

Critical Alert for Cyber warfare II

Inevitable Cyber warfare

전 상훈 (p4ssion@gmail.com)
2009.11

© Copyright 2009 sanghun , Jeon . All rights reserved.

Table of Contents

서문	3
배경	4
CONTENTS	5
최신 동향 분석	5
공격의 변화	8
기반시설의 위협 사례	13
기반시설의 공격 시나리오	16
예상하는 최악의 시나리오	18
SECURITY PLAN	21
REFERENCES	23
ABOUT	24

서문

일반적인 사이버전이라고 하면 사이버상에서만 발생 될 수 있는 위협이라고 한정을 한다. 그러나 고도화되고 밀접한 연관성을 지닌 현대의 사회에서는 실생활에도 많은 관계를 가질 수 밖에 없다. 이슈 형식으로 발생 되는 것은 하나의 사건일 뿐이다. 7.7 DDos 이슈도 하나의 사건일 뿐이다. 사이버 상에만 제한적으로 영향을 미쳤을 뿐이다. 그러나 이제는 실제 생활에도 심각한 영향을 끼칠 수 있는 모습으로 내일 당장 나타날 수도 있다. 발생 되지 않은 최악의 상황을 가정하여 준비하고 대비하여야만 실제 상황이 발생 하였을 때 흔들리지 않고 피해를 최소화 하고 빠른 대응이 가능하다.

유비쿼터스 세상으로 빠르게 진입 하는 시대에서 우리의 환경을 구성하고 편리성을 제공해 주는 도구들과 생활들은 인터넷 세상과 밀접한 연관을 가지고 있다. 밀접한 연관이라는 말은 실제 생활에도 사이버적인 역량만으로도 실생활에 영향을 줄 수 있다는 것과 동일하다. 앞으로의 사이버전은 목적을 달성 하기 위한 소규모 공격에서부터 전시를 방불케 하는 총력전으로 구분이 될 수 있다. 총력전이라는 의미는 국가 혹은 일정 수준 이상의 집단이 전력을 쏟아서 진행 하는 것을 의미한다. 국가적인 역량을 동원 하지 않더라도 일정 수준을 보유한 수십 여명의 그룹단위로도 치명적인 영향을 충분히 줄 수 있는 상태로도 볼 수 있다. 전 세계의 주요 국가들이 음으로 양으로 공을 들이고 있는 사이버 공격과 방어 태세는 이미 미래에 발생 할 수 있는 계획을 넘어 현재에 일어날 수 있는 사안으로 간주되고 준비가 이루어 지고 있다. 미래에 발생 될 정치, 사회, 경제적 분쟁에는 목적에 따라 치열한 사이버전은 일상적으로 발생 될 수 밖에 없으며 지금 이 순간에도 공격은 진행 되고 있다.

민족, 경제, 영토, 종교, 이념 등의 모든 저장도, 고강도의 분쟁에는 필수적으로 사이버전이 수반 될 수 밖에 없으며 일정 수준 이상의 고도화를 달성한 국가와 지역에 대해서는 테러를 넘어서는 수단으로 가장 선호 될 수 밖에 없는 상황에 도달해 있으며 앞으로 더 심각해 질 것이다.

최악의 상황을 가정 한다는 것은 전시와도 같은 상황에서 발생 될 수 있을 법한 이슈들을 찾아내고 위험성을 판단 하는 것이 가장 중요하다. 공격기술의 전체적인 동향과 움직임들은 어떻게 변해가고 있으며 현재상황은 어떤 상황인지 또한 앞으로 중점을 두어야 할 부분들은 무엇인지 똑바로 직시 해야만 할 것이다.

배경

서두에 밝혔듯이 앞으로의 분쟁은 사이버 전이 병행 되는 것은 당연한 논의 이고 점차 그 비중이 커질 수 밖에 없는 부분이다. 특히 첨단화 되고 중앙에서 통제가 이루어지는 시스템에 대해서는 보다 더 적은 비용과 노력으로 심각한 타격을 입힐 수 있어서 국가 차원이 아닌 소규모 그룹 차원에서도 국가 혹은 단위 구성 분야에 대해 심각한 위협을 가할 수도 있다.

사이버전에 대한 논의는 DDos 와 개인정보 유출의 범주를 떠나서 실제 최악의 상황에 직면 하였을 때 발생 할 수 있는 경우를 살펴보고 현재 상태의 발전이 특별한 고민이 없이 진행 된다면 어떠한 결과를 초래 할 수 있는 지도 반드시 논의 되어야만 한다. 앞으로의 전장은 총칼이 부딪히기 이전에 사이버 전쟁이 먼저 촉발이 될 것이다.

준비된 자와 준비되지 않은 자, 잃을 것이 있는 자와 잃을 것이 없는 자의 싸움은 사이버전에서 극명하게 차이를 드러낼 것이고 그 시작은 지금껏 일어나고 있는 서비스 거부 공격 (DoS)과 더불어 기반시설에 대한 직접적인 위협으로 시작 될 것이다.

기반시설에 대한 이슈 제기를 처음 [1] 제기 하였을 때는 2002년 이였고 당시에는 기반시설에 대한 침해사례와 실제 가능한 시나리오의 경우가 적어서 현실화 되기에는 많은 시일이 걸릴 것으로 예상을 하였다. 이후 몇 년의 시간이 지난 뒤에 무시 할 수 없는 수치의 사건들이 실제적으로 발생을 하였고 생활에 영향을 미쳤음을 충분히 알 수 있었다.

기반시설은 스마트 그리드의 형태로 점점 더 생활에 밀접하게 되고 통제의 범위도 대규모, 자동화, 집중화 되는 것으로 방향성이 잡혀지고 있으며 앞으로 더 심화될 것이다. 더불어 공격유형의 변화와 환경에 위협을 주는 요소들도 시대상황과 기술의 발전에 따라 많이 달라질 수 밖에 없고 그 상황에 대한 준비를 하고 대비를 하는 것이 사이버전에 대한 대응이 될 수 있을 것이다.

전체적인 공격 유형의 변화와 현재의 위협에 대해서 살펴보고 기반시설에서 발생된 문제를 살펴 볼 것이다. 이후에 다양한 공격 방안들이 어떻게 가능한지를 검토해보자. 최종적으로는 가상의 시나리오를 통해 최악의 경우가 어떻게 다가 오는 것인지 살펴 볼 것이다.

준비 해야 될 부분은 무엇이 있고 앞으로 어떤 관점에서 역량을 기울여야 하는 지에 대해서는 대책 부분에서 개념적으로 기술을 한다.

이제 사이버전은 인터넷 공간에서만 존재하는 것이 아닌 실제 생활에도 막대한 영향을 미치고 충격을 줄 수 있을 만큼의 거대한 연결고리를 가지고 있음을 명확히 하고자 하며 그 동안 개념적으로 이해해 왔던 여러 이슈들에 대한 설명을 통해 연관관계를 분석 하도록 할 것이다.

충분히 노력하지 않고 준비 하지 않는다면 그 결과는 최악에 가까워 질 것이다.

2002년의 문제제기가 주의를 촉구하는 것 이었다면 7년이 지난 지금은 경고의 의미이다.

Contents

최신 동향 분석

현재의 공격 기법과 보호 방안들 사이에는 차이가 존재한다. 그리고 그 차이는 시간이 지날수록 더욱 큰 차이를 보여주고 있다. 공격자들에게는 한계가 존재 하지 않으나 보호방안들에는 어마어마한 규모의 제약들이 존재한다. 거기에는 이익을 유지 하려는 목적들도 존재하고 국가간의 경계를 넘어서는 공격의 특성상 대응에는 한계가 따를 수 밖에 없다.

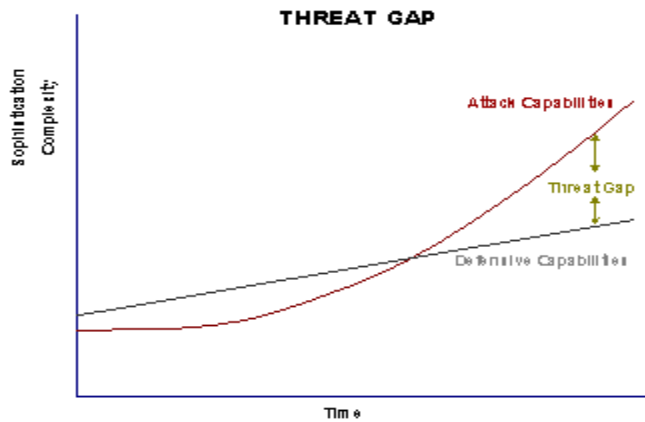


그림 1. Threat gap

2004 년에 미공군에서 발표한 [2] “ *A Dynamic Information Defense Solution in a Dynamic World* ” 에서 언급된 내용이다. 보다 더 정확하게 언급을 하면 국내의 상황에 맞추어서 분석한 내용은 다음과 같다.

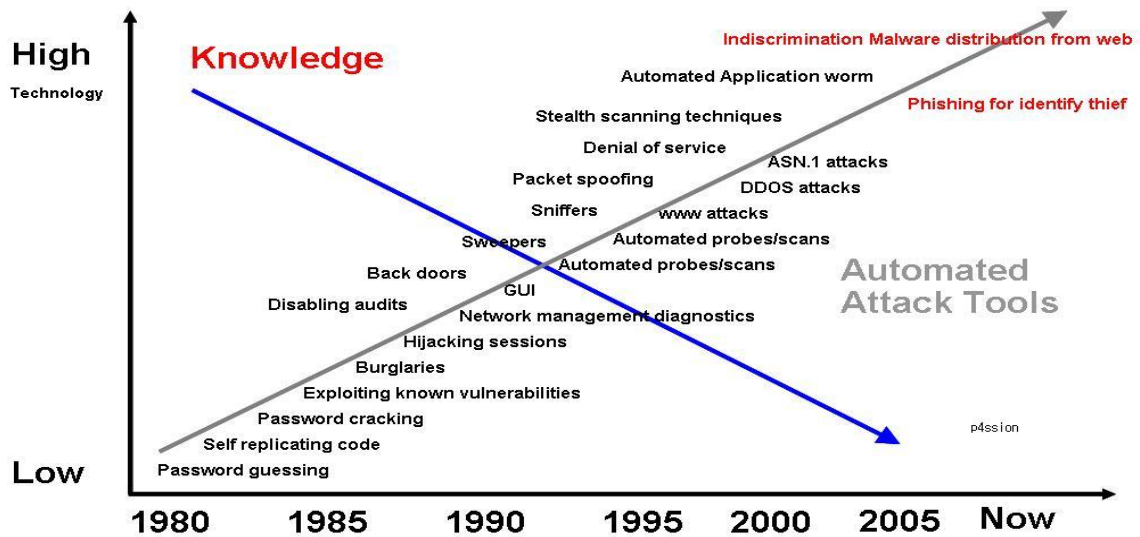


그림 2. 공격 기술의 발전

그림 2에서 나타내고 있는 내용은 공격자의 지식수준은 점점 낮아지고 있음을 의미한다. 공격자의 지식수준은 낮아지고 있으나 공격 도구의 자동화가 이루어지고 있어서 공격이 가능한 인력풀이 대폭 확대되고 있음을 나타내고 있다. 영향력은 전체의 인터넷 환경에도 영향을 미칠 수 있는 상태로 확대되고 있으며 2002년 이전의 특정 OS의 취약성들에 대한 집중 공격에서 2005년 이후에는 Application에 대한 공격으로 발전한 상태이며 또한 대량화된 공격을 자동적으로 진행할 수 있는 상태이다. 그러나 대응 기술 측면에서는 과급효과는 미미하며 발전 속도조차 그리 빠르지 않다. 그림 1과 그림 2에서 언급하고 있는 Threat gap은 시간이 지날수록 점점 더 격차를 벌리게 될 것이다. 보호 역량에서의 차이는 세부기술에 대한 대응이 아니라 전역적인 대응과 국제적인 대응 역량의 부족과 협력의 부재에서 극명한 차이를 두고 있다.

