S 리포트 | APT 보안-2부

지능형위협이 보안시장 변화… 허물어지는 경계

[디지털데일리 이유지기자]

최근 몇 년새 전세계 보안업계의 화두가 된 'APT'는 그 역사가 오래됐다. 지난 2001년 미국은 '9.11 테러'까지 거슬러 올려간다. 단순히 컴퓨터 해킹과 같은 수준의 전산시스템 공격을 이제는 국가 또는 반국가 집단, IS와 같은 테러집단이 선택할 수 있는 '테러' 전술(戰術)의 하나로 격상됐다. 즉, '대량살상 무기'와 같은 전쟁의 수단이 된 것이다. 일단 피해가 발생하면 그 강도가 이전과는 확연하게 차이가 된다.

더욱이 APT 공격의 종류와 범위가 모호하고, 실제로 공격이 현실화될 경우에는 치명적인 피해가 발생할 수 있다는 점에서 공포는 배가된다. 이는 한편으론 기존 보안시스템으로는 한계가 있을 수 밖에 없다는 의미이기도 하다.

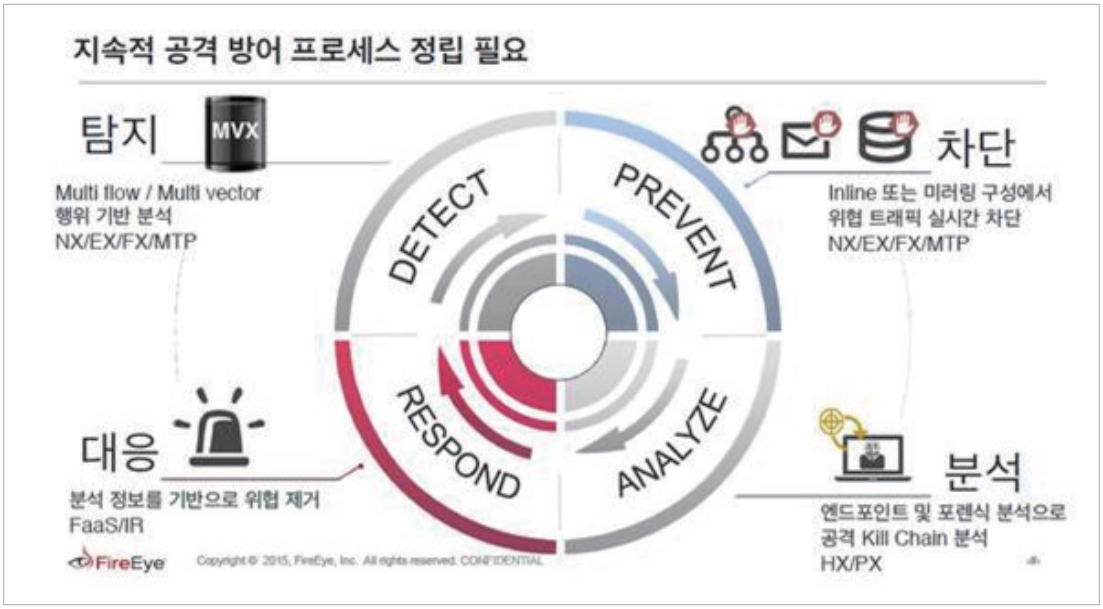
정부는 '사회 공공시설을 운용하는 공공(公共) 기간망의 경우 폐쇄형으로 운용되기 때문에 지나치게 우려할 필요가 없다'는 입장이지만 최근 한국수력원자력 해킹 사례에서 보듯이 APT 공격 수준으로 격상될 가능성은 언제든지 열려 있다는 게 전문가들의 지적이다.

이미 전세계적으로 화학공장과 발전설비, 상하수도시설, 교통시스템, 공공 및 금융시스템 등 대규모 기간시설과 사회 핵심시설에 대한 사이버공격이 크게 늘어나고 있는 것으로 보고되고 있다. 또한 주요 글로벌 보안업체들도 다양한 형태의 APT 공격을 지속적으로 대응, 업데이트하고 있다.

카스퍼스키랩은 올해 사이버 보안시장 전망과 관련, 사이버 범죄 집단이 기업화되면서 수익성을 극대화 할 방법을 찾고 있으며 자동제작 툴을 이용해 저렴하게 구입할 수 있는 악성코드를 이용해 대규모로 유포시켜 공격 성공률을 높이고 있다고 진단했다.

