DDos 문제의 핵심과 변화 (에스토니아, 7.7)

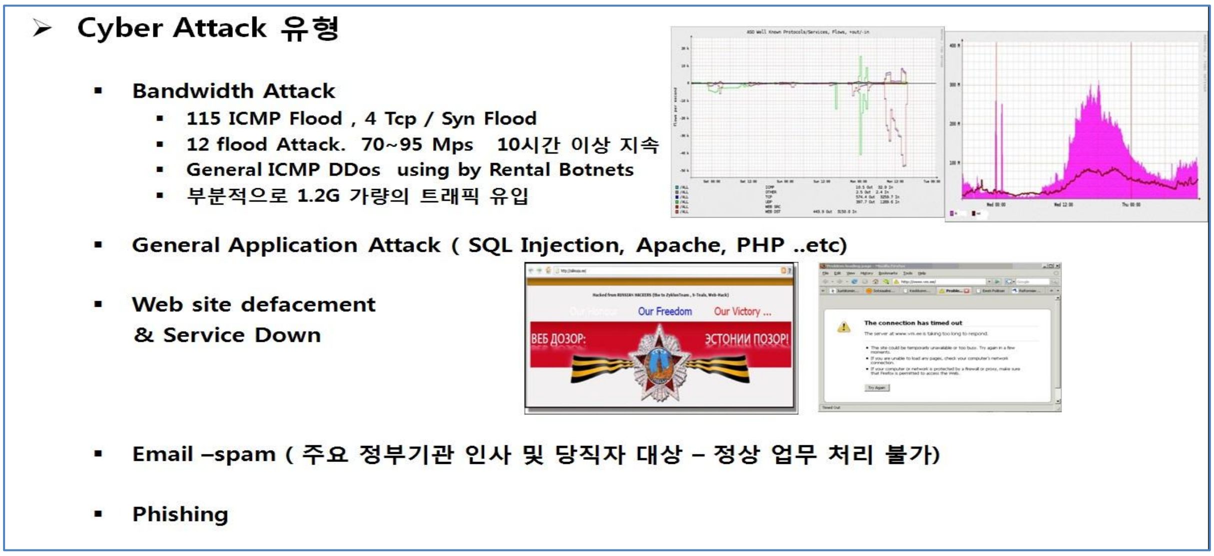
7.7 DDos 관련된 의견들이 1년이 지난 지금 시점에 다시금 많은 분야에서 회자 되고 있다. 문제에 대한 분석과 적절한 대응 체계에 대한 논의가 계속 되고 있는 시점에 DDos 논란의 핵심은 무엇인가 하는 명제에 대해서 명확한 설명은 아직 잘 설명 되지 않고 있는 듯 하다.

DDos에 대한 핵심적인 이해 분야에 대한 접근 방법도 상이한 점이 많이 있다. 공격 주체는 분명히 개인의 PC이며 공격을 받는 대상은 기업 및 기관의 서비스를 대상으로 하고 있다. 그러나 현재 논의 되고 있는 대책의 대부분은 공격 받는 대상의 보호대책을 강화하는 측면에만 머물러 있다. DDos 대응 장비의 도입과 체계의 도입은 단기적으로 타당한 방향이다. 그러나 근본적인 원인 제거를 하지 않는 다면 미봉책에 머물 뿐이다. 공격자들은 보다 더 많은 공격자원을 더 은밀하게 모집하고 더 대량의 자원을 동원하여 공격을 할 것이다. 실제로 은밀하게 모집 하려고도 하지 않는다. 일반적인 웹 서비스를 해킹하여 악성코드를 사용자 PC에 설치하는 행위는 너무나도 일반적으로 발생하는 현상일 뿐이다.

DDos 공격에 대해 보다 더 많은 대응자원을 투입하고 대응 실무인력을 투입하는 것은 무제한적인 공격도구 확보가 가능한 공격자들에 비한다면 수술이 필요한 환자에게 붕대만을 처방하는 행위가 될 뿐이다.

비근한 예로 2007년에 발생된 에스토니아의 DDos 사례와 7.7 DDos의 차이점에 대한 근본적인 고찰도 부족한 현 상황에서 대책이라는 부분은 지속되는 공격에 대한 소모성 대책과 다를 바가 없다.
본 컬럼에서는 근본적인 DDos 공격의 변화를 간략하게 살펴 보고 앞으로의 대응에 중점이 되어야 할 부분에 대해서 짚어 볼 수 있도록 한다.

