<아산 칼럼>

‘사이버 암’ APT(지능형지속위협)에 대비돼 있나

안성규 전문위원

미국의 사이버 보안 회사 Blue Coat는 2014년 12월 ‘The Inception Framework: Clouded-hosted APT’라는 보고서를 공개했다. 지능형지속위협(Advanced Persistent Threat)을 의미하는 APT는 가능한 모든 소프트웨어, 네트워크, 시스템을 엮어 지능적·지속적으로 새롭게 활용하는 신개념 해킹이다.

보고서에 따르면 이 APT 는 클라우드 서비스를 활용해 러시아와 구 동구권 국가를 공격했다. 한 공격 사례를 단순화 해 보면 다음과 같다. 러시아 굴지의 은행장에게 ‘Miss World’가 아닌 ‘Mrs. World’라는 이름으로 메일을 보낸다. 미모의 여성 사진과 그럴듯한 초청장을 첨부해 클릭을 유도하고, 수신자가 이를 여는 순간 고도로 난독화(obfuscation)된 악성코드가 몰래 다운된다. MS 오피스 프로그램의 공개되지 않은 취약점을 이용한 것이다. 곧이어 가상 메모리가 열리면, 신형 2 진법 암호체계 등의 새 수법이 동원돼 은행장의 PC 를 좀비로 만들어간다. 상대방의 보안 프로그램이 알아챌 듯하면 변신을 거듭해 탐지망을 벗어난다. 그렇게 해서 여러 국가 중요 인물의 PC 가 공격자의 손에 들어간다. 이 APT 는 호스트는 불가리아·룩셈부르크·라트비아·우크라이나에, IP 는 20 개 나라에, 공격 계정은 스웨덴의 CloudeMe.Com 에 100 개 이상 두고, 목표 컴퓨터뿐 아니라 안드로이드나 블랙베리 같은 운영체제도 해킹했다. 글로벌 네트워크를 이용, 지능적·지속적으로 탈취된 정부, 외교, 정치, 군, 금융 관련 정보는 암호화돼 소리 없이 누군가의 수중으로 넘어갔다.

이 같은 APT 현실을 한국에 대입하면 걱정스럽다. 우리 사회가 국정원의 핸드폰 해킹 의혹 같은 사이버 문제에는 시끄럽지만 그 못지 않게 심각한 APT 엔 관심이 없어 보이기 때문이다.

APT는 특정인의 컴퓨터를 겨냥, 수단을 다해 교두보를 확보한 뒤 맞춤형 악성 프로그램이나 코드를 몰래 심고, 국가와 산업의 고급, 비밀 정보를 빼돌린다. 악성코드를 독감이자 사이버 테러라 한다면 APT는 사이버 암이자 저강도 사이버 전쟁이다.

2015년 4월 미국 보안업체 Fire Eye는 중국을 배후로 지목하며 APT-30을 공개했다. 2005년 이후 동남아 각국의 주요 네트에 침투해 정치·경제 정보를 빼간 사이버 공작이다. 미국 보안업체 Mandiant도 2013년 2월 중국이 2006년 이후 최소 141개 미국 기관에서 정보를 대거 빼갔다고 발표하면서 그 해킹 수법과 집단을 통칭해 APT-1으로 불렀다. 평균 356일, 길게는 1764일 간 정부, 군, 금융, 기술 정보를 탈취했다.

미국도 러시아, 중국, 이란, 파키스탄의 컴퓨터와 네트워크에 영구적으로 작동하고 탐지가 어려운 바이러스를 심었다는 보도가 올해 초 나왔다. 2013년 시리아 전자군(SEA)은 구글의 특정 프로그램을 사용하는 PC를 대상으로 광범위하게 공격했고, 이란도 2012년 사우디 국영 석유회사인 아람코와 카타르의 천연가스기업 RasGas를 공격했다고 한 연구소는 공개했다. 2014년 10월엔 'Pawn Storm 작전'이라는 이름의 APT가 2007년부터 미국, NATO, 유럽, 중동, 아시아의 군, 정부, 방위산업체로부터 정보를 빼갔다는 보도가 나왔다.

APT 공격은 금전적 이익을 위해 개인 정보나 금융 정보를 빼가는 보통의 해킹과는 질적으로 다르다. 보통의 해킹이 금융 질서를 훼손하고 개인에 피해를 주는 범죄이긴 해도 국가의 정보 주권까지는 건드리지 않는다. 미국 보안 회사 Trend Micro의 2014년 연간 보고서에 따르면 APT의 주 표적은 정부 기관으로 상반기 78%, 하반기 74%를 차지했다. Fire Eye는 정부, 금융, 첨단-하이테크, 텔레콤, 교육, 군, 항공, 에너지 등 '국가안보와 관련된 모든 정보'가 대상이라고 지적한다. 러시아의 보안 업체 카스퍼스키는 2012년 러시아, 카자흐스탄 등 옛 소련권을 대상으로 한 APT 공격 'Red October'를 발표했는데 대상이 정부 인사, 외교관, 대사관, 연구기관, 무역·통상부문, 군, 핵·에너지·오일 관련 기관 등이었다. APT는 국가의 현재와 미래의 먹거리에 필수적인 정보를 빼가고, 안보에까지 직·간접 위협이 될 수 있다.

