

7.7 대란 DDoS 공격실태와 현황

2009 년 7 월 7 일, 이메일을 확인하려 했으나 사이트 접속이 되지 않는 것을 시작으로, 금융권, 언론기관, 정부사이트, 쇼핑몰 등 대한민국의 굵직굵직한 사이트가 해커의 DDoS 공격으로 모두 마비되었다. 7 월 10 일까지 이어진 인터넷 테러는 우리나라 보안 업계의 현실에 많은 시사점이 되어 주고 있다. 이번 DDoS 의 공격 현황과 그것으로 인해 확인할 수 있는 이야기들을 정리해 보았다.

필자 소개

강병탁 window31@empal.com, www.window31.com | Microsoft MVP Developer Security 로 활동하고 있다. 올해로 Y2K 버그 문제가 마지막으로 거론된 지 벌써 10 년이 지났다. 요즘 해킹·보안 업계와 그 시절 Y2K 버그와의 공통점은 발등에 불이 떨어져야 처리하는 사고방식이 아닌가 싶다. 1999 년이나 돼서야 리팩토링을 하는 것처럼 해킹 사고가 터져야만 인식을 하게 되는데, 올해 부터는 급한 불을 끄며 숨 가쁘게 움직이는 것 보다 먼저 나서서 예방하는 보안 인프라가 자리 잡았으면 하는 소망을 갖고 있다.

Copyright © 2009, 강병탁 (window31)

이 문서는 Creative Commons 라이선스를 따릅니다.

<http://creativecommons.org/licenses/by-nc-nd/2.0/kr/>

Intro

지난 7 월 7 일 오후, 대한민국의 상당수가 이용하고 있는 포털 사이트의 이메일이 접속되지 않았다. 또, 인터넷뱅킹을 이용하려던 사용자들도 은행 사이트에 접속할 수 없었다. 여러 유명 쇼핑몰 사이트 또한 페이지를 찾을 수 없다는 하얀 바탕위에 깨진 글자만을 출력했을 뿐, 접근이 불가능했다. 처음엔 단지 일시적인 인터넷 장애 증상이라고 생각했지만 시간이 지나면서 공공 기관 등 접속이 마비되는 사이트가 늘어나자 비로소 이것이 해커의 공격이라는 것을 알게 된다. 밤 늦은 시간이 되어가서야 사람들은 DDoS 공격에 의한 사이트 마비라는 것을 깨닫게 되고, 언론에서도 자정이 넘은 시간임에도 불구하고 뉴스를 발표하기 시작했다. 일부 사람들은 지난 1.25 대란이 다시한번 오는 것이 아닌가 하는 걱정까지 하기에 이르렀다.

이번 DDoS 공격 현황

사람들이 체감하기 시작한 날짜는 7 월 7 일이었지만, 실제 공격은 7 월 5 일부터였다. 미국의 20 여개 주요 정부기관을 공격하고 한국의 금융, 포털, 정부기관 등으로 이어지기 시작했는데, 우리나라의 공격이 7 월 7 일부터 본격화 되었기 때문에 한국에서 느끼는 본격적인 피해는 7 월 7 일부터로 각인하게 된다. 놀라운 것은 공격에 이용된 바이너리를 분석한 결과, 공격 시간이 정해져 있음으로 정해진 시간대에 공격을 하도록 설계되어 있다는 것이다. 날짜별 공격 현황을 정리해 보았다.

