WHITE PAPER

Protecting Media Logins From Credential Stuffing

Best practices for browser, gaming console, and OTT set-top box

Michael Smith, Security CTO

Alex Moening, Solutions Engineer

Kellen Kleinfelter, Security Architect

Shane Keats, Video Industry Analyst

Akamai

Contents

Introduction

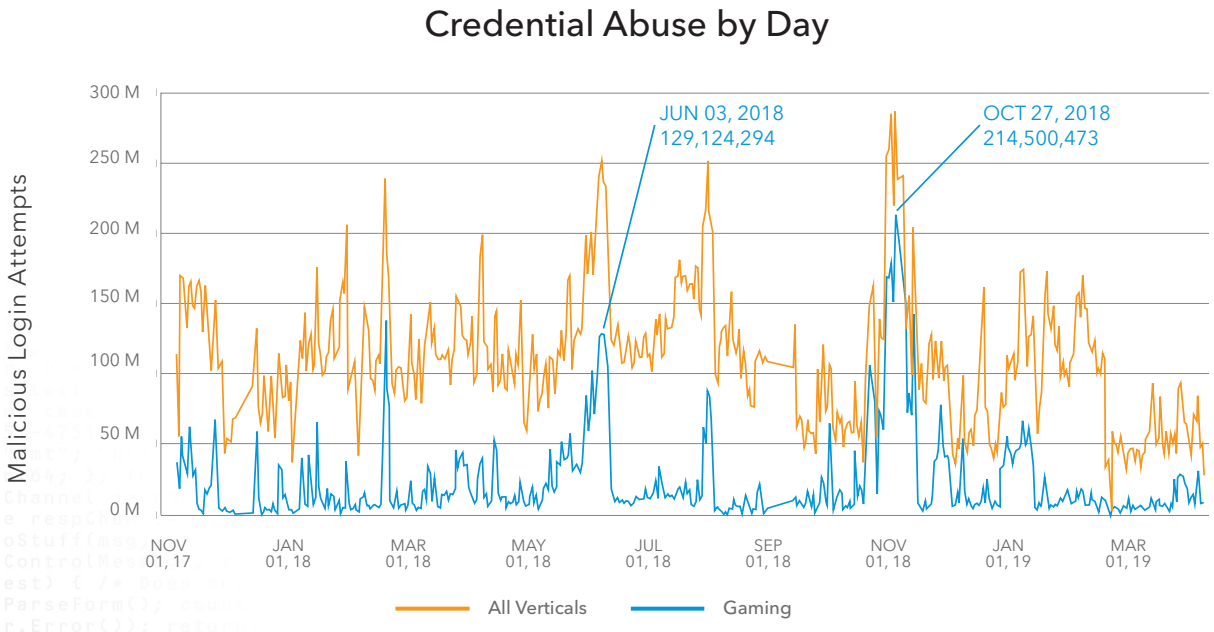
Akamai observed 55 billion credential stuffing attacks during a recent 17-month period (November 2017 through the end of March 2019). Akamai is not alone in observing this epidemic. What is new is that attackers have shifted their target. Media companies – OTT providers, newspapers, game publishers, etc. – have become the number one target. Video game companies alone accounted for one out of every five attacks Akamai logged.

The reasons for this surge are simple: Media companies now capture and store an enormous amount of data that has value on the dark web, but they are also complex – the device and login landscapes media companies must use to serve their customers lend themselves to attack.

In the inevitable arms race that has resulted, media companies find themselves in need of more advanced tools to fight back. Many media companies use a solution to this challenge called Bot Manager Premier (BMP) from Akamai. As a result of these deployments and the teamwork needed, we have developed a set of best practices on how to implement BMP to maximize its impact.

This document is written for companies that are considering using BMP and for companies that need to tune their implementation to better protect their device and login environments.

Credential stuffing is known by many names. No matter what the activity is called, however, this form of attack has been increasing. In 2018, for example, we observed five days with more than 200 million attacks and three days when fraudulent login requests exceeded 250 million. Video game companies were often the primary target.



Credential stuffing attacks by day during the reporting period

Source: State of the Internet report, Volume 5, Issue 3, Web Attacks and Gaming Abuse

Media Login: A Complex Ecosystem

Media organizations need to provide a wide variety of options for their customers to access their services; offering a multichannel experience adds complexity to login and has a notable impact on the ability of the industry to protect itself.

For example, a common scenario for a broadcaster's OTT service is to offer microservices that support logins for viewers using their website, their iOS and Android applications, and custom-developed applications for each supported OTT set-top box (STB). A popular gaming console might offer a login API as a resource for individual games that run on their console, and support a web version of their login API for users to create and manage their account. And some gaming consoles and mobile operating systems offer a "centralized" user identity, login API, and an SDK for application developers to integrate into their application.

