

D9: Off-chain attacks

Server vulnerabilities

Complex software runs all blockchains

- Too large to formally verify full node, all contracts are vulnerable from underneath
 - e.g. formally verified contracts can **still** be subverted if security assumptions of infrastructure running them are broken

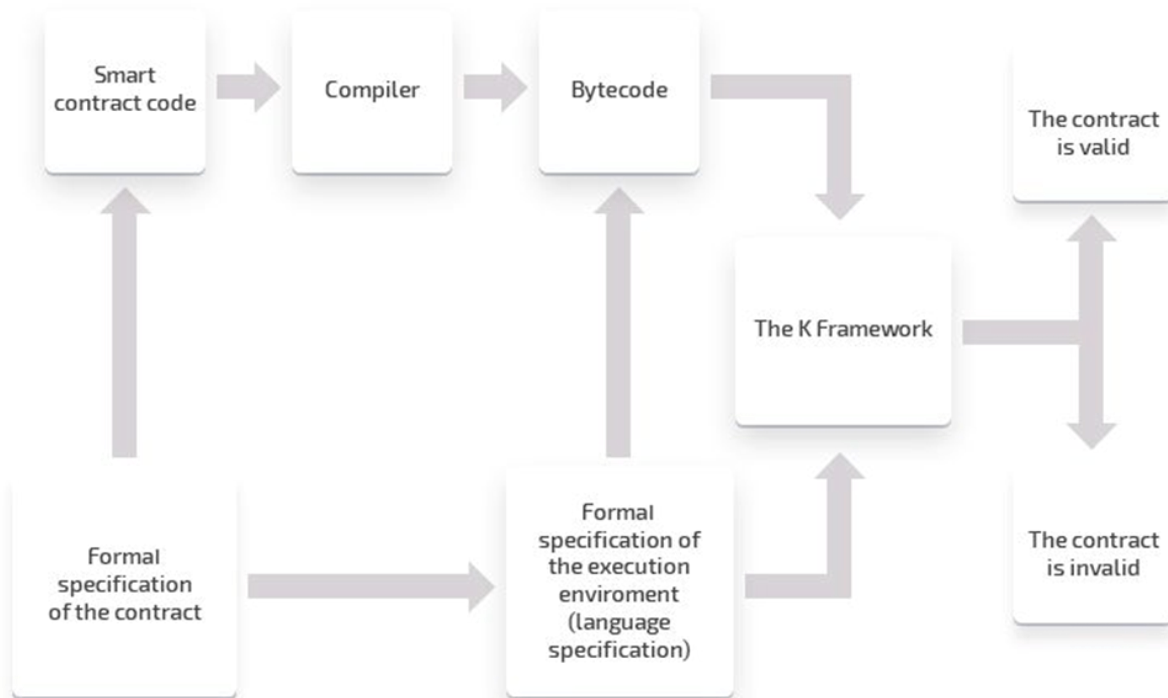
\$1.1 Million: Malicious Miner
Exploits Verge Network for
Seven-Figure Payday

 Josiah Wilmoth  05/04/2018  Altcoin News.

- Miner exploits the network's mining algorithm implementation to obtain \$1.1M (20M XVG)

Remediation

- Memory-safe languages
 - `geth` (Go Ethereum), `parity`, `lighthouse` (Rust Ethereum)
- Formally specified virtual machines and languages
 - Cardano (KEVM, IELE)
- [Formal verification](#) of EVM
- [Formal verification](#) of smart contracts



Supply-chain attacks

Poison software used

- Attack web3 . js front-end code
- Attack Javascript packages wallets use
- Example (11/2018)

NPM dependencies, supply chain attacks, and Bitcoin wallets

Posted by [Ksenia Peguero](#) on Friday, November 30th, 2018

- EventStream, a highly popular JavaScript library used in wallets
 - Downloaded 2 million times per week, but not maintained from 2012-2018
- Original owner transfers project ownership to a volunteer to maintain
- New owner is malicious
 - Adds a dependency to flatmap-stream a little-known library that had no downloads on NPM
 - Malicious code added to flatmap-stream to enable Bitcoins to be stolen from wallets using EventStream

- Trojan wallet software (11/2019)
 - 14-hour window of compromise
 - Attack grabs release code, adds code to steal keys, and uploads to compromised site for users to download

Official Monero website compromised with malware that steals funds

Official Linux CLI binary for the Monero cryptocurrency compromised with malware that steals users' funds.



By [Catalin Cimpanu](#) for [Zero Day](#) |
November 19, 2019 -- 17:08 GMT (09:08
PST) | Topic: [Security](#)



Linux, 64-bit

Linux, 64-bit

Current Version: 0.14.1.0 Carbon Chamaeleon

SHA256 Hash (GUI):

```
51739f0472ccbd49832a5828ca1000ebb1ce63b19d  
d57507b7905739bf8cf238
```

Linux, 64-bit Command-Line Tools Only

Current Version: 0.15.0.0 Carbon Chamaeleon

SHA256 Hash (CLI):

```
53d9da55137f83b1e7571aef090b0784d9f04a9801  
15b5c391455374729393f3
```

Remediation

- Monitor and validate your software supply chain
- Reduce dependencies
- Philosophical question: To patch or not to patch?
 - Similar to WannaCry vs CCleaner
 - Patch if you can trust the source (fix vulnerabilities)
 - Don't patch if you can't trust the source (avoid supply-chain attacks)
 - Increasingly, in a package-driven world, you might not want to!

