RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SEM-M03B

Cryptojacking: What's in your Environment?

Austin McBride

Threat Analytics Researcher
Cisco Umbrella
@armcbride1

RSAConference2019

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

cisco

RSAConference2019

Cryptocurrency

Cryptocurrency's Meteoric rise

- 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

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
- Where there is money, there are criminals – most of them are external

RSAConference2019

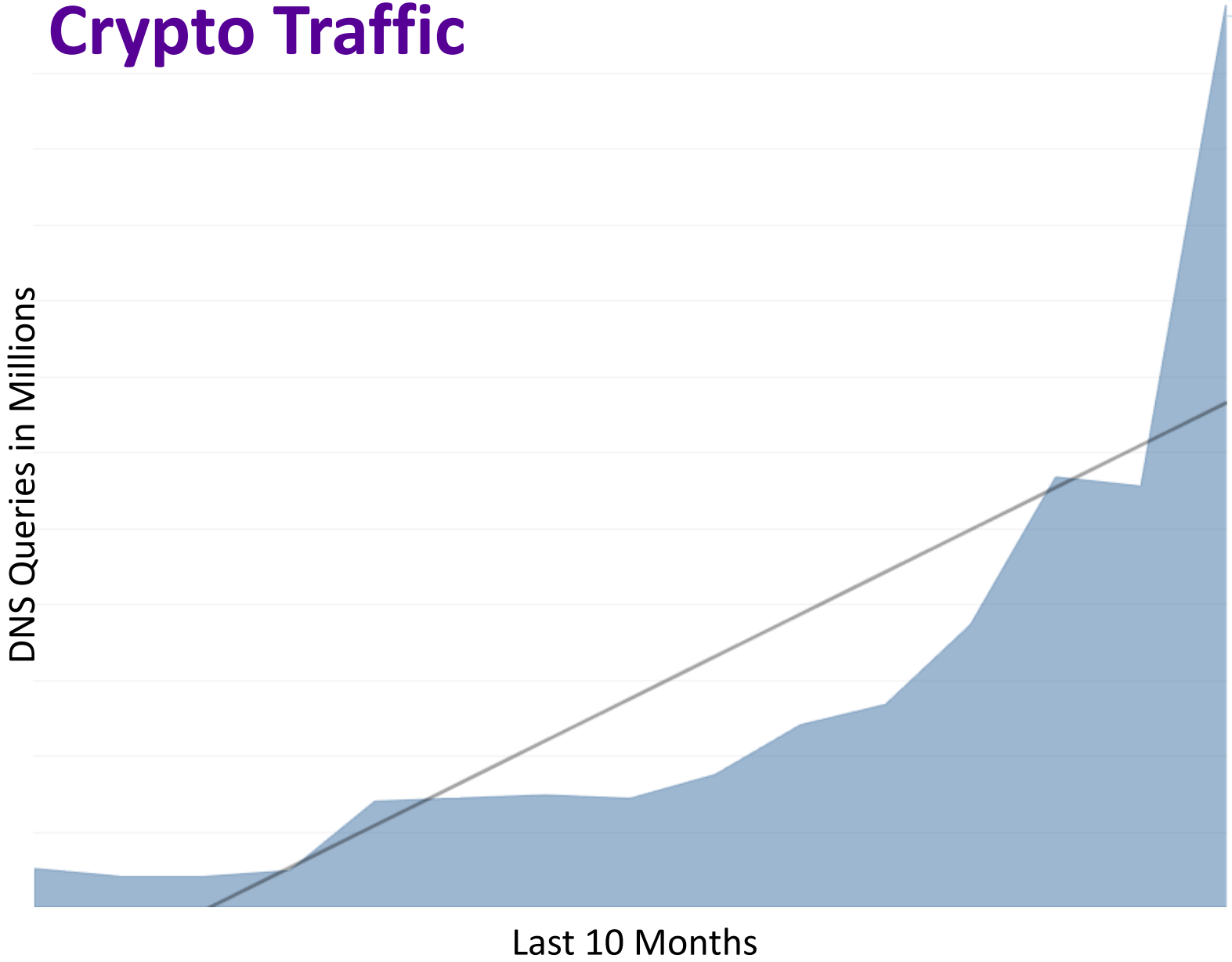
So how does cryptojacking fit in?

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.

