2015년 1분기 아카마이 인터넷 현황 보안 보고서 Executive Summary

이 보안 보고서는 다음과 같이 6가지 항목으로 구성되어 있습니다.

- 전분기 대비 및 전년 동기 대비 디도스(DDoS, 분산 서비스 거부 공격) 공격 관련 통계, 2015년 1분기 동안 가장 많이 사용된 웹 애플리케이션 공격 기법
- Booter/stresser 사이트에서 제공하는 툴을 사용한 100Gbps 이상의 디도스 공격, 그 중 특히 SSDP 반사 공격에 대한 집중 분석
- IPv4 주소 공간이 고갈되고 IPv6로 전환되는 과정에서 발생하는 보안 문제에 관한 연구 사례
- 아카마이의 Kona Site Defender WAF(Web Application Firewall)에서 감지된 8백만 건 이상의 공격을 검토하고 SQL 인젝션 공격 방식을 분석
- 도메인 하이재킹 시도와 웹사이트 변조 공격 감지 (공격 방어 및 완화에 관한 세부 정보 포함)
- 2015년에 발견된 취약점 및 공격 기법 (SSLv3 취약점, Joomla 반사 공격, MS SQL 반사 공격, 데이터 유출, 방어 전략 등)

/ 디도스 공격 통계 / 디도스 공격 횟수는 2015년 1분기에도 급격한 증가 추세를 이어갔고 Prolexic 네트워크에서 관찰된 디도스 공격 횟수는 다시 한 번 신기록을 경신했습니다. 디도스 공격 횟수는 2014년 4분기 대비 35% 증가했고 2014년 1분기 대비 117% 증가했습니다.

2015년 1분기 평균 공격 대역폭 및 규모는 감소하면서 악의적 공격자가 규모는 작지만 장시간 지속되는 공격을 선호하는 추세가 이어졌습니다. 2014년 1분기 대비 공격 지속 시간은 43% 증가했습니다. 이런 추세를 벗어나는 대규모 공격(100Gbps 이상)이 8번 발생했고 이 중 최대 공격 규모는 170Gbps입니다. 디도스 공격은 대부분 게임 회사를 대상으로 발생했고 게임 회사는 지속적으로 디도스 공격의 주요 대상이 되고 있습니다.

요약 내용

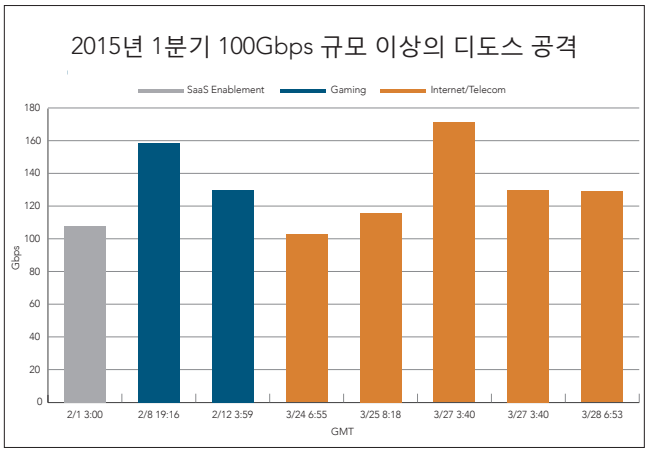
2014년 1분기와 비교

- 전체 디도스 공격 횟수 117% 증가
- 평균 최고 대역폭 39% 감소
- 초당 평균 최고 패킷 89% 감소
- 애플리케이션 레이어 디도스 공격 60% 증가
- 인프라 레이어 공격 125% 증가
- 평균 공격 지속 시간 43% 감소
- SSDP 공격: 전체 공격에서 차지하는 비중이 0%에서 21%로 증가