Attacks on exchanges, hot-wallets

Mt. Gox (2014)

- Founded in 2010
- Handled 70% of all BTC transactions at its peak in "hot" wallets
 - e.g. Mt. Gox stores private keys for wallets, connected to the Internet to perform transactions on behalf of its users
- Service compromised in 2011
 - Attackers break into computer of an auditor of Mt. Gox
 - Change BTC pricing to a penny
- Compromised again in 2014 (causing bankruptcy)
 - Obtained the private keys of Mt. Gox clients to generate transactions
 - At the time, all [crypto assets were kept in hot wallets](#)
 - Total value consisted of a massive \$460 million worth of Bitcoin at the time (\$17 billion at 2019 levels)

Coincheck (1/2018)

FINANCE • CRYPTOCURRENCY

How to Steal \$500 Million in Cryptocurrency



Early Friday morning in Tokyo, hackers broke into a cryptocurrency exchange called Coincheck Inc. and made off with nearly \$500 million in digital tokens.

"The company did own up to a security lapse that allowed the thief to seize such a large sum: It kept customer assets in what's known as a **hot wallet**, which is connected to external networks."

Binance (5/2019)

- From earlier discussion on 'reorg'
- 7th largest crypto exchange in 5/2019
 - <https://coinmarketcap.com/exchanges/binance/>
- Attack against high-value users to obtain account credentials on exchange

BRIAN BARRETT SECURITY 05.08.19 01:20 PM

HACK BRIEF: HACKERS STOLE \$40 MILLION FROM BINANCE CRYPTOCURRENCY EXCHANGE

- 7,000 BTC stolen (~\$40 million)
- 2FA codes and API tokens stolen
- CEO of Binance – "The hackers used a variety of techniques, including **phishing, viruses and other attacks**...It appears that hackers were able to compromise several high-net-worth accounts, whose bitcoin was kept in Binance's so-called **hot wallet**—which, unlike cold wallets, are connected to the internet—and filch those funds in a single transaction."
- "The bad news is, if your bitcoin was in Binance's hot wallet, it now belongs to bad guys."

Remediation

- Use hardware wallets
 - Exchanges now support transactions that must be signed by a hardware wallet the user carries
 - But now a single-point of failure (loss of wallet means loss of all \$ associated with it)
- Use hardware tokens to authenticate hot wallets
 - Binance CEO on 5/10/2019 after \$40M heist
 - "The company plans to give away 1,000 YubiKeys when the feature goes live"
 - U2F, FIDO2 security keys with better security than traditional 2FA
 - <https://bit.ly/pdx-yubi>
- Use cold wallet storage
 - Use exchanges that keep a majority of customer deposits in cold wallets
 - Keys kept offline (e.g. in a bank vault)
- Use multi-signature wallets
 - Require multiple sign-offs before funds can be moved
 - Adversary must compromise multiple wallets to transact

Weak or leaked keys

Improper use of crypto in wallets

- Software that doesn't appropriately manage randomness used in digital signatures allowing cryptanalysis to reveal private key

ACADEMIA

Researchers Find Vulnerability for Bitcoin, Ethereum, and Ripple Digital Signatures in Faulty Implementations



Mitchell Moos · Jan 11, 2019 · 4 min read



- Wallets generating cryptographic signatures on Bitcoin, Ethereum, and Ripple with flaw allowing attackers to calculate private keys and, consequently, steal any crypto in that wallet.
- Hundreds of Bitcoin private keys and dozens of Ethereum, Ripple, SSH, and HTTPS private keys vulnerable to this unique form of cryptanalytic attack
- <https://eprint.iacr.org/2019/023.pdf>

Improper key generation

- Key generation algorithm configured with insufficient entropy (allows private keys to be easily guessed)

Blockchain.info Security Disclosure

By Blockchain Team · December 08, 2014

When making a scheduled software update overnight to our web-wallet, our development team inadvertently affected a part of our software that ensures private keys are generated in a strong and secure manner.

