

Europe Community Meeting 2023





How to Protect Your Ecommerce Transactions

An Overview of PCI DSS v4.0 Changes for Ecommerce Sites (SAQ A, A-EP, D, ROC)

securityMETRICS®

Changes in eCommerce Threats

Most Common Threats Based on Forensic Analysis

- What attacks are most common lately?
 - eCommerce skimming
 - iFrame integrity compromises
 - Source change
 - Redrawing
 - Malicious scripts included
- Skimming not visible to customer or processor

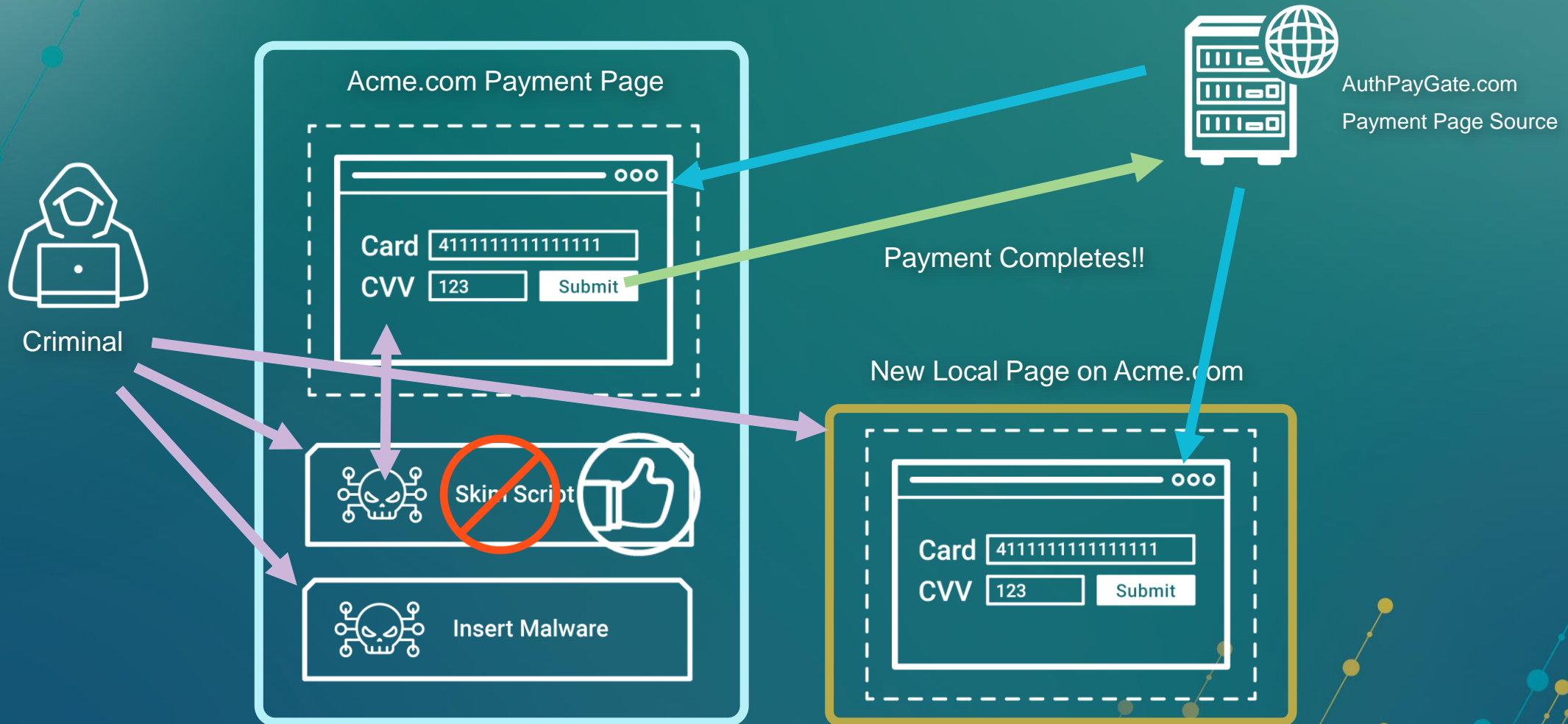
eCommerce Threats Today

eCommerce Primary Research being Conducted by SecurityMetrics

- Internet eCommerce Research
 - 96 million domains worldwide
 - 52 million ecommerce sites worldwide
 - Risk Check tests for common vulnerabilities, no false positives
 - Results
 - 29.7% of these sites had serious vulnerabilities
 - Only 17% were using CSP or SRI
 - What this means
 - Nearly 30% of ecommerce sites are vulnerable to being exploited by malware