그림 2에 언급된 2000년 이후의 변화는 극적이라고 볼 수 있다. 특히 2006년 이후에는 대량 공격을 위한 도구들까지 일반화된 상황이라서 Threat gap은 최대치로 확대된 상황이라 할 수 있다. 단적인 예로 다음과 같은 경우를 [3] 들 수 있다. 2008년 4월에 발생한 Mass sql injection[4]의 경우도 좋은 예가 된다.

단기간에 50만대의 웹서버를 해킹하여 악성코드를 유포하도록 한 행위를 통해서 현재의 심각도를 짐작할 수 있다. 정확하게는 50만대의 웹서버는 부수적인 것이고 50만대의 DB 서버를 해킹하여 부수적으로 웹서버의 소스코드를 변조한 것이 정확한 설명이라 할 수 있다. 참고자료 [4]에서 보듯이 단기간에 대량의 시스템들이 변조를 당하자 보안 관계자들조차도 특정 운영체제의 치명적인 버그가 발견되어 웹으로 유포되었을 것으로 인식을 하고 있다.

짧은 기사에서조차도 현재의 위험성을 충분히 인지할 수 있고 분석하고 대응하는 역량과 공격하는 기법 사이의 차이가 상당한 차이를 보이고 있음을 알 수 있다. 전문적으로 분석을 하는 전문가들의 입장에서조차도 문제 인식에서 잘못된 견해를 보이는 상황도 있어서 앞으로 상당한 우려를 할 수밖에 없다.

보안전문가들 사이에서 언급되는 오해 중의 하나가 내부자에 의한 정보 유출과 침해사고가 외부자에 의한 침해사고와 비교하여 8:2 가량으로 우세하다는 것이 1990년 중반 이후에서 최근 까지도 일부에서 논의되고 있다. 그러나 실제적인 조사에 따르면 외부자에 의한 공격 빈도와 성공 비율은 상당한 수준으로 올라와 있는 상태이다.

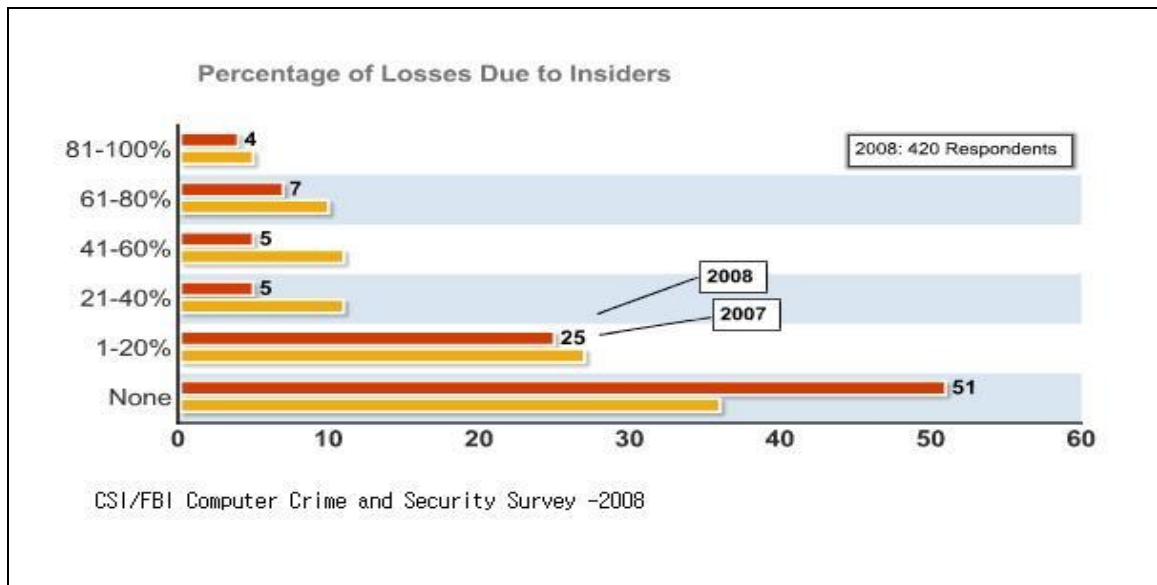


그림 3. 내부자에 의한 사고 비율

그림 3 은 CSI/FBI Computer Crime and Security Survey 에서 2008 년에 조사된 내용이다. 내부자에 의한 사고를 경험한 기업의 비율이 상당 부분 떨어진 것을 볼 수가 있다. 더불어 데이터 유출과 관련된 비율도 동일한 흐름을 관찰 할 수 있다.

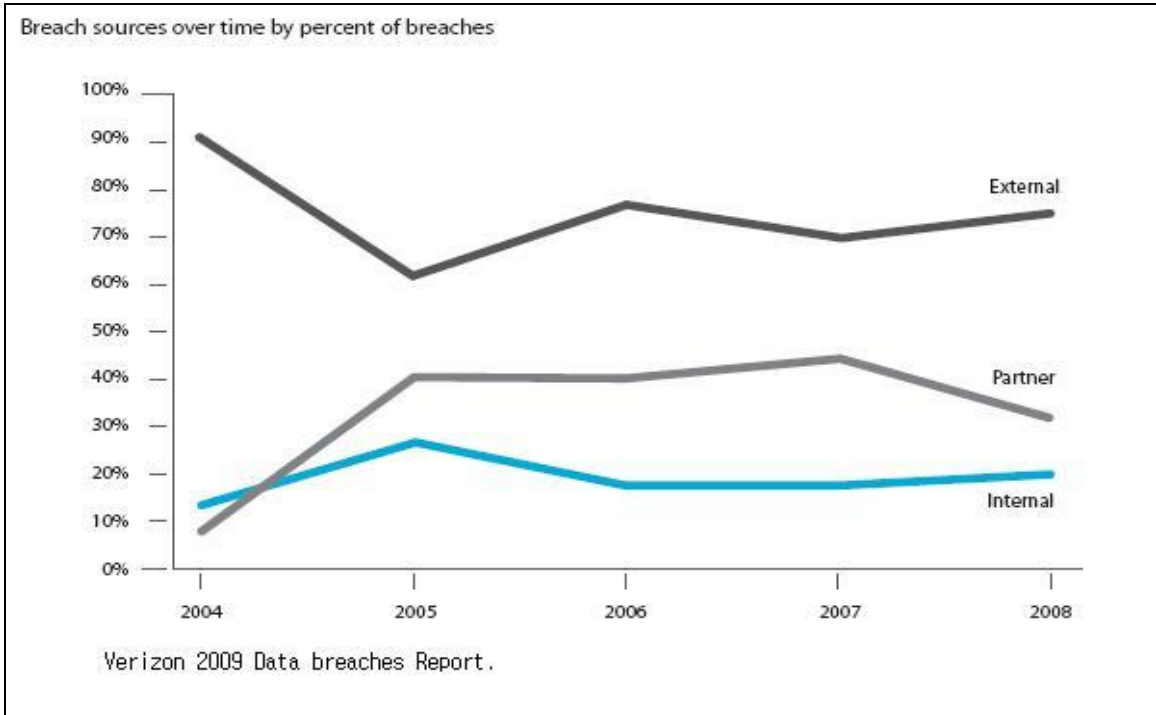


그림 4. Verizon 2009 Data Breach Report

일반적인 기업에서 발생된 데이터 유출 사례를 원인 별로 분석한 결과 [그림 4] 외부에서 공격이 시작된 비율이 높은 수준으로 유지됨을 볼 수 있다. 외부에서의 침입이 가능한 부분을 막기 위해 많은 비율의 예산이 투입 되었음에도 불구하고 외부에서의 공격이 줄지 않는 이유는 무엇일까?

그 문제의 원인은 공격자들의 지식과 공격 기법의 변화에 존재하고 있다. 보안장비들로서도 공격자들의 발전과 기법의 변화에 대해서 능동적인 대처가 어려움을 충분히 확인 할 수 있다. 물론 기본적인 보안 예산들이 투입 되지 않았다면 더 큰 차이가 발생 하였을 것이다.

공격자들은 이제 Web application 에 집중을 하여 기업의 내부망에 침입을 시도하고 있다. 내부망에 침입을 하기 위한 공격 이외에도 정보 수집을 위한 Malware 유포의 도구로서 병행해서 사용을 하고 있는 것이다.

사안을 보는 관점은 두 가지가 있다. 그림 3 과 그림 4 는 범주가 조금 다르다고 할 수 있다. 그림 3 에서 언급하는 것은 해결되었거나 시도가 된 모든 사건들을 포함하고 있다. 그림 4 는 실제 정보가 유출되고 피해를 입힌 경우에 대해서 조사가 된 것이다. 전체적인 현황을 보기에는 그림 3 에서 언급하는 내용들이 중요하며 실제적인 피해의 관점에서는 그림 4 의 데이터가 의미 있는 데이터가 된다. 공격 유형별 분석도 CSI/ FBI 의 Survey[5]와 Verizon 의 Data breach report[6] 의 특성에 대한 이해를 바탕으로 해야 정확한 분석이 된다.

전체적인 공격 유형의 특징과 실제 발생된 사례별 케이스로 접근을 하여야 하며 전문가의 입장에서는 전체적인 관점을 인지하고 실제 발생된 사례별 케이스로 접근하는 시도가 바람직하다고 할 수 있다.

공격의 변화

공격의 변화에 따라 공격 대상도 달라지고 있으며 실제 피해를 입는 케이스도 달라지고 있다. 공격흐름을 이해해야 하고 공격 방식에 대한 이해도 있어야 한다. 두 가지 정도의 통계치를 이용하여 설명을 하는 것도 전체적인 공격 동향과 주요 피해를 입히는 실질적인 부분을 비교하여 가장 시급한 부분이 어떤 부분인지에 대한 인식이 필요하다. 지금의 공격은 앞으로도 상당기간 Application에 대한 공격과 개인 PC에 대한 직접적인 공격으로 집중 될 것으로 예상되고 있다.