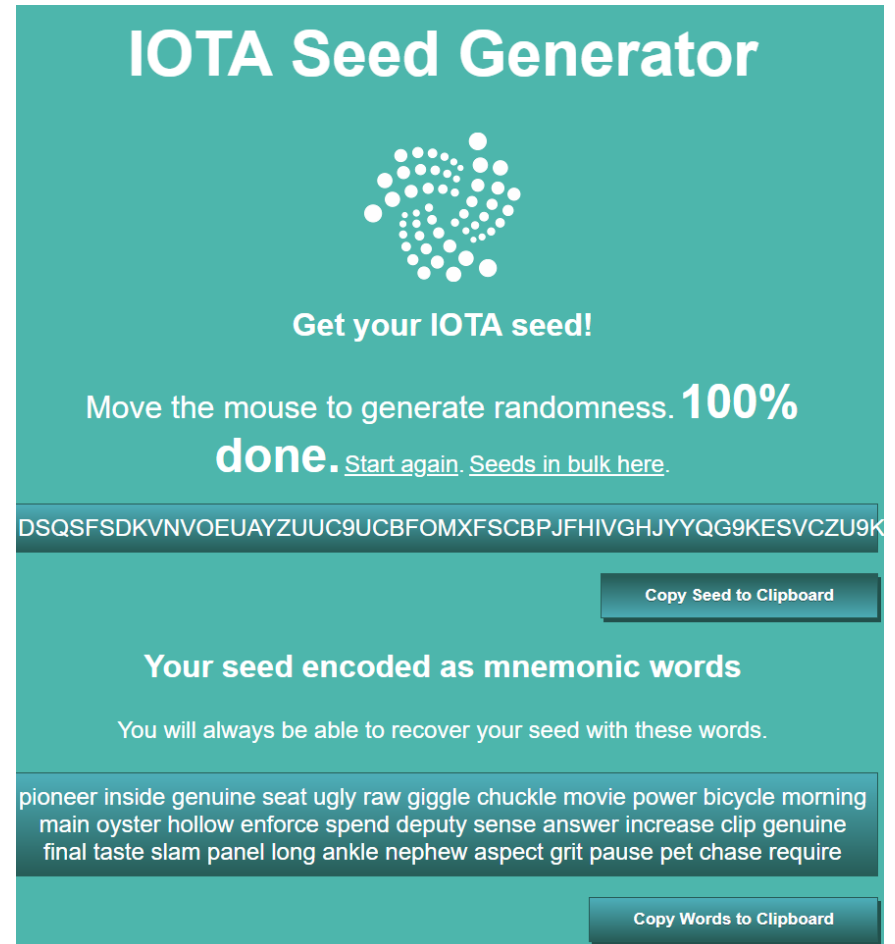
The issue was present for a brief period of time between the hours of 12:00am and 2:30am GMT on December the 8th 2014. **The issue was detected quickly and immediately resolved. In total, this issue affected less than ****0.0002% of our user base and was limited to a few hundred addresses. **

Fake key generation sites

- IOTA wallets (2018)
How a malicious seed generation website stole \$4 million

© Published January 28, 2018

- Phishing site masquerading as a legitimate site for generating unique cryptographic seeds for IOTA wallets
- Stores seeds instead to cashout wallets that used it



The screenshot shows a teal-colored web interface for a 'IOTA Seed Generator'. At the top, the title 'IOTA Seed Generator' is displayed in white. Below the title is a circular logo composed of white dots. The main text reads 'Get your IOTA seed!' followed by 'Move the mouse to generate randomness. **100% done.** [Start again.](#) [Seeds in bulk here.](#)'. Below this is a dark teal bar containing a long alphanumeric seed string: 'DSQSFSDKVNVOEUAYZUUC9UCBFOMXFSCBPJFHIVGHJYYQG9KESVCZU9K'. A button labeled 'Copy Seed to Clipboard' is positioned to the right of the seed string. Below the seed string, the text 'Your seed encoded as mnemonic words' is shown, followed by 'You will always be able to recover your seed with these words.' Below this is another dark teal bar containing a list of mnemonic words: 'pioneer inside genuine seat ugly raw giggle chuckle movie power bicycle morning main oyster hollow enforce spend deputy sense answer increase clip genuine final taste slam panel long ankle nephew aspect grit pause pet chase require'. A final button labeled 'Copy Words to Clipboard' is located at the bottom right of the interface.

- WalletGenerator.net (5/2019)
 - The site has been using a coding sleight of hand to generate private keys that are suspiciously trivial for the operators to guess...

RED FLAG —

Website for storing digital currencies hosted code with a sneaky backdoor

WalletGenerator.net and the mystery of the backdoored random number generator.

DAN GOODIN - 5/25/2019, 5:45 AM

- ...leaving all funds stored in the wallets open to theft.

Leaked private key in source repository

Hacker steals \$1,200 worth of Ethereum in under 100 seconds

Malicious bots are scanning GitHub uploads for private crypto keys and seed phrases.

By [Liam Frost](#)

3 min read · May 27, 2020

- Seed phrase accidentally left in a GitHub upload.
 - Immediately scanned by malicious bots that monitor code commits.
 - Less than two minutes before attackers siphoned the funds.