| 제 1차 공격 | 제 2차 공격 | 제 3차 공격 | 제 4차 공격 |
|--|---|---|--|
| 2009.07.05 02:00 ~ 2009.07.05 14:00 | 2009.07.07 18:00 ~ 2009.07.08 18:00 | 2009.07.08 18:00 ~ 2009.07.09 18:00 | 2009.07.09 18:00 ~ 2009.07.10 18:00 |
| www.whitehouse.gov whitehouse.gov www.faa.gov faa.gov evisaforms.state.gov www.whitehouse.gov www.faa.gov www.ustreas.gov www.dhs.gov www.state.gov www.dot.gov www.ftc.gov www.nsa.gov www.usps.gov www.voanews.com www.yahoo.com www.defenselink.mil travel.state.gov www.nyse.com www.nasdaq.com www.site-by-site.com www.marketwatch.com finance.yahoo.com www.usauctionslive.com www.usbank.com www.amazon.com | www.president.go.kr www.mnd.go.kr www.mofat.go.kr www.assembly.go.kr www.usfk.mil blog.naver.com mail.naver.com banking.nonghyup.com ezbank.shinhan.com ebank.keb.co.kr www.hannara.or.kr www.chosun.com www.auction.co.kr www.whitehouse.gov www.faa.gov www.dhs.gov www.state.gov www.voanews.com www.defenselink.mil www.nyse.com www.nasdaq.com finance.yahoo.com www.usauctionslive.com www.usbank.com www.washingtonpost.com www.ustreas.gov | www.mnd.go.kr www.president.go.kr www.ncsc.go.kr mail.naver.com mail.daum.net mail.paran.com www.auction.co.kr www.ibk.co.kr www.hanabank.com www.woonbank.com www.alttools.co.kr www.ahnlab.com www.usfk.mil www.egov.go.kr | mail.naver.com mail.daum.net mail.paran.com www.egov.go.kr www.kbstar.com www.chosun.com www.auction.co.kr |

<표 1> 시간대별 DDoS 공격 현황

1 차 공격 (2009.07.05 ~ 07.06)

1 차 공격은 미국의 20 여개 정부기관, 공공기관, 언론, 포털 등의 사이트가 대상이었다. 주요 리스트로는 미국 백악관, 미국 국무부, 미국 교통부, 미국 국가안전보장국, 나스닥, 야후, 미국옥션, 뉴욕 증권거래소 등 20 개이며, 전체 사이트가 접속 불능 상태가 되었다. 상당수의 좀비 PC 가 한국 IP 였기 때문에, 공격을 당한 대부분의 사이트에서는 한국 IP 를 전체 차단하는 방식으로 처리하였다. 따라서 사이트는 복구되었지만 한국에서는 여전히 접속할 수 없는 상태로 유지하게 되었다 (한국에서는 현재 이시간까지 접속이 되지 않고 있다)

2 차 공격 (2009.07.07 ~ 07.08)

2 차 공격이 시작되며 본격적으로 대한민국이 피해를 입게 된다. 공격 시작은 pm 6:00 부터였으며, 역시 미국과 마찬가지로 정부기관과 금융권, 포털을 중심으로 공격이 이뤄졌다. 대표적인 사이트로는 청와대, 외교통상부, 국방부, 국회, 네이버, 옥션, 농협, 외환은행, 조선일보 등이며 모두 사이트 접속 불가 상태가 되었다. 이 때부터 국내의 언론에 여기저기 DDoS 공격이 보도되기 시작했으며, 다음날은 9 시 뉴스에까지 등장하는 등 대한민국 전역에 공격 소식이 전파되었다. 미국에서도 1 차 공격때의 리스트가 그대로 공격이 지속되었지만 한국 IP 를 차단한 사이트에서는 큰 피해는 입지 않게 된다.

3 차 공격 (2009.07.08 ~ 07.09)

역시 2 차 공격때 이용된 리스트가 거의 그대로 이용되며 공격이 지속되었다. 네이버 등 몇몇 포털은 도메인을 리다이렉트 시키는 등 자체적인 대응방법으로 큰 피해를 입지는 않았지만, 그런 처리라도 할 수 없는 업체들은 여전히 사이트가 마비되는 상황이 지속되었다. 또 새로이 추가된 사이트가 있었는데, 대표적으로 안티바이러스 서비스 업체다. 3 차 공격이 시작된 때 즈음에는 이미 백신 개발사에서도 좀비 PC 를 치료할 수 있는 프로그램을 배포하기 시작한 때이므로, 공격을 지속하려면 백신 업데이트나 백신 이용부터 차단하자는 의도가 숨어 있는 것으로 보인다. V3 를 개발하는 안철수연구소나 알약을 서비스하는 이스트소프트 등의 접속을 차단시키며 공격이 계속되었다. 또, 이때부터 MBR 등 하드디스크를 손상시키는 변종이 발견되기 시작했는데 이러한 행동을 하는 이유는 좀비 PC 에 이용된 대상은 목적을 끝내고 존재를 은폐하도록 하기 위해서라고 추측된다. 하지만 다행히 실제 피해는 크지 않았으며 내용은 뒤에서 다시 설명하도록 하겠다.