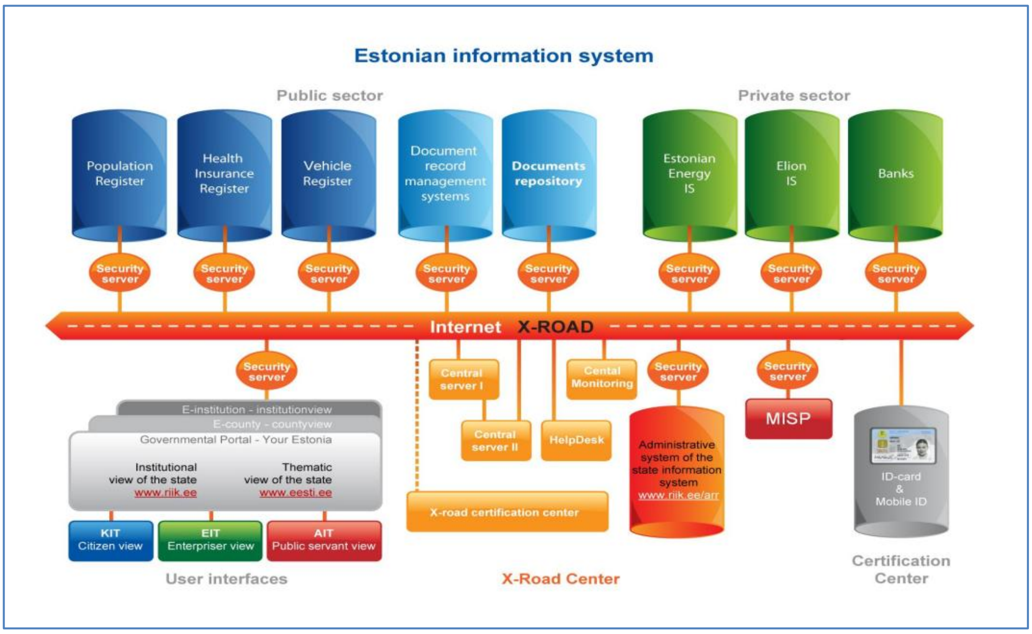
먼저 에스토니아를 향한 공격의 전체적인 동향은 다음과 같다.



일반적인 cyber 공격 유형이라 할 수 있는 통신 대역폭을 가득 채우는 공격과 함께 일반적인 혼란을 초래 할 수 있는 spam메일, Phishing, Web 변조 등이 동시 다발적으로 발생할 것을 확인 할 수 있다.

왜 에스토니아는 외부와 완벽하게 고립된 섬처럼 2~3주간에 걸쳐서 지속적인 피해를 입을 수 밖에 없었을까? 그만큼 취약한 국가였을까? 아니면 취약한 대응능력을 지니고 있었을까?
일반적으로 언론 기사를 통해서는 정확한 면모를 확인하는 것이 어렵다. 단순히 작은 국가가 대규모 공격에 의해 대응능력이 없이 무너졌다고 보는 측면이 강하다. 그러나 IT세상에서는 크고 작음의 판단 기준이 영토에 준하지는 않는다.

에스토니아 국가 자체가 IT화를 통해 국가 발전을 도모한 결과 EU와 NATO에 2004년 동시 가입 될 정도로 동유럽에서는 발전화된 시도를 많이 한 국가로 볼 수 있다. 또한 전세계 최초로 인터넷을 통한 선거를 실시함으로써 실험적인 시도를 많이 한 동유럽의 정보통신 강국의 하나였다.
왜 동유럽의 정보통신 강국은 고립된 섬이 될 정도로 심각한 피해를 입었을까?



