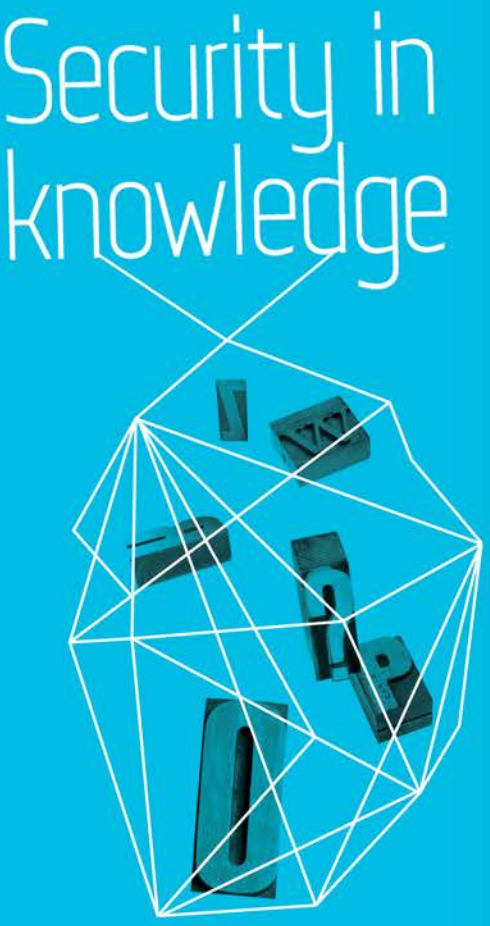
CUSTOMERS & CRIMINALS: USE WEB SESSION INTELLIGENCE TO DETECT 'WHO IS WHO' ONLINE



Jason Sloderbeck
Silver Tail Systems, Part of RSA

Session ID: SPO1-W22
Session Classification: General Track

Question

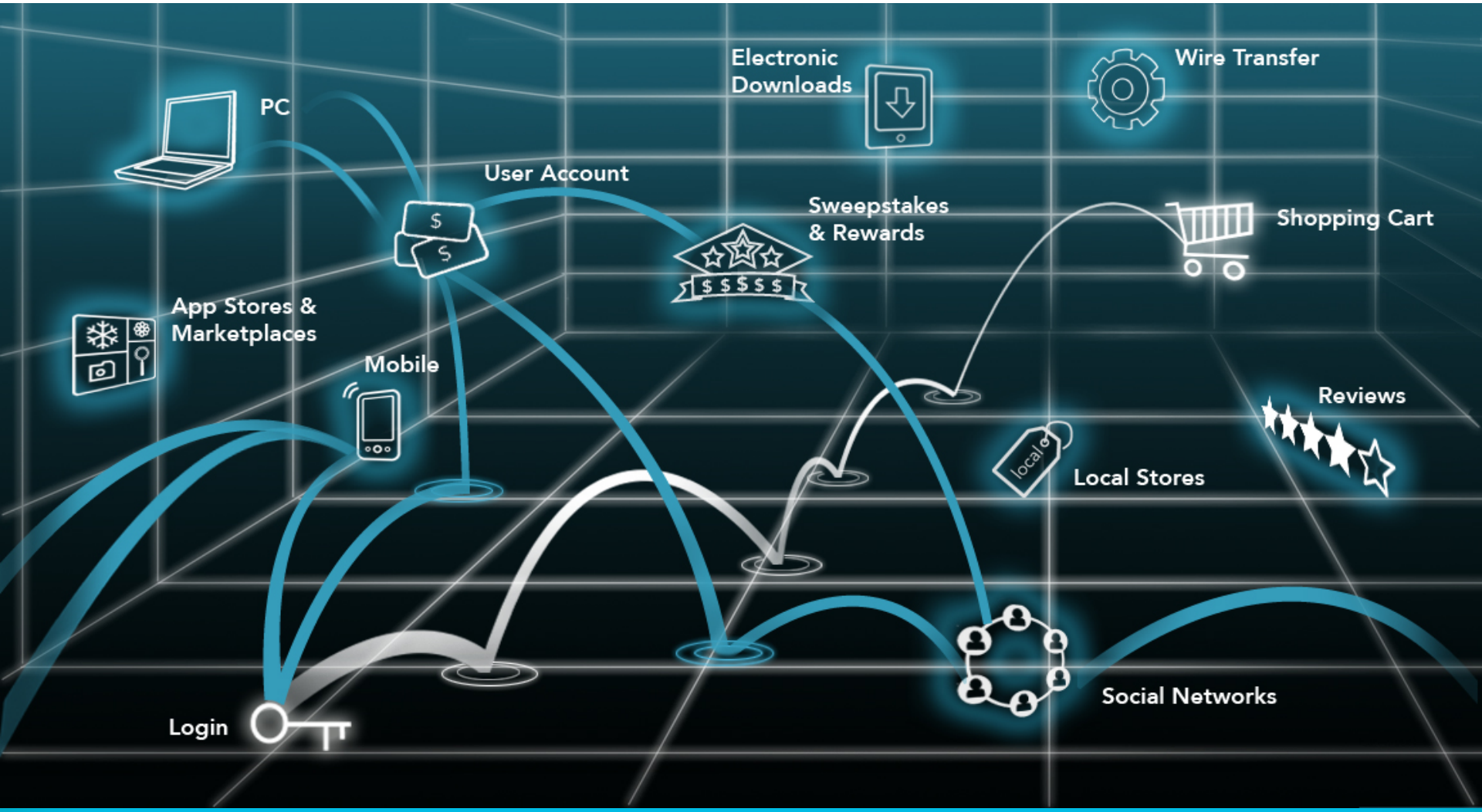
Do criminals in **a retail store** behave differently from typical customers?

