情 報 保 護 學 會 誌
第21卷 第4號, 2011. 6

네트워크 포렌식을 통한 분산서비스거부공격 비교분석

김 혁 준*, 이 상 진**

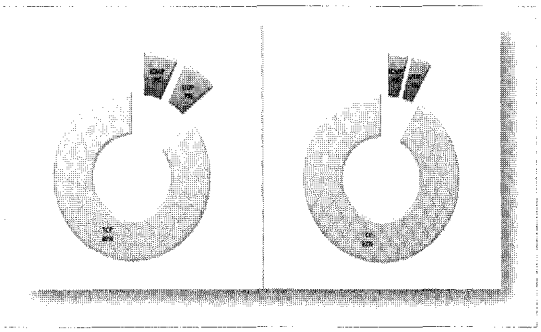
요 약

2011년 3월 4일 발생한 DDoS 공격은 악성코드 제작, 봇넷 구성 및 공격전개 방식에서 지난 2009년 발생한 7.7 DDoS 공격과 많은 유사점이 있다. 그러나 공격 전략과 공격 수행 방법 측면에서 좀 더 자세히 분석해보면 상호간의 유사점보다는 차이점이 더 많음을 알 수 있다. 7.7 DDoS 공격의 경우 공격자는 공격 전개를 위해 좀 더 많은 시간을 투자하였으며 당시 국내 DDoS 방어수준에 대한 정확한 이해를 바탕으로 매우 효과적인 공격을 수행하였다. 그러나 3.4 DDoS 공격의 경우 공격자는 공격 망 구성을 위해 충분한 시간을 투자하지 않았으며, 비록 악성코드 전개에 있어 진일보한 모습을 보였으나 DDoS 방어수준에 대한 충분한 이해가 부족하였던 것으로 나타났다. 본 고에서는 2011년 3.4일 발생한 DDoS 공격을 네트워크 수준에서 양 공격의 유사점과 차이점을 분석 비교한다.

Ⅰ. 서 론

DDoS 공격은 일반 해킹(Cracking) 공격과 비교해 볼 때 그 시작부터 공격이 방어자에게 노출되며 전술적으로 방어자는 네트워크 경계지점 (Network Perimeter)에서 공격자와 정면 대결을 피할 수 없다는 특성이 있다. 따라서 뛰어난 공격자는 최대한 방어가 어려운 방법을 택하며 뛰어난 방어자는 가용한 모든 정보를 사용하여 공격 트래픽과 정상 트래픽을 분리하여 정상 사용자의 가용성을 침해하지 않으면서 공격 트래픽을 선택적으로 차단한다.

7.7 DDoS 공격은 당시 대부분의 방어 체계가 대량 패킷 전송(Flooding Attack) 중심으로 운용되고 있었던 데 반해 어플리케이션 수준의 공격을 수행함으로써 많은 사이트에 큰 피해를 주었으며, 피해 사이트에서 공격 패킷과 정상 패킷을 완벽하게 분리할 수 없도록 많은 노력을 함으로써 매우 효과적인 방어가 어렵게 하였다. 따라서 코드 분석에 의해 공격 시간이 예고되었음에도 불구하고 많은 방어지점에서 효과적인 방어가 이루어지지 않았다. 당시 공격자는 Browser Pinning, TCP 연결 후 패킷복제, 패킷크기 및 시그니처 다변화 등 다양한 공격 전략을 구사하여 국내 인터넷 전반에 큰 혼란을 야기하였다.



