John Bartholomew

23 Years in Cyber Security

SVP, Strategic Relationships

SecurityMetrics, Inc.

securitymetrics®

PCI Security Standards Council®

Ecommerce Monitoring and Forensics Lessons

- Hacker Tactics
- Protection
- Shopping Cart Monitor

PCI Security Standards Council

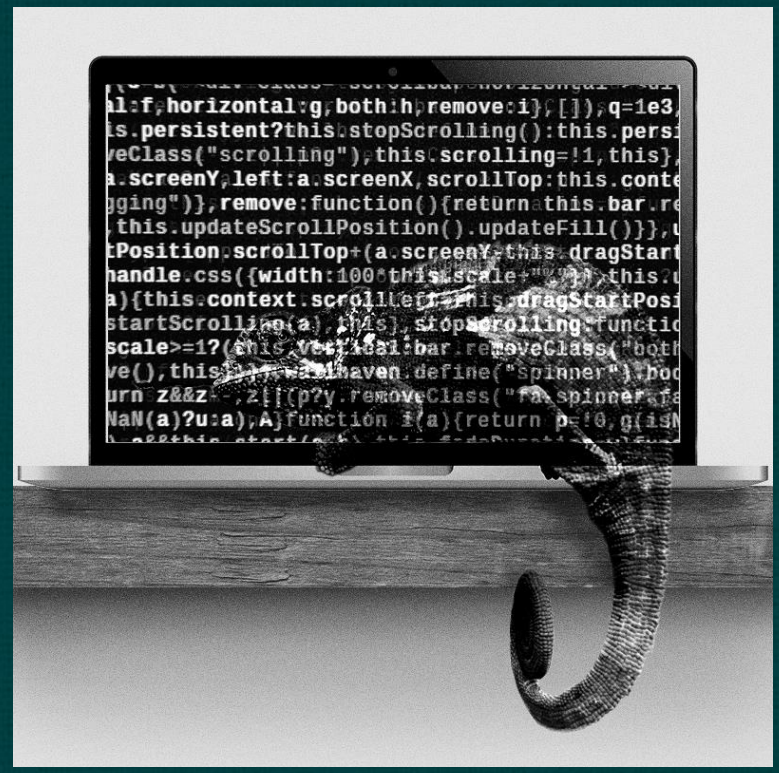
#1 Hacker Behavior

Improve Return on Investment

Hiding in Plain Sight

ROI #1 Blending

- Text one-offs - similar character, misspelling, add a dash/dot/comma…
- Code look-a-likes: Google, Facebook, code - calls malware function
- Function diversion:
  - GET used for Exfiltration,
  - OnError call malware (no image)
- Not what you thought
  - Site Logo contained binary malware
  - Analytics (rogue)
- Alternative Code
  - Detecting Dev Tools (monitoring) without mentioning dev tools



Ongoing battle of where to look for intrusive code

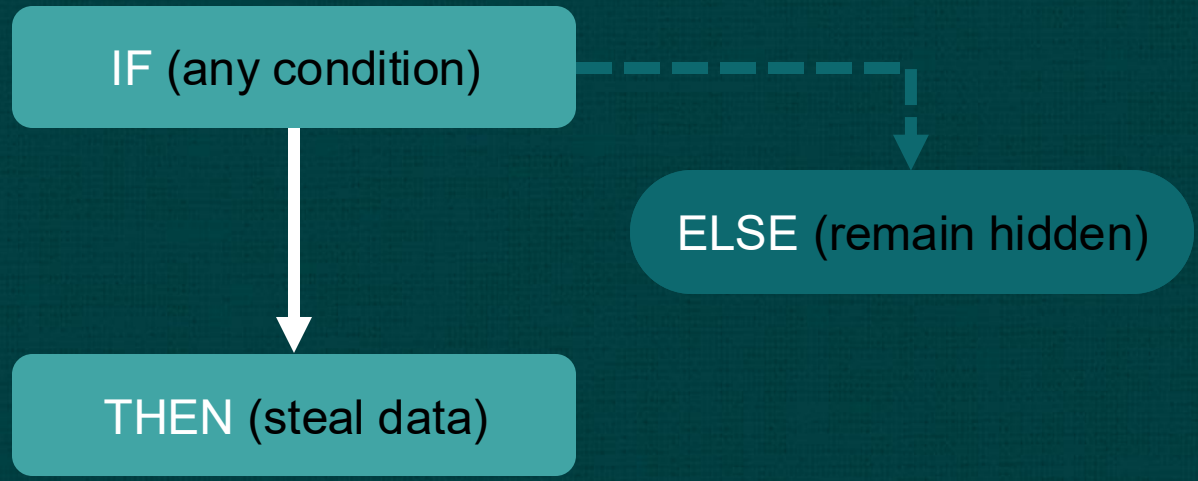
PCI Security Standards Council

Conditional Attacks

ROI #2

Examples:

