CYBER THREAT INTELLIGENCE

CRITICALSTART® Security Advisory

TLP CLEAR // [CS-SA-26-1101] Optimizely Malicious JavaScript

Executive Summary

The CRITICALSTART® Cyber Research Unit (CRU) is tracking OPTIMJACK, a client-side supply chain compromise in which an unauthorized party injected malicious JavaScript into customer projects on the Optimizely Web Experimentation platform on November 16, 2026.[1, 3, 4] Visitors to the websites of at least 178 organizations across banking, technology, retail, media, travel, and healthcare received a payload that swapped cryptocurrency wallet addresses, skimmed payment cards, stole cookies and page screenshots, and routed iPhone and iPad visitors to the Coruna and DarkSword iOS exploit kits.[1, 2] Optimizely confirmed an exploited vulnerability in Experimentation and states it is fixed.[3] OPTIMJACK is the third major third-party JavaScript compromise reported since late August 2026, following the Plerdy analytics and Polymarket incidents.[5, 7] Organizations that embed third-party scripts should verify what those scripts delivered, rotate exposed session tokens, and enforce a restrictive Content Security Policy (CSP). Critical Start Security Operations Center (SOC) has increased vigilance for malicious activity based on Appendix A indicators and Security Engineering is reviewing detection coverage for the threat.

Incident Overview

Optimizely Web lets customers run A/B tests by loading a JavaScript snippet on their pages. On November 16, that snippet carried attacker code for most of the day.[1] The OPTIMJACK campaign affected 178 organizations across 20 sectors, based on 188 affected snippets identified among 1,611 checked. Banking and finance organizations accounted for the largest share, with 32 affected entities, followed by the technology sector with 23. The campaign remained active between 04:21 and 21:52 UTC on November 16, 2026, with researchers identifying 26 different payload builds. Confirmed cryptocurrency theft reached approximately $7,040 by 19:25 UTC, while the total volume of stolen payment card details and browser cookies remains unknown. Optimizely confirmed the vulnerability and states it is fixed but has not disclosed its nature or how many projects were affected.[3, 4] Report URI links the actor to an earlier wave through other third-party scripts from November 13.[1] No public reporting connects OPTIMJACK to Optimizely's February 2026 voice-phishing incident.[14]

Attack Analysis

OPTIMJACK introduced no new techniques but chained five established threat categories into one delivery path, as summarized below:

1. **Web Supply Chain Attack:** The attacker wrote a loader into the Project JavaScript field of Optimizely customer projects, which runs on every page, and Optimizely's content delivery network (CDN) served it with its normal certificate.[1] Loader variants included a plain script tag for `1688360[.]cc/track.js`, a Base64-encoded copy that defeats string searches, and an inline `eval()` fallback. One snippet was reinfected after cleanup.[1]
2. **Client-Side Attack:** The payload ran only in visitors' browsers, so firewalls, file integrity monitoring, and code review had nothing to inspect. Of affected organizations assessed, 68 had no CSP and only 24 (15%) blocked the payload; policies that trusted the Optimizely host, used 'strict-dynamic', or allowed 'unsafe-eval' let it run.[1]

© 2026 Critical Start. All rights reserved.

3. **Magecart / E-Skimming:** A skimmer captured card number, expiry, and card verification value (CVV) from site-hosted forms; hosted payment iframes were out of reach. The script also took non-HttpOnly cookies and page screenshots.[1]
4. **Crypto-Clipping:** The payload replaced valid wallet addresses for eight cryptocurrencies in page text, forms, and the clipboard, earning about $7,040 in roughly nine hours.[1]
5. **Watering Hole Attack:** High-traffic news, retail, and finance sites put the payload in front of large audiences. On iPhones and iPads, a boot.js loader served Coruna (iOS 13 to 17) or DarkSword (iOS 18.x) in a hidden iframe.[1] Devices on iOS 18.6 or earlier reloaded the page every 60 seconds as the kit retried.[1] Cynet traced endpoint detection and response (EDR) alerts to the Optimizely resource; no physical device compromise has been confirmed.[2]

Relevant Vulnerability Context

The Optimizely vulnerability **has no** public Common Vulnerabilities and Exposures (CVE) identifier as of November 17, 2026.[3] However, the DarkSword chain served to iOS 18.x visitors relies on six patched vulnerabilities.[9, 10] Common Vulnerability Scoring System (CVSS) scores appear where published in the sources reviewed. Coruna, served to iOS 13 to 17 visitors, contains five chains and 23 exploits. The Cybersecurity and Infrastructure Security Agency (CISA) added three of its vulnerabilities (CVE-2021-30952, CVE-2023-41974, and CVE-2023-43000) to the Known Exploited Vulnerabilities catalog.[11]

