



San Francisco | March 4–8 | Moscone Center



A large, abstract graphic in the top right corner features a dense web of thin, curved lines in shades of blue, green, and yellow, radiating from a central point towards the edges of the frame, suggesting a complex network or data flow.

BETTER.

SESSION ID: **BAC-T09**

Cryptojacking: What's in Your Environment?

Austin McBride

Threat Analytics Researcher
Cisco Umbrella
@armcbride1

Ayse Kaya Firat

Head of Analytics and Customer Insights
Cisco Umbrella
@akfirat

#RSAC

Agenda

1

Cryptocurrency

2

Cryptojacking

3

Crypto Phishing

4

Shifting to Altcoins
and Exchanges

5

How to Protect
Yourself

\$ WHOIS Austin

- Threat Analytics Researcher at Cisco Umbrella
- B.S. in Data Mining and Economics
- Crypto enthusiast
- Hobbies: work, algorithmic crypto trading, and work



\$ WHOIS Ayse

- Head of Customer Insights and Analytics
- B.S in Applied Math and Industrial Engineering, M.S. in Engineering Systems & M.Eng. in Operation Research
- Other details: Data artist, Business Communicator, Analytics Translator
- Hobbies: Paragliding, running, travelling



Our Insights Team

- Data Science & Network Security
- Big Security Data
- DNS Traffic:
 - ~180B DNS requests per day
 - NEWLY SEEN DOMAINS!!
 - ...and now all of Cisco data!
- Daily Tasks:
 - Security Data Analysis
 - Customer Data Analysis
 - Big Data Engineering
 - Detection Algorithms
 - Data Viz



Image: igmurr

RSA® Conference 2019

Cryptocurrency



Cryptocurrency's Meteoric rise

Total Market Capitalization



- In less than one year crypto market cap \$26B to \$835B
- Crypto market going mainstream, but still “Wild Wild West”
- Under regulated, highly volatile, and full of malicious actors

Source: coinmarketcap.com

Cryptocurrency's Regulation



- Mt. Gox 2014
- FATF – Guidance of Risk-based Approach to Cryptocurrencies 2015
- FSA - Payment Services Act 2017
 - KYC, AML, Annual Audits
- CoinCheck JAN 2018
- JVCEA MAR 2018
- Where there is money, there are criminals – most of them are external

Why is Crypto Theft Attractive?



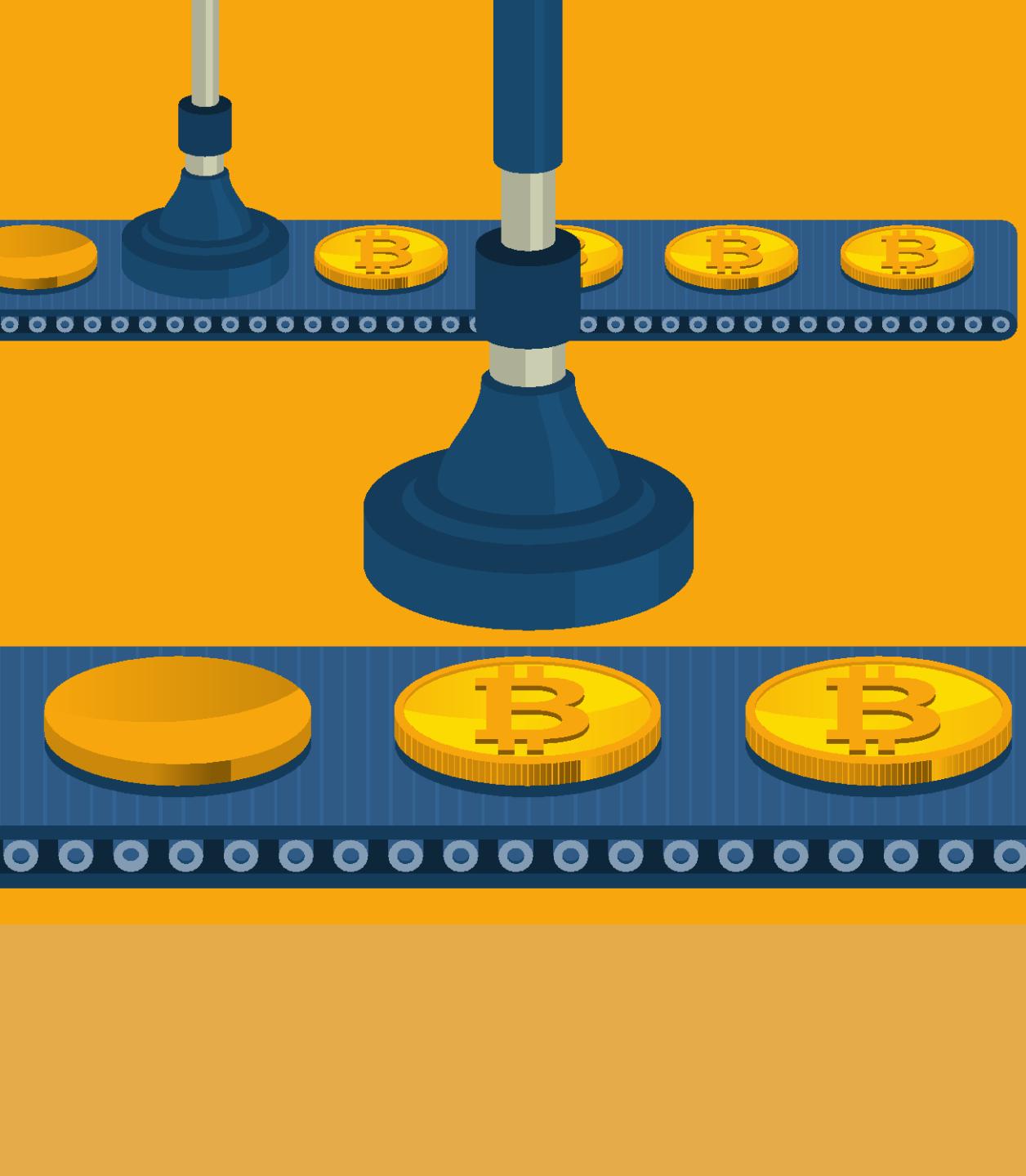
- Crypto asset theft and cryptojacking can be extremely lucrative and hard to spot
- Crypto exchanges security measures are not as mature compared to traditional equity exchanges
- Very anonymous and the asset value fluctuates giving them more purchasing power to buy malicious software, additional infrastructure

So how does
cryptojacking fit in?



Cryptomining

Cryptocurrency mining is simply the process of generating new units of the cryptocurrency. In the case of say Bitcoin, a miner uses their computing power to verify P2P Bitcoin transactions and is rewarded with new Bitcoins proportional to the amount of computing power they donated to the Bitcoin network.



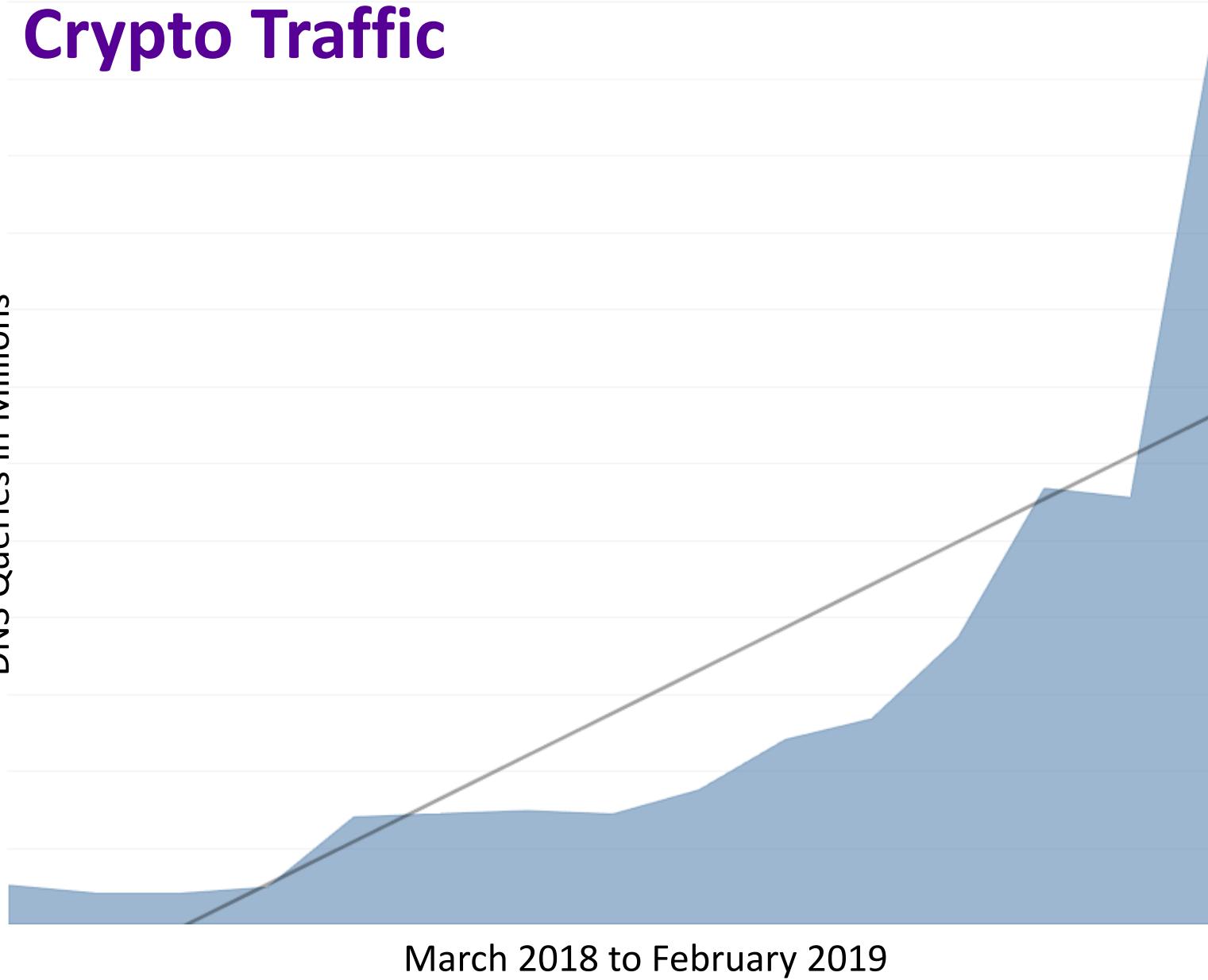
Cryptojacking

Cryptojacking is the secret use of your business' computing power to mine cryptocurrencies through individual machines in browser JavaScript exploits, cloud AWS instances, etc.



