DDoS 공격의 빠른 변화와 증가하는 위협

공격이 점점 더 정교해지고 자주 일어나고 있습니다. 모든 비즈니스는 경계를 늦추지 말아야 합니다.

모든 기업이 DDoS(분산 서비스 거부) 공격의 피해자가 될 수 있습니다. 협박, 핵티비즘, 복수에 관심을 기울이고 있는 사이버 범죄자들은 어느 기업이든 표적으로 삼아 대규모의 정교한 공격을 감행할 수 있습니다. 따라서 모든 디지털 중심 비즈니스는 DDoS 공격을 방어하기 위한 종합적인 솔루션이 필요합니다.

인터넷의 가장 초기 공격 유형 중 하나인 DDoS 공격

199년 7월 22일, 114대의 감염된 컴퓨터가 불필요한 데이터 패킷을 사용해 미네소타대학교의 컴퓨터 1대를 마비시켰습니다. 해당 컴퓨터는 오프라인 상태로 이틀을 보내야 했습니다.

MIT Technology Review에 따르면 이것이 최초로 기록된 DDoS 공격이었습니다.

핵티비스트 및 기타 사이버 범죄자들은 이런 공격을 얼마나 쉽게 시작할 수 있는지 알게 되었습니다. 그 후 몇 주, 몇 달 동안 CNN에서 Amazon에 이르는 주요 기업들이 다운되었습니다. 코드 몇 줄이면 충분했습니다.

DDoS는 온라인 사이트를 보유한 모든 비즈니스에 위협이 되었습니다.

증가하는 공격 규모와 정교함

DDoS 방어는 1999년 이후 계속 발전했지만, 범죄자들도 마찬가지로 진화했습니다. 오늘날의 DDoS 공격자들은 수십 가지의 공격 기법과 값싼 공격용 툴킷을 활용합니다. 또한 인터넷에는 그들의 공격을 증폭할 취약한 디바이스가 수없이 많습니다. 2016년 공격자들은 감염된 보안 카메라 DVR을 사용해 인터넷의 많은 부분을 다운시켰습니다.

그 후 인터넷에는 보호되지 않는 수억 개의 IoT 디바이스가 추가되었습니다. 미래의 5G 혁명으로 인해 그 수는 더 많이 늘어날 것입니다. 기하급수적으로 향상된 5G의 속도, 용량, 지연 시간을 발판삼아 공격이 얼마나 크고 막강해질 수 있을지 상상해보세요.

보호와 유지 관리에 소홀해 범죄자들이 증폭 및 반사 공격에 악용할 수 있는 인터넷상의 서버 개수가 급증하고 있습니다. 이러한 서버 중 다수(공격자들은 이 서버의 IP를 알고 있습니다)는 스푸핑된 요청을 5만 배 이상 증가시킬 수 있습니다.

연중무휴 긴급 DDoS 방어 및 차단

기존 Akamai 고객이 DDoS 공격의 협박을 받고 있는 경우 Akamai SOCC(Security Operations Command Center)에 문의하세요.

Akamai 고객이 아니지만 긴급 방어 서비스가 필요한 경우 **Akamai의 DDoS 핫라인 페이지에서 양식을 작성하거나 +1-877-425-2624**로 전화해 즉시 도움을 받으세요.

모든 업계를 노리고 있는 DDoS 공격

오늘날 Akamai는 매년 수천 건의 DDoS 공격을 방어하고 있습니다.

어떤 공격 케이스에서는 그 동기를 명확히 볼 수 있습니다. 게이머는 네트워크 속도를 저하시키고 라이벌 게이머들과의 경쟁에서 이기기 위해 DDoS 공격을 사용할 수 있습니다. 대학생들은 한 ISP의 고객들에게 실망스러운 경험을 유발하고 경쟁사의 비즈니스를 지원하기 위해 표적 DDoS 공격을 사용했습니다.

하지만 때로는 공격의 동기가 더 복잡하거나 모호합니다. 어떤 범죄자들은 DDoS 공격을 사용해 기업 인시던트 대응팀의 시선을 돌리고, 해당 기업의 다른 부서에 눈에 띄지 않는 공격을 시도했습니다.

