[인터넷 보안 현황 보고서]

2017년 2분기 Executive Summary

Akamai

전세계 콘텐츠 전송 네트워크(CDN) 분야를 이끌고 있는 Akamai는 전세계에 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.

Editor's Overview / 인터넷 보안 현황 보고서는 끊임없이 변화하는 보안 환경에 대해 중점적으로 다룹니다. 2017년 2분기에는 대규모 공격에 사용된 IP 주소의 수가 크게 감소했고 대규모 공격이 발생하지 않는 등 상당히 큰 변화를 보였습니다. 웹 애플리케이션 공격 발생 빈도는 지속적으로 증가했고 그 중 특히 SQL 인젝션(SQLi) 공격이 가장 큰 비중을 차지했습니다.

2017년 2분기에 Akamai가 관측한 DDoS 발생 건수는 증가했습니다. 최근에 많이 발생했던 100Gbps 이상의 메가톤급 공격은 3년 만에 처음으로 이번 분기에 발생하지 않았습니다. 전 세계적으로 많은 기업들이 WannaCry 및 Petya 멀웨어에 의해 큰 타격을 입었고 잠재적으로 40억 달러가 넘는 비용이 발생했습니다. 미라이(Mirai) 봇넷이 지속적으로 공격에 이용되고 있으며 Akamai 보안 인텔리전스 대응팀(SIRT)이 이번 분기 보고서에서 조사한 Pbot 봇넷처럼 기존의 멀웨어를 변경해 만들어진 새로운 공격 툴도 등장했습니다.

Akamai 연구원들은 도메인 생성 알고리즘(DGA)이라는 멀웨어 프로세스로 인해 생성된 트래픽을 조사했습니다. 봇넷은 DGA를 통해 수많은 도메인을 만들어내고 이를 C2(Command & Control) 채널로 사용함으로써 실제 채널로 사용되는 몇몇 도메인을 숨길수 있습니다. Akamai 연구원들은 봇의 연결 방식을 이해하기 위해 9개월여 동안의 미라이 C2 트래픽을 처음으로 살펴봤습니다. 이는 보다 깊이 있는 연구결과를 도출하기 위한 노력의 일환이었습니다.

인터넷 보안 현황 보고서 전문은 www.akamai.com/stateoftheinternet-security 에서 다운로드할 수 있습니다.

DDoS 업데이트 / 지난 세 분기 연속 감소세를 보였던 DDoS 공격 건수가 2017년 2분기에 28% 증가했습니다. 공격이 표적이 된 고객사당 평균 DDoS 발생 건수는 최대 32건으로 증가했는데 평균적으로 3일에 한 번씩 새로운 공격이 발생한 것입니다. 이번 분기에만 558건의 DDoS 공격을 받은 게임사도 있었습니다.

미라이 봇넷은 보안이 취약한 IoT 디바이스를 지속적으로 이용하고 있는 반면 이번 분기에 PBot이라는 기존의 멀웨어를 다시 활용한 공격 툴은 수만 개가 아닌 수백 개의 시스템을 감염시켜 표적을 공격했습니다. 이 봇넷은 이번 분기 금융기관을 겨냥해 발생한 최대 규모의 공격(75Gbps)에 사용됐습니다.

DoS 공격 규모는 어떤 공격 툴과 새로운 멀웨어 변종이 광범위하게 사용되고 있는지에 의해 크게 좌우됩니다. 2016년 최대 DDoS 공격 규모는 500-600Gbps를 넘어섰는데 이는 2014년과 2015년의 100Gbps에 비해 크게 증가한 규모입니다. 이번 분기 최대 공격 규모는 상대적으로 낮은 75Gbps를 기록했지만 이와 같은 추세는 오래 지속되지 않을 것으로 보입니다.

인프라 레이어에 대한 대용량 공격이 DDoS 공격의 99%를 차지했는데 대여 가능한 봇넷의 확산이 주요 원인입니다. 애플리케이션을 공격하는 증폭 공격은 매우 드물게 발생합니다. 이런 유형의 공격은 무차별 대입(brute force)보다는 웹 혹은 데이터베이스의 약점을 노렸을 때 더 큰 공격 효과를 거둘 가능성이 높아집니다.

대다수의 DDoS 트래픽은 반사 기법에 의해 생성됩니다. 스푸핑된 IP 주소를 사용해 일반적인 인터넷 프로토콜이 과도하게 쿼리되고 이에 대한 응답이 공격 대상으로 전달됩니다. 가장 일반적으로 사용되는 반사기는 DNS(Domain Name Service) 및 NTP(Network Time Protocol)로 트래픽이 최대 100배 이상으로 증폭되며 전 세계적으로 쉽게 사용 가능합니다.

DDoS 공격 [2017년 2분기 vs. 2017년 1분기]
- 총 DDoS 공격 건수 28% 증가
- 인프라 레이어(레이어 3 및 4) 공격 27% 증가
- 반사 기반 공격 건수 21% 증가
- 고객당 평균 공격 발생 건수 28% 증가

최대 규모의 DDoS 공격
- 2017년 2분기: 75Gbps
- 2017년 1분기: 120Gbps
- 2016년 4분기: 517Gbps
- 2016년 3분기: 623Gbps
- 2016년 2분기: 363Gbps

웹 애플리케이션 공격 / 웹 애플리케이션 공격 건수가 매 분기 지속적으로 증가하고 있습니다. 증폭 DDoS 공격이 사이트에 영향을 끼치는 시간은 몇 분, 몇 시간, 몇 주 지속되는 반면 웹 애플리케이션 공격은 사이트를 감염시킴으로써 비즈니스에 심각한 피해를 장기간에 걸쳐 끼칠 수 있습니다.

