KISC 분석보고서

KISC-T-04-001

MyDoom.A와 Doomjuice 웜 분석 및 대응 보고서

2004. 2.

인터넷침해사고대응지원센터 **(KISC)**

한국정보보호진흥원

1) KISC : Korea Internet Security Center, http://www.KrCERT.or.kr

2) 본 보고서의 전부나 일부를 인용시 반드시 [자료: 한국정보보호진흥원 (KISA)]를 명시하여 주시기 바랍니다.

MyDoom.A와 Doomjuice 웜 분석 및 대응 보고서

2004.02.13 / 분석대응팀

□ 개 요

멜리사로 시작된 전자메일을 주 매개체로 하는 웜은 그 배포 목적이 다양해지면서, 전파방법 및 감염 후 행동에 있어서 점차 지능적으로 변하고 있다. 이러한 웜은 무작위 다량 메일을 발송시켜, 사용자 컴퓨터와 전자메일서버 및 네트워크 자원의 부하를 크게 증가시킬 뿐만 아니라, 또다른 피해를 입히기 위한 중간단계로 이용된다는 점에서 초기의 신속한 대응이 필수적이다. 최근 국내외에 큰 피해을 입힌 MyDoom.A와 Doomjuice의 경우 이러한 변화 추세를 반영한 웜으로, 기존 웜보다 한층 발전한 새로운 개념이 적용되었다. 자세히 살펴보면, MyDoom.A는 공격 수행 웜인 Doomjuice를 전달받는 모듈을 설치하는 역할을 수행하며, Doomjuice는 실제 공격을 수행하는 모듈을 포함한 웜으로 MyDoom.A를 이용하여 자신을 전파시킨다. 구조상 서로 분리된 형태지만, 유기적으로 결합하여 활동을 하는 특성을 보여주고 있다. 공격의 중간 경유지 역할을 하는 MyDoom.A는 2004년 2월12일 02시28분57초(UTC 기준)에 소멸되지만, 이러한 유사 형태의 웜이 다른 서비스 포트를 사용하여 공격의 중간 경유지로 활용된다면, 그 피해는 상상할 수 없을 정도로 규모가 클 것으로 예측된다. 본 문서는 Mydoom.A 및 Doomjuice를 실제 분석하고, 그 행위를 관찰함으로서 대비책을 마련하고 앞으로 나타날 유사형태의 웜에 대해 사전에 대비하고자 한다.

□ MyDoom.A ; 공격수행 에이전트 설치 모듈

MyDoom.A는 실제 공격을 수행하는 공격 수행 웜을 전달받는 SOCKS 프락시 서버가 포함된 웜이다. 자기 자신을 전파시키기 위해 전자메일과 P2P서비스를 사용하며, 자체 SMTP엔진을 탑재하고 있다. 별도 명령 없이 자체적으로 www.sco.com에 대한 서비스 거부 공격을 수행하는데, 공격 감행 시작 시각은 2004년 2월1일 16시09분18초(UTC기준), 종료시각은 2004년 2월12일 02시28분 57초이다.[1] 테스트 결과 위의 시간 조건을 만족시키더라도, 25% 정도의 공격 성공률을 보였으며, 완전한 HTTP GET 메쏘드를 발생시키지 못했다. MyDoom.A의 가장 큰 특징은 다른 형태의 공격 모듈을 전달 받을 수 있는 SOCKS 프락시 서버를 설치한다는 점이다. 실제로 몇시간 뒤에 등장한 Doomjuice는 이를 이용해 www.microsoft.com에 대한 서비스 거부 공격을 실시하였다.

1. 전파 방법

MyDoom.A는 전자메일과 P2P 서비스인 KaZaA를 이용하여 자신을 전파시킨다.

구 분	MyDoom .A	MyDoom.B	Doomjuice
전파방법	- 전자메일 - P2P(Kazza)	- 전자메일 - P2P(Kazza)	SOCK Proxy이용

1) http://securityresponse.symantec.com/avcenter/venc/data/w32.mydoom.a@mm.html

2. 메일의 형태

이전의 메일 웜 혹은 메일 바이러스의 경우, 제목이 동일하거나 첨부되는 웜의 파일명과 확장자 명이 일정하여, 스팸메일 필터링 환경을 관리자가 설정하기 쉬웠고, 바이러스 월 또한 많은 부하 없이 이를 걸러낼 수 있었다. 그러나, 현재의 메일 웜/바이러스는 사회 공학적 기법을 이용하여 메일 제목이나 메일 내용을 지정하고, 첨부되는 파일명 및 확장자 명을 여러 가지 형태로 조합하여 동작하기 때문에 스팸필터에서의 환경설정 및 바이러스 월의 백신 제작을 어렵게 만들고 있다.

2.1 MyDoom.A와 MyDoom.B의 메일 특성

메일특성	MyDoom.A	MyDoom.B
메일제목	test, hi, hello, Mail Delivery System, Mail Transaction Failed, Server Report, Status, Error	Returned mail, Delivery Error, Status, Server Report, Mail Transaction Failed, Mail Delivery System, hello, hi
본문내용	Mail transaction failed. Partial message is available, The message contains Unicode characters and has been sent as a binary attachment, The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment, test	sendmail daemon reported:Error #804 occured during SMTP session. Partial message has been received, Mail transaction failed. Partial message is available, The message contains Unicode characters and has been sent as a binary attachment, The message contains MIME-encoded graphics and has been sent as a binary attachment, The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment
첨부파일명	document, readme, doc, text, file, data, test, message, body	document, readme, doc, text, file, data, test, message, body (혹은, 다른 이름이 선택될 수 있다)
첨부파일 확장자명	htm,txt,doc,pif,scr,exe,cmd,bat,zip	htm, txt, doc,.pif, scr ,exe, cmd, bat, zip
첨부파일크기	22,528 Byte	29,184 Byte
메일주소	확장자가 다음과 같은 참조파일에서 임의 추출 (htm,sht,php,asp,dbx,tbb,adb,pl,wab,txt)	확장자가 다음과 같은 참조 파일에서 임의 추출 (htm,sht,php,asp,dbx,tbb,adb,pl,wab,txt)

