CAMPUSGUARD™

ScriptSafe

source DEFENSE

Decentralized and Vulnerable

Why Higher Ed is the Perfect Target for Modern eSkimming

Critically Important Information Every Payment Security Professional Needs to Understand

March 4, 2026

Steve Ward – Source Defense

Key Takeaways

- Diversity of Higher Ed Transactions Makes it a Prime Industry for Adversaries
- eSkimming Attacks are Proliferating and Gaining Sophistication
- Attacks are Evolving to Evade Controls
- Compliance is Creating a False Sense of Security
- Adversaries Increasing Focus on Additional Forms of Data Theft
- Compromises are “Slow and Low” and Persist for Inordinate Amounts of Time

SESSION GUIDE

HOW TO USE THIS BRIEFING

FOCUS ON REAL-WORLD THREATS

We'll examine observed 2025 attack patterns and how they break existing defenses. This is a tactical briefing grounded in current threat intelligence.

BEYOND THE BASICS

This is not a "101" session. We'll speak uncomfortable truths. We assume baseline familiarity with eSkimming concepts and dive straight into what matters most.

INTERACTIVE FORMAT

Q&A at the end - drop questions in chat anytime. We'll address common concerns and specific scenarios during our discussion period.

aaaSecurity Point

nce

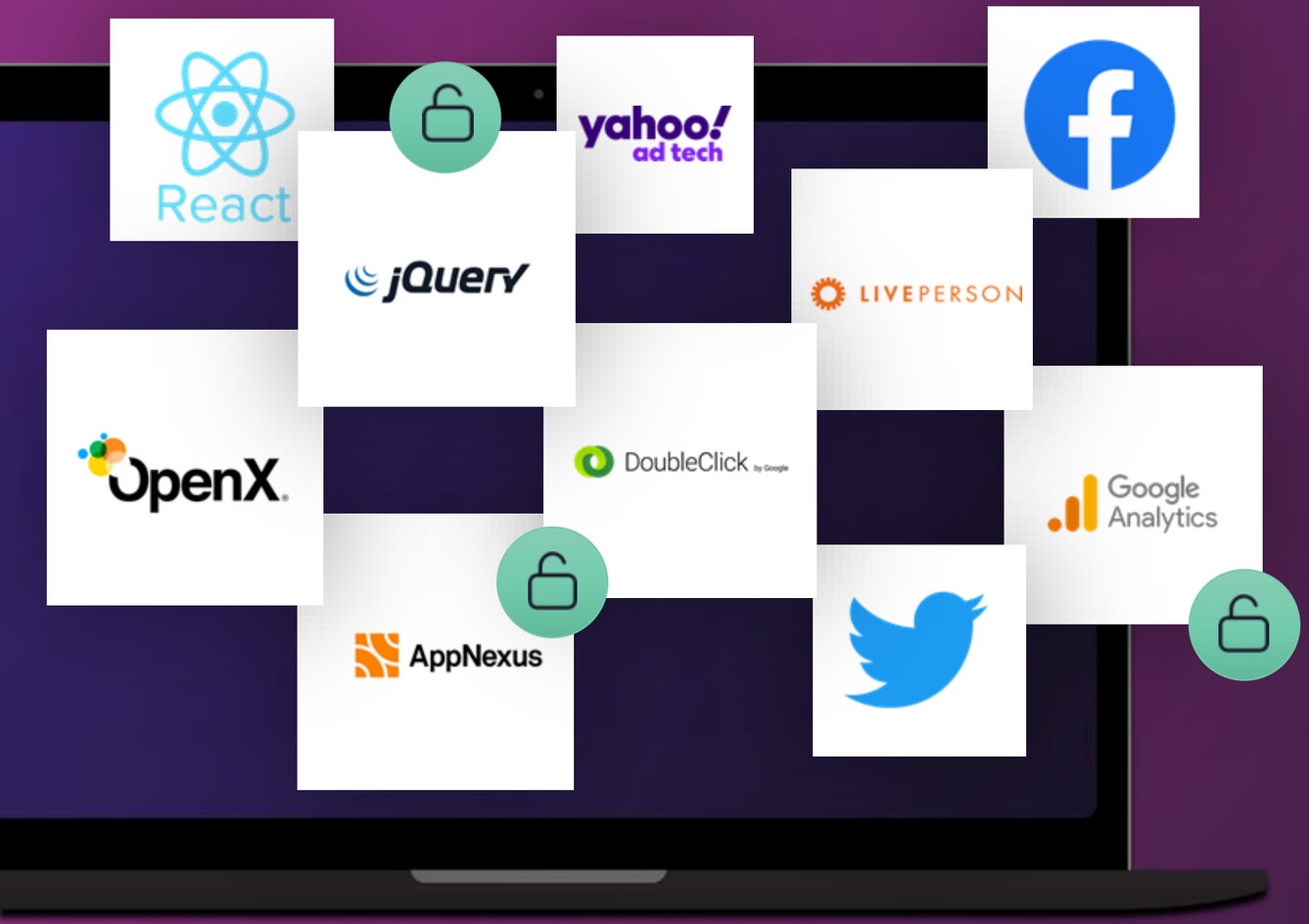
/ebsec

- Enabling 3rd party service int
- Addressing the last mile of 3
- Management
- Supporting zero-trust and SI

Protecting Data at the Point of Input

A New Challenge for the PCI Community

source DEFENSE



82%

of code and actions
are outside your control

What Makes Unmanaged Scripts So Dangerous?

