SOTI

10 YEARS
OF SECURITY INSIGHT

10권, 05호

높은 파고를 헤쳐 나가는 방법

금융 서비스의 공격 트렌드

Akamai

인터넷 보안 현황 보고서

목차

2 소개

3 FS-ISAC 게스트 칼럼: 컴플라이언스, 운영 안정성, 사이버 보안을 통한 금융 서비스 강화

4 핵심 인사이트

5 금융 서비스는 여전히 레이어 3 및 4 DDoS 공격의 주요 표적

9 보안 스포트라이트: 레이어 3 및 4 DDoS 공격 강도: 이벤트 vs Gbps

12 API에 대한 레이어 7 DDoS 공격 증가

14 금융 서비스 분야의 랜섬웨어 및 핵티비즘

17 친숙함을 이용한 공격: 금융 서비스의 브랜드 남용

23 심각한 리스크 수준의 사기 금융 서비스 사이트

24 브랜드 남용 분석

26 금융 서비스의 지역 피싱 및 브랜드 사칭 공격

28 게스트 칼럼: 진화하는 컴플라이언스: 글로벌 사이버 보안 규정이 금융 기관을 변화시키는 방법

29 제로 트러스트로 방어 강화

31 방어

33 결론

34 방법론

36 저자 소개

소개

금융 서비스 업계는 세계 경제의 기반일 뿐만 아니라 경제 성장과 발전의 생명선입니다. 시중 은행, 결제 처리업체, 자산 관리 회사, 투자 은행, 보험사 등 다양한 업계를 아우르는 금융 서비스는 끊임없이 진화하고 있습니다.

기술 발전으로 금융 서비스 환경이 계속 재편되면서 디지털 은행, 로보 어드바이저, 암호화 자산과 같은 금융 기술(핀테크) 혁신이 일어나고 있습니다. 핀테크 기업의 수는 미국과 중국을 중심으로 전 세계에서 급증하고 있습니다. 2024년 1월 현재, 10대 핀테크 기업 중 8곳이 미국과 중국에 기반을 두고 있습니다. 이러한 기술적 변화는 현금 없는 거래의 증가에도 반영되어 있으며, 특히 금융 접근성이 제한적인 지역에서 현금 없는 거래가 크게 증가할 것으로 예상됩니다. 하지만 혁신에는 취약점이 따르기 마련입니다.

사이버 범죄자들은 금융 기관을 끊임없이 표적으로 삼고 있으며, 공격의 영향은 재정적 손실에 국한되지 않습니다. 운영 중단, 평판 손상, 심각한 규제 처벌은 금융 서비스 업계의 기반이 되는 신뢰의 토대를 약화시킬 수 있습니다. 디지털 혁신의 속도가 사이버 위협의 정교함만큼이나 빨라지고 있는 지금, 금융 기관은 어떻게 효과적인 방어 체계를 구축할 수 있을까요?

이 인터넷 현황 보고서는 전 세계 금융 서비스 전문가, Akamai 고객사, 사이버 보안 연구원, 업계 리더들이 점점 더 복잡해지는 위협 환경을 헤쳐 나가는 데 도움을 주기 위해 특별히 작성되었습니다. 사이버 범죄자들의 주요 표적이 되는 금융 서비스 업계는 중요한 인프라를 보호하고, 기업과 고객을 보호하고, 금융 시장의 안정성을 보장하고, 경제 혼란을 방지하기 위해 공동의 노력이 필요합니다. 이 보고서의 리서치는 공격자들보다 앞서 나가고, 금융 업계의 중요 자산을 강화하고, 글로벌 금융 관계를 뒷받침하는 지속적인 신뢰와 안정성을 보장하고자 하는 기업에게 필수적인 자료입니다.

컴플라이언스, 운영 안정성, 사이버 보안을 통한 금융 서비스 강화

오늘날 글로벌 금융 업계가 직면한 중요한 과제 중 하나는 컴플라이언스와 운영 안정성을 강화해야 한다는 것입니다. 규제의 환경이 변화함에 따라 금융 기관은 이러한 새로운 요구사항을 충족하기 위해 선제적으로 적응해야 합니다. 예를 들어, DORA(Digital Operational Resilience Act)의 도입은 ICT(Information and Communication Technology)와 관련된 혼란을 견딜 수 있는 강력한 프레임워크의 필요성을 강조합니다. 2025년 1월에 발효될 예정인 DORA는 금융 기업과 해당 기업의 ICT 써드파티 공급업체를 위한 포괄적인 안정성 전략을 의무화해 기업이 보안 및 인시던트 대응 기능을 강화하도록 강제하고 있습니다.

미국 증권거래위원회의 업데이트된 가이드라인은 종합적인 사이버 보안 접근 방식의 필요성을 더욱 강조하고 있습니다. 이제 금융 기관은 사이버 리스크의 중요성에 중점을 두고 운영 안정성과 재해 복구를 전략에 통합해야 합니다. 이를 위해 중대한 위협과 인시던트가 재무 안정성과 운영에 미치는 영향을 깊이 있게 이해해야 합니다. 중요한 사이버 보안 인시던트를 신속하게 공개하고 연례 보고서에 리스크 관리 전략을 상세히 설명하도록 의무화한 것은 규제 기대치의 패러다임 전환을 의미합니다. 이러한 규제 환경을 탐색하려면 금융 기관은 최첨단 보안 솔루션과 가시성을 제공하는 기업과의 파트너십이 필요합니다. 이 리서치 결과에서 알 수 있듯이 Akamai의 전문성은 금융 서비스 기업이 엄격한 규제 요구사항 속에서 컴플라이언스뿐만 아니라 운영 무결성을 유지할 수 있도록 지원합니다.

이러한 상황을 고려할 때 금융 기관은 컴플라이언스 및 운영 안정성의 복잡성을 해결하기 위해 포괄적인 접근 방식을 도입해야 합니다. 여기에는 투자자의 의사 결정 과정에 상당히 영향을 미칠 수 있는 중대한 리스크를 식별하고 우선순위를 정하는 것이 포함됩니다. 금융 기관은 이러한 중대한 리스크를 리스크 관리 프레임워크에 통합하고 강력한 인시던트 대응 계획을 마련해야 합니다. 멀티레이어 심층 보안 전략을 도입하면 효과적인 운영 안정성을 확보하는 기반을 마련할 수 있습니다. 여기에는 네트워크 세그멘테이션 및 마이크로세그멘테이션을 통한 공격표면 감소, 미사용 데이터 암호화 구축, 서버 강화, 최신 위협 탐지 시스템과 결합된 웹 애플리케이션 방화벽 사용이 포함됩니다. 지속적인 모니터링과 정기적인 보안 평가는 리스크를 신속하게 파악하고 방어하는 데 매우 중요합니다.

금융 기관은 최신 위협 인텔리전스 및 Akamai의 인터넷 보안 현황(SOTI) 보고서와 같은 리서치를 기반으로 인시던트 대응 계획을 수립하는 연습을 해야 합니다. 이러한 연습은 실현 가능한 시나리오를 구축하고 새로운 툴, 기술, 절차가 등장할 때 금융 기관이 이에 적응할 수 있도록 도와줍니다. 이러한 사전 예방적 자세는 점점 더 변동성이 커지는 위협 환경에서 운영 안정성을 보장하고 고객의 신뢰를 유지하는 데 필수적입니다. 금융 서비스 업계가 진화함에 따라 컴플라이언스, 운영 안정성, 사이버 보안의 교차점에서 미래가 지속적으로 만들어질 것입니다. 금융 기관은 최신 보안 조치를 도입하고 가시성을 강화함으로써 규제의 복잡성을 해결하고 운영을 보호해 비즈니스에 필수적인 신뢰를 유지할 수 있습니다.

테레사 월시(Teresa Walsh)
FS-ISAC 글로벌 인텔리전스 책임자

핵심 인사이트

34%

금융 서비스 기관이 경험한 레이어 3 및 4 DDoS 공격 이벤트의 비율

금융 서비스는 여전히 레이어 3 및 4의 분산 서비스 거부(DDoS) 공격 이벤트가 가장 빈번하게 발생하는 업계입니다. 다음으로 게임이 18%, 하이테크가 15%로 그 뒤를 잇고 있습니다. 이러한 만연한 위협은 전 세계적으로 핵티비스트 활동이 급증한 이스라엘-하마스, 러시아-우크라이나 전쟁 등 지정학적 긴장이 지속되고 있기 때문인 것으로 보입니다.

API 증가로 인한 레이어 7 DDoS 공격 증가

웹 애플리케이션은 전통적으로 사이버 공격의 주요 표적이었지만, 이 보고 기간 동안 API에 대한 레이어 7 DDoS 공격이 눈에 띄게 증가했습니다. 진화하는 컴플라이언스 및 규제 요구사항을 충족하기 위해 금융 서비스에서 API 도입이 증가한 것이 주요 원인입니다. 기업이 API에 더 많이 의존함에 따라 공격자들은 기법을 조정하고 있으며, 이에 따라 API 보안은 현대 비즈니스의 중요한 우선 순위가 되었습니다.

트래픽이 급증하면서 DDoS를 빈도 및 규모별로 평가해야 할 필요성 발생

금융 서비스에서의 DDoS 공격은 중요한 인사이트를 보여줍니다. 이벤트 빈도와 공격 강도가 항상 상관관계가 있는 것은 아닙니다. 공격이 거의 발생하지 않았던 달도 있지만, 해당 Gbps 데이터는 상당한 트래픽 급증을 나타내며 DDoS 공격의 영향을 평가할 때 공격 빈도와 규모 모두 고려해야 한다는 것을 보여줍니다.

36%

금융 기관을 표적으로 삼는 의심스러운 도메인의 비율

금융 서비스 고객을 노리는 피싱 공격이 증가하면서 신원 도용 및 계정 탈취의 리스크가 높아지고 있습니다. 이러한 공격 트렌드로 인해 규제 기관이 금융 기관을 더 면밀하게 조사하게 되고, 유출로 인해 고객의 신뢰 문제가 발생합니다.

30%

피싱 및 브랜드 사칭 사이트로 연결되는 페이지 방문 비율

공격자는 정상적인 금융 서비스 웹사이트와 앱을 모방해 사기성 사이트로 트래픽을 성공적으로 유도합니다. 공격자는 금융 기관이 보유한 민감한 정보를 얻기 위해 피싱을 통해 금융 기관을 지속적으로 표적으로 삼고 있습니다.

금융 서비스는 여전히 레이어 3 및 4 DDoS 공격의 주요 표적

레이어 3 및 레이어 4 DDoS 공격은 네트워크 및 전송 레이어를 표적으로 삼아 네트워크 인프라를 마비시키고 서버 리소스와 대역폭을 고갈시킵니다. 이러한 공격은 엄청난 양의 트래픽을 전송해 네트워크 용량을 소모하고 정상적인 사용자의 성능을 저하시키는 것을 목표로 합니다. 모든 업계 중에서 금융 서비스 업계는 레이어 3 및 레이어4 DDoS 공격의 주요 표적이 되어 왔습니다(그림 1). 이런 트렌드는 몇 가지 상호연결된 요인에 의해 발생했는데 이로 인해 공격자들이 이용할 수 있는 퍼펙트 스톰과 같은 취약점과 기회가 만들어졌습니다.

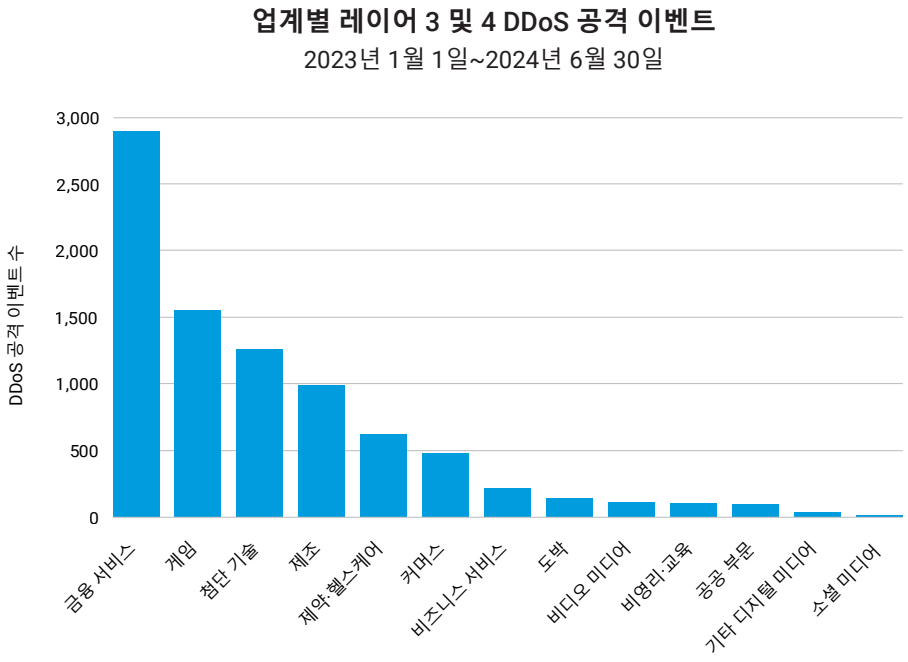


그림 1: 금융 서비스 업계는 레이어 3 및 4 DDoS 공격 이벤트에서 다른 업계에 비해 압도적인 우위를 점하고 있습니다.

