Crypto Challenge Mitigation for Radware Bot Manager

Table of Contents

The Bot Economy and CAPTCHA

Over 50% of all internet traffic today comprises bots, out of which, according to Radware research, an estimated 25% are malicious bots. These bad bots attack an organization's network in various ways, depending on the intention of the user. Bot attacks could be intended to skew the target's visitor/analytics data, exfiltrate sensitive customer or business information, take over user accounts, or damage the organization's goodwill and revenue. The sophistication of these malicious/bad bots has evolved to a level where they can now mimic human behavior, keystrokes, and mouse movements to evade detection and appear as genuine users to conventional security systems. By the time the deceptive behaviors are detected, it might be too late to prevent the threats posed by the malicious bots.

Organizations use several methods to block these automated programs, such as rate limiting and rule-based IP blacklisting to block known bad bot originators. Many organizations also use in-house bot management solutions or manual methods to identify and stop bot attacks. The most widely used technique to block bots is the "Completely Automated Public Turing test to tell Computers and Humans Apart" (CAPTCHA).

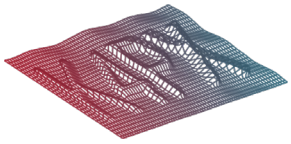
Every website, especially those engaged in business-to-customer interactions, tends to attract spammers, fraudsters and cybercriminals. Traditionally, CAPTCHAs are deployed to block bots and deter fraudsters as they are generally easy for humans to solve, but difficult for bots. However, the key question is: Do CAPTCHAs always work?

While using CAPTCHAs has been the most popular method of keeping bad bots from entering websites, CAPTCHAs can sometimes lead to a bad user experience, customer frustration, and churn. Additionally, with the evolution of CAPTCHA-solver tools and CAPTCHA-avoidance bots, keeping internet properties secure from bots has become a greater challenge than ever before.

Are CAPTCHAs Still Relevant?

Though CAPTCHAs were first developed as a way to mitigate bots and other malicious actors, CAPTCHAs are sometimes challenging for humans to correctly solve. In 2013, Business Insider reported on technology that could be used to solve CAPTCHAs at scale[1]. Today, we are seeing bots easily solving CAPTCHAs and even hiring humans to help them[2]. At the same time, bot masters can avoid CAPTCHAs altogether[3] by using techniques such as rotating proxies and user agents, randomizing the time between requests, using proxy APIs, anti-CAPTCHA plugins and CAPTCHA farms.

Being easily circumvented by sophisticated bots is not the only drawback that CAPTCHA has:

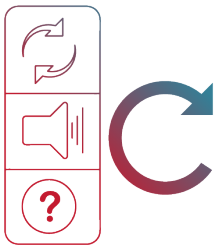


I. CAPTCHAs can be Hard to Solve

About 16% of e-commerce sites today use CAPTCHAs during the checkout process or when performing account-related tasks. A study by Stanford[4] University showed that while CAPTCHAs are made to keep malicious programs out of the network, they present humans with difficulties that often make them harder to solve. The study found that on an average, image-based CAPTCHAs take 9.8 seconds to solve. Audio CAPTCHAs are even harder, with an average time-to-solve of 28.4 seconds.

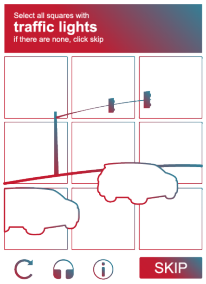
II. CAPTCHAs can be Inconvenient for Users

In a study conducted by Baymard[5], it was observed that 1.47% of the test subjects abandoned a larger incentivized survey, when presented with a CAPTCHA at the end of the survey — indicating that at some point, CAPTCHAs are frustrating and may lead to loss in sales due to users not willing to spend time on solving puzzles to get to their destination.



III. CAPTCHAs may not Translate Across Cultures and for Users with Impairments

Cultural and lingual intricacies and differences add to the CAPTCHA solving problem. Audio CAPTCHAs combined with static or heavy background noise are often hard to understand. Images can be blurry and uncomprehensive and if users have impaired sight or hearing, it is even more difficult for them to solve the CAPTCHAs.



IV. Increased Burden on Users to Prove their Humanity

While CAPTCHAs are still effective against the bulk of automated traffic that are scripted to carry out attacks like scraping; they have a significant drawback — they frustrate users who expect a seamless experience but are instead asked to solve challenges first to prove their being human.

V. Compromised Security

Even if one bot manages to break through defenses and enter a network, the threat of sophisticated account takeover (ATO) and identity theft attacks becomes very real. Securing websites and APIs against bots has become a central concern in today's security landscape and requires new mechanisms to allow continuous protection with minimal performance hazards. Additionally, the Turing test has become highly vulnerable to circumvention in several ways, as mentioned earlier. With highly advanced bots, CAPTCHAs as Turing tests often fail in their goal to detect bots.

