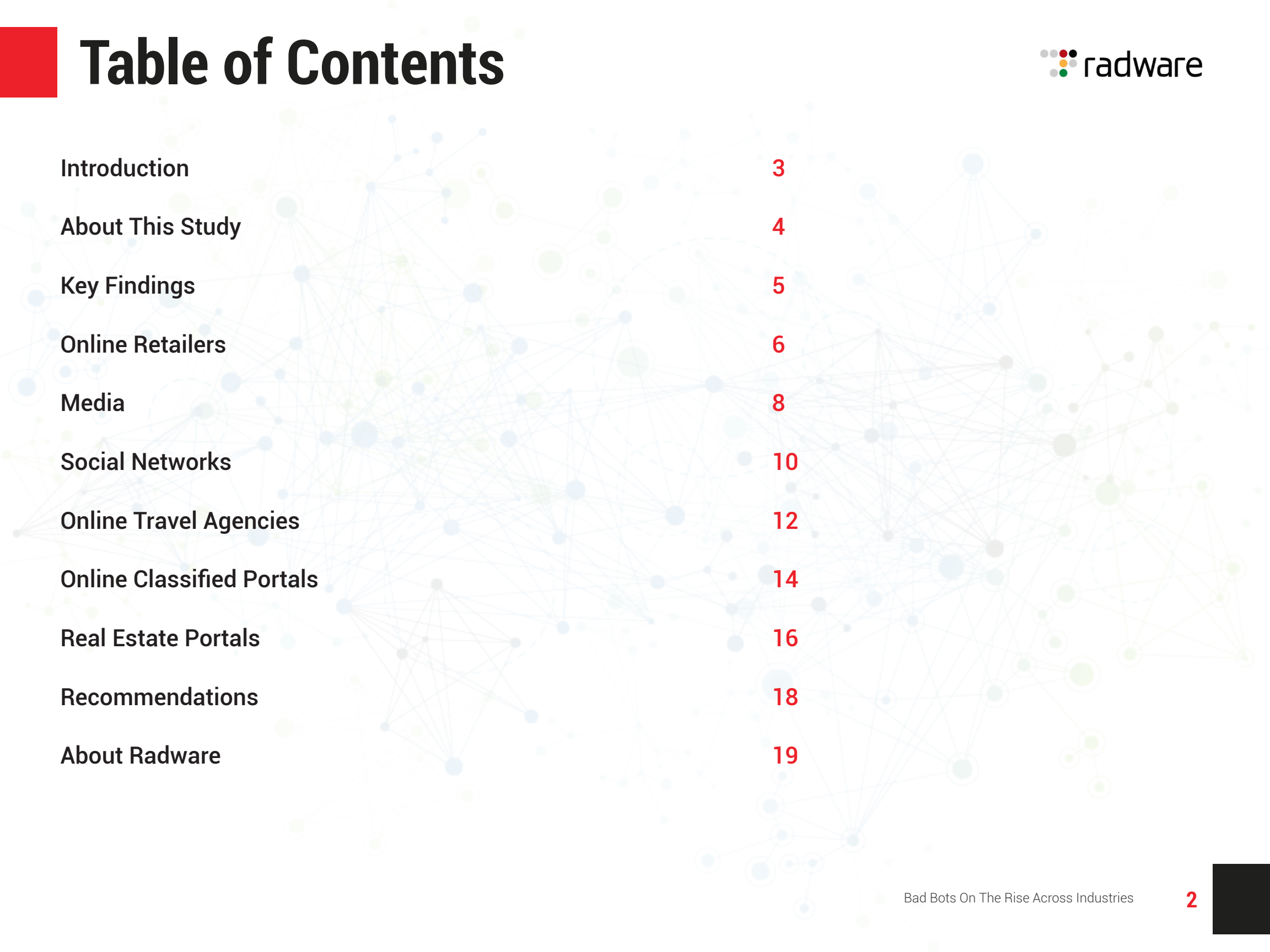


Radware Research

Bad Bots On The Rise Across Industries

August 2018

Table of Contents



Introduction	3
About This Study	4
Key Findings	5
Online Retailers	6
Media	8
Social Networks	10
Online Travel Agencies	12
Online Classified Portals	14
Real Estate Portals	16
Recommendations	18
About Radware	19

Introduction

Studies show that about [half of all internet traffic comprises bots](#). At Radware Bot Manager we process tens of billions of API calls every month, and we discovered that virtually every login page across our client base is targeted by bots. These findings bring up the question: Why do bots attack particular web pages from certain industries a lot more than others?

