Radware Bot Analyzer

Free Evaluation of Bot Traffic and Bot Attacks

Today, 24.5% of the total internet traffic is generated by bad bots. Unfortunately, many organizations cannot make a definitive distinction between good and bad bots[1]. As businesses rely heavily on good bots to accelerate business processes such as data collection and decision making, bad bots steal data and disrupt service, and are to be detected and blocked. This isn't a simple task at all, since new types of bots mimic human behavior and bypass security challenges easily. Radware Bot Analyzer is a free service for businesses susceptible to bot activity and those who'd like to get a better knowledge of the impact of malicious bots on their organization.

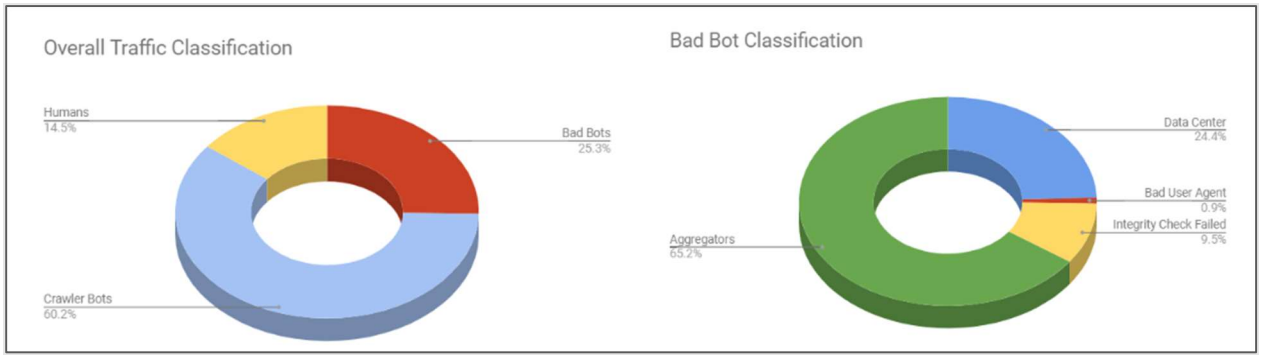

Figure 1: Bot traffic analysis

What Does Bot Analyzer Do?

Radware Bot Analyzer provides visibility into account takeover attempts, inventory holdups, payment frauds and webscraping against **websites, APIs and mobile applications**. combines deep behavioral analysis and semi-supervised machine learning to provide the most accurate snapshot of your bot traffic, including false positives and attacks that get through.

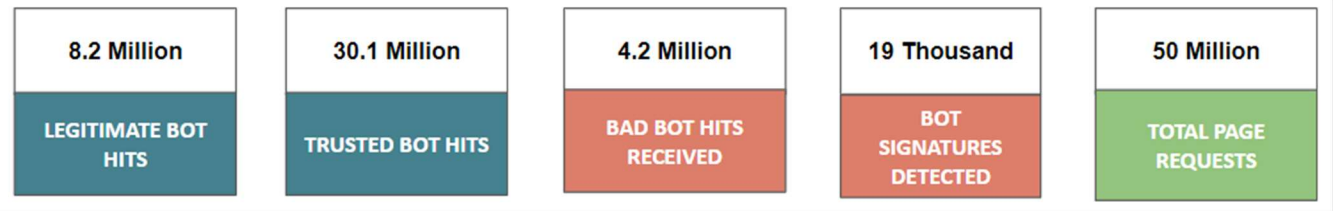

Figure 2: overall synopsis

[1] https://www.radware.com/products/bot-manager/#big-bad-bot-research

Three easy steps:

1. Sign up on https://www.radware.com/products/bot-manager-contact
2. Share server logs when contacted with instructions
3. Get a 360° analysis within 48 hours

The Analysis includes:

✓ Bot Traffic Analysis ✓ Genuine users ✓ Classification of Bad Bots types ✓ Classification of Good Bots types	✓ Targeted URLs ✓ Potential vulnerabilities ✓ Bot source analysis: Data Center / Proxy IPs Public cloud / ToR	✓ Bad bots by sophistication level ✓ Rotating IPs (Distributed Attacks) ✓ behavioral clustering & segmentation ✓ Origin by geography ✓ Recommendations