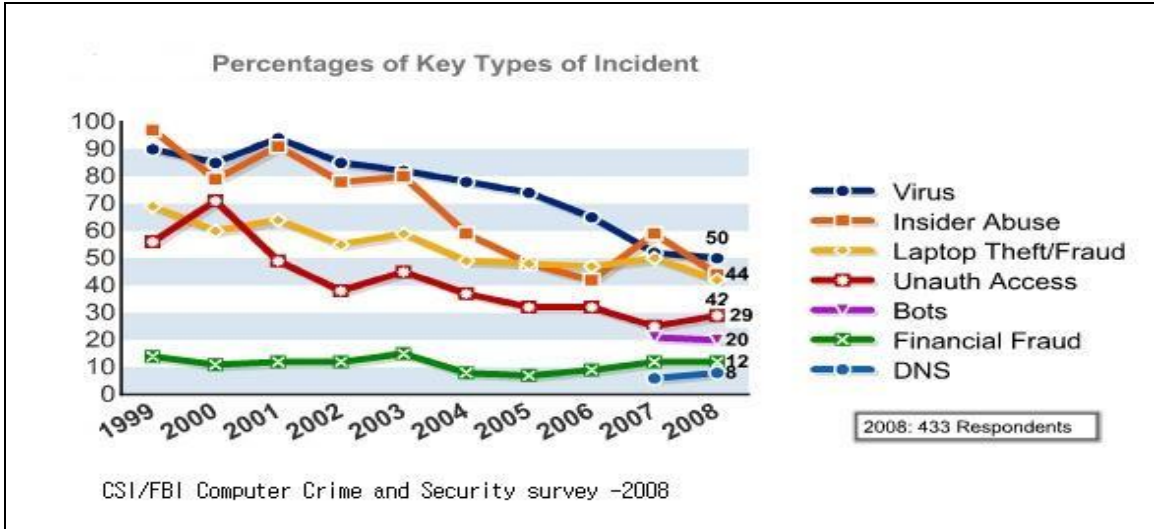


그림 5. Types of incident

그림 5의 사건의 유형들에 대한 조사결과는 전체적인 기업망에서의 사건 원인이 어디에서 기인을 하는지 확인 할 수 있다. 특이할 만한 사항으로는 Bot에 의한 사건들과 DNS에 대한 이슈들이 발생 하는 것을 확인 할 수 있다. CSI/FBI의 Survey[5]는 언급 하였듯이 전체적인 사건들에 대한 이슈들을 나타낸다. 여기에서는 각 년도 별로 경험했던 사건들에 대한 기록으로 볼 수 있으며 전체적인 사건들의 현황을 일부분 짐작 할 수 있다.

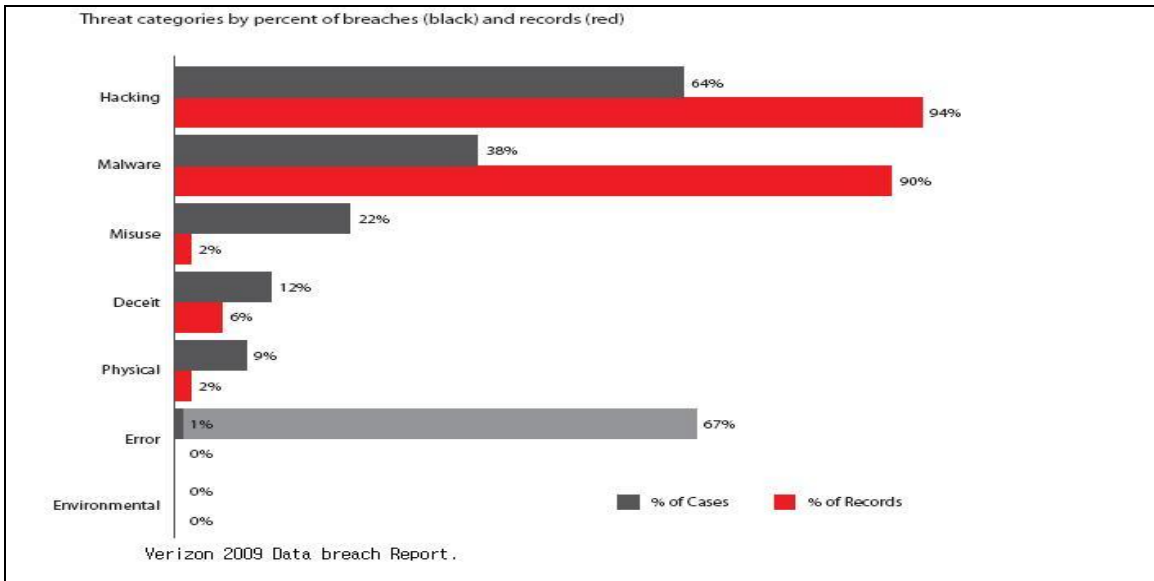


그림 6. Threat categories

반면 Verizon 의 Data breach report[6]의 경우에는 실제 피해 사례를 기반으로 하여 조사를 한 내용이라 현재 상태에서 가장 부족한 부분들이 어떤 부분인지를 알 수 있도록 해준다. 그림 6에서는 데이터 유출의 주된 방법으로 Hacking 과 Malware 가 사용이 되었고 67%의 경우가 Error 에 의해 발생 되는 것임을 나타내고 있다.

실제 기업망에서 심각한 피해를 유발하고 있는 사안 중 현재 가장 심각한 것은 직접적인 Hacking (여기에서 의미하는 Hacking 을 통한 정보유출의 경우는 90% 이상이 SQL Injection 공격에 의한 database 정보 유출을 의미한다.) 과 Malware 에 의한 Trojan 피해가 대부분을 차지 하고 있다.

CSI/FBI 의 Security Survey 와 Verizon Data breach report 는 침해사고의 근본적인 동향과 피해를 입히는 근본적인 부분이 어디에 있는지를 살펴 볼 수 있도록 해주고 있다.

보안 장비의 도입 증가 추세에서도 근래에 발생하는 이슈들의 흐름을 짐작 할 수 있다.

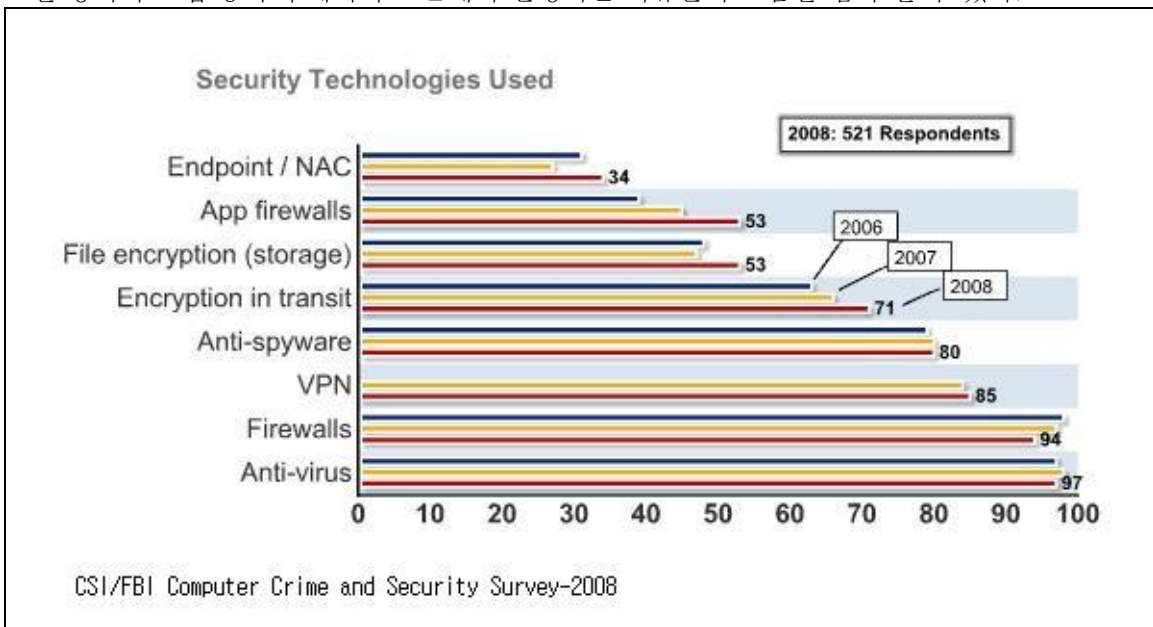


그림 7. Security Technologies used

2006 년부터 2008 년까지의 조사 결과를 보면 가장 큰 폭으로 증가하거나 변화가 있는 곳들이 실질적인 위협들에 대해서 대응하기 위한 행동으로 볼 수가 있다. Anti-virus 와 FW, VPN, Anti-spyware 의 경우 거의 변화가 없다고 느낄 정도로 특이 사항이 없다. 증가치에 대한 부분은 자연스런 발전 과정으로 볼 수가 있을 정도이다. 특이할 만한 변화들은 보호 단계에서 발생된다. 특히 App Firewalls 의 급격한 증가추세는 앞서 언급한 공격의 변화와 맞물려서 충분한 이해가 될 수 있을 것이고 PC 차원의 보호를 위한 NAC 의 증가 추세와 정보의 보호를 위한 암호화 부분들이 증가 추세를 유지하고 있다.

앞서 언급 하였듯이 현재의 위협은 Application 과 개인 PC 에 집중되어 있다. 대규모적인 정보 유출은 Application 의 취약성을 이용하고 개인정보의 유출과 좀비 PC 의 대규모 운영을 통한 서비스 중단 등은 개인 PC 를 직접 공격 함으로써 발생이 된다. 각 부분별 예산과 기술의 증가는 실질적인 위협의 증가가 어디에서 일어나고 있는지를 반영 한다고 볼 수 있다.

전체의 취약성 현황을 살펴 보기 위해 이전의 경우에는 Cert.org 에서 [7] 발표되는 취약성 통계를 사용 하였다. 그러나 현실적인 문제와는 현재 괴리가 있는 상태라고 볼 수 있다.

부터

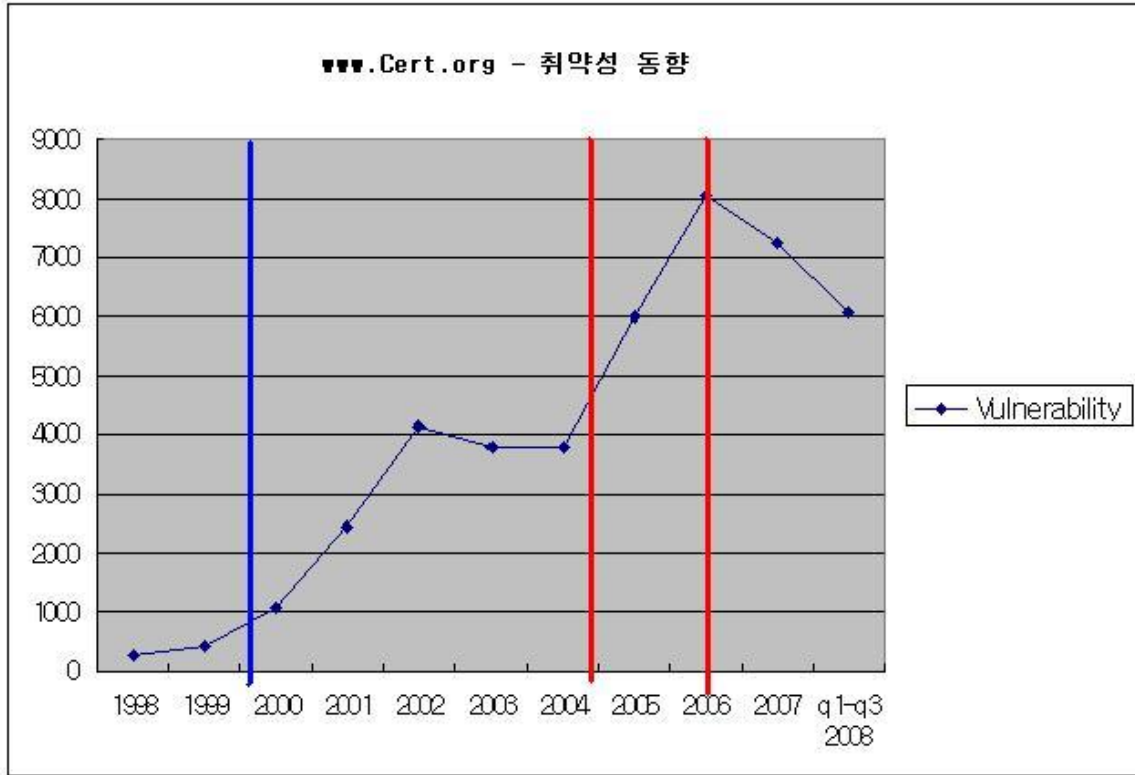


그림 8. cert.org vulnerability

www.cert.org에서 발표된 공식적인 취약성 수치를 도식화 한 것이다. 그러나 현재 도식화된 취약성의 개수로는 현재의 문제가 설명이 되지 않는다. 더불어 공격 방식의 변화에 따라 현재의 위험에 적용 하는 것도 무리가 존재한다.

