SOTI

10 YEARS
OF SECURITY INSIGHT

V10 ISSUE 01

Attack Trends Shine Light on API Threats

EMEA Snapshot

Akamai

State of the Internet/Security

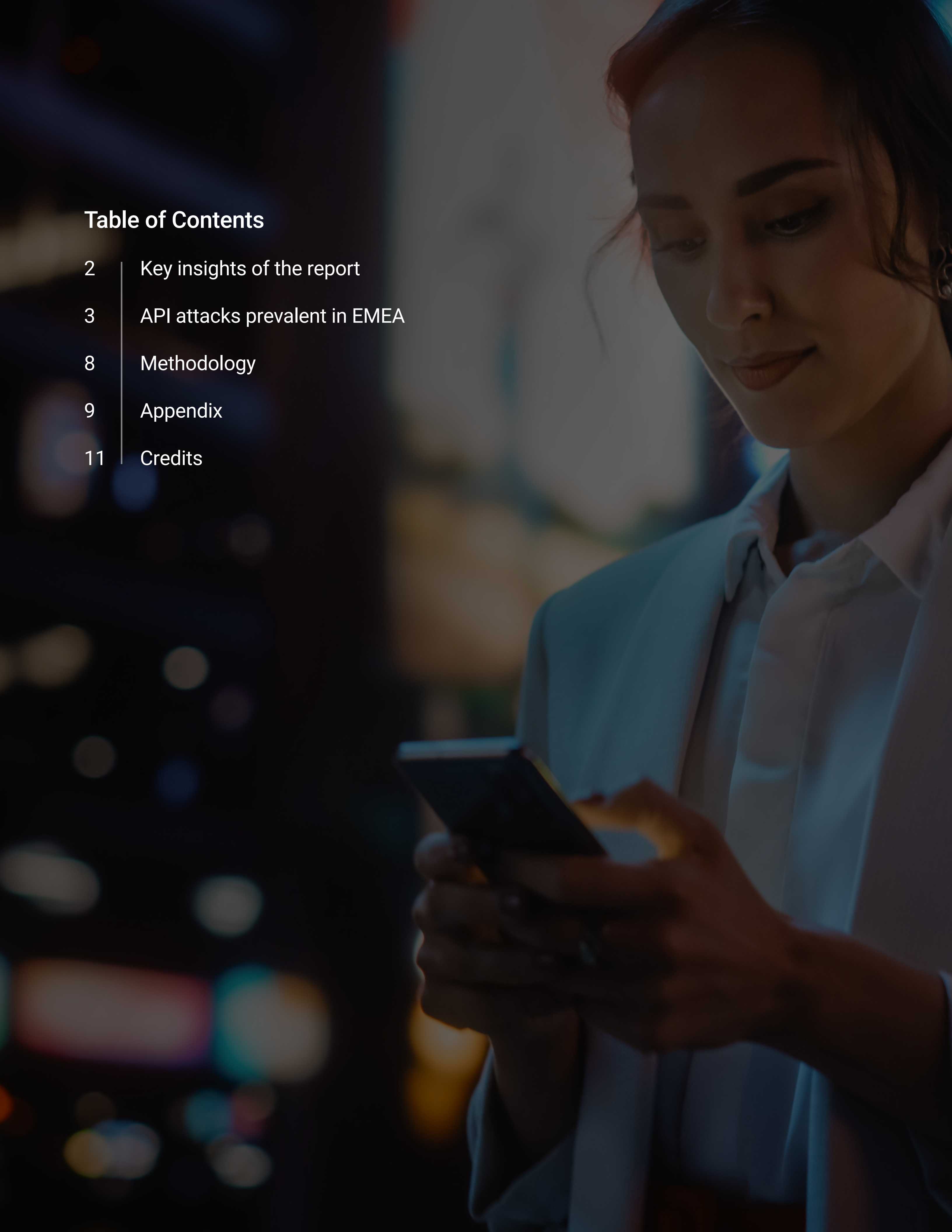


Table of Contents

Key insights of the report

The EMEA Snapshot is a companion piece to our larger API Security SOTI report, Lurking in the Shadows: Attack Trends Shine Light on API Threats (available in English only). Please refer to that report for detailed descriptions of how adversaries leverage the attack vectors we discuss in this snapshot, recommendations to safeguard your organization, and an explanation of our research methodologies and new dataset.

