OKLAHOMA CHRISTIAN UNIVERSITY

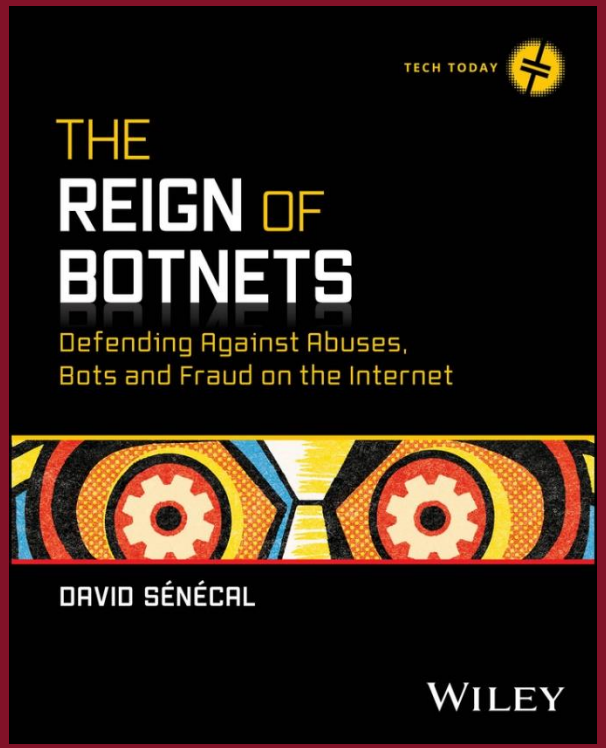
19TH ANNUAL AFCEA OKC CYBERSECURITY & TECHNOLOGY FORUM

DETECTION STRATEGIES AND DEFENDING AGAINST BOTS ON THE INTERNET:

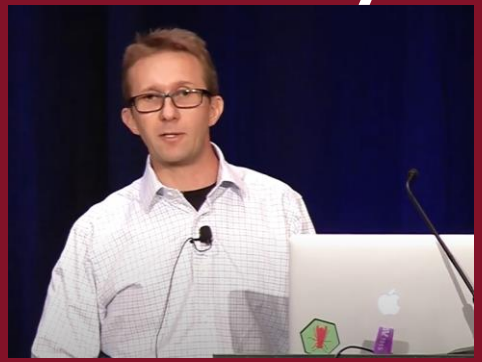
A REVIEW OF LESSONS LEARNED FROM DAVID SENECAL, "THE REIGN OF BOTNETS"

CENTER FOR CYBERSECURITY
OKLAHOMA CHRISTIAN UNIVERSITY
National Center of Academic Excellence in Cyber Defense

Curtis Coleman
Associate Professor, Director
National Cybersecurity Education Center
Email: Curtis.Coleman@oc.edu
Phone: (405) 425-5472



Senecal, David. (2024). *The Reign of Botnets: Defending Against Abuses, Bots and Fraud on the Internet.* Wiley & Sons, Inc.



David Senecal, Principal Product Architect, Akamai Technologies, OWASP AppSec USA, 2018

AGENDA

What are botnets?

How are botnets used for good?

The most common attacks using botnets

Drill-down specific bot attack:

- Account Takeover
- Web Scraping

Developing a Defense Strategy

HOW ARE BOTNETS USED FOR GOOD?

- The term "botnet" is a combination of the words "robot" and "network"
- Bots can be used for many beneficial purposes across various industries and applications. Here are some of the main ways bots are used for good:

1. Customer Service Chatbots

- Provide 24/7 customer support and answer common questions
- Guide users through processes and troubleshooting
- Improve response times and customer satisfaction

2. Search Engine Bots

- Crawl and index web pages to improve search results
- Help websites get discovered and ranked in search engines

3. Social Media Bots

- Automate posting and engagement on social platforms
- Provide automated customer service on social channels
- Monitor brand mentions and sentiment

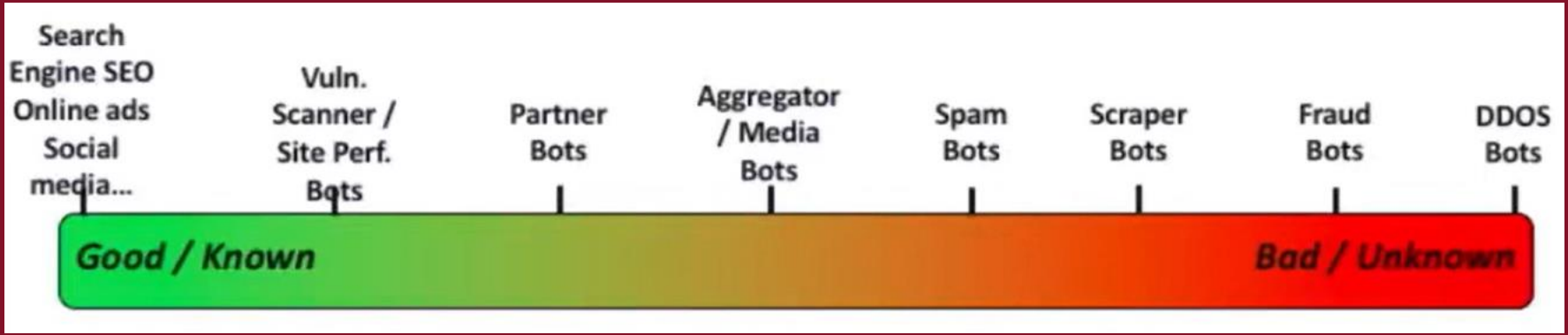
WHAT IS A MALICIOUS BOTNET?

