Signal Sciences

# Identifying Web Attack Indicators

Attackers are always looking for ways to compromise or abuse cloud, web, and mobile applications. In particular, web and cloud-based applications have become the vector of choice because these attacks are more likely to succeed. For example, in its 2016 Data Breach Investigations Report (DBIR), Verizon found that:

- **Web application attacks only accounted for eight percent of all incidents**
- **Yet they made up 40 percent of all successful breaches**

> *Web applications continue to be the top attack target in about 70 percent of breaches*

### Prominent Web Attack Types

- **Credential stuffing attacks have become the most popular attack to target cloud applications, and the second most popular attack overall, behind phishing.**
- **Nearly three out of every ten breaches involved stolen credentials, according to Verizon.**
- **With the popularity of RESTful APIs for applications, attackers also targeted APIs as another vulnerable surface area in applications, in much the same way that database injection attacks target structured query language (SQL) databases.**
- **Finally, a small, but significant, number of attacks focus on finding flaws in the design of applications to attempt business logic attacks.**

To prevent these web attacks, security teams should know the signs of these attacks, and requires insight into the threats targeting your business applications.  But the indicators are not always obvious. Attacks can either attempt to overwhelm your site, or take a "low and slow" approach that attempts to evade detection by blending in with other legitimate traffic.

Gaining visibility requires companies analyze their site traffic to create a baseline of the normal, expected traffic directed at your applications. Without knowing your expected traffic patterns, detecting and responding to attacks is much more difficult. In addition, application defenders need visibility into which traffic looks malicious and why. Systems that do not explain the signals that went into classifying an attack do not help your company become better at defense.

## Case 1: Credential Stuffing

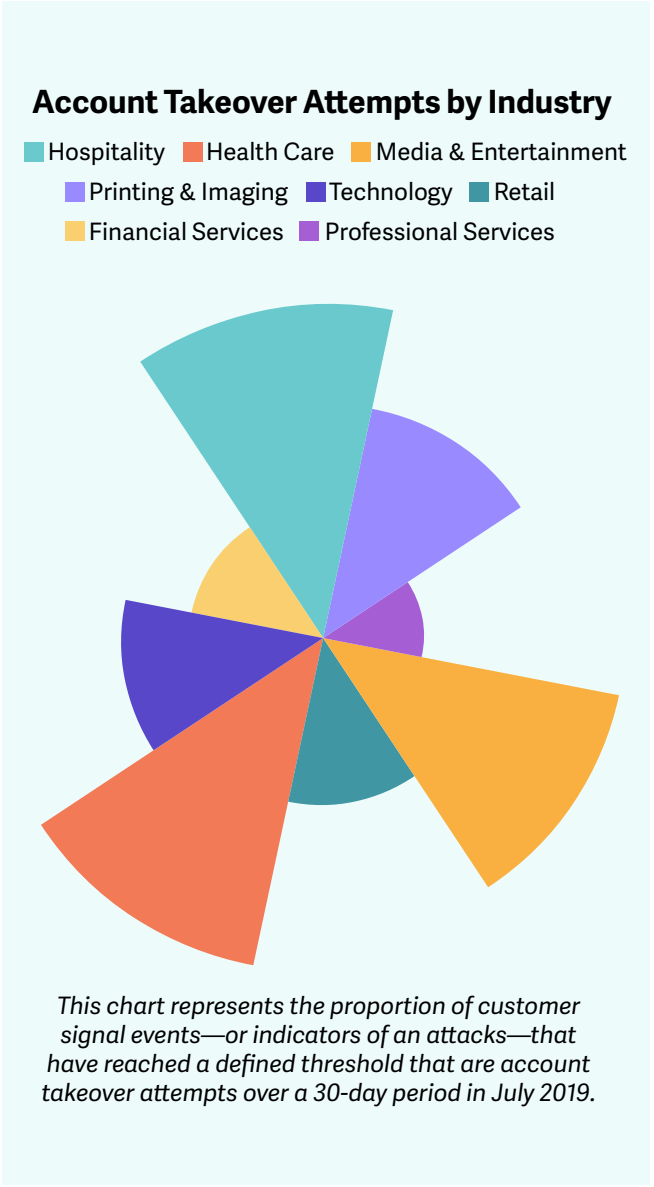
As organizations continue to migrate to the cloud or design and deploy cloud-native apps, the keys to business and user data are increasingly protected only by a simple username-and-password combination. No wonder, then, that credential stuffing has become the most successful attack type over the last year. According to Verizon, 29 percent of all breaches involved the use of stolen credentials to access sensitive data, second only to phishing.[1]

