2020년 1분기

랜섬웨어 동향분석

RANSOMWARE TRENDS & STATISTICS
FIRST QUARTER FOR 2020

KISA 한국인터넷진흥원

KISA 한국인터넷진흥원

CONTENTS

01 개요

주요 랜섬웨어

1분기에 발견된 신규 랜섬웨어는 Snake, Ako 등 20여 종에 대한 피해사례가 주류를 이루었다. 또한, COVID-19 정보관련 문서로 위장한 랜섬웨어 실행파일 유포 사례가 다수 등장하였으며, 랜섬웨어 스스로 Coronavirus등의 명칭으로 변경하는 사례도 발견 되었다.

국내 보안업체인 이스트시큐리티는 1분기 랜섬웨어 주요 동향으로 랜섬웨어 공격자들의 '코로나 키워드 활용' 및 기존 'Sodinokibi & Nemty 랜섬웨어에 의한 피해지속'를 꼽았다.

사건사고 타임라인

2020년 1분기는 Sodinokibi와 Nemty 등 기존 랜섬웨어의 변종이 다수 출현 하였으며, 외국 정부와 민간 기업 등 대상을 가리지 않는 공격이 주를 이루었다. 더불어 환전송금 기업과 은행전산업무 지원 기업 등 다양한 기업의 랜섬웨어 감염 사례가 발견되었다.

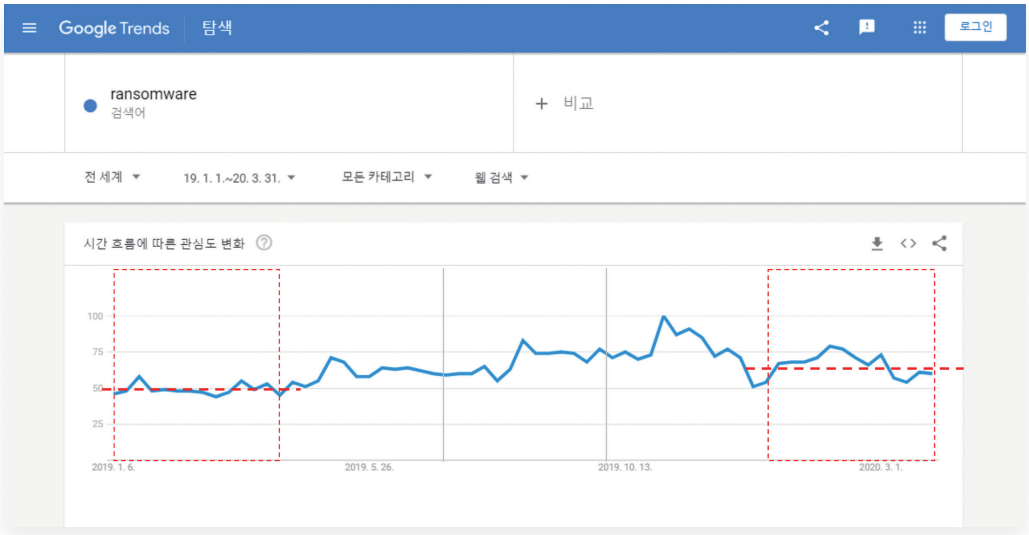
또한, COVID-19의 사태에 따라 다수의 랜섬웨어가 코로나바이러스 키워드로 전파를 시도 하여 사용자 주의를 요한다.

국내 랜섬웨어 통계

[그림 1] 1분기 국내외 랜섬웨어 동향 요약

국외 검색 통계로 본 랜섬웨어

2019. 1 ~ 2020. 3월 까지 구글트렌드 검색어 조사결과 작년 1분기 대비 2020년 1분기 Ransomware 검색량이 증가 한 것을 알 수 있다.



[그림 2] 구글 검색어 트렌드 - Ransomware 키워드

구글트렌드를 통하여 1분기 Ransomware를 검색한 사람들이 함께 검색한 관련검색어를 조사하였다.(2020.4.15. 검색기준) 랜섬웨어 정의와 공격 등에 대한 궁금증을 나타내는 검색키워드가 대부분을 이루었으며, 7위와 9위에서 Ryuk 랜섬웨어를 검색하는 키워드가 등장하였다.

[표 1] 랜섬웨어 관련 검색어

검색어	비율 (%)	비 고
ransomware attack	100	랜섬웨어 공격
virus ransomware	74	바이러스 랜섬웨어
malware	67	악성코드
what is ransomware	58	랜섬웨어란 무엇인가
ransomware attacks	43	랜섬웨어 공격
ransomware protection	42	랜섬웨어 방어
ryuk ransomware	38	[기존] Ryuk 랜섬웨어
ransomware decryptor	35	랜섬웨어 복호화도구
ryuk	33	[기존] Ryuk 랜섬웨어
ransomware meaning	30	랜섬웨어 의미

1분기 Ransomware를 검색한 사람들이 함께 검색한 검색어 중 검색량이 급증한 검색어는 다음과 같다. 증가율이 5000%가 넘거나 계산이 불가능한 경우는, 순위만 표시하고 증가율을 breakout으로 표기하였다. 순위별로 1~3위에서 Toll社와 Travelex社 등 랜섬웨어 피해사례를 확인 할 수 있었다. 4위에 신규 Mailto 랜섬웨어와 5위 Ako 랜섬웨어가 등장하였다. 6위에 Finastra社의 랜섬웨어 피해사례를 키워드로 검색한 것을 확인 할 수 있었다. 7위는 신규 Snake랜섬웨어가 등장하였다. 13위에 기존에 피해사례가 보고된바 있는 Sodinokibi 랜섬웨어가 등장하고 있는 것도 확인 할 수 있다.

[표 2] 랜섬웨어 관련 급증한 검색어

검색어	증가율 (%)	비 고
toll ransomware	breakout	[사고] Toll社 랜섬웨어 감염사고
travelex ransomware	breakout	[사고] Travelex社 랜섬웨어 감염사고
epiq ransomware	breakout	[사고] Epiq社 랜섬웨어 감염사고
mailto ransomware	breakout	[신규] Mailto 랜섬웨어
ako ransomware	breakout	[신규] Ako 랜섬웨어
finastra ransomware	breakout	[사고] Finastra社
snake ransomware	550	[신규] Snake 랜섬웨어
recent ransomware attacks	400	최근사고사례
ransomware detection	200	랜섬웨어 탐지
universiteit maastricht ransomware	110	[사고] 네덜란드 대학교 감염사고
ransomware statistics 2019	100	2019년 랜섬웨어 통계
ransomware o que é	70	랜섬웨어란 무엇인가
sodinokibi ransomware	70	[기존] Sodinokibi 랜섬웨어
ransomware prevention	60	랜섬웨어 예방
how does ransomware work	50	랜섬웨어 동작방법

검색어를 통하여 1분기 전세계적으로 Ransomware 관련 관심사에 대하여 확인해 보았으며, 이를 통하여 Mailto 랜섬웨어 및 Ako 랜섬웨어, Snake 랜섬웨어가 사람들의 관심이 높아지고 있다는 사실을 확인 할 수 있다. Ryuk 랜섬웨어와 Sodinokibi 랜섬웨어의 경우 기존에 발견된 랜섬웨어지만 지속적으로 검색어에 등장하고 있어 주의를 요한다. 다만, 2019년 보고된 랜섬웨어로 1분기 신규 랜섬웨어 분석에서는 제외하였다.

보고서 목적

본 보고서는 2020년 1분기에 등장한 신규 랜섬웨어 5종의 악성행위를 분석한다. 또한, 언론보도 자료를 기준으로 1분기에 발생한 해외 랜섬웨어 공격현황과 해외 사건사고를 소개한다.

기관, 기업의 보안담당자가 랜섬웨어 동향을 파악하기 위한 참고자료로 활용 할 수 있다. 추가로 랜섬웨어의 공격을 예방할 수 있는 조치사항을 파악하기 위한 참고자료로 활용할 수 있다.

기타 분기 특이사항

2020년 1월 14일 MS社는 자사 운영체제 Windows 7에 대한 기술지원을 종료 하였다. 기술지원이 종료되면 신규로 발견된 보안취약점에 대해서 보안조치가 불가능하여 이를 악용한 개인정보 유출, 랜섬웨어 감염 등 보안위협이 발생할 수 있다. 이는 취약점을 악용하는 랜섬웨어 등 악성코드가 확산 될 경우 백신 등 보안 프로그램이 설치되어 있어도 잠재적 위험에 노출 될 수 있음을 뜻한다. 따라서 Windows 7 사용자는 최신 OS로 업그레이드를 권고한다.

MS社 공지 https://support.microsoft.com/ko-kr/help/4057281/windows-7-support-ended-on-january-14-2020

2020년 3월 MS社 Windows 운영체제 네트워크 프로토콜(SMB)에서 심각한 취약점(CVE-2020-0796)이 공개되었다. 2017년 많은 피해사례가 보고된 워너크라이(WannaCry) 랜섬웨어 발견당시 네트워크 프로토콜(SMB) 취약점을 악용하여 급속히 전파된 사례가 존재한다. 따라서 본 취약점이 랜섬웨어에 의해 악용될 경우 급속한 전파가 예상되므로 MS Windows 시스템을 사용하는 기관 및 개인은 최신 보안조치 적용을 권고한다. 본 취약점은 3월 13일 MS 社에 의해 패치가 공개 된 상황이다.

보호나라 권고 https://www.boho.or.kr/data/secNoticeView.do?bulletin_writing_sequence=35295

02 해외 랜섬웨어 사고사례

2.1. 여행 환전업체 Travelex 서비스 중단과 복구 (1월)

- Revil (Sodinokibi 랜섬웨어 변종) 감염

영국 여행 환전업체 Travelex社는 지난해 12월 30일경 Revil (Sodinokibi 랜섬웨어 변종)에 감염되어 서비스를 전면 중단한바 있다.

Travelex 랜섬웨어 감염사고는 VPN(가상사설망 네트워크 보안장비)의 취약점을 악용하여 랜섬웨어를 유포한 것으로 알려졌다.

VPN제공 업체인 펄스 시큐어(Pulse Secure)는 2020년 1월 6일 보안패치를 수행 할 것을 고객들에게 권고 하였다. 해당 패치는 지난 4월에 배포한 것으로 일부 제품에서 발견된 치명적 위험도의 원격 코드 실행 오류 때문에 개발된 것이나, 일부 고객사의 경우 패치가 진행되지 않았고 이번 사고와 같은 기업의 치명적 피해로 연결되었다.

출처 보안뉴스(2020.01.07.) - "VPN제품에서 발견된 오류 통해 퍼지고 있는 레빌 랜섬웨어"

2.2. 英 핀테크기업 Finastra, 랜섬웨어 감염 및 복구 (3월)

3월 중순 영국 핀테크 기업 Finastra가 랜섬웨어에 감염사고가 발생하였다. Finastra는 8500개의 고객사를 보유하고 있으며, 세계 100대 은행 중 90%와 협업하고 있는 백오피스 및 금융서비스 기업이다.

기사에 따르면, 3월 중순 Finastra는 COVID-19 사태로 인한 재택근무를 위하여 시스템을 구성하던 중 이를 틈타 침입한 해커들에 의해 일부 시스템의 패스워드가 탈취되었다. 이로 인하여 빠르게 시스템에 백도어가 설치되었고 이를 보안팀에서 발견하여 대응하였다. 해커는 보안팀에 발각된 사실을 알고 Ryuk 랜섬웨어로 알려진 악성코드를 통하여 서버를 랜섬웨어에 감염 시켰다.

Finastra는 랜섬웨어 피해복구를 위하여 범죄자에게 비용을 지불하지 않았으며, 기업의 시스템을 복구하였다. 네트워크 전파를 막고 시스템을 복구할 수 있었던 이유는 감염 발견 시 클라우드 서비스에서 운영 중이던 자사의 가상서버를 빠르게 네트워크에서 격리시켜서 가능했다고 블룸버그는 밝히고 있다. 하지만, 블룸버그는 본 사건은 아직 조사가 진행 중에 있으며, 랜섬웨어로 부터 서비스를 완벽하게 보호하지는 못했다고 밝혔다. 실제 Finastra와 거래하는 여러 은행에서 3월 중순 금융거래 중 일부가 중단되는 사태를 겪었다.

출처 블룸버그(2020.04.07.) - Fintech Company Survived Ransomware Attack Without Paying Ransom

03 해외 랜섬웨어 관련 정책 동향

3.1. 美 FBI, 2019년 인터넷범죄 분석 보고서 발간

지난 2월 12일, 미국 FBI는 2019년 인터넷범죄 분석 보고서를 발간하였다. 보고서에 따르면, 지난 5년간 FBI에 접수된 사이버범죄 건수는 170만여 건에 달하며, 피해금액만 102억 달러로 추산하고 있으며, 인터넷범죄는 매년 지속적으로 증가하고 있다.

[그림 3] 최근 5년간 사이버 범죄 통계자료

2019년 미국 FBI에 접수된 주요 인터넷범죄 유형으로는 전자메일 범죄, 노인대상 금융사기, 전자금융 사기 등과 함께 랜섬웨어를 손꼽았다. 또한, 랜섬웨어 피해접수는 2047건으로 피해규모는 890만 달러로 추산된다. 이 보고서는 사이버범죄의 주요 피해국가 및 피해 지역에 대한 통계 등으로 구성되어 있으며, 랜섬웨어의 피해사례가 인터넷범죄의 큰 부분을 차지하는 것을 알 수 있다.

보고서에 따르면, 랜섬웨어의 가장 큰 예방법은 조직에 대한 인식제고와 교육이 중요하다고 언급하고 있다. 그리고 만약 랜섬웨어에 감염되더라도 범죄자에게 비용을 지불하지 말고 즉시 당국에 신고할 것을 권고하고 있다.

