멤캐시드 반사 공격:
새로운 DDoS 공격 시대를 열다

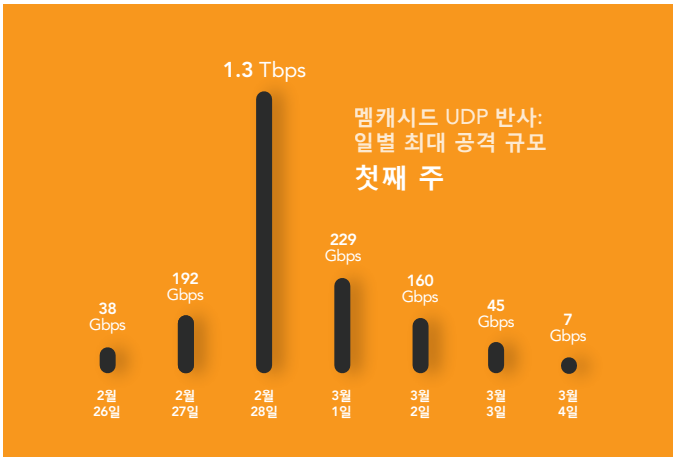
2018년 초 새로운 반사 및 증폭 기법이 발견되면서 DDoS 공격 규모가 2배로 증가했습니다. 멤캐시드(Memcached) UDP 반사라는 이름의 이 공격 기법은 멀웨어나 봇넷 없이 인터넷의 리소스를 자유롭게 공격에 이용해 공격 규모를 50만 배까지 증폭할 수 있습니다.

2018년 2월 28일 Akamai 고객사는 사상 최대 규모인 1.3Tbps의 DDoS 공격을 받았습니다. 멤캐시드 반사 기법을 이용한 공격이었고 기존에 미라이 IoT 봇넷에서 발생한 공격 규모보다 2배 이상 큰 규모입니다.

Akamai는 DDoS 방어 솔루션인 Prolexic을 통해 즉각적으로 공격을 방어했습니다. 멤캐시드(오픈 소스 데이터 캐싱 툴)가 디폴트로 사용하는 포트에서 발생하는 모든 트래픽을 Akamai의 DDoS 스크러빙 센터(유럽, 미국, 아시아 등에 위치)로 라우팅했고 클린 트래픽만 다시 고객의 네트워크로 전송했습니다. 고객의 비즈니스 운영에 추가적인 차질은 발생하지 않았습니다.

멤캐시드는 일반적으로 디스크와 데이터베이스 사이의 쿼리 응답 시간을 단축하기 위한 목적으로 사용됩니다. 하지만 공격자들은 멤캐시드를 DDoS 반사 공격에 악용했습니다. 멤캐시드 DDoS 반사 공격이 처음 발생한 후 불과 2일 후에 1.3Tbps 규모의 공격이 발생했습니다. 1.3Tbps의 공격이 발생했을 때 Akamai는 이미 자동 방어 시스템을 구축해 놓았기 때문에 멤캐시드 공격을 즉각적으로 방어할 수 있었습니다.

이 새로운 공격 기법이 등장한 첫 주에 여러 산업 분야의 Akamai 고객사를 타겟으로 19건의 멤캐시드 DDoS 반사 공격이 발생했습니다.



50만 증폭 계수의 위력과 패킷 전송률

멤캐시드의 증폭 계수는 50만이 넘기 때문에 210바이트의 요청이 100메가바이트(MB)의 응답을 발생시킬 수 있습니다. 멤캐시드 데이터는 그 구조상 전송 속도가 매우 높은데, 공격이 진행되던 중에 Akamai가 측정한 속도는 초당 1억 2,700만 패킷(127Mpps)이었습니다.

보안이 취약한 서버에서 UDP 커뮤니케이션 프로토콜이 디폴트로 사용되는데 멤캐시드는 스푸핑된 IP 주소를 포함해 요청하는 모든 사람에게 데이터를 전송합니다. 1천 개 이상의 ANS을 사용하는 수만 대의 서버가 1.3Tbps 공격에 사용됐고 각각의 서버는 평균 1Gbps의 공격 트래픽을 전송했습니다. 연구자들은 현재 인터넷상에 9만 대 이상의 멤캐시드 서버가 있는 것으로 추정하며 이 중 5만 대 이상이 반사기로 악용될 위험에 처해 있습니다.

멤캐시드 DDoS 와 랜섬 공격의 증가

반사 기법을 이용한 DDoS 공격은 지속적으로 증가해 왔습니다. 따라서 원격 시스템 관리자가 취약한 서버를 패치, 재설정, 제거하는 방법으로는 즉각적인 효과를 거두기는 어려울 것으로 보입니다. 멤캐시드 DDoS 공격은 앞으로도 발생할 수 있습니다.

멤캐시드를 이용한 DDoS 반사 공격은 봇넷의 봇을 컨트롤할 필요도 없고 멀웨어도 필요하지 않습니다. 다시 말해 기술이 부족한 공격자도 얼마든지 공격을 일으킬 수 있습니다. 최근 보안이 취약한 멤캐시드 서버를 스캐닝하는 활동이 증가하고 있습니다. 다양한 규모의 공격을 일으키기 위해 멤캐시드 서버를 악용하는 공격자들이 앞으로 증가할 것으로 예상됩니다. 또한, 멤캐시드 페이로드를 이용해 협박 메시지를 보내는 경우도 있는데 Akamai는 랜섬(몸값)을 지불하지 않을 것을 권장합니다.