Overview

As digital innovation and the API economy improve employee and customer experiences, they also present cybercriminals with new opportunities for exploitation. Attacks focused on APIs can lead to financial, brand, and reputational damage, as well as a loss of confidential data and customer trust. Given the expected surge in volume of API attacks and increasing cybersecurity regulatory oversight and reporting obligations as APIs are increasingly being used to exchange sensitive financial information, API security is more important than ever.

To better understand the API threat landscape, instead of looking at web application and API attacks as a whole, in 2024 we are using a new dataset that allows Akamai researchers to distinguish between the two attack types and focus on the percentage of attacks that target APIs. In this EMEA Snapshot, which spans the 12 months from January through December 2023, we delve into attack trends and what they mean for you.

- On a global basis, the Europe, Middle East, and Africa (EMEA) region had the highest percentage of web attacks targeting APIs at 47.5% — notably higher than the next closest region, North America at 27.1%.
- Consistent with the global trend, HTTP Protocol attack (HTTP) and Structured Query Language Injection (SQLi) are the predominant attack vectors for APIs in EMEA during the last 12 months.
- Bot requests are also an area of concern: 40% of the nearly four trillion suspicious bot requests targeted APIs.
- In the commerce industry, nearly three-quarters (74.6%) of all web attacks that impacted organizations were API attacks — more than twice the percentage of the next closest industry, high tech (35.5%).

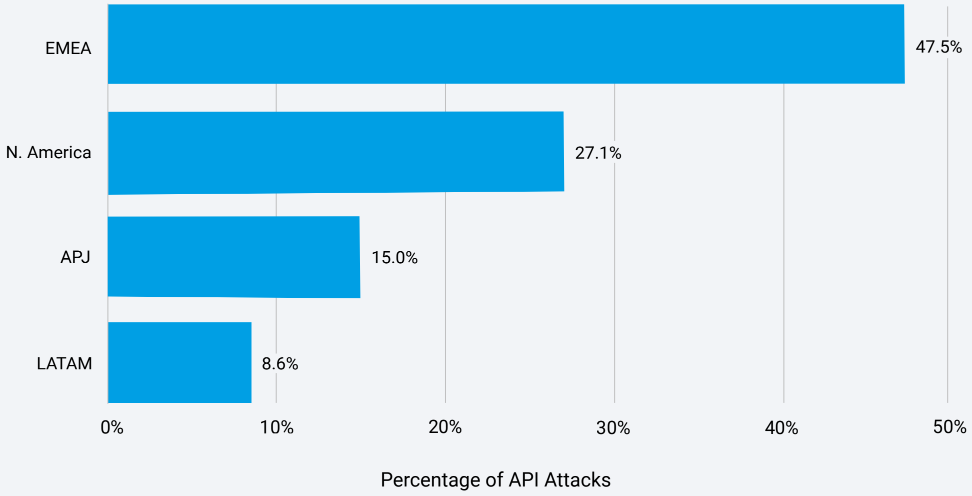
API attacks prevalent in EMEA

By leveraging a new dataset that specifically tracks API attack traffic, Akamai research revealed that the EMEA region has the highest percentage of API attacks on a global basis at 47.5% — by far exceeding the next closest region, North America at 27.1% (EMEA Figure 1). This is based on the total number of web attacks in each region and shows that APIs are in more danger in EMEA than in other regions.

