SOTI

V10 ISSUE 06

10 YEARS
OF SECURITY INSIGHT

Healthcare Under the Microscope

Attacks Focus on Applications and APIs

Akamai

State of the Internet/Security

Table of Contents

From vulnerability to visibility, untangling healthcare's cybersecurity situation

The state of the healthcare industry can be boiled down to one word: vulnerable. To address this, the primary theme for healthcare in 2024 should be visibility. More platforms, third-party software, and broadscale data exchange demand greater visibility, but technical modernization is moving so quickly in healthcare organizations that many struggle with true visibility over their ecosystem. Adding to the complexity are compliance measures that require more sharing but with stricter controls. Although this is a logical next step to eliminate data moats and network monopolies, it adds elements of technical sophistication that often exceed the current security capabilities of the majority of the industry, with the exception of the top players.

Threat actors are seeing one thing: opportunity. As each area of healthcare is opening up their systems to exchange our society's most sensitive information, we are combining new systems and new standards with decades of legacy infrastructure. So while that legacy infrastructure creates potentially massive technical debt of its own, it also provides an optimal environment in which malicious actors can thrive.

Unfortunately, the ever-increasing wave of cybersecurity attacks in healthcare is not surprising. In the United States, specifically, many healthcare organizations have treated cybersecurity as a check-the-box exercise during requests for proposals and vendor evaluations for years. Instead of building expertise in-house, organizations often simply require HITRUST, HIPAA-compliant, SOC 2–certified vendors, and use Business Associates Agreements to shift risk to these vendors. While that is a decent start, we're still seeing headline after headline trumpeting major financial issues, operational breakdowns, or — worse — threats to patient safety in the healthcare industry. Now, we realize this might ruffle some feathers, but when somewhere between one-quarter and one-half of the top 1,000 hospitals and health systems use the same spreadsheet-based "security checklist" to approve and onboard vendors, we have a problem.

It is worth focusing on the fact that payers are more exposed than ever before, with compliance measures pulling them out of their on-prem, batched systems of yesterday to meet the API-based data requirements of the modern ecosystem. While this modernization is providing payers with the access to clinical data that they have sought for years, the open-exchange is a new way of doing business that comes with new types of risks. Because they hold financial data and clinical data, payers must secure their infrastructure and thoughtfully uplevel their security posture as they adhere to each new compliance measure.

The bottom line: These market changes are here to stay. The healthcare industry will not be reverting from API and cloud requirements. Although security concerns about changes are normal, this emphasis on open data exchange is monumental progress for an industry historically plagued by data silos.

Neil Jennings
Vice President, Untangle Health

Chris Notaro
CEO, Untangle Health

Introduction

The healthcare industry has some unique challenges when it comes to cybersecurity.

- The stakes can be life or death.
- The value of the information is among the highest of any industry.
- The infrastructure includes both legacy systems and Internet of Medical Things (IoMT) devices.
- The systems are federated and often interdependent.
- The compliance requirements are among the most arduous.

In this State of the Internet (SOTI) report, we analyze threat data and trends related to risks to the healthcare ecosystem. The two threats that are having the biggest impacts in this industry are web application and API attacks and distributed denial-of-service (DDoS) attacks.

The participants across the healthcare ecosystem (payers, providers, and pharmaceutical and life science companies) also each face unique challenges that should inform their security strategy.

Insurance companies or payers have robust access to both clinical and financial data to determine eligibility, coverage, and payments, and are a key nexus of data sharing across the industry.

Pharmaceutical and life sciences organizations find that threat actors are focusing on their innovations, including the use of artificial intelligence and machine learning to analyze large datasets for myriad applications, which has put them firmly at the crossroads of innovation and risk.

Healthcare providers' funds are primarily funneled toward clinical innovations like telehealth and a burgeoning IoMT, with less organizational spend on more traditional functions like evolving cybersecurity approaches that are pivotal to organizational resilience.

The drive toward interoperability enables better patient and financial outcomes, but also introduces risk in the form of web application and API attacks.

From a historical perspective, threat actors have targeted the healthcare ecosystem for years. In 2024, for the 13th year in a row, the healthcare industry experienced the highest data breach costs of all industries, with the average cost hitting US$9.77 million, which was substantially higher than financial services, the next closest industry, at US$6.08 million.

APIs are one of the major technologies that impact all sub-verticals of the healthcare industry. APIs make it possible to share data among providers, payers, patients, and other third parties, such as electronic health record systems, medical device companies, and health information exchanges. The drive toward interoperability enables better patient and financial outcomes, but also introduces risk in the form of web application and API attacks.

Another common threat to the application layer are DDoS attacks. They are the current weapon of choice in Europe, Middle East, and Africa (EMEA), which is likely attributable to geopolitical developments and pro-Russian hacktivist groups in the region. However, no country or region is immune to attacks, as the number of groups perpetrating DDoS attacks and the tactics, techniques, and procedures they use continually shift.

