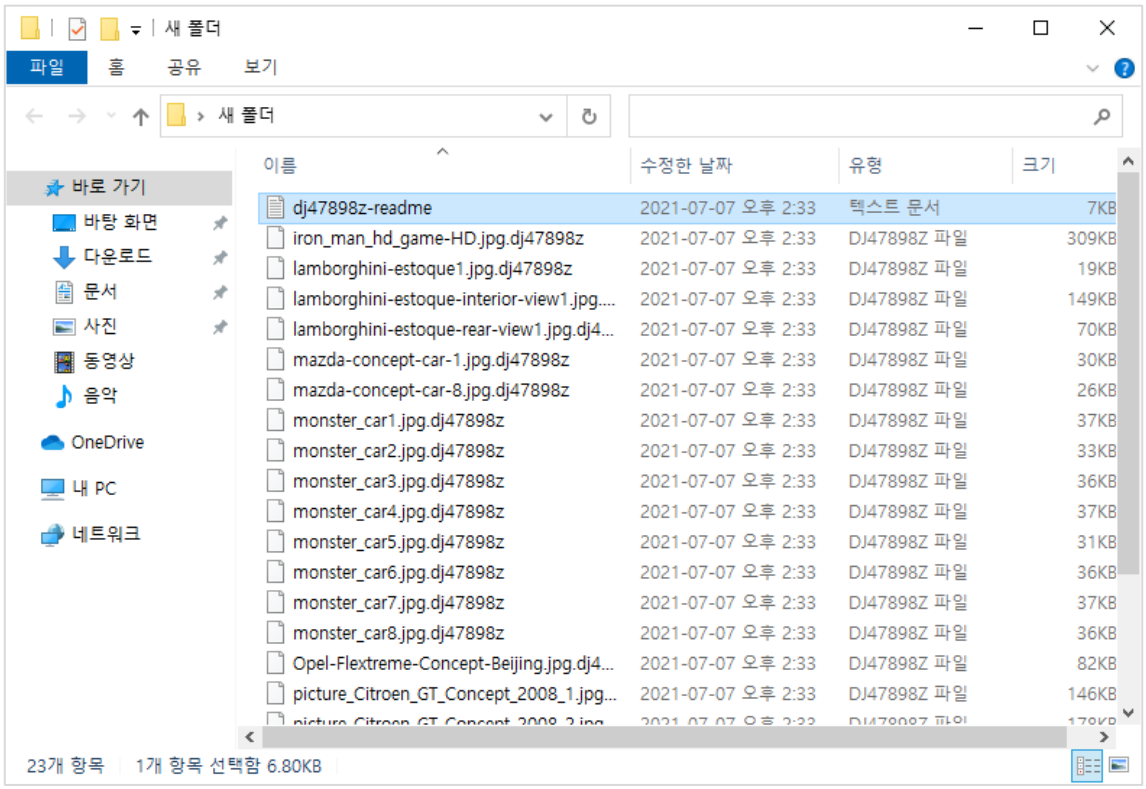
Today's Ransomware – Revil

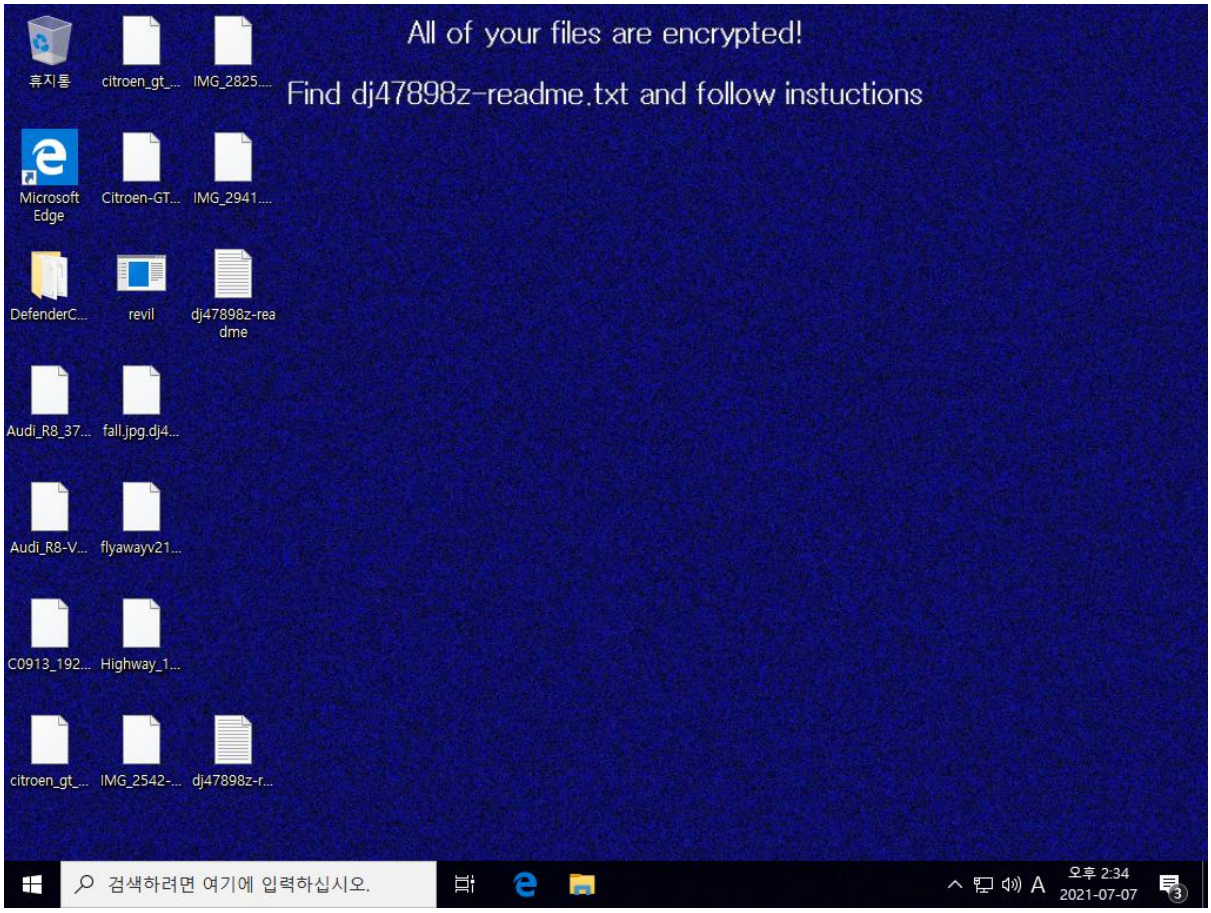
Jul 07, 2021

1. Blocked by TrojanCut®

2. Victim in case TrojanCut® was not installed - All file name's extensions were changed to Random Extension.



3. Screen of Victim



참조 기사

RaaS 대표주자 '레빌' 랜섬웨어, 지난해 최소 8,100 만 달러 수익

Lucian Constantin | CSO

레빌(REvil)은 서비스로서의 랜섬웨어(Ramsomware as a Service, RaaS) 공격으로, 지난 해 세계적으로 기관과 기업들로부터 큰 돈을 강탈했다.
레빌이란 이름은 영화 레지던트 에빌(Resident Evil)을 모티브로 한 랜섬웨어 에빌(Ransomeware Evil)을 의미한다. 보안업체들이 발간한 최근 보고서에서 따르면, 이는 가장 널리 퍼진 랜섬웨어 위협이며, 이의 배후 집단은 비즈니스 데이터까지 훔쳐 이를 공개하겠다고 위협함으로써 강탈 활동을 배가시켰다.