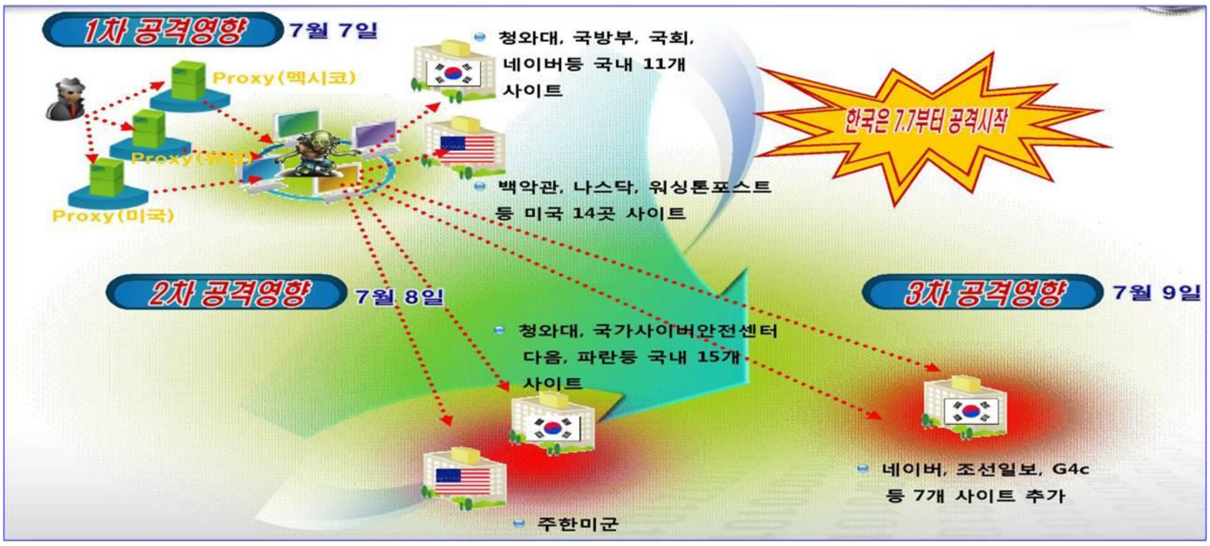
<http://www.riso.ee/en/information-policy/projects/x-road>

위의 이미지는 에스토니아의 기반 정보 시스템에 대한 간략화된 이미지 이다. X-road라는 정보시스템을 인터넷 기반으로 유지하고 있음을 볼 수 있다. 또한 국가 예산 및 운영에 필요한 가장 자원이라 할 수 있는 인구 통계와 차량등록, 건강보험 관련된 내용이 통합되어 300여 개 이상의 국가기관과 연동되어 서비스 되고 있으며 금융기관과도 연동된 형태로 서비스 되고 있음을 알 수 있다. 각 연결지점에는 해킹이나 데이터 유출에 대비하여 암호화된 지점들을 모두 운영 하고 있음에도 불구하고 연결 자체가 되지 않도록 하는 DDos 공격에는 무차별적으로 무너질 수 밖에 없는 구조를 가지고 있었다.

에스토니아의 사례는 국가나 한 산업 자체가 밀접한 연관을 가지고 있고 공개된 통로를 이용할 경우에 치명적인 피해를 입을 수 있는 Cyber war의 전형적인 모습을 관찰 할 수 있다. 이 당시에 활용된 DDos 공격은 일반적인 DDos 공격 세트라고 할 수 있는 각 프로토콜별 자원 고갈형의 공격이 지속 되었으며 공격에 대한 대응은 외부 유입되는 트래픽을 일시적으로 모두 차단 함으로써 일차적인 회복을 할 수 있었다. 국가 내부의 망은 정상화 시킬 수 있었으나 외부와 연결 되는 모든 통로를 차단한 채로 지낼 수 밖에 없어서 고립된 섬으로 불려진 것이다.

2007년에 발생된 에스토니아의 공격이 일반적인 DDos 공격 이외에도 다양한 공격이 병행되어 진행된 것을 볼 때 이후 3년의 시간이 지난 지금에 이르러서는 더 치명적인 내용으로 전개 될 수 밖에 없음은 명확하다.

2009년 7.7일에 발생된 DDos 공격의 경우 일반적인 DDos 공격과는 차이점이 존재하고 있으며 그 변화상을 일면 짐작 할 수 있다. KISA의 자료를 통해 7.7 DDos의 현황을 살펴 보면 다음과 같은 이미지로 간략하게 요약이 된다.



