[인터넷 보안 현황 보고서]

2017년 4분기 Executive Summary

Akamai

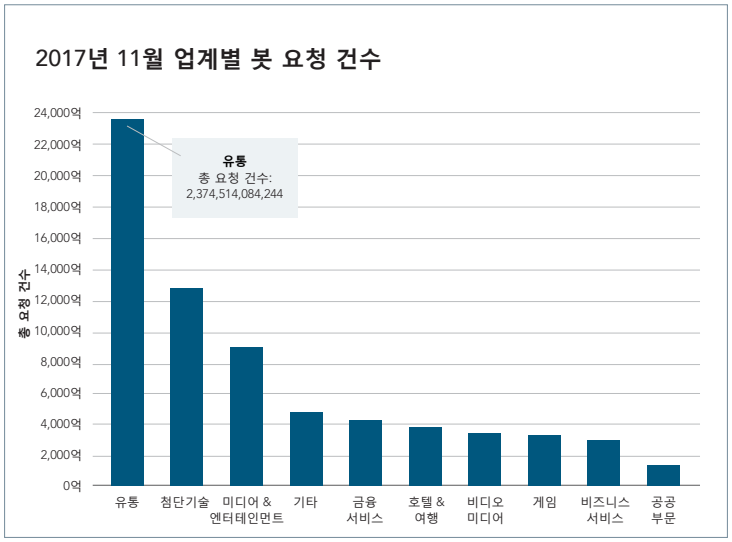
Executive Summary / 전세계 콘텐츠 전송 네트워크(CDN) 분야를 이끌고 있는 Akamai는 전세계에 분산된 Akamai Intelligent Platform™을 통해 매일 수조 건의 인터넷 트랜잭션을 처리합니다. Akamai는 이 과정에서 광대역 접속, 클라우드 보안, 미디어 전송 등의 지표에 관한 방대한 양의 데이터를 수집합니다. 인터넷 보안 현황 보고서는 Akamai에서 수집한 방대한 데이터와 그로부터 창출된 인사이트를 활용하여 기업과 정부에서 더 나은 전략적 의사 결정을 내릴 수 있도록 지원하기 위해 작성되었습니다. Akamai는 매 분기마다 수집된 데이터를 활용해 광대역 접속 속도 및 클라우드 보안에 대해 중점적으로 다루는 인터넷 현황 보고서를 발행합니다.

비즈니스에 미치는 영향 / 2017년 사상 최대 규모의 공격으로 인해 막대한 피해 금액이 발생하면서 사이버 보안이 비즈니스에 미치는 영향에 대한 인식이 크게 높아졌습니다. 스펙터(Spectre)와 멜트다운(Meltdown)을 발생시킨 하드웨어 결함을 이용하면 악성 프로그램이 권한 없이 컴퓨터 메모리의 데이터를 읽을 수 있습니다. 많은 보안 취약점들이 곳곳에 퍼져 있고 이로 인해 심각한 피해가 지속적으로 발생하면서 어느 누구도 낙관할 수 없는 상황입니다.

현재 대부분의 공격은 기존에 알려진 취약점을 악용하는데 이 취약점들은 이미 문서화되고 패치되었기 때문에 사전에 차단이 가능합니다. 직접 실천하는 것이 어렵기는 하지만 안전한 코딩, 신속한 패칭, 적절한 디바이스 설정, 신중한 패스워드 관리 등 기본적인 노력에 충실하면 보안을 강화하는 데 큰 도움이 됩니다.

공격자들이 새로운 공격 방식을 사용하면서 보안 환경 역시 지속적으로 변화하고 있습니다. 2018년에는 모바일 디바이스, 사물인터넷(IoT), API를 겨냥한 공격이 주로 발생할 것으로 예상됩니다. 공격 전략도 끊임없이 진화하고 있습니다. 기업 시스템을 타겟으로 한 공격 트렌드도 나타나고 있는데 기업의 데이터를 유출시킬 뿐만 아니라 컴퓨팅 리소스를 고갈시키는 공격입니다. 암호화폐와 채굴 리소스의 가치 상승이 이런 공격 트렌드의 원인 중 하나입니다. 또한, 4분기 인터넷 보안 현황 보고서에서는 Akamai 네트워크 접속, 봇넷 트래픽, 인증 도용에 대한 데이터를 면밀하게 분석했습니다. 그 결과 웹사이트에서 이루어지는 로그인 시도의 43%가 악성이라는 것을 확인했습니다. 디지털 기업은 이런 새로운 공격 트렌드를 반드시 인지하고 있어야 합니다.