로컬 네트워크 대역폭을 고갈시키는 DDoS 공격

Akamai는 CDN(콘텐츠 전송 네트워크) 서비스와 클라우드 기반 DDoS 방어 솔루션을 통해 이런 대규모 공격에 충분히 대응할 수 있습니다. 하지만 대규모 DDoS 공격, 특히 이번 멤캐시드 반사 공격과 유사한 규모의 공격이 발생했을 때 비즈니스를 정상적으로 운영할 수 있을 정도의 충분한 네트워크 용량을 갖춘 기업 또는 ISP는 극히 소수에 불과합니다. 공격이 발생하면 가장 먼저 데이터 센터와 엣지 라우팅 디바이스로 연결되는 네트워크 회선이 고갈되기 때문에 DDoS 방어 서비스가 효과를 발휘하지 못합니다.

DDoS 방어 계획의 중요성

이번 기록적인 규모의 DDoS 공격을 받은 Akamai 고객은 공격에 대한 사전 준비가 잘 되어 있었습니다. 따라서 고객사 트래픽을 Akamai로 라우팅하기 전까지 약 10분 미만의 시스템 중단만 경험했습니다. 고객사는 사전에 DDoS 방어 솔루션인 Prolexic을 구현했고 DDoS 런북을 개발·실천했기 때문에 누구에게 연락을 하고 어떤 조치를 취해야 하는지 잘 숙지하고 있었습니다. 네트워크 트래픽을 모니터링하던 중 비정상 트래픽을 발견하자마자 5분 안에 모든 네트워크 트래픽을 Akamai로 신속하게 라우팅했습니다.

Why Akamai: DDoS 공격에 안정적으로 대응

Akamai는 CDN, Prolexic 네트워크, 분산된 Fast DNS 인프라를 바탕으로 DDoS 공격으로부터 고객을 보호합니다. 또한, Akamai 플랫폼의 안정성을 강화하기 위해 끊임없이 투자하고 있습니다.

Akamai는 공격 규모가 증가하고 있는 상황을 감안해 용량 계획을 세울 때 지금까지 확인된 최대 규모의 DDoS 공격 규모보다 몇 배 더 많은 충분한 용량을 확보하고 있습니다. 따라서 대규모 DDoS 공격은 물론, 이번 공격과 같이 사상 최대 공격보다 2배 더 큰 규모의 공격까지 성공적으로 방어할 수 있었습니다.

Akamai의 Adversarial Resilience팀은 새로운 위협과 보안 사고를 지속적으로 평가해 Akamai 시스템 내에 잠재적 취약점이 있는지 확인합니다. 또한, 엔지니어링팀과 협력을 통해 자동 방어 시스템을 구축하고 모든 분야의 안정성을 강화합니다.

DDoS 공격에 대응하는 CDN의 안정성

Akamai 플랫폼은 단순히 DDoS 공격뿐만 아니라 예기치 못한 상황에서도 가용성과 안정성을 유지할 수 있게 설계되었습니다. Akamai는 전세계적으로 22만대의 서버를 배치했고 이 개별 서버의 상태, 장애, 혼잡상태 등을 고려해 자동적으로 트래픽을 라우팅합니다. 모든 서버는 전송률 제어(rate control), 블랙리스트, 지역별 차단(geo-blocking) 등의 다양한 DDoS 방어 기능을 제공합니다.

DDoS 공격에 대응하는 Prolexic 네트워크의 안정성

Prolexic 네트워크는 세계에서 가장 강력한 DDoS 스크러빙 서비스입니다. 7개의 글로벌 스크러빙 센터가 3.5Tbps가 넘는 용량을 제공하며 150명의 보안 전문가들이 매달 수천 건의 DDoS 공격을 방어합니다. 모든 스크러빙 센터는 다수의 Tier 1 통신사와 연결되어 있고 500개 이상의 피어링 파트너사와 피어링을 맺고 있으며 여러 단계의 OSI 스택에서 고성능 트래픽을 분석하고 적극적으로 공격을 방어합니다. Akamai는 지속적으로 DDoS 방어 용량을 확충하고 있습니다.

DDoS 공격에 대응하는 Fast DNS 인프라의 안정성

Akamai는 권한 DNS 서비스인 Fast DNS를 통해 가용성·속도를 유지하고 DDoS 공격에 대한 안정성을 확보합니다. 특정 Akamai 고객사를 향한 DDoS 공격이 다른 고객사들에 끼치는 영향을 최소화하기 위해 고객사에 할당된 네임 서버를 20개의 세그먼트화된 DNS 클라우드로 분산시킵니다. 네임 서버 클러스터와 여러 추가적인 기능을 통해 특정 지역에서 발생한 DDoS 공격이 다른 지역에 끼치는 영향력이 최소화됩니다.

결론

Akamai는 지난 20년 동안 DDoS 공격을 방어해 왔고 가장 큰 공격이 발생했을 때에도 인프라 가용성을 유지하는 등 우수한 방어 역량을 고객들에게 제공해 왔습니다. Akamai는 악성 공격자들보다 한발 앞서 나가기 위해 새로운 위협에 대해 끊임없이 조사 및 보고하고 있으며 프로세스와 역량을 강화해 나가고 있습니다. 고객사를 방어하면서 축적된 역량을 Akamai 솔루션의 방어 기능을 개선하는 데 활용됩니다. Akamai는 업계에서 가장 강력한 플랫폼을 고객들에게 제공하기 위해 최선을 다하고 있습니다.

기업의 DDoS 대응 능력 평가하기

귀사 인프라의 안정성을 검토하기 위해 Akamai의 도움이 필요한 경우 Akamai **Professional Services** 담당자에게 연락하시면 Security Architect와 상담할 수 있습니다.

https://www.akamai.com/memcached에서 자세히 알아보세요.

Akamai