Crypto Traffic

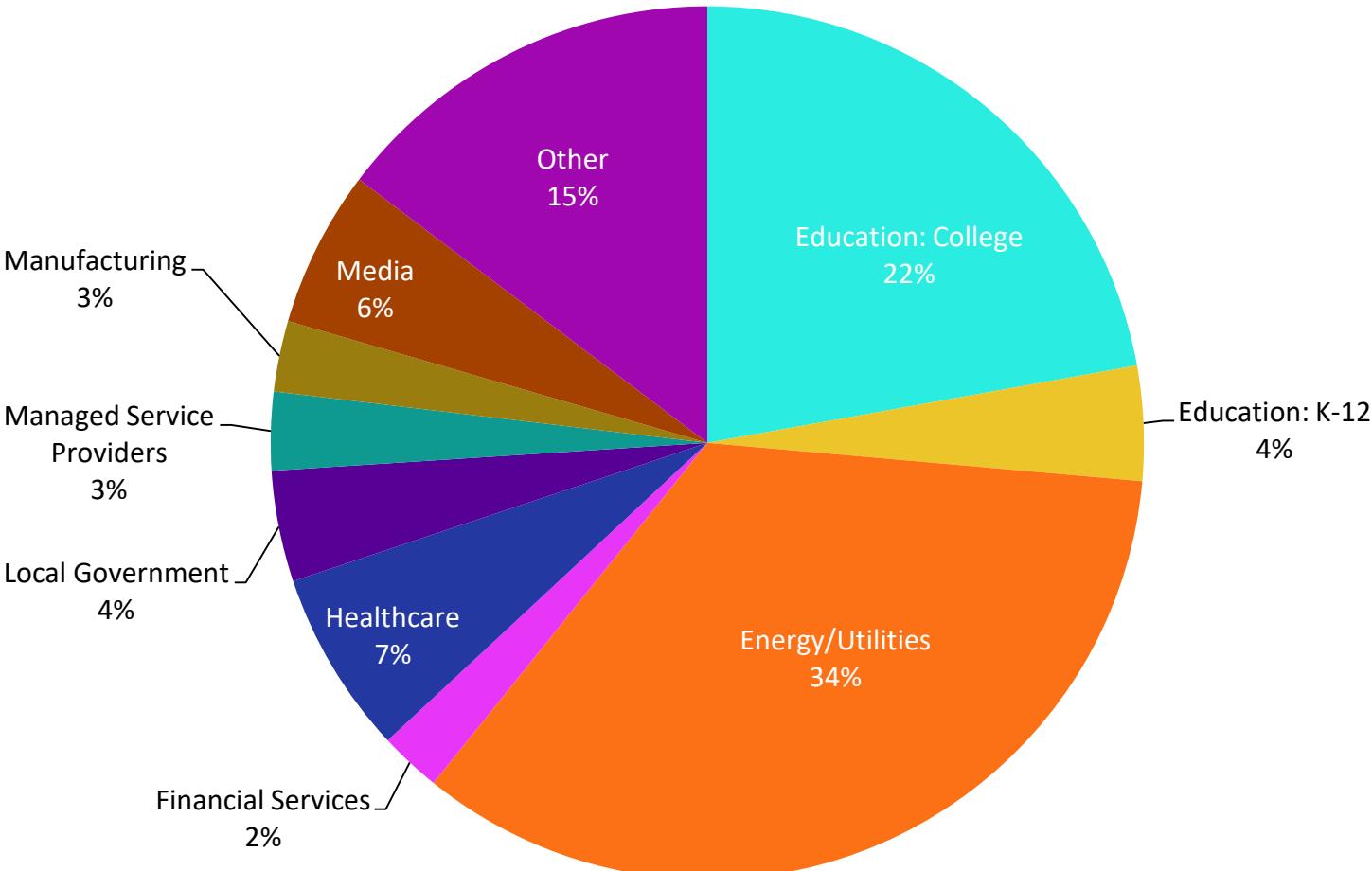
DNS Queries in Millions



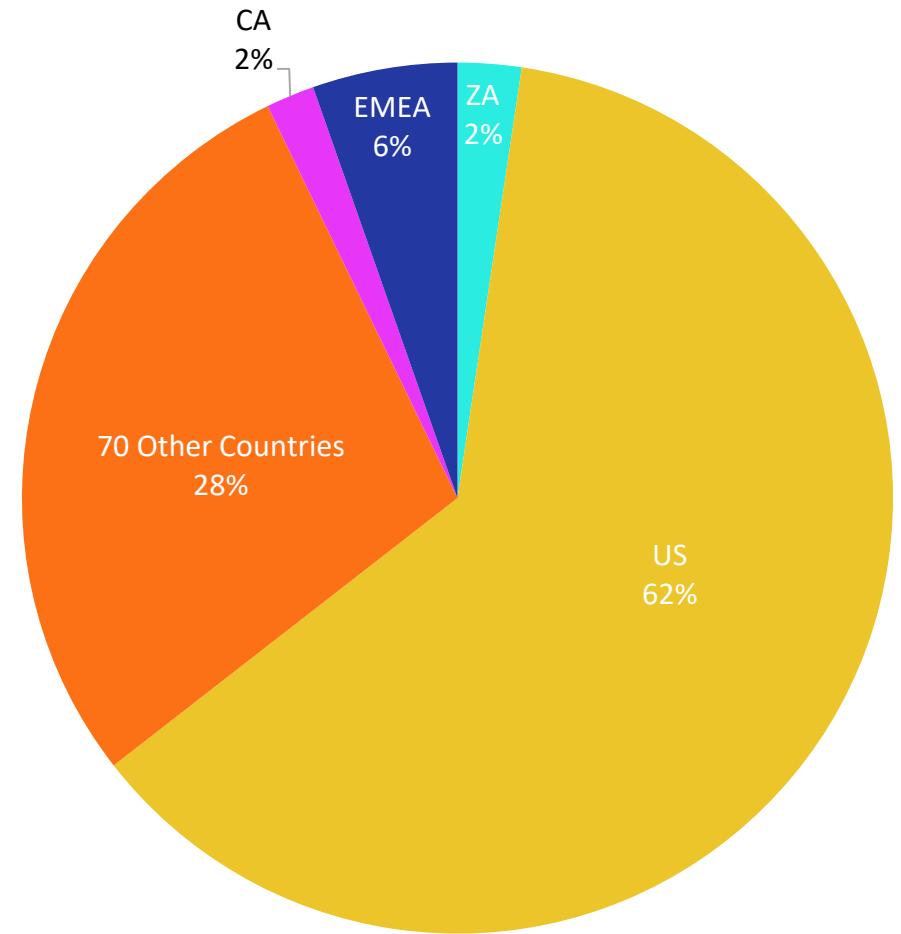
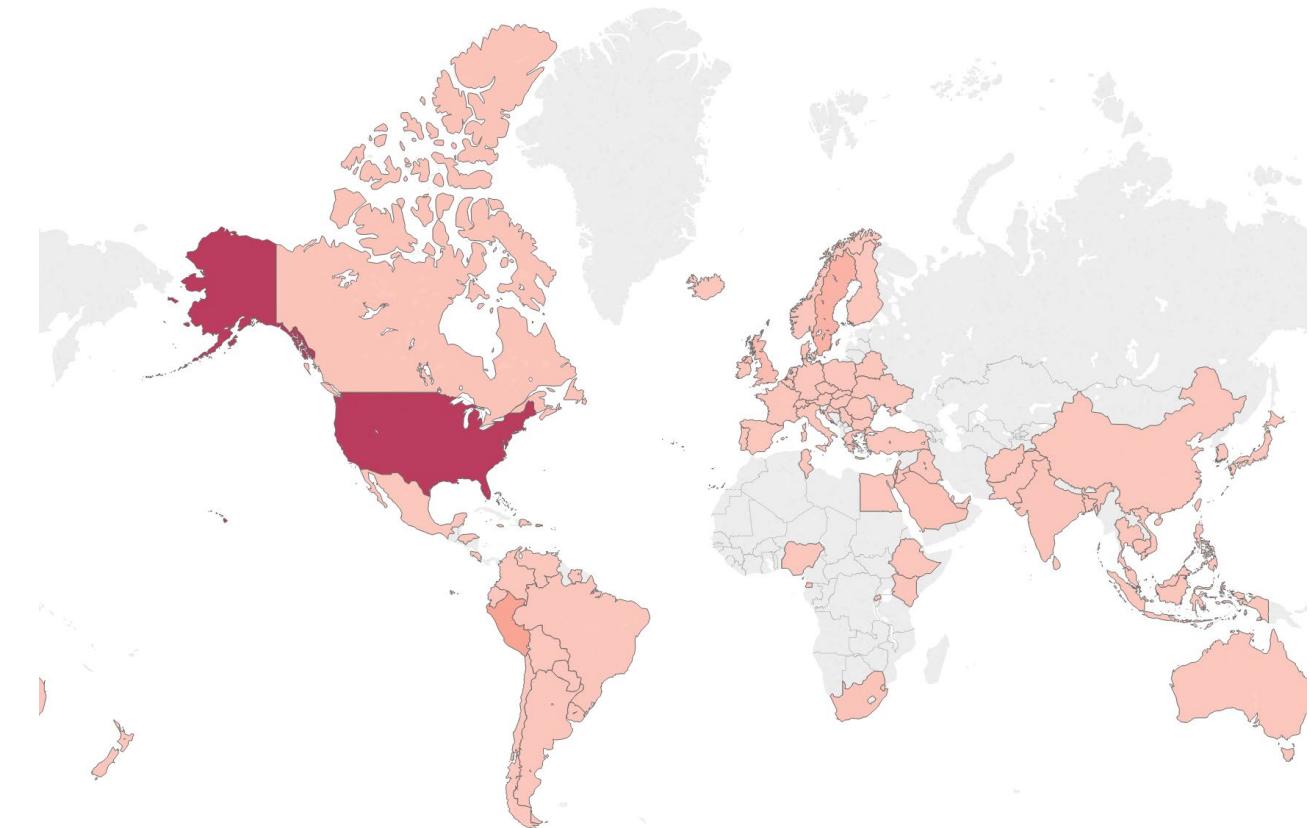
- Last 11 months: 200x increase in crypto related traffic
- The majority of traffic are cryptomining pools, but also some sites that drop mining software onto your machine
- Distribution of crypto traffic affects all industries, not just financial services

Crypto Traffic Industry Distribution

- Higher Education, Energy/Utilities, Local Government, Healthcare and Media industries have a surprising high volume of cryptomining traffic
- Top industry fluctuates every 2-3 months, but Higher Education is always in the top 2

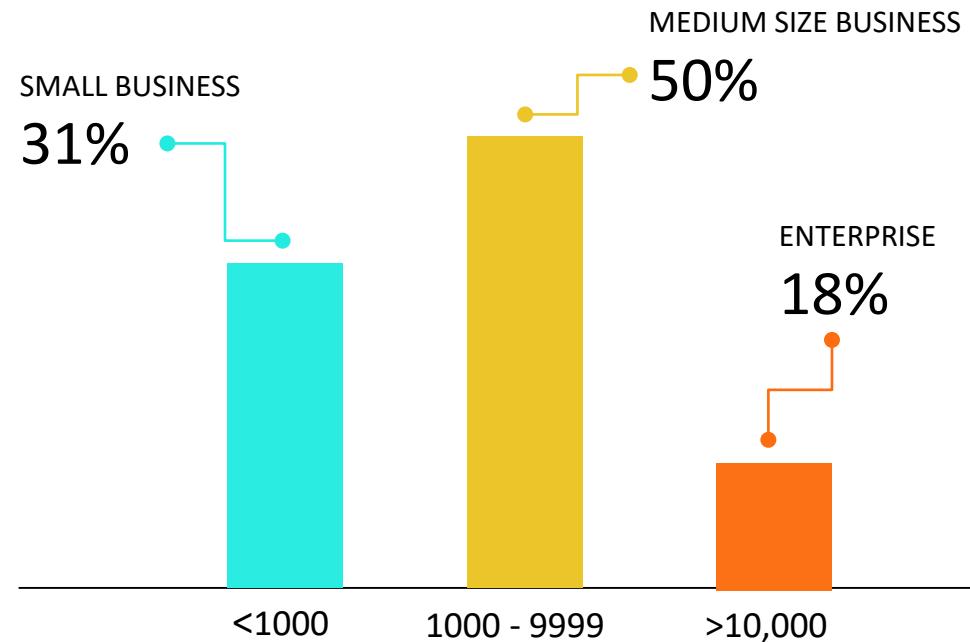


Crypto Traffic Geo Distribution



ZA: South Africa, CA: Canada, EMEA: Europe, Middle East & Africa, US: United States

SMBs Are More Vulnerable to Cryptomining Malware



Medium sized businesses accounts for slightly more than 50% of all crypto traffic.

