2009. Change of Global Threat - I

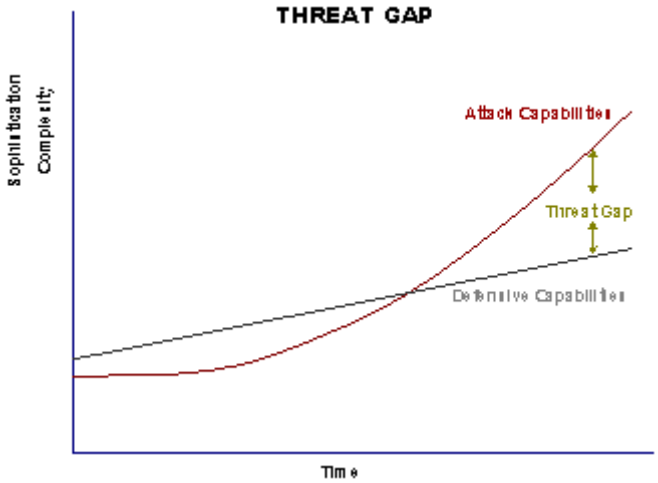
전 상훈 (바다란) P4ssion@gmail.com

공격과 방어의 현실

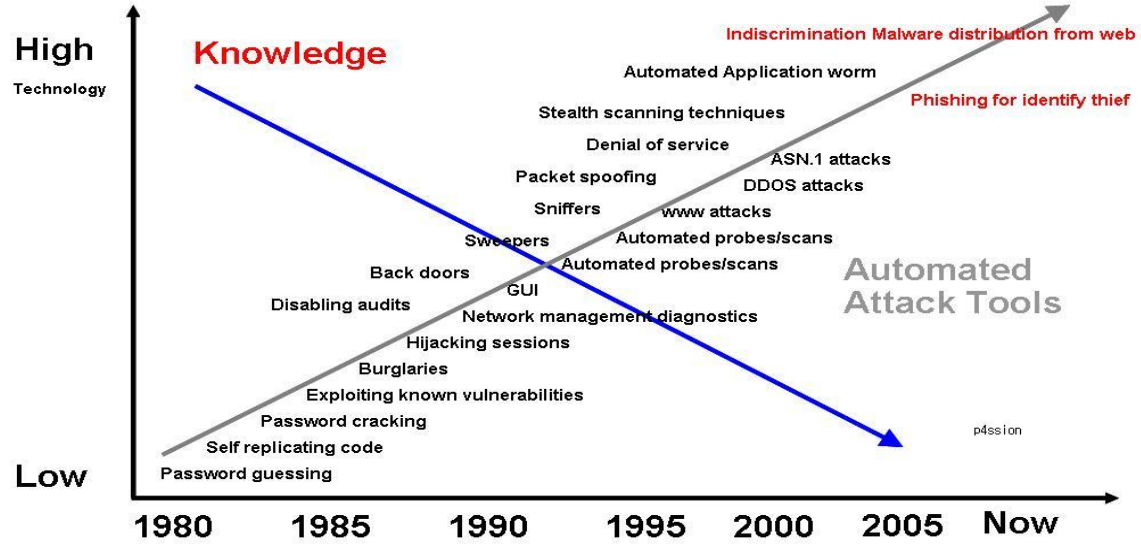
2005년 이후 격렬하게 이루어 졌던 어플리케이션에 대한 공격은 2008년을 거치면서 동아시아 권역을 넘어 전 세계적으로 파급력 있는 이슈들을 생산해 왔다. 2009년을 얼마 남겨 놓지 않은 지금 그 변화들은 어떤 과정과 결과를 만들었을까?

과연 지금 우리가 선택하고 하고자 하는 방향은 올바른 방향인가에 대해 고민하고 보다 더 나은 방향을 만들어야만 한다.

변화의 흐름을 보기 위한 자료들을 몇 가지 정도 취합을 하다 보니 확연하게 드러나는 결과들이 있어서 본 컬럼에서 설명을 하고 방향성에 대해서 찾아 보고자 한다.