3. 메일전송기법상 특성

기존 메일 웜/바이러스의 경우, 피해 호스트에서 추출한 메일 주소에서 도메인 부분을 추출하여, 사용자 계정과 임의로 결합하여 전송하였으나, MyDoom.A의 경우 피해 호스트에 설정된 DNS 서버에 목적지 도메인의 MX필드 값을 조회한 후, 자체 SMTP 엔진을 이용하여 메일을 전송한다. 이는 피해 호스트의 로컬 메일서버를 이용하지 않음으로서, 해당 메일서버의 정책 적용을 받지 않아, 대량의 메일을 빠른 속도로 전송할 수 있으며, 정확하지 못한 메일서버 주소 값으로 인한 메일 전송 실패 확률을 크게 낮출 수 있게 된다.

MyDoom.A는 정확한 메일 전송을 통해 피해 효과를 극대화시키며, DNS서버의 부하를 가중시키는 특성을 가지고 있다

4. 피해 증상

MyDoom.A 웜이 첨부된 메일을 받은 사용자가 첨부파일(즉, 웜)을 실행시키게 되면, 메모장이 실행되며, 알 수 없는 문자열을 사용자에게 보여준다. 이것은 사용자의 의심을 없애는 일종의 트릭 행위이며, 그 다음부터는 사용자의 컴퓨터 사용이나, 사용자는 자신도 모르게 웜을 전파시키는 매개체가 되어 자신의 주소록이나 쿠키, 혹은 방문한 홈페이지에서 추출된 이메일 주소로 메일을 무한정 배포시키게 된다. 다음 그림은 MyDoom.A의 메일을 받은 후 첨부파일을 실행시켰을 때 사용자에게 나타나는 화면이다.

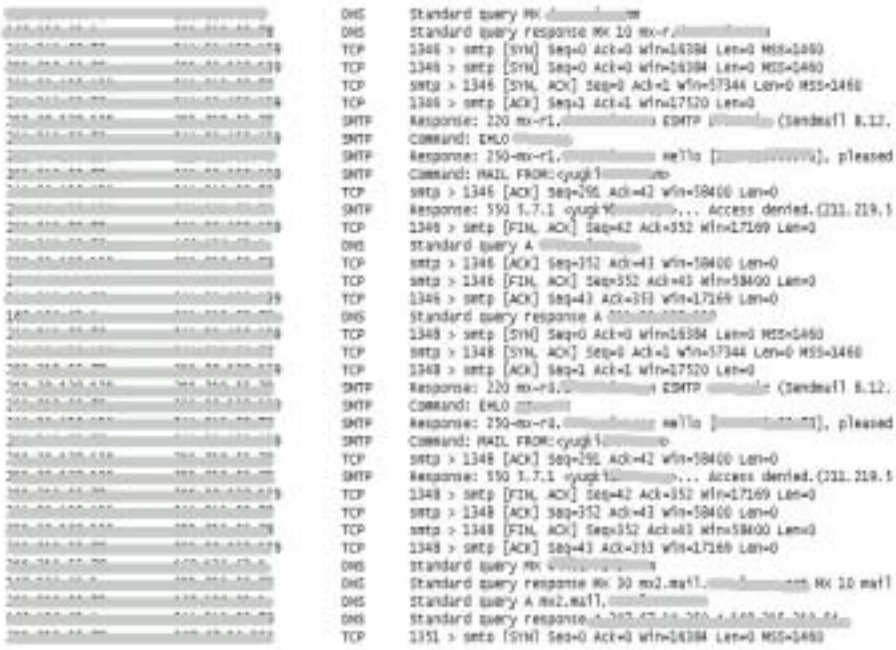
4.1 사용자 PC에서 전자메일 주소 추출

MyDoom.A 웜은 감염 PC에서 메일주소를 추출하는데, 추출대상이 되는 파일은 다음과 같은 확장자 명을 가진 파일이다. 여기서 추출한 메일주소를 바탕으로 발송자 주소와 수신자 주소를 결정하게 된다.

.htm	.sht	.php	.asp	.wab
.dbx	.tbb	.adb	.pl	.txt

4.2 웜이 첨부된 메일 무작위 전송

감염 PC에서 추출한 메일주소를 바탕으로 다음과 같이 메일을 발송하게 되며 테스트 결과 1초당 약 0.15개의 메일을 발송시키며, 메일크기는 약 30kbyte 정도이다.