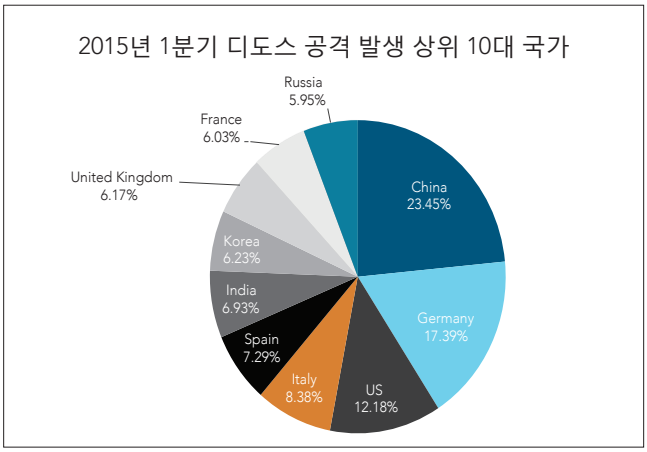
2014년 4분기와 비교

- 전체 디도스 공격 횟수 35% 증가
- 평균 최고 공격 대역폭 7% 감소
- 초당 평균 최고 패킷 4% 감소
- 애플리케이션 레이어 디도스 공격 22% 증가
- 인프라 레이어 공격 37% 증가
- 평균 공격 지속 시간 15% 감소
- SSDP 공격 42% 증가
- 최대 규모의 공격: 170Gbps vs 158Gbps

1년 전만 해도 거의 알려지지 않았던 SSDP 공격은 이번 분기에 인프라 기반 공격 중 가장 빈번하게 발생했습니다. 대부분의 SSDP 반사 공격은 보안이 취약한 가정용 기기를 이용하기 때문에 감지 및 방어 기술을 교묘히 피해갑니다. 2015년 1분기 가장 많이 사용된 상위 3대 디도스 공격 기법 중에서 SSDP 공격은 전체의 21%, SYN Flood 공격은 16%, UDP Flood 공격은 13%를 차지했습니다. 인프라 레이어 공격은 가장 일반적인 공격 유형으로 애플리케이션 레이어 공격보다 9배나 더 많이 발생했습니다. 하지만, 악의적 공격자가 인터넷상의 오픈 프록시를 이용하는 공격 스크립트를 선호하기 때문에 애플리케이션 레이어 디도스 공격은 여전히 위험성을 내포하고 있습니다. 1분기에 가장 빈번하게 발생한 애플리케이션 레이어 디도스 공격은 HTTP GET 공격으로 전체 디도스 공격의 7%를 차지했습니다.



2015년 1분기 아카마이 고객사를 대상으로 대규모 공격이 8번 발생했고 최대 공격 규모는 170Gbps에 육박했습니다.



2015년 1분기 방어한 디도스 공격 중 스푸핑으로 위장하지 않은 공격 IP 주소

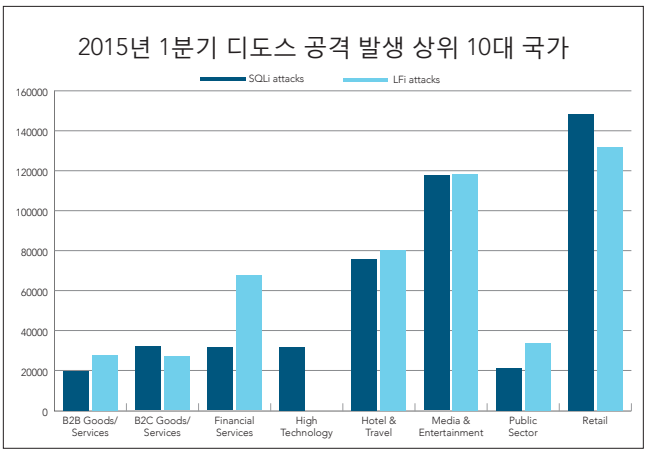
2015년 1분기 국가별 디도스 공격 발생률도 변화 양상을 보였습니다. 2014년 4분기 디도스 공격의 32%는 미국, 18%는 중국에서 발생한 반면 2015년 1분기에는 23%가 중국, 17%가 독일, 12%가 미국에서 발생했습니다. 전세계 디도스 공격 횟수가 급증했기 때문에 발생율의 감소가 공격 횟수의 감소를 의미하지는 않으며, 국가별 비중이 상대적으로 달라졌다는 것을 의미합니다. 1분기 동안 디도스 공격이 가장 많이 발생한 국가는 중국으로 중국의 공격 소스 IP는 미국 대비 66% 증가했습니다. 하지만, 아시아에서 리다이렉트된 트래픽이 증가하면서 공격 소스가 증가한 측면도 있습니다.

/ 웹 애플리케이션 공격 통계 / 아카마이는 2015년 1분기 엣지 네트워크에서 관찰된 1억 7,800만 건의 웹 애플리케이션 공격을 분석했고 가장 많이 이용된 7가지 웹 애플리케이션 공격 기법을 중점적으로 파악했습니다. 이 7가지 공격 기법은 SQL 인젝션(SQLi), 로컬 파일 인클루전(LFI), 원격 파일 인클루전(RFI), PHP 인젝션(PHPi), 커맨드 인젝션(CMDi), OGNL 자바 익스프레션 언어를 이용한 OGNL 인젝션, 악성 파일 업로드(MFI) 입니다.