위의 Threat gap은 공격 기술과 방어 기술간의 격차를 의미 하는 것으로서 실제 이와 같은 형식의 자료와 챠트들은 많이 있어왔다. 그러나 본 데이터는 2004년에 발간된 미공군의 기술자료에 언급이 된 내용이다. 실제 많은 사례들을 경험 하면서 기술간의 격차를 사실적으로 기술한 것으로 볼 수 있다. 다수의 보안 전문가들도 구체적인 데이터는 존재하지 않지만 많은 경험으로 인해 이미 오래 전부터 인지하고 있는 내용일 것이다. 공격 기술이 방어기술을 넘어선 전환점은 2001~2003년 간격으로 보고 있다. 그 사이에 우리는 최초의 무차별적인 전파와 확산을 하고 대규모 피해를 유발하는 최초의 웜인 Codered를 만났고 Nimda, Blaster, Welchia 등과 같은 운영체제에 존재하는 서비스를 직접 공격하여 권한을 획득하고 재 전파하는 유형의 공격들을 받았었다. 위의 Threat gap과 연관 하여 볼 수 있는 공격기술과 난이도에 대한 상관관계는 다음에서 살펴볼 수 있다.



전체적인 공격기술의 난이도는 어려워 지고 있다. 그러나 공격자들의 기술 수준은 점점 낮아지고 있다. Threat gap을 나타내는 것과 모순되는 점이 보인다. 이 모순의 핵심에는 공격 기술의 공유와 거래, 대량 전파 매커니즘 (웹서비스, 스팸, SNS)을 확보한 것인 가장 큰 핵심을 가지고 있다.

공격자들은 특별한 전문지식이 없이도 새로운 공격유형을 만들고 재생산 할 수 있는 제조 템플릿을 가지고 있으며 (웜 또는 바이러스 생성기) 공격에 사용되는 기본적인 유형들과 기능들은 공개된 상태로 통용이 되고 있다. 새로운 취약성이 나오게 되면 불과 하루 이틀 사이에 웜으로 발전이 되어 전 세계에 영향을 미친다. 이전에는 패치가 안된 운영체제의 경우 생존 기간이 길었으나 지금은 더욱 짧아지고 있다. 운영체제에 심각한 영향을 미치지 않으면서도 자연스럽게 권한을 획득 할 수 있는 Application에 대한 취약성들은 심각할 정도로 증가하고 있는 추세를 보이고 있다.

공격자들은 활발한 커뮤니티를 구성하고 거래를 통해 서로의 부족한 부분을 보충하고 개선한다. 특별한 공격방법이나 도구들이 출현하게 되면 그 즉시 그들의 세상에서는 빠르게 통용이 된다. 2005년쯤에 국내에서 최초 자동화된 공격이 목격 되었던 SQL Injection의 경우 2007년 무렵에 대규모 웹서버리스트들에 대해 무차별적인 공격을 수행하고 자동적으로 웹서비스에서 악성코드를 유포 할 수 있는 형태로 전환이 되었다. 이제 개인 PC의 제어권한을 하루에 십만 대 정도 확보하는 것은 일도 아닌 상태가 되어 버린 것이다. (참고: http://blog.naver.com/p4ssion/50031034464)

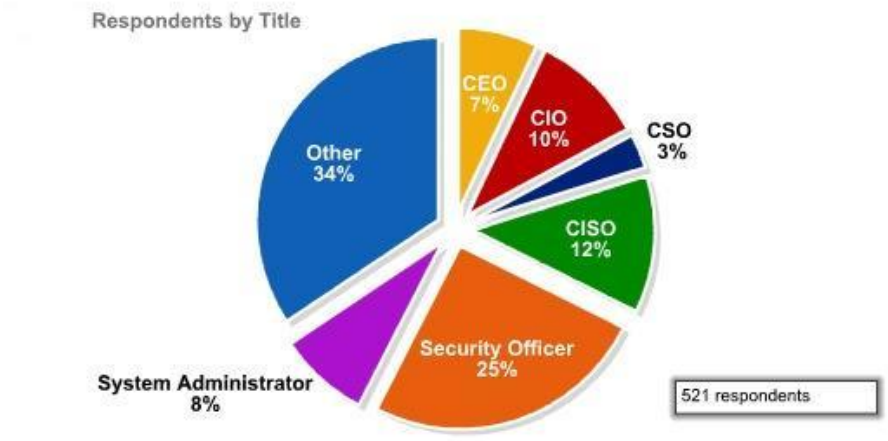
현재의 인터넷의 상태이고 현실이다. 보호되고 있다고 믿는 모든 것들은 무차별적인 공격 대상의 하나로 전락 하였고 도입만 하면 모든 위험들로부터 보호 될 수 있을 것이라 선전 되었던 많은 도구들은 하루가 다르게 변화에 뒤쳐지고 있다.