- We see more instances of cryptomining in Small and Medium Business (SMBs) environments

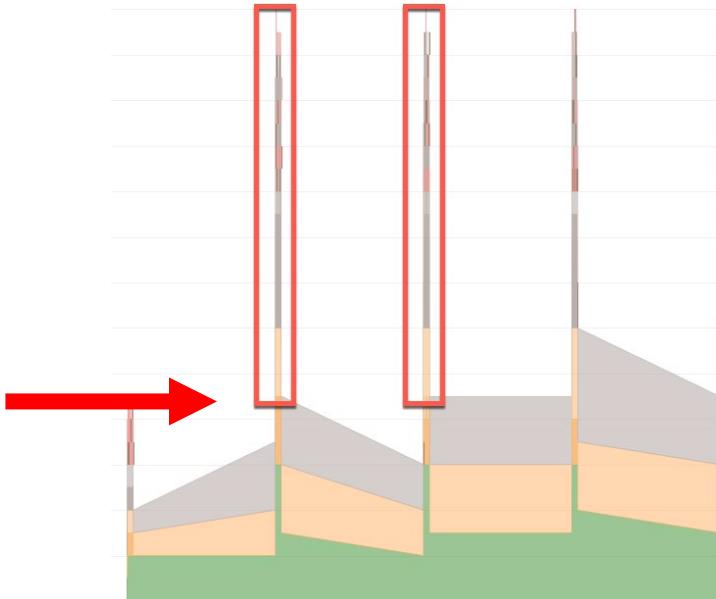
Weaponized Cryptomining?

Why We Should Care

1

Web-Based Miners:

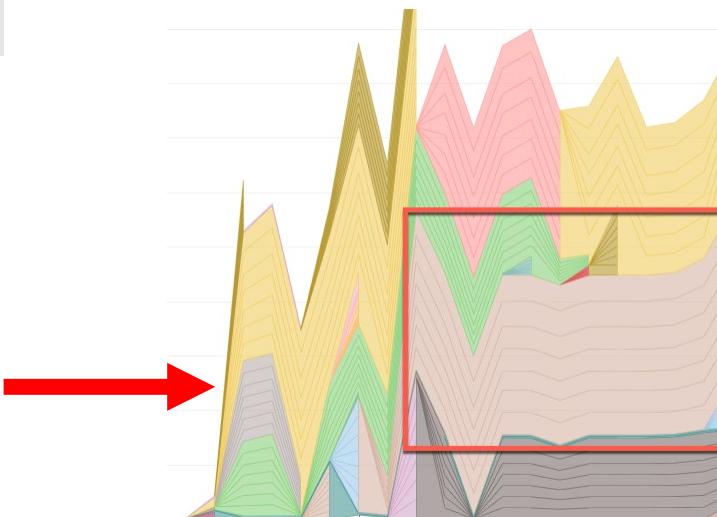
Generally only impact a machine while a user is on a webpage and does not persist after you close the page. Little risk of damaging machine hardware.



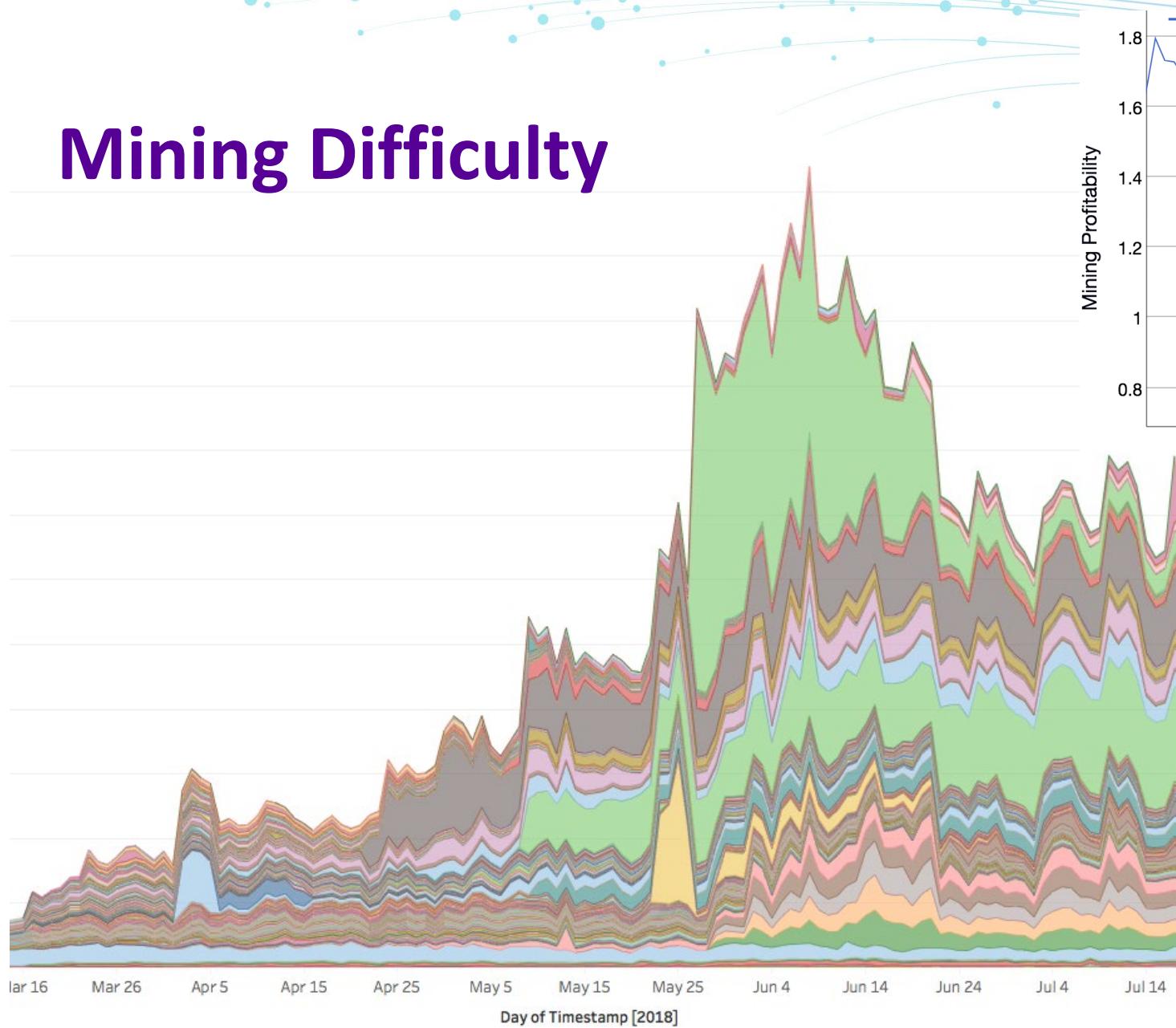
2

Software-Based Miners:

Actual software installed on a machine that persists while the machine is on and connected to the internet. Higher risk of damaging hardware.
Potentially an IOC.



Mining Difficulty



- Increases in mining difficulty has hurt mining profitability and halted many mining pools used by malicious actors
- Cryptojacking will decrease when the market is down and increase when the market it hot

Mining Costs



- With cloud based miners like Coinhive the cost to the malicious actor generally no more than 30% of whatever they were able to mine in your environment
- The real upfront cost for them is whatever they had to do leverage your machine (very inexpensive)

The screenshot shows a web browser window with the URL <https://coinhive.com> in the address bar. The page header includes the Coinhive logo (an orange hexagon icon), the word "Coinhive", a "Documentation" link, and "Login" and "Signup" links. Below the header is a large orange hexagon icon. The main content area features the text "A Crypto Miner for your Website". To the right, there are performance metrics: "HASHES/S" at 0, "TOTAL" at 0, "THREADS" at 8 (+/-), and "SPEED" at 100%. A blue circular button labeled "START MINING" with a play icon is positioned next to the threads setting. The background has a light gray gradient.

Coinhive Documentation Login Signup

A Crypto Miner for your Website

HASHES/S
0

TOTAL
0

THREADS
8 + / -

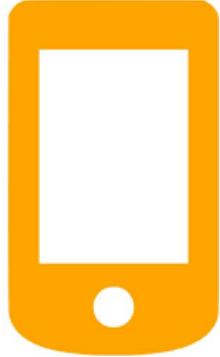
SPEED
100%

START MINING

Cryptojacking targets wide range of users



Servers



Smartphones



PC



Websites



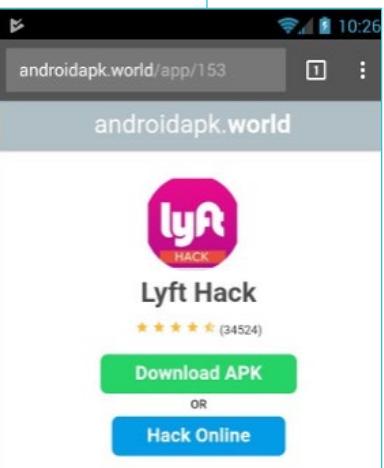
Amazon EC2

Cryptojacking

WIRED

LILY HAY NEWMAN SECURITY 02.20.18 05:06 PM

HACK BRIEF: HACKERS ENLISTED TESLA'S PUBLIC CLOUD TO MINE CRYPTOCURRENCY



Natasha Lomas @riptari / Feb 12, 2018

Cryptojacking attack hits ~4,000 websites, including UK's data watchdog



BAD PACKETS REPORT

SEPTEMBER 24, 2017 BY TROY MURSCH

Coinhive miner found on official Showtime Network websites in latest case of cryptojacking

Javascript Injections



A screenshot of a web browser window displaying a Javascript code snippet. The URL in the address bar is `https://coinhive.com`. The code itself is a script for mining cryptocurrency using the CoinHive library. It includes a dependency on `authedmine.min.js`, initializes a miner with a site key, and checks if the device is non-mobile and not opted-out within the last 4 hours before starting the mining process.

```
<script src="https://authedmine.com/lib/authedmine.min.js"></script>
<script>
  var miner = new CoinHive.Anonymous('YOUR_SITE_KEY', {throttle: 0

    // Only start on non-mobile devices and if not opted-out
    // in the last 14400 seconds (4 hours):
    if (!miner.isMobile() && !miner.didOptOut(14400)) {
      miner.start();
    }
</script>
```

- Malicious actors can inject a few lines of JS on a website and use visitors computing resources to mine cryptocurrency while they are visiting the site
- It's often that site visitors do not notice their degraded system performance

RSA® Conference 2019

Crypto phishing



Delivery Vectors

Email



Search Engine Ads

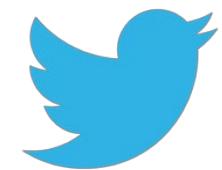
Google

bing



DuckDuckGo

Communication Channel



About 33,400 results (0.28 seconds)

MyMonero: Welcome - XMR Wallet - Send and receive Monero safely

Ad www.mymonero.com/ ▾

Send and receive Monero safely and securely, anywhere and any time

MyMonero: Welcome - XMR Wallet - Send and receive Monero

Ad www.my-monero.com/ ▾

Send and receive Monero safely and securely.