지정학적 긴장은 금융 기관에 대한 DDoS 공격 증가의 중요한 원인으로 작용했습니다. 현재 진행 중인 러시아-우크라이나 전쟁과 이스라엘-하마스 전쟁은 친러시아 및 친팔레스타인 핵티비즘의 현저한 증가와 맞물려 있습니다. 이러한 분쟁으로 인해 특히 우크라이나에 연고를 둔 유럽 은행을 겨냥한 DDoS 공격이 급증했습니다. 이러한 공격의 정치적 동기는 위협 환경을 더욱 복잡하게 만듭니다.

금융 기관은 높은 금전적 이득을 얻을 수 있기 때문에 DDoS 공격자들에게 특히 매력적인 표적입니다. 운영 중단이 되면 심각한 재정적 타격, 심각한 평판 손상, 글로벌 금융 시스템에 대한 신뢰 상실로 이어질 수 있습니다. 광범위한 결과를 초래할 가능성이 있기 때문에 금융 서비스는 혼란을 극대화하거나 정치적 주장을 퍼트리려는 자들의 주요 표적이 되고 있습니다.

기술의 발전으로 DDoS 공격자의 힘과 역량이 크게 증가했으며, 이제 가상머신(VM) 봇넷을 배포해 수많은 VM과 사물 인터넷(IoT) 디바이스에서 컴퓨팅 리소스를 활용하고 보다 효율적으로 공격을 일으킬 수 있게 되었습니다. 이러한 접근 방식은 클라우드 서비스의 분산된 특성을 악용하므로 공격을 방어하고 추적하기가 더 어렵습니다. 공격자는 높은 대역폭 가용성과 방대한 컴퓨팅 리소스를 활용해 다양한 전략을 기반으로 적응력 있고, 강력하고, 비용 효율적인 DDoS 공격을 실행할 수 있습니다.

금융 서비스 업계의 공격표면이 확대되는 것도 DDoS 공격의 증가에 기여했습니다. 디지털 서비스와 API의 사용이 증가하면서 공격자에게 더 많은 엔트리 포인트가 열렸습니다. 이러한 변화로 인해 금융 시스템이 복잡해지고 공격자가 악용할 수 있는 잠재적 취약점이 많아졌습니다. 문서화되지 않은 섀도 API는 정보 보안 팀이 그 존재를 인지하지 못해 보호되지 않는 경우가 많아 특히 우려됩니다. 공격자는 이러한 API를 악용해 데이터를 유출하거나, 인증 제어를 우회하거나, 방해 행위를 할 수 있습니다.

규제 압박으로 인해 금융 기관의 DDoS 공격에 대한 취약점이 의도치 않게 증가했습니다. 유럽연합에서 도입한 PSD2(Payment Services Directive 2)와 같은 요구사항에 따라 은행은 API를 통해 핀테크 기업과 같은 써드파티 공급업체에 시스템을 개방해야 합니다. 이를 통해 은행은 핀테크, 모바일 앱 및 기타 플랫폼과의 통합을 통해 높아지는 고객의 기대에 부응할 수 있지만, 보안 리스크가 증가하고 공격표면이 확대되는 단점도 있습니다. 이렇게 다양한 기업에서 API를 추가로 사용하면 공격자가 공격할 수 있는 잠재적 장애 지점이 더 많아집니다.

이러한 요인들이 종합적으로 작용해 금융 서비스 업계가 지속적으로 레이어 3 및 레이어 4 DDoS 공격의 주요 표적이 되고 있습니다. 지정학적 동기, 고부가가치 표적, 기술 발전, 디지털 기반 확대, 규제 압박이 결합되어 금융 기관에 대한 DDoS 공격이 그 어느 때보다 빈번하게 발생할 뿐만 아니라 잠재적으로 더 큰 피해를 입을 수 있는 환경이 조성되었습니다. 업계가 계속 진화함에 따라 점점 더 정교하고 끈질긴 위협에 대한 방어 체계도 발전해야 합니다.

공격자는 높은 대역폭 가용성과 방대한 컴퓨팅 리소스를 활용해 다양한 전략을 기반으로 적응력 있고, 강력하고, 비용 효율적인 DDoS 공격을 실행할 수 있습니다.

레이어 3 및 4 DDoS 공격 이벤트: 변동성이 심한 공격

금융 서비스 업계는 레이어 3 및 레이어 4 DDoS 공격 이벤트의 발생 빈도가 가장 높지만, 이러한 공격의 발생률은 연중 내내 변동이 심합니다(그림 2).

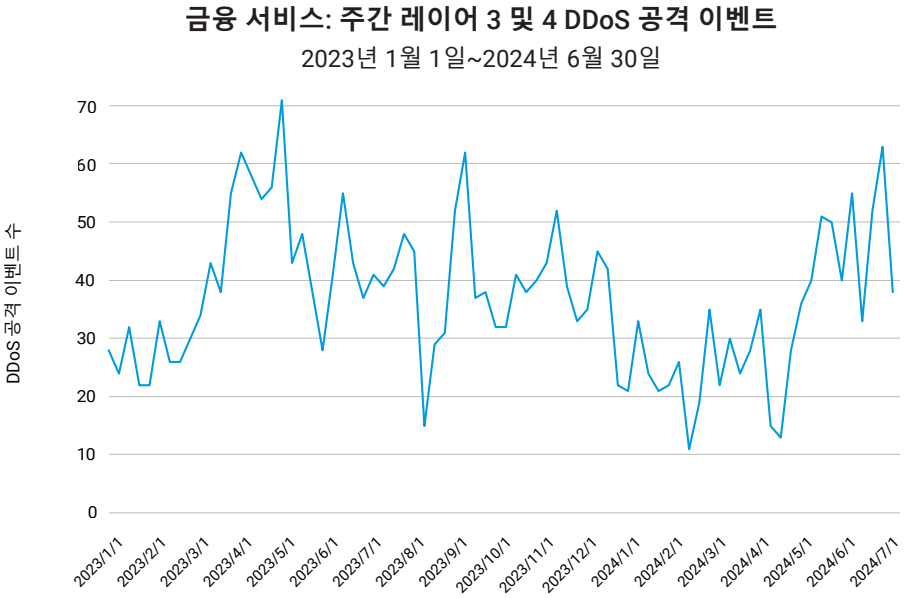


그림 2: 금융 서비스 업계의 레이어 3 및 4 DDoS 공격 이벤트의 증가 및 감소 패턴

2023년 3월과 4월, 2023년 8월과 9월, 2024년 4월과 5월에 금융 서비스 업계에 대한 레이어 3 및 레이어 4 DDoS 공격은 몇 가지 특정 요인에 기인한 것으로 볼 수 있습니다.

3월부터 4월까지의 봄은 미국의 소득세 신고가 활발히 진행되는 시기로, DDoS 공격자에게 매력적인 공격 기회를 제공합니다. 4월 16일부터 전국 및 지방 은행에서 계정 도용이 눈에 띄게 증가했는데, 이는 많은 은행이 1분기 실적을 발표하는 시기와 일치합니다. 또한 이 기간 동안 ID 및 접속 관리(IAM) 및 네트워크 공급업체(예: Okta, Cisco)는 온라인 서비스를 겨냥한 크리덴셜 스터핑 공격이 증가했고 그 규모가 상당했음을 보고했습니다.

특히 2023년 4월에는 SLP(Service Location Protocol) 고심도 취약점(CVE-2023-29552)이 발견된 것이 공격 활동의 급증에 영향을 미친 것으로 보입니다. 네트워크 레이어와 애플리케이션 레이어 모두에서 DDoS 공격을 증폭시킬 수 있는 이 취약점은 전 세계 2000개 이상의 기업과 인터넷의 5만 4000개 이상의 SLP 인스턴스에 영향을 미친 것으로 알려졌습니다. 공격자는 이 취약점을 악용했고 감염된 인스턴스를 사용해 대규모 DDoS 증폭 공격을 시작할 수 있습니다. 최대 2200배의 증폭 계수를 가진 이 취약점으로 인해 지금까지 기록된 가장 심각한 증폭 공격 중 하나가 가능했습니다.

Akamai는 2023년 8월과 9월에 발생한 주요 이벤트를 확인했습니다. Akamai는 2023년 9월 5일 미국 금융 기관에 대한 기록상 최대 규모의 DDoS 공격을 관측하고 차단했습니다. 이 공격은 ACK, PUSH, RESET, SYN 플러드 기술을 결합해 초당 633.7기가비트(Gbps), 초당 5510만 패킷(Mpps)의 최고 강도에 도달했습니다. 공격의 강도는 높았지만 공격 시간은 2분 미만으로 짧았습니다.

보안 스포트라이트

레이어 3 및 4 DDoS 공격 강도: 이벤트 vs Gbps

DDoS 공격이 금융 서비스 업계에 미치는 위협을 완전히 파악하려면 공격의 복잡성과 규모를 이해해야 합니다. 이러한 공격은 단순하고 고립된 인시던트가 아니라 기가비트의 데이터와 초당 수백만 개의 패킷을 네트워크에 넘쳐나게 하는 여러 차례의 대량 공격 시도를 수반하는 경우가 많습니다. 공격의 정교함, 강도, 기간이 증가하고 있으며 공격자들은 더욱 다양한 기술을 사용하고 있어 금융 기관의 리스크가 커지고 있습니다(그림 3).

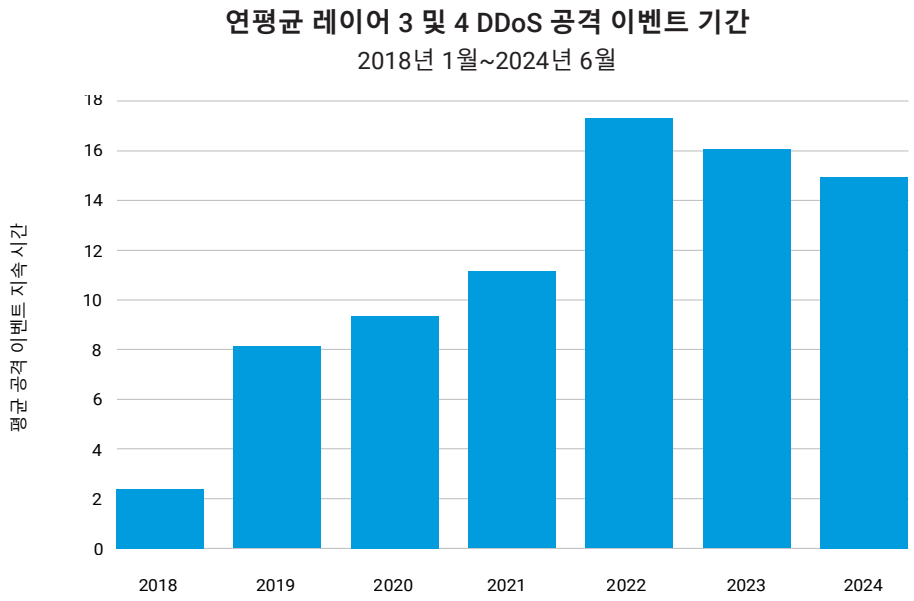


그림 3: 레이어 3 및 4 DDoS 공격 지속 시간의 글로벌 트렌드가 증가하고 있습니다

또한 금융 서비스 업계의 레이어 3 및 4 DDoS 공격 이벤트 수 그래프와 해당 DDoS Gbps 데이터를 비교하면 상당한 차이가 있음을 알 수 있습니다(그림 4). Gbps 그래프에는 공격 이벤트 그래프에 반영되지 않은 급격한 증가가 나타납니다. 이 차이는 중요한 개념을 강조합니다. 즉, 공격 이벤트가 상대적으로 적은 달에도 Gbps 기준으로는 매우 높은 양의 DDoS 트래픽이 발생할 수 있습니다.

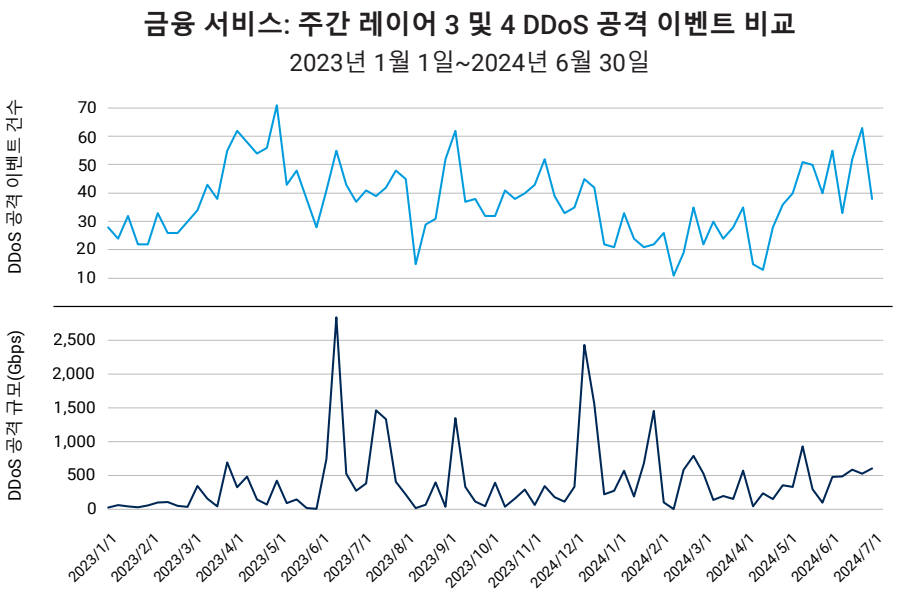


그림 4: 금융 서비스 업계의 레이어 3 및 4 DDoS 공격 이벤트를 Gbps 단위로 측정한 결과 비교

여기서 공격 이벤트의 빈도에만 의존하면 실제 위협을 심각하게 과소평가하게 된다는 중요한 사실을 알 수 있습니다. 각 공격의 트래픽 규모와 강도를 모두 고려해야 합니다. 소수의 고강도 DDoS 공격이 다수의 소규모 이벤트보다 훨씬 더 큰 피해를 유발할 수 있으므로 각 위협의 전체 범위를 평가하는 것이 필수적입니다.

