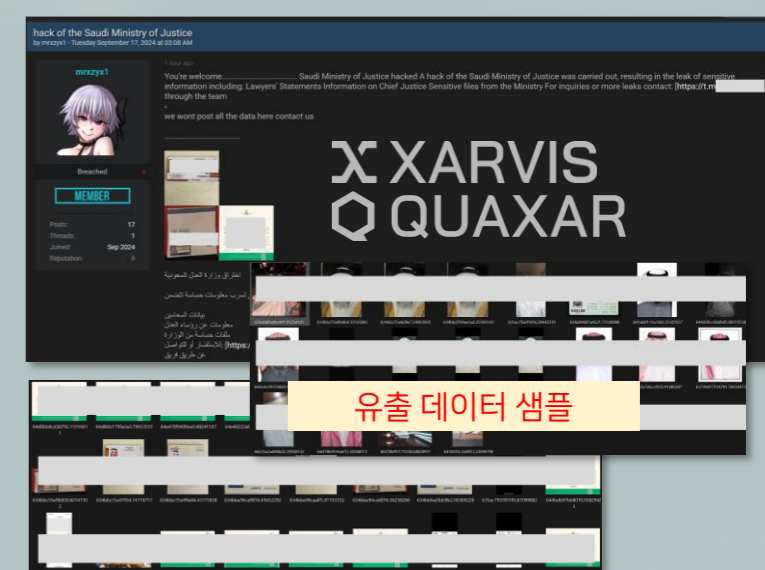


Dark web & Telegram Weekly Highlights

September Week 3

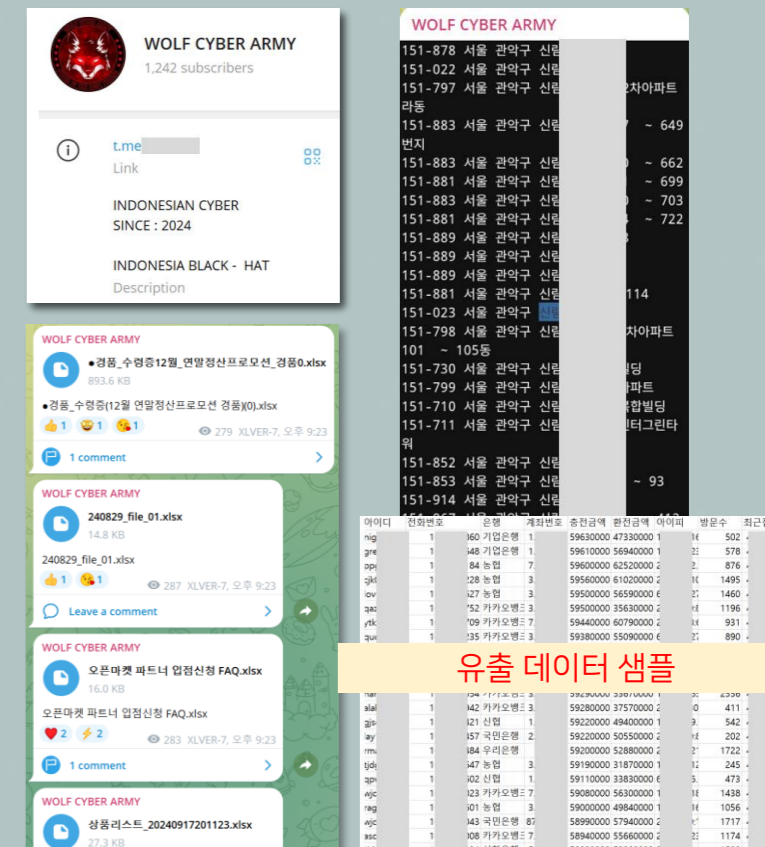
사우디 아라비아 법무부의 내부 자료 유출 포착. 정부 종사자의 신분증, 프로필 사진 등 포함

- 사우디아라비아의 법무부의 내부 자료가 유출되어 다크웹 해킹 포럼 BreachForums에서 판매되고 있는 정황이 포착됨
- 지난 9월 17일, 포럼 유저 mrxyz1은 사우디의 내부 자료를 판매한다는 포스팅을 게시했는데, 그는 유출한 데이터의 샘플로 사우디 사람의 신분증들과 문서를 공개했으며, 또한 별도의 텔레그램 링크를 기재했음
- 해당 텔레그램 링크에는 더 많은 샘플 파일이 공유되고 있는데 약 130여개의 신분증이나 정부 기관에서 작성한 문서, 인물들의 프로필 사진 등이 포함되어 있는 것이 확인되었으며, 가격은 900달러로 제시하고 있음



대한민국의 웹사이트 데이터 다수 유출. 인도네시아 해킹 그룹의 텔레그램 채널 통해 공유 중

- 몇몇 대한민국의 웹사이트로부터 유출된 데이터가 인도네시아 해커들에 의해 유출되어 텔레그램에서 공유되고 있음
- 텔레그램에서 주로 활동하는 해킹 그룹 WOLF CYBER ARMY는 지난 9월 17일, 자체적으로 운영하는 채널을 통해 약 10여개의 엑셀 파일과 텍스트 파일을 공유함
- 확인 결과 해당 데이터들은 대부분 각자 다른 사이트에서 유출된 것으로 보이며 대다수는 공시 자료나 공개 자료로 외부 유출 시 위험성이 없으나 일부 데이터는 민감한 내용을 포함하고 있음. 특히 불법 도박 사이트에서 유출된 내용도 포함되어 있으며, 도박 사이트 이용자들의 연락처가 계좌 정보, 송수금 내역, IP 주소 등이 포함되어 있음
- 해커 그룹은 인도네시아 해킹 그룹을 표방하는 그룹으로, 최근 인니 해킹 그룹에 의한 한국의 데이터 유출 사고가 일부 발생하고 있어 이에 대한 주의가 필요함



인도네시아 정부 기관 공격 전문 해커 Bjorka 활동 재개. 이번에도 인니 국세청 정보 유출

- 과거 인니 정부 기관을 상대로 수차례 사이버 공격을 가해 악명을 떨친 해커 Bjorka가 약 8개월 만에 BreachForums에서 다시 활동을 시작한 정황이 포착됨
- 올해 1월 이후 활동을 보이지 않던 그는 지난 9월 18일 약 8개월만에 포스팅을 게시했는데 이번에도 그는 인니 납세자의 개인 정보를 유출해 판매하고 있음
- 유출 데이터는 약 2GB이며 각 납세자의 이름, 식별 번호, 연락처, 주소 등과 같은 정보가 포함되어 있고, 특히 유출 명단에 인니 대통령과 그의 아들을 포함되어 있다고 함
- 활동을 재개한 Bjorka가 향후에도 인도네시아 정부 기관을 또다시 지속적으로 공격할지 관심이 주목되고 있음

