보안 이슈

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

랜섬웨어 조직들은 지난 2년간 어떻게 움직였나

AhnLab 2022-10-31

랜섬웨어 공격을 당한 적이 있습니까?

이제, 이 질문에 '그렇다'라고 답하는 기업이 적지 않을 것으로 예상된다. 랜섬웨어로 인한 피해는 올해에도 계속해서 발생하고 있다. 그리고, 전 세계적으로 여러 랜섬웨어 조직들이 다양한 랜섬웨어를 사용하며 활발하게 활동하고 있는 상황이다.

우리가 한 번쯤은 들어봤을 랜섬웨어 조직들은 어떻게 움직였을까? 또 이들이 사용하는 랜섬웨어는 어떻게 변화했을까? 이번 글에서는 지난 2년간 주요 랜섬웨어 조직과 랜섬웨어 동향을 알아본다.

랜섬웨어 동향을 본격적으로 알아보기에 앞서, 본문에 등장하는 공격 조직과 랜섬웨어의 영문 및 국문 표기를 [표 1]과 같이 정리한다.

영문	국문	영문	국문
Andariel	안다리엘	Gwisin	귀신
BlackCat	블랙캣	Hive	하이브
BlackMatter	블랙매터	LockBit	록빗
BlueCrab(Sobinoki)	블루크랩(소디노키비)	Lorenz	로렌즈
Bluesky	블루스카이	Magniber	매그니베르
BitLocker	비트로커	Masscan	매스스캔
Clop	클롭	Maui	마우이
Conti	콘티	Noberus	노베루스
DarkSide	다크사이드	Revil	레빌
GandCrab	갠드크랩	Wizard Spider	위자드 스파이더
GlobeImposter	글로브임포스터	Yanluowang	얀루오왕

[표 1] 공격 조직 및 랜섬웨어 영문 & 국문 표기

이하 본문에서는 해당 내용을 국문으로 표기한다.

랜섬웨어 주요 동향

1. 랜섬웨어 조직의 특징

먼저, 많은 랜섬웨어 조직이 서비스형 랜섬웨어(Ransomware-as-a-Service: RaaS) 형태로 운영되며, 협력자를 모집해 수익을 2:8 혹은 1:9로 나누는 등 점차 기업과 같은 모습을 보이고 있다.

언론 및 대중의 관심과 법집행 기관의 수사로 일부 랜섬웨어 조직원이 검거되면서 위기를 느낀 랜섬웨어 조직은 해체하거나 리브랜딩을 진행했다. 일례로, 다크사이드 랜섬웨어 조직은 2021년 5월 미국 콜로니얼 파이프라인(Colonial Pipeline) 랜섬웨어 공격 이후 법집행 기관의 관심이 집중되자 조직을 폐쇄하고 블랙매터로 리브랜딩하여 재등장했다.

문제는, 그간 법집행 기관에 검거된 인원들은 대체로 자금 세탁이나 유포 담당자로, 랜섬웨어 조직의 핵심 개발 인력은 대부분 검거되지 않았다는 것이다. 그리고, 기존 랜섬웨어 그룹이 해체되면 구성원들이 다른 랜섬웨어 조직에 입사(?)하기도 한다.

사이버 범죄 조직 외에도 국가 지원을 받는 것으로 추정되는 위협 그룹도 랜섬웨어를 사용하고 있다. 북한의 지원을 받는 것으로 추정되는 안다리엘 그룹은 한국에서 랜섬웨어 공격을 감행한 바 있다. 미국 정부는 북한의 지원을 받는 조직이 마우이 랜섬웨어를 이용해 의료시설을 공격했다고 밝혔으며, 보안업체 카스퍼스키(Kaspersky)는 마우이 랜섬웨어와 안다리엘 그룹의 연관성에 관한 내용을 공개했다.

또, 특정 지역에서만 활동하는 랜섬웨어 조직도 있다. 한국에서는 귀신, 매그니베르, 매스스캔 등의 랜섬웨어가 활동하고 있다.

일부 공격자들은 랜섬웨어 공격 시, 정보를 유출하는 인포스틸러(InfoStealer)를 함께 감염시키기도 한다. 암호화된 데이터로 협박하는 것을 넘어, 감염자의 정보도 유출해 수익을 극대화하기 위함으로 보인다.

