

# Eskimming Threat & Tools

The Rising Threat of Eskimming  
and What to Do About It

Presented by John Bartholomew, Sr. VP, Technology

# John Bartholomew

---

Sr. VP, Technology



## SecurityMetrics Insight from 500+ ecommerce sites

SecurityMetrics Services:

- **Shopping Cart Inspect**
- **Shopping Cart Monitor**
- **Incident Response  
Forensics**





# Increased Sophistication

- **Obfuscation**
  - Multi-layer encryption
  - Minification
  - Piggybacking
  - Deep Embedding
  - Similar naming
- **Intermittent Attacks**
  - Iterative
  - Randomized
  - Detection avoidance

*Staying under the threshold for detection*

# Cardholder Data Environment (CDE) is exploding with third parties



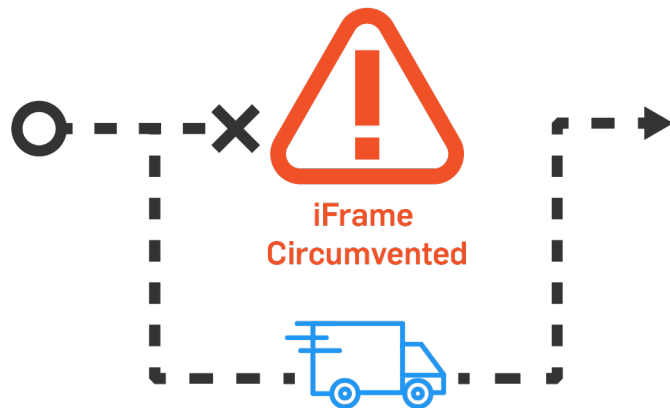
# Secure iFrame Circumvention

- 1 Step (not the known 2-step approach)
- Successful payment submission

## Genie is out of the bottle...

Unknown is how soon this will become widespread

Demo & discussion  
@SecurityMetrics Booth





## Primary Recommendations

- Web server & web dev security
  - SAQ A's improving hosting security
- External code/javascript accountability & authorization
- Monitoring Client-side Checkout Integrity

# Shopping Cart Inspect

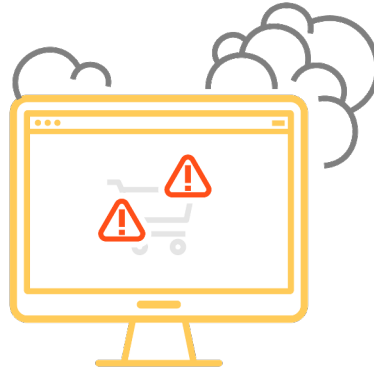
Abbreviated forensics of shopping cart client/browser-experience