JavaScript compromised by an adversary can:

Change page content

Record keystrokes

Add content (images, text, video, & form fields)

Track website behavior

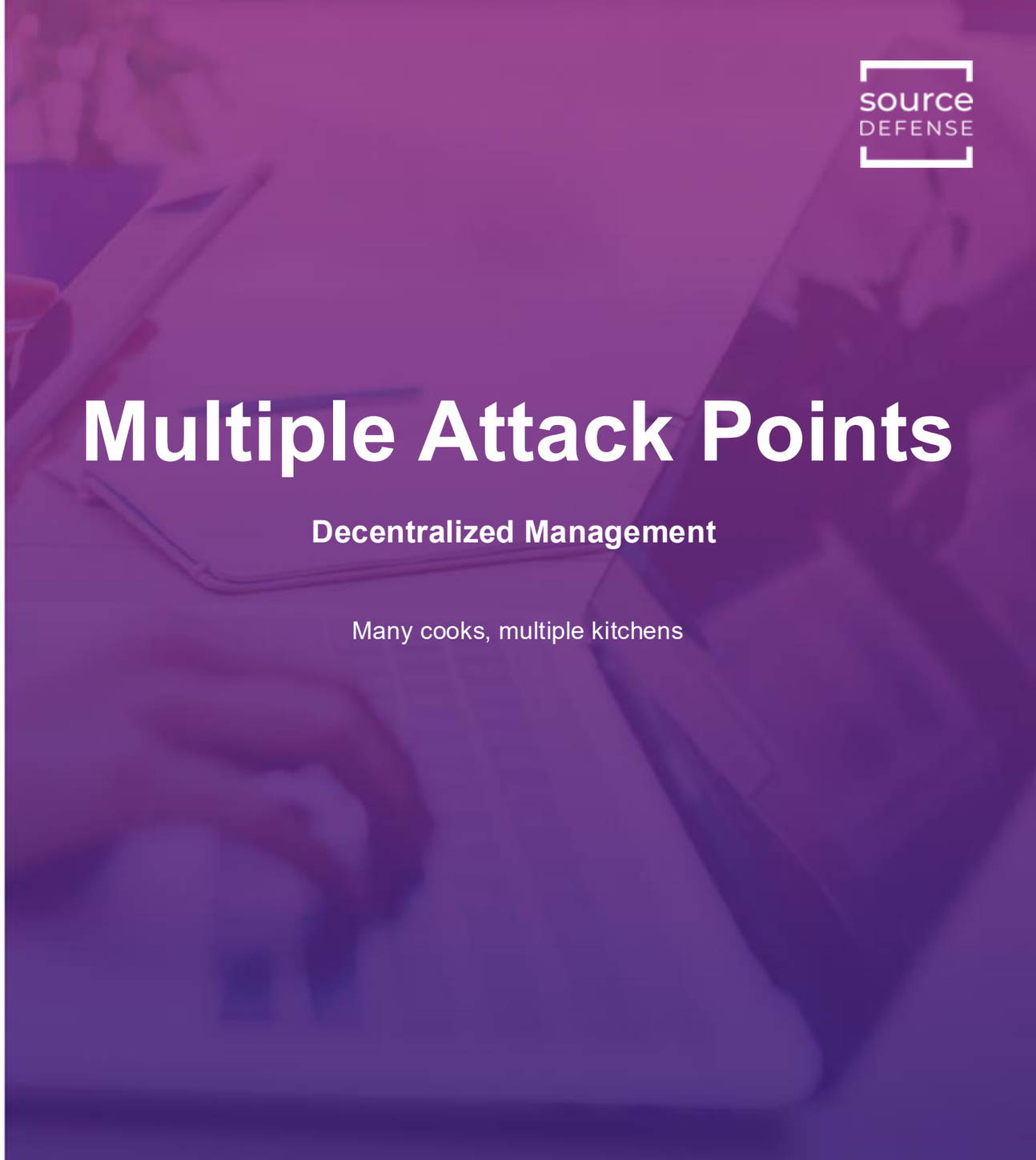
Capture and exfiltrate credit card data

Redirect visitors to websites under attacker control

HIGHER EDUCATION
Target Rich Environments

Multiple Payment Flows and Sensitive Data Collection Points

- Tuition and Fees
- Online Bookstores
- Athletic and Event Ticketing
- Alumni and Donation Platforms
- Department Level Micro-sites
- Healthcare and Insurance Services



Relevant Requirements for eSkimming

PCI DSS 4.0.1
Mandated as of 4.1.25

source DEFENSE

ScriptSafe

Maintain an inventory of all **payment page scripts** and justify why they are necessary
(6.4.3)

Confirm that each script is authorized
(6.4.3)

Assure the integrity of each script (6.4.3)

Monitor **Payment Page** headers for changes at least once every seven days
(11.6.1)

Alert and respond to all malicious scripts on your **payment pages**
(11.6.1)

2025 – A Year of Advancement Scaling and Shifting TTPs

Tens of Thousands

E-COMMERCE SITES ATTACKED

Compromised globally across verticals

- One to many attacks vs. targeted whales
- Higher Education
- Fashion and Apparel
- Travel and Leisure
- Transportation
- Media
- Government Services

source DEFENSE

92+

DISTINCT ESKIMMING CAMPAIGNS

Observed and documented throughout 2025

30+

GTM IDS COMPROMISED

Unique Google Tag Manager IDs abused

52

SCRIPT MODULAR ATTACK INFRASTRUCTURE

Discovered in a single campaign late 2025

2025 – A Year of Advancement Scaling and Shifting TTPs

1K+

SITES IN SINGLE CAMPAIGN

Attacked simultaneously

Modern eSkimming operations demonstrate industrial-scale sophistication with modular architectures