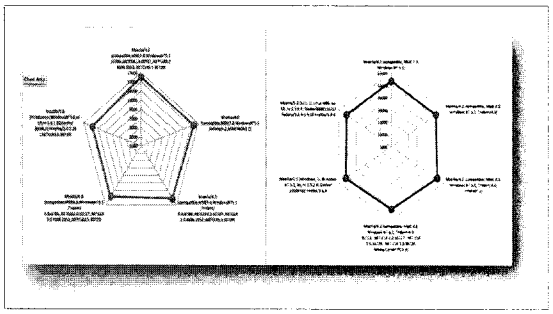
〔그림 1〕 공격프로토콜 분포 비교

Ⅱ. 공격의 유사점

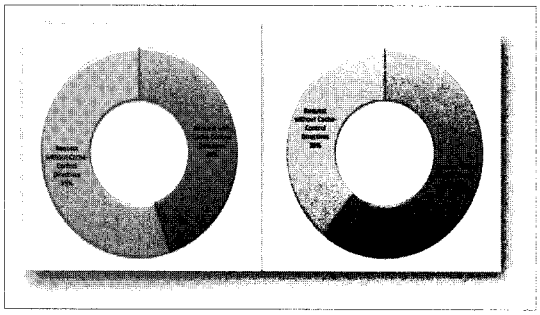
양 공격은 공격망 구성 방식에 있어 악성코드 전개·운용 및 좀비구성 측면에서 많은 유사점이 보이며 또한 DDoS 공격 측면에서도 다수의 서버를 목표로 한 것, TCP, UDP, ICMP와 같은 복수의 공격 프로토콜을 선택한 것, HTTP Cache-Control Directive를 사용한 것 등 외형적으로 많은 유사점을 찾아 볼 수 있다.

[그림 1]은 양 공격 당시 사용된 프로토콜 분포를 나타내는데 ICMP 및 UDP 패킷 비율이 각 7%에서 약 4%로 줄어든 것을 제외하면 연결성 공격인 TCP 공격

* 고려대학교 정보보호대학원, 나루씨큐리티(joonkim@narusec.com)
** 고려대학교 정보보호대학원 (sangjin@koera.ac.kr)



〔그림 2〕 HTTP User Agent 분포 비교



〔그림 3〕 Cache-Control Directive 사용비교

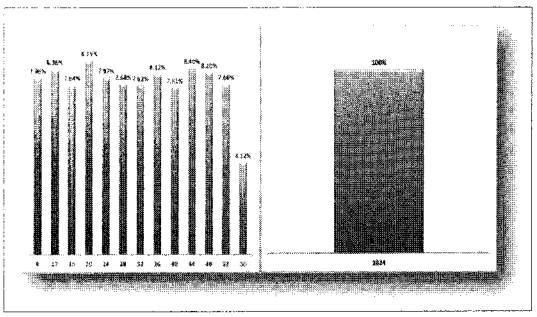
이 주종을 이루며, 비연결성 공격인 UDP 및 ICMP 패킷이 이에 종속적으로 사용되었다는 점에서 매우 유사한 형태를 이루고 있다. 또한 [그림 2]에서 보이는 것과 같이 HTTP User Agent 선택에 있서 오류가 존재하지 않는 다수의 유저 에이전트 스트링을 일정한 비율로 사용한다는 점에서도 상호 일맥상통 한다는 것을 알 수 있으며, 7.7 DDoS 공격의 대표적인 특징 중 하나인 HTTP 헤더의 Cache-Control 구문 사용 비율 역시 매우 유사한 것을 알 수 있다. [그림 3]은 양 공격에서 HTTP 헤더에 사용된 Cache-Control 구문 사용비율을 나타낸 것으로 왼쪽 그래프는 7.7 DDoS 공격에서 사용된 비율로 총 HTTP Request의 약 45%를 차지하고 있으며 오른쪽은 3.4 DDoS 공격에 사용된 것으로 약 40% 정도의 사용비율을 보이고 있다.

HTTP 헤더에 Cache-Control 구문을 사용한 CC-ATTACK은 헤더에 사용된 must-revalidate 구문이 RFC 표준에서는 정상적인 HTTP 요청 헤더(Request Header)에서 사용될 수 없다는 것이 입증되어 대표적인 공격차단 시그니처로 사용되어 왔다. 이러한 전제 하에 동 내용이 포함된 연결을 차단하는 방식을 사용할 경우에도 7.7 DDoS 공격의 경우 나머지 55%의 공격이 특별한 차단 시그니처가 없었으며 3.4 DDoS 공격의 경우 약 60%의 공격에서 해당 구문이 사용되었다. 그러나 이러한 사실은 다수의 분석보고서 또는 매체를 통해 일반에 널리 알려진 사실로 이를 바탕으로 양 공격을 수행한 공격자가 매우 유사하거나 혹은 동일 공격자라는 결론을 도출하는 것은 충분하지 않으며 이를 위해 보다 면밀한 분석이 수행되어야 한다.