Platforms

Desktops and Laptops

Desktop Web Browsers

Gaming Consoles

Set-Top Boxes

Mobile and Tablet Operating Systems

Mobile and Tablet Web Browsers

Applications

Web Browsers

Mobile and Tablet Applications

Platform-Specific Applications

Third-Party Applications

APIs

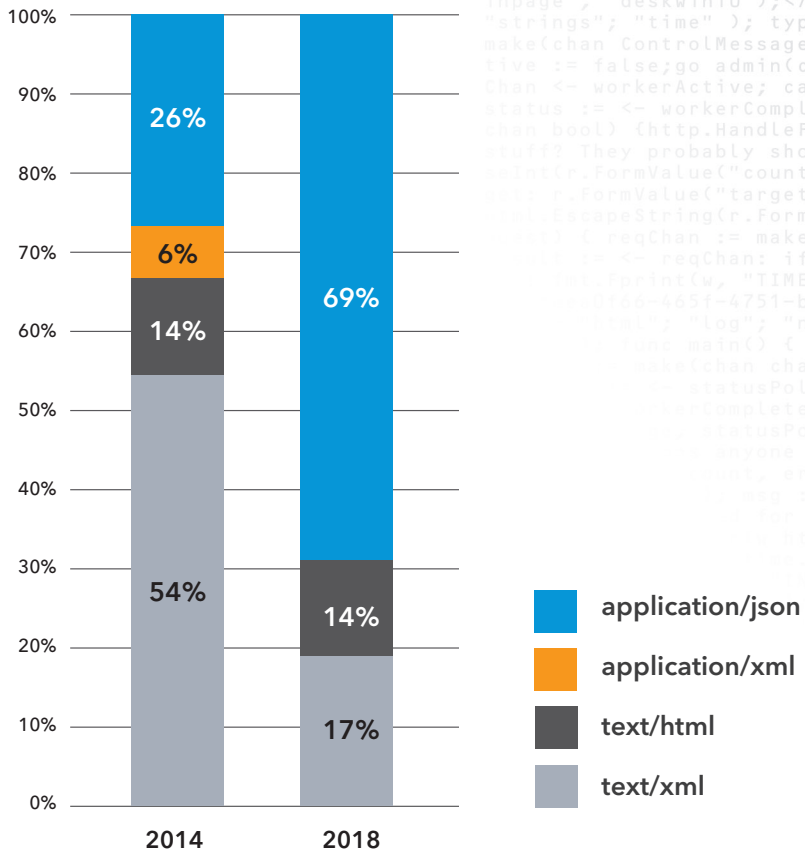
HTTP forms

REST

SOAP

Microservices

API Gateways



Source: State of the Internet report, Volume 5, Issue 2, Retail Attacks and API Traffic

The Growth and Vulnerability of API Login

API use has grown dramatically. For example, in a recent study of the retail sector, Akamai compared response object types from 2014 and 2018 and found that API objects surged 80% over four years, from 46% to 83% of all request and response traffic. We see similar trends in the media sector.

The biggest consumers of API requests are typically device-specific applications requesting status updates or content catalogs and single-page web applications that consist of a "shell" web page with items that are populated by a number of API requests. These two styles of APIs lead to automation that can simplify credential stuffing attacks.

The challenge to this increase in API traffic is that smart attackers will attack the least-defended target, because success results in access to the same data and functionality that they get with the well-defended services. Because APIs have smaller, templated requests and responses, they are easier for attackers to write tools for.

Challenges With Identifying Credential Stuffing Bots

Note: Because account checkers and AIO tools automate request traffic, they fit into a larger definition of what we traditionally think of as bot traffic. For the remainder of this paper, we will use "bots" as shorthand for this nonhuman traffic.

In the early days of bot management solutions, website defenders used rudimentary tools such as IP address and user-agent blocking. Over time, bot developers have evolved their tools to look more like legitimate clients. This has forced defenders to use more data available in the request context, and client characteristics that are added to the request by the user's web browser such as session token, operating system and browser versions, language encodings, etc.

When customers of a service use a standard web browser for login, defenders can successfully use this data to identify and manage bots. However, the majority of logins for broadcast, OTT, gaming, and publishing sites happen via applications running on mobile devices, STBs, and gaming consoles. This has several implications for the identification of bots.

- *Applications typically access services via API, and APIs normally receive requests with little contextual data about the human operating the application*
- *API request templates are easy to capture and replay*
- *APIs sometimes use nonstandard ports and protocols instead of the typical web-centric HTTP and HTTPS on TCP ports 80 and 443*

As a result, media companies that want to protect login and reduce account takeover need additional tools.