Key insights

41%

Percentage of API attacks in the healthcare ecosystem that targeted payer organizations

API attacks are growing steadily in the healthcare ecosystem, particularly attacks on payer organizations and insurance companies due to the wealth of information they hold: protected health information (PHI), claims data, and financial information.

API sprawl poses significant risks, like unauthorized access to data

API sprawl, or the unregulated proliferation of APIs within organizations, can create significant security gaps via a lack of visibility and their emergence outside of security controls. As a result, API sprawl expands an organization's attack surface and ushers in risks such as unauthorized access to sensitive data.

88%

Percentage of Layer 7 DDoS attacks against pharmaceutical organizations in EMEA

Pharmaceutical companies in the EMEA region experienced the highest volume of Layer 7 DDoS attacks, followed by North America and Asia-Pacific and Japan (APJ). A closer examination of H1 2024 data reveals that the number of attacks against EMEA and North America are on track to exceed the total for each region in 2023.

21 MILLION

Monthly average of web application and API attacks against healthcare providers

The push for data interoperability and other compliance requirements fueled the growth in web application and API use, which in turn created security risks for both providers and patients.

415 MILLION

Monthly average of Layer 7 DDoS attacks against healthcare providers

The healthcare industry is experiencing a surge in DDoS attacks, driven by hacktivism and the current geopolitical climate. These attacks can cause outages and disruptions that threaten patient outcomes. In 2023, Killnet launched a large-scale DDoS campaign that primarily impacted provider organizations.

Payers are at high risk for API abuse

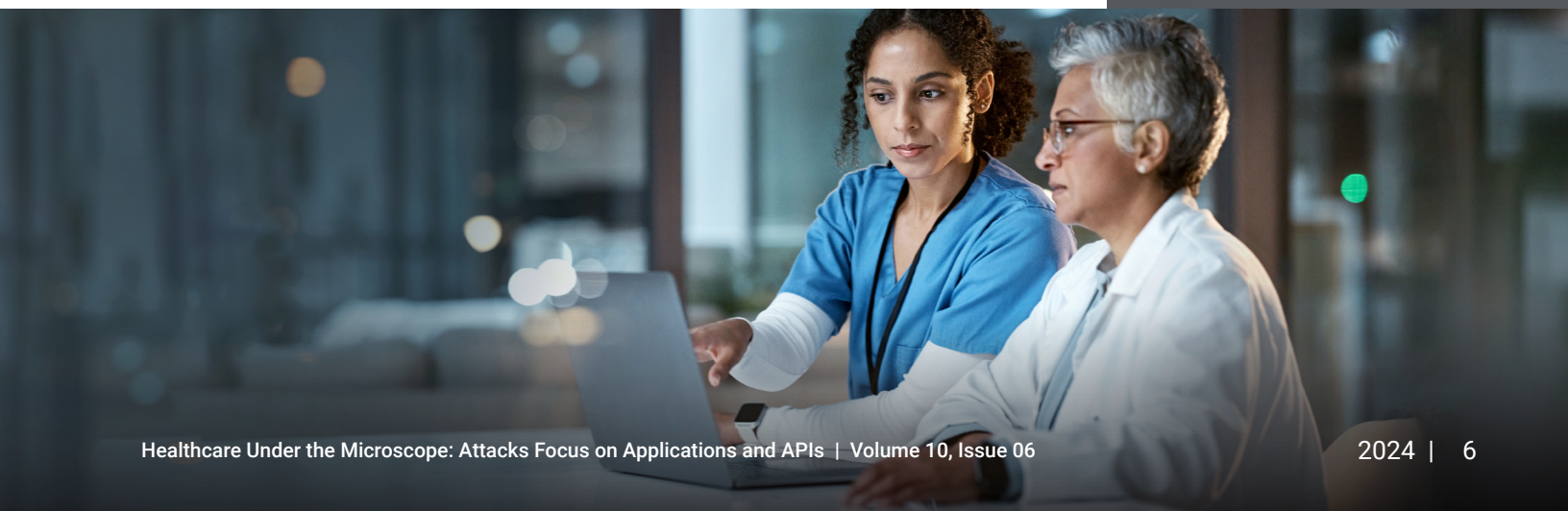
Although payers' high use of APIs to gather and process data across the healthcare ecosystem delivers tremendous benefits, it also comes with tradeoffs — notably, significant compliance requirements and security risks. Cybercriminals and aggregators are attacking and abusing these capabilities, which can result in both safety and privacy issues.

For payers, API-enabled attacks can also result in service disruptions that impact open enrollment and claims operations, lead to costly downtime, and damage the company's brand. The systemic attack that severely stymied payment processing at pharmacies across the United States in February 2024 is a recent and painful example.

API attack trends

Akamai research found that from January 2023 through June 2024, 41% of the API attacks that targeted the healthcare ecosystem were against payer organizations. This indicates that payers face a more concentrated risk of API abuse by attacks, which is consistent with the payers' importance in keeping the healthcare system moving, as approximately 67% of total U.S. healthcare expenditure runs through payers as of 2022.