Все в наличии · Низкие цены · Скидки 20% · Гарантия



<https://mymonero.com>



MY MONERO

[CREATE A NEW ACCOUNT](#)

[SUPPORT](#)

[LOG IN](#)

The Simplest Way to Use Monero

Send and receive Monero safely and securely, anywhere and any time.

[Create an Account](#)



<https://my-monero.com>



[CREATE A NEW ACCOUNT](#)

[SUPPORT](#)

[LOG IN](#)

The Simplest Way to Use Monero

Send and receive Monero safely and securely, anywhere and any time.

[Create an Account](#)

Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN) sni164186.cloudflaressl.com
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) Domain Control Validated
Serial Number 00:A3:71:A0:22:50:1A:FD:3C:CE:D2:57:21:99:DE:3B:3B

Issued By

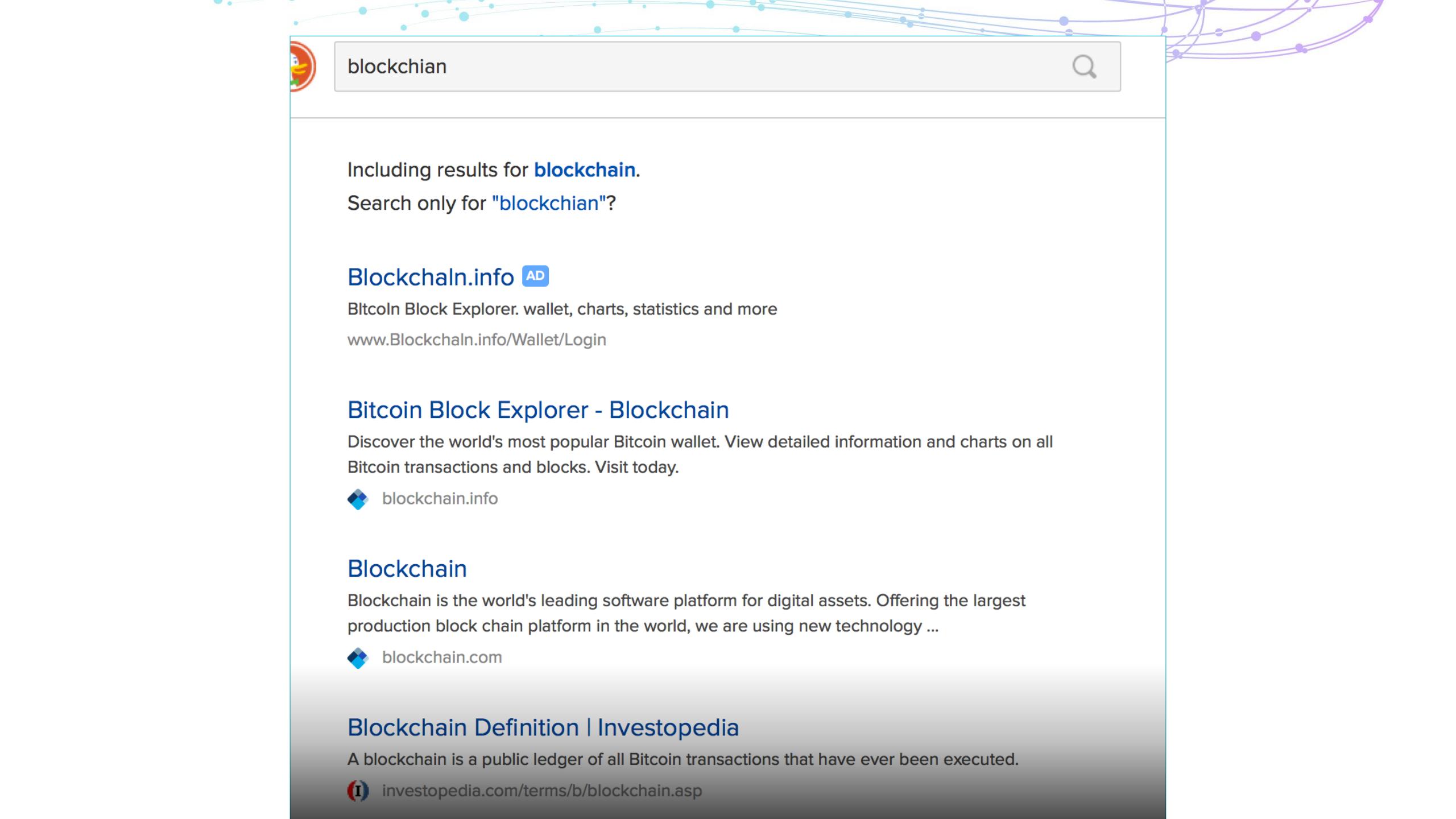
Common Name (CN) COMODO ECC Domain Validation Secure Server CA 2
Organization (O) COMODO CA Limited
Organizational Unit (OU) <Not Part Of Certificate>

Period of Validity

Begins On October 19, 2017
Expires On April 27, 2018

Fingerprints

SHA-256 Fingerprint C1:72:D7:AF:3B:B6:10:CD:60:11:9B:AF:E8:16:49:2A:
F0:C0:A8:58:D2:A0:FF:9F:3E:74:C2:30:76:21:5B:8C
SHA1 Fingerprint 64:36:36:37:19:20:4A:DA:C9:EE:C9:9C:E0:32:70:42:6B:5D:B1:8A



blockchian

Including results for **blockchain**.

Search only for "blockchian"?

Blockchalin.info AD

Bitcoln Block Explorer. wallet, charts, statistics and more

www.Blockchalin.info/Wallet/Login

Bitcoin Block Explorer - Blockchain

Discover the world's most popular Bitcoin wallet. View detailed information and charts on all Bitcoin transactions and blocks. Visit today.

 blockchain.info

Blockchain

Blockchain is the world's leading software platform for digital assets. Offering the largest production block chain platform in the world, we are using new technology ...

 blockchain.com

Blockchain Definition | Investopedia

A blockchain is a public ledger of all Bitcoin transactions that have ever been executed.

 investopedia.com/terms/b/blockchain.asp



About your business Your first campaign Payment

Payment

Provide your payment information below. Remember, you won't be charged until your ad starts showing and people start clicking it.

Your ad

Blockchain Digital Wallet - Easy Digital
Currency Exchange
 www.blockchain.info

Blockchain. The World's Most Popular Digital
Currency Wallet. Get A Free Wallet!

Your ad could be formatted differently to fit a user's device, but your ad text will stay the same.

Daily potential reach

387+ Clicks

Budget and bidding

\$25.00 daily budget

AdWords automatically sets your bids to help you get as many clicks as possible within your budget.

Payment information

Billing country

United States

Time zone

(GMT-07:00) Pacific Time

Google AdWords

New ad version

Headline 1
Blockchain Digital Wallet

Headline 2
Easy Digital Currency Exchange

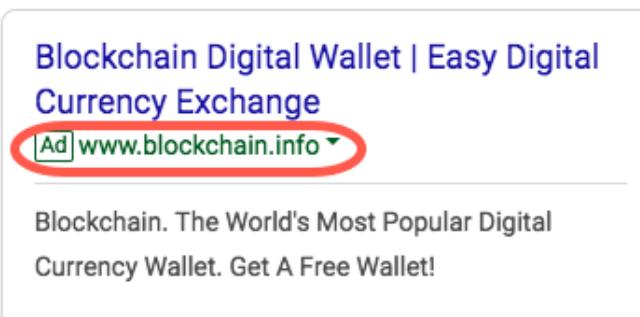
Description
Blockchain. The World's Most Popular Digital Currency Wallet. Get A Free Wallet!

SEE HOW YOUR AD WILL APPEAR

SAVE CANCEL

+ NEW AD VERSION 

Clicks on your ad go to
www.blockchain.info/wallet/im_gonna_phish_you



The preview shows the headline "Blockchain Digital Wallet | Easy Digital Currency Exchange" followed by the URL "[Ad] www.blockchain.info". The URL is highlighted with a red oval. Below the preview is the text "Blockchain. The World's Most Popular Digital Currency Wallet. Get A Free Wallet!" and a "SEE HOW YOUR AD WILL APPEAR" button.

Important notes:

- Redirects to alternate domains do not happen within a google ad they happen on the actual site in the ad (e.g. www.blockchain.info)
- The domain displayed in an ad cannot have a different sitename, but you can have different subdirectories (folders) as the final URL when someone clicks on an ad

Google AdWords

New ad version

Headline 1
Blockchain Digital Wallet

Headline 2
Easy Digital Currency Exchange

Description
Blockchain. The World's Most Popular Digital Currency Wallet. Get A Free Wallet!

Your ad preview on Desktop

Blockchain Digital Wallet | Easy Digital Currency Exchange
[Ad] www.blockchain.info

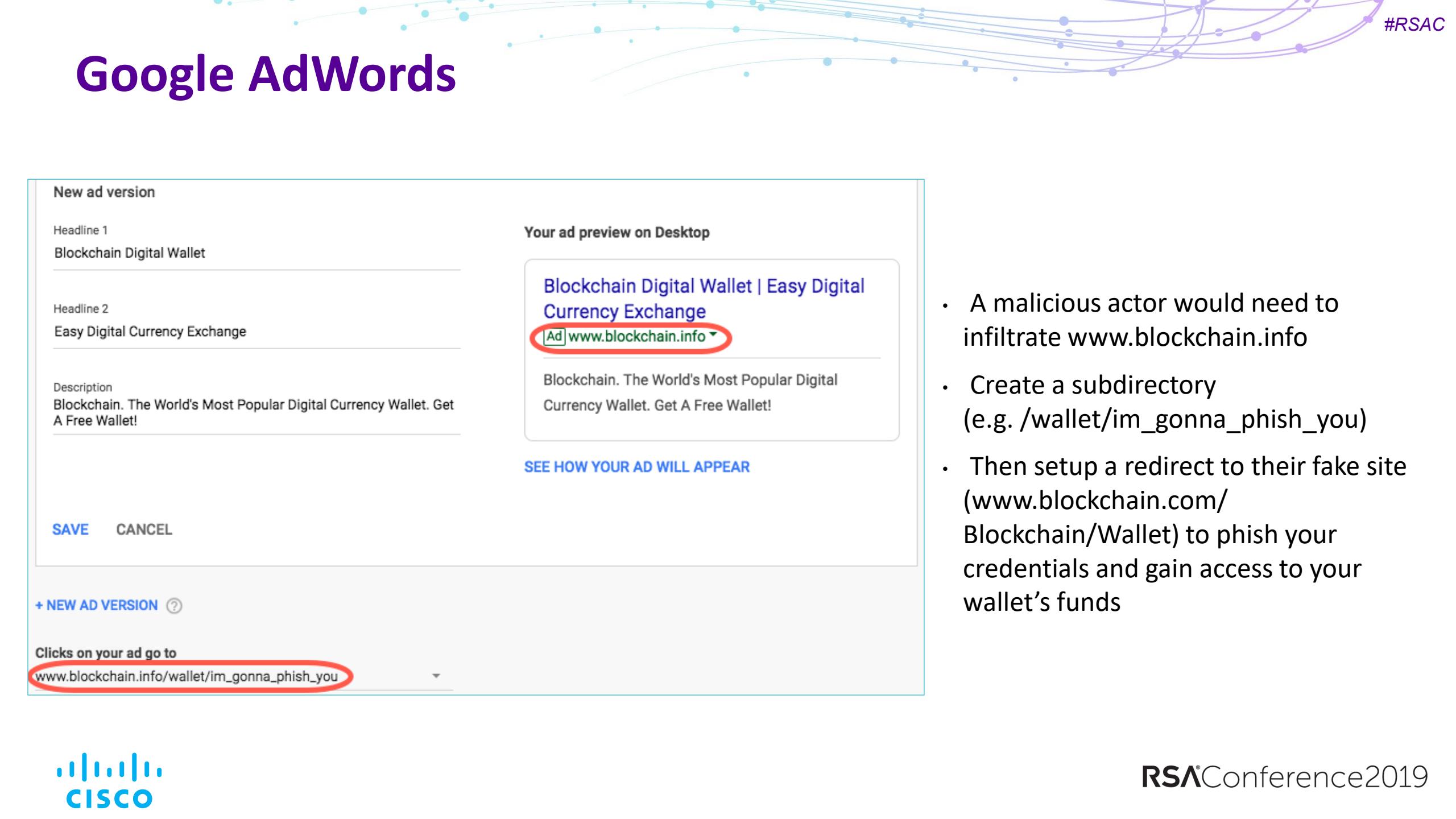
Blockchain. The World's Most Popular Digital Currency Wallet. Get A Free Wallet!

