IN-03-002

SDBot 트로이목마 테스트 및 사고대응

2003. 2. 12

CERTCC-KR cert@certcc.or.kr

이동련, ryuni@certcc.or.kr
오은숙, esoh@certcc.or.kr
이재용, jylee@certcc.or.kr
전병기, bkjeon@certcc.or.kr

1. 개요

2003년 1월부터 2월 사이 국외로부터 CERTCC-KR로 DDos 공격에 대한 접수가 증가하였고 1.30일경을 전후하여 과다한 이상패킷의 발생으로 네트워크 속도가 저하되는 등 부하를 일으키고 있다. 이에 CERTCC-KR에서는 신고된 사고에 대하여 직접적인 원인이 되는 이상패킷 발생 프로그램을 조사하기 위해 분석을 실시하였다.

신고된 이후 실제 모니터링 시에는 해당하는 패킷이 재발생하지는 않았으나 IRC를 이용한 트로이목마 프로그램들과 공격도구들이 발견되었고 이러한 프로그램 중의 하나인 SDBot의 소스가 공개되어 제한된 환경에서 테스트를 실시하였다.

본 테스트는 결과적으로 SDBot이 네트워크 부하를 발생시킨 직접적인 원인이 되는 도구가 될 수 있는지 그 가능성을 검토하기 위한 것으로 다음과 같은 사항을 중점적으로 시험하였다.

- o SDBot를 이용한 이상패킷 발생 여부
- o IRC를 통한 원격 조정 가능 여부
- o 생성되는 트래픽량

※ 본 테스트 결과는 네트워크 속도와 인터넷 공간이 제한된 환경에서 실시되었으며 실제 사이트에서 발견되는 SDBot 샘플과 차이가 있을 수도 있으므로 실제상황에서는 다른 결과 값이 나올 수 있다.

2. 공격대상

SDBot이 설치되면 레지스트리에 등록되어 윈도우 시작마다 자동으로 실행되며 113 포트를 오픈한다.
IRC 채널을 통해 공격하는데 IRC 채팅 프로그램을 사용하지 않은 경우도 SDBot 내에 IRC 채널에 접속하는 기능을 내포하고 있어 윈도우 환경에서는 이용될 수 있다.

3. 테스트 환경

테스트는 IRC 채널을 이용하는 SDBot를 시험하였으며 SDBot를 통하여 원격에서 공격도구들을 실행할 수 있는지 테스트하였다.

가. 테스트 환경

o 네트워크 환경
- 10Mbps LAN

o DDos 도구

본 테스트에서 사용한 DDos 도구는 실제 발생한 패킷들과 유사한 패턴을 생성하는 IGMP 브로드캐스팅 공격 도구와 신고된 사이트에서 입수된 프로그램 중 하나인 SYN Flooding 공격 도구를 사용하였다.

- OOOO : IGMP 브로드캐스팅 공격 도구
  · Destination IP : 255.255.255.255
  · Packet Size : 60 Bytes

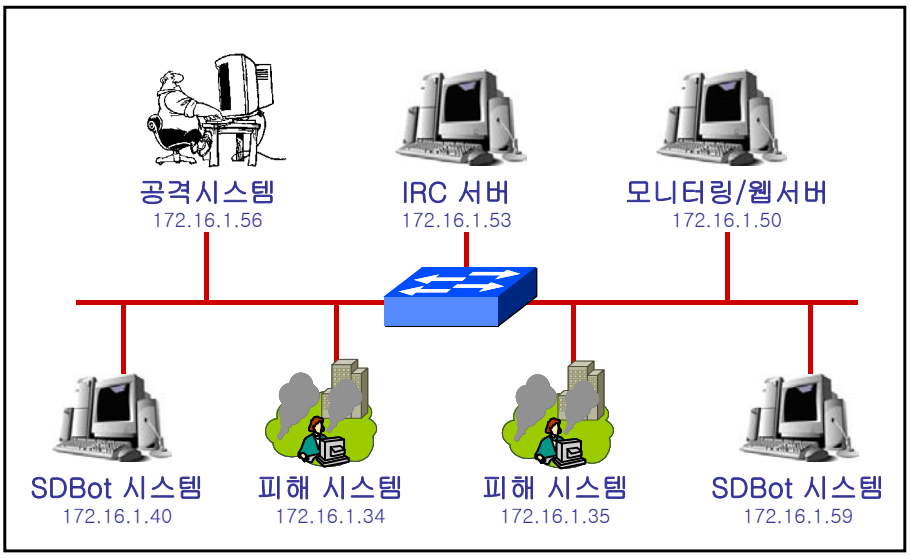
- XXXX : SYN Flooding 공격 도구
  · Destination IP : Random
  · Destination Port : 80