- Form selection: coupons, shipping method
- Random number
- Time of Day (or randomized per day)
- Geo-specific or country specific
- Ad networks
- Make up your own



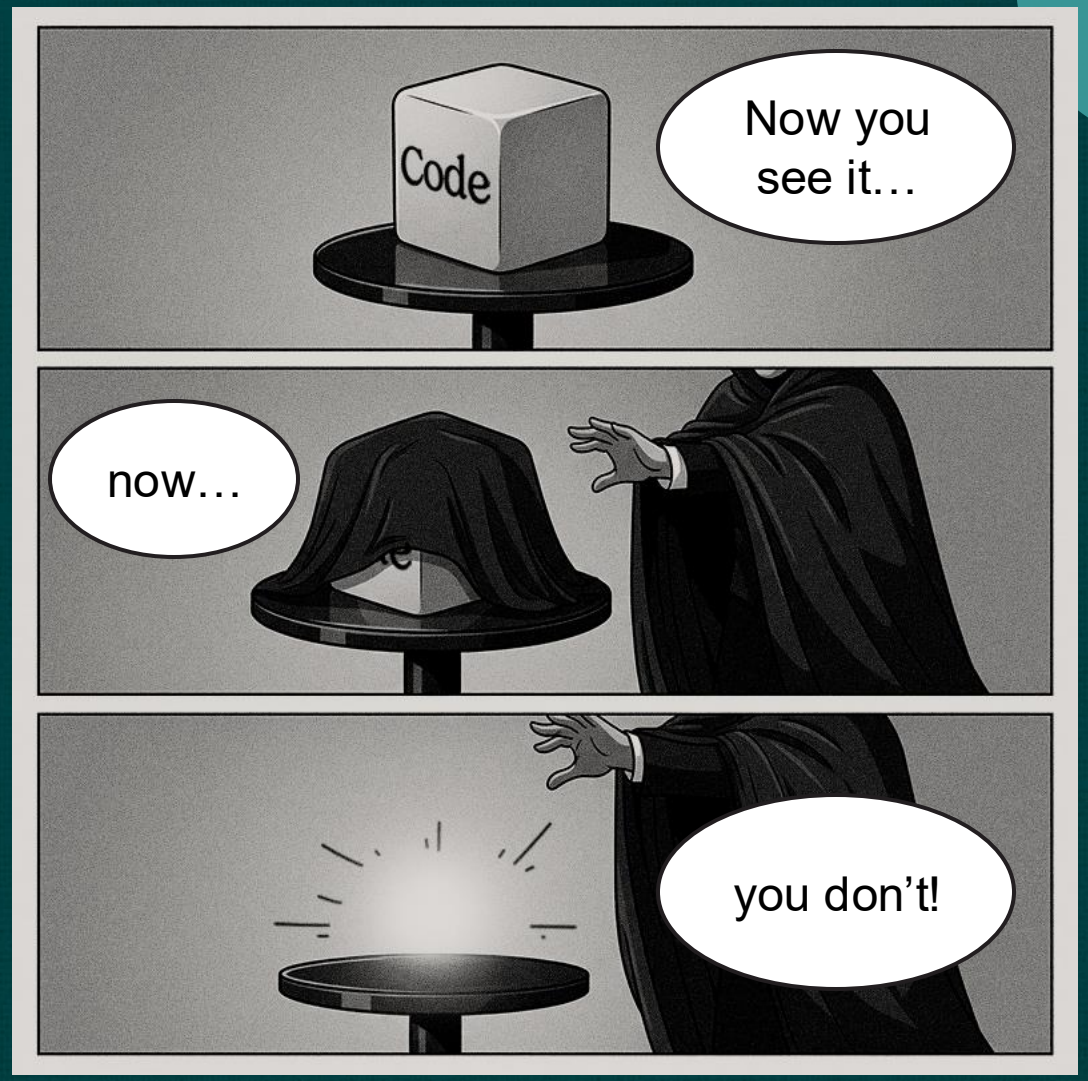
Result: random, sporadic or reduced data loss