Retail Circa 2013

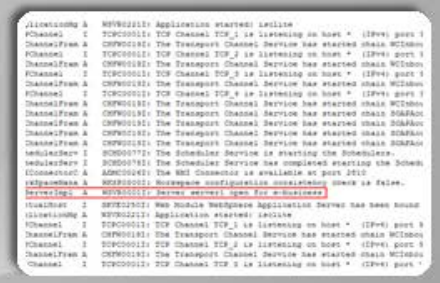
Question

Do criminals on **your web site** behave differently from typical customers?

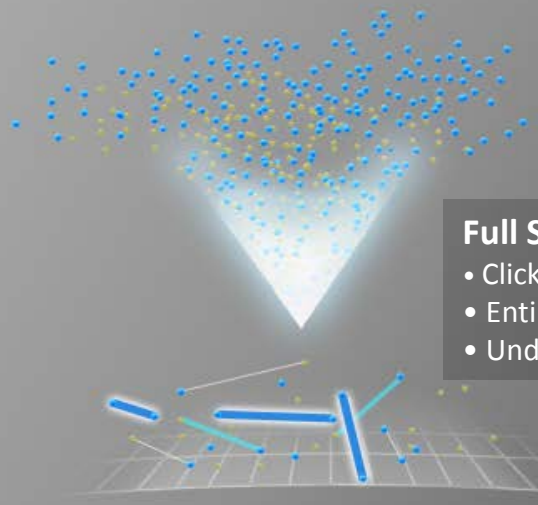
The Web Has Evolved



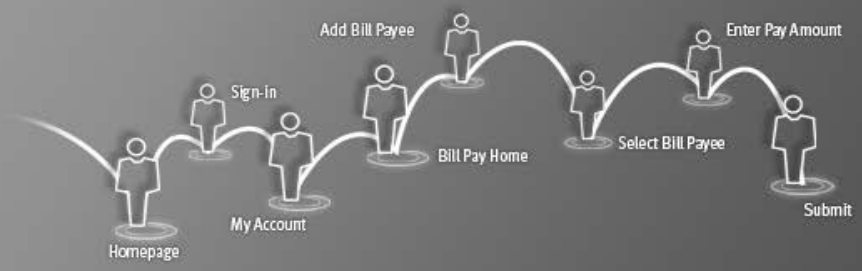
Big Data Meets Web Sessions



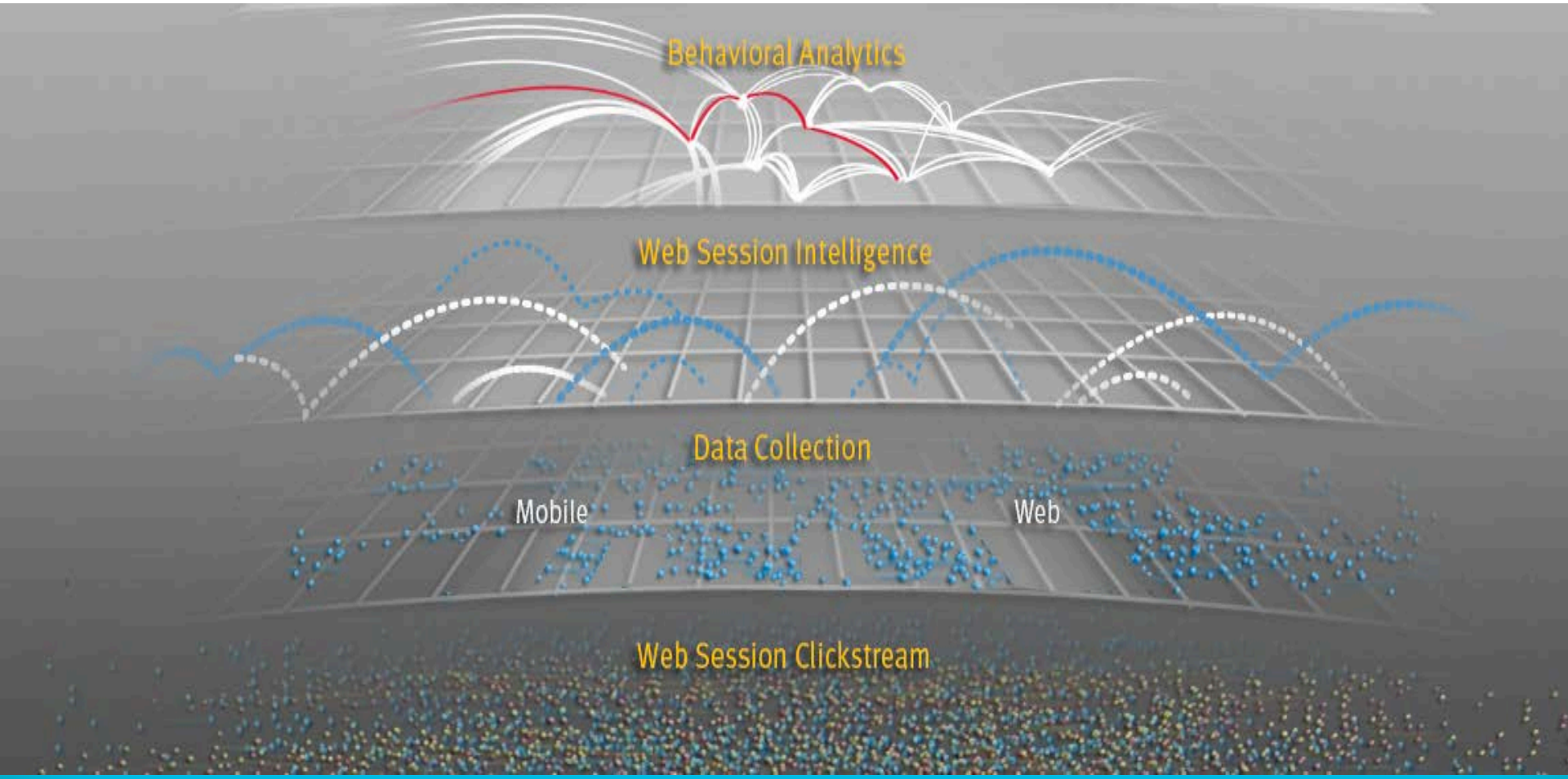
Just Logs
- Limited transaction visibility
- No traceability into behavior
- Disconnected story