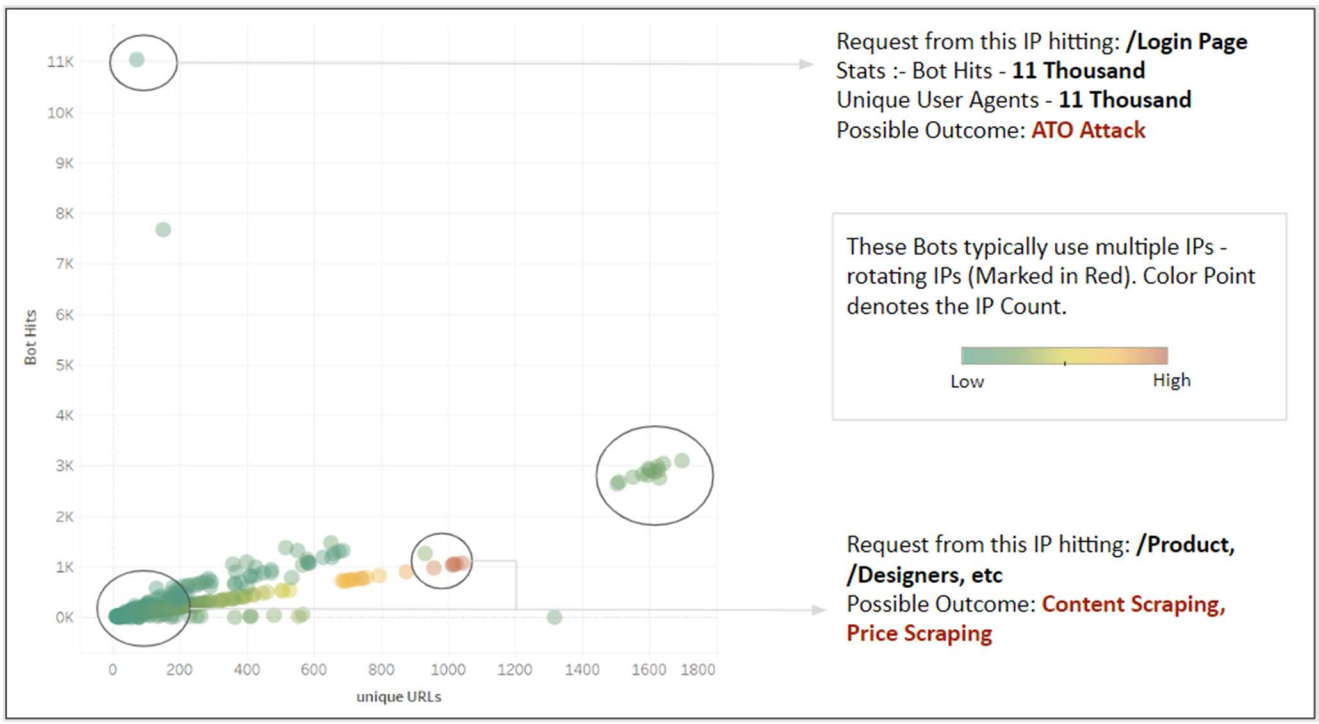

Figure 3: behavioral clustering and segmentation of Bad Bots

Cooperation is key to success:

- A reasonable log file size should be up to 5GB (consider uploading time)
- Please point out internal bots and IP ranges or domains to ignore
- Notify on triggers of specific internal API calls or multiple AJAX calls
- A more granular, customized analysis require additional 24 hours
- An NDA is optional where headers include User ID/Account ID data

Subnet_series	Unique_IPs	Bot Hits	Unique URLs	Unique UAs	ISP
[redacted]	256	141646	141620	258	[redacted]
[redacted]	255	7402	4411	2113	[redacted]
[redacted]	**252**	**10848**	**10785**	**10778**	[redacted] CRITICAL
[redacted]	**252**	**11014**	**10953**	**10936**	[redacted]
[redacted]	239	1262	989	637	[redacted]
[redacted]	237	1542	1201	728	[redacted]
[redacted]	221	1112	850	517	[redacted]
[redacted]	219	1212	906	555	[redacted]
[redacted]	189	785	598	343	[redacted]
[redacted]	172	569	447	289	[redacted]

Figure 4: Rotating IPs (Distributed Attacks)

©2020 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this press release are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details please see: https://www.radware.com/LegalNotice/. All other trademarks and names are property of their respective owners.