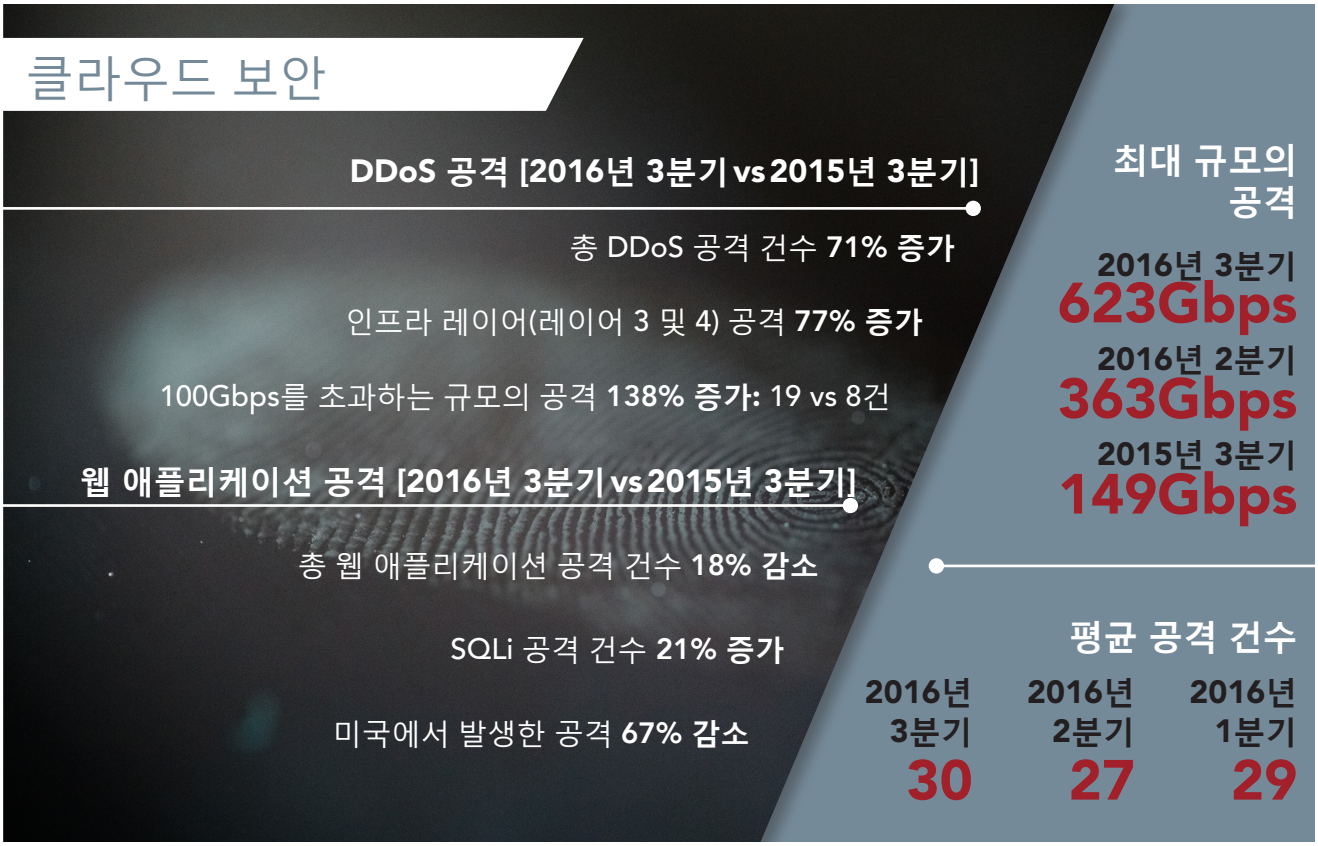
Akamai 인터넷 현황 보안 보고서

2016년 3분기 Executive Summary

Akamai 인터넷 현황 보안 보고서란? / 전세계 콘텐츠 전송 네트워크*(**CDN**)* 분야를 이끌고 있는 Akamai는 전세계적으로 분산된 Akamai Intelligent Platform™을 통해 매일 수조 건의 인터넷 트랜잭션을 처리합니다. Akamai는 이 과정에서 광대역 접속, 클라우드 보안, 미디어 전송 등의 지표에 관한 방대한 양의 데이터를 수집합니다. 정부와 기업이 인터넷 현황 보고서에 포함된 데이터를 적극 활용하면 보다 현명하고 전략적인 의사결정을 내리는 데 도움을 받을 수 있습니다. Akamai는 매 분기마다 수집된 데이터를 활용해 광대역 접속 속도 및 클라우드 보안에 대해 중점적으로 다루는 인터넷 현황 보고서를 발행합니다.



