SOTI

10 YEARS
OF SECURITY INSIGHT

10권, 06호

Healthcare Under the Microscope

애플리케이션과 API에 집중된 공격

Akamai

인터넷 보안 현황 보고서

목차

취약점부터 가시성까지, 헬스케어의 사이버 보안 현황 파악하기

헬스케어 업계의 현황은 '취약하다'는 한 단어로 요약할 수 있습니다. 이를 해결하기 위해 2024년 헬스케어의 주요 테마는 되어야 합니다. 더 많은 플랫폼, 써드파티 소프트웨어, 광범위한 데이터 교환으로 인해 더 높은 가시성이 요구되지만, 헬스케어 기업에서 기술 최신화가 너무 빠르게 진행되고 있어 많은 기업이 생태계에 대한 진정한 가시성을 확보하는 데 어려움을 겪고 있습니다. 더 많은 공유가 필요하지만 더 엄격한 통제가 요구되는 컴플라이언스 조치로 인해 복잡성이 가중되고 있습니다. 이는 데이터 해자와 네트워크 독점을 제거하기 위한 논리적인 다음 단계이지만, 상위 기업을 제외한 대다수 업계의 현재 보안 역량을 초과하는 기술적 정교함의 요소가 추가되는 경우가 많습니다.

공격자들은 기회를 보고 있습니다. 헬스케어 분야의 각 영역이 우리 사회의 가장 민감한 정보를 교환하기 위해 시스템을 개방함에 따라, 새로운 시스템과 새로운 표준이 수십 년간 축적된 레거시 인프라와 결합되고 있습니다. 그런데 이러한 레거시 인프라는 그 자체로 엄청난 기술적 부채를 야기하는 동시에 악성 공격자들이 활발하게 활동할 수 있는 최적의 환경을 제공하기도 합니다.

안타깝게도 헬스케어 분야에서 사이버 보안 공격이 계속 증가하는 것은 더 이상 놀라운 일이 아닙니다. 특히 미국에서는 수년 동안 많은 헬스케어 기업이 제안서를 요청하고 벤더사를 평가할 때 사이버 보안을 필수 항목으로 간주해 왔습니다. 기업은 자체적으로 전문성을 구축하는 대신 HITRUST, HIPAA 준수, SOC 2 인증 벤더사를 요구하고 비즈니스 관계자 계약을 체결하여 이러한 벤더사에 리스크를 전가하는 경우가 많습니다. 이는 좋은 출발점이기는 하지만 여전히 헬스케어 업계에서는 주요 재정 문제, 운영상의 문제, 더 심각하게는 환자 안전에 대한 위협을 대대적으로 보도하는 헤드라인이 계속 나오고 있습니다. 다소 거슬리는 이야기일 수도 있지만, 상위 1000개 병원과 헬스케어 시스템의 25%~50%가 동일한 스프레드시트 기반의 '보안 체크리스트'를 사용해 벤더사를 승인하고 온보딩한다면, 이는 큰 문제입니다.

주목할 만한 점은 컴플라이언스 조치로 인해 결제업체가 오늘날 생태계의 API 기반 데이터 요구사항을 충족하고자 과거의 온프레미스, 일괄 시스템에서 벗어나 그 어느 때보다 더 많이 노출되고 있다는 사실입니다. 이러한 최신화를 통해 결제업체는 수년간 추구해 온 임상 데이터에 접속할 수 있지만, 개방형 교환은 새로운 종류의 리스크를 수반하는 새로운 비즈니스 방식입니다. 금융 데이터와 임상 데이터를 보유하고 있기 때문에 결제업체는 인프라를 보호하고 새로운 컴플라이언스 조치를 준수하면서 보안 체계를 신중하게 강화해야 합니다.

중요한 사실은 이러한 시장 변화가 앞으로도 계속될 거라는 점입니다. 헬스케어 업계는 API 및 클라우드 요구사항을 되돌리지 않을 것입니다. 변화에 대한 보안 우려는 당연한 것이지만, 개방형 데이터 교환에 주력하는 것은 역사적으로 데이터 사일로에 시달려온 헬스케어 업계에게 기념비적인 진전이기 때문입니다.

닐 제닝스(Neil Jennings)
Untangle Health 부사장

크리스 노타로(Chris Notaro)
Untangle Health CEO

소개

헬스케어 업계는 사이버 보안과 관련해 몇 가지 독특한 과제를 안고 있습니다.

- 생사가 걸린 문제이기도 합니다.
- 정보의 가치는 그 어떤 업계보다도 높습니다.
- 인프라에는 레거시 시스템과 의료 사물 인터넷(IoMT) 디바이스가 모두 포함됩니다.
- 이러한 시스템은 연합되어 있으며 종종 상호 의존적입니다.
- 컴플라이언스 요구사항도 가장 까다롭습니다.

이 인터넷 보안 현황(SOTI) 보고서에서는 헬스케어 생태계에 대한 리스크와 관련된 위협 데이터와 트렌드를 분석합니다. 헬스케어 업계에서 가장 큰 영향을 미치는 두 가지 위협은 웹 애플리케이션 및 API 공격과 분산 서비스 거부(DDoS) 공격입니다.

헬스케어 생태계 전반의 참여자(결제업체, 공급업체, 제약 및 생명 과학 기업) 또한 각각의 고유한 문제에 직면해 있으며, 이를 보안 전략에 반영해야 합니다.

보험 회사 또는 결제업체는 자격, 보장 범위, 결제를 결정하기 위해 임상 및 재무 데이터에 대한 강력한 접속 권한을 가지고 있으며 업계 전반에서 데이터 공유의 핵심적인 연결고리입니다.

제약 및 생명 과학 기업은 공격자들이 인공지능과 머신 러닝을 사용해 수많은 애플리케이션에 대한 대규모 데이터 세트를 분석하는 등 혁신에 집중하고 있다는 사실을 인지하고 있으며, 이로 인해 혁신과 리스크의 기로에 놓여 있습니다.

헬스케어 공급업체의 자금은 주로 원격 헬스케어 및 급성장하는 IoMT와 같은 임상 혁신에 집중되고 있으며, 기업의 안정성에 핵심적인 사이버 보안 접근 방식 발전과 같은 전통적인 기능에는 상대적으로 적은 비용이 투입되고 있습니다.

상호 운용성을 높이면 환자 및 재정적 성과를 개선할 수 있지만 웹 애플리케이션 및 API 공격의 형태로 리스크를 초래하기도 합니다.

역사적 관점에서 볼 때, 공격자들은 수년 동안 헬스케어 생태계를 표적으로 삼아왔습니다. 2024년 헬스케어 업계에서 13년 연속으로 모든 업계 중 가장 높은 데이터 유출 비용이 발생했으며, 평균 비용은 977만 달러로 2위 업계인 금융 서비스(608만 달러)보다 훨씬 높았습니다.

API는 헬스케어 업계의 모든 하위 업계에 영향을 미치는 주요 기술 중 하나입니다. API를 사용하면 공급업체, 결제업체, 환자, 그리고 전자 건강 기록 시스템, 의료 기기 회사, 건강 정보 교환과 같은 기타 써드파티 간에 데이터를 공유할 수 있습니다. 상호 운용성을 높이면 환자 및 재정적 성과를 개선할 수 있지만 웹 애플리케이션 및 API 공격의 형태로 리스크를 초래하기도 합니다.

애플리케이션 레이어에 대한 또 다른 일반적인 위협은 DDoS 공격입니다. DDoS 공격은 현재 유럽, 중동, 아프리카(EMEA)에서 가장 많이 발생하고 있으며, 이는 이 지역의 지정학적 상황과 친러시아 핵티비스트 그룹에 기인하는 것으로 보입니다. 그러나 DDoS 공격을 일으키는 그룹의 수와 이들이 사용하는 기법, 절차는 지속적으로 변화하기 때문에 어떤 국가나 지역도 공격으로부터 자유로울 수 없습니다.

핵심 인사이트

41%

헬스케어 서비스 생태계에서 결제 기업을 표적으로 삼은 API 공격의 비율

헬스케어 생태계에서 API 공격은 꾸준히 증가하고 있으며, 특히 결제업체와 보험회사가 보유한 보호 건강 정보(PHI), 청구 데이터, 금융 정보 등 풍부한 정보로 인해 이들에 대한 공격이 증가하고 있습니다.

API 스프롤은 데이터에 대한 무단 접속과 같은 심각한 리스크를 초래합니다.

API 스프롤 또는 기업 내에서 규제되지 않은 API의 확산은 가시성 부족과 보안 제어 범위를 벗어난 API의 출현으로 인해 심각한 보안 공백을 야기할 수 있습니다. 결과적으로 API 스프롤은 기업의 공격표면을 확장하고 민감한 데이터에 대한 무단 접속과 같은 리스크를 초래합니다.

88%

EMEA 지역의 제약사를 대상으로 한 레이어 7 DDoS 공격의 비율

EMEA 지역의 제약사는 레이어 7 DDoS 공격을 가장 많이 경험했으며, 북미와 아시아 태평양 및 일본(APJ)이 그 뒤를 이었습니다. 2024년 상반기 데이터를 자세히 살펴보면 EMEA와 북미 지역에 대한 공격 건수가 2023년에 모든 지역의 총합을 넘어설 것으로 예상됩니다.

2100만

헬스케어 공급업체에 대한 월평균 웹 애플리케이션 및 API 공격 건수

데이터 상호 운용성 및 기타 컴플라이언스 요구사항에 대한 압박이 증가하면서 웹 애플리케이션 및 API 사용이 증가했고, 이로 인해 헬스케어 공급업체와 환자 모두에게 보안 리스크가 발생했습니다.

4.15억

헬스케어 공급업체에 대한 월평균 레이어 7 DDoS 공격 건수

헬스케어 업계에서는 핵티비즘과 현재의 지정학적 환경으로 인한 DDoS 공격이 급증하고 있습니다. 이러한 공격은 서비스 중단과 장애를 일으켜 환자의 치료 결과를 위협할 수 있습니다. 2023년, Killnet은 주로 헬스케어 기업에 영향을 미친 대규모 DDoS 캠페인을 시작했습니다.

API 남용 리스크가 높은 결제업체

결제업체가 헬스케어 생태계 전반에서 데이터를 수집하고 처리하기 위해 API를 많이 사용하면 엄청난 장점도 있으나 상당한 컴플라이언스 요구사항과 보안 리스크와 같은 단점도 있습니다. 사이버 범죄자와 애그리게이터는 이러한 기능을 공격하고 악용하고 있으며 이로 인해 안전 및 개인정보 보호 문제가 발생할 수 있습니다.

결제업체의 경우 API를 이용한 공격은 공개 등록 및 청구 운영에 영향을 미치는 서비스 중단을 초래하고, 비용 부담이 큰 다운타임으로 이어지며, 브랜드 평판이 손상될 수 있습니다. 최근 발생한 치명적인 사례로는 2024년 2월 미국 전역에서 약국의 결제 처리를 심각하게 방해한 시스템 공격이 있습니다.

API 공격 트렌드

Akamai 리서치에 따르면 2023년 1월부터 2024년 6월까지 헬스케어 생태계를 표적으로 삼은 API 공격의 41%가 결제업체를 겨냥한 것으로 나타났습니다. 이는 2022년 기준 미국 전체 헬스케어 지출의 약 67%가 결제업체를 통해 지출되는 만큼 결제업체가 API 공격의 집중적인 리스크에 직면해 있다는 것을 의미하며, 이는 헬스케어 시스템 유지에 있어 결제업체가 차지하는 중요성과도 일치합니다.

다른 규제 대상 업계, 특히 결제 시스템을 다루는 업계에서도 비슷한 트렌드를 보입니다. 예를 들어 금융 업계는 디지털 혁신의 여정에서 한발 더 나아가, 이미 비즈니스 모델의 일부로 더 많은 통합 API를 사용하고 있습니다. 오픈 뱅킹은 API 사용을 촉진하는 동시에 더 많은 보안 리스크를 초래하고 있습니다. 따라서 금융 부문에서는 API 보안 SOTI 보고서에서 볼 수 있듯 API에 초점을 맞춘 공격이 더 많이 발생하고 있습니다.

Akamai 연구원들이 2023년 1월부터 2024년 6월까지 18개월 동안의 결제업체 API 공격 데이터를 자세히 살펴본 결과, 특히 분기별로 활동의 변동이 관찰되었습니다. 각 분기 내 일반적인 상승 트렌드는 분기 말에 예측 데이터와 실제 데이터를 조정하기 위해 진행한 시스템 간 동기화를 반영할 수 있지만, 2023년 4분기의 전반적인 증가는 공격자들이 운영을 방해하기 위해 공개 등록 기간을 노렸기 때문일 수 있습니다(그림 1).

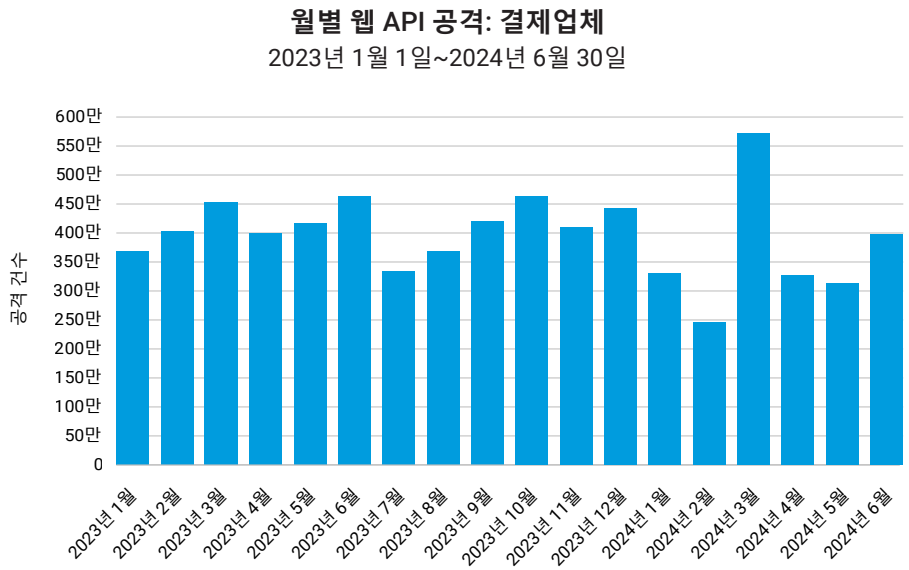


그림 1: API에 대한 웹 공격은 매 분기마다 증가하는 트렌드를 보였으며 2023년 4분기에는 전반적으로 증가했습니다.

모든 업계에 걸친 API 남용과 심각한 보안 문제

많은 API 보안 문제가 헬스케어 업계에만 국한된 것은 아니지만, API의 기본은 모든 업계에서 유사하기 때문에 우리가 방어해야 할 몇 가지 기술적 리스크를 검토해 볼 필요가 있습니다. 먼저, OWASP API Security 상위 10대 취약점에서 강조한 리스크에 집중해야 합니다. 그러나 개발자와 IT 직원은 체계 문제와 런타임 문제로 분류되는 보다 일반적인 취약점도 이해해야 합니다.

- **체계 문제**는 기업의 API 구축 취약점과 관련이 있습니다. 체계 문제를 나타내는 알림은 보안 팀이 공격자가 악용하기 전에 우선 순위가 높은 취약점을 식별하고 해결하는 데 도움이 됩니다. 일반적인 체계 문제에는 섀도 엔드포인트와 URL의 민감한 데이터가 포함됩니다.
- **런타임 문제**는 긴급한 대응이 필요한 활성 위협 또는 행동입니다. 이러한 중요 알림은 다른 종류의 보안 알림과 미묘한 차이가 있는데, 이는 보다 확실한 인프라 유출 시도와 다른 API 남용의 형태를 취하기 때문입니다. 일반적인 런타임 문제에는 인증되지 않은 리소스 접속 시도와 데이터 스크레이핑이 포함됩니다.

또한 보안 프로그램이 API 남용 및 악용에 대응할 수 있도록 한발 물러서서 API가 제시하는 세 가지 일반적인 문제를 살펴보는 것이 무엇보다 중요합니다.

1. **가시성**: 프로그램이 모든 API를 확실히 보호하도록 하기 위한 프로세스 및 기술적 제어 수단을 갖추고 있나요? API는 종종 혁신의 일부이거나 신제품에 내장되어 있어 많은 API가 기존 웹 제품과 동일한 수준의 지침, 보호, 검증을 제공하지 못하기 때문에 이는 중요한 문제입니다.

2. **취약점**: 기업 API가 개발 모범 사례를 따르고 있나요? OWASP의 가장 일반적인 잘못된 코딩 문제를 피하고 있나요? 또한 취약점을 추적하고 확인하고 있나요?

3. **비즈니스 로직 악용**: 예상 트래픽 기준선이 있나요? 의심스러운 활동이 무엇인지 파악했나요?

이러한 질문에 대한 답변은 여러분이 이해해야 할 내용의 기초가 됩니다. 전반적인 목표는 조사를 수행할 수 있는 가시성과 능력을 확보하고 위협을 신속하게 방어할 수 있는 프로세스를 수립하는 것입니다. 이는 환자 대면 및 내부 API 모두에 해당됩니다.

더 큰 리스크로 이어지는 성능 강화

환자들이 모든 애플리케이션에서 동일한 수준의 사용자 경험을 요구함에 따라 성능은 더 큰 관심사가 되고 있습니다. 즉, 헬스케어 생태계는 남용 공격은 물론 서비스 거부 공격을 방어해야 합니다. 또한 투명성에 대한 규제 요구사항에 따라 헬스케어 공급업체가 적시에 정보를 제공해야 할 필요성이 커지고 있습니다.

API 스프롤은 공격표면이 확장됨에 따라 가시성 저하로 이어지고 더욱 악화될 수 있습니다. API는 복잡한 디지털 혁신 프로젝트의 일부인 경우가 많기 때문에 헬스케어 기업의 보안 프로그램에는 잘 나타나지 않을 수 있습니다.

일상적인 비즈니스 활동과 관련된 헬스케어 및 금융 데이터 모두 엄격한 규제를 받고 있고 사이버 범죄자의 표적이 될 가능성이 높기 때문에 헬스케어 공급업체의 어려움은 더욱 가중됩니다.

API는 복잡한 디지털 혁신 프로젝트의 일부인 경우가 많기 때문에 헬스케어 기업의 보안 프로그램에는 잘 나타나지 않을 수 있습니다.

생명 과학 기업을 겨냥한 DDoS 공격이 증가하고 있습니다

백신 개발 리서치, 임상시험 데이터, 제조, 프로덕션, 출시 모두가 공격자들에게 공정한 게임으로 여겨졌던 코로나19 팬데믹 기간 동안 제약 사이버 보안에 대한 관심이 집중되었습니다. 오늘날 헬스케어 서비스는 미국의 중요 인프라로 분류되며, 새로운, 초당적 자금 지원으로 중요하다고 간주되는 부문 전반의 안정성 요구사항이 강화되었습니다. 그 이유는 분명합니다.

- 전 세계적으로 국제적 긴장이 계속 고조되고 있으며 PwC의 제25차 연례 글로벌 CEO 설문조사에서 임원들은 지정학적 환경이 큰 부담으로 작용한다고 답했습니다. 응답자의 거의 3분의 1이 지정학적 분쟁이 기업의 성장을 위협한다고 답했으며, 3분의 2 이상은 공급망 중단을 예상한다고 답했습니다.
- 현지화된 소싱 및 블록체인 기술 사용 강화와 같은 접근 방식을 통해 제약사는 안정성을 높이고 임상 및 비즈니스에 미치는 영향을 개선할 수 있습니다.
- 생명 과학 업계에 대한 Akamai의 글로벌 데이터에 따르면 DDoS 공격과 이 공격을 일으키는 그룹의 수가 계속 증가하고 있으며, 여기서 필요한 것은 바로 안정성입니다.

제약사를 겨냥한 애플리케이션 레이어 DDoS 공격의 표적이 된 EMEA 지역

Akamai 연구에 따르면 2023년 1월부터 2024년 6월까지 제약사를 표적으로 삼은 애플리케이션 레이어(레이어 7) DDoS 공격의 88%가 EMEA 지역에서 발생한 반면 북미와 APJ는 각각 7%와 5%를 차지했습니다. 2024년 상반기를 살펴보면 EMEA와 북미 지역의 공격 집중도가 증가하고 있으며 2023년에 각 지역의 총 공격 건수를 넘어서는 트렌드임을 알 수 있습니다(그림 2).

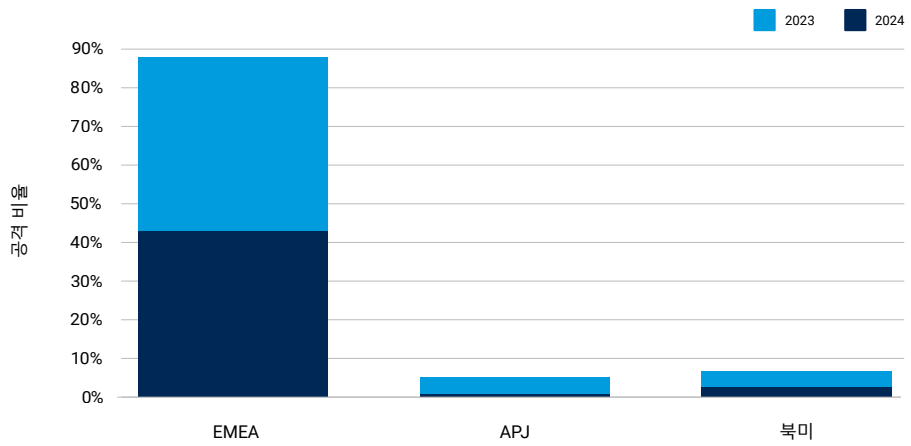


그림 2: 2023년부터 2024년까지 EMEA 지역의 레이어 7 DDoS 공격 집중이 지속되고 2024년 상반기에 급증했으며 북미 지역의 공격도 증가세를 보였습니다.

네트워크 및 전송 레이어 인프라를 압도하는 것을 목표로 하는 기존의 레이어 3 및 레이어 4 DDoS 공격과 달리, 레이어 7 DDoS 공격은 특정 애플리케이션 기능 또는 애플리케이션 서버 자체를 표적으로 삼습니다. 비교적 적은 양의 악성 트래픽을 통해 상당한 피해를 입힐 수 있습니다.

레이어 7 DDoS 공격은 CPU 및 메모리와 같은 애플리케이션 수준의 리소스를 표적으로 삼기 때문에 네트워크가 계속 사용 가능하더라도 표적이 된 애플리케이션이나 서비스가 느려지거나 완전히 응답하지 않을 수 있습니다.

유럽 연합의 헬스케어 및 생명 과학 업계에 대한 DDoS 공격 증가

ENISA 2023 위협 환경: 보건 부문 보고서에 따르면 유럽 연합의 헬스케어 및 생명 과학 업계에서 DDoS 공격이 증가하고 있습니다. 보고서에서 사이버 인시던트의 '핫스팟' 국가(특히 프랑스, 독일, 네덜란드)가 2022년 유럽 연합의 상위 1000대 기업에 포함된 제약 및 생명공학 기업의 지리적 집중도와 긍정적인 상관관계가 있다는 점이 흥미롭습니다.

ENISA(European Union Agency for Cybersecurity)는 DDoS 공격의 증가 원인을 지정학적 상황과 Killnet 같은 친러시아 핵티비스트 그룹 때문으로 보고 있습니다.

다음 표적은 미국 생명 과학 기업

Killnet은 유럽 병원을 표적으로 삼은 후 미국 거의 모든 주에 있는 병원으로 표적을 옮겼습니다. 병원에 대한 사이버 공격이 헤드라인을 가장 많이 장식했으나 2023년 4월 미국 HHS(U.S. Department of Health and Human Services)의 보고서는 실제로 Killnet의 DDoS 공격 표적이 된 기업의 비율이 제약 및 생명공학 기업에서 가장 높았다고 밝히고 있습니다.

미국의 생명 과학 분야 글로벌 시장 점유율(50%)이 EMEA(34%)보다 높다는 점을 고려할 때 미국에 기반을 둔 제약사에 대한 DDoS 공격 위협이 심화될 것으로 예상하는 것이 합리적입니다.

하지만 어떤 국가나 지역도 안전한 곳은 없습니다. 세계 최대의 일반 의약품 생산 및 수출국 중 하나인 인도는 작년에 17TB의 회사 데이터가 유출되는 사고로 큰 피해를 입었습니다. 랜섬웨어 기업이자 공격자인 ALPHV/BlackCat은 벤더사, 고객, 미국 직원 1500명의 문서에 대한 민감한 정보가 포함된 또 다른 랜섬웨어 공격을 일으켰다고 주장했습니다.

어떤 공격자들이 어떤 기법을 사용하나요?

ENISA 보고서는 올해 초 미국 공급망을 무너뜨린 그룹과 같은 ALPHV/BlackCat을 EMEA의 생명 과학 분야를 공격하는 주요 공격자 그룹 중 하나로 꼽았습니다.

Anonymous Sudan은 Killnet과 마찬가지로 정치적 동기가 있는 것으로 보고서에서 언급되었습니다. 처음에는 헬스케어 공급업체 그룹을 표적으로 삼았지만 이제는 헬스케어 생태계의 다른 곳으로 공격 대상을 확대하고 있다는 것입니다.

이러한 확장은 Anonymous Sudan의 최근 OpenAI에 대한 DDoS 공격에 대한 책임 주장과 같은 최근의 상황을 더욱 우려스럽게 만듭니다. 이 그룹은 최근 애플리케이션을 압도하고 오류를 발생시키기 위해 레이어 7 DDoS 공격에 대한 지원을 통합한 Skynet 봇넷을 사용했다고 밝혔습니다.

높은 리스크에 필요한 것은 보수적인 접근 방식

제약사는 오랫동안 인공 지능(AI), 특히 머신 러닝(ML)을 사용하는 헬스케어 업계의 선두주자였으며, 수많은 애플리케이션을 위해 대규모 데이터 세트를 분석하는 AI의 능력을 통해 많은 혜택을 누려왔습니다. 장점에는 질병의 조기 탐지, 신속한 신약 개발, 의약품 제조 개선 등이 포함됩니다. 그러나 금융 서비스 등 디지털 혁신을 수용한 다른 업계와 마찬가지로 생명 과학 분야도 혁신과 리스크의 기로에 서 있습니다.

실제로 Killnet의 DDoS 공격 표적이 된 기업의 비율은 제약 및 생명공학 기업에서 가장 높았습니다.

제약사는 이에 맞서고 있습니다. 다른 규제 대상 업계에서 레이어 7 DDoS 공격을 어떻게 처리하는지 살펴본 결과, Akamai 연구원들은 '거부' 조치와 '알림' 조치의 적용 비율에서 제약사가 비정상적인 활동을 높은 비율로 거부하는 보수적인 정책을 가지고 있다는 사실을 발견했습니다(그림 3).

하위 업계별 레이어 7 DDoS에 적용한 조치

2023년 1월 1일~2024년 6월 30일

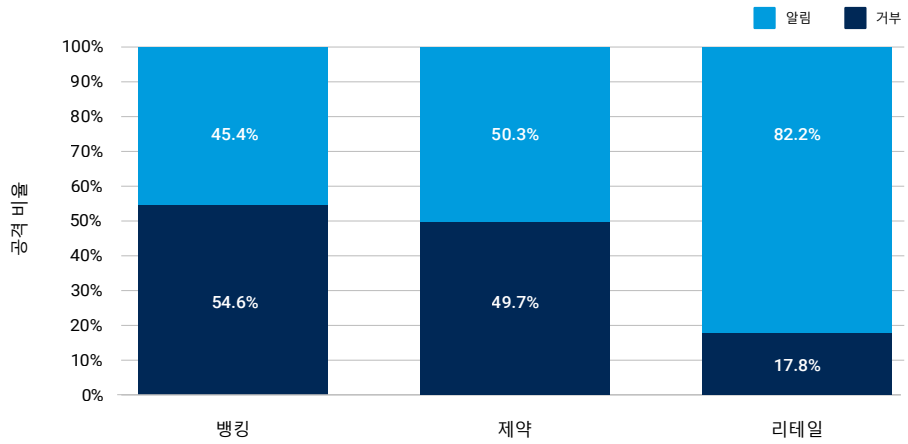


그림 3: 제약 및 생명 과학 기업은 알림 조치 대비 거부 조치의 비율이 높습니다.

2023년 1월부터 2024년 3월까지 거부 대 알림 통계를 처음 보고한 이후 거부 조치가 45.5%에서 49.7%로 4%포인트 이상 증가해 단기간에 주목할 만한 상승세를 보였습니다.

금융 서비스 및 은행업과 같은 다른 업계도 이와 유사한 보수적인 정책을 공유하고 있으며, 은행업과 생명 과학은 모두 핵심 인프라로 간주되어 규제가 엄격하다는 점에서 유사점이 많습니다.

또한 제약사의 경우 DDoS 공격이 성공하면 생명 유지 약품에 대한 접근이 지연되어 사람들의 생명을 위협하는 심각한 결과를 초래할 수 있습니다. 따라서 먼저 거부 조치를 취한 후 해당 활동을 조사하는 것이 좋습니다.

이와는 대조적으로 리테일 기업은 덜 공격적인 접근방식을 갖고 있었고, 알림을 받고 비정상 활동을 평가한 후에 조치를 취하기까지 더 많은 시간을 허용했습니다. 그러나 특히 AI/ML 사용과 관련된 새로운 규제가 시행되면 리테일 기업들 사이에서 거부 조치를 더 자주 취하는 방향으로 전환될 수 있습니다.

Akamai 연구원들은 '거부' 조치와 '알림' 조치의 적용 비율에서 제약사가 비정상적인 활동을 높은 비율로 거부하는 보수적인 정책을 가지고 있다는 사실을 발견했습니다.

포위당하고 있는 헬스케어 공급업체

헬스케어 정보 공유 및 분석 센터의 최고 보안 책임자는 2023년 12월에 발표된 HHS의 데이터 유출 분석을 인용하며 매시간 평균 3604건의 환자 기록이 유출되어 HHS에 보고되고 있다고 말했습니다.

공급업체와 병원에 대한 사이버 공격이 계속해서 급증하고 있습니다. 웹 애플리케이션에 의한 연결성과 상호 운용성, 그리고 API 사용 의무로 인해 공급업체와 환자가 리스크에 노출될 수 있습니다. 패치되지 않은 취약점과 레거시 기술로 인한 기술 부채는 비용이 많이 드는 문제로서 랜섬웨어 그룹이 이득을 취하기 위해 사용합니다.

또한 핵티비스트 그룹의 병원에 대한 지속적인 DDoS 공격 위협과 지정학적 환경으로 인해 환자 진료에 차질을 빚고 있습니다. 이 모든 것이 PHI 데이터 유출, 고객 관리에 대한 부정적인 영향, 경우에 따라서는 환자 안전 문제로 이어지고 있습니다.

헬스케어 기업에 대한 공격

Akamai 리서치에 따르면 2023년 1월부터 2024년 6월까지 18개월 동안 헬스케어 기업에 대한 웹 애플리케이션 및 API 공격이 꾸준한 페이스로 계속되고 있습니다(그림 4). 사이버 범죄자들이 진화하는 헬스케어 모델, 전달 방법, 혁신적인 시스템에 내재된 새로운 취약점과 이미 검증된 취약점을 모두 활용해 웹 애플리케이션과 API를 공격하고 악용함에 따라 이러한 트렌드는 어느 정도 변동에도 불구하고 계속 증가할 것으로 보입니다.

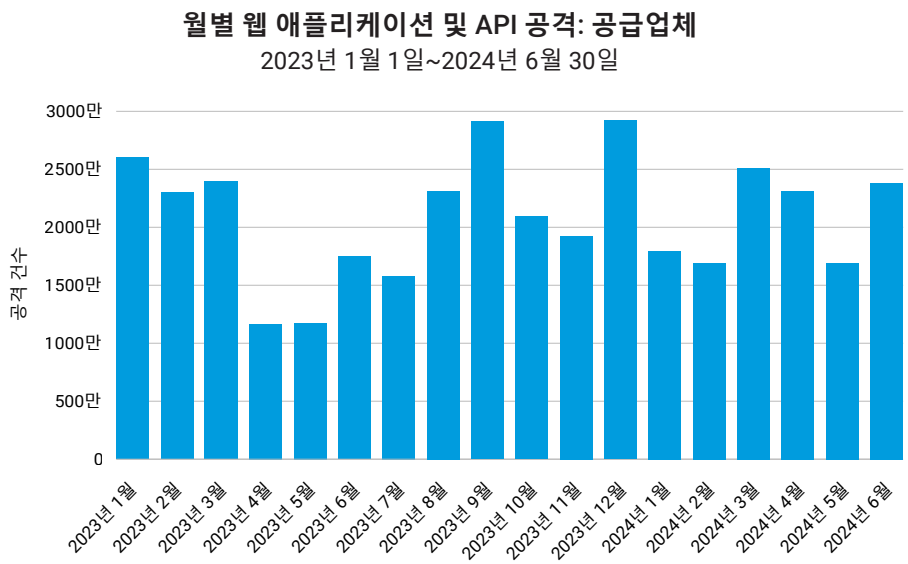
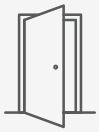


그림 4: 전 세계 헬스케어 기업에 대한 월간 웹 애플리케이션 및 API 공격은 평균 2100만 건에 달했습니다(참고: 한 고객이 데이터를 왜곡해 보고를 위해 삭제됨)



패치되지 않은 취약점과 레거시 기술로 인한 기술 부채는 비용이 많이 드는 문제로서 랜섬웨어 그룹이 이득을 취하기 위해 사용합니다.

웹 애플리케이션과 API를 통해 데이터를 공유하고 상호 운용성을 통해 치료를 조율하면 임상 및 재정적 결과를 개선할 수 있습니다. 그러나 API의 보안 영향이 아직 완전히 이해되지 않았기 때문에 헬스케어 업계는 상당한 리스크에 노출되어 있습니다.

최적의 치료 조율과 취약점으로 인한 리스크의 균형 맞추기

방대한 수의 환자 기록과 시스템 연결 지점으로 인해 헬스케어 공급업체는 치료 조율을 최적화하는 동시에 취약점으로 인한 리스크를 사전에 방어할 수 있는 가시성을 제공하는 제어 기능을 구축해야 합니다. API와 같은 새로운 기술과 인프라를 배포할 때 이러한 균형을 맞추기가 쉽지 않은 경우가 많습니다.

Akamai 연구원들이 또한 같은 18개월 동안 헬스케어 기업에 대한 레이어 7 DDoS 공격을 조사한 결과 2023년 1월 이후에도 서비스 중단이 꾸준히 발생하고 있음을 확인했습니다(그림 5). 이는 부분적으로는 친러시아 핵티비스트 그룹인 Killnet이 미국 내 헬스케어 기업을 중심으로 헬스케어 부문을 겨냥한 글로벌 DDoS 캠페인 때문인 것으로 추정됩니다. 이 기간 동안 사이버 범죄자들은 애플리케이션 기능 또는 애플리케이션 자체를 표적으로 삼아 환자 치료에 리스크를 초래하는 DDoS 공격을 지속적으로 활용했습니다.

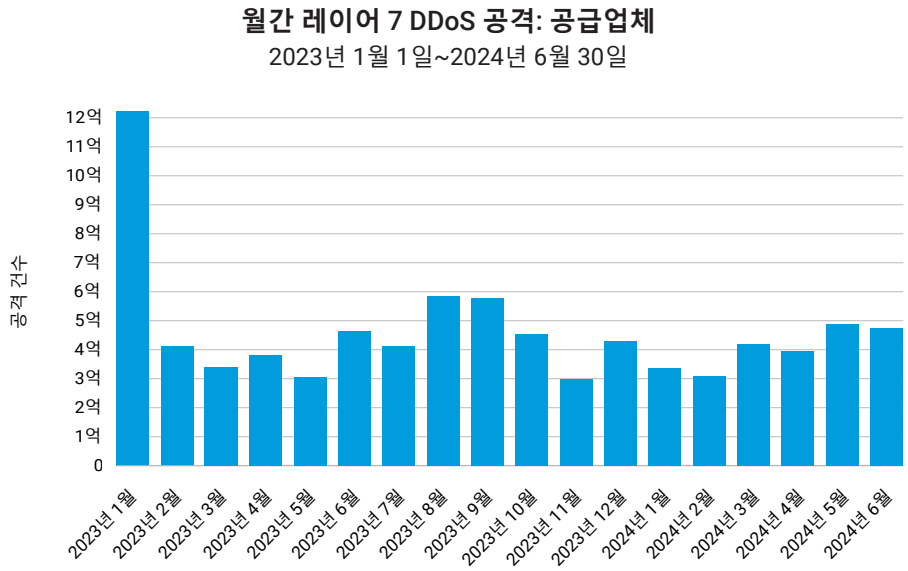


그림 5: 1월의 이례적인 급증을 제외하고 전 세계 헬스케어 기업에 대한 월별 DDoS 레이어 7 공격은 평균 4억 1500만 건에 달했습니다.

규모와 속도 면에서 새로운 기록을 세우고 있는 헬스케어 분야에 대한 DDoS 공격

지정학적 상황과 핵티비스트 그룹으로 인한 DDoS 활동의 증가로 인해 환자의 치료 결과를 위협할 수 있는 서비스 중단이 발생했습니다. 헬스케어 생태계 전체가 영향을 받았으며, 2023년에 발생한 Killnet의 대규모 DDoS 공격에서 헬스케어 기업이 가장 빈번한 표적이 되었습니다. HC3는 단 몇 시간이라도 헬스케어 서비스가 중단되면 일상적인 업무부터 중대한 업무에 이르기까지 모든 업무에 영향을 미쳐 잠재적으로 심각한 결과를 초래할 수 있다고 경고했습니다.

애플리케이션을 통한 헬스케어 상호 작용이 증가함에 따라 적시에 정보와 치료를 받는 것이 환자의 경험에 점점 더 중요해지고 있습니다. 따라서 보호 및 프로세스를 마련하는 것도 마찬가지로 중요합니다.

여러 전선에 걸친 공격으로 치료 조율 방해

공급업체는 DDoS 외에도 다른 인기 있는 공격에 직면하고 있습니다. 헬스케어 기록에 대한 접속을 제한하고 구급차를 우회하도록 하는 랜섬웨어 공격은 헬스케어 기록에 대한 접속 권한이 없으면 헬스케어 공급업체의 협력이 불가능하다는 사실을 강조합니다. 종이 기록으로 되돌아가면 환자 치료 작업의 추적, 주요 부서 간의 커뮤니케이션, 모든 주문 서비스가 중단됩니다.

2023년에 발생한 Killnet의 대규모 DDoS 공격에서 헬스케어 기업이 가장 빈번한 표적이 되었습니다.

민감한 데이터가 영향을 받는 경우 헬스케어 기업은 데이터 유출의 여파에 대응해야 합니다. 인기 있는 소프트웨어 툴의 취약점을 악용하면 권한이 없는 공격자가 PHI부터 건강 보험 및 의료 정보에 이르는 방대한 데이터에 접속할 수 있습니다.

반드시 데이터 보호를 포함해야 하는 환자 보호

환자 치료의 일부분은 환자 데이터에 대한 접속을 보호하고 제어할 수 있는 능력입니다. 전통적으로 헬스케어 분야의 사이버 보안 예산과 인력이 부족했기 때문에 데이터 보호에 어려움을 겪어 왔습니다. 그러나 헬스케어 공급업체 그룹에 대한 사이버 공격이 계속해서 헤드라인을 장식함에 따라 헬스케어 공급업체 그룹은 아웃소싱 보호 파트너십을 개선하고 사이버 보험 적용 범위를 확대하고 있습니다.

헬스케어 공급업체가 중요 인프라 부문의 안정성을 강화하기 위해 마련된 미국 정부의 정책 업데이트의 혜택을 받으면서 보호 개선에 대한 모멘텀은 계속 강화될 것입니다.

컴플라이언스 고려 사항

규제 환경은 점점 더 투명성을 요구하고 있으며, 이는 API의 사용을 촉진하고 있습니다. 컴플라이언스 조치는 공급업체와 결제업체 모두에게 광범위한 데이터 공유 요구사항을 부과하고 있습니다. 이러한 데이터 공유는 임상 및 재무 데이터의 교차 수분을 허용하기 위한 것으로, 지금까지는 각 당사자에게 어려웠지만 VBC(Value-Based Care)의 효과적인 실행을 위해 필요합니다.

비용을 염두에 두고 치료를 제공하는 VBC를 향한 움직임은 현재 공유해야 하는 정보의 양과 다양성을 보여주는 대표적인 예입니다. 결제업체는 오랫동안 환자 및 공급업체의 금융 데이터에 접속할 수 있었습니다. 그러나 복약 순응도 및 병원 입원과 같은 더 많은 VBC 데이터 포인트는 보다 혁신적이고 상호 운용 가능한 연속성을 필요로 하며, 이러한 데이터를 공유할 수 있는 수단이 필요합니다. 바로 API가 그 수단입니다.

최근 CMS 상호 운용성 및 환자 접속 최종 룰에 따르면 헬스케어 공급업체는 결제업체, 공급업체, 환자 간의 정보 흐름을 유지하기 위해 세 가지 주요 범주의 API를 유지해야 합니다.

1. 환자 접속 API: 이를 통해 회원의 의료 데이터에 대한 접속이 증가하고 회원 만족도가 높아질 수 있습니다.

2. 공급업체 디렉토리 API: 회원이 자신의 위치와 전문 분야를 기준으로 헬스케어 공급업체 및 시설을 검색할 수 있도록 함으로써 헬스케어 서비스에 대한 접속을 개선합니다.

3. 결제업체-공급업체 및 결제업체-공급업체 API: 이를 통해 환자 치료의 공백을 해결하고 줄일 수 있으며 중복되고 비용이 많이 드는 서비스도 줄일 수 있습니다.

또한 곧 시행될 CMS 상호 운용성 및 사전 권한 확인 최종 룰에 따라 영향을 받는 결제업체는 추가 사전 권한 확인 API를 도입해야 합니다.

컴플라이언스 조치에 따라 FHIR(Fast Healthcare Interoperability Resources) 표준을 통해 API의 포맷도 정해지고 있습니다. 이러한 요구사항과 표준은 시스템 간의 상호 운용성을 단순화하고 간소화하는 동시에 보안을 강화합니다. FHIR은 웹 애플리케이션 방화벽, 인증, 암호화, 개인정보 보호, 마이크로세그멘테이션과 같은 기본 기능을 포함하는 보안 프로그램이 존재할 것으로 기대합니다.

헬스케어 공급업체는 이전보다 더 많은 데이터를 적시에 (환자가 선택한) 환자 건강 애플리케이션에 연결할 수 있는 표준 포맷으로 공유해야 하지만, FHIR 표준의 의도는 관리 부담을 줄이고 투명성을 높이는 데 있습니다. 따라서 환자들은 향상된 서비스 수준을 기대할 수 있습니다.

또한 데이터 교환이 지연되면 정보 차단 과태료가 부과되는 등 의료 서비스에 부정적인 영향을 끼치고 종종 비용 증가로 이어질 수 있습니다. 따라서 최근 클라우드로 전환한 헬스케어 공급업체는 이러한 새로운 컴플라이언스 조치를 준수하기 위해 새로운 포맷의 외부 API를 빠르게 출시하고 있습니다.

API에 초점을 맞춘 공격의 리스크 외에도 DDoS 및 랜섬웨어와 같은 가용성 공격은 모든 업계에 걸쳐 계속해서 큰 영향을 미치고 있으며, 헬스케어 분야는 큰 영향을 받을 수 있는 분야 중 하나입니다. 이러한 종류의 공격에 대응하기 위한 규제는 안정성에 초점을 맞추는 경향이 있습니다. 예를 들어, 미국 HHS에서는 헬스케어 부문 DDoS 가이드를 발표했습니다. 또한 비영리 헬스케어 정보 공유 및 분석 센터에서는 헬스케어 부문의 안정성 문제에 대한 백서 안정성은 우리의 DNA에 있다를 발간했습니다.

조치 작업: 방어 권장 사항

리스크 관리 및 컴플라이언스 관점에서 API 보안은 그 어느 때보다 중요합니다. 그러나 API 스프롤로 인해 헬스케어 API를 식별, 분류, 보호하는 것이 점점 더 어려워지고 있습니다. 또한 헬스케어 기업은 서비스 가용성을 위협하는 DDoS 공격도 방어해야 합니다.

