Visibility into API Deployment

BLOG IN **API SECURITY**

BY **SYDNEY COFFARO**

Aug 16, 2021

APIs are becoming increasingly prevalent in the web applications we use each day. As the number of APIs increase across sites, the endpoints that are unsecured can be easily exploited by attackers.

There is usually a dangerous gap between the APIs that development teams *think* are deployed and the APIs that are *actually* trafficked. When trying to wrap your arms around your API attack surface, organizations must consider not only the legitimate API endpoints deployed behind their sites, but also rogue and zombie APIs – depreciated or misconfigured API endpoints left behind in production – which are ripe for exploitation.

Tension leads to API Vulnerabilities

The long-standing tension between developers and security teams is exacerbated by this potential risk. Rogue and zombie APIs expose enterprises to attack, and erode an organization's security posture. For highly distributed and horizontally scaled projects, it's frighteningly easy to let an endpoint "slip" into production after sound business logic testing, but absent vulnerability scanning or static analysis. These abandoned APIs that are exposed to both legitimate and malicious traffic are backdoors, and hackers will rattle those doorknobs trying to break it.

Overcoming Challenges with API Observability

The increased exploitation of APIs has shifted the dialogue from API *security* towards the concept of API *observability*. Organizations need to see what traffic the endpoints are seeing, and the details of that traffic; things like the methods used in calls and the keys passed to endpoints.

Organizations also need to understand the overall health of the production endpoint or system, making status code heuristics critical to their situational awareness. This observability will help security teams understand whether they are combatting a massive bot attack, or simply debugging a failed login.

Need to secure your API endpoints? ThreatX is here to help

profiles API endpoints, providing users with enhanced visibility into legitimate, rogue and zombie APIs in production.

Click here to learn more about how ThreatX can help your organization protect your modern web applications or set up a live demo today!

Tags

APIS ENDPOINTS OBSERVABILITY ROGUE APIS ZOMBIE APIS

About the Author

Sydney Coffaro
Experienced subject-matter expert focused in Cyber Security Automation, Incident Response, APIs, and Application Security with a demonstrated history of working in fast-passed early stage startups. Sydney is a certified Product Manager, Scrum Master, and has led technical sales initiatives for go to customer teams that resulted in the acquisition of hundreds of customers.

Ready to get started?

REQUEST A DEMO

SRC CYBER SOLUTIONS LLP THREATX REQUEST A DEMO

Contact Us
www.srccybersolutions.com
+91 120 232 0960 / 1
sales@srccybersolutions.com

Newsletter Sign Up →