4.3 P2P서비스를 이용한 웜 전파

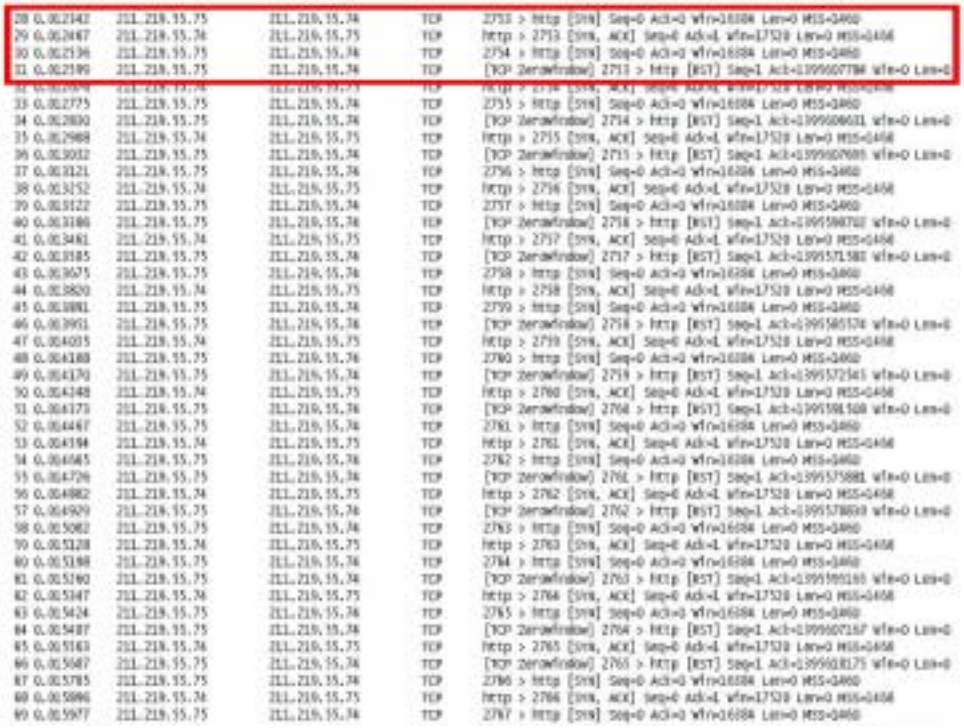
P2P 서비스를 제공하는 프로그램인 KaZaA가 설치되어 있으면 다운로드 디렉토리에 웜 원형을 다음의 이름으로 복사하여 놓는다.

① winamp5
② icq2004-final
③ activation_crack
④ strip-girl-2.0bdcom_patches
⑤ rootkitXP
⑥ office_crack
⑦ nuke2004

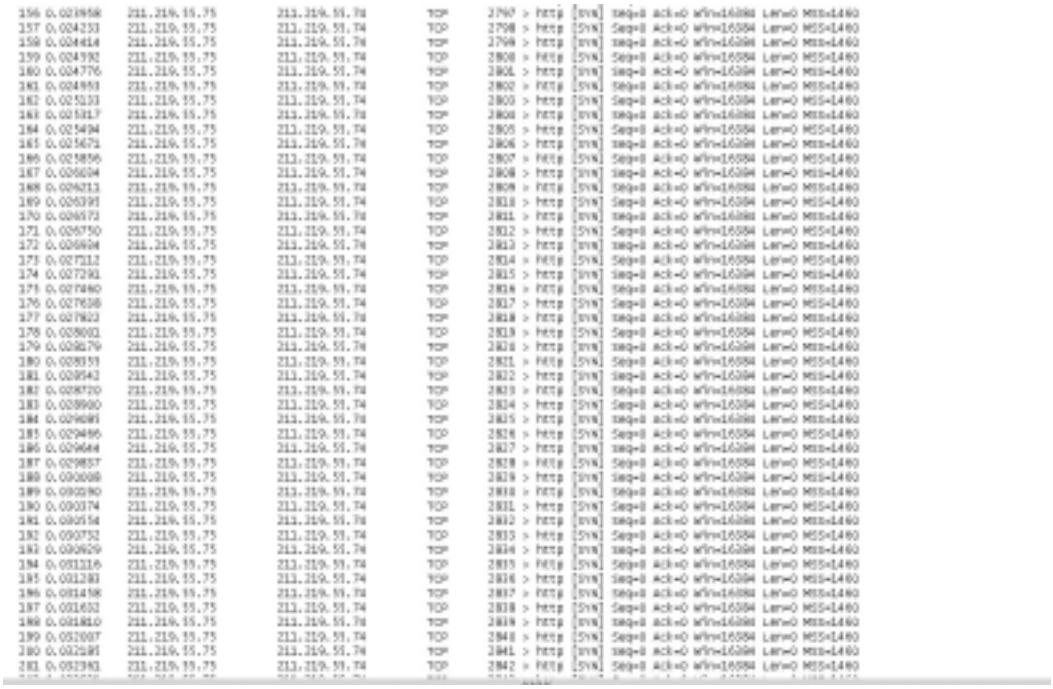
이 경우, 다른 KaZaA 사용자가 위의 키워드를 이용하여 파일을 찾고, 해당 파일을 내려 받아 웜을 실행시킬 경우 감염되게 된다

4.4 분산 서비스 거부 공격 수행

시스템 날짜가 2004년 2월 1일 16:09:18 (UTC기준) 이후이면, www.sco.com에 대한 서비스 거부 공격을 실시한다. 테스트 결과 약 64개의 쓰레드가 생성되며, 알려진 바와는 달리 완전한 HTTP GET 메쏘드를 생성시키지 않았다. 3-Way-Handshaking 과정 도중 Windowsize를 '0'로 셋팅한 Reset 패킷이 발생되어 웹서버와 자동으로 접속이 끊어지며 1초당 약 6000개의 패킷이 발생하였다.