- A malicious botnet is a network of compromised computers and devices that are under the control of a single attacking party, known as the "bot-herder"
- **3 Key Characteristics:**
  1. **Infected Devices:** Botnets are created by infecting computers and IoT devices with malware, turning them into "bots" or "zombie computers“
  2. **Remote Control:** The bot-herder can remotely command the infected devices to perform coordinated actions
  3. **Scale:** Botnets can comprise thousands or even millions of infected machines

Botnets are often used for malicious purposes. The most common bot attacks on the Internet include:

- **Distributed Denial-of-Service (DDoS) Attacks:** Overwhelming target systems with traffic.
- **Spam Campaigns:** Sending large volumes of unsolicited emails.
- **Data Theft:** Stealing sensitive information from infected devices.
- **Financial Fraud:** Directly stealing funds or credit card information.
- **Cryptocurrency Mining:** Using infected devices' processing power for mining.

THE SCALE OF BOTS



Source: OWASP

Account Takeover

A Deeper Dive

Account Takeover (ATO)

- Account takeover is such a problem that it ranked seventh in the OWASP top 10 security vulnerability as “Identification and authentication failure”

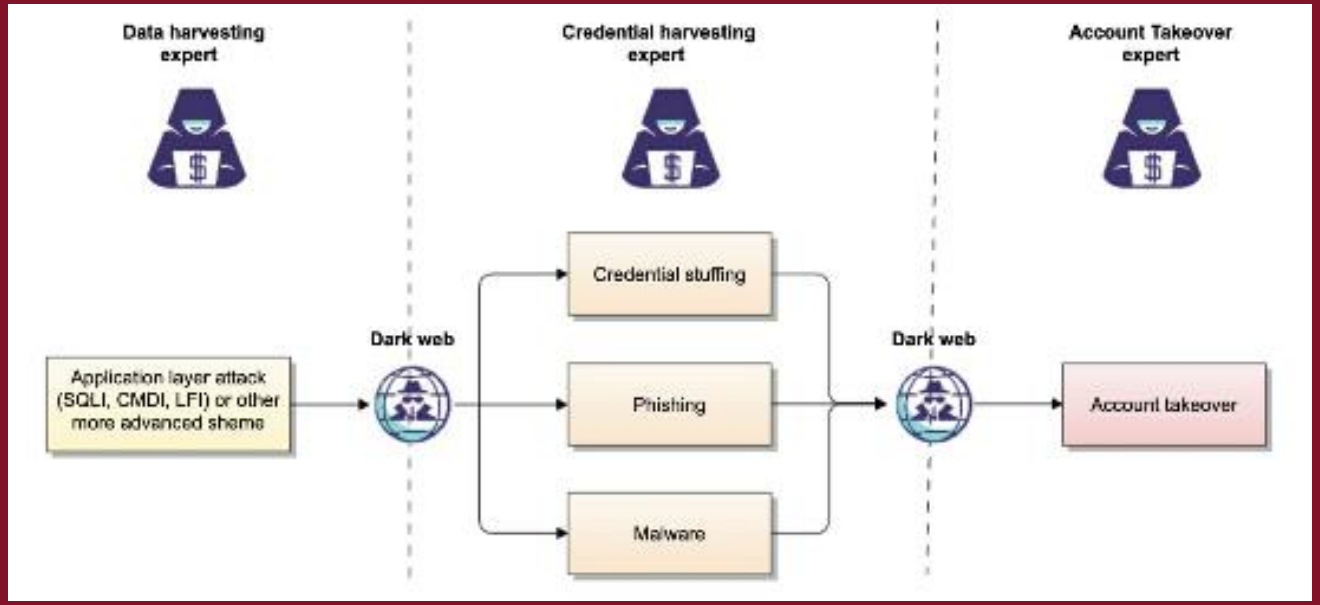


Figure 1.1 The three steps of account takeover

Senecal, David. The Reign of Botnets: Defending Against Abuses, Bots and Fraud on the Internet (p. 22). Wiley.

