의 확장자명은 감염 시 레지스트리에 등록하는 감염 PC의 고유 ID와 동일하다.



[그림 6] 케르베르 랜섬웨어 버전별 확장자명 변화

케르베르 버전 4부터 랜섬노트에 표시된 버전명을 확인할 수 있었지만, 2016년 12월 중순에 발견된, 이른바 크리스마스(Christmas) 버전은 버전명이 표시되지 않아 버전 확인이 어려워졌다. 앞으로 나타날 케르베르 랜섬웨어들이 버전 표시 없이 제작 및 유포될 가능성이 점쳐진다.



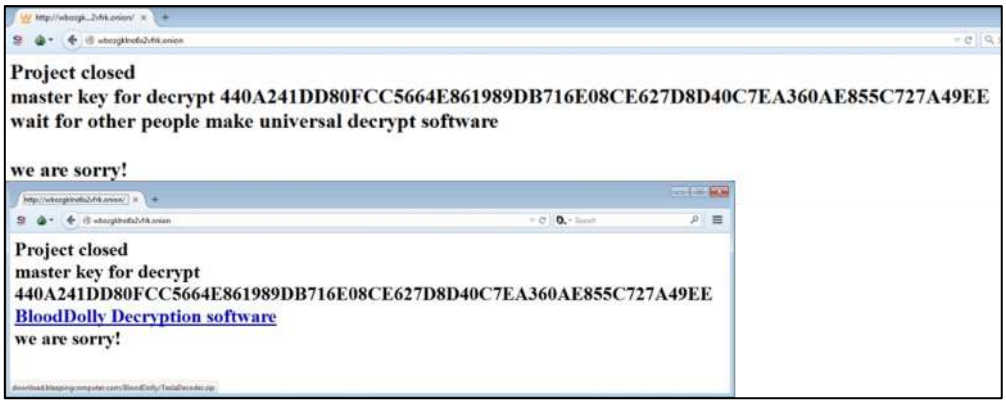
[그림 7] 버전 표시가 없는 케르베르 랜섬웨어 크리스마스 버전

갑작스럽게 활동을 종료한 크립트XXX(CryptXXX)

크립트XXX(CryptXXX)는 특히 국내에서 악명을 떨쳤는데, 2016년 6월 초 국내 스마트폰 관련 유명 커뮤니티에서 멀버타이징 기법에 의한 광고 배너를 통해 대량 유포되어 큰 피해를 입혔기 때문이다.

[그림 8] 크립트XXX 랜섬웨어

2016년 초부터 활발하게 활동하던 테슬라크립트(TeslaCrypt)가 2016년 5월 중순 갑작스럽게 활동을 종료한 이후 새롭게 등장한 것이 크립트XXX이다. 그러나 크립트XXX 또한 2016년 7월 말을 기점으로 활동이 중단됐다. 테슬라크립트는 활동 종료를 선언하면서 암호화된 파일을 복호화하는 마스터 키를 공개했다. 이에 반해 크립트XXX는 활동 종료와 관련한 별도의 언급이 없었기 때문에 활동 종료 여부를 단언할 수는 없다. 그러나 국내에서는 록키 랜섬웨어나 케르베르 랜섬웨어보다 활동이 활발했던 크립트XXX가 약 5개월 동안 나타나지 않았다는 점에서 일시적인 소강 상태로 보이지는 않는다.



[그림 9] 테슬라크립트 랜섬웨어의 활동 종료 선언 및 복호화 마스터키 공개

1. 크립트XXX 유포 방식

테슬라크립트와 동일한 형식의 랜섬노트를 사용한 크립트XXX는 지난 2016년 4월 말에 깜짝 등장했다. 스팸 메일뿐만 아니라 앵글러 EK와 뉴트리노 EK를 이용한 드라이브 바이 다운로드(Drive-by-download) 방식을 이용해 유포돼 큰 피해를 입혔다. 특히 EK를 통해 감염 시 드롭퍼(Dropper) 파일을 생성하는 대신 메모리에서만 동작하는 DLL 파일을 생성하고 암호화를 진행하는 방식을 사용했다. 또한 암호화 대상에 HWP 확장자명이 포함되어 있고, 버전 4.0부터는 랜섬노트 결제 안내 페이지에 한국어도 포함하는 등 한국 사용자도 주요 공격 대상으로 삼았다.

케르베르 랜섬웨어와 마찬가지로 변경 사항이 발생할 때마다 새로운 버전명을 부여한다. 2016년 6월 초에 발견된 버전 3.1에서는 SMB로 연결된 네트워크 공유 폴더 암호화 기법을 사용했다. 또 7월에는 보안 솔루션의 탐지 및 분석을 회피하기 위해 시스템 유입 후 일정 시간이 지난 후에 암호화를 진행하는 버전 5.0이 등장했다.

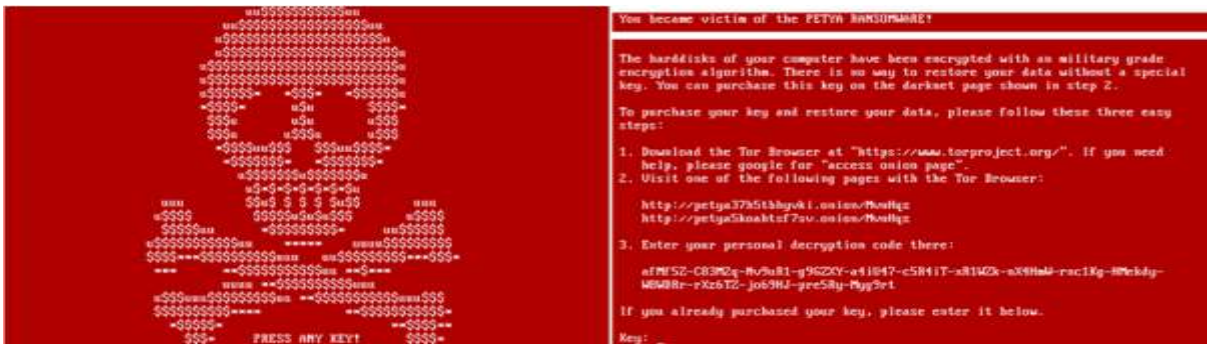
2. 크립트XXX의 확장자명 변화

2016년 4월 말 발견된 크립트XXX 최초 버전과 5월 중순에 발견된 버전 2.0은 '.crypt'를 확장자명으로 사용하였다. 이후 5월 말에 발견된 버전 3.0에서는 '.crypt' 또는 '.cryp1'을, 6월 초에 발견된 버전 3.1에서는 '.crypz'를 확장자명으로 추가했다. 버전 4.0은 암호화 후에도 확장자명을 변경하지 않음으로써 파일의 암호화 여부를 확인하기 어렵게 했다. 또 2016년 7월 초 마지막으로 발견된 버전 5.0에서는 32 자리의 무작위 파일명 변경과 함께 5 자리의 무작위 확장자명을 추가했다.

파일과 MBR을 암호화하는 랜섬웨어

1. MBR 영역을 암호화하는 페트야(PETYA)

지난 2016년 3월 말에 발견된 페트야(PETYA)는 파일을 암호화던 기존 랜섬웨어와 달리 MBR(Master Boot Record) 영역을 암호화해 충격을 주었다. 기존의 랜섬웨어는 윈도우 폴더만 암호화하지 않으면 감염 시스템을 이용하는 것에는 별다른 문제가 없었다. 그러나 페트야는 파일은 암호화하지 않는 대신, 시스템의 파티션 정보가 담겨 있는 MBR 영역과 윈도우의 NTFS(New Technology File System)에서 사용하는 파일에 관한 모든 정보가 담긴 MFT(Master File Table) 영역을 암호화하여 PC 사용 자체를 불가능하게 한다. 설사 수동으로 MBR을 복구하더라도 MFT가 암호화되어 있어 PC를 사용할 수 없다.

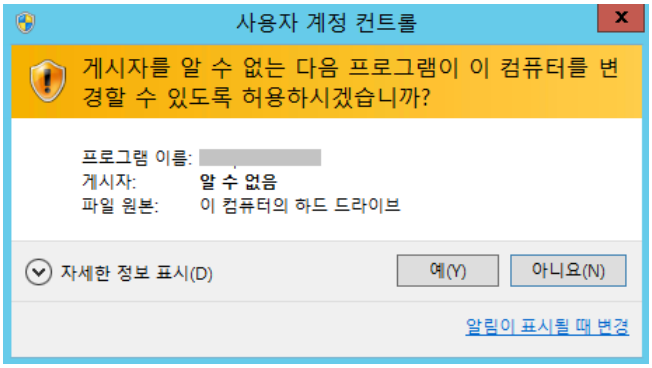


[그림 10] MBR을 암호화하는 페트야 랜섬웨어

2. MBR과 파일을 선택적으로 암호화하는 미샤(Mischa)

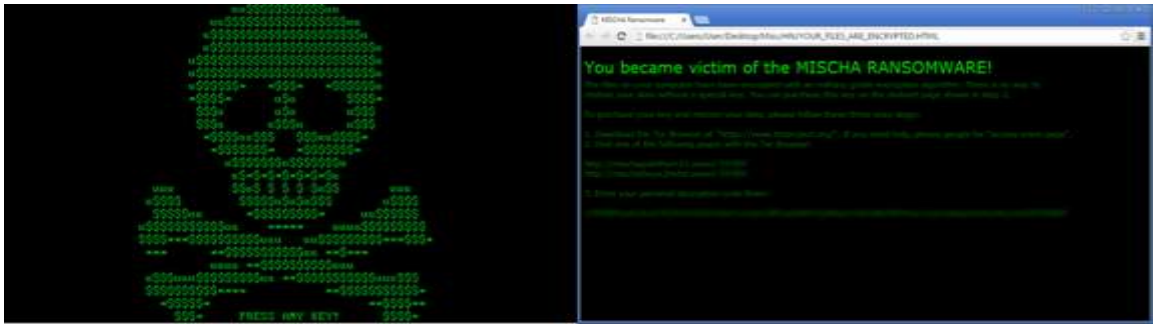
2016년 5월 중순에 발견된 미샤(Mischa) 랜섬웨어는 MBR과 파일을 선택적으로 암호화할 수 있다는 점이 특징이다. 미샤 랜섬웨어에 감염되면 [그림 11]과 같이 사용자 계정 컨트롤(User Account Control,

UAC) 창이 나타난다. 이때 사용자가 '예(Y)'를 클릭하면 MBR 영역의 암호화가 진행되고 '아니요(N)' 또는 우측 상단의 X 버튼을 누르면 파일 암호화가 진행된다.



[그림 11] 미샤 랜섬웨어가 노출하는 UAC 화면

MBR 암호화가 진행되면 페트야 랜섬웨어와 동일한 이미지가 나타나는데, 다만 붉은 색을 사용한 페트야와 달리 검은색 배경에 녹색 글씨를 사용한다는 점이 다르다. 파일 암호화 시에도 동일한 랜섬노트가 나타나는데, MBR 암호화와 달리 브라우저를 통해 출력된다. 또 파일 암호화 시에는 무작위의 4 글자가 확장자명에 추가된다.



