imperva

CHEATSHEET

Recommended Actions for Detection of Bad Bot Activity

1. Plan ahead when updating your website

Adding login functionality opens up the chances of Credential Stuffing and Credential Cracking attacks.

MARKETING CAMPAIGNS BRING MORE BOTS

For example - launching a limited quantity, high-demand product.
Whether it is a highly sought after pair of sneakers or a new generation gaming console, announce a date and time for a coveted product launch, and bots will be there to get their hands on it first. Make sure that you are prepared to handle the high volume of traffic that is going to include a high ratio of sophisticated bots trying to scoop up the products and deny your customers access.

NEW FUNCTIONALITIES BRING MORE BOTS

Some website functionalities are highly exploitable by bad bots. Adding login functionality opens up the chances of Credential Stuffing and Credential Cracking attacks. Adding a checkout form increases the chances of credit card fraud (Carding/Card Cracking). Adding gift card functionality invites bots to commit fraud. Make sure that these pages have extra security measures and a more strict ruleset.

2. Block or captcha outdated user agents/browsers

The default configurations for many tools and scripts contain user-agent string lists that are largely outdated. This won't stop the more advanced attackers, but it might catch and discourage some. The risk in blocking outdated user agents/ browsers is very low; most modern browsers force auto-updates on users, making it more difficult to surf the web using an outdated version.

We recommend you block or CAPTCHA the following browser versions:

	BLOCK End of Life more than 3 years	**CAPTCHA** End of Life more than 2 years
Chrome version	**<64**	**<72**
Firefox version	**<64**	**<72**
Safari version	**<64**	**<72**
Internet Explorer version	**<64**	**<72**

3. Block known hosting providers and proxy services

Even if the most advanced attackers move to other, more difficult to block networks, many less sophisticated perpetrators use easily accessible hosting and proxy services. Disallowing access from these sources might discourage attackers from coming after your site, API, and mobile apps. Consider blocking traffic from these data centers: *Host Europe GMBH, Dedibox SAS, Digital Ocean, OVH SAS & Choopa, LLC.*

4. Block All Access Points

Be sure to protect exposed APIs and mobile apps—not just your website—and share blocking information between systems wherever possible. Protecting your website does little good if backdoor paths remain open.

Protect exposed APIs and mobile apps—not just your website—and share blocking information between systems wherever possible.

5. Carefully Evaluate Traffic Sources

Monitor traffic sources carefully. Do any have high bounce rates? Do you see lower conversion rates from certain traffic sources? They can be signs of bot traffic.

6. Investigate traffic spikes

Traffic spikes appear to be a great win for your business. But can you find a clear, specific source for the spike? One that is unexplained can be a sign of bad bot activity.

7. Monitor for failed login attempts

Define your failed login attempt baseline, then monitor for anomalies or spikes. Set up alerts so you're automatically notified if any occur. Advanced "low and slow" attacks don't trigger user or session-level alerts, so be sure to set global thresholds.

Define your failed login attempt baseline, then monitor for anomalies or spikes.

8. Monitor increases in failed validation of gift card numbers

An increase in failures, or even traffic, to gift card validation pages can be a signal that bots such as GiftGhostBot are attempting to steal gift card balances.

9. Pay close attention to public data breaches

Newly stolen credentials are more likely to still be active. When large breaches occur anywhere, expect bad bots to run those credentials against your site with increased frequency.

10. Evaluate a bot protection solution

The bot problem is an arms race. Bad actors are working hard every day to attack websites across the globe. The tools used constantly evolve, traffic patterns and sources shift, and advanced bots can even mimic human behavior. Hackers who use bots to target your site are distributed around the world, and their incentives are high. In early bot attack days, you could protect your site with a few tweaks; this report shows that those days are long gone. Today, it's almost impossible to keep up with all of the threats on your own.

imperva.com
+1.866.926.4678