DEVICE MATRIX			
DEVICE	**SENDS VERBOSE HTTP HEADERS**	**RUNS JAVASCRIPT**	**CAN USE MOBILE SDK[3]**
Mobile (Application)	Yes. Very verbose	Yes for OS-provided web browser Possible for application with WebView[2]	Yes for Application with native API calls
OTT STB[1]	No. Terse requests	Possible with WebView[2] or OS-provided web browser	Possible but depends on OS, programming language, and device sensors[4]
Game Console[1]	No. Terse requests	Possible with WebView[2] or OS-provided web browser	Possible but depends on OS and language
Connected TV[1]	No. Terse requests	Possible with WebView[2] or OS-provided web browser	Possible but depends on OS, programming language, and device sensors[4]

Notes:

[1] Some STBs and connected TVs are built on top of Android OS. BMP capabilities on these platforms are exactly as per the Android mobile platform.

[2] WebView for both platforms needs to have support for JavaScript enabled with variables inside the WebView instance. See the "WebView Best Practices" on page 13.

[3] Mobile SDK requires integration. See the "Mobile SDK Best Practices" on page 14.

[4] When compared with running a mobile application using Mobile SDK on a mobile phone, the same application running on a different device might not have the full capabilities because of fewer on-device sensors (no gyroscope or accelerometer) and limited user interactivity (i.e., the user is using a remote control instead of a touchscreen).

How Bot Manager Premier Helps Protect Connected Device Login

Bot Manager Premier (BMP) is Akamai's solution for identifying and mitigating malicious bot traffic in complex connected device environments that are common to our broadcast, OTT, gaming, and publishing customers.

BMP uses JavaScript injection to extract more data from WebView and OS-provided web browser logins, and uses an SDK for mobile devices to get more telemetry from API-based login. For example, the BMP Mobile SDK collects telemetry from the gyroscope, accelerometer, and touchscreen. This telemetry allows BMP to evaluate these requests and generate a score that service providers can use to allow or reject the request.

The depth of data available depends on how the media application was built and what resources are provided by the underlying operating system. As we show in the table on page 10, success with BMP depends not only on the platform but on how the network connections of the application itself were implemented: typically with a web browser provided by the platform, a web browser inside the application (such as is available via WebView in both iOS and Android applications), or native API calls.

Implementing BMP for Best Results

Understand Capabilities, Requirements, and Expectations

Akamai has learned that Bot Manager Premier (BMP) can operate effectively in complex application, API, web, and login environments. But this requires realistic expectations around product capabilities and the integration required with existing applications and APIs. In some cases, for example, applications need to be slightly modified to provide telemetry for BMP. For a login service accessed by legacy applications and devices, those devices might need to be whitelisted inside BMP or managed by controls on the service origin.

Expect to use professional services for initial and ongoing work. Attackers are highly motivated because they are making money from compromising logins. As a result, they will constantly attempt to evade controls that a service applies to combat credential stuffing. While the technology in BMP is a solid foundation, attacks and their signatures will evolve over time to look more like legitimate logins. Because of this, it is highly recommended that customers using BMP to protect against credential stuffing where their traffic has nonbrowser clients should also get a large amount of professional services hours on their contract. This allows time for the following activities:

- *Initial configuration*
- *Analysis of traffic to build profiles for devices*
- *Testing of new devices and applications*
- *Analysis of new attack traffic patterns and reduction of false positives and negatives*
- *Change control*

Expect to Change or Adjust Login Delivery Configurations

Bot Manager Premier (BMP) can only protect login services that it delivers. Media customers typically use Akamai services for large-volume delivery of cacheable content, but some customers do not use Akamai for login service delivery, so the first step in integration is to configure basic delivery for these services.

Akamai as a content delivery network (CDN) serves as a distributed reverse web proxy for HTTP and HTTPS requests. Traffic delivery through the Akamai platform requires a minimal delivery configuration, a FQDN for Akamai to find the origin, and a DNS CNAME to an Akamai-controlled domain.

