등잔 밑이 어두운 내부 보안! 시스코 스위치로 환히 밝히세요(2)

시스코 코리아 엔터프라이즈 네트워크 솔루션 스페셜리스트 이창주 수석

지난 이야기에서 잘 나가 기업의 개인정보 유출 사건을 살펴보았습니다.

이번 이야기에서는 어떻게하면 알지 못하고 당하는 이런 보안 사고를 미연에 방지할 수 있을지 살펴보도록 하겠습니다

위의 그림을 가만히 들여다 보면 해커가 처음 멀웨어를 유입시키고 마지막으로 데이터를 유출하는 단계 사이에 여러 과정을 거치고 있음을 알 수 있습니다. 처음부터 DB 관리자의 계정과 비밀번호를 알고 있다면 몰라도, 그렇지 않은 경우 해커들은 최종 데이터를 접근하는 단계까지 가는데, 아주 조심스럽고 은밀하게 탐색을 하게 됩니다. 일단 이렇게 기업 네트워크 경계를 통과한 내부에서의 움직임들은 경계 보안 제품(방화벽, IPS 등)으로는 잡아내기가 매우 어렵겠죠? 그렇다고 또 이런 위협을 막겠다고 고가의 경계 보안 제품들을 내부 네트워크 전체에 설치한다는 것은 비용이나 관리 측면에서 현실적이지도 않습니다. 그럼 우리는 어떻게 이런 내부에서의 움직임을 정확히 파악할 수 있을까요?

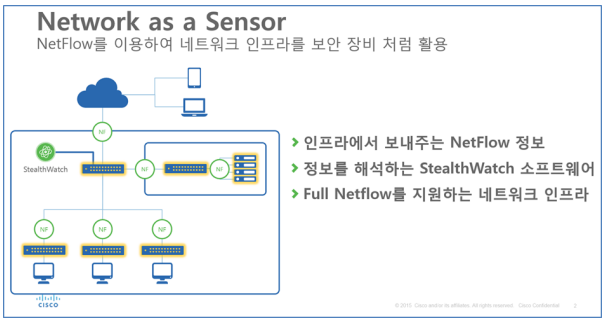
사실 우리에게는 이 모든 행위들을 샅샅이 볼 수 있는 굉장히 좋은 시스템을 이미 가지고 있습니다. 바로 이런 움직임들이 벌어지고 있는 그 곳, 즉 내부의 네트워크이지요. 위에서 보이는 모든 중간 단계들은 바로 내부 네트워크를 통해 이뤄지게 됩니다. 만약 네트워크를 단순히 통신 시스템이 아니라 커다란 보안 시스템으로 변신 시킬 수만 있다면 내부에서 일어나는 이런 이상 현상들을 모두 잡아 낼 수 있지 않을까요?

물론, 예전에도 그런 노력이 없었던 것은 아닙니다. 소위 말하는 패킷 캡처 툴(또는 "프로브")를 곳곳에 설치하고 모든 네트워크 링크에 탭(Tap)을 달아서 내부 패킷들을 일일이 검사를 하는 것이지요. 하지만 이런 방법은 보안적인 측면에서 그다지 성공적이지 못했습니다. 이유는 데이터 전체를 캡처하는 프로브의 경우 용량이 어마어마하게 커야 했고, 또한 캡처된 패킷들을 보안적인 관점에서 제대로 해석할 방법도 없었던 것이죠. 하지만 더 큰 고충은 이런 프로브를 네트워크 전반에 다 설치하는 데 드는 어마어마한 비용 때문이었습니다.

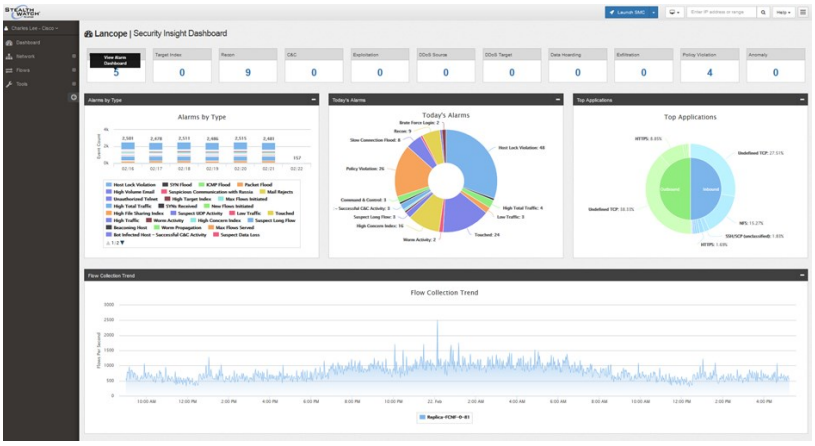
그래서 시스코에서는 이렇게 네트워크와 프로브로 구성되는 내부 보안 접근 방식을 대신할 새로운 솔루션을 내 놓았는데, 그것이 바로 Netflow 프로토콜을 이용하여 네트워크를 보안 센서로 동작하게 하는 NaaS, 즉 **Network as a Sensor** 솔루션입니다.