[그림 12] 미샤 랜섬웨어

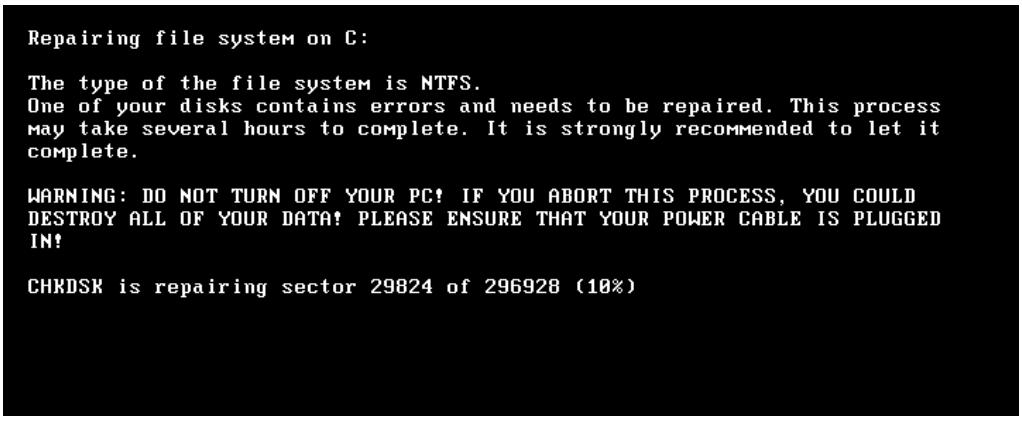
3. MBR과 파일을 동시에 암호화하는 골든아이(GoldenEye)

미샤 랜섬웨어 등장 이후 약 7개월 만인 2016년 12월 초에 발견된 골든아이(GoldenEye) 랜섬웨어는 페트야 랜섬웨어의 최신 버전이다. MBR만 암호화했던 페트야나 MBR과 파일을 선택적으로 암호화하는 미샤와 달리 파일과 MBR을 모두 암호화하는 것이 특징이다. 감염 시 파일 암호화를 먼저 진행하고, 이어 사용자 파일을 암호화한 후 무작위 8글자의 확장자명을 추가한다. 이후 MBR 영역의 부트 로더를 수정

한 다음 [그림 13]과 같은 랜섬노트를 출력한다. 이때 나타나는 화면은 페트야 랜섬웨어, 미샤 랜섬웨어와 거의 동일하며, 색상만 검은 색 배경에 노란 글씨로 변화되었다.

[그림 13] 골든아이 랜섬웨어

감염된 시스템을 재부팅하면 [그림 14]와 같이 하드디스크 점검(CHKDSK) 화면을 출력하고 진행률이 나타난다. 그러나 이는 가짜 화면이며, 실제로는 MBR 암호화가 진행되는 것이다.



[그림 14] CHKDSK로 위장한 골든아이 랜섬웨어의 MBR 암호화 화면

한편, 페트야와 미샤, 골든아이는 모두 야누스 신디케이트(Janus Syndicate)에 의해 제작된 랜섬웨어들로 알려져 있는데, 야누스 신디케이트는 영화 007 시리즈 중 골든아이(Golden Eye)편에 등장하는 범죄 조직의 이름이기도 하다.

4. 열차 시스템을 마비시킨 HDD크립터(HDDCryptor)

지난 2016년 11월 27일, 미국 샌프란시스코에서 시내 열차 시스템 중 발권 및 배차 시스템이 마비되는

사건이 발생했다. 사회기반시설의 랜섬웨어 감염으로 인해 실질적인 피해가 발생한 중요한 사례라 할 수 있다.

확인 결과, 해당 시스템이 HDD크립터(HDDCryptor)에 감염된 것으로 드러났다. HDD크립터는 MBR과 파일을 동시에 암호화하는 랜섬웨어로, 이로 인한 PC 부팅 불가가 서비스 마비의 주된 원인으로 밝혀졌다. 전체 시스템의 25%에 해당하는 2,000대 이상의 시스템이 피해를 입었고, 공격자는 7만 3,000 달러(한화 약 8천 500만원)를 요구한 것으로 알려졌다. 그러나 샌프란시스코시 교통국(San Francisco Transit Agency, SFMTA)은 실제 피해는 전체 시스템의 10%에 달하는 총 900대의 기기에서 발생했으며, 이로 인해 열차의 안전 운행 시스템이 영향 받지는 않았다고 전했다.

[그림 15] HDD크립터 감염 시 로그 파일

HDD크립터는 감염 직후 네트워크 암호 복구 툴(Network Password Recovery)을 이용해 감염 PC와연결된 공유폴더 및 네트워크 드라이브에 접근한다. 이후 오픈소스 툴인 디스크크립터(DiskCryptor)를 이용하여 PC 내 파일은 물론 공유폴더 내의 파일들까지 암호화한다. 마지막으로 MBR 영역을 수정하고 강제로 재부팅하여 정상적인 부팅이 불가능한 상태에 진입하고 랜섬노트를 출력한다.

[그림 16] HDD크립터 감염 후 재부팅 시 나타나는 랜섬노트

RaaS로 제공되는 랜섬웨어

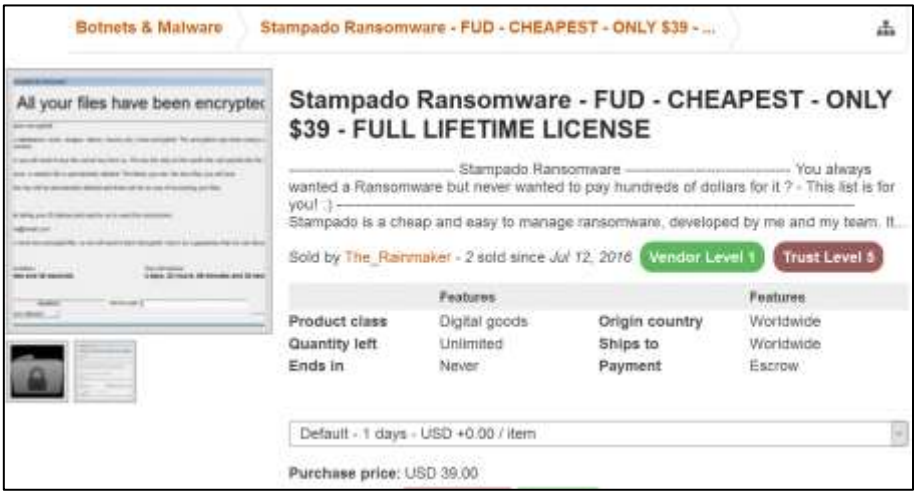
2016년 랜섬웨어 동향의 가장 큰 특징 중 하나는 RaaS(Ransomware-as-a-Service)이다. 비용만 지불하면 악성코드나 프로그래밍에 대한 전문적인 지식이 없어도 랜섬웨어를 제작하고 유포할 수 있으며, 범죄 수익 관리까지도 손쉽게 할 수 있게 된 것이다. RaaS는 다크웹과 같이 주로 공개되지 않고 익명을 보장하는 네트워크상에서 비트코인과 같이 추적이 어려운 가상 전자화폐로 거래된다. 일례로, 미샤 랜섬웨어 RaaS는 일주일당 수익이 5BTC(비트코인) 이하일 경우 수익의 25%를 제작자와 공유한다. 그러나 일주일당 수익이 125BTC 이상일 경우, 수익의 85%를 제작자와 분배하게 되어 있다.

[그림 17] 미샤 랜섬웨어 RaaS의 수익 배분 안내

2016년 상반기에는 랜섬32(Ransom32), 케르베르, 미샤 등의 랜섬웨어를 서비스하는 RaaS가 주목 받았다. 그러나 알려진 RaaS는 지극히 일부에 불과하고 알려지지 않은 다수의 RaaS가 다크웹에서 거래되고 있을 것으로 추정된다.

1. 가격 경쟁력을 내세운 RaaS: 스탬파도(Stampado)와 필라델피아(Philadelphia)

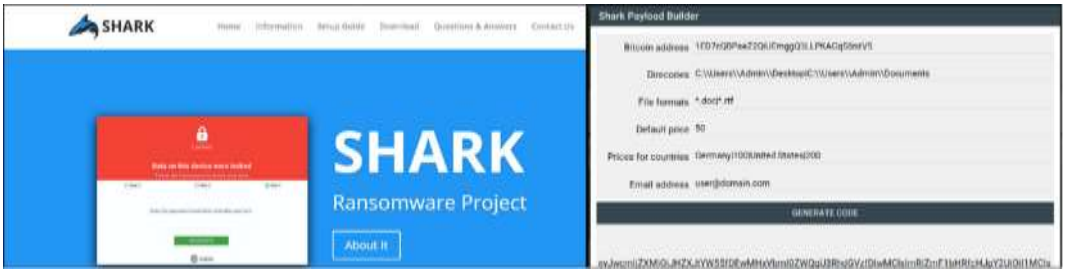
2016년 7월 중순에 발견된 스탬파도(Stampado)는 단돈 39달러라는 파격적인 가격에 서비스를 제공한다. 크립토락커와 비슷한 랜섬웨어로, '.locked'를 확장자명으로 추가한다. EXE, BAT, DLL, SCR, CMD 등 다양한 포맷의 파일을 생성할 수 있으며, 안티바이러스 제품의 탐지를 우회하는 기능도 포함하고 있다. 또한 케르베르, 테슬라크립트, 록키 등 다른 랜섬웨어에 의해 이미 암호화된 파일도 다시 암호화하는 방식이 적용되었다,



[그림 18] 파격적인 가격의 스탬파도 랜섬웨어 RaaS

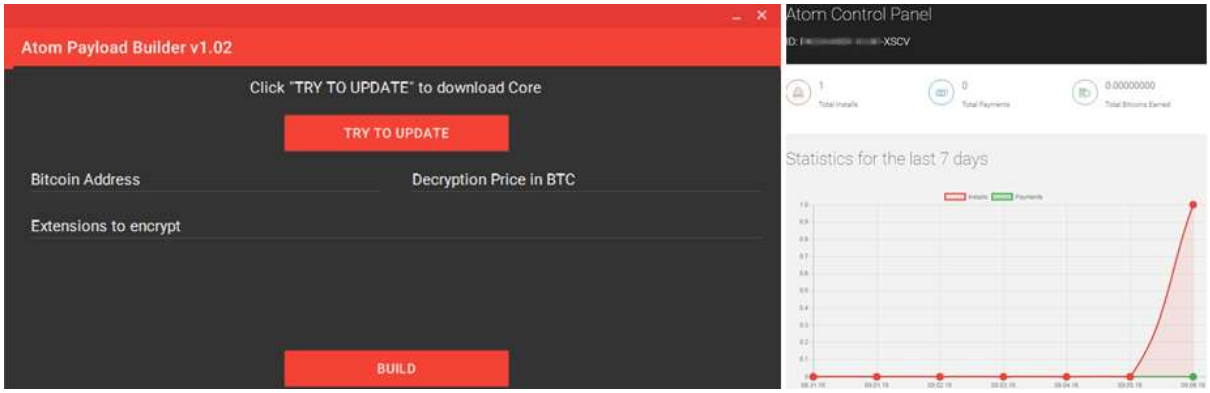
2016년 9월에 발견된 필라델피아(Philadelphia)는 스탬파도의 변형으로 알려져 있으며, 필라델피아본부(Philadelphia Headquarters)라는 관리용 콘솔도 제공한다. RaaS 비용으로 400달러를 요구하며, 확장자명은 스탬파도와 동일하게 '.locked'를 추가한다. 네트워크 드라이브와 공유 폴더, USB 드라이브를 암호화하는 기능을 갖고 있다.

