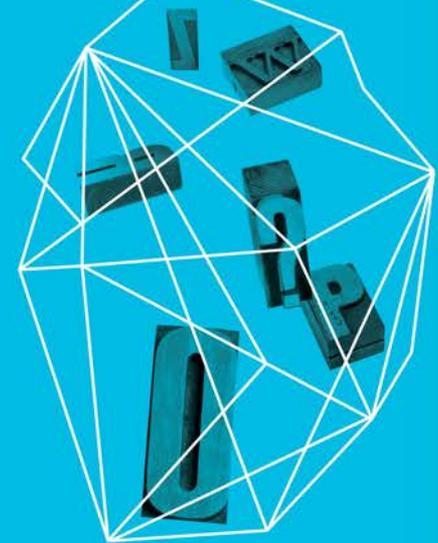


## CUSTOMERS & CRIMINALS: USE WEB SESSION INTELLIGENCE TO DETECT 'WHO IS WHO' ONLINE

Jason Sloderbeck

Silver Tail Systems, Part of RSA

Security in  
knowledge



# — Question

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

# Retail Circa 2013



Security camera-capture events



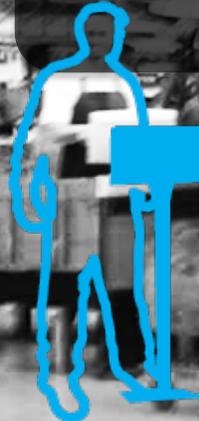
Security Guard – stop shoplifters



Price tag swapper- Mis-representing prices



Cashier – Protect & Ensure sales



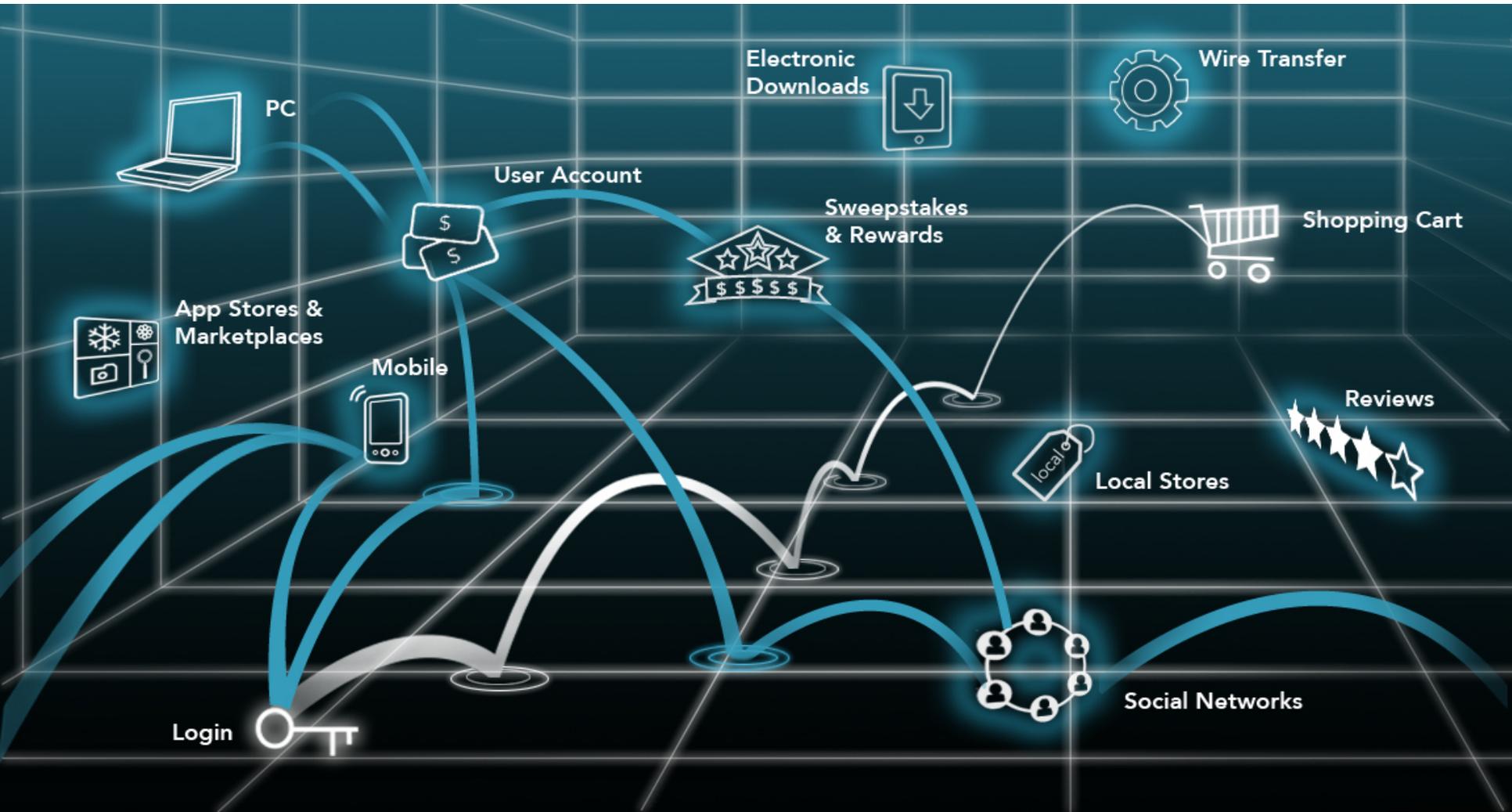
Shoplifter- Taking items



# Question

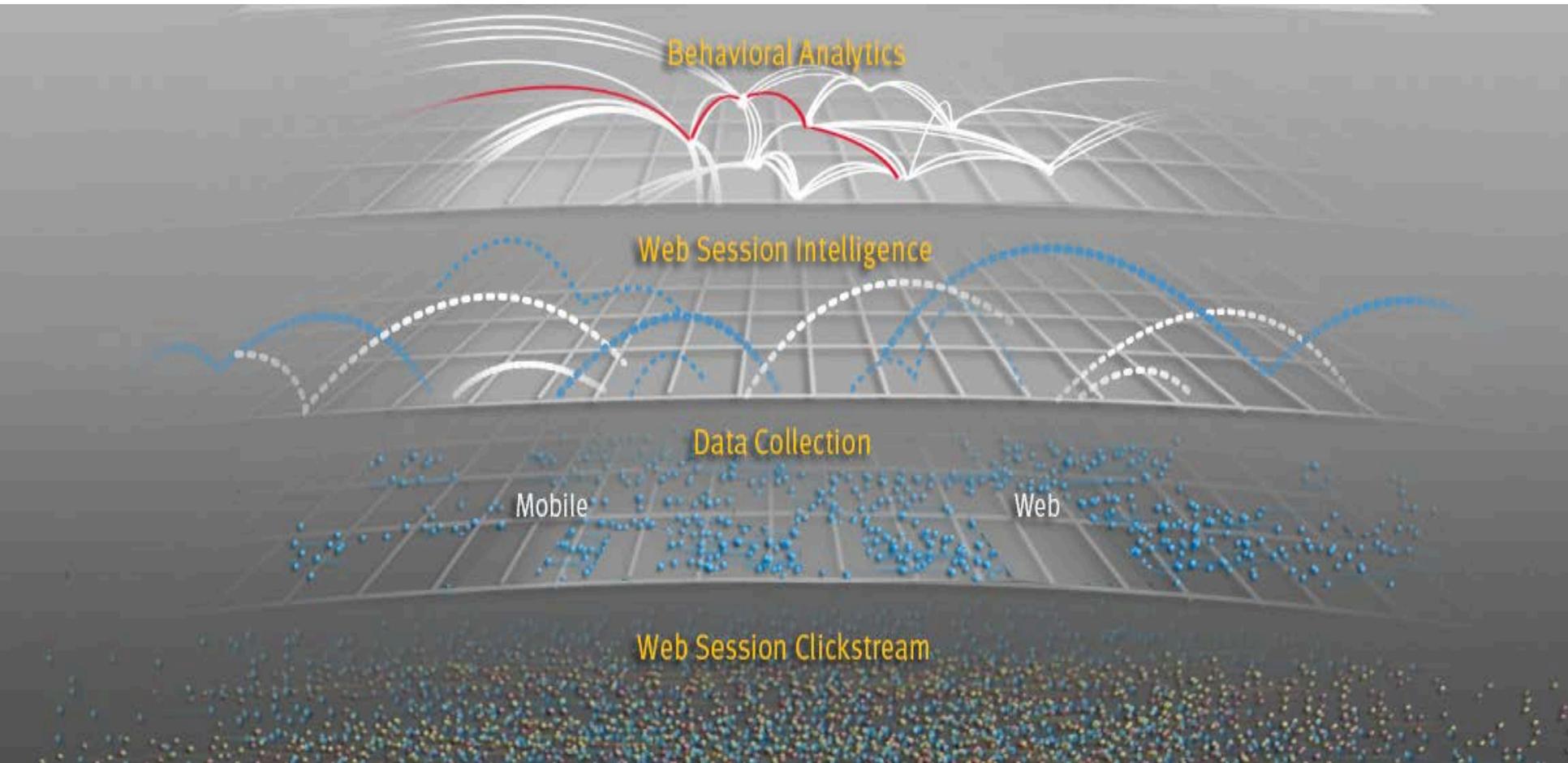
Do criminals on **your web site** behave differently from typical customers?

