S 리포트 | APT 보안-1부

‘지능형 사이버위협’ 대응, 보안업계의 지상과제

[디지털데일리 이유지기자]

‘보안 솔루션, 통합적인 지능형 사이버위협 대응으로 통한다.’

지능형 사이버공격 방어는 현재 국내 뿐만 아니라 전세계 보안업계가 직면한 최대 과제다. 나날이 더욱 정교하게 진화하고 있는 지능형 위협을 완벽하게 차단하는 ‘마법’같은 솔루션은 상상조차 할 수 없는 상황이다. 이 때문에 보안솔루션의 진화 또는 대응 프로세스의 진화가 요구되고 있다.

이미 수차례의 치명적인 해킹 사고를 경험한 금융권의 경우, 이같은 지능형 사이버위협에 적극적인 대응에 나서고 있으며, 관련하여 금융보안원을 중심으로 범 금융권을 아우르는 통합보안관제시스템을 올해부터 본격 가동하고 있다. 통합금융보안기구인 금융보안원 설립 이전에는 은행, 증권 등 각 권역별로 관제시스템을 운영해 왔으나 이제는 통합보안관제센터 체제로 사이버위협에 대한 전체적인 대응력을 높였다.

금융위원회를 비롯한 금융 당국은 통합보안 관제센터를 통해 사이버 공격에 대한 효율적인 통합대응이 가능해지고, 관제대상이 중소 금융회사로까지 확대됨에 따라 보안사각 지대가 크게 축소됐다고 분석하고 있다. 아울러 통합 보안관제 대상을 지속적으로 확대하고 관제 시스템 고도화 작업도 지속적으로 추진해 나갈 계획이다.

지능형지속위협(APT)으로 대변되는 사이버 표적공격은 취약점을 파고들어 조직 내부 네트워크에 침투한다. 주로 '스피어피싱' 등 사회공학기법을 이용해 취약한 사용자를 노려 내부망에 침투해 거점을 확보하고 오랜 기간 정찰하면서 은밀하게 실제 공격 목표를 달성하기 위한 작업을 수행한다. 공격자가 기업 내부에 침입하기 위해 사용하는 악성코드와 공격도구는 알려지지 않은 제로데이 위협을 사용하거나 특정 기업만을 위해 제작된 새로운 방식을 이용한다.

공격자들은 조직 내 존재하는 보안 솔루션 등도 미리 우회하기 때문에 기밀정보를 유출하거나 시스템 파괴 등 손상을 입히는 목표를 달성할 때까지도 침해사실을 탐지하고 대응하기 어려운 상황이다.

실체 드러나지않은 사이버위협, 갈수록 증가

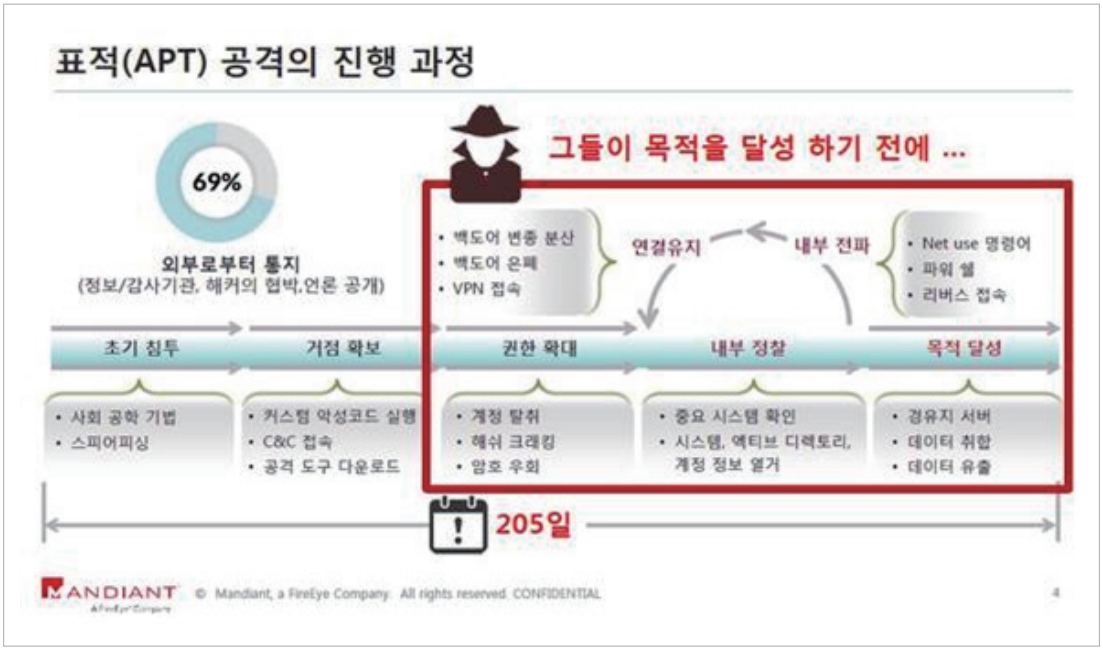
파이어아이에 따르면, 공격을 당해 피해를 입은 기업이 침해사실을 인지하기까지 평균 146일 걸린다. 작년에 집계된 이 수치도 그나마 2014년 205일에서 감소했다. 2012년에는 피해사실을 발견하기 전까지 공격자들이 기업의 네트워크에 머문 시간이 416일이나 됐다.

맨디언트 레드팀(Red Team)은 공격자들이 네트워크에 침투해 빠르면 3일 안에 도메인 관리자 크리덴셜(credentials)에 접근할 수 있다고 분석했다. 관리자 인증서나 접근권한이 유출되면 공격그룹이 타깃 정보에 접근하는 것은 시간 문제다.

침해 사실을 인지하는데 여전히 146일이나 소요되고 있다는 사실은 기업들이 사이버공격 피해를 최소화하는데 큰 어려움이 있다는 것을 보여준다.

더욱이 피해 기업의 절반(53%) 이상은 침해사실을 외부기관에 의해 발견하고 있는 것이 현실이다. 이 경우, 침해부터 탐지까지 평균 319.5일이 소요된다. 기업 내부에서 침해 사실을 탐지하기까지는 56일이 걸린다.

이에 따라 몇 년 전부터 보안업체들은 지능형 사이버공격을 효과적으로 탐지 · 대응하는데 주력하고 있다. 그러다보니 최근 들어 보안 솔루션 시장 경계도 급격하게 허물어지고 있다.



주요 보안업체들은 각자 집중해온 영역에서 탈피해 네트워크부터 엔드포인트까지 지원하는 보안 솔루션 영역을 대폭 확장하고 있다. 아울러 인텔리전스 기반의 통합적인 보안 솔루션으로 전환을 가속화하고 있다. 지능형 공격으로 인한 피해를 막기 위해서는 사이버위협에 대해 통합적인 대응체계가 마련돼야 하기 때문이다.

네트워크와 엔드포인트, 이메일 게이트웨이 등 위협이 들어오는 모든 길목과 제어지점을 포괄해 지속적인 차단(Prevent) · 탐지(Detect) · 대응(Respond)을 반복하는 프로세스가 필요하다. 모든 영역을 아우르는 '통합'된 접근방식에 대한 중요성이 강조되고 있는 이유다.

〈이유지 기자〉yjlee@ddaily.co.kr