<example.pcap 패킷 분석 보고서>

양경석(gaeng4@gmail.com)

* Example.pcap

[시나리오]
트래픽 증가로 인해 네트워크가 느려지고 있어 해당 네트워크에서
패킷을 캡쳐하였다. (TCP Port 80)
(문제)
1. 이 공격에 대해 설명하고 해결하기 위한 방법으로 어떤 것이 있는지 작성하시오.
2. 패킷내에서 잘못된 파일들을 찾아 암호를 찾고 풀어, 이 공격이
   언제 시작해서 언제 끝나는지 추정하시오.

I. 문제 분석
victim: 192.168.0.232 (00:1d:7d:a9:20:18)
네이버, 다음, 구글 등의 사이트에서 웹서핑을 하던 도중 악성코드에 감염된 것으로 판단됩니다.

와이어샤크로 패킷을 보던 중 no 7808, 7809의 cmd.htm 파일을 다운받은 이후 다량의 syn packet이 192.168.0.2로 유입되는 것을 발견하였습니다.

7808 103.540680	192.168.0.232	61.73.23.182	HTTP	418 GET /ph/cmd.htm HTTP/1.1
7809 103.587517	61.73.23.182	192.168.0.232	HTTP	511 HTTP/1.1 200 OK (text/html)

<악성코드로 의심되는 cmd.htm, 암호를 찾을 수 있는 logo1.jpg를 발견한 곳>

HxD로 파일을 분석해보니 signature가 zip파일의 것인 "PK"인 것을 발견하였습니다. cmd.htm의 확장자를 zip으로 변경한 후(cmd.htm.zip), 압축을 해제하려 시도하였으나 암호를 요구하였습니다. 따라서 victim이 다운받은 또다른 파일인 logo1.jpg를 분석하였습니다.

logo1.jpg 파일은 파일이 제대로 열리지 않아, HxD로 분석해 본 결과 signature 부분이 jpg파일의 signature가 아닌 다른 hex[09 09]가 들어있어, 이를 jpg 파일의 signature인 [FF D8]로 바꿔주니 이미지 파일을 열어볼 수 있었습니다. 수정된 파일의 출력 결과는 다음과 같습니다.

cmd.htm.zip 파일을 위에 나온 이미지에 적힌 글자인 "Google"을 압축 해제 시의 비밀번호로 입력하니 압축이 풀리고 아래와 같은 파일을 발견할 수 있었습니다.
파일 이름: cmd.php
파일 내용: OK,1278946800,1279292400,192.168.0.2,80,0

이 파일 내용에서 알아낸 점.
i) 1278946800,1279292400
epoch time형식인 것으로 판단하였습니다. 따라서 epoch를 human readable time으로 변환해주는 사이트(http://www.epochconverter.com/)에서 위 숫자를 입력한 결과 다음의 사항을 알 수 있었습니다.

epoch: 1278946800
GMT: Mon, 12 Jul 2010 15:00:00 UTC
Your time zone: 2010년 7월 13일 화요일 오전 12:00:00 GMT+9:00

epoch: 1279292400
GMT: Fri, 16 Jul 2010 15:00:00 UTC
Your time zone: 2010년 7월 17일 토요일 오전 12:00:00 GMT+9:00

ii) 192.168.0.2,80
-ip address와 port number인 것으로 판단됩니다.

iii) 의문사항
OK, 0의 의미는 정확히 파악하지 못하였습니다. 다만, OK는 시작의 의미, 0은 종료의 의미를 내포하는 것이라고 가정을 해 보았습니다.