지금까지 일관되게 현재의 위기 상황과 실태에 대해서 주장을 하여 왔다. 이제 시일이 지난 만큼 전세계적인 기업들에서는 기업의 보안현실과 노력들은 어떤 식으로 변화 하였는지 살펴 보자. 실제 시간이 지난 이후에 결과를 분석하는 것만큼 쉬운 일도 없다. 분석된 결과는 예상과 전망에

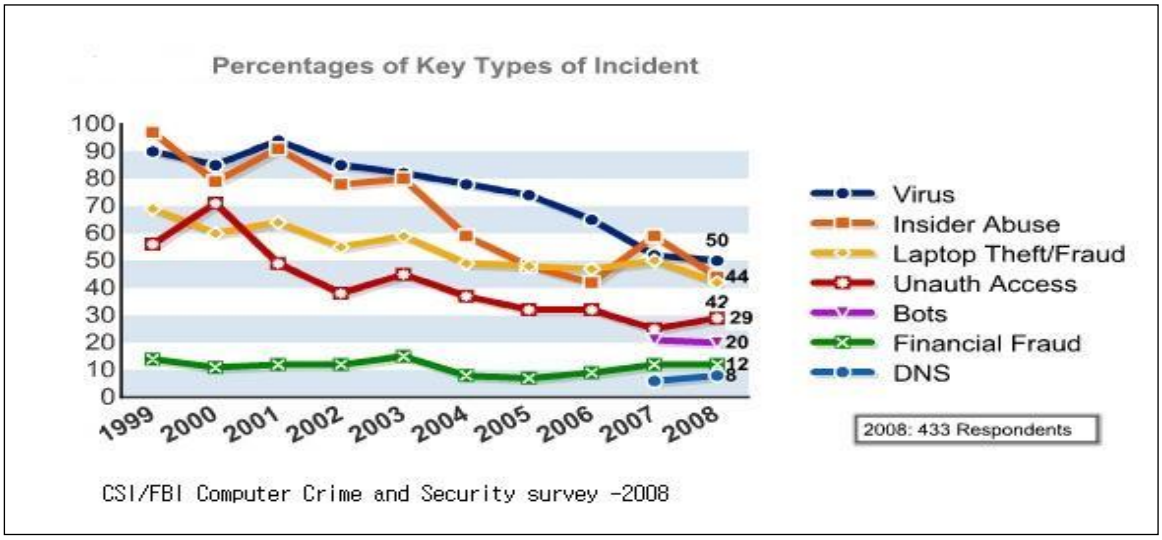
대한 강한 뒷받침이 되는 것은 두말 할 필요가 없을 것이다.

글로벌한 위협현황

매년 연말에 개최되는 CSI Conference에서는 주요 참가 기업의 담당자들을 대상으로 보안 활동과 침해사고에 대한 설문조사를 실시하고 있다. 담당자들의 구성 비율은 다음과 같다.



CSI/FBI Computer Crime and Security Survey -2008 의 설문조사에 응답한 응답자들의 직급을 보여주고 있다. 전체 응답자의 60% 이상이 주요정책 및 의사를 결정 할 수 있는 결정권자의 부분에 속하고 있음을 보여주고 있다. 단순한 실무를 담당하는 보안 담당자들의 의견을 취합한 것은 아니라는 점을 명확하게 보여 주고 있다.

