API: The Attack Surface That Connects Us All

[State of the Internet] / Security

Volume 7, Issue 4
Executive Summary

In this edition of the State of the Internet / Security report, we dive into the security of application programming interfaces (APIs). “By 2022, API abuses will move from an infrequent to the most-frequent attack vector, resulting in data breaches for enterprise web applications.”¹

In addition to our own research, we’ve partnered with Veracode for this report, as their insights into the application security space helped further our research into APIs and development challenges. Veracode’s Chief Research Officer, Chris Eng, wrote the guest essay in this report. He examines the (often repeated) patterns in security that are now impacting API security.

“This report focuses on API security, and if you’ve spent any time looking at APIs, you already know that security is too often an afterthought. The first rule of writing secure software is don’t make assumptions about how people will interact with the finished product.”

— Chris Eng, Chief Research Officer, Veracode

Concerning the state of attacks online, we looked at 18 months of attack traffic between January 2020 and June 2021. In June 2021, on a single day, Akamai observed 113.8 million attacks. That’s more than three times the number of attacks that we saw during the same time frame in 2020. With 6.2 billion attempts on record, SQL Injection (SQLi) remains at the top of the web attack trending list, followed by Local File Inclusion (LFI) with 3.3 billion, and Cross-Site Scripting (XSS) with 1.019 billion.

Credential stuffing has been the source of a steady stream of attacks so far this year, with both dips and peaks in the first two quarters. Akamai observed two notable peaks in January and May 2021, when the number of credential stuffing attacks surged past 1 billion. Coincidentally, the two peaks were recorded on the second day of each month; there is no indication as to why criminals were hitting their hardest on this particular day of the month.
The United States was the top target for web application attacks during this observed period, with nearly six times the amount of traffic than the United Kingdom, which ranked second. The United States was also in the top spot on the source list for attacks, taking first place away from Russia, with almost four times the amount of traffic.

Distributed Denial-of-Service (DDoS) traffic has remained consistent in 2021 so far, with peaks recorded earlier in Q1 2021. In January, Akamai recorded 190 DDoS events in a single day, followed by 183 in March.

Application security, either on the API side or the web application development side, is a complex mash-up of features, functions, and business demand. Finding balance within this realm isn’t as easy as one would think.

While teams are moving toward having security baked into the development lifecycle, the process is slow. This leaves organizations behind the eight ball and forces them in some cases to launch known vulnerable code into the wild, because the business use for said code is critical.

In addition to the research in this report, there are a few recommended practices in Appendix A, so you can help protect yourself, your business, and the APIs that you interface with.

Within this report, Akamai cited Gartner analysis and research data. The information attributed to them came from the following report:

1) Gartner ID: G00404900, 01-March-2021 API Security: What You Need to Do to Protect your APIs

To dive deeper into this research, read the full State of the Internet / Security report.

API: The Attack Surface That Connects Us All

Visit www.akamai.com/soti