Our experience in securing over 80,000 internet properties owned by global brands reveals that bots are much more likely to target certain categories of web pages to carry out their attacks. These attacks cause severe business problems such as theft and duplication of original content, increased fraud and chargebacks, downgraded search rankings, loss of revenue and goodwill, poor user experience, unavailability of inventory, and distorted analytics. This study highlights the incidence of bot attacks on certain categories of web pages, the business problems they cause, and the corresponding symptoms to pay heed to.

About This Study

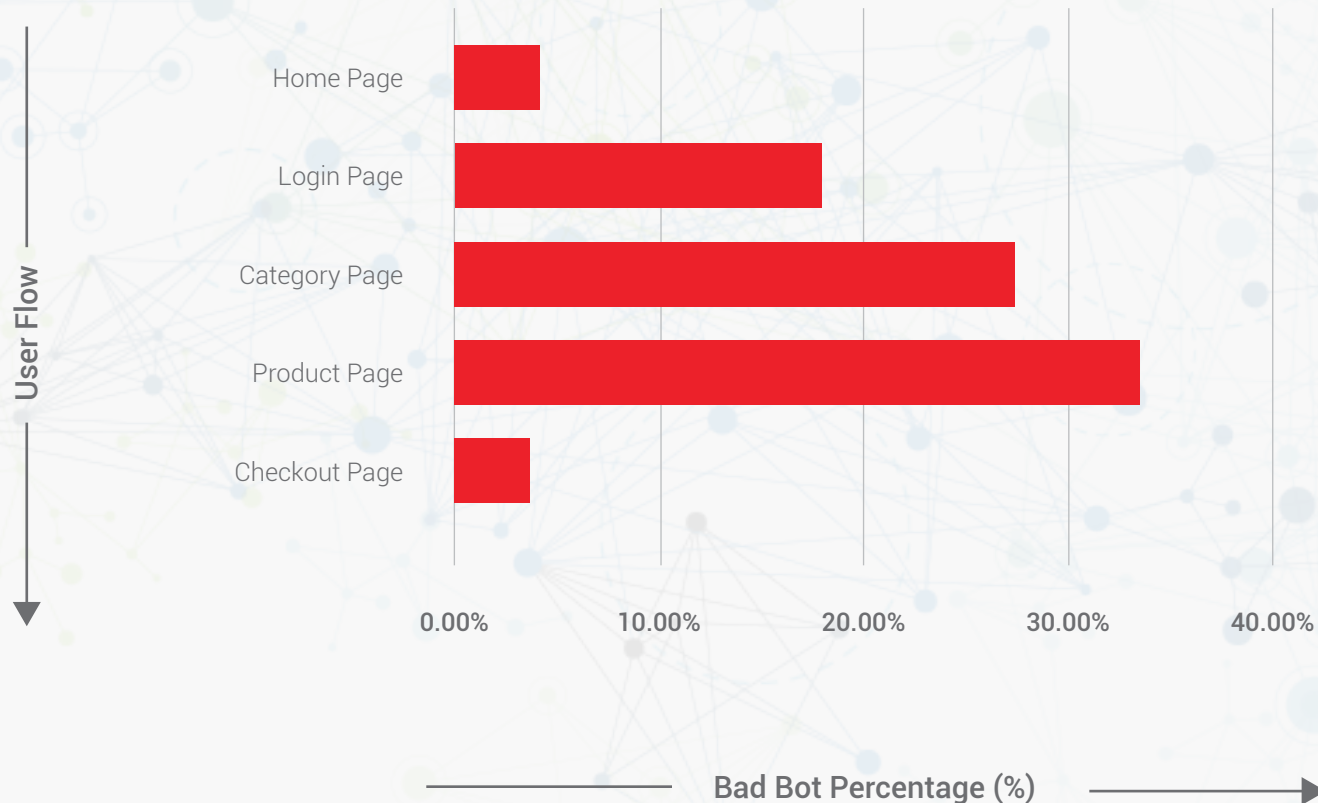
This brief study examines the page categories for each industry that are most targeted by bots, lists the key problems caused by bot attacks, and details the symptoms of bot attacks that website owners and operators need to watch out for. Our study is based on our analysis of representative Radware Bot Manager customers chosen from industries that see large-scale, persistent bot attacks, such as E-commerce, Media & Publishing, Social Networks, Online Travel Agencies, Classified Ads, and Real Estate

