보안 이슈

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

록빗 랜섬웨어, 기업을 노리는 또 다른 위협

AhnLab 2021-10-01

전 세계 기업들을 괴롭히고 있는 랜섬웨어는 공격 빈도 수 뿐만 아니라 그 종류도 점점 다양해지고 있다. 이 중, 비교적 최신으로 분류되는 록빗 랜섬웨어는 등장한지 2년여만에 한국을 포함한 전 세계 주요 기업들을 공격하면서 주요한 위협으로 떠오르고 있다.

이번 글에서는 록빗 랜섬웨어의 특징과 피해 사례를 살펴보고 구체적인 공격 방식을 분석해본다.

2019년 9월 처음 등장한 것으로 알려진 록빗 랜섬웨어(LockBit Ransomware)는 서비스형 랜섬웨어(Ransomware as a Service: RaaS)로 운영되고 있으며 미국, 중국, 인도, 인도네시아, 우크라이나 및 여러 유럽 국가에 기반을 둔 조직을 대상으로 공격을 감행했다.

초창기 록빗 랜섬웨어는 원래 파일을 암호화하고 확장자를 '.abcd'로 바꿨으며 이로 인해 ABCD 랜섬웨어로 알려졌었다. 이후에 확장자를 '.lockbit'로 변경하였고 2021년 6월에 2.0으로 업데이트되어 현재까지 유포 중에 있다. 2.0 버전에서는 AD 그룹 정책을 남용하여 Windows 도메인 전체를 암호화하는 기능이 추가되었다. 보안업체 트렌드마이크로(Trend Micro)는 2021년 7월 1일부터 8월 15일까지 칠레, 이탈리아, 대만, 영국에서 공격 시도를 탐지했다고 밝혔다. 또한, 2021년 7월 13일부터 BlueCrab(Sodinokibi, REvil) Ransomware의 유포가 중지된 이후 록빗 랜섬웨어의 유포량이 더욱 증가했다.

2021년 8월에는 한국 기업의 미국 법인 2곳도 공격을 받은 것으로 언론에 보도된 바 있어 주의가 요구되는 상황이다.

록빗 랜섬웨어의 특징

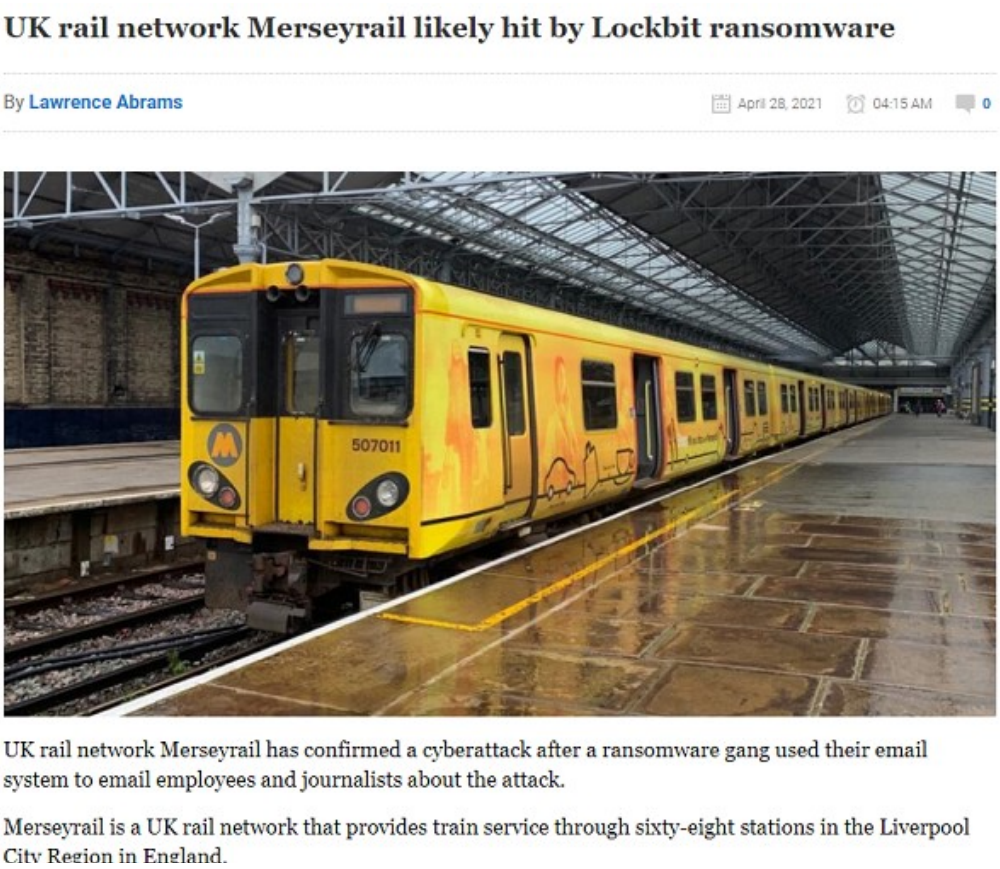
보안업체 사이버인트(Cyberint)에 따르면 록빗 랜섬웨어는 스피어 피싱 이메일을 통해 자격 증명을 수집하여 이를 활용하거나, 무차별 대입 공격을 통해 노출된 Windows 원격 데스크톱 연결 시도를 통해 침입한다. 또한, 시스템의 알려진 취약점을 악용하기도 하며, 호주 사이버 보안 센터ACSC)에 따르면 최근 Fortinet Fortios 및 FortiProxy 제품의 취약점(CVE-2018-13379)을 악용하는 것으로 알려졌다.