Attackers target broadly across the entire site.
Campaigns operate globally targeting all languages, geographies, and payment platforms - no merchant segment is immune

source DEFENSE

15+

LANGUAGES TARGETED

With localized attack modules

10+

PAYMENT PLATFORMS

Targeted by attackers

MANY

SERVICES WEAPONIZED

Legitimate services abused for attacks

PCI DSS 4.01. and The Illusion of eSkimming Security

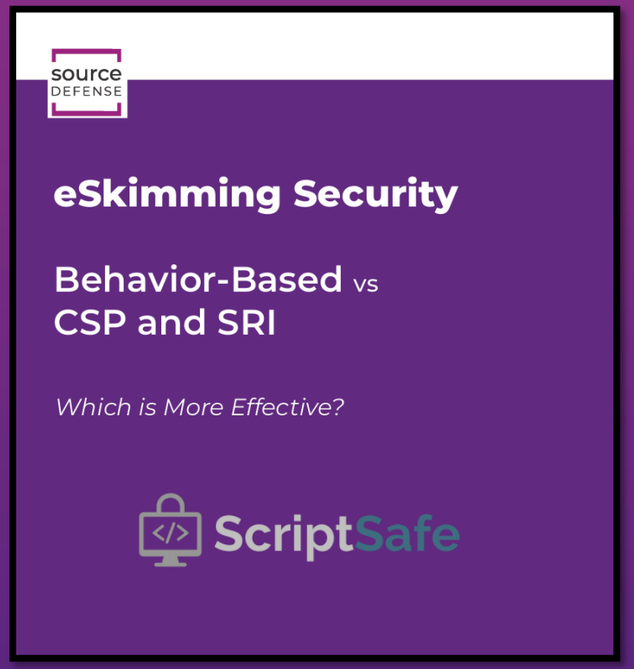
- **Misunderstanding the Threat**
  - Ignores guidance from experts in eSkimming and PCI Forensic Investigations
  - Relies on a myopic and static understanding of adversarial tradecraft
- **Misguiding the Global Community**
  - Emphasizes the wrong controls despite a chorus of warnings across the payments industry
  - Isolates focus instead of addressing the full attack surface
- **Missing the Point**
  - Descopes a critical target community
  - Provides loopholes for the richest of targets
  - Creates a compliance shell game
  - Does not deliver real security in current form

Issue # 1: Controls that Don’t Control

PCI DSS 4.0.1 Incorrectly Endorses CSP/SRI Based and Homegrown Solutions

CSP & SRI Cannot Stop eSkimming: Outdated Controls in PCI DSS 4.0.1

- **Static controls**, unable to track evolving JavaScript-based attacks
- PCI SSC’s **80-member eCommerce Guidance Taskforce** explicitly warned against their use
- CSP requires continuous updates, creates breakage, and lacks behavioral awareness
- SRI fails silently, cannot protect dynamic scripts, and offers no detection capability
- Core author to PCI DSS 4.0.1 now acknowledges that CSP/SRI do **not** prevent eSkimming
- Their inclusion in the DSS **misleads merchants** and creates false confidence



Call to Action:
Remove CSP/SRI as example controls; replace with explicit warnings against reliance; replace reference with real-controls

2025 Core Insights:
The Trust Model is the Attack Vector

HOW ATTACKERS WIN

- Hide inside "allowed" paths and trusted services
- Exploit narrow security scopes that create blind spots
- Leverage first-party trust and legitimate infrastructure
- Attack 3rd and 4th party partnerships, weaponizing the very tools meant to enhance site functionality

EXPANDING TARGETS AND ATTACK SURFACE

The threat has evolved beyond solely traditional payment card theft. Attackers now target the entire customer journey:

- Credentials during login and registration
- PII across account management flows
- Payment data through new injection vectors

30+

GTM IDS COMPROMISED

Unique Google Tag Manager IDs abused

LEGITIMATE SERVICES ABUSE

WHY REPUTATION-BASED LOGIC FAILS

Attackers increasingly leverage trusted, legitimate services to host and deliver skimming code. These platforms have strong reputations and bypass reputation-based security filters.

CDN AND EDGE PLATFORMS

Cloudflare, Fastly, AWS CloudFront used to host malicious scripts with high availability and trusted domain reputation

SERVERLESS AND CLOUD RUNTIMES

AWS Lambda, Google Cloud Functions, Azure Functions abused as exfiltration endpoints with legitimate HTTPS certificates

DEVELOPER PLATFORMS

GitHub, GitLab, Pastebin, JSFiddle used to host obfuscated payloads that appear as legitimate code repositories

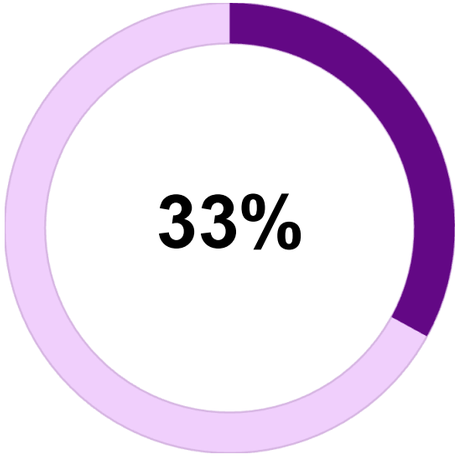
MESSAGING SERVICES

Discord webhooks, Telegram bots, Slack integrations repurposed as data exfiltration channels with encrypted connections

SOC takeaway: Focus on what scripts do, not just where they load from. Behavioral analysis trumps domain reputation.

