ITU Asia-Pacific Centre of Excellence Training
On
“Distributed Ledger Technologies (Blockchain) Ecosystem and Decentralization”

3-6 September 2018,

Bangkok, Thailand

Distributed Ledger Technologies (Blockchain)

Security Aspects of DLTs

Dr. Leon Perlman
Head: DFS Observatory @ CITI
Columbia University, New York, USA

Columbia Business School

@leonperlman

Due to a widespread start-up mentality in the crypto-economy, security often takes a **backseat** to growth.

Types of Security Threats

- Blockchain attacks
- Phishing
- Malware
- Cryptojacking
- Endpoint miners
- Implementation vulnerabilities
- Wallet theft
- Technology attacks
- Legacy attacks modernized
- Dictionary attack
- Quantum Computing

McAfee

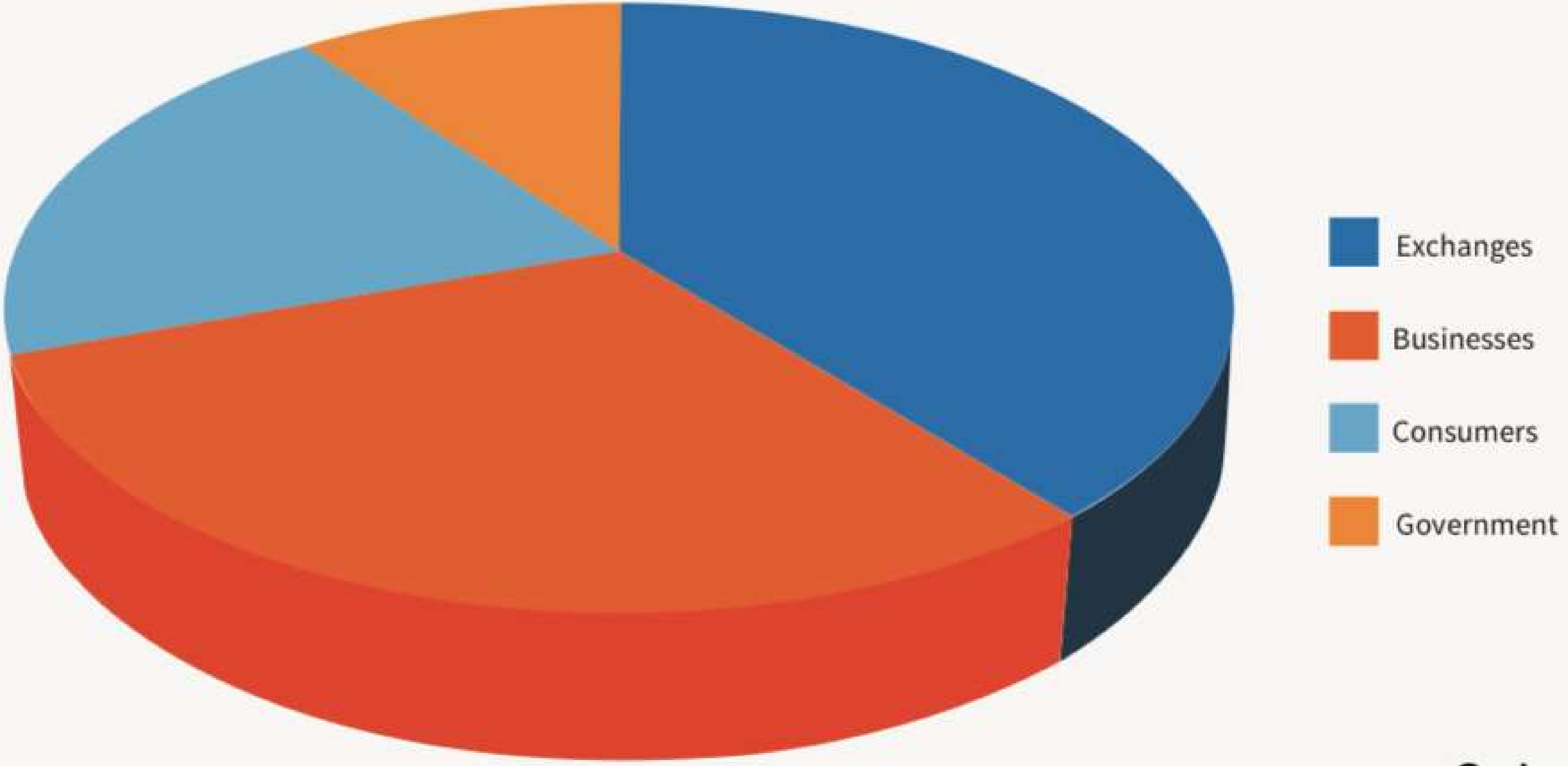
Attacks

2017: Hacking attacks were of 3 types:

