

[취재] 2011 하반기 넷이벤츠 인터뷰 VIII : 팔로알토 네트워크

[종목] 컴퓨터 [분야] IT일반 [작성자] 류재용 [작성일] 2011.11.20. 13:35

2011년 11월 16일과 17일 양일 간의 일정으로, 태국 푸켓 소재 인디고 펄 리조트(Indigo Pearl Resort, Phuket, Thailand)에서 '2011 넷이벤츠 아시아태평양 기자간담회(2011 NetEvents APAC Press Summit, 이하 넷이벤츠)'가 개최되었다. 지난 4월에 열린 상반기 행사에 이어 열린, 11월 정례 하반기 행사다.

넷이벤츠는 통신 및 네트워크, 보안 기업의 C 레벨 임원들과 관련 시장조사기관이 한 자리에 모여 업계 동향 및 각 기업의 전략 등을 소개하는 정기행사다. 이번 행사에서는 엔터프라이즈 네트워킹, IT 보안, 무선 기술, 영상 회의, 클라우드 컴퓨팅, 차세대 통신망, 통신 인프라 등 업계 이슈에 관한 기업 및 시장 조사기관의 발표와 패널토론 등이 진행되었다.

17일 넷이벤츠의 오후일정은 업계 주요 인사들과의 인터뷰 시간으로 할애되었다. 아크로팬은 이 자리를 통해 2011년도 하반기 넷이벤츠 기조연설자로 나선 팔로알토 네트워크 창업자 겸 CTO인 니르 주크(Nir Zuk)에게 궁금했던 사항을 물어볼 수 있었다.



▲ 팔로알토 네트워크 창업자 겸 CTO 니르 주크(Nir Zuk)

Q1. 앞서 블루코트 시스템즈 인터뷰에서, 그들은 시그니처는 리액티브한 보안으로 사후조치라며, 페이스북 레이디가가 페이지 보안사건을 예로 들어 소셜 네트워크를 통한 멀웨어 전파를 절대로 막지 못한다고 말했다. 이런 견해에 대해 어떻게 생각하는가?

일단은 복수의 기가비트 속도로 돌아가는 것을 감지하기 위해서는, 시그니처 외에는 감지할 수단이 없다. 고속으로 돌아가는 것에 대해서 감지하는 다른 매카니즘은 개인적으로 알기로는 없다. 프록시를 가지고는 그렇게 빠르게 돌아가지 않는다. 이는 초당 100메가비트 이상 속도면 몰라도 그 이하 속도는 못한다. 그래서 시그니처 이외의 것으로는 감지하기 어렵다. 여기에서 중요한 것은 시그니처를 어떻게 생성하는가 하는 것이다. 전통적인 시그니처를 생성시키는데에는 많은 시간이 걸렸다. 사후약방문이라는 말이 맞다. 그래서 와일드파이어는 휴리스틱스를 이용해 공격을 감지한다. 그 다음에 신속하게 시그니처를 생성해 고속으로 차단할 수 있다.

페이스북에서의 레이디가가 보안이슈를 이야기하자면, 표적공격이 아니라 많은 유저들 공격했던 사례다. 와일드파이어는 표적 공격 위한 것이다. 아주 적은 빈도로 발생하는 공격을 차단하겠다는 것이다. 그래서 타사와 이야기하는 것과 우리가 이야기하는 것은 그런 측면에서 차이가 있다. 이처럼 널리 퍼진 많은 유저 공격을 보면, 데미지 자체는 크지

않다. 이러한 때에는 신용카드 정보를 빼거나, 톨바를 설치하거나, 스파머로 이용하거나, 비아그라를 사라고 하거나 하는 그런 경우들이다. 그런데 표적공격은 그야말로 위험한 공격이다. 많은 돈을 손실보게 하거나 데이터 손실을 보게 하거나 고객 리스트를 빼가는 등의 심각한 것이 표적 공격이다.

Q2. 미국 Spot.US 데이비드 콘 디렉터가 한국에 왔을 때 미디어 플랫폼, 웹서비스 해킹에 대해 이야기 나눴던 적이 있다. 미국은 한국과 달리 중국발 해킹이 매우 덜한 편이라고 들었다. 그런데 어제 기조연설에서 '프로젝트 오로라'를 이야기하며 슬라이드에 중국 지도와 국기까지 내걸기도 했는데, 중국발 해킹에 대해 어떻게 생각하는가?

일단은 해킹과 관련해서는 어떤 국가가 어떤 국가 공격하는 건 그 분야 전문가가 아니라서 말 못한다. 구글에서 구글 사건과 관련해 중국에서 관련되었다고 그래서 그 이야기를 한 것이다. 이번 주에 발표한 것 또 하나를 관련해 이야기하자면, 보안은 모바일까지 확장한다는 것이 있다. 아이폰, 아이패드까지 확장된다. 와일드파이어에서 제공하는 수준의 보안은 모바일 유저가 전세계 어디에 있던 그 수준에 준하는 보안을 제공할 것이다.

Q3. 시만텍, 안철수연구소 등이 한국에서 개최한 행사들에서 APT 공격을 이슈로 다뤄지면서 패키지, 솔루션들이 선보여지고 그랬다. 엔터프라이즈에서 컨슈머 레벨까지 따로 협업하는 일이 있는가?

그들은 데스크톱 보안회사라고 말할 수 있다. 자사는 네트워크 보안회사로 보완적인 위치의 회사다. 자사는 엔터프라이즈 시장에 포커스를 맞추고 있다. 엔터프라이즈 시장에만 포커스를 맞추겠다고 하는 이유는, 자사가 높은 수준의 지원을 제공하기 위해서다. 작은 고객들이 많으면 높은 수준의 고객지원을 할 수 없어서 지금처럼 집중하기로 결정했다. 소규모 고객들은 비용에 민감해 UTM을 많이 쓴다. 반면 대기업들은 차세대 방화벽을 많이 구매한다.