나. 구성도

o mIRC 클라이언트 시스템 1대
o IRC 서버 1대
o 웹서버 1대
o SDBot이 설치된 시스템 2대

o SDBot이 설치되지 않은 윈도우 시스템

유형	운영체제	IP 주소	비고
공격시스템	Windows 2000 Server	172.16.1.56	mIRC 클라이언트 설치
IRC 서버	Windows 2000 Server	172.16.1.53	IRC 서버 설치
웹서버	Windows 2000 Server	172.16.1.50	IIS 웹서버 설치
감염 시스템	Windows 2000 Pro	172.16.1.40 172.16.1.59	SDBot 설치
피해시스템	Windows 2000 Pro	172.16.1.34 172.16.1.35	-



4. 공격방법 및 시나리오

가. 공격방법

mIRC는 IRC서버에 접속하여 채널을 형성해 메시지를 주고받는 채팅 프로그램이다. 즉, 누군가가 메시지를 보내면 IRC 서버로 전송되고 IRC 서버에서는 다시 같은 채널에 접속되어 있는 모두에게 전달한다.

이러한 점을 이용하여 SDBot는 IRC 서버로부터 특정 메시지를 받은 경우 공격자가 의도한 대로 명령을 실행하게 된다. mIRC 채널상에서 공격자가 정의한 특정 형태의 메시지를 보냄으로써 SDBot이 설치된 모든 시스템은 메시지를 명령어로 인식하고 명령을 수행하게 되는 것이다.

나. 공격 시나리오

1) 공격자의 mIRC 채널 접속

mIRC를 이용하여 IRC서버의 특정 채널(SDBot이 접속되어 있는)에 접속한다.

2) 감염 시스템의 채널 접속

SDBot이 설치된 감염 시스템 2대가 부팅되고 윈도우가 실행되면서 SDBot이 자동으로 실행되어 IRC 서버의 특정 채널에 접속된다.

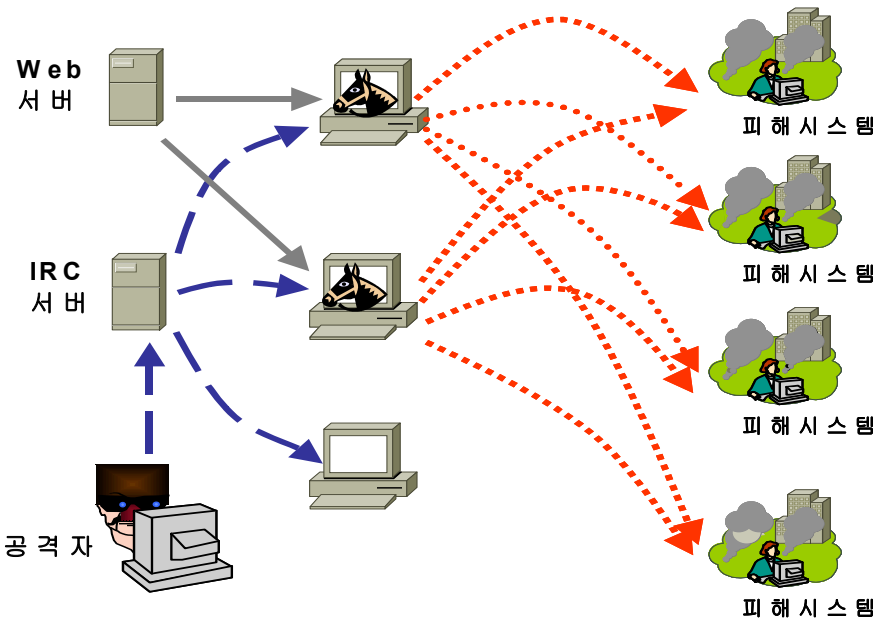
3) 공격도구를 감염시스템에 설치

공격자는 mIRC 채널상에서 특정한 채팅 메시지를 보내는데 SDBot이 설치된 시스템에서는 이를 명령어로 해석하여 웹서버로부터 공격도구를 다운로드 받아 설치하게 된다.