- In September 2019, Norton, a security company famous for its antivirus and anti-malware software, revealed the compromise of 172 million accounts on the gaming platform Zynga. The stolen data included usernames, email addresses, and hashed passwords.
- In April 2020, Forbes revealed that Zoom, a major online collaboration and video conferencing platform that helped the corporate world continue to function during the pandemic, had 500 million of its user credentials for sale on the dark web.
- These breaches fuel the combo and personal data lists found on various marketplaces on the dark web.
- These lists are continuously used to carry out credential stuffing, phishing, and malware attacks against multiple websites on the Internet.
- In March 2024, Troy Hunt's site, Have I Been Pwned, reported nearly 13 billion breached accounts from more than 600 websites.

- Assuming an average-quality combo list with 1 million credentials, the following table summarizes the estimated number of credentials harvested from the credential stuffing attack based on the expected hit rate per industry.
- A botnet is the most efficient way to validate thousands of credentials quickly.

Industry	Estimated Hit Rate	Estimated Credentials Harvested
E-commerce, social media	15%	150,000
Fintech/banking	10%	100,000
Gaming—bulk accounts	5%	50,000
Gaming—premium accounts	0.0075%	75

Senecal, David. The Reign of Botnets: Defending Against Abuses, Bots and Fraud on the Internet (p. 28). Wiley.

HOW DIFFICULT IS CREDENTIAL STUFFING?

- With tools like Sentry MBA, the barrier to gain access to a botnet is relatively low.
- Support, online tutorials, and a large community of users are also available to help get the most novice attacker up and running in no time.
- All the attacker must do is point the tool to the list of credentials to validate, the URL of the targeted website and, optionally, a list of proxy IP addresses to load balance the traffic and avoid detection.
- Once the setup is completed, what remains is to start the attack and return a few hours later to review the list of credentials that have been successfully validated.
- Fraudsters may be able to get a higher price for accounts that have a credit card, gift card, or loyalty points from a reward program attached to them

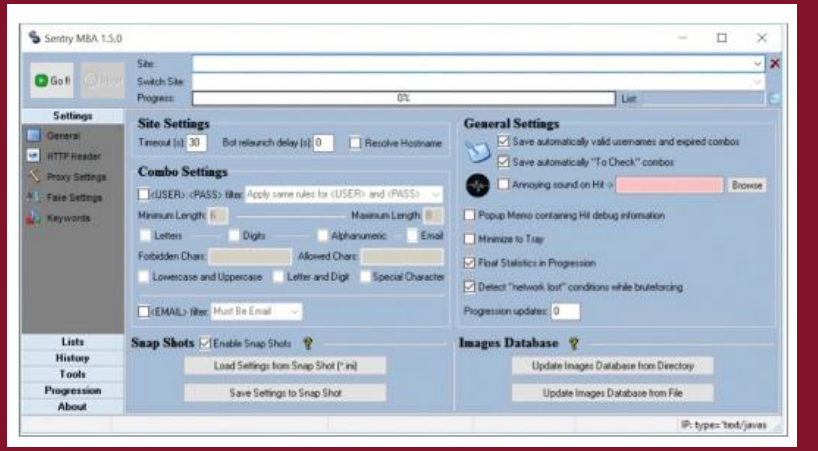


Figure 1.2 The Sentry MBA user interface

Senecal, David. The Reign of Botnets: Defending Against Abuses, Bots and Fraud on the Internet (p. 29). Wiley.

- Credential harvesting can yield several thousands of credentials per site.
- Once enough are collected, they are sold on the dark web marketplace.
- The following table breaks down potential revenue from selling stolen credentials by industry.