웹서버의 부하가 증가하게 되면 다음과 같이 SYN-Flooding 현상이 나타나게 된다

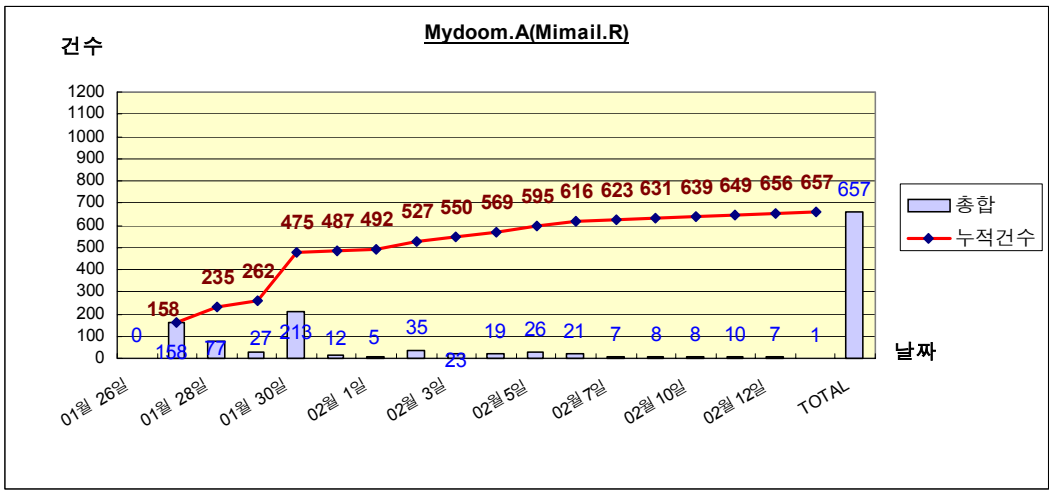


5. 국내외 피해 현황

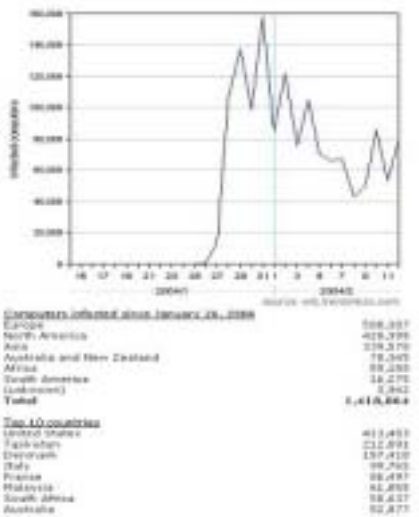
사용자가 직접 첨부파일을 실행시켜야 한다는 점에서 피해가 적을 것으로 예상되었으나 스팸 필터의 환경설정에 있어서 어려움이 있고 바이러스 웜의 백신 업데이트가 늦어 발생 초기 국내에 유입되었다.

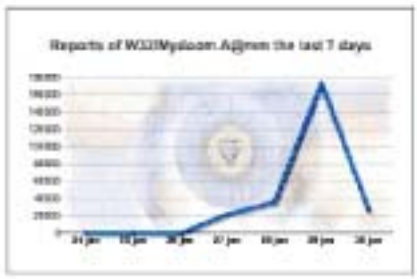
5.1 국내 감염 현황 분석

다음은 2004년 2월13일 현재까지의 국내에 접수된 MyDoom.A의 감염 현황이다.[2] 총 657건이 접수되었으나 이는 사용자의 자발적인 신고에 의한 통계이므로 실제 감염률과는 차이가 있을 수 있다. MyDoom.A의 접수건수는 다른 메일 웜/바이러스의 접수 건수에 비하면 미미한 것으로 나타났으나 SMTP 트래픽량이 보통 때보다는 증가한 것으로 나타나 실제 감염률은 이보다 높을 것으로 판단된다.



5.2 국외 감염 현황 분석





[Trendmicro] [f-secoure]

2) http://www.krcert.org

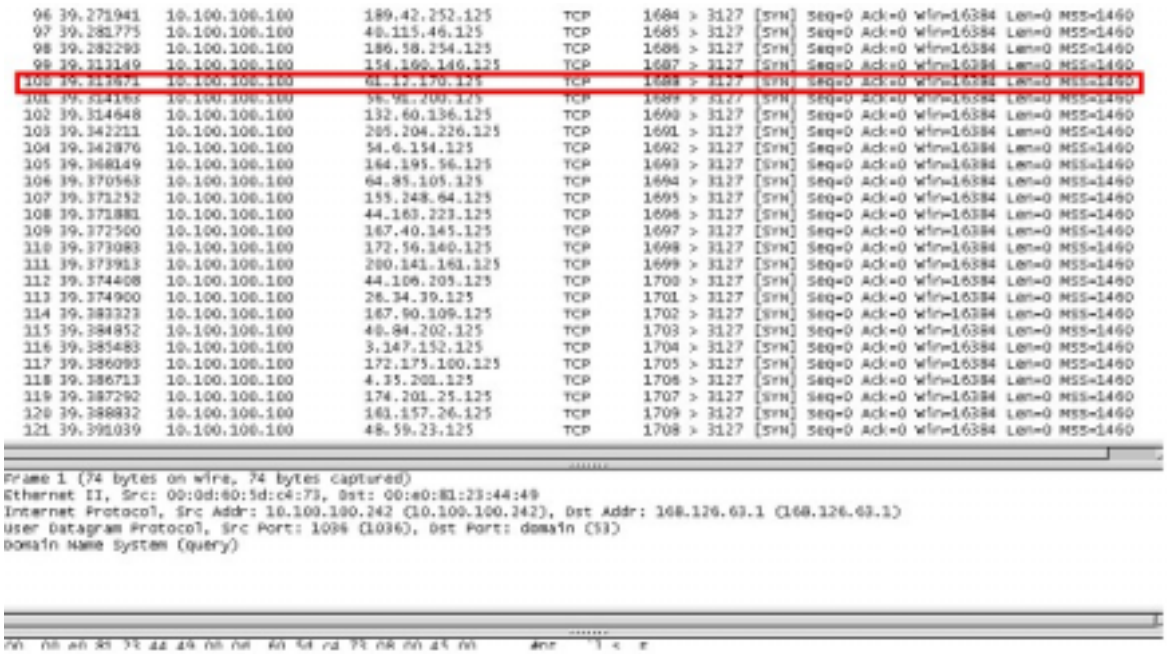
위 그래프는 트랜드마이크로와[3], f-secure가[4] 발표한 MyDoom.A의 감염 신고건수이다. 트랜드마이크로의 통계는 1월31일에 최고점을 기록하다가 시간이 가면서 점차 감소함을 볼 수 있고, F-Secure는 1월29일에 최고점에 달했음을 볼 수 있다. 트랜드마이크로의 국가별 감염 호스트 순위는 1위 미국, 2위 타지키스탄, 3위 덴마크, 4위 이탈리아, 5위 프랑스, 6위 말레이시아, 7위 남아프리카, 8위 호주, 9위 스웨덴, 10위 일본 순이었다.

