“보안 전제조건은 정확한 ‘스마트 데이터’ 분석·관리”

넷스카우트 아버(NetScout Arbor) 아라벨라 할라웰(Arabella Hallawell) 상무는 ‘지능형 사이버 위협 현황’에 대해 설명하며 사이버 위협은 맞서는 것이 아니라 얼마나 스마트하게 극복해내느냐가 관건이라고 사이버 위협 상황을 진단했다. 이에 기업 보안의 핵심 역할을 수행하는 스마트 데이터의 중요성을 강조했다. 한편 넷스카우트는 텍트로닉스, 아버, 플루크네트웍스, VSS 모니터링, 에어마그넷 등을 인수해 NPMD(Network Performance Monitoring and Diagnostics) 분야의 선두 입지를 고수하고 있고, 하이퍼스케일 데이터센터 분야에서도 글로벌 상위 공급사로 손꼽히고 있다. 〈강석오 기자·kang@datanet.co.kr〉

할라웰 상무는 “시시각각 진화하는 모습으로 나타나는 사이버 위협은 때로는 보유하고 있는 파괴력보다 더 큰 공포로 사람들을 두려움에 떨게 만든다”며 “앞으로 평화로운 사이버 시대는 더 이상 존재하지 않을 것이다. 사이버 위협은 맞서는 것이 아니라 얼마나 스마트하게 극복해내느냐가 관건이다”고 현재의 사이버 위협 상황을 진단했다.

DDoS 공격 위협 만연 … 매년 증가 추세

넷스카우트 아버가 올해 초 발표한 ‘전 세계 인프라스트럭처 보안 보고서’에 따르면 2017년에는 기업, 정부, 공공, 교육부문 사용자들은 실제 위협보다 최대 6배 이상 보안에 대한 위협을 느낀 것으로 나타났다. 지난해 사이버 공격의 특징은 해커들이 대규모 공격을 넘어 IoT 디바이스를 무기화해 활용하는 등 복잡성을 나타냈다. 특히 DDoS 공격으로 인해 매출 피해를 입은 기업은 전년 대비 2배 이상 증가할 정도로 매우 효과적이었고, 이는 DDoS 공격 위협이 도처에 만연해 있다는 것을 의미한다.

할라웰 상무는 지난 5월 1일 단 하루에 조사된 글로벌 위협 관련 자료를 예시로 제시하면서 현재의 사이버 위협의 심각성을 경고했다. 보고서를 보면 하루에만 총 115개 이벤트가 생성됐고, 132번의 공격이 이뤄졌으며, 17개의 멀티벡터 DDoS 공격이 감지된 것으로 나타났다. 특히 다양한 기술을 통해 짧은 시간에 다계층 또는 순차적으로 여러 계층에 공격이 이뤄지는 멀티벡터 DDoS 공격이 증가하는 것은 사용자들을 교란시키기 위한 위협이 그 만큼 진

화하고 있다는 것이다.

할라웰 상무는 "넷스카우트 아버의 ATLAS(Active Threat Level Analysis System) 인프라 데이터는 DDoS 공격이 2016년 680만 건에서 2017년 750만 건으로 증가했고, 2018년 가장 큰 규모의 DDoS 공격은 1.7Tbps에 이르는 것으로 나타났다"며 "올해 초 등장해 이론상 최대 5만배 패킷 증폭이 가능한 것으로 알려진 맴캐시드(memcached) DDoS 공격은 증폭/반사 및 DDoS 미티게이션 기능을 통해서만 효과적으로 대응할 수 있다"고 설명했다.

스마트 데이터, 기업 보안 핵심 역할 수행

할라웰 상무는 윈도우에서 IoT로 새로운 내부 공격이 시작된 부분도 지적했다. 지난해 2월 검색된 윈도우 씨더는 처음에 윈도우 기반의 시스템을 대상으로 하는 멀웨어에 불과했지만 방화벽 내부에서 IoT 기기로 확산되며 진화했고, 단일 윈도우 기기에서 광범위한 IoT로 감염시키는 모습을 나타냈다.