단독 공격 경향: 금융 서비스의 단일 기법 레이어 3 및 4 DDoS 공격

애플리케이션 또는 네트워크 멀티 기법 공격은 시스템을 손상시키거나 무단 접속을 시도하는 사이버 범죄자들이 흔히 사용하는 전략입니다. 그러나 금융 서비스 업계를 겨냥한 공격자들은 레이어 3 및 4의 DDoS에 있어 단일 기법 공격을 더 자주 시도하는 것으로 보입니다(그림 5).

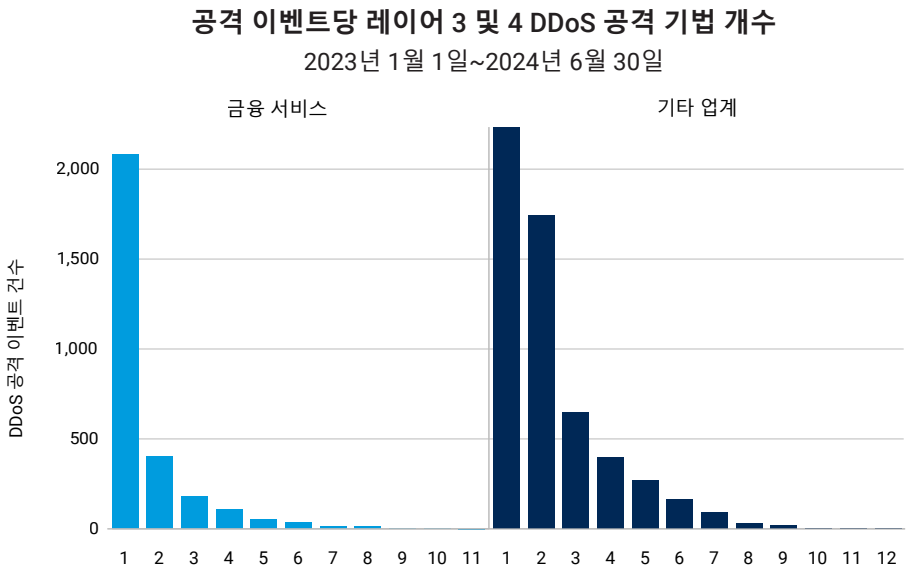


그림 5: 단일 기법 공격은 금융 서비스 업계에서 레이어 3 및 4 DDoS 공격에 더 널리 사용됩니다.

레이어 3과 4를 노리는 단일 기법 DDoS 공격은 더 적은 리소스를 필요로 하며 특히 더 복잡한 공격에 대해 강력한 방어 체계를 갖춘 금융 기관을 대상으로 매우 효과적일 수 있습니다. 일반적으로 멀티 기법 공격보다 실행하기 쉽고 조율이 덜 필요합니다. 또한, 보안에 의해 탐지될 수 있는 다른 공격 기법을 시도하는 리스크 없이 단일 기법 공격을 사용해 효과적으로 악용할 수 있는 잘 알려진 취약점이 레이어 3및 4에 존재할 수 있습니다.

금융 서비스 업계에서 단일 기법 공격을 선호하는 현상은 사이버 보안 팀에게 독특한 과제를 안겨줍니다. 복잡한 멀티 기법 공격에 대한 경계를 늦추지 않으면서 레이어 3과 4에 집중된 단일 기법 공격을 방어할 수 있는 방어 체계도 갖추어야 합니다.

API에 대한 레이어 7 DDoS 공격 증가

HTTP 또는 웹 트래픽 레이어 공격이라고도 하는 애플리케이션 레이어(레이어 7) DDoS 공격은 점점 더 널리 퍼지고 있으며, 현재 금융 서비스 업계를 노리는 공격자들이 선호하는 방법입니다. 이러한 공격은 특히 애플리케이션의 리소스 집약적인 구성요소에 집중해 정상적인 사용자의 접속을 효과적으로 거부합니다. 방화벽과 네트워크 보호 기능으로 방어되는 레이어 3 및 4 DDoS 공격과 달리 레이어 7 공격은 애플리케이션 서버를 마비시킬 목적으로 특정 애플리케이션 페이지나 검색 기능을 표적으로 삼아 정상적인 요청으로 위장해 이러한 방어 체계를 우회합니다.

일반적으로 금융 서비스 업계에서는 웹 애플리케이션이 API보다 더 자주 표적이 되어 왔지만, 최근 들어 API를 표적으로 하는 레이어 7 DDoS 공격이 급격히 증가하고 있는 것으로 나타났습니다(그림 6). 이러한 급증은 다른 업계의 전체 API 공격 패턴보다 훨씬 더 심각하고 다양합니다.

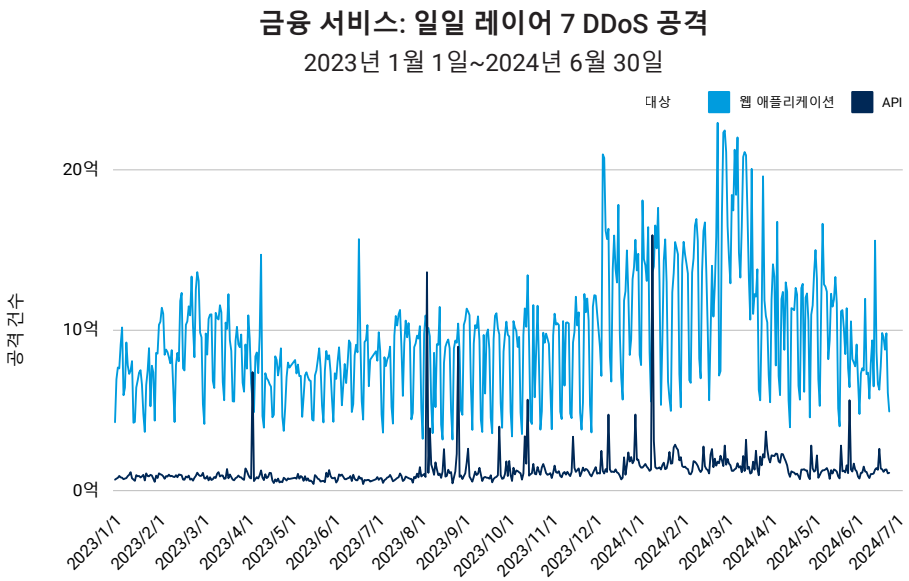


그림 6: 금융 서비스 업계에 대한 레이어 7 DDoS 공격의 공격 패턴은 공격 대상 웹 애플리케이션과 API에 따라 크게 다릅니다.

이러한 급증은 특히 2023년 4월, 2023년 8월, 2024년 1월에 발생했습니다. 더불어 이러한 급증은 레이어 3 및 4 공격에 영향을 미치는 요인과 유사한 요인과 함께 레이어 7에 특화된 요소가 추가되었기 때문인 것으로 분석됩니다.

공격자는 악용할 새로운 취약점을 지속적으로 찾고 있으며, 이러한 취약점이 발견되면 공격 빈도가 갑자기 증가할 수 있습니다. 예를 들어, 2023년 8월에 처음 발견된 HTTP/2 Rapid Reset 취약점(CVE-2023-44487)은 매우 효과적인 레이어 7 DDoS 공격을 가능하게 했습니다. 이 취약점을 통해 공격자는 겉보기에 정상적으로 보이는 로직을 악용해 여러 요청을 하나의 스트림으로 묶어 서버와 애플리케이션을 마비시킬 수 있었습니다. 이로 인해 지금까지 기록된 레이어 7 DDoS 공격 중 가장 큰 규모의 공격이 발생했습니다.

또한 계절에 따른 DDoS 공격은 금융 기관을 노리는 사이버 범죄자에게 인기 있는 기법으로, 세금 시즌과 휴가 기간에 눈에 띄게 급증하는 것으로 나타났습니다. 쇼핑 시즌인 2024년 1월에 크게 증가한 것은 공격자들이 온라인 거래 활동이 활발해지는 시기에 공격을 준비했음을 시사합니다.

금융 서비스 분야의 랜섬웨어 및 핵티비즘

금융 서비스 업계는 랜섬웨어 그룹과 같은 고도로 정교한 공격자의 표적이 되는 경우가 많습니다. 이러한 그룹은 금융 기관에 침투해 민감한 정보를 훔치고 거액의 몸값을 요구하기 위해 광범위한 기술을 사용합니다. 주로 금전적 동기에 초점을 맞추지만, 정치적 관계가 있을 수 있는 금융 기관을 표적으로 삼아 지정학적 측면과 관련되어 있을 수도 있습니다. 러시아에 기반을 둔 랜섬웨어 그룹 REvil(일명 Sodinokibi)의 경우가 여기에 해당합니다. 유명 은행에 대한 공격에서 볼 수 있듯이 BlackCat (ALPHV)도 이러한 방식에 연루되어 있습니다.

금융 기관을 포함한 대규모 기업을 공격하는 것으로 알려진 가장 활발한 랜섬웨어 그룹 중 하나는 여전히 LockBit입니다. 최근 LockBit에 대한 사법 기관의 조치에도 불구하고 활발하게 활동하고 있습니다. Europol과 Eurojust가 협력해 처음으로 국제 태스크포스를 구성한 Operation Cronos는 LockBit이 구축한 새로운 인프라에 의해 무너졌습니다. LockBit은 2024년 2월 사법 기관이 서버를 압수한 지 불과 며칠 만에 새로운 인프라와 다크 웹 유출 사이트를 통해 다시 등장했습니다. 그리고 LockBit은 Operation Cronos에 대응해 정부 네트워크에 대한 공격을 늘려 반격하겠다고 밝혔습니다.

랜섬웨어 그룹 CL0P도 계속 활동 중이며 특히 금융 기관을 비롯한 기업에서 널리 사용되는 파일 전송 소프트웨어의 취약점을 악용하는 것으로 유명합니다. 한 가지 주목할 만한 사례는 제로데이 취약점 CVE-2023-34362로, MOVEit Transfer 소프트웨어에 영향을 미쳤으며, MOVEit Transfer 웹 애플리케이션에 침투하기 위해 SQL 인젝션으로 시작했습니다. 최소 15개의 은행과 신용 조합에서 MOVEit 취약점으로 인한 데이터 유출을 확인했습니다. CL0P는 피싱을 비롯한 다른 기술을 통해서도 초기 접속 권한을 획득했으며 RaaS(Ransomware as a Service) 모델로 계속 실행되고 있습니다. 최근에는 금융 기관과 같은 표적에 대해 4중 갈취를 사용하는 방식으로 기법을 발전시켰습니다. 4중 갈취에는 3중 갈취와 관련된 기술 외에도 비즈니스 파트너, 직원, 고객, 고위 경영진, 미디어를 괴롭히는 메시지를 전송해 기업이 해킹당했다는 사실을 알리는 것도 포함됩니다. 그리고 이러한 기법으로 인해 랜섬웨어의 평균 지불액이 상승했습니다.

금융 기관을 표적으로 삼지만 랜섬웨어 그룹으로 분류되지는 않는 다른 핵티비스트 공격자로는 Anonymous Sudan, KillNet, NoName057(16) 등이 있습니다. 이들 모두 러시아-우크라이나 전쟁과 관련된 활동으로 유명하며, Anonymous Sudan은 이스라엘-하마스 전쟁에 대응하는 사이버 공격에 관여했다고 추가로 주장했습니다. 작년에 이들 그룹은 다른 수많은 공격자 그룹과 더불어 러시아-우크라이나 전쟁으로 인한 혼란을 이용해 주요 은행 인프라로 관심을 돌렸습니다.

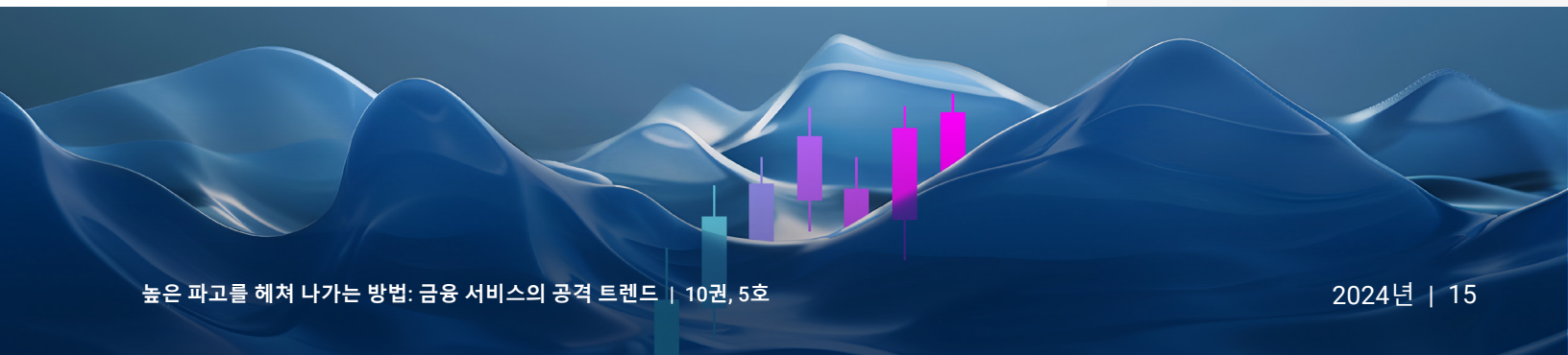
랜섬웨어 그룹으로 분류되지는 않았지만 금융 서비스 업계를 표적으로 삼는 것으로 알려진 다른 많은 공격자 그룹에는 Lazarus Group, MoneyTaker, Carbanak/FIN7, Cobalt, APT41 등이 있습니다.

