Dark web & Telegram
Weekly Highlights

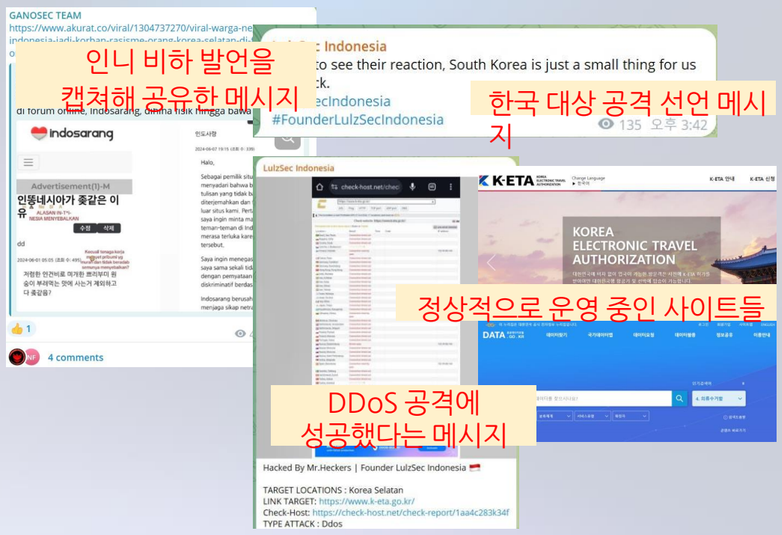
June Week 2

인도네시아 해킹 그룹, 한국 정부 기관 대상 DDoS 공격 감행. 타겟 사이트들은 정상 운영 중

- 지난 6월 11일, 인도네시아의 해킹 그룹 GANOSEC TEAM은 자체적으로 운영하는 텔레그램 채널을 통해 인도네시아의 한 한인 커뮤니티에서 인도네시아를 비하하는 발언이 포착되었다고 밝힘

- 이 메시지는 인도네시아 기반의 해킹 그룹들의 텔레그램 채널에 공유되었으며 이에 분노한 Lulzsec Indonesia라는 해킹 그룹은 한국을 대상으로 사이버 공격 활동을 펼칠 것이라 선언함

- 이들은 이후 문제가 된 한인 커뮤니티를 포함해 한국의 정부 기관들을 대상으로 DDoS 공격에 성공했다는 메시지를 자체 텔레그램 채널에 게시함. 다만, 확인 결과 이들이 공격했다고 밝힌 정부 기관 사이트들의 운영은 정상적으로 되고 있는 것으로 나타남

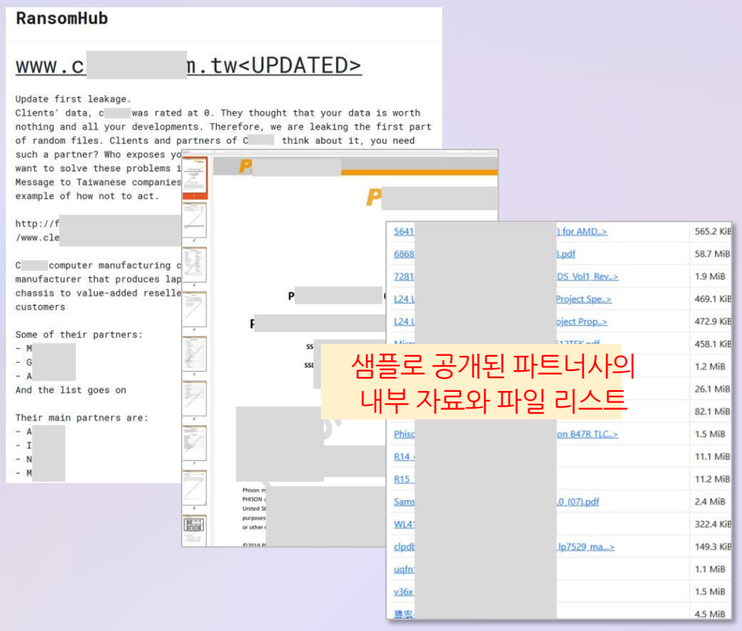


대만의 컴퓨터 제조업체, 랜섬웨어 감염 피해. 해킹 그룹은 파트너사 자료를 빌미로 협박 중

- 대만의 컴퓨터 제조업체 C사가 랜섬웨어에 감염되어 내부 자료가 유출되는 피해를 입은 것으로 확인됨
(최초 포스팅 5월 29일, 자료 유출 포스팅 6월 13일)

- 다크웹 랜섬웨어 그룹 RansomHub는 6월 13일, C사의 데이터 중 일부를 공개하며 이들을 압박하는 메시지를 첨부했는데 이에 따르면 랜섬웨어 그룹은 피해 기업에서 유출된 이들의 파트너사 데이터를 빌미로 협박했으며, 피해 기업은 이에 대해 금액을 지불하는 것을 거절한 것으로 보임

- 실제로 랜섬웨어 그룹이 공개한 데이터 내역을 확인한 결과, 파일명에서 미국, 대만의 반도체 기업이나 한국의 대기업 이름이 기재되어 있는 것으로 나타남

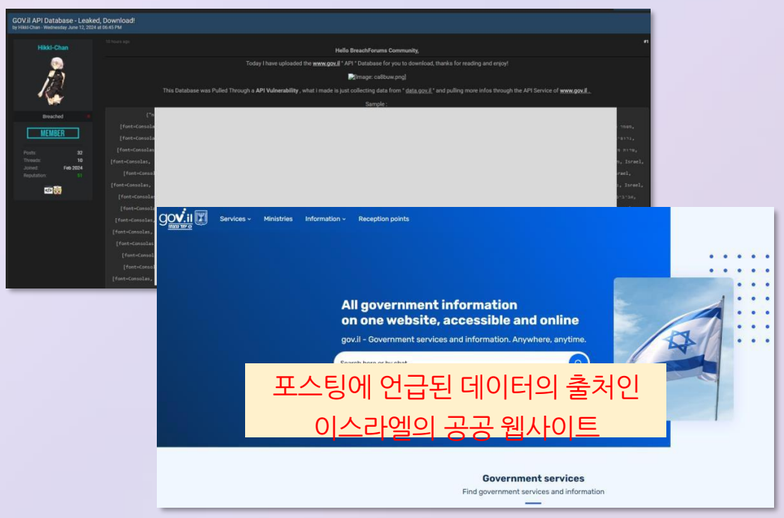


유명 해킹 포럼 내 이스라엘 정부 기관의 데이터 유출 포착. API 취약점 통한 유출 추정

- 지난 6월 12일, BreachForums에 이스라엘 정부 기관의 내부 자료를 유출하는 포스팅이 게시됨

- 포스팅을 게시한 유저 HikkI-Chan에 따르면, 그는 이스라엘 공공 데이터를 다루는 정부 기관의 웹사이트 API에 대해 취약점을 찾아 해당 데이터를 유출했으며, 공개한 샘플 외에도 다양한 데이터를 유출했다고 주장함

- 공개된 샘플 확인 결과, 이스라엘 시민으로 추정되는 이들의 이름과 연락처, 생년월일, 신원 등록 번호, 주소 등이 영어와 히브리어로 혼재되어 기재되어 있으며, 전체 데이터는 약 27만개라고 함



S2W