cisco

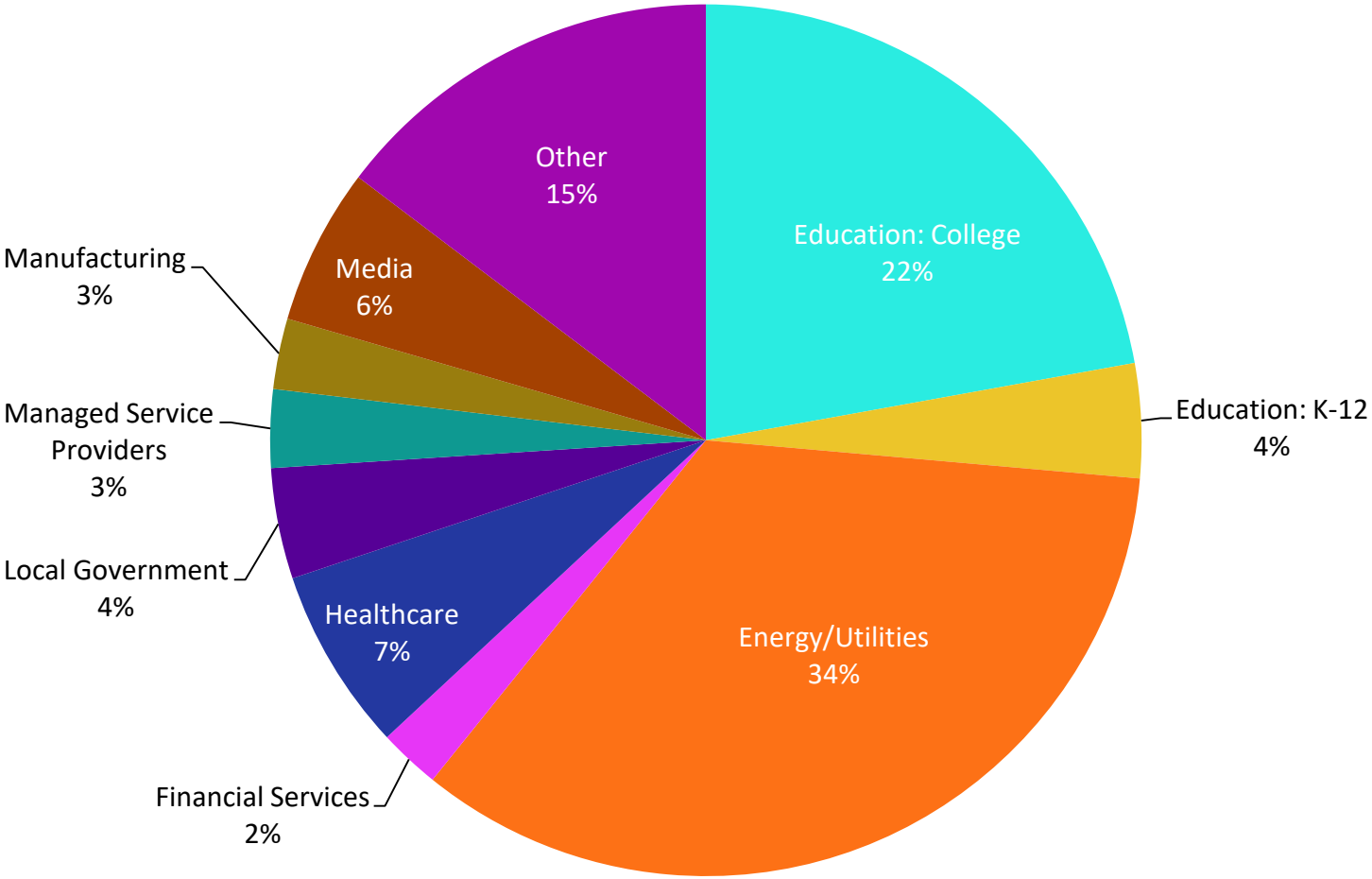
Crypto Traffic



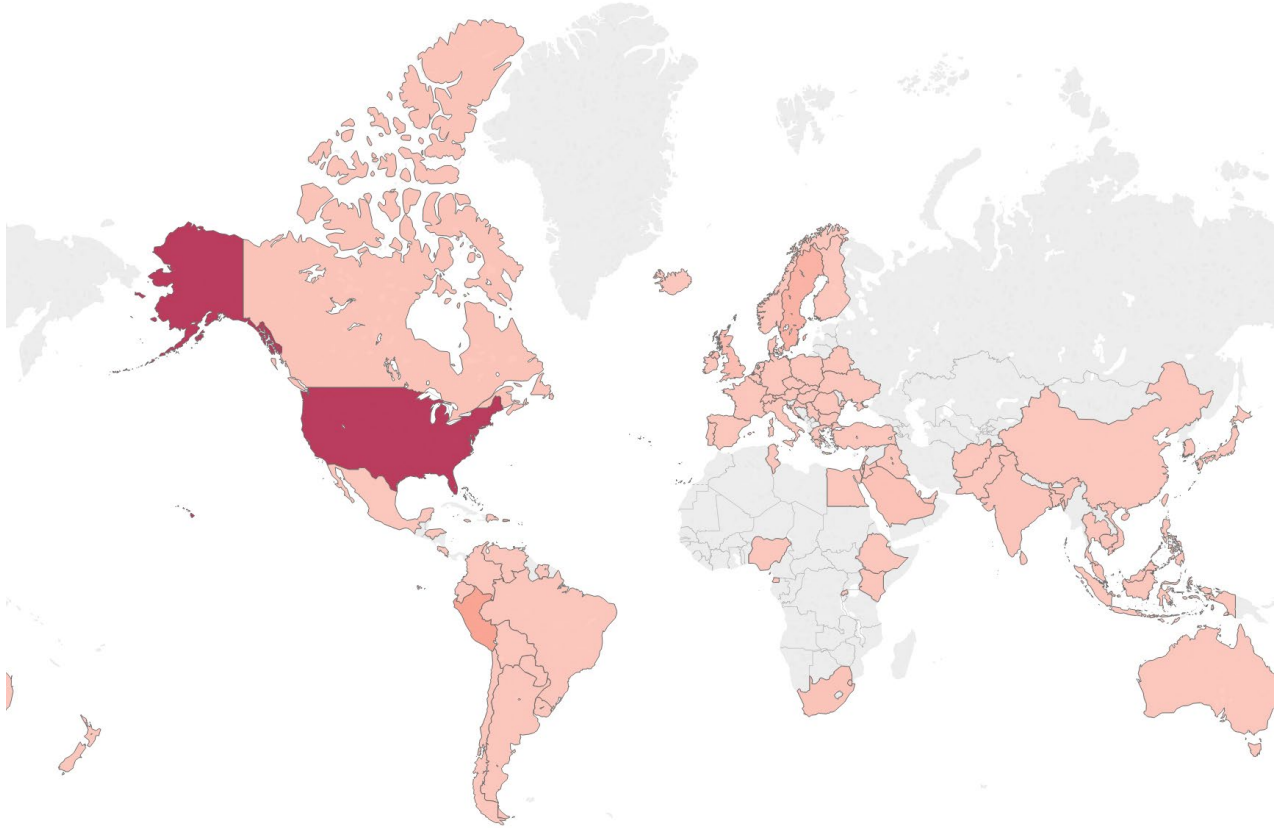
- Last 10 months: 200x increase in crypto related traffic
- The majority of traffic are cryptomining pools, but also some sites that drop mining software onto your machine
- Distribution of crypto traffic affects all industries, not just financial services

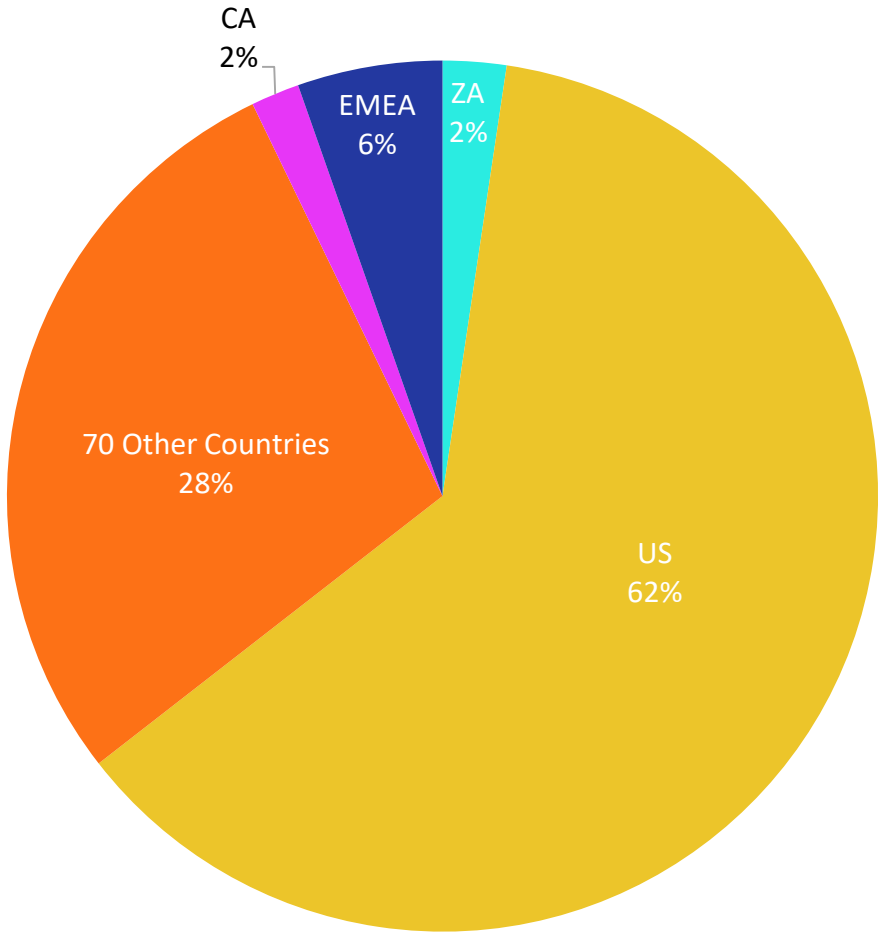
Crypto Traffic Industry Distribution

- 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



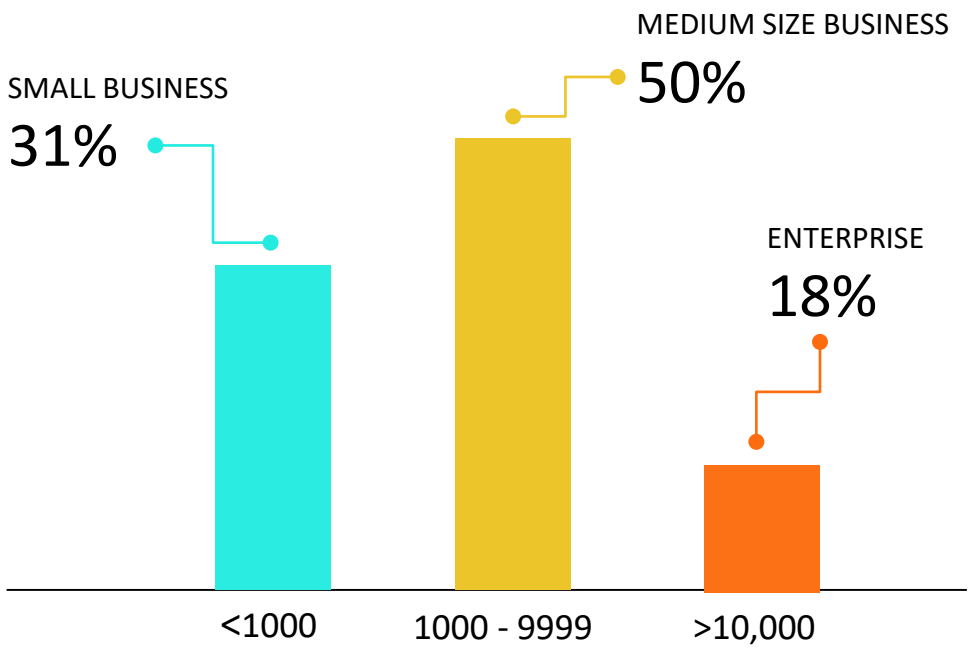
Crypto Traffic Geo Distribution





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

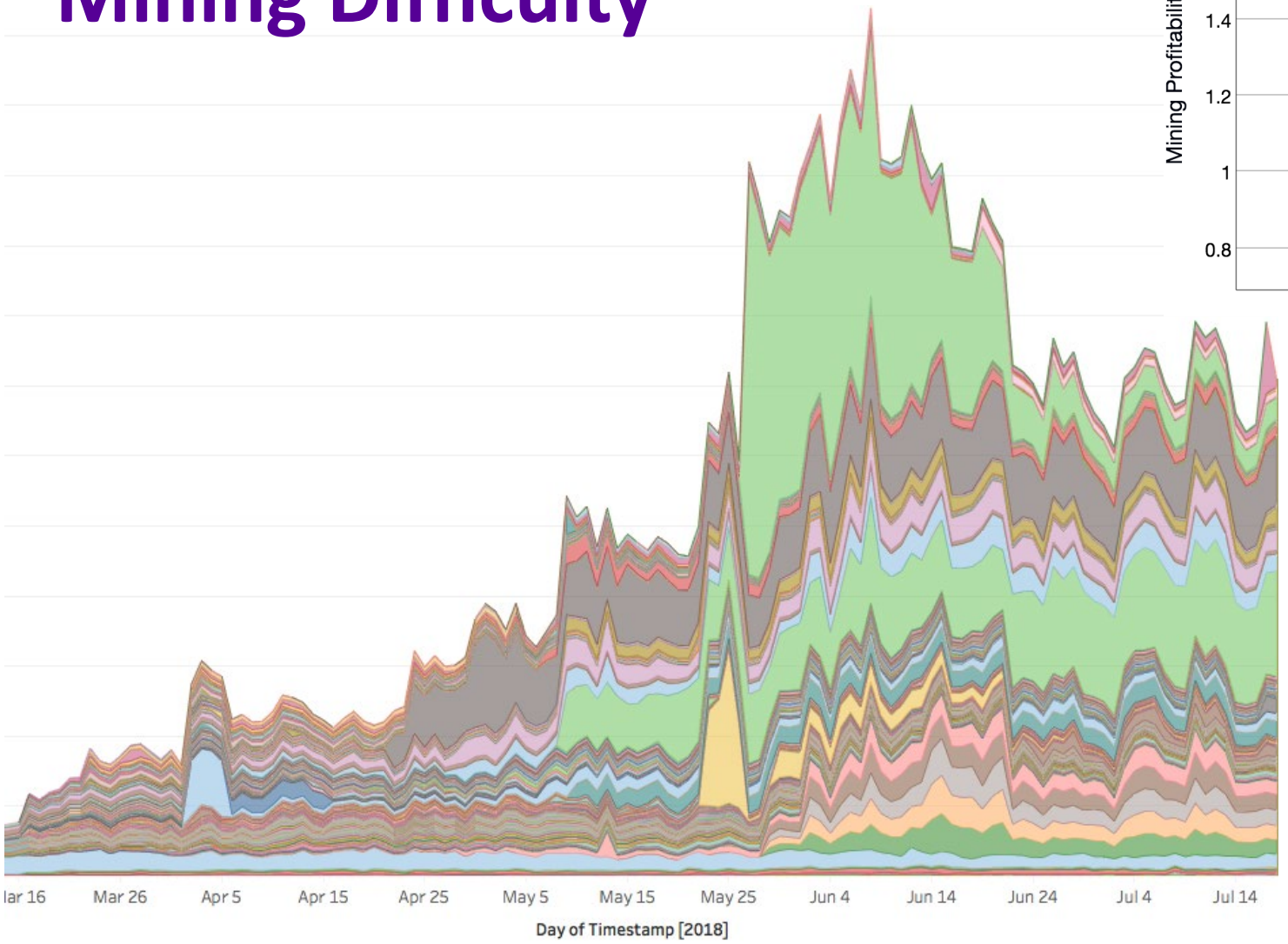
SMBs Are More Vulnerable to Cryptomining Malware