Attackers use these credentials to take over accounts, gain access to private Internet of Things (IoT) devices, and chain attacks by accessing account recovery email addresses.

In February 2019, Google sent an email to customers warning that hackers were attempting to use stores of credentials to take control of Nest devices.[2] In one instance, a hacker gained control over a family's Nest devices, talked to their baby, and increased the room temperature.[3]

Signal Sciences has seen a general increase in account takeover attacks using credentials since the release of two massive credential leaks. In January 2019, a security researcher found a database online (called Collection #1) that contained 773 million unique email addresses and 21 million unique passwords. A second dump, known as Collections #2-5, had more than 25 billion email and password records.[4] Those databases, and two others, brought together more than 26 billion user records.[5]

Signal Sciences observes over one trillion production web requests per month. In July 2019, credential stuffing attempts (a.k.a. account takeover) was the most frequent web layer attack to target Signal Sciences customers' web apps. Analysis of the observance of credential stuffing attempts by vertical provides the breakdown shown in the chart below. Each section of the chart represents the proportion of total credential stuffing attempts against customers in each industry vertical. Hospitality, healthcare and media and entertainment verticals are the leading targets.

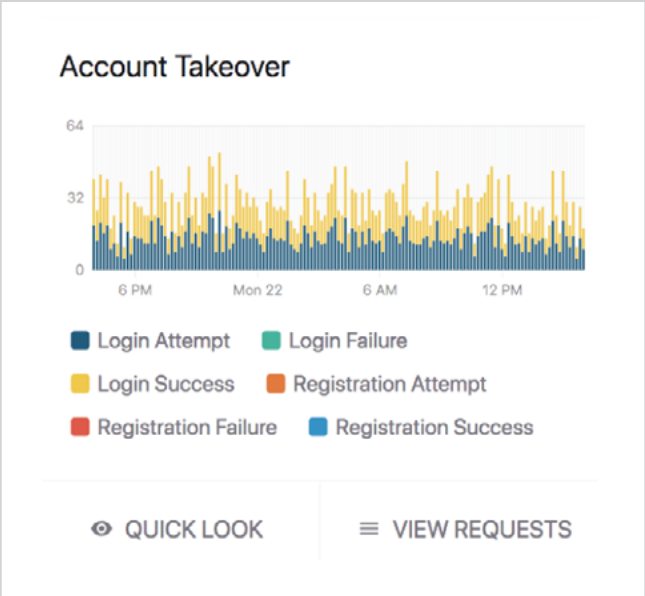



*This chart represents the proportion of customer signal events—or indicators of an attacks—that have reached a defined threshold that are account takeover attempts over a 30-day period in July 2019.*

## Indicators of Attack

Because credential stuffing is the primary tactic for account takeover attacks—rather than brute-force password guessing or dictionary attacks—the signs of an attack are different. This is especially true when attacks are distributed over a large number of IP addresses so that no single source sends a high volume of credentials. Indicators of an attack include:

- Login attempts from geographically diverse areas, different from users' normal geographies
- An increasing number of failed login attempts across all users
- Successful logins from suspicious IP addresses




*Visualization card from the Signal Sciences management console. Signal Sciences detects and stops ATO attacks by observing key authentication events such as login attempts, login failures, registration failures and others.*

## Mitigation

There are several key tactics to confirm valid users are initiating login attempts instead of outright blocking access. Companies should trigger additional security checks, such as two-factor authentication. Security and operations teams can also monitor the volume of requests on key authentication actions like login attempts, email address resets, and password reset requests. When expected thresholds are met, you should then temporarily block those requests. Security tools that allow businesses to peer into specific types of authentication events are key to detecting credential abuse.