4) 감염시스템에 설치된 공격도구 실행

3)에서와 같은 방법으로 특정한 채팅 메시지를 보내어 이번에는 공격도구를 실행한다.

즉 다음 그림과 같은 형태의 공격이 발생한다.

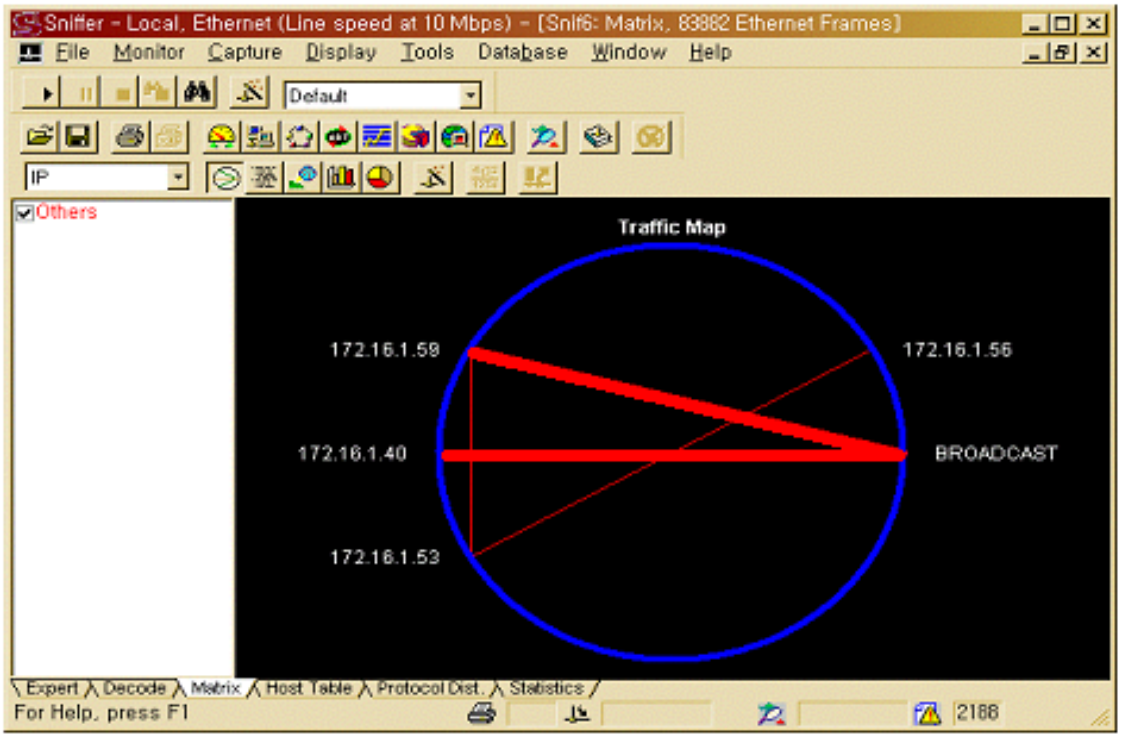


5. 피해증상

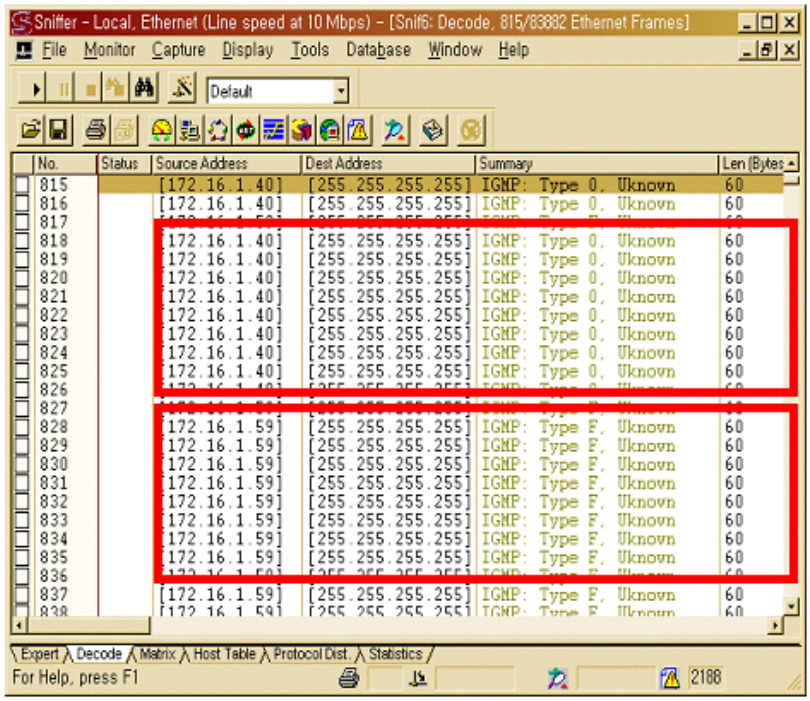