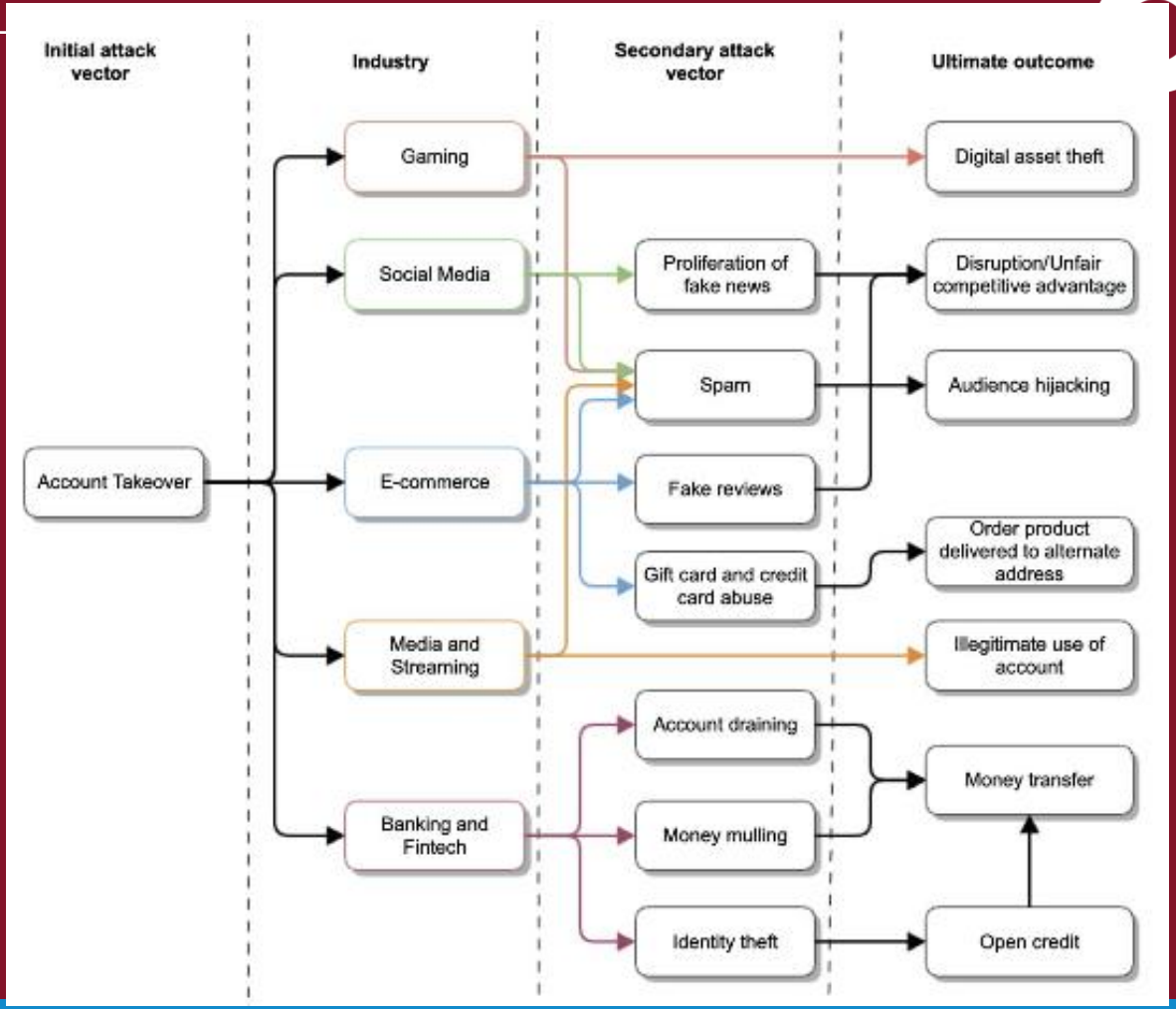
Industry	Average Revenue/ Credential	Potential Revenue per 100,000 Sold
E-commerce	$0.08	$8,000
Social media	$0.10	$10,000
Fintech/bank	$0.40	$40,000
Gaming (bulk)	$1.70	$170,000

Figure 1.3 Dark Web Prices of Credentials

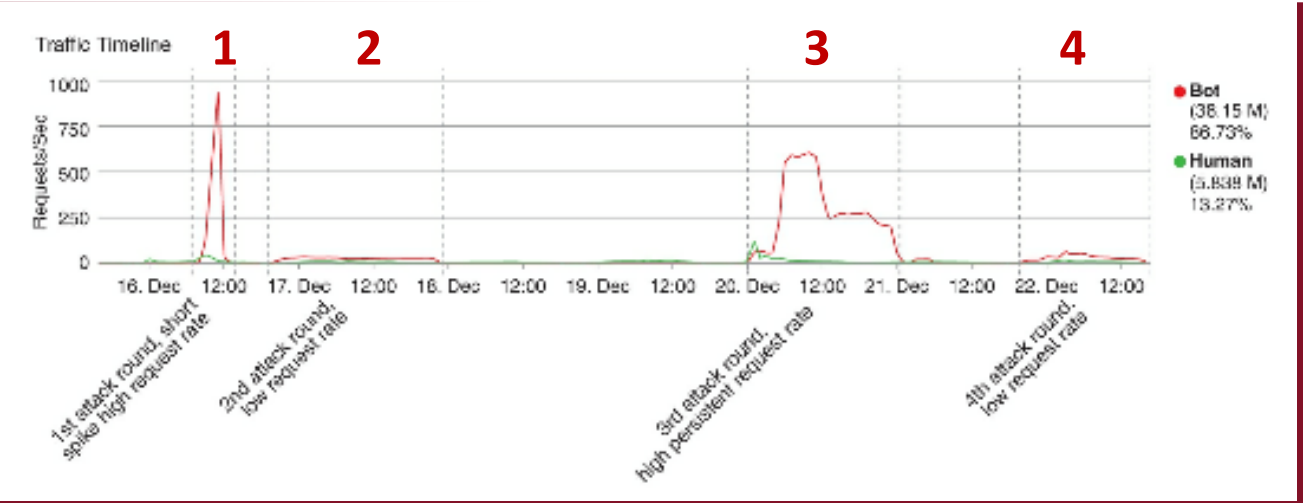
Senecal, David. The Reign of Botnets: Defending Against Abuses, Bots and Fraud on the Internet (p. 31). Wiley.

Figure 1.4 The impact of account takeover by industry

Senecal, David. The Reign of Botnets: Defending Against Abuses, Bots and Fraud on the Internet (p. 32). Wiley.