SEE HOW YOUR AD WILL APPEAR

SAVE **CANCEL**

+ NEW AD VERSION 

Clicks on your ad go to
www.blockchain.info/wallet/im_gonna_phish_you



- A malicious actor would need to infiltrate www.blockchain.info
- Create a subdirectory (e.g. /wallet/im_gonna_phish_you)
- Then setup a redirect to their fake site (www.blockchain.com/ Blockchain/Wallet) to phish your credentials and gain access to your wallet's funds

Google AdWords

Blockchain Digital Wallet | Easy Digital Currency Exchange  www.xn--blockchan-n5a.info

Ad www.blockchaín.info ▾

Blockchain. The World's Most Popular Digital Currency Wallet.
Get A Free Wallet!

- We have also seen heavy use of punycode which can make it much harder for users to spot fake sites
- e.g. www.xn--blockchan-n5a.info which displays as www.blockchaín.info

RSA® Conference 2019

Targeting Exchanges and AltCoins



Crypto Phishing and Scams

Crypto exchange phishing sites are on the rise and they are using advertisements on search engines to lure people into giving up their credentials

[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/> ▾

 binance @biunuce_2018 · 10h
Replying to @binance_2017

We're giving away 500 ETH to our followers! Send 0.2 ETH below and We'll send you 2 ETH back, through the same address you used in the transaction.

0x9558BeCA8790cbC465D466fD0A96583Dc6 4CF1e8

If you're late, your ETH will be sent back. - Binance team

 **BINANCE**
Free
ETHEREUM

105 75 185

 binance @biunuce_2018 · 10h
There is still time left to enter! There are still

We're giving away ETH! Just send me 0.2 ETH and I'll send you back 2 ETH. Send me your crypto to the address below...

Crypto Phishing targeting exchanges

www.bivnance.com = www.binance.com Right?

<http://www.bivnance.com>

Market	Symbol	Price	Change	Volume
Binance Lists	WePower (WPR)	\$0.0016185	1.23%	4,792.01 BTC
Binance Lists	XVG/BTC	\$0.00000671	19.18%	6,124.27 BTC
Binance Lists	TRX/BTC	\$0.00000469	-5.63%	8,926.05 BTC
Binance Lists	QLC/BTC	\$0.0002033	1.35%	1,379.42 BTC
Binance Lists	ONT/BTC	\$0.00030602	-0.87%	1,118.46 BTC

Market Summary:

Market	Symbol	Price	Change	Volume
Binance Lists	WePower (WPR)	\$0.0016185	1.23%	4,792.01 BTC
Binance Lists	XVG/BTC	\$0.00000671	19.18%	6,124.27 BTC
Binance Lists	TRX/BTC	\$0.00000469	-5.63%	8,926.05 BTC
Binance Lists	QLC/BTC	\$0.0002033	1.35%	1,379.42 BTC
Binance Lists	ONT/BTC	\$0.00030602	-0.87%	1,118.46 BTC

Trading View:

Pair	Last Price	24h Change	24h High	24h Low	24h Volume
TRX/BTC	\$0.00000469 / \$0.03	-5.63%	\$0.00000498	\$0.00000436	8,926.05322982

<https://www.binance.com>

Market	Symbol	Price	Change	Volume
Binance Lists	WePower (WPR)	\$0.0016185	1.23%	4,792.01 BTC
Binance Lists	XVG/BTC	\$0.00000671	19.18%	6,124.27 BTC
Binance Lists	TRX/BTC	\$0.00000469	-5.63%	8,926.05 BTC
Binance Lists	QLC/BTC	\$0.0002033	1.35%	1,379.42 BTC
Binance Lists	ONT/BTC	\$0.00030602	-0.87%	1,118.46 BTC

Market Summary:

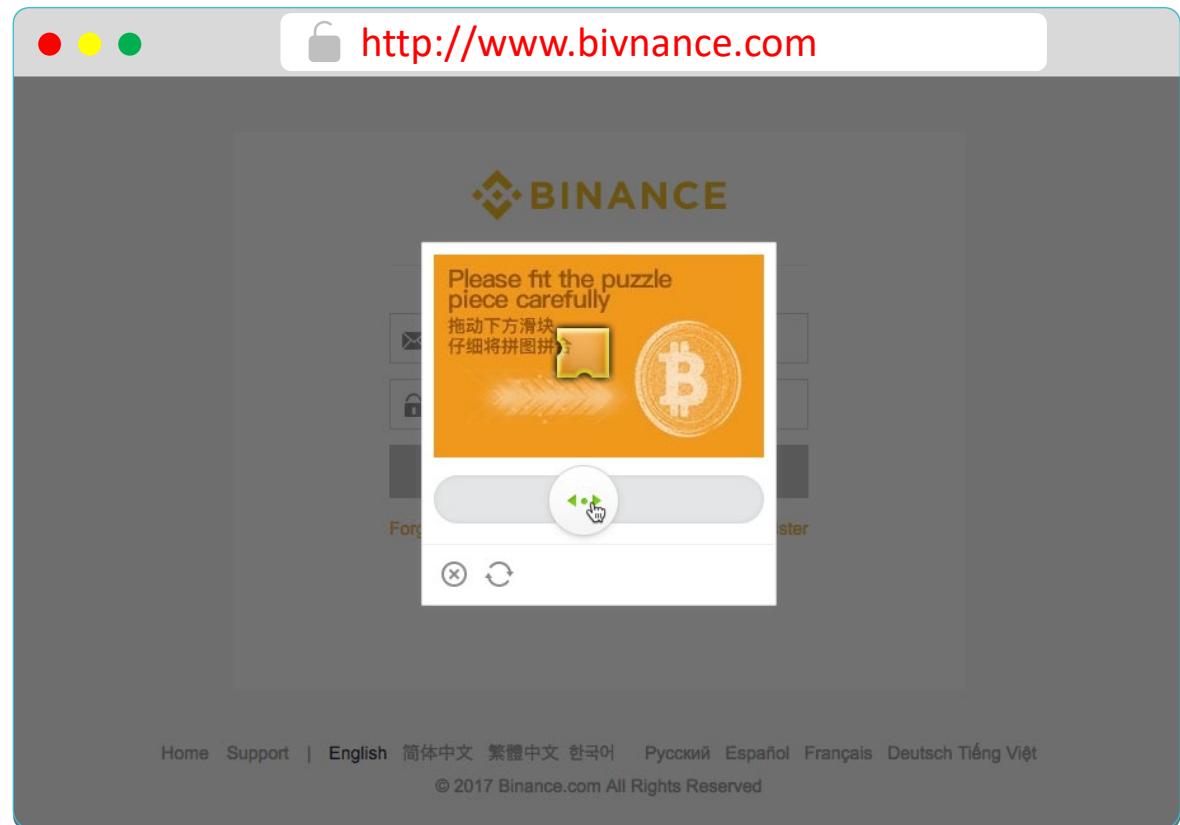
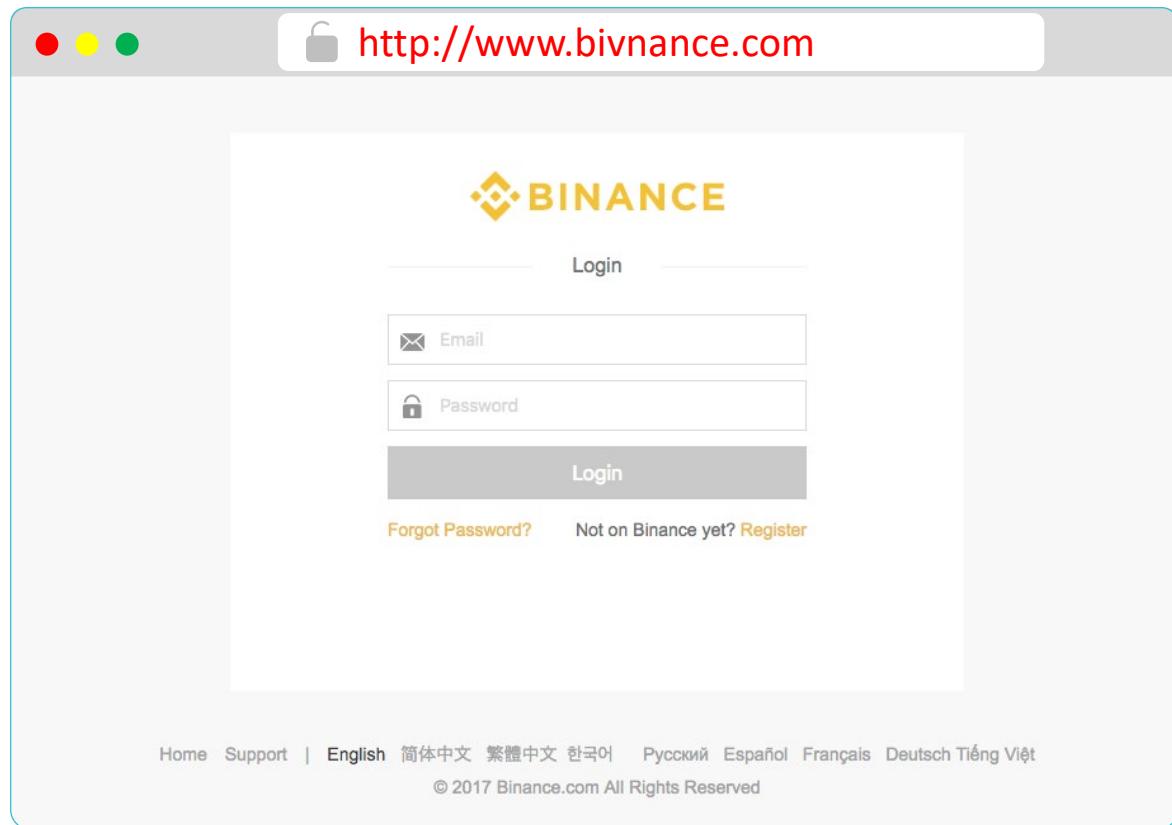
Market	Symbol	Price	Change	Volume
Binance Lists	WePower (WPR)	\$0.0016185	1.23%	4,792.01 BTC
Binance Lists	XVG/BTC	\$0.00000671	19.18%	6,124.27 BTC
Binance Lists	TRX/BTC	\$0.00000469	-5.63%	8,926.05 BTC
Binance Lists	QLC/BTC	\$0.0002033	1.35%	1,379.42 BTC
Binance Lists	ONT/BTC	\$0.00030602	-0.87%	1,118.46 BTC