# The Web Has Evolved





# Behavioral Analytics



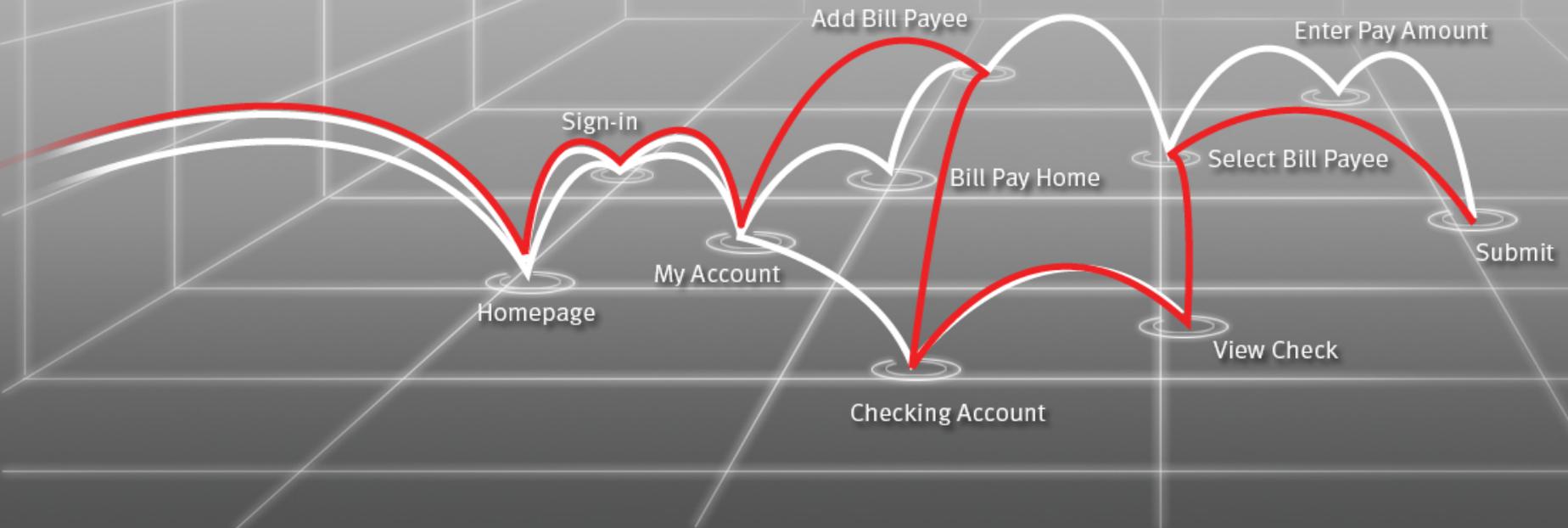
# Population-based Behavior



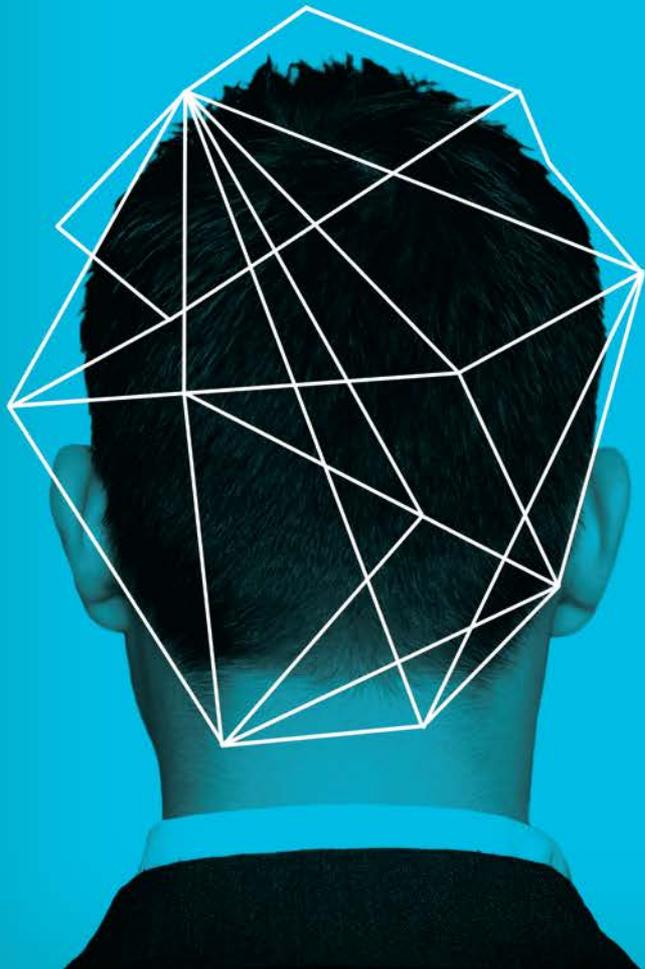
# Man-in-the-Browser Attack

## 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

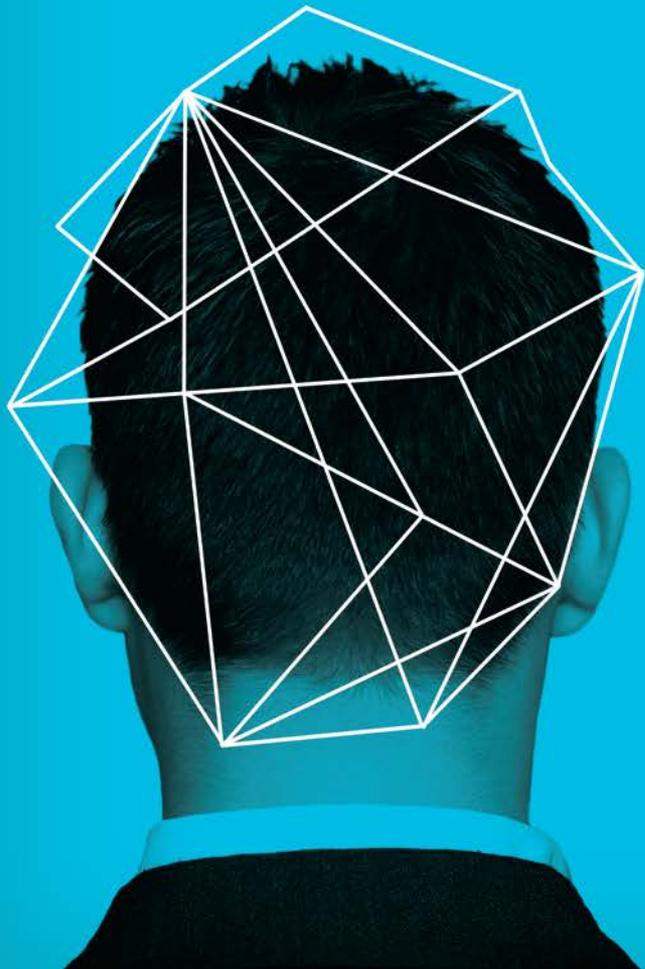
74%

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

The image shows a security dashboard with two main sections. The top section, titled 'CLICKS', displays a table of user interactions. The bottom section, titled 'Transaction', provides a detailed view of a specific transaction.

**CLICKS Table:**

UTC Time	Click Delta	IP Address	Page	Threat Score
2011-07-26 07:26:52.980	00:00:00.621	165.193.42.77	/errors/404.aspx	Yellow