⚠ PRIMARY ATTACK VECTOR

GOOGLE TAG MANAGER: AN ALARMING INTRUSION PATH



GTM ATTACK PREVALENCE

Shows up in over one-third of all 2025 documented attacks

WHY GTM IS SO ATTRACTIVE

- **Centralized control:** Single point for injecting malicious code across all pages
- **Rapid deployment:** Changes propagate immediately without developer involvement
- **Trusted delivery:** Loaded from Google's infrastructure, bypasses many security filters
- **Complex chains:** Containers can load other containers, creating layered attack opportunities

Key takeaway: Allowlisting GTM does not equal safety. The container content and behavior must be continuously validated.

GTM ATTACK PATTERN EXAMPLE: CHAIN ATTACKS

LEGITIMATE CONTAINER

Initial trusted GTM container loads normally

SECONDARY CONTAINER

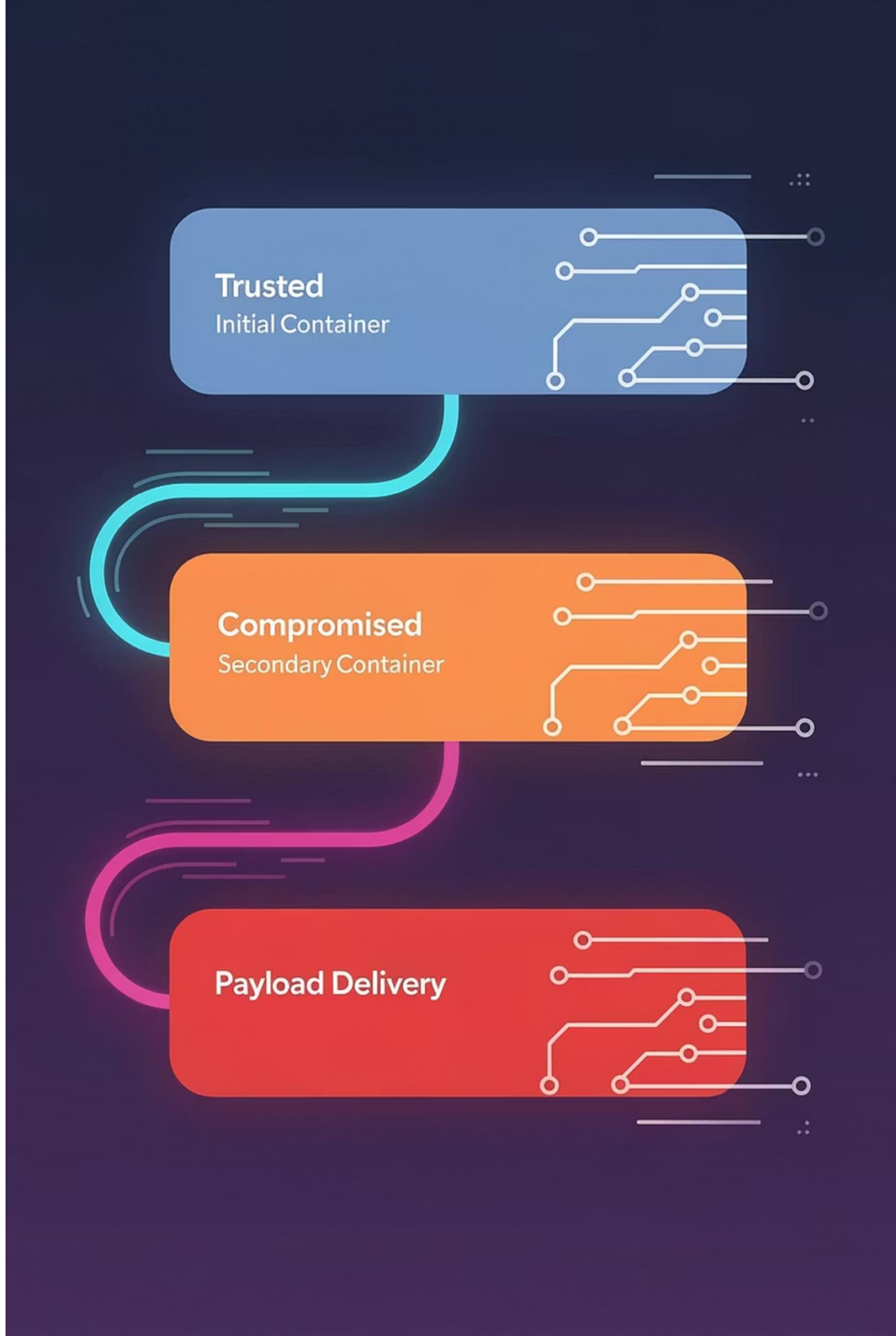
First container calls another compromised container

MALICIOUS PAYLOAD

Final container delivers the skimming code

Compromised containers calling other compromised containers creates multi-hop attack chains. This makes single-container review fundamentally insufficient for detecting threats.

