Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

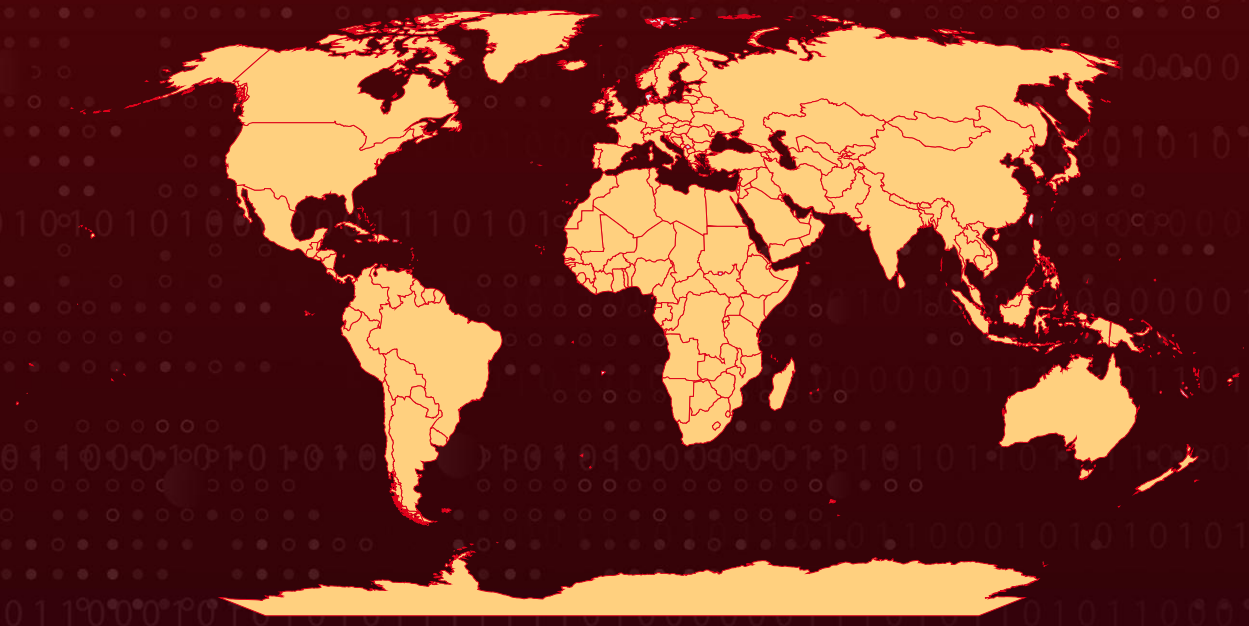
OPTIMJACK: Optimizely Web Supply-Chain Attack

Date of Publication	Admiralty Code	TA Number
November 18, 2026	A1	TA2026342

Summary

First Seen: November 16, 2026
Targeted Regions: Worldwide
Targeted Platforms: Web browsers, iOS (iPhone/iPad)
Targeted Products: Optimizely Web
Targeted Industries: Banking & Finance, Technology & SaaS, Retail & Fashion, Streaming & Entertainment, News & Media, Airlines & Travel, Healthcare & Pharma, Industrial & Manufacturing, Telecoms, Crypto & Trading, Insurance, Real Estate, Food & Hospitality, Smart Home, Nonprofit, Gambling, Professional Services, Logistics, Automotive, Education
Campaign Name: OPTIMJACK
Malware: JavaScript Kit (track.js (clipper/skimmer))
Attack: On November 16, 2026, an unattributed actor gained write access to the Project JavaScript field of Optimizely Web customer projects and injected a loader into 188 snippets belonging to 178 organisations, including Zoom, the BBC, CNN, Salesforce, GitLab, IKEA, HSBC, Equifax and Ledger. Served from the trusted cdn.optimizely.com host, the loader pulled a multi-purpose JavaScript kit (track.js) that swapped cryptocurrency wallet addresses, skimmed payment cards, stole cookies and page screenshots, and delivered the Coruna and DarkSword exploit chains to iPhone and iPad visitors. Roughly $7,040 in cryptocurrency was confirmed stolen before most snippets were cleaned the same evening.