2. 랜섬웨어 공격 방식의 진화

랜섬웨어 공격 방식도 계속 진화하고 있다. 메일에 악의적인 링크나 파일을 첨부하는 방법 뿐만 아니라, 메일이나 웹서버 취약점을 이용해 침투하기도 한다. 공급망(Supply Chain)을 이용한 내부 침투도 있지만 일반적인 방법은 아니다. 일부 랜섬웨어는 자체 전파 기능도 가지고 있다.

특정 대상을 노린 타겟형 공격은 일반적인 해킹이나 APT(Advanced Persistent Threat) 공격과 유사하다. 최초 침입 후, 내부 시스템을 하나씩 장악하고 내부 정보를 유출하는 공격 과정은 동일하고 마지막에 랜섬웨어를 유포하는 차이만 있다. 아울러, 방어자들이 랜섬웨어에 대비하기 위해 다양한 보안 제품을 사용하는 가운데, 이를 무력화하거나 우회하기 위한 다양한 시도들을 하고 있다.

랜섬웨어 기법 자체도 진화를 거듭하는 중이며, 주요 특징 세가지는 다음과 같다.

첫째, 클라우드 환경이 확대되는 가운데 공격자도 변화하는 환경에 적응해가고 있다. 이에, 윈도우 랜섬웨어 뿐만 아니라, 클라우드 환경을 노린 리눅스 랜섬웨어를 제작하기도 한다.

둘째, 과거 랜섬웨어는 실행하면 바로 파일을 암호화하고 랜섬노트를 보여주는 형태였다. 하지만, 귀신, 하이브, 록빗 등 최근 랜섬웨어는 실행을 위해 인자값이 필요하다. 인자값을 알지 못하면, 악의적인 기능을 수행하지 않는다. 이로 인해, 행위 기반 보안 제품의 탐지를 통과하고 분석가도 랜섬웨어 유무를 판단하기 어렵게 된다.

셋째, 윈도우 랜섬웨어의 경우 파일 암호화에 방해가 될 수 있는 정상 서비스를 종료하고, vssadmin.exe 등으로 볼륨 쉐도우(Volume Shadow) 복사본을 삭제하거나 백업 시스템을 파악한다. 이 때문에, 백업된 데이터도 복구가 어려워진다.

3. 랜섬웨어 주요 공격 대상 및 사례

최근 1년 간 공개된 분석 보고서와 안랩의 정보 등을 종합한 결과를 토대로 정리한 2021 ~ 2022년 랜섬웨어 공격 사례는 [표 2]와 같다.

연월	국가	산업	내용
2021년 4월	영국	철도	영국 철도 네트워크 머지레일(Merseyrail), 록빗 랜섬웨어 감염
2021년 8월	미국	의료	미국 오하이오 메모리얼 헬스 시스템(Memorial Health System), 하이브 랜섬웨어 감염
2021년 8월	태국	항공	록빗 랜섬웨어 감염, 방콕 에어 고객 정보 유출
2021년 11월	대한민국	식품	하이브 랜섬웨어 감염
2022년 1월	프랑스	법무부	록빗 랜섬웨어 감염
2022년 1월	-	제조	전력 부품 공급 업체 콘티 랜섬웨어 감염
2022년 2월	대한민국	중공업	하이브 랜섬웨어 감염
2022년 4월	대한민국	의료	귀신 랜섬웨어의 리눅스 버전 발견
2022년 5월	대한민국	의료	귀신 랜섬웨어 감염
2022년 5월	코스타리카	정부	코스타리카 정부 콘티 랜섬웨어 감염으로 비상사태 선언.
2022년 7월	대한민국	IT	매스스캔 랜섬웨어 감염
2022년 7월	대한민국	에너지	매스스캔 랜섬웨어 감염
2022년 7월	대한민국	의료	귀신 랜섬웨어 감염
2022년 7월	대한민국	IT	록빗 3.0 감염
2022년 7월	대한민국	제조	블루크랩 랜섬웨어 감염
2022년 7월	대한민국	섬유제품 제조	비트로커를 이용한 파일 암호화
2022년 7월	대한민국	중공업	하이브 랜섬웨어 감염
2022년 7월	대한민국	의료	매스스캔 랜섬웨어 감염
2022년 8월	대한민국	기업	비트로커를 이용한 파일 암호화

[표 2] 2021 ~ 2022년 주요 랜섬웨어 공격 사례

한국에서는 하이브, 록빗, 매그니베르 등의 랜섬웨어 왕성하게 활동하고 있으며, 귀신, 매스스캔과 같이 한국 조직만 노린 랜섬웨어 활동도 계속 보고되고 있다.