A CREDENTIAL STUFFING ATTACK EXAMPLE



1. A sustained high request rate of almost 1,000 requests per second on December 16. The attack lasted only three hours, and more than 5.8 million requests were blocked.
2. The second round of attack starts 8 hours later. It is much lower in intensity, between 30 and 40 requests per second - More than 2.8 million requests were denied.
3. The third attack was high intensity for 24 hours, 26 million requests blocked. The fourth attack was low intensity for 20 hours, 4.2 million requests blocked.
4. The total campaign was one-week, a single actor, and over 37 million requests.

- The attack originated from five countries, with the United States leading in terms of volume, followed by Turkey, Germany, the Netherlands, and the United Kingdom
- leveraged a total of 87,723 unique IP addresses distributed in 4,320 networks

Figure 1.6 Attack distribution by country of origin

Senecal, David. The Reign of Botnets: Defending Against Abuses, Bots and Fraud on the Internet (p. 37). Wiley.

Source: Experian - Account Takeover Prevention
https://www.experian.com/business/solutions/fraud-management/account-takeover-fraud

Web Scrapping

A Deeper Dive

- Web scraping is the process of extracting data from websites.
- Information is collected using automated software applications (bots) and structured into a usable form.
- Web scraping is also known as *data scraping*, *data extraction*, *data crawling*, *web crawling*, *web harvesting*, or *screen scraping*.
- When the data collected are prices or product inventory information, it may also be referred to as *price scraping* and *inventory scraping*, respectively.
- When a botnet scrapes a website, it harvests publicly available information.
- Despite the problems it may cause, there is little that a website owner can do legally to prevent the activity.

