SOTI

V10 ISSUE 01

10 YEARS
OF SECURITY INSIGHT

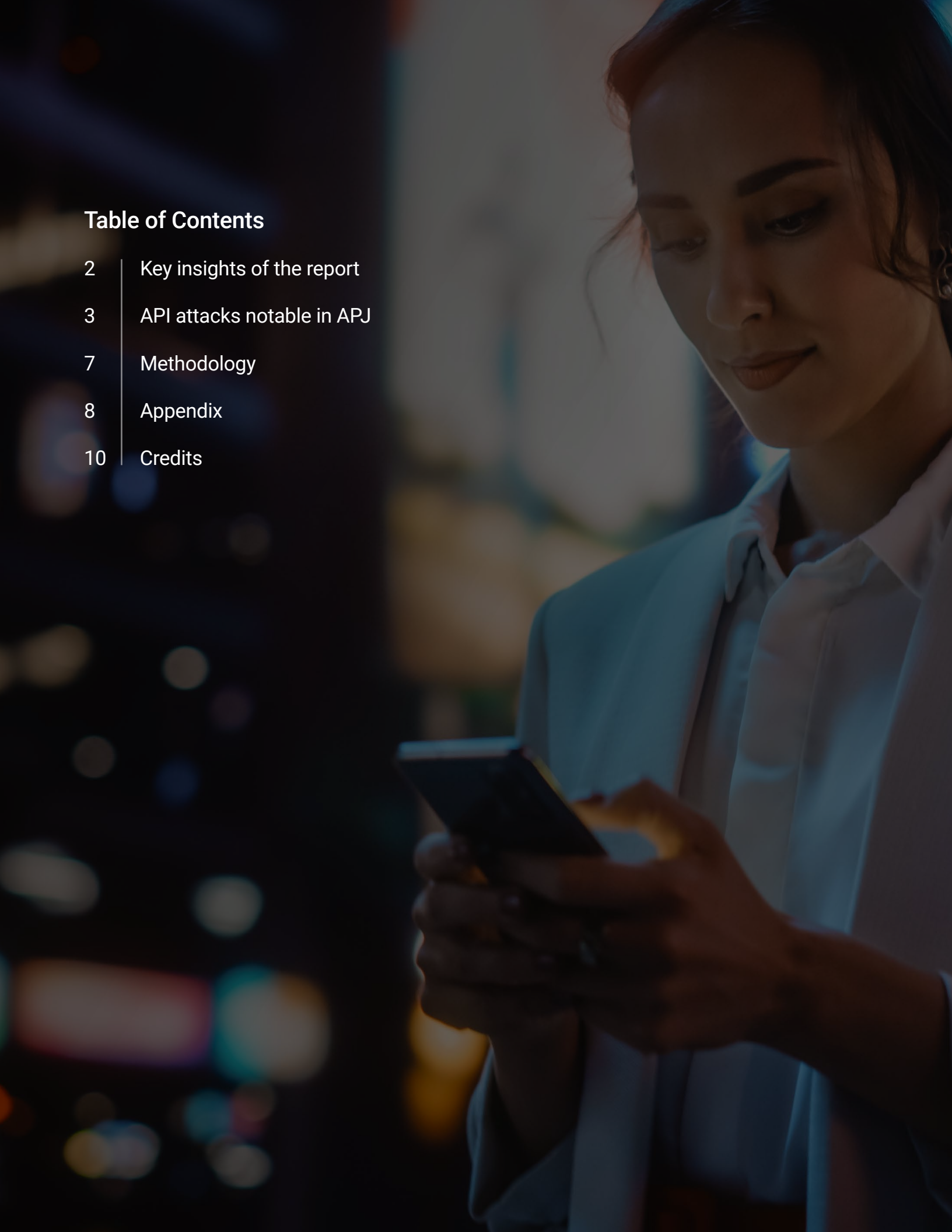
Attack Trends Shine Light on API Threats

APJ Snapshot

Akamai

State of the Internet/Security

Table of Contents



Akamai

Key insights of the report

The APJ 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 APJ 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 Asia-Pacific and Japan (APJ) region had the third highest percentage of API attacks at 15.0%, behind the Europe, Middle East, and Africa (EMEA) region at 47.5% and North America at 27.1%.
- Consistent with previous reports in which we looked at overall web attacks, Local File Inclusion (LFI) remains a prevalent attack vector in APJ for APIs. Additionally, the new dataset reveals that Command Injection (CMDi) and Server-Side Request Forgery (SSRF) are also popular techniques in API attacks.
- Bot requests are also an area of concern: 40% of the more than two trillion suspicious bot requests were aimed at APIs.
- The manufacturing industry had the highest percentage of API attacks at 31.2%, followed by gaming (25.2%), high tech (24.4%), video media (24.4%), and commerce (22.3%).