4 차 공격 (2009.07.09 ~ 07.10) – 공격종료

이번 공격의 특이점은 타겟의 리스트가 대폭 감소되었다는 것이다. 아마도 공격이 네번쯤 지속되다 보면, 내부적으로도 자구책을 충분히 마련했으리라는 생각하고 몇몇 사이트만 더욱 집중적으로 공격하자는 계산이 깔린 것이 아닐까 한다. 사이트는 10 개 이하로 줄었으며 대부분이 지난 공격에 이용되었던 리스트에 해당된다. 다행인 것은 이미 상당히 많은 사이트가 도메인 주소를 변경하거나, GSLB 구성, DDoS 대응 장비 업그레이드 등으로 대비를 하기 시작해서 지난 공격만큼 큰 피해를 입진 않았다. 그리고 공격의 파워가 느슨해진 4 차를 마지막으로 7 월 10 일 pm6:00 부터 공격이 종료되었다.

DDoS 공격의 피해

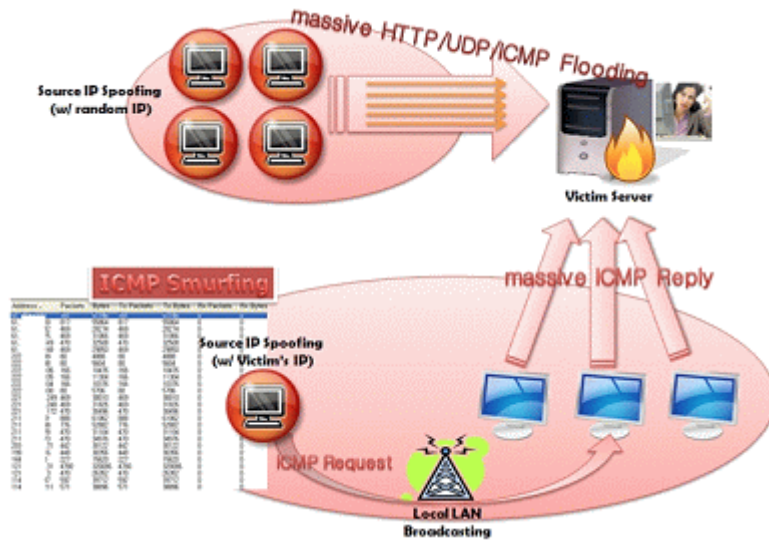
DDoS 공격을 당해본 분들은 알고 있을 것이다. DDoS 공격을 피하는 이들은 백이면 백 모두 금전적인 대가가 목적이다. 예를 들어 인터넷 사이트를 운영하는 어떤 사이트에 갑자기 3 분 정도 접속마비 상태가 일어난다. 그리고 발신지를 알 수 없는 어떤 사람으로부터 메시지가 날아온다. 방금의 사이트 마비 증상은 자신이 일으킨 DDoS 공격이며 몇시간 내에 얼마에 해당하는 금액을 자신에게 보내지 않으면 사이트를 다운시켜 버리겠다는 협박을 한다. 그러면 당장 대책도 없고 어찌해야 할 바를 모르는 기업의 입장에서는 사이트가 다운되면 업무를 중단할 수 밖에 없고, 그러면 매출을 올릴 수 없게 되므로 해커가 원하는 요구사항을 들어줄 수밖에 없게 된다. 그리고 회사 이미지상 이러한 내용을 언론에 보도할 수도 신고하기도 까다로운 입장이다. 마치 자식을 유괴당한 후, 돈을 보내주고 경찰에 신고도 하지 못하는 그런 상황과 유사하다고 볼 수도 있다. 이처럼 예전부터 DDoS 공격에 대한 이슈는 계속 존재했었다. 하지만 그것을 다들 쉬쉬했기 때문에 수면 위로 떠오르지 않았을 뿐 이처럼 잠재된 문제점이 심각했고 그 뒤에는 항상 금전적인 대가가 목적으로 깔려 있었다.

하지만 이번 공격은 어떠한 금전적인 요구도 없이 단지 파괴와 공격만을 자행했으며, 기존 DDoS 교과서와는 매우 다른 양상을 보여주었다. 이만큼 대규모의 공격을 감행했으면 그만큼 기업에 끼치는 매출 손실도 엄청날 것이므로 원하는 금액을 얻어갈 수도 있었을 텐데(예를 들어 옥선의 경우는 언론에 보도된 내용에 의하면 이번 DDoS 공격으로 입은 피해액이 70 억에 이른다고 한다), 전혀 그러한 행위가 없어서 더욱 오리무중 상태다. 살인사건에서도 복수 등 살인자의 의도를 알 수 있는 사건은 추적이 용이하지만 어떠한 논리도 없이 살인을 자행하는 살인마는 추적하기 힘든 것처럼, 의도가 깔리지 않은 사건은 배후를 파악하기 힘들다. 이번 DDoS 공격도 의도를 전혀 알 수 없으므로 현재 배후조차 발견하지 못하고 있다.