4. 공격 방법(Attack Vectors)

랜섬웨어 조직이 사용하는 공격을 전개하는 방법은 일반적인 공격자의 방법과 큰 차이가 없다.

개인 대상 공격은 메일과 웹사이트를 해킹해 방문하는 사용자 시스템을 감염시키는 방법을 주로 사용한다.

기업 대상 공격은 다양한 방법이 사용된다. 클롭 랜섬웨어 수사 내용에 따르면, 공격자는 목표 기업의 직원 700명에게 악성코드가 포함된 메일을 보냈다. 3명이 첨부파일을 열어보고 악성코드에 감염되었으며, 52 시간 이내에 조직에 랜섬웨어가 유포되었다.

아울러, 기업에서 사용하는 데이터베이스, 메일, 웹서버 취약점을 이용해 침입한 뒤, 내부 시스템을 추가 장악하고 파일 배포 기능이 있는 자산 관리 프로그램 등을 이용해 랜섬웨어를 유포하기도 한다.

피해 사례들은 보면, 기업들은 액티브 디렉토리(Active Directory: AD)를 운영하는 경우가 많은데, 피해 시스템들은 로컬 어드민(Administrator) 계정이 활성화되어 있었고, RDP(Remote Desktop Protocol) 접속이 가능했다. AD 서버의 도메인 컨트롤러에서 그룹 정책을 생성해 현재 도메인과 연결된 다른 컴퓨터에 랜섬웨어 파일을 유포했다.

또, 관리 편의성을 위해 조직 내에서 운영하는 서버나 직원에게 지급된 기기들이 동일한 암호를 사용하는 경우가 많아 내부 시스템이 생각보다 쉽게 내부 시스템이 침해 당하는 것을 알 수 있었다.

주요 랜섬웨어와 조직들의 활동

2022년 주요 랜섬웨어 조직의 활동 현황은 [표 3]과 같다. 이어서, 최근 활동이 활발한 6개 랜섬웨어 조직에 관한 내용을 소개한다.

조직 이름	랜섬웨어	활동 상태	설명
블랙캣(ALPHV)	블랙캣	높음	다크사이드와 블랙매터 후계로 추정
레빌	블루크랩(소디노키비)	보통	갠드크랩의 후계
블루스카이	블루스카이	보통	-
클롭	클롭	보통	-
위자드 스파이더	콘티	해체	내부 정보 유출 후 활동 중단 상태
글로브임포스터	글로브임포스터	보통	-
귀신	귀신	보통	한국에서만 활동
하이브	하이브	높음	-
록빗	록빗	높음	-
매그니베르	매그니베르	높음	한국에서만 활동이 높음
매스스캔	매스스캔	높음	한국에서만 활동
안루오왕	안루오왕	보통	-

[표 3] 주요 랜섬웨어 조직 활동 동향

1. 비트로커를 이용한 공격

공격자들은 랜섬웨어는 아니지만 윈도우에 포함된 비트로커를 공격에 활용하는 경우도 있다. 비트로커는 ▲Windows Server 2008 ▲Windows 7 ▲Vista 8, 8.1, 10, 11에 내장된 디스크 암호화 기능이다. GUI(Graphic User Interface)와 CLI(Command-Line Interface) 방식을 지원하며 CLI 방식에서는 원격 암호화를 지원하기 때문에 악용될 수 있다.

원격으로 비트로커를 실행하기 위해서는 대상 시스템의 비트로커 서비스 시작 유형이 '수동'(윈도우 기본 설정)이어야 한다. 그리고, '자동' 서비스 준비 상태에서도 해당 시스템의 관리자 권한이 있으면 실행 가능하다.

비트로커를 활용해 원격으로 대상 시스템 드라이브를 암호화할 때, 명령 받은 대상 시스템에서는 해당 드라이브의 암호화 진행 창이 표시되면서 암호화가 진행된다. 따라서, 암호화 진행 여부를 인지할 수 있지만, "-lock" 인자 값을 사용해 암호화가 완료되기 이전에 드라이브에 대한 접근을 차단할 수 있다.