CVE	CVSS	Description	Relevance
CVE-2025-31277	8.8	Processing maliciously crafted web content may lead to memory corruption; patched in iOS 18.6	DarkSword initial read/write primitive[9, 15]
CVE-2025-43529	8.8	A use-after-free issue was addressed with improved memory management; exploited as zero-day	DarkSword initial read/write primitive[10]
CVE-2025-14174	8.8	ANGLE memory corruption; exploited as zero-day	DarkSword WebKit stage[10]
CVE-2025-43510	7.8	Memory corruption issue addressed with improved lock state checking	DarkSword privilege escalation[10]
CVE-2025-43520	5.5	Memory corruption issue; patched in iOS 26.1 and 18.7.2	DarkSword privilege escalation[9]
CVE-2026-20700	7.8	Memory corruption issue; patched in iOS 26.3 after zero-day exploitation	DarkSword chain component[9]

MITRE ATT&CK Mapping

The mapping below, drawn from the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework, describes behaviors that are in scope:[5]

Technique	Name	Context
T1195.002	Supply Chain Compromise: Compromise Software Supply Chain	Loader injected into Optimizely customer projects and served to downstream sites
T1189	Drive-by Compromise	Visitors infected by loading affected pages; iOS chains delivered in hidden iframes
T1059.007	Command and Scripting Interpreter: JavaScript	track.js and boot.js executed in visitor browsers
T1592	Gather Victim Host Information	iOS version and device fingerprinting before exploit selection
T1203	Exploitation for Client Execution	Coruna and DarkSword WebKit and kernel exploit chains

© 2026 Critical Start. All rights reserved.

Technique	Name	Context
T1115	Clipboard Data	Clipboard monitoring for wallet addresses
T1565.002	Data Manipulation: Transmitted Data Manipulation	Wallet address replacement in outgoing requests and navigation
T1056.003	Input Capture: Web Portal Capture	Card number, expiry, and CVV capture from site forms
T1539	Steal Web Session Cookie	Exfiltration of non-HttpOnly cookies
T1113	Screen Capture	html2canvas rendering of the page
T1027	Obfuscated Files or Information	Base64-encoded loader and inline `eval()` fallback
T1041	Exfiltration Over C2 Channel	sendBeacon transfers to card.php and hit.php

Implications for Organizations

The OPTIMJACK campaign poses significant financial, operational, and reputational risks to organizations that rely on third-party JavaScript and website integrations. Malicious scripts can replace cryptocurrency wallet addresses, capture payment card details, and collect sensitive information entered through legitimate webpages, potentially exposing customers to financial theft and data breaches. The campaign also highlights third-party supply chain risks, as attackers can abuse trusted services such as Optimizely to inject malicious code without directly compromising an organization's primary infrastructure. Successful exploitation could damage customer trust, trigger regulatory investigations, and create potential compliance and breach notification obligations. Device-selective loading and conditional script execution further complicate detection and incident response, allowing malicious activity to remain hidden during routine security checks. Organizations should review third-party scripts and integrations, monitor suspicious DNS and browser connections, verify script integrity, and investigate potential exposure of customer and payment information.

Prioritized Mitigation Strategies

To improve your organization's security posture considering OPTIMJACK exploitation, CRU recommends the following:

Immediate (Within 24 Hours)

- Inspect Optimizely Project JavaScript, experiment code, and snippet history for `1688360`, `atob(`, `eval(`, and unfamiliar scripts; ask Optimizely which project IDs changed.[1, 4]
- Block Appendix A domains and subdomains at Domain Name System (DNS), web gateway, and endpoint controls.[2]
- Hunt DNS, proxy, and EDR telemetry from the last 30-60 days for Appendix A indicators.[1, 2]
- Rotate session tokens and secrets held in non-HttpOnly cookies on affected sites.[1]
- Identify users who accessed affected websites with mobile or PC during the exposure window. Investigate potential exposure of credentials, payment information, and cryptocurrency transactions. Notify affected users and coordinate payment card replacement or transaction monitoring where warranted.

Short-Term (Within Two Weeks)

- Audit write access to Optimizely and other tag platforms, rotate credentials, and enforce multi-factor authentication (MFA).[1]
- Treat card data entered in site-hosted forms within attack time frame as exposed.[1]
- Require managed iOS devices to run iOS 26.3.1 or 18.7.6 or later.[15]

© 2026 Critical Start. All rights reserved.