Trading View:

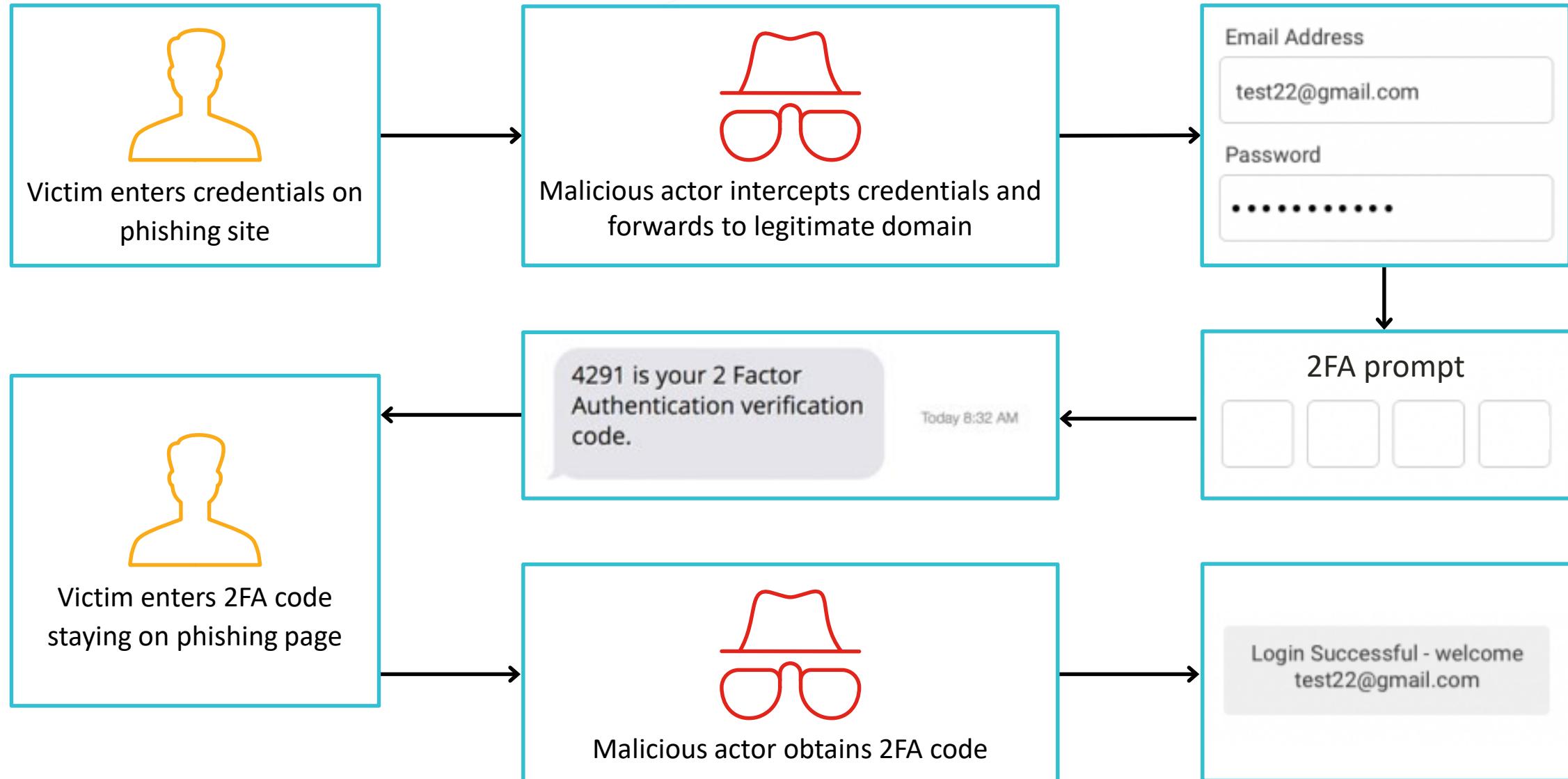
Pair	Last Price	24h Change	24h High	24h Low	24h Volume
TRX/BTC	\$0.00000469 / \$0.03	-5.63%	\$0.00000498	\$0.00000436	8,926.05322982

Crypto Phishing targeting exchanges

www.bivnance.com = www.binance.com Right?



2FA Bypass



What do we know about www.bivnance.com?

 **Investigate**

SEARCH PATTERN SEARCH

bivnance.com INVESTIGATE

WHOIS Record Data

Registrar Name: Center of Ukrainian Internet Names (UKRNAMES) IANAID: 1436

Created: February, 16, 2018

Updated: February, 16, 2018

Email Address

black13@unseen.is

Associated Domains

15 Total - 4 malicious

IPs

195.123.225.64 (TTL: 3600)

Domains Associated with black13@unseen.is

Domain Name	Security Categories	Content Categories	Last Observed
myethhexwallet.com	Phishing		Current
myethxrwallet.com	Phishing		Current
mynotherwallet.com	Phishing		Current
nnyettiervwailet.com	Phishing		Current

What else is
black13@unseen.is
after?

Known domains hosted by 195.123.225.64

bitinance.com bivnance.com www.bilimance.com www.btnance.com biginance.com
blimance.com www.bilinamce.com www.bivnance.com mail.bwnance.com
resource.blimace.com www.bilrnance.com bvnance.com www.blimance.com
www.bwnance.com bilimance.com www.bornance.com www.bvnance.com
mail.bilrnance.com bwnance.com mail.bvnance.com ww.bivnance.com bilrnance.com
www.blimace.com bornance.com btnance.com bilinamce.com mail.btnance.com
blimace.com resource.bilimance.com resource.blimance.com bimanec.com
blnanco.com blnancie.com www.binancit.com

Maybe all of your
ERC20 tokens...

Altcoins vector

- Another tactic used by malicious actors involves pump and dumps
- Malicious actors setup phishing sites to get user's exchange credentials (several hundred accounts)
- Create API keys for those accounts and enable API trading
- Setup a bot to liquidate user's altcoin positions into BTC and purchase all open orders for VIA coin to pump its price
- Then the malicious actor can sell their own VIA coins at the top of the pump and walk away with a 10,000% gain on their own VIA coin holdings



Altcoins vector

- In the case of the VIA coin pump the malicious actor plan backfired and they walked away with nothing