이러한 공격자들의 지속적인 위협을 고려할 때, 금융 기관은 현재의 위협 환경을 인식하고 공격자의 동기와 기술을 더 잘 이해해 보다 효과적인 방어 전략을 개발해야 합니다. 이 보고서 뒷부분의 방어 조치 섹션에서 권장되는 보호 조치를 참조하세요.

최근 중동 지역에서 금융 기관을 대상으로 한 DDoS 핵티비즘 공격 발생

최근 중동의 금융 서비스 업계는 지정학적 긴장으로 인해 정교하고 지속적인 DDoS 공격이 급증하고 있습니다. 이러한 트렌드는 특히 EMEA(Europe, Middle East, Africa) 지역에서 널리 퍼져 있으며 금융 기관에 대한 정치적 동기를 가진 DDoS 공격의 위협이 증가하고 있음을 보여줍니다.

이러한 트렌드의 주목할 만한 사례에는 올해 초 친팔레스타인 핵티비스트 그룹인 BlackMeta(일명 DarkMeta)가 아랍에미리트(UAE)의 한 금융 기관을 대상으로 6일간 레이어 7 DDoS 공격을 감행한 사건이 있습니다. 이 공격은 DDoS 공격 대행 서비스인 InfraShutdown을 통해 이루어졌으며, 공격 툴의 접근성이 점점 더 높아지고 있음을 보여주었습니다. 2023년 11월부터 활동한 BlackMeta는 이스라엘, UAE, 미국의 기업을 표적으로 삼은 전력이 있습니다.



UAE 금융 기관에 대한 공격은 기간과 강도 면에서 모두 상당했습니다. 이 공격은 약 100시간 동안 진행되었으며 웹 요청 급증이 4~20시간 동안 지속되었고 초당 평균 450만 건의 요청이 발생했습니다. 이 공격으로 인해 은행은 70%의 시간 동안 공격을 받아 서비스에 상당한 영향을 받았습니다. BlackMeta의 은행 공격은 팔레스타인과 무슬림에 대한 부당함에 항의하기 위한 광범위한 노력의 일환이었으며, Anonymous Sudan이 사용한 것과 유사한 기법을 사용했습니다.

다행히 금융 기관의 방어 노력으로 더 큰 혼란을 막았지만 이 인시던트는 정치적 동기를 가진 사이버 공격이 증가하고 있는 트렌드를 보여줍니다. 또한 핵티비스트 그룹이 대규모 공격을 감행할 수 있는 장벽을 낮춰주는 DDoS 공격 대행 서비스가 증가하고 있다는 점도 강조합니다. 이러한 사건은 지속적인 대규모 위협을 방어하는 강력한 사이버 보안 조치의 필요성을 강조합니다.

2024년 7월 15일에는 정치적 동기에 의한 것으로 의심되는 또 다른 DDoS 공격이 발생해 이스라엘의 주요 금융 서비스 회사를 표적으로 삼았습니다. 전 세계에 분산된 봇넷에서 시작된 이 대규모 공격은 거의 24시간 동안 지속되었으며 최고 798Gbps에 달했습니다. Akamai는 DNS 반사, UDP 플러드 등 다양한 기법을 포함하는 레이어 3과 4에 대한 DDoS 공격을 성공적으로 방어했습니다.

이 공격이 진행되는 동안 Akamai는 3시간 동안 약 389테라바이트의 악성 트래픽을 집중적으로 차단했으며 전체 기간 차단된 총 트래픽은 약 419테라바이트에 달했습니다. 같은 날 이스라엘 금융 기관에서 또 다른 서비스 중단이 발생한 것은 조직적인 공격이 있었음을 시사하며, 지능형 DDoS 공격의 위협이 증가하고 있음을 더욱 강조합니다.

리소스를 충분히 보유한 이 공격자가 이전에 90일 동안 동일한 금융 서비스 고객을 27회 공격한 적이 있다는 사실에 주목할 필요가 있습니다. 이 고객은 이스라엘과 하마스의 전쟁이 시작된 2023년 4분기부터 반복적으로 DDoS 공격의 표적이 되었습니다. Akamai의 내부 DDoS 위협 인텔리전스 그룹은 2024년에 이스라엘의 기관과 기업이 전례 없는 수의 DDoS 공격을 경험했다고 보고했습니다. 이러한 지속적이고 공격적인 캠페인은 이러한 위협의 규모와 강도가 증가하고 있으며, 공격자들이 더욱 끈질기고 리소스가 풍부해지고 있다는 것을 분명히 보여줍니다.

친숙함을 이용한 공격: 금융 서비스의 브랜드 남용

금융 서비스가 고객 경험, 운영 효율성, 혁신, 전반적인 매출, 가시성을 향상시키기 위해 디지털 우선 접근 방식을 도입함에 따라 사이버 공격자들은 브랜드 사칭 사기를 통해 기업과 고객 간 형성된 신뢰를 악용하고 있습니다. 그림 7은 잘 알려진 금융 기관을 모방한 사기 사이트의 사례를 보여줍니다. 피싱과 브랜드 사칭은 일반적인 방법이지만, 사기 웹사이트의 수가 놀라울 정도로 많고 공격자가 원래 사이트를 오프라인으로 전환한 후 새로운 도메인을 만드는 속도가 빠르다는 점이 특히 우려스럽습니다. 이러한 급속한 확산은 금융 서비스 부문에 점점 더 큰 위협이 되고 있습니다.

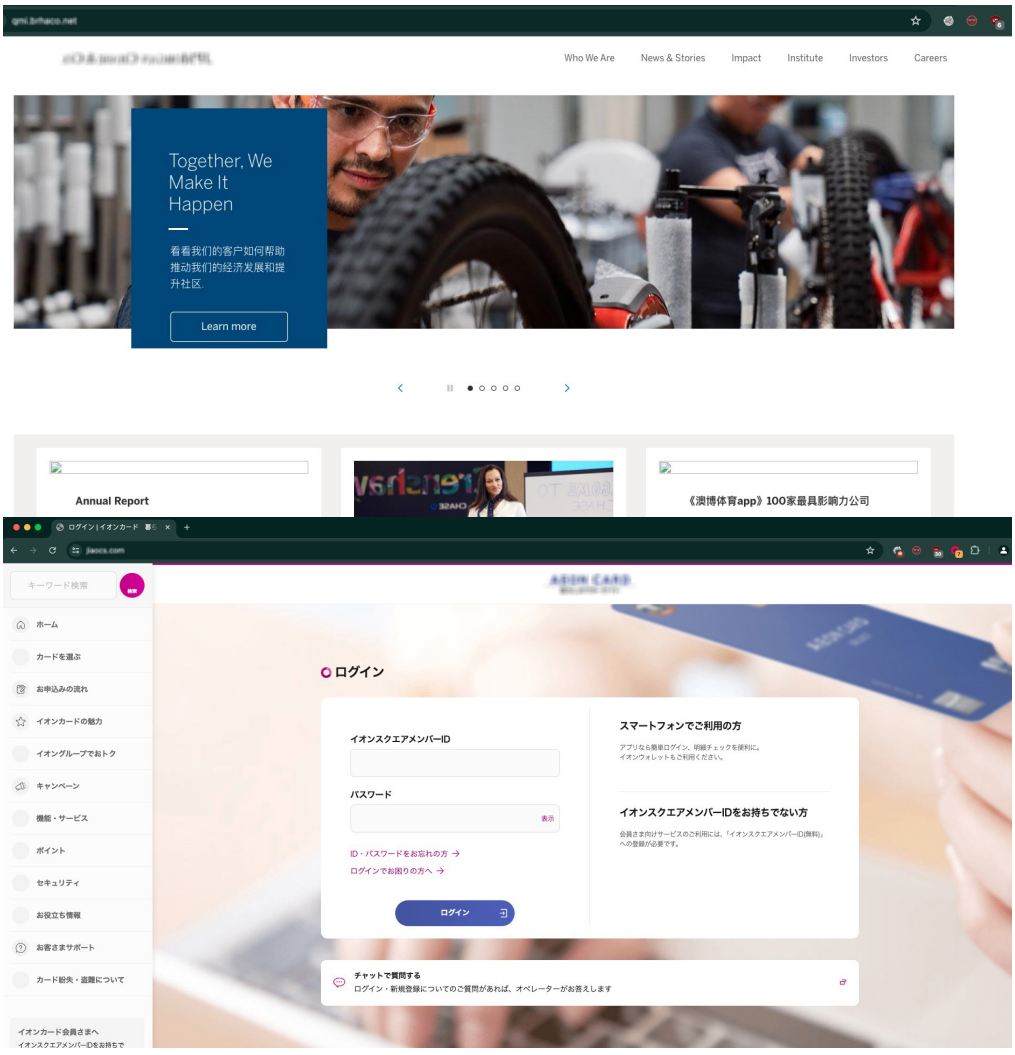


그림 7: 알려진 금융 기관을 모방한 사기 피싱 사이트의 샘플

피싱 서비스 플랫폼과 툴킷의 등장으로 브랜드 남용의 환경이 크게 변화했습니다. 이러한 리소스는 사이버 범죄자들의 진입 장벽을 낮춰 금융 서비스 및 고객을 대상으로 한 피싱 공격의 규모와 범위에 큰 영향을 미쳤습니다. Anti-Phishing Working Group은 2023년에 약 500만 건의 피싱 공격을 기록했으며, 2023년을 '역사상 최악의 피싱 해'로 규정했습니다.

브랜드 남용은 신원 도용 및 계정 남용과 같은 리스크를 확대하는 원동력이 될 수 있습니다. 공격자는 고객 정보를 다크웹에서 판매하거나 계정 탈취에 사용하는 경우가 많습니다. 보안 관점에서 브랜드 공격에 대한 조기 개입이 매우 중요합니다. 공격 수명 주기를 조기에 차단하면 공격자가 악의적인 목적으로 인증정보를 수집하는 것을 방지할 수 있습니다.

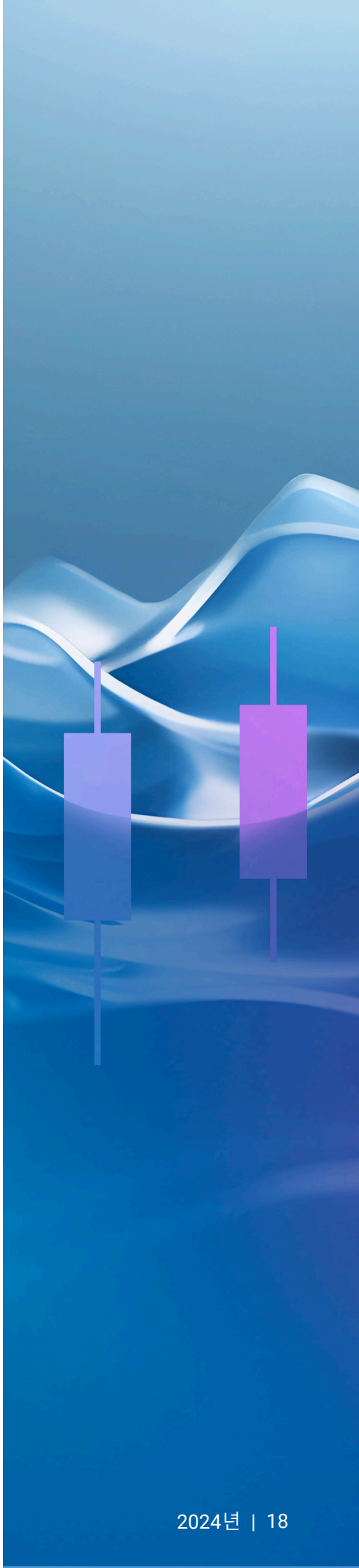
브랜드 남용의 파급 효과는 즉각적인 보안 문제를 넘어섭니다. 기업은 평판 손상, 컴플라이언스 및 법적 문제, 심지어 위조 제품으로 인한 매출 손실로 인해 상당한 금전적 손실을 입을 수 있습니다. 오늘날의 디지털 환경에서는 브랜드 사칭 공격을 조기에 탐지하는 것이 고객 신뢰와 비즈니스 연속성을 유지하는 데 가장 중요합니다.

기만 포인트: 사칭 공격 자세히 살펴보기

보안 팀은 다양한 온라인 플랫폼에서 발생할 수 있는 브랜드 남용을 방어해야 하는 어려운 과제에 직면해 있으며, 정상적인 사용자와 공격자 모두 디지털 자산에 접속할 수 있기 때문에 디지털 자산을 보호하기가 어렵습니다. 공격자는 온라인 뱅킹 포털과 같은 공개 자산의 콘텐츠를 스크레이핑해 자신만의 스푸핑 사이트를 만들고 철자가 틀린 도메인을 등록해 의심하지 않는 사용자를 속이는 경우가 많습니다. 또한 사이버 공격자는 피싱 이메일, 소셜 미디어 게시물 및 기타 디지털 채널을 통해 잠재적인 피해자를 악성 사이트나 가짜 앱으로 유인하는 캠페인을 시작합니다.