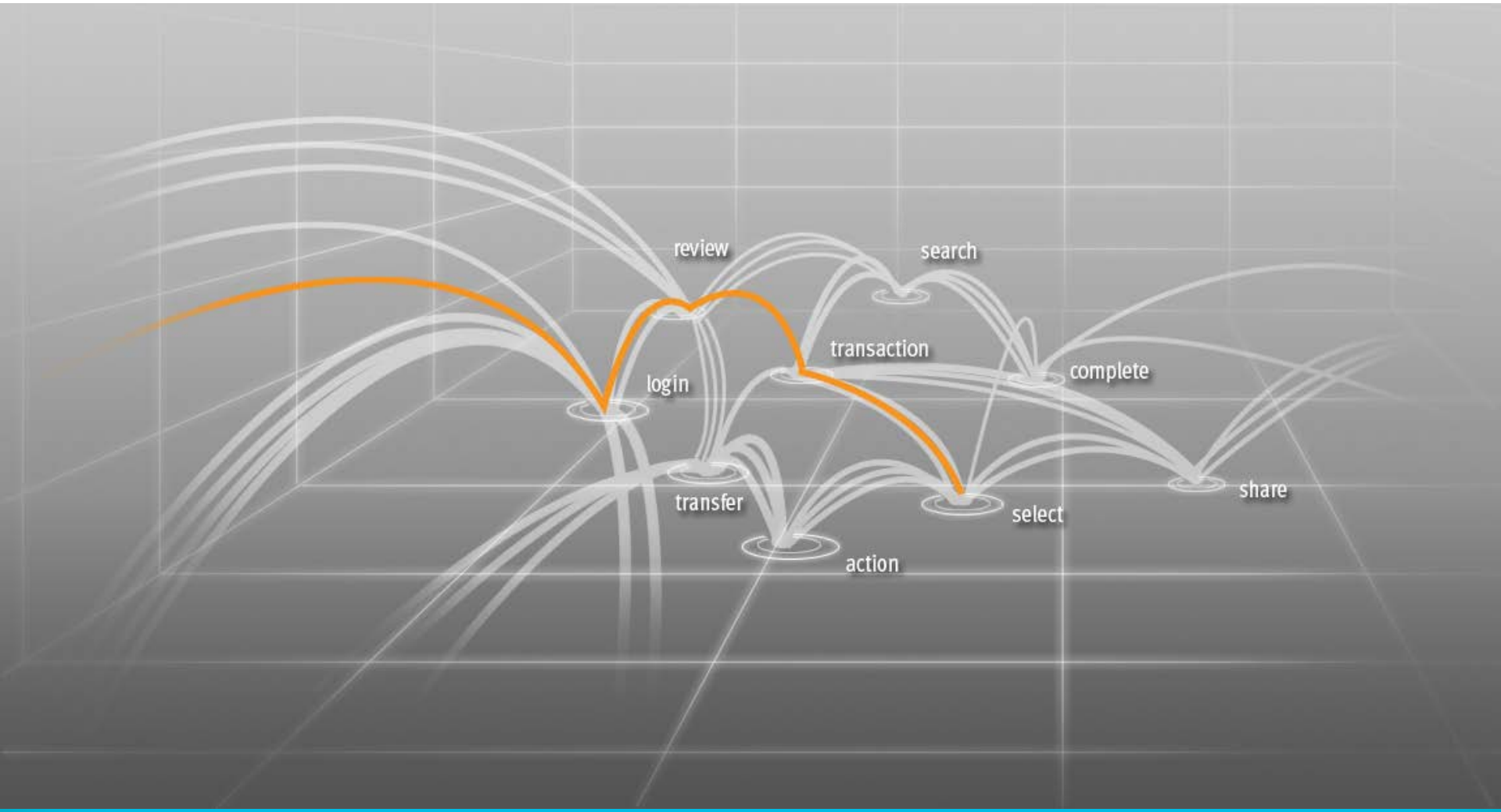
Full Session Data
- Click-by-click visibility
- Entire HTTP request insight
- Understand behavior



Behavioral Analytics



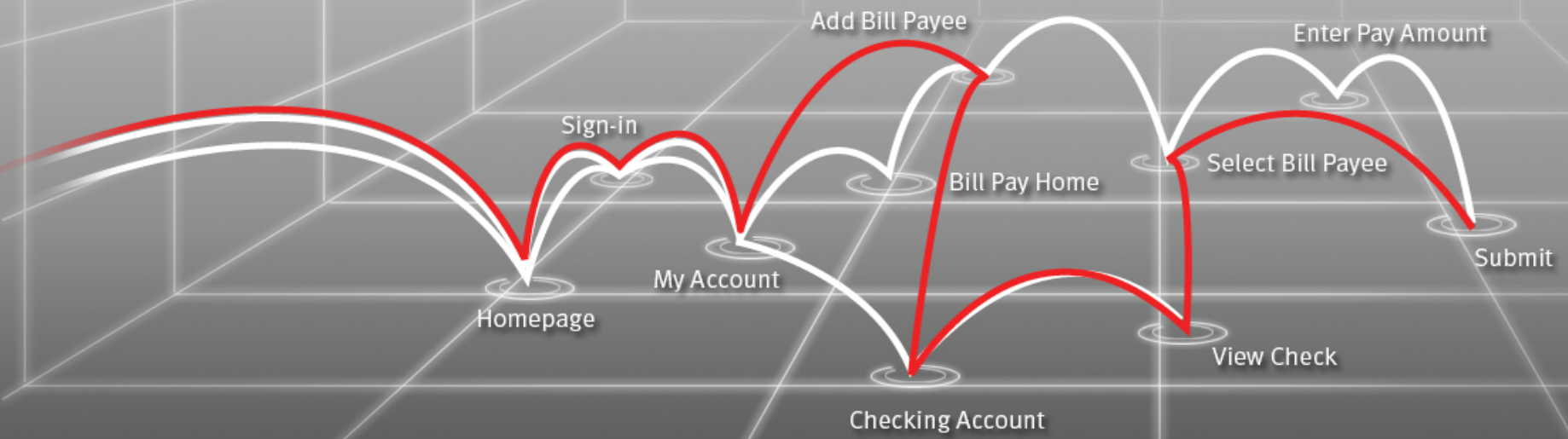
Population-based Behavior



Man-in-the-Browser Attack

Criminals Look Different than Customers

- Velocity
- Page Sequence
- Origin
- Contextual Information



Business Logic Abuse

What is Business Logic Abuse?

