이것만은 알아야 할 네트워크 보안 이야기

Part 6. DDoS 2. DDoS 공격의 탐지 방안

글. 이선응 아이크래프트 수석

연재 목차

지난 호에 이어 DDoS 공격을 어떻게 탐지하는지 알아보도록 하겠다. DDoS 공격으로 대용량의 트래픽이 들어올 때, 이것이 공격으로 발생한 트래픽인지 아니면 정상적인 사용자가 짧은 시간 내에 폭주해서 발생한 트래픽인지 구분하기가 쉽지 않다. 필자의 경우 2008년 한 신문사의 온라인 시스템의 방화벽을 관리하고 있을 때, 갑자기 방화벽의 CPU 사용량이 70% 이상 넘어가고, 방화벽이 모니터링하는 세션 수가 장비의 한계치까지 사용 중이라는 연락을 받고 장비를 점검한 적이 있다. 해당 고객사의 방화벽은 평상시 1~2만 개의 세션만 사용하고 있었는데 방화벽이 관리 가능한 50만 개의 세션 수를 이미 사용하고 있어서 신규로 세션을 생성할 수 없어 사용자들이 신문기사를 읽을 수 없는 상황이 되었다. 방화벽이 관리하는 50만 개의 세션을 강제로 삭제하였더니 10초가 지나면 다시 세션이 Full이 차는 증상이 반복되었고, 이런 현상은 2시간이 지나서야 해소되었다. 나중에 안 사실이지만, 그때 한 연예인의 자살 기사가 해당 신문사의 온라인 기사로 올라왔고, 우연히 해당 기사가 포털 사이트의 메인화면에 노출되면서 많은 사용자가 호기심에 해당 기사를 클릭하면서 발생한 해프닝이었다.

돌이켜보면, 이런 현상은 정상적인 단말이 특정한 이벤트가 발생하면서 트래픽이 폭주한 상황이다. DDoS 공격은 아니지만, 결국은 DDoS 공격과 동일하게 서비스가 불가능하게 된 것으로 이런 증상이 반복된다면, 방화벽의 용량과 서버의 용량을 증설하는 것이 최선의 방법이고 지금이라면 클라우드를 통해 짧은 시간 안에 대응이 가능할 것이다. 그럼 만약 그 당시에 DDoS 방어 장비가 있었더라면, 이 현상을 공격으로 탐지했을까, 아니면 정상적인 트래픽으로 판단했을까. DDoS 방어 장비 운영자의 딜레마가 여기에 있다. 보통 공격탐지는 임계치 이상이면 공격으로 탐지하고, 이하이면 정상적인 트래픽으로 판단한다. 만약에 임계치를 너무 낮게 설정한다면, 정상적인 경우에도 공격탐지로 인식되어 알람이 빈번하게 일어날 것이다. 반대로 임계치를 너무 높게 설정하면 공격이 일어난 경우에도 정상상황으로 인식하여 공격을 탐지하지 못할 확률이 높다. 정리하면 임계치(Threshold)를 어느 레벨로 설정하느냐가 공격탐지의 정확도와 직결된다.

지난 호에서 DDoS 장비에는 인라인과 아웃오브패스방식 2가지가 있다고 설명해 드렸다. 인라인장비는 탐지와 차단을 하나의 장비에서 수행하고, 아웃오프패스 장비는 탐지와 차단이 2개의 전용 장비에서 각각 수행된다.
이번 호에서는 아웃오프패스방식의 탐지 장비에서 공격을 어떻게 탐지하는지 설명하겠다. 이후 설명에서 아웃오브패스 장비는 아웃라인 장비로 호칭하도록 하겠다.

아웃라인 장비의 특징은 트래픽이 흐르는 회선을 직접 모니터링하지 않기 때문에 동시에 여러 개의 회선을 모니터링할 수 있는 장점이 있다고 하였다. 이런 동작이 가능한 이유는 트래픽을 처리하는 라우터와 스위치에서 트래픽 정보를 수집하기 때문에 가능한 기능이다. 라우터가 패킷(큰 데이터를 잘게 쪼갠 단위)을 받아서 처리할 때 전송한 패킷의 여러 정보를 확인할 수 있다. 패킷의 출발지, 목적지 IP 주소, Port 넘버, 프로토콜 종류 및 세부 정보, 패킷의 개수 및 바이트 양, 처리시간, 패킷이 들어오고 나간 인터페이스 정보 등 다양한 정보를 확인하여 상세한 트래픽 모니터링에 활용 가능하다. [그림 1]과 같이 NetFlow가 지원되는 네트워크 장비에서는 패킷을 처리할 때 생성한 정보를 분석 서버로 전송이 가능하다.