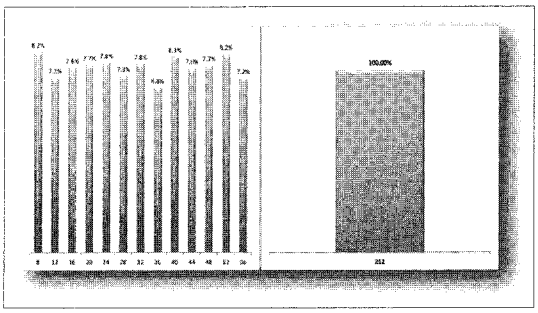
Ⅲ. 공격의 차이점

앞서의 유사점에도 불구하고 양 공격을 좀더 심도있게 비교해 보면 공격 전략 수립 측면에서 많은 차이가 발생한다는 것을 알 수 있다. [그림 4]와 [그림 5]는 비연결성 플러딩 공격에 사용된 UDP, ICMP 패킷 크기의 분포를 나타내는데 그림 왼쪽에 표시된 7.7 DDoS 공격의 경우 차단을 어렵게 하기 위해 의도적으로 다양한 크기의 패킷을 생성하였으나, 3.4 DDoS 공격의 경우 전 공격에서 단일 크기의 패킷이 생성된 것을 알 수 있다.

또한 이러한 차이점은 7.7 DDoS 공격의 속성 중 일

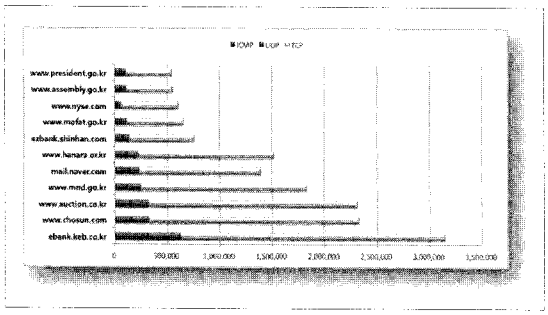


〔그림 4〕 UDP 패킷 크기 분포 비교



〔그림 5〕 ICMP 패킷크기분포 비교

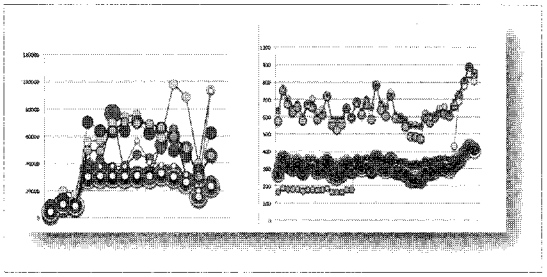
〔그림 6〕 Duplicated ACK 패킷비율 비교



〔그림 7〕 7.7 DDoS 공격 사이트별 패킷전송비율

반인에게 거의 알려지지 않은 복제 패킷 전송 부분에서 뚜렷한 차이를 보인다. 7.7 DDoS 공격 당시 공격자는 다단계공격전략(Attack-in-Depth)을 구사하였는데 ACK 패킷 복제는 이 중 대표적인 것으로 종단 서버의 TCP 스택에 도달하기 전에는 기술적으로 차단이 불가능한 기연결 ACK 패킷을 복제하여 IPS 등 시그니처 기반 접근제어 장치에 부하를 유발하였다. 그러나 3.4 DDoS 공격의 경우 정상적 TCP Retransmission을 제외한 패킷전송은 전혀 이루어 지지 않았다. 특히 3.4 DDoS 공격에 사용된 HTTP GET Flooding 헤더에는 Proxy-Connection 헤더 필드가 존재한다. 이는 다수의 HTTP 요청을 소수의 TCP 연결을 통해 전송하는 방법으로 DDoS 공격시 발생하는 서버의 부하를 감소시키는 효과를 가져온다는 점에서 공격자의 의도가 명확하지 않고 또한 HTTP 1.1 표준에 벗어나는 사용법으로 3.4 DDoS 공격의 주요 차단 시그니처로 동작했다.