## Case 2: API Abuse

With the explosion of mobile device usage, developers found the best way to access data from a web application was through an application programming interface, or API. As applications are increasingly deployed to cloud infrastructure and maintained by specific development or DevOps groups, these APIs have proliferated. Both RESTful APIs and microservices expose a specific set of functions to authorized users and applications.

The popularity of APIs has opened up the technology to attacks. Injection attacks are the top attack type in the OWASP Top 10 list of software insecurities. Brute-force attackers often find a critical API service and overwhelm it with requests, breaking an application because it cannot access a critical resource. More subtle attackers look for ways to use an API to their own ends, such as stealing data by sending requests that appear to be legitimate.

In 2017, security researcher Dylan Houlihan discovered that an insecure API on the website of bakery and cafe chain Panera Bread allowed access to customer records. Among other security flaws, the API sequentially numbered customer records, which allowed a bot to easily scrape more than seven million customer records from the site. Later information suggested that more than 37 million customer records may have leaked.[6] This technique of scraping business data using APIs is a common attack that companies need to detect and block.

A similar problem occurs when companies want to offer a free trial to potential customers. Signal Sciences finds that this opens up servers to attackers

who install the software and then use it to access a critical API. While free trials can often accelerate your sales process, it opens up the business' infrastructure to abuse. The solution is not to throttle all customers, but to block only potential clients who installed a trial version of the software.

In addition, attackers look for APIs that allow anyone to guess the identifiers for resources—for example, a user account or the validation of a consumer reward. If your API lacks security, or has a broken authentication mechanism, it can open the system to abuse. In one case, the Amadeus reservation system used by Israel's national airline and 140 other carriers, allowed the enumeration of booking identifiers, with which anyone could retrieve passenger data and flight information.[7]

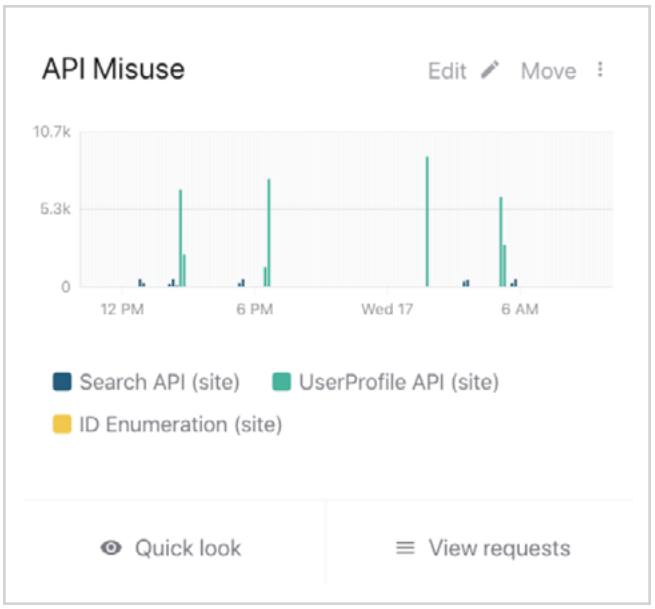
## Indicators of Attack

Attacks on APIs, like SQL injection, often appear legitimate but contain strange patterns, use out-of-date credentials, or occur much more frequently than legitimate traffic. Indicators of an attack on an API:

- More than 50 API requests per second (these are given a suspicious label)
- API requests that are not valid, have the improper cookie, or attempt to connect from an untrusted device
- API requests lacking proper authorization, coming from a suspicious geography, or attempting to access protected data

## Mitigation

Because most businesses do not want to prevent their cloud-based application from working, initial mitigation involves alerting the customer that an attack may be occurring. Investigation of suspicious IP addresses and attack clusters can reveal patterns in the attack that could be the basis for more extensive mitigations. Eventually, you can create a rule to block certain attack patterns and IP addresses from accessing the API, blunting future attacks.