이 보고서에서 지난 12개월 동안 활성 도메인에서 관찰된 브랜드 사칭 및 피싱 활동을 분석해 금융 서비스를 중심으로 업계 전반에 걸친 브랜드 사칭의 확산에 대한 인사이트를 제공했습니다. Akamai의 포괄적인 가시성과 독점 솔루션은 다음과 같은 기능을 제공합니다.

- 마켓플레이스를 포함한 피싱 및 브랜드 사칭 사이트를 통한 트래픽 추적
- 활성 악성 도메인의 개수 파악
- 악성 도메인의 심각도 점수 평가



Akamai가 모니터링한 모든 의심스러운 사이트 중 가장 많이 사칭된 업계는 금융 서비스(36.25%)였습니다(그림 8). 이 결과는 특히 금융 서비스 업계가 브랜드 사칭 및 악용에 취약하다는 점을 강조합니다. 커머스(26.41%) 및 비즈니스 서비스(18.90%) 업계의 기업이 각각 2위와 3위를 차지했습니다.

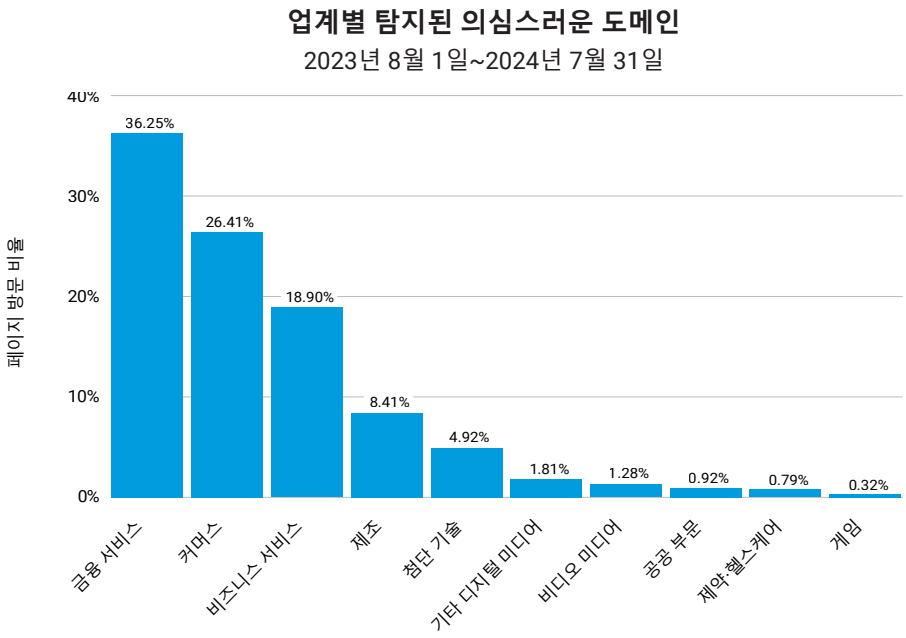


그림 8: 피싱 및/또는 브랜드 사칭 도메인 중 금융 서비스가 36.3%를 차지했습니다

금융 서비스 업계는 은행 인증정보 및 개인 식별 정보(PII)와 같은 방대한 양의 민감하고 가치가 높은 데이터를 보유하고 있기 때문에 브랜드 사칭 공격의 주요 표적이 되고 있습니다. 사이버 범죄자는 위조 은행 사이트에서 얻은 정보를 통해 손쉽게 계정에 접속해 계정을 탈취할 수 있습니다. 마찬가지로, 전자 지갑 및 암호화폐 계정의 인증정보(다크 웹에서 120~400달러에 거래됨)와 같은 다른 고가의 금융 정보도 얻을 수 있어 공격자는 계정에 있는 정보를 전송하거나 암시장에서 판매할 수 있습니다. 이러한 기법의 높은 수익률로 인해 금융 서비스는 브랜드 남용 및 피싱 공격의 주요 표적이 되고 있습니다.

마찬가지로 이커머스 및 온라인 쇼핑이 부상하면서 인증정보 및 기타 개인 정보를 빼낼 기회를 제공하는 커머스 기업도 브랜드 남용의 수익성 높은 표적이 되었습니다. 서비스를 제공하는 제조 기업과 써드파티 벤더사도 브랜드 남용에 똑같이 취약합니다. 디지털화는 전반적인 비즈니스 성장을 촉진하지만, 많은 기업에게 취약점이 되어 브랜드 사칭 공격의 확산과 피싱 시도의 증가로 이어지고 있습니다.

[브랜드 사칭] 기법의 높은 수익률로 인해 금융 서비스는 브랜드 남용 및 피싱 공격의 주요 표적이 되고 있습니다.

기업은 진화하는 디지털 환경에서 브랜드와 고객 모두를 보호하기 위해 경계를 늦추지 말고 보안 조치를 구축해야 합니다. 여기에는 브랜드 오용에 대한 지속적인 모니터링, 사기성 사이트에 대한 신속한 삭제 절차, 잠재적인 사칭 시도를 인식하기 위한 고객 교육 등이 포함됩니다. 이러한 노력에 우선순위를 두면 점점 더 복잡해지는 위협 환경에서 기업의 평판과 고객의 신뢰를 더욱 효과적으로 보호할 수 있습니다.

브랜드 남용의 표적이 된 금융 서비스

브랜드 사칭 및 피싱의 영향을 종합적으로 파악하기 위해 의심스러운 웹사이트의 페이지 방문 횟수도 분석했습니다. 그 결과, 금융 기관을 가장한 사이트가 30%, 커머스 기업을 모방한 사이트가 20%로 그 뒤를 이었습니다(그림 9). 이러한 결과는 요청 수로 측정하든 도메인으로 측정하든 금융 서비스와 커머스가 일관되게 상위권을 차지했습니다. 이러한 일관성은 해당 업계가 브랜드 남용 및 사칭의 주요 표적이 되고 있으며 그럴 만한 이유가 있다는 것을 보여줍니다.

금융 서비스에는 잘 알려진 은행부터 보안 리소스가 적은 소규모 기관까지 다양한 표적이 포함되며, 모두 높은 리스크에 노출되어 있습니다. 컴플라이언스 포럼(예: Payment Card Industry Data Security Council)에서 서비스 업계와 유사한 수준의 감시를 하고 있는 커머스 업계 역시 방대한 고객 정보를 보유하고 있기 때문에 상당한 리스크에 직면해 있습니다.

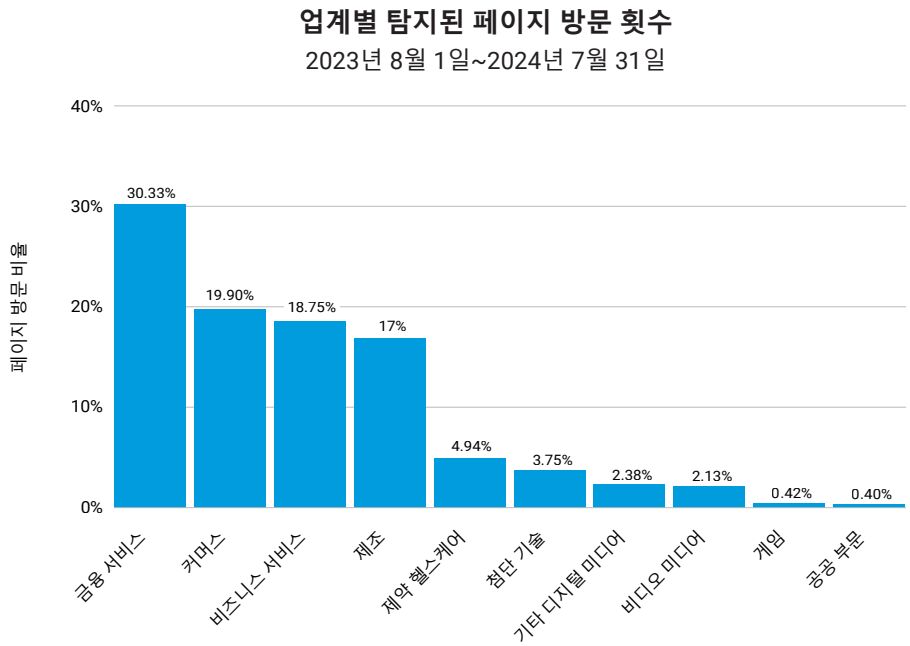


그림 9: 보고 기간(2023년 8월~2024년 7월) 동안 페이지 방문의 30% 이상이 정상적인 금융 서비스 사이트로 가장한 의심스러운 사이트로 이동했습니다.

흥미로운 점은 업계별로 도메인 사칭 순위와 실제 방문 횟수 사이에 약간의 차이가 있다는 것입니다. 예를 들어, 하이테크는 사칭 도메인 순위에서 상위 5위 안에 들었지만 실제 방문 횟수에서는 6위로 떨어졌습니다. 마찬가지로 제약 및 헬스케어를 사칭하는 도메인의 수는 적지만 이러한 도메인의 방문 횟수는 더 높습니다.

인증정보를 도용하기 위한 피싱

브랜드 남용은 정상적인 기업의 로고와 디자인을 그대로 베낀 유사 사이트, 사기성 앱, 기업 공식 계정을 모방한 가짜 소셜 미디어 프로필 등 다양한 형태로 이루어집니다. 이 문제의 정도를 파악하기 위해 위조 페이지를 분석해 브랜드 사칭, 피싱, 악성 앱, 가짜 스토어, 페이월 우회, 가짜 소셜 프로필 및 스토어 등의 종류로 분류했습니다. 모니터링하는 페이지에 따라 단일 기업의 도메인이 여러 가지로 분류될 수 있다는 점에 유의해야 합니다.

분석 결과, 금융 서비스 기관을 표적으로 하는 위조 도메인이 전체 기록된 사례의 무려 68%를 차지하며 피싱이 가장 많은 비중을 차지하고 있는 것으로 나타났습니다 (그림 10). 브랜드 사칭은 전체 기록된 도메인의 24%를 차지하며 2위에 올랐습니다. 사용자가 자주 방문하는 사이트 중에서는 피싱과 브랜드 사칭이 각각 1, 2위를 차지했습니다. 가짜 소셜 미디어 프로필이나 스토어와 같은 다른 형태의 브랜드 남용은 다른 업계에 비해 금융 기관에서 덜 심각합니다. 악성 앱을 노리는 공격은 줄어들었지만, 공격자가 공격 범위를 넓히기 위해 점점 더 창의적인 방법을 도입하고 있다는 점에 유의해야 합니다.

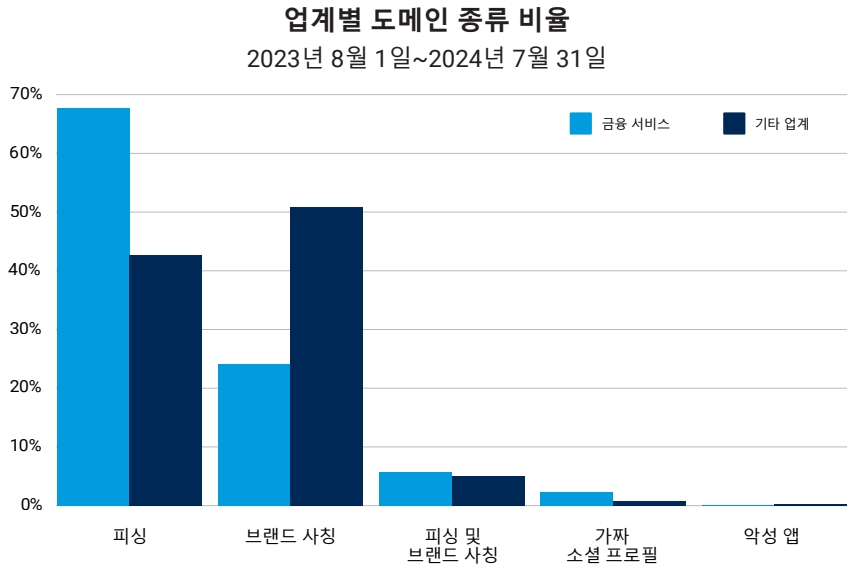


그림 10: 금융 서비스에 대해 기록된 도메인의 대부분은 피싱 웹사이트이며, 심지어 다른 모든 업계를 합친 것보다 더 많습니다.

금융 기관은 신뢰도가 높은 기관으로 인식되기 때문에 이러한 신뢰를 악용하는 사기꾼들의 주요 표적이 되고 있습니다.

피싱으로 인한 리스크에 대한 인식이 높아졌음에도 불구하고 인적 요소는 여전히 상당한 보안 공백으로 남아 있습니다. 이러한 격차는 공격자가 사용하는 정교한 기법(자세한 내용은 브랜드 남용 분석 섹션 참조)으로 인해 더욱 심화되며, 훈련되지 않은 사람의 눈으로는 가짜 페이지를 발견하기 어렵습니다. 금융 기관은 신뢰도가 높은 기관으로 인식되기 때문에 이러한 신뢰를 악용하는 사기꾼의 주요 표적이 됩니다. 공격자는 이러한 기관을 사칭해 사용자가 기꺼이 인증정보를 넘기도록 속이고, 기관의 평판을 활용해 사기를 더욱 설득력 있고 효과적으로 수행합니다.