좀비 PC

이번 좀비 PC 에는 세가지 시사점을 가지고 있다. 첫번째로 대규모 숫자의 동원이다. 이번 좀비 PC 에 동원된 컴퓨터는 약 20 만대이며, 일반적으로 알려져 있던 DDoS 공격 중 거의 최대규모라 할 수 있다. 두번째로는 대부분의 좀비 PC 가 한국의 가정집 PC 라는 점이다. 미국 등을 공격했으면서 한국의 PC 들을 이용해서 공격을 자행했다는 점은 해커가 언제든지 원하면 개인 PC 를 자신의 군사력에 동원할 수 있다는 의미로 우리나라의 보안 실태를 그대로 보여주는 한 사례라고 생각할 수 있다. 마지막으로 세번째는 공격 방식의 변화다. DDoS 공격 바이너리를 개발한 해커는 기존 장비에 대해 잘 알고 있는 사람으로 추정된다. 공격에 사용된 패킷은 매우 작은 크기이다. 매우 소량의 공격 (100pps, 1Mbps 이하) 만을

이용함으로써 기존 DDoS 방어 장비를 가볍게 우회하도록 개발되었다. 이런 이유 때문에 장비를 갖추어도 불구하고, 조기대응이 늦어지게 되었다.

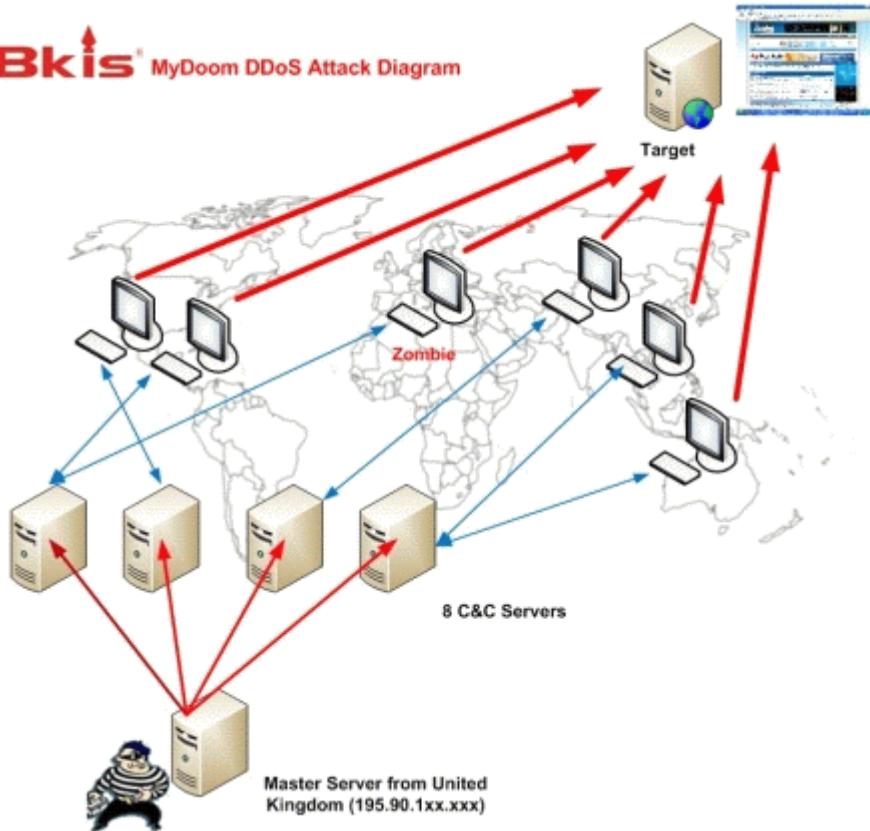


<화면 1> 7.7 대란 DDoS 공격 트래픽 유형 (자료출처 : Ahnlab)

C&C 서버는 존재하지 않았다?