출처 미국 FBI(2020.02.12) - “2019 Internet Crime Report”

04 | 1분기 신규 랜섬웨어 동향

1분기 피해사례가 확인된 랜섬웨어는 약 50종이 발견되었으며, 이중 21종이 기존 랜섬웨어의 변종으로 파악된다. 발견된 랜섬웨어 중 Nemty 랜섬웨어를 포함하여 다수의 랜섬웨어가 이력서 및 COVID-19관련 정보로 위장하여 랜섬웨어를 전파하고 있는 것을 확인 할 수 있었다. 그리고 약 30종의 신규 랜섬웨어가 발견되었다.

본 보고서에서는 1분기 신규 랜섬웨어 중 5종을 선정하고 이를 분석하였다. 첫 번째 선정된 랜섬웨어는 Coronavirus 랜섬웨어로 COVID-19이슈로 문제가 되고 있는 코로나바이러스 명칭을 사용하고 있는 랜섬웨어를 선정하여 분석 하였다. 두 번째 랜섬웨어는 Snake 랜섬웨어로 산업제어시스템을 표적으로 공격되는 것으로 유추되는 랜섬웨어를 선정하였다. 세 번째로는 Ravack 랜섬웨어로 유튜브 채널을 통해서 불법소프트웨어에 위장되어 유포되고 있어 사용자 피해가 우려되는 상황이다. 네 번째로는 Mailto 랜섬웨어로 호주의 거대물류회사인 톨 그룹의 IT시스템을 감염시켜 물류 서비스의 차질을 발생시켰다. 마지막으로 선정된 랜섬웨어는 Ako 랜섬웨어로 익명브라우저(Tor브라우저)를 통하여 데이터 복구비용과 방법을 안내하고 있어 주의를 요한다.

앞에서 언급한 Mailto, Ako, Snake 랜섬웨어의 경우 구글 검색엔진의 랜섬웨어 신규 연관검색어로 각각 4위, 5위, 7위에 등장하여 대중적인 관심도가 높은 랜섬웨어로 확인되었다.

4.1. CoronaVirus 랜섬웨어

CoronaVirus 랜섬웨어에 의한 윈도우 복구 무력화 안랩블로그(2020.3.25.)
“게임 앱, 알고 보니 악성코드”…코로나19로 유인하는 ‘앱 주의보’ 동아닷컴(2020.3.30.)

사례 1.

CoronaVirus.txt 이름의 랜섬노트를 생성하는 랜섬웨어가 국내에 유포 중인 것을 확인하였다. 암호화된 사용자의 파일의 복구를 대가로 비트코인 지불(0.008 btc: 50$)을 요구한다. 윈도우 백업을 통한 복구기능을 무력화하여 피해를 심화시켜 주의를 요한다.

사례 2.

신종 코로나바이러스 감염증(코로나19) 이슈를 악용한 온라인상 ‘공격’이 계속 진화하고 있다. 정상 애플리케이션에 악성프로그램을 삽입해 유포하는 사례까지 등장했다. 악성코드 제작자들은 실시간 추적기 앱이나 코로나19의 감염 증상을 확인할 수 있는 내용의 앱을 만든 뒤 내부에 애드웨어, 트로이목마 악성파일 등을 삽입했다. 일부 ‘공격자’들은 앱 스토어의 순위를 높이기 위해 앱 이름과 설명 등에 코로나19와 관련된 키워드를 끼워 넣기도 했다. 게임 앱인 ‘버블 슈터 머지’같은 경우가 대표적이다.

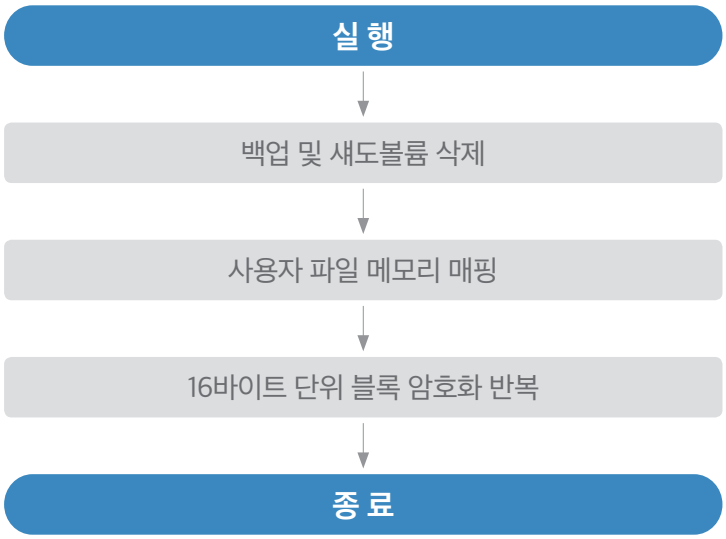
4.1.1. CoronaVirus 랜섬웨어 개요

최근 심각한 사회적 이슈인 COVID-19 사태로 인하여 세계적 관심이 집중되고 있는 가운데 Coronavirus라는 캠페인코드를 사용하는 랜섬웨어가 유포되고 있다. 코로나바이러스(Coronavirus)랜섬웨어는 악성 웹사이트나 전자우편 첨부파일 형태로 유포된다. 공격자는 복구를 위한 비용으로 0.008비트코인을 요구하고 있다.

4.1.2. CoronaVirus 랜섬웨어 특징

o 랜섬웨어 암호화 과정

Coronavirus 랜섬웨어에 적용된 암호화 알고리즘은 공격자에 의해 자체개발 된 암호화 알고리즘을 적용하고 있다. 이 암호화 알고리즘은 128비트 단위의 블록 암호화 알고리즘의 특성을 나타내고 있으며, 현대 암호 알고리즘에서 많이 사용되고 있는 문자변환 과정인 치환과 위치변경 과정인 전치 과정을 반복적으로 수행하는 특징을 보이고 있다. 전치와 치환 과정이 끝나고 암호키와 암호화할 데이터를 논리곱(XOR) 연산을 수행하여 파일을 암호화 하고 있다.

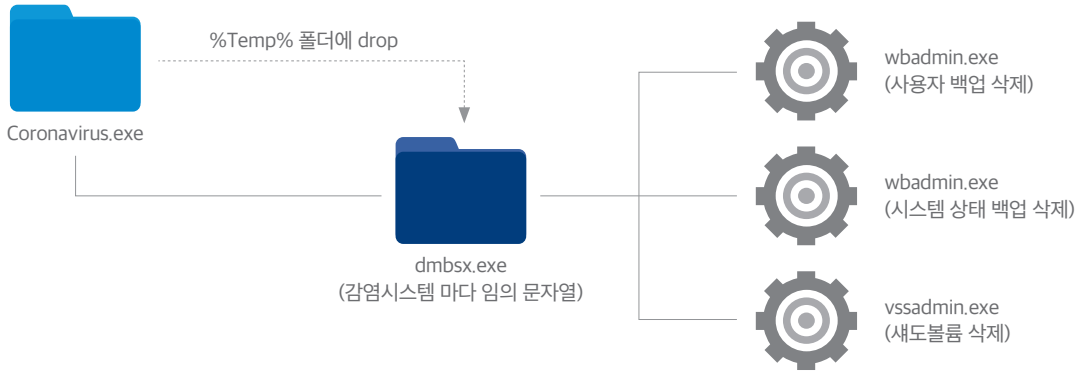


[그림 4] Coronavirus 랜섬웨어 암호화 과정

o 랜섬웨어 기능분석

1. 감염과정

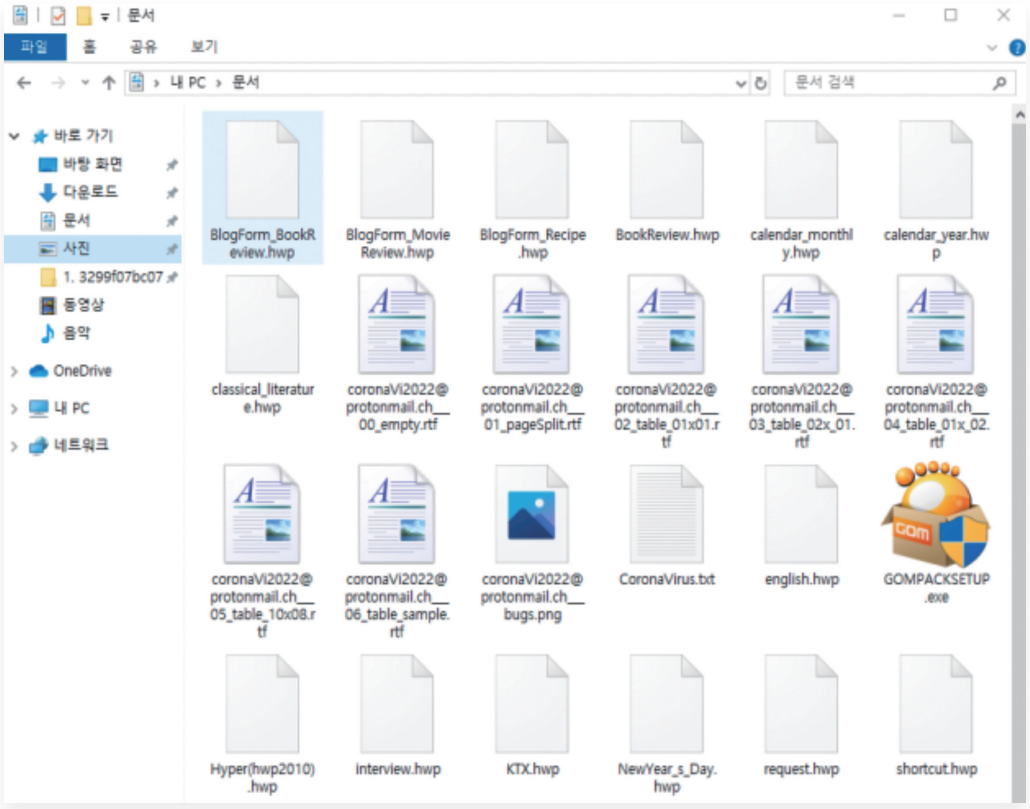
랜섬웨어는 트로이목마나 전자메일 첨부파일 등을 통하여 주로 전파되며, 감염 시 임시폴더(%Temp%)에 악성코드를 생성 후 사용자의 파일을 암호화한다. 이때, 사용자가 백업데이터를 활용한 복구를 하지 못하도록 사용자 및 시스템 백업 데이터와 섀도볼륨을 삭제 한다.



[그림 5] Coronavirus 랜섬웨어 프로세스 실행흐름

2. 랜섬웨어 감염 시 피해범위

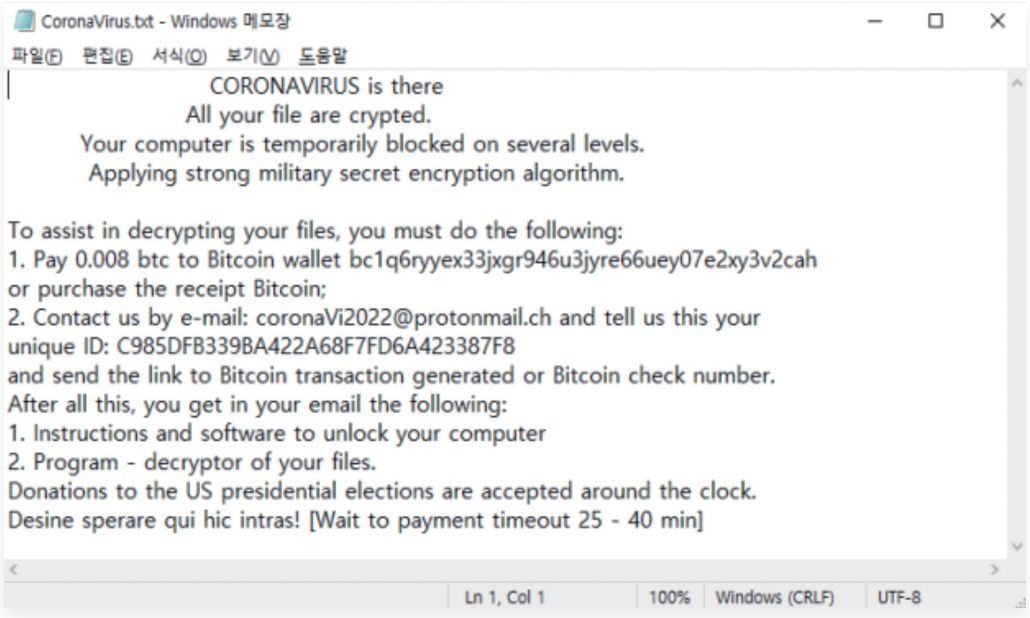
파일 암호화 시 Microsoft office 문서, PDF, 그림파일 뿐만 아니라, 데이터베이스 등을 압축한다. 하지만, 한글워드프로세서 파일 확장자인 hwp와 실행파일 등은 암호화 하지 않는 것을 볼 수 있다.



[그림 6] 랜섬웨어에 암호화 된 파일

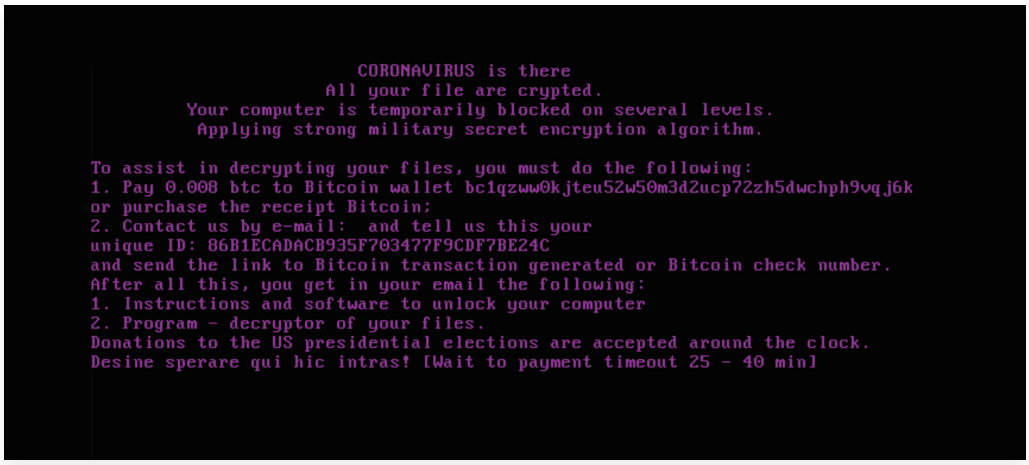
3. 랜섬웨어 감염확인

Coronavirus 랜섬웨어 감염 시 암호화 과정이 완료되면 화면에 노트패드가 실행되고 랜섬노트를 출력하며, 시스템 을 즉시 재부팅 한다.