넷스카우트 아버가 조사한 사이버 공격의 타깃 분포도를 보면 개인사용자를 비롯해 금융, 클라우드/호스팅, 정부, 공공, 게임, 교육, e커머스, 겜블링, 제조, 헬스케어, 사회기간산업, 법률서비스 등의 순서로 많은 공격이 이뤄지고 있었다. 여기에 ISP의 22%는 네트워크에 연결돼 있는 IoT 디바이스에서 발생하는 공격을 경험했다고 응답했고, 사용자의 36%는 한 분기에만 클라우드 서비스를 대상으로 한 공격을 직접 확인했다고 말했다.

이처럼 위협은 다변화하고 있으며, 쉴 새 없이 진행되고 있다. DDoS 공격의 파괴력이 커짐에 따라 사용자들의 직접적인 금전 피해도 빠르게 늘고 있다. 넷스카우트 아버의 설문 응답자의 절반 이상은 지난해 2016년 대비 두 배에 달하는 10억~100억달러에 달하는 피해를 겪었다.

할라웰 상무는 "보안을 위한 전제조건은 '스마트 데이터'를 얼마나 정확하게 분석하고 관리할 수 있는지 여부"라며 "스마트 데이터는 실제 가치를 만들어낼 수 있는 양질의 데이터로, 빅데이터에서 정확하고 의미 있는 정보 추출과 세심한 분석 및 활용을 가능하게 하는 기술력이 필요하다. 즉 정확하고(Accurate), 실행 가능하고(Actionable), 민첩한(Agile)을 의미하는 이른바 3A 조건을 만족시켜야만 한다"고 강조했다.

> "스마트 데이터는 실제 가치를 만들어낼 수 있는 양질의 데이터로, 정확하고(Accurate), 실행 가능하고(Actionable), 민첩한(Agile)을 의미하는 이른바 3A 조건을 만족시켜야만 한다"

와이어 데이터와 스마트 데이터, 유기적으로 분석·관리해야

넷스카우트 아버 솔루션은 스마트 데이터를 기반으로 기업 내부에서는 아버 어드밴스 프로텍션 시스템으로, 인터넷에서는 아버 클라우드, 아버 위협 미티게이션 시스템, 아버 SP로 방어체계를 구현할 수 있다. 이들 모두는 넷스카우트 아버의 인텔리전스 플랫폼인 '아틀라스(ATLAS)'에서 구동된다. 아틀라스는 시간당 전 세계 인터넷 트래픽의 1/3을 측정할 수 있어 위협 관련 행위와 이를 기반으로 한 분석을 통해 최신 공격 정보를 수집한다.

넷스카우트 아버의 보안 솔루션은 스마트 데이터를 기반으로 DDoS 방어 및 보안, 서비스 보장, 가상화와 클라우드, 모바일 사용자 경험, 저비용 고품질 데이터 수집을 독창적으로 구현한다. DDoS 공격 조기 경보 시스템은 30개 이상의 봇넷을 관찰해 보안 엔지니어링 대응팀(ASERT)의 봇넷 추적 프레임 워크와 C2 활동을 포착하도록 설계된 봇 에뮬레이터 리플리컨트(Replicants)로 추적한다.

이후 탐지된 봇넷 명령을 수집하고, 세심히 검토한 후 위협 요소가 일치하는 경우 세부 내역을 사용자의 이메일로 통보해 준다. ATLAS 인텔리전스(AIF)는 DDoS 레퓨테이션 위협, 명령 및 제어, 멀웨어, 위치 기반 위협, 이메일, 표적, 모바일 등 다양한 공격을 방어한다.

할라웰 상무는 "보안의 관건은 애플리케이션 딜리버리 체인을 구성하는 L2~7 데이터인 와이어 데이터와 스마트 데이터를 얼마나 유기적이고, 효과적으로 분석 및 관리하느냐에 달려있다"며 "실시간 인텔리전스 배포, 보호 기능 딜리버리, 고성능 애플리케이션 및 서비스, 탁월한 사용자 경험 제공, 지능형 사이버 및 DDoS 공격 위협을 탐지 및 수정 등의 기능은 필수다"고 강조했다.