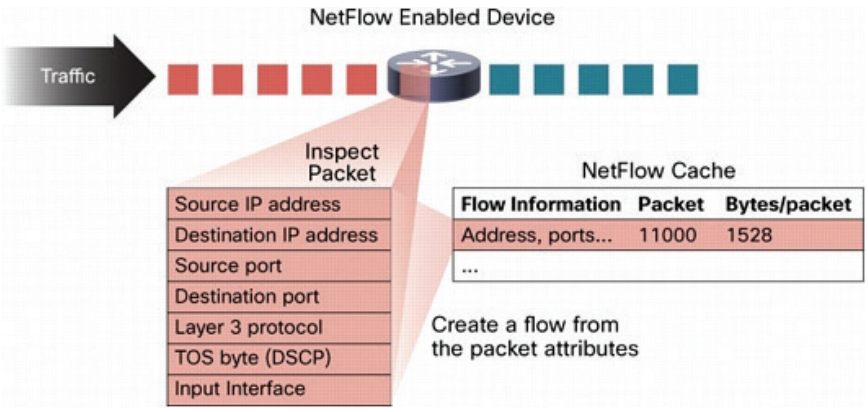

그림 1. NetFlow 생성 방식 및 보유 정보 / 출처 : CISCO SYSTEMS

아웃라인 타입의 탐지 장비는 모니터링 대상인 라우터가 보내주는 Netflow 정보를 수신하고, 라우터의 여러 인터페이스를 통해 들어오는 트래픽을 분석하여 DDoS 공격을 모니터링하게 된다. 장비관리자가 먼저 해야 할 일은 DDoS 공격으로부터 방어할 서버들의 IP 주소를 지정하는 것이다. 탐지 장비가 수집하는 Netflow 정보의 출발지, 목적지 IP 정보와 모니터링 대상 IP 주소를 매칭해서 방어 대상 서버의 트래픽을 모니터링할 수 있기 때문이다. 실제로 탐지 장비가 하는 일은 보호 대상 서버 IP 주소를 기준으로 들어오고 나가는 트래픽 정보를 모니터링하다가 관리자가 설정한 임계치를 넘으면 경보를 보내고 해당 서버로 가는 트래픽을 차단 장비로 우회시키는 일이다.

탐지 장비가 세부적으로 어떻게 공격으로 판단하는지 알아보자. 탐지 장비는 모니터링 대상 서버 IP가 설정되면, 해당 IP 주소를 기준으로 별도의 DB 테이블을 생성한다. 생성 이후 수신되는 Netflow 정보 중에서 해당 서버의 IP 정보가 출발지 혹은 목적지에 있으면 Netflow가 가지고 있는 다양한 정보를 선별적으로 DB에 기록하고 모니터링한다. 먼저, 모니터링 대상이 목적지가 되는 정보는 해당 서버로 들어오는 트래픽을 모니터링하는 것이고, 출발지가 되는 정보는 서버가 외부로 보내는 트래픽을 모니터링하게 되는 것이다.

일반적인 서버는 인터넷을 통해 불특정 다수의 클라이언트가 서버로 접속하기 때문에 모니터링되는 출발지 IP가 매우 많은 것이 보통이다. 탐지 장비는 서버에 접속한 클라이언트가 1,000개라고 하면 각각의 클라이언트가 서버로 보내는 트래픽을 각각 모니터링하고 있다가 특정한 클라이언트가 임계치 이상의 트래픽을 보내게 되면 해당 클라이언트를 공격자로 판단하게 된다. 즉 1,000개의 연결을 동시에 모니터링하면서 트래픽 양이 설정한 임계치를 넘는지 확인하는 것이다. 임계치는 [그림 2]와 같이 다양한 프로토콜과 조건에 해당하는 트래픽에 대해 1, 2차 임계치로 분리하여 설정한다. 먼저 Total Traffic은 각각의 출발지 IP 기준으로 모든 트래픽에 대한 임계치를 설정하는 것이고 그 외에 DNS, ICMP, TCP SYN, UDP 등 다양한 프로토콜별 항목에 대해 개별적으로 1, 2차 임계치를 설정한다. 얼마나 모니

터링하는 서버의 특성에 맞게 임계치를 최적화에서 설정하느냐에 따라 탐지의 정확성이 높아질 수도 있고 낮아질 수도 있다.