또한 공격자의 공격 패킷 분산 방법 역시 상이한 모습을 보였다. DDoS 공격 중 GET Flooding과 같은 연결성 공격의 경우 최대 공격량은 피해 서버의 웹 가용성(HTTP CPAPCITY)에 제한적이며 따라서 공격자는 좀비에서 생성되는 TCP SYN 패킷 생성비율을 조절할 수는 있으나 서버와 클라이언트 사이의 실 TCP 연결수



〔그림 8〕 사이트 별 연결요청수분포 비교

를 제어할 수는 없다. 따라서 공격자는 충분한 공격 에이전트를 확보한 경우 별도의 흐름 제어 메커니즘을 구현하지 않아도 TCP Congestion Control과 피해 사이트의 가용성에 따라 가변적인 트래픽을 전송하게 되며 이는 [그림 7]에 나타난 것과 같이 7.7 DDoS 공격시 국내 주요 사이트에 전송된 패킷 수 분표를 통해 알 수 있다.

Ⅳ. 유효 공격량

유효 공격량이란 피해 사이트에 설치된 DDoS 방어 장치에서 대응이 불가능한 공격 트래픽을 나타낸다. 양 공격의 비교를 위해 7.7 DDoS 공격 당시의 유효 공격량을 100으로 보았을때 3.4 DDoS 공격의 유효 공격량은 아래와 같이 구해질 수 있다. [표 1]은 3.4 공격 차단에 사용된 2개의 HTTP 헤더에서 추출한 시그니처 값인 Cache-Control 스트링과 Proxy- Connection 스트링의 분포를 나타낸다.

〔표 1〕 HTTP 헤더 상의 차단 시그니처 분포

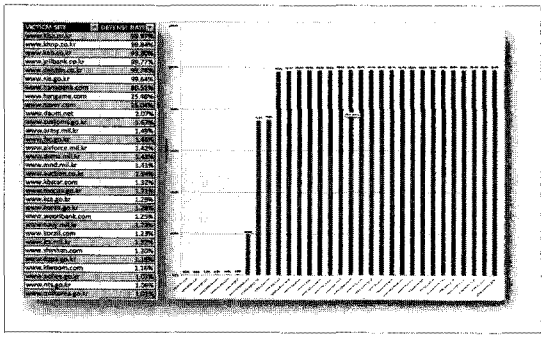
분 류	해당요청 수	비 율
HTTP REQ	317717	100%
Cache-Control	191025	60.1%
Proxy-Connection	317727	100%
모두 포함	191025	60.1%

앞에서 나타난 내용과 3.4 DDoS 공격 직후 발표된 안철수연구소의 공격비교표에 나타난 좀비 및 공격사이트 수를 참조하여 차단 시그니처가 모두 적용된 경우 아래와 같은 각 사이트 별 초당 유효공격수를 구할 수 있다.[1)]

1) 어플리케이션 수준의 공격 특성상 각 사이트 별 정확한 유효 공격량을 예측할 수는 없으나 사용된 좀비의 수 공격 대

유효공격수 = 좀비수 × 요청수 × 차단불가율2)

⌘ 좀비수 = 좀비IP수/피해사이트수
⌘ 요청수 = HTTP Request 수
⌘ 차단불가율 = 시그니처미포함트래픽/전체트래픽



〔그림 9〕 사이트별 방어현황

〔표 2〕 유효공격수

분류	좀비	대상	요청	차단	유효
7.7	20만	23	11.4	0.5	5K
3.4	11만	40	8.7	1	0

⌘ 좀비 :공격시 사용된 것으로 보고된 좀비수
⌘ 대상 : 공격대상 사이트 수
⌘ 요청 : 초당 평균 요청 수
⌘ 차단 : 차단비율(1=100%)
⌘ 유효 : 차단불가(시그니처미포함) 요청