□ Doomjuice ; 공격수행 모듈 배포 웜

Doomjuice는 MyDoom.A가 설치한 SOCK 프락시 서버를 이용해 분산 서비스 거부 공격을 수행하는 모듈을 전파시키는 웜이다. 3127(TCP)포트를 스캔한 후, MyDoom.A가 설치한 프락시 서버로부터 응답이 있는 호스트에 공격을 실행하는 코드를 전달하여 자신을 전파시킨다. 전달된 공격 모듈은 자동으로 실행되며, MyDoom.A의 소스코드를 감염호스트에 설치하는 특성을 가지고 있다. Doomjuice는 MyDoom.A와 연결선상에 있으며, 서로 유기적으로 작용하여 새로운 형태의 공격을 수행하게 된다. MyDoom.A가 www.sco.com에 대한 서비스 거부 공격을 수행하는 것과는 달리, Doomjuice는 www.microsoft.com에 대한 서비스 거부 공격을 수행한다.

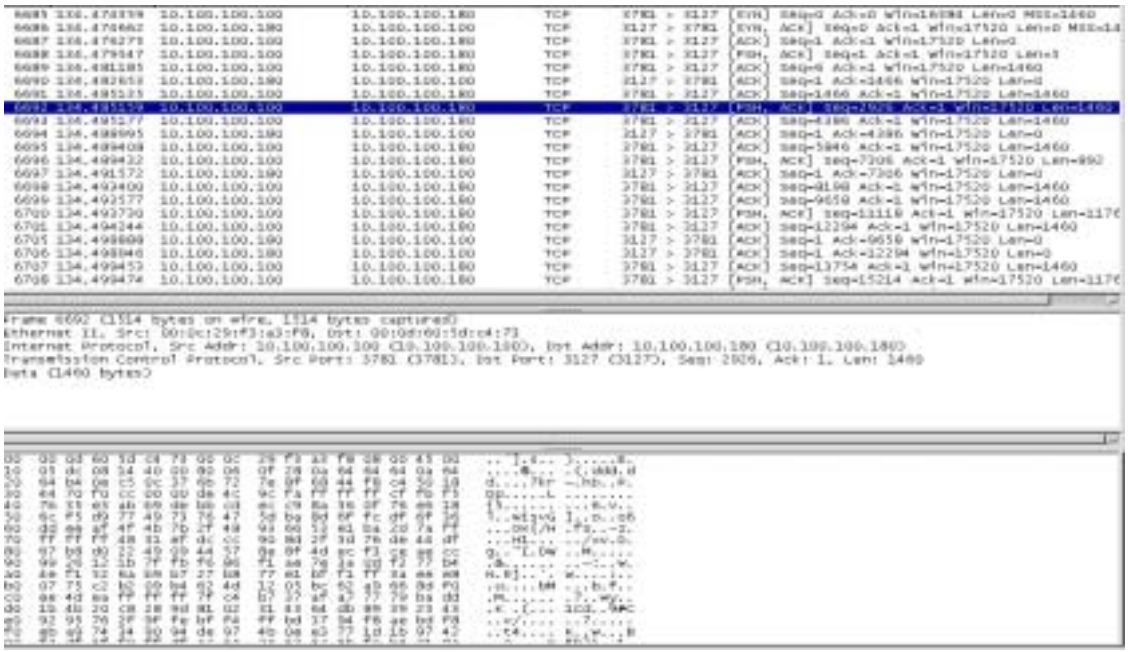
1. 전파방법

대상 IP를 선택하여, MyDoom.A에 의해 설치된 프락시 서버 설치 포트인 3127(TCP)에 대한 스캔을 실시한다. 스캔대상은 무작위 IP인 것처럼 보이지만 실제로는 스캔을 실시하는 각각의 쓰레드가 자신만의 IP대역을 선택한 후 해당 IP에 대역에 대해 주소 값을 순차적으로 증가시키면서 스캔을 실시한다. 1초당 60~70개의 SYN 패킷이 발생되었다.



3127(TCP)포트가 열려있는 호스트를 발견하면, 해당 포트에 웜을 전달한다.