주요 공격 동향을 보면, 2022년 8월 FRP(Fast Reverse Proxy)를 이용해 국내 20 여개 기업을 공격한 공격자가 활동을 계속해오고 있다. 공격 사례를 보면, 먼저, 취약한 서버에 침투하여 웹쉘(WebShell)을 설치하고 리버스쉘(ReverseShell) 설정 및 RDP 연결을 진행했으며, 마지막에 비트로커를 활성화하여 C드라이브를 제외한 모든 드라이브를 암호화했다.

로렌즈 랜섬웨어 조직은 마이텔(Mitel)의 마이보이스(MiVoice) VoIP 어플라이언스 취약점(CVE-2022-29499)을 이용해 침입 후 로렌즈 랜섬웨어와 비트로커를 사용해 공격한 것으로 알려졌다.

비트로커 원격 실행을 예방하기 위해서는 비트로커 기능을 사용하지 않을 때, 반드시 서비스를 중지하고 서비스 시작 유형을 '사용 안 함'으로 설정해야 한다.

2. 블랙캣(ALPHV)

블랙캣 랜섬웨어는 ALPHV, 노베루스 등으로도 불리며 러스트(Rust) 언어로 개발되었다. 2021년 12월, 다크웹(Dark Web) 포럼에서 공개되었지만 실제 활동은 2021년 11월 말부터 시작되었다. 피해 기업 국가를 보면 미국이 가장 많고 캐나다, 오스트레일리아, 영국 순이다.

블랙캣 랜섬웨어는 RaaS 비즈니스 모델로 운영된다. 제작자는 공격자(계열사)를 구인하고 수익은 개발자가 10~20%, 공격자가 나머지 수익을 가져가는 것으로 알려졌다. 윈도우와 리눅스 버전이 있고, 러스트 언어로 컴파일된 특징에 따라 [그림 1]과 같은 문자열을 확인할 수 있다.

[그림 1] 블랙캣 랜섬웨어의 특징적 문자열

3. 귀신

귀신은 2021년 9월부터 한국 기업만 공격하고 있는 랜섬웨어 조직이다. 이름에서 알 수 있듯 한국에 대해 잘 알고 있으며, 유출 사이트에도 한국어로 '귀신'을 포함하기도 한다.

귀신 랜섬웨어는 표적형 공격으로, 세간에 잘 알려지지 않았고 2022년 7월부터 언론 기사를 통해 일부 알려지기 시작했다. 보도에 따르면, 귀신은 2022년 5개 이상의 한국 기업을 공격했지만 자세한 침투 방법은 알려지지 않았다. 안랩은 2022년 8월 고객 피해를 처음 접수 받아 자사 ASEC 블로그에 관련 내용을 공개했다. 8월말에는 한국인터넷진흥원(KISA)에서 귀신 랜섬웨어 분석 리포트를 발간한 바 있다.