2. 수익의 20%를 요구하는 샤크(Shark)와 아톰(Atom)



[그림 19] 샤크 RaaS 안내 페이지 및 파일 생성 페이지

2016년 8월 중순에 발견된 샤크(Shark)도 RaaS 형태로 제공되는 랜섬웨어다. 일반적으로 토르(Tor) 네트워크를 이용한 다크웹에서 거래되는 반면, 워드프레스(WordPress)를 이용하여 정보를 제공한다. 수익의 20%를 요구하는 것이 특징이며, 복호화 툴(Decryptor) 페이지는 30개의 언어를 지원하고 있다. 스탬파도와 마찬가지로 '.locked'를 확장자명으로 추가한다.



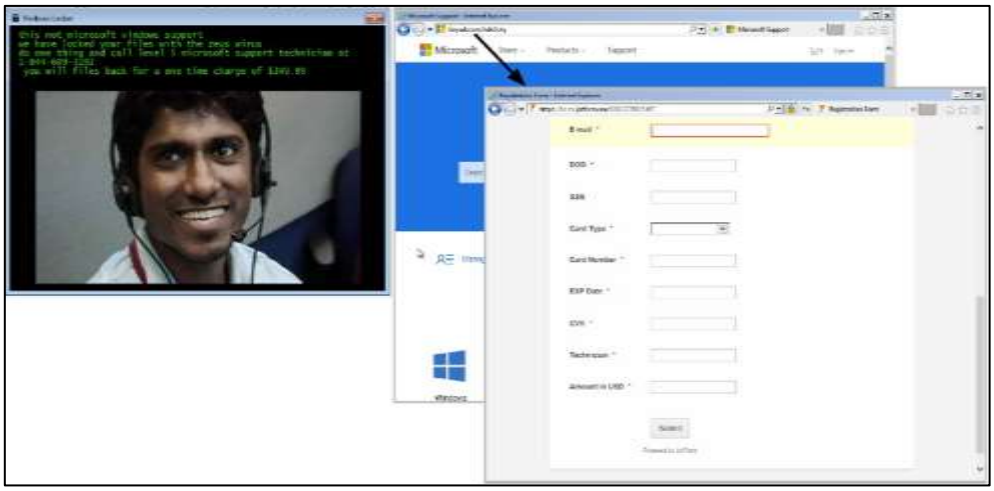
[그림 20] 편리한 기능을 제공하는 샤크의 파일 생성 및 관리 페이지

뒤이어 2016년 9월 중순에 발견된 아톰(Atom)은 샤크의 변형으로, 동일한 제작자가 만든 것으로 알려져 있다. 파일을 생성할 때마다 고유한 추적ID(Tracking ID)가 생성되고, 분석을 어렵게 하기 위한 고도의 난독화 기술이 적용되어 있다. 웹 기반의 관리 패널을 통해 유포 현황 및 통계도 쉽게 확인할 수 있다. 아톰 역시 스탬파도와 마찬가지로 '.locked'를 확장자명으로 추가하는데, 이처럼 확장자명이 같은 이유는 상당수의 랜섬웨어가 연구 및 학습 목적의 오픈소스 랜섬웨어 소스코드를 악용하여 제작되었기 때문으로 추정된다.

국가별 랜섬웨어와 사회공학기법

1. 인도: 콜센터까지 제공하는 VindowsLocker

2016년 11월 말에 발견된 VindowsLocker는 마이크로소프트(Microsoft)의 기술지원센터로 위장한 콜센터까지 운영했다. 감염 시 확장자명으로 '.vindows'를 추가하는데, Vindows는 윈도우(Windows)의 인도식 표기이다.



[그림 21] 실제 콜센터를 운영한 VindowsLocker

VindowsLocker에 감염되면 복구 비용으로 350달러를 요구하며 콜센터 번호를 안내한다. 해당 번호로 전화를 하면 원격지원 연결을 유도한다. 원격지원이 연결되면 마이크로소프트의 기술지원 홈페이지 창을 띄운 후 수동으로 재빨리 가짜 창으로 바꿔치기 하고 결제정보 입력을 요구한다. 그러나 코드 완성도가 낮아 파일 복구가 이루어지지 않을 가능성이 높다.

2. 이슬람 국가: 포켓몬고(PokemonGo) 게임으로 위장한 랜섬웨어

[그림 22] 포켓몬고 게임으로 위장한 랜섬웨어

지난 해 선풍적인 인기를 끌었던 포켓몬고(PokemonGo) 게임으로 위장한 랜섬웨어가 2016년 8월 중순 등장했다. PokemonGo.exe라는 파일명으로 위장했으며, 게임의 주요 캐릭터인 피카츄의 이미지를 실행

파일의 아이콘으로 사용했다. 또 암호화 후 출력하는 랜섬 노트가 아랍어로 표기되어 있어 이슬람 국가의 사용자들을 노린 것으로 추정된다. 공유폴더를 암호화하는 코드가 포함되어 있지만 실제로 사용되지는 않는다. 파일 암호화 후 '.locked'를 확장자명으로 추가한다. 실행 시 'Hack3r'라는 이름의 윈도우 관리자 계정을 생성하는데 추후 백도어로 활용하기 위한 것으로 보인다.

3. 한국: 카카오톡으로 위장한 랜섬웨어

한국에서는 이른바 '국민메신저'로 불리는 카카오톡으로 위장한 랜섬웨어가 발견되었다. 2016년 8월에 발견되었으며, 한국어로 구성되어 있다. 또 파일 암호화 후 '.암호화됨'이라는 한글로 된 확장자명이 추가된다. 오픈소스 랜섬웨어인 히든 티어(Hidden Tear) 소스코드를 악용한 랜섬웨어다.

[그림 23] 카카오톡 메신저로 위장한 랜섬웨어

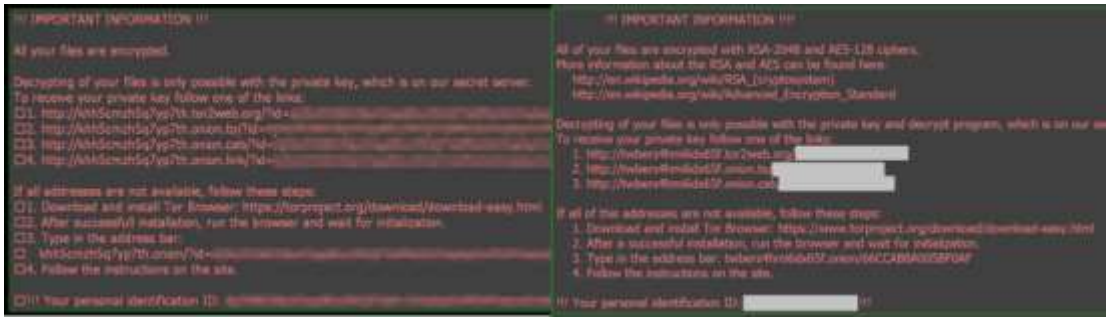
4. 미국: 대통령 선거 이슈를 노린 랜섬웨어

[그림 24] 미국 대선 후보의 이름을 도용한 랜섬웨어

미국 대통령 선거가 한창 진행 중이던 지난 2016년 9월 말, 당시 대선 후보였던 도널드 트럼프의 사진과 이름을 도용한 랜섬웨어가 발견되었다. 실행되면 '.encrypted'라는 확장자명이 추가되지만 실제 파일 암호화는 진행되지 않았다. 개발 중이던 파일이 외부로 유출된 것으로 추정되는데, 실제로 유포되어 피해를 입힌 사례는 확인되지 않았다. 한편, 파일 내부에는 실제 암호화 함수가 포함되어 있으며, 화면의 언락(Unlock) 버튼을 클릭하면 파일명이 원상 복구된다.

기존 랜섬웨어를 모방한 랜섬웨어

1. 록키 랜섬웨어와 매우 유사한 바트(Bart)



[그림 25] 바트 랜섬웨어(왼쪽)와 록키 랜섬웨어(오른쪽)의 랜섬노트

2016년 6월 말에 발견된 바트(Bart) 랜섬웨어는 록키와 매우 유사한 형태를 보인다. 록키 제작자 중 한 명 또는 일부가 만든 것으로 알려져 있다. 다운로더 역할을 하는 자바 스크립트 파일을 암호화 압축하여 스팸 메일에 첨부하는 방법으로 유포되었다. 자바 스크립트 파일과 스팸 메일을 이용하는 방법 또한 록키 랜섬웨어와 동일하다.

랜섬노트에 사용된 언어 역시 영어, 스페인어, 프랑스어, 독일어 등으로 록키와 거의 동일하게 구성하고 있다. 운영체제 언어가 러시아어, 벨로루시어, 우크라이나어로 설정되어 있으면 실행되지 않는 점으로 미루어 동유럽 혹은 러시아 쪽에서 제작된 것으로 추정된다.

2. 크립트XXX와 닮은 크립트MIC(CryptMIC)

[그림 26] 크립트XXX 4.0과 아주 유사한 크립트MIC

2016년 상반기를 휩쓸었던 크립트XXX와 매우 유사한 크립트MIC(CryptMIC)이 2016년 7월 말에 발견되었다. 크립트XXX를 흉내냈거나 크립트XXX 제작 그룹 중 일부가 만든 것으로 추정되었다. 감염 방식, 비트코인 요구, 통신 방법 등 크립트XXX와 상당한 유사점을 보이며, 특히 확장자명 변경이 없다는 점과 랜섬노트의 형태가 크립트XXX 4.0과 매우 유사하다.

3. CTB-록커 닮은꼴 마르스조크(MarsJoke)

크립토락커, 크립토월, 테슬라크립트와 함께 2015년 랜섬웨어 4대천왕으로 군림했던 CTB-록커(CTB-Locker)를 모방한 랜섬웨어도 발견되었다. 2016년 9월 중순부터 10월 초 사이에 발견된 마르스조크(MarsJoke)는 CTB-록커의 닮은꼴로 유명해졌으며, 주로 미국 정부기관 및 교육기관을 노렸던 것으로 알려져 있다. 확장자명을 변경하지 않아 암호화 여부를 인지하기 어렵고, CTB-록커와 마찬가지로 암호화된 파일을 최대 5개까지 무료로 복호화 해준다.