Web Scrapping can be used for good or bad

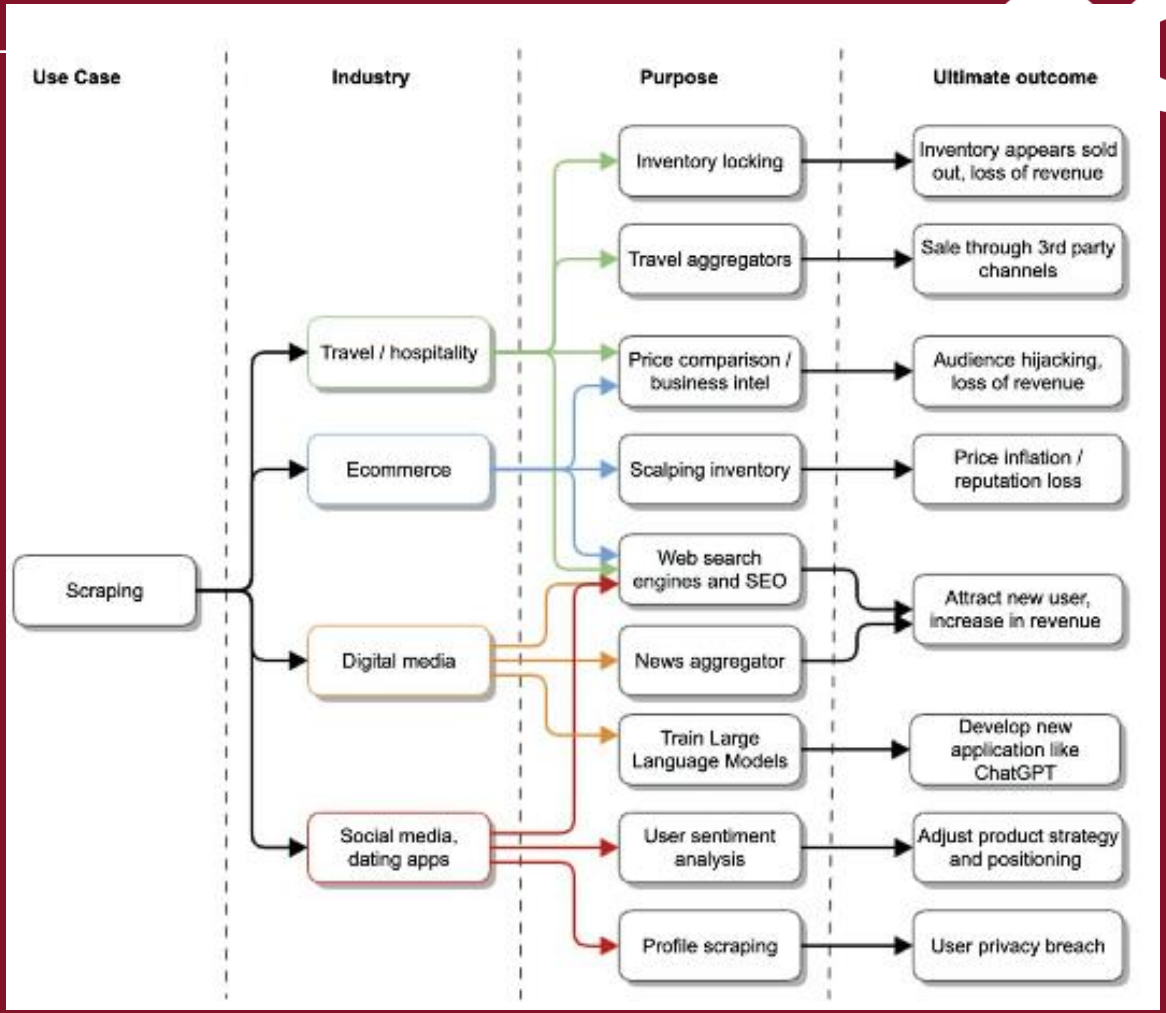


Figure 1.7 The outcome of scraping activity by industry

Senecal, David. The Reign of Botnets: Defending Against Abuses, Bots and Fraud on the Internet (p. 50). Wiley.

WEB SCRAPPING CONSEQUENCES

1. Finding a targeted product
2. Data collected and analyzed
3. Targeted product is bought from the best sale site
4. Product is then placed on an Amazon marketplace at a markup
5. Product is sold to consumer and the Scalper pockets the markup difference

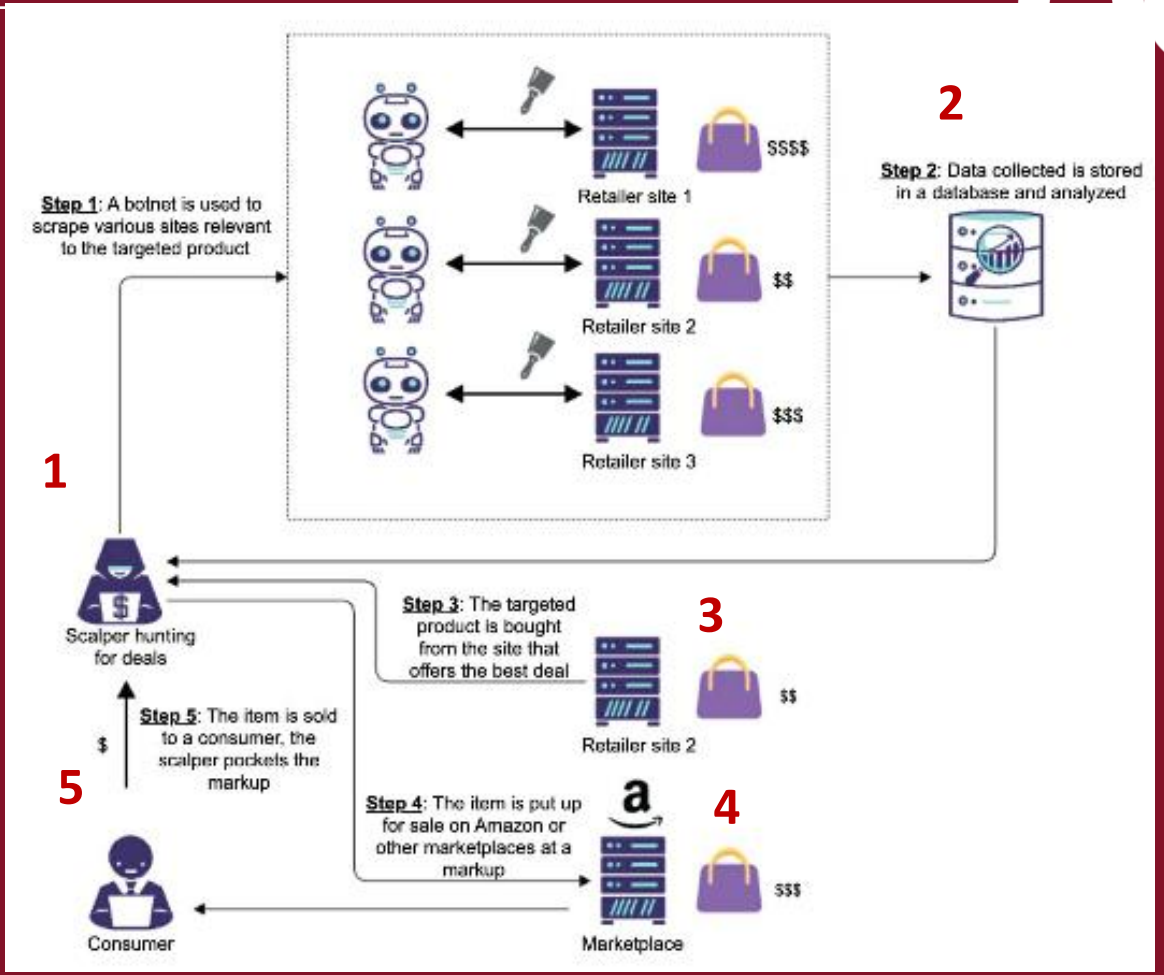


Figure 1.8 Bargain hunting life cycle

Senecal, David. The Reign of Botnets: Defending Against Abuses, Bots and Fraud on the Internet (p. 54). Wiley.