레빌은 소디노키비(Sodinokibi)라고도 하며 2019 년 4 월 처음 출현했는데, 갠드크랩(GranCrab)이라는 다른 RaaS 집단이 활동을 중단한 후 유명세를 타기 시작했다. 레빌이 처음 출현했을 때 전문가와 보안업체는 이를 갠드크랩의 변종으로 봤으며, 변종이 아니더라도 최소한 이들 사이에는 연관성이 있다고 주장했다. 하지만 이 공격 집단의 구성원으로 추정되는 언노운(Unknown)이라는 필명을 사용하는 인물은 최근 인터뷰에서 레빌이 새로운 창작물이 아니라, 이들이 입수한 오래된 코드베이스를 바탕으로 구축했음을 확인해줬다.

이 RaaS 공격의 배후에 있는 개발자는 이른바 '협력자(affiliates)'라고 알려진 사이버 범죄자에 의존해 랜섬웨어를 유포했다. 랜섬웨어의 개발자는 불법 수익금의 20~30%를 가져가고, 나머지는 실질적으로 기업 네트워크에 접속하고 악성코드를 배포하는 일을 하는 '협력자'가 가져간다. RaaS 공격이 성공적일수록 유능한 협력자를 유인할 가능성이 높아지고, 한 공격이 끝나면 협력자는 신속히 다른 공격으로 넘어간다. 이는 과거 갠드크랩(GandCrab)에서 나타났고, 좀 더 최근에는 메이즈(Maze)에서 발생했다. 이의 구성원들이 이번 달 초 활동 중단을 발표하자, 협력자들은 에그리거(Egregor), 또는 세크메트(Sekhmet)라고 알려진 새로운 랜섬웨어 계열로 신속히 이동했다.

레빌, 얼마나 성공했는가?
9 월, IBM 시큐리티 엑스포스 사건 대응(IBM Security X-force Incident Response) 팀은 올해 피해를 입은 사이버보안 사건 가운데 1/4 이 랜섬웨어 감염이었다고 밝혔다. 나아가 랜섬웨어 감염 가운데 1/3 이 레빌/소디노키비였다.
보안 전문가는 "IBM 시큐리티 엑스포스가 2020 년 가장 많이 목격한 랜섬웨어 종류는 레빌(소디노키비)이다. 이는 RaaS 공격 모델이고, 올해 혼합된 랜섬웨어 공격을 이행했다"면서, "이 악성코드는 랜섬웨어 및 데이터 탈취 공격에 관여했고, 랜섬웨어 운영자는 피해자가 몸값을 지불하지 않을 때 기밀 데이터를 훔쳐 인터넷에서 경매로 처분했다. 또한 소디노키비는 2020 년 전체 IBM 시큐리티 엑스포스 랜섬웨어 업무의 29%를 차지했다. 이는 소디노키비 운영자가 다른 랜섬웨어 종류와 비교할 때 피해자의 네트워크에 접속하는 능력이 더 우월함을 시사한다"라고

설명했다. IBM 시큐리티 엑스포스는 레빌이 2019 년 출현한 이래 최소한 140 개의 기관과 기업을 공격했다고 추산했고, 주요 표적 업종은 도매, 제조, 전문 서비스였다(법률, 회계 등). 약 60%의 피해자가 미국의 기업이었으며, 그 다음은 영국, 호주, 캐나다 순이었다. 또한 레빌 피해자 가운데 1/3 이 몸값을 지불했고, 1/10 은 기밀 정보가 다크 웹에서 경매 처분된 것으로 추정했다. 피해자의 1/3 이 데이터를 절취 당했다.

레빌 공격 집단은 피해 조직의 연간 매출을 기준으로 몸값을 요청한 것으로 보인다. 그래서 요구 금액이 1,500 달러에서 4,200 만 달러, 피해자 연매출의 최대 9%에 이르기까지 크게 달랐던 것이다. 또한 IBM 은 레빌과 사이버범죄 조직인 FIN7 ('카바낙(Carbanak)'으로도 알려짐) 사이의 일부 중복을 확인했다. '협력자'가 두 집단과 모두 계약하면 이런 일이 벌어질 수 있다.
IBM 은 지난 해 레빌의 수익이 최소 8,100 만 달러인 것으로 추정했다. 레빌 집단의 대리자로 추정되는 '언노운'과 한 러시아인 블로거와의 인터뷰를 보면 이런 추산이 틀리지 않은 듯하다. 이 사이버범죄자는 이 랜섬웨어 공격으로 1 억 달러 이상을 벌었다고 주장했다.
블리핑컴퓨터(BleepingComputer)는 지난 9 월, 이 집단이 한 해커 포럼에 비트코인으로 100 만 달러를 예치했고, 이는 유능한 해커를 '협력자'로 모집하려는 시도였다고 보도했다.