[그림 27] CTB-록커(왼쪽)과 마르스조크(오른쪽) 랜섬노트

4. 록키를 모방한 헝가리의 허키(Hucky)

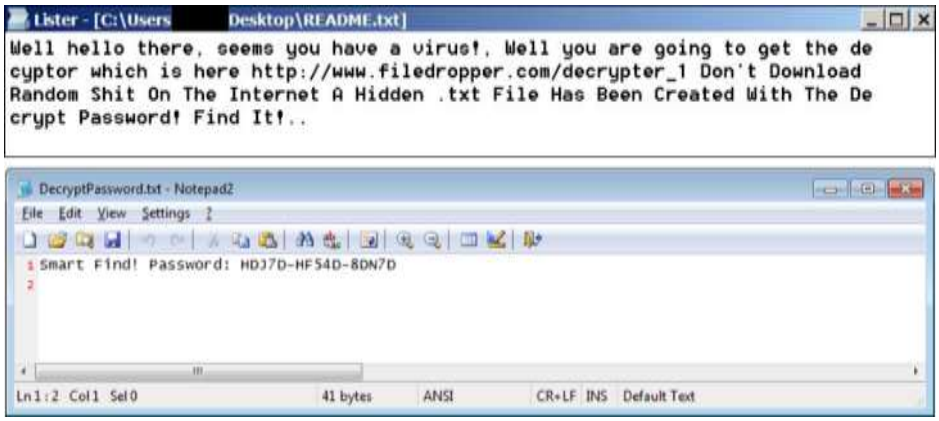
[그림 28] 록키(왼쪽)과 허키(오른쪽) 랜섬노트

2016년 10월 말, 헝가리에서 발견된 허키(Hucky) 랜섬웨어는 이른바 가짜 록키 랜섬웨어로 유명하다. 허키는 헝가리안 록키(Hungarian Locky)를 조합한 명칭이며, 랜섬노트는 영어와 헝가리어로 표시된다. 파일명은 더미로 바꾸고 확장자명에 '.locky'를 추가한다. 그러나 정작 록키 랜섬웨어는 2016년 6월 이후로 더 이상 '.locky' 확장자명을 사용하지 않고 있다. 또한 록키 랜섬웨어는 Visual C++로 작성된 것에 반해 허키 랜섬웨어는 Visual Basic으로 작성되어 있다.

스타크래프트2, 월드오브탱크, 마인크래프트 등의 게임 파일도 암호화 하는 것으로 알려져 있으며, 헝가리어로 nothing을 의미하는 semmi.exe와 헝가리 전설 속의 새 이름인 turul.exe라는 이름으로 유포되었다.

교육 및 연구 목적의 랜섬웨어

1. 경각심을 주기 위한 에듀크립트(Educrypt)



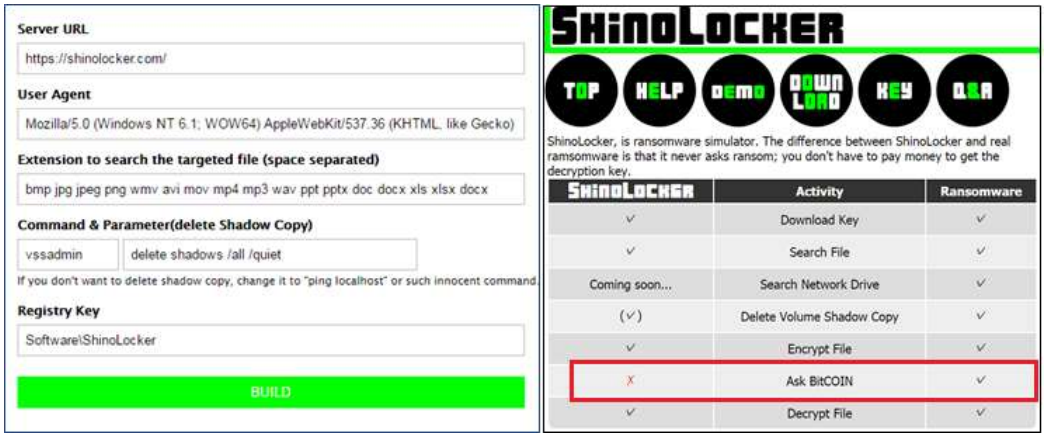
[그림 29] 에듀크립트(Educrypt)의 감염 메시지

2016년 6월말에 발견된 에듀크립트(Educrypt)의 주 목적은 돈이 아니라 사용자에게 경각심을 심어주는 것이다. 감염되면 '인터넷에서 랜섬웨어를 다운로드 하지 말라'는 메시지를 보여주며 복호화 패스워드를 제공한다. 패스워드는 항상 같은 값으로 고정되어 있다. 오픈소스 랜섬웨어인 히든티어(Hidden Tear) 기반으로 제작되었으며, '.isis'를 확장자명에 추가한다.

2. 랜섬웨어의 모든 과정을 체험할 수 있는 시노락커(ShinoLocker)

2016년 8월 초에 발견된 시노락커(ShinoLocker)는 랜섬웨어 제작부터 복구까지의 전 과정을 직접 체험할 수 있다. 보안 연구원이 조직의 보안 수준과 효율성을 점검하기 위해 제작한 것으로 알려져 있다. 감염 시 메모리상에 존재하는 복호화 키를 추출하기 위한 포렌식 기술 향상의 목적으로도 활용 가능하다.

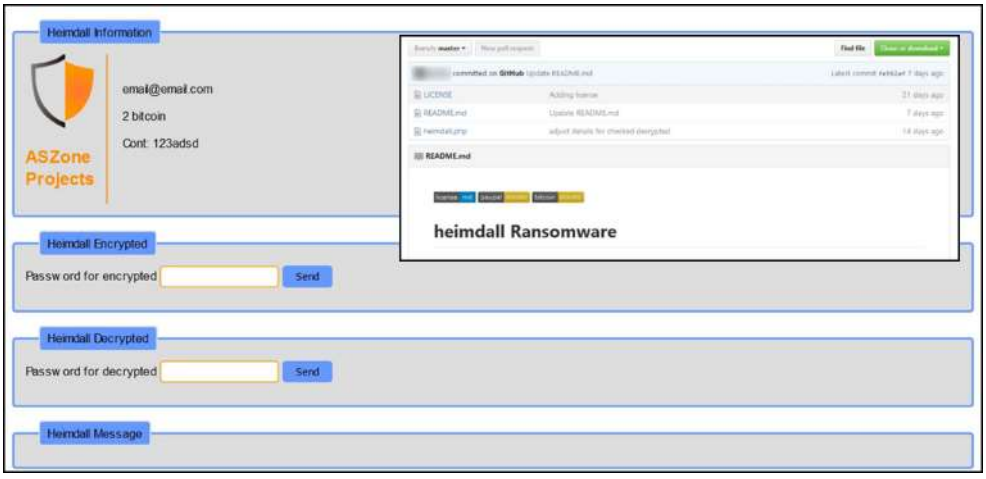
RaaS와 같이 웹페이지를 제공하며, 각종 기능과 옵션을 직접 설정할 수 있다. 암호화에 성공하면 '.shino' 확장자명이 추가되며, 별도의 복구 비용은 요구하지 않는다. www.shino.com 웹사이트를 통해 테스트를 할 수 있다. 단, 실제 랜섬웨어와 상당히 유사하게 제작되어 있어 취급에 주의가 필요하다.



[그림 30] 랜섬웨어 시뮬레이터로 활용 가능한 시노락커

3. PHP 기반의 연구용 헤임달(Heimdall)

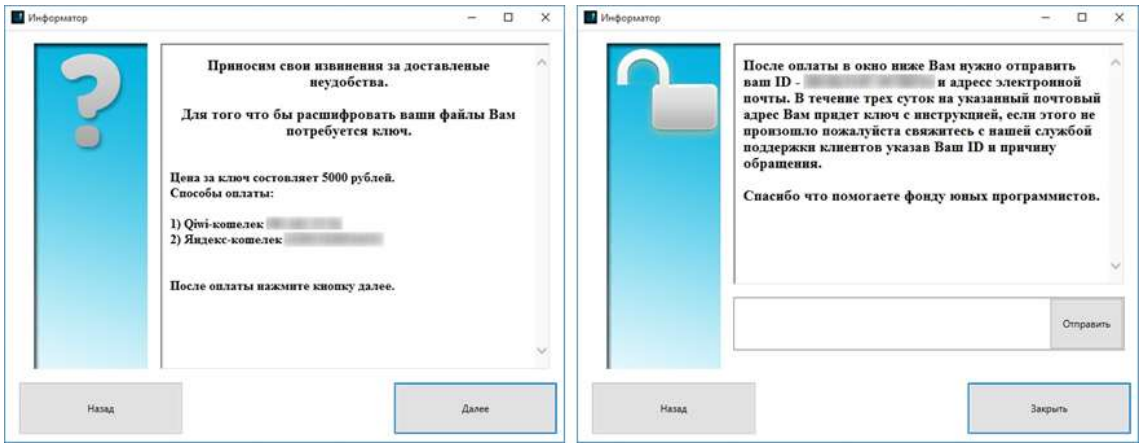
2016년 11월 초에 발견된 헤임달(Heimdall)은 웹 서버를 대상으로 하는 PHP 기반의 오픈소스 랜섬웨어로, 브라질 개발자가 교육 및 연구 목적으로 한정하는 조건으로 2016년 10월 말에 깃허브(Github)에 공개했다. 공격자가 암호를 입력하면 암호화가 진행되며, 웹 서버의 웹페이지 루트 경로에 존재하는 모든 폴더와 파일을 암호화한다. 암호화되면 파일명 앞에 'Heimdall--'을 추가한다.