- Attack on:
  - The blockchains
  - Cryptocurrency exchanges
  - ICOs
- Distribution of software to do hidden mining
- Attacks directed at users' crypto wallets.

Hackernoon

MOST OFTEN TARGETED BY CRYPTOCURRENCY-RELATED ATTACKS



Carbon Black.

Attacks

- In most cases, the **consumers** of blockchain technology are the easiest targets.

- Attackers have adopted several methods to target consumers and businesses using well-established techniques.

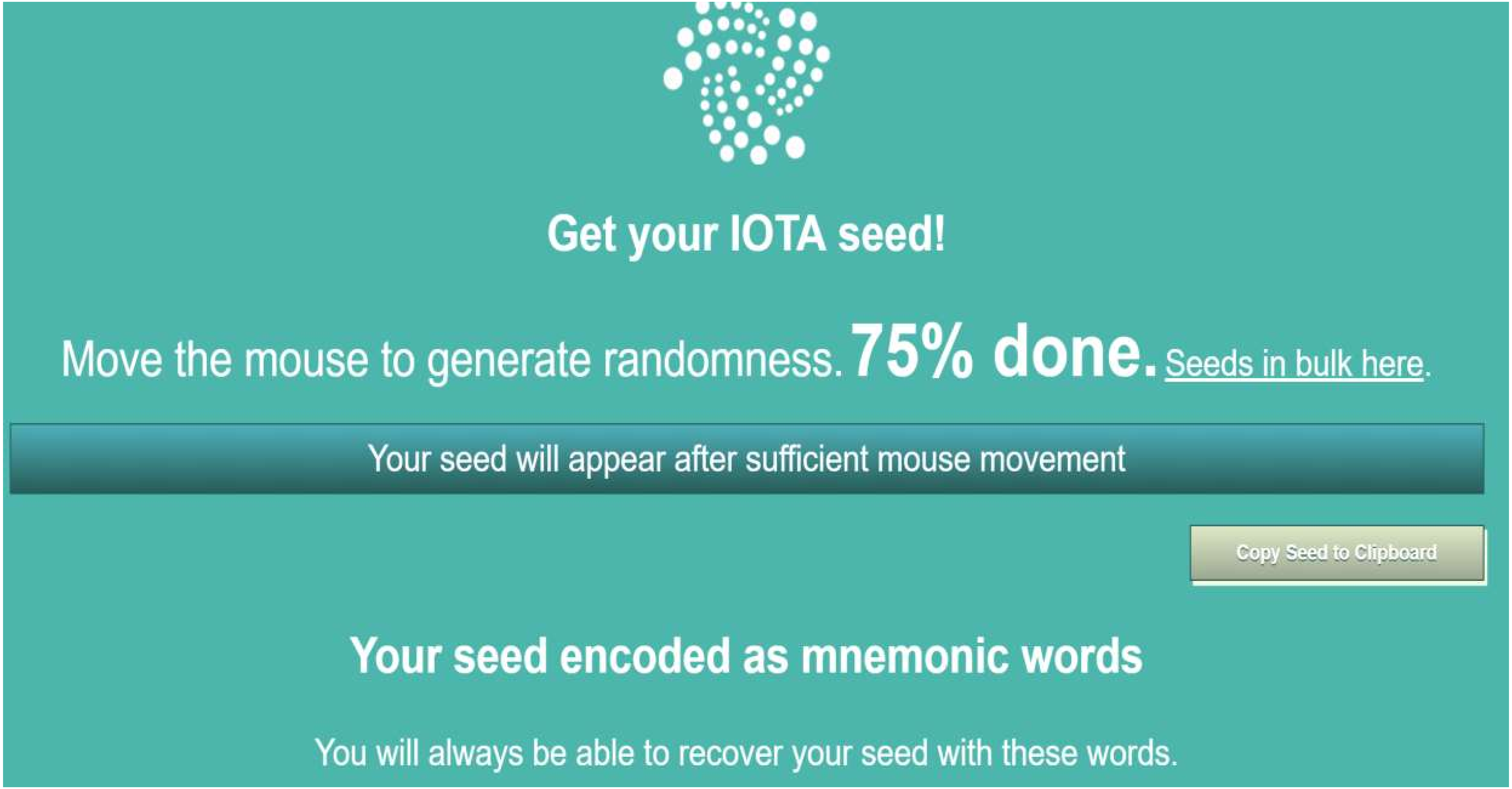
- **Primary** attack vectors include:
  - Phishing
  - Malware (examples: ransomware, miners, and cryptojacking)
  - Implementation vulnerabilities
  - Technology
  - Phishing