API Attacks by Region

January 1, 2023 – December 31, 2023

EMEA Fig. 1: Web attacks are significantly more likely to

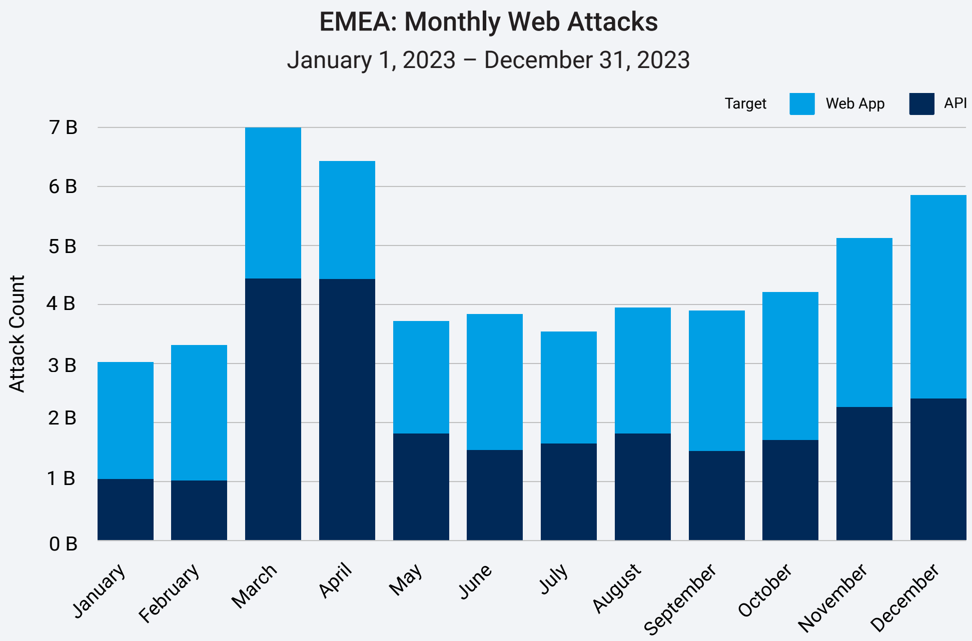


target APIs in EMEA than in any other region

We may be able to attribute this relatively high percentage of attacks in EMEA (when compared with the percentage of attacks on other regions) in part to the relatively large open API market size versus North America and Asia-Pacific, reflecting higher API adoption rates in EMEA, as well as to open banking and the Payment Card Industry Data Security Standard (PCI DSS) v4.0 that are driving the use of APIs and can introduce the security risks discussed in the global report.

Within EMEA, the areas with the highest percentage of web attacks that target APIs are Spain (94.8%), Portugal (84.5%), the Netherlands (71.9%), and Israel (67.1%). This is not to say that the number of web attacks overall is higher in these countries than in others in EMEA — rather, these countries face a much more concentrated risk from API abuse because of attackers' focus on that vector.

The monthly trends during the reporting period from January through December 2023 show that web attacks that targeted APIs in EMEA increased fairly steadily, starting at 34% in January and rising to 41% by the end of the year (EMEA Figure 2). The exceptions were in March and April when Akamai researchers saw a spike in API attacks as the commerce sector in Spain — a country with an already huge API attack concentration — experienced large-scale, focused attacks. This spike shows how quickly attackers can shift their focus among regions and industries, so it is worth tracking broader trends.

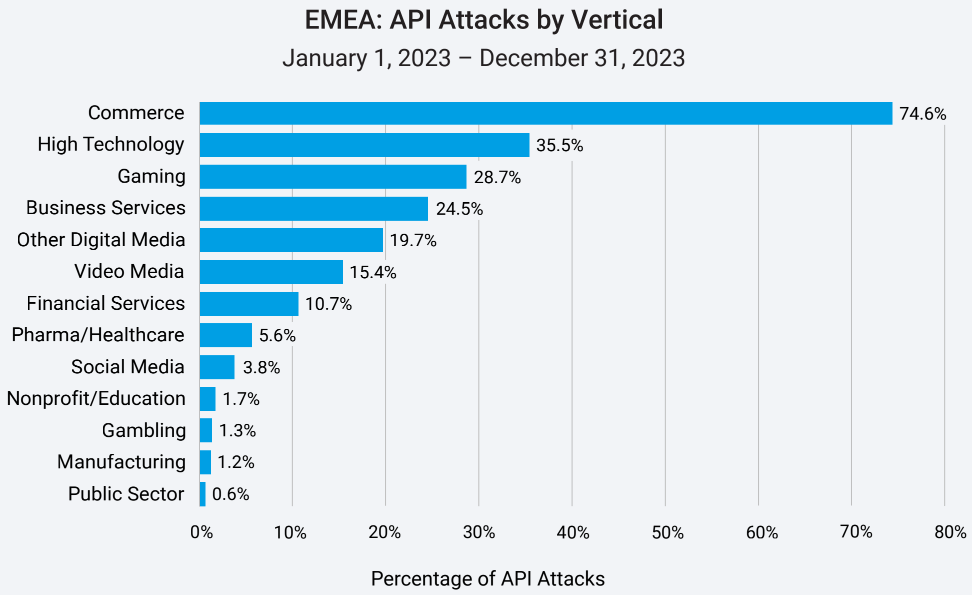

EMEA: Monthly Web Attacks

January 1, 2023 – December 31, 2023

EMEA Fig. 2: With the exception of March and April, when API attacks spiked, API attacks slowly increased throughout 2023, rising to 41% of all attacks by the end of the year