[그림 7] coronavirus 감염 시 생성되는 랜섬노트

Coronavirus 랜섬웨어는 감염된 PC의 부팅과정을 조작하여 정상적인 부팅을 방해하고 랜섬노트를 출력하여 복구비용 지불을 유도한다.

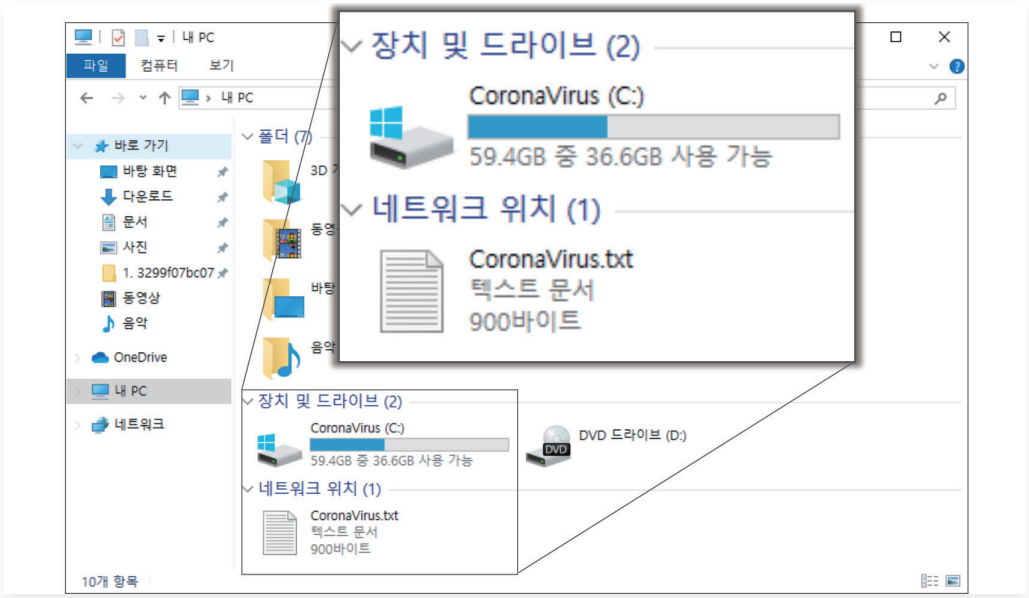


[그림 8] 정상 부팅을 방해하고 랜섬노트를 출력하는 화면

하지만, Windows 10의 경우 구형 시스템과 하드디스크의 부팅영역 구성이 달라 랜섬웨어가 임의로 부팅영역을 조작을 시도한다. 랜섬웨어의 의도와 다르게 조작된 부팅영역이 정상적으로 동작하지 않아 아래와 같이 부팅에 실패하고 에러코드가 출력되는 것을 볼 수 있다.

[그림 9] Windows 10 운영체제 감염 시 부팅실패

Coronavirus 랜섬웨어에 감염되면 아래 그림과 같이 C:볼륨의 이름을 CoronaVirus로 변경되는 것을 볼 수 있다.



[그림 10] 볼륨 명칭을 CoronaVirus로 변경함

4. 암호화 알고리즘

Coronavirus 랜섬웨어가 사용하는 암호화 알고리즘은 128비트 블록암호화 특성을 가지고 있으며, 해당 암호화 알고리즘은 공격자가 자체 제작한 알고리즘으로 추정된다.

외부 라이브러리를 사용하지 않고 랜섬웨어 내부에 암호화 알고리즘을 작성하였다. 아래 그림에 표시된 부분과 같이 불필요한 변수에 무의미한 값을 대입하거나 초기화한 변수를 추가 사용하지 않는 등 데이터 흐름에 대한 분석을 방해하는 코드난독화 기술을 적용하고 있다.

```
v1 = alloca(24656);
ms_exc.old_esp = (DWORD)&v24;
v2 = lpFilename;
if ( lpFilename )
{
  ms_exc.registration.TryLevel = 0;
  _mm_storel_pd((double *)&szFileSize, 0i64);
  GetCurrentThreadId();
  sub_4017E0();
  SetFileAttributesW((LPCWSTR)lpFilename, 0x80u);
  hFileHandle = CreateFileW((LPCWSTR)lpFilename, 0x12019Fu, 7u, 0, 3u, 0x80u, 0);
  hFileHandle__ = hFileHandle;
  hFile = hFileHandle;
  if ( hFileHandle != (HANDLE)-1 )
  {
    if ( GetFileSizeEx(hFileHandle, &szFileSize) )
    {
      dwMaximumSizeLow = szFileSize;
      if ( szFileSize != 0xFFFFFFFFi64 && szFileSize )// file size check
      {
        szBlockExtraSize = szFileSize % 16;
        if ( szBlockExtraSize )
          dwMaximumSizeLow = szFileSize + (unsigned int)(szFileSize % 16) - 1;// 16바이트 단위로 나머지 파일데이터 크기 계산 - 블록암호화 특징인
        hFileMappingHandle = CreateFileMappingA(hFileHandle__, 0, 4u, 0, dwMaximumSizeLow, 0);
        v8 = hFileMappingHandle;
        hcFileMappingHandle = hFileMappingHandle;
        if ( hFileMappingHandle )
        {
          lpBaseAddress = MapViewOfFile(hFileMappingHandle, 0xF001Fu, 0, 0, 0);
          szFileSize__ = szFileSize;
          _mm_storel_pd((double *)&dummy36, 0i64);// nemzero
          dummy9 = dummy36;
          LODWORD(lpBaseAddress__) = dummy39;
          while ( SHIDWORD(szFileSize__) >= 0 && (SHIDWORD(szFileSize__) > 0 || (_DWORD)szFileSize__) )// filesize not null
          {
            HIDWORD(v11) = HIDWORD(dummy36);
            dummy12 = __CFADD__(dummy9, 16) + HIDWORD(dummy36);
            if ( (signed __int64)(__PAIR__(HIDWORD(dummy36), dummy9) + 16) > dwMaximumSizeLow )// 암호화할 용량이 16바이트보다 작은경우 예외처리
            {
              dummy13 = (dwMaximumSizeLow - __PAIR__(HIDWORD(dummy36), dummy9)) >> 32;
              LODWORD(lpBaseAddress___) = dwMaximumSizeLow - dummy9;
              lpBaseAddress__ = (char *)lpBaseAddress + dummy9;//          /
              HIDWORD(lpBaseAddress__) = (lpBaseAddress__ + __PAIR__(dummy13, dummy9)) >> 32;
              dummy9 = dwMaximumSizeLow;
              HIDWORD(dummy36) = HIDWORD(lpBaseAddress__);
              HIDWORD(lpBaseAddress___) = lpBaseAddress__;//              /
            }
            else
            {
              LODWORD(lpBaseAddress___) = 16;
              dummy13 = 0;
              HIDWORD(lpBaseAddress___) = (char *)lpBaseAddress + dummy9;
              lpBaseAddress__ = (char *)lpBaseAddress + dummy9;
              dummy9 += 16;
```

[그림 11] 난독화 되어 있는 암호화 코드

5. 복구도구

현재 복구도구는 공개되어있지 않다.

6. 주의사항

- 의심스러운 메일의 첨부 파일을 내려 받은 경우, 파일확장자를 확인하여 실행파일이면 실행 금지
- 시스템 업데이트를 최신상태로 유지

4.2. Snake 랜섬웨어

"SNAKE Ransomware Is the Next Threat Targeting Business Networks"
BleepingComputer (2020.1.8)

산업 현장 겨냥 랜섬웨어 등장…"감염 시 ICS 프로세스 종료" ZDnetKorea(2020.2.6)

사례 1.

MalwareHunterTeam에서 최초 발견된 것으로 보이는 악성코드이다. 랜섬웨어는 프로그래밍 언어 '고(go)'로 작성되었으며, 산업제어시스템, 가상머신, 원격관리도구, 네트워크관리 소프트웨어 등과 관련된 수많은 프로세스를 종료시킨다.

사례 2.

산업제어시스템(ICS)을 공격하기 위해 개발된 랜섬웨어가 등장함에 따라 보안업계가 잇따라 분석을 내놓고 있다. 이 랜섬웨어는 '에칸스(EKANS)'로 지난해 12월 발견됐다. 거꾸로 읽은 '스네이크(SNAKE)'로도 불린다. 프로그래밍 언어 '고(GO)'로 작성됐으며, 감염 시 ICS에서 사용하는 프로세스를 종료시키는 게 특징이다. 미국 보안 업체 센티넬원은 SNAKE에서 이전에 볼 수 없었던 방식의 난독화 기술이 반영돼 있다고 분석했다.

4.2.1. Snake 랜섬웨어 개요

1분기 주요 검색엔진에서 랜섬웨어 연관검색어로 확인된 신규 랜섬웨어중 하나인 Snake랜섬웨어가 있다. 이 랜섬웨어는 감염 시 암호화 된 파일내용의 마지막에 SNAKE의 알파벳 역순인 EKANS라는 문자를 남긴다. Snake 랜섬웨어의 특이한 점으로는 구글에서 개발된 프로그래밍 언어 '고(Go)'를 사용하여 개발되었으며, 산업제어 시스템에서 사용되는 프로세스 등을 종료시키는 기능을 담고 있다.

Snake 랜섬웨어 감염 시 프로세스를 일부 종료 시키며, 감염된 시스템의 파일을 암호화 한다. 이때, 랜섬웨어가 종료를 시도하는 프로세스는 주로 산업제어 프로그램에서 사용되는 프로세스 들이 다수 포함되어 있다.

기존에 랜섬웨어에서 일반적으로 사용되는 난독화 방식과는 다른 방식을 사용하고 있다.

4.2.2. 특이사항

o 랜섬웨어 암호화 과정도식

[적용된 암호화 알고리즘 및 도식도]

윈도우 내장 암호라이브러리(advapi32.dll)를 사용하며, 암호화 키 생성 시 고정된 시드 없이 엔트로피를 사용한 윈도우용 난수생성 API를 활용하여 난수를 생성한다. 생성된 난수를 대칭 암호화키로 사용하여, AES-256블록 암호화 방식으로 사용자 파일을 암호화 한다. 암호화가 종료되면 해당 암호화 키는 RSA-2048을 이용하여 암호화 한다. 각 파일별로 이 암호화 과정을 반복한다.

[그림 12] Snake 랜섬웨어 암호화 과정

o 랜섬웨어 기능분석

1. 감염과정

Snake 랜섬웨어는 트로이목마나 전자메일 첨부파일 등을 통하여 주로 전파된다. 랜섬웨어 감염 이후 암호화를 수행하며, 자체에 전파기능은 존재하지 않는다.

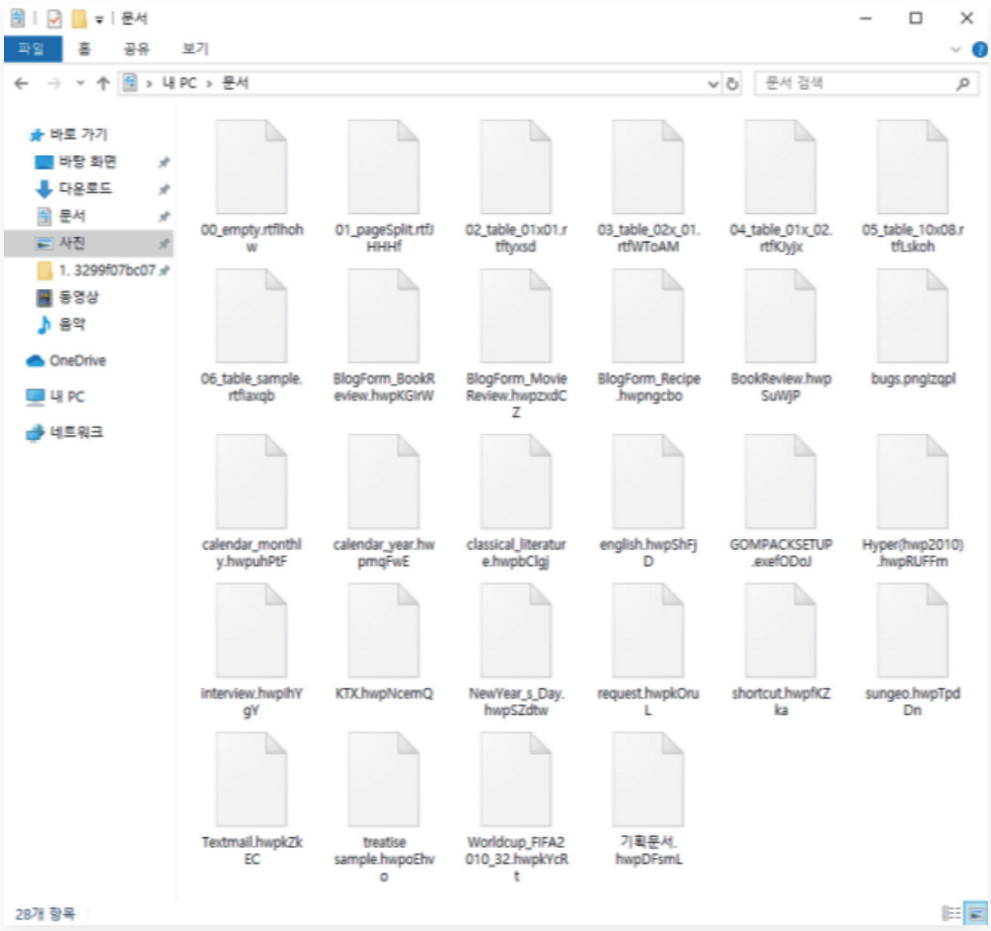
2. 랜섬웨어 감염 시 피해범위

특정 프로세스를 강제로 종료 시키며 아래와 같이 예외 폴더를 제외하고 나머지 시스템의 모든 경로의 파일을 암호화 한다.