*Visualization card from the Signal Sciences management console that shows the volume of API Misuse attack signals over a specific time frame.*

## Creating Proactive Feedback for DevOps

Companies are increasingly focused on rolling out new features, patching code, and blocking attacks as fast as possible. If you use DevOps processes to develop, deploy, and manage your applications, you need alerting integrated into your communications channel for tracking issues and fixes. An application security and performance tool that provides real-time feedback into the DevOps cycle can be the difference between responding to application security issue in real time or a breach.

## Case 3: SQL Injection

A majority of websites connect to backend SQL databases. WordPress sites, for example, use the PHP programming language for creating the website, but fetch data for display and configuration from databases running Postgresql, MySQL, or another flavor of SQL.

Attacks on these databases have often compromised all the customer records stored in the database. No wonder, then, that attackers continue to focus on SQL injection (SQLi), with nearly two-thirds of Internet scans[8] attacking backend databases.

Because of the popularity of SQL databases, which contain valuable information, attackers often try to directly access your database through the website. These SQL injection attacks can discover sensitive product data (such as inventory information), collect data on users (such as addresses, phone numbers, and credit card information), or, in the worst cases, steal usernames and passwords.

In March 2019, the company behind the popular Magento e-commerce application reported that Magento 2.x had a vulnerability that could allow attackers to access its backend database.[9] Criminals started targeting the vulnerability within 16 hours and many successfully compromised the storefront software, often leaving behind malware that stole payment card data from customers.

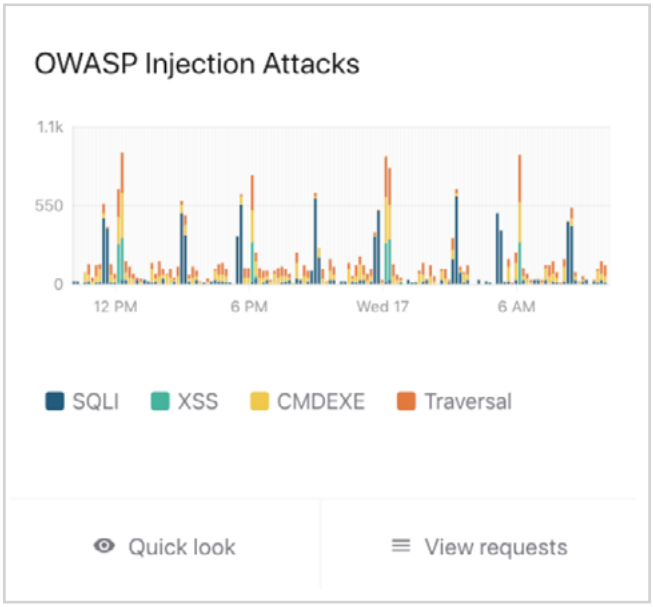
One Signal Sciences e-commerce client detected a series of abnormal SQL requests. The requests came from a variety of Chinese IPs and targeted a variety of website paths, including user.php and products.php. This generated Signal Sciences alerts that SQLi attacks had been blocked, after which the client searched on the content of the request and discovered a Japanese page that described a new attack on backend WordPress databases.

SQL Injection attacks are frequent across multiple industries as observed in Signal Science alalyzed attack telemetry in July 2019 (see appendix charts).

### Indicators of Attack

Simple pattern matching can detect SQL injection attacks but is prone to false positives and might miss new attacks. To automatically block attacks, businesses need highly accurate detection, including:

- Whether attacks exceed a threshold of 50 SQL requests in a minute
- SQL server responses with 405 ("method not allowed")
- Pattern matches to common attacks or searches revealing attack code




*Visualization card from the Signal Sciences management console that shows the volume for specific OWASP attack signals over a specific time frame.*

### Mitigation

Blocking attacks based on exceeding a predefined request threshold is a good initial mitigation. However, depending on the cadence of the attack, each incident should be referred to an analyst to decide whether a specific group is targeting your company's web assets.