API attacks across industries

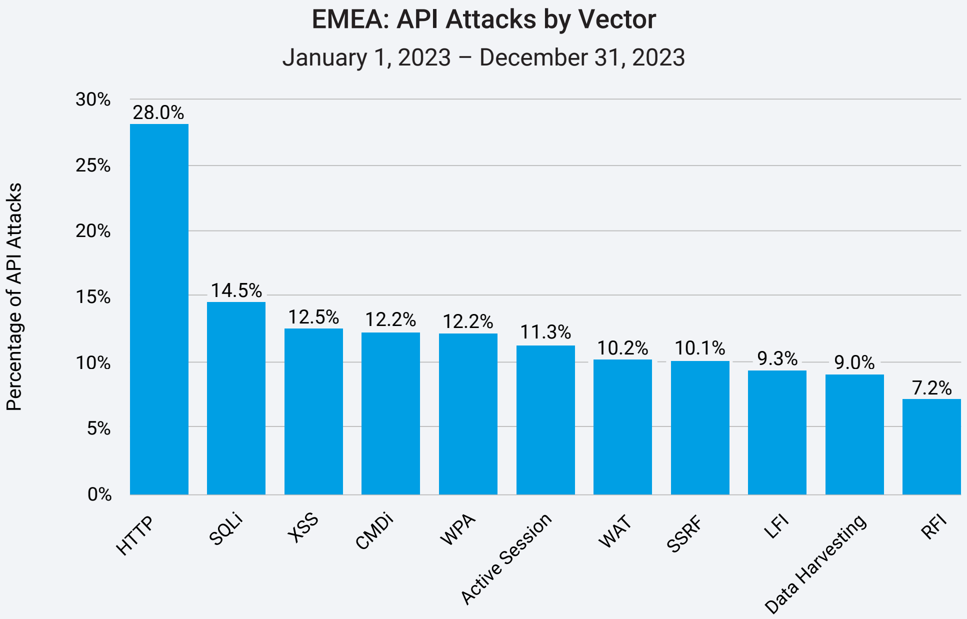
During the reporting period, Akamai researchers found that the commerce industry had the highest percentage of overall web attacks that impacted organizations at 74.6%, which is more than twice the percentage of the next closest industry — high tech at 35.5%. They were followed by gaming at 28.7%, business services at 24.5%, and other digital media at 19.7% (EMEA Figure 3).



EMEA Fig. 3: The commerce vertical had the highest percentage of API attacks, partially due to the complex nature of its ecosystem, its high reliance on APIs, and the valuable data organizations in this sector possess

APIs under attack: Traffic analysis

Consistent with the global trend, HTTP and SQLi have been the predominant ways in which adversaries have targeted APIs in EMEA during the last 12 months, and Local File Inclusion (LFI) has moved further down the list in comparison with its dominance in web application attacks (EMEA Figure 4).



EMEA Fig. 4: HTTP, SQLi, and XSS are the most relevant vectors to API attacks; LFI is less prevalent for API attacks, but still actively used for attacks against web applications

In EMEA, Cross-Site Scripting (XSS) remains a favored technique, even for API attacks, and Command injection (CMDi) is also prevalent. The new dataset enables us to monitor for additional attack vectors in APIs. For example, Server-Side Request Forgery (SSRF; which we discussed in our 2023 report) is now an up-and-coming vector. (See the appendix for a complete list of attack vector definitions.)

Our research also revealed that bot requests are an area of concern. During the same 12-month reporting period, 40% of the nearly four trillion suspicious bot requests were aimed at APIs.

Conclusion

Defending APIs is a clear imperative from a security and risk management perspective. In addition, the existing laws and regulations and emerging reforms to keep cybersecurity legislation apace with the threat landscape also make it imperative to protect APIs.