이 Network as a Sensor는 아래의 세가지 요소로 구성된 솔루션입니다.

- 시스코 Netflow 프로토콜
- Full Netflow가 지원되는 네트워크 스위치, 라우터, 무선랜 컨트롤러
- Netflow 정보를 모으고 분석하는 StealthWatch 소프트웨어

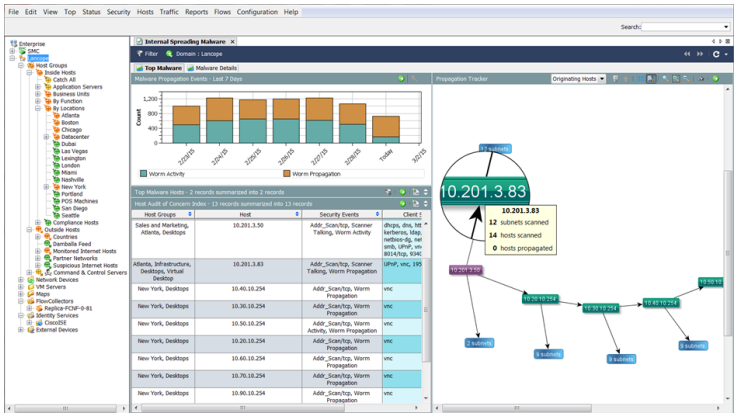


NaaS가 동작하는 방식은 이렇습니다. 기업 내부에 설치된 스위치, 라우터에서 Netflow를 이용하게 되면 그런 장비들이 처리하는 모든 플로우 정보를 StealthWatch 플로우 컬렉터(FlowCollector)로 보내주게 됩니다. 이 Flow Collector는 수집된 단방향 플로우 정보를 사용자가 잘 볼 수 있는 양방향 세션으로 구성을 하게 되고, 중복된 플로우나 NAT된 플로우들을 정리해 줍니다. 이렇게 정리된 플로우 정보는 StealthWatch의 관리 콘솔(SMC)에서 보여지게 되는데, 이 SMC에서는 단순히 플로우 정보를 확인하는 것뿐 아니라, 플로우 정보들을 갖고 있는 내부 보안적 측면에서의 의미까지도 해석해서 보여줍니다. NaaS 솔루션을 이용하여 내부 플로우들을 분석하기 시작하면 DDoS (Distributed Denial of Service) 공격의 전조 증상, 데이터 유출을 위한 사전 수집 단계, 실제적인 데이터 유출 단계들을 감지해 낼 수 있고, 관리자는 SMC가 제공하는 대시보드를 통해 한 눈에 확인을 할 수 있게 됩니다.



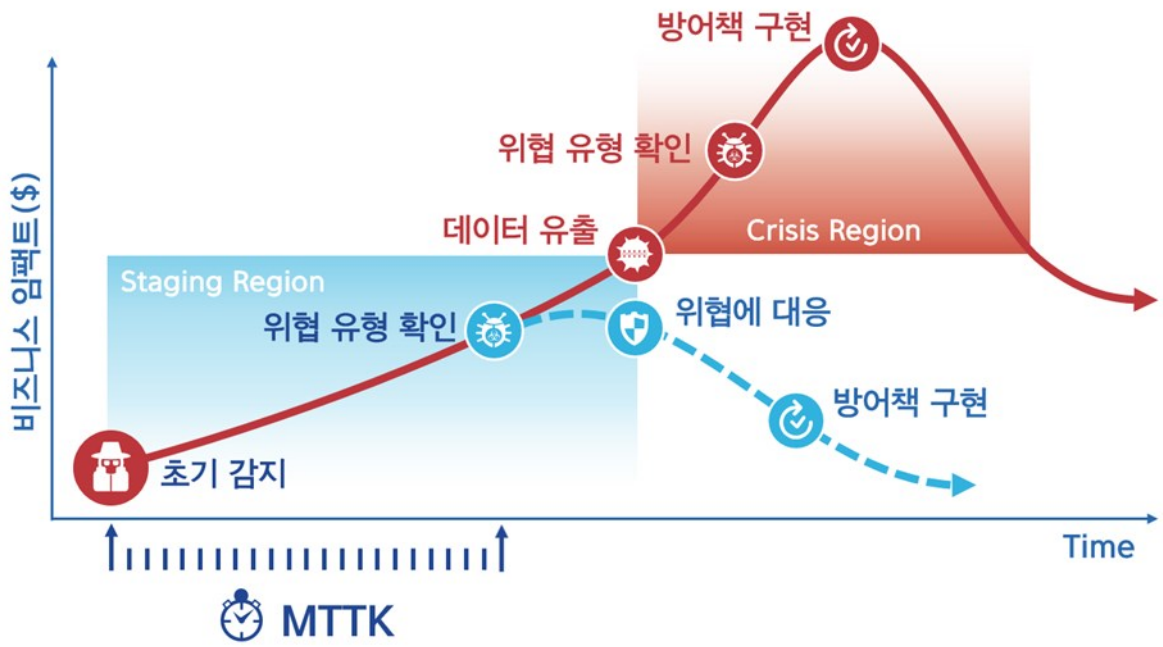
그럼 이 NaaS를 사용하기 위해서는 어떻게 시작을 해야 할까요?

