



http://www.parkoz.com/zboard/view.php?id=contentsagent&page=1&sn1=&divpage=1&sn=off&ss=on&sc=off&select_arrange=headnum&desc=asc&no=1619

[취재] 넷이벤츠 기초연설 : 니르 주크 CTO

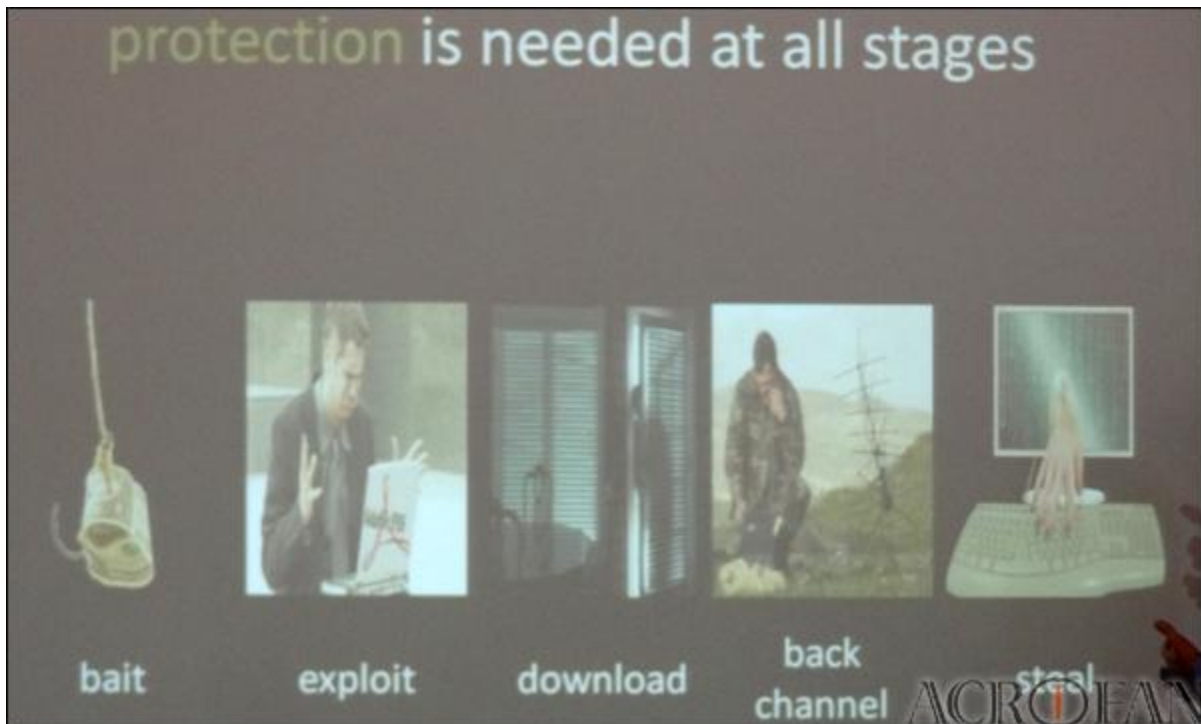
2011년 11월 16일과 17일 양일 간의 일정으로, 태국 푸켓 소재 인디고 펄 리조트(Indigo Pearl Resort, Phuket, Thailand)에서 '2011 넷이벤츠 아시아태평양 기자간담회(2011 NetEvents APAC Press Summit, 이하 넷이벤츠)'가 개최되었다. 지난 4월에 열린 상반기 행사에 이어 열린, 11월 정례 하반기 행사다.

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.

2011년도 하반기 넷이벤츠의 첫 세션이자 기초연설 순서는 팔로알토 네트워크 설립자 겸 CTO 니르 주크(Nir Zuk)가 진행했다. 그는 방화벽 등 네트워크 보안장비 시장의 개척자 중 한 명으로 저명한 인사. 그는 최근의 보안 위협 동향과 자사의 솔루션 소개에 주안점을 두었다.



▲ 팔로알토 네트워크 설립자 겸 CTO 니르 주크(Nir Zuk)



▲ 일명 APT(Advanced Persistent Threat) 공격은 크게 다섯 단계로 구성된다.