II. 파일을 다운받은 이후의 현상.

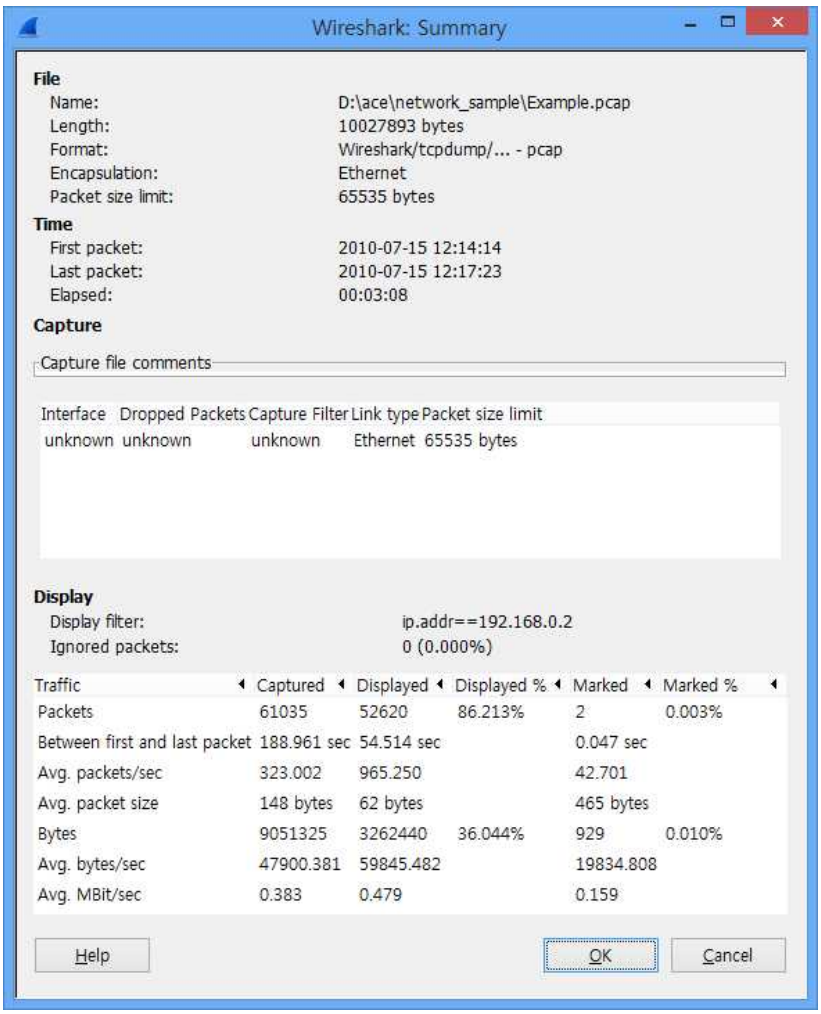
8416 134.447048	22.107.1.118	192.168.0.2	TCP	62 29208→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
8417 134.447061	68.85.103.150	192.168.0.2	TCP	62 32798→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
8418 134.447074	94.153.196.191	192.168.0.2	TCP	62 18187→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
8419 134.447088	64.224.198.217	192.168.0.2	TCP	62 6979→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
8420 134.447101	59.43.103.93	192.168.0.2	TCP	62 54278→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
8421 134.447114	131.32.116.34	192.168.0.2	TCP	62 20266→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
8422 134.447128	195.108.206.155	192.168.0.2	TCP	62 60762→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
8423 134.447141	230.245.80.13	192.168.0.2	TCP	62 4726→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
8424 134.447153	139.13.102.175	192.168.0.2	TCP	62 42863→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
8425 134.447168	168.3.240.71	192.168.0.2	TCP	62 39240→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
8426 134.447180	249.66.162.138	192.168.0.2	TCP	62 22549→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
8427 134.447193	106.189.180.191	192.168.0.2	TCP	62 22804→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
8428 134.447206	216.115.88.238	192.168.0.2	TCP	62 37972→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
8429 134.447219	136.183.150.94	192.168.0.2	TCP	62 1900→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
8430 134.447232	45.252.65.175	192.168.0.2	TCP	62 12606→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
8431 134.447245	173.55.164.175	192.168.0.2	TCP	62 38738→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
8432 134.447258	170.86.92.94	192.168.0.2	TCP	62 17211→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
8433 134.447271	27.3.239.13	192.168.0.2	TCP	62 16395→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1

<중략>

```
61019 188.539546   69.202.40.75     192.168.0.2   TCP   62 25936→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
61020 188.570796   249.89.143.180   192.168.0.2   TCP   62 7520→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
61021 188.586417   200.183.30.123   192.168.0.2   TCP   62 37694→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
61022 188.602047   39.250.141.201   192.168.0.2   TCP   62 1625→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
61023 188.633294   134.127.180.21   192.168.0.2   TCP   62 47896→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
61024 188.664543   217.160.52.174   192.168.0.2   TCP   62 31561→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
61025 188.680175   189.220.36.101   192.168.0.2   TCP   62 4880→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
61026 188.695794   184.205.172.134  192.168.0.2   TCP   62 54384→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
61027 188.727064   212.56.33.197    192.168.0.2   TCP   62 4454→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
61028 188.758294   223.244.210.161  192.168.0.2   TCP   62 41734→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
61029 188.773916   181.200.190.186  192.168.0.2   TCP   62 26684→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
61030 188.805167   248.185.157.142  192.168.0.2   TCP   62 48906→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
61031 188.836414   70.70.109.48     192.168.0.2   TCP   62 3685→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
61032 188.867667   172.20.129.93    192.168.0.2   TCP   62 15637→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
61033 188.883290   214.19.92.158    192.168.0.2   TCP   62 14386→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
61034 188.914539   113.8.13.69      192.168.0.2   TCP   62 28966→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
61035 188.961439   19.4.112.206     192.168.0.2   TCP   62 23366→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
```

cmd.htm 파일을 다운받은 103.540680초(캡쳐시작한 시간을 0초로 기준으로한 시간. 이하 같음) 이후 30.906368초 후인 134.447048초 부터 다량의 [SYN] 패킷이 192.168.0.2의 80번 포트로 유입되는 것을 확인할 수 있었습니다.