록빗 랜섬웨어는 네트워크 스캐너를 사용하여 네트워크 구조를 식별하고 대상 도메인 컨트롤러를 찾는다. 이후, 프로세스 해커(Process Hacker), PC 헌터(PC Hunter)와 같은 정상 도구를 사용하여 시스템의 프로세스 및 서비스를 종료한다. 도메인 컨트롤러에 접속하면 새로운 그룹 정책을 만들어 네트워크의 모든 장치에 윈도우 디펜더(Windows Defender)를 비활성화하고 록빗 바이너리를 배포 및 실행한다. 그리고 록빗 랜섬웨어 운영자는 2021년 8월 2일 기준 잘 알려진 랜섬웨어 중에서 가장 빠른 암호화 속도를 가지고 있다고 자랑하고 있다.

알려진 주요 피해 사례

1. 영국 철도 네트워크 '머지레일' 공격

미국 IT 보안 매체 '블리핑컴퓨터(BleppingComputer)'에 따르면, 2021년 4월 영국 철도 네트워크 '머지레일(Merseyrail)'이 록빗 랜섬웨어의 공격을 받았다. 록빗 랜섬웨어 운영자가 해당 네트워크 관리자 이메일을 통해 블리핑컴퓨터, 다양한 영국 신문 및 머지레일 직원에게 'LockBit Ransomware Attack and Data Thef'라는 제목의 메일을 발송했으며 이를 통해 공격당한 사실을 알게 되었다.



UK rail network Merseyrail likely hit by Lockbit ransomware

By Lawrence Abrams

April 28, 2021 04:15 AM 0

UK rail network Merseyrail has confirmed a cyberattack after a ransomware gang used their email system to email employees and journalists about the attack.

Merseyrail is a UK rail network that provides train service through sixty-eight stations in the Liverpool City Region in England.

