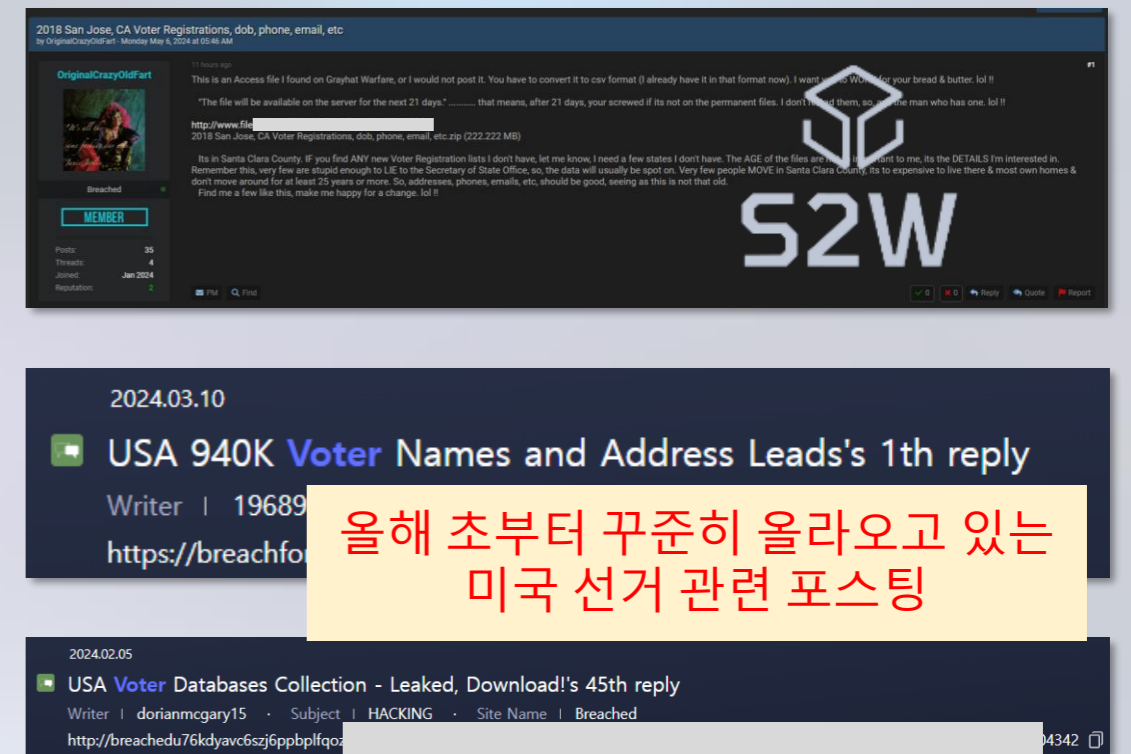


Dark web & Telegram Weekly Highlights

May Week 2

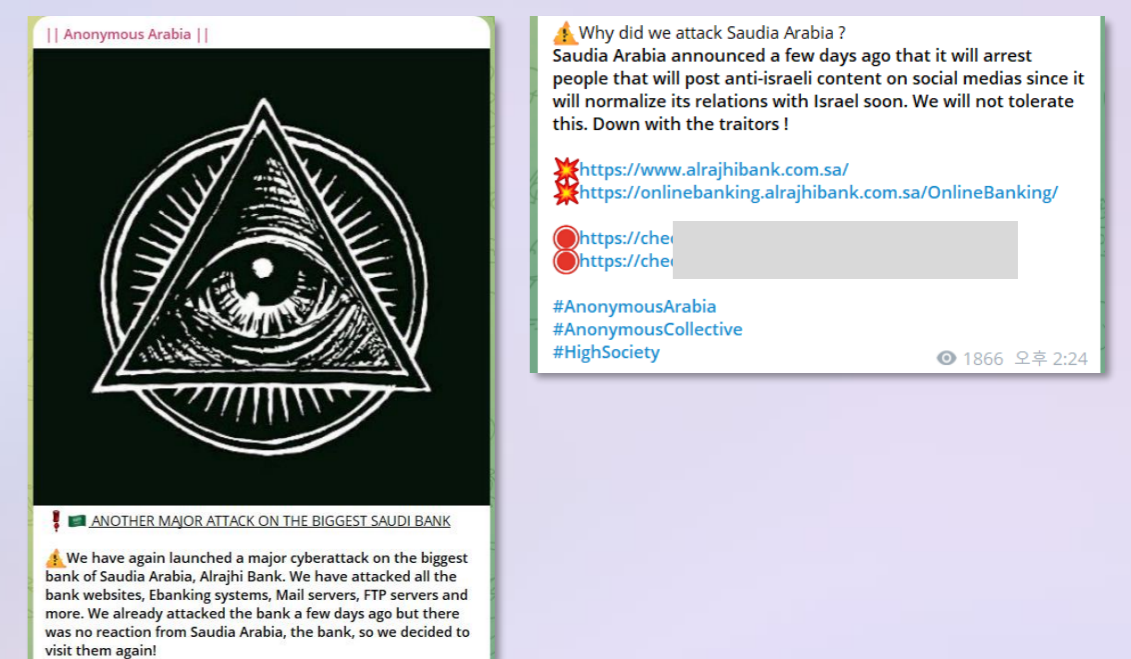
미국 캘리포니아 지역 유권자 정보 유출 및 무료 공개 포착. 최근 선거 관련 데이터 지속 유출 중

- 지난 5월 6일, 다크웹 해킹 포럼 BreachForums에서 활동하는 유저 OriginalCrazyOldFart는 미국 캘리포니아 주 산호세 지역의 유권자 관련 데이터를 유출하며 무료로 공개함
- 유출된 데이터는 약 200MB 파일로 유권자들의 이름, 생년월일, 연락처, 이메일 주소와 등록 번호 등이 포함되어 있으며, 유출 시기는 2018년임
 - ✓ 유출한 유저는 지역 특성 상 높은 거주 비용으로 인구 이동이 원활하지 않아 데이터의 신뢰도가 높을 것이라 주장함
- 올해 11월 미국 대선을 앞두고 다크웹과 텔레그램 등지에서 유권자 정보 유출이나 선거 관련 포스팅이 자주 게시되고 있음



세계 최대 이슬람 은행, 사이버 공격 피해. 최근 자국 정부의 對이스라엘 유화 정책이 공격 배경

- 사우디아라비아의 대표적인 은행 Alrajhi Bank가 국제 정치적인 목적에 의해 사이버 공격을 당해 시스템에 피해를 입은 정황이 포착됨