클라우드 보안 /2016년 3분기 인터넷 현황 보안 보고서는 DDoS(Distributed Denial-of-Services) 스크러빙 센터와 Akamai Intelligent Platform™에서 수집된 웹 애플리케이션 및 DDoS 공격 관련 데이터를 통합해 작성되었습니다.

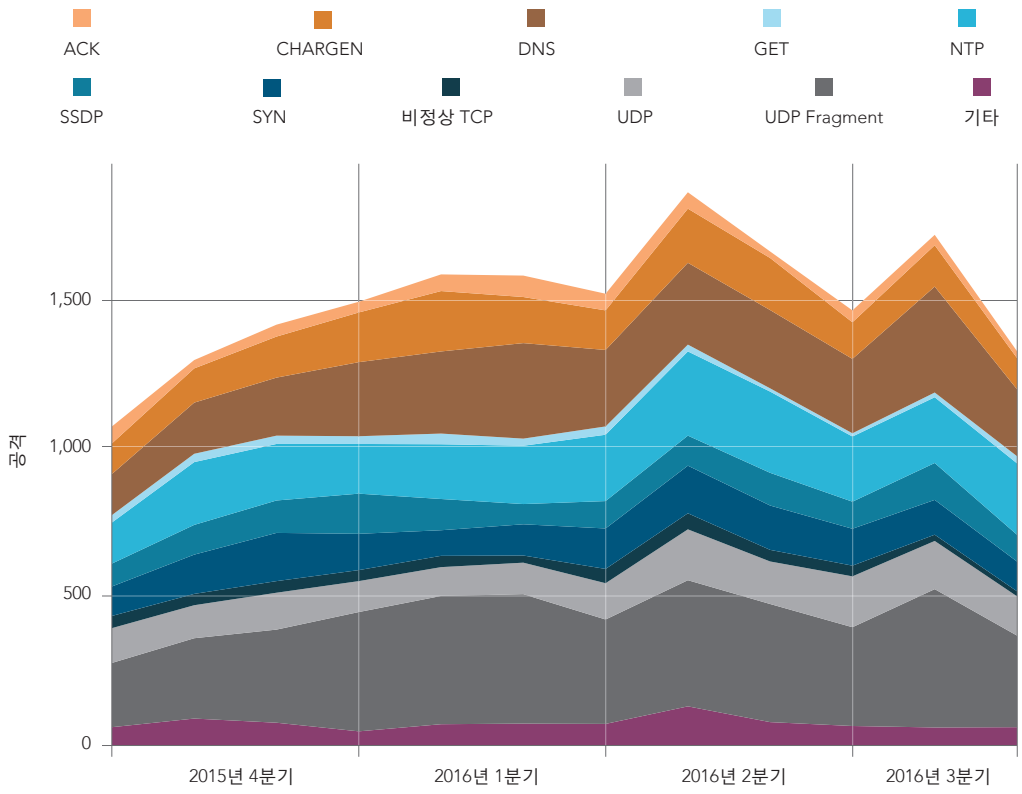
DDoS 업데이트 / 이번 분기에는 최대 공격의 규모가 2배 가까이 늘어났습니다. 623Gbps와 555Gbps 규모의 DDoS 공격이 발생하며 신기록을 수립했는데, 종전 최대 규모인 363Gbps 대비 대폭 증가한 규모입니다. 이 공격은 사이버보안 전문 블로거인 브라이언 크렙스(Brian Krebs, www.krebsonsecurity.com)를 겨냥했고 최근 브라이언이 포스팅을 게시한 이후 Mirai(미라이) 봇넷을 이용해 발생했습니다. 555Gbps 규모의 공격에는 ACK flood와 NTP 반사 기법이 사용되었던 반면, 623Gbps 규모의 공격은 멀웨어 기반의 봇넷을 통해 감염된 사물 인터넷(IoT) 디바이스를 이용하는 매우 이례적인 형태의 공격이었습니다.