[그림 1] 영국 철도 네트워크 머지레일 공격 관련 기사

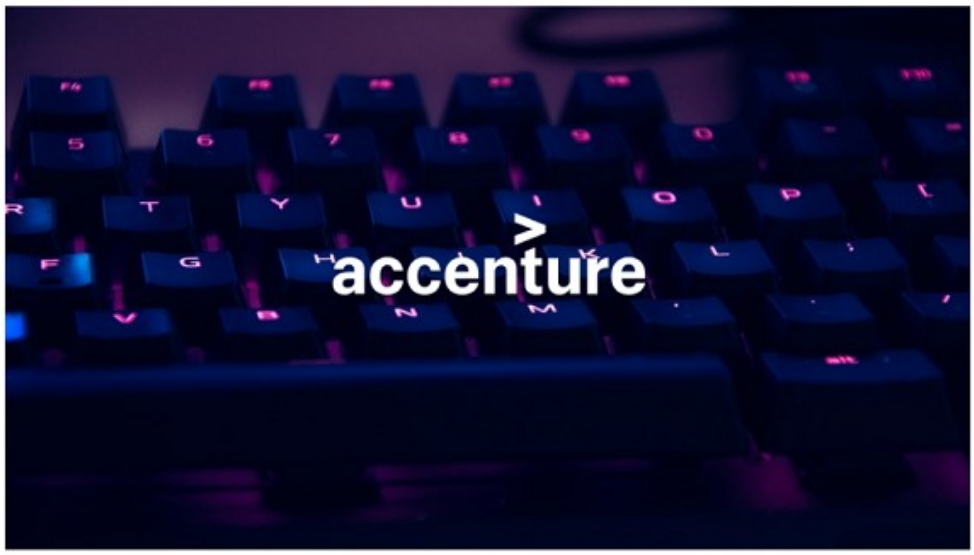
2. 글로벌 IT 컨설팅 기업 '엑센추어' 공격

2021년 8월에는 자동차, 은행, 정부, 기술, 에너지, 통신 등 다양한 산업 분야에 서비스를 제공하는 글로벌 IT 컨설팅 기업 '엑센추어(Accenture)'가 록빗 랜섬웨어 공격을 당했다. 엑센추어는 블리핑컴퓨터를 통해 영향을 받은 시스템은 백업을 통해 모두 복구했으며, 비즈니스 운영에 영향이 없다고 밝혔다.

다만, 보안업체 '사이블(Cyble)' 연구팀에 따르면 록빗 랜섬웨어 운영자는 엑센추어로부터 6TB의 데이터를 훔쳤다고 주장하며 5천만 달러의 비용을 요구했다. 이들은 엑센추어 내부자를 통해 기업 네트워크에 침입했다고 주장하기도 했다. 또 다른 보안업체 '허드슨 락(Hudson Rock)'은 엑센추어 직원과 파트너가 보유한 컴퓨터 2,500대가 감염되었다고 밝혔다.

Accenture confirms hack after LockBit ransomware data leak threats

By Ax Sharma August 11, 2021 12:22 PM 1



Accenture, a global IT consultancy giant has allegedly been hit by a ransomware cyberattack from the LockBit ransomware gang.

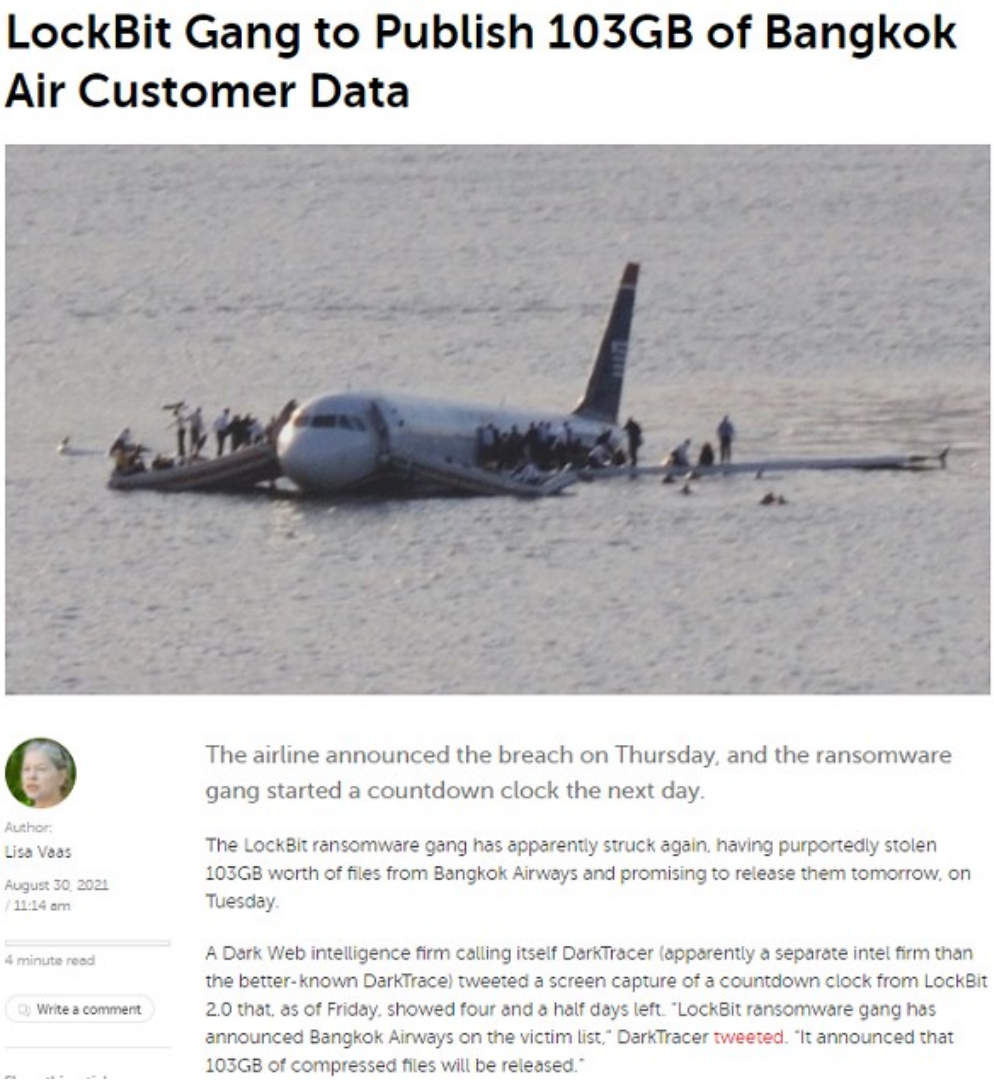
Accenture is an IT giant known to serve a wide range of industries including automobiles, banks, government, technology, energy, telecoms, and many more.