[그림 31] PHP로 제작된 오픈소스 랜섬웨어 헤임달

그 외 주목할 만한 랜섬웨어

1. 텔레그램 메신저의 프로토콜을 이용하는 텔레크립트(Telecrypt)

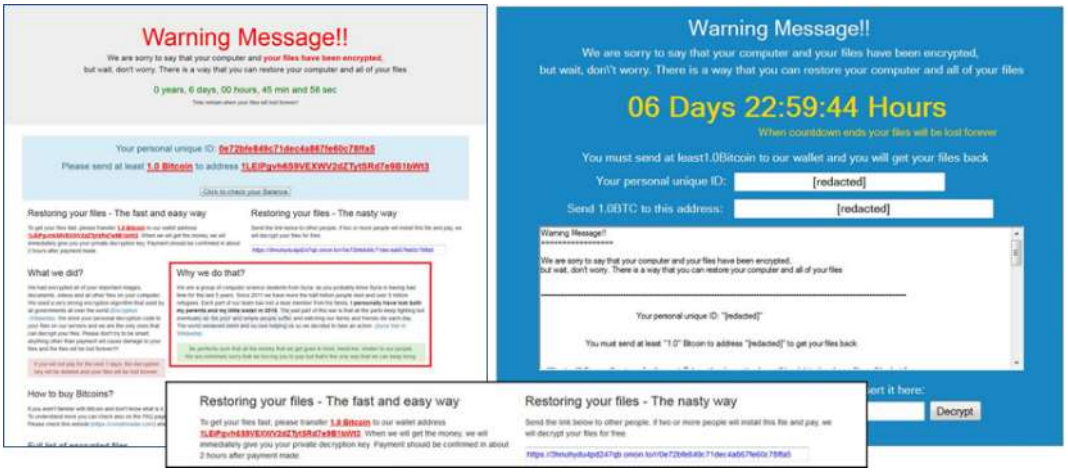


[그림 32] 텔레그램 메신저의 프로토콜을 이용하는 텔레크립트

2016년 11월 초에 발견된 텔레크립트(Telecrypt)는 유명 메신저 프로그램인 텔레그램(Telegram)의 통신 프로토콜을 최초로 사용한 랜섬웨어로 유명하다. 텔레크립트는 감염 시 발생하는 통신 패킷의 내용을 보호하기 위해 텔레그램의 API를 이용하여 통신 암호화 기법을 적용한다. 텔레그램 메신저는 높은 보안성으로 유명한 프로그램이다. 러시아어 사용자를 대상으로 하며, 델파이로 작성되었다. 암호화 후 '.Xcri' 라는 확장자명을 추가하거나 확장자명을 변경하지 않기도 한다.

2. 인질을 요구하는 악질적인 팝콘타임(Popcorn Time)

2016년 12월 초에 발견된 팝콘타임(Popcorn Time)은 감염 시 금전 지불 외에 또 다른 선택을 제공한다. 두 명 이상을 추가로 랜섬웨어에 감염시킬 경우 무료로 복구 키를 제공하는 것이다. 스스로도 '끔찍한 방법(The nasty way)'이라고 언급하면서 랜섬웨어를 타인에게 전달하기 위한 전용 URL을 제공하고 있다. 또 2시간 이내에 복구 비용을 지불하지 않거나 4번 이상 잘못된 값을 입력하면 암호화한 파일을 삭제한다. 암호화 후 확장자명에 '.filock' 또는 '.kok'를 추가한다. 팝콘타임 랜섬웨어 제작자는 랜섬노트를 통해 수익금(?)은 시리아 내전 피해자 지원에 사용될 것이라고 주장하고 있다.

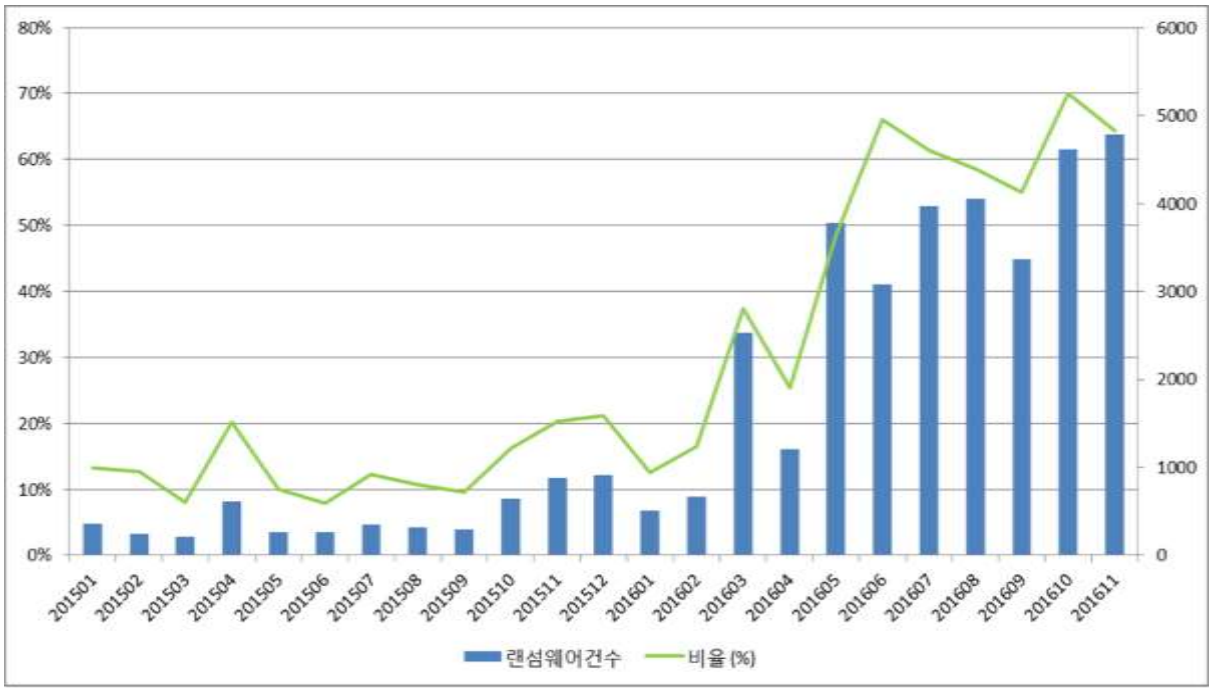


[그림 33] 팝콘타임 랜섬웨어

최신 랜섬웨어 동향

2016년 한해 동안 지속적으로 증가하던 랜섬웨어는 특히 하반기에 들어 더욱 기승을 부렸다. ASEC에 신고되는 보안 침해 사고의 비율만 보더라도 2016년 초에는 전체의 15%에 불과하던 것이 11월 말에는 4배 가량 증가해 60% 이상을 차지했다.

[그림 34]의 최근 2년간의 랜섬웨어 신고 건수를 살펴보면, 2015년 4월 유명 커뮤니티사이트를 통한 크립토락커(CryptoLocker) 유포로 랜섬웨어 신고 비율이 증가한 것을 알 수 있다. 이후 2016년 3월에 록키(Locky)와 케르베르(Cerber)가 등장하면서 본격적인 랜섬웨어 증가 추세가 나타나며, 5월 이후에는 랜섬웨어 관련 문의가 폭발적으로 증가한 것을 알 수 있다.



[그림 34] 2015년~2016년 랜섬웨어 신고 추이

일반적인 악성코드는 다양한 경로를 통해 시스템을 감염시키고 내부에 침투하여 중요 정보를 유출하는 악의적인 행위를 수행한다. 대개 정보를 파괴하는 방식보다는 탈취한 내부 기밀 정보를 두고 피해자와 협상을 벌이는 행태를 취한다. 이때 협상이 원활하지 않으면 탈취 정보의 공개 등으로 협박하거나 제3자에게 판매하는 경우도 있다.

피해자 관점에서 정보 자료 파괴에 대한 두려움 보다는 기밀 자료의 외부 유출에 대한 공포가 더 크기 때문이다. 따라서 피해자에게 중요도가 높은, 외부에 알려지길 원치 않는 기밀 자료일수록 공격자에게도 가치가 높은 매력적인 타깃(target)이 된다.

이에 반해 랜섬웨어는 감염 후 PC 내 자료를 암호화하는 악성코드로, 정보를 탈취하는 대신 피해자가 파일을 이용하지 못하게 하는데 집중한다. 공격자, 즉 랜섬웨어 제작자 관점에서는 정보 유출이 목적이 아니기 때문에 암호화된 자료의 중요도는 중요하지 않다.

물론, 피해자에게 중요한 자료일수록 복구 비용을 지불할 가능성이 높아지겠지만, 만일 비용을 지불하지 않는다면 망설임 없이 암호화된 정보를 삭제해버리면 그뿐이다. 다른 악성코드와 마찬가지로 랜섬웨어 역시 피해자에게 공포를 유발하지만, 차이는 자료의 파괴 자체에 대한 공포감이다.

	일반 악성코드	랜섬웨어
제작 및 유포 목적	• 정보 유출 및 이슈화를 통한 수익 추구	• 즉각적, 직접적 수익 창출
감염 방식 및 악성 행위	• 악성코드를 통한 내부 시스템 침입 • 직접 정보 탈취 및 유출	• 악성코드를 통한 PC 감염 • 피해 시스템(PC) 내 파일 암호화
금전적 수익 구조	• 정보 공개를 빌미로 협박 • 정보 요구자에 재판매	• 복호화 키 제공을 조건으로 금전 요구 • 직접적인 수익 발생 가능
정보 중요도/민감도	• 피해자: 중요(내부 기밀자료) • 공격자: 중요(금전적 가치 존재 필요)	• 피해자: 중요(개인적 소장 가치 또는 업무 자료) • 공격자: 자료 중요도 무관 (이익 창출의 수단에 불과)

[표 1] 일반 악성코드와 랜섬웨어의 차이점

최근의 랜섬웨어는 크게 (1)사용자에게 잘 알려져 있는 유형 (2)자체 개발 후 타인에게 판매하는 유형 (3)오픈소스를 활용한 유형 등으로 구분할 수 있다. 특히 (2)개발 후 판매하는 랜섬웨어 형태를 RaaS(Ransomware as a Service)라고 하는데, 이것이 2016년 랜섬웨어의 가장 큰 특징이다. 또 (3)연구 및 공부 목적으로 제작된 오픈소스 형태의 랜섬웨어는 본래의 의도와 달리 랜섬웨어 유포를 활성화하는 원인이 되기도 했다. 최신 랜섬웨어의 동향을 좀 더 자세히 살펴보면 다음과 같다.

랜섬웨어 제작 방식

1. 수익금의 재투자

랜섬웨어의 제작부터 감염까지의 과정을 간략하게 정리하면, 악성코드 제작자가 랜섬웨어를 만들어 악성코드 유포 그룹에게 넘기고, 유포 그룹이 대량으로 랜섬웨어를 유포하여 사용자들을 감염시키는 형태다. 이후 피해자가 복구 비용을 지불하면, 랜섬웨어 제작자와 유포 그룹이 일정한 비율로 수익을 배분한다.