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

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

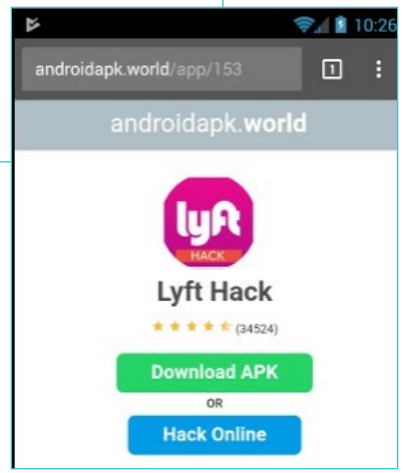
- With cloud based miners like Coinhive the cost to the malicious actor generally no more than 30% of whatever they were able to mine in your environment
- The real upfront cost for them is what ever they had to do leverage your machine (very inexpensive)

Cryptojacking

WIRED

LILY HAY NEWMAN SECURITY 02.20.18 05:06 PM

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



TC

Natasha Lomas @riptari / Feb 12, 2018

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

Javascript Injections

https://coinhive.com

```
<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

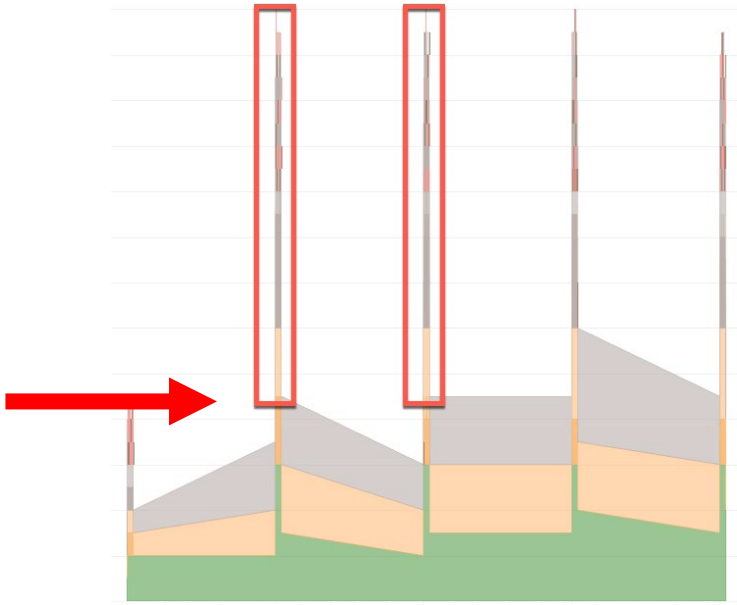
Weaponized Cryptomining?

Why We Should Care

1

Web-Based Miners:

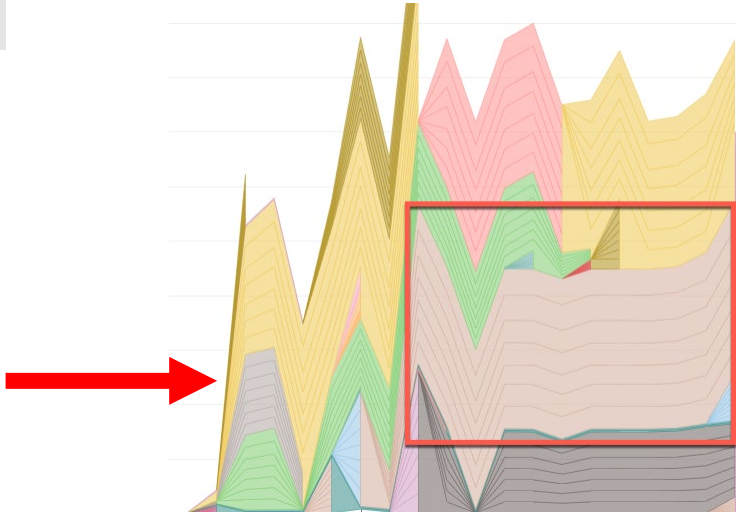
Generally only impact a machine while a user is on a webpage and does not persist after you close the page. Little risk of damaging machine hardware.