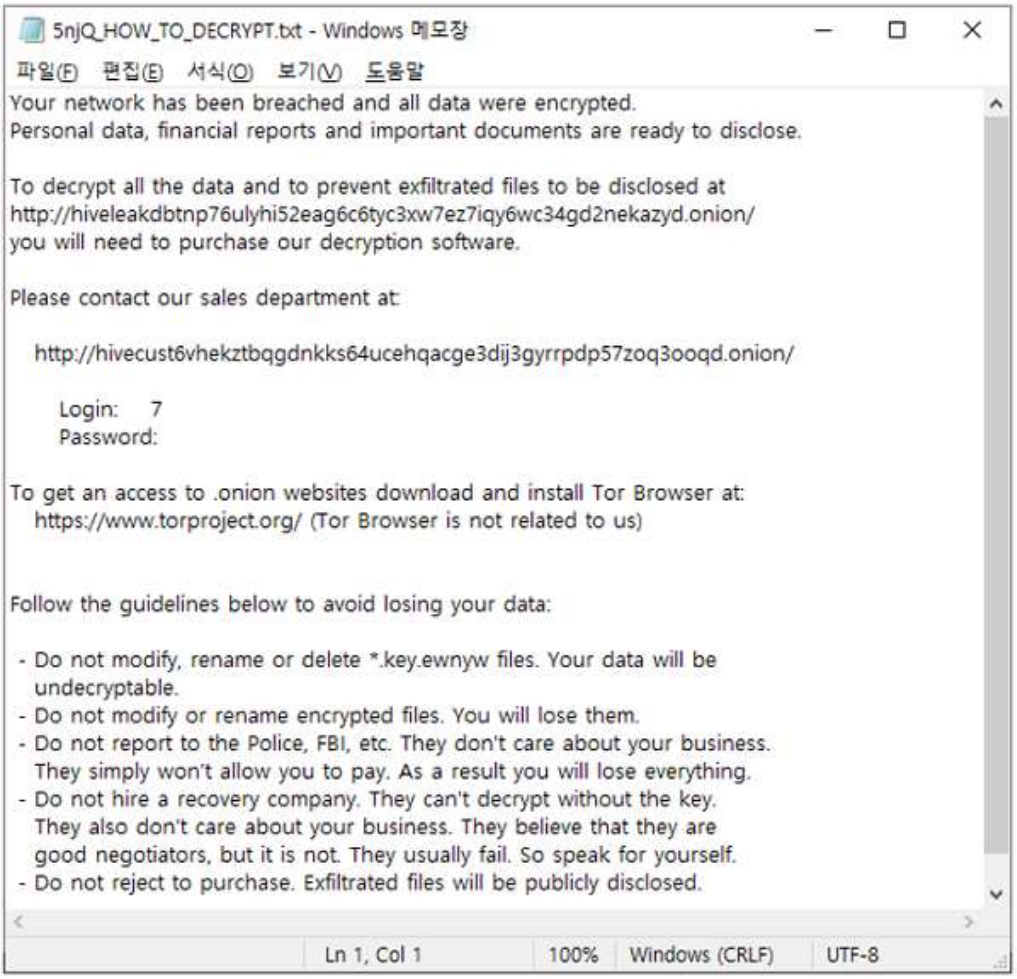
공격 과정을 보면, 먼저 내부 시스템을 장악한 뒤 파일 배포 프로그램을 이용해 악성 MSI 파일을 배포한다. MSI 파일 내에 Binary.helper 파일이 존재하고, 실행을 위해 인자(SERIAL, LICENSE, SMM, ORG)가 필요하다.

랜섬노트는 '!!!_HOW_TO_UNLOCK_(업체이름)_FILES_!!!.txt'이며 영문으로 피해 업체 이름, 유출 정보 등을 포함하며, 복호화키, 정보 공개, 취약점 등을 활용해 3단계에 걸쳐 협상을 하는 것이 특징이다.

4. 하이브

하이브 랜섬웨어는 2021년 6월 처음 보고된 후, 현재까지 왕성하게 활동 중이다. 정보 유출과 랜섬웨어 감염 등 공격을 이중으로 진행하고, 랜섬웨어 복호화 금액 협상이 이뤄지지 않으면 하이브 리크스(Hive Leaks) 사이트에 탈취한 정보를 공개한다. 2021년 8월, 미국연방수사국(FBI)은 하이브 랜섬웨어 활동에 대해 경고한바 있다.

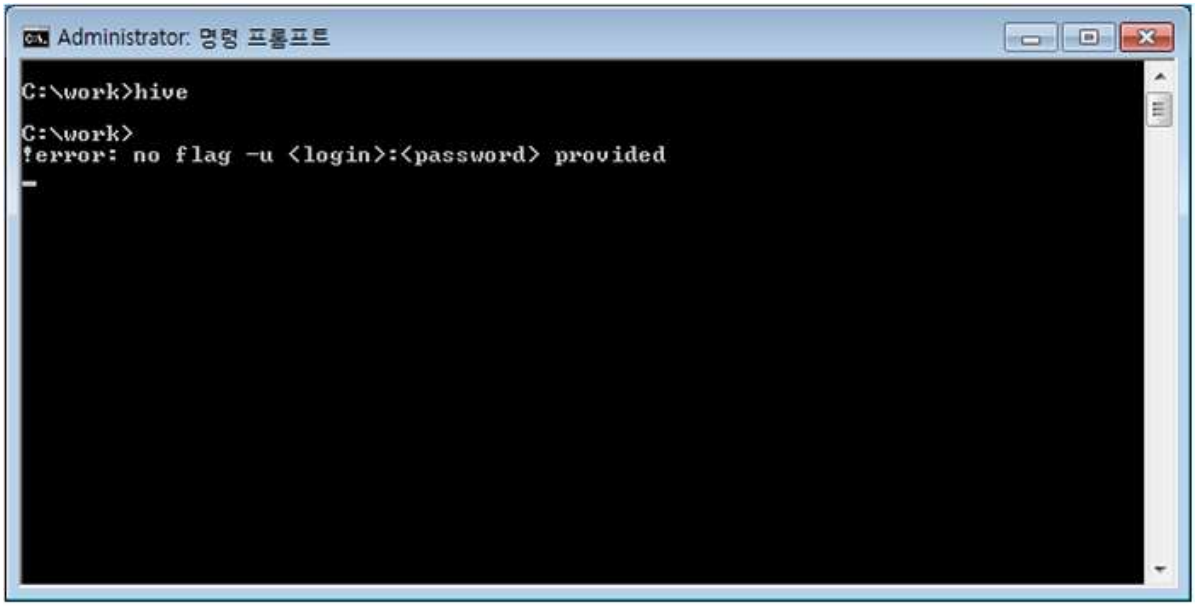
특징을 살펴보면 2021년 10월, 리눅스와 FreeBSD 시스템 버전이 발견되었으며, 초기에는 고(GO) 언어로 작성되었다가 2022년 7월 이후 러스트 언어로 변경했다. 랜섬웨어를 감염시킨 뒤 피해자에게 접속할 수 있는 주소와 로그인 정보를 담은 랜섬노트를 남긴다.