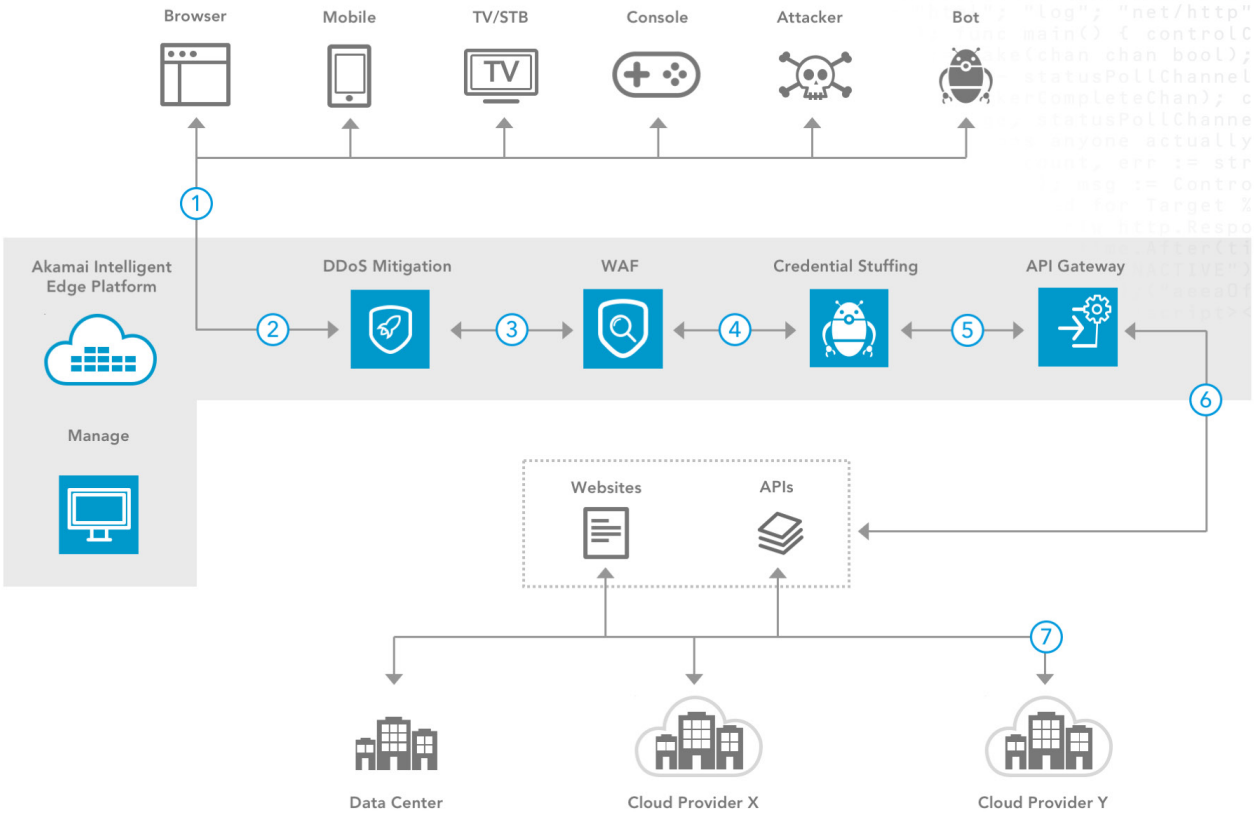
For data protection and compliance reasons, Akamai can only use TCP ports 80 and 443 for customer traffic. This might require port translation or other infrastructure and application changes.

Explore Using BMP to Protect Against Other Attacks

There are several other activities related to credential stuffing that can also be addressed by Akamai:

- Trial account abuse: *Attackers use trial account codes to generate a free account and then create a new account when the trial expires*
- Bulk account creation: *Attackers generate a large amount of accounts at one time using automation*
- Account lockout and denial of service*: Attackers attempt to log in as a legitimate user with an invalid password in order to get the user's account (or multiple users' accounts) locked for excessive number of failed logins*
- Password brute-forcing: *Attackers attempt to log in as a legitimate user by using sequential, incrementing strings as their password*
- Password spraying: *Attackers attempt to log in as many users using the same commonly used password, such as "password" or the name of the service*

BMP resides on the Akamai Intelligent Edge Platform as part of a larger ecosystem of controls that can be added to protect and deliver logins. The following architecture diagram shows some of the basic products and features of the platform:



1. The Akamai Intelligent Edge Platform discards all non-HTTP, non-standards–compliant network traffic.
2. Akamai caches objects that are delivered to multiple endpoints, including SSL/TLS delivery.
3. Akamai's Kona Site Defender (KSD) uses its rate controls to throttle traffic from endpoints that are sending large volumes of requests.
4. KSD also uses its web application firewall (WAF) to inspect traffic for application attacks. This WAF also supports some rules for API protection.
5. BMP checks for credential stuffing or other activity such as data scraping.
6. Akamai's API Gateway combines and publishes APIs, enforces API schemas, and controls rogue clients by using connection throttling.
7. The Akamai Intelligent Edge Platform can perform load balancing or failover between a variety of origin infrastructures.