Comedy bug: Leaking private key in spellchecker

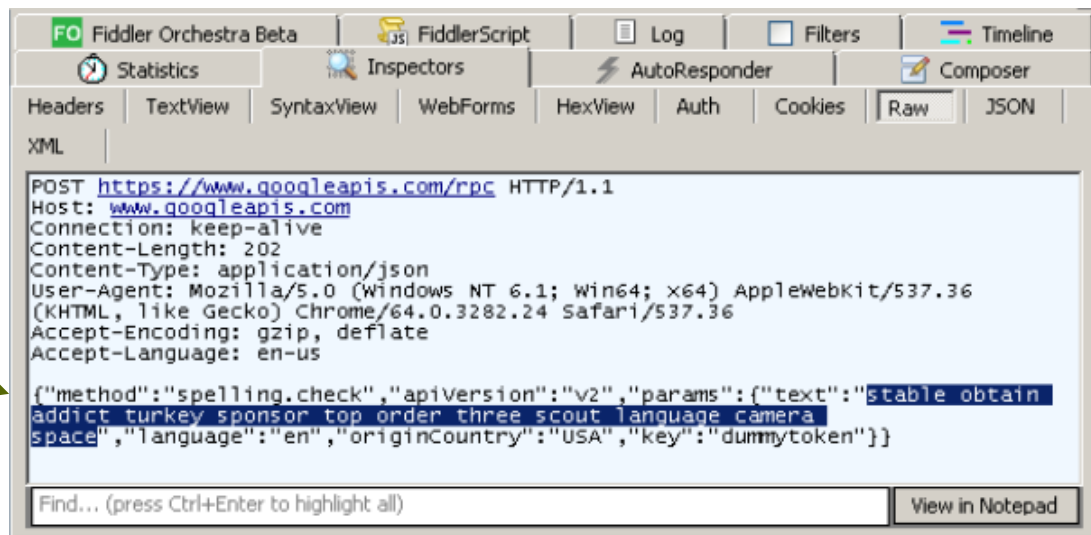
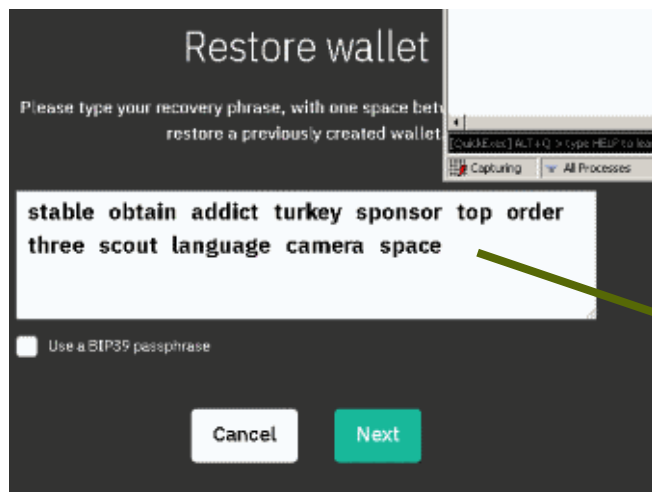


Cryptocurrency wallet caught sending user passphrases to Google's spellchecker



By Catalin Cimpanu for Zero Day | February 27, 2019 -- 17:23 GMT (09:23 PST) | Topic: Security

The issue came to light yesterday after an angry write-up by Oman-based programmer [Warith Al Maawali](#) who discovered it while investigating the mysterious theft of 90 percent of his funds.



Phishing users

Spoofing Ethereum addresses

- Modify a company's advertised Ethereum address off-chain (e.g. replace address on web page)
 - Coindash ICO (\$7M in ETH lost)



Token Sale Site Security Breach

This is an emergency message delivered to you in order to stop you from sending your money to an unauthorized ETH address

It seems like our Token Sale page was tempered and the sending address was changed. Please stop from sending your funds to any of the addresses until we say otherwise.

Warning! There are reports that the Coindash Crowdsale address has been compromised.



Overview | FAKE_Coindash



Misc

Tools

ETH Balance: 43,438.455089113668079212 Ether

ETH USD Value: \$7,607,811.02 (@ \$175.14/ETH)

No Of Transactions: 2130 txns

Address Watch

Add To Watch List

Token Tracker

View Token Balances

1

Transactions

Internal Transactions

Token Transfers

Comments

Latest 25 txns from a total Of 2130 transactions (+1 PendingTxn)

View All

TxHash	Block	Age	From		To	Value	[Tx Fee]
0x2162b224ef2fe2b...	(pending)	1 hr 33 mins ago	0x84c08128311877...	IN	0x6a164122d5cf7c8...	39.99 Ether	(pending)
0x905647c5c2efd29...	4035258	3 hrs 41 mins ago	0x61e0b020c77f965...	IN	FAKE_Coindash	2.992 Ether	0.000021
0xea8d1f2e28e0c2b...	4035239	3 hrs 48 mins ago	0xdf201a0d03d6c15...	IN	FAKE_Coindash	2.5 Ether	0.000021
0x386467a7c169dd0...	4035125	4 hrs 22 mins ago	0xa647d8f486d5341...	IN	FAKE_Coindash	0.17 Ether	0.000798
0x7d70b5c45eb07ef...	4035071	4 hrs 40 mins ago	0xfad1dc72590bf3f8...	IN	FAKE_Coindash	2 Ether	0.000021

Spoofing legitimate sites

Fraudsters Spoof Blockchain.com to Steal \$27M in Cryptocurrency

By [Ionut Ilascu](#)



June 27, 2019



11:24 AM



0

- 6/2019

"Law enforcement agencies in Europe arrested a group of six individuals for emptying cryptocurrency wallets of at least 4,000 victims by setting up a website that impersonated Blockchain.com."

- Typosquatting combined with advertisements placed using Google AdWords to lure victims

Bitcoin Wallets Block Explorer - Get Your Online Wallet Today

Ad www.blokchien.info/wallet ▼

Start Yours Today

How Blockchain Works - IBM Think Academy - ibm.com

Ad www-01.ibm.com/blockchain ▼

See **Blockchain** in Action In This IBM Think Academy Video. Watch Now!

block-clain.info - Wallet from Block Chain - Free, simple, secure and safe

Ad www.block-clain.info/ ▼

Discover the world's most popular wallet.

Blockchain

<https://www.blockchain.com/> ▼



BLOCKCHAIN

Welcome Back!

or [Sign Up](#)

Sign in to your wallet below

Wallet ID

Find the login link in your email, e.g. [blockchain.info/wallet/1111-222-333](#)... The series of numbers and dashes at the end of the link is your Wallet ID.