[그림 2] 엑센추어 공격 관련 기사

3. 방콕 에어웨이 공격

보안업체 '다크 트레이서(Dark Tracer)'는 2021년 8월 25일, 태국 항공사 '방콕 에어웨이(Bangkok Airways)'가 록빗 랜섬웨어 공격을 당했다는 트윗을 게시했다. 보안 전문매체 '쓰렛 포스트(Threat Post)'의 보도에 따르면, 공격자들은 기존 103GB 가량의 데이터를 갖고 있으며, 비용을 지불하지 않을 시 이를 8월 31일에 공개할 것이라 밝혔다. 하지만, 약속했던 시간보다 3일 빠른 8월 28일, 돌연 입장을 바꿔 데이터를 공개했다는 공지를 올리고 자신들이 200GB 이상의 데이터를 보유하고 있다고 주장했다.

방콕 에어웨이 측은 8월 23일에 록빗 렌섬웨어 공격을 받았으며, 이로 인해 승객 이름, 성, 국적, 성별, 전화번호, 이메일 주소, 기타 연락처, 여권 정보, 과거 여행 기록, 신용카드 정보 일부, 특별 기내식 정보가 노출 되었을 수 있음을 확인했다고 8월 26일 발표한 바 있다.


LockBit Gang to Publish 103GB of Bangkok Air Customer Data

The airline announced the breach on Thursday, and the ransomware gang started a countdown clock the next day.

Author:
Lisa Vaas

August 30, 2021
/ 11:14 am

4 minute read

Write a comment

The LockBit ransomware gang has apparently struck again, having purportedly stolen 103GB worth of files from Bangkok Airways and promising to release them tomorrow, on Tuesday.

A Dark Web intelligence firm calling itself DarkTracer (apparently a separate intel firm than the better-known DarkTrace) tweeted a screen capture of a countdown clock from LockBit 2.0 that, as of Friday, showed four and a half days left. "LockBit ransomware gang has announced Bangkok Airways on the victim list," DarkTracer tweeted. "It announced that 103GB of compressed files will be released."

[그림 3] 방콕 에어웨이 공격 관련 기사

4. 한국 기업 공격

2021년 8월 23일 보안뉴스는 산업용 고무 제품 및 오일씰 제조업체와 식품 제조업체의 미국법인이 록빗 랜섬웨어 공격을 받았다고 밝혔다. 정확한 공격 날짜와 피해 규모 등 세부 정보는 알려지지 않았으나, 해당 사례는 국내 기업 역시 록빗 랜섬웨어로부터 안전하지 않다는 사실을 시사했다.