Implementing Bot Manager Premier

Client Integration

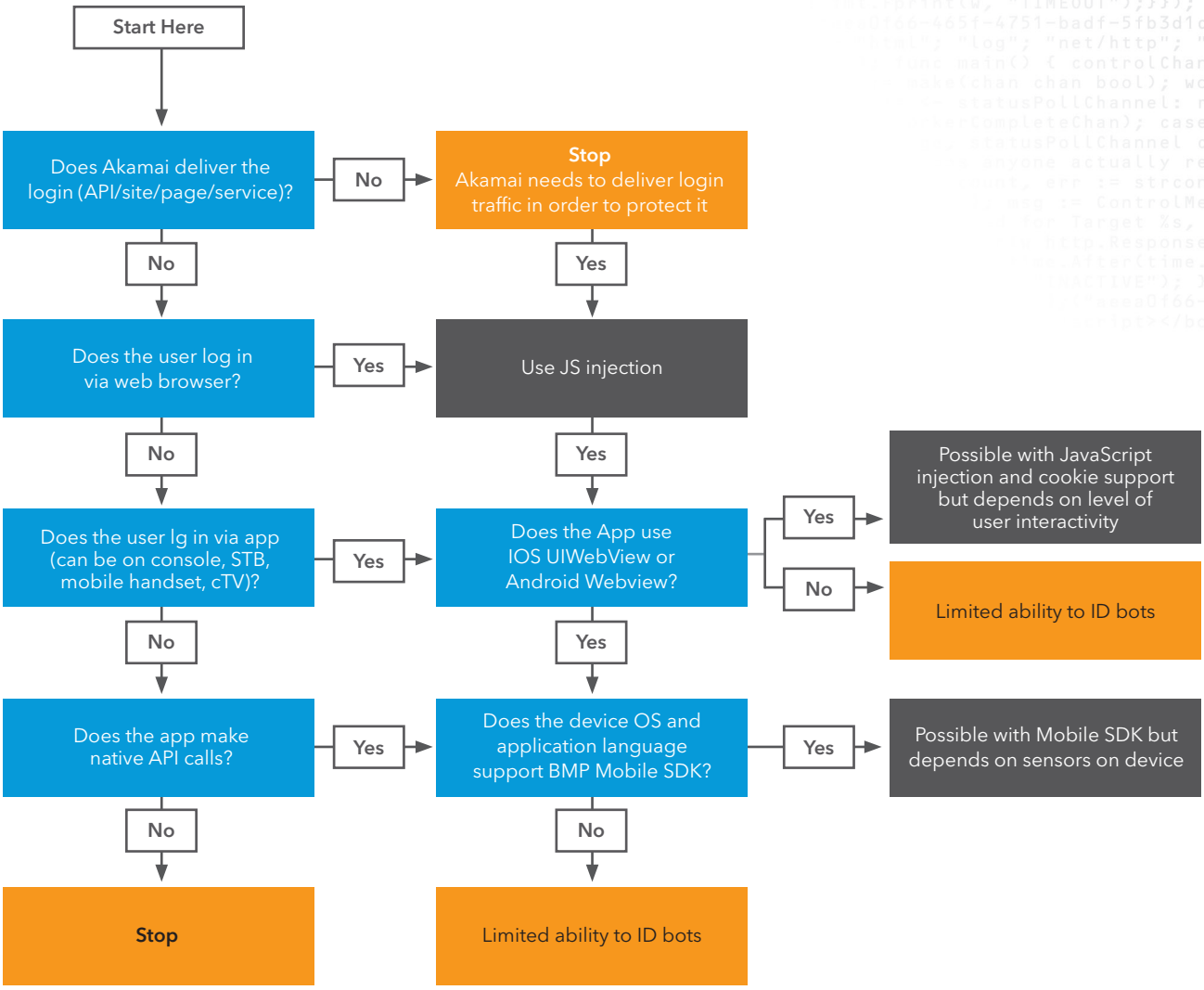
The complex ecosystem of applications and devices can be reduced into several categories of clients based on the amount of data that is provided to Bot Manager Premier (BMP) and its JavaScript injection and application SDK.

LOGIN INTERFACE	BMP USABILITY
Web browser on a desktop/laptop/mobile	Yes. Use JavaScript injection
Mobile/platform application using WebView with JavaScript enabled	Yes. Use JavaScript injection
Mobile/platform application using WebView without JavaScript enabled	Yes, but with highly reduced accuracy leading to more false positives or false negatives*
Mobile/platform application with native API calls and SDK	Yes. Telemetry provided by Mobile SDK
App with native API calls, no SDK	Yes, but with highly reduced accuracy leading to more false positives or false negatives*

* False positives mean a legitimate client is blocked. False negatives mean that a bot was allowed to log in. Customers with applications and devices falling into these categories should have a discussion with an Akamai Security Services Architect to discuss options.

In addition to protecting against credential stuffing attacks, Akamai BMP can prevent trial account abuse, bulk account creation, account lockout and denial of service attacks, password brute-forcing, and more.