웹서버로부터 다운로드받아 설치된 공격 도구(OOOO, XXXX)가 SDBot에 감염된 두 대의 시스템에서 실행된다.

가. IGMP 브로드캐스팅 공격 도구에 대한 피해증상

다음 그림에서는 패킷을 생성하여 브로드캐스팅하는 IGMP 공격도구의 트래픽 현상을 보여준다.

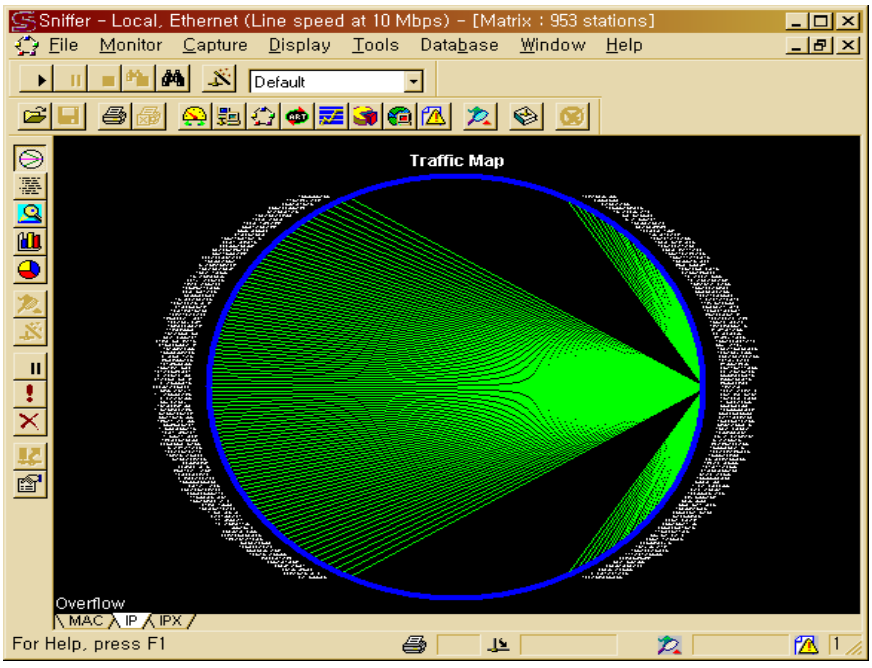


패킷의 형태는 다음과 같은 모습을 하고 있다.