We see a similar trend in other regulated industries — especially those that handle payment systems. The finance industry, for example, is further along in its digital transformation journey and is already using more integrated APIs as part of its business models. Open banking is driving its use of APIs and introducing more security risks. Therefore, the finance sector is experiencing a higher concentration of API-focused attacks, as found in our API security SOTI report.



By looking more closely at payer API attack data, Akamai researchers observed fluctuations in activity during the 18-month period from January 2023 through June 2024, particularly quarterly. The general upward trend within each quarter may reflect syncing among systems at the end of the quarter to reconcile predicted and actual data, but the overall increase in Q4 2023 can likely be attributed to attackers targeting open enrollment periods to disrupt operations (Figure 1).

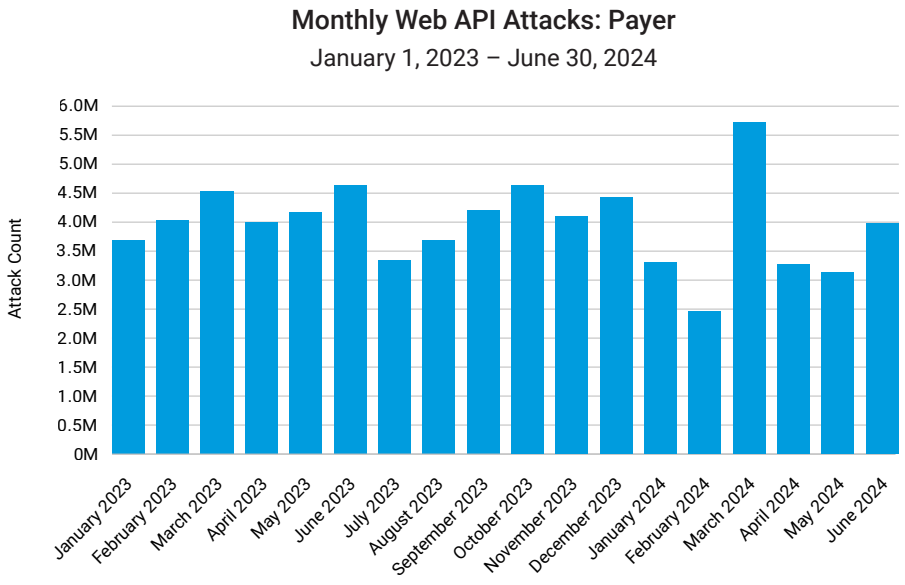


Fig. 1: Web attacks against APIs trended upward within each quarter, with an overall increase in Q4 2023

API abuse and critical security challenges across all industries

While many API security challenges are unique to healthcare, the basics of APIs are similar across all industries, and it is worth reviewing some of the more technical risks we all need to mitigate. First, we should concentrate on the risks highlighted by the OWASP API Security Top 10. But we also need to make sure our developers and IT staff understand the more common vulnerabilities that we categorize as posture problems and runtime problems.

- **Posture problems** pertain to flaws in the enterprise's API implementation. Alerts indicating posture problems help security teams identify and remediate high-priority vulnerabilities before they can be exploited by attackers. Common posture problems include shadow endpoints and sensitive data in a URL.
- **Runtime problems** are active threats or behaviors that require an urgent response. These critical alerts are more nuanced than other types of security alerts since they take the form of API abuse (versus more explicit infrastructure breach attempts). Common runtime problems include unauthenticated resource access attempts and data scraping.

It is also paramount to step back and look at three more general challenges that APIs present to ensure that your security program covers API abuse and exploitation.

1. **Visibility**: Do you have process and technical controls to ensure that all APIs are protected by your program? This is a key issue as APIs are often part of the transformation or embedded in new products, so many do not have the same level of directions, protections, and validations of a traditional web presence.

2. **Vulnerabilities**: Are your APIs following best practices for development? Are you avoiding OWASP's most common poor coding issues? Furthermore, are you tracking and checking for vulnerabilities?

3. **Business logic abuse**: Do you have a baseline of expected traffic? Have you established what constitutes suspicious activities?

The answers to these questions form the basis of what your team should understand. The overall goals should be to have the visibility and ability to conduct investigations and to have processes established to rapidly mitigate threats. This is true for both patient-facing and internal APIs.

Better performance may equal bigger risk

Performance is becoming a bigger concern as patients are demanding the same level of user experience across all their applications. This means the healthcare ecosystem needs to be protected from denial-of-service attacks as well as abuse attacks. Additionally, providers are under regulatory requirements for transparency that are driving the need for the timely availability of information.

API sprawl can lead to poor visibility that becomes even murkier as the attack surface expands. APIs are often part of complex digital transformation projects, so they may not be on the radar for healthcare organizations — security programs, even less so.

The types of data — both medical and financial — involved in daily business activities are both highly regulated and liable to be targeted by cybercriminals, which just compounds the challenges for payers.

APIs are often part of complex digital transformation projects, so they may not be on the radar for healthcare organizations — security programs, even less so.