McAfee

Phishing

- Phishing scams are the most familiar blockchain attacks due to their prevalence and success rate.
- **Iota** crypto-currency phishing attack (January 2018)
  - Victims lost US$4 million in a phishing scam that lasted several months.
  - Attacker registered iotaseed.io
  - Providing a generator for un/pw for Iota wallets.
  - The service worked as advertised and enabled victims to successfully create and use their wallets as expected, providing a false sense of security and trust.
  - The attacker then waited, patiently taking advantage of the building trust.
  - Collected logs for 6 months and then began the attack.
  - Attacker transferred all funds from the victims’ wallets.

McAfee



Get your IOTA seed!

Move the mouse to generate randomness. **75% done.** Seeds in bulk here.

Your seed will appear after sufficient mouse movement

Your seed encoded as mnemonic words

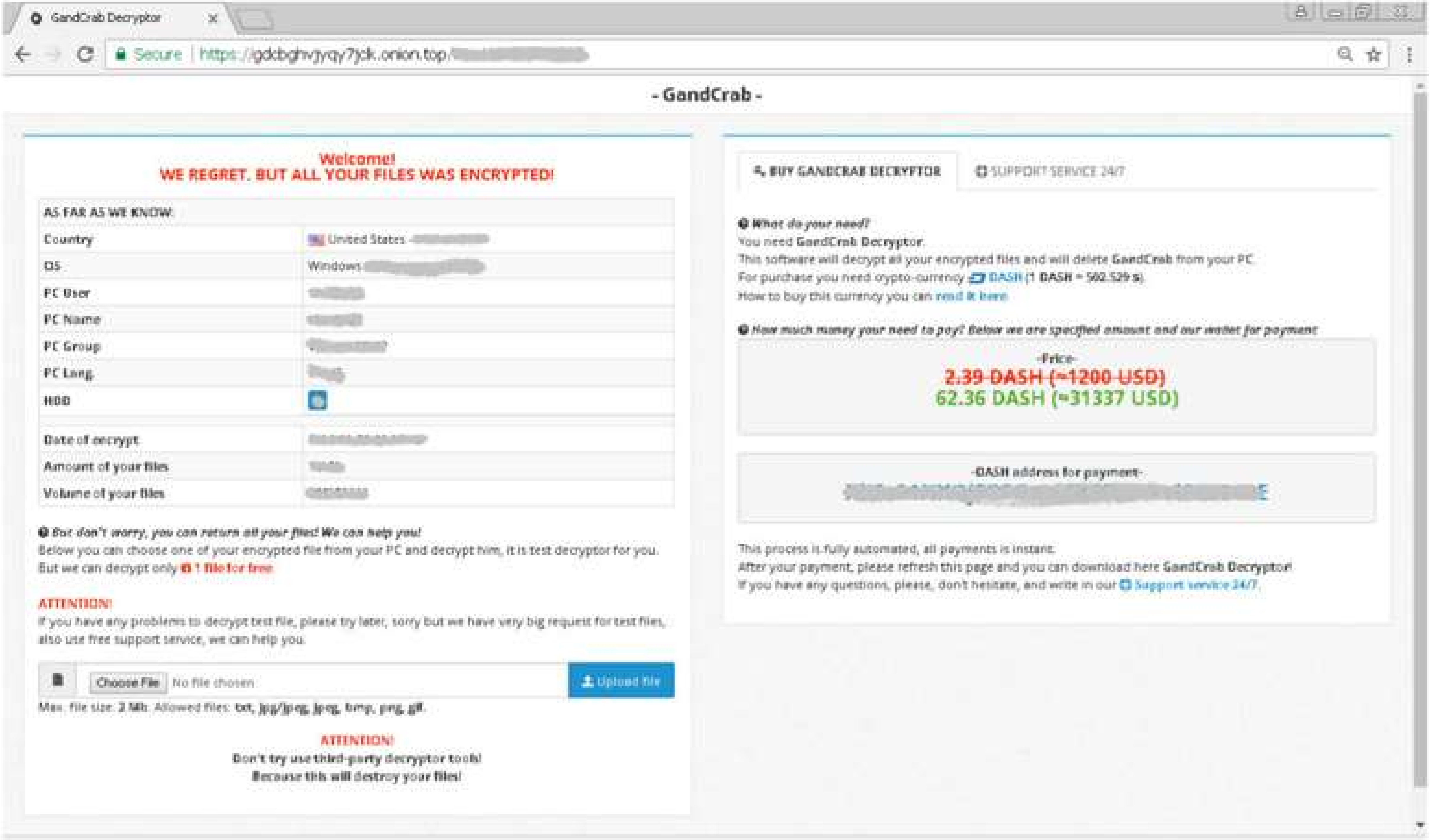
You will always be able to recover your seed with these words.