[그림 2] 하이브 랜섬웨어 랜섬노트

하이브 랜섬웨어는 피싱 메일이나 프록시쉘(ProxyShell) 등 익스체인지 서버(Exchange Server) 취약점(CVE-2021-34473, CVE-2021-34523, CVE-2021-31207)을 이용해 침투한다. RDP를 활용해 내부에 침입하며, 내부 시스템 장악 후 코발트 스트라이크 비컨(Cobalt Strike Beacon)을 통해 시스템을 제어하고, 랜섬웨어를 유포한다.

최근의 변형은 실행을 위한 인자값이 필요해 샘플만으로 분석이 어렵다.



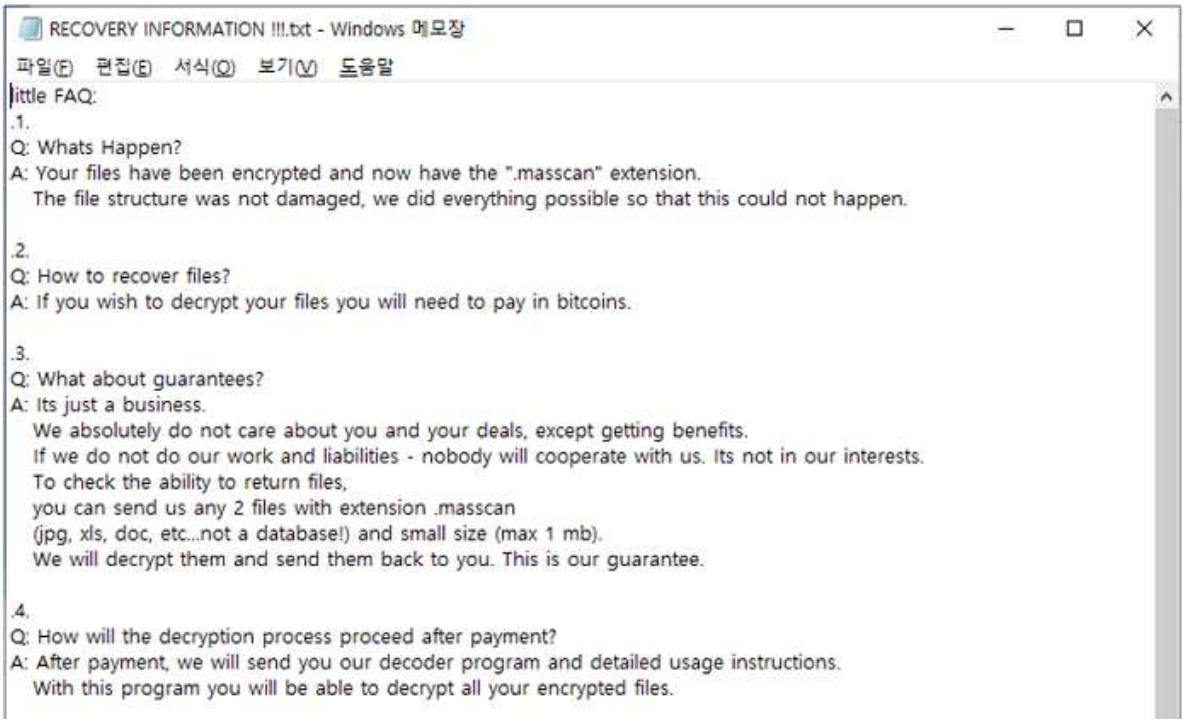
[그림 3] 인자값이 없는 하이브 랜섬웨어 실행 화면

5. 매스스캔

매스스캔은 2022년 6월부터 한국에서 활동하고 있는 랜섬웨어 조직으로 한국 외 타국에서의 활동은 확인되지 않았다.

KISA에 따르면 취약한 데이터베이스 서버를 공격해 침입한다고 한다. 파일을 암호화할 때 'masscan_알파벳_랜덤8자리 확장자'를 추가해 매스스캔 랜섬웨어로 불리며 발견된 변형에서는 알파벳 F, G, R를 추가한다.

매스스캔은 [그림 4]와 같이 랜섬노트로 RECOVERY INFORMATION !!!.txt 파일을 생성한다.



[그림 4] 매스스캔 랜섬노트

파일을 실행하려면, 설정 파일(setting.asd)이 필요하지만 현재까지 설정 파일이 확인되지 않아 완전한 재현은 하지 못하고 있다.

6. 록빗

2019년 처음 등장한 것으로 알려진 록빗 랜섬웨어는 2021년 6월, 버전 2.0으로 업데이트 되어 유포되었다. 2.0버전에는 AD 그룹 정책을 남용하여 윈도우 도메인 전체를 암호화하는 기능이 추가되었다.