2011-07-26 07:26:53.627	00:00:00.629	165.193.42.77	/errors/404.aspx	Yellow
2011-07-26 07:26:53.892	00:00:00.266	165.193.42.77	/errors/404.aspx	Yellow
2011-07-26 07:26:54.144	00:00:00.250	165.193.42.77	/errors/404.aspx	Yellow
2011-07-26 07:26:54.360	00:00:00.224	165.193.42.77	/errors/404.aspx	Yellow
2011-07-26 07:26:54.630	00:00:00.263	165.193.42.77	/errors/404.aspx	Yellow
2011-07-26 07:26:54.832	00:00:00.207	165.193.42.77	/x	Green
2011-07-26 07:26:55.920	00:00:01.087	165.193.42.77	/x	Green
2011-07-26 07:26:56.330	00:00:00.414	165.193.42.77	/errors/500.aspx	Green
2011-07-26 07:26:56.480	00:00:00.146	165.193.42.77	/x	Green
2011-07-26 07:26:56.800	00:00:00.322	165.193.42.77	/errors/500.aspx	Green
2011-07-26 07:26:56.940	00:00:00.137	165.193.42.77	/x	Green

**Transaction Details:**

UTC Time	Class	Type	Name Value Pairs
07:26:53.627	Txn Start	STTX	ip=165.193.42.77
	Data	REQUEST	method=GET&page=/
	Data	HEADERS	referer=http://...&host=...&user-agent=Mozilla/5.0 (compatible; MSIE 7.0; MSIE 4.0; Firefox/2.0.0.3)
	Data	ARGS	aspxerrorpath=.../etd/passwd

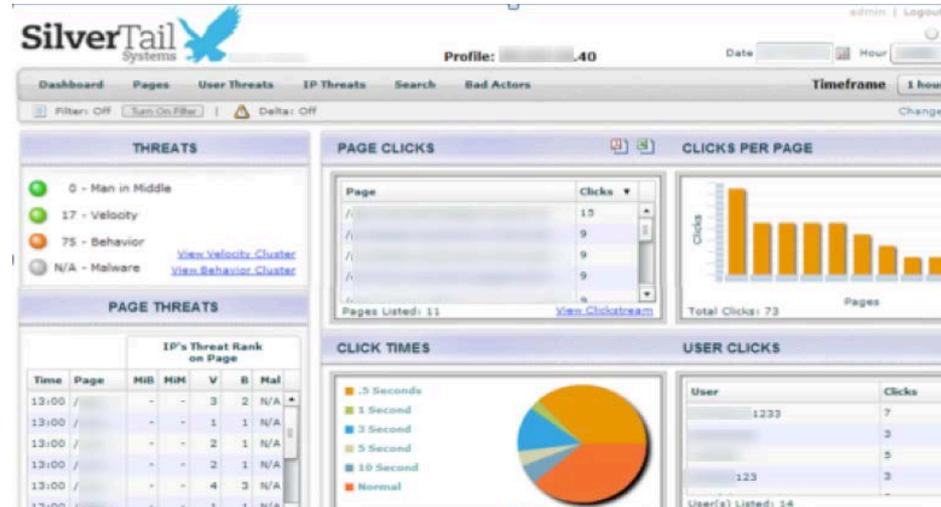
# Horizontal Password Guessing

## 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



```
username=s[REDACTED]123&password=f92c0ff0f313a  
username=v[REDACTED]123&password=f92c0ff0f313a  
username=h[REDACTED]123&password=f92c0ff0f313a
```