Editor's Overview / 새해를 시작하면서 2017년에 발생한 보안 사고에서 배울 점을 찾아보는 것이 중요합니다.



DDoS 및 웹 애플리케이션 공격은 매년 꾸준히 증가하고 있습니다. 공격자들은 이미 증명된 오래된 공격 기법을 지속적으로 이용하고 있습니다. 따라서, 올바른 설정 적용, 인터넷 연결 디바이스 패치, 안전한 코딩 가이드라인 준수(데이터 인풋 확인 등) 등 기본적인 보안 수칙을 준수하는 것이 무엇보다 중요합니다.

4분기에 미라이(Mirai) 봇넷은 변화를 거듭했습니다. 이번 분기의 인터넷 보안 현황 보고서에서는 지난 1년 동안 미라이 봇넷의 활동과 변화 양상에 대해 살펴보고 이에 적극적으로 대응할 수 있는 방법에 대해 알아봅니다. Akamai SIRT 팀원인 래리 캐시달러(Larry Cashdollar)는 반드시 알아야 하는 2가지 CVE에 대해 심층 연구를 진행했습니다. 큰 관심을 모았던 취약점은 인증 없이 시스템에서 실행될 수 있는 가장 심각한 종류였습니다. 또한, 이번 분기 보고서에는 기존의 인터넷 보안 현황 보고서에서 다루지 않았던 봇 트래픽 및 인증정보 도용 시도에 대한 분석 데이터도 포함되어 있습니다.

마지막으로 2018년에는 암호화폐가 보안 관련 기사에 많이 등장할 것으로 전망됩니다. 기업 시스템의 컴퓨팅 리소스를 이용하기 위한 공격이 예상되고 해커들이 공격 전략을 수립하는 과정에서 암호화폐가 여러 측면에서 중요한 요소로 부각될 것입니다.

DDoS 공격 [2017년 4분기 vs 2017년 3분기]

- 총 DDoS 공격 건수 1% 미만 감소
- 인프라 레이어(레이어 3 및 4) 공격 1% 감소
- 반사 기반 공격 건수 3% 감소
- 애플리케이션 레이어 공격 건수 115% 증가

DDoS 업데이트 / DDoS 공격은 사이트를 다운시키고 비즈니스를 중단시키며 리소스를 고갈시킵니다. 또한, 데이터 또는 시스템 유출을 교묘하게 은폐하기도 합니다. DDoS 공격은 2017년 2, 3분기 연속 증가하다가 4분기에는 전분기 대비 소폭(1% 미만) 하락했습니다. 애플리케이션 레이어 공격은 전분기 대비 115% 증가했지만 전체 DDoS 공격에서 차지하는 비중은 1% 미만입니다. DDoS 공격은 2016년 4분기에 비해 14% 증가해 장기적으로 증가하는 추세를 보였습니다.

4분기 DDoS 공격의 79%가 발생한 게임 업계는 가장 큰 공격 대상이었습니다. 그다음은 4분기에 DDoS 공격이 크게 증가한 금융 서비스 분야가 차지했는데 1주일 사이에 최고 45건의 공격이 발생했습니다. DDoS 공격이 증가하면서 강력한 DDoS 공격 방어 솔루션의 필요성 역시 커지고 있습니다. 서비스 장애를 예방해야 할 뿐만 아니라 교묘한 시스템 유출 시도를 은폐하기 위한 수단으로 DDoS 공격을 이용하는 활동 역시 차단해야 합니다.