The number of DDoS attacks against life sciences organizations is increasing

The focus on pharmaceutical cybersecurity became laser sharp during the COVID-19 pandemic, when vaccine development research, trial data, manufacturing, production, and rollout were all considered fair game by threat actors. Today, healthcare is classified as U.S. critical infrastructure, and new bipartisan funding elevates resilience requirements across sectors that are deemed critical. The reasons are clear:

- International tensions continue to rise globally, and the geopolitical climate weighs heavily on the executives who responded to PwC's 25th Annual Global CEO Survey. Almost one-third of the respondents said that geopolitical conflict threatens their companies' growth, and more than two-thirds said it's an expected factor in supply chain disruption.
- Approaches like localized sourcing and enhanced use of blockchain technology can help pharmaceutical companies boost resiliency and improve clinical and business impacts.
- Akamai global data for the life sciences industry suggests that DDoS attacks — and the number of groups perpetrating them — are only growing; resilience is just what this sector needs.

EMEA targeted by application-layer DDoS attacks on pharmaceutical organizations

Akamai research found that from January 2023 through June 2024, the EMEA region experienced 88% of all application-layer (Layer 7) DDoS attacks that targeted pharmaceutical organizations, while North America and APJ accounted for 7% and 5% of those attacks, respectively. By looking at H1 2024, we can see the concentration of attacks in both EMEA and North America were on the rise and on a path to eclipse the total number of attacks for each region in 2023 (Figure 2).

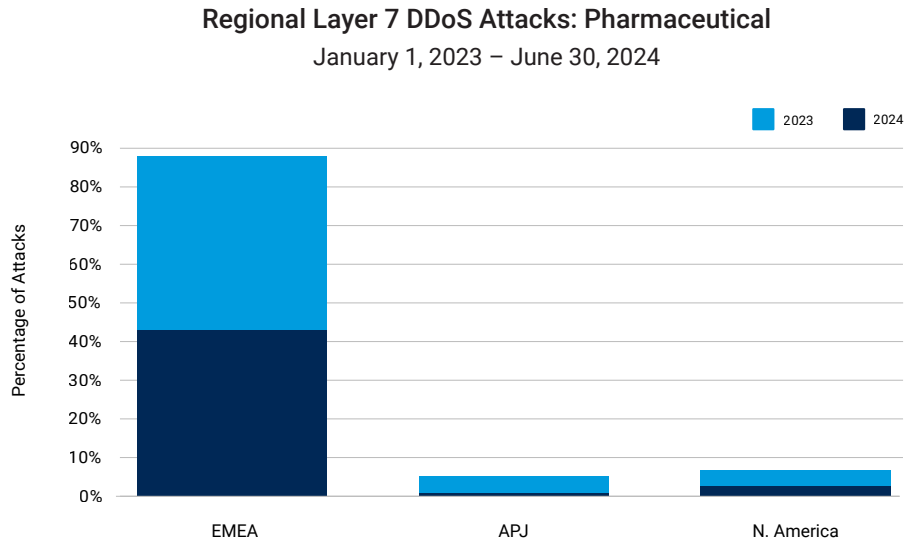


Fig. 2: The concentration of Layer 7 DDoS attacks in EMEA continues from 2023 to 2024 and surged in H1 2024, while attacks in North America were also on the rise

Unlike traditional Layer 3 and Layer 4 DDoS attacks, which aim to overwhelm network and transport-layer infrastructure, Layer 7 DDoS attacks target specific application functionalities or the application server itself. They are capable of causing significant damage even with a relatively small amount of malicious traffic.

Layer 7 DDoS attacks target application-level resources, such as CPU and memory, so the targeted application or service may become slow or entirely unresponsive even if the network remains available.

Increased DDoS attacks on the healthcare & life sciences industry in the European Union

The ENISA 2023 Threat Landscape: Health Sector report confirms an increased number of DDoS attacks in the healthcare & life sciences industry in the European Union. It's interesting to note that the "hot spot" countries for cyber incidents in the report (especially France, Germany, and the Netherlands) positively correlate with the geographic concentration of the pharmaceutical and biotech companies in 2022's leading 1,000 companies in the European Union.

ENISA (the European Union Agency for Cybersecurity) attributes the increase in DDoS attacks to geopolitical developments and pro-Russian hacktivist groups such as Killnet.

U.S. life sciences organizations targeted next

Killnet targeted European hospitals before moving on to hospital targets in nearly each U.S. state. Although those cyberattacks on hospitals created the most headlines, an April 2023 report from the U.S. Department of Health and Human Services (HHS) notes the percentage of organizations targeted by Killnet with DDoS attacks was actually highest among pharmaceutical and biotechnology companies.

Given that the United States has a larger global market share of life sciences (50%) than EMEA (34%), it is reasonable to expect that the threat of DDoS attacks on pharmaceutical companies based in the United States will intensify.

But no country or geography is immune. India, one of the world's largest producers and exporters of generic medicines, suffered major consequences last year after a data breach that leaked 17 TB of company data. The ransomware gang and threat actor ALPHV/BlackCat claimed responsibility for another ransomware attack that included sensitive information on vendors, customers, and documents for 1,500 U.S. employees.

The percentage of organizations targeted by Killnet with DDoS attacks was actually highest among pharmaceutical and biotechnology companies.

Which threat actors are using which tactics?

The ENISA report cites ALPHV/BlackCat as one of the main attacker groups against life sciences in EMEA — the same group that clobbered the U.S. supply chain earlier this year.

Like Killnet, Anonymous Sudan is mentioned in the report as being politically motivated; this criminal organization first targeted provider groups but is now expanding its targets to include other parts of the healthcare ecosystem.

That expansion makes recent developments like Anonymous Sudan's claim of responsibility for recent DDoS attacks against OpenAI even more worrisome. The group says it used the Skynet botnet, which recently incorporated support for Layer 7 DDoS attacks to overwhelm applications and generate errors.

High stakes require a conservative approach

Pharmaceutical companies have long been healthcare industry leaders in the use of artificial intelligence (AI), specifically machine learning (ML), and have benefited from AI's ability to analyze large datasets for myriad applications. Those benefits include earlier detection of disease, faster drug discovery, and drug manufacturing improvements. However, similar to other industries that have embraced digital transformation (such as financial services), life sciences is at the crossroads of innovation and risk.

Pharmaceutical organizations are taking a stand. By looking at how other regulated industries handle Layer 7 DDoS attacks, Akamai researchers found that when it comes to the percentage of “deny” versus “alert” actions applied, pharmaceutical companies have conservative policies that deny anomalous activity at a high rate (Figure 3).

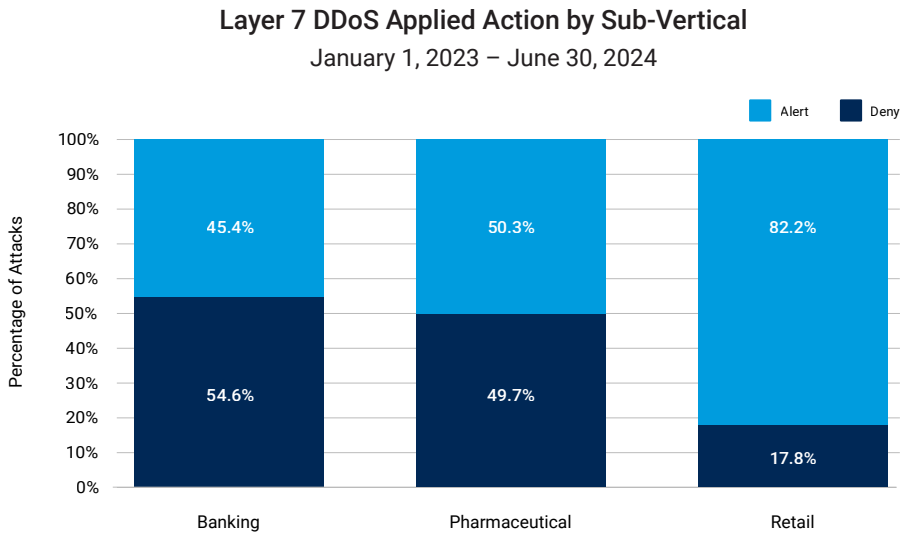


Fig. 3: Pharmaceutical and life sciences companies have a high percentage of deny versus alert actions

Since we first reported this deny versus alert statistic from January 2023 through March 2024, the rate has increased more than four percentage points, with deny actions rising from 45.5% to 49.7% — a noteworthy jump in a short period.

Other industries, such as financial services and banking, share these similarly conservative policies; both banking and life sciences are considered critical infrastructure and thus heavily regulated, which accounts for many parallels.

Additionally, in the case of pharmaceutical organizations, the consequences of a successful DDoS attack can be severe, potentially endangering people’s lives by delaying access to life-sustaining medications. It makes sense to lean into applying a deny action and then investigating the activity.

In contrast, retail takes a less aggressive stance, allowing for more time to receive an alert and assess anomalous activity before taking action. But we may see a shift to more frequent deny actions among retailers if new regulations come into play, particularly around the use of AI/ML.

Akamai researchers found that when it comes to the percentage of “deny” versus “alert” actions applied, pharmaceutical companies have conservative policies that deny anomalous activity at a comparatively high rate.

Healthcare providers are under siege

Citing the HHS analysis of data breaches published in December 2023, the chief security officer for the Health Information Sharing and Analysis Center said there were 3,604 patient records breached every hour and reported to HHS, on average.

The number of cyberattacks on providers and hospitals continues to spike. Connectivity and interoperability fueled by web applications and the mandated use of APIs can expose providers and patients to risk. Unpatched vulnerabilities and technical debt from legacy technology is a costly challenge that ransomware groups use to their advantage.

And both the ongoing threat of DDoS attacks on hospitals attributed to hacktivist groups and the geopolitical climate is disrupting patient care. All this is leading to data breaches of PHI; negative impacts on customer care; and, in some cases, patient safety issues.

Attacks pound provider organizations

Akamai research found that during the 18-month reporting period from January 2023 through June 2024, web application and API attacks against provider organizations continued at a steady pace (Figure 4). This trend will likely continue to grow, with fluctuations, as cybercriminals take advantage of both new and tried-and-true vulnerabilities inherent in evolving care models, delivery methods, and innovative systems to attack and abuse web apps and APIs.

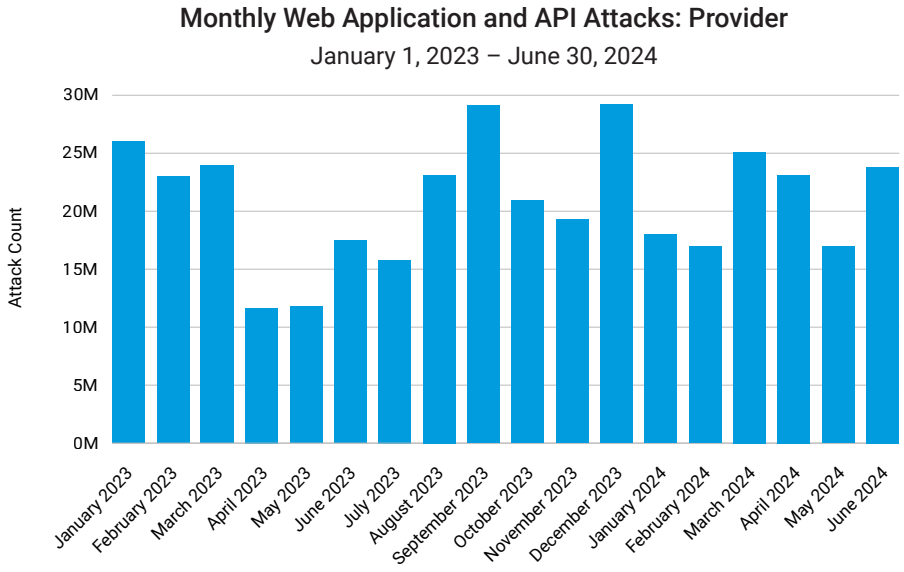
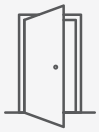


Fig. 4: Monthly web application and API attacks against provider organizations globally averaged 21 million (NOTE: One customer skewed the data and was removed for the sake of reporting)



Unpatched vulnerabilities and technical debt from legacy technology is a costly challenge that ransomware groups use to their advantage.

Care coordination enabled by data sharing and interoperability through the use of web apps and APIs allows for better clinical and financial outcomes. However, that puts the healthcare industry at significant risk as the security implications of APIs are not yet fully understood.

Balancing optimal care coordination with the risk from vulnerabilities

Because of the vast number of patient records and system connectivity points, healthcare providers need to optimize care coordination while also implementing controls to provide visibility to proactively mitigate the risk from vulnerabilities. This balance is often challenging when deploying new technologies and infrastructure like APIs.

Akamai researchers also looked at Layer 7 DDoS attacks against provider organizations during the same 18-month period, and found a steady cadence of disruption after January 2023 (Figure 5). We can attribute this, in part, to a global DDoS campaign by pro-Russian hacktivist group Killnet against healthcare, with a focus on provider organizations in the United States. Throughout the period, cybercriminals continued to leverage DDoS attacks that targeted application functionalities or the applications themselves and introduced risk to patient care.

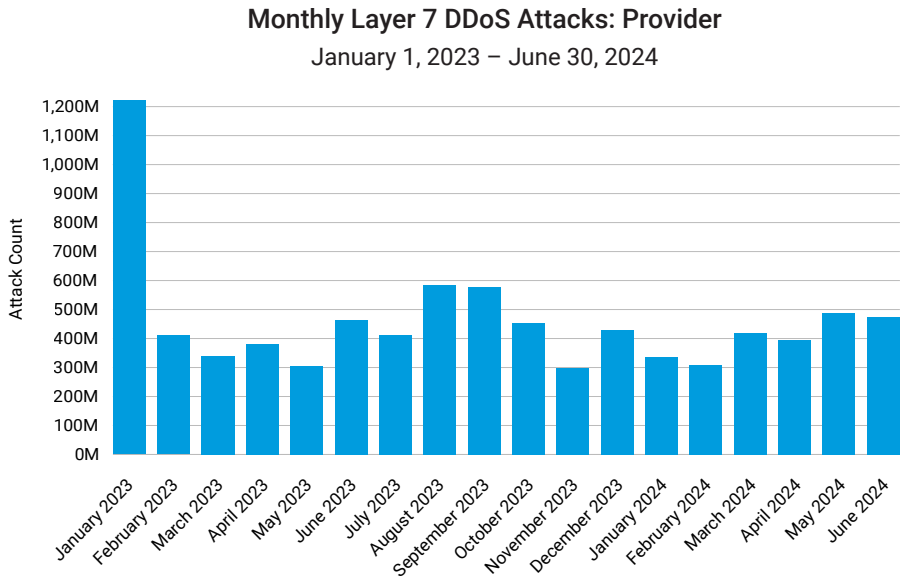


Fig. 5: With the exception of an isolated spike in January, monthly DDoS Layer 7 attacks against provider organizations globally averaged 415 million

DDoS attacks on healthcare are setting new records for scale and speed

A rise in DDoS activity, attributed to geopolitical developments and hacktivist groups, has caused outages that can threaten patient outcomes. The entire healthcare ecosystem has been affected — provider organizations were the most frequent targets in Killnet's large-scale DDoS strike in 2023. HC3 has warned that healthcare service outages of even just a few hours can affect the spectrum of day-to-day operations — from routine to critical — with potentially significant consequences.

With more healthcare interactions happening via apps, it is increasingly critical to the patient experience to get timely information and care. So, it is equally critical to make sure you have protections and processes in place.

Attacks on multiple fronts prevent care coordination

In addition to DDoS, providers face other popular attack types. Ransomware attacks that limit access to healthcare records and force ambulances to divert highlight the fact that without access to medical history, it's impossible for healthcare providers to coordinate. Reverting to paper records disrupts the tracking of patient care operations, the communication among key departments, and all ordering services.

When sensitive data is affected, provider organizations also have to deal with the impact of a data breach. Exploitation of vulnerabilities in popular software tools allow unauthorized threat actors to gain access to a treasure trove of data, from PHI to health insurance and medical information.

Patient protection must include data protection

Part of patient care is the ability to protect and control access to patient data. Traditionally, healthcare cybersecurity budgets and teams have been slim, which has contributed to data protection challenges. But as cyberattacks against healthcare provider groups continue to make headlines, the provider groups continue to improve outsourced protection partnerships and increase cyber insurance coverage.

The momentum to improve protection will continue to build as healthcare providers benefit from U.S. government policy updates that are designed to enhance resilience across critical infrastructure sectors.

Provider organizations were the most frequent targets in Killnet's large-scale DDoS strike in 2023.

Compliance considerations

The regulatory landscape increasingly requires transparency, which is driving the use of APIs. Compliance measures are imposing broad data sharing requirements on both providers and payers. This data sharing is intended to allow for the cross-pollination of clinical and financial data, which historically has been difficult for each party but is required for effective execution of value-based care (VBC).

The move toward VBC — that is, delivering care with costs in mind — is a prime example of the amount and variety of information that now needs to be shared. Payers have long held access to patient and provider financial data. But more VBC data points, like medication adherence and hospital admissions, require a continuum that's not only more innovative but more interoperable — and require a means to share this data. APIs are the conduits.

The recent CMS Interoperability and Patient Access Final Rule requires payers to maintain three main categories of APIs to keep information flowing between payers, providers, and patients:

1. Patient access API: This will increase members' access to their own medical data and likely enhance member satisfaction.

2. Provider directory API: This allows members to search for healthcare providers and facilities based on their location and medical specialty, enhancing access to care.

3. Payer-provider and payer-to-payer APIs: This can help address and reduce patient care gaps and possibly cut duplicative and costly services.

And, coming soon, the CMS Interoperability and Prior Authorization Final Rule will require impacted payers to adopt an additional prior authorization API.

Compliance measures are also dictating the format for APIs through the Fast Healthcare Interoperability Resources (FHIR) standard. These requirements and standards will simplify and streamline interoperability among systems while driving security. The FHIR expectation is that a security program exists and includes basic features such as a web application firewall, authentication, encryption, privacy, and microsegmentation.

Although providers are required to share more data than ever before, and in a standard format that enables them to connect to patient health applications (of the patients' choice) in a timely fashion, the intent of the FHIR standard is to reduce the administrative burden and increase transparency. Therefore, patients can expect an improved level of service.

Furthermore, delays in the exchange of data can result in adverse (and often costly) medical impacts, including being subjected to information blocking penalties. So, providers that have recently become cloud-modernized are now rapidly rolling out externally facing APIs in the new format to adhere to these new compliance measures.

In addition to the risk of API-focused attacks, availability attacks like DDoS and ransomware continue to have major impacts across all industries, and the healthcare sector is one that may be heavily affected. The regulations that aim to address these types of attacks tend to focus on resilience. For instance, in the United States, the HHS has released a Healthcare Sector DDoS Guide. In addition, the nonprofit Healthcare Information Sharing and Analysis Center has published a white paper on the issue of resilience in the healthcare sector titled Resilience is in our DNA.

Akamai

Taking action: Mitigation recommendations

API security is more important than ever from a risk management and compliance perspective. However, because of API sprawl, it has become increasingly challenging to identify, catalog, and protect healthcare APIs. Additionally, healthcare organizations must defend against DDoS attacks that threaten service availability.