[표 3] Snake 랜섬웨어 암호화 예외폴더

windir
SystemDrive
:\$Recycle.Bin
:\ProgramData
:\Users\All Users
:\Program Files
:\Local Settings
:\Boot
:\System Volume Information
:\Recovery
\AppData\

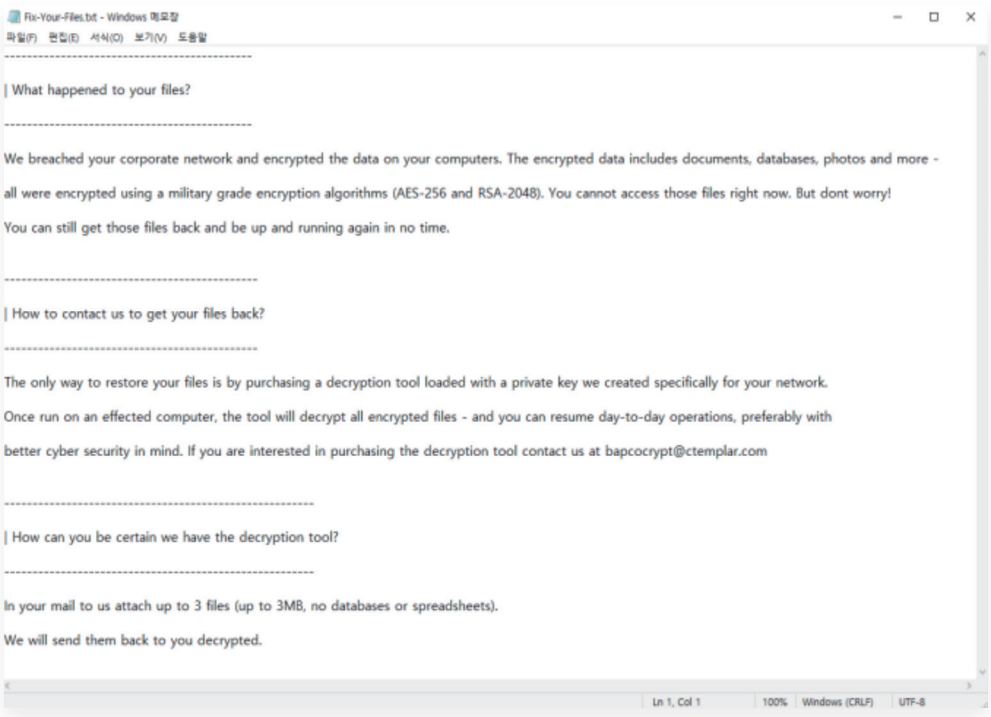
파일이 암호화 될 경우 기존 파일명 뒤에 각 파일마다 다른 임의문자 5글자가 추가 되는 것을 확인 할 수 있다.



[그림 13] Snake 랜섬웨어에 암호화 된 파일

3. 랜섬웨어 피해확인

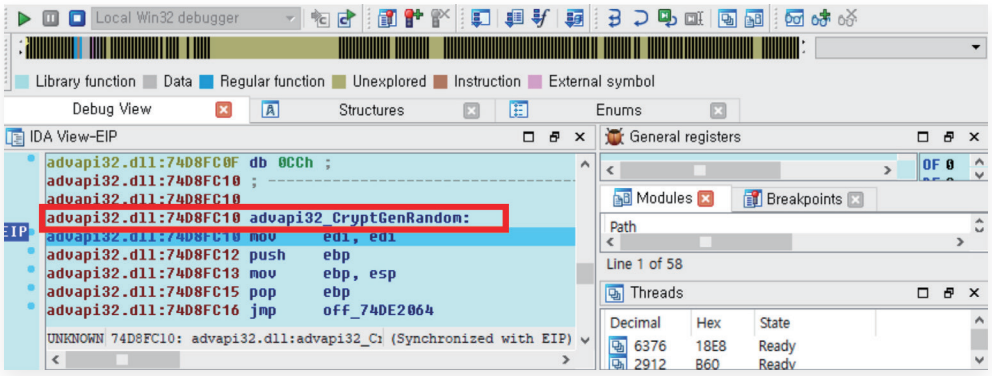
Snake 랜섬웨어는 감염이 완료된 후 바탕화면에 'Fix-Your-Files.txt'파일을 생성하고 복호화 비용을 요구한다. 랜섬노트 내용은 다음과 같다. 랜섬웨어 감염 시 전자메일로 3개 내외의 파일을 공격자에게 보내면 샘플로 복호화 해 주겠다고 밝히고 있다. 공격자에게 비용을 지불할 경우 감염된 네트워크 모든 시스템에 대하여 복구가 가능한 도구를 제공한다고 주장하며 복호화 비용 지불을 유도한다.



[그림 14] Snake랜섬웨어 감염 시 생성되는 랜섬노트

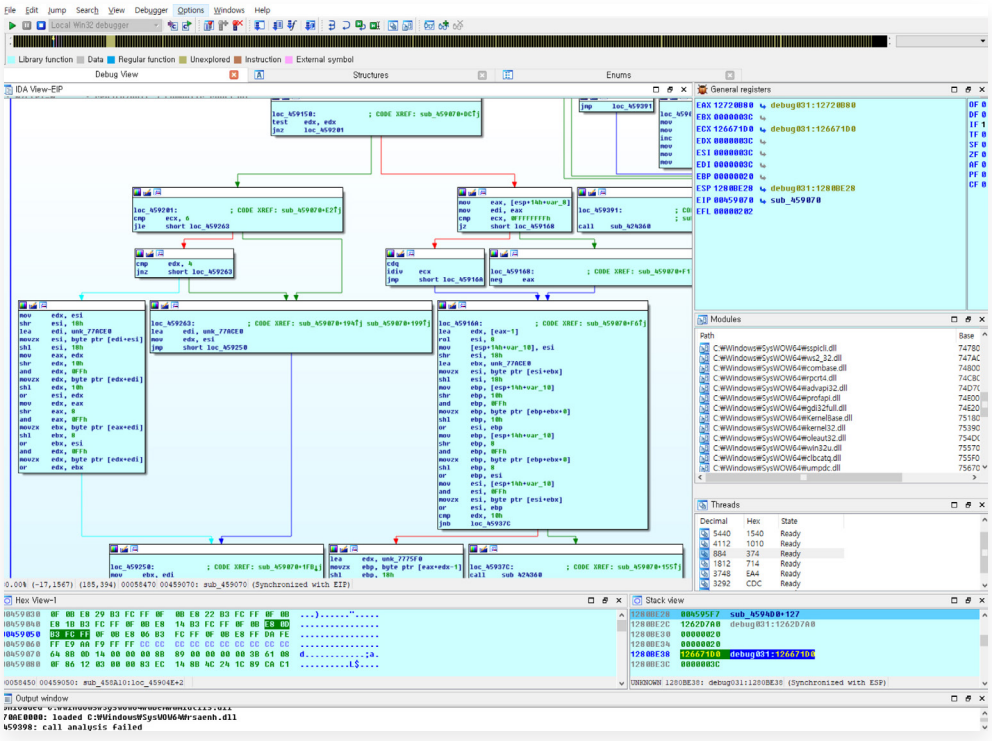
4. 암호화 알고리즘

랜섬웨어는 AES-256, RSA-2048을 사용하고 있다. Key생성 과정에서 사용되는 윈도우 제공 API(CryptGenRandom 함수)는 시드 값 생성에 윈도우시스템에서 제공 되는 엔트로피[1]를 사용하여 시간시드 난수생성 취약점[2]을 방지하고 있다. 다음 그림은 난수를 생성하여 AES암호화 알고리즘 키로 전달하기 위한 API실행 화면이다.



[그림 15] 암호화키 사용 시 호출되는 난수생성 함수 CryptGenRandom

다음그림은 앞에서 생성된 난수를 이용하여 암호화를 진행하는 암호화 루틴 실행코드 부분이다.



[그림 16] Snake 랜섬웨어 암호화 루틴

5. 복구도구

복구도구는 공개 되어있지 않으나, 백업기능을 활성화 하였을 경우 섀도볼륨이나 백업파일을 통하여 복구가 가능하다.

6. 주의사항

- 의심스러운 메일의 첨부 파일을 내려 받은 경우, 파일확장자를 확인하여 실행파일이면 실행 금지
- 시스템 업데이트를 최신상태로 유지

1) 엔트로피 : PC에서 생성되는 불확실성을 만들 수 있는 데이터를 다수 수집하여 유추하기 힘든 임의 값을 추출한 값으로 CryptAcquireContext 함수를 이용해 생성한다. 이 엔트로피 값은 CryptGenRandom 함수를 통하여 재현하기 어려운 유사난수로 생성된다.

2) 시간시드 난수생성 취약점 : 컴퓨터에서 사용하는 난수 생성기는 시드 값에 따라서 동일한 순서로 동일한 난수를 생성 하므로 난수 생성 시 입력한 시드 값과 난수 생성 회수를 유추하면 생성된 난수를 유추 할 수 있는 취약점이 존재 한다. 따라서 시드값 유추를 어렵게 하기 위하여 프로그램 실행시간을 시드 값으로 종종 활용한다. 하지만 실행시간을 시드 값으로 활용할 경우에도 파일 생성시간 등을 통하여 시드 값 입력에 사용된 시간을 유추 할 수 있는 가능성이 존재 한다.

4.3. Ravack 랜섬웨어

12만 구독자를 가진 유튜브에서 유포하는 RAVACK 랜섬웨어 유포 주의
체크멀블로그 (2020.3.4)

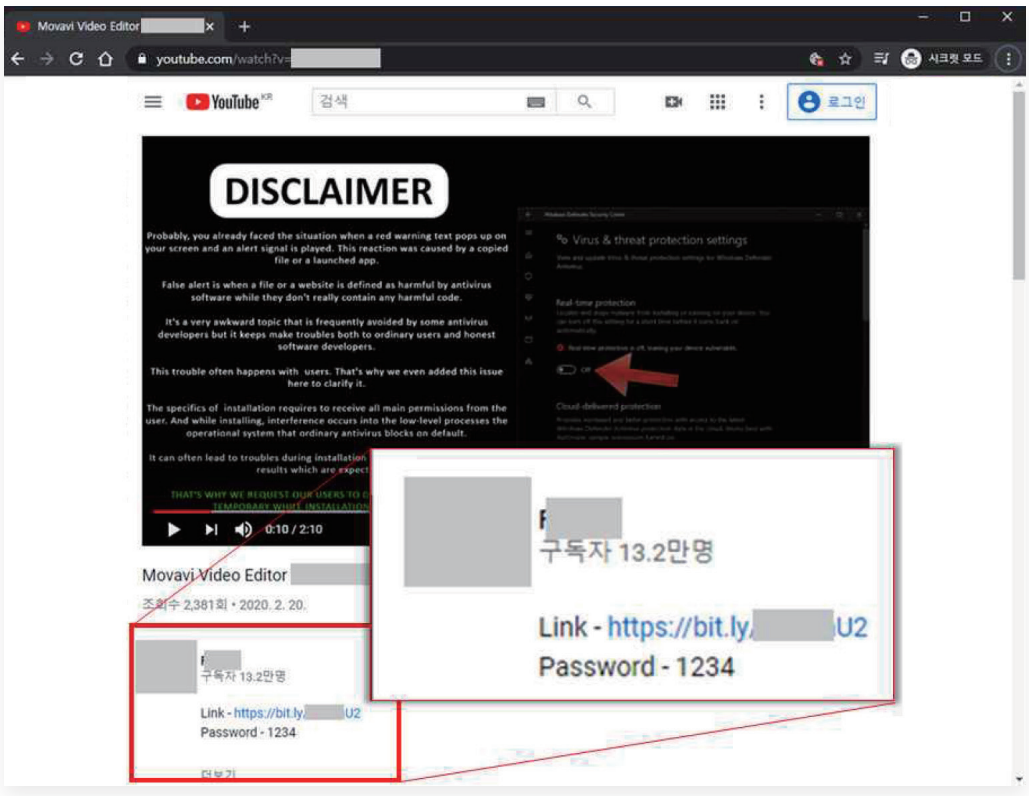
사례 1.

유튜브 채널을 통해 랜섬웨어가 배포되는 사례가 발견되었다. 해당 유튜브는 불법으로 소프트웨어 활성화라이선스키를 유포하는 행위를 하고 있었으며, 현재도 채널은 정상적으로 운영 중에 있다.

유포되는 랜섬웨어는 동영상편집 프로그램 설치파일에 삽입되어 실행 시 악성코드가 파일로 분리되어 실행된다.