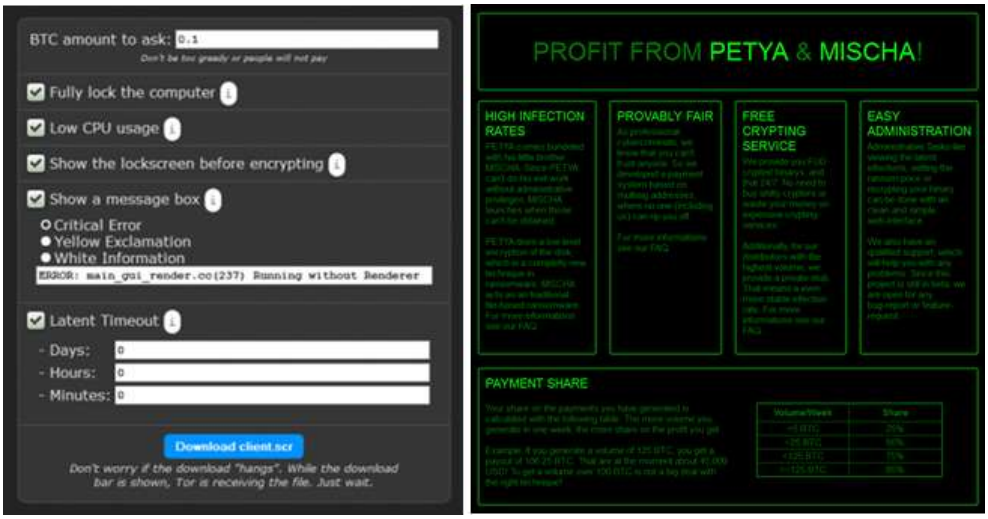
일부 악명 높은 랜섬웨어의 경우, 막대한 수익을 거둬들이고 수익의 일부를 랜섬웨어의 기능 강화에 재투자하는 것으로 보인다. 감염 기법을 바꾸거나 안티바이러스 등 보안 솔루션의 탐지를 우회하고, 암호화 범위를 확대하거나 암호화 방법을 개선하여 효율을 높였다. 또 오류 여부를 점검하는 품질 보증(QA) 과정까지 도입하기도 했다. 이렇게 더욱 개선된 랜섬웨어를 다시 유포 그룹에게 전달하여 또 수익을 얻고 지속적으로 기능 개선에 재투자하는 등 규모의 경제를 이루는 형세다. 이처럼 공격자 측면에서 경제적 효과를 거둔 랜섬웨어로는 케르베르, 록키, 크립토락커, 테슬라크립트, 크립트XXX, CTB-락커, 크립토월 등이 있다.

2. 랜섬웨어의 서비스화: RaaS

최근의 랜섬웨어는 제작자에 의한 단방향적인 판매가 아니라 구매자가 원하는 요구 사항을 반영해 제작과 유포가 가능하도록 서비스 형태로 거래되고 있다. 이를 RaaS(Ransomware as a Service)라고 부른다.

구매자는 랜섬웨어 파일 유형, 암호화 대상, 랜섬웨어 유포 방법 등 다양한 요소를 선택 및 요구할 수 있으며, 심지어 이런 요구 사항을 쉽고 빠르게 반영할 수 있도록 자동화 환경이 구축되어 있는 경우도 있다. 제작자는 구매자가 이용한 랜섬웨어를 통해 발생한 수익의 일부를 비용으로 요구한다.

RaaS의 장점은, 우선 구매자들이 프로그래밍 등 IT 전문 지식이 부족하더라도 비용만 지불하면 손쉽게 랜섬웨어를 제작 및 유포할 수 있다는 점이다. 또 초기 자금이 부족한 랜섬웨어 제작자 관점에서는 자금 확보에 유용한 방법이라 할 수 있다. 록키 랜섬웨어와 케르베르 랜섬웨어도 초기에는 이 같은 방법을 통해 확산되었으며, 이 밖에도 Ransom32, 페트야, 미샤, 스탬파도(Stampado), 필라델피아(Philadelphia), 샤크(Shark), 아톰(Atom) 등이 있다.



[그림 35] Ransom32와 미샤 랜섬웨어의 서비스(RaaS) 안내 화면

3. 오픈소스 랜섬웨어

오픈소스가 갖는 개방성이라는 특징으로 인해 악용될 경우 누가 책임질 것인가에 관한 논쟁은 오픈소스라는 개념이 처음 등장한 이후부터 현재까지 계속되고 있다. 오픈소스는 집단 지성을 활용한 정보 공유를 통해 기술 발전을 도모할 수 있다는 긍정적인 측면이 크지만 단순히 공짜라는 점만 관심을 갖는 일부의 인식이나 범죄에 악용될 소지가 있다는 점 또한 간과할 수 없다.

순수한 연구 또는 교육 목적으로 제작한 오픈소스 랜섬웨어 역시 이러한 논쟁에서 벗어날 수 없다. 선의의 목적으로 제작하여 사용 범위를 제한하는 공지와 함께 공개하더라도 범죄자들은 이러한 제약 사항에 대한 관심은커녕 거리낌없이 악용하기 때문이다. 지난 2016년 발견된 랜섬웨어 중 상당수가 오픈소스 기반의 랜섬웨어였다.

한편 RaaS가 완제품을 구입하는 것이라면 오픈소스 랜섬웨어는 직접 조립해서 사용해야 하는 DIY로 비유를 할 수 있다. 별다른 IT 관련 지식이 없더라도 비용만 지불하면 손쉽게 랜섬웨어를 제작하고 유포할 수 있는 RaaS에 비해 오픈소스 랜섬웨어는 코드를 작성 또는 수정할 수 있는 스킬이 있어야 한다. 대표적인 오픈소스 랜섬웨어로는 히든 티어(Hidden Tear), EDA2, 헤임달(Heimdall) 등이 있으며, 그 밖의 오픈소스 랜섬웨어는 대부분 히든 티어와 EDA2 랜섬웨어를 기반으로 제작되었다.

[그림 36] 오픈소스 랜섬웨어

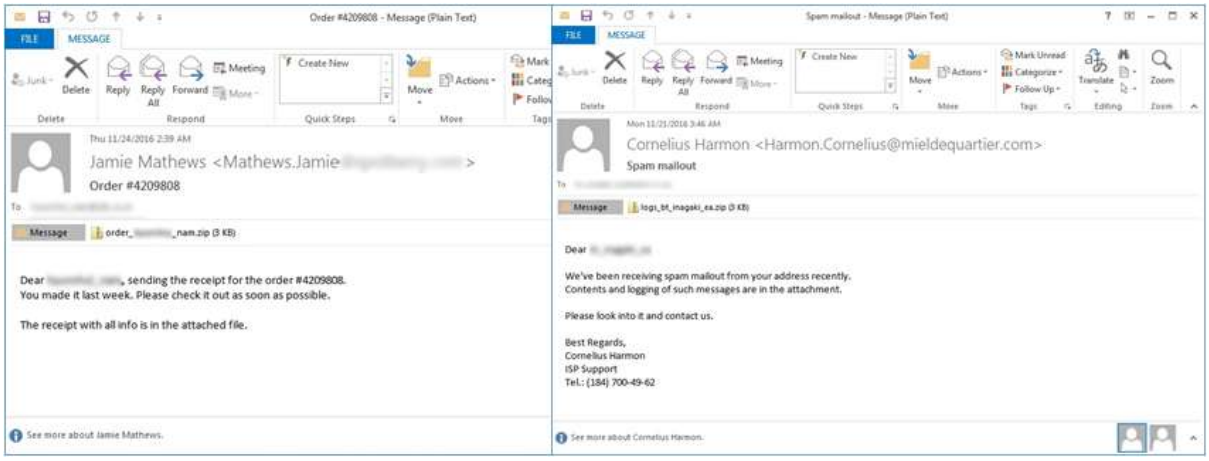
랜섬웨어 유포 방식

랜섬웨어 제작 방식의 변화와 더불어 랜섬웨어 유포 방식 또한 다변화되면서 더 큰 피해를 낳고 있다. 대표적인 랜섬웨어 유포 방식으로는 ▲스팸 메일 ▲익스플로잇킷(EK) ▲멀버타이징(Malvertising) 등이 있다. 또 최근에는 원격 데스크톱 프로토콜을 이용한 랜섬웨어 유포도 지속적으로 확인되고 있다.

유포 방식	주요 특징
스팸 메일	• 전통적인 악성코드 유포 기법 • 이메일 제목 및 내용, 첨부 파일 등으로 사용자를 속여 메일 또는 첨부 파일을 열도록 유도
익스플로잇킷(EK)	• 웹 취약점(Drive-by-download) 이용 • 불특정 다수의 감염에 효과적 • 다양한 EK 그룹 활동 중
멀버타이징	• EK와 광고 모듈이 결합된 방식 • 불특정 다수의 감염에 효과적

[표 2] 랜섬웨어 주요 유포 방식

1. 스팸 메일을 이용한 랜섬웨어 유포



[그림 37] 스팸 메일을 이용한 랜섬웨어 유포

전통적인 악성코드 유포 기법인 스팸 메일은 랜섬웨어 유포에도 활발하게 사용된다. 록키 랜섬웨어와 케르베르 랜섬웨어도 주로 스팸 메일을 통해 유포되고 있다. 스팸 메일은 사용자를 속이기 위한 사회공학적 기법을 많이 사용한다. 국내 스팸 메일은 이벤트, 경품, 배송 관련 메일로 위장하는 편이며 해외에서는 주로 송장(invoice), 금융 안내, 이력서 등으로 위장한 사례가 많다. 첨부 파일을 사용자가 직접 실행해야 한다는 단점이 있다.

최근 이메일에 첨부된 EXE 파일에 대한 차단이 강화되면서 암호가 설정된 압축 파일이나 난독화된 스크립트 파일을 이용하여 보안 솔루션의 진단과 탐지를 우회하는 형태를 보인다. 스팸 메일로 유포된 대표적인 랜섬웨어로는 록키, 케르베르, 페트야, 미샤, 골든아이, 테슬라크립트 등이 있다.

2. 불특정 다수의 최대 감염을 노리는 익스플로잇킷

취약한 웹사이트를 통해 악성코드를 유포하는 기법인 드라이브 바이 다운로드(Drive-by-download)에 필수적으로 사용되는 것이 익스플로잇킷(Exploit Kit, EK)이다. 익스플로잇킷은 보안이 취약한 웹사이트를 통해 악성코드를 유포하는데 주로 사용되며, 다수의 인터넷 관련 프로그램의 취약점을 패키지로 구성한 것이라 할 수 있다. 웹사이트 방문 시 악성코드가 다운로드되고 실행되기 때문에 사용자로서는 악성코드 감염 및 실행을 인지하기 어렵다. 웹사이트 취약점을 이용한다는 점에서 불특정 다수의 감염을 이끌어 낼 수 있으며, 이전에도 온라인게임핵이나 파밍 악성코드 유포에 악용되었다.

불특정 다수를 대상으로 최대 다수의 감염을 성공시키기 위한 필수 조건으로는 크게 ▲사용자의 이용이 많으면서 보안이 취약한 웹사이트 ▲대부분의 사용자들이 이용하는 소프트웨어의 취약점 ▲대부분의 안티바이러스에서 아직 진단하지 않는 악성코드 등이 있다. 따라서 공격자들의 주요 타깃은 인터넷 기반의 프로그램이면서 구조적으로 취약한 프로그램이거나 많은 웹사이트에서 범용적으로 사용하고 해당 프로그램을 설치한 사용자 수가 많은 프로그램이다. 대표적으로 인터넷 익스플로러, 플래시 플레이어, 자바, 실버라이트(Silverlight) 등이다.

