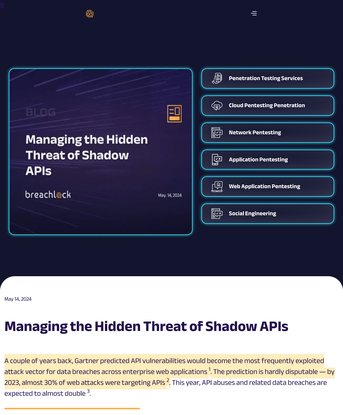

May 14, 2024

Managing the Hidden Threat of Shadow APIs

A couple of years back, Gartner predicted API vulnerabilities would become the most frequently exploited attack vector for data breaches across enterprise web applications [1]. The prediction is hardly disputable — by 2023, almost 30% of web attacks were targeting APIs [2]. This year, API abuses and related data breaches are expected to almost double [3].

Why APIs and API Security Matter

APIs act as pre-built conduits that allow different applications and systems to communicate and interact with each other. They allow developers to integrate functionalities of existing software components and services without having to write everything from scratch. With the rise of cloud and microservices, APIs have essentially become the glue that holds together different parts of distributed applications and systems

As APIs increasingly handle sensitive data and power mission-critical business capabilities, they have become a lucrative target for cybercriminals. Their complex nature and lack of standardization and governance make them an easy one, too. Modern applications may rely on many APIs, creating a vast attack surface for malicious actors.

To demonstrate the potential impact of API attacks, consider the June 2021 LinkedIn data breach [4]. An authentication-free API allowed malicious actors to scrape data from 700 million LinkedIn users, including sensitive information like email addresses and phone numbers, all in a single breach. The data was sold at dark web forums, posing a significant risk for targeted phishing attacks. Similarly, in January 2023, T-Mobile suffered a data leak affecting 37 million users in an API attack [5].

Given the prevalence and consequences of API attacks, OWASP API Security Project periodically updates its list of the top 10 most critical API and application security vulnerabilities and provides best practices and tools for securing APIs throughout the Software Development Life Cycle (SDLC). However, shadow APIs present a different kind of challenge — you can't protect what you can't see.

What are Shadow APIs?

Shadow APIs are undocumented and unauthorized APIs that exist and operate in an organization without the knowledge or approval of IT and security teams. While organizations are actively investing in the security and governance of their API ecosystem, shadow APIs bypass those official, monitored channels and established governance processes to create hidden backdoor connections into the organization's systems.

Shadow APIs can exist in a digital ecosystem for many reasons, such as:

- **Faster development:** Developers may build or integrate APIs hastily without following tedious governance and security processes to meet deadlines.
- **Flexibility and innovation:** Developers may knowingly create shadow APIs as a workaround to rigid and restrictive IT policies.
- **Internal testing:** APIs created for testing or as a proof-of-concept (PoC) may end up being used in production without proper oversight.
- **Third-party SaaS:** Organizations may be unaware of APIs embedded in external apps, services, and SaaS.

The Security Risks of Shadow APIs

While intentions behind building or integrating shadow APIs may initially appear benign, they pose significant security risks and present unique challenges for security teams:

- Shadow APIs create a hidden attack surface. Attackers can discreetly exploit shadow APIs and the applications using them.
- Without documentation and oversight, IT and security teams simply cannot assess the security posture of shadow APIs.
- They can expose organizations to vulnerabilities that they wouldn't know to patch. For instance, a shadow API may be using the Log4j library in an organization that does not directly use it, thus exposing the organization to the Log4Shell vulnerability.
- Traditional security tools designed to scan known entry points may miss their hidden connections.
- Since shadow APIs bypass monitoring, attackers can use them to spread malware, steal sensitive data, or disrupt business operations.
- In addition to the security risks, shadow APIs can lead to compliance failures in sectors where data privacy regulations like GDPR and CCPA demand strict control over data flows.

As such, the growing threat of shadow APIs demands new strategies for detection and attack surface management.

How to Detect and Manage Shadow APIs?

