==== 김치콘 2017 BEST CFP #02 ====

submitted at 2017. 5. 17 오전 11:35:39

제목	**Operation RIFLE : Andariel, The Maiden of Anguish**	소요 시간	45분~50분
키워드	Forensics / Incident Response, Threat Analysis		

[초록]

국내 기업 및 정부기관만을 대상으로 사이버 공격을 수행하는 Nation-Sponsored 위협그룹에 대한 프로파일링 결과이며 국내 침해사고들의 연관성에 대해 발표

[개요]

2016년 2월, 유명 보안업체의 코드서명 인증서를 도용한 악성코드가 최초 식별한 이후 S사 DRM으로 위장한 악성코드가 이어서 발견 되었습니다. 관련 샘플과 분석 결과를 토대로 수사기관들과 공조하여 조사를 진행했고 C&C 서버와 기업 내부 피해 PC 등에서 수집한 샘플들을 프로파일링한 결과, 2015년 11월, 방위산업체를 공격했던 그룹과 동일한 그룹이었습니다. 이후 2016년에 벌어졌던 많은 침해사고 (국방부 기밀 문서 탈취 사고를 포함한 비공개 사고까지)에서 그들의 흔적을 지속적으로 찾을 수 있었으며, 2017년 C사의 ATM에서 카드 정보를 탈취해간 공격 역시 동일한 그룹에 의한 사고였습니다.
2016년부터 있었던 주요 국내 침해사고는 대부분 동일한 그룹에 의해 수행 되었습니다.
더불어 해당 위협 그룹은 최근 사행성 게임을 해킹하는 악성코드를 유포하는 등 외화벌이를 위한 부업도 열심히 하고 있으며 시중은행 보다는 영세한 전자금융업자를 공격하는 양상을 보이고 있습니다. 점점 이들의 공격은 Cyber terror와 Cyber crime 사이에서 그 경계가 모호해질 것입니다.
본 발표에서는 해당 위협 그룹이 자주 사용하는 악성코드들의 특징과 거점 확보 방식 (백신 취약점, 보안 솔루션 취약점, 웹쉘 등)에 대해 설명하고, 이를 토대로 위협 그룹 프로파일링 방법에 대해 말씀 드리려고 합니다. 또한 최근 지속적으로 이슈되고 있는 Lazarus와의 차이점 역시 알아보고자 합니다.

[발표 목적]

지금까지 국내에서 발생한 북한발 공격에 대해 상세한 프로파일링 결과가 발표된 적은 거의 없습니다. 단순히 "북한"이라고만 발표되고 있는 실정이고 이러한 프로파일링 결과가 공개되는 것을 꺼려하는 분위기가 있습니다. 코드 레벨에서 프로파일링을 하고 있는 사람도 극히 일부인 것 같습니다. 하지만 해외에서는 카스퍼스키, 탈로스, 팔로알토 등에 의해 Operation Blockbuster, Bluenoroff 등등 상세한 프로파일링 내용이 이미 많이 공개가 되어 있습니다.

분단 국가라는 한국의 특수한 상황상 공격 주체가 북한인지 아닌지에 대한 규명도 필요하다고 생각합니다.

하지만 위협 분석 업무를 하는 입장에서 그 이상에 대한 기술적인 위협 분석(프로파일링)이 필요하고 또 관련 정보가 공유되고 토론될 수 있어야 한다고 생각합니다.
본 발표를 통해서 청중들이 최근 국내를 대상으로 하는 공격과 공격조직에 대해 조금 더 상세히 알 수 있기를 바랍니다. 이러한 지식을 통해 최근에도 지속적으로 언급 되고 있는 "북한" 이슈들에 대한 청중 스스로의 판단력과 통찰력이 생기리라 생각합니다.

[고려사항]

녹화, 녹음 금지 및 슬라이드 역시 일부 내용만 제공 가능합니다. 발표자 이름 역시 익명으로 부탁드립니다.

[투고 이유]

비공개적인 성격이 강하고 참가인원도 소수인 점 때문에 투고하게 됐습니다.

이전에 다른 컨퍼런스에서 발표된 내용입니까? 아니오
새로운 도구에 대한 내용입니까? 아니오
새로운 취약점에 대한 내용입니까? 아니오
시연을 포함하고 있습니까? 예
기타 사항: