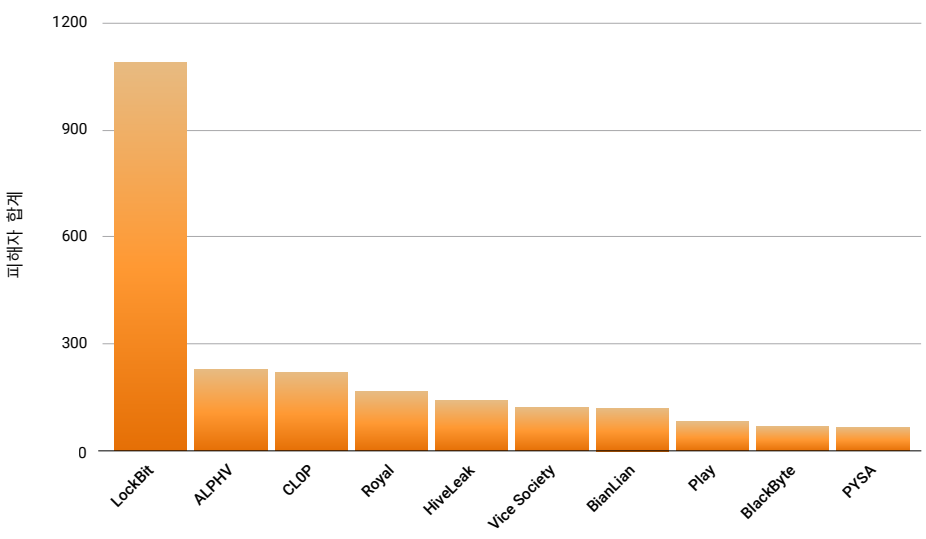
멈추지 않는 랜섬웨어

진화하는 악용 기술과 활발한 제로데이 공격

랜섬웨어 그룹은 기업에 미치는 피해를 극대화하기 위해 제로데이 및 원데이 취약점 악용, 다중 갈취 전략과 같은 공격적인 방법을 사용하고 있습니다.

피해 기업의 39%를 차지하며 랜섬웨어 분야를 장악하고 있는 LockBit

랜섬웨어 그룹별 피해자 수
2021년 10월 1일 ~ 2023년 5월 31일



LockBit는 소프트웨어를 지속적으로 개선하면서 성공을 거뒀습니다. 하지만 CL0P는 파일 전송 소프트웨어의 제로데이 취약점을 악용하는 수법으로 유명해지면서 세력을 확장하고 있습니다.

143% ↑

CL0P와 같은 그룹이 제로데이 및 원데이 취약점을 적극적으로 악용하면서 증가한 랜섬웨어 피해자

여러 랜섬웨어 그룹의 공격을 받은 피해자는 **첫 3개월 이내에 후속 공격을 받을 가능성이 6배 가까이 높습니다**

39% ↑
2021년 4분기 대비 2022년 4분기 **헬스케어 업계의 피해 기업** 증가율

42% ↑
2021년 4분기 대비 2022년 4분기 **제조 업계의 피해 기업** 증가율

65%
미화 5천만 달러 이하의 **소규모 매출 구간**에 속하는 피해 기업

77%
유럽, 중동, 아프리카(EMEA)의
랜섬웨어 피해자 증가

204%
아시아 태평양 및 일본(APJ)의
랜섬웨어 피해자 증가

공격자가 갈취 기법을 극대화하는 방법

초기 거점
(Spear) 피싱, 제로데이 및 원데이 취약점, 인증정보 도용

측면 이동
피해나 영향을 극대화하기 위해 네트워크 전체로 확산

유출
중요 데이터 발견 및 유출은 갈취하는 주된 방법이 되어가고 있음

암호화
복구를 차단하고 운영을 방해하는 효율적이고 안전한 암호화

랜섬 수요
피해자가 랜섬을 지불하거나 공격자가 유출 사이트에 기밀 데이터를 게시

랜섬웨어 그룹의 취약점 악용은 데이터 도난의 직접적인 원인이 될 수 있습니다

최근 몇 달 동안 유출된 데이터만으로 랜섬을 요구한 랜섬웨어 공격자들이 있었습니다

DDoS 공격
운영을 중단시키기 위해 DDoS 공격이 추가적인 갈취 기법으로 사용됨

협박 및 괴롭힘
공격자가 피해자의 고객이나 파트너에게 전화나 이메일을 보내 압박을 가함

랜섬을 지불하도록 피해자에게 가해지는 추가적인 압력

랜섬웨어 트렌드, 공격 기술의 변화, 방어 전략에 대한 자세한 정보와 인사이트는 보고서 전문을 참조하세요.

보고서 전문 다운로드

 | 지원 | 2023년 08월 발행