웹 애플리케이션 공격 업데이트 / DDoS 공격과 달리 웹 애플리케이션 공격은 애플리케이션 취약점을 표적으로 삼아 데이터를 유출하거나 시스템을 감염시킵니다. 웹 애플리케이션 공격은 DDoS 공격보다 훨씬 더 일반적으로 발생하며 공격자들은 취약한 웹사이트를 찾기 위해 인터넷을 스캔합니다. 웹 애플리케이션 공격은 2017년 3분기에 전분기 대비 30% 급증했다가 4분기에는 소폭 감소했습니다. 하지만 2017년 전반에 걸쳐 증가 추세를 보였고 2018년에도 동일한 추세가 계속될 것으로 전망됩니다.

웹 애플리케이션 공격 [2017년 4분기 vs. 2017년 3분기]

- 총 웹 애플리케이션 공격 건수 9% 감소
- 미국에서 발생한 공격 29% 감소
- SQLi 공격 건수 9% 감소

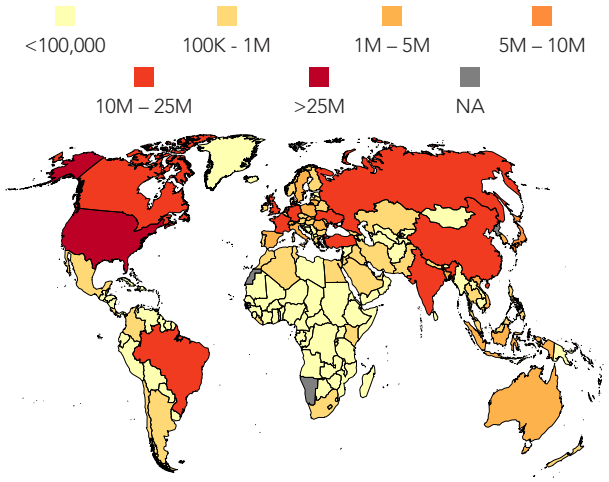
가장 많이 사용되는 공격 기법은 SQLi입니다. 전체 웹 애플리케이션 공격에서 차지하는 비중이 2017년 3분기에는 47%를 기록했고 4분기에는 50%로 증가했습니다. 이 공격은 자동화하기 쉽고 확장성도 높일 수 있기 때문에 기업이 사용자 입력값을 확인하는 등의 적절한 조치를 취하지 않을 경우 앞으로도 공격 효과가 계속될 것입니다.

Akamai가 관측한 웹 애플리케이션 공격 트래픽의 가장 큰 발원 국가이자 표적 국가는 기존과 동일하게 미국이었습니다. 미국은 4분기에 2억 3800만 건의 웹 애플리케이션 공격을 받았으며 이는 3분기의 3억 2300만 건에서 감소한 수치지만 2위인 브라질에 비해 10배 이상 높은 수준입니다. 미국에서는 4분기에 1억 3200만 건의 공격이 발원되었으며 2위인 네덜란드는 4700만 건의 공격이 발원되었습니다.

분석 및 연구에 대한 자세한 내용은 보고서 전문을 다운로드하십시오.

2017년 4분기 인터넷 보안 현황 보고서는 Akamai 글로벌 인프라 전체에서 취합한 공격 데이터를 기반으로 작성되었고 다수의 팀에서 진행한 연구 결과를 제공합니다.

2017년 4분기 웹 애플리케이션 공격 발원 상위 국가



인터넷 보안 현황 보고서 / 보안팀
호세 아르테아가, Akamai SIRT 팀장, 데이터 랭글러 — 공격 분석 결과
데이브 루이스, 글로벌 보안 고문 — DDoS 활동, 웹 애플리케이션 공격 활동
채드 시먼, Akamai SIRT — 공격 분석 결과
윌버 메히아, Akamai SIRT — 공격 분석 결과
알렉산더 라플럼, Akamai SIRT — 공격 분석 결과
래리 캐시달러, Akamai SIRT, Akamai SIRT, 수석 엔지니어 — 웹 취약점 감시
리차드 윌리, 수석 데이터 과학자 — 행성규모 네트워크 실현 방법
엘라드 슈스터, 보안 데이터 분석가, 위협 연구소
존 톰슨, 고객 애널리틱스

편집부
마틴 맥키, 수석 보안 전문가, 수석 편집자
아만다 파크레딘, 수석 테크니컬 라이터 겸 편집자

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

보고서 전문 다운로드

[인터넷 보안 현황 보고서]
2017년 4분기 보고서 전문