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.

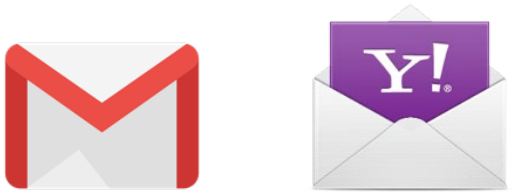


RSAConference2019

Crypto phishing

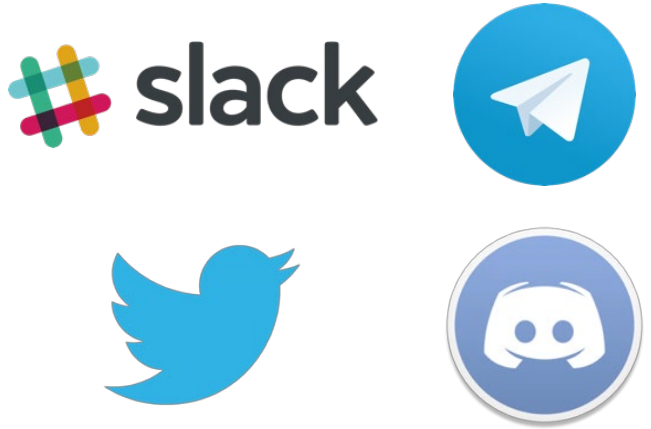
Delivery Vectors

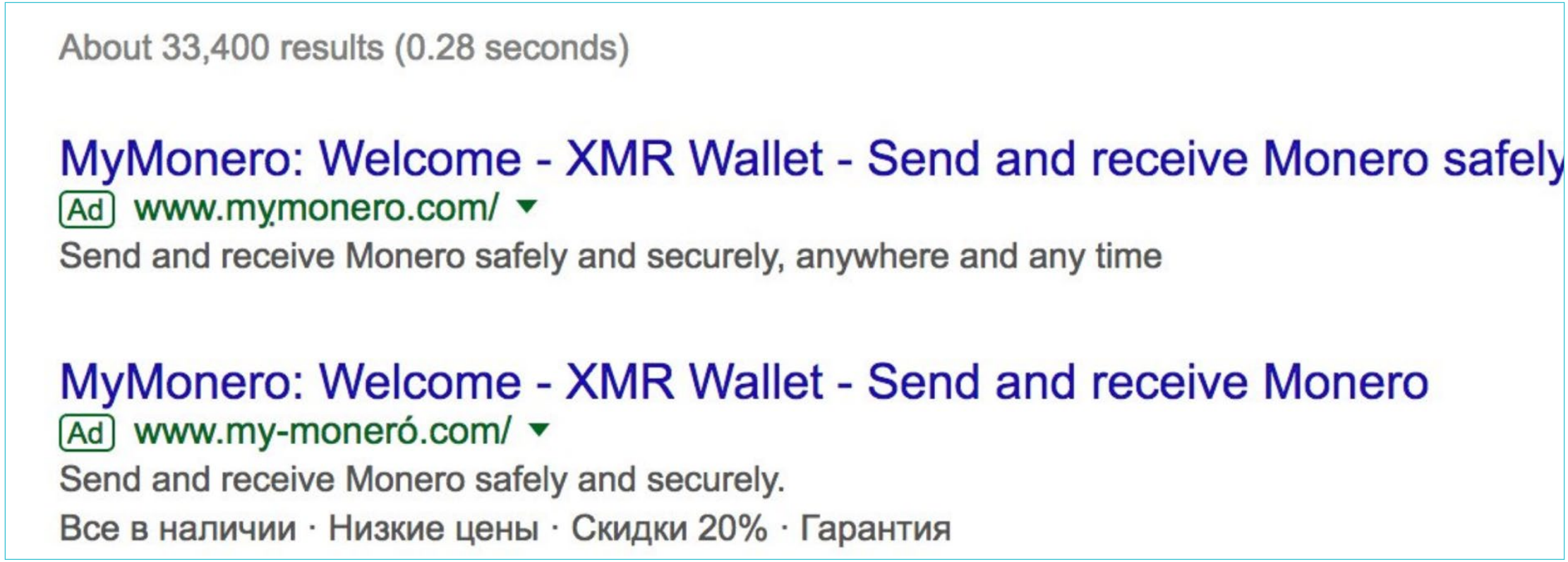
Email

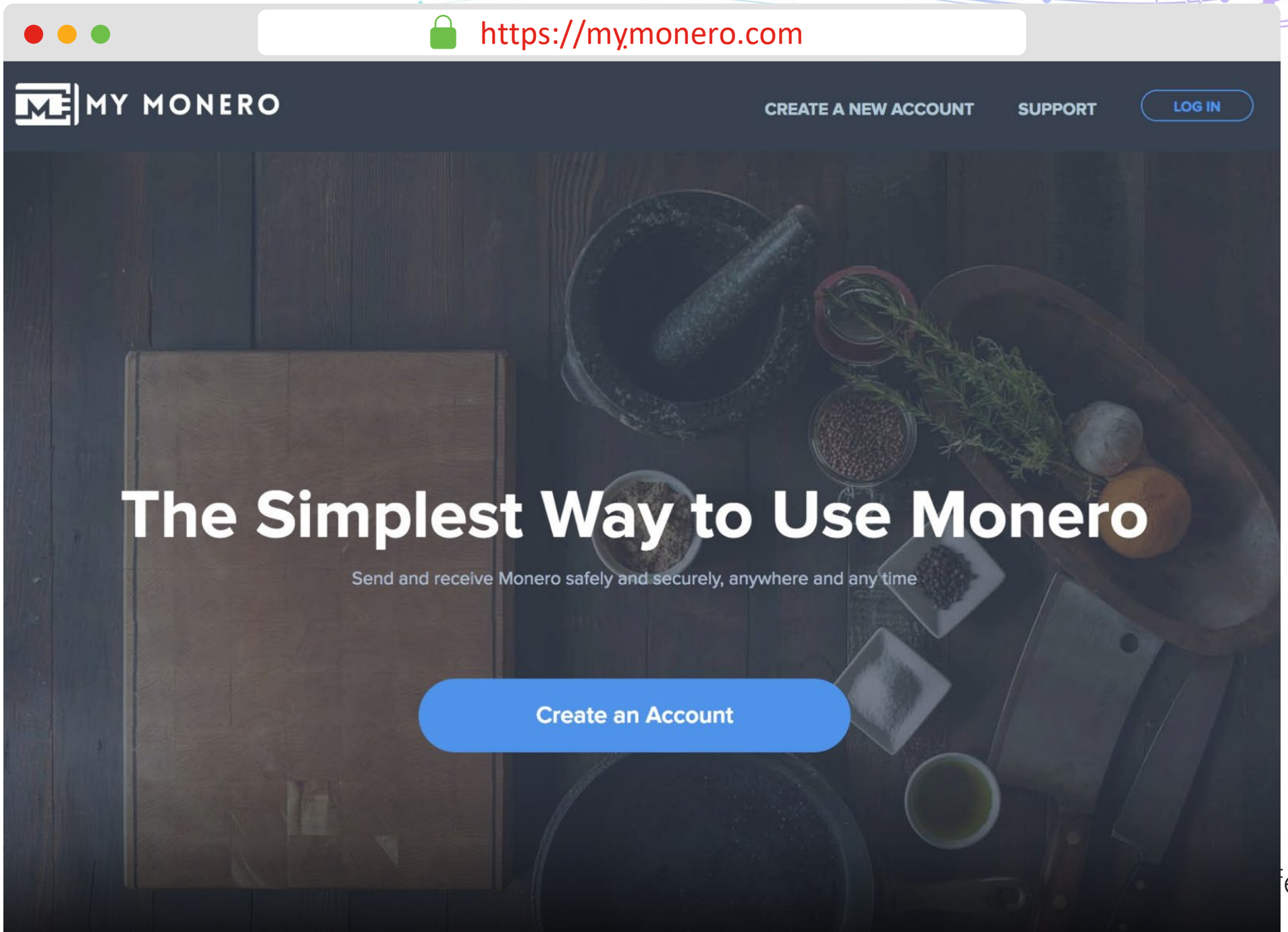


Search Engine Ads

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-moneró.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

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>

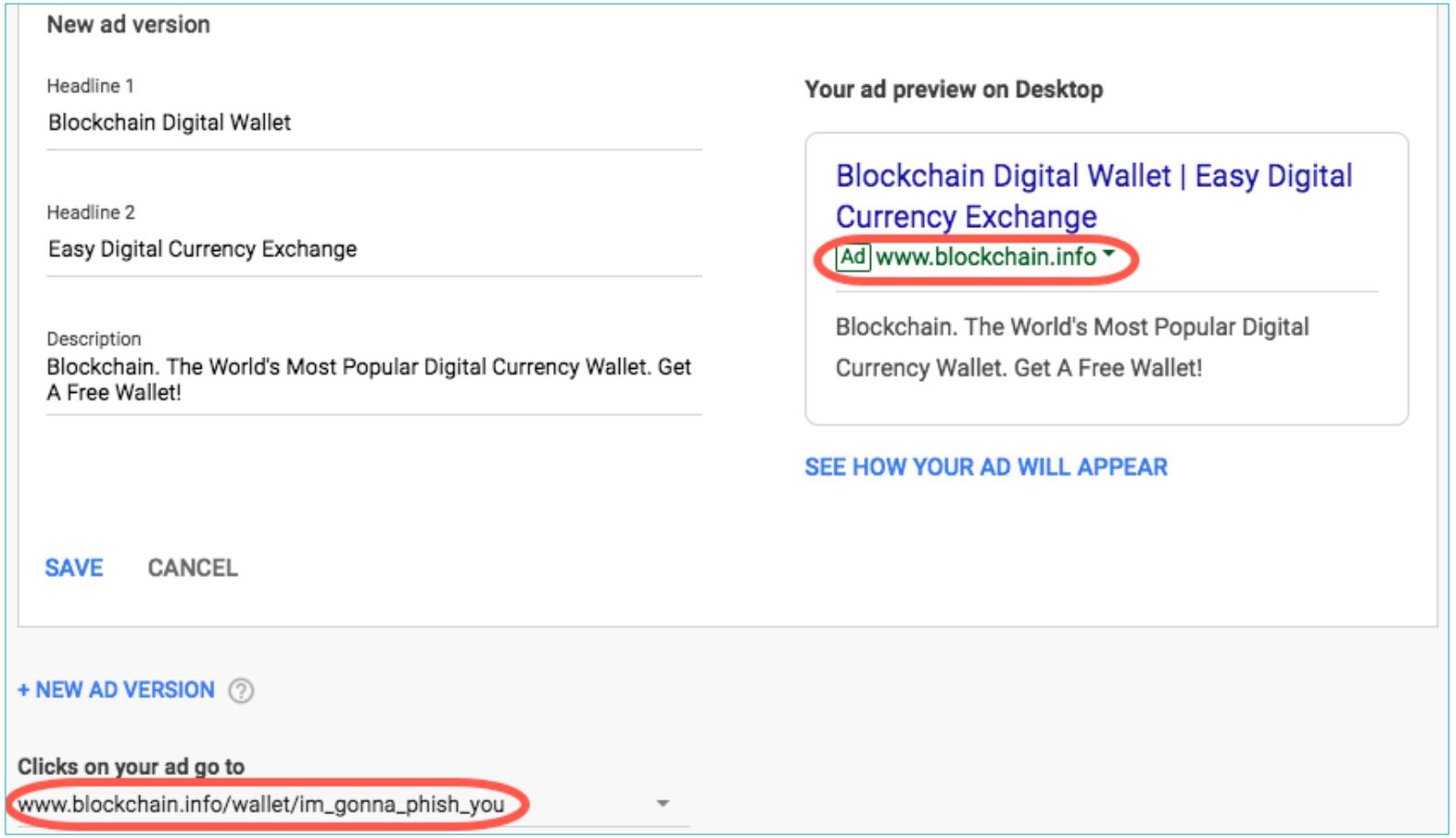
Period of Validity

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

Google AdWords



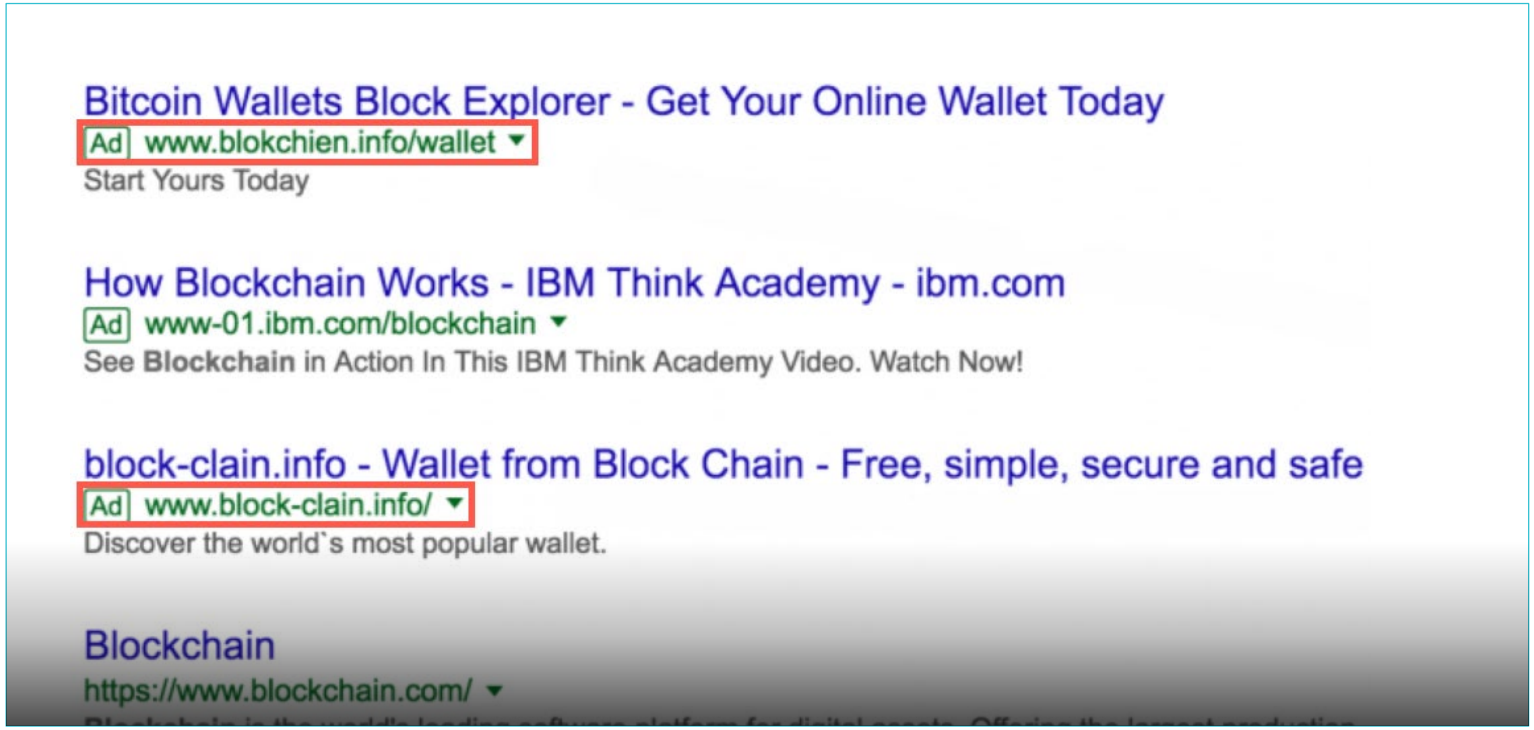
- A malicious actor would need to infiltrate www.blockchain.info
- Create a subdirectory (e.g. /wallet/im_gonna_phish_you)
- Then setup a redirect to their fake site (www.blockchain.com/Blockchain/Wallet) to phish your credentials and gain access to your wallet's funds