미라이 봇넷은 디폴트로 설정된 사용자 이름(username)과 암호를 이용해 디바이스를 감염시키며 빠른 속도로 확산됐습니다. 감염된 디바이스는 공격 명령어를 받아들이는 동시에 취약한 디바이스를 지속적으로 스캐닝합니다. 공격에는 UDP, GRE, ACK, SYN, DNS, Valve Engine, HTTP Flood 등의 기법이 사용되었습니다.

2016년 1분기와 마찬가지로 3분기에도 100Gbps가 넘는 메가톤급 공격이 19회 발생했습니다. 전체 공격 건수는 8% 줄어들었지만, 대규모 공격의 건수와 규모는 오히려 늘어났습니다. 19건의 메가톤급 공격 중 13건이 미디어·엔터테인먼트 업계, 4건이 게임 업계, 그리고 2건이 소프트웨어·기술 업계를 겨냥했습니다.

DDoS 스크러빙 센터에서 확인된 총 DDoS 공격 건수는 4,556건으로, 전년 동기 대비 71% 증가했고 전 분기 대비 8% 감소했습니다. 전체 공격 건수가 줄어든 것은 다행이지만 이런 추세가 앞으로 계속될 가능성은 낮습니다. 연말 쇼핑 시즌에는 DDoS 공격 건수가 증가하는 추세가 오랫동안 이어져 왔고, 악성 공격자들은 IoT 디바이스를 이용한 봇넷 툴을 다시 악용할 가능성이 큽니다.

