THREATX

DATA SHEET

API and App Security: Q3 2023

Executive Brief

We recently analyzed data collected on the ThreatX API and Application Protection platform from August through October 2023.

Key takeaways

» Attackers are employing a wide variety of tactics against APIs and apps, and the attack landscape varies across industries.

» Bot attacks are rampant across companies of every size and in every industry.

» Credential stuffing attacks are an extremely popular attacker tactic.

» The banking industry sees the most attention from attackers – and specifically with authentication attacks.

Figure 1 below highlights the top five most common attacks observed across industries:

1. Programmatic Access: 25.49%
2. Credential Stuffing: 3.53%
3. Directory Traversal: 3.29%
4. Error Rate: 3.16%
5. Evasion: 2.58%

Average Percentage of Each Attack Type Across All Tenants

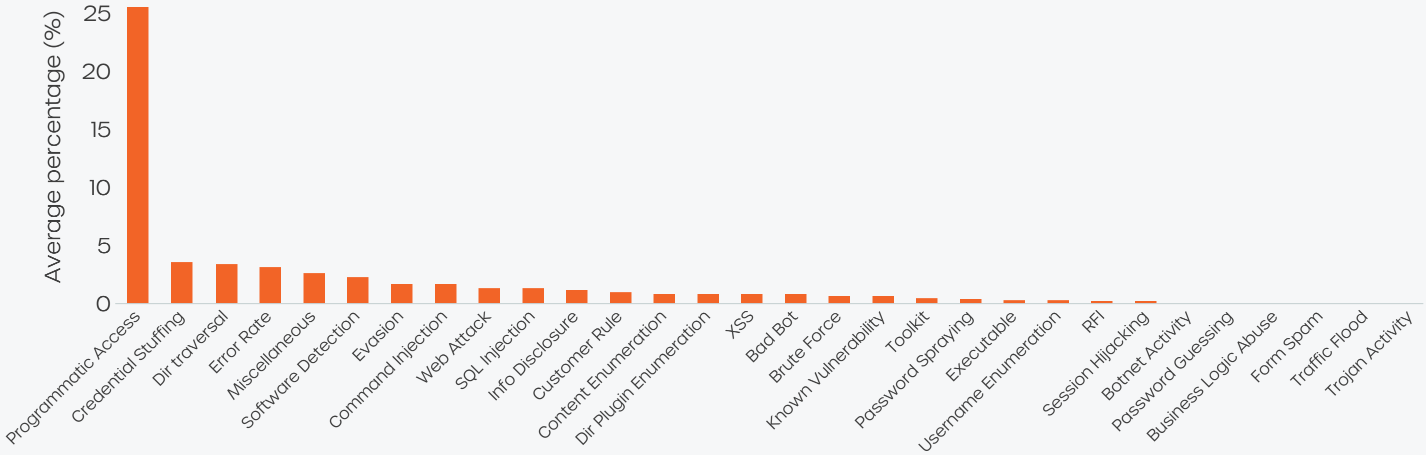

Figure 1: API and application attack types

Most Disproportionate Attack Types by Industry

Industry	Most Disproportionate Attack Type
Banking	Programmatic Access
Business Services	Bot Attacks (Aggregate)
Consulting	Bot Attacks (Aggregate)
Education	Programmatic Access
Electronics	SQL Injection
Finance	Miscellaneous
Government	Bot Attacks (Aggregate)
Healthcare	Programmatic Access
Insurance	Bot Attacks (Aggregate)
Manufacturing	Error Rate
Media & Entertainment	Programmatic Access
Other	Programmatic Access
Professional Services	Plugin Enumeration
Retail & Distribution	Programmatic Access
Software & Technology	Directory Traversal
Telecomm	Bot Attacks (Aggregate)
Transport	Programmatic Access
Utilities	Customer Rule