4.3.1. Ravack 랜섬웨어 개요

불법 소프트웨어를 유포하는 전문채널을 운영하는 유튜버에 의해 랜섬웨어가 유포 되고 있다. 해당 유튜버는 12만 구독자를 가진 해외 유튜버로 영상을 통하여 불법 소프트웨어 자료에 랜섬웨어를 포함하여 배포하고 있다. 해당 소프트웨어는 랜섬웨어를 실행파일 내부에 포함하고 있어 소프트웨어 설치 과정에서 랜섬웨어와 악성코드가 생성 되고 실행된다. 현재도 해당 불법소프트웨어는 지속적으로 배포 되고 있으나 백신 등에 랜섬웨어 포함 여부가 탐지되지 않아 주의를 요한다.[3)]



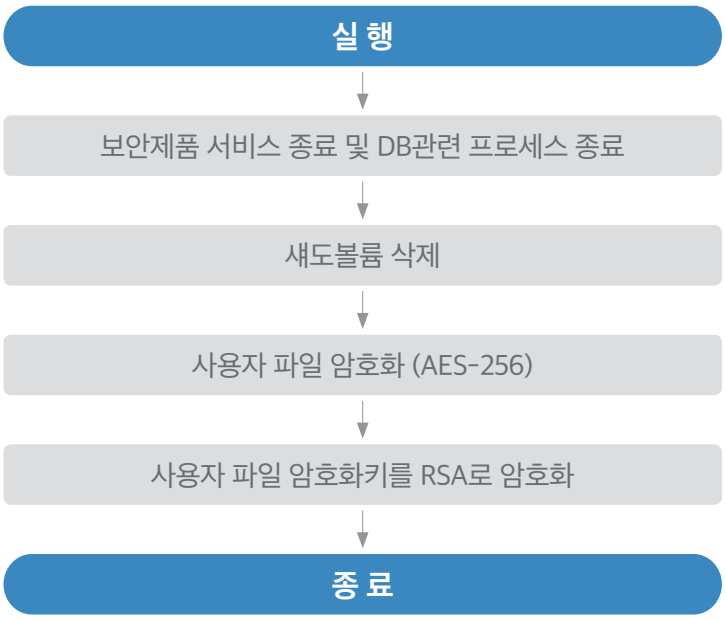
[그림 17] 동영상 추가정보란에 링크로 악성코드를 배포

3) 현재('20.04.30기준) Virustotal 기준 66개 백신 중 V3, 알약, 바이로봇을 포함 29개 백신에서 탐지하고 있음

4.3.2. 특이사항

o 랜섬웨어 암호화 과정도식

Ravack 랜섬웨어는 대칭 암호화키를 생성하여, AES-256블록 암호화 방식으로 사용자 파일을 암호화 한다. 암호화가 종료되면 해당 AES 암호화 키는 RSA-2048을 이용하여 암호화 한다.

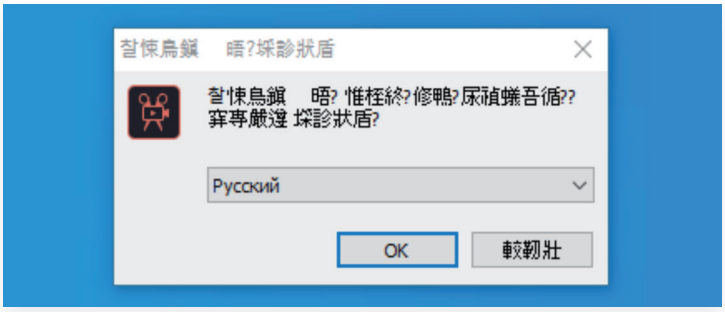


[그림 18] Ravack 랜섬웨어 암호화 과정

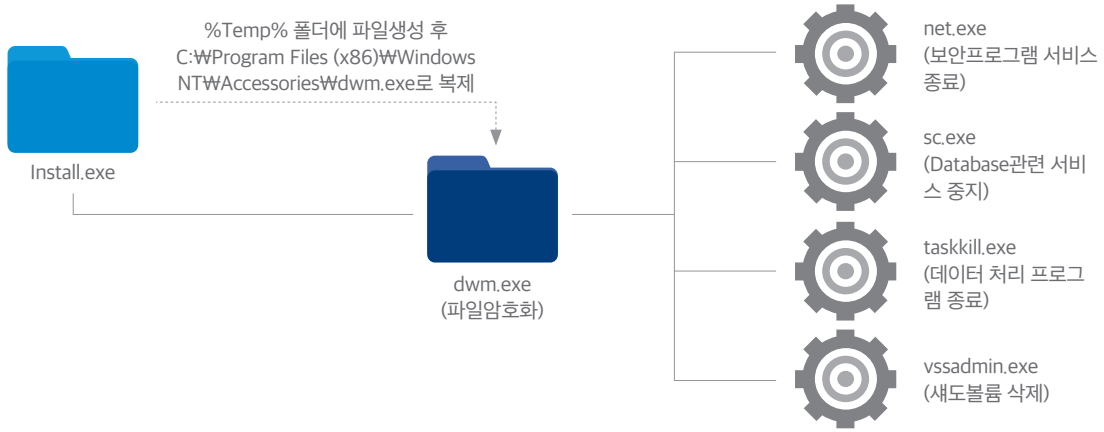
o 랜섬웨어 기능분석

1. 감염과정

Ravack 랜섬웨어는 불법복제 프로그램으로 위장하여 사용자들의 설치를 유도한다. 랜섬웨어 감염 이후 암호화를 수행하며, 자체에 전파기능은 존재 하지 않는다.



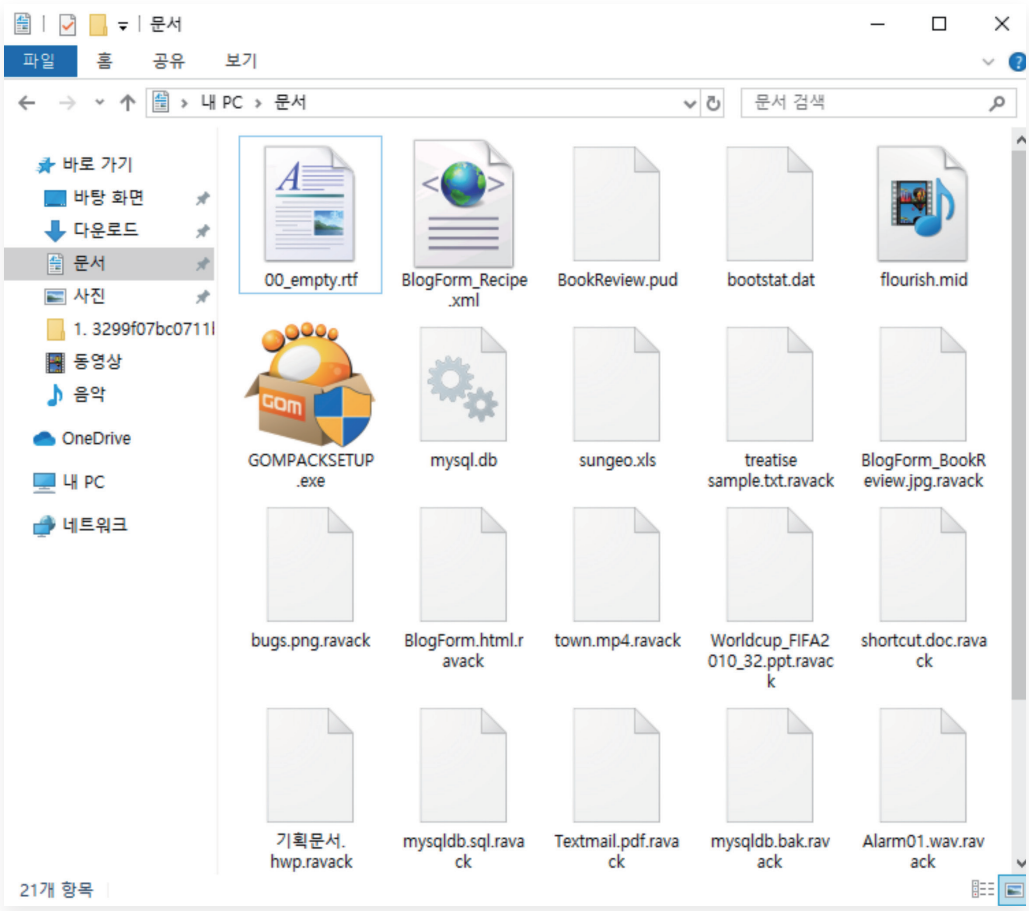
[그림 19] 위장된 불법복제 프로그램 설치 화면



[그림 20] Ravack 랜섬웨어 프로세스 실행 흐름

2. 랜섬웨어 감염 시 피해범위

Ravack 랜섬웨어에 감염되면, 보안프로그램과 데이터베이스나 Ms퍼블리셔 등 데이터를 상업적으로 제작하는 도구를 강제로 종료시켜 시스템이나 사용자가 작업 중인 파일도 암호화 할 수 있도록 동작한다. 감염대상 파일의 확장자는 sql, bak, zip, txt, doc 등으로 감염된 파일은 끝에 '.Ravack'이라는 확장자를 추가한다. 특징으로 hwp파일도 공격 대상에 포함되어 있다.



[그림 21] Ravack 랜섬웨어 감염된 파일

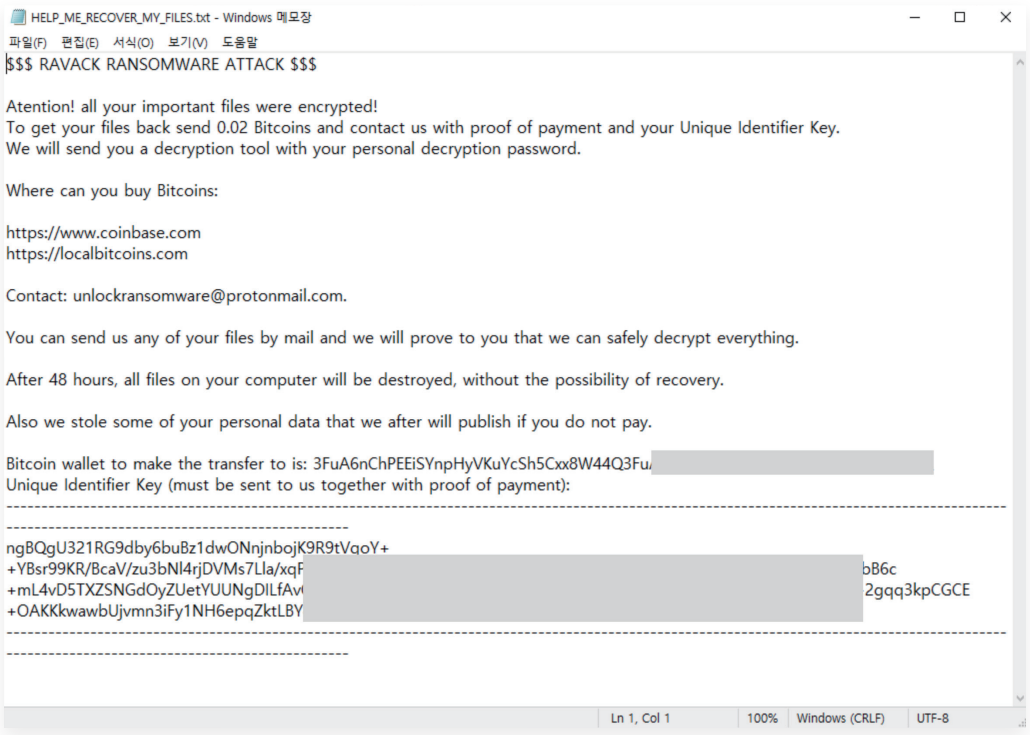
암호화 대상 파일은 확인된바 다음과 같다. 일부 파일포맷(.xls, .rtf, .db)이 제외 되어 있으나 일반적인 사용자가 많이 사용하는 파일포맷을 대부분 포함하고 있다.

[표 4] Ravack 랜섬웨어 암호화 대상 파일 확장자

포함된 파일 확장자 .xlsx, .docx, .doc, .txt, .jpg, .png, .ppt, .pptx, .hwp, .pdf, .mp3, .mp4, .avi, .html, .sql, .bak 등

3. 랜섬웨어 피해확인

Ravack 랜섬웨어는 감염이 완료된 후 바탕화면에 'HELP_ME_RECOVER_MY_FILES.txt' 파일을 생성하고 복호화 비용을 요구한다. 복호화 비용은 0.02비트코인을 요구하며, 비트코인 주소를 공개하고 있다. 48시간 내에 보내지 않을 경우 복구가 불가능 하다는 내용과 함께 랜섬노트에 적힌 Unique ID를 보낼 것을 요구하고 있다. 랜섬노트 내용은 다음과 같다.



[그림 22] Ravack 랜섬웨어 감염 시 생성되는 랜섬노트

4. 암호화 알고리즘

AES-256, RSA-2048 알고리즘을 사용하고 있다. 파일 암호화 수행 시 AES-256 알고리즘을 사용하여 암호화를 수행한다. 파일 암호화에 사용된 AES 암호화키는 RSA 알고리즘으로 암호화 되며, base64로 인코딩 되어 랜섬노트에 기록된 것을 확인할 수 있다.

5. 복구도구

현재 복구도구는 공개되어있지 않다.

6. 주의사항

불법 소프트웨어에 악성코드를 포함시켜 유포시키는 행위가 발견된 사례로 사용자에게 직접적인 피해가 발생 할 수 있다.

4.4. Mailto 랜섬웨어

"Toll says IT systems infected by new variant of 'Mailto' ransomware"
CSOonline (2020.2.4)

"Spanish hospitals targeted with coronavirus-themed phishing lures in Netwalker ransomware attacks" computing (2020.4.24.)

사례 1.

호주 물류운송 전문기업 톨그룹이 지난 1월 31일 Mailto 랜섬웨어 공격으로 다수의 IT시스템이 멈추었으며, 물류운송에 차질을 초래했다. 톨그룹은 50여 개국에 진출해 있으며 연 매출은 80억 달러에 이르는 것으로 알려져 있다. 톨그룹은 Mailto 랜섬웨어의 공격으로 인하여 일부 물류 IT시스템을 수동으로 전환하여 운영하였다. 최근 다른 신규 랜섬웨어의 공격을 받은 것으로 알려져 있다.

사례 2.

스페인 경찰은 스페인의 병원이 Mailto 랜섬웨어의 공격을 받았다고 발표 하였다. 3월말 COVID-19에 대한 정보를 위장한 악성코드를 포함한 전자메일 공격이 있었다. 스페인 경찰은 병원 등 의료시설에 대하여 COVID-19 정보로 위장한 전자메일 공격이 발생하고 주의를 당부 하였다.