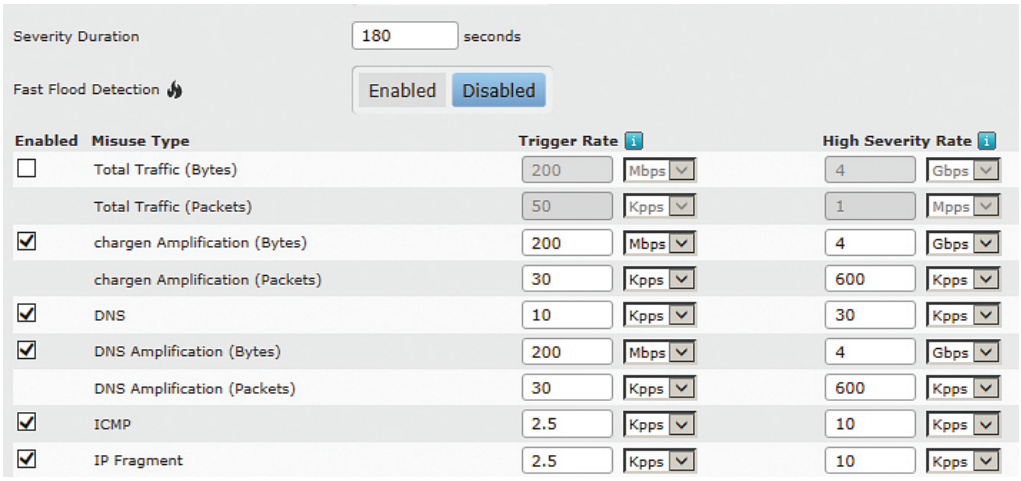

그림 2. 모니터링 대상에 대한 세부적인 임계치 설정 화면

DDoS 공격을 탐지하는 인라인 장비와 아웃라인 장비를 포함하여 대부분의 장비는 임계치를 이용하여 공격 여부를 판단한다. 특정 클라이언트가 공격대상 서버로 얼마나 많은 트래픽을 짧은 시간에 보내는지를 모니터링하다가 임계치를 넘을 경우 공격으로 인식하는 것인 기본적인 탐지원리이다. 여기서 탐지의 정확도를 높이기 위해 트래픽 양뿐만 아니라 트래픽을 보내는 시간 값을 추가하여 탐지의 정확도를 높이는 전략을 사용한다. [그림 3]과 같이 가로축은 시간이고 세로축은 트래픽 양을 나타내는 그래프가 있다. 즉, 시간에 따라 트래픽 양이 어떻게 변화하는지를 표현한 그래프이다. 트래픽 양에 대한 임계치는 Trigger Rate, Middle Line, High Severity Rate라는 값이 있고, 시간 값에 대한 임계치는 Host Detection Start/End Latency, Severity Duration 값들이 있다. 각각의 임계치에 대해 설명을 하면 아래와 같다.·

- **Trigger Rate :** 경보가 발생하기 위해 반드시 넘어야 하는 트래픽 양(이하 1차 임계값)
- **High Severity Rate :** 경보가 High 레벨로 올라가기 위해 넘어야 하는 트래픽 양(이하 2차 임계값)
- **Middle Line :** Trigger Rate와 High severity Rate 사이의 75%의 트래픽 양(이하 중간값)
- **Start Latency :** Trigger rate 값 이상에서 얼마 동안 있어야 공격으로 탐지할지 결정하는 시간 값(이하 시작판단시간)
- **End Latency :** Trigger rate 값 이하에서 얼마 동안 있어야 공격경보를 종료할지 결정하는 시간 값(이하 종료판단시간)
- **Severity Duration :** High 레벨 경보로 등급이 올라가기 위해 High Severity Rate 값 이상에서 머물러야 하는 시간 값(이하 등급판단시간)