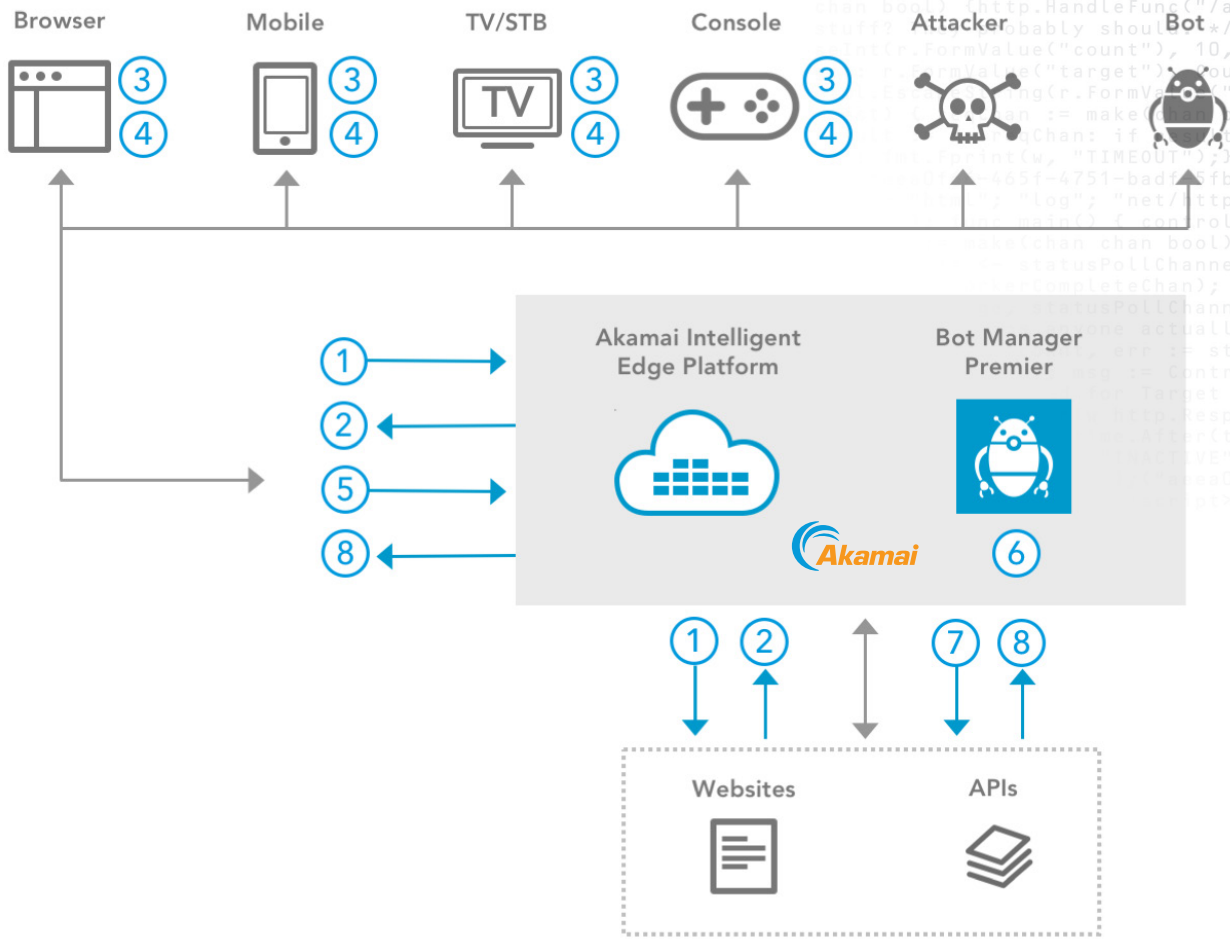
The following flowchart shows the decision tree for when to use each BMP integration on a per-device basis. While the majority of users can be satisfied with JavaScript injection or the Mobile SDK for mobile devices, the other nonbrowser, nonmobile operating systems need to have a strategy outside of BMP. This strategy should be discussed with Akamai Security Services Architects.



JavaScript Injection

Bot Manager Premier (BMP) supports a JavaScript injection method for users who are using a standard web browser on a desktop, laptop, or mobile device. The JavaScript is added to HTML forms, and collects user interface events and uses them to generate a score of how likely the user is a real human or a bot. This score is sent inside the form submission and is paired with other contextual data on the Akamai Intelligent Edge Platform.

Applications Using WebView



The process flow is as follows:

1. Client requests a login form
2. Server responds with form; BMP adds JavaScript injection inside the response form as a <script> tag
3. Client displays the form and runs JavaScript injection
4. Behavior data is collected on the client by JavaScript injection and a score is generated
5. The set of scores is sent in the form submission
6. BMP receives the form submission and the score, and evaluates the submission using the score in addition to a wide variety of other techniques
7. If the client is determined to be human, BMP forwards the form submission to the customer's origin
8. Origin processes the form and sends a response with a login token

More information is available at the Bot Manager Premier product page.