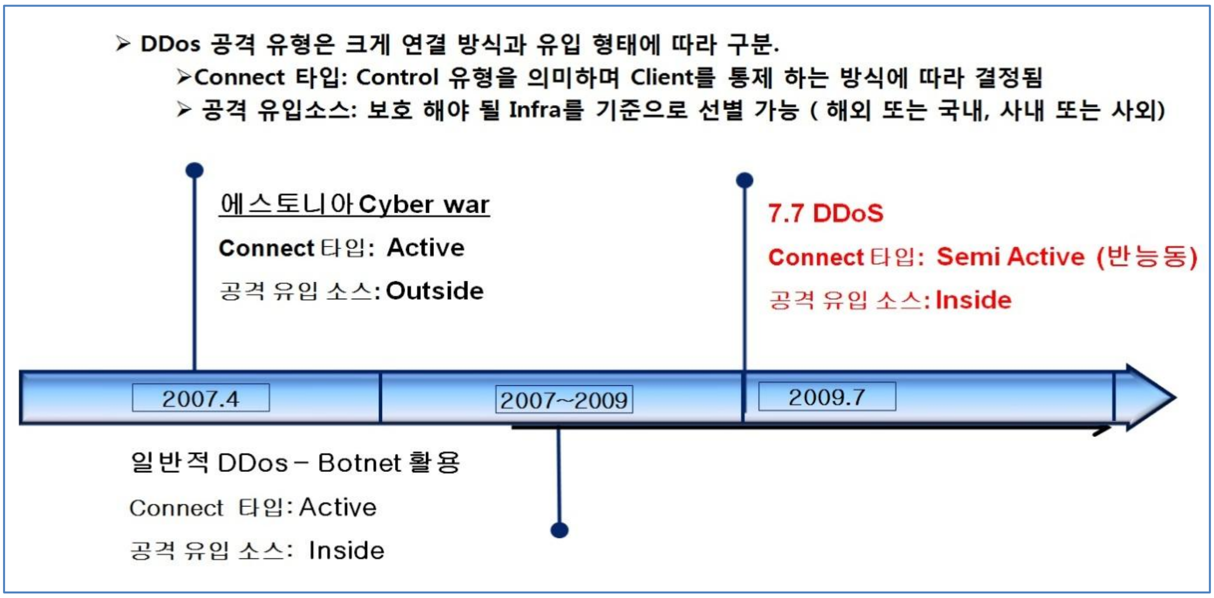
< ref: KISA >

1차, 2차, 3차로 세분화된 공격의 특징은 지정된 일시에 지정된 목표를 향해 예정된 공격을 수행 했다는 특징이 있다. 단순한 트래픽 소모를 위한 DDos 공격과는 별개로 서비스 자원 소모를 위한 DDos 공격도 병행되어 활용이 되었으며 해외로부터 유입되는 공격의 경우 손쉽게 차단되는 점을 이용하여 국내에 존재하는 대량의 좀비PC를 활용 했다는 점이 눈에 띄게 달라진 점이라고 판단된다.

일반적인 DDos 발생시에 대응은 좀비PC를 조종하는 C&C (Command & Control) 서버를 찾아 연결을 차단함으로써 좀비 PC에 설치된 공격도구를 무력화 시키는 방식으로 진행이 이루어 진다. 그러나 7.7 에서는 왜 예정된 3일의 공격을 무력화 시키지 못했을까?

그 이유는 이미 3일간의 공격이 세분화 되어 예정이 되어 있었기 때문이며 좀비 PC를 직접 통제하는 형태가 아닌 좀비 PC에서 명령이 존재하는 서버로 연결을 하고 추가적인 명령을 확인 하는 형태로 구성이 되어 있기 때문이다.

중요한 차이점은 기존의 DDos 공격 방식에 대한 대응으로는 어려울 수 밖에 없는 이미 예정된 공격이었다는 점이다.



간단하게 정리한 DDos 형태의 변화이다.
DDos 공격 유형은 공격 형태에 따라 기술적인 분류가 가능하나 현재 나타난 여러 유형의 DDos 현상을 형태적으로 분석해 보면 연결타입과 공격유입소스라는 부분을 통해 구분을 할 수가 있다. 각 연결 형태와 공격유입 소스의 출발점에 따라 대응은 모두 달라질 수 밖에 없다.