기업과 고객을 모두 보호하려면 도메인 이름, 모바일 앱, 이메일 커뮤니케이션 등 브랜드의 무단 사용을 사전에 모니터링할 수 있는 브랜드 모니터링 기능을 갖춘 보안 기술을 사용해야 합니다. 무단 사용이 확인되면 다음 단계는 브랜드 남용 및 피싱으로 인한 리스크(데이터 도용 등)에 고객을 잠재적으로 노출시킬 수 있는 트래픽을 차단하는 조치를 취하는 것입니다.

사례 연구: 금융 기관에 대한 크리덴셜 스터핑 공격의 정교함 증가

미국의 한 핀테크 기업은 2023년과 2024년에 걸쳐 고객 대면 애플리케이션 중 하나를 표적으로 삼은 크리덴셜 스터핑 공격을 끊임없이 받았습니다. 이러한 공격의 규모는 엄청났으며, Akamai는 24시간 동안 탈취한 인증정보를 사용해 계정에 침투하려는 여러 IP 주소에서 3000건 이상의 알림을 탐지했습니다. Akamai는 한 IP 주소가 최소 115개의 사용자 이름과 비밀번호 조합을 시도하는 것을 관찰했습니다. 2024년 7월에는 총 10만 건 이상의 알림을 기록했습니다.

심각한 리스크 수준의 사기 금융 서비스 사이트

글로벌 엣지의 독점적인 인텔리전스와 써드파티 위협 인텔리전스의 추가 데이터 피드를 결합하면 브랜드 사칭을 탐지하는 데 뚜렷한 장점이 있습니다. Akamai는 포괄적인 시스템을 사용해 위협 점수를 기반으로 각 도메인을 꼼꼼하게 검사하고 분류합니다.

위협 점수는 세 가지 주요 요인을 사용해 계산합니다.

1. **신뢰도 점수** - 이벤트가 피싱 시도라고 확신하는 정도
2. **심각도 수준** - 이벤트와 관련된 리스크 정도(심각, 높음, 중간, 낮음)
3. **빈도 요소** - 주어진 기간 내에 사이트와 관련된 이벤트 및 세션 수

Akamai의 점수 시스템은 신뢰도, 심각도, 빈도라는 세 가지 주요 요인의 균형을 맞추고 있습니다. 이러한 점수를 결합해 각 의심스러운 도메인에 대해 포괄적인 위협 점수(최고 점수: 99점)를 생성해 잠재적인 위협에 대한 종합적인 평가를 보장합니다.

최근 분석에 따르면 금융 서비스 부문의 위협 점수 중앙값이 85점으로 금융 업계가 계속해서 심각한 리스크에 직면하고 있는 것으로 나타났습니다(그림 11). 이 점수는 금융 기관이 방대한 양의 민감한 데이터를 집요하게 노리는 사이버 범죄자의 표적이 되고 있음을 의미합니다.

업계별 위협 점수

업계	위협 점수 중앙값	업계	위협 점수 중앙값
공공 부문	**95**	게이밍	**65**
금융 서비스	**85**	제조	**64**
비즈니스 서비스	**85**	기타 디지털 미디어	**62**
제약 헬스케어	**85**	커머스	**61**
비디오 미디어	**71**	첨단 기술	**60**

그림 11: 위협 점수 중앙값을 계산한 결과 금융 서비스가 놀라울 정도로 높은 점수를 받았습니다.

민감한 정보가 많고 보안 리소스가 제한되어 있기 때문에 공공 부문이 가장 높은 위협 점수 중앙값을 기록했지만, 금융 서비스 역시 공격자가 막대한 금전적 이득을 얻을 수 있는 잠재력을 가진 매력적인 표적이 되고 있습니다. 비즈니스 서비스와 제약 및 헬스케어와 같은 분야도 비슷한 점수를 기록하며 사이버 범죄자가 표적을 다양화하고 있지만 데이터의 중요성으로 인해 금융 기관이 여전히 주요 표적이 되고 있습니다.

이처럼 위협 수준이 높기 때문에 위협이 심각한 금전적, 평판 피해로 이어지기 전에 즉시 조치를 취해 방어를 강화하고 진화하는 위협을 방어해야 합니다.

브랜드 남용 분석

사기 및 브랜드 남용의 성공 여부는 소셜 엔지니어링 미끼로서 브랜드가 가진 힘에 크게 좌우됩니다. 공격자는 소비자가 유명 브랜드에 대해 갖는 친숙함과 내재된 신뢰감을 이용해 정상적인 웹사이트를 매우 유사하게 모방한 가짜 웹사이트를 설계합니다. 경우에 따라 사기꾼은 정확한 코드를 복사해 불법 사이트를 실제 사이트와 거의 동일하게 보이게 만들기도 합니다. 사기꾼들이 철자와 문법 오류를 제거하는 데 도움이 되는 생성형 AI 툴이 등장하면서 소비자들이 진짜 사이트와 가짜 사이트를 구별하기가 더욱 어려워졌습니다.

피싱 및 사칭 캠페인의 규모는 피싱 툴킷의 존재로 인해 더욱 악화되었습니다.

피싱 및 사칭 캠페인의 규모는 피싱 툴킷의 존재로 인해 더욱 악화되었습니다. 공격자는 50달러만 있으면 피싱 툴킷을 구매해 그럴듯한 피싱 사이트를 만들 수 있습니다. 피싱 툴킷을 개발하고, 구축하고, 판매하는 사이버 범죄 기업은 피싱 및 사칭 캠페인을 실행하는 진입 장벽을 크게 낮추고 있습니다. 대표적인 피싱 툴킷으로 Kr3pto와 16Shop이 있습니다. Kr3pto는 2단계 인증을 우회해 영국 은행을 표적으로 삼았고, 16Shop은 PayPal, Amazon 등 주요 브랜드에 집중했습니다. 2023년 8월, 국제 사법 기관의 작전으로 16Shop의 제작자가 체포되었습니다. 이러한 사례는 피싱 공격의 정교함이 진화하고 있으며 사이버 범죄에 대응하기 위해 공동의 노력이 필요하다는 점을 강조합니다.

과소평가되었지만 효과적인 콤보스쿼팅

브랜드 남용의 또 다른 중요한 측면은 정상적인 웹사이트와 매우 유사한 도메인 이름을 사용한다는 점입니다. 일반적으로 공격자는 자체 피싱 사이트를 구매하거나 구축한 후 도메인을 등록합니다. 이때 사이버스쿼팅과 그의 다양한 변종처럼 검증된 기술이 중요한 역할을 합니다. 한 가지 일반적인 기법은 타이포스쿼팅으로, 공격자는 소비자가 오타를 내기를 바라며 회사 이름의 철자를 약간 변경한 도메인(예: acamai[.]com)을 등록합니다. 또 다른 방법인 콤보스쿼팅은 도메인 이름에 'support', 'login' 또는 'help' 등의 키워드를 추가합니다. 이 기법은 정상적인 회사 웹사이트에서 흔히 볼 수 있는 마이크로사이트를 활용합니다.

Akamai의 리서치에 따르면 콤보스쿼팅(키워드 추가) 기법은 잘 알려지지 않았지만 활성 도메인 수에서 타이포스쿼팅(문자 추가, 제거, 교체)을 능가하는 것으로 나타났습니다. 흥미롭게도 사기 사이트에 가장 많이 추가된 키워드 중 하나가 'com'이었습니다.

소비자가 사칭 사이트를 식별하기 어렵게 만드는 다른 기법도 관찰되고 있으며, 이러한 기법은 공격의 성공률을 높일 수 있습니다.

배포 메커니즘

위조 및 피싱 웹사이트는 다양한 메커니즘을 통해 전달되고 판매되는데, 그중 가장 대표적인 메커니즘은 이메일입니다. 이러한 이메일 메시지는 정상적인 로고를 사용해 그럴듯하게 보이며 계정 정보 업데이트 요청과 같은 긴급한 메시지를 담고 있습니다. 그러나 브랜드 남용은 웹사이트와 이메일에만 국한되지 않습니다. 공격자는 소셜 미디어를 통해서도 위협을 퍼뜨리며 그 범위와 속임수 기법을 더욱 확장하고 있습니다.

잘 보이는 곳에 숨겨진 링크

소비자가 사칭 사이트를 식별하기 어렵게 만드는 다른 기법도 관찰되고 있으며, 이러한 기법은 공격의 성공률을 높일 수 있습니다. 예를 들어 SMS에 단축 URL, QR 코드, 이미지 하이퍼링크, 텍스트 링크를 사용해 악성 링크를 난독화합니다. 이러한 악용을 방지하는 스팸 필터가 있는 이메일과 달리 문자 사기는 차단되지 않을 가능성이 높으며 읽거나 열어볼 가능성이 높습니다.

금융 서비스의 지역 피싱 및 브랜드 사칭 공격

브랜드 남용은 전 세계 기업과 소비자에게 영향을 미치지만, 일부 지역은 브랜드 사칭 및 피싱 사이트로의 트래픽 집중으로 인해 사기 및 도용에 더 취약한 것으로 나타났습니다. 분석 결과, 지난 12개월 동안 탐지된 피싱 및 사칭 사이트로의 트래픽이 가장 많은 지역은 EMEA 지역으로, 심지어 북미 지역을 능가하는 것으로 나타났습니다(그림 12). 이 순위는 금융 서비스 및 기타 업계를 모두 포함합니다.

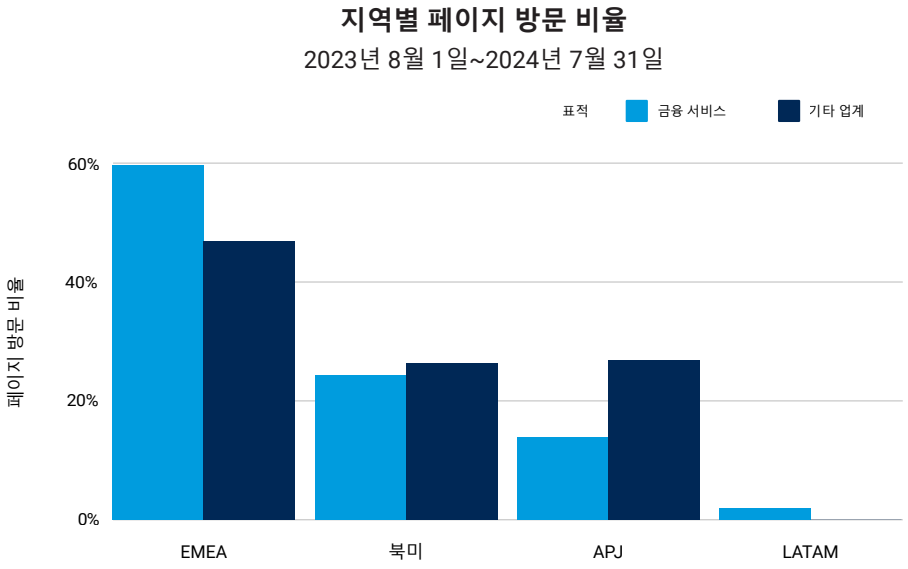


그림 12: 금융 서비스 분야에서 피싱 및 브랜드 남용의 영향을 가장 많이 받는 지역은 EMEA로 북미를 뛰어넘었습니다

라틴 아메리카와 아시아 태평양 및 일본(APJ) 지역의 페이지 방문 건수는 상대적으로 적었지만 공격이 적었다는 것을 의미하지는 않습니다. 오히려 이러한 결과는 북미와 EMEA 지역에 대규모 고객 기반을 보유한 글로벌 브랜드가 집중되어 있기 때문일 가능성이 높습니다. 이는 공격자가 공격할 수 있는 잠재적 피해자의 풀이 더 커진다는 것을 의미합니다. 또한 2023년부터 유럽 은행을 표적으로 삼은 V3B와 같은 피싱 툴킷이 등장한 것도 이러한 결과에 영향을 미쳤을 수 있습니다.

의심스러운 도메인과 페이지 방문 횟수에서는 EMEA가 대부분의 지역을 앞섰지만 위협 점수 중앙값은 97로 아시아 태평양 및 일본이 가장 높았습니다. 라틴 아메리카는 사이트 방문 횟수가 가장 적음에도 불구하고 위협 점수 중앙값이 94점이라는 놀라운 수치를 기록했습니다. 이는 라틴아메리카와 아시아 태평양 및 일본의 소비자들이 웹사이트 방문 시 은행 정보 및 기타 민감한 데이터를 도난당할 리스크가 더 높다는 것을 의미합니다.

아시아 태평양 및 일본에서 금융 서비스에 대한 브랜드 남용의 리스크가 증가하는 데에는 몇 가지 요인이 있습니다. 첫째, 아시아 태평양 및 일본의 대부분의 금융 서비스 기관은 고도로 디지털화되어 있어 실제 지점을 방문하지 않고 거의 모든 서비스를 온라인으로 이용할 수 있습니다. 아시아 태평양 및 일본의 인터넷 보급률과 디지털 도입률은 전 세계에서 가장 높은 수준이기 때문에 사이버 범죄자에게 매력적인 표적이 되고 있습니다. 둘째, 아시아 태평양 및 일본에는 전 세계에서 소셜 미디어가 가장 활발히 사용되는 국가들이 있습니다. 그리고 금융 서비스 기관들은 시장 점유율 경쟁과 고객 충성도 향상을 위해 소셜 미디어 플랫폼을 통한 고객 참여를 강화하고 있습니다. 아시아 태평양 및 일본에서 소셜 미디어와 메시징 앱이 널리 사용됨에 따라 사이버 범죄자는 소셜 미디어 플랫폼에 대한 사람들의 신뢰를 악용해 피싱 및 사칭 공격을 수행할 수 있는 추가 기법을 이용할 수 있습니다.

