

Case Study

Large Mobile Phone Carrier Discovers Thousands of Unmanaged and Insecure APIs

API Spyder Enables the Security Team to Get Full Visibility into Their API Attack Surface and Secure It

One of the nation's largest mobile phone carriers with over 100 million wireless subscribers wanted to get complete visibility into its API footprint. API applications play a critical role in helping to support and manage their large nationwide network. The security team wanted to ensure that they had complete visibility into all APIs regardless of where they were deployed to ensure that they had complete oversight and control.

The carrier's security team was using Cequence's network-based API discovery capabilities which identify APIs as they transact data. However, they wanted to ensure that any APIs that weren't actively transacting data, such as "zombie" or forgotten APIs, were also discovered. Cequence API Spyder crawls an organization's domains to discover the complete API attack surface, part of Cequence UAP, provides an attacker's view into an organization's public-facing resources and identifies external API hosts, unauthorized hosting providers, and API-specific security issues.

The Results

Complete Attack Surface Visibility

After running API Spyder, the security team's suspicions were confirmed. There were thousands of unmanaged APIs that existed that the team had no visibility into and therefore no control over. API Spyder crawled through their entire public-facing APIs regardless of where they were hosted, building out their entire API footprint.

With API Spyder the security team was able to discover the following:

- **Complete API Footprint:** Obtain a complete API footprint of all API servers regardless of where they were hosted.
- **Automated Discovery:** API Spyder eliminated the manual process of discovering and maintaining a list of external-facing API servers. The process of maintaining a complete list of APIs was laborious, never-ending, incomplete, and error-prone.
- **Continuous Discovery:** API Spyder provided a dashboard that ensured that if a new API application were deployed, the team would be immediately aware.
- **No Security Blind Spots:** They now were able to surface any potential unmanaged and unprotected API applications that could serve as backdoor into their environment.
- **Third-Party Risk:** They were able to ensure that OpenAPI specification files used by third-party API integration partners were secure and not exposed publicly.



Customer Profile

One of the nation's largest mobile phone carriers with over 100 million wireless subscribers.

Goals

- ✓ **Obtain a complete attack surface report** of all API servers regardless of where they were hosted
- ✓ **Discover** if their understanding of the existing API server inventory was accurate
- ✓ **Remediate** any security issues on any API that could serve as a backdoor into their environment

What They Discovered

Using API Spyder, the security team was able to discover the following:

- **Full API Host Discovery:** Over 1000 API servers that were not actively protected.
- **Non-Production Servers:** Over 18% of their overall servers were unsecured, non-production servers exposed to the internet.
- **Log4J Vulnerable Servers:** Despite a rigorous patching program, they had discovered that several API applications with the Log4J vulnerability were not patched.
- **SSL Issues:** Over 30% of their API servers had SSL security issues such as invalid or expired certificates, potentially enabling MITM (man-in-the-middle) attacks.
- **Exposed Files:** Over 100 files exposing private keys that could be used to gain access to mission-critical business information.