For such reasons, a more comprehensive defense system that is capable of adding a protective layer to web-based application security, based on user behavior and continuous risk assessment (along with a Turing test) offers organizations an effective and reliable way to deter evolving threats.

Crypto Challenge Mitigation for Bot Manager

Based on the principles of Blockchain's 'Proof of Work,' Radware Bot Manager enhances its bot mitigation capabilities with a new Cryptographic Challenge mitigation option that is immune to third-party tampering and makes for a seamless and CAPTCHA-free user experience.

This mitigation method requires bots or automated programs to keep solving cryptographic puzzles until they stop their attacks. If they fail to do so, it will slow down their attacks to a standstill, driving costs up for the attackers. The increasing complexity of the challenge makes the attacker expend greater computing (CPU) resources and increases the cost of their attack.

The Technology Behind Crypto Challenge Mitigation

The Crypto Challenge mitigation is based on the now well-known "Proof of Work" concept which is prominently used in the context of Blockchain applications. Putting crucial elements of this into practice, Radware's Crypto Challenge provides a way to mitigate bots using cryptographic Proof of Work-based CPU challenges that must be solved in the visitor's browser. In the context of Blockchain technology, the CPU-intensive challenges are the "Proof of Work" and the website visitors are the miners.

How Does The Crypto Challenge Mitigation Technique Work?

A JavaScript (JS) agent is transferred to the client via a web request for web application protection, or is downloaded and runs in the background when a request is made. While the server responds to the request, a call is simultaneously made to Radware's bot engine to receive the information from the JS agent.

If Crypto Challenge-based mitigation is configured, the moment Radware Bot Manager's bot detection engine detects a source as a bot based on any anomalous behavior, and if any security policies are infringed, the engine reacts instantly by throwing a CPU-intensive cryptographic puzzle-based challenge on the browser, with increasing difficulty. The logic of increasing difficulty is based on several factors, such as the end user's behavior in terms of traversal patterns, for example, has crossed the baseline which is calculated continuously and automatically.

As the difficulty level is increased exponentially, the browser starts to see larger computing resources getting consumed — and beyond a certain difficulty level, the CPU processing becomes so high that the browser hangs, and the malicious actor is just not be able to get through.

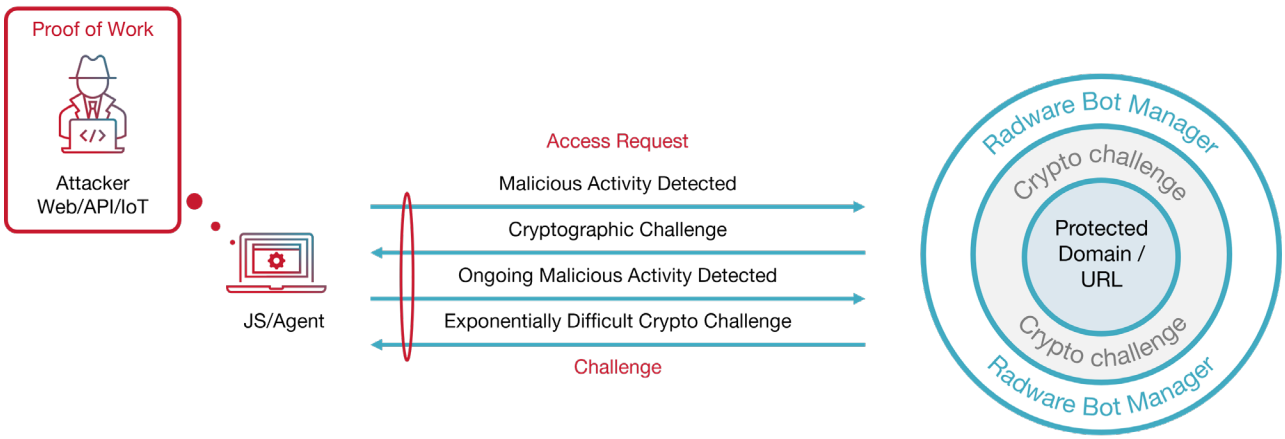


Figure 1: How Does The Crypto Challenge Mitigation Technique Work

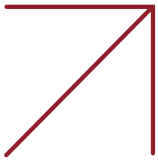
Benefits of Crypto Challenge Mitigation

I. **Security for Grace Period** — Grace period is the duration of time between receiving a valid response to a current CAPTCHA and a new challenge being sent to the user (assuming that the source is still perceived to be suspicious). A bot manager detects incoming traffic using various JavaScript (JS) parameters, however, sophisticated bots such as CAPTCHA solvers and CAPTCHA avoiders can sometimes bypass the first level of CAPTCHA mitigation and proceed to enter the website. Following the first CAPTCHA solved, there is a grace period, only after which the system can block suspected bots. Usually, grace periods are static and can be set in seconds or minutes, but that is sufficient for a bot to cause damage before it is redirected to the CAPTCHA page. With Crypto Challenge, the bot detection system's ability to challenge suspicious visitors is active between challenges, allowing Radware Bot Manager to react to malicious bot activities.