Structural

- Enforce a CSP with explicit `script-src` hosts, restrictive `connect-src`, no 'unsafe-eval', and reporting.[1]
- Keep non-essential third-party scripts off checkout and login pages, and capture cards only in hosted payment iframes.[1]
- Deploy client-side script integrity monitoring that alerts on changed script content and new data destinations, and add script providers to vendor risk reviews.

Conclusion

OPTIMJACK demonstrates how compromising a single trusted third-party provider can expose hundreds of organizations and their customers to financial theft, session hijacking, and potential mobile device exploitation. The campaign highlights the limitations of perimeter-based defenses when malicious code executes directly in users' browsers through legitimate website integrations. Organizations should treat third-party JavaScript as an extension of their attack surface, not an inherently trusted component. Reviewing historical script activity, revoking potentially exposed credentials, strengthening Content Security Policy enforcement, and continuously monitoring client-side script integrity are essential to reducing exposure. Ultimately, preventing similar incidents requires greater visibility and control over the external code organizations allow to execute on their websites.

For more threat reports, including PHP2SHELL visit Critical Start's Intel Hub. This advisory was written using the best intelligence available at the time and is subject to change as additional information becomes available.

What Critical Start is Doing

The CRITICALSTART® Cyber Research Unit (CRU) disseminated a brief of the threat as part of the 11-17-2026 CTI Update and is providing this Security Advisory as a follow up. The Critical Start Security Operations Center (SOC) has increased vigilance for malicious activity based on Appendix A indicators. Security Engineering is reviewing coverage for Appendix A indicators and evaluating hunting logic for Base64-encoded loaders served from trusted CDNs. CRU will continue to monitor the situation and work closely with the SOC and Security Engineering team to implement any relevant detections. Critical Start customers are encouraged to reach out to their Customer Success Managers or email support@criticalstart.com for any further enquiries.

© 2026 Critical Start. All rights reserved.

Further Reading

[1] Report URI (Nov. 16, 2026). World's Largest Brands Infected With Malware Via Optimizely. https://blog.report-uri.com/worlds-largest-brands-infected-with-malware-via-optimizely/

[2] Cynet (Nov. 17, 2026). OPTIMJACK: Malicious Web Injection Across CNN, Zoom, Salesforce, Fox and More. https://www.cynet.com/blog/optimjack-malicious-web-injection-across-cnn-zoom-salesforce-fox-and-more/

[3] Optimizely (Nov. 17, 2026). Web Experimentation Security Incident. https://status.optimizely.com/incidents/ftw0fh9wx43z

[4] Security Affairs (Nov. 17, 2026). OPTIMJACK: BBC, CNN and Zoom Among Targets of Optimizely Script Hijacking. https://securityaffairs.com/203289/malware/optimjack-bbc-cnn-and-zoom-among-targets-of-optimizely-script-hijacking.html

[5] BleepingComputer (Oct. 29, 2026). Polymarket Halts Trading After Crypto-Draining Script Breach, $2.5M Traced. https://www.bleepingcomputer.com/news/security/polymarket-halts-trading-after-crypto-draining-script-breach-25m-traced/

[6] Daily Security Review (Oct. 2026). Polymarket Halts Trading After Hacked DebugBear Script Drains Wallets. https://dailysecurityreview.com/?p=45171

[7] Security Affairs (Nov. 5, 2026). Russian APT29 Targets Mobile Users with Watering Hole Attacks. https://securityaffairs.com/202473/apt/russian-apt29-targets-mobile-users-with-watering-hole-attacks.html

[8] Trend Micro (Jan. 22, 2026). Watering Hole Attack Targets EmEditor Users With Information-Stealing Malware. https://www.trendmicro.com/en_us/research/26/a/watering-hole-attack-targets-emeditor-users.html

[9] Help Net Security (Mar. 19, 2026). DarkSword: Researchers Uncover Another iOS Exploit Kit. https://www.helpnetsecurity.com/2026/03/19/darksword-ios-exploit-iphone/

[10] Security Affairs (Mar. 19, 2026). DarkSword Emerges as Powerful iOS Exploit Tool in Global Attacks. https://securityaffairs.com/189662/hacking/darksword-emerges-as-powerful-ios-exploit-tool-in-global-attacks.html

[11] Help Net Security (Mar. 3, 2026). Coruna: Spy-Grade iOS Exploit Kit Powering Financial Crime. https://www.helpnetsecurity.com/2026/03/03/coruna-ios-exploit-kit/