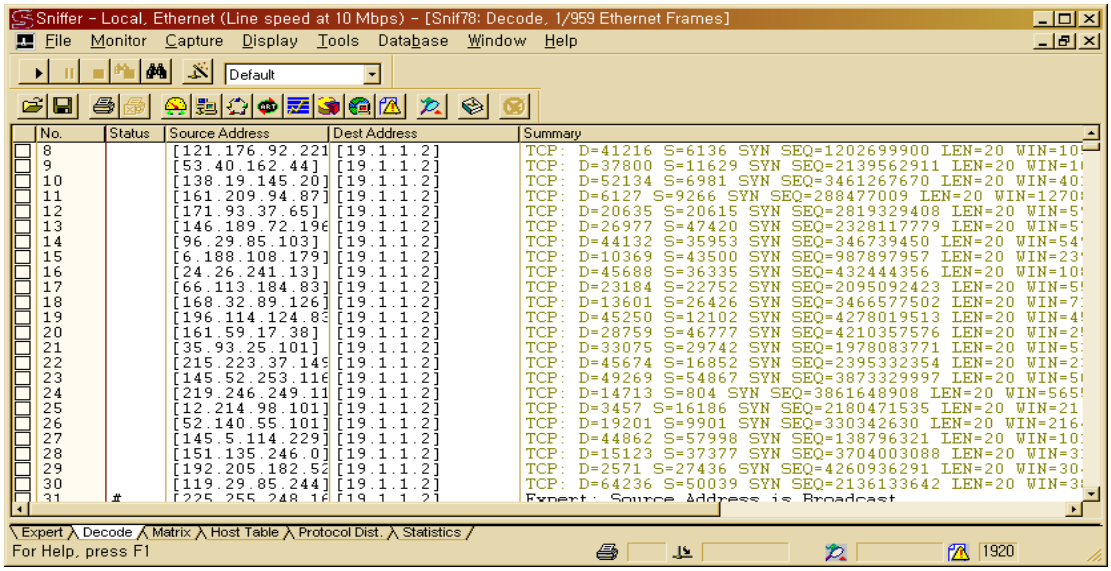


나. SYN Flooding 공격 도구에 대한 피해 증상

소스 IP가 스푸핑된 패킷을 생성하는 SYN Flooding 공격도구에 대한 트래픽 현상이다.



패킷 형태는 다음과 같다.



6. 결과 및 대응방법

본 테스트에서는 SDBot에 감염된 경우 mIRC 클라이언트를 통하여 원격 제어가 가능함을 보여주었다. 즉 SDBot에서 처리될 수 있도록 정의된 특정 형태의 메시지에 의해 어떤 프로그램도 실행 할 수 있으며 이때 사용되는 공격도구에 따라서 네트워크에 부하를 주는 대량 패킷을 생성시킬 수도 있고 패킷의 형태 또한 공격도구에 따라서 다양할 수 있다.

따라서 1월 30일을 전후하여 발생한 네트워크 부하 현상의 원인으로 SDBot이 사용되었을 가능성을 확인하였다. 실제 테스트시 SDBot 이 설치된 두 개의 시스템에서 동시에 공격도구가 실행되었을 때 CPU를 대부분 점령하고 네트워크가 마비될 정도의 부하가 발생하여 PC 가 다운되기도 하였으며 이는 제한된 환경에서 이루어진 시험이므로 실제 환경과 다소 차이는 있겠으나 공격자가 사용하는 공격도구에 따라서 네트워크 마비현상을 초래할 수도 있음은 배제할 수 없을 것이다.

이에 대한 대응방법으로는 사용자 자신도 모르는 사이에 감염 뿐 아니라 공격도구가 실행되기 때문에 근본적으로 SDBot과 같은 트로이목마에 감염되지 않는 것이 중요하다. 따라서 mIRC 채팅 중이나 메일, 웹 게시판에서 출처 및 용도가 불분명한 특정 프로그램을 다운로드 받는 경우 트로이목마일 수 있으므로 다운받지 않도록 하며 다운받은 경우 실행에 앞서 백신을 이용한 검사를 선행해야한다.

또한 시스템이 느려지는 등의 이상 증상이 발생하는 경우 스니핑을 통해 네트워

크 트래픽을 모니터링하여 어떤 시스템에서 어떠한 패킷이 발생하는지 추적하고 차단할 수 있어야 한다.

테스트에서 사용한 SDBot의 경우 시스템 디렉토리에 Syscfg32.exe 파일이 생성되며 레지스트리에 등록되어 윈도우 시작 시 마다 자동 실행 되도록 설정한다. 이는 현재 공개되어 있는 버전마다 파일명이 다르며 공개된 소스에서 파일명을 임의로 수정하여 새롭게 제작 가능하므로 어떠한 이름으로도 생성될 수 있다. 따라서 생성된 파일명을 정확히 알 수 있는 경우 해당 파일과 등록된 레지스트리 정보를 삭제해야 하고 이와 같은 치료작업은 백신 프로그램을 이용할 수도 있다.