Password

LOG IN

[Log in via Mobile](#)

Having some trouble? [View Options](#)



[DATA](#)

[ABOUT](#)

[BLOG](#)

[SUPPORT](#)

Remediation

- Password managers, 2FA
- U2F, FIDO2 authentication
- Multi-signature wallets for high-value accounts

Network vulnerabilities

DNS rebinding

- Wallet software running on local interface (e.g. `geth`'s JSON RPC interface)
 - Connections only from local machine allowed
- User goes to a malicious web site "evil.com"
 - Loads DNS entry for "evil.com" that has a short TTL
 - Upon loading, "evil.com" quickly rebinds site DNS record to point to local interface (127.0.0.1) to allow access to internal process housing wallet (e.g. `geth`'s JSON RPC interface)
 - User attempts to load embedded objects on "evil.com"
 - Is redirected to local interface
 - If interface written to not require continual reauthentication per request, attacker gets unauthenticated JSON-RPC access (and complete control) over your wallets

MARCH 11, 2018 BY ARMIN DAVIS

Ethereum clients found to be vulnerable to DNS rebind attack

rebinddns.ml

rebinddns.ml

This is the PoC of Geth DNS Rebinding

Click the button Below to Start

Start

Wait 00:09

An embedded page at w17dejx8iiks53xr.etherclient.ml: 8545 says:
Found 1 ether accounts
0xc22668da781f01ffd537a7cba7eff4e6fcddcc79 --> 0

OK

Example

- Accessing unlocked private keys

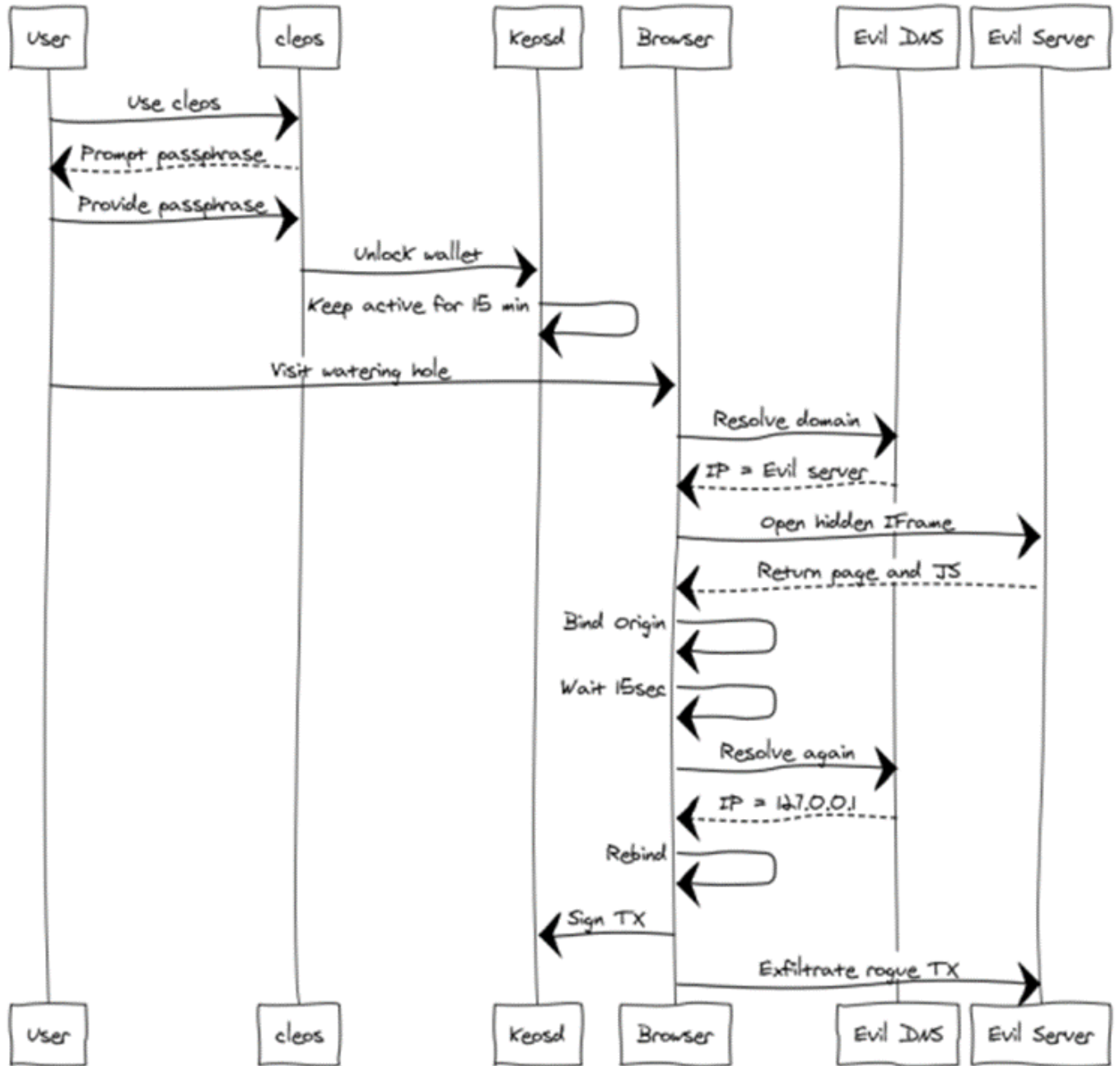
The call is coming from inside the house —
DNS rebinding in EOSIO keosd wallet