To provide a more accurate representative sample of bot traffic on websites from each industry, we aggregated the anonymized bot traffic data from several firms in each industry, and plotted bot traffic percentages and the key pages or page categories most targeted by bots. We then listed the key business problems caused by bot attacks on these industry categories, along with the symptoms that indicate the prevalence of bot attacks on each website.

Key Findings

- ▶ Bots preferentially target business-critical pages such as login and checkout pages, payment processing pages, and product and search listing pages.
- ▶ Though the majority of the representative websites have existing security systems such as Web Application Firewalls (WAF), bot hits on web pages continued unabated.
- ▶ While most of these representative websites used analytics suites from leading vendors such as Google and Adobe, their marketing and business teams did not have insight into the actual volumes of bot traffic on their most-attacked pages and page categories.
- ▶ Bots mutate. Attackers quickly adapt and change their attack techniques to evade conventional security systems. Hence these representative websites decided to deploy a real-time bot management solution because of the growing sophistication of bot attacks.

Trend Of Automated Traffic On Pages Across Online Retailers



Business Problems

- ▶ Competitive scraping of products, prices, and availability; Undercutting of prices
- ▶ Bots were carrying out account takeover attacks through credential stuffing to steal referral bonuses
- ▶ Botnet operators partnered with unscrupulous affiliates to send non-human traffic
- ▶ Large-scale distributed brute force attacks

Business problem

Associated symptoms

Competitive scraping of products, prices, and availability; Undercutting of prices

- ▶ Unusually high activity on new and/or discounted product pages
- ▶ Decreased search engine ranking
- ▶ Increased server and network usage, often with website slowdowns

Bots were carrying out account takeover attacks through credential stuffing to steal referral bonuses

- ▶ Sequential login attempts with different credentials from the same web client (based on IP, User Agent, device, fingerprint, patterns in HTTP headers, etc.)
- ▶ A large number of failed login attempts
- ▶ Increased customer complaints of account hijacking through customer support or social media