RSA, Sony, Epsilon 등 올해 이슈가 되었던 대형 보안사고들을 소개한 니르 주크 CTO는 새로운 멀웨어 공격이 대두되면서 기존 기술로는 공격을 막지 못했다는 점을 지적했다. 이는 공격자들이 실 데이터를 원함에 따라, 과거와 같이 데이터센터를 공격한다거나 대규모 컴퓨터를 동원한다거나 하는 양태에서 벗어나 엔드유저를 핀포인트로 공략하는 전략 및 전술이 실천함에 따른 것이다. 수백만 달러 인프라를 공격하는 게 아니라, 조직 내 희생자 1명을 노리는 셈.

예전에는 해커들이 재미삼아 공격을 자행하곤 했다. 그러나 지금은 국가 단위나 조직범죄단체 등이 주요 공격집단으로 추정되는 시대다. 이처럼 공격자들의 수준이 더욱 더 위협적이 됨에 따라, 5단계 방법론이 공격방식으로 고착화되고 있다.

1단계로, 스피어 피싱 형태의 공격이 이루어진다. 여기에서는 플래시, 영화/음악 파일, 웹사이트 방문 유도, 문서 열람 등을 통해 개인을 노린다. 대상자의 링크드인, 페이스북, 트위터 등을 조사해서 해당 타겟의 취향을 파악해 이메일, 메신저, 페이스북, 드롭박스 등 여러 애플리케이션 방식으로 보내기도 한다. 엔드유저와 그의 친구들을 파악하고 그들이 신뢰하고 열만한 문서를 보내 노리는 것이다.

2단계에서는 알려지지 않은 보안 취약점을 지닌 문서 파일 등으로 엔드유저를 노린다. 아주 조그만한 코드가 머신에서 동작하게 되는데, 이를 통해 해킹 전초단계가 성립된다. 이를 업계에서는 'Exploit'이라고도 부른다.

3단계에서는 'Exploit'이 인터넷에서 큰 프로그램 파일을 다운로드 받아 설치한다. 이 단계를 지나면 4단계인 백 채널 레벨에 들어선다. 여기에서는 백도어가 생성된다. 이 백도어가 연결선(Back Channel)을 생성시키는데, 이를 통해 공격자가 네트워크에 들어온다. 그 다음 5단계에서 공격 또는 탈취 또는 둘 다가 벌어진다.



▲ 소셜 네트워크 서비스 및 애플리케이션은 보안담당자 입장에서는 말 그대로 '재앙'

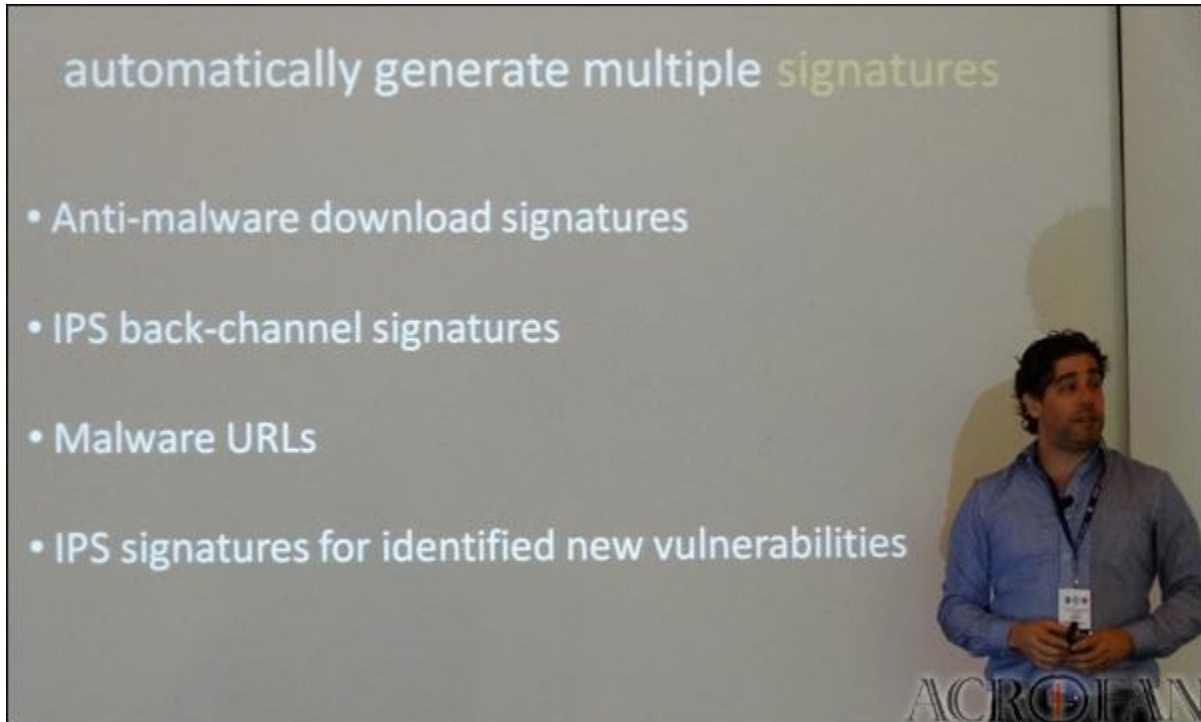
니르 주크 CTO는 공격에 대한 보호책을 마련하기 위해서는 각 단계에서 보호 방어가 필요하지만, 각 단계에서 또 그 어떤 단계에서도 아주 잘 보호되는 것은 없다는 현실을 지적했다. 먼저 'Bait Protection'은 거의 불가능하다고 언급했다. 공격자가 엔드유저로 하여금 문서를 열게 만드는데, 이는 막는 것이 불가능하다. 사용자가 문서를 못 보게 한다는 것이 불가능하기 때문이다.