다양한 종류의 익스플로잇킷이 존재하는데 현재는 RIG, RIG-E, 뉴트리노(Neutrino), 매그니튜드(Magnitude) 등이 활발하게 활동 중이다. 뉴클리어(Nuclear EK)나 앵글러(Angler EK)는 지난 2016년 상반기에 활동을 종료했고, 이후 뉴트리노 와 RIG EK로 무게 중심이 이동했다. 익스플로잇킷을 이용해 유포된 랜섬웨어는 대표적으로 록키, 케르베르, 크립트XXX, 테슬라크립트 등이다.

3. 광고 모듈과 서버로 확대되는 멀버타이징(Malvertising) 공격

앞서 언급한 것처럼 드라이브 바이 다운로드(Drive-by-download) 기법을 이용해 불특정 다수의 최대 감염을 달성하기 위한 조건은 사용자의 이용이 많으면서 보안이 취약한 웹사이트다. 그러나 이들 두 가지 조건을 모두 만족하는 웹사이트는 그리 많지 않다.

이러한 한계를 극복하기 위해 공격자들은 보안이 취약한 웹사이트 대신 온라인 광고 모듈 또는 광고 서버로 공격 대상을 바꾼다. 일반적으로 유명 사이트에 나타나는 광고는 대부분 광고 업체의 자체 서버를 통해 제공되는 경우가 많다. 문제는 이러한 광고 업체들이 영세하거나 광고 서버의 보안이 취약한 경우가 많다는 점이다.

공격자는 바로 이 취약한 광고 서버를 통해 악성코드가 삽입된 광고를 배포하는 것으로, 해당 광고를 제공받는 다수의 웹사이트들은 보안이 취약하지 않음에도 불구하고 이들 웹사이트를 방문한 사용자들이 악성코드에 감염되는 것이다. 이러한 기법을 멀버타이징(Malvertising)이라 하는데, '악의적인'이라는 뜻의 영어 Malicious와 광고를 의미하는 Advertising의 합성어이다.

이처럼 정상 사이트를 이용했음에도 불구하고 멀버타이징 기법에 의해 악성코드에 감염된 경우, 악성코드 감염 경로를 추적하기가 매우 어렵다. 한편, 웹 광고에는 주로 플래시 플레이어 프로그램이 사용되는데, 이러한 점을 악용한 악성코드 유포 사례가 빈번하다. 멀버타이징 기법을 이용해 유포된 대표적인 랜섬웨어는 케르베르, 록키, 크립트XXX 등이다.

4. 원격 데스크톱 프로토콜을 이용한 랜섬웨어 유포

원격 데스크톱 프로토콜(Remote Desktop Protocol, RDP)은 마이크로소프트(Microsoft)사에서 개발한 것으로, 다른 컴퓨터에 원격으로 연결하여 GUI(Graphic User Interface)를 제공하는 것이다. 주로 서버 관리나 원격 접속을 위해 사용하며, 서버의 관리자나 사용자 계정 정보를 필요로 한다. 문제는 사용자나 관리자들이 암호를 제대로 설정하지 않는다는 것이다. 귀찮거나 다른 사람과 공유하기 편하도록 '1', '1234', 'abcd', 'password'와 같은 단순한 암호로 설정하는 경우가 많다.

최근 원격 데스크톱 프로토콜을 이용한 랜섬웨어 감염 사례가 다수 발견되고 있다. 주로 무작위 암호 대입 공격을 통해 로그인을 시도하는데, 원격 데스크톱 프로토콜을 이용하는 관리자나 사용자가 복잡한 암호를 사용하지 않는다는 점을 노린 것이다. 무작위 암호 대입공격을 통해 접속에 성공하면 랜섬웨어 실행 파일을 시스템에 복사해서 직접 실행한다. 이러한 방식을 통해 랜섬웨어에 감염된 사례가 늘고 있는 만큼, 비밀번호 관리에 주의를 더욱 기울일 필요가 있다. 원격 데스크톱 프로토콜을 이용한 대표적인 랜섬웨어는 UmbreCrypt, Bucbi, Xpan, DXXD, Kangaroo 등이 있다.

[그림 38] 원격 데스크톱 프로토콜을 이용한 접속 화면

랜섬웨어 피해 양상

현재 랜섬웨어는 국가와 지역을 가리지 않고 전세계에서 동시다발적으로 발견되는 것이 특징이다. 지역별 감염 빈도를 살펴보면, 북미 지역과 러시아를 포함한 유럽 전역이 압도적이지만 한국, 일본, 인도, 대만 등 아시아권으로 피해가 확산되는 추세다.

특히 테슬라크립트, 록키, 케르베르, 크립트XXX의 감염 빈도가 높은 것으로 나타났다. 이들 랜섬웨어의 경우 스팸 메일이나 익스플로잇킷에 의한 유포 빈도와 PC 사용자 수 등에 따른 약간의 지역적 차이는 있지만, 주로 북미 지역을 중심으로 유럽과 아시아 지역에서 고른 분포를 보였다.

산업군별 피해 양상을 살펴보면, 지난 2016년에는 개인은 물론 의료기관과 공공기관 등을 중심으로 랜섬웨어 피해 사례가 보고 되었다. 그러나 앞으로는 이들뿐만 아니라 금융, 제조업을 비롯해 다양한 서비스 산업까지 피해가 확산될 가능성을 배제할 수 없다. 특히 기존 랜섬웨어의 활동이 점차 확대됨에 따라 피해 범위 또한 확대될 가능성이 높다.

결론(Conclusion)

2015년 본격화되기 시작한 랜섬웨어의 위협은 2016년에 변화를 거듭하며 급속도로 진화하였다. 2016년 상반기에는 PC 내 파일을 암호화하는 기본적인 형태가 주를 이뤘으나, 하반기부터는 파일 암호화는 물론 MBR을 암호화하는 랜섬웨어가 등장하고 RaaS가 활성화되는 양상을 보였다.

향후 더욱 다양한 형태의 랜섬웨어가 나타날 것은 명약관화한 일이다. 더 많은 새로운 변종이 출현하고, MBR 뿐만 아니라 시스템의 다른 영역으로 암호화 대상을 확대하거나 감염 기법을 고도화하고 안티바이러스 무력화를 비롯해 보안 솔루션의 탐지를 우회하기 위한 적극적인 시도가 예상된다. 이와 함께 RaaS는 더욱 활성화될 전망이다.

특히 랜섬웨어 시장의 경쟁 심화로 인한 부익부빈익빈 현상이 가속화되면서 결국 더 강력한 랜섬웨어들

이 살아남아 활개를 칠 것으로 보인다. 앞서 살펴본 것처럼, 지난 2016년 한해 동안 록키와 케르베르 랜섬웨어가 지속적으로 변종을 쏟아낸 반면, 초반에 맹위를 떨치던 테슬라크립트와 크립트XXX는 소멸하는 모습을 보였다. 이는 랜섬웨어를 유포하는 익스플로잇킷(EK)의 주도권 싸움과도 밀접한 관계가 있다. 앵글러 EK의 활동 중단과 뉴트리노 EK의 성장세가 대표적인 예다.

EK를 이용한 랜섬웨어 유포 외에도 최근 제로데이 취약점을 이용한 멀버타이징 기법을 통한 랜섬웨어 유포가 크게 증가하고 있다. 스팸 메일을 이용한 랜섬웨어 유포 방식의 경우, 지금까지 확인된 JS, DOCX, DOCM, WSF, HTA 외의 다른 포맷의 첨부 파일을 이용할 가능성이 높다. 이와 함께 추적이 어려운 비트코인을 주요 결제 수단으로 사용하는 랜섬웨어 활동이 더욱 활발해질 것으로 예상된다.

그러나 랜섬웨어 유포 방식은 사실 전혀 새로운 형태는 아니다. 스팸 메일과 익스플로잇킷을 이용한 드라이브 바이 다운로드 공격은 이미 수년 전부터 존재해온 방식으로, 단지 유포 대상이 랜섬웨어로 바뀌었을 뿐이다. 이는 결국 전통적인 보안 수칙을 준수하고 기존의 보안 솔루션을 효율적으로 운용하면 상당한 랜섬웨어 예방 효과를 볼 수 있다는 의미이기도 하다.

익스플로잇킷을 이용한 드라이브 바이 다운로드 공격이나 멀버타이징에 의한 랜섬웨어 감염을 예방하는데 효과적인 것은 운영체제(OS) 및 주요 프로그램의 최신 보안 업데이트를 적용하는 것이다. 2016년 한국인터넷진흥원(KISA)의 통계 자료에 따르면, 국내 컴퓨터 사용자 중에서 적극적인 윈도우 업데이트 설치 비율은 단 11%에 불과하다. 자동 업데이트를 설정한 72%의 사용자들도 최초 설정 이후에는 무관심한 경우가 대부분이며, 의도적으로 업데이트를 하지 않는 비율도 17%에 달한다. 공격자들은 새로운 취약점을 발견하기 위해 끊임없는 노력을 기울이고 있다. 언제든 새로운 취약점이 발견될 수 있는 만큼 사용자들의 꾸준한 관심과 보안 업데이트 적용이 매우 중요하다. 또 평소 데이터를 백업하는 습관도 랜섬웨어 피해 최소화에 상당한 도움이 된다.

특히 기업의 경우 기업 내 사용자들의 보안 수칙 준수 노력과 더불어 각 업무용 시스템의 보안 상태를 중앙에서 관리하고 강제할 수 있는 방안을 마련해야 한다. 또 네트워크단과 엔드포인트단에서 각각 악성코드 유입을 탐지하고 차단하는 입체적이며 다계층화된 대응이 필요하다. 특히 엔드포인트단에서의 악성코드 확산을 방지하는 한편, 최초 감염 시스템의 랜섬웨어 피해도 방지할 수 있는 방안을 마련해야 한다.