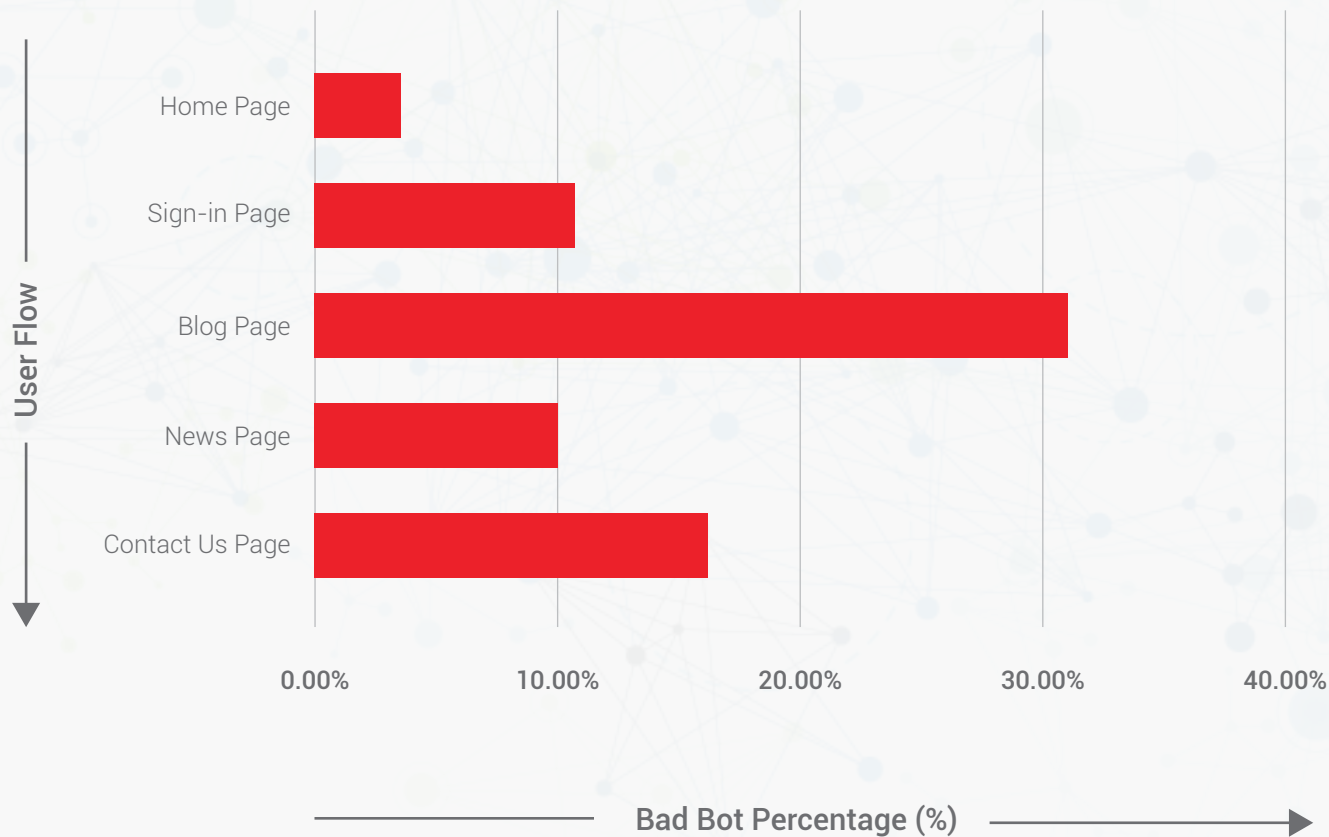
Botnet operators partnered with unscrupulous affiliates to send non-human traffic

- ▶ Lower conversion rates on product pages with affiliate programs
- ▶ Higher than expected bounce rates on product pages with limited availability sales and affiliate programs

Large-scale distributed brute force attacks

- ▶ Bot attacks from thousands of IPs through hundreds of genuine ISPs
- ▶ Many authentication attempts with minor account name and/or password variations
- ▶ Increased account lock rate

