APIs: The Development Tool of Choice

APIs are increasing in popularity, but also represent an increasing risk for enterprises. In 2021, APIs accounted for over 70% of application requests, up from just 14.4B requests in previous years. This growth in usage comes with a rise in malicious activity, with 941% more API traffic originating from malicious sources than in 2020.

ATTACK PATTERNS OBSERVED

- **Usage Patterns**
  - **GraphQL**: grew by 133%.
  - **User Authentication, Login or Account Registration**: grew by 95%.
- **Content Scraping**: increased by 178%. This is commonly caused by competitive snooping of product or technical information, resulting in wasted compute resources and cost overruns.

**MALICIOUS TRAFFIC** originated from around the world with the top 10 COUNTRIES shown in the map. From June to December 2021, 70% of blocked traffic was API-based.

**API-BASED REQUESTS TOTAL APPLICATION REQUESTS**

- 14.4B of the 21.1B application requests were API-based.

**CONTENT SCRAPING**, commonly caused by competitive snooping of product or technical information, was up 178% resulting in wasted compute resources and cost overruns.

Modern cars, every mobile app we use, our favorite shopping site, and our finance management all rely on APIs to deliver an engaging user experience. For these same reasons, threat attackers love APIs. So much so that Gartner predicts that by 2022, API attacks will become the most-frequent attack vector, causing data breaches for enterprise web applications.

**APIs EXPOSING SENSITIVE DATA** like payment (PCI) or personally identifiable information (PII) increased by 87% emphasizing the continued need for strong security and privacy in API development.

**APIs** referencing OpenAPI or Swagger specifications jumped 352% signaling increased adoption, but their public nature can provide an API attack blueprint.

Today, software is eating the world and APIs ARE TAKING THE BIGGEST BYTE. Modern cars, every mobile app we use, our favorite shopping site, and our finance management all rely on APIs to deliver an engaging user experience. For these same reasons, threat attackers love APIs. So much so that Gartner predicts that by 2022, API attacks will become the most-frequent attack vector, causing data breaches for enterprise web applications.

**API-BASED REQUESTS TOTAL APPLICATION REQUESTS**

- 14.4B of the 21.1B application requests were API-based.

**MALICIOUS TRAFFIC** originated from around the world with the top 10 COUNTRIES shown in the map. From June to December 2021, 70% of blocked traffic was API-based.

**ATTACK PATTERNS OBSERVED**

- **Usage Patterns**
  - **GraphQL**: grew by 133%.
  - **User Authentication, Login or Account Registration**: grew by 95%.
- **Content Scraping**: increased by 178%. This is commonly caused by competitive snooping of product or technical information, resulting in wasted compute resources and cost overruns.

**MALICIOUS TRAFFIC** originated from around the world with the top 10 COUNTRIES shown in the map. From June to December 2021, 70% of blocked traffic was API-based.

**CONTENT SCRAPING**, commonly caused by competitive snooping of product or technical information, was up 178% resulting in wasted compute resources and cost overruns.

Modern cars, every mobile app we use, our favorite shopping site, and our finance management all rely on APIs to deliver an engaging user experience. For these same reasons, threat attackers love APIs. So much so that Gartner predicts that by 2022, API attacks will become the most-frequent attack vector, causing data breaches for enterprise web applications.

**APIs EXPOSING SENSITIVE DATA** like payment (PCI) or personally identifiable information (PII) increased by 87% emphasizing the continued need for strong security and privacy in API development.

**APIs** referencing OpenAPI or Swagger specifications jumped 352% signaling increased adoption, but their public nature can provide an API attack blueprint.

**ACCOUNT TAKEOVERS**, often the precursor to fraud, data loss or system compromise, increased 62%. This is commonly caused by competitive snooping of product or technical information, resulting in wasted compute resources and cost overruns.

**APIs** referencing OpenAPI or Swagger specifications jumped 352% signaling increased adoption, but their public nature can provide an API attack blueprint.