CSO
FROM IDG

June 15, 2020 www.csoonline.com

REVIEW

Auth0 Signals analyzes logins to block bots

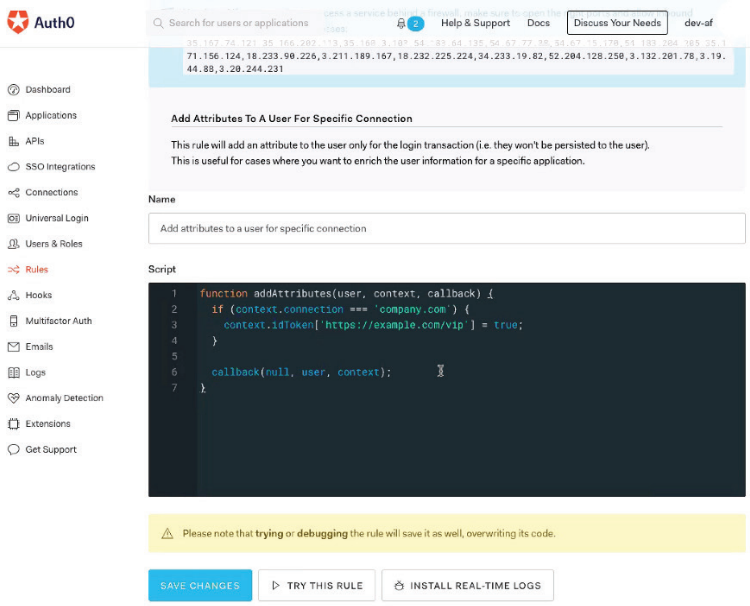
Auth0 Signals, a key component to the Auth0 identity management platform, analyzes login attempts against four key criteria to identify and block script-based or bot attacks.

By John Breeden II

For the past 30 years, computer security has mostly centered on users authorizing themselves at the front door of applications and websites. Once they have entered their correct name and password, an entire site is generally open to them. Auth0 is trying to change that with a platform that offers identity as a service and works throughout the user engagement process, even adding extra security when needed.

The biggest hurdle to such efforts aimed at continuous identity protection, and why most attempts fail, is the sheer number of bot-based and scripted login attempts leveled at websites and applications these days. Those attacks are more than enough to overload most platforms that are trying to analyze users.

To counter these threats, Auth0 Signals was created as a key component to the Auth0 identity management software as a service (SaaS) platform, and in our testing, could stop most script-based attacks, or those leveled by bots.



```
71.156.124,18.233.90.226,3.211.189.167,18.232.225.224,34.233.19.82,52.204.128.250,3.132.201.78,3.19.
44.88,3.20.244.231
```

Add Attributes To A User For Specific Connection

This rule will add an attribute to the user only for the login transaction (i.e. they won't be persisted to the user). This is useful for cases where you want to enrich the user information for a specific application.

Name

Add attributes to a user for specific connection

Script

```
function addAttributes(user, context, callback) {
  if (context.connection === 'company.com') {
    context.idToken['https://example.com/vip'] = true;
  }

  callback(null, user, context);
}
```

⚠ Please note that **trying** or **debugging** the rule will save it as well, overwriting its code.

CSO

The Auth0 Signals engine generates a score for every protected process on a website monitored by the platform. Once a score is generated, users can define rules through the web portal or within their own applications. Possible actions include everything from blocking the transaction to throwing up a captcha challenge.

How Auth0 works

The Auth0 identity as a service platform analyzes various tasks that users can perform, including things like signing up for a website, requesting an account recovery, logging in and renewing a session. When any of those monitored tasks are performed at a company protected by Auth0 (about 25,000 as of this writing, according to company officials), details about that transaction are sent to the anomaly detection engine in the cloud. It will then provide a confidence score that can be used to create rules or trigger responses like blocking that user or throwing up a captcha challenge.

Rules can be created within the web portal, or companies can use the risk assessment score to program their own responses. In either case, nothing is installed within the hosting organization.

Auth0 also has a set of tools for use by developers so that they can easily include the offloading of identity analysis to the platform. There are even widgets for easy drag and drop functionality.

Combating scripted attacks

The Auth0 platform uses four key criteria, called signals, to determine if a login or other attempt to use an identity is valid: velocity, context, IP reputation and predictions based on data. A fifth, behavioral biometrics-based signal is still in development.

Velocity

Velocity basically means how many login attempts are allowed from a single IP address. Most scripted attacks slam multiple login or other attempts through a website as quickly as possible, hoping to find valid username and password combinations. Velocity thresholds limit those attempts to something like 80 to 100 tries within a 24-hour period and are completely configurable.

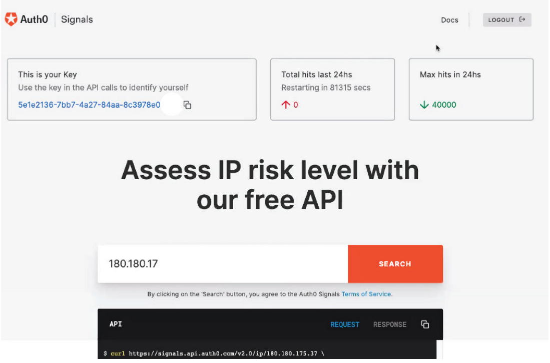
If an attacker realizes that attacks above a certain velocity are getting blocked, they may try to throttle their bots back a little bit, keeping just below the threshold. Auth0 can automatically adjust the threshold to keep blocking the scripted attacks.