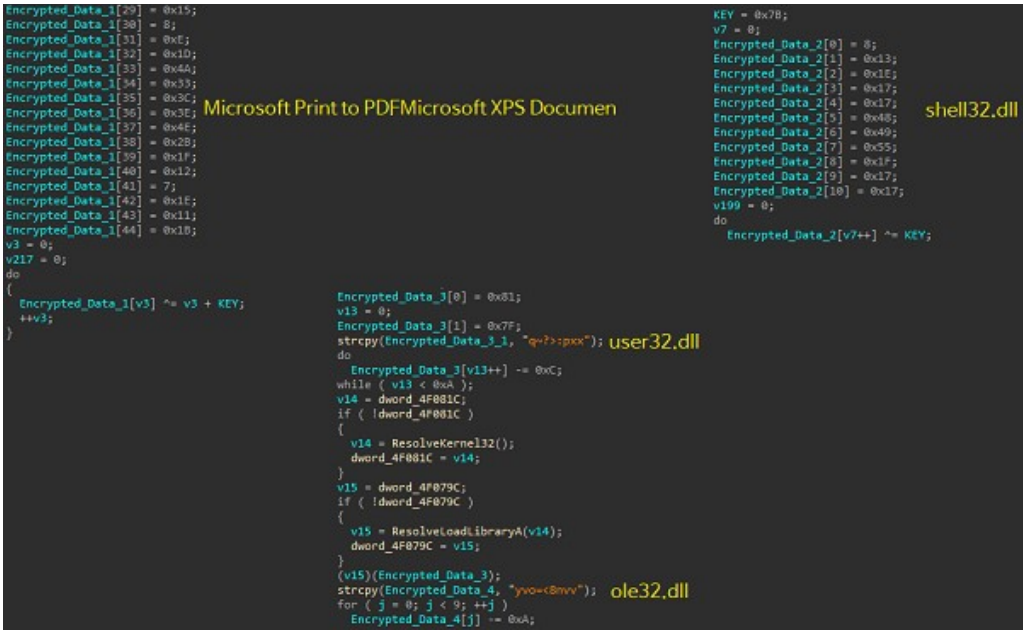
록빗 랜섬웨어 공격 분석

먼저, 안랩이 분석을 진행한 록빗 랜섬웨어 분석 대상의 기본 정보는 다음과 같다.

항목	내용
길이	959KB (985,528 bytes)
생성 시간	2021년 7월 26일 7시 34분 1초 (UTC 기준)
MD5	6fc418ce9b5306b4fd97f815cc9830e5
SHA1	95838a8beb04cfe6f1ded5ecbd00bf6cf97cd564
SHA256	0545f842ca2eb77bcac0fd17d6d0a8c607d7dbc8669709f3096e5c1828e1c049
주요 기능 및 특징	파일 암호화 (LockBit Ransomware 2.0)
안랩 진단명	Trojan/Win.Generic.C4565305 **(2021.07.25.00)**

[표 1] 파일 정보

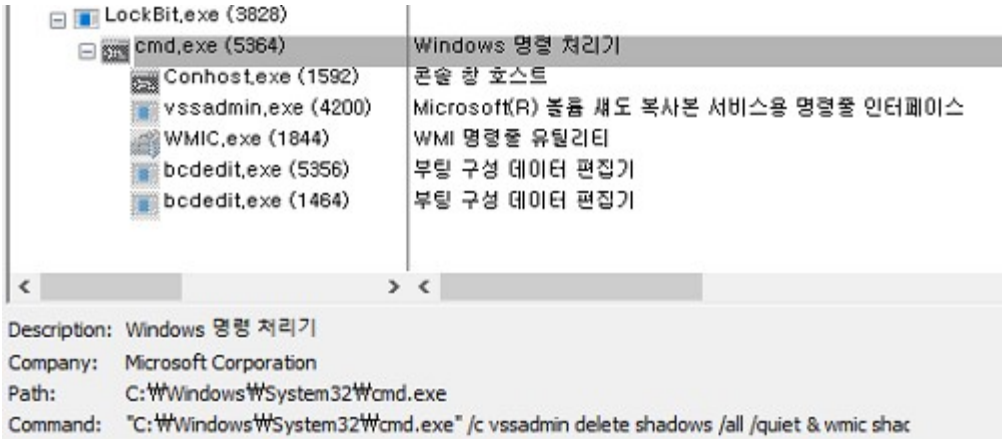
분석 결과를 보면, 많은 문자열들이 각각 다른 방식으로 서로 다른 키(KEY)를 사용하여 암호화 되어 있다.