# 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

The image displays two screenshots of a web proxy tool interface, showing network transactions. The top screenshot shows a transaction from IP 64.255.164.67 with a user agent string for Opera Mini. The bottom screenshot shows a transaction from IP 129.33.192.170 with a user agent string for Mozilla/5.0 (iPhone). A blue callout box labeled "Different UA Strings" points to the user agent strings in both screenshots. Another blue callout box labeled "Same Cookie" points to the "utma" cookie value in both screenshots, which is "108514819.631523246.1304230250.1304230250.1304230250.1".

UTC Time	Class	Type	Name Value Pairs
06:32:22.799	Txn Start	STTX	ip=64.255.164.67
	Data	REQUEST	method=GET&page=..._login.aspx&serverip=...&serverport=...&clientport=...
	Data	HEADERS	user-agent=Opera/9.80 (J2ME/MIDP; Opera Mini/6.24093/24.854; U; en) Presto/2.5.25 Version/10.54;host=pcaccess.nefcu.com&referer=https://pcaccess.../scripts/lbank.dll?Func=SSignOn&homepath=cu3&cookie2=...&Version=1&pragma=no-cache&connection=Keep-Alive&operamini-features=advanced,file_system,camera,touch,folding,routing&operamini-phone=LG#VM510&operamini-phone-ua=LGE-VM510 NetFront/3.5.1 (GUI) MMP/2.0&forwarded=209.236.250.245
	Data	COOKIE	__utnz=108514819.1298236980.4.1.utmcsr=(STID=0cd1283203f4ac27134768a5fab6593c; __utma=108514819.1567447603.1282357651; __utmb=108514819.1.10.1305959524; __utmc=217379465.1298236966.5.1.utmcsr=( __utma=217379465.1590461777.1282357612; __utmb=217379465.2.10.1305959336
	Data	USER	guid=0cd1283203f4ac27134768a5fab6593c&id=537160&userfrom=form
	Data	STATUS	200

UTC Time	Class	Type	Name Value Pairs
	Txn Start	STTX	ip=129.33.192.170
	Data	REQUEST	method=GET&page=..._login.aspx&serverip=...&serverport=...&clientport=...
	Data	HEADERS	host=pcaccess...&user-agent=Mozilla/5.0 (iPod; U; CPU iPhone OS 4_3 like Mac OS X; en-us) AppleWebKit/533.17.9 (KHTML, like Gecko) Version/5.0.2 Mobile/8F190 Safari/6533.18.5&referer=https://pcaccess.../scripts/lbank.dll?Func=SSignOn&homepath=cu3&connection=keep-alive
	Data	COOKIE	__utma=108514819.631523246.1304230250.1304230250.1304230250.1; __utnz=108514819.1304230250.1.1.utmcsr=(direct) utmcmd=(none); STID=0cd1283203f4ac27134768a5fab6593c; __utma=217379465.570106303.1304230214.1304230214.1305960087.2; __utmc=217379465.2.10.1305960087; __utmb=217379465.1.1.1305960087; __utmc=217379465; __utmb=217379465.1304230214.1.1.utmcsr=(direct) utmcmd=(none)
	Data	USER	guid=0cd1283203f4ac27134768a5fab6593c&id=537160&userfrom=form
	Data	STATUS	val=200