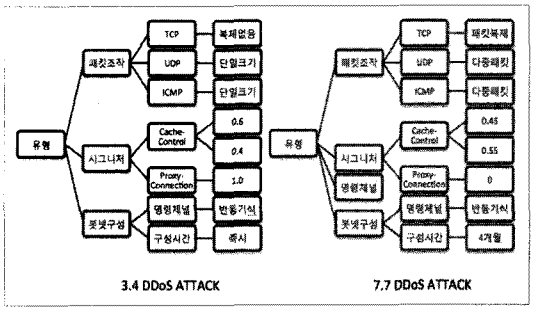
[그림 9]는 각 각 사이트 별 유효 공격량을 분석한 것으로 3.4 DDoS 공격 에이전트에 감염된 PC에서 발생된 공격패킷 분석을 통해 얻어진 정보이다.

3.4 DDoS 공격 발생 시 공격대상 사이트는 전반적인 가용성을 유지하고 있었기에 공격 당시 공격 클라이언트와 피해서버 간의 TCP연결(삼중연결 완성기준) 수와 HTTP GET 요청의 전달 수 비교을 통해 각 사이트의 방어 수준을 유추할 수 있다. 인터넷진흥원, 한국수력원자력 등 상위에 위치한 사이트들은 99% 이상의 방어가 이루어졌다. 이는 해당 공격이 방어가능한 공격이었으며 빠르고 정확한 대응이 이루어진 사이트의 경우 대부분의 공격 패킷이 차단 된 것을 나타낸다. [그림 9]에서 중위권과 하위권에 위치한 사이트는 각각 적용된 시그니처의 수와 적용시점에 따라 80%에서 1%의 방어가 이루어진 것으로 유추할 수 있다.3)

V. 공격자 프로파일링

공격자 프로파일링(Criminal Profiling)이란 공격자의 특성을 수집된 증거 및 정황에서 추론하는 것으로 본 고에서는 7.7 DDoS 공격과 3.4 DDoS 공격 당시 수집된 네트워크 데이터 분석을 통해 1차적인 공격자의 특성을 분석하는데 사용된다. [그림 10]은 2009년 7월 7일 발생한 DDoS 공격과 2011년 3월 4일 발생한 DDoS 공격을 공격의 통제측면에서 분석한 것이다.

3.4 공격의 경우 기술적으로 통제가 어려운 TCP ACK 패킷 복제는 전혀 발생하지 않았고, ICMP 및 UDP 패킷전송 시 전송크기를 단일화하여 사이즈 정보를 통한 패킷통제를 용이하게 하였고 특히 HTTP헤더에 삽입된 Cache-Control 스트링과 Proxy- Connection 스트링을 통해 HTTP 세션의 100% 차단을 용이하게 하였다.



〔그림 10〕 공격자프로파일링 비교

또한 공격에이전트 생성에 충분한 시간을 투자하지 않아 공격 에이전트의 수가 7.7 DDoS 공격에 크게 못 미치는 수준으로 구성되었다. 반면 7.7 공격의 경우

상 사이트의 수 및 차단가능한 공격의 수를 이용하여 전체적인 수준에서의 유효 공격량을 구할 수 있다.

2) 각 공격 일시 별 대상 사이트의 수 등 많은 부분의 데이터는 안철수연구소의 3.4 DDoS 공격분석보고서값으로 단순화되어 계산하였으며 양 공격 당시 알려진 시그니처가 모두 적용된 경우를 나타낸다.

3) 해당정보는 하나의 공격 에이전트에서 생성된 패킷을 분석한 것으로 다른 공격에이전트에서는 이와 상이한 값을 생성할 수 있다

TCP 전송시 기 연결된 패킷의 복제를 통해 중간차단장치에서 통제가 불가능하였고, 다중 크기의 ICMP 및 UDP 패킷을 생성하여 사이즈를 이용한 패킷통제가 용이하지 않도록 구성하였으며 특히 캐시장비 우회를 위한 Cache-Control 구문 사용 시 해당 구문이 추가된 헤더의 수가 그렇지 않은 헤더의 수보다 적게 구성하여 동 시그니처를 통해 차단이 이루어진다고 해도 시그니처가 존재하지 않는 나머지 55%의 패킷이 트래픽 종단지점까지 전송되도록 구성하였다. 또한 약 4개월에 걸친 숙성과정을 거친 공격봇넷은 공격대상사이트를 모두 무력화하기에 충분한 크기로 이루어졌다.