원래는 파일을 암호화하고 확장자를 ".abcd"로 바꿨는데, 이로 인해 'ABCD 랜섬웨어'로 알려지기도 했었다. 록빗 랜섬웨어는 2019년부터 미국, 중국, 인도, 인도네시아, 우크라이나 및 여러 유럽 국가에 기반을 둔 조직을 대상으로 공격을 감행해왔다. 록빗 랜섬웨어 역시 RaaS 형태로 운영되고 있으며, 한국에서는 이력서 등으로 가장한 메일 유포와 기업을 표적으로한 공격을 병행하고 있다.

2022년 7월, 록빗 3.0을 출시했으며, 현재도 활발하게 활동하고 있다. 록빗 조직은 록빗 3.0을 출시하며 랜섬웨어 버그를 찾아주면 포상금을 주는 버그바운티도 진행해 눈길을 끌었다.

특징은 파일을 암호화할 때 다중 스레드를 사용하며, 파일당 4KB의 데이터만 암호화한다. 또, 하이브 랜섬웨어와 유사하게 실행 시 인자값이 필요하다.

보안 제품 무력화와 우회 시도

기본적으로, 기업의 컴퓨터와 서버에 설치된 보안 제품과 보안 체계는 공격을 막는 역할을 한다. 랜섬웨어 피해로 인한 피해가 커지면서, 최근의 보안 제품들은 파일 암호로 추정되는 행위 차단, 암호화 시 원본 파일 복구 등의 기능을 토대로 랜섬웨어 보안을 구현하고 있다. 공격자 입장에서 보면, 보안 제품의 '안티 랜섬웨어' 기능은 공격을 성공시키기 위해 넘어야 할 도전과제가 되었다. 이에, 보안 제품을 무력화하거나 우회하기 위한 여러가지 방법들을 시도하고 있다.

1. 보안 제품 무력화

공격자가 보안 제품을 무력화 시킬 수 있다면, 백신에서 진단되는 랜섬웨어를 통해서도 공격을 수행할 수 있다. 이를 위해, 공격자는 시스템 권한을 얻고 난 뒤, 보안 제품의 실시간 및 행위 감시 기능을 끄거나 프로그램 자체를 제거한다. 윈도우 디펜더(Windows

Defender)와 유명 보안 제품을 무력화 하는데, 정상 드라이버 이용하기도 한다.

이와 같은 공격을 예방하려면, 조직 차원에서 백신을 올바르게 설정하고 가급적 개별 사용자가 설정을 변경하지 못하게 해야 한다.