Ransomware

- 2016: new ransomware families exploded – holds your data for ransom
- In 2017, ransomware developers broadened their interest in cryptocurrencies.
- Malicious actors began experimenting with various alternative cryptocurrencies (altcoins).
    - Monero favorite alternative
    - Ransomware GandCrab discarded Bitcoin in favor of Dash.

McAfee

- Ransomware developers used Ethereum in early 2018.
    - Ransomlware *Planetary* allows victims to pay the equivalent of $700 per infected system or $5,000 for all the nodes infected on the victim's network.



Secure | https://gdcbghvjyqy7jclk.onion.top/[redacted]

- GandCrab -

Welcome!
WE REGRET. BUT ALL YOUR FILES WAS ENCRYPTED!

AS FAR AS WE KNOW:	
Country	🇺🇸 United States - [redacted]
OS	Windows [redacted]
PC User	[redacted]
PC Name	[redacted]
PC Group	[redacted]
PC Lang.	[redacted]
HDD	
Date of encrypt	[redacted]
Amount of your files	[redacted]
Volume of your files	[redacted]

But don't worry, you can return all your files! We can help you!
Below you can choose one of your encrypted file from your PC and decrypt him, it is test decryptor for you.
But we can decrypt only 1 file for free

ATTENTION!
If you have any problems to decrypt test file, please try later, sorry but we have very big request for test files, also use free support service, we can help you.

Max. file size: **2 Mb**. Allowed files: **txt, jpg/jpeg, jpeg, bmp, png, gif**.

ATTENTION!
Don't try use third-party decryptor tools!
Because this will destroy your files!

What do your need?
You need **GandCrab Decryptor**.
This software will decrypt all your encrypted files and will delete **GandCrab** from your PC.
For purchase you need crypto-currency DASH (**1 DASH = 502.529 $**).
How to buy this currency you can read it here.

How much money your need to pay? Below we are specified amount and our wallet for payment