Leave NO TRACE

ROI #3

Ghost Code

Result: forensics & detection solutions may miss the moment



PCI Security Standards Council

Access Protection

Protect Access Points

- Hosting Environments
  - Website
  - 3rd,4th,5th… Party Code
- Secure Coding

Basic security practices reduce hacker opportunities

Proper Monitoring

Identifies breaches even when:

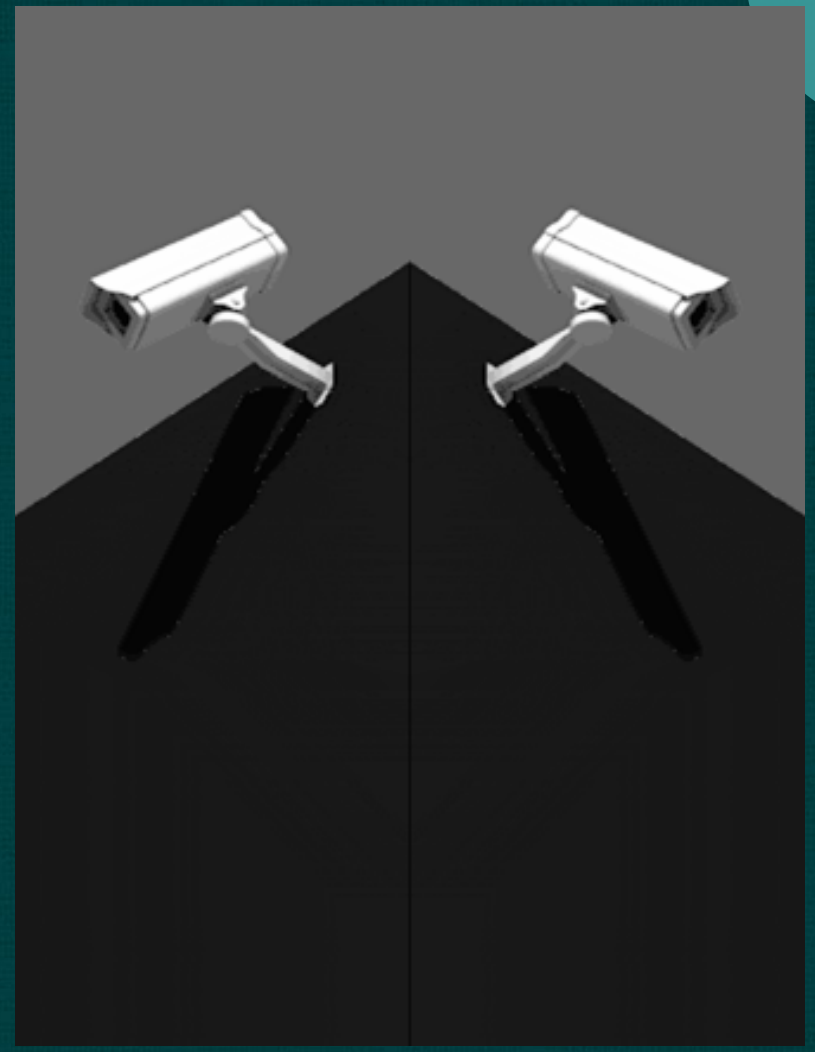
- Blending
- Conditional
- No Trace

Minimal Blind Spots

Shopping Cart Monitor

20+ Years of Ecommerce Forensics

- Agentless
  - Deep DOM perspective
  - Improved monitoring reliability
- Purpose-Built for PCI & Integrated
- 3 Versions SCI: Basic, Plus, Pro
  - SMB's: Basic & Plus – Simplicity & Affordability
  - Enterprise: Pro - Simplicity & Forensics "eyes on glass"



PCI Security Standards Council

Shopping Cart Monitor Process

1
Initialization

SCM Basic:

Merchant

SCM Plus

SecurityMetrics

SCM Pro

SecurityMetrics

2
Baseline

SCM Basic:

Merchant

SCM Plus

Merchant

SCM Pro

SecurityMetrics*

3
Revisits

SCM Basic:

Merchant

SCM Plus

SecurityMetrics

SCM Pro

SecurityMetrics

4
Changes & Alerts

SCM Basic:

Merchant

SCM Plus

Merchant

SCM Pro

SecurityMetrics*

*Merchant contacted if needed

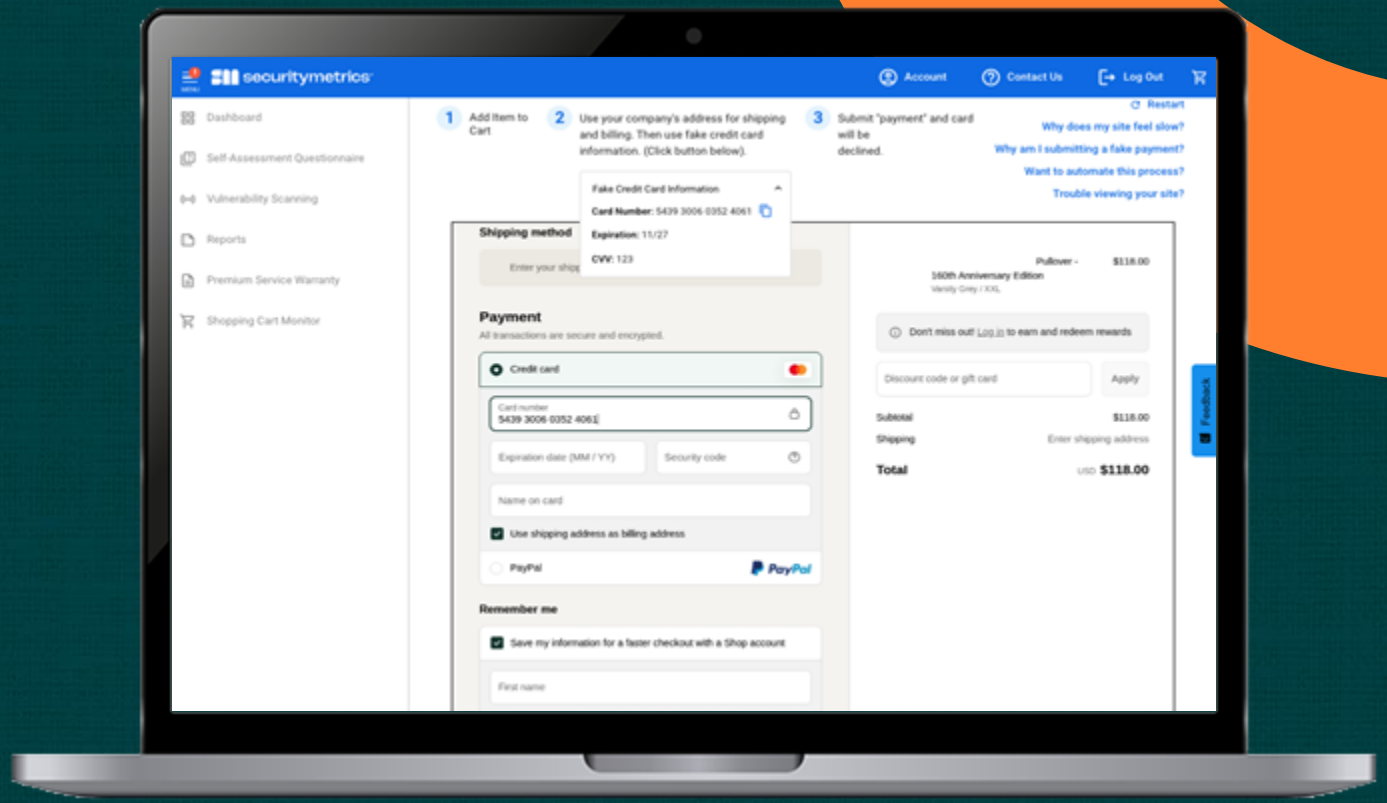
PCI Security Standards Council

Shopping Cart Monitor

Initialization

Features

- Begin Immediately
  - No Software installation
  - Targeted Risk Analysis
- Simple Experience
  - Step by step
  - Tech skill = Online purchase!
  - Test CC provided
  - Extensive helps
- 24x7x365 tech support