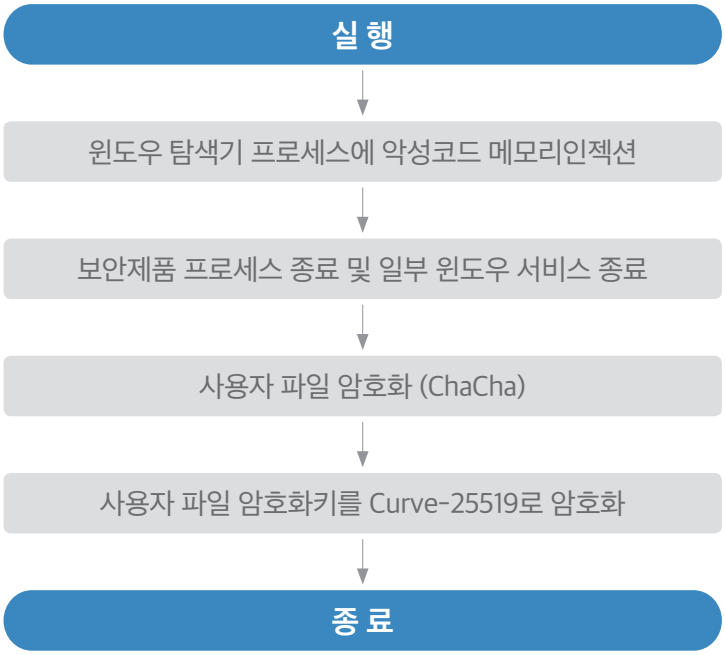
4.4.1. Mailto 랜섬웨어 개요

Mailto 랜섬웨어는 지난 2019년 8월 경 처음 발견된 랜섬웨어로 2020년 1분기(2020.01.01.~2020.03.31.) 구글트렌드 랜섬웨어 상승 연관검색어 4위에 포함된 악성코드 이다. Mailto 랜섬웨어에 감염될 경우 파일 확장자에 .mailto[<email>].<숫자, 알파벳 5글자> 형식의 문자열이 추가 된다. Netwalker로도 알려져 있다. 일부 의료관련 기관에 COVID-19관련 정보를 위장한 전자메일 첨부파일로 공격을 시도한 사례가 발견되었다.

4.4.2. 특이사항

o 랜섬웨어 암호화 과정도식

Mailto 랜섬웨어는 chacha알고리즘으로 파일을 암호화 하며, 암호화에 사용된 키는 Curve25519 타원곡선 알고리즘을 사용하여 비대칭키 형식으로 암호화 된다. 이때 사용된 키는 랜섬노트를 통해 피해자에게 보이며, 이를 공격자가 전자메일을 통해 송신할 것을 요구한다.

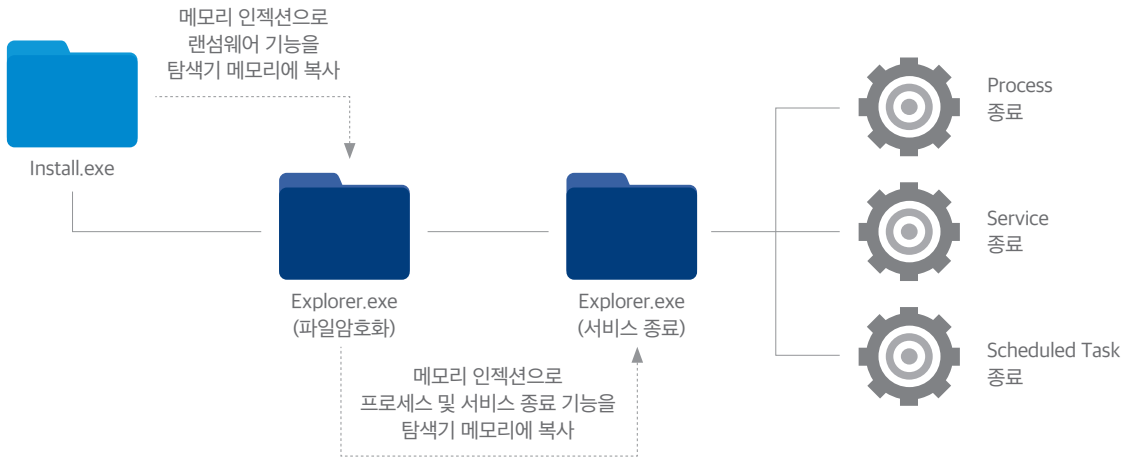


[그림 23] Mailto 랜섬웨어 암호화 과정

o 랜섬웨어 기능분석

1. 감염과정

Mailto 랜섬웨어는 전자메일 첨부파일이나, 드라이브 바이 다운로드[4] 방식으로 전파된다. 감염될 경우 악성코드 백신을 회피하기 위하여 윈도우 탐색기 프로세스를 실행시키고 탐색기 메모리에 악성코드를 복사하고 이를 실행 시킨다[5]. 복사된 악성코드는 파일을 암호화하는 랜섬웨어 기능으로 동작한다.



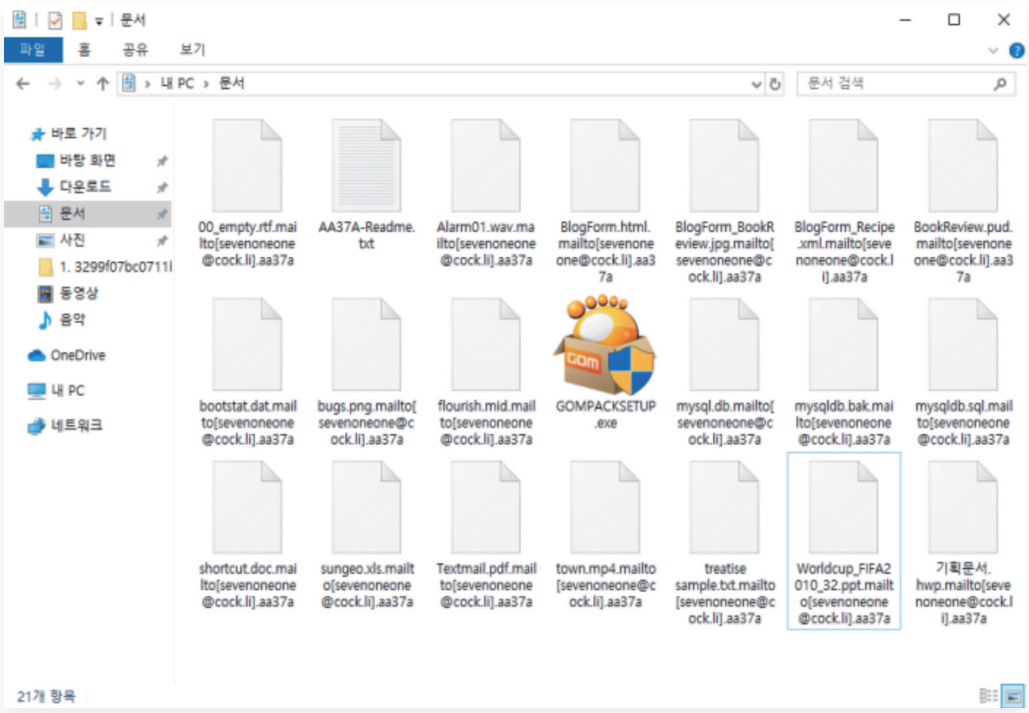
[그림 24] Mailto 랜섬웨어 실행 흐름

4) 드라이브 바이 다운로드(drive-by-download) : 드라이브 바이 다운로드는 웹 사이트를 방문하거나 전자메일 메시지를 볼 때 또는 팝업 윈도우를 클릭할 때 실행파일이나 액티브엑스(ActiveX) 등의 다운로드를 자동으로 수행하는 기능이다. 웹 사이트 사용자의 편의를 위해 개발된 기능이나 악성코드에 의해 자동으로 시스템을 감염시키는 기능으로 악용되기도 한다.

5) 악성코드 백신 회피 : 백신의 경우 악성코드를 탐지하기 위하여 디스크에 저장된 파일이 실행되는 시점에서 실행 파일의 시그니처를 탐지 하는 방식을 사용한다. 따라서 프로세스가 생성되고 난 뒤 메모리에 악성행위를 하는 코드를 복사 할 경우 백신 프로그램에서는 확인이 불가능한 약점이 존재 한다.

2. 랜섬웨어 감염 시 피해범위

Mailto 랜섬웨어에 감염되면 특정 서비스와 예약실행 등의 기능이 중지되며, 사용자 파일을 암호화 시킨다. 암호화 되는 파일은 아래 그림과 같이 파일명 뒤쪽에 mailto[공격자메일주소].<랜덤한5글자> 형식으로 확장자를 추가한다.



[그림 25] Mailto 랜섬웨어로 암호화된 파일

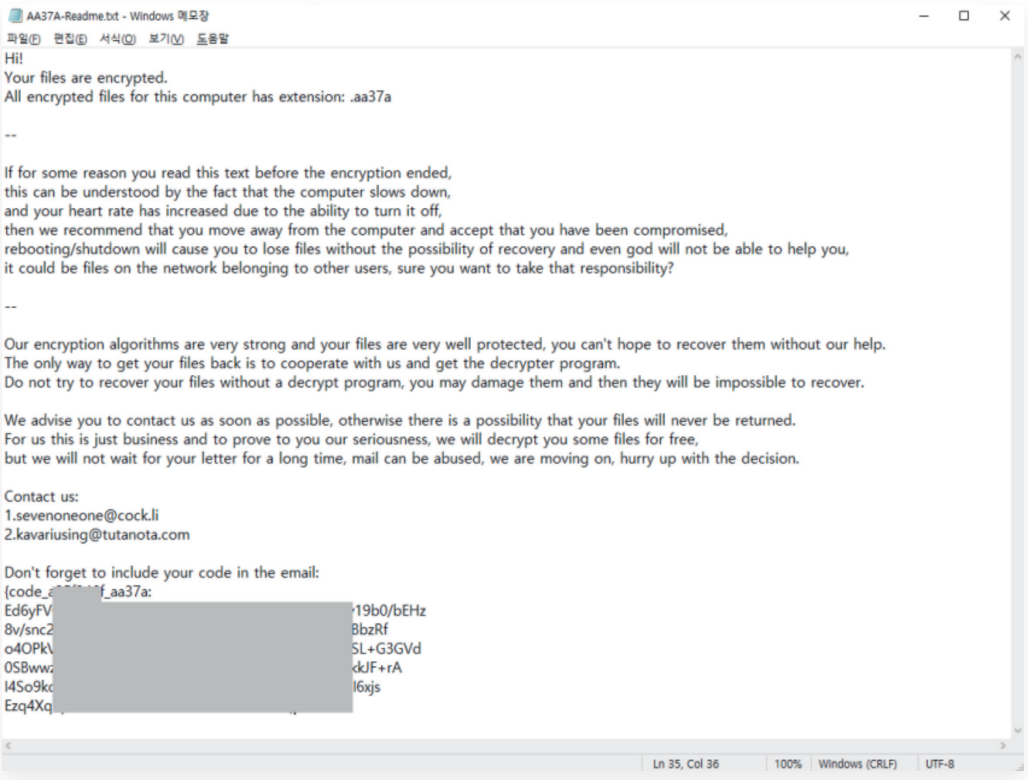
Mailto 랜섬웨어 감염은 실행파일과 dll 파일 등을 제외하고 대부분의 파일을 암호화 하며, 시스템 구동에 필요한 Windows 폴더와 Program Files 폴더 등을 제외한 대부분의 폴더를 대상으로 파일을 암호화 한다. 암호화 예외 파일은 다음과 같다.

[표 5] Mailto 랜섬웨어 암호화 예외 폴더 및 파일

구 분	대 상
예외 폴더	Windows, Windows.old Program Files, Program Files (x86), PerfLogs ProgramData users**temp, \\users*\\AppData 등
암호화 예외 파일 확장자	.exe .com .dll .sys .ocx .msc .msp .clb .mui .rgtrans-ms .ps1 .mpa .cpl .icl .msu .msi .nls .scr .adv .386 .com .hlp .ini .cfg 등

3. 랜섬웨어 피해확인

Mailto 랜섬웨어는 감염이 완료된 후 바탕화면에 '<랜덤5글자>-Readme.txt' 파일을 생성하고 복호화 비용을 요구한다. 랜섬노트 내용은 다음과 같이 복호화를 위하여 공격자에게 전자메일을 송신할 것을 요구한다. 랜섬노트 내에서는 몇 개의 파일에 대해서만 비용 없이 복호화를 진행해 준다고 언급하고 있다. 랜섬노트 내에서는 복호화 비용에 대하여 금액을 언급하고 있지 않다.



[그림 26] Mailto 랜섬웨어 감염 시 생성되는 랜섬노트

4. 암호화 알고리즘

ChaCha stream 암호화 알고리즘과 Curve-25519 비대칭키 암호화 알고리즘을 사용하고 있다. 파일 암호화 수행시 ChaCha 알고리즘을 사용하여 암호화를 수행한다. 파일 암호화에 사용된 암호화키는 Curve-25519알고리즘으로 암호화 되며, base64로 인코딩 되어 랜섬노트에 기록된 것을 확인 할 수 있다.

5. 복구도구

현재 복구도구는 공개되어있지 않다.

6. 주의사항

전자메일을 통한 악성코드 전파에 자주 악용되는 랜섬웨어 사례로서 전자메일 첨부파일 확인 시 확장자를 확인하여 실행파일의 경우 실행하지 않는다.

모르는 사람이나 의심스러운 전자메일은 확인하지 않고 삭제 한다.

4.5. Ako 랜섬웨어

"Ako Ransomware Uses Spam to Infect Its Victims", BleepingComputer (2020.1.15.)
"다양한 유포 방식으로 감염될 수 있는 Ako 랜섬웨어 주의", 체크멀블로그(2020.1.24.)

사례 1.