[그림 4] 암호화된 문자열

록빗 랜섬웨어는 LDAP(Lightweight Directory Access Protocol)를 사용하여 AD(Active Directory) 도메인의 연결된 시스템을 쿼리 할 수 있다. 쿼리 문자열에서 CN은 일반 이름, DC는 도메인 구성 요소를 나타내며, 이 정보를 연결된 다른 네트워크 및 시스템을 검색하는데 사용한다. 이후 윈도우 디펜더의 실시간 보호, 경고 샘플 제출, 악성 파일 탐지에 대해 기본 동작을 비활성화하는 새로운 그룹 정책 업데이트가 생성된다. 마지막으로 도메인 내 모든 시스템에 방금 생성한 그룹 정책을 업데이트하는 파워쉘(PowerShell Script)를 실행한다.

또, 볼륨 섀도 복사본 삭제, 시스템 복구 모드 OFF, 윈도우 오류 복구 알림창 표시 OFF를 통해 시스템 복원을 하지 못하도록 한다.

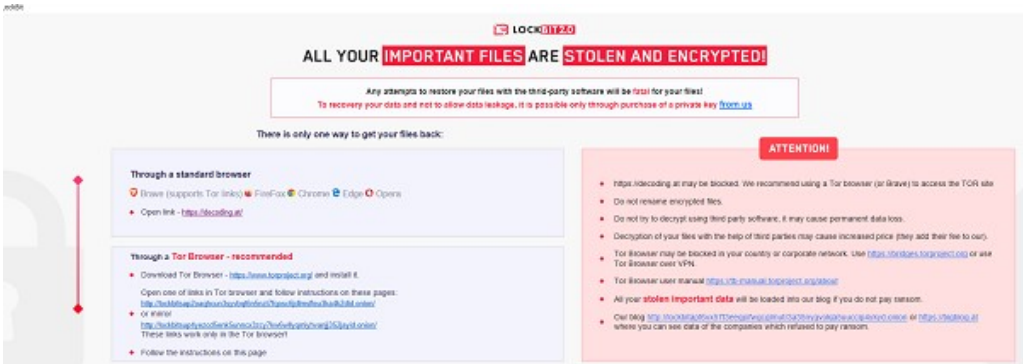


[그림 5] 시스템 복원 무력화

록빗 랜섬웨어는 파일 암호화 이전/이후에도 실행 중인 서비스와 분석, 백신, 원격 서비스 및 관련 프로세스를 모두 종료한다. 아울러, 특정 폴더, 확장자, 파일을 제외한 모든 파일을 암호화하고 랜섬노트를 생성한다. 암호화된 파일들은 록빗 랜섬웨어 전용 아이콘으로 변하게 되며 파일 이름 맨 끝에 '.lockbit' 확장자가 추가된다.

[그림 6] (좌) 암호화 전 (우) 암호화 후

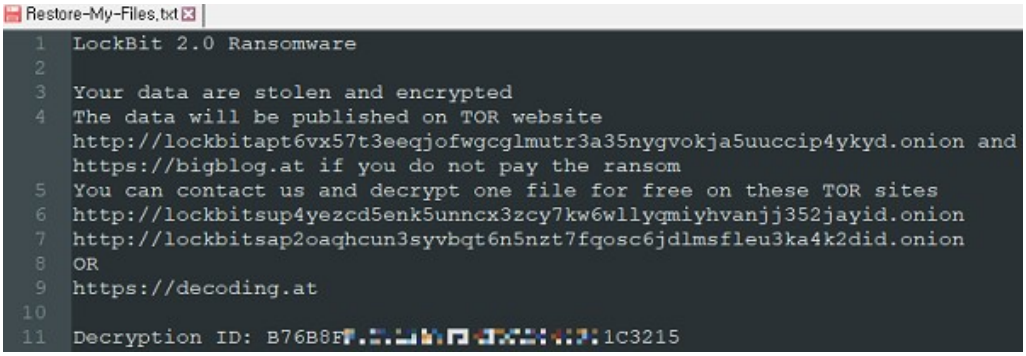
파일을 모두 암호화하고 나면 바탕화면 변경과 HTA를 통해 창을 띄움으로써 감염됐다는 사실을 통보한다.