가장 많이 관찰된 웹 애플리케이션 공격 기법 2가지는 전체의 66%를 차지한 LFI와 29%를 차지한 SQLi 이었습니다. LFI 공격 시도의 상당 부분은 독일 IP가 대형 유통업체 2곳을 대상으로 실시한 공격과 연관성이 큰데, 이 공격은 WordPress RevSlider 플러그인을 대상으로 한 대규모 공격의 일환이었습니다. 반면, SQLi 공격의 상당 부분은 호텔 및 여행 업체 2곳을 대상으로 한 공격과 관련성이 큰데, 대부분의 공격 IP가 아일랜드에서 발생했습니다.

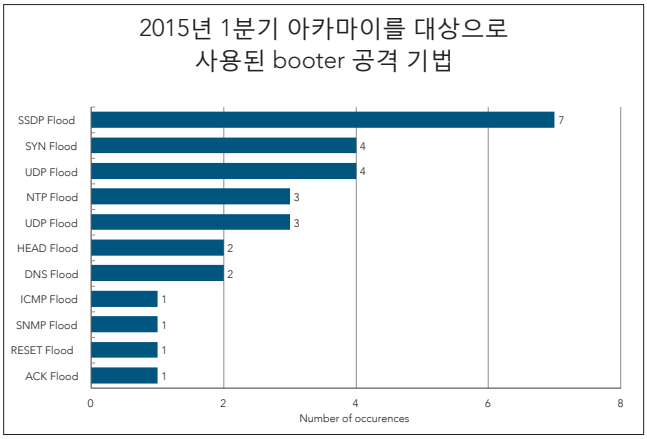
웹 애플리케이션 공격의 경우, 미국에서 가장 많은 공격 IP(전체의 52%)가 발생했고 그 뒤를 이어 중국, 브라질이 각각 11%, 6%를 차지했습니다. 2015년 1분기 웹 애플리케이션 공격의 82%가 미국에 위치한 웹사이트를 대상으로 집중적으로 이루어졌고 한 국가가 전체 공격의 2% 이상을 받은 경우는 미국 외에는 없었습니다.

웹 애플리케이션 공격의 주요 타겟은 유통, 미디어, 엔터테인먼트, 호텔 여행업계였습니다. 이런 결과는 과거 주요 공격 대상이던 금융기관들이 자사 사이트 보안을 대폭 강화하면서 다른 업계로 공격 타겟이 이동한 측면이 큽니다. 반면, 2014년 유통회사 및 미디어 기업을 대상으로 한 공격이 대대적으로 보도되면서, 해커들은 해당 업계를 만만한 공격 대상으로 인식하고 취약점을 파고들었습니다.



2015년 1분기 유통, 미디어, 엔터테인먼트 사이트가 웹 애플리케이션 공격의 주요 대상이었습니다.

/ 공격 집중 분석 / 2015년 1분기 아카마이 고객사를 대상으로 한 공격은 디도스 공격을 대행해주는 booter/stresser 사이트를 통해 이루어졌습니다. 이 중 최대 공격 규모는 100Gbps를 넘어섰습니다. 또한, 공격 기법을 살펴보면 해커들이 공격의 파괴력을 극대화하는 기법을 개발하고 있다는 점을 알 수 있는데 전문가들은 이런 추세가 앞으로도 계속될 것으로 예상하고 있습니다. 우려했던 것처럼, 디도스 공격 대행 서비스 시장에서 사용하기 쉬운 공격 기법을 제공하고 있기 때문에 비전문가들도 파괴력이 큰 공격을 감행할 수 있게 됐습니다. 본 보고서에서는 SYN Flood 공격, UDP Flood 공격, UDP Fragment Flood 공격, RESET Flood 공격, DNS Flood 공격, ACK Flood 공격, NTP Flood 공격, SSDP Flood 공격 등 모든 종류의 공격 기법을 분석합니다.