실질적으로 취약성은 줄은 것으로 발표 되고 있다. cert 에서 수집하는 취약성은 주요 Application 과 운영체제에 관한 치명적인 취약성들을 주로 통계화 하고 있으며 실질적으로 Third party application 에 대한 취약성 통계는 별도로 잡히지 않고 있다. 2000 년 이후부터 2004 년 까지는 운영체제들에 대한 주요 취약성들이 발표가 되었고 이후 2004 년 무렵에는 운영체제 및 주요 Application 들에 대한 취약성들이 발표 되고 있다. 2006 년 이후에는 눈에 띄게 취약성의 발표가 줄어 들고 있는데 여러 가지 요인들이 있을 수 있다. 금전적인 이득을 위해 공식적인 취약성 발표를 하지 않는 이슈 하나와 지역별 혹은 국지적인 Application 에 대한 취약성 통계를 수집 하지 않는 점을 들 수 있다. 가장 중요한 점은 2006 년 이후에는 개인 PC 에 영향을 미칠 수 있는 Application 에 대한 취약성들이 다수를 차지 하고 있다는 점이다.

Sans 의 Report 에서도 관련 내용을 확인 할 수 있다. [8]

개인 PC 로 볼 수 있는 Client 단위에 설치가 되는 다수의 Application 은 여전히 문제가 있는 상태로 방치가 되고 있으며 보안패치 등의 문제도 여전히 존재하고 있다. 또한 인터넷 연결이 되어 있는 대부분의 Web Service 들이 취약성을 가지고 있고 직접적인 공격을 받고 있으며 또한 위험성을 가지고 있음을 언급하고 있다. Sans 의 Report 에서 지적한 또 하나의 이슈는 운영체제에서 드물게 발견되는 치명적인 취약성은 즉시 Worm 으로 발전이 되고 있다는 점과 Application 에 대한 Zeroday 취약성이 계속 증가하고 있음을 나타내고 있다. 사이버전을 준비하고 있고 연구하고 있는 단체라면 발표되지 않은 취약성을 가지고 있고 연구하고 있으며 언제든 사용 할 수 있는 상태로 준비를 하고 있을 것이다. 그림 8 에서 도식화된 취약성 발표 수치는 빙산의 일각으로 보는 것이 가장 정확한 시각이라고 생각 된다.

취약성이 있다고 하여도 실제 피해사례를 조사한 것은 유의미한 결과를 도출 할 수가 있다. Verizon 의 Data 유출 사례 조사에서 일반적으로 가장 큰 피해를 입은 경우를 그림 6 에서 보듯이 Hacking 과 Malware 라고 볼 수 있다. 직접적인 해킹과 우회적인 방식을 통해 설치한 Malware 를 통해 기밀정보를 유출하는 방식이 가장 큰 피해를 입힌 방식으로 조사가 되었다. 각 분야별로 살펴 보면 변화를 알 수가 있다.

그림 9 에서는 실제 피해사례에서 사용된 공격 기법들과 가장 많은 피해를 입은 경우를 나타내고 있다.

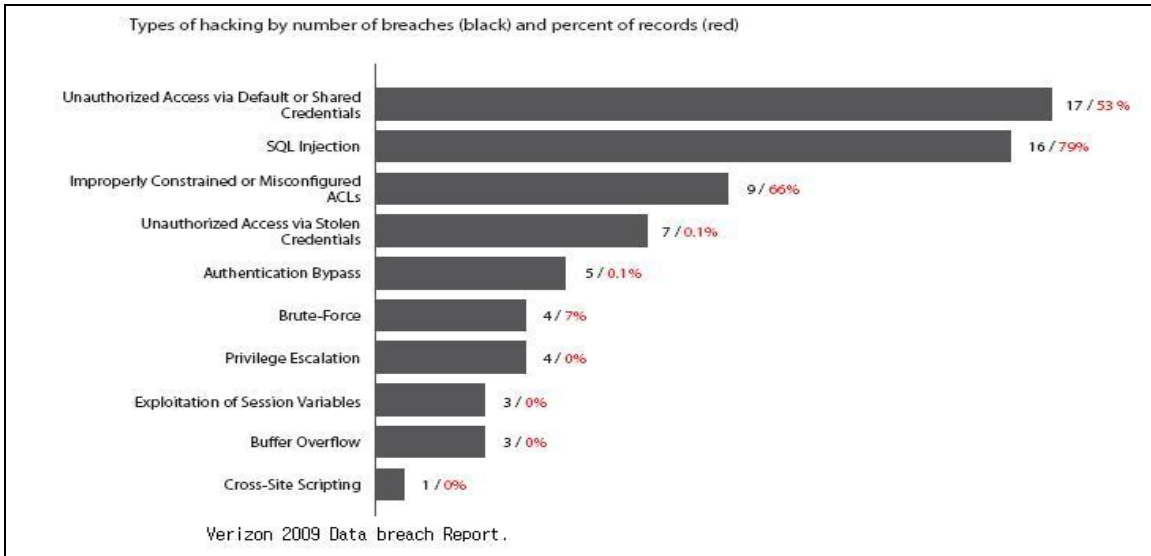


그림 9. Types of hacking

기업망에 대해 실제 피해를 가져온 경우는 기본 공유나 기본 설정에 관련된 문제와 SQL Injection , 잘못 적용된 ACL 에 대한 이슈들이 대부분의 사건사고를 차지하고 있다. 관점의 차이에서 보면 기업내부의 피해를 직접 입힐 수 있는 사안과 개인 사용자들에게 피해를 입히는 사안은 좀 더 다른 관점에서 볼 수가 있을 것이다. 악성코드의 유포의 관점에서는 SQL Injection 과 CSS 취약성이 높은 가중치를 가지게 될 것이고 기업내의 기밀정보의 유출의 관점에서는 잘못된 설정과 관리, SQL Injection 기법이 가장 높은 가중치를 가지게 될 것이다.

SQL Injection 은 두 가지 관점 모두에서 논의가 되었는데 특징을 가지고 있기 때문에 그러하다. 일반적인 SQL Injection 공격은 웹서버를 매개체로 하여 Database 서버를 공격 하는 것이다. 즉 내부망에 대한 공격이 직접 발생 할 수 있음을 의미한다. Database 서버를 공격 한다는 의미는 기밀정보에 대한 직접 유출이 가능하다는 점을 의미하고 악성코드의 유포는 Database 서버의 권한 획득 이후에 신뢰된 관계에 있는 웹서버의 소스코드를 변조함으로써 악성코드를 방문자들에게 배포하도록 하는 사안들이 현재도 계속 발생 되고 있어서 두 가지 관점 모두에서 중요한 사안이라 할 수 있다.

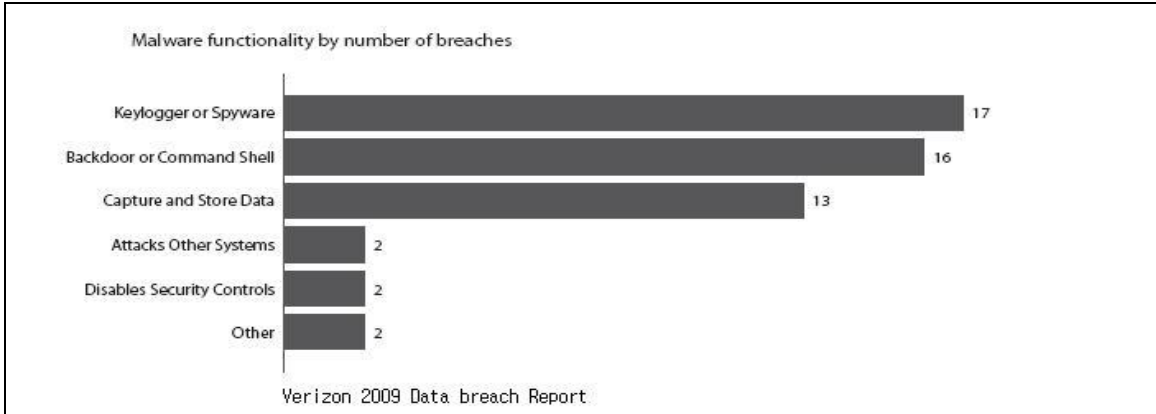


그림 10. Malware functionality

그림 10에서는 Malware에 대한 기능들을 나타내고 있다. 키로깅과 Backdoor, Capturing 기능은 다수의 Malware들이 가지고 있는 기능이라 할 수 있다. 조사 내용 중 특이 할 만한 사항은 그림 11과 같다. 공격자가 직접 제작한 Malware의 비율이 급증하고 있는 것을 볼 수 있다.

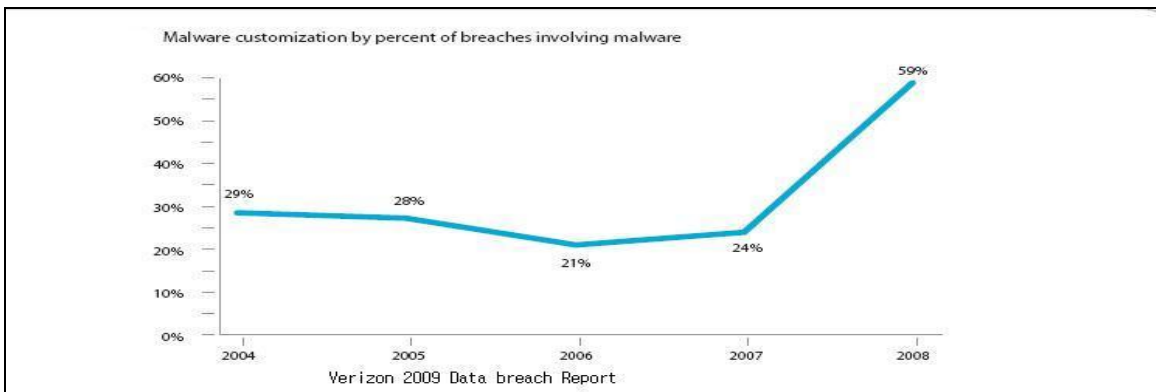


그림 11. Malware customization

Malware의 변형이 급증한다는 논점은 Anti-virus의 탐지를 회피하도록 만들어 지는 것으로 볼 수 있다. 앞으로 이와 같은 변형의 관점은 계속 증가할 것으로 예상된다. 즉 탐지가 되지 않는 악성코드들이 더욱 증가한다는 사실을 알 수 있다.

Malware의 변형증가와 공격 기법들의 발전은 실제 기업망이나 보호되고 있는 망에 대해서 목적을 지니고 공격을 하는 유형이 관찰되고 있다.

Targeted vs. opportunistic attacks by percent of breaches



다음의 차트에서는 일반적으로 발생되는 공격들이 목적을 가지고 또는 대상을 한정된 상태로 공격이 발생됨을 보이고 있다.

정보유출 사고의 대부분이 특정 대상을 목표로 이루어졌고 또 성공하였음을 나타내고 있다. 직접적인 공격과 여러 개의 목표를 가지고 공격한 비율이 72%나 됨을 관찰할 수 있다.