III. 세부 분석 및 공격 방법 판단.
이를 wireshark의 Summary 기능을 활용하여 자세히 분석해보겠습니다.



*의심되는 syn packet 분석

-총 패킷의 수: 52620개
-전송기간: 54.514초
-평균 패킷수: 965.250 (패킷/초)
-평균 패킷의 크기: 62바이트(모두 62바이트로 동일함)
-총 바이트수: 3262440 바이트
-평균 전송 크기: 59845.482 (바이트/초)

초당 965개 이상의 패킷이 패킷 수집이 종료될 때 까지인 54초 이상 지속되고 있습니다. 패킷 각각의 크기는 62바이트에 불과하나, 초당 전송된 패킷의 총 크기가 59메가 이상이 되어 충분히 수신자에 부담이 될 수 있으리라 판단됩니다.
이와 같은 상황을 종합해보아 다음과 같은 결론에 이르게 되었습니다.

공격 방법: syn flooding - DDOS(Distribute Denial of service)

ip spoofing을 통해 ip를 바꾸어가면서 192.168.0.2에 대하여 계속 syn을 보냄.

공격자 피해자
syn-------->syn_recv
<--------syn/ack
(ack ------>)원래는 ack를 보내야 하는데 이 과정을 생략함.

syn요청에 대해 ack응답이 없으면 ack응답이 있는 동안 일정 시간 대기를 하게 됩니다.

대기시간이 종료하기 전에 다시 syn요청이 있으면 무한대로 응답을 대기하게 되고, 다른 응답에 요청하지 못하는 상태가 됩니다.
SYN Flooding 공격은 TCP 의 취약점을 이용한 공격의 형태이므로 먼저 TCP 에 대해 알아야 하는데, TCP는 UDP와는 달리 신뢰성 있는 연결을 담당합니다.
따라서 서버와 클라이언트간에 본격적인 통신이 이루어지기 전에는 소위 "3 Way handshaking" 이라는 정해진 규칙이 사전에 선행되어야 한다.
결과적으로 TCP의 장점인 신뢰성이 TCP의 약점이 되는 것이며 이를 이용하여 DOS공격이 이루어지는 것입니다.

src MAC: 00:1d:7d:a9:20:18(동일)
src IP : 가변

위 공격은 MAC 주소는 동일하나, 출발지 ip를 계속 바꾸어주면서 syn을 보내주는 ipspoofing을 같이 한 것으로 판단됩니다.

클라이언트의 ACK 응답이 없으면 서버에서는 클라이언트의 접속 정보를 잠시 log에 쌓아 두는데, 이러한 요구가 증가했을 경우 시스템은 log 기록 공간을 충분히 확보하지 못하게 되고, 결국 네트워크 중단으로 이어져 서비스 거부가 일어나게 됩니다.
결과적으로 공격자가 80번 포트로 syn만 계속 보내어 다른 사용자의 응답을 받을 수 없는 상태가 되어 인터넷 사용이 불가한 상태에 이르게 됩니다.

IV. 방어방법

1. 감염 차단

(1)Signature based detection
협의적인 IPS에 대해 널리 이해되고 있는 기능입니다. 공개된 취약점에 대한 Exploit Code가 존재할 때 이를 signature화 하고 DB 형태로 관리하며 입력된 패킷의 payload를 이 DB에서 검색하여 패킷에 유해 signature가 포함되어 있는지 검사하는 방법으로, 발견된 signature를 통해 공격 종류를 적시할 수 있으며, 공격에 대해서 IP 주소, 프로토콜, 포트 등에 관계없이 명확하게 탐지해 낼 수 있는 반면 Signature가 명확하지 않으면 False Positive가 발생할 확률이 높다는 단점이 있습니다.

(2)Anti-Virus
Payload를 하나의 파일로 형성(Assemble)하여 Virus 검사 엔진에 전송하고 감염여부를 리턴 받아 해당 파일을 원래 세션을 통해 전달(Dissemble)하는 방식으로 Assemble/Dissemble 과정을 거치므로 속도가 현저히 떨어집니다. 신규 바이러스 패턴의 신속한 업데이트도 필요합니다.

2. 감지 후 차단, 확인 후 통과

일단 바이러스나 웜에 감염되어 공격 시도 및 2차 감염 시도가 발생하면 전체 세션의 증가, 특정 포트에 대한 트래픽 증가 등 어떤 변화가 발생하게 되고 네트워크 길목에 위치한 IPS에서는 이러한 이상 징후에 기반하여 특이 상황 인지를 할 수 있으며, 차단도 가능하다. 이상 징후들과 그에 대한 대처 방안을 살펴보면, 다음과 같습니다.

