Distil Networks
Whitepaper

Do Your Website Bot Defenses Address the Changing Threat Landscape?

Don't let bots turn a minor incident into a mega security breach

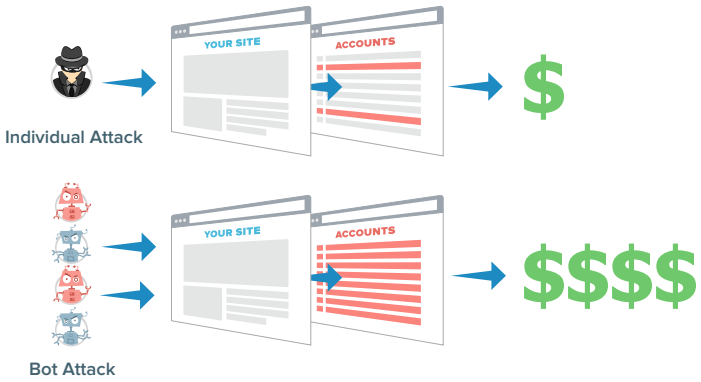
distil networks

www.distilnetworks.com
@Distil
sales@distilnetworks.com
phone: 1.866.423.0606

Executive Summary

The website security threat landscape has dramatically shifted in recent months. Yes, hackers, criminals and other nefarious actors continue to launch sophisticated attacks intended to penetrate and take over website infrastructure. That's not new. What is new is that attackers are increasingly relying on bots to amplify minor incidents into mega security breaches.

BOTS AMPLIFY SECURITY BREACH PAIN

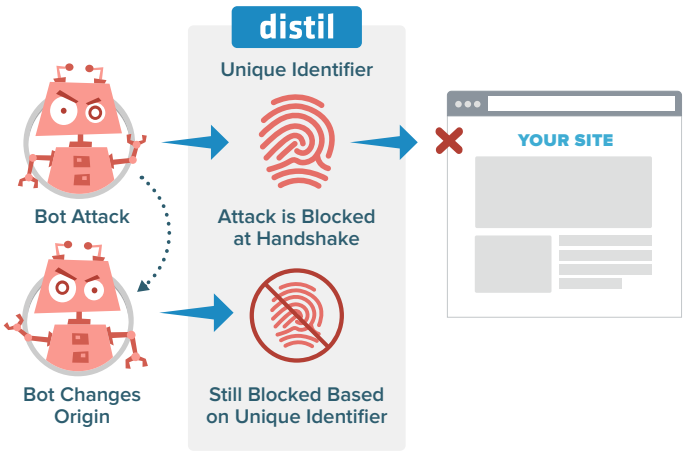


Website managers and IT security professionals must take immediate steps to ensure that a small security breach does not erupt into a high-volume event. Fortifying defenses today can mean the difference between a few compromised database fields or accounts versus a complete loss of brand value and customer loyalty.

The ease with which attackers can use bots to amplify and morph attack origins has rendered helpless the normal arsenal of website security tools. For example, Web Application Firewalls (WAFs) were never designed to stop and manage the volume, variety and sophistication of today's bots. WAFs block website users based on their IP address, but that approach doesn't block all bots. WAFs paint with too broad a brush, blocking legitimate user requests that might share an IP range with the bot. Bots can come from sources websites normally want to engage, such as servers and personal computers, thus reducing the effectiveness of IP-based strategies.

There is a clear need for an automatic and accurate way to detect and block malicious bots, malware and competitors without impacting legitimate users. Distil Networks is maniacally focused on doing just that. Distil analyzes over 40 bits of information from each client request to build a fingerprint that sticks to the bot even if it attempts to reconnect from random IP addresses or hide behind an anonymous proxy. Distil can even detect browser automation tools and bad bots masquerading as good bots (e.g., Google, Bing, etc.). Bad bots are added to Distil's Known Violators Database, which contains the collective intelligence of all Distil-protected sites. Finally, the technology uses machine-learning algorithms to pinpoint behavioral anomalies specific to your site's unique traffic patterns.