Attack Regions



Attack Details

#1 Visitors to the websites of 178 organisations were served attacker code from a source their browsers already trusted: Optimizely's own CDN. The attacker planted it in the Project JavaScript field of Optimizely Web snippets, which runs on every page of a customer's site.

#2 Optimizely confirmed the attacker gained write access by exploiting a vulnerability in its public-facing Experimentation account signup process, since patched. Delivered under Optimizely's own certificate, the code loaded as trusted content on every affected site.

#3 The first injection appeared on November 16, 2026 in the BBC's snippet. The same actor had used this injector before, against Turkish websites since September and in an earlier November wave through other third-party marketing and media scripts.

#4 Three loader variants delivered the payload, including an encoded copy and an inline fallback designed to run even when the attacker's server was blocked. The payload was rebuilt 26 times during the day, and snippets that were cleaned were re-infected.

#5 Once loaded, the kit replaced cryptocurrency wallet addresses across eight blockchains in page text, forms, the clipboard and outgoing requests. A card skimmer also captured complete card details from payment forms; hosted payment iframes such as Stripe and Adyen were out of reach.

#6 On iPhones and iPads, the script loaded iOS exploit chains in a hidden iframe, choosing the chain by iOS version. From late afternoon, devices on older iOS versions were targeted directly, with pages reloading every 60 seconds to retry exploitation.

#7 Infected snippets reached 188 across 178 organisations in finance, retail, media, telecoms, crypto and other sectors. Content Security Policy rarely helped: of 256 affected hosts, only 24 blocked the payload outright, as common policy settings let the code run.

#8 The kit sent stolen data, including cookies, wallet addresses and page screenshots, to the attacker's server. The attacker's wallets received about $7,040 before a mass clean-up that evening, after which only one organisation's snippet remained infected.

Recommendations

Audit Optimizely Code: Review the Project JavaScript and the custom code of every experiment across all Optimizely Web projects, and remove any script your team did not write.

Lock Down Optimizely Access: Remove unneeded users, API tokens and integrations with write access, rotate the remaining credentials, and enforce MFA for every dashboard user.

Block and Hunt for Campaign Activity: Block the attacker infrastructure listed in the IoC section, and search proxy, DNS and web logs for connections to it from November 16 onward.

Contain Data Exposure: Treat cards entered in first-party forms on November 16 as compromised, invalidate sessions held in non-HttpOnly cookies, and advise users to verify recent crypto transfers.

Patch iOS Devices: Update managed iPhones and iPads to iOS 18.7.3 or 26.3 or later, starting with devices that browsed affected sites on November 16, and check them for signs of compromise.

Restrict Scripts and Card Entry: Deploy a Content Security Policy with strict script and connect allowlists, remove 'unsafe-eval' and 'unsafe-inline', and collect cards through hosted payment iframes.

Monitor Third-Party Scripts: Fingerprint third-party scripts, alert on changes or new data destinations, and require change alerts, audit logging and MFA from tag and experimentation vendors.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
	T1608: Stage Capabilities	T1608.004: Drive-by Target
Initial Access	T1195: Supply Chain Compromise	T1195.002: Compromise Software Supply Chain
	T1190: Exploit Public-Facing Application	
	T1189: Drive-by Compromise	
Execution	T1059: Command and Scripting Interpreter	T1059.007: JavaScript
	T1203: Exploitation for Client Execution	
Defense Evasion	T1027: Obfuscated Files or Information	
	T1140: Deobfuscate/Decode Files or Information	
Discovery	T1082: System Information Discovery	
Credential Access	T1539: Steal Web Session Cookie	