공격을 조종하고 명령을 내리는 서버인 C&C (Command & Control) 에 대한 이야기로 언론에서 여러 번의 반복이 있었다. 먼저 처음 DDoS 발표 당시에는 기존 DDoS 와의 비교내용을 설명하며 C&C 서버가 없는 것이 기존과의 차이점이라며 부각하였다. 하지만 베트남 Bkis 의 보안 분석에 따르면, C&C 는 존재하고 있었으며, 특이한 것은 중간 경유지가 별도로 또 존재하고 있었다는 것을 알 수 있다. 마스터에 해당하는 C&C 가 있지만 여기서 좀비 PC 에게 곧바로 명령을 내리는 것은 아니며 8 대의 중간 컨트롤러들에게 명령을 내리면 좀비 PC 들은 그 중간 PC 들에게 지령을 받아 공격을 수행한다는 것이 요점이다. 기존 DDoS 는 C&C 와 지속적으로 통신을 하며 커뮤니케이션을 하지만, 이번 DDoS 의 경우는 Sleep() 등으로 계속 잠자고 있다가 간헐적으로 한번씩 C&C 와 교류하는 까닭에 아마 급하게 분석하다보니 이러한 부분을 놓치고 발표하게 되어서 초반에는 C&C 가 없었다는 식으로 언론 보도가 나가지 않았나 싶다.

Bkis MyDoom DDoS Attack Diagram



<화면 2> BKis 에서 분석한 C&C Server 와의 교류 내역

공격 배후

최초에 공격을 발견한 7 월 7 일 당일만 하더라도 앞뒤 가리지 않고 중국이라는 생각을 했었다. 이유는 지금까지의 대부분의 DDoS 공격은 중국에서 이뤄졌으며, 그에 따라 “DDoS = 중국” 이라는 공식이 자연스럽게 성립되어 있었기 때문이다. 하지만 중국은 언제나 금전적인 대가를 요구했고 이번에는 어떠한 요구사항도 없이 무차별 공격만이 자행되었던 점, 그리고 아직도 배후 추적이 불확실한 점을 들어 중국이라는 결론이 희미해질 수밖에 없었다. 중국에 이어 다음으로 부각된 곳은 북한이다. 공격목표가 미국과 한국이라는 점, 북의 첩보요원이 임무를 끝내고 자결하듯이 바이러스가 자폭하는 점, 또한 언론에서 발표한 110 호 연구소와 관련된 부분 등을 들어 북한이라고 지목하고 있지만, 그것도 추측일 뿐 정확한 근거는 현재 나오지 않았다(북한의 ISP 기반을 설명하며 배후가 북한이라는 것은 근거없는 낭설이라는 주장도 제기되고 있다). 여러 가지 설이 난무하고 있는 가운데, 현재는 C&C 의 마스터 서버가 영국, 미국이라는 것 뿐, 더 이상의 정확한 증거는 나오지 않고 있다.

더욱 의심스런 내용들

이번 DDoS 공격에 이용된 여러가지 정황들은 기존 DDos 에 대한 상식을 깨뜨리는 행동이 많다. 그 내용들을 하나씩 정리해 보자.

1) 금전적인 대가를 요구하지 않음.

DDoS 공격은 거의 100% 금전적인 요구사항이 있다. 하지만 이번 공격은 어떠한 요구도 없이 무차별 파괴만이 있었다는 점이 의문스럽다.

2) 공격 기술이 고전적이다.

패킷 조립 방식이 굉장히 고전적이다. HTTP Get Flooding 과 CC Attack 을 혼합한 방식을 이용하였다. 이것은 지금은 잊혀질 만한 단순한 구식 공격기법이다. 고도의 공격루트와 대규모 공격에 자폭기능까지 포함한 점을 생각해 보았을 때 이 같은 구식 기술을 사용한 것이 이해가 되지 않는다는 것이 보안업계의 분위기다(물론 문제는 이 같은 구식 기술도 대규모로 자행한다면 현재의 보안 장비에서는 버티지 못한다는 것이다)

3) 바이너리 보호 기술이 없다.

요즘 악성코드나 상용 소프트웨어나 바이너리 패키징을 하지 않는 경우는 거의 없다. 오히려 일반적인 악성 코드는 바이너리 패키징에 안티디버깅 각종 스텔기 코드로 무장하는 것이 기본인데, 이번 좀비 PC 에 동원된 악성코드는 패키징조차 하지 않은 채 덩그러니 배포되었다. 의문이 가는 부분이다.