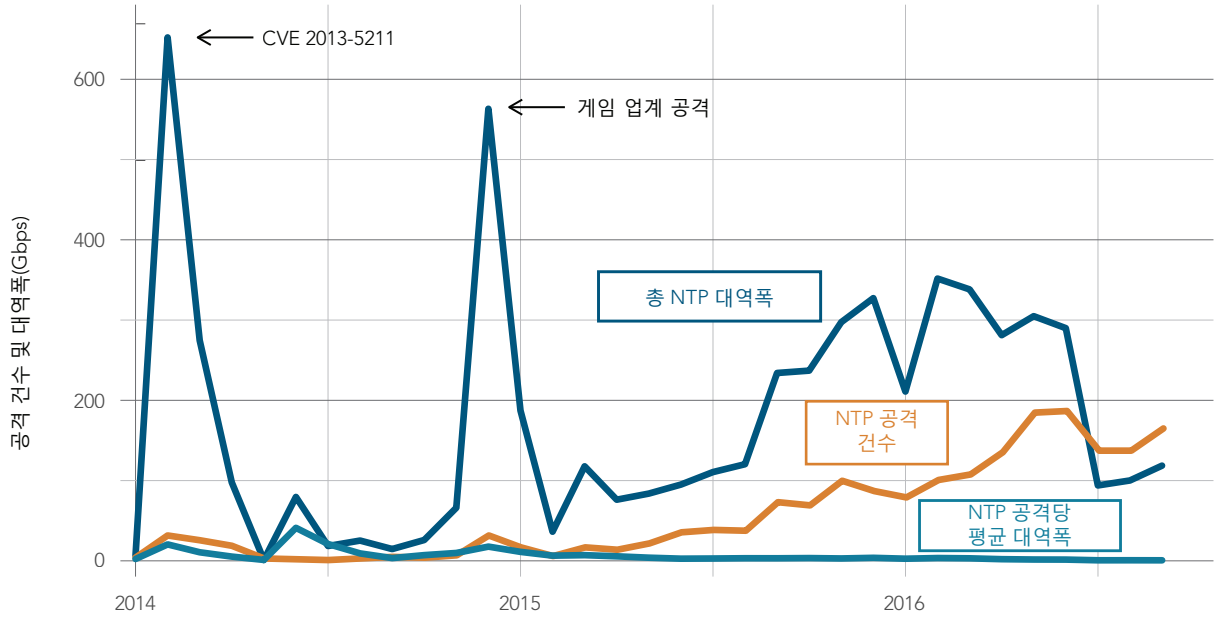
분기별 상위 10대 공격 기법



8월에 일시적으로 공격이 증가하기는 했으나 3분기의 전반적인 공격 건수는 2016년 2분기 대비 감소했습니다.

2016년 2분기에는 전년 동기 대비 NTP 공격 건수가 276% 증가했습니다. 3분기에도 NTP 공격 건수는 높았지만 공격에서 발생한 트래픽은 크게 줄었습니다. 왜냐하면 공격자들이 악용하는 패치가 되지 않은 NTP 서버 숫자가 지속적으로 감소하고 있기 때문입니다. 2014년 연말 NTP flood 평균 공격 규모가 40Gbps를 넘어선 반면 2016년 3분기에는 700Mbps에 미치지 못하면서 대역폭이 98% 감소했습니다.

2014~2016년 NTP 공격

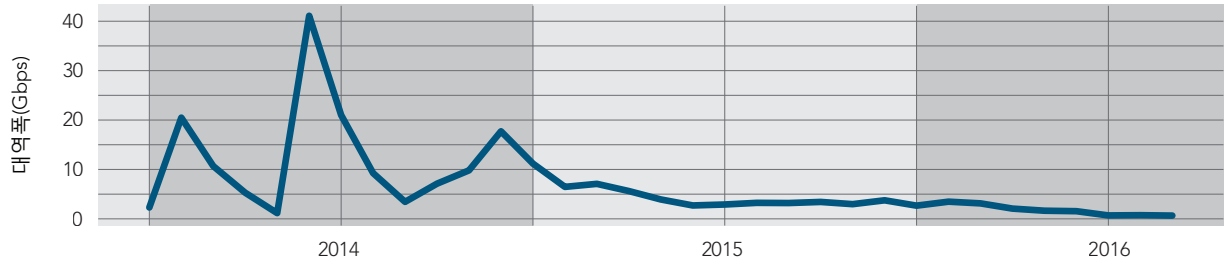


NTP 'Monlist' 취약점이 공개되면서 NTP 공격 트래픽이 폭증했고, 2014년 12월 게임사를 겨냥한 공격이 집중적으로 발생했습니다.

이번 미라이 공격에는 GRE(Generic Routing Encapsulation) flood가 대대적으로 사용됐지만, 아직 GRE가 전체 공격 기법 중에서 차지하는 비중은 매우 낮습니다. 하지만 최근 공격이 크게 보도되면서 앞으로 GRE flood가 점차 광범위하게 사용될 가능성이 큽니다. 공격 트래픽을 증폭시키는 반사 공격과 달리 GRE flood는 봇넷 노드의 공격 실행 능력에 의해 크게 좌지우지됩니다.