- 텔레그램에서 활동하는 해킹 그룹 Anonymous Arabia는 지난 5월 6일, 자체적으로 운영하는 텔레그램 채널에서 피해 기관에 대한 공격 성공을 선언했으며 이번 공격으로 피해 기관의 온라인 banking, 메일/FTP 서버 등에 피해를 입었다고 주장함
- 해킹 그룹은 이번 공격의 배경으로 최근 사우디 정부의 對 이스라엘 유화 정책을 문제 삼았으며, 향후 다른 기관에 대한 공격을 암시함



다크웹 생태계 다시 활성화 중. 대형 블랙마켓, 랜섬웨어 그룹 부활 등 이후 유저 +30% 증가

- 텔레그램의 활성화 이후 잠시 주춤했던 다크웹 생태계의 규모가 올해 들어 다시 성장하고 있는 모습이 확인됨
- S2W 데이터 확인 결과, 올해 1~4월 동안 다크웹 페이지의 수집량이 작년의 그것과 비교해 약 50% 가량 증가했으며, 다크웹 브라우저인 TOR에서 발표하는 일평균 유저 규모 역시 전세계 기준 약 30% 증가한 것으로 나타남
- 최근 이러한 다크웹 주요 수치 증가의 배경에는, 텔레그램으로 이탈한 유저들이 다크웹에서 활동을 이원화하여 활동을 재개함과 더불어 꾸준히 활동 중인 랜섬웨어 그룹들, Mega Market이나 Kraken Market과 같은 대형 러시아 블랙마켓의 등장 등이 영향을 미치고 있을 것으로 추정됨