[그림 3]에서 트래픽 양이 증가하다가 1차 임계값을 통과하면 바로 경보가 시작되지 않고 시작판단시간이 경과된 시점에서 Low 레벨 경보가 시작된다. 이후에 트래픽 양은 중간값을 넘지 못하고 아래에서 유지되다가 1차 임계값 이하로 떨어진다. 이때 바로 경보가 종료되는 것이 아니고, 종료판단시간 동안 트래픽 양이 1차 임계값을 다시 통과하지 못하면 해당 공격경보를 종료하게 된다. 여기서 시작판단시간이 필요한 이유는, 트래픽이 급하게 올라갔다가 짧은 시간 내에 떨어지는 것은 공격보다는 정상적인 사용자들의 트래픽 사용 증가일 확률이 높아, 어느 정도의 시간 동안 트

래픽이 유지되어야 공격일 확률이 높기 때문이다. 마찬가지로 종료판단시간은 트래픽 양을 잠시 중지시켰다가 재개하는 공격을 개별적인 공격이 아니고 하나의 연속된 공격으로 관리하기 위해 필요한 값이라고 할 수 있다.

다음으로 Medium 레벨 공격이 탐지되는 원리를 알아보자. [그림 4]와 같이 트래픽이 1차 임계값을 통과해서 시작판단시간이 지나면서 Low 레벨 경보가 생성된다. 이후에 트래픽 양이 중간값을 넘어서 2차 임계값을 넘으면 바로 Medium 레벨 경보로 상향된다. 그러나 2차 임계값을 등급판단 시간 동안 유지하지 못하고 다시 떨어지면 High 레벨로 상향되지 못하고, 계속 중간값 이상에서만 트래픽 양이 머물러 있으면 Medium 등급만 유지되게 된다.

마지막으로 High 레벨 공격이 탐지되는 원리를 알아보자. [그림 5]와 같이 트래픽이 1차 임계치를 통과하여 시작판단 시간 동안 트래픽을 유지하면 Low 레벨 경보가 발령되고, 트래픽 양이 2차 임계치를 넘어서면 Medium값으로 경보 등급이 상향된다. 이후에 2차 임계치 이상의 트래픽 양을 등급판단 시간 동안 유지한 시점에 경보 등급이 High로 상향 조정된다.

이런 원리를 이용하여 3개 등급의 경보가 적절히 발생할 수 있도록 1, 2차 임계값과 시간 값들을 적절히 조정해 줘야 한다. 모니터링하는 서버의 평소 트래픽에 비해서 1, 2차 임계값이 너무 낮으면 공격경보가 자주 발생할 것이고, 임계값이 너무 높으면 공격이 발생하더라도 공격경보가 발생하지 않을 것이다. [그림 6]을 보면 모니터링 대상