- "Business logic abuse results … when a criminal uses the legitimate pages of the website to perpetrate cyber attacks, hacks or fraud."

Source: Ponemon Institute 'The Risk of Business Logic Abuse: U.S. Study' (September 2012)

Scope of Business Logic Abuse

- Site Scraping
- Account Hijacking
- Password Guessing
- Pay-per-click Fraud
- Testing Stolen Credit Cards
- Denial of Service
- eCoupons
- eWallet Abuse
- App Store Abuse
- Mass Registration
- Fraudulent Money Movement
- Vulnerability Probing

Survey of US IT Executives

90%

Report lost revenue due to Business Logic Abuse

64%

No clear visibility into their web session traffic

74%

Can't tell if a web session is a customer or a criminal

1/3

Do not know who is responsible for addressing business logic abuse

Real-world Examples

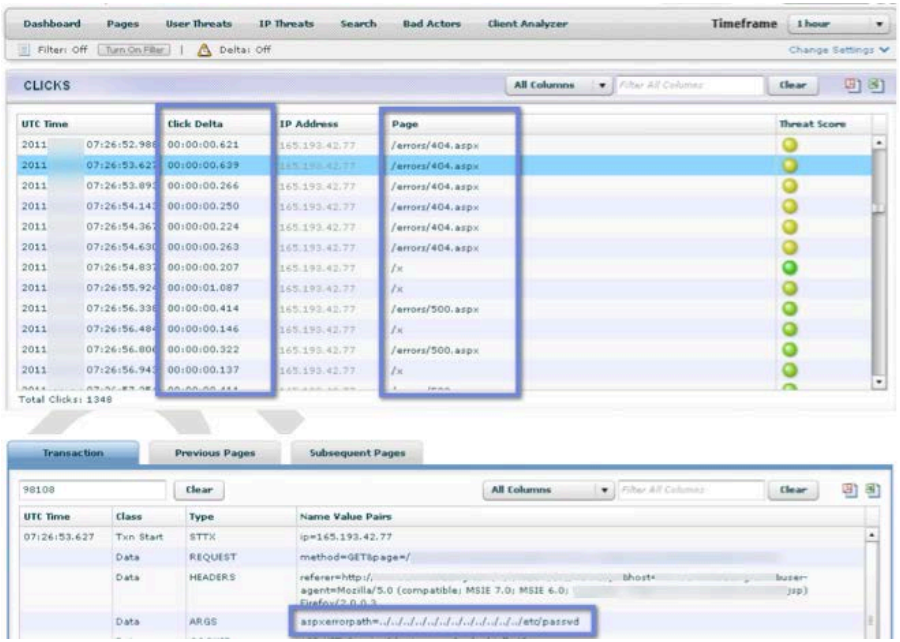
Vulnerability Probing

What were they doing?

- Jiggling doorknobs
- Probing for vulnerabilities
- Site reconnaissance

What looked suspicious?

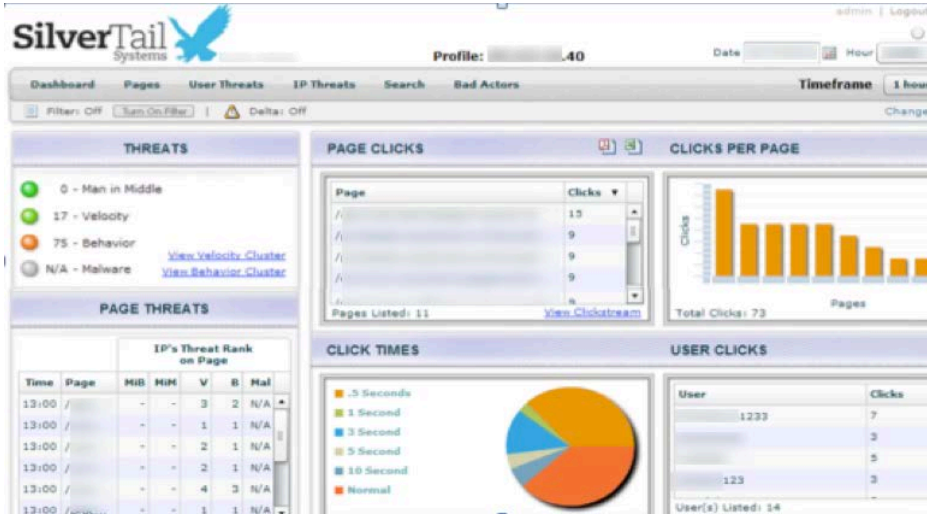
- Sub-second clicks
- Modified user-agent strings
- Alphabetical page requests
- Multiple password reset attempts
- Requests for non-existent pages