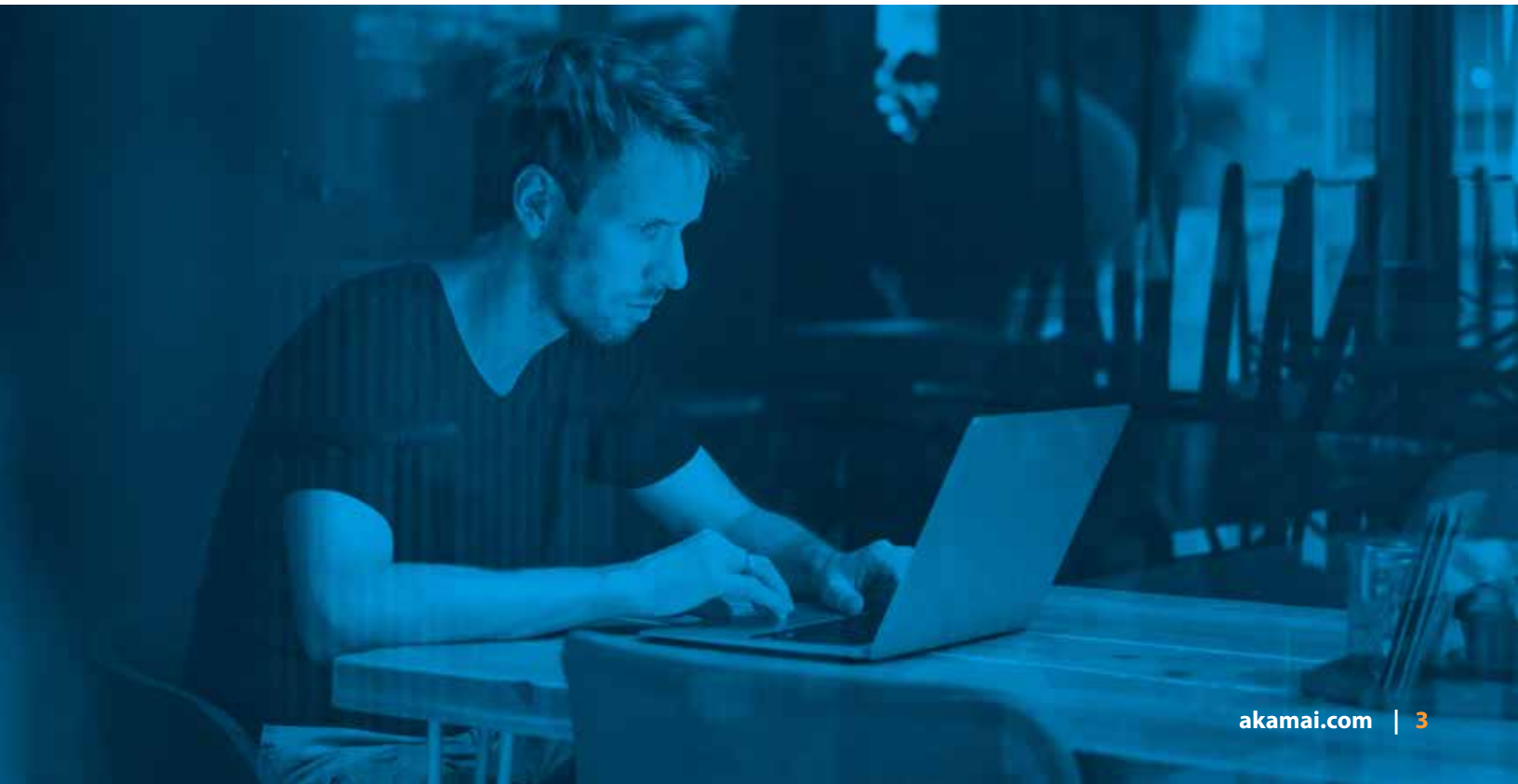
다크넷에는 기술을 갖추지 못한 공격자를 위한 'DDoS 외주' 비즈니스가 존재합니다. 가격은 5달러/5분부터 시작해 400달러/24시간까지 높아집니다. 공격을 작정한 사람은 단돈 200~300달러를 지불하고 기업에 수백만 달러의 비용을 초래할 수 있습니다.

2020년, 더욱 정교한 대규모 공격 발생

Akamai는 2020년 상반기 초당 1.44테라비트(Tbps) 및 초당 8억9백만 패킷(Mpps) 규모의 공격을 방어했습니다. 이는 사상 최대 규모의 Mpps 공격입니다.

Akamai는 이 공격을 1초 안에 방어했습니다. 이 공격은 100Gbps 이상의 대규모 공격 발생 트렌드를 보여주고 있습니다. 많은 공격자들이 여러 기법을 고유한 방법으로 복잡하게 조합해 사용합니다. 이들은 방어 시스템을 압도하거나 우회하려고 하며, 기업의 인시던트 대응 리소스를 고갈시키려고 합니다.

자동화된 대응뿐만 아니라 사람의 직접적인 개입이 필요한 공격도 증가하고 있습니다.



사상 최대 규모의 DDoS 협박 공격

2020년 8월 Akamai 보안 인텔리전스 연구팀은 다양한 업계에 있는 기업들이 DDoS 협박 이메일을 보냈다고 경고하며 보안 알림을 보냈습니다. 공격자들은 비트코인으로 랜섬을 지불하지 않으면 기업 운영을 방해하고 막대한 다운타임 피해와 재정적 손실을 일으킬 것이라고 협박했습니다.

불과 몇 주 후 FBI는 전 세계 수천 곳의 기업이 유사한 협박 이메일을 받았다고 보고했습니다. 공격자들은 특정 업계에 있는 기업을 공격하고 위협한 다음, 다시 다른 업계를 표적으로 삼고 연이어 협박했습니다. 공격자들은 고도로 조직화되어 이전에 협박 대상으로 삼았던 기업/업계를 다시 협박하기도 했습니다.