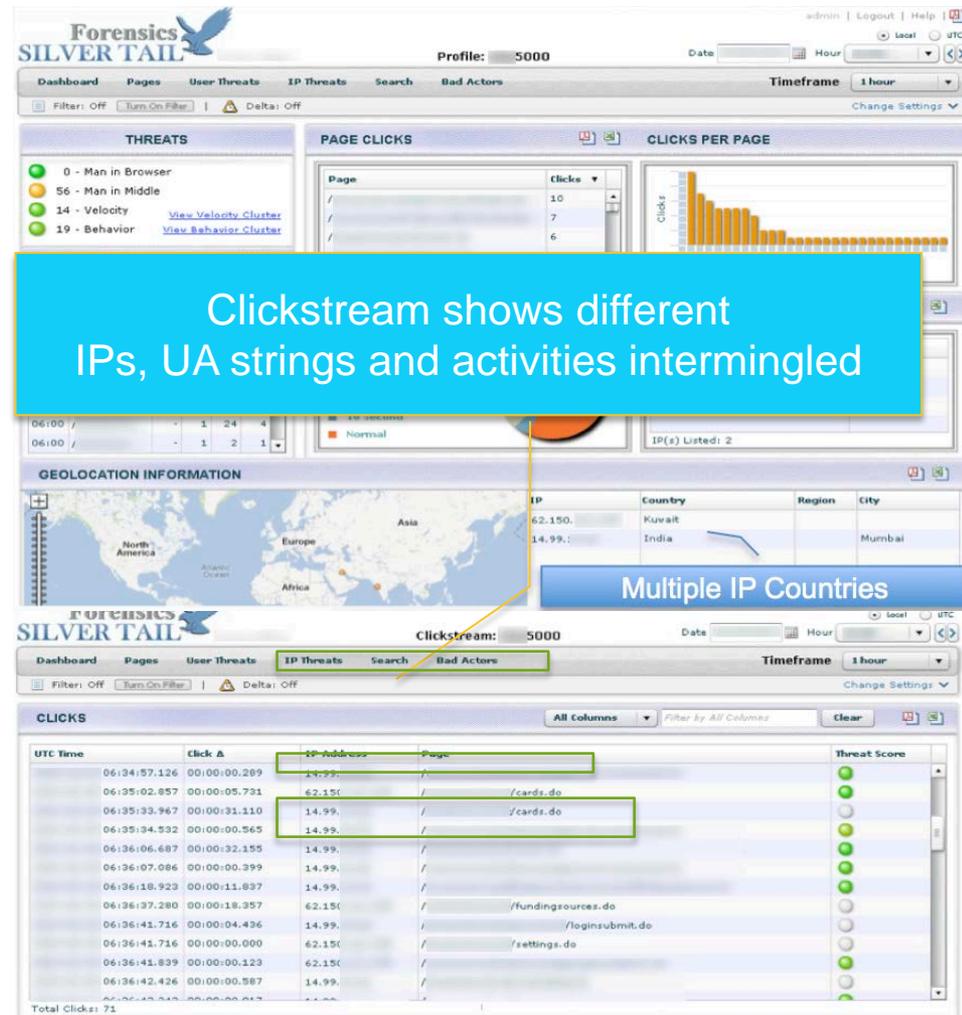
# Fraudulent Money Movement

## What were 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



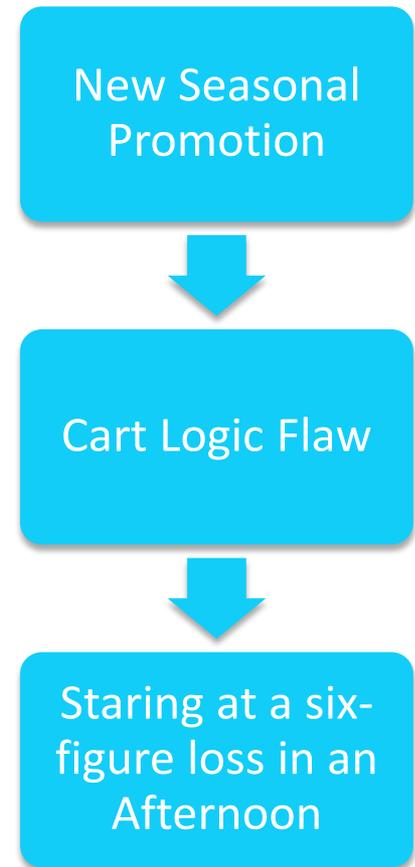
# E-Commerce Fraud

## 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 were they doing?

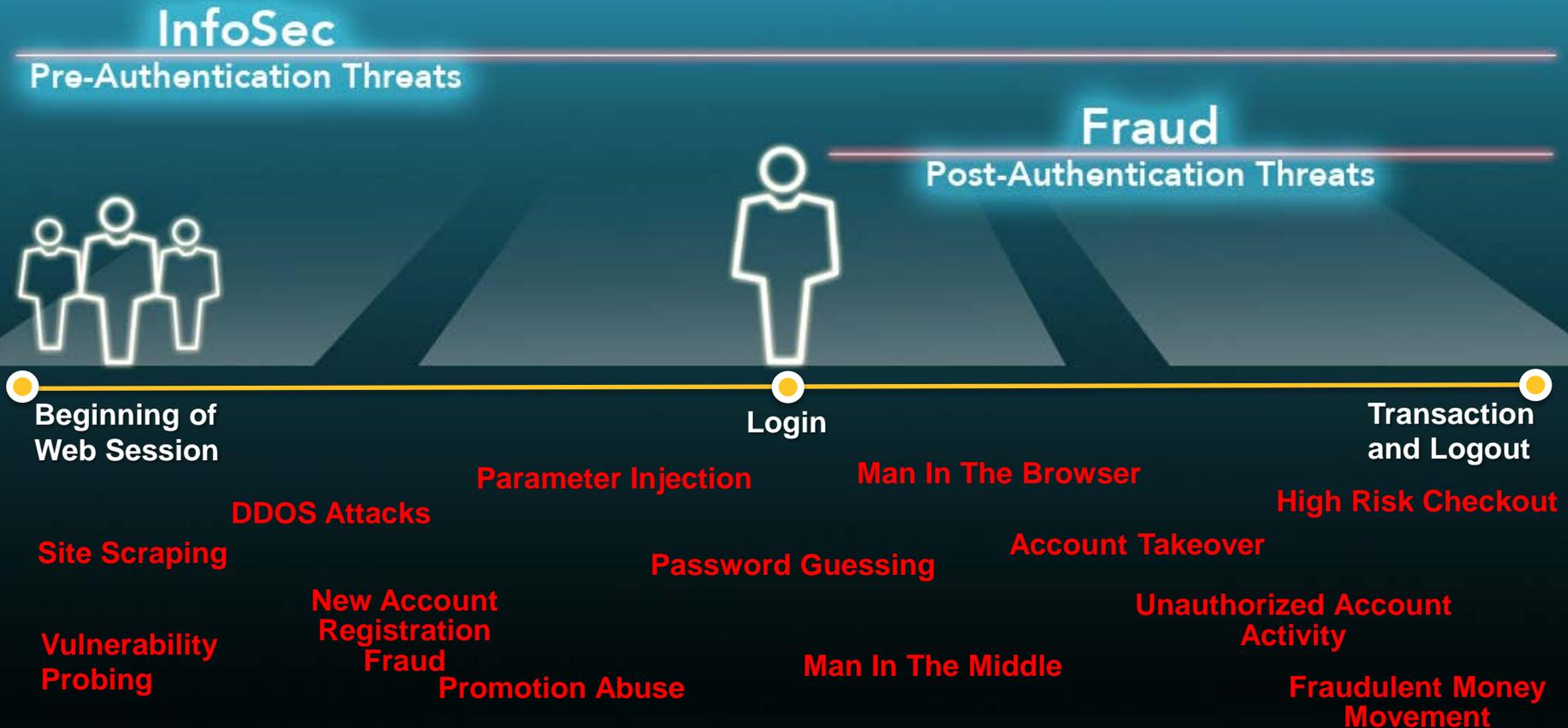
- ▶ Application resource exhaustion
- ▶ Botnets sending Search, Login New Account, Purchase queries

## 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](mailto:jason.sloderbeck@rsa.com)

[info@silvertailsystems.com](mailto:info@silvertailsystems.com)