바로 Netflow를 고성능으로 처리할 수 있는 좋은 스위치가 필요합니다. 바로 시스코 Catalyst 3650과 3750, 4500의 Sup-8, Catalyst 6800/6500의 Sup-2, 그리고 Nexus 7000의 M 타입 모듈이 바로 이 Netflow를 고성능으로 처리하는 ASIC(UADP ASIC)을 탑재하고 있습니다. 이런 스위치들은 Netflow를 종전과 같이 샘플 방식(Sampled)으로 처리하는 것이 아니라 모든 플로우에 대해 Netflow 정보를 생성하기 때문에 보안 분석에 활용할 수 있는 충분한 가시성을 제공하는 것이지요. 만약 여러분께서 이미 이런 스위치를 사용하고 계시다면 추가로 필요한 항목은 StealthWatch 소프트웨어입니다. 이 StealthWatch는 앞서 설명드린 대로 FlowCollector와 Monitoring Console 즉, SMC로 구성이 되어 있고 하드웨어 어플라이언스 타입 또는 VM(Virtual Machine) 타입 두가지로 제공되고 있습니다.



자, 이제 여러분의 네트워크에 Netflow를 켜고 이 Netflow 정보를 StealthWatch로 보내주는 것 만으로 여러분의 네트워크는 이미 거대한 보안 센서로 동작을 시작하게 될 것입니다. 잠깐만요! 그럼 지금 쓰고 있는 스위치들이 위에 나와 있는 종류가 아니면 또는 타 사의 스위치를 사용하고 있다면 지금까지 설명한 NaaS 솔루션을 사용할 수 없나요? 결론부터 말씀 드리면 그런 환경에서도 NaaS를 쓸 수 있습니다! 다만 추가적으로 FlowSensor라는 별도의 툴을 사용해야 하는데요, 이 FlowSensor를 각 스위치에 연결해 주면 스위치 대신 Netflow를 대신 생성해 주기 때문에 이 NaaS를 사용할 수가 있지요.

자, 이제 다시 한 번 김똑똑 사원의 이야기로 돌아가 볼까요? 급속히 변화하는 IT 환경에서 외부 위협에의 노출(attack surface)은 갈수록 넓어져 가고 해커들의 공격은 점점 더 지능화 되고 집요해 지고 있습니다. 김똑똑 사원의 의도하지 않은 클릭 한 번으로 해커는 쉽게 잘 나가 기업에 침투할 수 있었지만, 침투 후 발생하는 여러가지 데이터 유출의 전조 증상들을 조금만 더 빨리 알아차릴 수 있었다면 이런 큰 사고는 막을 수 있지 않았을까요?



실제로 위협을 알아차리는 데 걸리는 평균 시간(Mean Time To Know)는 실제로 비즈니스에 대한 해킹의 실제 영향을 최소화 하는 데 매우 중요한 요소가 됩니다. 실제로 보안 위협에 대응하는 전체 시간 중에 이 MTTK가 70%까지 차지한다고 하니, 이 시간을 줄이는 것이 실제로 해킹의 피해를 줄이는 데 매우 중요한 요소가 됩니다.

경영학의 아버지로 잘 알려진 고 피터드러커가 경영에 대해서 이런 말을 했죠? "측정할 수 없는 것은 관리할 수 없다.(You can't manage what you can't measure)" 보안에 있어서도 마찬가지입니다. "볼 수 없는 것은 막을 수 없다.(You can't protect what you can't see.) 그동안 경계 보안/관문 보안에 밀려 잘 신경 쓰지 못했던 여러분의 내부 네트워크 보안, 과연 여러분은 얼마나 잘 보고 얼마나 잘 알고 계신가요? 시스코 NaaS 솔루션으로 여러분 내부 네트워크를 환히 밝혀 볼 수 있다면 얼마나 좋을까요?