4) 자폭 기능이 있다.

7월 10일, 공격을 마친 후 악성 코드 바이너리는 하드디스크의 MBR 을 망가뜨리며 자폭을 하게 되고, 리부팅 후 컴퓨터는 제대로 부팅이 되지 않는 현상이 발생한다. 포렌식 등의 추적을 방지하기 위해 처리한 것으로 예상된다. 이 기능이 복한 배후설에 많은 설득력을 주기도 했다.

5) 자폭은 하지만 효과가 없었다.

보통 악성코드는 어셈블리로 작성하거나 비주얼 스튜디오 6.0 등으로 개발한다. 이유는 괜히 상위 버전의 컴파일러로 빌드했다가는 그 프로그램이 돌아가지 않는 사태가 발생하기 때문이다. 따라서 감염만 시켜놓고 실제 동작은 하지 않는 상황이 있을 수 있으니, 보통은 어떤 PC 에서도 가동될 수 있는 언어나 머신으로 개발한다. 하지만 이번에 자폭 전용으로

개발된 바이너리는 비주얼 스튜디오 2008 로 개발되었기 때문에 msvc90.dll 이 없는 PC 에서는 가동되지 않는다. 당연히 일반 가정 PC 에서는 msvc90.dll 이 없는 환경이 많을 수 밖에 없으며, 좀비 PC 에 감염되었지만 자폭 증상까지는 발생하지 않은 경우가 아주 많았다. 이것도 의문이 드는 부분이다. 이정도 DDoS 공격을 준비한 해커가 겨우 플랫폼 호환성 정도도 고려하지 않고 만들었다는 것은 업계에서 이해할 수 없다는 입장이다.

6) 파일을 분산시켜 놓았다.

보통 파일을 최소화 시키기 위해서 한두개의 파일에 모든 공격 처리내용을 다 담는 것이 일반적이는데, 이번 DDoS 공격에 이용된 바이너리는 여러 파일에 각 기능을 분산시켜 놓았고 또 그 파일이 유기적으로 연계하도록 구성되어 있다. 이런식으로 개발하면 해커 한두명이 개발하기에도 불편하고 테스트 하기에도 어렵다. 조직적으로 개발된 것이라는 의심과 동시에 기존 교과서와 일치하지 않는 악성코드 개발 방식이라 의문스럽다.

7) 시간대별 공격이 이뤄졌다.

C&C 의 크리티컬한 컨트롤을 받지 않고 예정된 시간에 일제히 공격을 시도하고 멈추고, 다시 시간대에 공격하고 하는 형태로 가동되었다. 마치 어느 사이트가 얼마만큼의 시간만에 대응을 하는 지 살펴보기라도 하듯이 지정된 시간에 질서있게 공격이 이뤄졌다. 이 역시 의문을 해결하지 못한 부분이다.

잘못된 상식들

어느 업계나 그렇겠지만, 전문가들이 볼 때는 비전문가들이 작성하는 내용에 대해서 반발심을 갖게 마련이다. 특히나 언론 보도에 관해서는 더욱 그렇다. 전혀 사실과 무관한 내용이 언론으로 발표될 때 업계의 많은 관계자들은 눈살을 찌푸리게 된다. 이번 DDoS 사건은 너무나 많은 언론에 노출되었고, 각 보도사에서 여러 자료 화면을 이용하는 가운데, 전문가들이 볼 때 너무나 현실을 왜곡시키는 듯한 데이터가 많이 등장했다는 것이 문제다. 대표적으로 <화면 3>과 같은 이미지이다. DDoS 에 이용된 좀비 PC 를 살펴보는 장면인데, 실제로 좀비 PC 에 이용된 것은 프로그램에 불과하지만 PC 본체의 내부를 뜯어 조사하는 장면이 아래 화면 외에도 여러 언론사에 이용되었다. 그 때문에 좀비 PC 가 무엇인지 잘 모르는 사람들이 볼 때는, 컴퓨터에 어떠한 물리적이거나 화학적인 외적 침입이 있는 것으로 오해하게 된다 (필자도 개인적으로 이러한 질문을 많이 받았었다). 예전에 70~80 년대에 컴퓨터 바이러스가 처음 등장하게 된 때에 바이러스라는 이름 탓인지 플로피 디스켓에 위생 처리를 하거나 소독을 하는 듯한 황당한 자료화면이 보도된 적이 있는데 사실 지금

생각하면 누구나 웃고 넘어갈 일이지만 이번 좀비 PC 의 경우는 대중들에게는 역시 처음 소개된 용어이기 때문에 비슷한 오해를 살 소지가 있다.