진화하는 컴플라이언스: 글로벌 사이버 보안 규정이 금융 기관을 변화시키는 방법

악명 높은 은행 강도 윌리 서튼(Willie Sutton)은 왜 은행을 털었느냐는 질문에 "돈이 있는 곳이기 때문"이라고 대답한 것으로 유명합니다. 서튼의 이 말은 오늘날 금융 기관에 대한 사이버 공격에도 쉽게 적용될 수 있습니다. 그러나 금전적 이득이라는 동기는 이야기의 일부분일 뿐입니다. 금융 기관은 지정학적 전략적 동기뿐만 아니라 정치적 우려에 의해 동기를 부여받은 공격자로부터 점점 더 많은 공격을 받고 있습니다. 금융 기관이 가장 많이 공격받는 업계로 부상하고 있는 가운데 이러한 동기는 '돈이 있는 곳'이라는 사실과 결합해 금융 기관에 완벽한 폭풍을 일으키고 있습니다.

이는 놀라운 일이 아닙니다. 금융 업계는 항상 사회에서 중요하고 중심적인 역할을 해왔으며 상당한 규제의 대상이 되어 왔습니다. 과거 금융 기관에 대한 규제는 금융 기관과의 거래에서 소비자를 보호하는 데 중점을 두었지만, 이제 규제 당국은 금융 기관과 서비스 회사에 중요 인프라 스타일의 보안 및 안정성 규제를 적용하려고 합니다. 이러한 새로운 트렌드에는 금융 기관 자체뿐만 아니라 ICT 공급업체에 대한 요구사항도 포함됩니다.

사이버 보안 및 운영 안정성 규제의 사례는 무수히 많습니다. 유럽연합에서는 DORA에 따라 금융 기관과 공급업체가 강력한 ICT 리스크 관리 프레임워크를 갖추고 정기적인 테스트와 인시던트 보고를 수행하도록 의무화하고 있습니다. 미국에서는 SEC(Securities and Exchange Commission)가 금융 기관을 포함한 상장 기업이 운영에 중대한 영향을 미칠 수 있는 사이버 인시던트를 공개하도록 요구하는 사이버 중대성 규제를 도입했습니다. 호주에서는 APRA(Australian Prudential Regulation Authority)가 기업에 정보 자산에 대한 위협의 규모와 정도에 상응하는 정보 보안 기능을 유지할 것을 요구하는 표준을 제정했습니다(규정 CPS 234). 이러한 사례는 진화하는 리스크를 차단하고 금융 안정성을 보장하기 위해 금융 부문의 사이버 보안 및 운영 안정성을 강화하려는 글로벌 트렌드를 보여줍니다.

이러한 규제를 고려하면 금융 기관은 ICT 및 보안 서비스를 구매할 때 실사를 통해 공급업체가 이러한 엄격한 기준을 준수하는지 확인해야 합니다. 안정적인 서비스를 제공할 뿐만 아니라 관련 규제를 이해하고, 진화하는 위협을 식별 및 방어하는 데 필요한 가시성을 제공하고, 해당 인텔리전스를 지속적인 운영에 적용하는 데 도움을 주는 공급업체를 선택해야 합니다.

자신이 가지고 있는 것 또는 연결되어 있는 것을 알지 못하면 보호할 수 없고, 존재하는지도 모르는 위협을 방어할 수 없기 때문에 가시성이 중요합니다. Akamai Guardicore Platform과 같은 서비스는 공격에 대한 방어뿐만 아니라 고객이 데이터 흐름을 이해하고, 비정상을 식별하고, 네트워크 자산을 적절히 분류해 위협을 방어할 수 있도록 지원합니다. 마찬가지로 API 보안 서비스는 API 트래픽을 식별해 섀도 API를 지원할 뿐만 아니라 API를 통한 잠재적 공격을 인식하도록 설계되었습니다.

은행은 기존의 CIA 3요소(기밀성, 무결성, 가용성)에 가시성을 추가해 가시성, 기밀성, 무결성, 가용성이라는 새로운 트렌드인 VCIA(Visibility, Confidentiality, Integrity, Availability)를 반영해야 합니다.

제임스 케이시(James Casey)
Akamai 부사장,
최고 개인정보 보호 책임자

제로 트러스트로 방어 강화

신뢰는 금융 기관의 평판을 구축하는 기반이 됩니다. 하지만 복잡한 환경과 기밀 데이터를 보호하는 데 있어 신뢰는 큰 부담이 될 수 있습니다. 공격자는 다음과 같은 다양한 방법으로 암묵적 신뢰를 악용합니다.

- 기업 내 개인을 사칭하는 피싱 공격
- 써드파티 공급업체의 보안 취약점을 악용해 가치가 높은 표적에 접근하는 공격
- 악의적인 목적으로 접속을 악용하는 내부자 위협

공격이 점점 더 정교해짐에 따라 내부 모든 트래픽을 신뢰할 수 있는 것으로 간주하는 기존의 경계 기반 보안이 부적절해졌습니다. 금융 서비스의 높은 위험도를 고려하면 안정적인 보안 체계를 유지하는 것이 매우 중요합니다. 바로 이 점에서 제로 트러스트 프레임워크가 필수적입니다. 제로 트러스트 보안 접근 방식은 모든 연결 요청, 사용자 또는 디바이스가 잠재적인 리스크 요소라는 원칙에 따라 작동합니다. 지속적으로 검증하고 암묵적 신뢰를 제거해, 요청자가 인증되고 권한이 부여되지 않으면 기본적으로 리소스에 대한 접속을 거부합니다.

제로 트러스트는 규제 대상 데이터를 처리하는 시스템을 보호해 금융 기관에 대한 진화하는 규제 요구사항을 준수하고 감사 실패로 인한 불이익을 피할 수 있도록 합니다. 또한 레거시 시스템에 대한 추가 제어 기능을 제공해 중요한 애플리케이션에 접속하려는 권한이 없는 사용자를 탐지할 수 있는 정밀한 가시성을 제공합니다.

제로 트러스트 모델은 중요 시스템에 대한 네트워크 접속을 제한하고 랜섬웨어와 같은 위협의 측면 이동을 방지해 동서 트래픽을 제한합니다. 이 격리 전략은 감염된 시스템을 격리해 필수 데이터와 자산을 보호합니다. 금융 서비스에 대한 랜섬웨어 공격이 크게 증가함에 따라 민감한 정보를 보호하는 데 있어 제로 트러스트의 중요성은 아무리 강조해도 지나치지 않습니다. 제로 트러스트는 정밀한 가시성을 통해 복잡한 환경 내에서 위협을 탐지하고 무력화하기 때문에 랜섬웨어 확산을 방지하고 중요 자산을 보호하는 데 매우 중요합니다.

제로 트러스트의 또 다른 장점은 클라우드 기반 애플리케이션의 안전한 배포에 필수적인 애플리케이션 간의 데이터 흐름을 보호할 수 있다는 것입니다. 이는 최신화를 촉진할 뿐만 아니라 끊임없이 변화하는 위협 환경에서 기밀 정보를 보호하기 때문에 금융 기관은 보안을 희생하지 않고 혁신할 수 있습니다. 제로 트러스트 프레임워크를 구축하면 보안 체계를 강화하고 진화하는 위협에 대응하는 미래를 만들어 나갈 수 있습니다.

세그멘테이션보다 더 효과적인 마이크로세그멘테이션

세그멘테이션은 성능과 보안을 강화하기 위해 네트워크를 더 작은 세그먼트로 나누는 아키텍처 접근 방식입니다. 마이크로세그멘테이션은 네트워크를 개별 워크로드 수준까지 논리적으로 별개의 보안 세그먼트로 나눌 수 있는 보안 기술입니다. 그리고 고유한 각 세그멘테이션에 대해 보안 제어 및 서비스 전송을 정의할 수 있습니다.

마이크로세그멘테이션은 제로 트러스트의 근간이기도 합니다. 최근 Akamai 보고서에서 금융 서비스 사이버 보안 리더들은 세그멘테이션 프로젝트를 구축하는 가장 큰 동인으로 제로 트러스트의 발전을 꼽았습니다. 실제로 세그멘테이션을 도입한 거의 모든 리더가 제로 트러스트 보안 프레임워크를 배포 중이거나 이미 배포한 경험이 있지만(99%), 절반 미만(47%)만이 제로 트러스트 프레임워크가 완전히 완성되고 정의되어 성숙했다고 응답했습니다.

마이크로세그멘테이션은 기존 시스템과 함께 작동하며 방화벽과 같은 기존 방법보다 빠르게 배포할 수 있습니다. 이 접근 방식은 랜섬웨어 대응 속도를 최대 13시간까지 단축하고 모든 IT 환경에서 관리를 간소화합니다. 또한 정밀한 데이터 제어를 통해 컴플라이언스 요구사항을 충족하는 데 도움이 됩니다.

실제 사례에서 최신 마이크로세그멘테이션의 효과를 볼 수 있습니다. 한 프로젝트에서 단 한 명의 엔지니어로 구축 시간을 2년에서 6주로 단축하고 비용은 85% 절감했습니다. 이 사례는 마이크로세그멘테이션이 기업의 시간과 비용을 어떻게 절약할 수 있는지 보여줍니다. IT 책임자는 이러한 결과를 현재 보안 비용 및 구축 시간과 비교해야 합니다.

금융 기관은 사이버 보안 체계를 강화하기 위해 고급 세그멘테이션 전략 구축에 우선순위를 두어야 합니다. CISO는 강력한 제로 트러스트 아키텍처의 초석으로 마이크로세그멘테이션을 통합해 진화하는 업계 표준에 맞춰 보안 조치를 조정하는 노력을 주도해야 합니다. IT 책임자는 정기적인 보안 감사 및 전략 업데이트 주기를 설정해 정교한 사이버 위협에 대한 안정성을 유지할 수 있도록 해야 합니다.

이러한 사전 예방적 접근 방식은 현재의 취약점을 방어하는 데 도움이 될 뿐만 아니라 기업이 새로운 사이버 보안 과제에 효과적으로 대응할 수 있는 기반을 마련합니다. 금융 기관은 이러한 조치를 도입함으로써 즉각적인 우려 사항과 장기적인 리스크 관리를 모두 해결하는 포괄적인 보안 프레임워크를 구축할 수 있습니다.

[마이크로세그멘테이션]은 현재의 취약점을 방어할 뿐만 아니라 기업이 새로운 사이버 보안 과제에 효과적으로 대응할 수 있도록 지원합니다.

방어

다양한 사이버 위협으로부터 금융 기관을 보호하려면 다각적인 접근 방식을 구축해야 합니다. 피싱, 브랜드 사칭, DDoS 공격, 랜섬웨어에 대한 주요 방어 전략을 살펴보겠습니다.

피싱 및 브랜드 사칭 방지

피싱 및 브랜드 사칭으로부터 금융 기관을 보호하려면 써드파티 브랜드 보호 서비스를 사용해 사기성 콘텐츠를 신속하게 탐지하고 삭제하는 것을 고려하세요. 직원과 고객도 교육해야 합니다. 피싱 및 사칭 시도를 인식하는 방법에 대한 직원 대상 보안 인식 교육을 정기적으로 실시하고 금융 기관에서 보낸 정상적인 커뮤니케이션을 식별하는 방법에 대해 명확한 가이드를 제공하세요. 그리고 파트너와 고객에게 ID 사기에 대해 알리는 프로세스를 포함해 사칭 시도에 대한 신속한 대응 계획을 수립하세요.

또한 다음과 같은 보안 기술을 구축하세요.

- 유사 도메인 이름을 등록해 타이포스쿼팅을 방지하고 도메인 모니터링 서비스를 사용해 유사 도메인을 탐지하세요.
- 강력하고 고유한 비밀번호와 비밀번호 관리자를 사용해 인증 프로토콜을 강화하고, 모든 계정과 시스템에 대해 강력한 멀티팩터 인증(MFA)을 구축하세요.
- 이메일 스푸핑을 방지하기 위해 SPF(Sender Policy Framework), DKIM(DomainKeys Identified Mail), DMARC(Domain-Based Message Authentication, Reporting and Conformance) 등의 이메일 인증 프로토콜을 배포하세요. 피싱 방지 솔루션과 고급 이메일 필터링을 사용해 악성 이메일을 탐지하고 차단하세요.
- SSL 인증서를 획득하고, HTTPS를 구축하고, 사기 방지 툴을 사용해 웹사이트와 모바일 앱에서 의심스러운 활동을 탐지함으로써 웹사이트와 디지털 채널을 보호하세요.
- 보안 포털을 제공하고 민감한 서신은 암호화된 메시징을 구축해 커뮤니케이션 채널을 보호하세요.

DDoS 방어

DDoS 공격으로부터 금융 기관을 보호하려면 멀티레이어 방어 전략이 필요합니다. 전문 DDoS 탐지, 방어 및 보호 제품 사용, 전송률 제한 설정, CDN에 콘텐츠 캐싱과 같은 사전 예방적 전략을 구축하세요. 또한 패치 관리, 인시던트 대응 계획, DDoS에 노출된 IP 주소 및 중요 서브넷에 대한 방어 제어, 접속 제어 정책, 네트워크 세그멘테이션, 방화벽 등의 보안 조치에 대한 정보를 지속적으로 파악하세요. 전송률 제한 설정, CDN에서 콘텐츠 캐싱, 전문 DDoS 탐지, 방어, 보호 제품 사용과 같은 사전 예방적 전략을 구축하세요.