RSAConference2019

Targeting Exchanges and AltCoins

Crypto Phishing and Scams

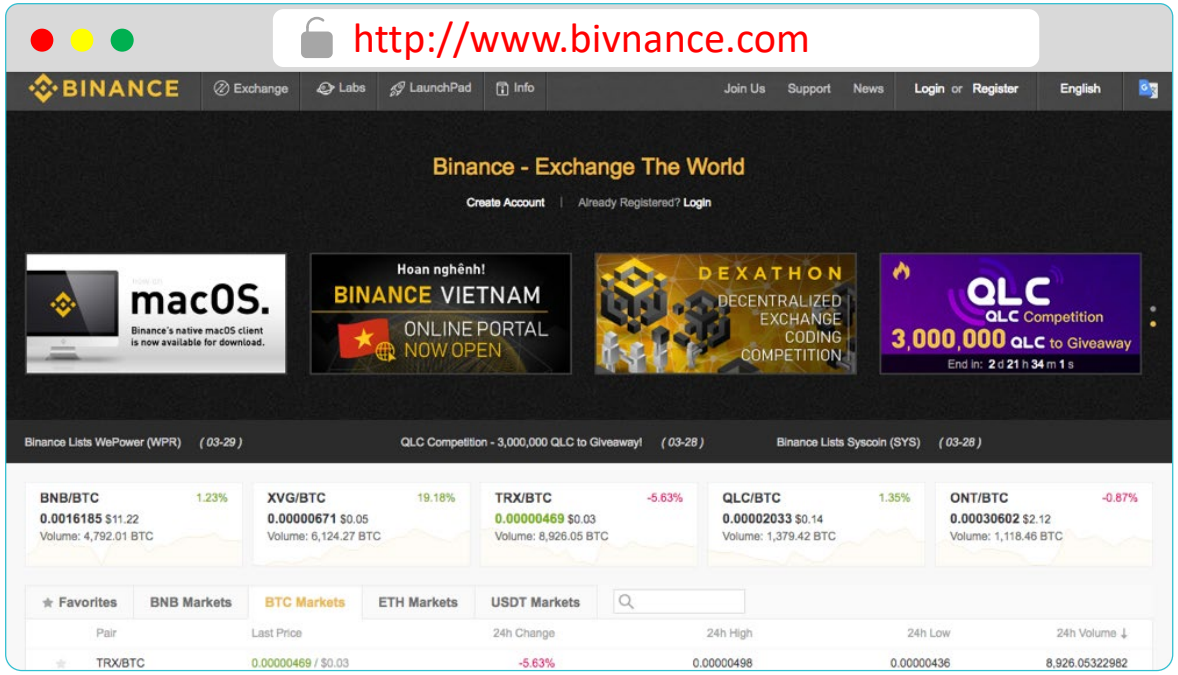
Crypto exchange phishing sites are on the rise and they are using advertisements on search engines to lure people into giving up their credentials

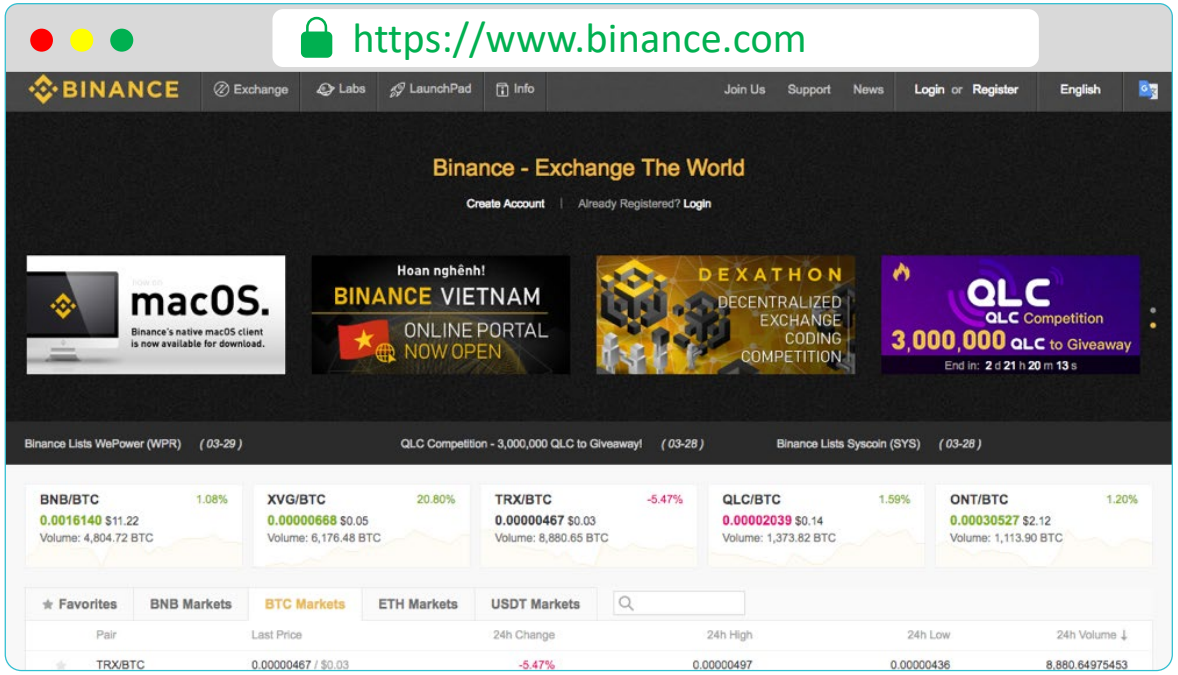


We’re giving away ETH! Just send me 0.2 ETH and I’ll send you back 2 ETH. Send me your crypto to the address below…

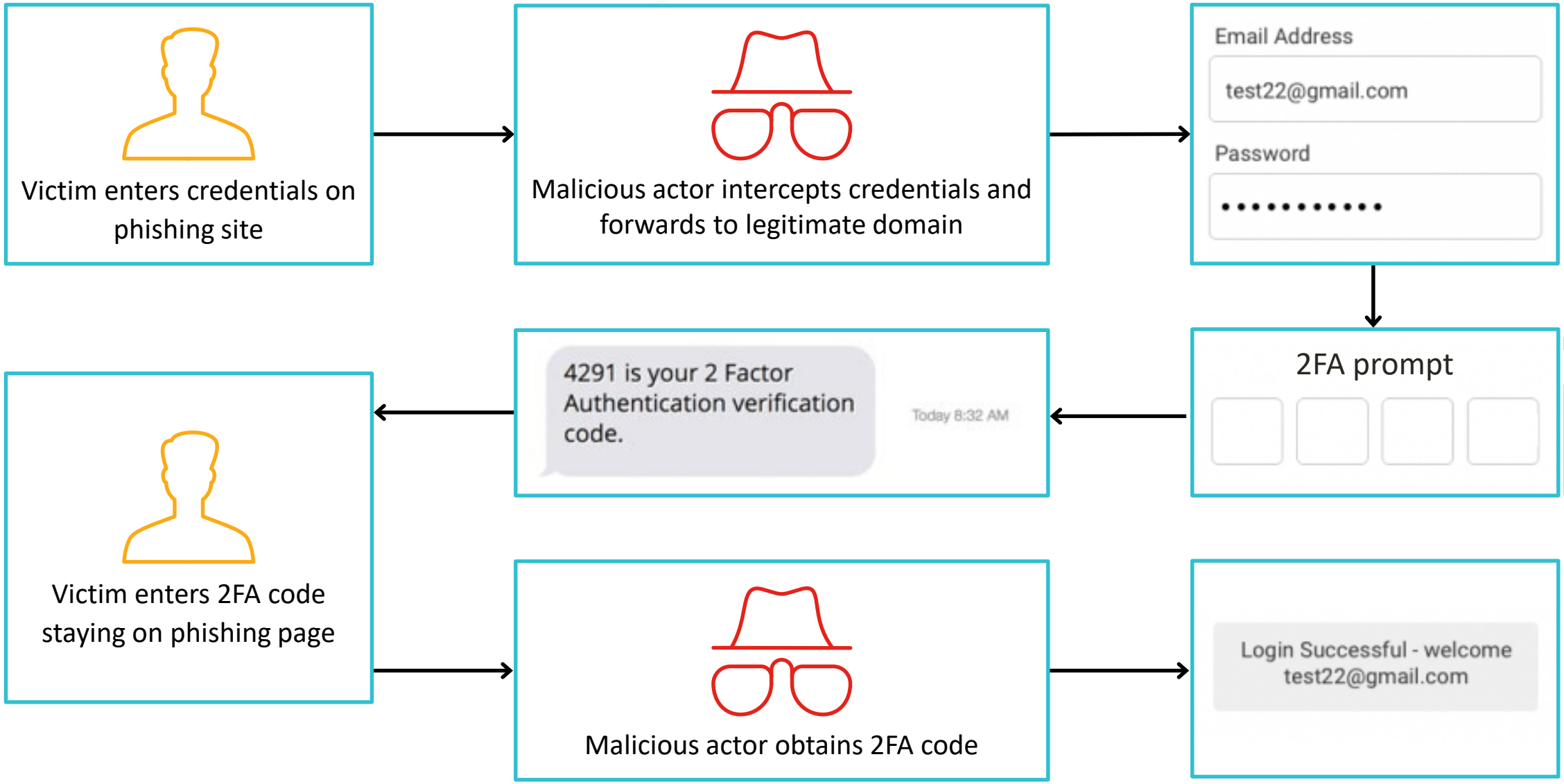
Crypto Phishing targeting exchanges

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

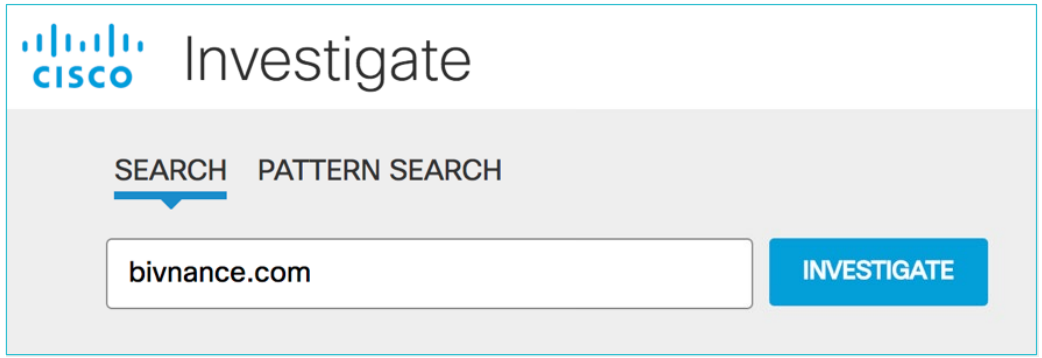


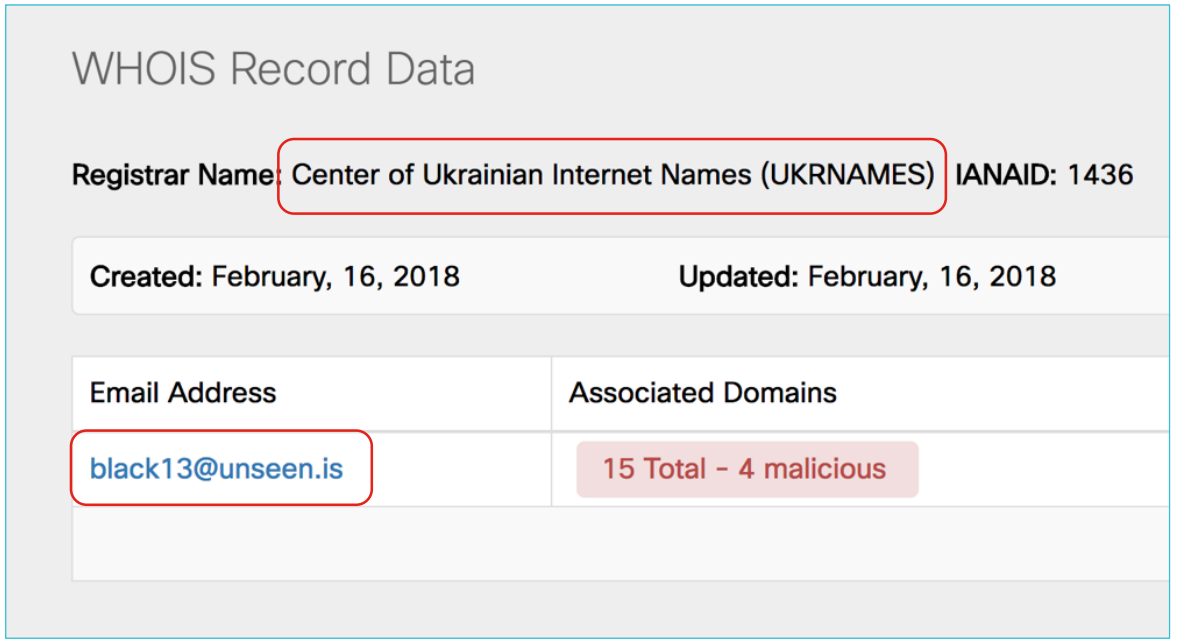


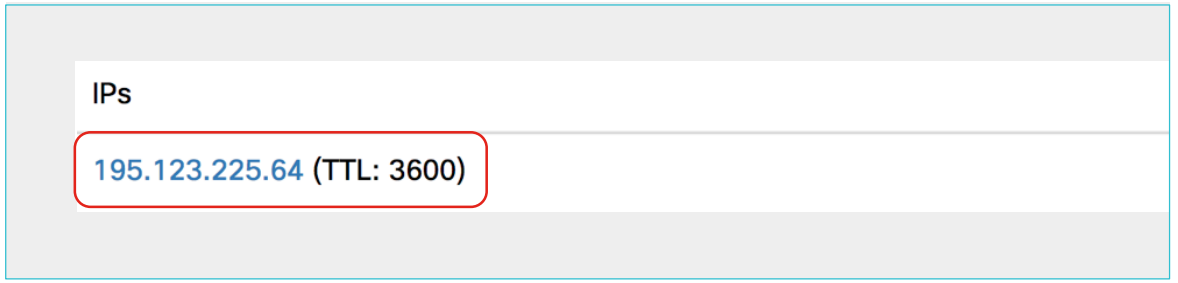
2FA Bypass


Victim enters credentials on phishing site
Malicious actor intercepts credentials and forwards to legitimate domain
Email Address
test22@gmail.com
Password
2FA prompt
4291 is your 2 Factor Authentication verification code.