Demo of an iFrame Skimming Attack

iFrame Same Origin Policy Defeat



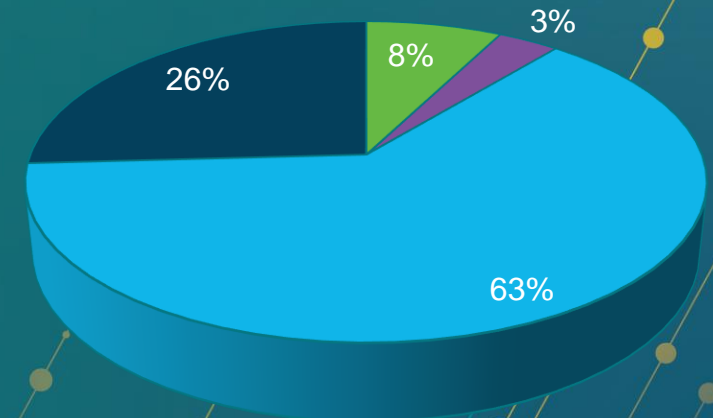
Ecommerce Threats - Skimming

Ecommerce Primary Research being Conducted by SecurityMetrics

- Shopping Cart forensic investigations
 - 1400 sites reviewed for skimming attacks
 - 92.4% of sites had security issues
 - 2.44 issues per site on average
 - 3% actively loosing card data
- Apply this to ecommerce as a whole
 - ~1.56M sites currently leaking card data
 - Current trends show that in 5 years this could be ~15 million sites infected and leaking

Shopping Carts Tested

■ No issues
■ Suspicious
■ Malicious
■ Concerning



How Fight Skimming Attacks?

- Most malicious scripts are very difficult to find
 - Analysis and scanning must occur in the browser execution environment (Document Object Model - DOM)
- PCI DSS v4.0 adds requirements to help
 - Dynamic script scanning really is needed
- What should eCommerce Merchants do?
 - Goal is to regain control of referring pages and payment pages
 - Start now testing tools

PCI DSS 4.0 Addresses Threats

Requirements 6.4.3 and 11.6.1 Added to Control Trends in eCommerce skimming

- Requirement 6.4.3 – keep track of scripts used
 - We have found over 300 scripts on a single payment page
- Requirement 11.6.1
 - Periodic (weekly) scanning to detect changes or additions
 - Consider use of prevention HTTP techniques (SRI, CSP)
 - Hard to search pages generated dynamically
- End Result: controlled, simpler, & secure payment pages

SAQ A eCommerce Requirements

- Changes to SAQ A will be a challenge
 - ASV scanning
 - Future dated script scanning
- How to get ready?
 - Start ASAP getting used to doing ASV scans
 - Start testing tools for script scanning requirements
- There won't be a delay in PCI DSS 4.0 deadlines
 - If using iFrame redirect - investigate script tools

Script Scanning Tools

What are characteristics of these tools? What is needed?

- Detect changes/additions on payment pages via DOM
- Tool setup types
 - Agentless
 - Agent installation required by merchant
- Not like VA scan, much more complex
- Ease of use for merchants is important for adoption
 - SAQ A, A-EP, & D
- Start testing soon so you are ready for March 31, 2025

Key Takeaways

- New eCommerce attacks are real and prevalent
- Changes to PCI DSS v4.0 help address threats
- Work with SAQ A merchants as early as possible
- Join Risk Check research



Thank You!



Europe Community Meeting 2023