Context

Common sense logic rules are used to protect against attackers using captured credentials. For example, if a user logs into their account from Kansas every morning and then suddenly logs in from the Ukraine in the middle of the night, that would be flagged as highly suspicious.

IP reputation

Acquiring IP addresses is not all that difficult for attackers with a little bit of money. But they do tend to reuse the ones they control quite a lot, for reasons of both economy and convenience. That means that many of the scripted attacks are coming from IP address that are known to be bad.



Auth0 | Signals — Docs — LOGOUT

This is your Key
Use the key in the API calls to identify yourself
5e1e2136-7bb7-4a27-84aa-8c3978e0

Total hits last 24hs
Restarting in 81315 secs
↑ 0

Max hits in 24hs
↓ 40000

Assess IP risk level with our free API

180.180.17 — SEARCH

By clicking on the 'Search' button, you agree to the Auth0 Signals Terms of Service.

API — REQUEST — RESPONSE

```
$ curl https://signals.api.auth0.com/v2.0/ip/180.180.175.37 \
```

CSO

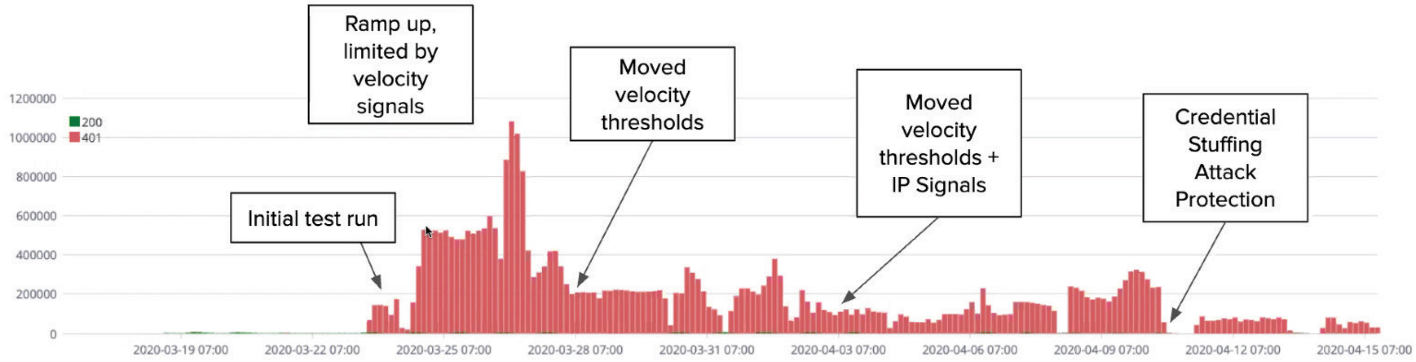
To show proof of concept, Auth0 Signals is making its IP reputation signal available for free. Simply type in an IP address and the company will show all of its collected data about that address.

Data-based predictions

Unlike context, which is based on a single site's users, the predictions signal looks at the overall picture collected from all of the different companies and organizations using the Auth0 platform. For example, an attack from a specific IP address may be targeting multiple companies.

Once a score has been created for a login or other process, applying a rule is almost instantaneous. Valid users won't ever know that their request has been analyzed against the four signals. Actions can include blocking a user or an IP address when the score is high enough that there is total confidence that it's a scripted attack. However, if there is any uncertainty, throwing up a captcha challenge is a perfect way to weed out the bots. Valid users won't have any problem clicking on stoplights, trees or whatever they need to do in order to prove their humanity, but bots will fail every time. And because Auth0 is so careful about cross referencing different signals to get a score, it's likely that only the bots will get the test. If a human somehow does, it won't slow them down very much.

- A very large credential stuffing attack starting on March 23
- Most traffic results in failed logins



CSO

This graph shows how a scripted attack generated hundreds of thousands of login errors as bots tried to invade a financial institution's website in March. As different Auth0 Signals were activated, they knocked down the attack numbers. But the attackers adapted too, trying to get around the protection. Once the entire Auth0 Signals platform was activated, it stopped further intrusion attempts. Normally, the entire platform activates right away, but this customer was wary of causing friction to the user experience.

The bottom line

Pricing for the Auth0 identity management platform is based on the number of valid users that have access to a protected site. For something like an ecommerce site where the number of potential users is unknown, Auth0 has an enterprise plan that provides protection at a reasonable price based on scale. And the analysis of all four Auth0 Signals are included at every tier.

Until someone figures out a better way for users to prove their identity, apps and websites will remain vulnerable to scripted attacks. The Auth0 identity as a service platform does a great job at stopping those attacks. And it not only prevents scripted login attempts, but can also protect every point where a user must prove their identity.

As the platform evolves and adds additional signals like behavioral biometrics, it will get even more precise. But even with the signals it has right now, it can halt most scripted attacks and bots in their tracks. It's a good defense for a sometimes overlooked but critical area in cybersecurity.

Auth0
info@auth0.com
@auth0
www.auth0.com