EMC도 보고서를 통해, 행동주의 해커집단과 사이버 공격의 목적이 더욱 다양해지고 있다고 분석하고, 산업기반시설의 보안위협이 최고조에 이르고 있다고 진단했다. 정치 · 사회적인

입장을 드러내기 위해 사이버 공격을 저지르는 핵티비스트, 금전을 원하는 공격자, 뛰어난 공격기술을 선보여 인정을 받으려 하는 등 공격 목표는 매우 다양해지고 있다고 밝혔다.



보안솔루션 전략 큰 변화, '통합' 중심으로 재편

지능형 지속 위협(APT)로 통칭되는 최근의 위협 트렌드는 위협 '차단'과 개별 솔루션 중심의 보안 시장을 완전히 뒤흔들었다. 사이버위협 '예방'과 '차단'이 가능 하다는 환상에서 벗어나 침입을 '인지'하고 '대응' 하는데 더욱 초점을 맞춰야 한다는 목소리가 보안업계에서 높아졌다.

대표적으로 엔드포인트단에서는 시그니처 기반의 안티바이러스(백신)가, 네트워크단에서는 방화벽과 침입방지시스템(IPS) 등의 한계가 지적됐다. 대신에 새로운 위협, 표적공격을 위한 특화된 위협과 침해흔적을 신속하게 탐지해 낼 수 있는 장치가 떠올랐다.

파이어아이가 시장을 개척한 가상화 기반 행위분석 기술인 '샌드박스'는 지능형위협을 탐지하고 대응하는데 있어 필수요소가 됐다. '샌드박스'는 의심스러운 행위를 하는 외부에서 유입되는 의심스러운 파일 등을 가상환경에서 미리 실행해보고 위협여부가 판단되면 차단 조치 하는 기술이다.

'시큐리티 애널리틱스(분석)'와 '위협 인텔리전스'의 중요성도 크게 강조되고 있다. 알려진 위협은 물론, 알려지지 않은 지능형 위협에 대응하기 위해서는 시시각각 발생하는 방대한 정보를 수집하고 서로 연관해 보다 신속하고 정확한 분석을 거쳐 의미있는 위협정보를 파악

해야 하기 때문이다. 정보를 수집했더라도 해당 정보가 잘못됐거나 즉각적인 조치가 필요한 심각한 위협인지 여부를 파악하지 못한다면 활용할 수 없다.

나아가 보안업체들 간, 정부와 민간의 협력 등 서로 위협정보를 공유하려는 움직임도 활발해졌다.

주요 보안업체들은 기존에 강점을 갖고 있는 주력 보안제품을 기반으로 샌드박스 기능과 보안 분석 솔루션을 추가, 연동 · 통합하는 등 지능형 위협 대응에 필요한 다양한 요소를 추가 · 확장하며 APT 보안 시장에 본격 뛰어들었다.

특히 위협이 들어오는 모든 길목과 제어지점을 아우르는 통합된 접근방식과 공격 라이프사이클 전체에 대한 지속적인 대응체계가 중요해지면서, 특화된 시장에서 강점을 보였던 보안업체들의 영역이 급격하게 허물어지고 있다.

전통적인 네트워크 보안 시장 강자인 시스코, 체크포인트, 팔로알토네트웍스, 포티넷은 엔드포인트 보안영역까지 확장했다. 파이어아이도 초창기에는 네트워크 영역에 집중해오다 엔드포인트 솔루션 출시했으며, 이 솔루션의 기능을 꾸준히 강화하고 있다.

전통적인 엔드포인트 보안 시장 강자인 시만텍, 인텔시큐리티(맥아피), 트렌드마이크로 등도 인수합병과 제품 확장으로 네트워크를 비롯해 모든 지점을 포괄하는 통합형 솔루션을 갖추고 있다.

국내 업체로는 일찌감치 APT 보안 솔루션을 출시한 안랩과 함께 최근 윈스가 가상머신을 이용한 악성코드 탐지 · 수집 기술을 탑재한 APT 보안 신제품으로 관련시장 공략을 강화하고 있다.

지란지교시큐리티는 강점을 가진 이메일 분야 기술 노하우를 바탕으로 다른 APT 보안 솔루션 업체들과 협력해 이메일 APT 보안 솔루션을 출시했다.

이들 국내 보안업체들도 위협 인텔리전스 확보를 위한 투자도 가속화하고 있다. 사이버위협이 한층 정교화되면서 앞으로 보안 솔루션 시장은 고유의 시장 경계가 사라지며 주요 업체들 간 경쟁은 앞으로 더욱 치열해질 전망이다.

〈이유지 기자〉yjlee@ddaily.co.kr