### Better Blocking for Web Apps

In the past, blocking has been a major tradeoff with web application firewalls (WAF). Until a WAF is well-tuned, any attempt at automated blocking poses a significant risk. This is because false positives—customers identified as attackers—could turn away real business. Web security technologies need to take into account the context of each request to ensure a false positive success rate that is low enough to allow companies to block default attacks without worrying about lost revenue. The better the accuracy of the technology, the less work application security teams need to do to maintain baseline security, and the more they can focus on other attacks.

## Case 4: Business Logic

Often attackers will learn how an application works and try to abuse specific parts, or key interaction points, of its design to achieve their aims. These so-called "business logic" attacks can combine publicly allowed features to steal information, gain access to accounts, or cause service disruption.

For instance, parameters that are passed to the server (i.e., to maintain a logged-in state) could be reverse-engineered and abused to provide additional privileges for the attacker. E-commerce sites that provide discounts based on user profiles could be circumvented by changing the profile. A web application for a concert venue that holds seats for five minutes could be manipulated by an attacker to hold a high volume of tickets.

One security researcher abused a helpdesk ticketing system and took advantage of the propensity of companies to allow anyone who signs up to Slack with a corporate domain to join team chats. Because some helpdesk ticketing systems respond with a unique email using the domain of the company for each trouble ticket, the researcher just submitted a ticket to the company and then used that email address to sign in to Slack. As a result, they gained access to Slack channels at development company GitLab and video hosting firm Vimeo.[10]

In another case, attackers targeted an online ticket sales company that issued a redemption code for the tickets. The client suffered from an API abuse attack, because the attacker used an automated script that attempted to discover valid redemption codes for the tickets.

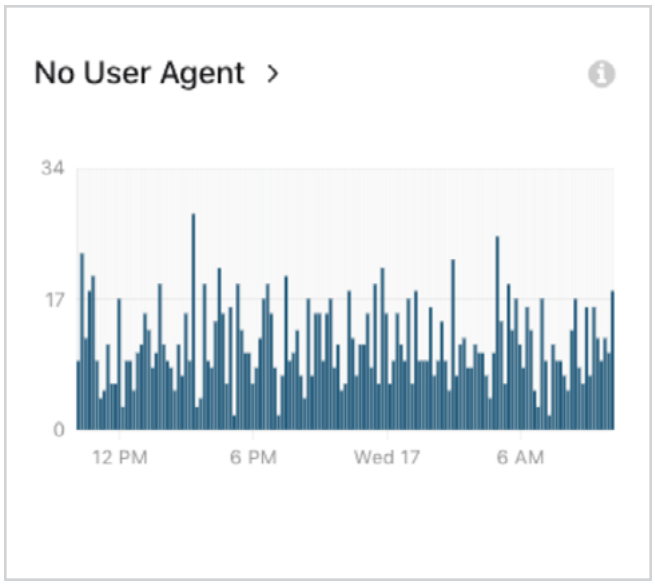
### Indicators of Attack

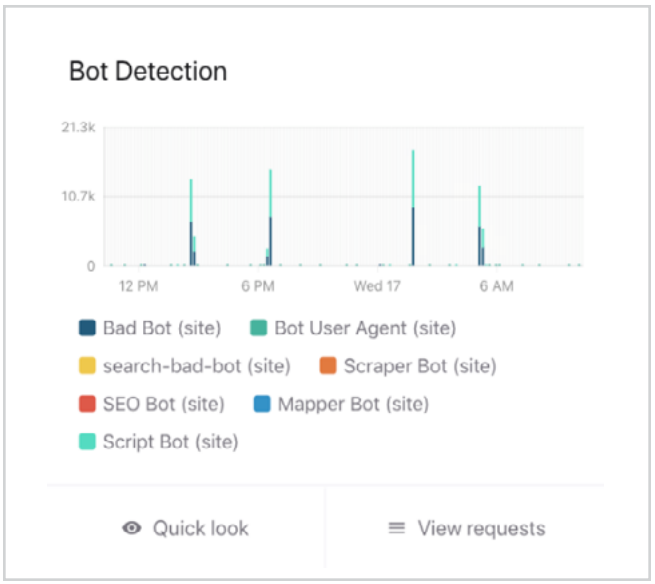
Because they use valid application features, business logic attacks can be difficult to detect. Companies need to track signals that could indicate someone abusing an application, and put into place application controls that check potentially risky inputs, like:

- Application using too many resources or slowing performance
- Anomalous API calls or use of services
- Service outages

### Mitigation

Once an attack is detected, misuse can be blocked using specific rules until the application can be updated with mitigations. The best security tools allow you to define rules based both on specific signals extracted from the application-user interaction and external data, such as user agents, request parameters, cookies and other data that could be linked to an attacker. Using these rules, a company can gain better visibility into the attack and define automated actions.




*Using rules that provide insight into application user interaction, software developers and operations staff can gain visibility into an attack and define automated actions to stop it. Above left: Volume of requests lacking a user agent. Right: Automated bot requests.*

## Choosing the Best Tool for Web Layer Defense

Companies looking to gain better visibility into attacks on their web applications and cloud infrastructure need tools that work with their business and processes, rather than requiring employees to adapt to security technologies that reduce productivity. A web application firewall (WAF) should offer flexible deployment options and work with edge tools to catch attacks that would otherwise be missed. These tools also need to provide signals and actionable data that helps engineers and developers focus efforts as they fix problems and improve the application. Finally, it should not matter if your application is deployed as a website, on cloud infrastructure, or as the backend for a mobile application. The best web application security tools can virtually patch issues to protect the core application, while providing decision makers with the data they need on uptime, performance, and potential attacks.

## Conclusion

To successfully avoid getting compromised, your company first has to be aware that its applications are under attack. For that reason, visibility into what is happening to your applications is key to effectively detecting attacks.

Products that rely only on baked-in rules or regex patterns to anomalous and malicious activity can miss too much. Rule-based systems often overlook the signs of attacks because attackers frequently change their techniques until they find a method that works. Companies need more flexible systems that react faster than most humans and offer automated protection that does not require constant rules tuning.

Signal Sciences next-generation web application firewall provides visibility into a broad range of signals. This allows companies to easily diagnose problems with their web applications and react quickly to actionable intelligence.

By exposing the necessary context to application security teams, we help them protect valuable data served by their web apps, APIs or microservices. In addition to our out-of-the-box protection that requires no rules tuning, our solution also allows you to define, when necessary, advanced rules that automate responses to specific attacks, rather than limit the detection of attacks.

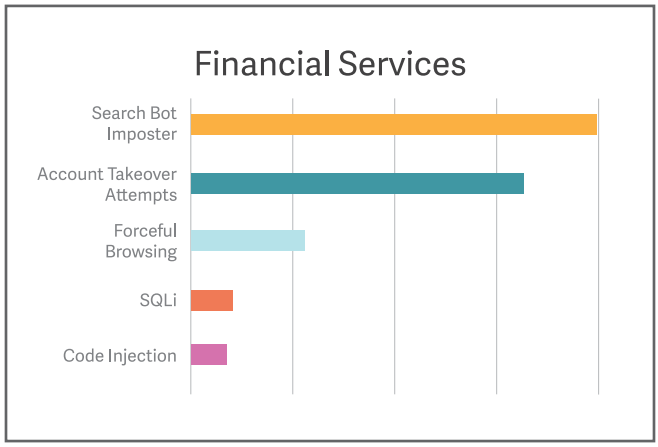
## Web Application Security with Increased Visibility