Defense Suggestion: Implement chain-aware auditing that traces all container relationships and monitors cross-container calls. Static point-in-time reviews miss the dynamic nature of these attacks.



WHAT GTM CAMPAIGNS REVEAL

CENTRALIZED CONTROL AND FAST SWITCHING

OPERATIONAL MATURITY

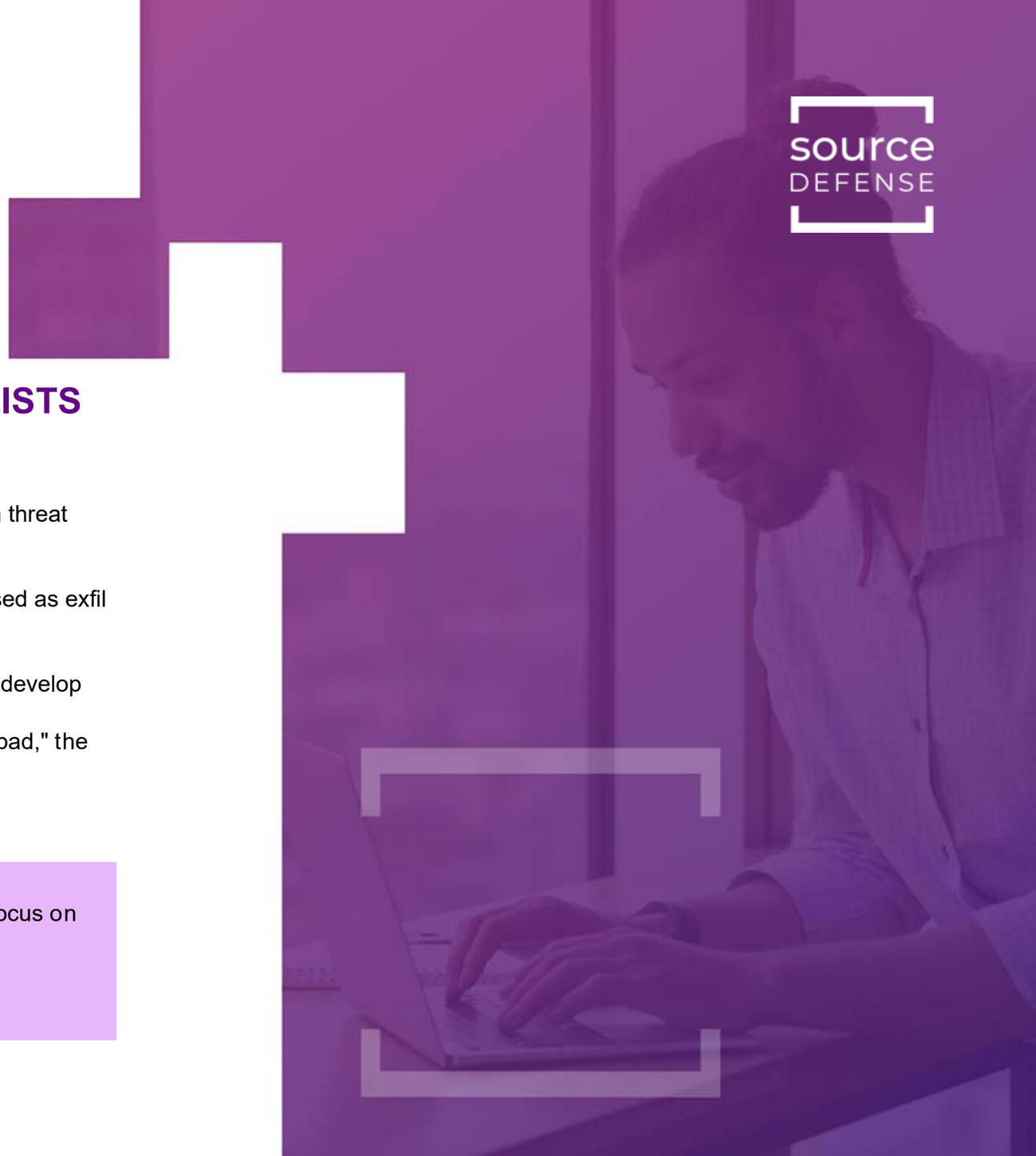
Coordinated domain switching patterns demonstrate sophisticated infrastructure management. Attackers rotate exfiltration domains rapidly across compromised sites simultaneously.

This reveals centralized command and control—not opportunistic individual compromises, but organized campaign operations.

WHY "KNOWN BAD" LISTS FAIL

- New domains appear faster than threat feeds update
- Legitimate services get repurposed as exfil endpoints
- Domain reputation takes time to develop
- By the time a domain is "known bad," the campaign has moved

SOC takeaway: Detect behaviors and new connection patterns, not just domains. Focus on anomalous outbound connections and data transmission patterns.