데이터 절취, 강탈, 허위 약속

2020 년 11 월 초, 랜섬웨어 사건 대응 전문업체인 코브웨어(Coveware)는 레빌/소디노키비가 16%의 감염률로 2020 년 3 분기 최대의 랜섬웨어 점유율을 차지했다고 보고했다. 또한 이는 이전 분기에도 1 위였다. 코브웨어가 조사한 랜섬웨어 사건의 절반 가까이가 탈취한 데이터를 공개하겠다는 위협했고, 이 위협을 활용하는 집단의 수도 증가했다.
이 보안업체는 "코브웨어는 데이터 탈취 전략이 임계점에 도달했다고 느낀다"면서, "일부 회사는 탈취된 데이터를 공개하지 않도록 위협 행위자에게 돈을 주기로 선택하지만, 코브웨어는 데이터를 제거하겠다는 사이버범죄자의 약속이 흐지부지되는 것을 목격했다"라고 말했다.
특히, 코브웨어는 돈을 이미 지불한 피해자가 몇 주 후 동일 데이터를 공개하겠다고 다시 위협받는 사태를 목격했다. 다른 집단들 역시 약속을 지키지 않고, 돈을 지급한 피해자의 데이터를 공개하거나 데이터를 삭제했다는 허위 증거를 제시했다.
코브웨어는 "암호 키에 대한 협상과 달리 탈취 데이터의 비공개에 대한 협상은 확실한 결말이 없다"면서, "피해자가 암호 키를 받으면 빼앗길 수 없고 변질되지 않는다. 탈취된 데이터라면 위협 행위자는 미래의 어느 시점에든 돈을 받기 위해 다시 돌아올 수 있다. 이에 관한 추적 기록이 너무 짧고 약속 불이행은 선택적으로 일어난다는 증거는 이미 쌓이고 있다. 따라서 데이터 피해자가 강경하면서도 책임있는 단계들을 취하도록 조언한다. 예를 들어 유능한 프라이버시 변호사의 조언을 받고, 어떤 데이터가 탈취됐는지 조사하고, 이런 조사 및 상담에 따라 필요한 통지를 행하는 식이다"라고 설명했다.
레빌의 대리인인 '언노운'은 러시아 블로거에게 다른 기법 역시 도입하는 것을 검토 중이라고 말했다. 예를 들어 분산 서비스 거부 공격(DDoS)을 개시해 협상을 지연하는 조직을 압박하는 것 등이다.

레빌이 작동하는 방식

레빌은 인간이 조정하는 랜섬웨어 캠페인 가운데 하나이고, 류크(Ryuk), 웨이스티드로커(WastedLocker) 등과 비슷하다. 해커는 침입이 성공하면 다양한 툴과 기법을 이용해 네트워크를 매핑하고 횡적 이동을 수행하고 도메인 관리자 권한을 획득하고 랜섬웨어를 모든 컴퓨터에 전개해 영향을 최대화한다.

레빌은 여러 '협력자'에 의해 유포되기 때문에, 최초 접속 경로는 다양하다. 다시 말해 악성코드는 첨부된 피싱 이메일, 훼손된 RDP(Remote Desktop Protocol) 인증서, 이미 잘 알려진 취약점 악용 등으로 확산된다. 예를 들어, 지난 해 레빌 공격자는 오라클 웹로직(Oracle Weblogic)의 알려진 취약점(CVE-2019-2725)을 악용해 시스템에 접속했다.