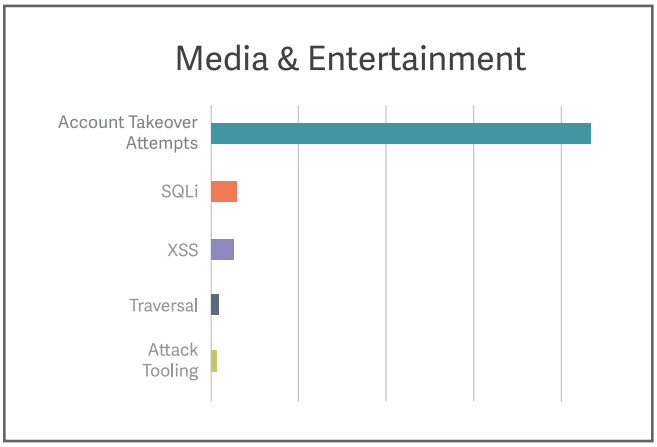
Signal Sciences secures the most important web applications, APIs, and microservices of the world's leading companies. Our next-gen WAF and RASP help you increase security and maintain site reliability without sacrificing velocity, all at the lowest total cost of ownership.

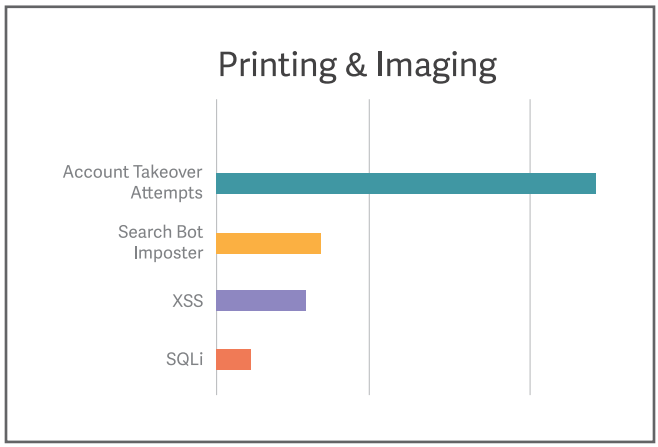
Learn how our patented approach can help you: for a demo of our web application security solution visit www.signalsciences.com.

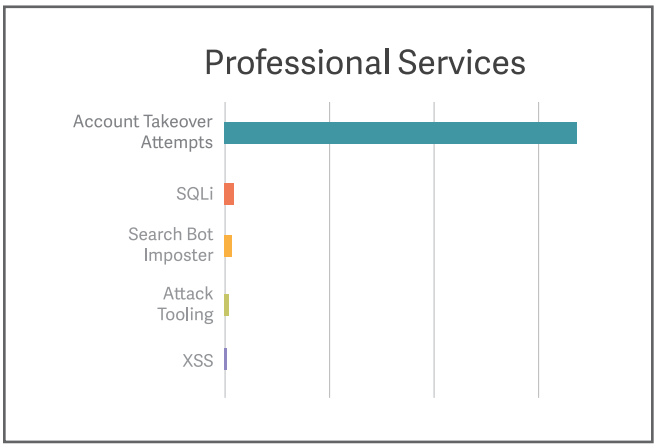
## Appendix: Top Attack Signals by Vertical

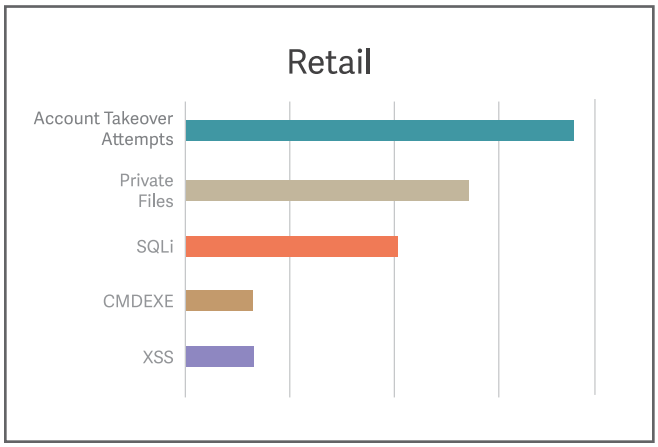
Leveraging the visibility into the broad range of attacks and anomalous signals that our unique approach provides, an analysis revealed the top signals, by industry, that reached a defined indicator of attack. Across the Signal Sciences customer base, many verticals must detect and stop account takeover attempts. Data represented is based on telemetry data collected during July 2019.