Comprehensive management of shadow APIs requires a holistic approach, encompassing poractive offensive security strategies. Here's what organizations can do to mitigate the threats arising from shadow APIs:

1. **API Inventory:** Create and maintain a comprehensive inventory of all authorized APIs to create a baseline for acceptable use, network connections, and data flows. Regularly review and update the inventory.
2. **API Gateway Monitoring:** Implement an API gateway to monitor all API traffic entering and leaving the internal network to detect unauthorized connections.
3. **Log Analysis:** Scrutinize application logs and compare against established baselines to detect unusual data flows or API calls that may indicate shadow APIs.
4. **Code Scanning:** Regularly conduct automated scans of code repositories for undocumented API references or calls.
5. **Attack Surface Management:** Leverage ASM tools to map your entire attack surface, including hidden assets like internal and external shadow APIs. ASM also helps prioritize any associated vulnerabilities.
6. **API Penetration Testing:** Regularly perform API penetration testing to proactively validate and mitigate security vulnerabilities in known and uncovered APIs before attackers can exploit them.
7. **Shadow API Management:** Establish processes to isolate and apply access control to discovered shadow APIs. Depending on whether there is a legitimate business need for the shadow API, organizations may choose to either standardize or decommission it.
8. **Security Awareness:** Foster awareness among developers about API security best practices and the importance of following security processes, as it will help prevent shadow APIs from popping up in the first place.

Bring Shadow APIs to Light with BreachLock

BreachLock offers a comprehensive suite of offensive security solutions that empower organizations to detect hidden APIs and manage the risks they carry. As a first step, BreachLock's Attack Surface Management (ASM) solution provides a comprehensive view of your attack surface, encompassing both internal and external assets. BreachLock's advanced, ASM solution provides continuous attack surface discovery to identify and catalog all known and unknown assets, including shadow APIs, as soon as they emerge.

The External Attack Surface Management (EASM) component is particularly crucial in this regard, as it offers an outside-in view of the attack surface, mimicking the perspective of an attacker. It helps BreachLock identify exposed APIs along with their most critical entry points for attackers. This enables organizations to prioritize vulnerabilities that attackers are most likely to target first, significantly optimizing security resources.

BreachLock's comprehensive suite of Attack Surface Discovery and Penetration Testing solutions identify, validate, prioritize, and mitigate risks through Penetration Testing as a Service (PTaaS), which includes dedicated applications, web applications, and API penetration testing. The continuous security testing approach closely aligns with DWASP best practices and DevSecOps resource optimization and efficiency. However, a team of cybersecurity experts meticulously validate and scrutinize the findings to eliminate false positives and ensure comprehensive coverage..

BreachLock equips organizations to confidently confront the threats posed by Shadow APIs and safeguard their digital ecosystem. Bring shadow APIs to light and take full control of your API ecosystem. Schedule a free discovery call with a BreachLock expert today to learn how we can help!

About BreachLock

BreachLock is a global leader offering human-delivered, AI-powered, and automated solutions for Attack Surface Management , Penetration Testing as a Service and Continuous Penetration Testing and Red Teaming as a Service . Collectively, these solutions go beyond providing an attacker's view of common vulnerabilities and exposures to provide enterprises with evidence-based risk across their entire attack surface to determine how they will respond to an attack.

Know your risk. Contact BreachLock today!

References:

1. https://www.gartner.com/en/documents/4009103
2. https://www.akamai.com/resources/state-of-the-internet/lurking-in-the-shadows
3. https://www.gartner.com/en/doc/746066-top-10-aspects-software-engineering-leaders-must-know-about-apis
4. https://therecord.media/hackers-leak-linkedin-700-million-data-scrape
5. https://salt.security/blog/t-mobile-api-breach-what-went-wrong

breachlock
hello@breachlock.com
+1 302 516 7152

BreachLock Inc.
1345 Avenue of the Americas
33rd Fl, Office #56, New York, NY 10105
+1 917 779 0009

BreachLock NL B.V.
Kon. Wilhelminaplein 1, Tower 4
1062 - HG Amsterdam
+31 20 3030 007