Issue # 2 – Compliance Scope the Misses the Scope of the Threat

Eskimming Occurs Site-Wide, Not Just on Payment Pages
Payment Page Focus = False Security

- Real-world attacks compromise **analytics, tag managers, personalization tools**, not payment forms

- Source Defense + Verizon research:
  - **129,897** scripts analyzed across 7,000+ merchant sites
  - **77,929** scripts running on non-payment pages (massive attack surface)
  - **51,968** scripts running on payment pages – with **17,002** accessing PII; **3,636** accessing payment data; **3,222** accessing credentials

- Visa's 2024 report: attackers increasingly compromise **non-payment infrastructure** first

- iFrames do NOT stop upstream compromise – site wide and parent page JavaScript remains exposed

Call to Action:
Shift PCI DSS from "payment page protection" to site-wide JavaScript governance

THE EVIDENCE IS CLEAR

2,000 forensic investigations involving eSkimming…

“In 100% of the cases where card data eSkimming occurred, the security failure was present on the merchants' referring page and not because of a malicious script on the third-party hosted payment page…”

SecurityMetrics – March 4, 2025

THE "PIZZA METHOD"

PAYMENT FLOW WEAPONIZATION

01

INJECT NEW PAYMENT OPTION

Malicious script adds a fake payment method to the checkout UI, appearing as the legitimate payment flow

02

FORCE GATEWAY REDIRECT

When selected, user is redirected to attacker-controlled "payment gateway" that mimics legitimate processor branding

03

CAPTURE FULL DETAILS

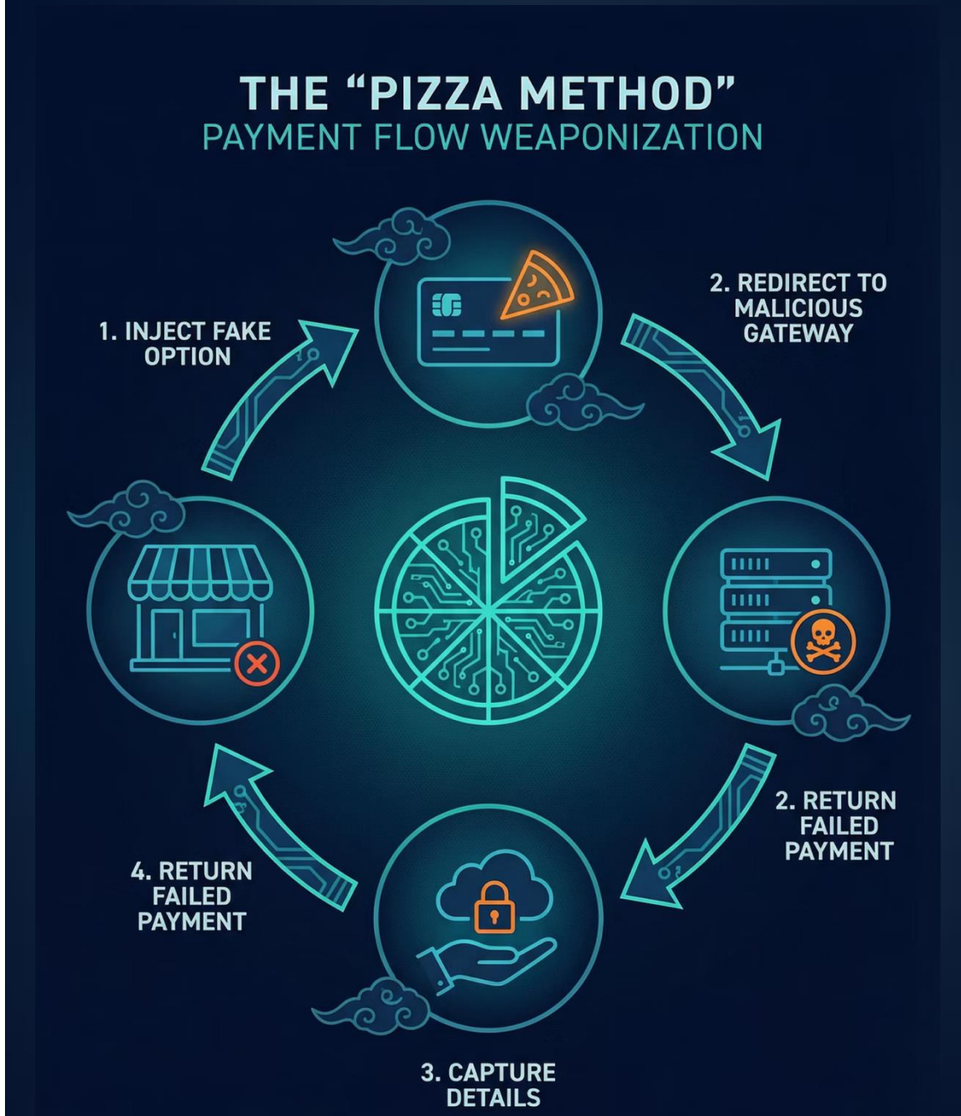
Fake gateway collects complete payment card details including CVV, presenting a convincing checkout experience

04

RETURN TO MERCHANT

After theft, user is redirected back with "payment failed" error, forcing them to retry with legitimate payment method

Critical: This should alarm payment page only and “we’re fine because we outsource the payment page" merchants who believe they're immune because payment processing happens off-site. The parent page UI is still exploitable.



Silent Skimming: The Invisible Threat

NO VISIBLE SIGNS

No popup, no overlay, no obvious form manipulation - yet payment data is still stolen. These attacks happen completely invisibly to the user

HOW IT WORKS

- Intercept form submissions via event listeners
- Stage captured data in cookies or localStorage
- Exfiltrate on later navigation events
- Leave no trace of form manipulation

source DEFENSE

Critical implication: "We did not see a fake form" is not proof of safety. Absence of visible indicators does not mean absence of compromise.