공격을 막을 수 있는 강력한 보안

사이버 범죄자라고 해서 여타 범죄자들과 다르지 않습니다. 그들은 약점을 찾기 위해 범죄 대상을 잘 살펴봅니다. DDoS 공격의 경우 범죄자는 표적의 DNS, 웹 애플리케이션, 인터넷 연결 데이터센터 자산을 살펴보며 약점을 찾습니다.

사이버 범죄자는 이 '정찰'에서 취약한 리소스, 사이트, 서비스를 찾으면 이를 통해 침투하고, 표적의 보안 체계가 강력하면 다른 대상을 찾아 떠납니다.

Prolexic을 새롭게 비상 가동한 고객 중 이전에 공격을 받았던 적이 있는 고객의 대다수는 Prolexic 방어 솔루션을 배치한 후 다시 공격받지 않았습니다. 공격자 입장에서는 다른 표적을 얼마든지 찾을 수 있는데 굳이 Prolexic을 사용하는 고객을 공격하기 위해 시간을 들일 이유가 없습니다.

종합적인 DDoS 방어 솔루션의 효과

Akamai는 175Tbps가 넘는 총 네트워크 용량을 갖춘 전용 엣지, 분산형 DNS, 클라우드 스크러빙 방어 솔루션으로 구성된 투명한 메쉬를 통해 심층적인 DDoS 방어 체계를 제공합니다. 이러한 맞춤형 클라우드는 DDoS 보안 체계를 강화하는 동시에 공격면을 줄일 수 있도록 설계되었습니다. 이 엔드투엔드 DDoS 보안은 방어의 품질을 향상하고 오탐을 줄이며 가장 정교한 대규모 공격에 대한 안정성을 높입니다.

또한, 웹 애플리케이션이나 인터넷 기반 서비스의 개별 요구사항에 맞춰 솔루션을 세밀하게 조정할 수 있습니다.

엣지 보안

Akamai는 전 세계적으로 분산된 인텔리전트 엣지 플랫폼을 포트 80과 443을 통해 들어오는 트래픽만 허용하는 리버스 프록시로 설계했습니다. 모든 네트워크 레이어 DDoS 공격은 0초 SLA를 통해 엣지에서 즉시 차단됩니다.

API를 통해 시작된 이벤트를 비롯한 애플리케이션 레이어 이벤트의 경우 Kona Site Defender가 공격을 흡수하는 동시에 정상 사용자에게 접속 권한을 부여합니다.

DNS 방어

Akamai의 권한 DNS 서비스인 Edge DNS도 엣지에서 트래픽을 필터링합니다. Akamai가 특별히 설계한 Edge DNS는 다른 DNS 솔루션과 달리 DDoS 공격이 발생해도 가용성과 안정성을 유지하도록 특별히 설계되었습니다. Edge DNS는 네임서버, PoP(Point of Presence), 네트워크, 분리된 IP Anycast 클라우드 등 여러 단계에서 아키텍처 이중화를 지원하고 뛰어난 성능을 전송합니다.

클라우드 스크러빙 방어

Prolexic은 20개의 글로벌 스크러빙 센터와 8.2Tbps의 전용 DDoS 방어 체계를 통해 모든 포트와 프로토콜에 걸쳐 DDoS 공격으로부터 전체 데이터센터와 하이브리드 인프라를 보호합니다. 이 용량은 인터넷에 연결된 자산을 항상 사용할 수 있도록 설계되어 있으며, 이는 모든 정보 보안 프로그램의 토대입니다.

Prolexic은 완전한 매니지드 서비스이며 포지티브 및 네거티브 보안 모델을 구축할 수 있습니다. Akamai 글로벌 SOCC 네트워크의 전문적인 방어와 자동 방어 기능을 결합합니다. Prolexic은 **또한 선제적 방어 제어를 통해 업계 최고의** 0초 방어 SLA를 제공합니다.

Prolexic이 기록적인 공격을 차단한 방법

2020년 6월 809Mpps 규모의 공격은 인터넷 전반에서 관측된 공격 중 가장 큰 PPS(초당 패킷) 공격이었습니다. PPS 공격은 인바운드 인터넷 파이프라인을 압도하는 일반적인 초당 비트 공격과 달리 데이터센터나 클라우드에서 네트워크 장비를 고갈시키기 위한 것입니다.

이 막대한 규모의 공격에는 대량의 소스 IP 주소가 포함되어 있었습니다. 그 중 96% 이상이 과거 공격에서 관측되지 않았습니다. 이 공격은 2분 만에 418Gbps에서 809Mpps로 증가했습니다.

다행히도 표적이 된 기업은 0초 SLA를 기반으로 한 Prolexic 솔루션을 사용하는 고객이었습니다. Akamai SOCC는 이 고객과 협력해 평상시 트래픽 기준 프로필을 파악하고 DDoS 공격을 차단하기 위한 제어 및 보안 정책을 즉시 수립했습니다.

지금 바로 맞춤형 위협 브리핑을 신청하세요.

akamai.com/ddos-briefing 방문하기