Today 8:32 AM
Victim enters 2FA code staying on phishing page
Malicious actor obtains 2FA code
Login Successful - welcome test22@gmail.com

What do we know about www.bivnance.com?







Domains Associated with black13@unseen.is

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

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.binanceit.com

What else is black13@unseen.is after?

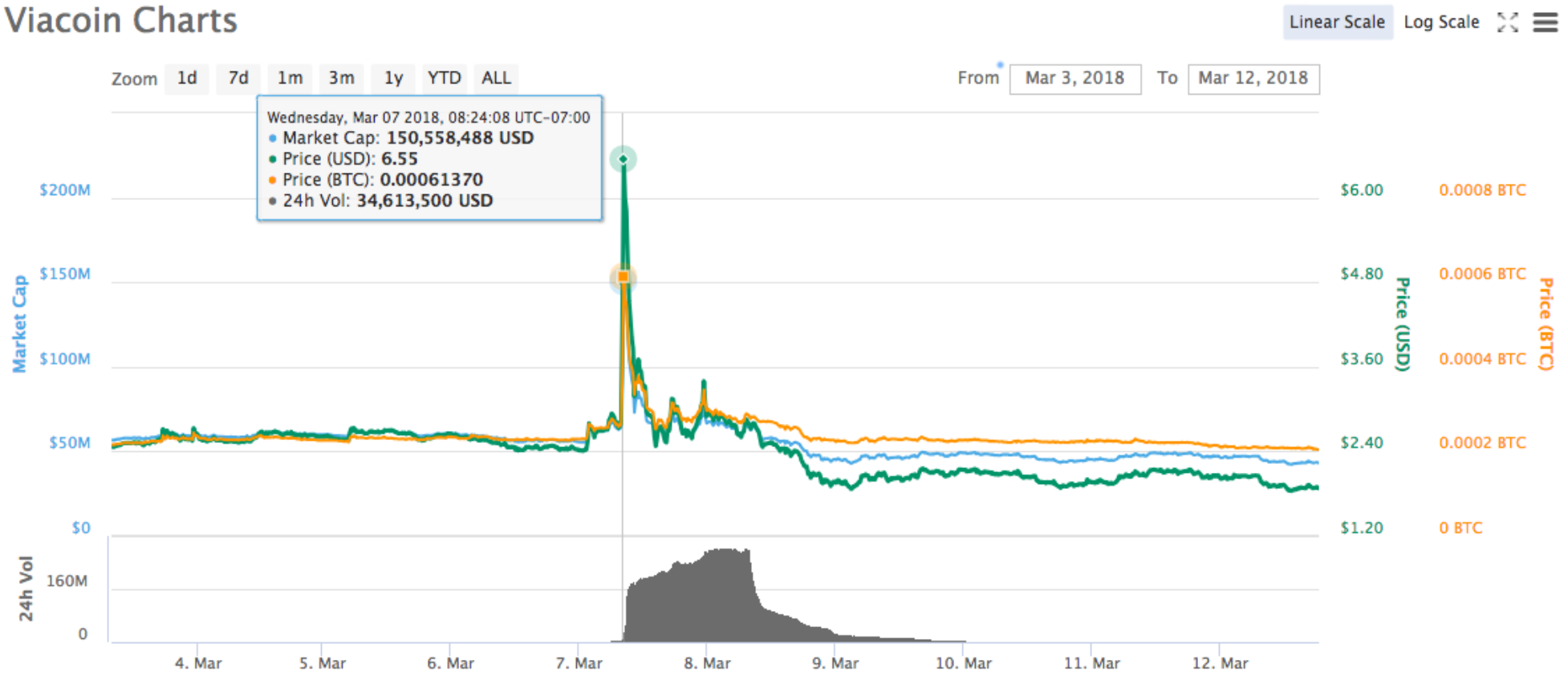
Maybe all of your ERC20 tokens…

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



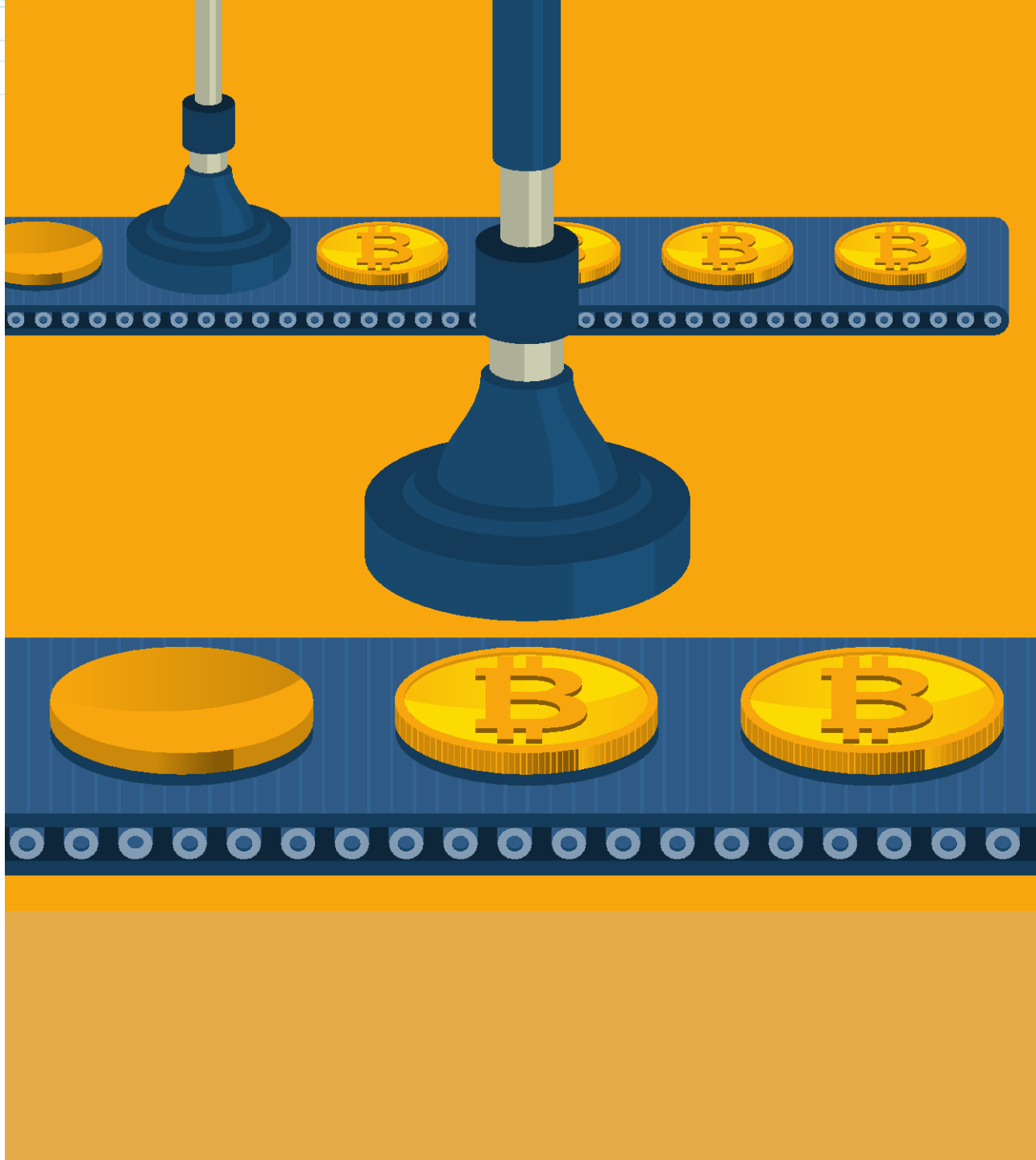
RSAConference2019

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

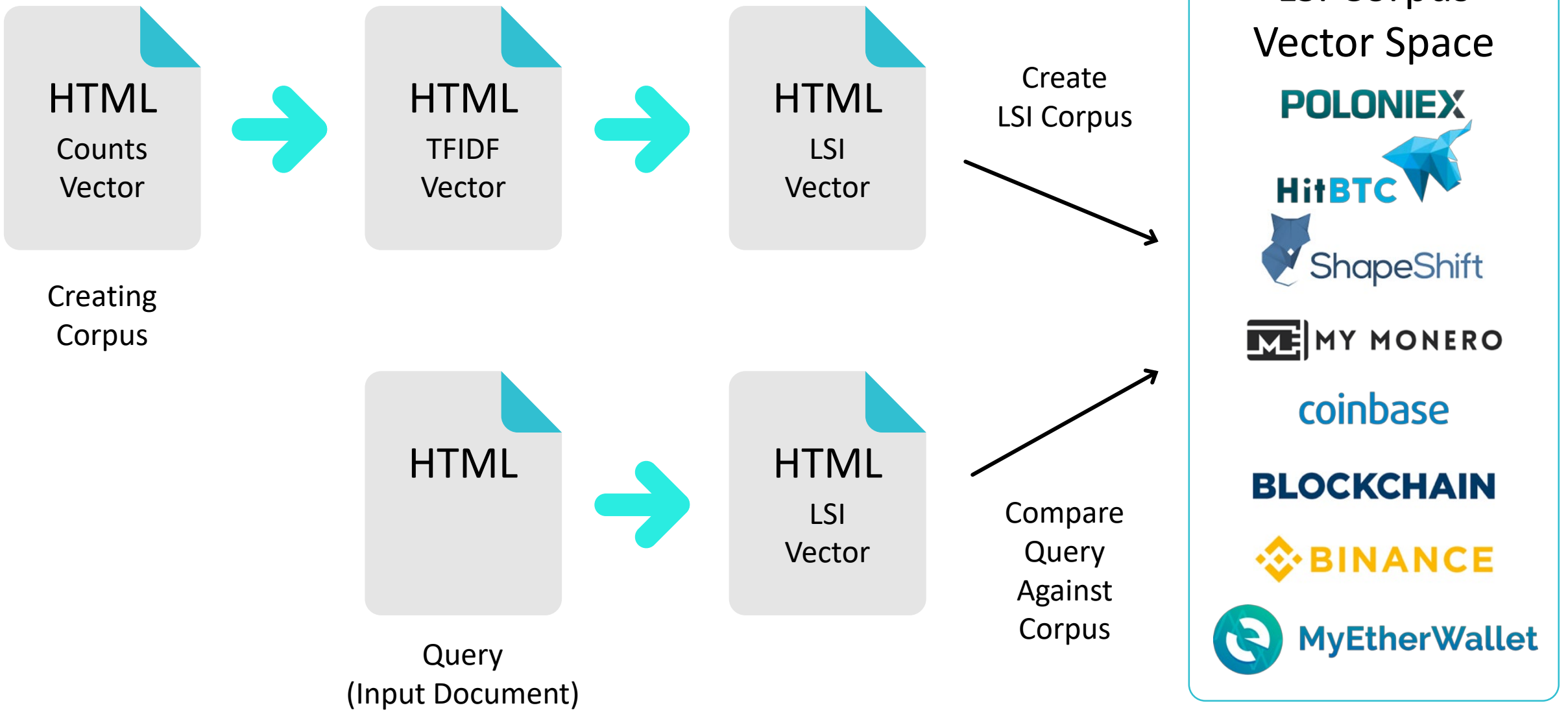


coinhive.com INVESTIGATE BACK TO TOP

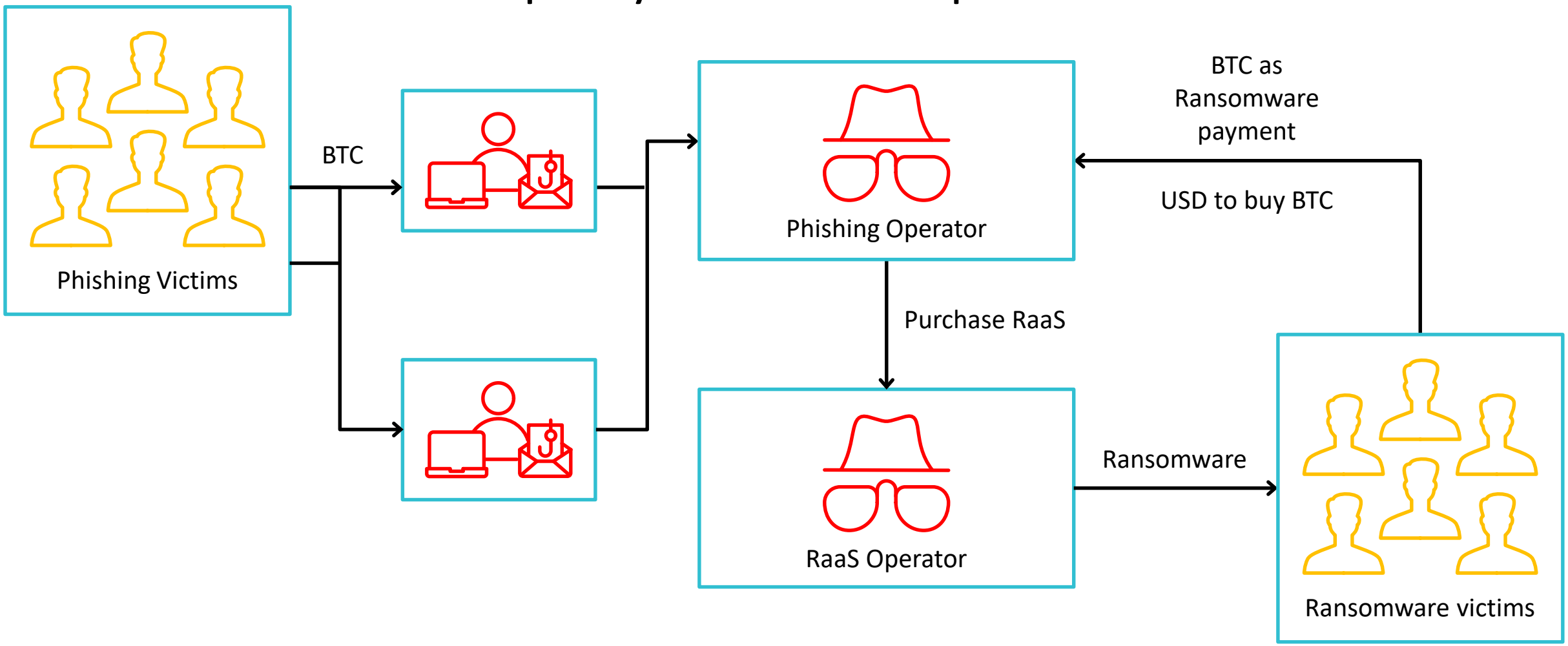
Co-occurrences

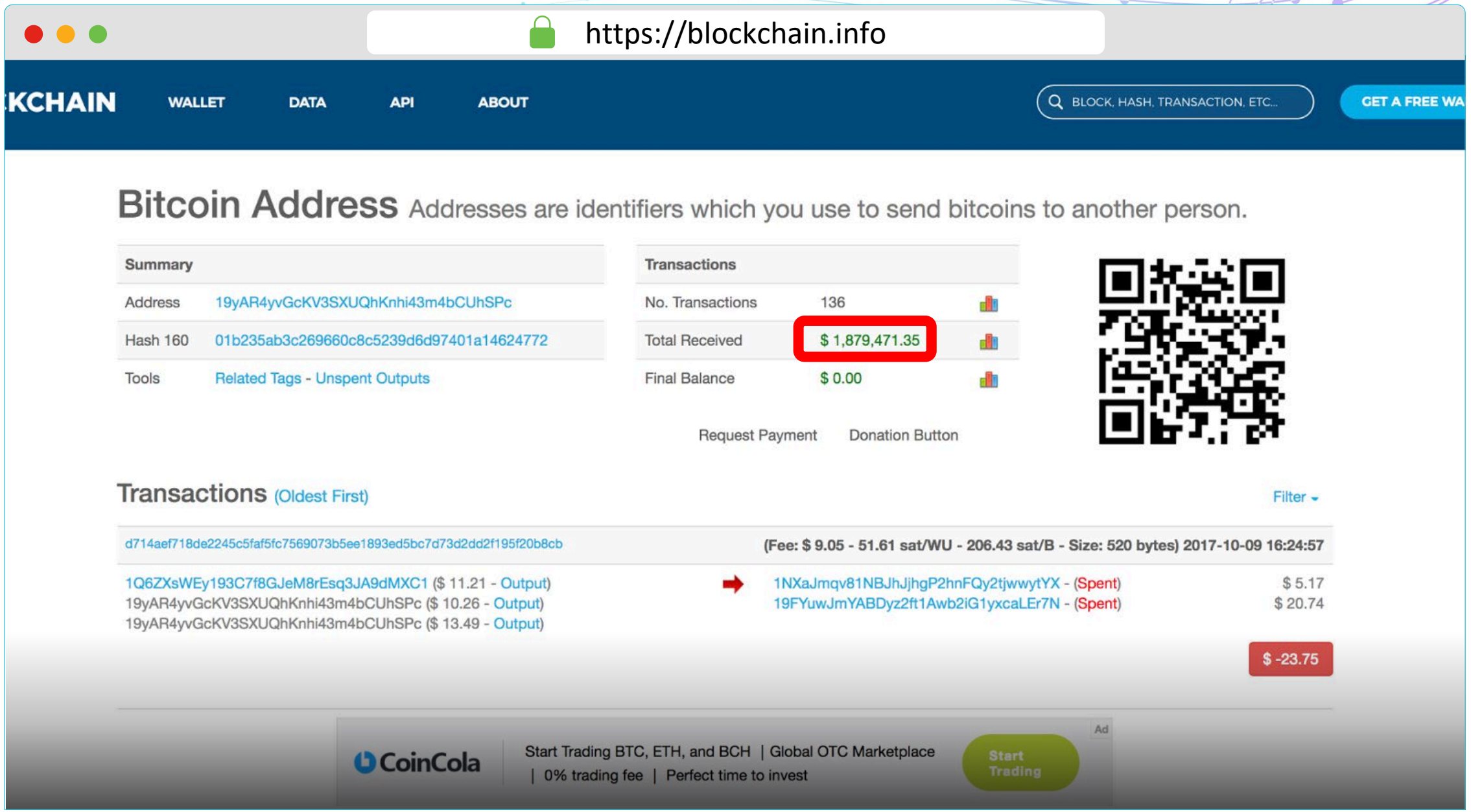
asset.epub.pub (4.91) hemnes.win (4.91)
https-bookmp3-ru.disqus.com (4.91)
img.p2pbg.com (4.91) l4oecosq.com (4.91)
www.tv-vip.com (4.91) pl14313817.puserving.com (4.43)