A surprisingly large number of mobile, STB, and gaming console applications use WebView or a functional equivalent for user login. This allows the organization the ability to reuse the same login service or microservice across multiple endpoint APIs. Akamai has seen instances where even STBs and connected TVs operated with a remote control generate enough sensor data inside a WebView with our JavaScript injection to identify human behavior. However, this is highly dependent on the device itself and the application-specific login workflow.

WebView Best Practices

There are several best practices to follow when using WebView in combination with BMP.

Use a unique user-agent for each application version, minor revision, and platform. This allows BMP to perform a match against other data points that we use to profile the application.

Applications that use WebView should be supported with the JavaScript injection features of BMP by turning on support for JavaScript inside the application source code. This requires a slight modification to the application source code as described below.

Enabling JavaScript in WebView may create vulnerabilities in the application, so it is recommended that a separate WebView instance be used specifically for login if the developer does not wish to turn on JavaScript support globally inside the application.

WebView needs to accept and receive cookies. This is for BMP to identify the browser for the duration of the login session.

WebView in iOS

UIWebView allows the developer to enable JavaScript support by setting a variable in the application source code (see https://developer.apple.com/documentation/webkit/wkpreferences/1536203-javascriptenabled).

```
var javaScriptEnabled: Bool { get set }
```

WebView in Android

Android WebView allows the developer to use Java or Kotlin to enable JavaScript and accept cookies (see https://developer.android.com/guide/webapps/webview).

Java:

```
WebView myWebView = (WebView) findViewById(R.id.webview);
WebSettings webSettings = myWebView.getSettings();
WebSettings.setJavaScriptEnabled(true);
CookieManager.getInstance().setAcceptCookie(true);
```

Kotlin:

```
val myWebView: WebView = findViewById(R.id.webview)
myWebView.settings.javaScriptEnabled = true
```

Applications Using Native API Calls

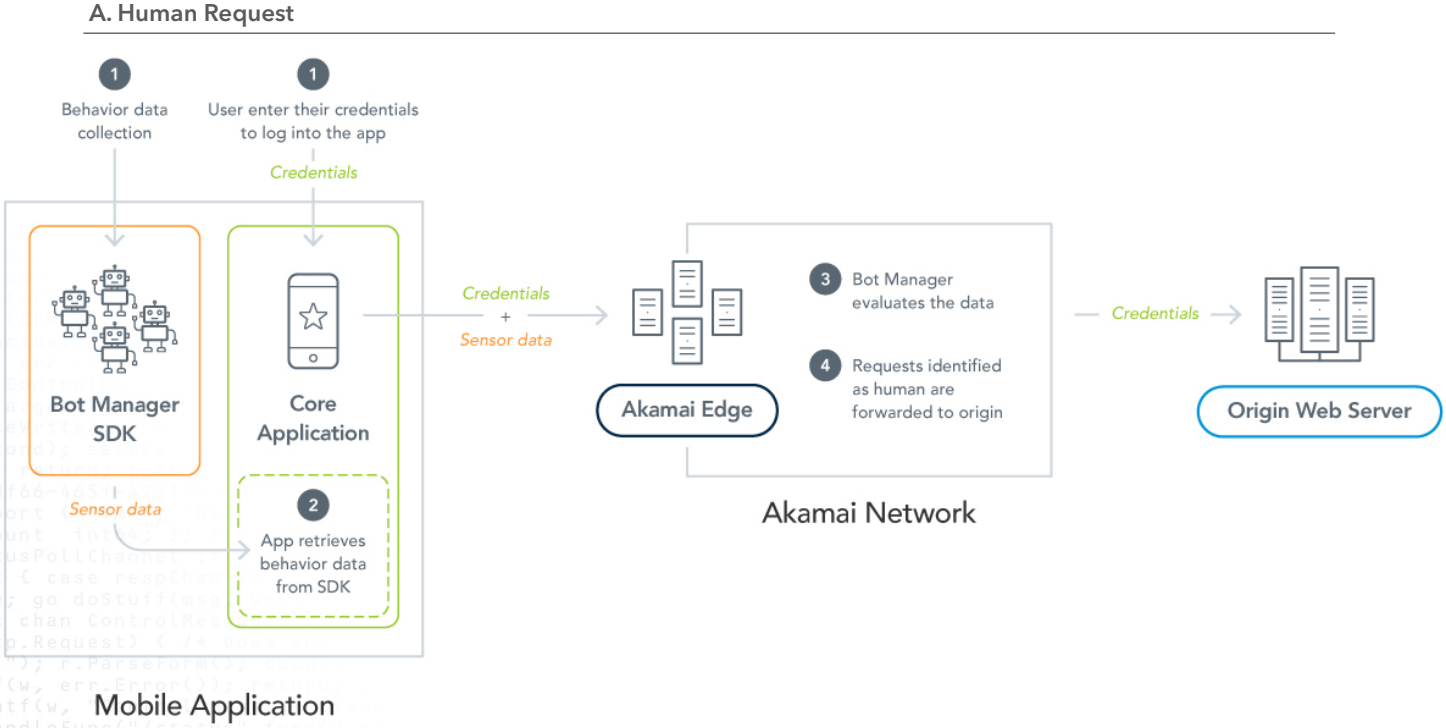
Bot Manager Premier (BMP) Mobile SDK takes the fundamental technology of the product's use of JavaScript injection and applies it to applications running on mobile and embedded platforms such as iOS and Android that use native API calls instead of WebView. The SDK collects behavioral data while the user is interacting with the application. This behavioral data, also known as sensor data, includes the device characteristics, device orientation, accelerometer data, touch events, etc.