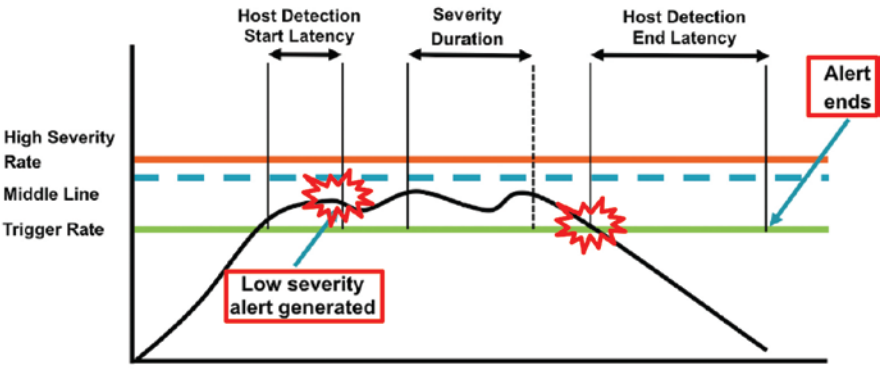

그림 3. Low 레벨 공격탐지를 위해 사용하는 트래픽 양과 시간 값

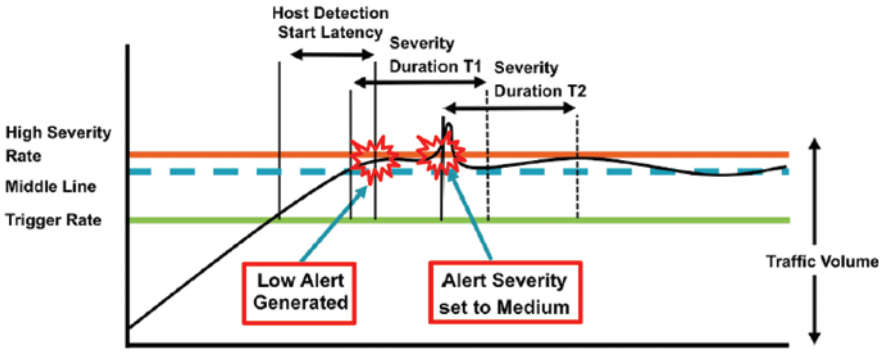

그림 4. Medium 레벨 공격탐지를 위해 사용하는 트래픽 양과 시간 값

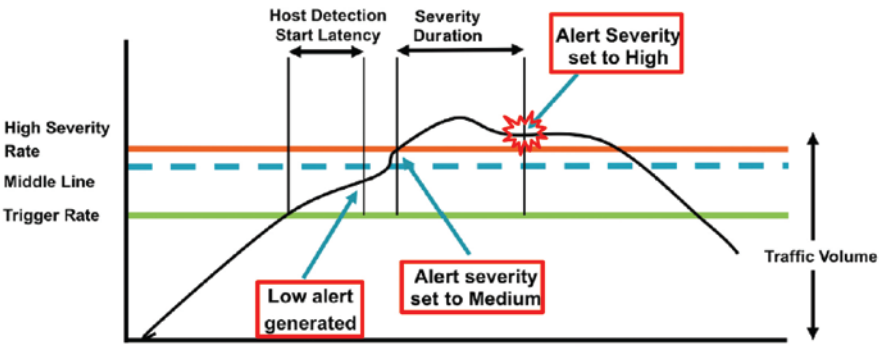

그림 5. High 레벨 공격탐지를 위해 사용하는 트래픽 양과 시간 값

장비별로 설정한 임계치 및 시간 값을 기준으로 공격으로 탐지된 경보를 표시하였다.

[그림 6]은 탐지된 공격경보리스트를 캡처한 것이다. 해당 경보들은 고유 ID, 트래픽 변화를 간편하게 확인하기 위한 미니 트래픽그래프, 공격 강도를 확인할 수 있는 경보 레벨, 탐지된 공격트래픽을 pps 단위와 bps 단위로 환산한 양, 공격대상 IP, 탐지된 DDoS 공격의 종류, 공격이 시작 및 종료된 시간, 지속시간 등을 확인할 수 있다. 이 리스트를 통해 공격 종류 및 강도, 공격대상별로 정렬해서 일목요연하게 공격에 대한 발생 현황을 확인할 수 있다.