François Proulx

Jul 19, 2018 · 6 min read

KEOSD DNS Rebinding attack



- Normal operation
 - Wallet's keys unlocked and displayed after correct password given
 - Access allowed for 15 minutes without a password
- DNS rebinding attack within 15 minutes displays keys
 - Wallet software returns 404 on rest of the page assets

The image shows a browser window on the left and a terminal window on the right. The browser window displays a modal dialog with the following text:

```
...time.127.0.0.1.20time.repeat.rebind.network:
8900 says
EOS6MRyAjQq8ud7hVNYcfnVPJqcVpscN5So8BhtHuGYqET5GDW5CV
```

The terminal window shows the following commands and output:

```
1: fproulx@iridium:~/projects/hackerone/eosio/dns-rebind
d_handler ] add api url: /v1/wallet/unlock
2346565ms thread-0 http_plugin.cpp:201 ha
ndle_http_request ] 404 - not found: /
2346615ms thread-0 http_plugin.cpp:201 ha
ndle_http_request ] 404 - not found: /favicon.ico
[]

2: fproulx@iridium:~/projects/hackerone/eosio/dns-rebind
[dns-rebind ]$ cat wallet.passphrase |pbcopy
[dns-rebind ]$ ./cleos wallet unlock
password: Unlocked: default
[dns-rebind ]$ ./cleos wallet keys
[
  "EOS6MRyAjQq8ud7hVNYcfnVPJqcVpscN5So8BhtHuGYqET5GDW
5CV"
]
[dns-rebind ]$ []
```

The browser's Network tab shows the following requests:

Name	Method	Status	Schema	Domain	Type	Initiator	Size	T	Waterfall
a.35.203.53.123.1t...	GET	200	http	a.35.203.53.123.1t...	docu...	Other	485 B	95	
favicon.ico	GET	404	http	a.35.203.53.123.1t...	text/...	Other	386 B	21	
get_public_keys	POST	200	http	a.35.203.53.123.1t...	fetch	index.c6	174 B	16	

DNS Hijacking



Ethereum's Original Wallet

- MyEtherWallet.com (MEW)
- Lots of \$, enormous target for exploitation (4/2018)

Security

AWS DNS network hijack turns MyEtherWallet into ThievesEtherWallet

Audacious BGP seizure of Route 53 IP addys
followed by crypto-cyber-heist

By Shaun Nichols in San Francisco 24 Apr 2018 at 19:04

42 SHARE ▼

≡ Forbes



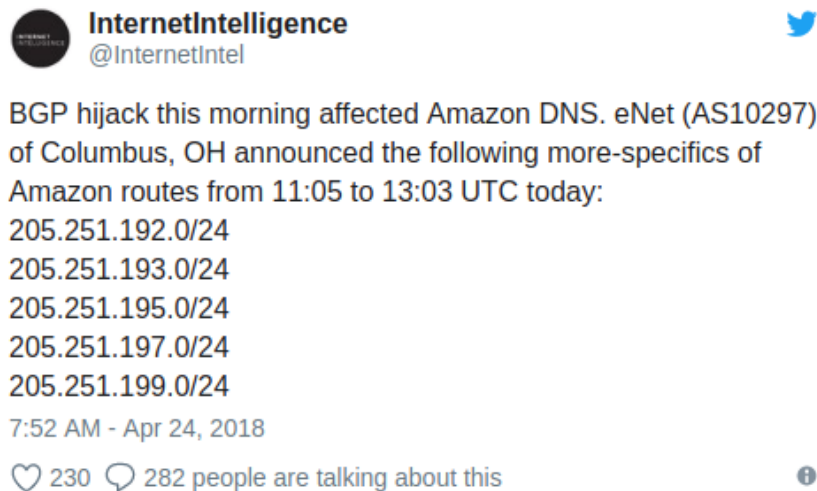
Security / #CyberSecurity

APR 24, 2018 @ 02:10 PM 3,399

A \$152,000 Cryptocurrency Theft Just Exploited A Huge 'Blind Spot' In Internet Security