중국은 4분기 연속 DDoS 공격이 가장 많이 발생한 국가로 기록되었습니다. 이번 분기에 전체 DDoS 공격 트래픽의 30%가 중국에서 발생했는데, 한 가지 고무적인 점은 중국에서 발생하는 공격 트래픽 비율이 56% 감소하면서 전체 공격 건수가 8% 감소했다는 점입니다. 중국 다음으로 미국, 영국, 프랑스, 브라질이 그 뒤를 이었습니다.

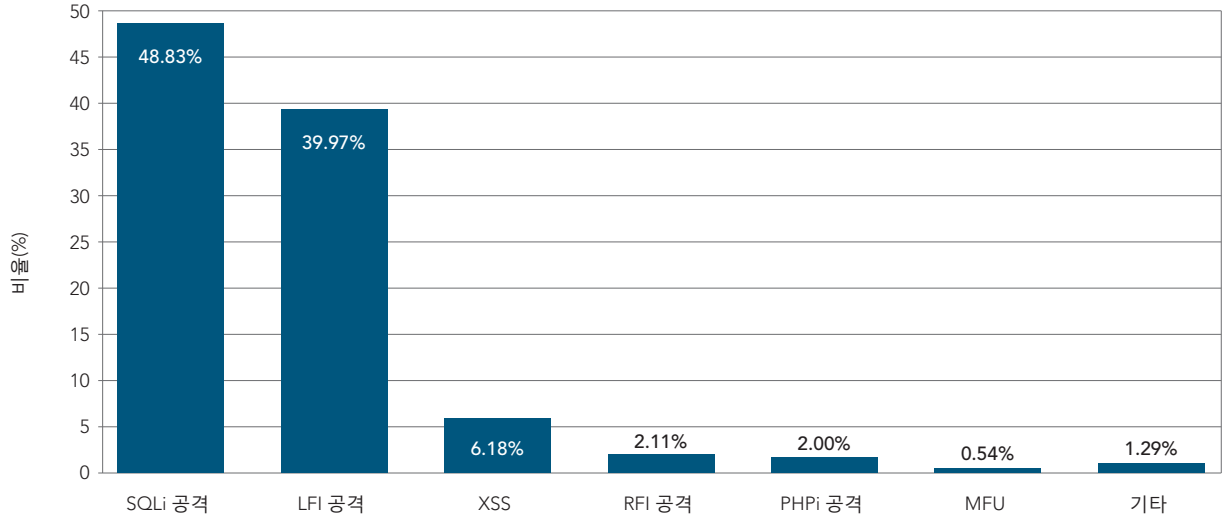
이번 분기에 기업당 평균 DDoS 공격 건수는 30% 증가했습니다. 즉, 처음 공격을 당한 이후 추가 공격을 당할 가능성이 매우 높고 지속적으로 공격을 받는 경우도 있었습니다. 가장 빈번하게 공격을 받는 기업의 경우 하루 평균 3~5회 공격을 받았고, 공격으로 인해 하루에 여러 차례 서비스가 중단될 경우 비즈니스에 치명적인 영향을 끼칠 수 있습니다.



2016년 6월 NTP 반사 대역폭이 대폭 감소하면서 봇넷 공격 실행자들은 다른 프로토콜로 옮겨가기 시작했습니다.

웹 애플리케이션 공격 통계/미국에서 발생한 웹 애플리케이션 공격 건수가 13% 줄어들었음에도 불구하고 미국은 공격 트래픽 발생 국가 순위에서 1위 자리를 되찾았습니다. 2분기에 1위를 차지했던 브라질은 이번 분기에는 네덜란드와 러시아에 이어 4위를 차지했습니다. 예상을 깨고 네덜란드(18% 차지)가 2위를 차지했는데 공격자들은 프록시 서버를 이용해 웹 애플리케이션 공격 발생지를 의도적으로 숨기기도 합니다. 공격 발생 국가 순위는 마지막으로 관측된 최종 구간의 소스 IP 주소를 기반으로 작성되었습니다.