*Targeted attacks accounted for 90% of all compromised records.

기반시설의 위협 사례

앞서 설명한 단락에서 현재의 공격 동향의 변화와 Hacking 과 Malware 의 특성에 대해서 살펴 보았다. 최종적으로 목적을 가지고 대상을 한정된 공격과 Malware 의 변형을 통해 Anti-Virus 의 탐지로직을 우회 하는 것이 증가 하고 있음을 확인 할 수 있었다.

또한 주요 보안 장비와 기능들의 도입 비율을 통해 현재 가장 문제가 되고 있는 부분들이 무엇이고 어떤 대응들이 있는지 살펴 보았다. 이제 안전하다고 일반적으로 생각 하고 있는 기반 시설들에 대한 문제를 짚어 보도록 하자.

참고문헌 [1]에서 2002 년에 우선 지적한 기반시설에 대한 위협요소들은 다음과 같다.

1. 기업정보 시스템과 제어시스템의 연결 시에 침해 사고 발생가능성 존재함
2. 제어 시스템에 대한 Utility 와 Tool 을 이용한 외부에서의 원격 침해 가능성
3. 제어시스템을 제작한 Vendor 들의 원격지원이나 접근을 위한 서비스나 포트의 연결로 인한 침해 (백도어 및 트로이 목마 포함 가능성도 존재)
4. 내부자가 원격에서 Remote management tool 을 이용하여 제어시스템을 통제하려고 할 때의 침해 발생 가능성
5. Trojan 을 이메일등을 통해 침입 시킨 후 Reverse shell 연결을 통해 내부 시스템에 침입

위의 다섯 가지 경우를 일반적인 위협 요소로 짚을 수 있다. 이중 5 번의 경우에는 최근에도 발생이 가능하고 Sans 에서도 분석이 된 내용[8]으로 확인 할 수 있다.

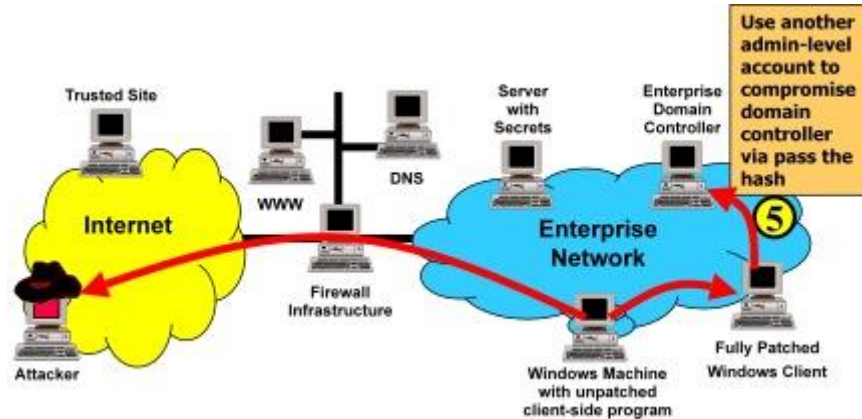


그림 12. Sans.org Reverse Shell Intrusion

그림 12 의 시나리오는 인터넷 사이트를 통해 클라이언트에 Malware 를 설치하도록 하고 설치된 Malware 가 Reverse channel 을 공격자에게 열어주어 내부망에 대해서 취약성을 공격 하고 권한을 획득하도록 이루어진 시나리오 이다. 체계적으로 보호 및 관리되고 있는 기업 내부망을 공격 하기 위해 사용이 되는 시나리오 이나 이 시나리오는 SCADA 망에 대한 직접적인 공격에도 매우 유용하게 사용이 될 수 밖에 없다. 신뢰된 상급자를 사칭한 메일을 보내 악성코드 설치를 유도하게 하고 Anti-Virus 에서 탐지가 되지 않는 Malware 를 내부 사용자의 PC 에 설치를 한다면 보다 더 쉽게 내부망에 대한 침입이 가능하다. 위에 언급한 다섯 가지 경우의 침입 시나리오는 부분적으로 사례 검증이 된 케이스도 존재하며 실제 위험성이 입증된 케이스 이다.

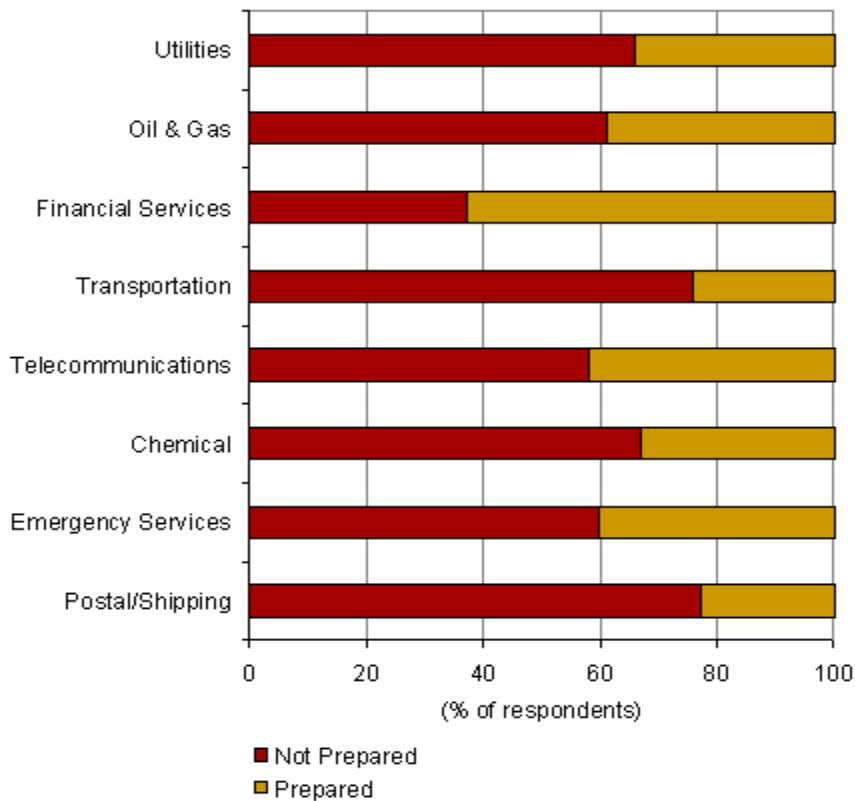


그림 13. Secure Computing survey

그림 13의 조사는 Secure Computing사에서 200여명의 각 산업계 리더들에게 조사를 한 내용이다. 각 기반 시설 산업별로 Cyber attack에 대해 준비가 되고 있는지를 조사한 2008년 통계치 데이터이다. 금융 관련된 산업에서는 준비 비율이 높게 나오고 있으나 그 외의 산업 전반에 걸쳐서는 상당부분 준비가 미흡함을 인지하고 있는 상태라 할 수 있다.

도로, 교통, 항공, 전력, 운송, 통신, 화학, Oil & Gas 등의 모든 부분에서 위험성이 상존하고 있음을 의미한다. 준비가 각 분야별로 체계적으로 진행되고 있다는 미국에서조차도 위험성에 대해서 인정을 하고 있는 상황이나 산업의 IT화와 고도화가 빠르게 진행되고 있는 국내에서는 얼마나 많은 노력을 각 산업별로 진행하고 있는지는 돌이켜 볼 부분이 존재한다.

일반적인 인식과 실제의 차이가 얼마나 있는지는 다음의 예로 확인 할 수 있다.

2007년 8월 IBM의 ISS의 Researcher인 Scott Lunsford는 핵발전소에 대한 침투 시험을 제안 받는다. 처음 설명을 들었을 때 외부네트워크와는 완벽하게 분리가 되어 있다는 설명을 들을 수 있어서 상당히 어려울 것으로 예상 하였다. 그러나 실제 침입을 시도하자 예상과 다르게 하루 만에 네트워크망에 연결을 할 수 있었고 일주일 이 지나자 핵발전소 전체를 제어 할 수 있게 되었다고 한다. [10]

완벽하게 분리가 되어 있고 외부에서는 접근 통로가 없을 것이라고 당연히 되는 중요 기반시설인 발전소 부분에도 문제가 있음은 위의 Lunsford의 사례를 들지 않고서도 충분히 가능하다.

2003년 1월 국내에는 인터넷 대란이라 불리는 1.25 대란이 슬래머 웜으로 촉발되어 큰 이슈를 낳긴바 있다. 이 시기에는 기반시설에 대한 환상을 깨뜨리는 또 다른 이슈가 존재 하였다. 완벽하게 분리되어 보호 되고 있을 것으로 여긴 핵발전 시설에 웜이 침입을 하여 5시간 이상의

가동이 중단된 사례가 발생한 것이다.[11] Ohio 핵발전소의 중단의 직접적인 원인은 Slammer 웜이였으며 완벽하게 분리된 내부망과 연결된 또 다른 직접 라인을 타고서 웜은 전파가 되었고 내부에 보안 패치 및 보호 장치가 없는 기반시설 운영 장비들은 감염이 되고 마비가 되었다. 핵발전소의 안정성을 감시하는 모니터링 장비들이 이상 증세를 보임에 따라 핵발전소의 운영은 전면 중단 될 수밖에 없는 상황에 직면한 것이다.

직접적인 공격에 영향을 받은 것은 항만 시설에 대한 사례도 존재한다. 텍사스 휴스턴의 항만은 대규모 항만으로서 군용, 민수용의 항만 시설이 동시에 존재한다. 이 항만의 시스템들에 대해 인터넷상에서 DoS 공격 (Unicode Exploit 에 의한)이 발생 됨에 따라 기상 시스템과 항해 시스템이 접속 불가 상태에 빠짐에 따라 정보를 수신 할 수 없는 상태에 처해 항만 운영이 중단된 사례가 존재한다. [12] 이 사례는 영국의 19 세 소년의 컴퓨터가 포함된 공격 그룹들이 공격을 함으로 인해 사건이 발생 되었고 보도가 된 바 있다.

2003 년은 이전의 Codered 웜과 같은 운영체제의 서비스를 직접 공격하여 권한을 획득하고 자신을 복제하여 다른 시스템들을 공격하는 웜들이 활성화된 시기이다. 블래스터웜과 웰치아 웜들이 그 부류에 속한다. 더욱 더 많은 기반시설의 문제 사례는 이 웜들이 활성화된 시기에 일반적으로 나타나고 있다.

2003 년 8 월에 발생된 뉴욕 대정전의 원인중의 일부에도 블래스터 웜이 존재할 것이라는 것은 당연시 되고 있다. 이 당시에 있었던 사건으로는 Air canada 의 항공 예약 시스템의 마비로 인해 운송이 중단 되었던 것과 CSX 기차의 연착 사고는 대표적으로 언급 되는 사례라 할 수 있다. [13,14]

대부분의 기반시설에 대한 모니터링 장비와 운영 장비들은 IP 연결이 가능하도록 구성이 되고 있고 상용 소프트웨어나 운영체제를 사용 하도록 변경이 계속 되고 있어서 향후에도 연결지점을 명확하게 끊고 최악의 상황을 대비한 보호 체계를 수립하지 않는다면 문제는 계속 될 수 있고 더 심각한 상황으로 손 쉽게 치달을 수 있을 것이다.