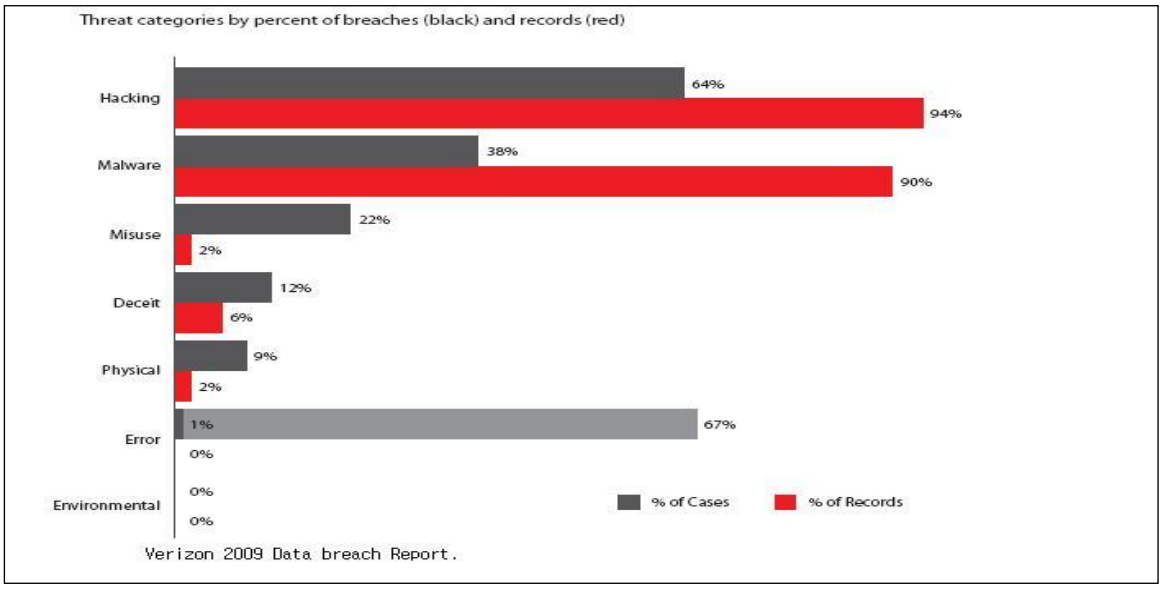


설문 결과 중에서 사고의 유형을 퍼센테이지로 도식화한 챠트이다. 2007년 이후부터 출현한 항목으로는 DNS에 대한 직접공격과 Bot을 이용한 공격들이 활성화 되는 것을 볼 수 있다. 사고의 발생 비율을 보면 정보유출로 인한 사고들과 Malware가 포함된 Virus에 의한 사고들은 여전히 높은 상태를 보이고 있으며 내부자에 의한 사고들도 꾸준함을 볼 수 있다. 주의 깊게 살펴 보아야 할

것은 2007년 이전의 Botnet(공격자가 자유자재로 다룰 수 있는 좀비 PC들의 네트워크망)을 구축하는 것보다 앞으로 시간이 지날수록 더욱더 손쉽게 대규모 Botnet을 구축 할 수 있다는 점이 의미 심장하고 Bot 관련된 계열은 별도로 독립하여 큰 범주를 이룰 것으로 예상 할 수 있다.

내부자에 의한 사고와 외부자에 의한 사고 부분은 별도의 컬럼에서 정리하고자 한다. 그 동안 알려진 것들과는 다른 개연성들을 충분히 유출 할 수 있으므로 별도의 컬럼에서 정리한다.

CSI의 조사에서 언급한 사건들은 실제 사건을 사례별로 조사한 것이라 영향력과 파급력 부분은 고려되지 않은 데이터라 할 수 있다. 전체적인 수치와 비율을 참고하는 정도로만 사용 할 수 있다. 그러나 2008년 까지의 데이터 유출 사례를 실제로 조사하고 분석한 Verizon의 레포트에는 좀 더 실질적인 위협이 되는 부분을 살펴 볼 수 있다.



