Executive Summary:
[인터넷 보안 현황 보고서]

5권, 3호

웹 공격 및 게임 도용

Intelligent Security Starts at the Edge

Editor's Note:

이번 인터넷 보안 현황 보고서는 지난 17개월 동안 게임 업계를 대상으로 발생한 웹 공격 및 인증정보 도용 트렌드에 대해 알아봅니다.

이번 보고서에서는 게임 업계를 집중적으로 살펴봅니다. 게임 계정은 인증정보 도용을 통해 지하 경제에서 활발하게 거래가 이루어지고 있고 거래 규모 역시 빠르게 성장하고 있습니다. 또한, 웹 애플리케이션 공격 기법으로 점차 많이 사용되고 있는 SQL 인젝션(SQLi)과 웹 애플리케이션 공격 및 크리덴셜 스터핑의 상위 발원 국가도 함께 살펴봅니다.

객원 저자: 모니크 보너(Monique Bonner)

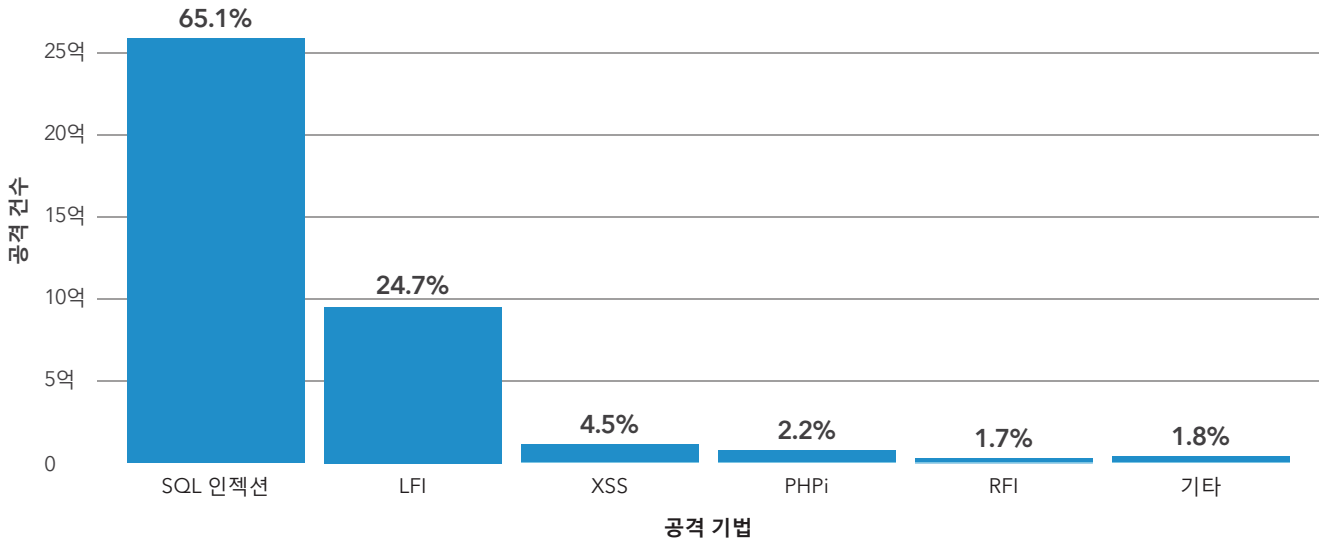
이번 보고서에서 Akamai의 최고 마케팅 책임자(CMO)인 모니크 보너는 3년 전에 이 직책을 맡은 이후 보안팀과 협업하면서 얻은 교훈에 대해 설명합니다.

"저는 Akamai의 보안 제품 및 연구팀들이 다른 기술기업의 팀들과 비슷할 것이라 생각했습니다. 비용과 ROI에 신경 쓰면서 혁신과 개선사항에 집중할 거라 예상했습니다. 제가 함께 일을 해보니 물론 이것도 보안팀의 업무 영역에 포함되지만 팀원들을 이끄는 원동력은 아니었습니다. 팀원들의 호기심을 유발하거나 DDoS 공격을 받는 동안 고객사의 웹사이트를 보호하기 위해 24시간 지원에 전념하도록 만드는 것은 따로 있었습니다."