알지 못하는 공격은 방어할 수 없습니다. 따라서 먼저 모든 자산을 발견해 보안 프로그램에 포함시킬 수 있도록 해야 합니다. 그런 다음 어떤 취약점이 존재하는지 파악하고 성능 및 보안과 관련해 어떤 일이 일어나고 있는지 상황을 인식해야 합니다. 마지막으로 자동화된 테스트와 전통적인 펜 테스트를 통해 시스템의 보안을 검증해야 합니다.

다음 API 보안 및 DDoS 방어 전략 이정표를 충족하면 강력한 보안 프로그램을 구축하는 데 도움이 될 수 있습니다.

5가지 API 보안 전략 이정표

강력한 API 보안 프로그램을 도입하면 모든 API에 대한 가시성을 개선하고 리스크에 대한 노출을 파악해 보안 수준을 높일 수 있습니다.

1. 악성 또는 섀도 API를 체계적으로 발견해 인프라 사각지대를 제거하고, 각 API가 폐기되거나 API 보안 제어에 통합되도록 합니다.

2. 일반적인 알림의 종류를 분석하고 API 코드의 결함을 수정하고, 잘못된 설정 문제를 해결하고, 교훈을 바탕으로 향후 취약점을 방지하기 위한 프로세스를 구축해 리스크 체계를 결정하고 강화합니다.

3. 정상적인 행동을 이해하고 API 보안 알림의 급증을 기반으로 잠재적인 악용을 식별해 위협 탐지 및 대응을 강화합니다. 그런 다음 잘 정의된 대응 절차에 따라 리스크 및 알림 규모를 정상 수준으로 낮춥니다.

4. 교육과 전문 지식을 모두 제공하는 벤더사와 협력합니다. 벤더사는 프로젝트 기반 지원부터 복잡하고 통합된 사이버 보안 솔루션을 올바르게 설정하고 관리하는 데 도움이 되는 완전 관리형 서비스까지 다양한 서비스를 제공해야 합니다.

강력한 API 보안 프로그램을 도입하면 모든 API에 대한 가시성을 개선하고 리스크에 대한 노출을 파악해 보호 수준을 높일 수 있습니다.

5. 대응 시나리오로 확대되기 전에 가능한 위협을 식별하는 것을 목표로 공식적인 API 위협 탐지 규율을 수립해 더 강력한 공격을 개발합니다.

DDoS 방어 전략의 네 가지 이정표

레이어 7 웹 페이지 및 API, 레이어 3 및 4 인프라, DNS 시스템에 대한 DDoS 공격에 대한 새로운 기록이 수립됨에 따라 서비스 및 기능의 가용성을 보장하는 것이 매우 중요해졌습니다. 이는 최신 공격의 규모, 범위, 속도에 대응할 수 있는 능동적인 방어 체계를 갖추는 것을 의미합니다.

1. 공격에 대한 가시성을 확보하고 신속하게 대응할 수 있는 시스템을 구축해야 합니다. 여기에는 레이어 7, 레이어 3 및 4, DNS 인프라가 포함되어야 합니다.

2. 온프레미스 어플라이언스에 과부하를 주는 공격으로부터 보호하는 하이브리드 DDoS 방어 플랫폼으로 온프레미스 DDoS 방어 기능을 백업합니다.

3. 사전 예방적 보안 체계를 도입하는 데 도움이 되는 실행 가능한 애널리틱스를 실시간으로 제공하는 정책을 쉽게 관리하고 IP 허용 목록을 유지할 수 있는 공급업체 또는 시스템을 사용합니다.

4. 테스트를 통해 알림, 보호 기능, 위기 관리 프로세스를 검증하고 모든 인프라가 적절한 보호 기능을 갖추고 있는지 확인합니다.

자세한 내용은 Akamai 최신 리서치나 블로그를 참조하세요.

레이어 7 웹 페이지 및 API, 레이어 3 및 4 인프라, DNS 시스템에 대한 DDoS 공격에 대한 새로운 기록이 수립됨에 따라 서비스 및 기능의 가용성을 보장하는 것이 매우 중요해졌습니다.

방법론

웹 애플리케이션 및 레이어 7 DDoS 공격

이 데이터는 웹 애플리케이션 방화벽(WAF)을 통해 관측된 트래픽에 대한 애플리케이션 레이어 알림을 설명합니다. 애플리케이션 공격 알림은 보호하고 있는 웹사이트, 애플리케이션, API에 대한 요청에서 악성 페이로드를 탐지하면 트리거됩니다. 레이어 7 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.

2024년 데이터 업데이트

Akamai는 10주년을 기념해 데이터 세트에 대한 몇 가지 업데이트를 발표하게 된 것을 기쁘게 생각합니다. Akamai의 웹 애플리케이션 및 봇 공격 데이터 세트에 몇 가지 업그레이드가 있었습니다. 각각의 수집 방법이 변환, 간소화, 최적화되었습니다. 인사이트가 더 깊어지고 범위가 넓어졌습니다. SSRF와 같은 추가 공격 기법에 대한 항목이 추가되었으며, API 엔드포인트를 겨냥한 공격의 식별도 각 데이터 세트에 추가되었습니다. 이번 보고서에서 이러한 새로운 개선 사항 중 일부를 소개하게 되어 기쁘게 생각합니다. 인터넷 보안 현황 보고서의 이번 이정표를 기념하면서 앞으로 독자 여러분과 함께 이런 업데이트를 계속 공유할 수 있기를 기대합니다.

저자 소개

리서치 책임자
미치 메인(Mitch Mayne)

편집 및 작성
닐 제닝스 (Neil Jennings)
바제트 트리베이 (Badette Tribbey)
크리스 노타로 (Chris Notaro)
마리아 벨라스크 (Maria Vlasak)
샬럿 펠리시아 (Charlotte Pelliccia)
스티브 윈터펠드 (Steve Winterfeld)

검토 및 주제별 기여
클레어 브룸 (Claire Broome)
셰인 키츠 (Shane Keats)

데이터 분석
첼시 터틀(Chelsea Tuttle)

홍보 자료
바니 빌(Barney Beal)

마케팅 및 출판
조지나 모랄레스 햄프(Georgina Morales Hampe)
에밀리 스핑크스(Emily Spinks)

인터넷 보안 현황 보고서 정보

Akamai의 지난 인터넷 보안 현황 보고서를 읽고 다음 보고서를 확인하세요. 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

헬스케어 업계를 노리는 위협에 대한 Akamai 솔루션에 대한 자세한 내용은 **헬스케어 및 생명 과학 페이지**를 참조하시기 바랍니다.