2015년 1분기 아카마이 고객사를 대상으로 한 공격 기법

/ IPv6 보안 관련 취약점 / IPv4 주소 공간이 고갈되고 새롭게 IPv6가 만들어지면서 10의 27제곱의 79배라는 상상하기 힘든 숫자만큼의 주소 공간이 생겨났습니다. 하지만, IPv4 주소 고갈 문제를 해결하는 과정에서 또 다른 문제점들이 생겨났습니다. IPv6 주소 공간 크기와 관련된 보안 문제가 발생했고 전환 기술에서 취약점이 발견된 것입니다. IPv4에서 쉽게 방어할 수 있었던 위협들이 IPv6에서는 방화벽이나 보안 기능을 우회하는 경우가 몇몇 사례에서 나타나고 있습니다. IPv6 네트워킹은 기본값으로 활성화되기 때문에 IPv4에 대한 보안 기능들이 있어도 서비스와 프로토콜이 노출될 수 있다는 사실을 대부분의 사용자와 관리자들이 모르고 있기 때문입니다. 이번 항목은 인터넷 주소 체제의 변화 과정과 IPv6의 장점에 대해 설명합니다.

/ SQL 인젝션 공격 / SQL 인젝션은 오래된 공격 기법의 하나로, 악의적 공격자들은 여러 작업을 수행하고 인젝션 툴을 자동화시키기 위해 이 기법을 지속적으로 수정해가며 사용하고 있습니다. 이 보고서에서는 실제로 발생하고 있는 10가지 유형의 SQL 인젝션 공격을 분석합니다. 가장 일반적인 유형은 SQL 인젝션 탐색(probing)으로서

IPv6 공격 기법을 강화시키는 요인

- 보안 컨트롤을 우회하기 위해 전환 기술을 악용
- IPv6로 활성화된 애플리케이션과 서비스에 IPv6 프로토콜을 사용함으로써 IPv4 보안 컨트롤을 우회
- IPv6 IP, ID, 방화벽 기술을 우회하기 위해 IPv6 프로토콜 구조 수정
- IPv6에서 작동하도록 애플리케이션 레이어 공격 수정
- IPv6 프로토콜에서 작동하도록 공격 기법(Exploitation Framework) 수정
- IPv6 프로토콜 구조만을 타겟으로 하는 서비스 거부 툴 및 기법

모든 SQL 인젝션 공격의 첫 번째 단계입니다. 그 다음, 데이터베이스의 종류를 확인하고 데이터베이스로부터 콘텐츠를 가져오게 됩니다. SQL 인젝션 공격의 상당수는 사용자 인증 정보를 유출할 목적으로 진행되지만 명령어를 실행하고, 데이터를 손상시키고, 서비스를 거부할 목적으로 실시되기도 합니다.

/ 웹 사이트 변조 및 도메인 하이재킹 / 2015년 1분기에 발생한 웹사이트 변조와 도메인 하이재킹 시도 사례를 분석해보니 동일한 IP 주소를 사용하고 동일한 서버에서 호스팅되는 웹사이트들이 피해를 입은 것으로 나타났습니다. 즉, 악의적 공격자가 취약한 사이트를 하나만 발견해도 전체 서버가 감염될 수 있다는 의미입니다. 이 보고서에서는 웹 사이트 변조와 도메인 하이재킹을 모두 막을 수 있는 방어 수단을 제공합니다.

/ 2015년 1분기 자문 내용 요약 / 아카마이는 2015년 1분기 SSL(Secure Socket Layer) 사용을 본격적으로 중단하고 대신 TLS(Transport Layer Security)를 사용하기 시작했습니다. Poodle, Shellshock, Heartbleed 등의 취약점 때문에 이런 전환을 진행하게 되었습니다. 이 항목에서는 SaaS(Software as a Service) 공급업체를 위협하는 공격, Linux 시스템에 영향을 주는 GNU C 라이브러리의 취약성, 마이크로소프트 SQL Server Resolution Protocol(MC-SQLR)을 악용한 공격, 공유되고 있는 유출 데이터를 복호화해서 인증정보를 빼내려는 시도 등을 집중 분석합니다. 이 보고서에서는 해당 위협을 방어하고 완화하는 기법에 대한 정보를 제공합니다.

2015년 1분기 인터넷 현황 보안 보고서 전문을 읽으시려면 아래 사이트로 이동하시기 바랍니다.
www.stateoftheinternet.com/security-report

아카마이®란?

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

아카마이는 미국 매사추세츠주 케임브리지에 본사를 두고 있으며 전 세계 40여 개의 지사를 운영하고 있습니다. 아카마이의 우수한 솔루션과 고객 서비스는 기업들이 사용자들에게 쾌적한 인터넷 경험을 제공할 수 있도록 도와줍니다. 당사의 모든 주소, 전화번호 및 연락처 정보는 *www.akamai.com/locations*에서 확인할 수 있습니다.