s1.cpmaffiliation.com (4.02) xmrmsft.com (4.00)
cdn.multiup.org (3.66) down.foxbeen.com (2.85)
callumaumusic.com (2.60) cdn.mngwefal.com (2.54)
adserpub.com (2.49) sihirdarrehberi.com (2.33)
cosmic-bio.com (2.04) www.linkslot.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) alibestru.ru (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


HTML
Counts
Vector
HTML
TFIDF
Vector
HTML
LSI
Vector
Create
LSI Corpus
LSI Corpus
Vector Space
POLONIEX
HitBTC
ShapeShift
MY MONERO
coinbase
BLOCKCHAIN
BINANCE
MyEtherWallet
Creating
Corpus
HTML
HTML
LSI
Vector
Compare
Query
Against
Corpus
Query
(Input Document)

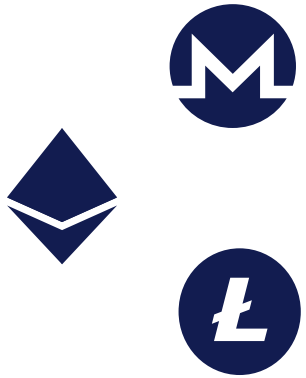
Multiple cybercriminal operations




https://blockchain.info
KCHAIN
WALLET
DATA
API
ABOUT
BLOCK, HASH, TRANSACTION, ETC...
GET A FREE WA
Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.
Summary
Address 19yAR4yvGcKV3SXUQhKnhi43m4bCUhSPc
Hash 160 01b235ab3c269660c8c5239d6d97401a14624772