Horizontal Password Guessing

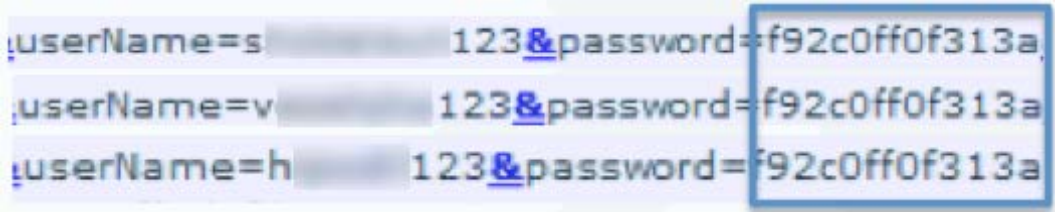
What was happening?

- Testing a common password
  e.g. **Faceb00k!**



What looked suspicious?

- Spike in login page hits
- Multiple login attempts with one password
- Scripted variability
- Elevated behavior scores for sessions driving the spike



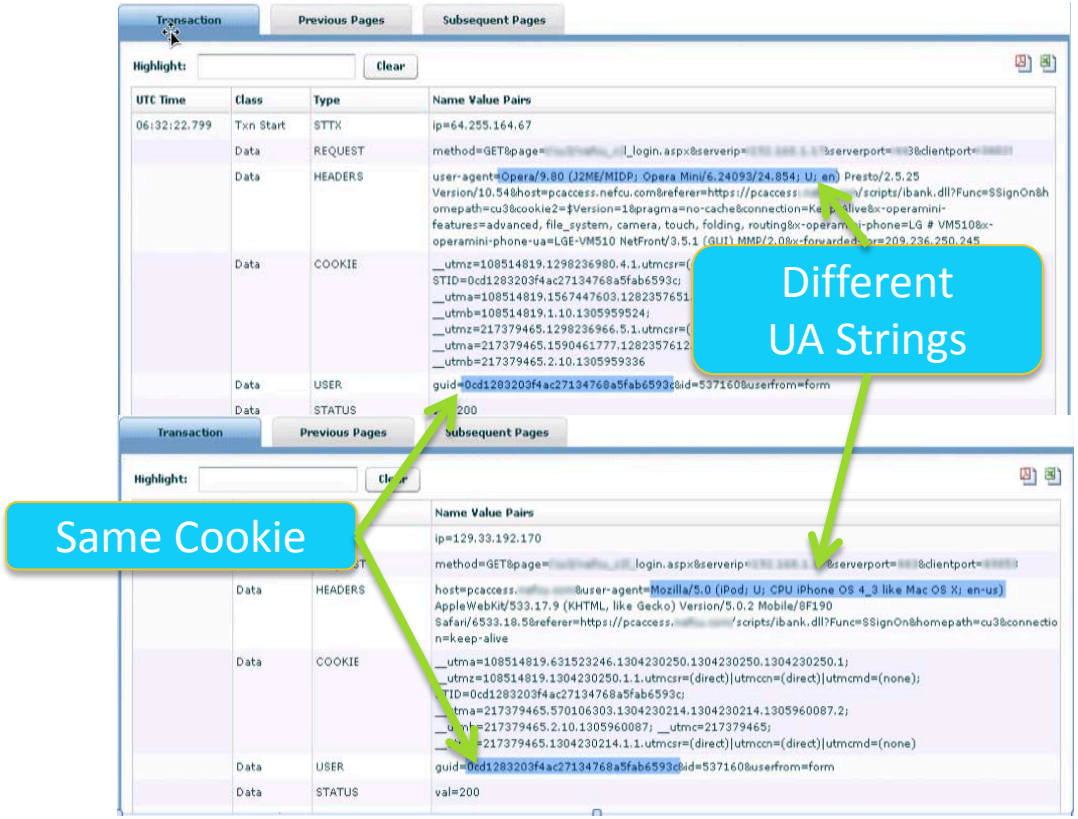
Mobile Account Penetration

What were they doing?

- Stealing credentials on public WiFi from low-security mobile application
- Spoofing mobile user agents

What looked suspicious?