DNS 인프라를 보호하려면 인바운드 DNS 트래픽을 지속적으로 모니터링 및 분석하고 기존 DNS 방화벽이 아닌 하이브리드 플랫폼을 선택해야 합니다. 공격자가 사용하는 기법, 기술, 절차를 이해하면 더 효과적으로 DDoS 공격을 방어할 수 있습니다.

랜섬웨어 방어

앞서 언급했듯이 네트워크 세그멘테이션, 특히 마이크로세그멘테이션을 통해 제로 트러스트를 달성하는 것은 금융 기관 전체에 랜섬웨어가 확산되는 것을 제한하는 데 매우 중요합니다. 이와 같은 강력한 사이버 보안 조치를 구축하면 랜섬웨어 공격자가 사용하는 고급 기술에 대응하는 데 도움이 됩니다. 또한 경계를 늦추지 말고 MITRE ATT&CK 프레임워크를 사용해 공격자가 사용하는 일반적인 기법과 기술에 대한 인사이트를 얻고 그에 따라 플레이북을 강화해 랜섬웨어 킬 체인을 끊어야 합니다.

지속적으로 방어를 업데이트하고 직원들이 잠재적인 위협을 인식하고 효과적으로 대응할 수 있도록 교육하고 강력한 경계 방어, 엔드포인트 보호, 이메일 필터링, 정기적인 패치 관리를 통합하세요. 그리고 네트워크 트래픽, 시스템 로그, 사용자 행동에 대한 지속적인 모니터링을 수립하고 랜섬웨어 위협을 선제적으로 식별하는 위협 탐지 관행을 구축하세요.

에어 갭 백업을 포함한 정기적이고 안전한 데이터 백업을 구축해 랜섬웨어 공격 시 중요한 정보를 신속하게 복원할 수 있도록 하고 모든 사용자 계정에 MFA를 구축해 보안 레이어를 추가하세요.

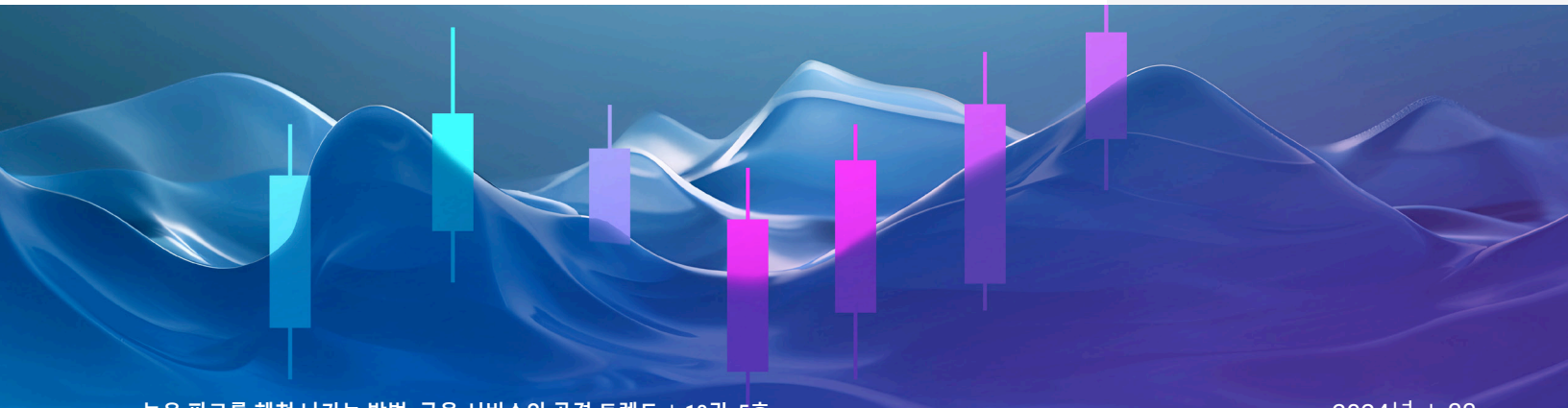
이러한 포괄적인 방어 전략을 구축하면 금융 기관이 다양한 사이버 위협을 방어하고, 운영 연속성을 보장하고, 평판을 보호하고, 고객 신뢰를 유지하는 능력을 크게 향상시킬 수 있습니다.

결론

금융 기관이 고객 경험, 운영 효율성, 경쟁력 강화를 위해 디지털 혁신을 진행하면서 보안 도전과제가 더욱 심화되고, 규제 환경 변화를 헤쳐 나가야 하는 압박도 가중되고 있습니다. 이번 SOTI 보고서에서는 금융 서비스 업계가 직면하고 있는 끈질기고 새로운 위협을 살펴보고 보안 솔루션에 대한 지속적인 평가와 개선의 필요성을 강조했습니다. 위협이 더욱 정교해짐에 따라 방어를 강화하고 보안 전략을 개선해 앞서 나가야 합니다.

금융 기관에 대한 DDoS 공격이 오랫동안 최고의 표적으로 여겨지던 게임 업계를 넘어선 것은 이러한 리스크 증가 트렌드가 얼마나 심각한지를 보여줍니다. 핵티비즘과 지정학적 환경과 같은 요인으로 인해 그 어느 때보다 금융 서비스가 취약해졌습니다. 이와 함께 금융 기관을 표적으로 삼는 브랜드 사칭 및 피싱 사이트에서 발생하는 트래픽의 규모와 심각성은 물론 공격자가 초기 사이트가 다운된 후 새로운 도메인을 생성하는 속도도 주목할 만합니다. 이러한 활동을 추적하는 데 기업의 많은 리소스가 소요될 수 있으므로 보안 팀은 여러 디지털 채널에서 브랜드 사칭 및 피싱을 탐지하고 차단 서비스와 위협 인텔리전스를 포함하는 솔루션이 필요합니다.

소비자와 규제 기관은 피싱 및 기타 사기의 피해를 입은 후 직접적인 잘못이 없는 경우에도 금융 기관에 책임을 묻는 경우가 많습니다. 더 중요한 것은 피싱과 브랜드 사칭이 더 위험한 공격의 전조로 작용하는 경우가 많기 때문에 공격 주기를 조기에 차단해야 한다는 점입니다. 단호한 조치를 취하면 기관의 평판과 고객의 신뢰를 보호할 수 있고 단호한 조치를 취하지 않으면 유출 사고로 인해 내일 헤드라인을 장식할 수 있습니다.



금융 기관에 대한 공격이 지속적이라는 점을 고려하면 사기 및 악용을 방지하기 위해 기밀 정보를 보호하는 것은 여전히 어려운 도전 과제입니다. 직원을 노리는 피싱 공격을 효과적으로 방어하고 랜섬웨어가 네트워크 내에서 확산되어 중요 자산에 도달하는 것을 방지하는 동시에 기존 및 새로운 글로벌 규정을 준수하려면 제로 트러스트와 같은 보안 프레임워크를 도입하는 것이 필수적입니다.

이 보고서는 금융 서비스 업계의 최신 공격 트렌드에 대한 실행 가능한 인사이트를 제공해 방어를 강화할 수 있도록 지원합니다. 경계를 늦추지 않고 이 보고서에서 설명하는 전략을 구축하면 증가하는 위협 환경으로부터 기업과 고객을 더 효과적으로 보호할 수 있습니다.

Akamai의 보안 리서치 허브에서 최신 리서치를 확인하세요.

방법론

DDoS(레이어 7)

이 데이터는 웹 애플리케이션 방화벽(WAF)을 통해 관측된 트래픽에 대한 애플리케이션 레이어 알림을 설명합니다. L7 DDoS 알림은 보호하고 있는 웹사이트, 애플리케이션, API에 대한 요청 건수에서 대규모 비정상을 탐지하면 트리거됩니다. 이러한 알림은 악성 요청과 정상 요청 모두에 의해 트리거될 수 있습니다. 일반적으로 요청 자체는 정상이지만 요청의 양이 많다는 것은 악의적인 의도가 있음을 시사합니다. 알림이 트리거됐다고 해서 공격이 성공한 것은 아닙니다. 이러한 제품은 높은 수준의 사용자 맞춤화가 가능하지만 Akamai가 여기에 제공한 데이터는 프로퍼티의 맞춤형 설정을 고려하지 않는 방식으로 수집했습니다.

이 데이터는 130여 개국 약 1300개 네트워크, 4000개 이상의 위치, 약 34만 대의 서버로 구성된 Akamai Connected Cloud에서 탐지된 보안 이벤트를 분석하는 내부 툴에서 추출한 것입니다. Akamai 보안 팀은 매달 페타바이트 규모의 데이터를 활용하여 공격을 연구하고, 악성 행동을 식별하며, Akamai 솔루션에 인텔리전스를 추가합니다.

이 데이터는 2023년 1월 1일부터 2024년 6월 30일까지 18개월 동안 수집되었습니다.

DDoS(레이어 3, 4)

Akamai Prolexic Routed는 모든 포트와 프로토콜을 포함해 애플리케이션, 데이터 센터, 클라우드, 하이브리드 인터넷 기반 인프라(퍼블릭 또는 프라이빗)에 도달하기 전에 공격 및 기타 원치 않는 악성 트래픽을 차단해 DDoS 공격으로부터 기업을 방어합니다. Akamai SOCC(Security Operations Command Center)의 전문가들은 공격을 즉각적으로 탐지 및 차단하기 위해 선제적인 방어 제어를 조정하고 나머지 트래픽에 대한 실시간 분석을 진행해 필요에 따라 추가적인 방어 조치를 결정합니다. 이렇게 방어된 공격은 공격 이벤트로 정리 및 그룹화되며, 모든 관련 데이터는 SOCC에서 분석하기 위해 기록됩니다.

이 보고서의 데이터는 달리 명시되지 않는 한 2023년 1월 1일부터 2024년 6월 30일까지 18개월 동안의 데이터를 대상으로 합니다.

브랜드 사칭 공격

Akamai Brand Protector는 피싱, 위조 웹사이트, 가짜 소셜 계정, 악성 애플리케이션과 같은 브랜드 사칭 공격으로부터 기업과 고객을 보호하기 위해 설계된 남용 방지 솔루션입니다. 이 솔루션은 매일 900TB 이상의 데이터를 분석하는 Akamai의 글로벌 엣지 네트워크를 사용해 위협이 고객에게 영향을 미치기 전에 탐지합니다. 이 인텔리전스는 파트너의 써드파티 피드를 통해 강화되어 다양한 온라인 플랫폼에서 잠재적 위협에 대한 폭넓은 시각을 제공합니다.

탐지된 각 의심스러운 도메인의 다양한 특성을 분석해 결정된 리스크 수준이 도메인의 위협 점수를 계산하는 데 사용됩니다. 이러한 의심스러운 도메인을 모니터링하고, 관련 데이터를 추적하고, 영향을 받는 고객에게 브랜드 아이덴티티를 악용하려는 악성 캠페인에 대한 경고를 보냅니다.

이 보고서의 데이터는 2023년 8월 1일부터 2024년 7월 31일까지 12개월 동안 탐지된 의심스러운 도메인을 대상으로 합니다.

Akamai

저자 소개

리서치 책임자

미치 메인(Mitch Mayne)

편집 및 작성

제임스 케이시(James Casey)
바데트 트리비(Badette Tribbey)
랜스 로즈(Lance Rhodes)

검토 및 주제별 기여

셰릴 키오디(Cheryl Chiodi)
갈 메이리(Gal Meiri)
지브 엘리(Ziv Eli)
리차드 메우스(Richard Meeus)
루벤 코(Reuben Koh)
스티브 윈터펠트(Steve Winterfeld)

데이터 분석

첼시 터틀(Chelsea Tuttle)

홍보 자료

바니 빌(Barney Beal)

마케팅 및 출판

조지나 모랄레스(Georgina Morales)
에밀리 스핑크스(Emily Spinks)

인터넷 보안 현황 보고서 정보

Akamai의 지난 인터넷 보안 현황 보고서를 확인하고, 다음 발행될 보고서를 가장 먼저 읽으세요. akamai.com/soti

Akamai 위협 연구팀 정보

akamai.com/security-research에서 최신 위협 인텔리전스 분석, 보안 보고서, 사이버 보안 리서치 내용을 확인하세요.

이 보고서의 데이터 확인

이 보고서에 참조로 사용된 그래프와 차트의 고품질 버전을 확인하세요. Akamai가 제공한 소스라는 점이 정식으로 인정되고 Akamai 로고가 보존되는 경우 이러한 이미지를 무료로 사용 및 참조할 수 있습니다. akamai.com/sotidata

Akamai 솔루션 정보

금융 서비스 업계를 표적으로 삼는 위협에 대한 Akamai 솔루션에 대한 자세한 내용은 **금융 서비스 페이지**를 참조하시기 바랍니다.

Akamai

Akamai Security는 성능이나 고객 경험에 영향을 주지 않으면서 모든 상호 작용 지점에서 비즈니스의 원동력이 되는 애플리케이션을 보호합니다. 글로벌 플랫폼의 규모와 위협에 대한 가시성을 활용해 고객과 협력함으로써 위협을 예방, 탐지, 방어하고 브랜드 신뢰를 쌓고 비전을 실현할 수 있도록 지원합니다. Akamai의 클라우드 컴퓨팅, 보안, 콘텐츠 전송 솔루션에 관한 자세한 정보는 akamai.com과 akamai.com/blog에서 확인하거나 X(기존의 Twitter)와 LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 2024년 9월 발행.