Percentage of Attacks that Are Bot-Driven by Industry

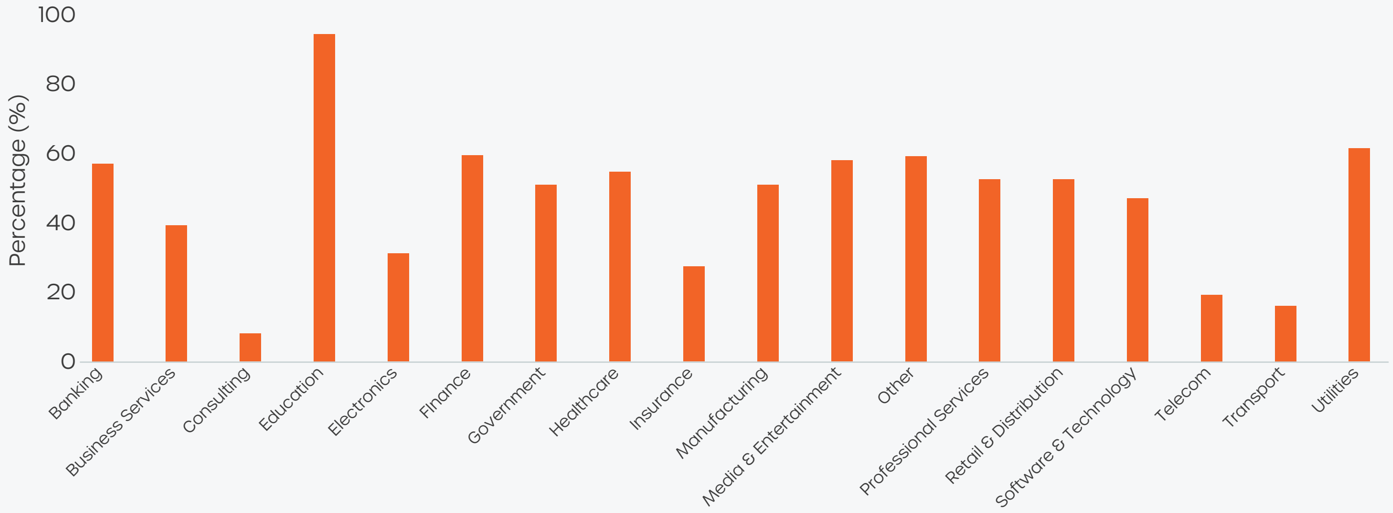

Figure 2: Bot attacks by industry

Top 3 API Attacks Types by Industry

Industry	Top 3 API Attack Types
Banking	**Credential Stuffing (24.7%)** Programmatic Access (21.7%) Brute Force (9.9%)
Business Services	**Programmatic Access (38.7%)** Misc (11.3%) XSS (Cross-Site Scripting) (11.2%)
Consulting	**Directory Traversal (21.9%)** Programmatic Access (17.5%) Command Injection (12.5%)
Education	**Programmatic Access (93.9%)** Password Spraying (3.7%) Traffic Flood (1.5%)
Electronics	**Programmatic Access (30.3%**) SQL Injection (14.4%) Directory Traversal (14.1%)
Finance	**Programmatic Access (58.9%)** Misc (7.1%) SQL Injection (6.6%)
Government	**Programmatic Access (49.7%)** Bad Bot (24.5%) Misc (16.7%)
Healthcare	**Programmatic Access (48.8%)** Error Rate (14.6%) Misc (13.6%)
Insurance	**Programmatic Access (19.7%)** Software Detection (19.3%) Customer Rule (18.2%)
Manufacturing	**Programmatic Access (50.4%)** Error Rate (19.8%) Toolkit (12.5%)
Media & Entertainment	**Programmatic Access (58.0%)** Plugin Enumeration (13.7%) Toolkit (11.5%)
Other	**Programmatic Access (58.6%)** Plugin Enumeration (11.4%) Error Rate (9.6%)
Professional Services	**Programmatic Access (38.1%)** Credential Stuffing (16.5%) Toolkit (10.9%)
Retail & Distribution	**Programmatic Access (47.0%)** Misc (12.3%) Error Rate (9.4%)

Top 3 API Attacks Types by Industry (con't)

Industry	Top 3 API Attack Types
Retail & Distribution	**Programmatic Access (47.0%)** Misc (12.3%) Error Rate (9.4%)
Software & Technology	**Programmatic Access (43.9%)** Directory Traversal (17.2%) Evasion (13.5%)
Telecomm	**Error Rate (26.2%)** Programmatic Access (24.2%) Information Disclosure (11.8%)
Transport	**Web Attack (29.3%)** SQL Injection (14.1%) Programmatic Access (12.4%)
Utilities	**Programmatic Access (61.6%)** Customer Rule (12.4%) Error Rate (11.1%)

Key Takeaways

Emphasize defense against programmatic access: Given that programmatic access (a wide variety of automated or non-human interactions with web applications and APIs, potentially aiming to scrape data, perform unauthorized transactions, or exploit vulnerabilities) is significantly higher than other types of attacks, it's crucial to implement robust anti-bot solutions and enhance user authentication and validation mechanisms.

Prioritize credential defense mechanisms: Credential stuffing is prominent. Implement multi-factor authentication, monitor for suspicious login activities, and encourage users to employ strong, unique passwords.

Keep in mind that credential stuffing techniques are able to sidestep traditional WAF signatures and rate-based rules for several reasons. Most notably, the techniques do not rely on an exploit or other overt malicious action, and instead, use/abuse the exposed functionality of an application in unexpected ways.

In this case, the attacker, usually in the form of a bot, is using the application's login functionality in much the same way that a legitimate user does. Additionally, since attackers have many username/-password combinations to cycle through, the work is typically done by a large, distributed botnet or other forms of malicious automation. This not only speeds up the work, but it allows the attacker to distribute the attack over a large number of IP addresses so that it isn't obvious that the attack traffic is coming from a specific set of IPs.

Prevent directory traversal and examine error rates: Ensure secure configurations and apply necessary patches to prevent directory traversal attacks. Analyzing error rates can potentially provide insights into misconfigurations or vulnerability exploits. Keeping logs and alerts for high error rates can be pivotal for early detection of an attack.

Address evasion techniques: Consider implementing solutions that can identify and block requests trying to evade detection, such as through the use of VPNs, proxies, or other anonymization tools.

To learn more, get a demo of ThreatX API and Application Protection.

THREATX

www.threatx.com | info@threatx.com