전체 공격의 66%가 미국을 겨냥해 발생했고 전체 공격의 20%가 미국에서 발생했습니다.



SQLi 공격이 웹 공격의 절반가량을 차지합니다.

이번 분기 웹 애플리케이션 공격의 95%는 SQL 인젝션(SQLi), 로컬 파일 인클루전(LFI), 크로스 사이트 스크립팅(XSS)이 차지했습니다. 반면 리모트 파일 인클루전(RFI), PHP 인젝션(PHPi), 악성 파일 업로드(MFU)가 차지하는 비중은 각각 2%대 전후에 불과했습니다.

Akamai는 대규모 스포츠 행사와 웹 애플리케이션 공격과의 관련성도 살펴봤습니다. 2016년 유로 챔피언십 결승전 당시 포르투갈과 프랑스에서 발생한 공격이 전월 대비 각각 68%, 95% 줄어든 것으로 나타났습니다. 브라질 하계 대회 기간에도 비슷한 추세를 볼 수 있었는데, 브라질에서 발생한 공격 건수는 대회가 개최되기 한 달 전 730만 건에서 대회 기간(17일) 동안 100만 건으로 크게 감소하는 등 주목할 만한 결과를 보였습니다. 하지만 Akamai는 스포츠 이벤트가 진행되는 기간에도 방화벽을 활성화 상태로 유지할 것을 권장합니다.

리소스/2016년 3분기 Akamai의 사이버 보안 리소스 확인하기:

1. Kaiten/STD 라우터 DDoS 멀웨어 보안 위협 주의보
2. SSHowDowN 보안 위협 주의보: IoT 디바이스를 악용한 메가톤급 공격

[인터넷 현황 보안 보고서]

인터넷 현황 보고서 / 보안팀
마틴 맥키, 수석 보안 전문가, 수석 편집자
호세 아르테아가, Akamai SIRT
아만다 파크레딘, 편집자
데이브 루이스, 보안 전문가
래리 캐시달러, Akamai SIRT
채드 시먼, Akamai SIRT
존 톰슨, 고객 애널리틱스
라이언 바넷, 위협 연구소
에즈라 캘텀, 위협 연구소

디자인
숀 도티, 크리에이티브 디렉션
브렌던 오하라, 아트 디렉션 및 디자인

연락처
SOTIsecurity@akamai.com
Twitter: @akamai_soti / @akamai
www.akamai.com/StateOfTheInternet

보고서 전문 다운로드

[인터넷 현황 보안 보고서]
2016년 3분기

Akamai FASTER FORWARD

전세계 콘텐츠 전송 네트워크(CDN) 서비스 분야를 이끌고 있는 Akamai는 빠르고 안전하며 신뢰할 수 있는 인터넷 환경을 제공합니다. Akamai는 웹 성능, 모바일 성능, 클라우드 보안, 미디어 전송과 관련된 우수한 솔루션을 공급하고 있으며 이 과정에서 사용 디바이스나 장소에 상관없이 소비자, 기업, 엔터테인먼트 경험을 최적화하는 방법을 크게 바꿔놓고 있습니다. Akamai의 인터넷 전문가들과 솔루션이 어떻게 기업의 성장을 뒷받침하고 있는지 자세히 알아보려면 Akamai 홈페이지(***www.akamai.co.kr***) 혹은 블로그(***blogs.akamai.com***)를 방문하거나 Twitter에서 ***@Akamai***를 팔로우하십시오.

Akamai는 미국 매사추세츠주 케임브리지에 본사를 두고 있으며 전세계 57여 개의 지사를 운영하고 있습니다. Akamai의 우수한 솔루션과 고객 서비스는 기업들이 전세계 고객들에게 우수한 인터넷 경험을 제공할 수 있도록 도와줍니다. Akamai 코리아는 서울시 강남구 강남대로 382 메리츠타워 21층에 위치해 있으며 대표전화는 02-2193-7200입니다.