1. Scalper competes with consumers to get limited-edition product
2. Scalper places their product on ebay with markup
3. Consumer is eager to get the limited-edition product and buys it at the markup premium from the Scalper

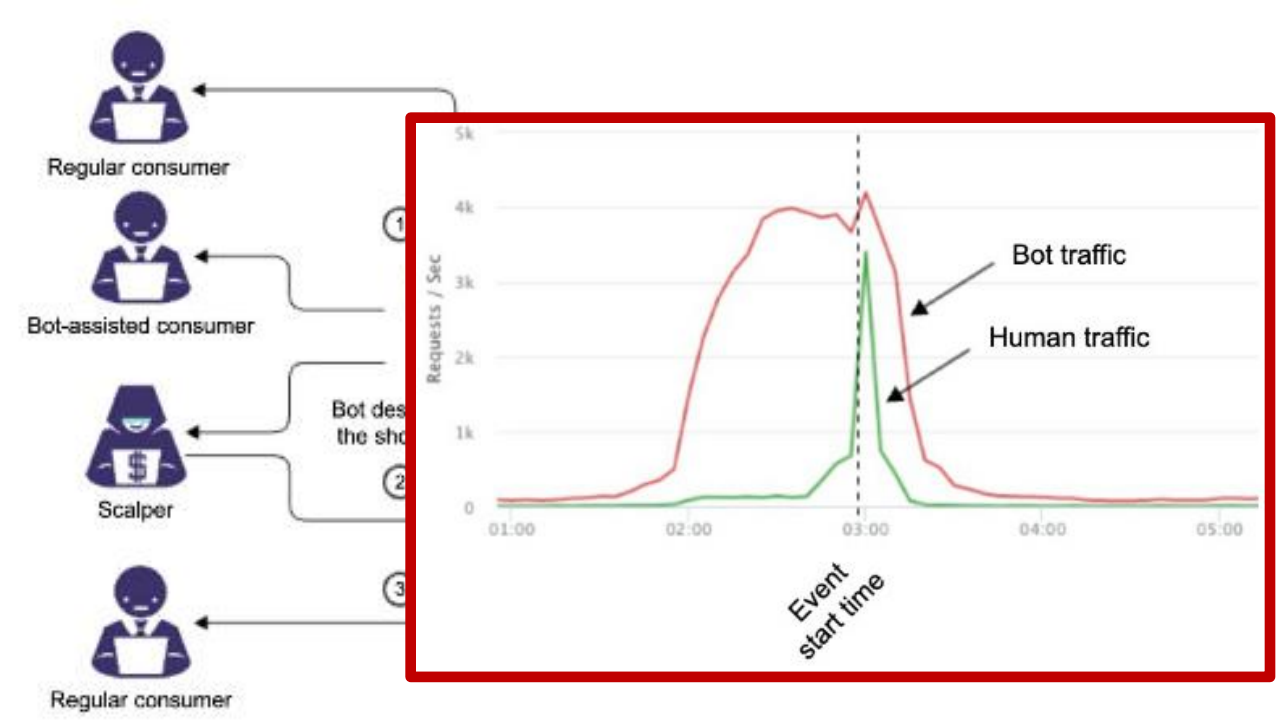


Figure 1.10 Scalping

Senecal, David. The Reign of Botnets: Defending Against Abuses, Bots and Fraud on the Internet (p. 59). Wiley.

