최신

보안 동향

레포트

2025년 현재, 가장 위험한 랜섬웨어 그룹: LockBit

Name : 조민혁

Class Number : 5

Phone Number : 010-4923-2198

- 2025년 현재, 가장 위험한 랜섬웨어 그룹: LockBit -

그림 1. LockBit Group

랜섬웨어(Ransomware)란 몸값(Ransom)과 소프트웨어(Software)의 합성어로 컴퓨터 시스템의 데이터를 암호화한 뒤 이를 해제해주는 조건으로 금전을 요구하는 악성 소프트웨어를 의미한다. 단순한 악성코드와 달리 최근의 랜섬웨어 공격은 조직화된 범죄 집단이 체계적인 방식으로 수행하며 이들을 흔히 '랜섬웨어 그룹'이라 부른다. 이들은 정부 기관, 병원, 제조업체 등 사이버 보안이 취약하거나 고가치 정보를 보유한 대상을 집중적으로 노린다.

2025 년 현재 LockBit 은 세계에서 가장 활발하고 위협적인 랜섬웨어 그룹 중 하나로 손꼽힌다. 이 그룹은 2019 년 처음 등장한 이후 빠르게 진화하며 범죄 생태계를 확장해왔다. 특히 이들은 'RaaS (Ransomeware-as-a-Service)'라 불리는 랜섬웨어 서비스 형태로 조직 외부의 공격자를 모집하여 전 세계를 무대로 공격을 수행한다. 이를 통해 LockBit 은 단일 그룹이 아닌 하나의 플랫폼처럼 작동하며 그 파급력은 매우 크다.

LockBit 의 가장 큰 특징 중 하나는 자동화된 암호화 프로세스와 속도다. 이들은 공격자가 표적 시스템에 접근하는 즉시 파일을 암호화하고, 피해 기업의 네트워크를 분석해 백업 데이터까지도 손상시킨다. 이와 동시에 피해자의 민감 정보를 탈취해 이중 협박 전략을 구사한다. 피해자가 복호화를 거부하거나 지불을 거절할 경우 이 정보를 다크웹에 공개하겠다고 협박하는 방식이다.

2023 년부터 2025 년까지 LockBit 은 다수의 대규모 공격으로 전 세계 언론의 주목을 받았다. 미국의 항공우주 산업, 유럽의 공공기관, 일본의 물류기업 등이 LockBit의 표적이 되었으며 일부 피해 사례에서는 수백억 원 규모의 비트코인 몸값이 오갔다. 또한 이들은 공격 전 단계에서 기업 내부의 보안 상태를 정밀하게 분석하며 사회공학 기법을 동반한 피싱 이메일로 초기 침투를 시도하는 등 고도화된 전략을 구사한다.

2024 년 2 월 20 일, 국제 수사기관의 공조로 LockBit 인프라 일부가 무력화되었고, 핵심 관계자 2 명이 체포되었다는 공식 발표가 있었다. 그러나 단지 나흘 만에 LockBit 은 다시 활동을 재개하며 그 존재를 과시했다. 이는 랜섬웨어 생태계의 특징 중 하나인 "지속적인 부활력"을 잘 보여주는 사례이며 단순한 일회성 수사나 제재만으로는 이러한 범죄 조직을 근본적으로 제거하기 어렵다는 점을 시사한다.

이에 따라 글로벌 보안 커뮤니티와 수사기관들은 랜섬웨어 조직의 주요 수익원인 몸값 지불을 금지하는 원칙을 강조하고 있으며 법적 대응과 기술적 차단을 위한 국제적 공조도 계속해서 강화되고 있다. 그럼에도 불구하고 랜섬웨어 피해는 지속적으로 증가하고 있으, LockBit 사례처럼 조직의 일부가 해체되더라도 동일한 인프라와 전략을 기반으로 재조직화 및 변종 그룹의 출현이 이어지고 있는 상황이다.

결론적으로, LockBit 은 단순한 해커 집단을 넘어 사이버 범죄 산업의 상징적 존재로 자리 잡고 있다. 이들의 위협에 대응하기 위해서는 전 세계적 수준의 공조와 더불어 기술적·법적·정책적 수단이 유기적으로 연계된 강력한 대응체계가 시급히 마련되어야 할 것이다.

References

[1] 랜섬웨어란?, Akamai:

https://www.akamai.com/ko/glossary/what-is-ransomware

[2] 세계 최대 랜섬웨어 그룹 '록빗', 국제공조로 드디어 잡혔다!, 보안뉴스:

https://www.boannews.com/media/view.asp?idx=126891&kind=&sub_kind

[3] 국제 공조의 대대적인 성공 이후 1 주일 만에 돌아온 록빗, 보안뉴스:
https://m.boannews.com/html/detail.html?idx=127091

[4] '록빗(LockBit)' 그룹 검거로 알아보는 랜섬웨어 생태계:

https://www.igloo.co.kr/security-information/%EB%A1%9D%EB%B9%97lockbit-%EA%B7%B8%EB%A3%B9-%EA%B2%80%EA%B1%B0%EB%A1%9C-%EC%95%8C%EC%95%84%EB%B3%B4%EB%8A%94-%EB%9E%9C%EC%84%AC%EC%9B%A8%EC%96%B4-%EC%83%9D%ED%83%9C%EA%B3%84

[5] 2024 년 사이버 위협 동향 리뷰 2025 년 전망, AhnLab

[6] 2025 년 보안 위협 전망 보고서, SK Shieldus