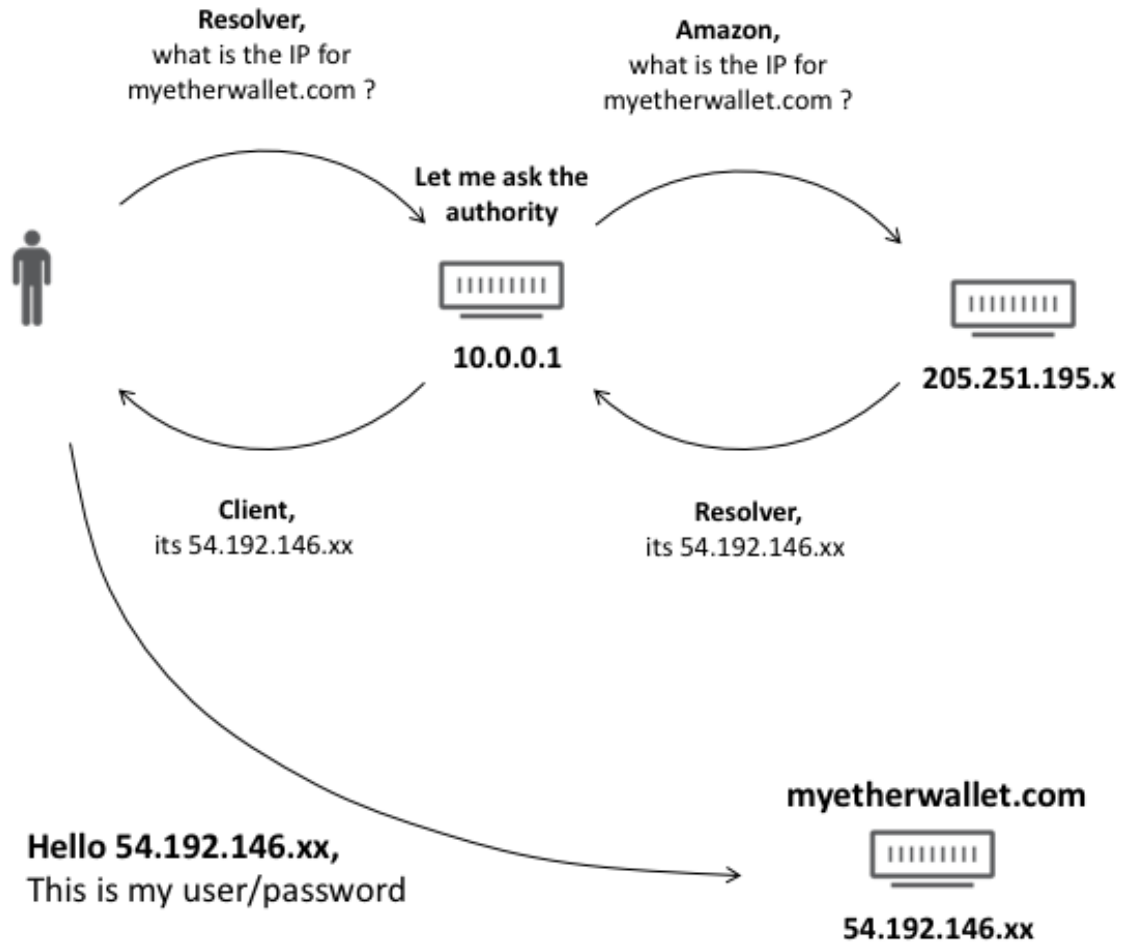
- Impact
 - \$152,000 → 216 Ether known to be stolen
 - But, two wallets used in the attack eventually held more than 520 Ether (~\$365,000 at the time)

- MEW using AWS Route 53 to provide DNS
 - BGP hijack from ISP in Ohio
 - Adversary advertises a more specific route to AWS Route 53 DNS (/24)



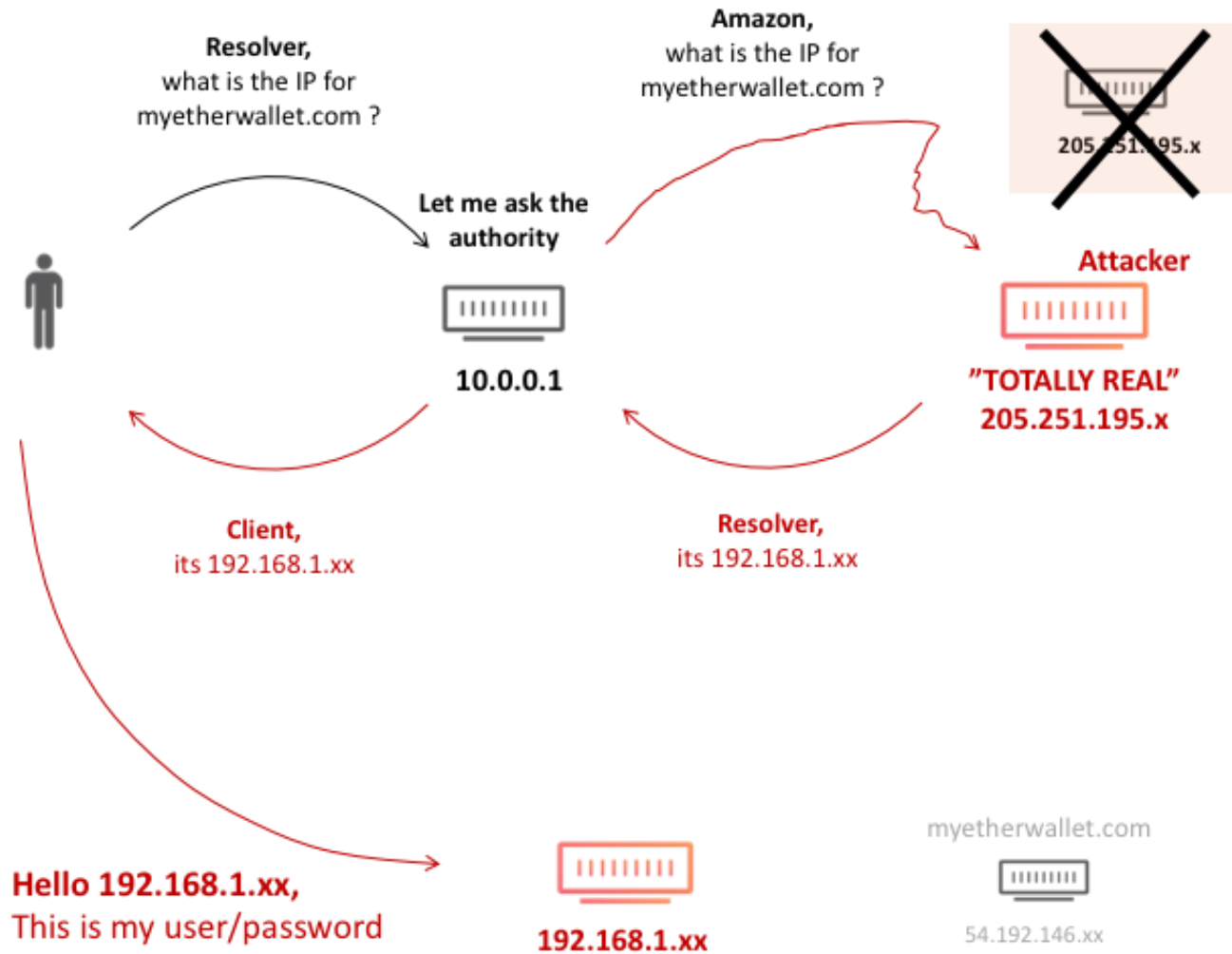
- Redirects DNS for MEW to point to fake web servers in Russia that impersonate MEW
 - “a couple of Domain Name System registration servers were hijacked around 12PM UTC 24 April to redirect users to a phishing site.”
- Users visit fake MEW site and enter their private seeds which captures the credentials