3) http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MYDOOM.A&VSect=S&Period=1m
4) http://www.f-secure.com/virus-info/statistics/



2. 서비스 거부 공격 수행

전달된 웜은 자동 실행되며 시스템 날짜를 확인하여 2월8일부터 2월12일 사이이면 약간의 휴지기간을 갖는 쓰레드를 생성하고, 시스템 날짜가 2월12일 이후이면 휴지기간 없는 80개의 쓰레드를 생성하여 www.microsoft.com에 대한 서비스 거부 공격을 실시한다. MyDoom.A와는 달리 완벽한 HTTP 데이터 전송 과정을 구현하였으며, 1초당 약 100~120개의 HTTP GET 메쏘드를 발생시켰다.

□ 영향력 분석

Doomjuice는 MyDoom.A가 설치한 프락시 서버를 이용하여 새로운 공격을 수행하는 모듈을 배포하는 웜이다. 비교적 유포가 쉬운 전자메일을 통해 공격 경유지로 이용되는 웜을 유포하고 그 웜에 내포된 프락시 서버를 설치하여 2차 공격을 수행하였다. 이러한 형태는 처음 발견되는 것으로 웜 개발 기술이 한 단계 도약했음을 보여 주고 있다. 또한, MyDoom.A의 소스코드가 공개됨에 따라 앞으로 이와 유사한 형태의 웜이 등장할 것으로 예상된다. 웜이 발견되면 초기에 그 영향력을 분석하고 이에 대한 대비책을 마련하는 것이 필수적으로 이번 MyDoom.A와 Doomjuice의 경우 초기에 자체 테스트를 통해 영향력을 분석하고, 그 대응책을 마련하여 피해범위를 최소한으로 줄일 수 있었다.

1. 네트워크에 미치는 영향 분석

1.1 SMTP 트래픽에 미치는 영향 분석

MyDoom.A가 자신을 전파시키기 위해 발생시키는 메일은 1분당 약 9개이며 평균 크기는 30Kbyte였다. 이를 근거로 했을 경우 피해 호스트당 약 4608BPS의 트래픽이 유발될 것으로 예측된다. 피해 호스트를 1000대로 가정하면 예상되는 BPS 값은 4,608,000이며, 피해 호스트가 10,000대 라고 가정했을 경우 예상되는 BPS 값은 46,080,000이다. 감염에 의해 유발되는 이들 트래픽은 정상적인 SMTP 트래픽 형태를 유지하고 있기 때문에 BPS값 증가시 PPS값은 이전과 비슷하거나 완만한 상승곡선을 그릴 것으로 예상하였다.

1.2 서비스 거부 공격으로 인해 네트워크에 미치는 영향 분석

MyDoom.A의 경우www.sco.com에 대한 서비스 거부 공격을 실시하게 되어있으나 테스트 결과 약 25% 정도만이 공격을 수행하는 것으로 확인되었다. 그러나, 크기가 62byte인 패킷을 초당 6000개 정도 발생시켜 순간적인 PPS값 증가로 인해 네트워크 장비에 미치는 영향은 상당할 것으로 판단되었다. 이때 유발되는 트래픽은 80(TCP)에 대한 비정상적인 트래픽으로 크기가 작은 패킷이 다량 발생됨에 따라 BPS값 증가에 비해 PPS값의 급속한 증가 현상이 관찰될 것으로 예측되었다.

Doomjuice는 3127(TCP)포트에 대한 스캔을 실시 한 후 www.microsoft.com에 대한 서비스 거부 공격을 수행한다. 3127(TCP)포트에 대한 스캔은 크기가 62byte인 패킷이 1초당 60~70개 발생하여 해당 포트에 대한 BPS 및 PPS값이 증가할 것으로 예측하였다. 서비스 거부 공격시 HTTP GET 요청이 초당 100~120개 발생되나 정상적인 HTTP트래픽과 구별할 수 없어 네트워크 상에서 관찰할 수 있는 인자는 없으나 감염 호스트가 많을 경우 80(TCP)에 대한 BPS 및 PPS값이 증가 할 것으로 예측되었다.

2. 메일서버에 미치는 영향 분석

자체 테스트 결과, MyDoom.A의 경우 1초당 0.15개의 메일이 발송됨이 확인되었다. 개인 사용자의 컴퓨터 사용시간을 하루 10시간이라 가정했을 경우 약 5400개의 메일이 한 대의 피해 호스트로부터 발생되며, 피해 호스트가 1000대라 가정했을 경우 약 540만개의 메일이 발송 되게 된다. 물론 하나의 전자메일 서버로 순간적으로 발송되지 않고, 여러 메일 서버로 10시간에 걸쳐 전송되는 것이지만 메일서버에 미치는 부하는 매우 클 것이라 판단하였다.

3. 개인 PC사용자에 미치는 영향 분석

메일 전송 및 서비스 거부 공격 과정에 생기는 부하로 인해 컴퓨터 및 네트워크 속도 저하 현상이 나타날 것으로 예측되었다.