Detection requires monitoring all data exfiltration patterns and outbound connections, not just looking for visual form overlays.

source DEFENSE

DOUBLE-ENTRY OVERLAYS

Fake payment forms that overlay legitimate checkout flows - observed at industrial scale with hundreds of compromises per campaign.

HIGH BELIEVABILITY DESIGN

Overlays mimic legitimate payment provider interfaces with pixel-perfect accuracy. Users cannot distinguish fake from real without careful inspection.

DUAL DATA CAPTURE

Victims enter payment details twice: once in the fake overlay (captured by attacker), then again in the real form. The second entry ensures the transaction completes normally.

SCALE AND SOPHISTICATION

These aren't custom one-off attacks. Modular overlay kits target multiple payment providers with localized variants for different markets.

Issue # 3: Playing a Compliance Shell Game

SAQ-A Changes Created Compliance Confusion
Jan 2025 SAQ-A Revision Disrupted Merchant Readiness

- SAQ-A eligibility changed **two months** before enforcement deadline – politically driven / against an absolute outcry from the community
- Many merchants paused their compliance programs, believing controls no longer required
- Ostensibly done to make compliance easier for Level 3 & 4 Merchants (CORE targets of eSkimming attacks!)
- Demonstrated major problem with PCI Compliance Management – Huge number of Level 1 merchants use SAQ-A
- Confusion undermined uptake of eSkimming protections across the ecosystem

Call to Action:
Change SAQ-A and FAQ 1588 guidance; eliminate the compliance loophole game; de-emphasize the role of PSPs in eSkimming security

source DEFENSE

80 Members of the PCI Council's own eCommerce Guidance Taskforce + A Majority of QSAs Warned DO NOT DO THIS!!!

"As a QSA, we and many of our clients are confused and frustrated by this change to SAQ A only a few weeks before the future-dated requirement deadline. PCI SSC normally asks for stakeholder commentary on changes to help identify and clear up confusion, similar to what we have experienced for the past few weeks, before final publication. In this case, it's hard to understand why PCI SSC would remove requirements 6.4.3 and 11.6.1 from the SAQ…" TrustedSec

INDUSTRIAL SCALE OPERATIONS

INDUSTRIALIZED ESKIMMING-AS-A-SERVICE

MODULAR LOADER

Core injection framework deployed across compromised sites

INTERCHANGEABLE COMPONENTS

Tailored modules loaded based on target characteristics

GEO-TARGETED EXECUTION

Region and payment-provider specific payloads delivered dynamically

Modern eSkimming operates like commercial software-as-a-service platforms. Attackers deploy standardized loaders that call specialized modules optimized for specific:

- **Geographies:** Language, currency, regional payment methods
- **Payment providers:** Stripe, PayPal, Braintree, Adyen-specific overlays
- **Merchant platforms:** Magento, WooCommerce, Shopify variants

This isn't a collection of one-off injections - it's a scalable operating model with infrastructure investment, versioning, and maintenance cycles.

WEBSOCKETS: PERSISTENT, ADAPTIVE DELIVERY

REAL-TIME CODE DELIVERY

WebSocket connections enable live payload updates without page reloads. Attackers can adapt code on-the-fly in response to detection attempts or changing site conditions.

EVENT-BASED TRIGGERS

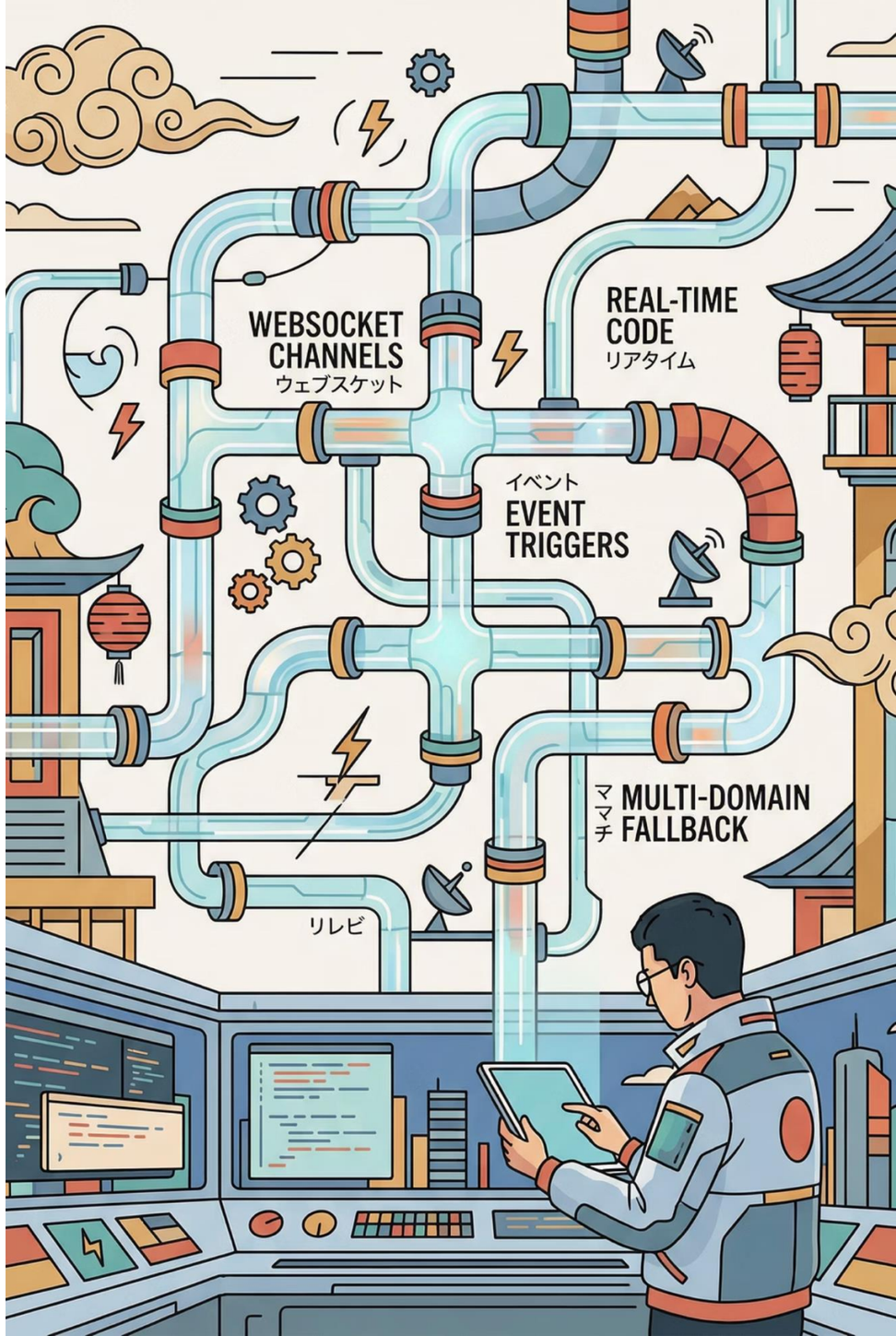
Scripts leverage onerror and onload patterns to establish fallback communication channels. If primary delivery fails, backup mechanisms activate automatically.