"agreement.zip" 라는 전자메일 첨부파일로 배포되었으며, 협정서로 위장하여 수신된 전자메일이 신고 되었다. 해당 첨부파일은 암호화된 암축파일로 작성되어 있다. 압축을 풀면 agreement.scr 이라는 파일을 생성하며, 실행 시 파일을 암호화 하는 것으로 밝혀졌다.

사례 2.

2020년 1월 19일 새벽 2시경 국내에서 실행된 Ako 랜섬웨어 변종의 경우에는 원격 제어(RDP)를 통해 시스템에 접속하여 랜섬웨어 악성 파일을 직접 실행하였을 것으로 추정 된다.

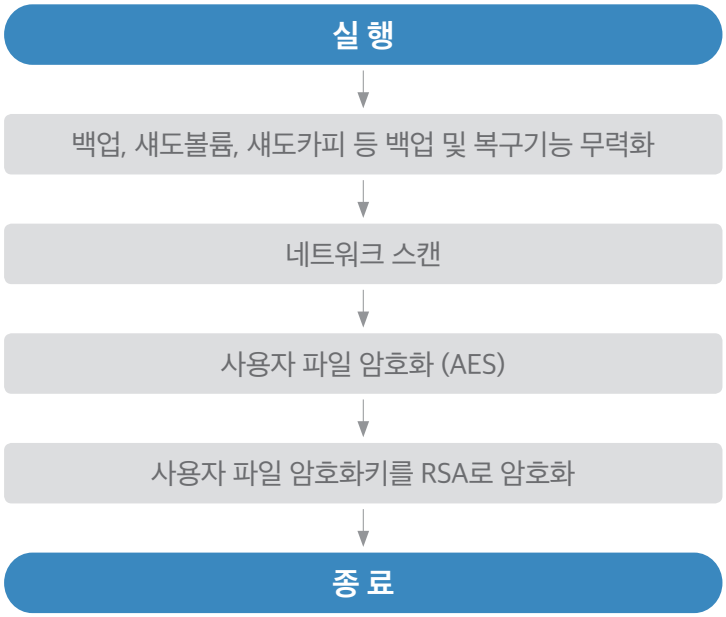
4.5.1. Ako 랜섬웨어 개요

Ako 랜섬웨어는 1월 초에 처음 발견된 랜섬웨어로 2020년 1분기('20.01.01.~'20.03.31.) 구글트렌드 랜섬웨어 상승 연관검색어 5위에 포함된 악성코드이다. 일부 변종의 경우 토르(Tor)브라우저를 설치하고 특정 사이트로 접속할 것을 요구하는 경우도 존재 한다. 일부 사례에서는 협정서라는 이름으로 첨부파일을 위장하여 사용자가 실행하도록 유도하고 있다.

4.5.2. 특이사항

o 랜섬웨어 암호화 과정도식

대칭 암호화키를 생성하여, AES블록 암호화 방식으로 사용자 파일을 암호화 한다. 암호화가 종료되면 해당 암호화키는 RSA를 이용하여 암호화 한다.



[그림 27] Ako 랜섬웨어 암호화 과정

o 랜섬웨어 기능분석

1. 감염과정

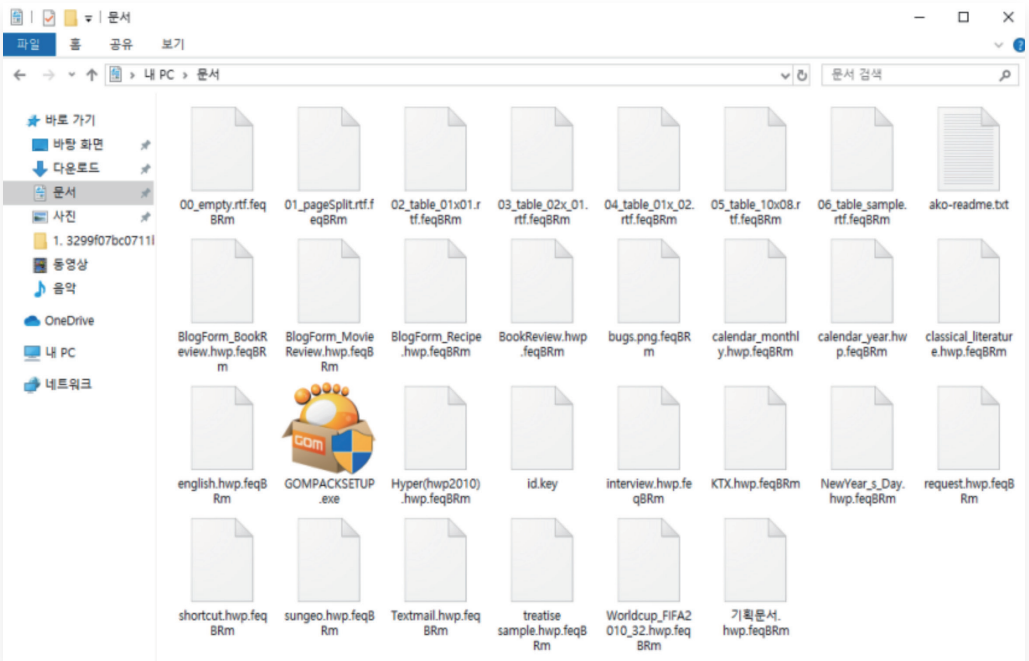
Ako 랜섬웨어는 전자메일 첨부파일 등으로 감염된다. 감염될 경우 시스템의 복원기능을 무력화하기 위한 기능이 동작된다. 아래 표와 같이 명령어를 실행하여 섀도볼륨과 섀도카피, 시스템 백업도 삭제한다. 또한 네트워크 스캔을 시도하며, 네트워크 관련 전파를 시도하기 위한 기능이 일부 구현되어 있는 것으로 보인다.

[표 6] 섀도볼륨과 섀도카피 삭제 등 복구기능을 무력화 하는 명령어

```
vssadmin.exe Delete Shadows /All /Quiet
bcdedit.exe /set {default} recoveryenabled No
bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
wbadmin DELETE SYSTEMSTATEBACKUP
wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
wmic.exe SHADOWCOPY /nointeractive
```

2. 랜섬웨어 감염시 피해범위

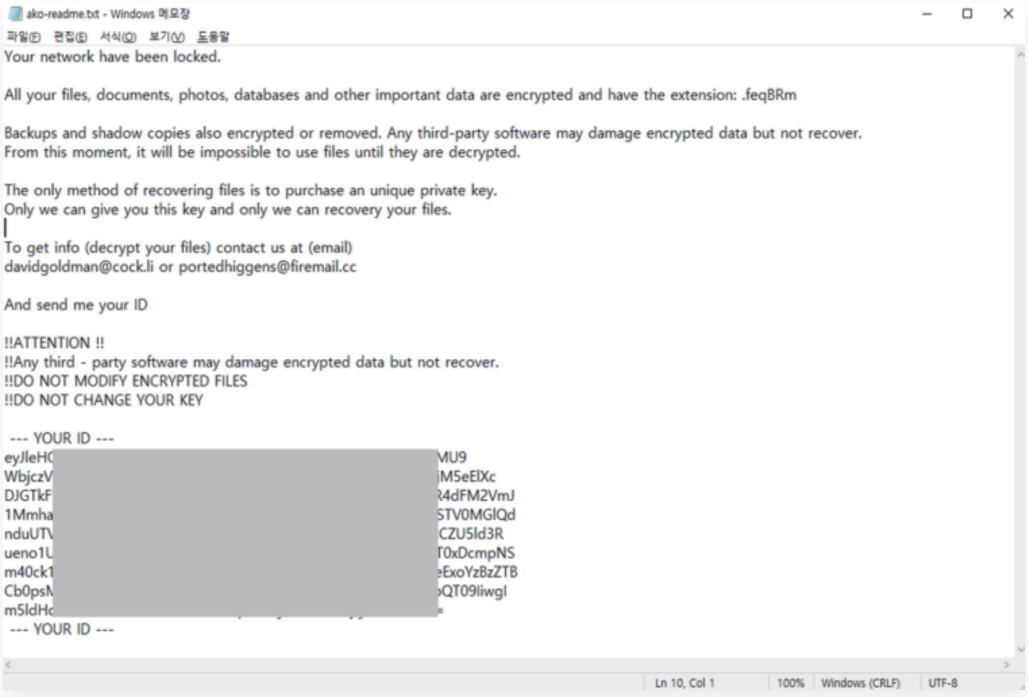
Ako 랜섬웨어 감염 시 시스템 구동에 필요한 windows폴더와 Program Files 폴더 등을 제외하며, Ako 랜섬웨어는 실행파일 및 바로가기 등 일부 파일을 제외하고 모든 파일을 암호화 한다. 다음 그림은 각종 확장자 파일에 대한 암호화 결과를 볼 수 있다. 암호화 된 파일은 파일명 뒤에 <랜덤한 6글자>의 확장자를 모든 파일에 동일하게 추가 하는 것을 알 수 있다.



[그림 28] Ako 랜섬웨어로 암호화된 파일

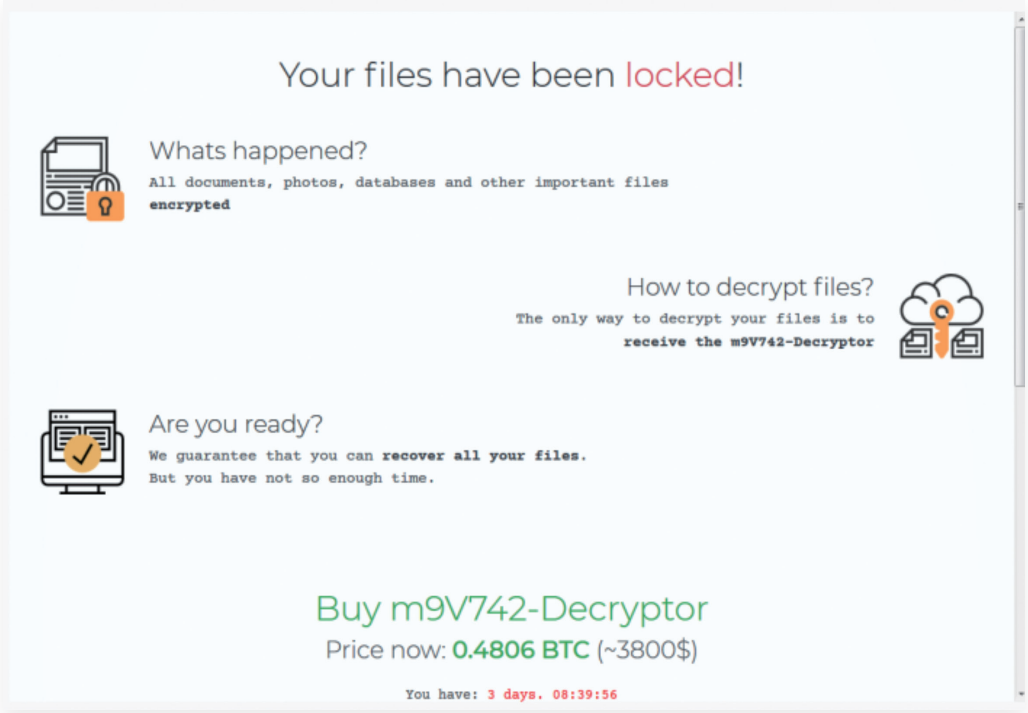
3. 랜섬웨어 피해확인

Ako 랜섬웨어는 감염이 완료된 후 바탕화면에 'ako-Readme.txt' 파일을 생성하고 복호화 비용을 요구한다. 랜섬노트 내용은 다음과 같다.



[그림 29] Ako 랜섬웨어 감염 시 생성되는 랜섬노트

버전1.0 이상의 변종의 경우 토르(Tor)브라우저를 설치하고 특정 사이트로 접속할 것을 요구하는 경우도 존재 한다. 일정 시간 이후에 비용을 두 배로 올릴 것이라고 협박하고 있다. 비용은 미화 3000~8000불을 기준으로 비트코인을 요구하고 있으며 배포시마다 다른 비용을 요구하고 있다.

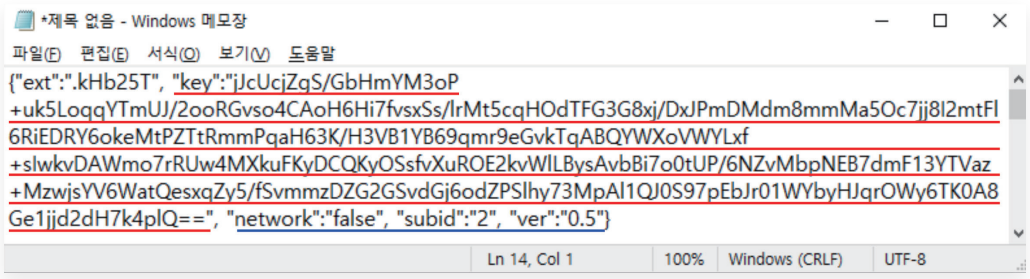


[그림 30] 토르브라우저를 통하여 복호화 비용을 요구하는 사이트

4. 암호화 알고리즘

Ako 랜섬웨어는 AES 암호화 알고리즘과 RSA 비대칭키 암호화 알고리즘을 사용하고 있다. 파일 암호화 수행 시 AES 알고리즘을 사용하여 암호화를 수행한다. 파일 암호화에 사용된 AES 암호화키는 RSA 알고리즘으로 암호화되며, base64로 인코딩 되어 암호화된 폴더에 id.key파일명으로 저장되어 있다. 버전 1.1이상의 랜섬웨어에 경우는 해당 파일명이 do_not_remove_ako.<암호화 확장명>_id.key로 다르게 저장된다.

랜섬노트에 작성된 "Your ID" 는 id.key파일의 내용을 다음 그림과 같이 사용자의 정보를 바탕으로 base64로 다시 한 번 인코딩 하여 기록하고 있다.



[그림 31] 피해자 감염정보를 해커에게 전송하기 위한 ID 문자열 복호화한 내용

5. 복구도구

현재 복구도구는 공개되어있지 않다.