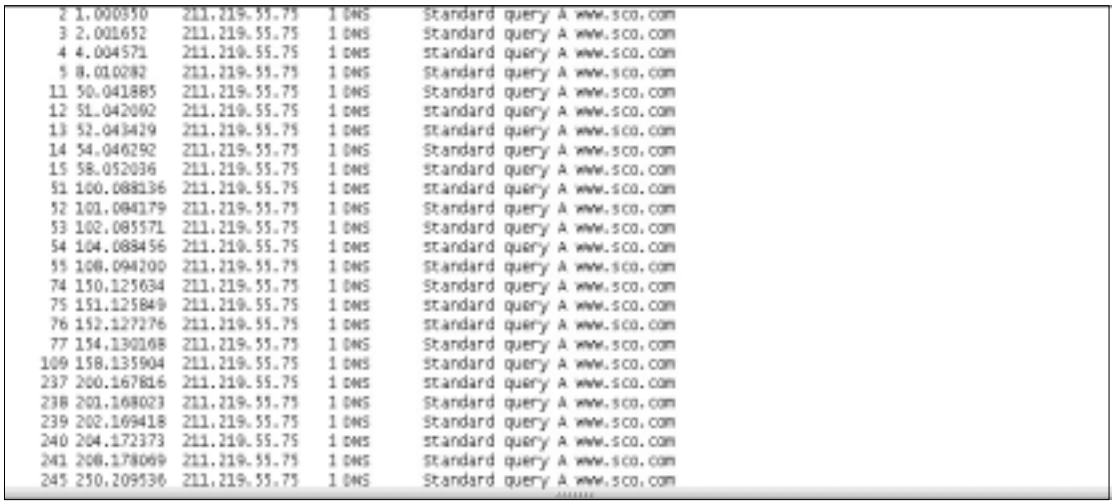
□ 대응책 및 결과

1. MyDoom.A에 대한 대응책 및 결과

1.1 서비스 거부 공격에 대한 대응책

o DNS서버에서의 삭제를 통한 방어

특정 웹 사이트에 대한 서비스 거부 공격은 공격 수행 전 대상 사이트에 대한 DNS 질의가 필수적이다. 공격 호스트의 대상 사이트에 대한 DNS 질의가 실패하게 되면, 공격 또한 실패하므로 DNS 엔트리에서 해당 사이트에 대한 값을 삭제하는 방법은 가장 손쉬운 방어수단 중 하나이다. 그러나, 해당 사이트 관리자의 동의 없는 임의 삭제는 불가능하며, 설령 삭제하더라도 그에 따라 생기는 DNS서버의 부하 등의 역효과에 대한 사전 검증이 필수적이다. 자체 테스트 결과, MyDoom.A는 www.sco.com에 대한 DNS질의 실패시 1분당 36개의 DNS 질의를 DNS서버에 전송하는 현상이 관찰되었다. 이 결과를 바탕으로 DNS 서버에서의 www.sco.com에 대한 값을 삭제할 것을 권고하여 실제 서비스 거부 공격을 방어할 수 있었다.



o 트래픽 모니터링에 의한 서비스 거부 공격 발생 여부 확인

MyDoom.A가 발견되자, 대부분의 보안관련 회사에서는 www.sco.com에 대한 공격형태를 정상적인 HTTP 트래픽에 의한 서비스 거부 공격일 것이라고 예측했다[5][6]. 자체 테스트 결과 25%정도의 확률로 www.sco.com에 대한 서비스 거부 공격이 발생되었으나, 완전한 HTTP 트래픽이 아닌, 62byte 크기의 패킷이 초당 약 6000개 정도 발생한다는 사실을 확인하였다. 이는 해당 포트(TCP:80)에 대한 갑작스런 PPS값의 증가를 의미하며, 이를 바탕으로 80(TCP)포트에 대한 PPS값 변화도를 관찰하여 서비스 거부 공격이 현재 진행되고 있는지

5) http://securityresponse.symantec.com/avcenter/venc/data/w32.mydoom.a@mm.html
6) http://www.f-secure.com/v-descs/novarg.shtml

여부에 대해 집중 모니터링 할 수 있는 인자로 활용 할 수 있었다

1.2 2차 감염에 대한 대응

MyDoom.A에 감염되면, 3127(TCP)포트에 프락시 서버가 설치되는 현상이 관찰되어 2차 감염에 대한 대비로 3127(TCP)포트에 대한 필터링을 권고하였다. 결국 몇 시간 뒤에 나타난 Doomjuice가 국내에 거의 유입되지 않은 결정적인 역할을 하게 되었다.

1.3 전자메일을 통한 전파에 대한 대응책

MyDoom.A는 자체 SMTP 서버를 이용하여 메일을 전송하기 때문에, 빠르고 정확하게 감염된 메일을 유포할 수 있었다. 사전에 이러한 감염 메일 전송을 차단 할 수 있으면, 웜의 유포를 효과적으로 막을 수 있다. 감염메일의 전송을 차단하기 위하여 다음과 같은 방법을 사용할 수 있다.

- 스팸메일 필터를 이용한 차단 방법
  - 스팸 메일을 처리하는 방식으로 이러한 웜 유포를 사전에 차단 할 수 있다. 한 가지 방법으로 발신자의 IP주소와 발신자 도메인의 MX레코드 값이 일치하는지 여부를 확인한 후, 수신 여부를 결정하면 무작위 감염 호스트로 부터의 웜 전파를 사전에 막을 수 있다.
- 바이러스 월을 이용한 차단
  - 관련 업체에서 제공하는 해당 백신을 업데이트 한다.
- Layer-7 스위치를 이용한 차단
  - 관련 업체에서 제공하는 관련 필터를 업데이트 한다.