실제 기업내부의 중요데이터가 유출 되거나 기밀이 누설된 케이스를 분석한 결과는 사뭇 다르다. CSI의 통계치 에서는 전체적인 공격 유형과 위협의 유형들을 볼 수 있으나 Verizon의 데이터 유출 관련된 분석 보고서에서는 실제 어떤 위협들이 중요 데이터를 유출 시킨 것과 직접적인 관련이 있었는지를 보여 주고 있다.

가장 많이 발견된 사례는 Hacking과 Malware, Misuse를 들 수 있다. 바이러스 백신들과 다수의 보안장비들이 도입이 되어 공격에 대한 탐지로그들은 매우 많음을 확인 할 수 있고 잘못된 사용 또는 실수라고도 할 수 있는 Misuse 부분에서는 탐지 할 수 있는 근거자료나 로그들이 매우 적음을 관찰 할 수도 있다. 일반적으로 공격시도에 대해서 대부분 Hacking이라고 일반적인 표현을 하나 Verizon Report에서 언급한 Hacking의 대부분은 Web application에 대한 SQL Injection 공격과 Remote Access 도구에 대한 접근,기본 설정 및 권한에 대한 공격으로 분석이 되고 있다.

Hacking과 Malware, Misuse와 같은 대부분의 정보유출의 원인들에는 사용자, 관리자, 개발자의 실책에 대한 이슈가 67% 가량을 차지하고 있음을 볼 수 있다. 웹 URL의 인자가 필터링 되지 않는

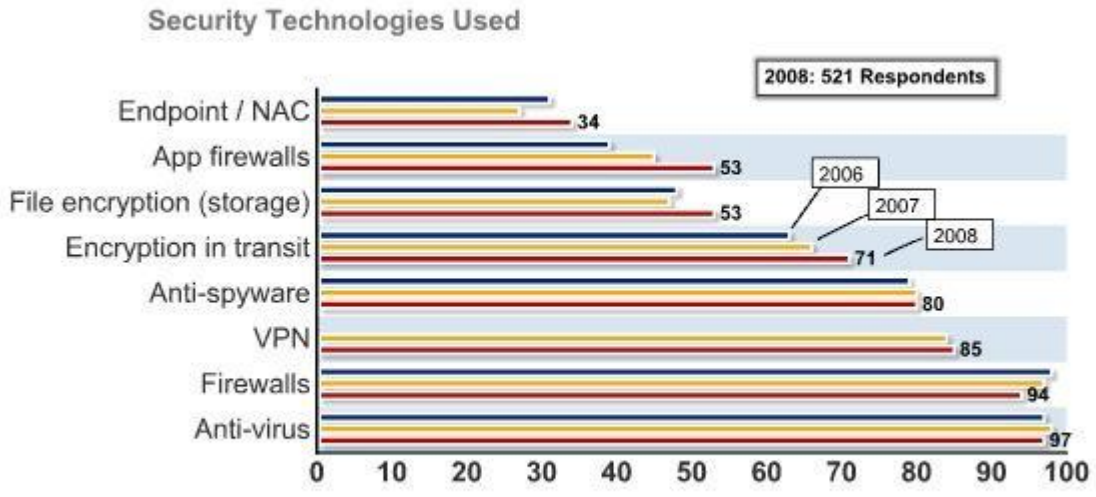
경우를 공격하는 SQL Injection의 경우에도 Error라고 표시가 되기는 하였으나 **현실적으로 취약성을 빠른 시간 이내에 발견하고 수정을 할 수 있도록 하는 도구가 없음**으로 인해 실질적인 Error 항목에 기입하기에는 어려움이 있다.

각 조사에서 보듯이 전체적인 사건의 2008년까지의 발생 현황은 새로운 공격흐름을 보여주기도 하며 실제 피해 사례에 가장 큰 영향을 미치고 중요성을 지니고 있는 부분이 어떤 부분인지를 보여주고 있다.

국내의 사례는 지금껏 공개적으로 조사되고 분석되어 종합된 자료가 없다. 그러나 전 세계적인 동향과 위협들의 범주에서 벗어날 수는 없다. 사건, 사고 사실을 의도적으로 무시하는 것은 보다 더 큰 치명적인 피해를 유발 할 수 밖에 없다는 점에서 국내의 심각성은 더 높은 상태가 아닐까 생각 된다.