DISTIL IDENTIFIES AND STOPS INITIAL ATTACKS AND REPEAT ATTACKS FROM MALICIOUS BOTS AUTOMATICALLY

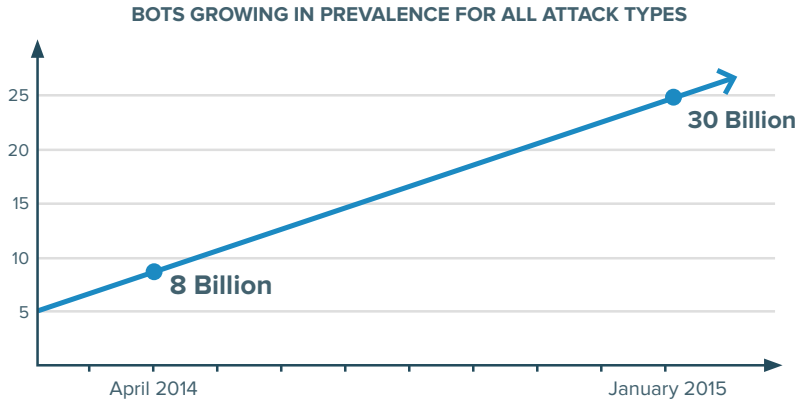


distil networks
www.distilnetworks.com
@Distil
sales@distilnetworks.com
phone: 1.866.423.0606

Bots Amplify Website Security Threats

Cloud computing and virtualization have enabled attackers to launch bot attacks faster and at a lower cost than ever before. Why hack 10 accounts manually when you can use an automated bot to hack 100,000? Attackers can use bots to uncover website security vulnerabilities at scale, then launch an attack using scraper bots from a virtualized environment. Attackers can dynamically spin up scraper resources, spin them down, change IP address, and then spin them up again—all in an effort to avoid detection or out-maneuver your web defenses.

Bots have become so prevalent that Distil Networks has fingerprinted and blocked more than 30 billion (that's right, billion!) bots as of January, 2015, the majority of which were launched in the last 12 months.



Reactive, IP-based Bot Blocking Solutions Don't Work

To understand the benefit of proactive bot detection and mitigation, let's view it through the lens of a massive security breach.

In August 2014, Russian hackers assembled a list of 1.2 billion stolen usernames and passwords. Using this list, attackers leveraged bots to attempt to penetrate user accounts at the domain registrar Namecheap.com. The bots emulated the login process of legitimate users with Firefox, Safari and Chrome browsers. As PC World put it, "The attackers are trying brute-force attempts to gain control of accounts, which involves repeatedly trying different usernames and passwords until the right combination grants access."

Namecheap relied on the all-too-common method of bot mitigation based on damage already done. According to a Namecheap statement issued on September 1, 2014, "Overnight, our intrusion detection systems alerted us to a much higher than normal load against our login systems. Upon investigation, we determined that username and password data gathered from third party sites is being used to try and gain access to Namecheap.com accounts. As a precaution, we are aggressively blocking the IP addresses that appear to be logging in with the stolen password data..." The attackers succeeded in bot-driven logins and Namecheap countered by aggressively blocking IP addresses. Namecheap's reactive approach failed to protect their website and customer data.