MULTI-DOMAIN FALLBACK

Persistent communication channels rotate through multiple domains and protocols. Blocking one connection doesn't stop the attack—another activates immediately.

Traditional HTTP/HTTPS monitoring misses WebSocket traffic entirely. Most security controls focus on request/response patterns and don't inspect persistent bidirectional connections.

Defense gap: WebSocket behavior requires dedicated monitoring and inspection separate from traditional web traffic analysis.



BELIEVABILITY AND TIMING

HOW CAMPAIGNS IMPROVE CONVERSION

LOCALIZATION

Overlays adapt to user language, currency, and regional payment norms. Forms display familiar logos, terminology, and field labels that match local expectations.

VERIFICATION DECEPTION

"Security verification" or "fraud prevention" messaging reduces suspicion. Users believe they're completing additional authentication required by their bank.

CONDITIONAL TRIGGERS

Overlays activate based on URL patterns, user paths, language settings, and targeting rules. Not every user sees the attack - selectivity avoids detection.

DUAL EXFILTRATION

Stolen data flows to both malicious infrastructure and compromised legitimate sites. Mixed exfil patterns complicate detection and attribution.

EXPANDING SCOPE

BEYOND CARDS: BROADER THEFT AND PERSISTENCE

CREDENTIAL AND PII HARVESTING

Attackers target registration, login, and account management flows—not just payment pages. Stolen credentials enable:

- Account takeover for future purchases
- Identity theft using complete profiles
- Credential stuffing across other services

PERSISTENCE MECHANISMS

Sophisticated campaigns establish long-term access:

- **Rogue admin accounts:** Backdoor access for re-compromise
- **Database manipulation:** Persistent code injection in CMS
- **Supply chain hooks:** Compromised plugins and dependencies

ANTI-FORENSICS TECHNIQUES

- **Test card detection:** Scripts identify security testing via common test card patterns and disable malicious behavior
- **Checksum manipulation:** Modify page integrity markers to hide presence from monitoring tools
- **Selective activation:** Only trigger on specific user agents, IPs, or session characteristics to evade sandboxes

DEFENSE REALITY CHECK

WHAT THIS BREAKS IN COMMON PCI COMPLIANT DEFENSES

CSP AND SRI LIMITATIONS

Content Security Policy and Subresource Integrity do not hold up against the methods used in eSkimming attacks. Trusted third-party compromises, first-party compromises, GTM container manipulation, and WebSocket channels often bypass these controls entirely.

PAYMENT-PAGE-ONLY FOCUS

Protecting only checkout pages misses upstream journey risk. Credential theft during login/registration, persistence mechanisms in admin panels, and staged data in earlier session steps all fall outside narrow payment-page scopes.

IFRAME HARDENING INSUFFICIENT

IFrame sandboxing and isolation techniques protect the payment form itself, but parent page context still matters. GTM running in parent can intercept pre-iFrame data, inject fake payment options, or manipulate the overall checkout flow.

2026 LOOK-AHEAD

MORE "AS-A-SERVICE" MODULAR OPERATIONS

Expect continued industrialization with better targeting, faster adaptation, and more sophisticated evasion techniques built into standardized frameworks.

INCREASED SUPPLY CHAIN TARGETING

Attackers will target shared dependencies, popular plugins, and upstream services to compromise multiple merchants simultaneously with single intrusions.

CONTEXT-AWARE FORM MANIPULATION

More adaptive overlays that respond to user behavior, device characteristics, and session context. Attacks will feel increasingly "native" to the genuine experience.

CREDENTIALS AND IDENTITY FOCUS

Continued shift beyond payment cards into account credentials, identity theft, and long-term access. Entire customer profiles become the target, not just transactions.

Thank you!