- Cluster of IPs generated a high behavior score
- Clickstream showed the same cookie being used by two devices



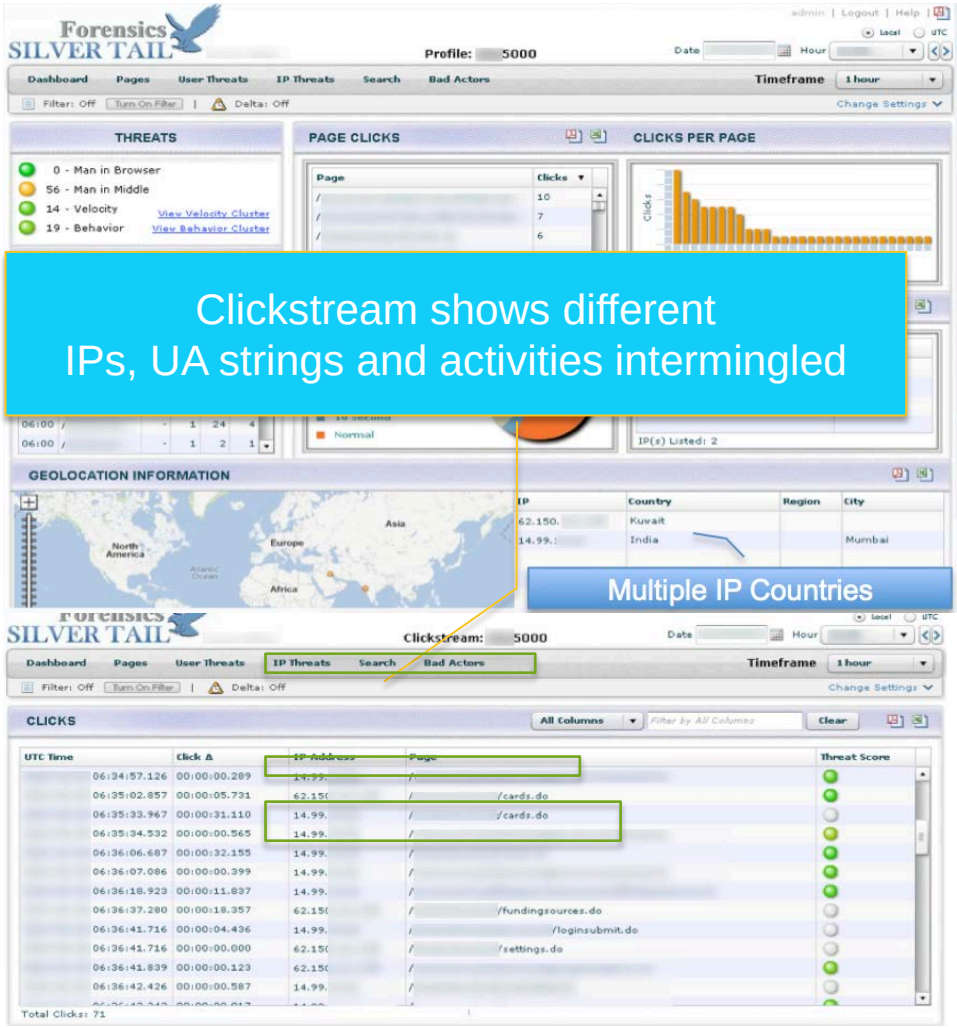
Fraudulent Money Movement

What where they doing?

- Compromising accounts with malware
- Creating a virtual account number (VAN)
- Receiving a new line of credit
- Maxing credit limit with fraudulent purchases

What looked suspicious?

- High Man-in-the-Middle score
- Fast clicks
- Multiple IP addresses in one session
- IPs traced to disparate geographies
- User-agent variation



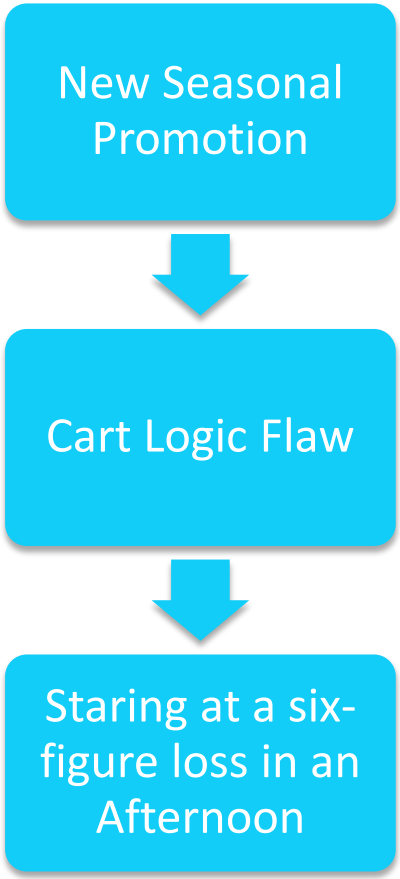
E-Commerce Fraud

The customer knew the "what"…

- Omniture reported revenue drop for affiliate orders

Behavior exposed the "how" in minutes…

- Users added a sale item to their cart
- The sale price persisted in the cart after the sale ended
- Users stacked the next promotion in their cart
- Inconsistent price floors were exploited
- Accepted orders were sub-floor or negative value



