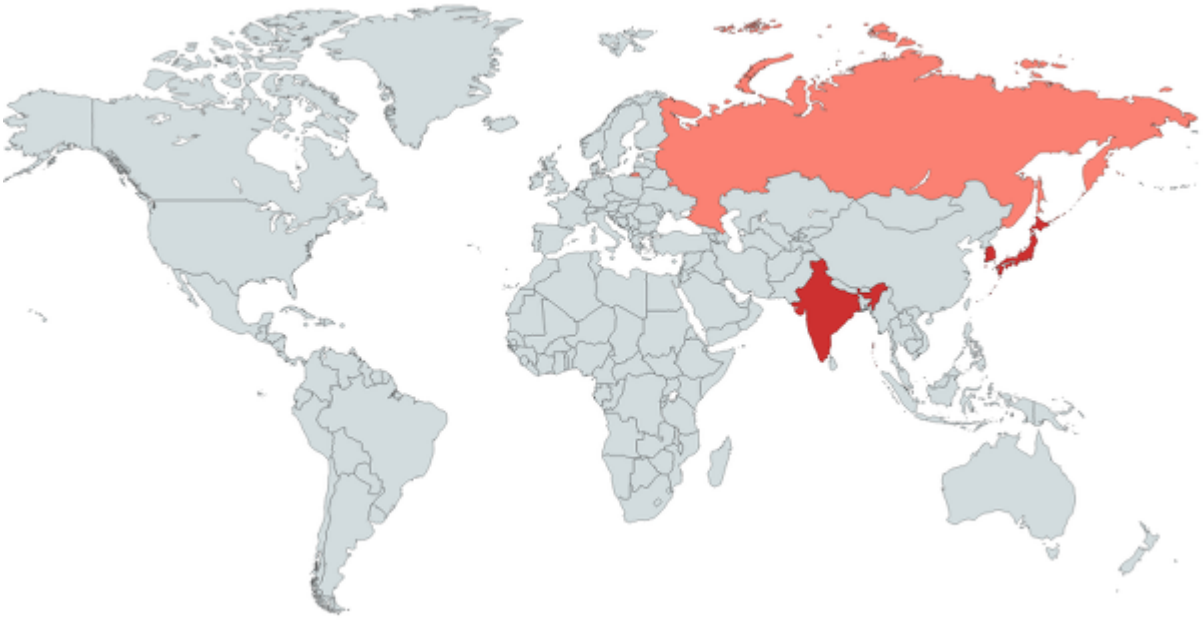
10년 가까이 군 정보 노리고 있는 오퍼레이션 비터 비스킷 - ASEC

By ATCP

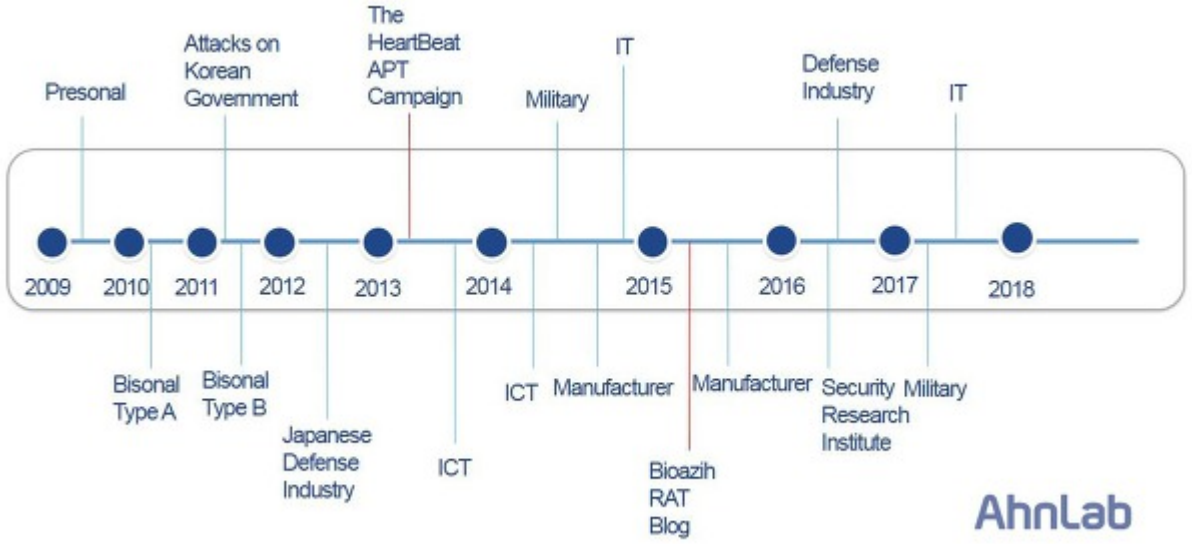
Published: 2017-10-15 · Archived: 2026-04-05 19:04:46 UTC