API attacks notable in APJ

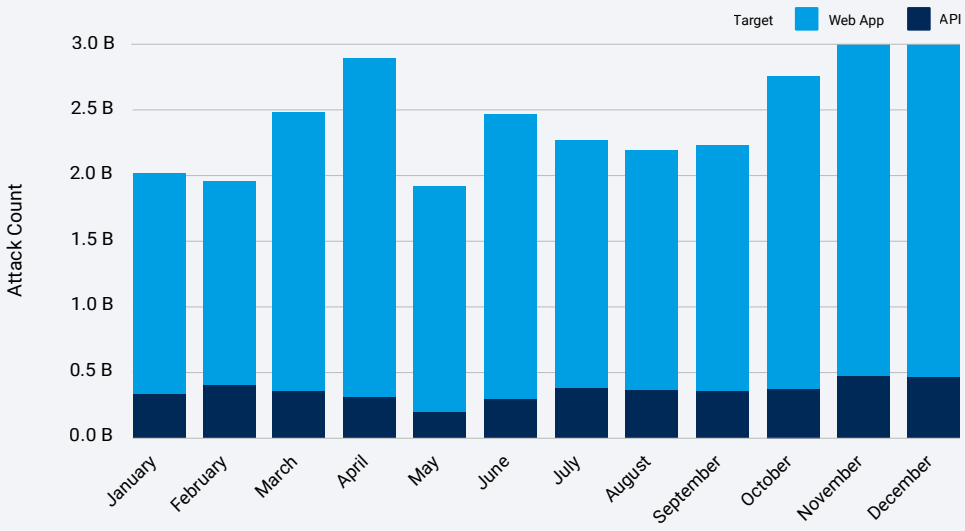
By leveraging a new dataset that specifically tracks API attack traffic, Akamai research revealed that 15.0% of all overall web attacks in the APJ region targeted APIs. On a global basis, the APJ region had the third-highest percentage of API attacks behind the EMEA region at 47.5%, and North America at 27.1%.

During the reporting period from January through December 2023, web attacks targeting APIs fluctuated between 11% and 21% on a monthly basis (APJ Figure 1). We may be able to attribute this relatively low percentage of attacks (compared with the percentage of attacks on other regions) in part to the relatively small open API market size versus Europe and North America and thus lower adoption rates by organizations in APJ.

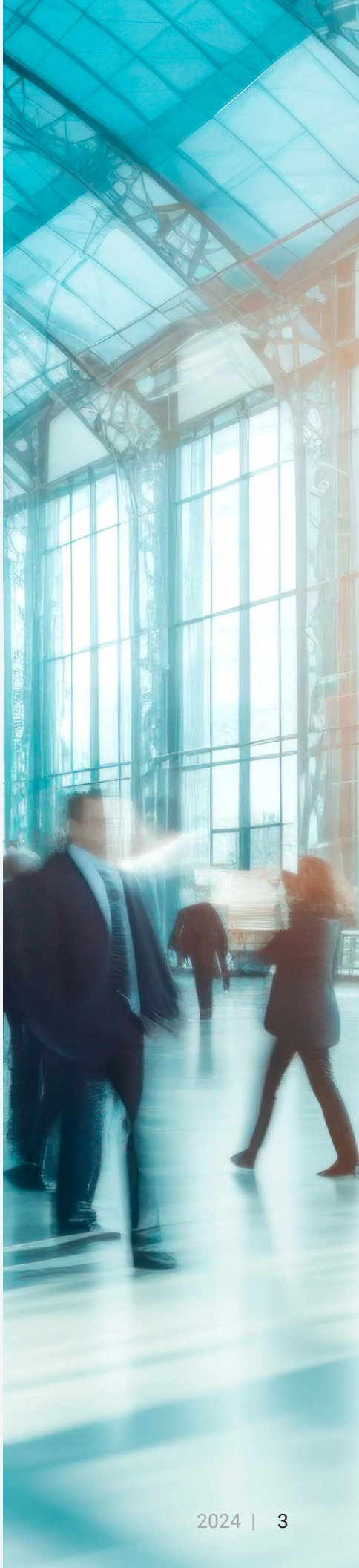
APJ: Monthly Web Attacks

January 1, 2023 – December 31, 2023

APJ Fig. 1: Attacks targeting APIs averaged 15.0%, even as overall web attacks increased