Had Namecheap included proactive bot detection and mitigation as part of its security posture, the bots attempting the bruteforce logins would have been fingerprinted (identified and marked) in real time. Thus, after the first few login attempts, the technology would have automatically blocked all further bot-driven login activities and notified Namecheap's security team.

distil networks

www.distilnetworks.com
@Distil
sales@distilnetworks.com
phone: 1.866.423.0606

Skyrocketing Costs of a Website Security Breach

As the Namecheap brute-force attack shows, bot attacks are being launched on a larger scale and penetrating more assets than ever before. Today, the average cost of a website security breach is $300,000.[i] But it can be much, much more. For example, a phishing hack of a single customer account may not amount to much, but damage from a phishing attack that affects 500 customer accounts can quickly reach $1.4 million..[ii]

Losses from a website security breach can include:

- Lost revenue from website downtime
- Losses from breached accounts
- Repercussions from fraudulent purchases
- Increased customer service costs
- Increased server and bandwidth costs
- Loss of user confidence and trust
- Damage to the brand and reputation

Each one of these costs can grow exponentially when bots automate the attack and deliver faster, wider reaching damage before anyone notices a breach has occurred. In addition to the immediate hard dollar costs, businesses that fall victim to website security breaches lose significant brand loyalty. In a recent study, 42 percent of consumers said they are less likely to do business with a brand if that brand exposes them to a cyberattack.[iii]

Common Website Security Threats

Bots are constantly scanning websites looking for security vulnerabilities. And with today's technology, bots are becoming increasingly sophisticated and have the capability to unleash major attacks, multiplying your website vulnerability exponentially. Bots can perform brute-force login attacks like the one described in the Namecheap.com example above, as well as scan for code vulnerabilities and then launch specific types of attacks to exploit those vulnerabilities.

In its most recent report of the "Top Ten" website security breaches, the Open Web Application Security Project (OWASP) highlighted Cross-Site Scripting (XSS) and Injection Attacks among the most common threats to websites. Our own data from 2014 concurs with those findings and supplements them with an additional top threat, Remote Code Execution.

---

i Webinar with Dyn, data source IBM

ii Webinar with Dyn , data source Malcovery

iii Webinar with Dyn, data source Return Path

distil networks

www.distilnetworks.com
@Distil
sales@distilnetworks.com
phone: 1.866.423.0606

Conclusion

To date, website managers and IT professionals have attempted to fend off bot-based and other malicious activity with a variety of security technologies that were never designed for this purpose. Standard firewalls, web application firewalls (WAFs) and CDN-based protection against attacks have failed to keep pace with the fast-changing nature of bots and cannot register real threats. As a result, bots bypass these security solutions mostly unnoticed.

Some IT professionals have developed their own homegrown solutions to identify and block bad bots, but they quickly realize that the ever-changing nature of bot attacks requires a large set of resources and dedication to full-time bot detection. Dealing with bots manually places a huge tax on product management and technical teams. In the end, tedious Whack-A-Mole strategies cannot keep up, and their security stance grows obsolete quickly.

Fortunately, IT professionals can now deploy very specific and proactive bot defenses, enabling them to continuously fend off bot attacks accurately and automatically.

Connect with Distil Networks Today

Distil's bot detection and mitigation solution is simple to understand and can be implemented in hours. Contact us today by calling 1.866.423.0606 or sending an email to sales@distilnetworks.com to get a no-obligation free trial, or a free threat analysis for your site.

distil networks

www.distilnetworks.com
@Distil
sales@distilnetworks.com
phone: 1.866.423.0606

About Distil Networks

Distil Networks, the global leader in bot detection and mitigation, offers the most automated and accurate way to identify and police malicious website traffic, blocking 99.9% of bad bots, malware and competitors — without impacting legitimate users. Distil protects against web scraping, competitive data mining, account hacking, form spam and click fraud while slashing the high tax that bots place on your internal teams and web infrastructure. For more information on Distil Networks, visit us at www.distilnetworks.com or follow @DISTIL on twitter.

Visit us on the web at

http://www.distilnetworks.com

Our Cloud Locations

Seattle, WA	New York, NY	Amsterdam
San Jose, CA	Washington, DC	Singapore
Los Angeles, CA	Miami, FL	Hong Kong
Denver, CO	São Paulo	Tokyo
Dallas, TX	Dublin	Sydney
Chicago, IL	London	

distil networks

www.distilnetworks.com
@Distil
sales@distilnetworks.com
phone: 1.866.423.0606