위와 같은 사례 이외에 목적을 가진 명확한 공격들도 이전부터 있어 왔으며 그 중의 한 사례로 지금도 언급 되는 사례는 폐기물을 처리하는 SCADA 시스템을 직접 공격하여 오작동을 일으키도록 한 사례이고 현재 까지도 언급이 되고 있다.

http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/
호주 퀸즐랜드에서 2000 년에 발생된 사례는 지금까지도 Scada 시스템에 대한 직접 공격으로 언급이 되고 있는 케이스다. NIST[9] 의 FISMA Control 항목과 관련되어 다양한 보안 대책에 대한 문제점을 지적하는 케이스로 언급이 되고 있다.

<http://www.wired.com/threatlevel/2009/03/feds-hacker-dis/>
캘리포니아 해안의 석유시추 플랫폼에 대해서 고용불만에 대한 항의로 내부자 계정으로 접근을 하여 석유유출 감지 시스템이 동작하지 않도록 한 케이스도 실례로 존재를 하고 있다.

기반시설에 대한 일반적인 오해는 대표적으로 세가지가 존재한다.

- 제어 시스템은 물리적으로 분리된 독자적 네트워크 상에 존재한다.
- SCADA 시스템과 기업 정보 시스템과의 연결은 강한 접근제어 정책을 보호 되고 있다.
- SCADA 시스템을 운영하기 위해서는 특별한 지식이 필요하며 침입자가 접근하고 제어하기가 어렵게 만든다.

이 세 가지의 오해 중에서 두 가지는 앞서의 예로서 충분히 해당 사항이 없음을 확인 할 수 있다. 마지막으로 SCADA 제어 시스템의 운영에 특별한 지식이 필요하다는 점에 대해서는 2007 년 8 월 라스베거스에서 있었던 Defcon 컨퍼런스에서 발표된 세션에서 환상이 깨졌다.

컨퍼런스에서는 Tipping Point 의 연구원으로 있던 Ganesh Devarajan 에 의해 SCADA 제어 프로토콜의 조작과 개요에 대한 시연[15]이 있었다. 여기에서 발표된 프로토콜과 조작법들은 일정수준을 보유한 전문가 그룹들에게는 그리 어렵지 않은 수준 이었다. 또한 프로토콜도 이미 공개된 상태이고 모니터링을 통해 손쉽게 조작법을 이해 할 수 있는 수준 이었으며 공격 및 분석을 위한 샘플 시연도 쉽게 이루어 진 상태임을 증명 하였다.

2008 년 1 월의 포브스 기사에서는 뉴올리언스에서 열린 Sans Conference 에서 CIA 의 관료인 Tom Donahue 에 의해 미국 외의 지역에서 미국의 전력 시스템에 침입을 하였으며 최소한 하나 이상의 경우가 여러 도시에서의 정전과 분명한 관련 있다는 언급을 함으로써 기반시설에 대한 침입이 실제로 발생되고 피해가 발생 되고 있음을 공언한 바가 있다. [17]

Scada 시스템에 관련된 정보들은 이미 70~80% 이상이 온라인 상에 오픈이 되어 있으며 현재의 Smart Grid 활성화에 IT 관련 대기업들은 적극적으로 참여를 하려고 하고 있는 상태이다. 규모의 경제를 이루어 내기 위해서는 대규모적인 판매가 이루어 져야 하고 표준화된 장비들의 도입이 필수적일 수 밖에 없다.

문제는 이제 전면에 드러날 수 밖에 없는 상태에 놓여진 것이다.

기반시설의 공격 시나리오

기반시설에 대한 공격 시나리오는 참고문헌[1]에서 공개한 공격 방식은 여전히 유효한 방식이다. 각 부분별로 살펴 보도록 하자.

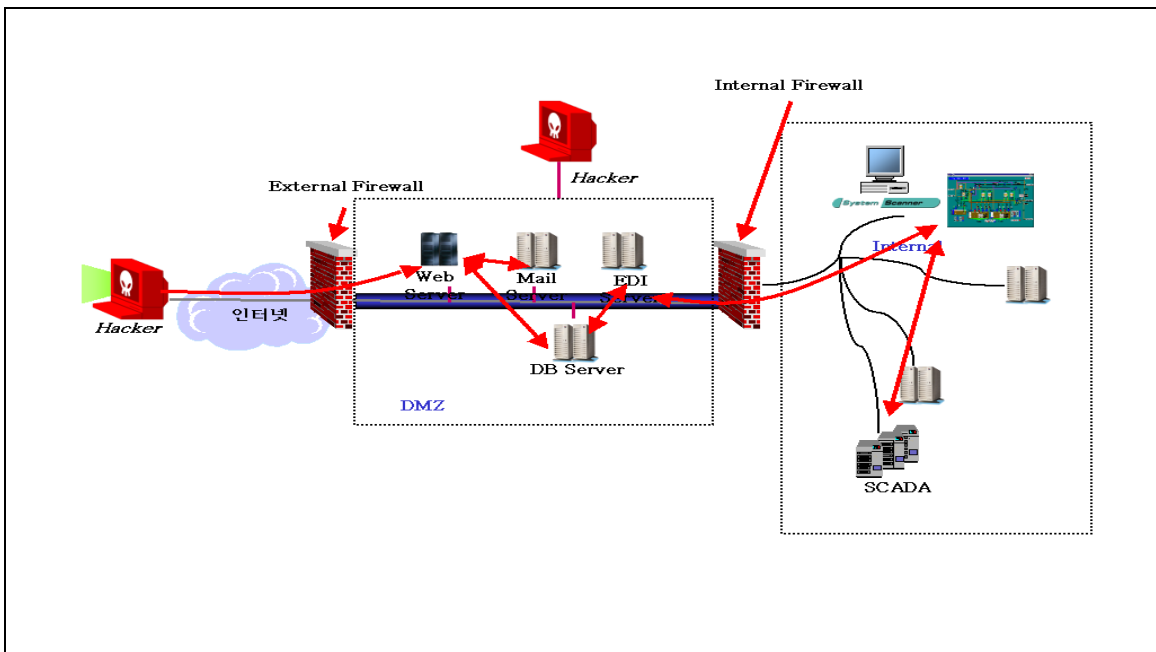


그림 14. 공격 시나리오 1

공격 시나리오 1 은 대외적인 서비스를 위한 DMZ 망을 웹 어플리케이션 취약성을 이용해 공격을 하고 Web Server 와 Database server 의 권한을 획득한 이후 내부망에 대한 공격을 진행 하여 권한을 획득하는 것을 의미한다. 여기에서 원격으로 접속을 시도 하도록 만드는 Reverse shell 공격은 매우 유효한 공격이 될 수 있다. 내부망에 침입한 이후 Scada 장비의 운영이나 모니터링 시스템에 침입을 하여 피해가 발생 될 수 있도록 조작을 할 수 있을 것이다.

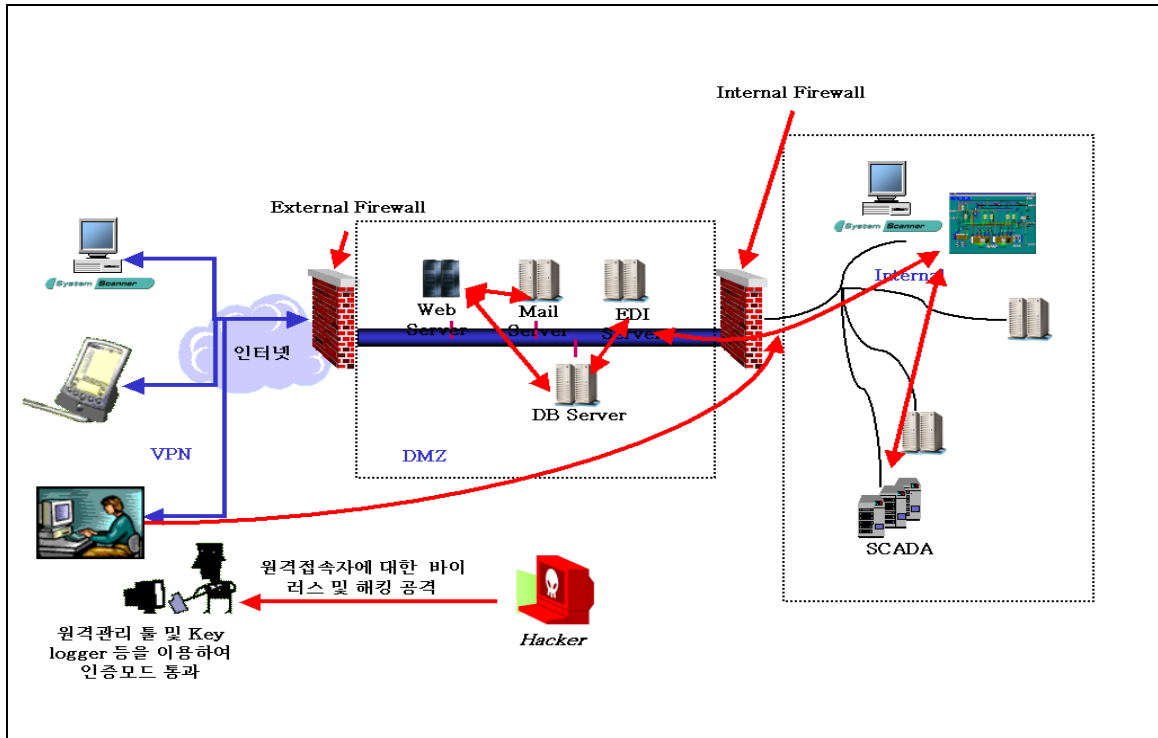


그림 15. 공격 시나리오 2

공격 시나리오 2 의 경우는 외부에서 연결하는 개인 사용자를 직접 공격 하는 유형으로 볼 수 있다. 타겟화된 공격을 진행을 하여 상급자의 PC 등을 Malware 를 통해 권한을 획득한 이후 사회공학적인 기법을 이용하여 접근에 관련된 담당자들을 공격 하여 권한을 획득한다. 공격동향에서 살펴 보았듯이 변형된 Malware 의 경우 Anti-virus 에서의 탐지 확률은 매우 낮을 수 밖에 없으므로 안정적인 백도어 운영이 가능할 것이다. 이후에 원격 관리나 비상시 장비 가동을 위해 접근하는 통로를 운영자가 입력 할 때까지 기다려서 찾아내면 장비에 대한 통제는 끝이 난다.

공격 시나리오 2 에서는 조금 더 다른 가능성이 Scada 장비에 이상이 생길 경우 즉시 조치가 이루어 져야 하고 상태에 대한 모니터링이 가능해야 하는데 현장에서 모든 기술자들이 모여서 즉시적인 조치를 하기에는 어려움이 있을 수 밖에 없다. 따라서 외부에서 접근 할 수 있는 통로들이 존재할 수 밖에 없을 것이다. 군 내부망에 접근하기 위한 인증서를 절취하여 내부망에 접근하여 정보를 유출한 2009년 3월의 국내 사례도 동일한 케이스를 반증 한다고 볼 수 있다. [16] (http://www.dt.co.kr/contents.html?article_no=2009101902010351739002)

앞으로의 기반시설에 대한 침입도 동일한 과정을 통해서 일어날 수 있을 것이다. 또한 권한 획득이 목적이 아닌 마비가 목적이라면 내부망에서만 동작하는 워코드를 작성하여 내부로 침입을 시킬 수 있을 것이다. 본격적인 사이버전이 도래하면 기본적인 인터넷 망을 이용한 공격 [18]

이외에도 내부망의 마비와 기반시설에 대한 마비를 위한 공격들도 헤아릴 수 없이 많이 일어 날 것이다.