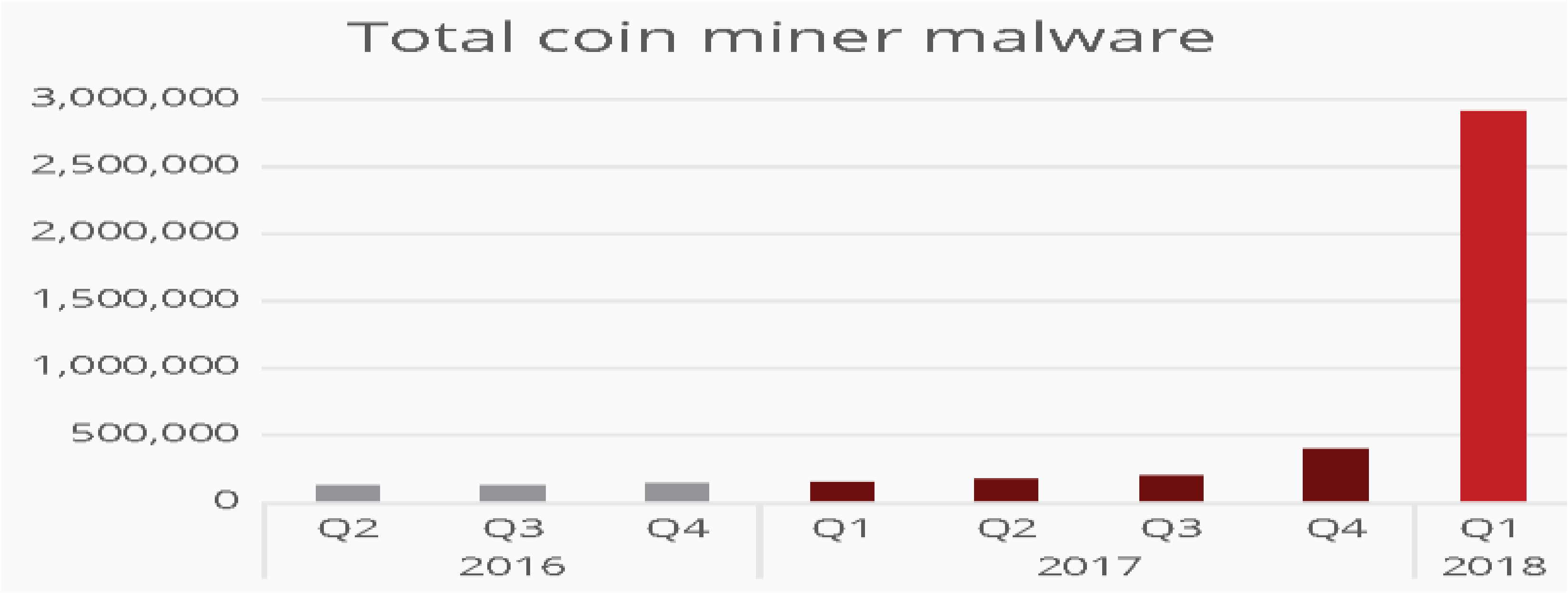
-Price-
~~2.39 DASH (≈1200 USD)~~
62.36 DASH (≈31337 USD)

-DASH address for payment-
[redacted]

This process is fully automated, all payments is instant.
After your payment, please refresh this page and you can download here **GandCrab Decryptor**!
If you have any questions, please, don't hesitate, and write in our Support service 24/7.