Trend Of Automated Traffic On Pages Across Digital Publishers



Business Problems

- ▶ Scraping of news and original or premium content
- ▶ Ad fraud

Business problem

Scraping of news and original or premium content

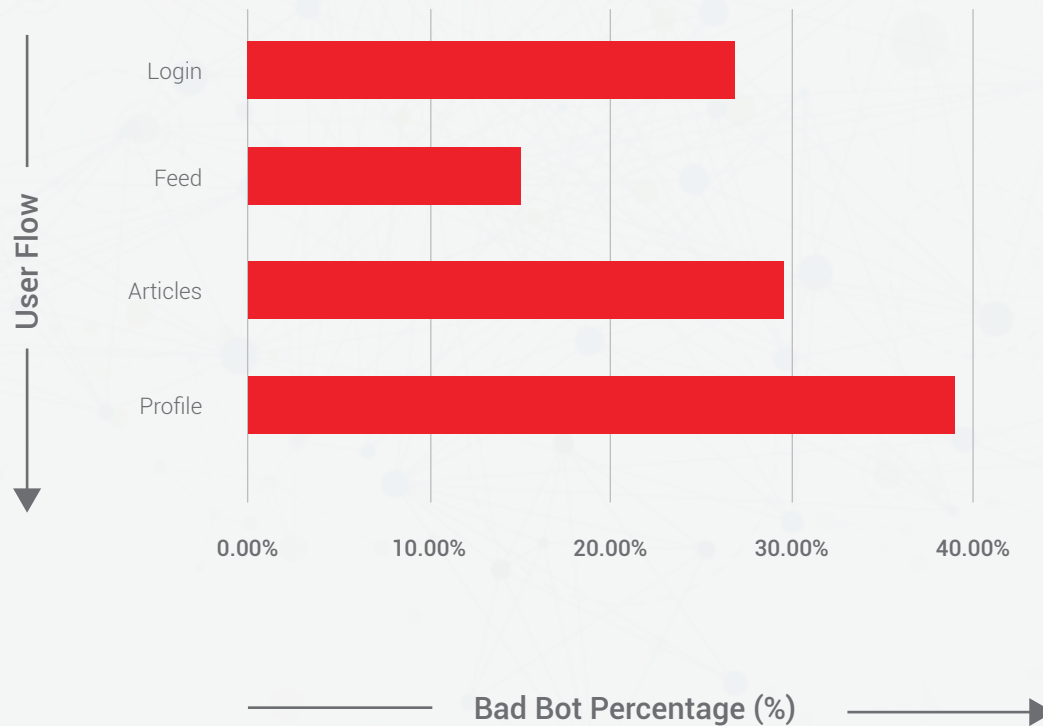
Ad fraud

Associated symptoms

- ▶ Unusual request activity for selected resources (e.g. higher than average page loads for premium content)
- ▶ Duplicated content from multiple sources in search engine results
- ▶ Decreased search engine ranking
- ▶ New competitors with similar or identical content

- ▶ Unusual peaks in the number of clicks or impressions
- ▶ Reduced page view numbers and higher bounce rates during spikes in impressions or clicks

Trend Of Automated Traffic On Pages Across Social Networks



Business Problems

- ▶ Comment spam
- ▶ Ad fraud
- ▶ Fake account creation
- ▶ Scraping of trending content

Business problem

Associated symptoms