2. Doomjuice에 대한 대응책 및 결과

Doomjuice는 MyDoom.A에 감염된 피해 호스트의 3127(TCP)에 설치된 프락시 서버를 통해 새로운 공격 모듈을 전달하는 웜으로, www.microsoft.com에 대한 서비스 거부 공격을 수행한다. 자체 테스트 결과 1초당 약 100~120개의 HTTP GET 요청 패킷을 발생시켜 네트워크에 부하를 줄 것으로 예측하였다. 그러나, MyDoom.A 발견 당시 3127(TCP)포트에 대한 차단을 사전에 권고하였기 때문에 국내 유입이 불가능했을 것이라 판단하였으며 실제로 신고된 피해건수도 극히 미비하였다.[7)]

서비스 거부 공격시 유발되는 패킷은 정상적인 HTTP GET 요청 패킷이었지만, Host필드를 제외한 기타 HTTP 헤더 부분이 생략되어 있어 웹 브라우저에서 발생시키는 HTTP GET 요청 패킷과는 그 내용 및 크기가 다르다는 특징이 있다.

2.1 웜 전파 억제를 위한 대응책

전파경로로 사용되는 3127(TCP)포트에 대한 차단 정책 적용

2.2 서비스 거부 공격에 대한 대응책

서비스 거부 공격시 발생되는 트래픽은 일반 웹 트래픽과 유사하며, 단지 공격에 사용되는 HTTP GET 요청 패킷의 헤더 부분 중 Host 필드를 제외한 모든 부분이 생략되어

7) **http://www.krcert.org**

있어 패킷 내용과 크기가 정상적인 HTTP GET 요청 패킷과 다르다. 공격시 사용하는 HTTP GET 요청 패킷의 크기는 100byte이며 정상적인 www.microsoft.com에 대한 HTTP GET 요청 패킷 크기는 505byte이다. 이를 이용하면 Layer 7 스위치에서 필터를 만들어 공격에 대비할 수 있다.

※ Protocol: TCP(HTTP), Port: 80 , Contents: GET / & Host:www.microsoft.com:80 Packet size <=100

□ 결 론

이번 MyDoom.A와 Doomjuice는 다음과 같은 특징으로 요약될 수 있다. 앞으로 이와 같은 형태의 변형된 웜이 출현할 것으로 예측되며 이에 따른 대비책을 사전에 적용시켜야 할 것이다.

1. 웜 형태의 진화

MyDoom.A는 공격 수행 웜인 Doomjuice를 전달받는 모듈을 설치하는 역할을 수행하며 Doomjuice는 실제 공격을 수행하는 모듈을 포함하는 웜으로 서로 유기적으로 결합되어 공격을 수행한다. 이러한 형태는 스팸메일을 전송시키는 스패머들이 주로 사용하였으나 결국 이번에 웜으로 등장하였다. 공격 경유지로 사용되는 프락시 서버의 설치 서비스 포트가 3127(TCP)로 네트워크단에서의 차단 규칙을 적용하여 대응하기가 상대적으로 쉬웠으나 80(TCP)이나 25(TCP)등의 포트를 공격 경유지 포트로 사용할 경우에 대한 대비책을 마련해야 할 것이다

MyDoom.A는 공격 경유지로 이용되는 프락시 서버를 설치하기 위해 자체 SMTP엔진을 사용하였다. 감염 메일은 사회공학적 기법을 이용하여 제목과 본문내용 및 첨부파일명이 가변적이며, 이에 따라 스팸 필터에서의 환경설정 및 바이러스 웜의 백신 제작이 어려웠다. 또한, 감염된 모든 사용자의 IP주소가 메일서버 역할을 하므로 이런 방식의 웜이 다량 발생할 경우 과다한 메일 증가로 인한 메일 서버 부하 및 네트워크 트래픽 증가가 우려된다. **메일서버에서의 메일 수신시 발신자 메일서버에 대한 인증을 어떤 형태로든지 수행하게 하면, 이러한 메일을 통한 웜 전파력은 크게 약화 될 것이다.**

2. 서비스 거부 공격 형태의 변화

이전의 특정 사이트로의 분산 서비스 거부 공격시 위조된 IP 주소를 발신지 주소로 하여 대량의 SYN패킷을 발생시키는 SYN-Flooding 공격이 주류를 이루었으나 이번 서비스 거부 공격의 경우 완벽한 HTTP GET 요청 패킷을 다량 발생시켜 공격을 수행하는 한층 발전된 기법을 이용하였다.

2.1 MyDoom.A의 www.sco.com에 대한 서비스 거부 공격

MyDoom.A가 수행한 서비스 거부 공격은, 완벽한 HTTP GET 요청 패킷을 만들지 못하였으며, 62byte크기의 패킷을 초당 6000개 정도 발생시켜 www.sco.com을 무력화시켰다. 국내에서는 이에 대한 대응으로 www.sco.com에 대한 DNS 엔트리를 삭제 하였으며 2차 공격에 대비해 공격 경유지 포트인 3127(TCP)를 차단하여 후속으로 나타난 Doomjuice에 대해 효과적으로 대응할 수 있었다.

2.2 Doomjuice의 www.microsoft.com에 대한 서비스 거부 공격

Doomjuice가 서비스 거부 공격 수행시 발생시키는 트래픽은 완벽한 HTTP GET 요청 패킷으로 이루어지며 이는 정상적인 HTTP 트래픽과 구별이 힘들다. 그러나, HTTP 헤더의 대부분이 생략되어 있어 패킷 내용 및 그 크기가 정상적인 패킷과 다르다는 특징이 있다. 앞으로 특정 사이트에 대한 서비스 거부 공격은 정상적인 트래픽이지만, 빠르고 많은 수의 패킷을 발생시키기 위해 크기가 작은 패킷으로 이루어 질 것으로 보이므로 이러한 트래픽을 식별할 수 있는 기법의 개발 등 대비책을 마련해야 할 것으로 보인다.

참고자료

http://www.symantec.com
http://www.trendmicro.com
http://www.f-secure.com
http://www.math.org.il/newworm-digest1.txt