코브웨어 보고서에 따르면, 현재 레빌은 주로 훼손된 RDP 세션(65%), 피싱(16%), 소프트웨어 취약점(8%)을 통해 유포된다. '언노운'은 또한 인터뷰에서 RDP 를 훼손하기 위해 무차별 대입 공격을 이용하는 레빌 '협력자'가 많다고 확인해주었다.

레빌은 RSA 대신 엘립틱 커브 알고리즘인 디피-헬먼(Diffie-Hellman) 키 교환, AES 대신 살사 20(Salsa 20)을 이용해 파일을 암호화한다는 점에서 다른 랜섬웨어 프로그램과 차별화된다. 이들 암호화 알고리즘은 짧은 키를 이용하고 매우 효율적이고 정확히 구현되면 깨뜨릴 수 없다.

레빌 랜섬웨어는 감염된 머신의 프로세스를 중지시킨다. 예를 들어 이메일 클라이언트, SQL 및 여타 데이터베이스 서버, 마이크로소프트 오피스 프로그램, 브라우저, 중요 파일을 잠근다. 이 후 윈도우 섀도우 파일 사본과 여타 백업을 제거해 파일 복구를 못하게 한다.

레빌 대응 방법

조직은 언제나 강력한 인증서와 2 요소 인증으로 원격 접속을 보안해야 하고, 이를 VPN 으로 제한하는 것을 고려해야 한다. 공공에 노출된 서버, 애플리케이션, 기기는 계속해서 업데이트해야 하고, 정기 검사를 통해 취약점, 구성 오류, 의심스러운 행위를 확인해야 한다. 가급적이면, 허위 인증서에 의한 과도한 로그인 시도를 차단하는 무차별 대입 공격 보호 역시 이행해야 한다. 기업 네트워크 내에서 다음과 같은 조치를 취해야 한다.

- 횡적 이동에 사용될 수 있는 불필요한 엔드포인트 간 SMB(Server Message Block) 및 RPC(Remote Procedure Call) 통신을 차단
- 특권 계정의 의심스러운 행위에 대한 모니터링
- 폴더 및 프로세스에 관한 엄격한 접속 제어 규칙으로 엔드포인트 공격 표면 축소
- 보안된 네트워크 공유
- 피싱 시도를 탐지하기 위한 방법에 관한 직원 교육
- 외부에 백업을 저장하고 백업으로부터 복귀가 적시에 이뤄지는 것을 테스트하는 데이터 백업 프로세스 배치
- 공격이 탐지되면 즉시 조치를 취할 수 있도록 명확한 사건 대응 계획을 배치. 여기에 관여하는 사람과 이들의 책임을 명시. NIST 는 랜섬웨어를 탐지하고 대응하는 가이드를

발행했다.

코브웨어 연구진은 "의료 등의 특정산업은 기밀 데이터와 시스템 중단에 대해 민감하기 때문에 다른 산업보다 표적이 되기 쉽다"면서 "그러나 목격한 바에 따르면 특정산업 내에 보편화되고 악용하기 쉬운 취약점이 존재하기 때문에 산업 편중이 일어나는 것이다"라고 말했다.
코브웨어 연구진은 법률 또는 회계사무소 등 전문서비스가 특히 취약하다고. 420 만 개에 이르는 미국의 전문서비스 기업은 미국내 기업의 14%를 차지하지만, 공격은 25%에 이른다.
코브웨어는 "이들 기업은 랜섬웨어 위협을 덜 심각하게 받아들이는 경향이 있다. 이들은 흔히 RDP 같은 취약점을 인터넷에 열어두고 있어 다른 업종의 기업보다 훨씬 더 자주 피해를 입는다. 소규모 전문 서비스 기업은 작다고 해서 표적이 되지 않는 것이 아님을 이해해야 한다. 사이버 범죄의 세계는 그런 식으로 돌아가지 않는다. 인터넷에 쉬운 취약점을 노출하면 공격받는다. 이는 시간 문제일 뿐이다"라고 경고했다. editor@itworld.co.kr