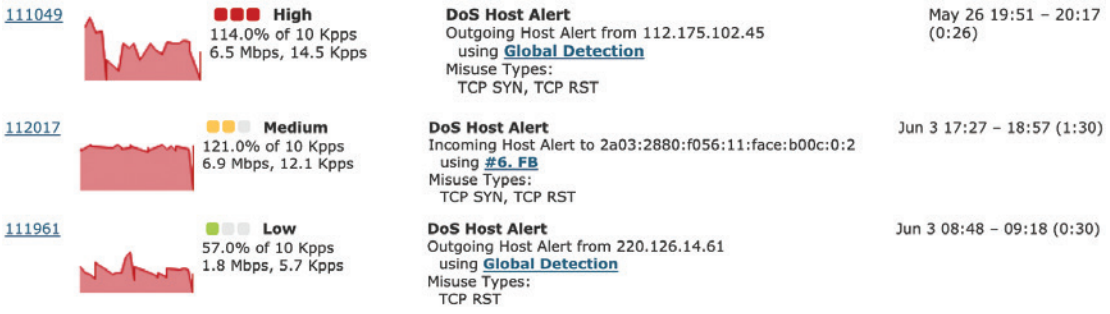

그림 6. DDoS 공격으로 탐지된 경보 리스트

좀 더 자세한 탐지 내역 확인을 위해 해당 리스트를 클릭하면 [그림 7]과 같이 세부적인 탐지 내역 확인이 가능해진다. 확대된 그래프를 통해 TCP SYN과 RST 트래픽 양이 시간에 따라 어떻게 변화하였는지 확인이 가능하다. 그래프 하단의 Top Traffic Pattern에서는 트래픽을 보낸 IP 주소와 공격대상이 되는 IP 주소를 확인할 수 있고, 각각의 출발지 IP가 얼마나 많은 트래픽을 공격대상으로 보냈는지 Top 10 방식으로 정렬되어 표시되어 있다. 이를 통해 보안담

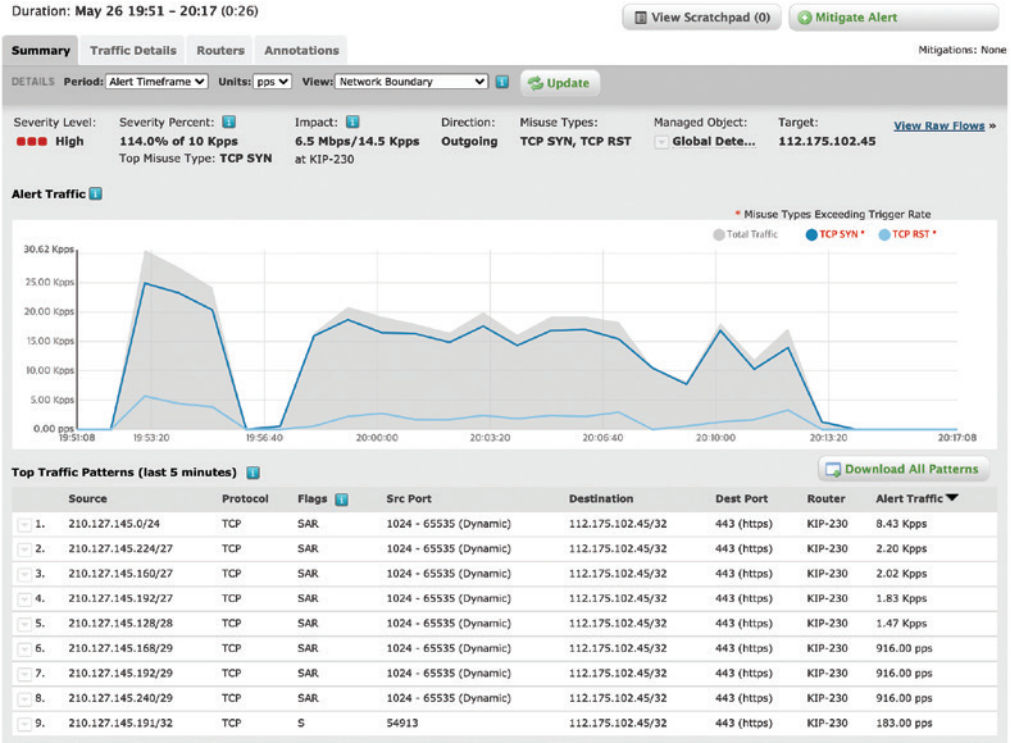

그림 7. DDoS 공격경보에 대한 상세 내역

당자는 같은 시간대에 해당 서버에서 실제 서비스 장애가 발생하였는지, CPU 등의 사용량이 높아졌는지 등을 확인하여 해당 트래픽이 서버에 영향을 미치는 레벨인지 판단이 가능하다. 이를 통해 해당 서버에 대한 임계치 조정을 통해 조금씩 공격탐지 정확도를 높여 갈 수 있다.

방어 장비를 최초로 도입한 이후에는 최초 모니터링 대상 및 임계치를 설정할 때 정확한 과거 데이터가 없어 일반적으로 장비의 기본값으로 모니터링을 시작한다. 이후에 발생하는 공격경보를 검토하여 해당 알람이 실제 서버에 영향을 미쳤는지 확인하고, 서비스에 영향이 없었다면 임계치를 좀 더 높이 설정하여야 한다. 반대로 특정 서버의 서비스에 영향이 발생하였는데 방어 장비에서 별다른 공격경보가 나타나지 않았다면 임계치를 지금보다 더 낮춰야 한다. 모든 보안 장비가 마찬가지겠지만 장비를 도입하여 설치만 하였다고 모든 공격이 정확하게 자동으로 차단되지는 않는다. 담당자 혹은 공급업체를 통해서 지속적인 모니터링과 임계치 조정, 장비 추가도입 혹은 구성변경에 따른 장비의 설정값 변경 등 인력과 운영 시스템의 지원이 지속해서 이루어져야 장비 도입에 대한 효과를 기대할 수 있다.