For example, the European Union's Global Data Protection Regulation (GDPR) is focused on the protection of personal data, and APIs are now at the forefront of how this data is used and shared. Additionally, the new Network and Information Security Directive (NIS2) specifically calls for the establishment of a robust API security program. Outside the EU, countries such as Saudi Arabia have introduced data protection laws similar to the GDPR, which create obligations for entities dealing with personal data. Additionally, Section 6 of the upcoming Payment Card Industry Data Security Standard (PCI DSS) v4.0 specifically includes new standards on the use of APIs in the development and maintenance of systems and software to reduce the risk of data compromise.

As regulators put initiatives and policies in place to strengthen cybersecurity standards for APIs, it is important to understand best practices and guidelines so that you can integrate APIs into your security program to improve visibility, strengthen defenses, and map to compliance requirements.

For more information, please refer to the global API security SOTI report, Lurking in the Shadows: Attack Trends Shine Light on API Threats.

Methodology

Web application and bot attacks

This data describes application-layer alerts on traffic seen through our web application firewall (WAF) and bot management tool. The web application attack alerts are triggered when we detect a malicious payload within a request to a protected website, application, or API. The bot alerts are triggered when we detect a bot payload within a request to a protected website, application, or API. These bot alerts can be triggered by both malicious and benign bots. 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 global network of 4,000+ edge points of presence 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.

The data in this report covered the 12-month period from January 1, 2023, through December 31, 2023.

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 upgrades. The collection method for each has been transformed, streamlined, and optimized. The range and depth of our insights have 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 State of the Internet/Security milestone with our readers.

Akamai API Security insights

Special thanks to our Akamai API Security Solution Engineering team for their contributions of real-world insights with a look into API risks and their potential impacts based on our API Security alerts.

Appendix

Attack Vector	Definition
Active Session	Attack traffic has been recently flagged for the client and repeated requests will be blocked for the duration of the session
Command injection (CMDi)	An adversary injects new items into an existing command to modify the interpretation away from what was intended and toward actions of their choosing
Cross-Site Scripting (XSS)	An adversary embeds malicious scripts in content so that the target software executes the scripts with the users' privilege levels when the content is served to web browsers
Data Harvesting	An adversary exploits weaknesses in the design or configuration of the target and its communications to get it to reveal more information than intended; this is often executed to gather data in preparation for another type of attack, but gaining access to the information may also be the end goal of the adversary
HTTP Protocol (HTTP)	An adversary takes advantage of weaknesses in the protocol by which a client and server are communicating to perform unexpected actions; exploiting different types of protocols can lead to different end goals of attacks
Local File Inclusion (LFI)	An attacker manipulates inputs to the target software to gain access to, and perhaps modify, areas of the file system that were not intended to be accessible

Attack Vector	Definition
Remote File Inclusion (RFI)	The adversary loads and executes remote arbitrary code, subsequently hijacking the targeted application and forcing it to execute their own instructions
Server-Side Request Forgery (SSRF)	The attacker abuses the functionality of the server to read or update internal resources
Structured Query Language injection (SQLi)	An attacker crafts input strings so that when the target software intends to construct SQL statements based on user input, the resulting SQL statement instead performs actions the attacker intended; successful injections can cause information disclosure as well as the ability to add or modify data in the database
Web Attack Tool (WAT)	An adversary actively probes the target in a manner that is designed to solicit information that could be leveraged for malicious purposes; as a result of these probes, the adversary is able to obtain information from the target that aids the attacker in making inferences about its security, configuration, or potential vulnerabilities
Web Platform Attack (WPA)	An attack against a software platform (cloud, web, or application layer) that is not categorized in another attack group

Credits

Editorial and writing

Badette Tribbey – Editor in Chief
Charlotte Pelliccia – Lead Writer (regionals)

Editorial contributors

James Casey
Edward Roberts
Steve Winterfeld

Review and subject matter contribution

Tom Emmons
Reuben Koh
Rob Lester
Richard Meeus
Abigail Ojeda
Menachem Perlman
Yariv Shivek

Data analysis

Chelsea Tuttle

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 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 API attacks, visit our **App and API Security page**.

Akamai protects your customer experience, workforce, systems, and data by helping to embed security into everything you create — anywhere you build it and everywhere you deliver it. Our platform's visibility into global threats helps us adapt and evolve your security posture — to enable Zero Trust, stop ransomware, secure apps and APIs, or fight off DDoS attacks — giving you the confidence to continually innovate, expand, and transform what's possible. Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on X, formerly known as Twitter, and LinkedIn.

Published 03/24.