오퍼레이션 비터 비스킷(Operation Bitter Biscuit)에 이용된 비소날류 악성코드는 2010년 최초 발견된 후 현재까지 한국, 일본, 인도에 대한 공격이 확인되었으며, 디코이(decoy) 파일을 통해 러시아권 사용자에게도 추가 공격을 가한 것으로 보인다. 일본의 경우 2012년 방위산업체에 대한 공격이 있었으며, 인도 CERT에서는 2015년 비소날 악성코드의 변형인 바이오아지흐(Bioazih)에 대해 경고한 바 있다. 하지만 최근에는 한국을 제외한 나머지 국가에서는 관련 공격이 확인되지 않았다.



한국에서는 2011년부터 군사 기관, 방위산업체, IT 업체 등 국내 주요 기관을 대상으로 한 지속적인 공격이 계속되고 있다. 2011년부터 2012년 사이에는 주로 국내 기관에 대한 공격이 집중적으로 진행되었으며, 2013년부터 2015년에는 국내 기업과 군사 기관까지 점차적으로 공격 범위가 확대됐다. 가장 최근인 2016년부터 2017년 사이에는 방위산업체와 연관 기업에 대한 공격도 확인됐다. 공격에 사용된 악성코드 종류는 다소 다르지만 동일한 C&C 서버를 사용하는 악성코드의 공격이 지난 2009년부터 존재해온 점으로 미루어 관련 공격 그룹은 오래 전부터 국내에서 활동했을 가능성이 있다.

비소날류 악성코드의 주요 공격 사례는 다음과 같다.



비소날류의 악성코드를 이용한 공격이 오랜 기간 동안 지속되면서 안랩을 비롯해 코세인크(Coseinc), 파이어아이(FireEye), 트렌드마이크로(TrendMicro) 등 국내외 보안 업체에서는 관련 내용을 수 차례 언급한 바 있다. 트렌드마이크로는 이를 '하트비트 APT(HeartBeat APT)'로 명명하기도 했는데 부 악성코드 내부에 'HeartBeat'라는 문자열이 존재하기 때문이다. 또한 2015년에는 마이크로소프트에서 하트비트 APT와 연관된 바이오아지흐 RAT(Bioazih RAT)에 대한 정보를 공개했다.

2015년 3월 안랩에서도 비소날 악성코드와 관련하여 군사 기관 공격에 대한 내용을 공개했다.

지금까지 살펴본 바와 같이 비소날 혹은 비스콘(Biscon)은 2011년부터 국내를 공격하고 있는 악성코드로 하트비트 APT와 비소날 변형인 바이오아지흐와 밀접한 연관성이 있으며, 이로 미루어 공격자는 특정 그룹이거나 공개된 소스코드를 이용한 다수의 그룹일 가능성이 있다.

자세한 내용은 ASEC 리포트 2017년 3Q (Vol. 88)를 참고하면 된다.

– ASEC 리포트 2017년 3Q (Vol. 88)

Source: https://asec.ahnlab.com/1078