[그림 7] 감염 사실 통보

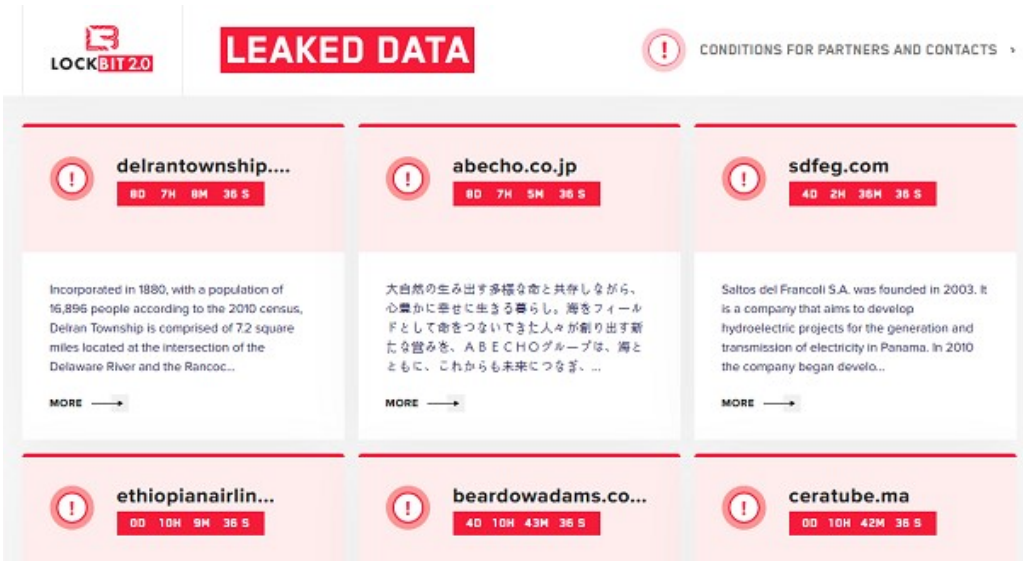
[그림 8] 변경된 바탕화면

랜섬노트를 통해 TOR 웹 복호화 사이트 접속 및 복호화를 유도한다. 만약 복호화 비용을 지불하지 않으면 'Leaked Blog'에 데이터를 유포하겠다고 협박한다. 또한, 프린터를 통해 랜섬노트를 출력시키는데 이는 과거 '에그레고르 랜섬웨어(Egregor Ransomware)'가 사용했던 기능이다.



[그림 9] 랜섬노트

랜섬노트에 안내된 TOR 웹 복호화 사이트를 접속하면 복호화 비용은 표시되어 있지 않으며 채팅을 통해 운영자와 연락하여 합의 이후 복호화를 진행하는 것으로 추정된다. Leaked Blog에 접속해 보면 피해를 당한 것으로 추정되는 기업들의 홈페이지들이 적혀 있고, 게시글을 통해 록빗 파트너를 모집하고 있다.



[그림 10] 피해를 당한 것으로 추정되는 기업들

결론

록빗 랜섬웨어는 미국, 중국, 인도, 인도네시아, 우크라이나 및 여러 유럽 국가를 대상으로 공격을 진행했지만 최근 한국 기업도 공격 당하면서 기업들의 각별한 주의가 요구된다. 특히, 록빗 랜섬웨어 2.0 버전은 AD 그룹 정책까지 남용하여 윈도우 도메인 전체를 암호화 하므로 피해가 더욱 커지게 된다.

공격자들은 초기 침입을 위해 스피어 피싱을 통해 획득한 정보를 사용하거나 무차별 대입 공격을 활용한다. 따라서, 출처가 불분명한 이메일은 열람을 지양해야 하며 최신 버전의 보안 프로그램을 통해 주기적인 검사를 진행하여 의심스러운 파일이나 악성코드가 존재하는지 여부를 지속적으로 확인해야 한다.

AhnLab TI개발팀 최일봉 연구원