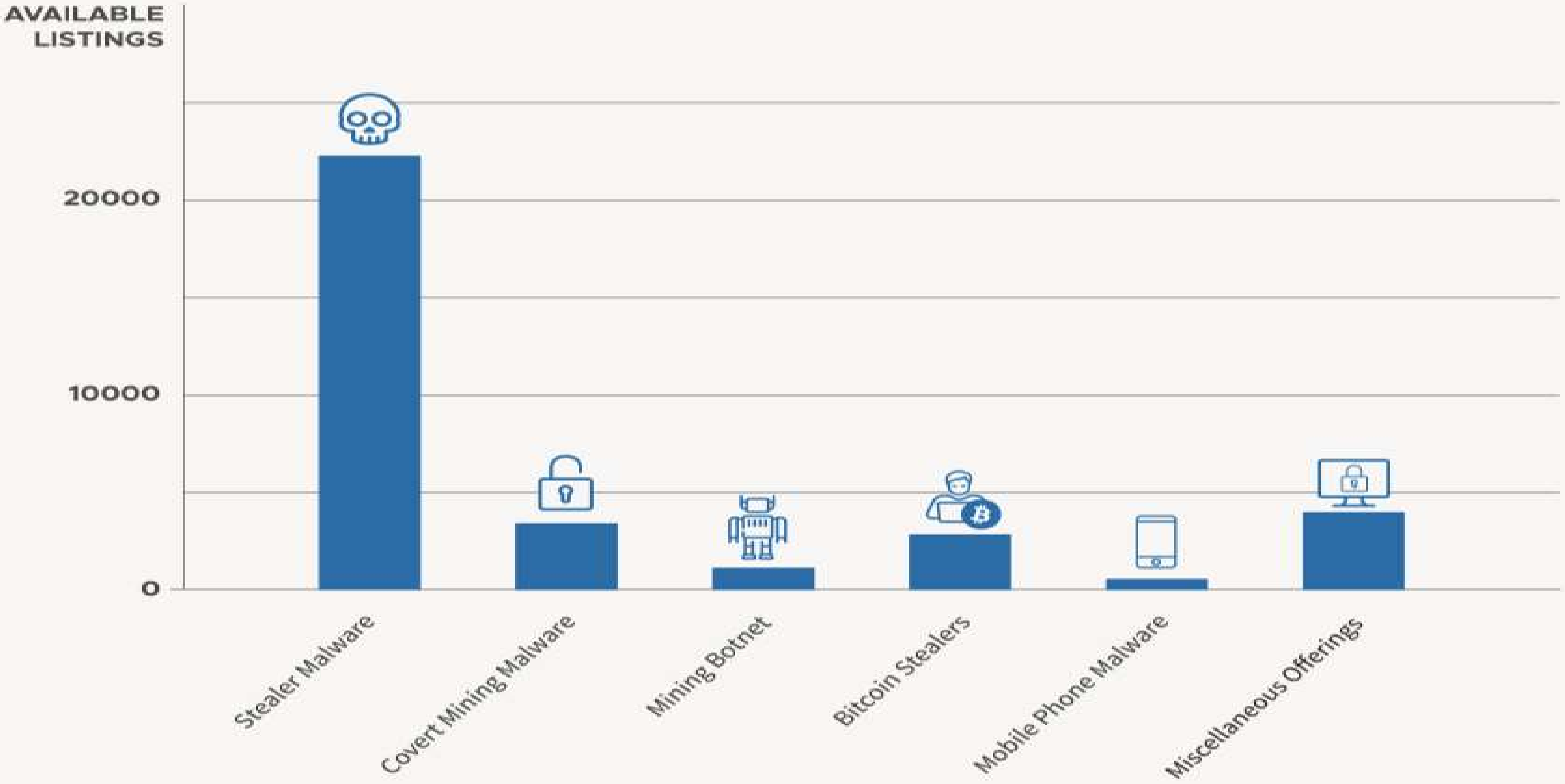
Malware

- **Mal**icious soft**ware**, is any program/file harmful to a computer user.
  - Includes computer viruses, worms, Trojan horses and spyware.
- Malware developers migrated from ransomware to **cryptocurrency mining**
  - Ransomware attacks declining 32% in Q1 2018 from Q4 2017
  - Coin mining increased by **1,189%.**
- Miners primarily target PCs, but other devices are also victims.