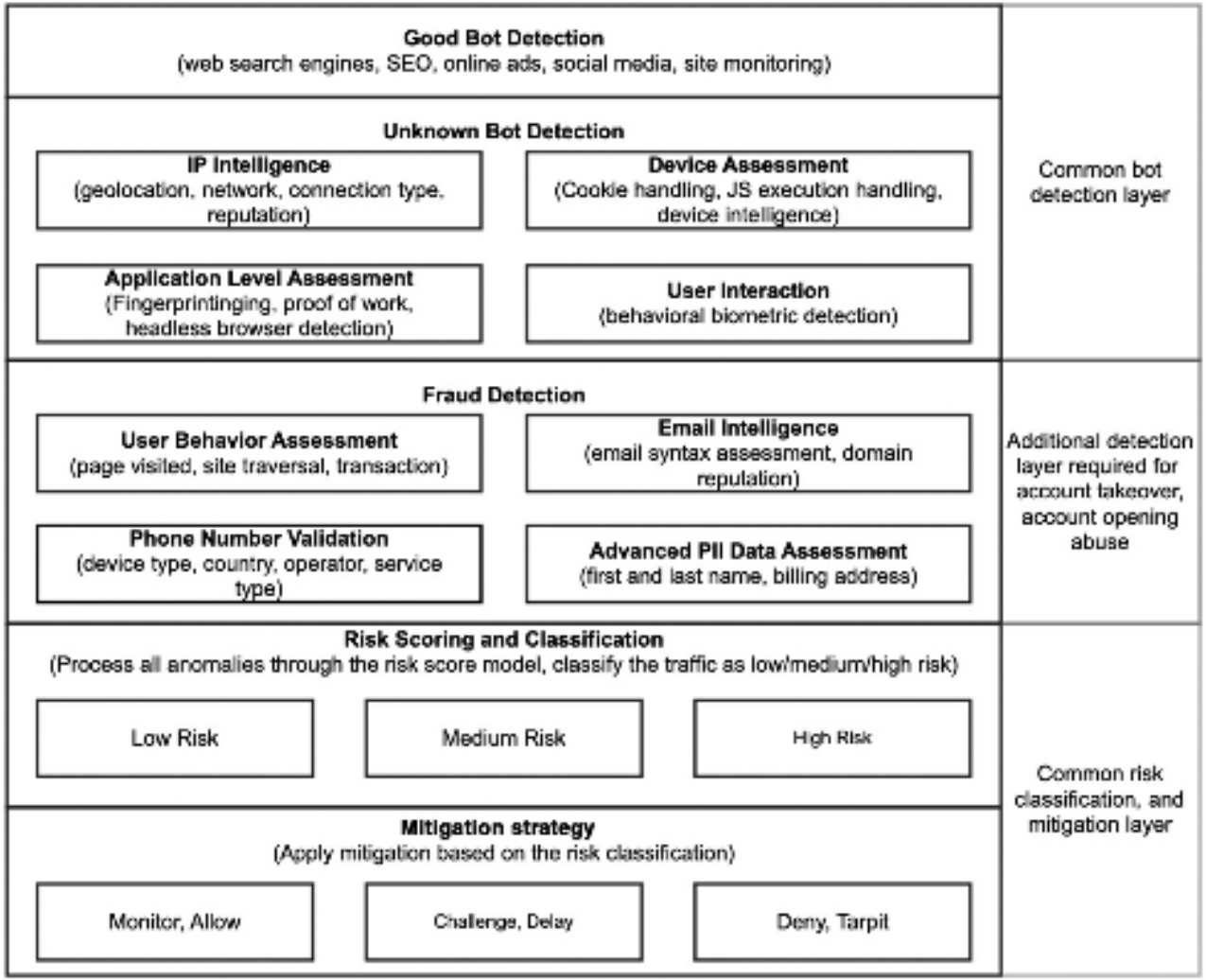
Developing a Defense Strategy

- Define your defense strategy: a good detection and mitigation strategy with strong operational procedures includes:
  1. explain what is to be protected,
  2. for what purpose, and
  3. how often the bot activity and setup should be assessed
- The strength of the defense strategy and the discipline of the web security team executing it is key to success.
- This is not a race. This is a marathon, so be prepared to consistently follow the defense strategy in the long run.

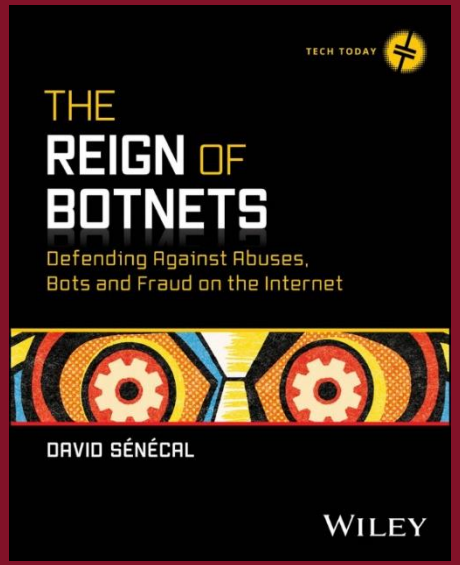
- You should realize that successfully managing bots and preventing fraud is not an easy proposition.
- You need to expect all sorts of botnets with various levels of sophistication to hit the critical workflows of your website.
- Security teams tend to focus on simple detection methods based on anomalies found in the HTTP request headers, which are visible to all web servers, without implementing any complex JavaScript-based data collection.
- This leads to developing detection methods or rules tailored to the moment's threat – creating a blind spot to future bot changes.
- Sometimes, adversaries only need to change a value in the HTTP headers or send requests from different locations or IP addresses to defeat the defense strategy.

Figure 1.11 Bot and fraud management component architecture

Senecal, David. The Reign of Botnets: Defending Against Abuses, Bots and Fraud on the Internet (p. 186). Wiley.



PURCHASE A BOT MANAGEMENT SY



OKLAHOMA CITY CHAPTER AFCEA

19TH ANNUAL AFCEA OKC CYBERSECURITY & TECHNOLOGY FORUM

OC

I highly recommend this book!

QUESTIONS?

NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA

OC CENTER FOR CYBERSECURITY OKLAHOMA CHRISTIAN UNIVERSITY

U.S. DEPARTMENT OF HOMELAND SECURITY

National Center of Academic Excellence in Cyber Defense

Curtis Coleman, CISSP, CISM
Associate Professor, Director
National Cybersecurity Education Center
(405) 425-5472
Curtis.Coleman@oc.edu