참고자료

1. 랜섬웨어 관련

1) 랜섬웨어도 "$how me the MONEY!"

http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=25198

2) 2016년 상반기 키워드는 랜섬웨어·표적 공격! 하반기는?

http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=25300

3) 2016년 보안 위협, 적자생존 속 진화 중!

http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=25780

4) 랜섬웨어, '이것'이 궁금하다!

http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=25176

2. Locky

1) Locky ransomware, disguised in Word docs, latest from Dridex creators
http://www.scmagazine.com/dridex-actors-likely-behind-vicious-locky-ransomware-strain/article/475420/

2)New Locky version adds the .Zepto Extension to Encrypted Files

https://www.bleepingcomputer.com/news/security/new-locky-version-adds-the-zepto-extension-to-encrypted-files/

3) Locky / Zepto Ransomware now being installed from a DLL

https://www.bleepingcomputer.com/news/security/locky-zepto-ransomware-now-being-installed-from-a-dll/

4) Locky Ransomware now uses the .ODIN extension for Encrypted Files

https://www.bleepingcomputer.com/news/security/locky-ransomware-now-uses-the-odin-extension-for-encrypted-files/

5) Locky Ransomware's new .SHIT Extension shows that you can't Polish a Turd

https://www.bleepingcomputer.com/news/security/locky-ransomwares-new-shit-extension-shows-that-you-cant-polish-a-turd/

6) Locky Ransomware switches to THOR Extension after being a Bad Malware

https://www.bleepingcomputer.com/news/security/locky-ransomware-switches-to-thor-extension-after-being-a-bad-malware/

7) Locky Ransomware now using the Aesir Extension for Encrypted Files

https://www.bleepingcomputer.com/news/security/locky-ransomware-now-using-the-aesir-extension-for-encrypted-files/

8) Locky Ransomware putting us to sleep with the ZZZZZ Extension

https://www.bleepingcomputer.com/news/security/locky-ransomware-putting-us-to-sleep-with-the-zzzzz-extension/

9) Facebook Spam Campaign Spreading Nemucod Downloader and Locky Ransomware

https://www.bleepingcomputer.com/news/security/facebook-spam-campaign-spreading-nemucod-downloader-and-locky-ransomware/

10) Locky Ransomware switches to Egyptian Mythology with the Osiris Extension

https://www.bleepingcomputer.com/news/security/locky-ransomware-switches-to-egyptian-mythology-with-the-osiris-extension/

3. CERBER

1) The three heads of the Cerberus-like Cerber ransomware

https://blogs.technet.microsoft.com/mmpc/2016/03/09/the-three-heads-of-the-cerberus-like-cerber-ransomware/

2) Cerber Ransomware – New, But Mature

https://blog.malwarebytes.com/threat-analysis/2016/03/cerber-ransomware-new-but-mature/

3) Cerber Ransomware version 2 Released, Uses .Cerber2 Extension

https://www.bleepingcomputer.com/news/security/cerber-ransomware-version-2-released-uses-cerber2-extension/

4) Cerber Ransomware switches to .CERBER3 Extension for Encrypted Files

https://www.bleepingcomputer.com/news/security/cerber-ransomware-switches-to-cerber3-extension-for-encrypted-files/

5) Cerber Ransomware switches to a Random Extension and Ends Database Processes

https://www.bleepingcomputer.com/news/security/cerber-ransomware-switches-to-a-random-extension-and-ends-database-processes/

6) Cerber Ransomware 4.10 now shows the Version Number in Ransom Notes

https://www.bleepingcomputer.com/news/security/cerber-ransomware-4-10-now-shows-the-version-number-in-ransom-notes/

7) Cerber Ransomware 5.0 Released with a Few Changes

https://www.bleepingcomputer.com/news/security/cerber-ransomware-5-0-released-with-a-few-changes/

8) Cerber Ransomware Spreads via Fake Credit Card Email Reports

https://www.bleepingcomputer.com/news/security/cerber-ransomware-spreads-via-fake-credit-card-email-reports/

4. TeslaCrypt / CryptXXX

1) TeslaCrypt shuts down and Releases Master Decryption Key

https://www.bleepingcomputer.com/news/security/teslacrypt-shuts-down-and-releases-master-decryption-key/

2) TeslaCrypt Developers recommend TeslaDecoder to Decrypt Files

https://www.bleepingcomputer.com/news/security/teslacrypt-developers-recommend-tesladecoder-to-decrypt-files/

3) CryptXXX: New Ransomware From the Actors Behind Reveton, Dropping Via Angler

https://www.proofpoint.com/us/threat-insight/post/cryptxxx-new-ransomware-actors-behind-reveton-dropping-angler

4) Decrypted: Kaspersky releases free decryptor for CryptXXX Ransomware

https://www.bleepingcomputer.com/news/security/decrypted-kaspersky-releases-free-decryptor-for-cryptxxx-ransomware/

5) Kaspersky releases updated Decryptor for CryptXXX 2.0

https://www.bleepingcomputer.com/news/security/kaspersky-releases-updated-decryptor-for-cryptxxx-2-0/

6) CryptXXX updated to version 3.0, Decryptors no longer Work

https://www.bleepingcomputer.com/news/security/cryptxxx-updated-to-version-3-0-decryptors-no-longer-work/

7) CryptXXX ransomware again updated, can now encrypt network shared files

https://www.scmagazine.com/cryptxxx-ransomware-again-updated-can-now-encrypt-network-shared-files/article/528252/

8) CryptXXX Ransomware moves from the Crypz extension to a Random One

https://www.bleepingcomputer.com/news/security/cryptxxx-ransomware-moves-from-the-crypz-extension-to-a-random-one/

9) CryptXXX providing free keys for .Crypz and .Cryp1 Versions

https://www.bleepingcomputer.com/news/security/cryptxxx-providing-free-keys-for-crypz-and-cryp1-versions/

10) New CryptXXX changes name to Microsoft Decryptor

https://www.bleepingcomputer.com/news/security/new-cryptxxx-changes-name-to-microsoft-decryptor/

11) CryptXXX Ransomware is now scrambling the filenames of Encrypted Files

https://www.bleepingcomputer.com/news/security/cryptxxx-ransomware-is-now-scrambling-the-filenames-of-encrypted-files/

5. PETYA / Mischa / GoldenEye

1) Petya Ransomware skips the Files and Encrypts your Hard Drive Instead

https://www.bleepingcomputer.com/news/security/petya-ransomware-skips-the-files-and-encrypts-your-hard-drive-instead/

2) Petya Ransomware's Encryption Defeated and Password Generator Released

https://www.bleepingcomputer.com/news/security/petya-ransomwares-encryption-defeated-and-password-generator-released/

3) Petya is back and with a friend named Mischa Ransomware

https://www.bleepingcomputer.com/news/security/petya-is-back-and-with-a-friend-named-mischa-ransomware/

4) The Petya and Mischa Ransomware are part of a new Affiliate Service

https://www.bleepingcomputer.com/news/security/the-petya-and-mischa-ransomwares-part-of-a-new-affiliate-service/

5) Petya Ransomware Returns with GoldenEye Version, Continuing James Bond Theme

https://www.bleepingcomputer.com/news/security/petya-ransomware-returns-with-goldeneye-version-continuing-james-bond-theme/

6. HDDCryptor (Mamba)

1) HDDCryptor Ransomware Overwrites Your MBR Using Open Source Tools

https://www.bleepingcomputer.com/news/security/hddcryptor-ransomware-overwrites-your-mbr-using-open-source-tools/

2) Ransomware Hits San Francisco Public Transit System, Asks for $73,000

https://www.bleepingcomputer.com/news/security/ransomware-hits-san-francisco-public-transit-system-asks-for-73-000/

3) San Francisco SFMTA Denies That Hacker Stole 30GB of Data from Its Servers

https://www.bleepingcomputer.com/news/security/san-francisco-sfmta-denies-that-hacker-stole-30gb-of-data-from-

its-servers/

7. RaaS로 제공되는 랜섬웨어

1) Stampado Ransomware campaign decrypted before it Started

https://www.bleepingcomputer.com/news/security/stampado-ransomware-campaign-decrypted-before-it-started/

2) Stampado: Taking Ransomware Scumbaggery to the Next Level

https://www.bleepingcomputer.com/news/security/stampado-taking-ransomware-scumbaggery-to-the-next-level/

3) The Philadelphia Ransomware offers a Mercy Button for Compassionate Criminals

https://www.bleepingcomputer.com/news/security/the-philadelphia-ransomware-offers-a-mercy-button-for-compassionate-criminals/

4) The Shark Ransomware Project allows you to create your own Customized Ransomware

https://www.bleepingcomputer.com/news/security/the-shark-ransomware-project-allows-to-create-your-own-customized-ransomware/

5) Shark Ransomware Rebrands as Atom for a Fresh Start

https://www.bleepingcomputer.com/news/security/shark-ransomware-rebrands-as-atom-for-a-fresh-start/

8. 사회공학기법을 이용한 랜섬웨어

1) VindowsLocker Ransomware Mimics Tech Support Scam, Not the Other Way Around

https://www.bleepingcomputer.com/news/security/vindowslocker-ransomware-mimics-tech-support-scam-not-the-other-way-around/

2) PokemonGo Ransomware installs Backdoor Account and Spreads to other Drives

https://www.bleepingcomputer.com/news/security/pokemongo-ransomware-installs-backdoor-accounts-and-spreads-to-other-drives/

3) New Open Source Ransomware Based on Hidden Tear and EDA2 May Target Businesses

http://blog.trendmicro.com/trendlabs-security-intelligence/new-open-source-ransomwar-based-on-hidden-tear-and-eda2-may-target-businesses/

4) The Donald Trump Ransomware tries to Build Walls around your Files

https://www.bleepingcomputer.com/news/security/the-donald-trump-ransomware-tries-to-build-walls-around-your-files/

9. 기존 랜섬웨어를 모방한 랜섬웨어

1) Bart Ransomware being Spammed by the same devs behind Locky

https://www.bleepingcomputer.com/news/security/bart-ransomware-being-spammed-by-the-same-devs-behind-locky/

2) Side-by-side comparisons of the CrypMIC and CryptXXX Ransomware Infections

https://www.bleepingcomputer.com/news/security/side-by-side-comparisons-of-the-crypmic-and-cryptxxx-ransomware-infections/

3) MarsJoke Ransomware Mimics CTB-Locker

https://www.proofpoint.com/us/threat-insight/post/MarsJoke-Ransomware-Mimics-CTB-Locker

4) Polyglot – the fake CTB-locker

https://securelist.com/blog/research/76182/polyglot-the-fake-ctb-locker/

5) Hucky Ransomware: A Hungarian Locky Wannabe

https://blog.avast.com/hucky-ransomware-a-hungarian-locky-wannabe

10. 교육과 학습을 위한 랜섬웨어

1) The EduCrypt Ransomware tries to teach you a Lesson

https://www.bleepingcomputer.com/news/security/the-educrypt-ransomware-tries-to-teach-you-a-lesson/

2) New educational ShinoLocker Ransomware Project Released

https://www.bleepingcomputer.com/news/security/new-educational-shinolocker-ransomware-project-released/

3) Heimdall Open-Source PHP Ransomware Targets Web Servers

https://www.bleepingcomputer.com/news/security/heimdall-open-source-php-ransomware-targets-web-servers/

11. 주목할 만한 랜섬웨어

1) Telecrypt Ransomware Uses Telegram as C&C Server

https://www.bleepingcomputer.com/news/security/telecrypt-ransomware-uses-telegram-as-candc-server/

2) Telecrypt Ransomware Cracked, Free Decryptor Released by Malwarebytes

https://www.bleepingcomputer.com/news/security/telecrypt-ransomware-cracked-free-decryptor-released-by-

malwarebytes/

3) New Scheme: Spread Popcorn Time Ransomware, get chance of free Decryption Key

https://www.bleepingcomputer.com/news/security/new-scheme-spread-popcorn-time-ransomware-get-chance-of-free-decryption-key/

4) This Ransomware Unlocks Your Files For Free If You Infect Others

http://thehackernews.com/2016/12/ransomware-malware.html

5) Popcorn Time ransomware, pay up the ransom or spread it to decrypt the files

http://securityaffairs.co/wordpress/54237/malware/popcorn-time-ransomware.html