Comment spam

- ▶ Higher rate of complaints from users about spam content
- ▶ High appearance of typically fraudulent keywords in user-generated content
- ▶ High hyperlink density
- ▶ Inclusion of hyperlinks to web hosts that redirect, or with low reputation, or that host malicious content

Ad fraud

- ▶ Common patterns such as the same Referrer or User Agent in click or impression spikes (peaks)
- ▶ Unusual peaks in the number of clicks or impressions
- ▶ Drop in the number of page views during peaks in impressions or clicks
- ▶ Higher bounce rate during peaks in impressions or clicks

Fake account creation

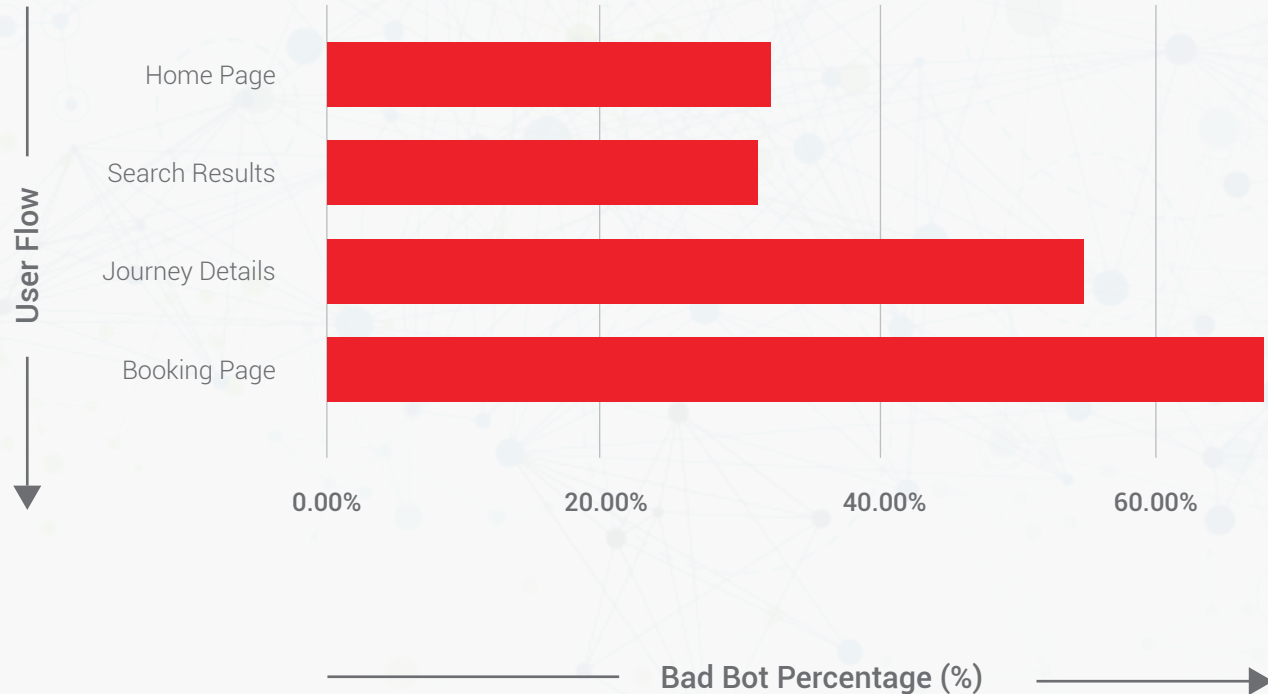
- ▶ Accounts with incomplete information relative to the typical account holders
- ▶ Accounts created but which are not used immediately or remain dormant for long periods
- ▶ Accounts created with disproportionate use, and/or misuse of the application's functionalities