웹 애플리케이션 공격 [2017년 2분기 vs. 2017년 1분기]
- 총 웹 애플리케이션 공격 건수 5% 증가
- 미국에서 발생한 공격 4% 증가(최다 공격 발생 국가)
- SQLi 공격 건수 21% 증가

주요 웹 애플리케이션 공격 기법 (2017년 2분기)
- SQL 인젝션(SQLi): 51%
- 로컬 파일 인클루전(LFI): 33%
- 크로스 사이트 스크립팅(XSS): 9%

증폭 공격은 과도한 트래픽을 발생시켜 서비스를 마비시키는 반면, 웹 애플리케이션 공격은 서버의 취약점을 악용해 서비스와 시스템을 감염시킵니다. 가장 일반적인 웹 애플리케이션 공격은 SQL 인젝션(SQLi), 로컬 파일 인클루전(LFI), 크로스 사이트 스크립팅(XSS)으로 웹 서버의 취약점을 악용하거나 데이터 유출을 시도합니다.

Akamai에서는 행동 분석 기법을 사용해 악의적일 가능성이 있는 활동을 감지하고 웹 애플리케이션 공격을 차단합니다. 2분기에는 멀웨어에 감염된 네트워크에서 나타나는 비정상적인 행동을 파악하기 위해 Akamai CSI(Cloud Security Intelligence) 플랫폼에 기록된 DNS 관련 트래픽을 조사했습니다. 일부 일반적인 봇넷은 매일 새로운 도메인 네임을 생성하는 DGA(도메인 생성 알고리즘) 기법을 통해 C2(Command & Control) 인프라를 변경해 탐지를 피하기도 합니다. 관련 특성을 파악하고 머신 러닝 알고리즘을 실행함으로써 비정상적인 행동을 탐지하고 결과적으로 멀웨어 활동을 탐지 및 차단할 수 있습니다.

비즈니스에 미치는 영향 / 이번 분기 Akamai 고객사를 겨냥한 DDoS 및 웹 애플리케이션 공격 건수는 모두 증가했습니다. 지난 세 분기와 비교해 보면 DDoS 공격 건수는 다시 증가세로 돌아섰습니다. 앞으로 DDoS 공격 건수가 계속 증가할지 확실하게 예측할 수는 없습니다. 하지만 웹 애플리케이션과 DDoS 공격 모두 주기적으로 순환하는 특징이 있고 공격이 보다 강력해지는 경우도 있습니다. 이 같은 상황에 대응하려면 인터넷의 특성에 대한 구조적인 변화가 필요합니다. 따라서 연휴 계획을 미리 세우는 것처럼 향후 공격 트래픽 증가에 대비한 계획을 수립해야 합니다.

미라이(Mirai)나 PBot과 같이 현재 공격에 사용되는 툴을 이해하면 앞으로 등장할 공격도 예측할 수 있습니다. 도메인 생성 알고리즘(DGA)과 같이 멀웨어가 탐지를 피하기 위해 사용하는 방법을 연구하면 멀웨어를 컨트롤하는 트래픽의 실체 역시 파악할 수 있습니다. 악의적인 공격자가 몰래 무엇을 하고 있는지 많이 이해할수록 Akamai 고객들의 시스템을 보다 효과적으로 보호할 수 있습니다.

분석 및 연구에 대한 자세한 내용은 보고서 전문을 다운로드하십시오.

2017년 2분기 인터넷 보안 현황 보고서는 Akamai 글로벌 인프라 전체에서 취합한 공격 데이터를 기반으로 작성되었고 다수의 팀에서 진행한 연구 결과를 제공합니다.

[인터넷 보안 현황 보고서]

인터넷 현황 보고서 / 보안팀
호세 아르테가, Akamai SIRT 리드, 데이터 랭글러 — 공격 분석 결과
데이브 루이스, 글로벌 보안 전문가 — DDoS 활동, 웹 애플리케이션 공격 활동
채드 시먼, Akamai SIRT — 공격 분석 결과, 미라이 지휘 통제 클러스터
윌버 메히아, Akamai SIRT—공격 분석 결과
알렉상드르 라뿔림, Akamai SIRT — 공격 분석 결과
엘라드 슈스터, 보안 데이터 분석가, 위협 연구소
오르 카츠, 주요 리드 겸 보안 연구원 — 도메인 생성 알고리즘
존 톰슨, 고객 애널리틱스
쉬리지타 바타차르야, 인턴 — 미라이 지휘 통제 클러스터

편집부
마틴 맥키, 수석 보안 전문가, 수석 편집자
아만다 파크레딘, 수석 기술 작가 겸 편집자

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

연락처
sotisecurity@akamai.com
Twitter: *@akamai_soti* / *@akamai*
www.akamai.com/stateoftheinternet-security

보고서 전문 다운로드

[인터넷 보안 현황 보고서]
2017년 2분기 보고서 전문