Tools Related Tags - Unspent Outputs
Transactions
No. Transactions 136
Total Received $ 1,879,471.35
Final Balance $ 0.00
Request Payment
Donation Button
Transactions (Oldest First)
Filter
d714aef718de2245c5faf5fc7569073b5ee1893ed5bc7d73d2dd2f195f20b8cb
(Fee: $ 9.05 - 51.61 sat/WU - 206.43 sat/B - Size: 520 bytes) 2017-10-09 16:24:57
1Q6ZXsWEy193C7f8GJeM8rEsq3JA9dMXC1 ($ 11.21 - Output)
19yAR4yvGcKV3SXUQhKnhi43m4bCUhSPc ($ 10.26 - Output)
19yAR4yvGcKV3SXUQhKnhi43m4bCUhSPc ($ 13.49 - Output)
1NXaJmqv81NBJhJjhgP2hnFQy2tjwwytYX - (Spent) $ 5.17
19FYuwJmYABDyz2ft1Awb2iG1yxcaLEr7N - (Spent) $ 20.74
$ -23.75
CoinCola
Start Trading BTC, ETH, and BCH | Global OTC Marketplace
| 0% trading fee | Perfect time to invest
Start Trading
Ad

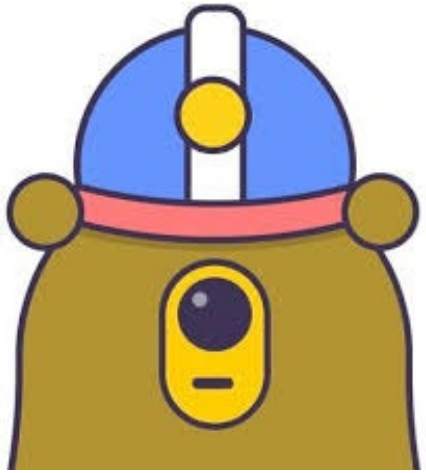
RSAConference2019

Conclusion



1

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.



2

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

www.umbrella.cisco.com