[12] SecurityWeek (2026). Coruna iOS Exploit Kit Likely an Update to Operation Triangulation. https://www.securityweek.com/coruna-ios-exploit-kit-likely-an-update-to-operation-triangulation/

[13] ThreatCluster (Aug. 10, 2026). Coruna and DarkSword iOS Exploit Kits Targeting Users Globally (summarizing iVerify research). https://threatcluster.io/cluster/coruna-inside-the-nation-state-grade-ios-exploit-kit-we-ve-b-363e1b02

[14] UpGuard (Feb. 24, 2026). Overview: Optimizely Data Breach. https://www.upguard.com/news/optimizely-data-breach-2026-02-25

[15] SecurityWeek (Mar. 2026). DarkSword iOS Exploit Kit Used by State-Sponsored Hackers, Spyware Vendors. https://www.securityweek.com/darksword-ios-exploit-kit-used-by-state-sponsored-hackers-spyware-vendors/

© 2026 Critical Start. All rights reserved.

Appendices

Appendix A: Indicators of Compromise (IOC)

Type	Indicator	Notes
Domain	1688360[.]cc	Primary command and control (C2): track.js, card.php, hit.php, html2canvas.min.js[1, 2]
Path	hxxps://1688360[.]cc/track.js	Main payload; script.js also reported[2]
Path	hxxps://1688360[.]cc/card.php	Payment card exfiltration endpoint[1]
Path	hxxps://1688360[.]cc/hit.php	Cookie, screenshot, and swapped-address exfiltration[1]
Domain	5vobauua3ojpklx[.]icu	iOS exploit router serving boot.js; registered Nov. 9, 2026[1]
Domain	eil786npto9u5bq[.]icu	iOS router; Coruna and iOS 26 pages, including /JIUJIU888/weifile.html[1, 2]
Domain	l7bcsnwc7nzr3uo[.]icu	Coruna telemetry, POST /api/iptj[1]
Domain	webshell[.]lol	Injector get.js used in earlier wave[1]
Domain	linkforge[.]cc	Search engine optimization (SEO) panel script carrying the injector[1]
Domain	je4ft3gn8vxudum[.]icu, q1ls1ho9x7wsxlu[.]icu, ios-hack[.]icu	Fallback C2 hard-coded in boot.js[1]
Domain	p55abnw2pnsz0bo[.]icu, 1y69gy2mdzaltz1[.]icu, gm38duxoihbmy5o[.]icu	Share certificates and IPs with the kit[1]
IP	136.113.106[.]136	Hosts 1688360[.]cc[1, 2]
IP	34.96.213[.]201	Hosts 5vobauua3ojpklx[.]icu[1]
IP	34.87.36[.]58	Hosts eil786npto9u5bq[.]icu[1]
SHA-256	814a963c0da480e2449d9b6664480156e1cd6d731014117401bf635badec3a0f	track.js, 17:13 UTC build[1]
SHA-256	f7b84b9a94f749f8ced3f0112d0a66894e8bbc3b4aa5592021d1b8976a9bad40	track.js, 17:57 UTC build[1]
Artifact	window._k7, window.__k7b	Global markers set by payload[1]
Artifact	data-channel-code="02111110"; BIGNIAO	iOS loader script attribute; Coruna telemetry channel code[1]
Search string	1688360, atob(	Hunt strings for Project JavaScript and experiment code[1]

Do not block cdn.optimizely[.]com or its associated IP addresses. It is a legitimate delivery host observed in the chain, not attacker infrastructure.[2]

Attacker wallets:

Bitcoin `19g9rZcPeiz8rUvyWpTRyXXhPnjsWrc3kW`;

Ethereum and compatible chains `0xC4026b06D82b0F0B363eda0642D61CfbDc17884e`;

TRON `THvs6p56XkUiMkJeSc51cAP64u2RsTYqxa`;

Solana `FVtL8NMYS9PA1v3HE67XUGCtGA9JaZUvqav2fU2LrV5n`;

© 2026 Critical Start. All rights reserved.

TON `UQAgM1VqSZQiJLSG5w-ovurq5CZdxLEK3_7CMmwALTA5e09p`;

Litecoin `ltc1q3wp7g6ds0ggg6fl6kncpa4sepn0q3qfacgred5`;

Bitcoin Cash `qzkaaf8n6grmpr0d9lx8xutn3r9lk722f566hhpe58`;

Dogecoin `DBEGrxRF7KMSuhTS4c1MFviStU6efdMnu5`.

© 2026 Critical Start. All rights reserved.