위협에 대한 대응 노력

위협들은 실질적으로 Application에 대한 직접적인 공격과 대량화, 자동화된 공격, Client에 대한 직접 공격으로 축약 할 수 있다. 2008년은 물론이고 지금까지도 또 앞으로 몇 년 이상을 이와 같은 동향은 계속 유지 될 것으로 전망된다. 각 기업들의 대책들은 어떤 방식으로 이루어 졌을까?



CSI/FBI Computer Crime and Security Survey-2008

기업이든 국가이든 형식적인 공격이 아니라 실제의 피해를 일으키는 공격에 대해서만 반응을 하게 마련이다. CSI의 조사는 2006년부터 2008년까지의 각 기업 혹은 기관별로 사용된 보안 기술들을 나타내고 있다. 위협의 변화에 따라 달라진 부분을 확연하게 볼 수 있다.

VPN, Firewall, Anti-Virus와 같은 보안장비는 이미 일상화된 보안 도구로 볼 수가 있다. 증가된 폭

을 보게 되면 App firewall의 도입이 큰 폭으로 증가 추세에 있음을 볼 수 있다. 실제 공격이 집중되고 피해가 발생 하기 때문에 도입 될 수 밖에 없는 부분이다. 두 번째로는 개인 PC와 자료의 보호를 위해 NAC 장비의 도입, 암호화 장비나 도구의 사용이 늘어나는 현상을 관측 할 수 있다. 실제 피해사례를 조사한 Verizon의 보고서에서 원인으로 제시된 항목들은 조사 이전부터 계속 발생 되어온 문제이다. 집중적으로 문제가 발생 되는 부분에 대해 대책을 세우는 과정에서 드러난 현상으로 Application에 대한 보안 강화, Endpoint에 대한 보안 강화, 자료의 암호화를 통한 강화를 중점적으로 살펴 볼 수 있다. 국내의 변화도 마찬가지가 아닐까 싶다.

각 기업들은 어느 정도의 위험성을 알고 있고 대비하기 위해 어떤 부분에 중점을 두고 노력을 하였을까를 알아보는 것도 위협의 변화와 연관성이 높다. 공격 기술과 방어기술의 차이를 염두에 두면 방어기술의 진보는 느리고 더디게 나아간다. 즉 변화가 있다고 하여도 공격기술의 발전 정도에는 미치지 못함을 사전적으로 알고 있으면 미래의 방향을 예측 하는 것이 보다 쉽다.

전체적인 공격동향을 보고 세부적으로는 중요 정보의 실제 유출 사례 조사를 살펴 보면서 우리는 앞으로 중점을 두어야 할 부분이 어디이고 세계 속의 기업과 기관들은 어떤 준비와 대응을 해왔는지 고려해야 한다.

지난 몇 년간 꾸준하게 예상을 해온 바들도 Client 보안과 Application에 대한 직접적인 보안 강화에 대해서 강조를 했었다. 전체를 정확하게 볼 수 있는 분석들은 아니지만 동향을 확인 할 수 있다는 점에서 인용된 자료들은 충분한 근거를 제시하고 있다.

노력하고 준비하지 않으면 이제는 더 나아가기 힘든 상황이 올 것이다. **보안은 완벽하게 막기 위해 존재하는 것이 아니라 이미 알려진 것들에 대해서는 막을 수 있도록 하고 피해를 최소화하며 빠르게 대응을 하는 것이 핵심이다.**

국내는 완벽하게 막는 것이 보안인 것으로 종종 오해를 한다. 현실은 가혹하다. 더 많은 비용과 인력을 투입하고서도 완전해 지지 못하는 세계적 기업과 기관, 국가들이 많다. 공격 기술과 방어기술의 차이는 점점 더 벌어 질 수 밖에 없는 구조라 앞으로 더 어려움이 있을 것이다.

내일을 살펴 보려 하지 않고 준비하지 않는 자에게는 지금이 마지막의 시작일 수도 있을 것이다.
– 다음 컬럼에 계속