RSA® Conference 2019

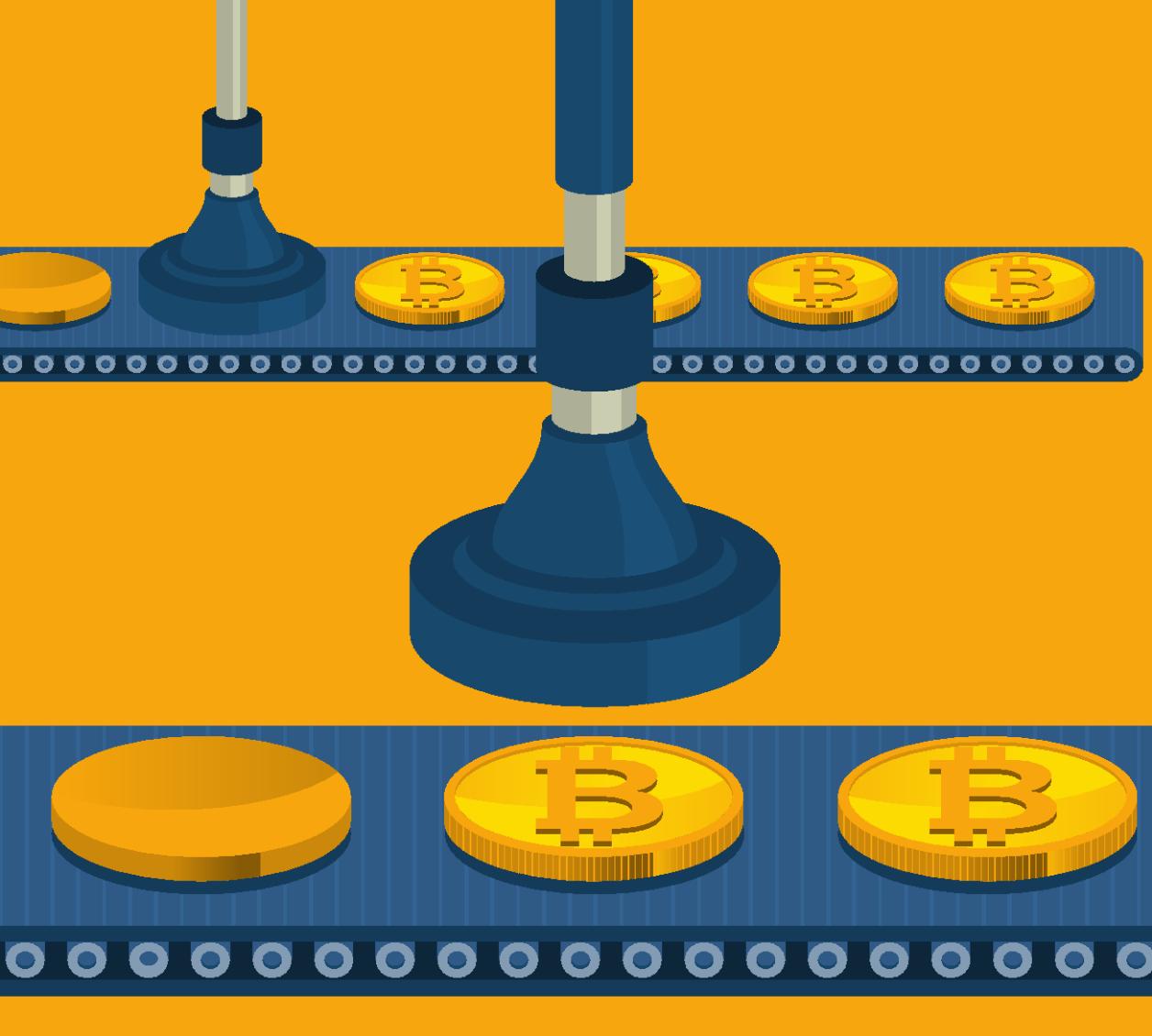


How to Protect Yourself

Cryptojacking

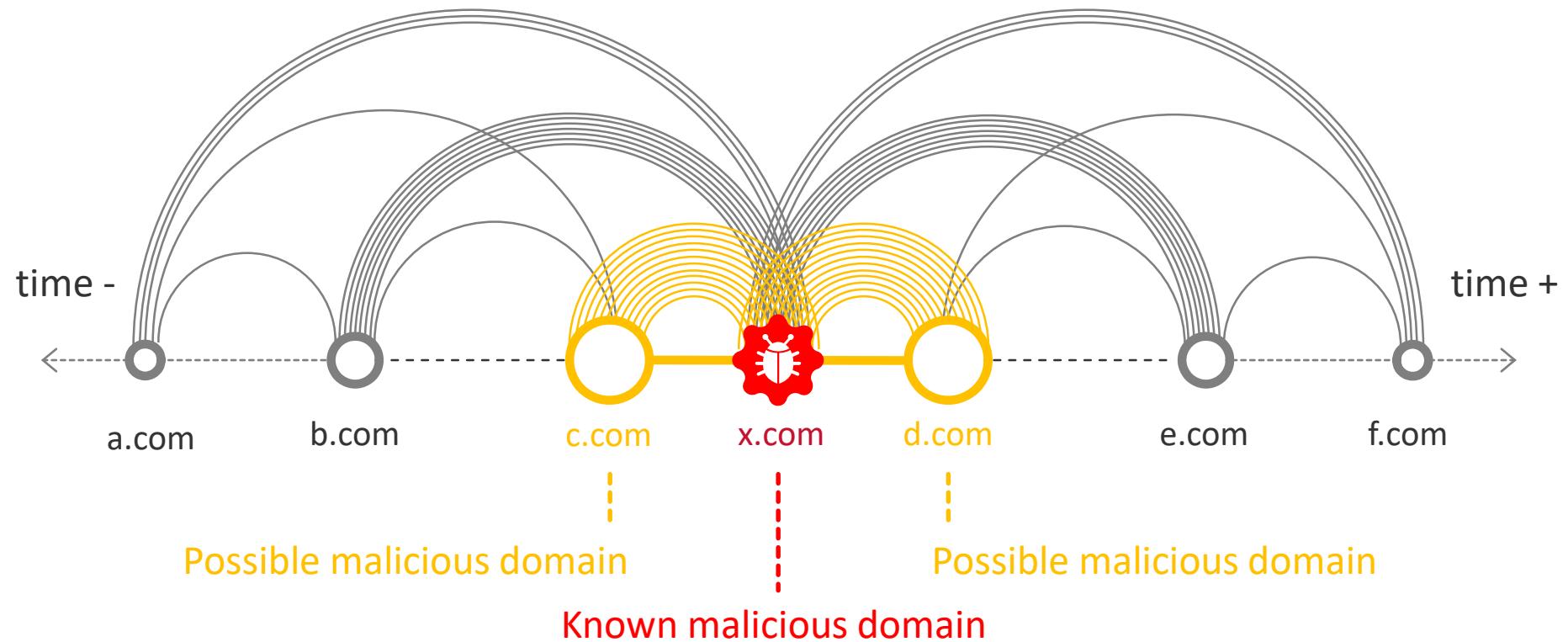
DNS level domain blocking can be effective for known pool miners

For cloud computing instances, look for increases in CPU utilization – could be as small as a 10%-15% increase



Co-occurrence model

Domains guilty by inference



Co-occurrence of domains means that a statistically significant number of identities have requested both domains consecutively in a short timeframe

Co-occurrences

asset.epub.pub (4.91) hemnes.win (4.91)
https-bookmp3-ru.disqus.com (4.91)
img.p2pbг.com (4.91) l4oecosq.com (4.91)
www.tv-vip.com (4.91) pl14313817.puserving.com (4.43)
s1.cpmaffiliation.com (4.02) xmrrmsft.com (4.00)

cdn.multiup.org (3.66) down.foxbeen.com (2.85)
callumaumusic.com (2.60) cdn.mngwefal.com (2.54)
adserpub.com (2.49) sihirdarrehberi.com (2.33)
cosmic-bio.com (2.04) www.linksbot.su (2.03)
cdn.mngappnf.com (1.99) spread.epub.pub (1.92)
babbano.com (1.92) cdn.starexample.com (1.89)
w5j3j9d9.hwcdn.net (1.78) www.foxbeen.com (1.44)
cdn.mngepvra.com (1.17) cdn.jheberg.net (1.07)
customs.go.kr (1.04) free.pagepeeker.com (1.01)
tainiesonline.xrysoi.online (0.99) superplacid.com (0.91)

webmining.co (0.86) cdn.adult.xyz (0.82)
vuuwd.com (0.80) proxyfl.info (0.76) www.siska.tv (0.75)
sandiegozoo.tumblr.com (0.68) coin-hive.com (0.65)
identies.com (0.59) alibestruru (0.54) c.clover.com (0.54)
dogeminer2.com (0.53) i.poopeegirls.com (0.53)

Malicious domains associated with phishing and browser redirect

CryptoJacked domains serving Coinhive miner script

Another source for the mining script

Cryptofishing detection



“Newly Seen”

Shallow Layer

FQDN Classification

Fetch Page Source

HTML Content Classification

Deeper Layers

Malicious Infrastructure Classification | Cisco Umbrella

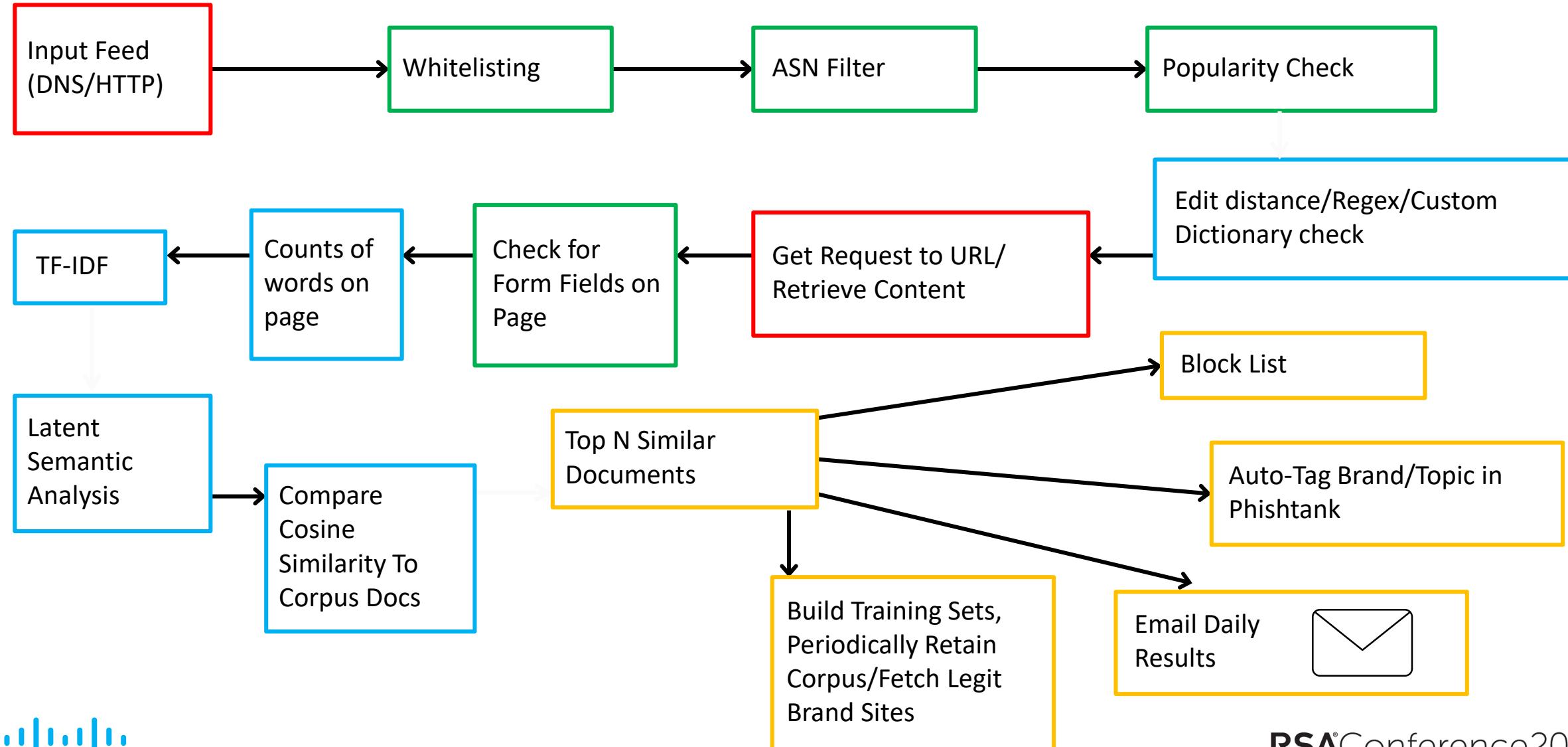
Blocking/Threat Intelligence/LE Reporting

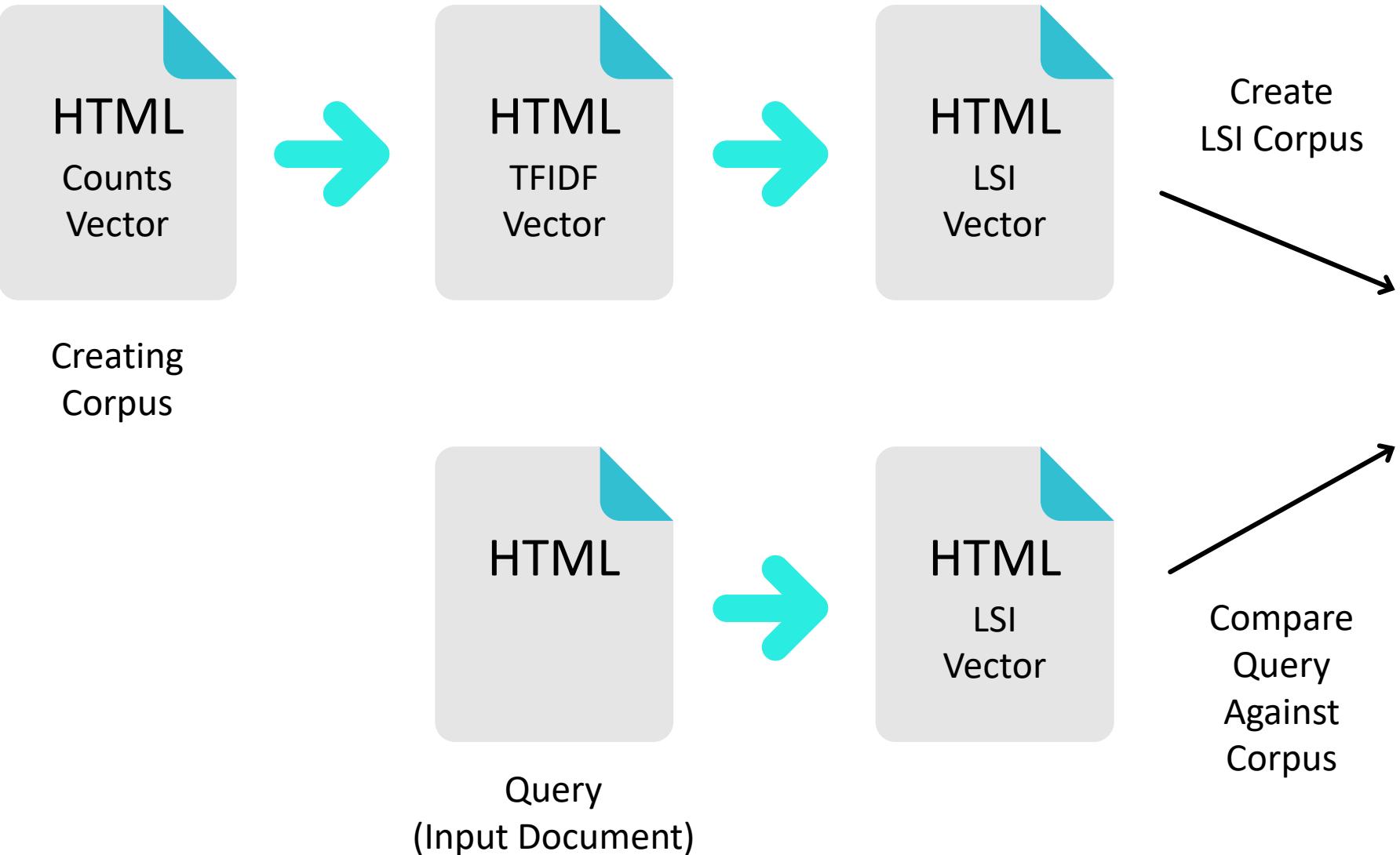
Acquiring Data

Filtering

NLP

Output





Detected Site: **Icoinbase.com**

Score: **0.9941726922988892**

Corpus hit: **Coinbase/www.coinbase.com.html**

Timestamp: **2016-08-01T01:44:05.296Z**

Icoinbase.com

[INVESTIGATE](#)