웹 공격 개요

이번 보고서에서 추적한 17개월 동안 Akamai는 SQLi 공격이 전체 웹 애플리케이션 공격의 약 2/3를 차지한다는 것을 확인했습니다. 모든 애플리케이션 공격 기법이 전반적으로 증가하는 추세를 보이지만 SQLi처럼 빠르게 증가하는 공격 기법은 없습니다. 이 공격의 발원 국가는 어디일까요? 공격 발원 국가와 공격 표적 국가 모두 미국이 1위를 차지했습니다. 러시아, 네덜란드, 중국도 웹 공격 발원 국가 목록에서 높은 순위에 올랐습니다.

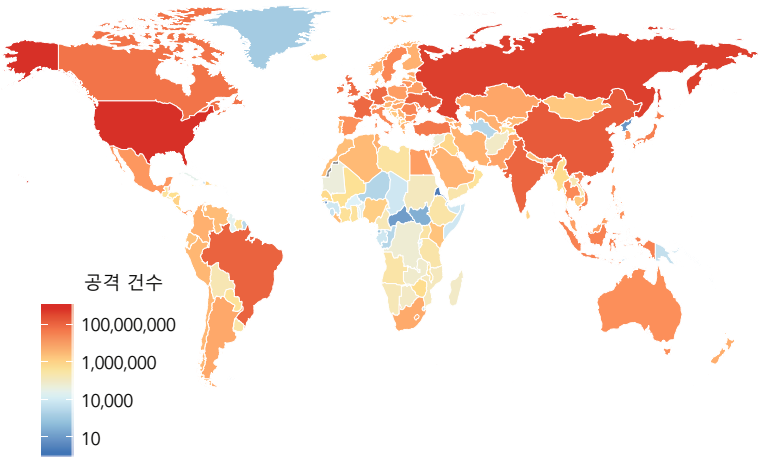
상위 웹 공격 기법
2017년 11월~2019년 3월



상위 10대 웹 공격 발원 국가
2017년 11월~2019년 3월

국가	총 공격 건수	글로벌 순위
미국	967,577,579	01
러시아	608,655,963	02
네덜란드	280,775,553	03
중국	218,015,784	04
브라질	155,603,585	05
우크라이나	154,887,375	06
인도	142,621,086	07
프랑스	121,691,941	08
독일	113,233,187	09
영국	102,531,816	10

상위 발원 국가 - 모든 산업 분야



인증정보 도용 및 게임

범죄자들은 수익을 추구합니다.

지난 17개월 동안 Akamai는 총 550억 건의 크리덴셜 스터핑 공격을 관측했으며, 이중 120억 건은 게임 산업에서 발생했습니다. 게임 업계를 노리는 범죄자들은 주로 인기 있는 게임의 사용자들을 표적으로 삼고 탈취 가능한 계정을 찾는 데 주력합니다. 공격자들은 탈취한 인증정보를 판매 또는 거래할 수 있습니다. 지하경제에서 인증정보 거래는 수익성이 높은 사업입니다.

대부분의 게임사들은 플레이어들에게 여러 웹사이트와 게임에서 동일한 비밀번호를 재사용하지 말 것을 강력하게 권장합니다. 크리덴셜 스터핑 공격이 성공하는 주요 원인은 비밀번호의 재사용입니다. 사용자는 인증정보를 엄격하게 관리해야 할 책임을 갖고 있습니다. 하지만 기업들 역시 고객과 사용자를 안전하게 보호하기 위해 지식 격차를 반드시 해결해야 합니다.

모든 산업에 걸쳐 미국은 여전히 크리덴셜 스터핑 공격 발원 국가 1위를 차지합니다. 하지만 게임 분야에서 미국은 러시아와 중국의 뒤를 이어 3위에 올랐습니다.

상위 공격 발원 국가 – 게임

국가	총 공격 건수	글로벌 순위*
러시아	2,674,783,777	02
캐나다	1,486,753,732	04
미국	1,435,752, 015	01
베트남	617,097,561	09
인도	599,317,123	06

*모든 산업 분야

향후 전망

게임 산업은 공격의 표적으로 인기를 얻고 있습니다. 최신 인터넷 보안 현황 보고서에 소개된 사례와 관련 데이터에 따르면 이러한 트렌드는 가까운 미래에도 계속될 것으로 예상됩니다. 게임사들은 자사 방어 체계를 지속적으로 혁신하고 강화하는 한편 소비자들에게 스스로 보호하고 공격을 방어하는 방법을 지속적으로 교육해야 합니다. 소비자와 기업이 모범 사례를 따르면 인증정보 도용 공격의 영향을 제한할 수 있습니다.

보다 자세한 내용은 보고서 전문을 다운로드하시기 바랍니다.
State of the Internet / Security: Web Attacks and Gaming Abuse