이런 DDoS 공격을 하기 위한 다양한 공격 툴이 최근 사용하기 쉽고 성능 높은 파이썬(Python), 고(Go) 등의 프로그래밍 언어가 많이 보급되면서, 옛날보다 더 적은 시간으로 더 효율적이고 다기능의 해킹 도구를 개발할 수 있는 환경이 되었다. 더욱이 다양한 오픈소스들이 공유되고 개발되면서 깃허브(GItHub) 같은 오픈소스 공유사이트를 통해 손쉽게 다양한 공격도구를 다운로드받아 테스트 할 수 있다. [그림 8]과 같이 ddos로 검색한 결과를 보면 다양한 DDoS 테스트 도구, 공격 도구 혹은 방어 도구 등 다양한 오픈소스를 확인할 수 있다.

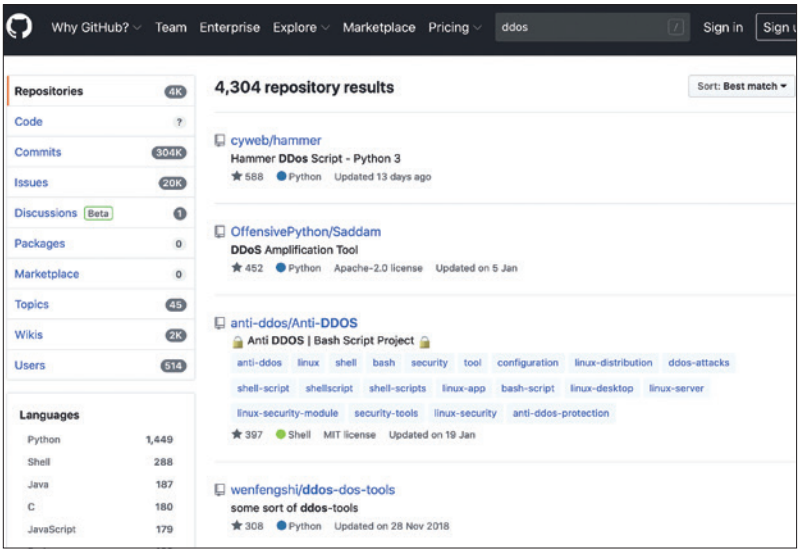

그림 8. 깃허브(GItHub)에서 ddos를 검색한 결과 화면

여기서 두 번째 OffensivePython/Saddam을 클릭해 보았다. [그림 9]와 같이 라이센스 정보, 설명서, 실행 파일 소스 코드 등을 확인할 수 있다. 이 프로그램은 사담이라는 이름의 DDoS 공격 도구이며, 공격을 수행하는 방식은 서비스 반사증폭공격에 특화된 도구로 설명되어 있다. 주로 사용하는 프로토콜은 DNS, NTP, SNMP, SSDP 등을 이용하며, 기능이 간단한 초보적인 실행 파일로 판단된다.