Typical operation



<https://blog.cloudflare.com/bgp-leaks-and-crypto-currencies/>

Hijacked operation



Short-address attack

How to Find \$10M Just by Reading the Blockchain



Paweł Bylica

[Follow](#)

Apr 6, 2017 · 4 min read

transaction, I discovered that there *had* to be a problem in the way the exchange was preparing data for the transaction. “*Oh no,*” I thought, “*this bug could be used to empty the whole GNT account on the exchange!*” And quite a large number of tokens were stored there!

- Unnamed exchange uses insecure marshalling between web API and programming language (Web3/Solidity) and underlying execution environment (Ethereum Virtual Machine)

Walkthrough

- Web interface of DApp calls into `sendCoin` function in the smart contract that takes a recipient address and an amount

```
sendCoin(address _to, uint256 _amount)
```

```
function sendCoin(address to, uint amount) returns(bool sufficient) {  
    if (balances[msg.sender] < amount)  
        return false;  
    balances[msg.sender] -= amount;  
    balances[to] += amount;  
    Transfer(msg.sender, to, amount);  
    return true;  
}
```

- `sendCoin` has a 4-byte keccak hash of `0x90b98a11` and interaction with it uses padded arguments (multiples of 32 bytes)
- Bob has a wallet address ending with `0x00`
(`0x3bdde1e9fbaef2579dd63e2abbf0be445ab93f00`)
 - Asks Alice to transfer him 2 tokens, but maliciously gives her his address truncated to remove the trailing byte (last 2 zeroes).

- Bob `0x3bdde1e9fbaef2579dd63e2abbf0be445ab93f00` asks Alice to send him `2 ETH` via `sendCoin(address, uint)` call (`0x90b98a11`)
- If Bob was not malicious, sends through web form the 20-byte address above and the integer 2.
 - Alice, via Web interface code, generates `msg.data ...`

```

0x90b98a11
0000000000000000000000000000000000000000000000003bdde1e9fbaef2579dd63e2abbf0be445ab93f00
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000002

```

- Notice 20-byte address padded out to 32-bytes in `msg.data` with exactly 12 bytes because API assumes it will **always** be given a 20-byte address

- Malicious Bob instead sends

0x3bdde1e9fbaef2579dd63e2abbf0be445ab93f

not

0x3bdde1e9fbaef2579dd63e2abbf0be445ab93f00

- Alice, via the Web API that improperly marshals data generates

0x90b98a11

```
00000000000000000000000000003bdde1e9fbaef2579dd63e2abbf0be445ab93f00
000000000000000000000000000000000000000000000000000000000000000002
```

not

0x90b98a11

```
00000000000000000000000000003bdde1e9fbaef2579dd63e2abbf0be445ab93f00
000000000000000000000000000000000000000000000000000000000000000002
```

- Missing byte of an address pulled from subsequent arguments
 - EVM appends a byte of `00` at the end of `msg.data` since one byte is missing

0x90b98a11

```
00000000000000000000000000003bdde1e9fbaef2579dd63e2abbf0be445ab93f00
000000000000000000000000000000000000000000000000000000000000000200
```

- Results in Bob receiving `0x200` (512) ETH!

Remediation

- Validate input
 - Check address lengths provided by user
 - Generate transaction data sent to contract function, but check against user input before execution
- Only use checksummed addresses
 - Done in-band with Bitcoin (appended to end of address)
 - Now done for Ethereum addresses via EIP55 standard
 - See EthSum
- Use vetted implementations for marshalling user addresses into transactions
 - e.g. `web3.js`
- Change EVM to throw on data underflows (rather than pad silently)?
- Use Solidity versions > 0.5
 - Short address attack checks no longer needed and are being [removed](#)