'Exploit' 레벨에서 나쁜 문서를 받는 것을 막는 방법이 강구되는데, 여기에서 침입방지시스템(IPS)가 제 역할을 하느냐는 문제점이 대두된다. 현재 IPS는 이메일 정도나 스캐닝하는 수준인데, SNS 트렌드 감당에는 취약하다. 특히 공격의 양과 질이 폭증하는 현실에서, IPS가 즉시성, 시의성을 가지고 보호여건을 만드는 부분은 특히 어려운 부분이기도 하다.

그는 일례로 '프로젝트 오로라' 사례를 언급했다. 이는 구글, 모건스탠리 등이 공격당했던 것으로, 공격자로 중국 정부가 큰 의심을 받고 있는 사안이다. 이 공격은 2010년 1월 중반 중에 팔로알토 네트워크에서 알게 된 익스플로어 취약점 문제였는데, 공격 감지 4개월 전에 보고된 부분이었다. 그런데 보고 이후로도 IPS 조치가 없다가 사고가 난 다음에 조치가 이루어졌다.

'Download'는 Exploit 성공 이후에 프로그램 다운로드가 발생하는 것과 관련이 있다. 이 때부터는 백신이 방어해줘야 된다. 여기에서도 IPS와 마찬가지로 문제가 나온다. 아주 짧은 치명적인 인스턴스가, 게다가 재차 발생하지 않는 공격이 나오는데, 이를 백신 벤더들이 방어하는 것은 지극히 난해한 문제다. 주로 아주 많은 공격이 있어야 공격으로 정의하고 대응하는 패턴이 일반화되어 있는데, 그러기에는 너무나 지엽적인 사안이 된다. 게다가 이를 연구할 인력 자체도 부족한 것이 현실이다.

'Back Channel'은 핀포인트 어택으로 인해 여러 단계를 거쳐야만 IPS 시그니처가 나오는 특성과 연관이 깊다. 게다가 백채널들은 암호화되어 있는데, 이러한 대부분의 암호화 시그널은 IPS들이 감지를 잘 하지 못한다. 이 다음 단계인 'Explore and Steal' 레벨에서 보호 솔루션으로 나온 것들은 대개 엔터프라이즈 엣지 레벨을 보호하는 형태다. 그런데 현대 멀웨어들은 이런 것에 상관하지 않는다. 대부분의 네트워크는 외부만 보호하고 내부는 보호하지 못하는데, 공격자는 내부 희생자를 백도어로 삼아 네트워크 상에 올라가는 것만 노린다.



▲ '자동화'를 추진하는데 있어서, 주의해야 될 부분이 네 가지로 정리되어 소개되었다.