Scraping of trending content

- ▶ Unusually high activity on trending content
- ▶ Duplicated trending content appearing on other sites

Online Travel Agencies

Trend Of Automated Traffic On Pages Across Online Travel Agencies



Business Problems

- ▶ Unauthorized GDS Queries; scraping of travel and hotel information, reviews and prices
- ▶ Bot attacks on checkout pages led to blocking of low fare deals

Online Travel Agencies

Business problem

Unauthorized GDS queries; scraping of travel and hotel information, reviews, and prices

Bot attacks on checkout pages led to blocking of low fare deals

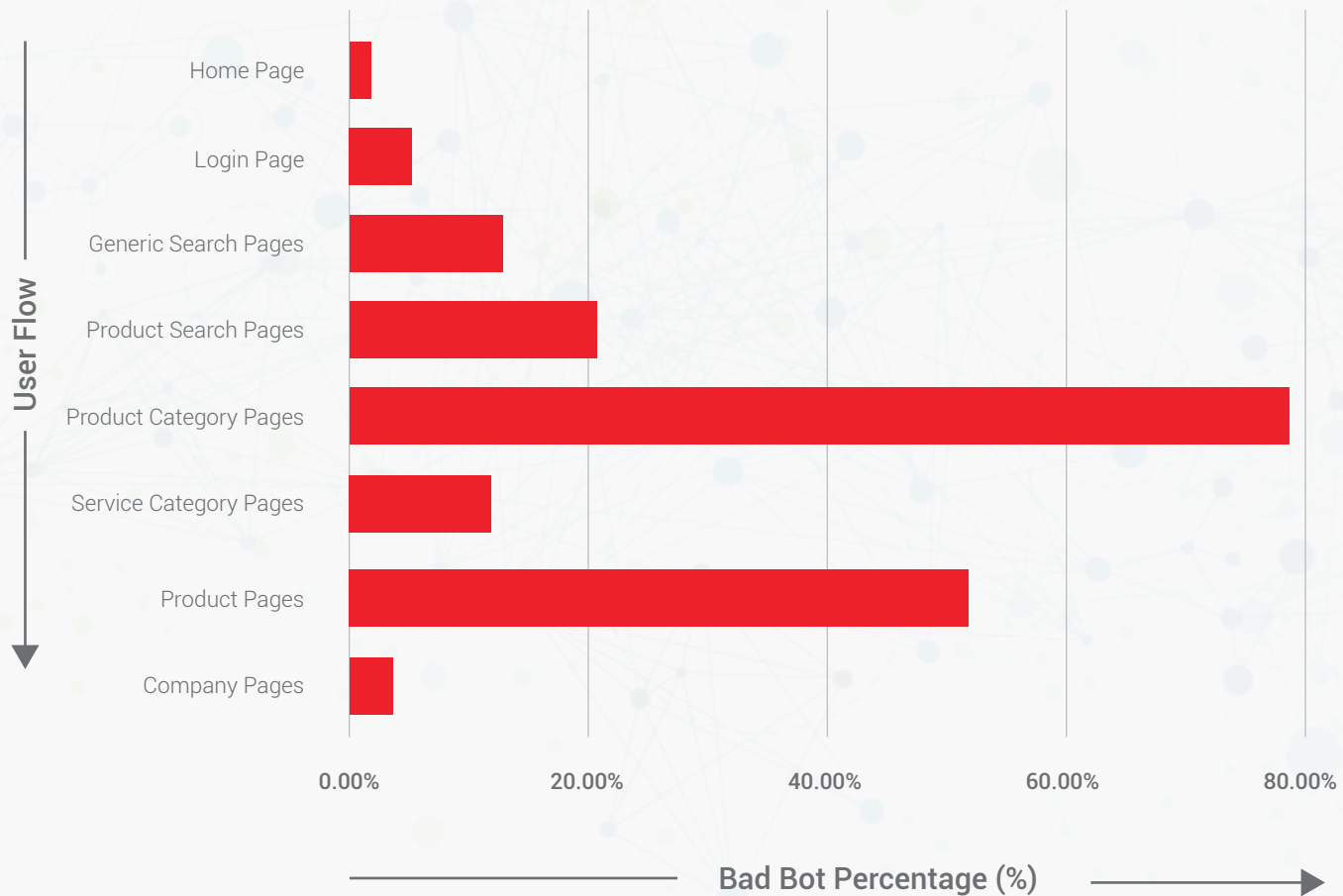
Associated symptoms

- ▶ Unusually high browsing activity on travel and accommodation pages at certain times
- ▶ Identical or highly similar deals from other websites and competitors

- ▶ Rapid reduction in available inventory
- ▶ Increase in reservations added to checkout pages but without payments made
- ▶ Increasing complaints from users about their inability to make bookings using deals

Online Classified Portals

Trend Of Automated Traffic On Pages Across Online Classified Portals



Business Problems

- ▶ Scraping of classified ad listings
- ▶ Fake leads, Spam entries and comments led to poor customer experience