2. 보안 제품 우회

공격자가 보안 제품을 무력화시키지 못하는 경우에는 이를 우회하기 위한 방법들을 시도한다.

일반적으로, 공격자는 랜섬웨어 제작자로부터 랜섬웨어를 제공 받거나 생성기를 활용해 랜섬웨어를 만드는데, 보안 제품에서 진단되는 랜섬웨어로 공격하는 경우도 발생한다. 공격자가 랜섬웨어를 실행했지만 보안 제품이 두 번 차단하자, 랜섬웨어 파일을 암호화하고 로더(Loader)를 만들어 랜섬웨어를 메모리에서 실행하는 방식을 사용한 경우도 있다.

또, 보안 제품에는 미끼 파일을 만들고 미끼 파일이 변조될 때 랜섬웨어로 탐지하는 기능이 있는데, 일부 랜섬웨어는 보안 제품이 설치되어 있는 경로나 보안 제품에서 생성한 미끼 파일은 암호화에서 제외시키는 방식으로 우회한다.

블루크랩, 블랙 바스타(Black Basta) 등의 랜섬웨어는 윈도우를 안전 모드(Safe Mode)로 부팅해 암호화를 진행한다. 보안 제품이 행위를 감시하는 상황에서 암호화하면, 탐지 & 차단될 수 있으므로 안전 모드로 강제 부팅시키는 것이다. 이 경우, 보안 제품이 실행되지 않은 상태에서 랜섬웨어가 방해를 받지 않고 파일을 암호화할 수 있다.

랜섬웨어 공격은 보안 제품을 우회해 한 번에 성공하는 경우도 있지만, 한두 번 차단되었다가 보안 제품을 우회해 들어오는 경우도 있다. 따라서, 보안 담당자는 보안 제품에서 랜섬웨어 진단 로그가 발생하면, 해당 시스템과 감염 경로를 조사해야 한다.

결론

랜섬웨어 조직은 서비스 형태로 진화하면서 점차 기업화 & 분업화되고 있다. 다크웹에서는 이미 악성코드 제작자, 개인정보 유통, 초기 침입 브로커(Initial Access Brokers: IAB), 랜섬웨어 배포, 돈 세탁 등에 분업화가 체계적으로 되어 있다.

다만, 특정 목표를 노리는 타겟형 랜섬웨어 조직의 공격 방식은 일반적인 해킹 조직과 큰 차이가 없다. 공격자가 다양한 방법으로 침투해 내부 시스템을 장악하고 정보를 유출하는 과정까지는 동일하다. 이후 정보만 유출하고 사라지느냐, 랜섬웨어로 추가 공격을 진행하느냐에 대한 차이가 있을 뿐이다. 따라서 랜섬웨어 공격 예방을 위한 노력은 다른 공격을 예방하는 효과도 볼 수 있다.

예방을 위한 노력을 기울이더라도, 랜섬웨어로 인한 피해는 발생할 수 있다. 대다수는 랜섬웨어에 감염되면 비용을 지불하고 시스템을 복구하는데, 공격자의 침입 방법을 조사해 개선하지 않으면 또 다시 다른 랜섬웨어 조직에게 해킹 당할 수 있다.

따라서, 랜섬웨어 피해가 발생하면 보안 업체에 의뢰하여 감염 경로 등을 조사하고, 보안 체계 관점에서 부족한 부분을 개선해 나가야 한다. 또한, 직원의 개인정보나 로그인 정보가 다크웹에 유출되었는지 주기적인 확인이 필요하다. 참고로, 기업을 공격할 때 전직원에게 메일을 보내는 방법도 사용되곤 하는데, 이는 메일 주소가 사전에 유출되었을 가능성이 높다.

안랩은 위협 그룹들의 활동을 추적하며 관련 악성코드를 대응해오고 있다. 이들의 활동이 최근에 파악된 경우라고, 안랩 제품군에서 과거 관련 악성코드를 진단했을 수 있다. 다만, 아직 확인되지 않아 진단되지 않는 변형이 존재할 수 있다.

랜섬웨어 조직 및 랜섬웨어에 관한 보다 상세한 분석 내용과 침해지표(IoC)가 담긴 보고서 전문은 AhnLab TIP 구독 서비스를 통해 확인할 수 있다.

▶ATIP 포털 바로가기

AhnLab TI개발팀 차민석 수석연구원, 최일봉 연구원