<화면 3> 잘못된 보도자료

이번 DDoS 공격으로 얻은 것

이번 DDoS 공격으로 얻을 수 있는 것은 업계에서 느낀 점과 일반 대중들이 체감한 것 두가지로 분류할 수 있다. 먼저 업계에서 확인할 수 있는 것은 현재 대한민국의 보안 수준으로는 마음먹고 DDoS 가 들어온다면 당할 수밖에 없는 무방비 상태라는 것을 알 수 있다. 업체 중에는 DDoS 공격이라는 것을 확인한 것이 6 시간 이상이나 지나서야 알아챈 경우도 있고, 다음 공격이 또 올거라는 것을 뻔히 알면서도 그냥 당하기만 했던 곳도 있다. 또한 구식 기술로 대한민국 굴지의 사이트가 힘없이 무너져내렸다. 인터넷 강국이라고 불리우고 있지만 보안 인프라는 후진국 이하라는 사실을 쉽게 각인시켜준 사례다.

그리고 일반 사람들에게는 DDoS 공격이 무엇인지, 인터넷 공격으로 기업을 이렇게까지 망가뜨릴 수 있는지, 자신들이 집에서 사용하는 컴퓨터가 해커들의 테러에 이용될 수도 있다는 것을 확인시켜 주었다. 이제는 DDoS 라는 단어를 모르는 사람들은 없다. 그리고 윈도우 보안 패치와 백신 설치가 얼마나 중요한 것인지를 많은 사람들이 깨닫게 되었다.

이제부터는

보안 예산이 턱없이 작다는 이야기가 이제서야 많이 들려온다. 하지만 슬픈 현실은 많은 기업들이 생각하기에, 보안 장비가 있어도 결국 똑같이 당하지 않았느냐는 태도를 고수하고 있다는 것이다. 이것은 정말 잘못된 생각이다. 해킹과 보안은 창과 방패의 싸움이다. 결국

언젠가는 당할 수 있어도 일단 새 창이 나오면 어쨌든 그 창은 방어할 수 있는 방패가 나오기 마련이다. 왜냐하면 해킹이 등장하게 되면 어쨌든 그걸 방어하기 위한 솔루션은 등장하게 되어 있기 때문이다. 그리고 더 이상 같은 창으로 찌를 수 없는 방패로 최소한의 무장은 해야 한다. 그렇게 되면, 적어도 같은 사태가 여러 번 되풀이되는 것만은 예방할 수 있다. 또 그러다 보면 새 창이 나오기 전에 더 훌륭한 방패가 나올 수도 있다. DDoS 쪽도 기존 장비의 기술에 너무 의지하고 있다. 물론 이것이 보안회사 측의 연구태만이라는 문제로 생각할 수도 있겠지만, 그것을 구매하는 기업의 문제가 더 크다. 기업 입장에서 더욱 적극적으로 각종 보안 장비 수급화를 위해 노력해야 한다. 그렇게 되면 보안 장비의 인프라도 더욱 늘어나게 되고, 장비를 개발하는 입장에서도 더욱 훌륭하고 질 좋은 장비를 보급하기 위해 노력하게 될 수밖에 없다. 기업이 장비 구입을 꺼려하고 보안 예산을 낮춘다면 당연히 생산하는 측에서도 퀄리티가 떨어질 수밖에 없고, 그런 상황에서 나중에 해킹 사고가 발생하고 나서 그 책임을 장비의 한계로 돌린다면 정말 앞뒤가 맞지 않는 행동이라 볼 수 있다.

또한 개인들 역시 PC 관리에 더욱더 관심을 가져야 한다. 나의 PC 가 인터넷 전쟁이나 테러에 동원될 수 있다는 사실을 이번 기회에 많은 분들께서 깨달은 것으로 알고 있다. 따라서 지속적으로 백신 검사와 보안 패치 설치 유무를 확인하고, PC 를 깔끔히 관리하는 것을 게을리하지 않아야 한다.

참고자료

<http://blog.bkis.com/?p=718>

<http://www.hauri.co.kr>

<http://kr.ahnlab.com>