Tactic	Technique	Sub-technique
Collection	T1056: Input Capture	T1056.003: Web Portal Capture
	T1113: Screen Capture	
	T1115: Clipboard Data	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1008: Fallback Channels	
Exfiltration	T1041: Exfiltration Over C2 Channel	
Impact	T1565: Data Manipulation	T1565.002: Transmitted Data Manipulation
		T1565.003: Runtime Data Manipulation
	T1657: Financial Theft	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	814a963c0da480e2449d9b6664480156e1cd6d731014117401bf635badec3a0f, f7b84b9a94f749f8ced3f0112d0a66894e8bbc3b4aa5592021d1b8976a9bad40
Domain	1688360[.]cc, 5vobauua3ojpklx[.]icu, eil786npto9u5bq[.]icu, l7bcsnwc7nzr3uo[.]icu, webshell[.]lol, linkforge[.]cc, je4ft3gn8vxudum[.]icu, q1ls1ho9x7wsxlu[.]icu, ios-hack[.]icu, p55abnw2pnsz0bo[.]icu, 1y69gy2mdzaltz1[.]icu, gm38duxoihbmy5o[.]icu
IPv4	136[.]113[.]106[.]136, 34[.]96[.]213[.]201, 34[.]87[.]36[.]58
URL	hxxps[:]//1688360[.]cc/track[.]js, hxxps[:]//1688360[.]cc/card[.]php, hxxps[:]//1688360[.]cc/hit[.]php, webshell[.]lol/get[.]js
Filename	track.js, boot.js, get.js, card.php, hit.php
HTTP Request	POST /api/iptj

TYPE	VALUE
Bitcoin Address	19g9rZcPeiz8rUvyWpTRyXXhPnjsWrc3kW
Ethereum/EVM Address	0xC4026b06D82b0F0B363eda0642D61CfbDc17884e
TRON Address	THvs6p56XkUiMkJeSc51cAP64u2RsTYqxa
Solana Address	FVtL8NMYS9PA1v3HE67XUGCtGA9JaZUvqav2fU2LrV5n
TON Address	UQAgM1VqSZQiJLSG5w-ovurq5CZdxLEK3_7CMmwALTA5e09p
Litecoin Address	ltc1q3wp7g6ds0ggg6fl6kncpa4sepn0q3qfacgred5
Bitcoin Cash Address	qzkaaf8n6grmpr0d9lx8xutn3r9lk722f566hhpe58
Dogecoin Address	DBEGrxRF7KMSuhTS4c1MFviStU6efdMnu5
JavaScript Global Marker	window._k7, window.__k7b
HTML Attribute	data-channel-code="02111110"
Channel Code	BIGNIAO

Affected Websites

https://www.zoom.com
https://zoom.us
https://www.bbc.com
https://www.bbc.co.uk
https://www.cnn.com
https://www.foxnews.com
https://pardot.com
https://exacttarget.com
https://evergage.com
https://salesforce-scrt.com
https://gitlab.com
https://about.gitlab.com
https://client.home-design.ikea.com
https://asos.com
https://www.us.hsbc.com
https://www.hsbc.com.hk
https://www.hsbc.com.mx
https://www.insurance.hsbc.com.sg
https://www.hsbc.com.au
https://www.hsbc.ae
https://www.hsbc.com.my
https://www.hsbc.com.tw
https://www.hsbc.com.vn
https://www.hsbc.com.eg
https://www.hsbc.com.ph
https://www.equifax.com
https://my.equifax.com
https://wwws.airfrance.fr
https://russia.airfrance.com
https://www.klm.be
https://liberia.klm.com
https://www.alaskaair.com
https://www.peacocktv.com
https://www.virginmediao2.co.uk
https://www.vodafone.com.au
https://www.ledger.com
https://www.ig.com
https://www.oanda.com

https://help.smartsheet.com
https://www.talktalk.co.uk
https://optimizely.com
https://login.optimizely.com

References

https://blog.report-uri.com/worlds-largest-brands-infected-with-malware-via-optimizely/

https://unit42.paloaltonetworks.com/optimjack-supply-chain-attack/

https://status.optimizely.com/incidents/ftw0fh9wx43z

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

November 18, 2026 • 01:30 PM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com