In order to use the SDK to protect the application, add it as a library to the source of the application and then invoke the library with a system call.

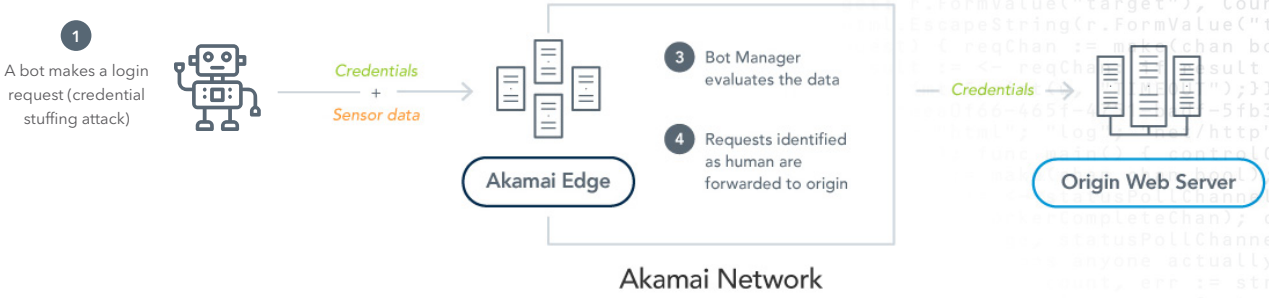
Mobile SDK Best Practices

There are several best practices to follow when using the BMP Mobile SDK. A critical one is to use a unique user-agent for each application and minor revision. This allows BMP to perform a match against other data points that we use to profile the application. More details on the BMP Mobile SDK are available on the developer's portal.

Overview of Mobile SDK



B. Bot Request



High-Level Integration Project Plan

For customers who wish to use Bot Manager Premier (BMP) to protect their logins, the following steps describe the integration process.

1. Configure web and API delivery on Akamai for login.

   Akamai supports several products and features to deliver web applications and APIs. This also requires a DNS CNAME to direct the production traffic to Akamai and an origin DNS FQDN for Akamai to find the origin application server. Additionally, the traffic needs to be HTTPS on TCP port 443.

2. Turn on BMP in "monitor mode."

   This allows BMP to start collecting data and profiling devices and traffic.

3. Optional: Build login flows for logins and other features of BMP.

4. If necessary, add JavaScript and cookie support to WebView applications.

   This will require that the application be updated and released on the relevant application store.

5. Add support for JavaScript injection inside BMP for browser-based and WebView applications.

6. If necessary, add the Mobile SDK to applications that make native API calls.

   This will require that the application be updated and released on the relevant application store.

7. Identify traffic inside of BMP on a per-device, per-application basis.

   This will require Akamai services to assist on identifying traffic.

8. Identify traffic inside BMP for low-use and legacy clients to increase accuracy.

   This could require exceptions to BMP enforcement for some devices. Exceptions should be avoided if possible, and customers needing exceptions should talk to an Akamai Security Services Architect about options.

9. Set the default policy to deny for BMP to only allow known clients operated by real users to access the login.

Conclusion

Serving today's media consumer requires companies to provide and support increasingly complicated login ecosystems. This has led to an increase in both login attacks and the complexity of defending against these attacks. Akamai customers are using Bot Manager Premier to detect and combat credential stuffing, login abuse, and account takeover. However, the profitability of credential stuffing means attackers are strongly motivated to rapidly evolve in the face of new defenses. In the experience of Akamai and our customers, strong technology coupled with analytics and skilled operators makes the difference in finding new vulnerabilities and attack techniques as they are developed.

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone – and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at akamai.com/locations. Published 1/20.