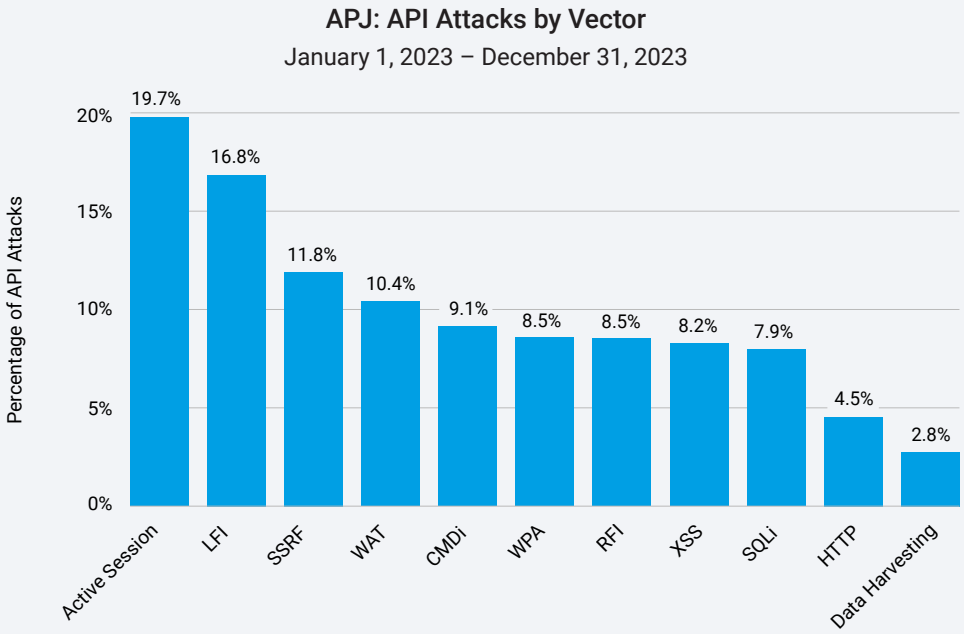


Within APJ, the areas with the highest percentage of web attacks targeting APIs were South Korea (47.9%), Indonesia (39.6%), Hong Kong SAR (38.7%), Malaysia (26.4%), Japan (23.4%), India (19.0%), Australia (15.6%), Singapore (5.8%), the Philippines (5.5%), and New Zealand (4.8%).



APIs under attack: Traffic analysis

Consistent with previous reports in which we looked at overall web attacks, LFI remains a top attack vector for APIs in APJ. However, Cross-Site Scripting (XSS) and Structured Query Language Injection (SQLi) have moved further down the list as related to API attacks specifically (APJ Figure 2).



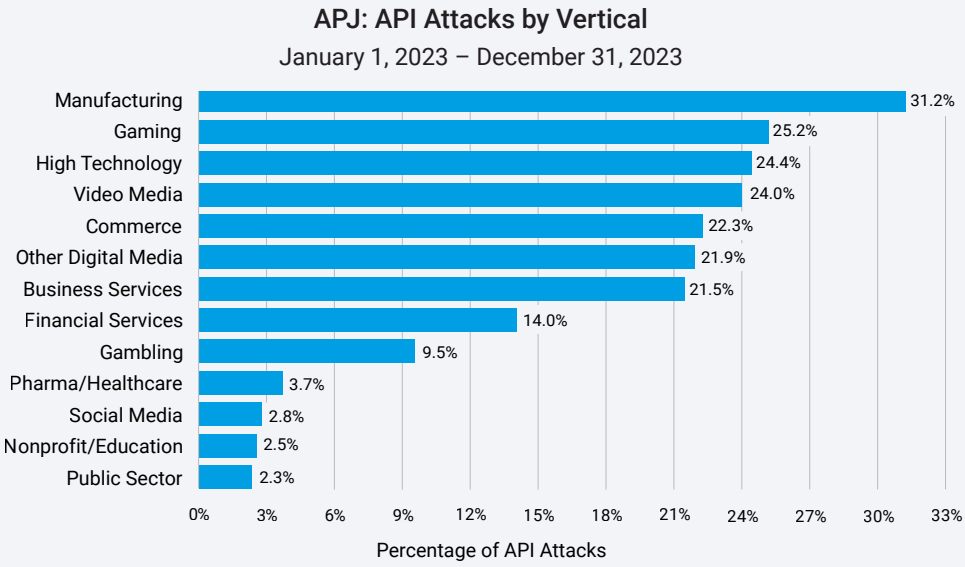
APJ Fig. 2: LFI remains a prevalent attack vector and our new dataset reveals additional favored attack techniques against APIs

The new dataset enables us to surface additional favored API attack vectors. For example, CMDi is a popular technique in API attacks, and SSRF (which we discussed in our 2023 report) is now among the most frequently used vectors. Of note, Active Session indicates suspicious behavior during that session, which results in a temporary block. (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 more than two trillion suspicious bot requests were aimed at APIs.

API attacks across industries

During the reporting period, Akamai researchers found that the manufacturing industry had the highest percentage of overall web attacks that targeted APIs at 31.2%, followed by gaming at 25.2%, high tech at 24.4%, video media at 24.0%, and commerce at 22.3% (APJ Figure 3).



APJ Fig. 3: The manufacturing vertical had the highest percentage of API attacks, partially due to the increasing connectivity of this critical infrastructure sector via APIs and the potential for supply chain disruption

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, India is in the process of drafting the Digital India Bill, which will be a major overhaul of the IT Act, starting with the passing of the Digital Personal Data Protection Act in August 2023. The Australian government released the 2023-2030 Australian Cyber Security Strategy on November 23, 2023, with a pillar focused on safe technology and ensuring trust in digital products and software. 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 compromise.

Regulators are putting initiatives and policies in place to strengthen cybersecurity standards for APIs, which are increasingly being used to exchange sensitive financial information. Understanding best practices and guidelines is important 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.

Akamai

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**.