에스토니아

연결타입 : Active – 해외의 Botnet을 이용한 공격
공격유입소스: Outside – 해외에 존재하는 좀비 PC 활용

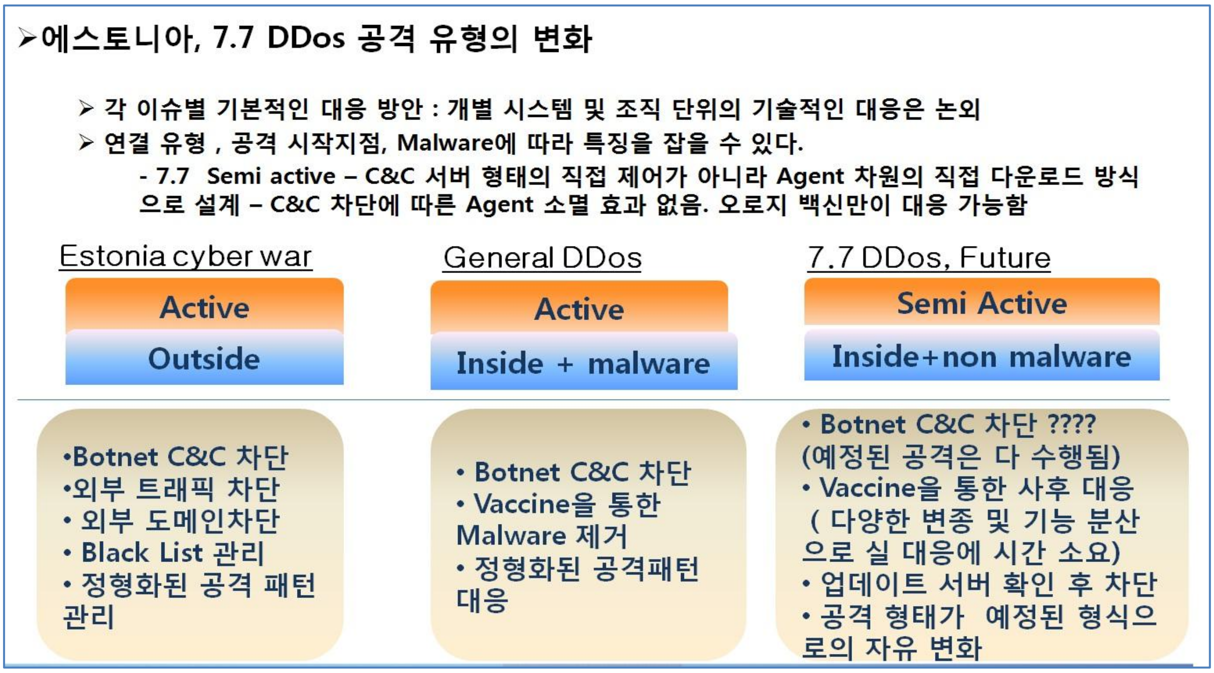
일반적 DDos

연결타입: Active – Botnet을 이용한 공격
공격유입소스: Inside – 국가 내의 PC를 공격하여 획득한 좀비 PC Agent를 활용한 봇넷 공격 (알려진 유형의 공격이 일반적임)

7.7 DDos

연결타입: Semi Active – Botnet C&C 서버가 직접 통제하는 것이 아닌 좀비PC들이 여러 서버들에 접근하여 공격정보를 획득하는 유형
공격유입소스: Inside – 국가내의 PC를 공격하여 좀비 PC 획득 (알려지지 않은 유형의 공격기법 사용으로 사전탐지 안되었음)

각 형태별 대응방식의 변화를 간단하게 도식화 하면 다음과 같다.



DDos 공격에 대한 기본적인 기술대응은 논외로 하더라도 형태의 변화에 따른 심각성은 충분하게 나타난다고 볼 수 있다. 백신에서 사전탐지가 되지 않는 Malware성의 도구 유포와 반능동방식의 조정을 통한 공격 효과는 7.7 DDos에서 보듯이 명확한 효과를 나타내고 있다. 만약 1년이 지난 지금 시점에도 동일한 공격이 더 대규모로 발생 된다면 기술적인 대응을 일정수준 이상 끌어 올린 기업들 조차도 어려움을 겪을 수 밖에 없을 것이다.

근본적으로 DDos 대응의 과제는 이제 일반적인 PC 환경을 얼마나 클린하게 만들고 사전에 위험을 인지 할 수 있고 또 즉각적인 협력과 대응을 통해 피해를 최소화 할 수 있느냐 하는 점에 집중이 되어야 한다.

24시간이 지나면 몇 만대 이상의 웹서비스들이 자동화된 도구에 의해 해킹을 당하고 악성코드를 유포하는 상황에서 좀비 PC의 확보는 더 이상 어려운 일도 아니고 너무나도 쉬운 과제임에는 명확하다. 근본적으로 악성코드가 손쉽게 퍼지는 환경을 개선하는 것이 가장 시급한 과제이며 대응장비의 증설과 대응인력의 확대는 눈 앞의 위험만을 피하고자 하는 대책일 뿐이다. 근본 환경의 개선은 현상적인 문제가 드러난 7.7 이후 달라진 점은 없다고 본다.

앞으로도 근본 환경의 개선 없이는 사태는 점차 심각한 국면으로 진입 할 수 밖에 없을 것이다. 다음 컬럼에는 Mass sql injection에 대한 컬럼을 게재할 예정이다.

* 좀 더 상세한 자료 및 관련 발표 자료는 블로그에서 찾을 수 있습니다.
http://p4ssion.tistory.com/entry/에스토니아-77-DDos-그리고-미래
http://p4ssion.tistory.com/attachment/cfile10.uf@165F670E4C16F178AE44ED.pdf <- 발표자료
twitter: @p4ssion