Ⅵ. 결 론

이러한 분석으로 지난 7.7 DDoS 공격과 3.4 DDoS 공격이 동일한 공격자에 의해 수행된 것인지 혹은 단순 COPYCAT을 통해 수행된 것인지 밝혀내는 것은 사실상 불가능할 것이나 분석된 사실을 바탕으로 다음과 같은 내용을 유추할 수 있다.

3.4 DDoS 공격은 7.7 DDoS 공격과 비교 시 악성코드 운용에서는 보다 향상된 공격기법을 선보였으나 DDoS 공격 시 공격 구별이 가능한 문자열의 삽입, 단순화된 패킷 생성 등 DDoS 공격차원에서는 2009년 공격보다 퇴화된 모습을 보였다. 7.7 DDoS공격자는 당시 국내 사이트의 DDoS 공격 방어수준 및 DDoS 공격기법에 대해 폭넓은 이해를 갖추고 이를 통해 국내 사이트를 무력화 하기 위한 공격을 수행하였다.

3.4 DDoS 공격자는 공격 내용으로 볼 때 DDoS 공격 및 현 방어수준에 대한 충분한 이해를 갖추기 못하였으며 본 고에서 기술된 다양한 정황적 사실을 통해 공격 통제에 보다 많은 노력을 기울인 것을 알수 있다.

이는 7.7 DDoS 공격과 3.4 DDoS 공격을 가장 명확하게 구분하게 하는 것으로 7.7 DDoS 공격은 피해 사이트의 서비스거부를 목적으로 한 전문가의 자발적 공격이라는 성격이 크며 3.4 DDoS 공격은 제 3자의 요청을 받고 공격을 수행하여 유시시 공격의 강·약 및 차단정도를 조절할 수 있는 청부공격의 성격을 가진다고 볼 수 있다.

2011년 현재 DDoS 공격자들은 차단 시그니처가 존재하지 않는 브라우저 수준으로 동작하는 봇넷을 구성하여 운영하고 있으며 이러한 공격기법을 이용한 공격은 현재의 방어수준으로는 쉽게 방어 할 수 없다는 것이 사실이다. 비록 3.4 DDoS 공격이 국내 인터넷에 큰 피해를 주지 못하였지만 이 사실이 앞으로 발생한 많은 공격이 3.4 DDoS 공격과 같이 대응됨을 의미하지 않는다. 따라서 방어자는 빠르게 진화하는 공격자의 움직임을 파악하고 이에 대응할 수 있는 방어기제를 개발·적용하는 것이 무엇보다 필요하다고 하겠다.

참고문헌

[1] 김혁준 "일회성 봇넷의 출현과 DDoS 위협관리", 제13회 해킹방지워크샵, pp. 120-143, 2009년 11월
[2] 안철수연구소 "3.4 DDoS 분석보고서", 2011년 3월
[3] 금융보안연구원, "3.4 DDoS공격 분석결과" pp. 2-6, 2011년 3월

〈著者紹介〉

김 혁 준 (Hyukjoon Kim)
정회원
2004년 6월: 캐나다 알버타주립대학교 컴퓨터공학과 졸업
2009년 2월 : 고려대학교 정보경영공학전문대학원 수료
2011년 1월~현재 : 나루씨큐리티 기술이사
관심분야 : 정보보호 지표화, 정보보호 시각화, 침해사고대응, DDoS 공격대응

이 상 진 (Sangjin Lee)
종신회원
1987년 2월: 고려대학교 수학과 학사
1989년 2월: 고려대학교 수학과 석사
1994년 2월: 고려대학교 수학과 박사
1989년 2월 - 1999년 2월 : 한국전자통신연구원 선임연구원
1999년 2월 - 2001년 8월 : 고려대학교 정보경영공학대학원 교수
<관심분야> 대칭키 암호, 정보은닉이론, 디지털 포렌식