You can not defend against attacks you are not aware of. Therefore, first, you need to discover all assets so you can include them in your security program. Then, you need to know what vulnerabilities exist and have situational awareness with respect to what is happening relative to both performance and security. Finally, you need to validate your systems' security through both automated and classical pen testing.

Meeting the following API and DDoS protection strategy milestones can help you achieve a strong security program.

Five API protection strategy milestones

Adopting a strong API security program helps you improve visibility into all your APIs and understand your exposure to risk, so you can ramp up protection.

1. Remove infrastructure blind spots by systematically discovering rogue or shadow APIs, and ensure that each one is either decommissioned or incorporated into API security controls.

2. Determine and harden risk posture by analyzing common alert types and correcting flaws in API code, addressing misconfiguration issues, and implementing processes to prevent future vulnerabilities based on lessons learned.

3. Sharpen threat detection and response by understanding normal behavior and identifying potential abuse based on spikes in API security alerts. Then, engage well-defined response procedures to bring risk and alert volume down to normal levels.

4. Partner with vendors that provide both training and expertise. They should offer a range of services from project-based support to fully managed services that can help correctly configure and manage complex and integrated cybersecurity solutions.

Adopting a strong API security program helps you improve visibility into all your APIs and understand your exposure to risk, so you can ramp up protection.

5. Develop a stronger offense by establishing a formal API threat hunting discipline with the goal of identifying possible threats before they escalate to a reactive scenario.

Four DDoS protection strategy milestones

With new records being set for DDoS attacks against Layer 7 web pages and APIs, Layers 3 and 4 infrastructure, and DNS systems, it is critical to ensure the availability of your services and capabilities. Today, that means having active protections in place that can meet the size, scope, and speed of the latest attacks.

1. Have a system in place that provides visibility and rapid response to attacks. This should cover Layer 7, Layers 3 and 4, and DNS infrastructure.

2. Back up your on-prem DDoS protection with a hybrid DDoS mitigation platform that protects against attacks that overload your on-prem appliances.

3. Engage providers or use systems that allow you to easily manage policies and maintain IP allowlists that provide actionable analytics in real time to help you adopt a proactive security posture.

4. Validate your alerting, protection capabilities, and crisis management processes via testing, and ensure that all your infrastructure is behind appropriate protections.

For more information, read our latest research or our blog.

With new records being set for DDoS attacks against Layer 7 web pages and APIs, Layers 3 and 4 infrastructure, and DNS systems, it is critical to ensure the availability of your services and capabilities.

Methodology

Web application and Layer 7 DDoS attacks

This data describes application-layer alerts on traffic seen through our web application firewall (WAF). The web application attack alerts are triggered when we detect a malicious payload within a request to a protected website, application, or API. The Layer 7 DDoS alerts are triggered when we detect volumetric anomalies in the number of requests to a protected website, application, or API. These alerts can be triggered by both malicious and benign requests. Typically the requests themselves are benign, but the high volume of requests indicates malicious intent. The alerts do not indicate the successfulness of an attack. Although these products allow a high level of customization, we collected the data presented here in a manner that does not consider custom configurations of the protected properties.

The data was drawn from an internal tool for analysis of security events detected on Akamai Connected Cloud, a network of approximately 340,000 servers in more than 4,000 locations on nearly 1,300 networks in 130+ countries. Our security teams use this data, measured in petabytes per month, to research attacks, flag malicious behavior, and feed additional intelligence into Akamai's solutions.

This data covered the 18-month period from January 1, 2023, through June 30, 2024.

2024 data update

We are happy to announce some updates to our datasets for our 10th anniversary. Our web application and bot attack datasets have received a few updates. The collection method for each has been transformed, streamlined, and optimized. The range and depth of our insights has been broadened. Classifications for additional attack vectors, such as SSRF, have been added. Identification of attacks targeting API endpoints have also been added to each dataset. We enjoyed highlighting some of these new improvements in this report, and we are looking forward to continuing to share these updates throughout the year and beyond as we celebrate this SOTI/Security milestone with our readers.

Akamai

Credits

Research director

Mitch Mayne

Editorial and writing

Neil Jennings
Chris Notaro
Charlotte Pelliccia
Badette Tribbey
Maria Vlasak
Steve Winterfeld

Review and subject matter contribution

Claire Broome
Shane Keats

Data analysis

Chelsea Tuttle

Promotional materials

Barney Beal

Marketing and publishing

Georgina Morales Hampe
Emily Spinks

More State of the Internet/Security

Read back issues and watch for upcoming releases of Akamai's acclaimed State of the Internet/Security reports. **akamai.com/soti**

More Akamai threat research

Stay updated with the latest threat intelligence analyses, security reports, and cybersecurity research. **akamai.com/security-research**

Access data from this report

View high-quality versions of the graphs and charts referenced in this report. These images are free to use and reference, provided that Akamai is duly credited as a source and the Akamai logo is retained. **akamai.com/sotidata**

More on Akamai solutions

To learn more information on Akamai solutions for threats targeting the healthcare industry, visit our **healthcare & life sciences page**.

Akamai