2017년 2분기

인터넷 보안 현황 보고서

DDoS 공격 트렌드

100 Gbps

메가톤급 공격 감소

최근에 많이 발생했던 **100Gbps** 이상의 메가톤급 공격은 3년 만에 처음으로 이번 분기에 발생하지 않았습니다.

방심하기에는 이른 상황

공격자들은 PBot을 소규모 DDoS 봇넷으로 사용해 **75Gbps 규모의 DDoS 공격**을 일으켰는데 이는 이번 분기 최대 규모의 DDoS 공격이었습니다.

75 Gbps

개조된 Mirai와 PBot

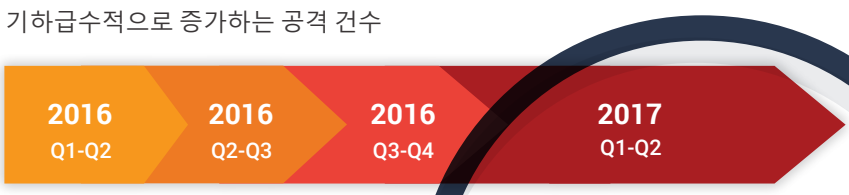
PBot은 **수만 개가 아닌 수백 개의** 감염된 노드를 사용해 표적을 공격했습니다. 이 봇넷은 이번 분기 금융기관을 겨냥해 발생한 최대 규모의 공격(**75Gbps**)에 사용됐습니다.

웹 애플리케이션 공격 트렌드

취약점 이해하기

SQLi 공격

기하급수적으로 증가하는 공격 건수

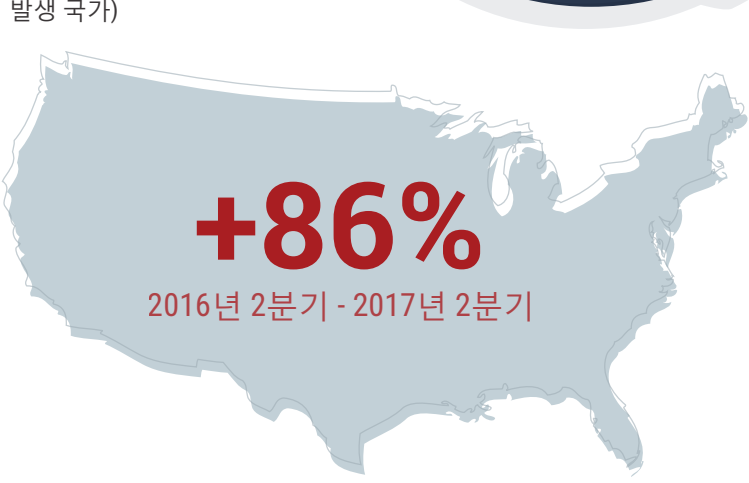


+44%

+21%

미국에서 발생하는 공격

(최다 공격 발생 국가)



+86%

2016년 2분기 - 2017년 2분기

지속적으로 발생하는 교묘한 공격

도메인 생성 알고리즘을 통한 탐지 회피

정상적인 네트워크는 **1%–5%** 의 NXDomain 응답을 보여주는 반면, **감염된 네트워크는** **15%–33%** 의 NXDomain 응답을 보입니다.

(이러한 응답 코드는 도메인이 존재하지 않음을 의미합니다)

시간당 접속하는 평균 고유 도메인 개수의 경우 **감염된 네트워크**는 **정상적인 네트워크**에 비해 룩업(lookup) 비율이 **15배** 높았습니다.

Akamai

Akamai는 가장 신뢰를 받는 세계 최대 규모의 클라우드 전송 플랫폼을 기반으로 고객이 사용하는 장소와 디바이스에 상관없이 안전하고 쾌적한 디지털 경험을 손쉽게 제공할 수 있도록 지원합니다. 전 세계 각지에 촘촘히 분산 배치된 Akamai 플랫폼은 130개 국가에 위치한 20만대의 서버로 구성되어 있으며 고객에게 탁월한 성능을 제공하고 위협을 방어합니다. 웹·모바일 성능 향상, 클라우드 보안, 기업 접속, 비디오 전송 솔루션으로 구성된 Akamai의 솔루션은 우수한 고객 서비스와 24시간 연중무휴 모니터링 서비스를 제공합니다. 대표적인 금융 기관, 이커머스 기업, 미디어·엔터테인먼트 사업자, 정부 기관이 Akamai를 신뢰하는 이유를 알아보려면 Akamai 홈페이지(www.akamai.com) 또는 블로그(blogs.akamai.com)를 방문하거나 Twitter에서 @Akamai를 팔로우하십시오. 전 세계 Akamai 연락처 정보는 www.akamai.com/locations에서 확인할 수 있습니다. Akamai 코리아는 서울시 강남구 강남대로 382 메리츠타워 21층에 위치해 있으며 대표전화는 02-2193-7200입니다. 2017년 8월 발행.