(1)세션 폭주 탐지
통계 분석 기법에 의해 비정상 트래픽을 차단하는 방식으로 알려지지 않은 유해 트래픽의 피해를 최소화 할 수 있습니다.

(2)세션 제한
특정 트래픽에 대해 전체 세션 제한을 설정하는 방법으로 네트워크 장비들을 보호할 수 있으나, 정상적인 세션까지 영향을 받을 수 있는 단점이 있습니다.

(3)한계 값 초과 탐지
특정 목적지로의 SYN 요청이 단위 시간당 한계 값을 초과하는 경우 해당 목적지 IP 주소로 향하는 모든 패킷을 차단하는 방식으로 유해 트래픽 차단은 이루어지나, 해당 목적지 서버가 수행하는 서비스가 전면적으로 불통될 수 있다는 것이 단점입니다.

(4)발신지 IP 주소에 대한 확인
실제 존재하는 발신지 주소인지 혹은 유효한 주소인지 검증 후 패킷의 통과 여부를 결정하는 방식으로 다음과 같은 차단 방법들이 있습니다.
・RFC1912에서 정의한 비공인 IP 주소는 차단한다.
・255.255.255.255 등과 같은 도저히 발신지 IP 주소로 사용할 수 없는 주소는 차단한다.
・IANA가 할당하지 않은 IP 주소이면 차단한다.
・IP Header를 이용하여 TTL 값이 일정하면서 발신지 IP 주소가 변하는 SYN Packet들을 차단한다.
・모든 SYN 패킷에 대해서 발신지 확인 패킷을 보내고 해당 응답에 따라서 통과 및 차단을 결정한다.

(5)White List기법
SYN Flooding에 의해 발생하는 IP 주소들은 대부분 실제로 존재하지 않는 경우가 대부분이라는 점을 이용한 기법이다. 이때, IPS는 실제로 존재하는 IP 주소 List를 가지고 있다면, 이 List에 존재하지 않는 IP 주소를 목적지로 하거나 발신지로 하는 Packet들을 모두 차단하는 기능이다.

3. 발생 차단

이 방법은 유해 트래픽을 발생시키는 클라이언트를 찾아내어 발생 자체를 차단하는 방법으로 발생의 근원을 네트워크에서 완전히 격리시키게 된다.
내부의 모든 Client들에 Agent를 설치하여, 이들 Agent와 IPS가 통신을 하며, 이상 트래픽 검출 시 해당 트래픽을 유출하는 컴퓨터에 강제 차단 명령을 보내어 네트워크로부터 격리시킨다. 다양한 경로를 통하여 침투된 Worm 및 Virus를 신속히 격리하는 가장 효과적인 방법이다. 이를 위해 Agent의 설치, 탐지 및 격리 3단계의 작업이 수행된다.

4. 최선의 방법 선택

SYN Flooding이라는 단 하나의 구체적 위협에 대한 방어가 다양한 측면의 다양한 기능이 어떤 구체적인 방법으로 이루어지는지를 살펴보았습니다. 위에서 설명한 방법들은 제 각각 단점은 있지만 독립된 기능으로써도 충분한 가치는 있습니다. 어느 한가지 가장 최선의 단 한가지 방법을 선택할 수는 없습니다.
왜냐면 각각의 기능들이 제 각각의 단점과 장점을 가지고, 각 사이트 상황에 따라 적용의 효과가 다르게 나타나기 때문입니다. 따라서, 최선은 각각의 단점들을 상호 보완할 수 있는 즉, 위 3가지 방법들의 기능을 하나의 통합된 IPS로 구현하여, 3중의 방어체계를 갖추도록 하는 것입니다. IPS는 앞에서 기술되었듯이 인터넷의 위협들에 대해 다측면 방어를 수행하는 통합 보안 장비여야 합니다.
[월간 정보보호21(info@boannews.com)에 실린 나원택 시큐아이닷컴 NXG 혁신팀 팀장 님의 글을 일부 발췌 및 인용하였습니다.]

V. 결론

위 상황을 종합하여 볼 때, 한국시간으로 2010년 7월13일 화요일 오전 12시에 공격 명령을 시작 2010년 7월17일 토요일 오전 12시에 공격 명령을 종료하는 명령에 따라 처음 패킷이 수집된 2010년07월15일 12:14:14분부터 103.540680초 지난 시기에 악성코드를 다운받아 그로부터 30.906368초 후인 134.447048부터 ip spoofing을 통한 DDOS(SYN FLOODING) 공격에 노출되었습니다. 이에 공격 종료 예상시기인 2010년 7월17일 토요일 오전 12시까지 별다른 조치가 없는 경우 인터넷 사용이 불가할 것으로 판단됩니다. 위의 방버방법 중 한개 이상의 조치를 취하여 DDOS공격에 대비해야 할 것입니다.