Online Classified Portals

Business problem

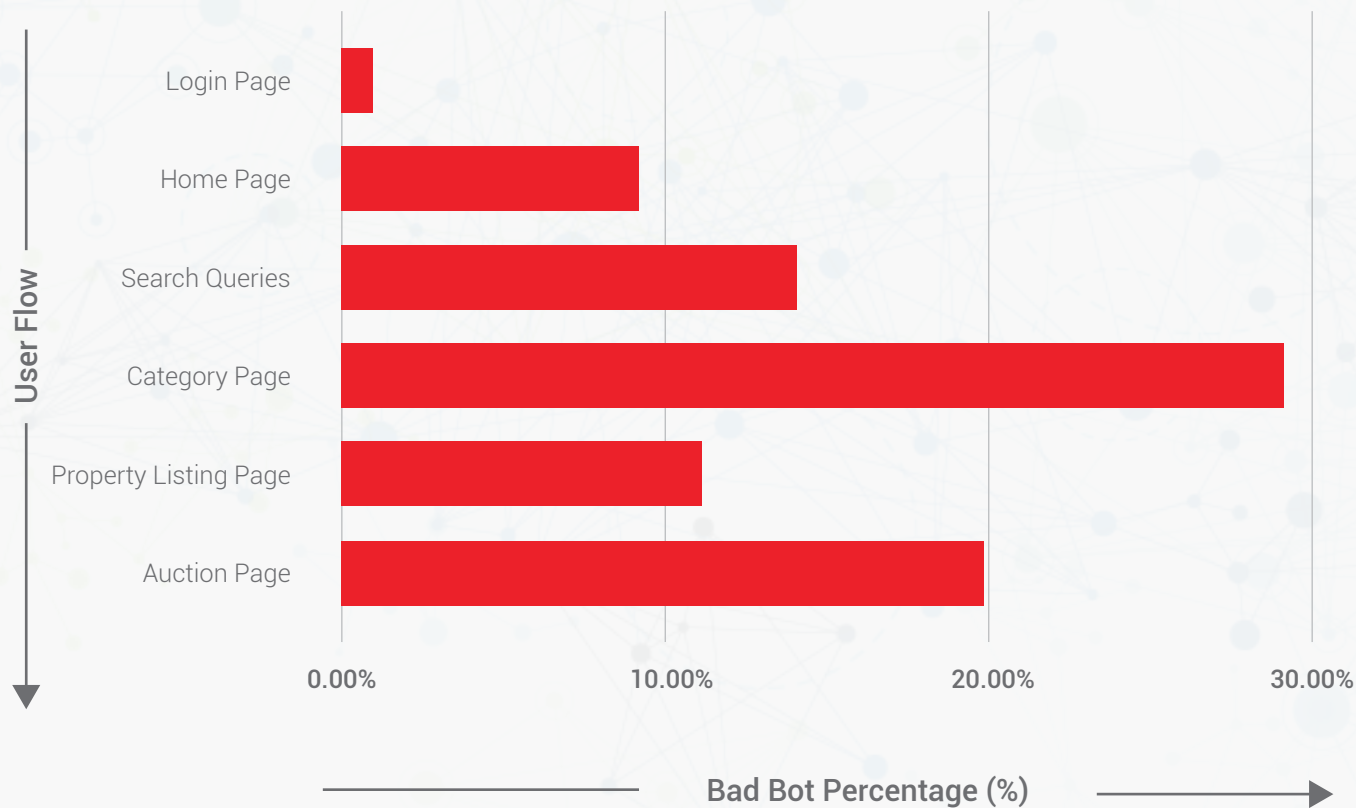
Scraping of classified ad listings

Fake leads, spam entries and comments led to poor customer experience

Associated symptoms

- ▶ Higher than normal browsing activity on new and popular ad listings
- ▶ Presence of identical listings on other ad portals and search engine results
- ▶ Increase in the rejection rate of user-generated content by moderation processes
- ▶ Higher rate of complaints from advertisers about spam leads
- ▶ High incidence of fraudulent keywords and spammy hyperlinks in user-generated content

Trend Of Automated Traffic On Pages Across Real Estate Portals



Business Problems

- ▶ Unique property listings were being scraped by automated techniques soon after being posted
- ▶ Bots were carrying out 'Auction Sniping' - Bidding at the last moment to affect the outcome
- ▶ Fake leads & Spam listings

Real Estate Portals

Business problem

Unique property listings were being scraped by automated techniques soon after being posted

Bots were carrying out 'auction sniping' – bidding at the last moment to affect the outcome

Fake leads & spam listings

Associated symptoms

- ▶ Unusually high requests for new and/or desirable listings soon after being published
- ▶ Presence of identical listings from multiple sources in search engine results
- ▶ Decline in search engine rankings
- ▶ Competitors with identical or similar products and services

- ▶ Complaints from large numbers of users who are unable to bid
- ▶ Certain users with a suspiciously high success rate on their bids

- ▶ Advertisers complaining about fake leads and invalid contact details
- ▶ High hyperlink density with spammy and keyword-laden listings
- ▶ Requests from source IP addresses, devices, and fingerprints that appear on spam lists

Recommendations

- ▶ Enterprises must step up to confront the business challenges posed by sophisticated bots that mimic human behavior to evade detection by conventional security measures.
- ▶ Telltale symptoms of bot attacks (such as the ones listed in this report) are the 'canaries in the coalmine' that provide operators of websites and applications with the first indications of automated attacks.
- ▶ Conventional Web Application Firewalls, IP blacklists, and rate-limiting systems are incapable of detecting – leave alone blocking – today's advanced bots. Enterprises experiencing symptoms of bot attacks should look for solutions that help them uncover the intent behind automated attacks. Identifying intent helps in managing bot traffic and developing specialized tactics to handle different types of bots, i.e., good, bad, and partner bots.
- ▶ The GDPR laws in Europe have hugely added to compliance requirements, and securing users' personal data has never been more vital. However, sophisticated bots can exploit a range of technical vulnerabilities to access personal data – [as we outlined in our Special Report](#). A dedicated bot mitigation solution is crucial in preventing data breaches that could lead to litigation, penalties, and loss of trust and brand value.

For more information on how Radware Bot Manager's real-time anti-bot solution can secure your business, reach out to us at botmanager_info@radware.com.

About Radware

Radware® (NASDAQ: RDWR), a leading provider of cyber security and application delivery solutions, [acquired ShieldSquare](#) in March 2019. ShieldSquare is now Radware Bot Manager.

[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.

www.radware.com

www.shieldsquare.com



Disclaimer

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services or processes described herein are subject to change without notice.

© 2021 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this document 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.