II. **Blocking CAPTCHA Solvers and CAPTCHA Avoiders** — Since the challenges are at the browser level and cannot be seen by the visitor, they cannot be easily evaded even by CAPTCHA farms, smart AI-based CAPTCHA solvers, or humans with malicious intent.

III. **Inflicting Damage on Sophisticated Bots** — Crypto Challenge can also be regarded as a behavior-enforcing mechanism that detects anomalies against a baseline of normative behavior. When it detects a user behaving anomalously the user's device is presented with CPU-intensive challenges that gradually increase in difficulty.. The increasing difficulty of the challenge is exponential by nature, forcing the attacker's CPU to work harder every time it is challenged, effectively creating a 'Cyber Counter Strike' that causes the bots to discontinue their attacks. The attempts to solve the progressively difficult browser challenge use up the CPU spend and push the cost of attack to the attacker; the mitigation approach takes a toll on the attacker's resources, thereby curbing their motivation to run further attacks on the application. For a legitimate user, the CPU usage is insignificant, because even if the browser experiences crypto challenge, the initial difficulty level will be low and there would be no perceivable difference in the CPU usage.

IV. **Multi-layer Protection** — Crypto Challenge mitigation can also be used in conjunction with other mitigation options. For instance, customers can choose to protect certain resources or sections of the Web application with Crypto Challenge mitigation, while other mitigation options can be chosen to protect the other sections, thus providing multi-layered mitigation. The benefit of this method is that an organization can truly focus on protecting the most crucial sections of their digital assets.



Why Choose Crypto Challenge Mitigation

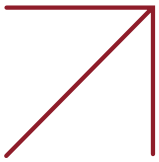
I. **Better user experience** — Crypto Challenge provides visitors with a better user experience since they are not challenged by CAPTCHAs during their journey. Only if their activity deviates from the baseline, the Bot Manager mitigates the malicious hits. In addition, Crypto Challenge's *CAPTCHA-less* flow does not penalize genuine users by throwing them into CAPTCHA loops, while simultaneously preventing sophisticated bots from harming the website or application.

II. **Continuous challenge** — The Crypto Challenge generator is always active as it continuously tracks and tests the website visitors against pre-determined policies for any anomalous behavior that deviates from regular patterns.

III. **Browser level challenges** — Since the challenges are at the browser level and cannot be seen by the visitor, they cannot be easily evaded. One of the reasons why bad actors are successful in carrying out their attacks is because they conduct a pre-vulnerability scan of the targeted application to find potential weaknesses. However, if the bad actors are unaware of how they will be challenged or what those challenges will be, it is difficult for them to evade such it. Mitigation done without a CAPTCHA cannot be bypassed through CAPTCHA farms, smart AI-based CAPTCHA solvers, or humans with malicious intent.

IV. **Damage to the bad actor** — Crypto Challenge confronts bad actors to prove their identity with CPU-intensive challenges and transfers the cost of the mitigation to the attackers. This directly impacts the amount of

time and effort that a malicious actor can afford to invest in bot attacks. It also makes it difficult for bad actors to carry out 'low and slow' attacks since all their resources are fully engaged in submitting the "Proof of Work". Bot masters are soon forced to abandon their attacks as they are confronted with escalating challenges that use up increasing amounts of their computer's processing power.



Conclusion

In today's automated threat landscape, cybercriminals are adept at evading security defenses. They have advanced tools, exploit kits, and deception techniques to program their bots to masquerade as humans and undermine information security solutions. They adapt and evolve their attack methods to keep their bots effective and take advantage of unmonitored traffic flows and ungated access to sensitive data.

Organizations must transition beyond a one-size-fits-all solution and traditional defense mechanisms, and deploy dedicated bot management solutions that combine evolving machine-learning models to deal with increasingly sophisticated bot volumes targeting their internet properties.

Sources:

[1] https://www.businessinsider.in/enterprise/tiny-startup-vicarious-is-creating-a-human-like-brain-that-runs-on-a-laptop/articleshow/24831257.cms

[2] https://www.methodmi.com/reports/in-plain-sight

[3] https://www.bestproxyreviews.com/how-to-avoid-captcha/

[4] http://theory.stanford.edu/people/jcm/papers/captcha-study-oakland10.pdf

[5] https://baymard.com/blog/captchas-in-checkout

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.