6. 주의사항

전자메일을 통한 악성코드 전파에 자주 악용되는 랜섬웨어 사례로서 전자메일 첨부파일 확인 시 확장자를 확인하여 실행파일의 경우 실행하지 않는다.

모르는 사람이나 의심스러운 전자메일은 확인하지 않고 삭제 한다.

05 랜섬웨어 복구동향

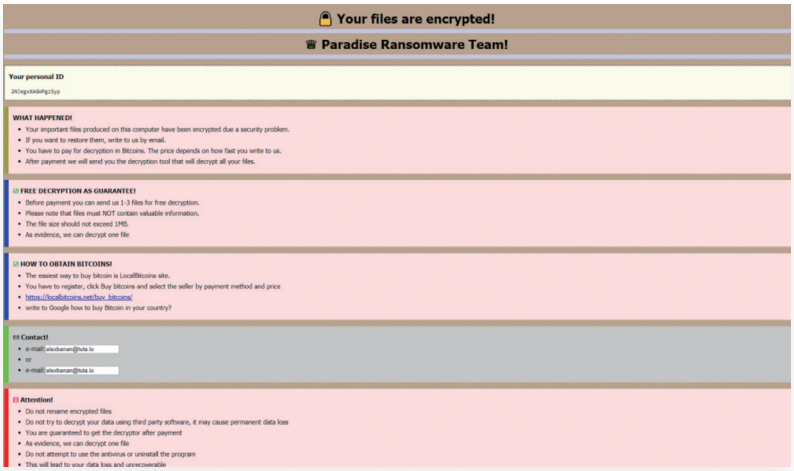
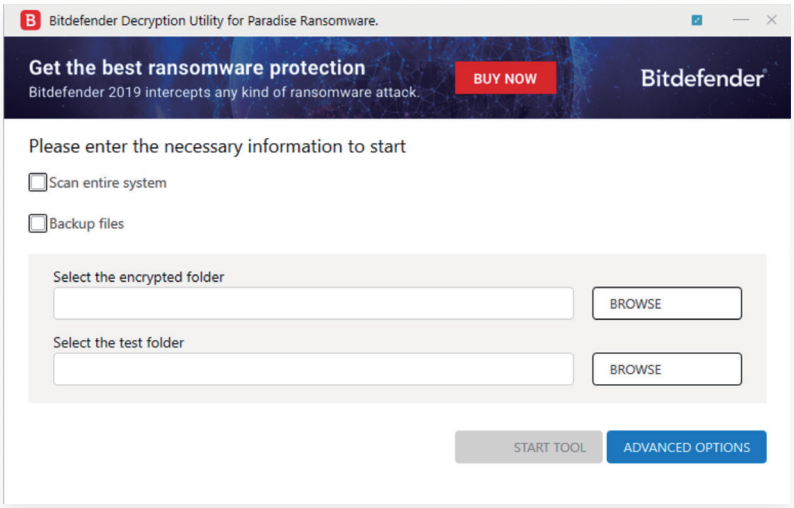
5.1. 2020년 1분기 랜섬웨어 복구도구 현황

2020년 1분기동안 개발된 신규 랜섬웨어 복구도구는 총 2종이다. 1분기에는 비트디펜더(Bitdefender)에서 1종, 엠시소프트(Emsisoft)에서 1종 총 2종의 랜섬웨어 복구도구를 개발하였다.

랜섬웨어명	감염확장자	복구기관	링 크
Paradise	. FC, . 2ksys19, . p3rf0rm4, . Recognizer, . VACv2, . paradise, . CORP, .immortal, . exploit, . prt, . STUB, . sev, . sambo	Bitdefender	https://labs.bitdefender.com/2020/01/paradise-ransomware-decryption-tool/
Ransomwared	.ransomwared	Emsisoft	https://www.emsisoft.com/ransomware-decryption-tools/download/ransomwared

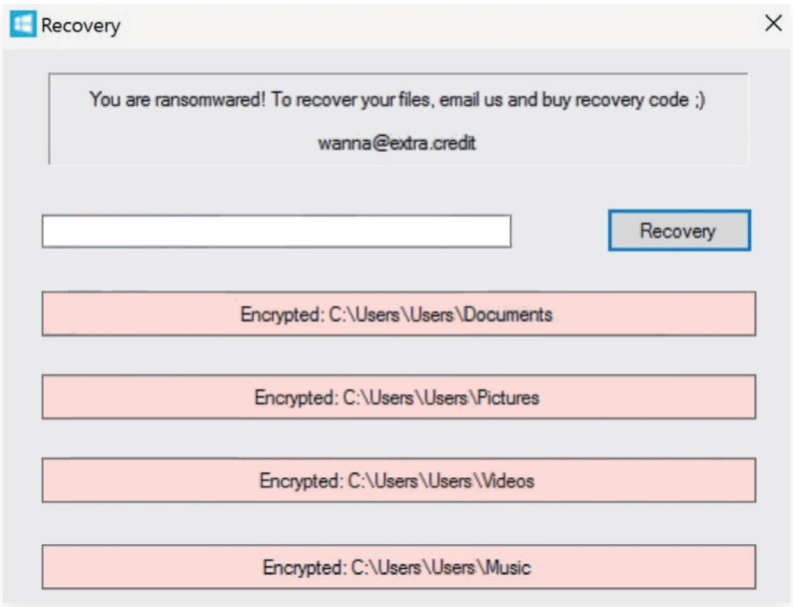
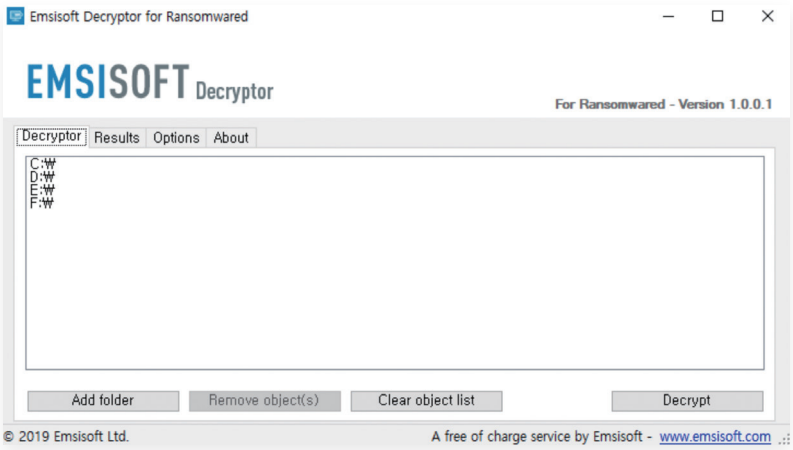
5.1.1. Bitdefender 복구도구 1종

Bitdefender사에서 Paradise 랜섬웨어에 대한 복구도구를 공개하였다. Paradise 랜섬웨어는 2017년 공개되었으며, 감염 시 키보드 언어가 러시아어, 카자흐어, 벨로루시 또는 우크라이나로 설정되어 있는지 확인하고 해당 언어가 아닐 경우 사용자의 파일을 암호화 한다.

구 분	내 용
랜섬웨어명	Paradise
복구가능 확장자	. FC, . 2ksys19, . p3rf0rm4, . Recognizer, . VACv2, . paradise, . CORP, .immortal, . exploit, . prt, . STUB, . sev, . sambo
랜섬노트 화면	
복구도구 공개기관	Bitdefender
복구도구	https://labs.bitdefender.com/2020/01/paradise-ransomware-decryption-tool/
복구도구 화면	
사용방법	https://labs.bitdefender.com/2020/01/paradise-ransomware-decryption-tool/

5.1.2. Emsisoft 복구도구 1종

두 번째로 확인된 복구도구는 Emsisoft사에서 공개한 Ransomwared 랜섬웨어 복구도구다. Ransomwared 랜섬웨어는 2018년에 발견된 랜섬웨어로 감염 시 사용자 파일을 암호화 하고 해커에게서 구입한 코드를 입력하는 창을 띄우는 특징이 있다.

구 분	내 용
랜섬웨어 명	Ransomwared
복구가능 확장자	.ransomwared
랜섬노트 화면	
복구도구 공개기관	Emsisoft
복구도구	https://www.emsisoft.com/ransomware-decryption-tools/ransomwared
복구도구 화면	
사용방법	https://www.emsisoft.com/ransomware-decryption-tools/howtos/emsisoft_how-to_ransomwared.pdf

06 결론

2020년 1분기는 국내외 주요 포털사이트 검색어 기준으로 전년 동기 대비 대중의 랜섬웨어에 대한 검색 횟수가 줄어들었다.[1] 또한, 보안회사의 랜섬웨어 탐지 결과에서도 2019년 1분기 대비 랜섬웨어 탐지 및 차단 횟수는 감소하였다[2][3].

하지만, 해커는 핀테크 해외 업체나 여행환전 업체 등의 감염사례에서 볼 수 있듯이 더 많은 몸값을 요구 할 수 있는 대기업 등에 대한 공격을 지속적으로 늘려나가고 있다. 특히, 미국 뉴올리언스 정부와 미국 국방성 계약업체 랜섬웨어 공격 사례 등에서 알 수 있듯이 공공부문에 대한 공격도 줄어들지 않음을 알 수 있다. 랜섬웨어 공격은 정부, 군사, 교육 제조, 금융 등 서비스 분야나 국적에 관계없이 위협이 증가하고 있는 것을 알 수 있다.[4][5]

감염방식으로 보면 1분기에 발견된 다수의 랜섬웨어를 배포하는 공격자가 전자메일로 감염파일을 전송하고 실행을 유도하고 있어 사용자의 각별한 주의를 요한다. 다만, 트래블엑스 사의 랜섬웨어 감염 사고에서 VPN 제품 자체의 취약점을 활용한 공격이 확인되었다. 이 사례에서 확인된 바와 같이 취약점을 통한 랜섬웨어 감염 사례도 확인되고 있다. 따라서 사용자는 자신의 시스템에 지속적인 보안패치를 수행하고 관리하는 노력이 필요하다.

- ⦿ 키생성 방식 : 대칭키와 비대칭키를 어떻게 생성방법
- ⦿ 공격대상 : 해당 랜섬웨어의 공격대상
- ⦿ 동작운영체제 : 랜섬웨어가 동작하는 운영체제 환경
- ⦿ 복구가능 여부 : 현재 복구도구가 개발되었는지 여부

등장 년도	활동 국가	랜섬웨어명	대칭키		비대칭키		동작 운영체제	공격 대상	복구가능 여부
			키생성방식	알고리즘	키생성방식	알고리즘			
2020	국외	Coronavirus	알려지지않음	임의제작	알려지지않음	알려지지않음	Windows	기업	불가능
2020	국외	Snake	CryptGen Random API 활용	AES-256	알려지지않음	RSA-2048	Windows	기업	불가능
2020	국외	Ravack	알려지지않음	AES-256	알려지지않음	RSA-2048	Windows	개인	불가능
2020	국외	Mailto	알려지지않음	ChaCha	알려지지않음	Curve25519	Windows	기업	불가능
2020	국외	Ako	알려지지않음	AES	알려지지않음	RSA	Windows	기업	불가능

[1] 구글 및 네이버 검색트렌드 자료
[2] 2019년 1분기, 알약 랜섬웨어 공격 행위차단 건수: 320,506건!
[3] 2020년 1분기, 알약 랜섬웨어 공격 행위차단 건수: 185,105건!
[4] The Journal Times('20.02.03.), Ransomware knocks city of Racine offline
[5] Fox8('2020.01.15.), City of New Orleans says it will take months to recover from recent cyber attack

레퍼런스

안랩블로그	2020.3.25.	CoronaVirus 랜섬웨어에 의한 윈도우 복구 무력화
보안뉴스	2020.1.07.	“VPN제품에서 발견된 오류 통해 퍼지고 있는 레빌 랜섬웨어”
블룸버그	2020.4.07.	Fintech Company Survived Ransomware Attack Without Paying Ransom
미국 FBI	2020.2.12.	“2019 Internet Crime Report”
구글 및 네이버 검색트렌드		Ransomware
이스트시큐리티	2019.4.10.	2019년 1분기, 알약 랜섬웨어 공격 행위차단 건수: 320,506건!
이스트시큐리티	2020.4.22.	2020년 1분기, 알약 랜섬웨어 공격 행위차단 건수: 185,105건!
The Journal Times	2020.2.03.	are knocks city of Racine offline
Fox8	2020.1.15.	City of New Orleans says it will take months to recover from recent cyber attack
CSOonline	2020.2.04.	Toll says IT systems infected by new variant of ‘Mailto’ ransomware
BleepingComputer	2020.1.15.	Ako Ransomware Uses Spam to Infect Its Victims
체크멀블로그	2020.1.24.	“다양한 유포 방식으로 감염될 수 있는 Ako 랜섬웨어 주의”

랜섬웨어 암호기능 분석 보고서 작성공헌자

구 분	소 속	직 위	설 명
책임자	KISA	팀 장	박창열
작성자	KISA	책 임	최은영
		책 임	김기문
		선 임	김대운

KISA 한국인터넷진흥원

랜섬웨어 동향분석
2020년 1분기

RANSOMWARE TRENDS & STATISTICS
FIRST QUARTER FOR 2020

2020년 5월 인쇄
2020년 5월 발행

발 행 처 | 한국인터넷진흥원
주　　소 | [나주본원] (58324) 전라남도 나주시 진흥길 9 한국인터넷진흥원
[서울청사] (05717) 서울시 송파구 중대로 135 (가락동) IT벤처타워
대표번호 | 1433-25(수신자 요금 부담)

[해킹 · 스팸개인정보침해 신고 118]

랜섬웨어 동향분석 2020년 1분기
RANSOMWARE TRENDS & STATISTICS
FIRST QUARTER FOR 2020

랜섬웨어 동향분석
2020년 1분기

RANSOMWARE TRENDS & STATISTICS
FIRST QUARTER FOR 2020

KISA 한국인터넷진흥원