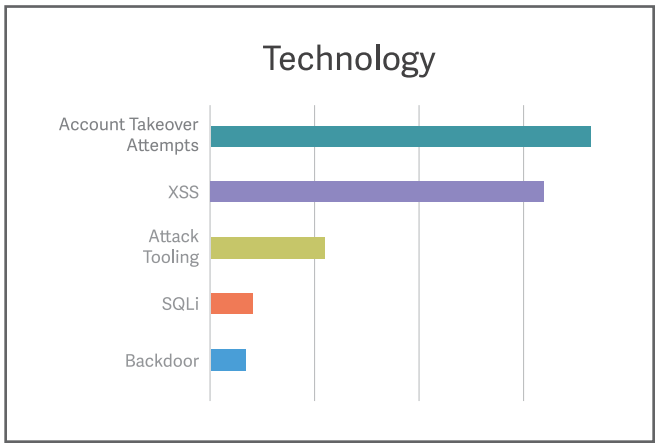





Signal Sciences

## Endnotes


[1] "2019 Data Breach Investigations Report | Verizon Enterprise Solutions." Accessed July 17, 2019. https://enterprise.verizon.com/resources/reports/dbir/.

[2] "Google Warns Nest Users to Update Security ... - Popular Mechanics." Accessed July 17, 2019. https://www.popularmechanics.com/technology/security/a26214078/google-nest-hack-warning/.

[3] "Hacker talks to baby through Nest security cam, jacks ... - Naked Security." Accessed July 17, 2019. https://nakedsecurity.sophos.com/2019/02/01/hacker-talks-to-baby-through-nest-security-cam-jacks-up-thermostat/.

[4] "Hackers Are Passing Around a Megaleak of 2.2 Billion Records | WIRED." Accessed July 17, 2019. https://www.wired.com/story/collection-leak-usernames-passwords-billions/.

[5] "Security firm identifies hacker behind Collection 1 leak, as ... - ZDNet." Accessed July 17, 2019. https://www.zdnet.com/article/security-firm-identifies-hacker-behind-collection-1-leak-as-collection-2-5-become-public/.

[6] "Panerabread.com Leaks Millions of Customer Records — Krebs on ...." Accessed July 17, 2019. https://krebsonsecurity.com/2018/04/panerabread-com-leaks-millions-of-customer-records/.

[7] "Over 140 International Airlines Affected by Major Security Breach." Accessed July 17, 2019. https://www.bleepingcomputer.com/news/security/over-140-international-airlines-affected-by-major-security-breach/.

[8] "SQL Injection Attacks Represent Two-Third of All Web App ...." Accessed July 17, 2019. https://www.darkreading.com/attacks-breaches/sql-injection-attacks-represent-two-third-of-all-web-app-attacks/d/d-id/1334960.

[9] "Two hacking groups responsible for huge spike in hacked ... - ZDNet." Accessed July 17, 2019. https://www.zdnet.com/article/two-hacking-groups-responsible-for-huge-spike-in-hacked-magento-stores/.

[10] "This hacker gained access to hundreds of companies through their ...." Accessed July 17, 2019. https://thenextweb.com/security/2017/09/21/ticket-trick-see-hackers-gain-unauthorized-access-slack-teams-exploiting-issue-trackers/.



## Author

Brendon Macaraeg, Sr. Director of Product Marketing, Signal Sciences



## Special Thanks

Christine Cole, Senior Product Manager, Signal Sciences: provided signal data analytics that form the basis of the information graphics.

Web layer attacks technical subject matter experts, Signal Sciences:

Zane Lackey, CSO and Co-founderDoug Coburn, Director of Professional Services

Jack Zarris, Senior Sales Engineer

Phillip Maddux, Sr. Technical Account Manager

Orlando Barrera, Technical Account Manager