# Sample Shopping Cart Inspect Findings



**CONCERNING**



**SUSPICIOUS**

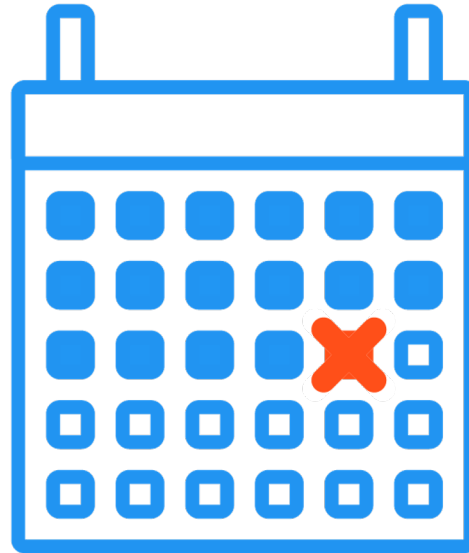


**MALICIOUS**

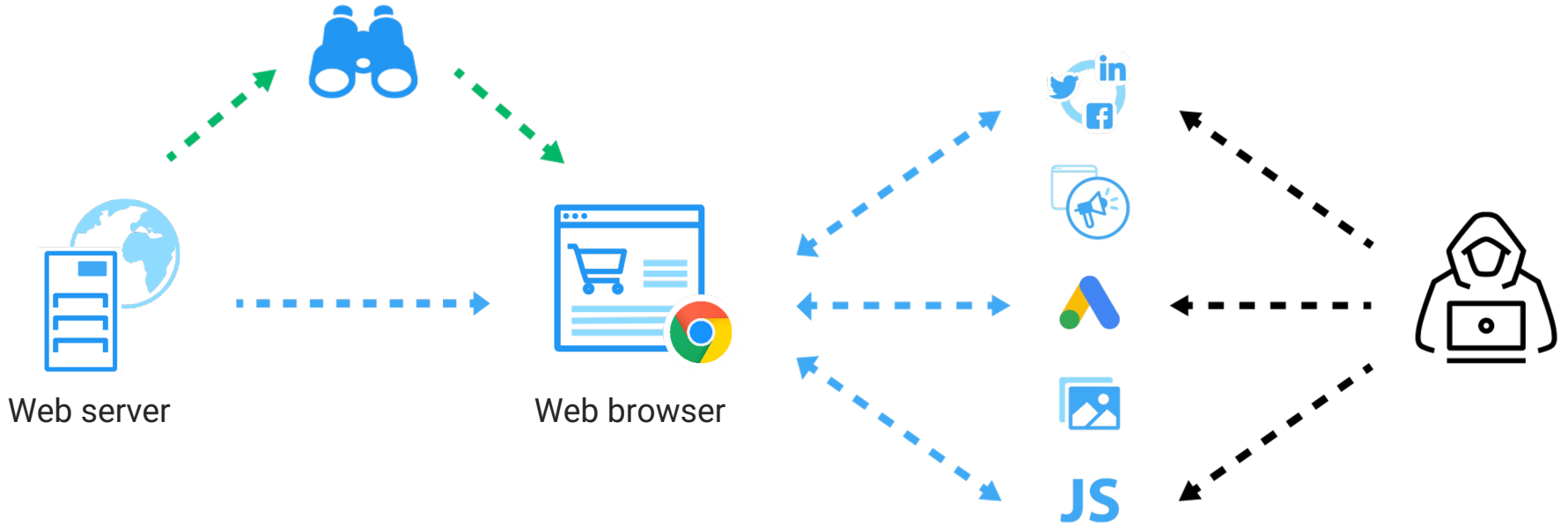
# Shopping Cart Monitor

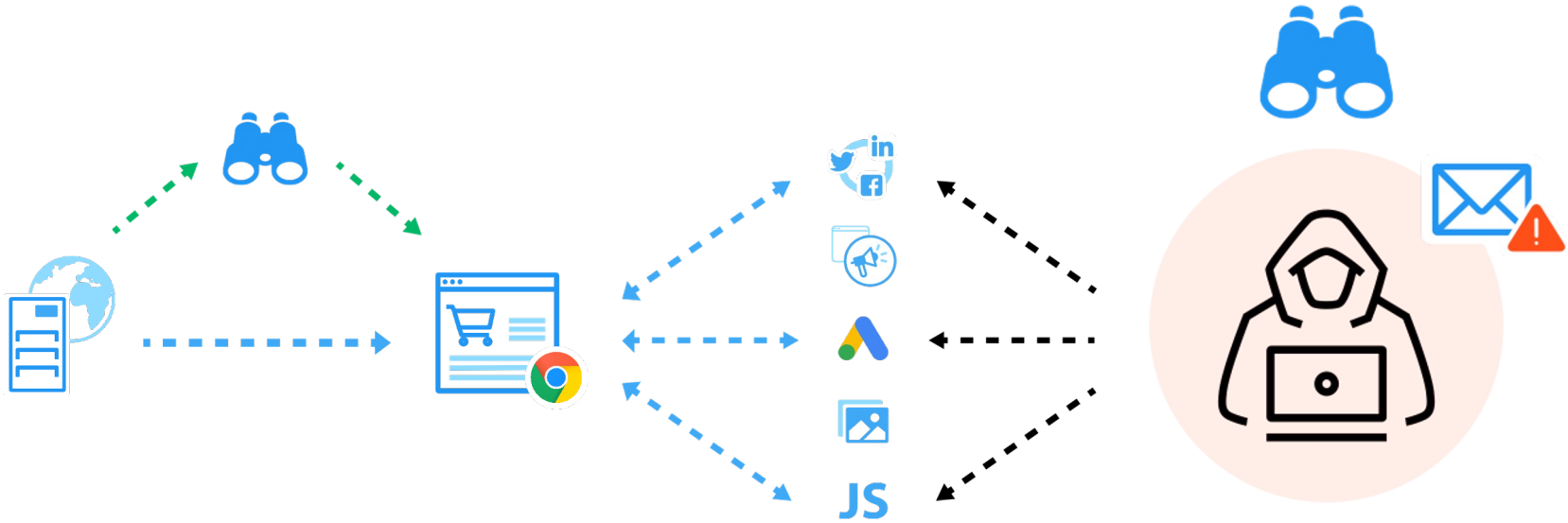
Recurring client-side ecommerce checkout review

Timely breach notification



Client: **Synthetic** Sally Shopper  
Shopping exactly like the real Sally Shopper



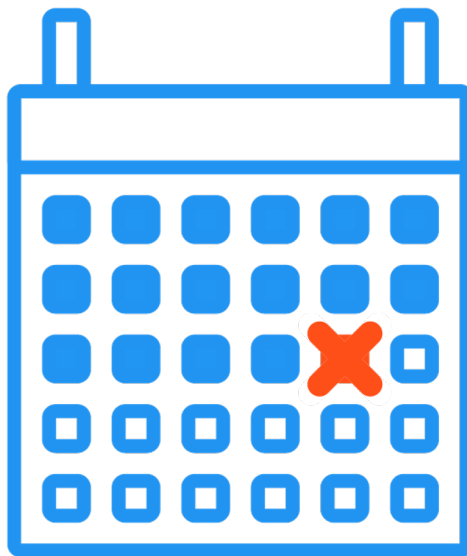


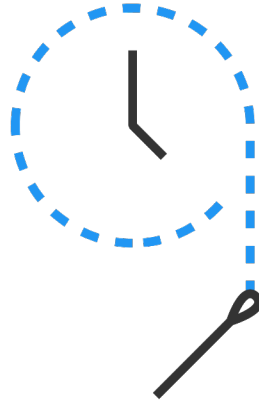
Threat Intelligence Center  
alerts the customer

# Shopping Cart Monitor

## Advantages

- No customer installation
- Minimal site impact  
= One customer shopping
- **Effective injection identification**





**a stitch in time saves  
time, money, and jobs**



# Come visit us!

John Bartholomew  
[jb@securitymetrics.com](mailto:jb@securitymetrics.com)