PCI Security Standards Council

Shopping Cart Monitor

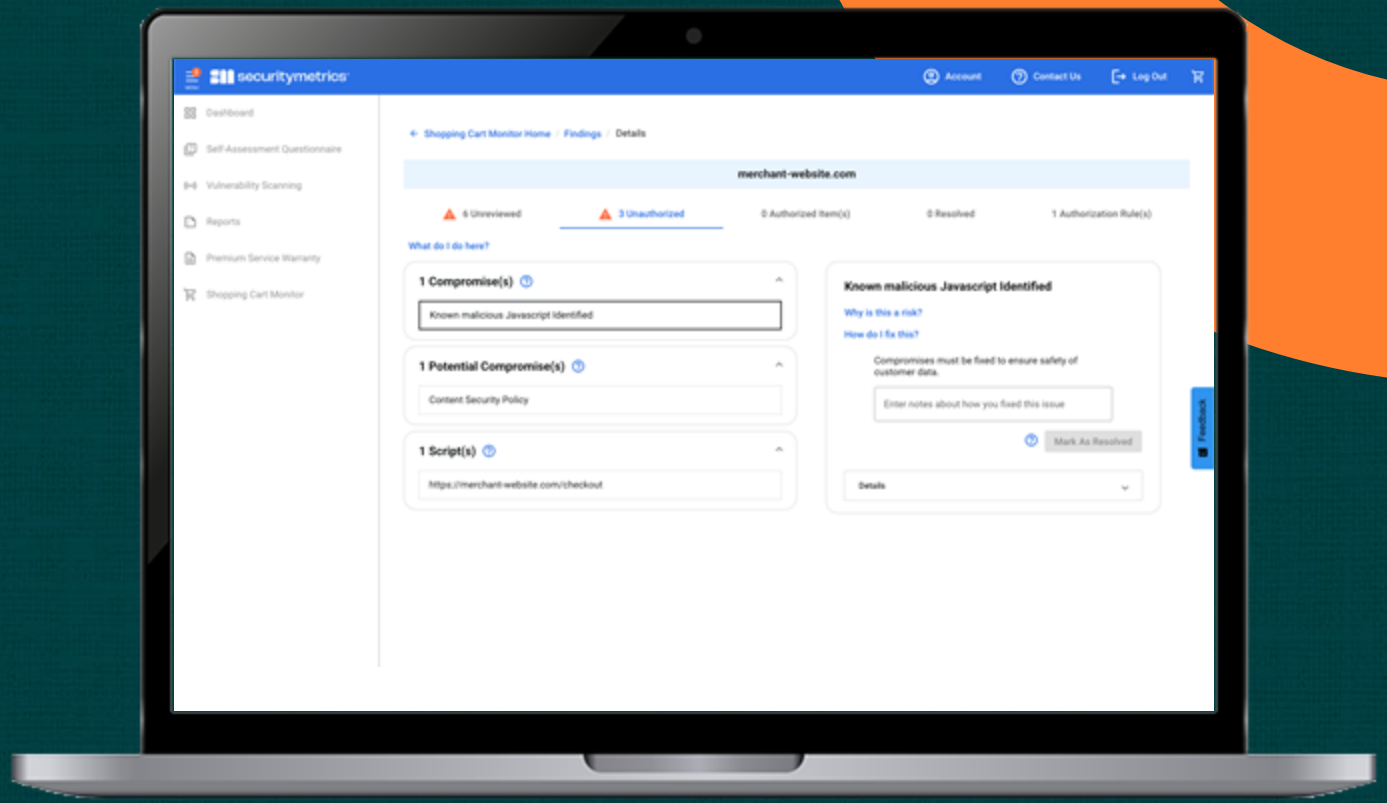
Baseline

Discoveries

- New Scripts
- Potential Compromise
- Compromise

6.4.3 Features

- Presented by Domain
- Authorize (indiv, group)
- Dynamic (domain, path, indiv)



PCI Security Standards Council

Shopping Cart Monitor

Additionally

Additionally:

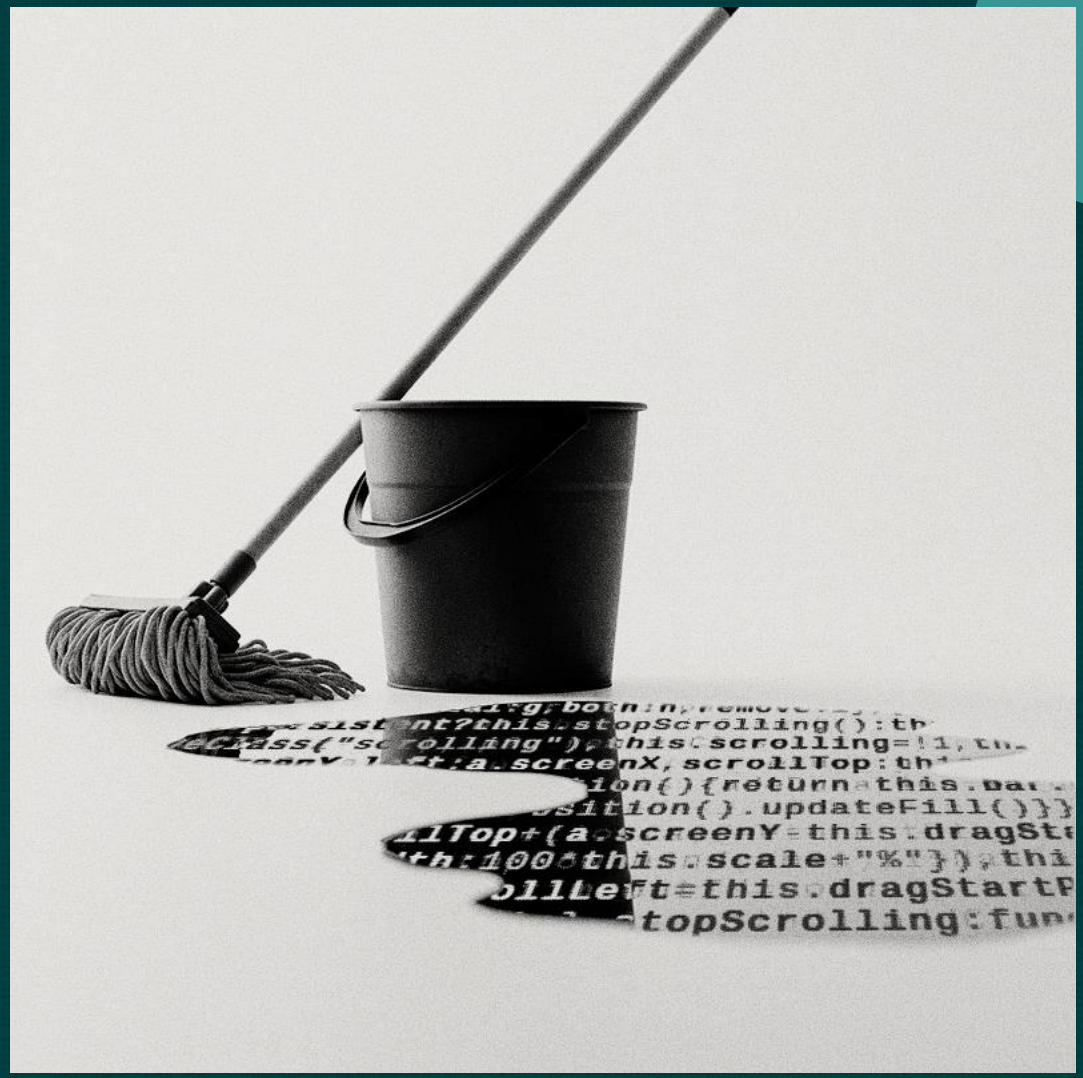
- (Potential) Compromises reviewed regardless of baseline
- Dynamic solution per ongoing forensics & pen testing
- More Reliable
  - Zero footprint for hacker discovery
  - No website performance degradation
  - Not possible for hacker to defeating monitoring script
  - No blocking accidents

Cleanup

Research & Remediate:

1. Access methods
2. Theft processes (obtaining data and exfiltration)
3. Potential back door installed.

Partial remediation is recipe for recurring attacks



PCI Security Standards Council

More Info

securitymetrics®

PCI Security Standards Council®