한국도 이미 APT의 대상이다. Fire Eye가 2015년 발표한 APT-30 표적엔 동남아 국가뿐 아니라 한국도 들어 있고, 2013년 APT 보고서엔 Fire Eye의 고객(이름은 공개 하지 않음) 가운데 한국은 두 번째로 공격을 많이 받은 나라였다. 2014년 한수원 해킹, 2013년 3.20 사이버 공격 양상을 보면 북한도 APT 능력을 갖췄다고

봐야 한다.

ATP 대응에는 탐지-예방이 무엇보다 중요하다. 끊임없이 변신하며 치명적 정보를 빼가는 APT 의 위협을 국가적 과제로 격상해 대응해야 한다. 국제사회의 주요 사이버 보안 연구 기관들은 2014 년 이미 APT 를 주요 사이버 위협으로 지목했다. 이를 조금 복잡한 해킹이나 악성코드로 여기는 방식을 넘어 끈질기고 종합적인 탐지-대응체계를 마련해야 한다.

APT 탐지는 '건초더미에서 바늘 찾기'로 비유된다. 국제사회에서는 민간 연구기관이 우연히 발견하는 경우도 잦다. 민간, 정부의 개별 노력뿐 아니라 공동 노력도 필요하다는 의미다. 해킹 기술이 빠르고 교묘하게 진화하는 점도 국가 역량이 종합적으로 동원돼야 할 필요성을 보여준다. 지금까지 드러난 대부분 APT 공격이 국가가 후원하거나 국가와 사이버 세력의 결탁이라는 점도 고려할 필요가 있다. Fire Eye 는 2015 년 APT-29 사례를 발표했다. 러시아 정부의 후원을 받는 것으로 추정되는 이 APT 가 사용한 악성소프트웨어 HAMMERTOSS 는 알려진 기술을 새로운 방식으로 결합했을 뿐인데, 그럼에도 이 회사가 목격한 가장 강력한 백도어가 됐다고 평가했다.

여러 과정을 거쳐 APT 가 드러날 경우 배후를 가려야 하는데 이 귀속(Attribution)문제도 민-관이 협동할 영역이다. Mandiant 는 APT-1 의 배후로 중국 인민해방군 총참 3 부 2 국 산하 61398 부대를 꼽았다. 오랜 조사를 통해 사무실 위치, 관련 중국 정부 문서, 천 명 이상 일하는 건물, 해킹 방식, 훔쳐간 정보, 공격에 동원된 IP 의 주소지가 상하이 푸동에 있는 사이버 부대와 같은 점 등을 알아냈지만 혐의자를 Naming and shaming 하는 데 그쳤다. 현장을 잡을 수 없었기 때문이다. 배후를 잡으려면 첩보를 모으고, 필요하면 도청하고, 범인들의 컴퓨터나 핸드폰을 해킹하고 국제적으로 협력해야 한다. 정부와 민간이 협력해야 하는 이유다.

그런데 한국은 이 모든 것에 준비가 잘 안 돼 있어 보인다. 우리의 대응 체계가 개인정보 보호에 치중돼 있기 때문이다. 악성 코드나 APT 공격의 주요 진입로가 피싱 이메일 등을 통한 개인정보 탈취임을 감안하면 이런 조치가 일리는 있다. 그러나 APT 의 침입로가 이메일에서 웹으로 이동하는 최근 추세를 감안할 때

대응 방법도 달라져야 한다. APT 의 치명도가 보통의 해킹보다 훨씬 높다는 점은 특히 고려할 사항이다. 그 점에서 2014 년 APT 공격 대응 기술을 10 대 수출 전략 제품으로 만든다는 정부의 결정은 한가해 보인다. 올해 사이버 전문가가 청와대 안보 특별보좌관에 임명됐지만 APT 에 대한 사회적 관심을 높이는 노력도 눈에 띠지 않는다.

현재 사이버 위기를 다루는 주요 법령인 국가사이버안전관리규정은 대통령 훈령으로 중앙행정기관, 지자체, 공공기관의 정보 통신망에 적용된다. 그러나 APT 공격이 민간과 정부를 가리지 않는다. 사이버 강국들은 서로 APT 전쟁을 펼치고, 우리에게 공격이 언제 닥칠지, 또 어떤 게 이미 들어와 숨었을지 모른다. 그래서 평시-위기 모두 민-관이 유기적으로 연계돼 활동할 수 있게 하는 사이버테러방지법 같은 종합 체계가 필요하다. 그러나 사이버테러방지법 같은 것을 만들면 국정원에 인터넷 감시권을 주고 국민 사생활은 침해될 것이란 주장에 막혀 몇 년째 표류 중이다. 사이버 탐지는 필수이며, 사생활 침해 같은 부작용은 제도로 막으면 된다는 점은 거론조차 막히는 분위기다.

최근 해킹 프로그램 논쟁 과정에서 "국정원이 세계 해커들에게 호구가 될 것"이란 말이 나왔다. 그런데 APT 에 대응하는 우리 사회의 모습을 보면 앞으로가 아니라 이미 현실이 그렇게 돼 있는 것 아니냐는 걱정이 든다.