McAfee

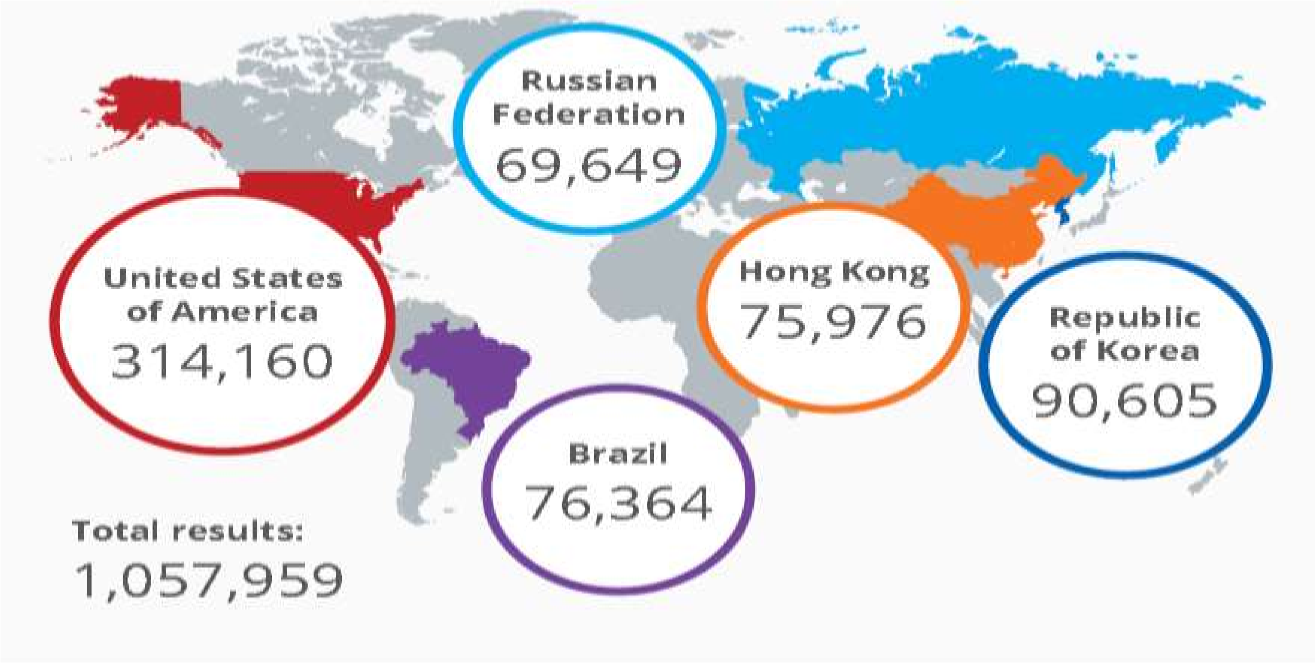
MALWARE OFFERINGS



Carbon Black.

Malware

- **China:** Android phones were exploited **to mine Monero coin** by ADB.Miner, which acts as a worm and runs over **port 5555,** which is more commonly used for the ADB debugging interface.



McAfee

Figure 5: A Shodan.io search for port 5555 devices.

- **Russia**: Malware aimed at unsuspecting gamers on a Russian forum, with the malware disguised as a “mod” to enhance popular games.

Cryptojacking

- Hijacking a **browser** to mine cryptocurrency
  - Cryptojacking resides in a grey area.

- In late 2017, the Archive Poster plug-in for the Chrome browser was found to be mining Monero coins without consent. Victims first learned of the issue when some started complaining of high CPU usage.

- A flaw in Youtube allowed malicious advertisers to inject cryptojacking code into ads to mine Bitcoin or Ethereum.

Krebsonsecurity/McAfee

Cryptojacking

- Cryptocurrency mining service **Coinhive** said to be top malicious threat to Web users
  - Ostensibly, a way for Web site owners to earn income without running ads
  - Can be used on hacked Web sites to steal the CPU power of its visitors' devices without the owner's knowledge or permission.
  - Easily embeds mining into websites or tools
  - Many organizations implement Coinhive and other miners to monetize their visitors' device resources - if they agree, then mining is considered not malicious, though potentially unwanted, behavior.
  - However, many sites do not disclose mining, and visitors are left uncertain about slow performance.

Krebsonsecurity/McAfee

Wallet Theft

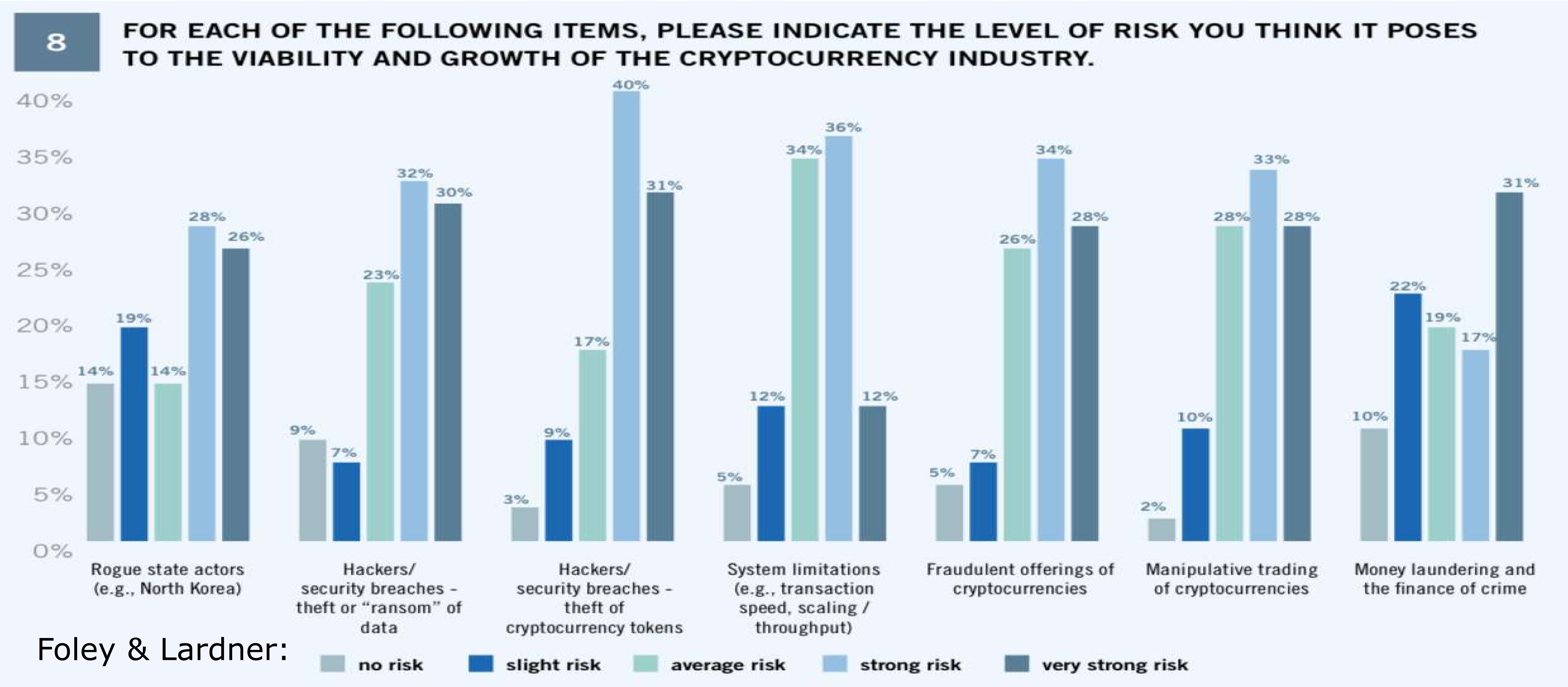
- Happens even with a super secure Hardware Wallets
- Need to pay attention!