사이버전의 전초라고 볼 수 있었던 2007 년의 에스토니아와 2008 년의 그루지아에 대한 러시아의 공격도 기반시설에 대한 공격에는 미치지 못했다. 실제로 그 정도까지 진행 할 필요성을 느끼지 못해서 일수도 있지만 전체적인 진행 강도를 살펴 볼 수는 있다. [18]

동원된 공격을 살펴 보면 다음과 같다.

- 주요 사이트에 대한 Web site 변조
- 언론, 관공서에 대한 Dos, DDos 공격 (결국 백본망의 네트워크 장비를 무력화 시킴)
- 웹서버 해킹을 통한 (SQL Injection) 악성 소프트웨어, Malware 의 대량 유포
- 주요 정치인들에 대한 스팸(대량 메일 발송)

에스토니아와 그루지아에 대한 공격에서 사이버전이 발발 하였을 경우 발생 될 수 있는 케이스를 일정 부분 참고 할 수 있다. 그러나 일정수준의 정보화와 산업화가 규모를 이루고 있는 국가와 지역의 경우에는 단순한 사이버 상의 피해로만 끝나지는 않을 것이며 산업 전반을 흔들 수 있는 큰 피해를 감내 해야 할 것이다.

예상하는 최악의 시나리오

지금까지 환경의 변화와 기반시설에 대한 논의, 문제점들을 살펴 보았다. 이제는 최악의 시나리오는 어떤 방식으로 나타날 수 있고 어떤 부분에 영향을 미칠 수 있는지 가상의 시나리오를 가볍게 구성하여 발생 될 수 있는 위험 요소는 어떤 방향인지 확인을 해보고자 한다. 지금까지 논의 되었던 공격의 특징들과 기반시설의 문제점들이 다 이용이 될 것이다. 가상으로 작성 하는 부분이므로 허구적인 부분들도 있으나 내부에 논의된 기술은 충분히 가능한 공격 방식으로 보아야 한다.

개요:

교통, 전력 (한전, 발전소, 전력거래소), 통신 (이동통신- 2 개사 이상), 인터넷 ISP (KT 포함 2 곳 정도), IPTV, Internet Phone, Ubiquitous Apartment 모두가 공격의 범주에 들어 간다.

구성

공격 그룹은 사전 준비 6 개월 가량에 4~5 개 팀 이며 각 팀당 4~5 명으로 구성할 경우 역할은 충분할 것으로 예상된다.

공격 방식:

이메일을 통한 신규 백도어의 설치, 직접 해킹을 통한 내부망 침투, Reverse 기능을 가진 Backdoor 를 통한 내부 침투, 일부 대리점 망에 대한 직접 침입, 웹서버 및 웹하드 업체를 해킹 하여 신형의 악성코드 여러 종을 사전 유포 하도록 한다.

실제 SCADA 동작 방식에 대한 이해를 하기 위해서 6 개월의 시간이 필요한 것으로 산정 하였으나 단순한 마비를 위해서라면 기간은 대폭 줄어 들 것으로 예상이 된다.

공격의 준비

1. 각 공격 그룹들은 서로 연결 되지 않으며 중복되지 않은 목표를 할당 받으며 각자 다른 방식의 악성코드와 연결 구조를 가진 Botnet 을 3~4 종 이상을 개발하여 설치 하도록 한다.
2. 4~5 개의 팀에서 개발된 악성코드는 20 여가지 이상이며 모두 다양한 백신들에서 탐지가 안되는 형태로 만들어져 있다. 또한 7.7 DDos 에서 사용 되었던 정기적으로 흩어진 명령 전송 서버에 접근 하여 명령과 공격 방식을 전달 받는 방식도 혼재 하여 정체가 드러나는 것을 최소화 한다.
3. 각 팀들은 영역을 나누어 각 기반 시설의 담당자 정보와 담당자 정보에 기반된 사회공학적인 공격을 실시 하여 내부 시스템에 접근하기 위한 권한을 획득 하고 내부 시스템들에 Reverse 연결이 가능한 백도어 들을 설치 하도록 한다.
4. 정보의 분석과 운영 모델의 이해
공개된 기반시설 장비와 조정이 가능한 장비, 불가능한 기반시설 장비를 선별하여 조정하여 혼란을 줄 것인지 마비를 시킬 것인지 결정
5. D-Day 를 기다리며 내부에 침입 시킨 백도어들에게 고유의 기능을 부여한다.
ISP 에서는 내부에서만 작동되는 워를 개발하여 침투를 시킨다.
6. 발전소와 댐, 홍수 통제소 등에 접근 권한을 획득 한다. (장비 납품 업체나 유지 보수 업체, 관리자에 대한 사회공학적인 해킹등 다양한 경로를 통해 권한을 획득)
7. 국내 및 해외의 중요한 웹서버들을 해킹 하여 대량의 악성코드를 유포한다. 웹 하드 업체의 해킹 이후 자동 업데이트 기능을 이용하여 최소 100 만대 이상의 좀비 PC 네트워크를 구성 할 수 있도록 한다. (7~15 일 이내에 가능)
8. IPTV 의 업데이트 기능 및 Internet Phone 의 업데이트 기능에도 백도어를 숨기도록 노력함.

D-Day [가장 혼란을 초래 할 수 있는 시점을 잡을 것으로 예상됨]

201X 년 12 월의 어느 날.

연말 결산과 송년회로 바쁜 한 주가 시작되는 월요일 그날이 D-Day 가 될 것이다.

전날에 서울 시내와 전국의 최근 신축된 아파트 일부에서 온도 설정이 안되거나 거실의 조명이 점멸 되는 현상이 관측 된다. 기온이 영하로 떨어진 새벽. 날이 밝아 올 무렵에 여름철에만 가동되는 홍수통제소의 경보 메시지가 주요 지점으로 가짜 메시지가 전파가 된다. 진위를 확인 하기 위해 허둥지둥 하는 시점에 상류의 댐 중 한 곳의 수문이 열리는 현상이 관측된다. 긴급하게 통제소에서는 전화를 통해 확인 해 보고자 하지만 전화는 연결이 되지 않는다.

하류에 위치한 한강 수계의 주민들에게 대피 및 주의를 하고자 경고방송을 시행한다. 10 분 후 국내의 3 개중 두 개의 통신사 회원들 전체에게 긴급 메시지가 발송이 된다. “ 전쟁 발발 사상자 속출 긴급대피 “ 오전 출근을 준비하고자 하는 시민들은 긴급한 소식에 TV 를 켜보지만 디지털 아카이브 시스템으로 방송 송출을 하는 시스템들이 오작동을 일으켜 TV 에서도 시그널이 제대로 나오지 않는 상황 발생.

메시지는 3분 간격으로 계속 전달이 되어옴. 동시에 국내 주요 포털 및 언론사에 대한 DDos 공격 시작됨. 9시를 기해 증권사, 은행, HTS, 방송사, 신문사, Internet Phone, IPTV 망에 대한 대규모적인 DDos 공격이 시작됨.

초고층 아파트와 사이버 관리가 일반화된 아파트들에서는 조명이 계속 점멸이 되고 온도는 최저 온도로 계속 설정이 됨. 전화 연결 불통 현상 지속됨. ISP 내에서는 내부망을 공격 하는 웹들이 대량 트래픽을 발송 하여 서버가 죽었다가 살아나는 현상이 계속됨.

절반 이상의 Internet Phone 은 주요 신고 전화망을 지속적으로 Fake calling 을 함으로써 연락체계와 대응체계를 마비시킴.

전력 체계가 부분 단절 되어 일부 지역의 정전이 일어남.

불과 30분 이내의 시간 동안 완벽하게 연결체계를 마비시키는 상태가 발생.

혼란에 빠진 시민들은 이곳 저곳에 안부를 묻고 소식을 묻고자 하나 대부분의 전화는 과도한 이용으로 불통상황에 빠짐. 도로로 쏟아져 나온 차들은 자동화된 고속도로의 시그널이 전부 붉은색으로 표시 됨에 따라 진행을 하지 못함.

시간이 지남에 따라 항만 활동도 정지가 되고 운송시스템에 대한 통제들도 마비가 되어 전국의 교통망은 마비가 된 상태에 돌입한다. 전력, 교통, 운송, 통신, 인터넷 ISP, 포털 및 언론사, 주요 서비스 업체들에 대한 대규모 적인 공격과 교란은 제한된 인력으로 순차적인 해결을 진행 할 때 까지 계속해서 문제를 일으킨다. 최소 2주에서 4주 이상을 계속되는 혼란 속에서 지낼 수 있을 것이다. 그리고 공격자들은 그들이 원하는 목적을 충분히 달성한 상태가 될 것이다. 국도의 혼란 속에서 그 어떤 것도 벌일 수 있을 것이다.

결론:

고도화된 기술과 전략, 팀을 구성 할 수 있는 단위 조직을 가지고 있는 모든 곳들은 충분한 공격이 가능하며 향후 발생 될 수 있는 사안이라고 볼 수 있다.

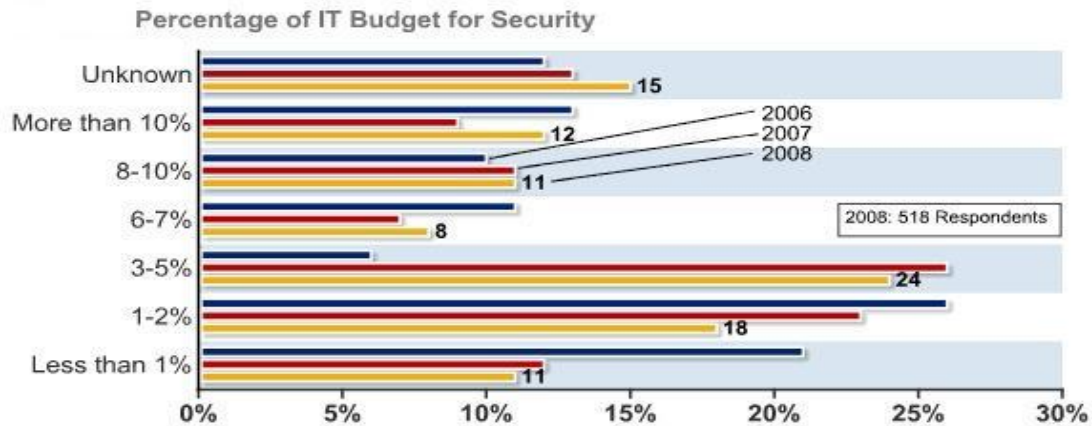
국도의 혼란과 문제 상황은 알려지지 않은 백도어와 악성코드들을 3~40종을 대량으로 운용하며 DDos 공격이 가능한 좀비 PC를 대량으로 확보하고 대응이 불가능 하도록 함으로써 완벽하게 혼란에 빠지게 할 수가 있다. 대응 인력의 분산과 공격 대상의 다각화, 대규모적인 시스템의 운영, 다양한 방식의 Malware 등을 활용 함으로써 공격자들 혹은 공격 그룹은 소기의 목적을 달성 하게 될 것이다. 제 삼자에 의한 전쟁 상태 유도 및 경제적 공황의 초래는 심각한 피해를 유발하게 될 것이다. 제 삼자는 가상의 적국이 될 수도 있고 경제적 위기로 인한 오늘의 동지가 적이 될 수도 있을 것이다.