[BACK TO TOP](#)

WHOIS Record Data

Registrar Name: REGISTER.COM, INC. IANAID: 9

Last retrieved July 27, 2016

[GET LATEST](#)

[REPAIR](#)

Created: July 27, 2016

Updated: July 27, 2016

Expires: July 27, 2017

[Raw data](#) 

Email Address

Associated Domains

Email Type

Last Observed

joellima221@hotmail.com

1 Total - 1 malicious

Administrative, Registrant, Technical

Current

[Show past data](#)

Showing 1 of 3 Results



http://lcoinbase.com

coinbase

Products ▾

Help

Charts

Sign In

Sign Up

Sign In

Email



Password

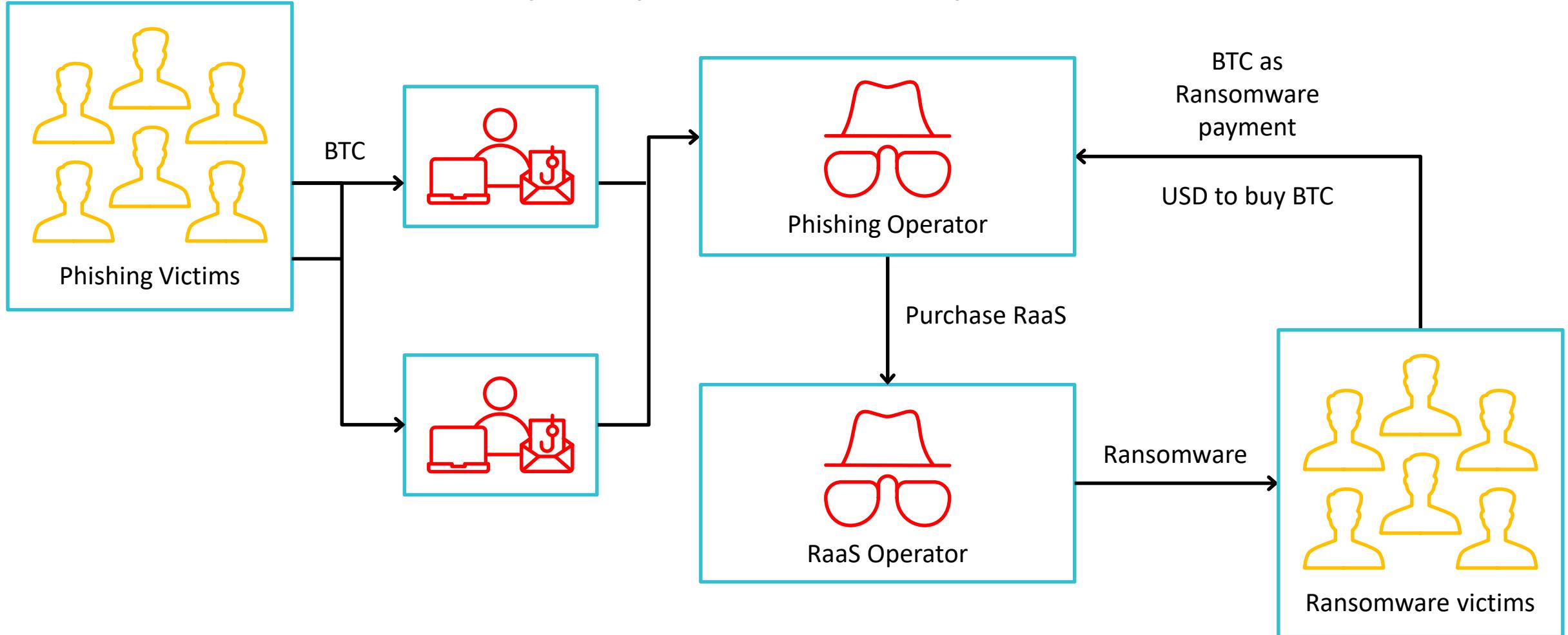


Keep me signed in on this computer

SIGN IN

Forgot password? · Don't have an account? Sign Up

Multiple cybercriminal operations



https://blockchain.info

KCHAIN WALLET DATA API ABOUT GET A FREE WA

Bitcoin Address

Addresses are identifiers which you use to send bitcoins to another person.

Summary		Transactions	
Address	19yAR4yvGcKV3SXUQhKnhi43m4bCUhSPc	No. Transactions	136
Hash 160	01b235ab3c269660c8c5239d6d97401a14624772	Total Received	\$ 1,879,471.35
Tools	Related Tags - Unspent Outputs	Final Balance	\$ 0.00

Request Payment Donation Button



Transactions (Oldest First)

(Fee: \$ 9.05 - 51.61 sat/WU - 206.43 sat/B - Size: 520 bytes) 2017-10-09 16:24:57

d714aef718de2245c5faf5fc7569073b5ee1893ed5bc7d73d2dd2f195f20b8cb	→	1NXaJmqv81NBjhJjhgP2hnFQy2tjwwytYX - (Spent)	\$ 5.17
1Q6ZXsWEy193C7f8GJeM8rEsq3JA9dMXC1 (\$ 11.21 - Output)		19FYuwJmYABDyz2ft1Awb2iG1yxcaLER7N - (Spent)	\$ 20.74
19yAR4yvGcKV3SXUQhKnhi43m4bCUhSPc (\$ 10.26 - Output)			
19yAR4yvGcKV3SXUQhKnhi43m4bCUhSPc (\$ 13.49 - Output)			

\$ -23.75

CoinCola Start Trading BTC, ETH, and BCH | Global OTC Marketplace
| 0% trading fee | Perfect time to invest

Start Trading

Oops, your files have been encrypted!

English



What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Payment will be raised on
5/16/2017 00:47:55

Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55

Time Left
06:23:57:37

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
[Copy](#)

[Check Payment](#) [Decrypt](#)

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

WARNING 0.203GB

```
> use WARNING
switched to db WARNING
> show collections
WARNING
system.indexes
> db.WARNING.find()
{ "_id" : ObjectId("5859a0370b8e49f123fcc7da"), "mail" : "harak1r1@sigaint.org"
, "note" : "SEND 0.2 BTC TO THIS ADDRESS 13zaxGVjj9MNc2jyvDRhLyYpkCh323MsMq AND
CONTACT THIS EMAIL WITH YOUR IP OF YOUR SERVER TO RECOVER YOUR DATABASE !"
}
> exit
bye
```

Time left before the price goes up
40:00:43

Price for decryption:
B = 0.05

Your computer files have been encrypted. Your photos, videos, documents But, don't worry! I have not deleted them, yet. You have 24 hours to pay 150 USD in Bitcoins to get the decryption key. Every hour files will be deleted. Increasing in amount every time. After 72 hours all that –

you are the victim of Zyk

Your important files encryption produced on this computer. Photos, videos, documents etc. Here is a complete list of encrypted files. You can verify this.

Encryption was produced using a unique public key, which is stored on a secret server on the Internet. To decrypt your files you need to obtain the private key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet, the server will delete files after 72 hours. After that, nobody and never will be able to access them.

To obtain the private key for this computer, which will automatically decrypt files, you need to pay 170 USD / 170 EUR to the BTC address below.

1GmQBH9ra2dqA8CgRgBa8Fngx4qJb2hLDW

If you do not have bitcoins you can buy them from LocalBitcoins.com. Thank you!

IMPORTANT INFORMATION !!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers. More information about the RSA and AES can be found here:
[http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server. To receive your private key follow one of the links:
1. <http://tor2web.org/>
2. <https://www.onion.cat/>



Event chain of the ransomware infection



- Infection & Encryption
- Incident response
- Restore from backup
- If no backup or backup isn't available - purchase cryptocurrency
- Pay
- Keep the rest of currency secured

RSA® Conference 2019

Conclusion



1

We are witnessing a **restructuring of the criminal economy and the methodology to launder their newly stolen digital assets.**

Anti-money laundering laws coming into play just moving 1 BTC making converting large amounts of crypto to fiat currencies no easy task. Criminals will have to figure out how to convert their money to FIAT via other means without tipping off law enforcement agencies of their fraudulent identity.

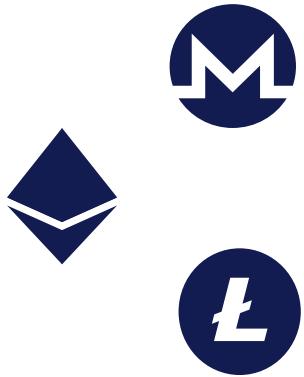


2

Individuals in crypto attacks are much “softer” targets than going after established financial institutions. Criminals from all realms, organized crime and nation-state are taking notice of this. As crypto asset technologies develop and enable millions to become their own bank. It is important to keep in mind that when you’re your own bank, security is imperative!

3

With recent Law Enforcement measures, such as take down of BTC-E exchange, criminals shifting their focus from well known and widely spread crypto currencies to new and upcoming currencies. They have also started to heavily target exchanges and startups working with crypto, which are easier targets and usually have limited or almost no security.



4

Protect your environment and look for not only Web based miners but also cryptomining software like Honeyminer that make DNS queries. DNS level identification is a great way to determine if your environment has a cryptomining problem or not – then you can remediate. This type of activity will considerably increase in the next few years. Make sure you are keeping an eye on your environment.



Apply What You Have Learned Today

- Next week you should:
 - Look through your DNS query logs for substantive (500+ queries a day) cryptomining pool traffic from one or several machines
 - For cloud computing instances, look for increases in CPU utilization – could be as small as a 10%-15% increase
- In the first three months following this presentation you should:
 - Add popular cryptomining sites to your domain block lists for all of your endpoints
 - If you find considerable and consistent cryptomining DNS traffic - you might have mining software installed which means someone internally or externally installed it (potential IOC)
- Within six months you should:
 - Stay vigilant and keep adding new mining pool sites to your blocklist (they popup every couple of weeks)
 - Consider using a vendor (Cisco Umbrella) who has security policies designed to block cryptomining traffic

Questions?

@armcbride1

aumcbrid@cisco.com

@akfirat

ayse@cisco.com

www.umbrella.cisco.com