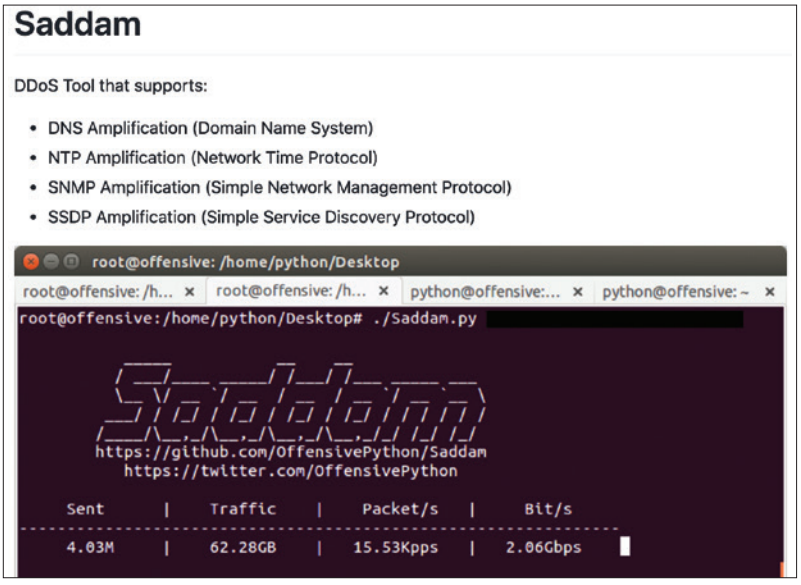

그림 9. DDoS 반사증폭 공격 도구 - 1

그 외에도 [그림 10]과 같이 Memcrashed라는 프로토콜을 이용한 반사증폭공격을 할 수 있는 공격 도구도 확인할 수 있다. 이 프로토콜은 사용하는 서버가 많지는 않지만 증폭 비가 51,200:1이라는 어마어마하게 효율적인 공격이 가능하다. 즉 이론적으로는 이 공격 도구를 통해 1Mbyte의 트래픽을 전달하면 해당 서버는 공격대상으로 51.2Gbps의 트래픽을 전송하는 효과가 있다고 할 수 있다. 이 실행 파일은 위의 '사담'이라는 초보적인 도구에서 진화하여 반사증폭공격에 사용할 서버를 스스로 찾아서 공격을 자동화할 수 있는 기능이 추가되었다.

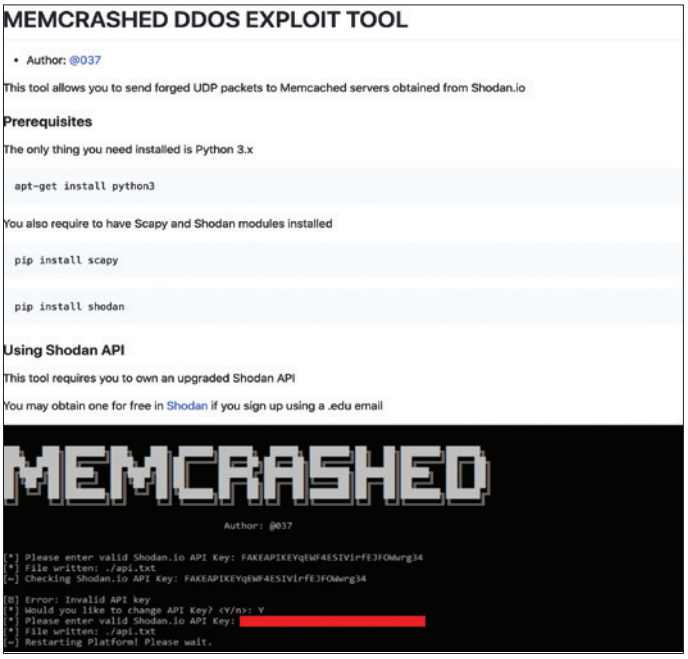

그림 10. DDoS 반사증폭 공격 도구 - 2

깃허브 같은 오픈소스 공유사이트에서 이런 공격 도구만 있는 것이 아니라 실제로는 공격 방어 도구가 더 많이 공유되어 있다. [그림 11]과 같이 최근 가볍고 고성능을 제공하는 대표적인 웹데몬인 엔진엑스(NGINX)에 확장방식으로 추가되어 DDoS 등 다양한 공격 시도에 대응할 수 있는 방어 도구 등을 제공하고 있다. 이런 프로그램은 상용으로 판매되는 프로그램에 비해서는 별도의 기술지원이 없거나 기능이 한정적이기는 하지만, 무료로 사용할 수 있는 장점이 있어 특정한 기능만 필요한 보안담당자의 경우 부분적으로 사용을 고려해 볼 수 있다.

그림 11. 다양한 공격으로부터 웹서버데몬(NGiNX)을 보호하는 방어 도구

다음 호에서는 DDoS의 마지막 편으로 공격으로 판단되는 트래픽을 어떻게 최대한 정확하게 선별해서 효율적으로 차단할 수 있는지 설명하도록 하겠다.