위의 시나리오는 간략하게 작성 하였으나 각 산업 및 제어시설 부분에 침입이 실제로 가능함을 이전의 항목들에서 사례를 들어 설명을 하였다. 사이버 제어가 가능한 유비쿼터스 도시와 아파트, IP 기반의 통신망 서비스, IP 기반으로 통제되고 운영 되고 있는 제어 시스템들에 대한 상세한 침입과 가능성은 각 항목별로 개별로 설명이 되어야 한다. 전체적인 위험성과 공격 가능성을 보인다는 측면에서 본 논문에서는 개략화되고 간결화된 시나리오로 대체한다. 최초의 사례가 대규모로 발생 할 가능성은 점차 높아지고 있다. 이제는 공격동향을 주시하고 각 산업 분야별로 체계화되고 종합된 노력을 기울이지 않는다면 그 날의 초침은 더 빨리 돌아 갈 것이다. 전체의 관점에서 어떤 점들을 준비해야 하고 노력 해야 하는지 개괄적으로 살펴 본다.

Security Plan

모든 것의 시작은 중요성과 비중을 얼마나 두느냐에 따라서 달라지고 있다. AFCOM's 2009/2010 Data Center Trends 에서 조사된 바에 의하면 [19] 1/3 정도의 기업만이 재해복구에 대한 계획을 가지고 있다고 한다. 조사대상의 60% 이상의 기업이 cyberterrorism 이 위협이 된다고 인식을 하고 있었으나 조사대상의 20.8% 만이 보안정책과 절차를 가지고 있는 것으로 나타났다.

특히 예산이 뒷받침 되지 않는 보안 행위는 의미가 없는 경우가 많이 있다. 그만큼 중요도에 인식도 낮을 수 밖에 없을 것이다. 아래의 그림 16 은 CSI/FBI 에서 조사된 결과는 IT 예산 중 Security 예산의 비중을 조사한 것이다. 시간이 지날수록 많은 기업들이 IT 예산 중 보안 관련 예산을 증가 시키는 것을 확인 할 수 있다.



CSI/FBI Computer Crime and Security Survey -2008

그림 16. IT Budget for Security

예산의 증가는 보안 관련된 위협들이 심각할 정도로 나타나고 있어서 관심을 가지고 노력을 하고 있음을 의미한다. 전체 IT 예산에서 보안 관련된 예산이 차지하는 비중도 늘고 있으며 다수의 기업들이 비율을 높여서 보안 분야에 투자를 하고 있다. 위협에 대한 인식이 예산결정권자에게 있을 때에 생겨날 수 있는 변화라고 할 수 있다.

국내의 현실은 과연 어떻게 조사하기가 두려울 정도이다. 각 산업별로 어느 정도의 위협을 인식하고 대비를 하고 있는지 어떤 노력들을 진행하고 있는지 반드시 짚어 보는 것이 필요할 것이다.

보안 대책에서 가장 중요한 부분은 위협을 인지하는 부분과 위협을 제거하기 위해 노력 하고 투자하는 부분이 가장 중요한 역할을 차지한다.

위험의 인지 부분은 Awareness 로 확인 할 수 있으며 국내의 현실과 한번 비교해 볼 필요성이 있을 것이다.

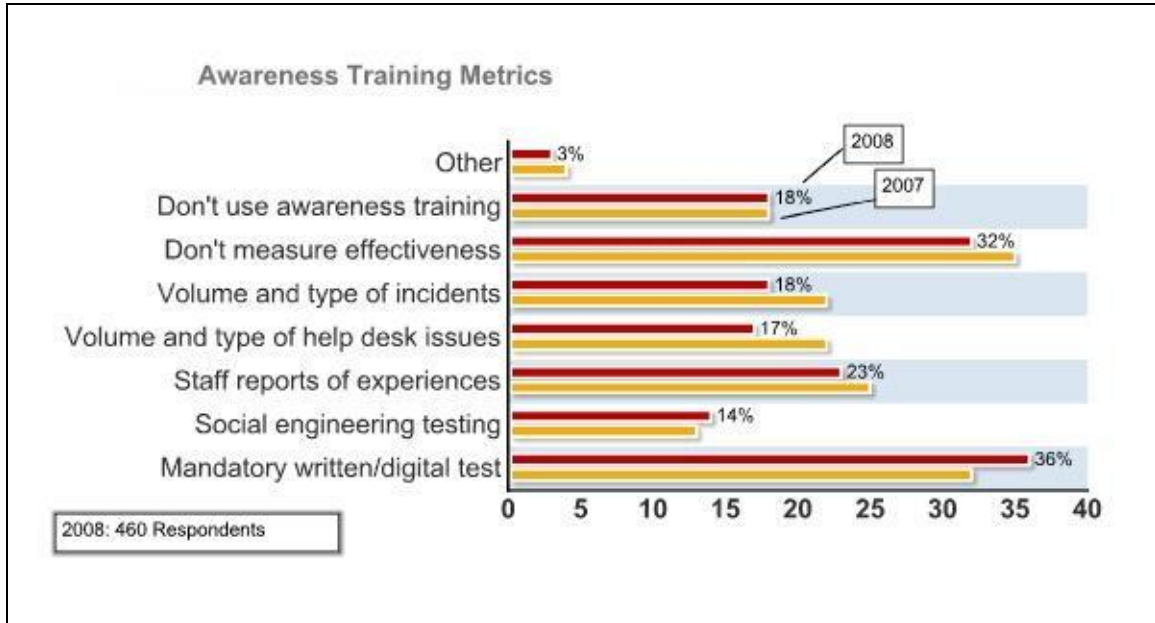


그림 17. Awareness Training

비율적으로 그림 17 에서 언급하는 케이스들에서 의미 있는 것은 2007 년과 2008 년의 비교에서 증가된 부분을 중점적으로 보면 된다. Social engineering testing (Fake mail) 과 Mandatory written/digital test 부분의 증가 폭을 유심히 보면 관점의 변화를 알 수가 있다.

Awareness Training 부분에 지켜야 되고 준수해야 될 내용을 기술하고 이행 하도록 하며 주기적으로 상기시키는 것이 포함이 되고 실제적인 테스트를 통해서 위험성을 줄일 수 있도록 만들어 가는 과정이라 볼 수 있을 것이다.

국내에 위험성에 대한 인지가 먼저이며 기반시설에 대한 위험성의 논의를 제한적이거나 공개적으로 할 수 있어야만 문제의 현실들이 드러날 것이다. 공개적인 문제의 논의 이후에 대책들이 가능하며 산업 전반의 인식도를 높여서 실제적인 대응 행동을 할 수 있도록 만드는 것이 중요하다.

문제점 항목별로 심도 있는 인터뷰와 다양한 전문가들의 의견을 수렴하여 문제 항목을 도출하고 각 항목별로 지켜야 되고 준수해야 될 기술적, 정책적 가이드 라인을 제공 함으로써 도움이 되도록 하여야 한다. 보다 더 중요한 것은 위험성에 대한 인식이 가장 먼저라고 판단된다.

각 항목별로 수준의 파악은 NIST 와 같은 표준 Control 항목을 규정[20]하고 각 항목별로 준수 사항을 체크하는 것이 가장 중요한 시작점이 될 수 있을 것이다.

창의적인 인력들이 많은 부분을 적극적으로 커버하지 않는다. 그러나 창의적인 인력들의 의견을 경청 하고 반영 할 수 있다면 현실에서 발생 될 수 있는 문제와 이미 알려진 문제로부터의 피해를 최소화 하고 막을 수 있을 것이다.

기술적인 사안들과 세부적인 보호 방안들에 대해서는 참고문헌[1]의 내용들은 여전히 유효함으로 참고 할 수 있을 것이다.

기술적으로 향후 가장 시급하게 요구되는 부분은 악성코드에 대한 종합적인 정보와 분석을 진행 할 수 있는 글로벌한 규모의 분석업무 수행이 가능한 기관이나 단체가 필수적으로 요구되며 또한 기술중립적인 입장에서 진취적인 노력과 가능성 측면을 고양 해야만 한다.

두 번째로는 긴급사안이 발생 하였을 경우 통제가 가능한 대책 및 통제 기구의 필요성이 심각하게 대두 된다.

세 번째로는 인터넷 보안 분야에서 창의적인 인력들이 양성 될 수 있도록 환경을 만들어가고 성장할 수 있는 바탕을 만들어 감으로써 전체적인 산업과 시너지를 내는 것이 필요하다.

기반시설은 현재의 수준과 상태를 표준적인 값과 비교하여 상대적인 수준을 파악하는 것이 가장 급선무라 할 것이다. 그래야 그 다음 단계의 대책들에 대해서 논의를 할 수 있기 때문에 더욱 그러하다.

앞으로 가야 할 길과 과정은 너무나도 먼 길이다. 그러나 움직이지 않으면 당장에라도 마주칠 수 있는 위협이다. 어떤 인식을 가지고 걸어 가느냐에 따라 시간은 점점 더 느리게 다가 올 수 있을 것이다.

References

1. <http://blog.naver.com/p4ssion/50001878886> -기반시설에 대한 보안문서 2002 년 10 월
2. <http://www.airpower.maxwell.af.mil/airchronicles/cc/McNeal.html>
3. <http://blog.naver.com/p4ssion/50031034464> - 상상하기 어려운 위협 대규모 sql injection 공격에 대한 동향 분석 문서
4. http://www.computerworld.com/s/article/9080580/Huge_Web_hack_attack_infects_500_000_pages
5. <http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2008.pdf>
6. http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf
7. <http://www.cert.org/stats/>
8. <http://www.sans.org/top-cyber-security-risks/#zero-day>
9. http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf

10. http://www.forbes.com/2007/08/22/scada-hackers-infrastructure-tech-security-cx_ag_0822hack.html

11. <http://www.securityfocus.com/news/6767>

핵발전소의 워에 의한 중단 사례를 기술

12. <http://news.zdnet.co.uk/security/0,1000000189,39116978,00.htm>

<http://news.bbc.co.uk/2/hi/technology/3202116.stm>

13. <http://www.pcmag.com/article2/0,2817,1226680,00.asp>

14. <http://www.cbsnews.com/stories/2003/08/21/tech/main569418.shtml>

15.

<http://www.dc414.org/download/confs/defcon15/Speakers/Devarajan/Presentation/dc-15-devarajan.pdf> Defcon 2007 에서 Scada Protocol 관련 내용의 발표.

16. http://www.dt.co.kr/contents.html?article_no=2009101902010351739002

17. http://www.forbes.com/2008/01/18/cyber-attack-utilities-tech-intel-cx_ag_0118attack.html

18. <http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf>

19. http://news.cnet.com/8301-1009_3-10385230-83.html

20.

http://csis.org/files/publication/Twenty_Critical_Controls_for_Effective_Cyber_Defense_CAG.pdf NIST 의 보호 방안과 연계된 Control 항목을 기술.

About

주말의 하루를 온전하게 이 글을 작성하는데 할애 해준 사랑하는 아내와 딸 서운에게 감사를 전합니다. 짧은 시간에 여러 고민을 녹여 넣는 과정에서 무리한 부분들도 있었고 가급적 위험성에 대해서는 많은 사람들에게 널리 알리고픈 마음에 급하게 작성을 하게 되었습니다.

부족한 부분에 대해서는 깊은 아량으로 봐주시고 사이버전 시나리오 부분에 대해서는 소설 같은 예상을 하지 않으려 하였습시다만 급하게 쓴 관계로 그냥 두도록 하겠습니다.

미치지 못하면 도달하지 못한다는 말이 있습니다. 어느 분야나 마찬가지 이겠지만 인터넷 보안 분야는 더 심하다는 것을 느낍니다. 많은 선.후학님들의 다방면으로의 노력이 끊이지 않기를 바랍니다.

[- 바다란 세상 가장 낮은 곳의 또 다른 이름](#)