니르 주크 CTO는 "현대 기술은 타겟팅 기술을 다 알지도 못하고, 방어책 부분도 충분한 시간 내에 내놓지 못하고 있다"고 말했다. 특히 고객들은 장비를 옛지 레벨에서는 쓰고 있으나, 유저는 보호하지 못하고 있다고 지적했다. 이러한 환경에서, 모든 애플리케이션에 보호책이 적용될 수 있어야 된다고 부연했다.

그는 특히 대응시간이 매우 중요하다고 언급했다. 통상적으로 시그니처 확립과 배급에 2개월 가량 걸리는데, 현실은 1주일도 길다. 특히 타겟팅 공격은 분석할 것이 너무 많고, 모든 네트워크 트래픽을 각각 다 분석해야 한다는 부담이 있다. 또 단 1번, 단 1명이 들어가면 네트워크가 와해된다는 문제점도 있다. 여기에서 대안으로 제시된 것이 '자동화'다. 프로세스 자체(오브젝트 분석-대응)를 자동화시켜야 주장이다.

팔로알토 네크웍스의 솔루션은 '샌드박스'가 코어가 된다. 모든 걸 새롭게 인스톨이 된 버츨머신 안에서만 동작시키고, 머신에서 어떤 일이 벌어지는지 조사한다. 머신에 어떤 걸

인스톨하지 못하면 공격이 성공하지 못함을 주목한 방법론이다. 샌드박스로 전 과정을 관제할 수 있다면 공격 방지가 가능하다고 보는 것이다. 또 시그니처를 만드는 프로세스를 자동화시켜 수천 수만에 이르는 버찰머신들을 커버하는 것이 데이터센터 레벨에서 중요해질 것이라고 전망했다.

한편, 자동화 이점과 주의점으로 네 가지가 소개되었다. 안티 멀웨어 다운로드 시그니처, IPS 백채널 시그니처, 멀웨어 URLs 등이 특히 주목해야 될 포인트로 소개되었다, 이어, 어떤 취약성이 이용되었는지, 어떤 시그니처가 필요한지 등을 파악하는 데에는 보안전문가 꼭 필요하다는 현실적인 여건도 언급되었다.



▲ 팔로알토 네트워크는 차세대 '와일드 파이어'를 주력으로 밀고 있다.

니르 주크 CTO는 일련의 프로세스를 자동화시키면 대응시간을 1시간으로 단축할 수 있다고 말하고, 전통적인 방식으로는 2개월 이상 소요되는데에서 발생하는 보안위협을 자사 솔루션으로 대처할 수 있다고 주장했다.

여기에 더해 자동화 방법론이 차세대 방화벽에 일부로 들어가게 위해서는 솔루션은 전사적으로 방화벽이 있는 모든 곳에 있어야 된다는 점과 인 라인으로 들어가 트래픽 안에 디플로이 되어야 실행이 되어야 된다는 전제를 설명하고, 자동화 방법론이 실시간으로 고속으로 차단해야 되기 때문에 통합된 IPS와 안티 바이러스 체계가 필요하다고 덧붙였다.

한편, 팔로알토 네트워크가 공급하고 있는 '와일드 파이어'의 차세대 서비스는 자동화 방법론을 채택한 클라우드 서비스로 구축되고 있다. 이는 앞서 주장된 자동화 방법론이 접목되어 있다. 스위치를 키기만 하면 오브젝트를 보내주고, 새로운 Exploit 또는 어택을 바로 경고해주는 기능을 담고 있다.

이렇게 만들어진 배경에는 와일드파이어 베타테스트 경험이 컸다. 니르 주크 CTO에 따르면, 소수 고객들이 솔루션을 테스트했을 때, 몇 달 동안 700여개의 멀웨어 패밀리가 나왔다. 이중 57%는 당시 전통적인 안티바이러스나 방화벽으로는 탐지 못하던 것이었고, 이를 탐지하고 나서 다른 벤더들 소프트웨어로 체크해 보니 탐지한 것 중 57%는 전혀 탐지 못하는 경우였다. 차세대 와일드파이어는 이런 경험을 바탕으로 제작, 튜닝되고 있다고 소개되었다.