Session DDoS

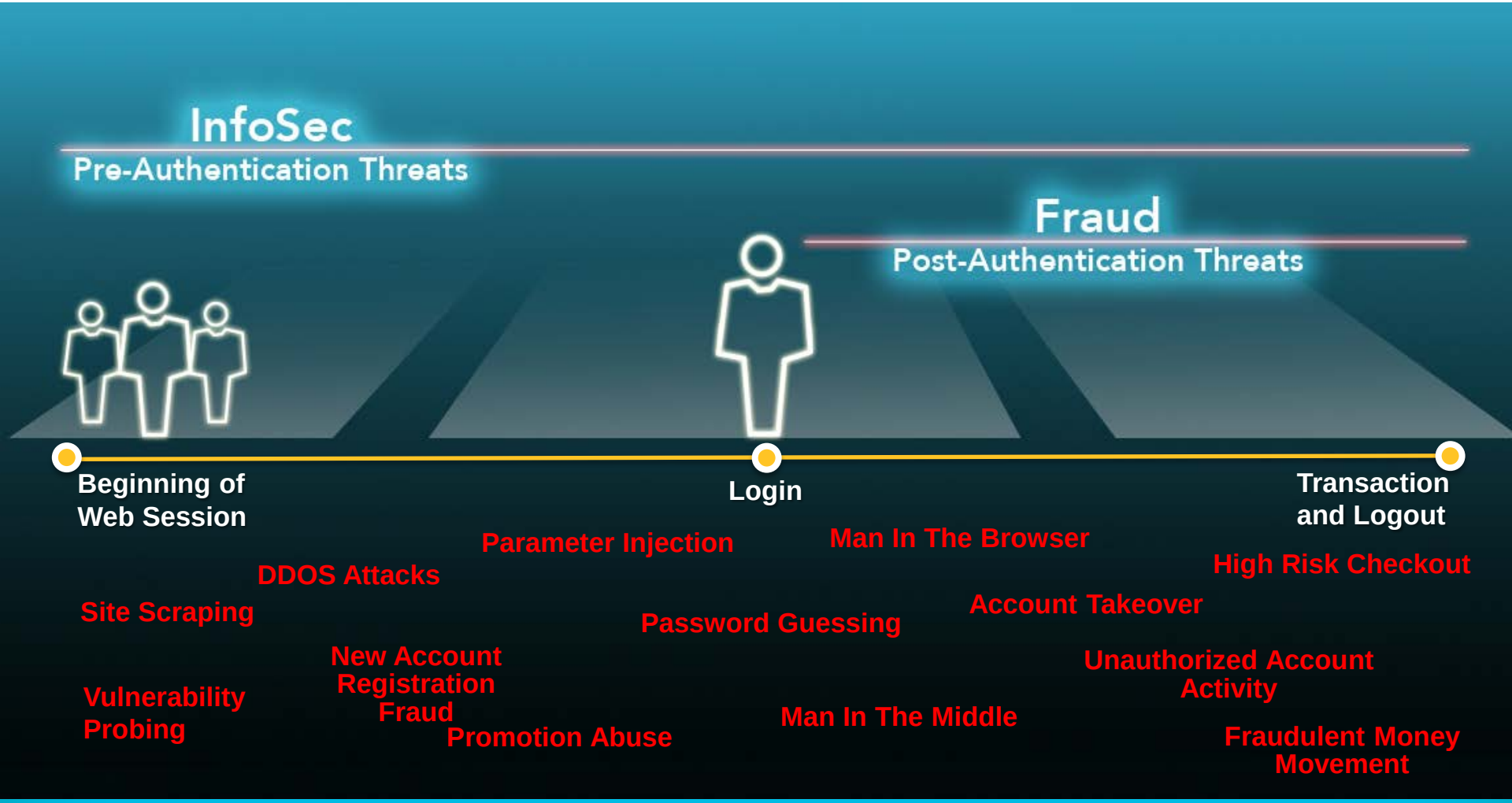
What where they doing?

- Application resource exhaustion
- Botnets sending Search, Login New Account, Purchase queries

What looked suspicious?

- Device ID / User-Agent randomization
- Thousands of IP addresses were acting in concert
- Identical activity on a specific set of pages

Spectrum of Threats



Thank You

jason.sloderbeck@rsa.com

info@silvertailsystems.com