> "Most issues are not with the technology but with he fact that the users do not know the 'basic concepts' that underlie all issues of computing. "

- McAfee report

- Most issues happen in the "points of connection" with the wallet, not with the wallet itself.
  - Steal your private keys
  - Trick you to send coins/tokens to wrong destination.

71% of large cryptocurrency traders & investors attribute theft of cryptocurrency as strongest risk that negatively affects market.



8

FOR EACH OF THE FOLLOWING ITEMS, PLEASE INDICATE THE LEVEL OF RISK YOU THINK IT POSES TO THE VIABILITY AND GROWTH OF THE CRYPTOCURRENCY INDUSTRY.

Foley & Lardner:

Copy Paste

- You copy/paste this address into your wallet.
- But CryptoShuffler will replace the address you just copied with hacker address

Hacked Mobile Apps:

- Publish real (fake) trading apps to trade on exchange
- Just sending money to a dummy hacker account.

Browser extensions

- Some extensions say will improve your user experience on tradin sites.
- Actually are key loggers

hackernoon

Clone Websites:

- URL bar hacked by another close URL pointing to a very similar website with the same exact look and feel and logo.
- Look for the https certificate

Fake Google Ads/SEO

- Hackers squat the top paid results (or organic) with similar URLs

Mobile SMS 2FA

- Ask your mobile phone number to register or activate 2FA (two factor security)
- Hacker can intercept your credentials via SMS

Wifi hacking

- WPA, the security protocol for most wifi routers used has been compromised, and public Wifi (eg airport wifi).

Attacks against DLT Technologies

Key Risks….

- Quantum Computing Risk
- Consensus Forking Risk
- Key Management Risk
- Data Privacy Risk
- ID Fraud Risk
- Software Quality Risk
- Business Continuity & Performance Risk
- Majority attacks

51% Majority Attacks

- A majority attack has **never been implemented successfully against Bitcoin due to its large base**
- But **has** been successfully implemented against Verge and other coins.
- Much smaller coins are acutely at risk.
- Hacker group **'51 Crew**' targeted other Eth small coins and held them for ransom.
  - Shift and Krypton networks refused to pay the ransom and subsequently had their blockchains hijacked by the attackers.
  - Also did double-spending the KR in their possession by selling the KR for Bitcoin on Bittrex, then reversed the transaction by rolling back the Krypton Blockchain.
- This risk also applies to **internally developed blockchains**.
  - Many organizations are examining blockchain technologies
  - If the contributing base, or hash rate, of these custom networks is not large enough, an attacker could use cloud technology, botnets, or pools to attack the system.

McAfee **hackernoon**

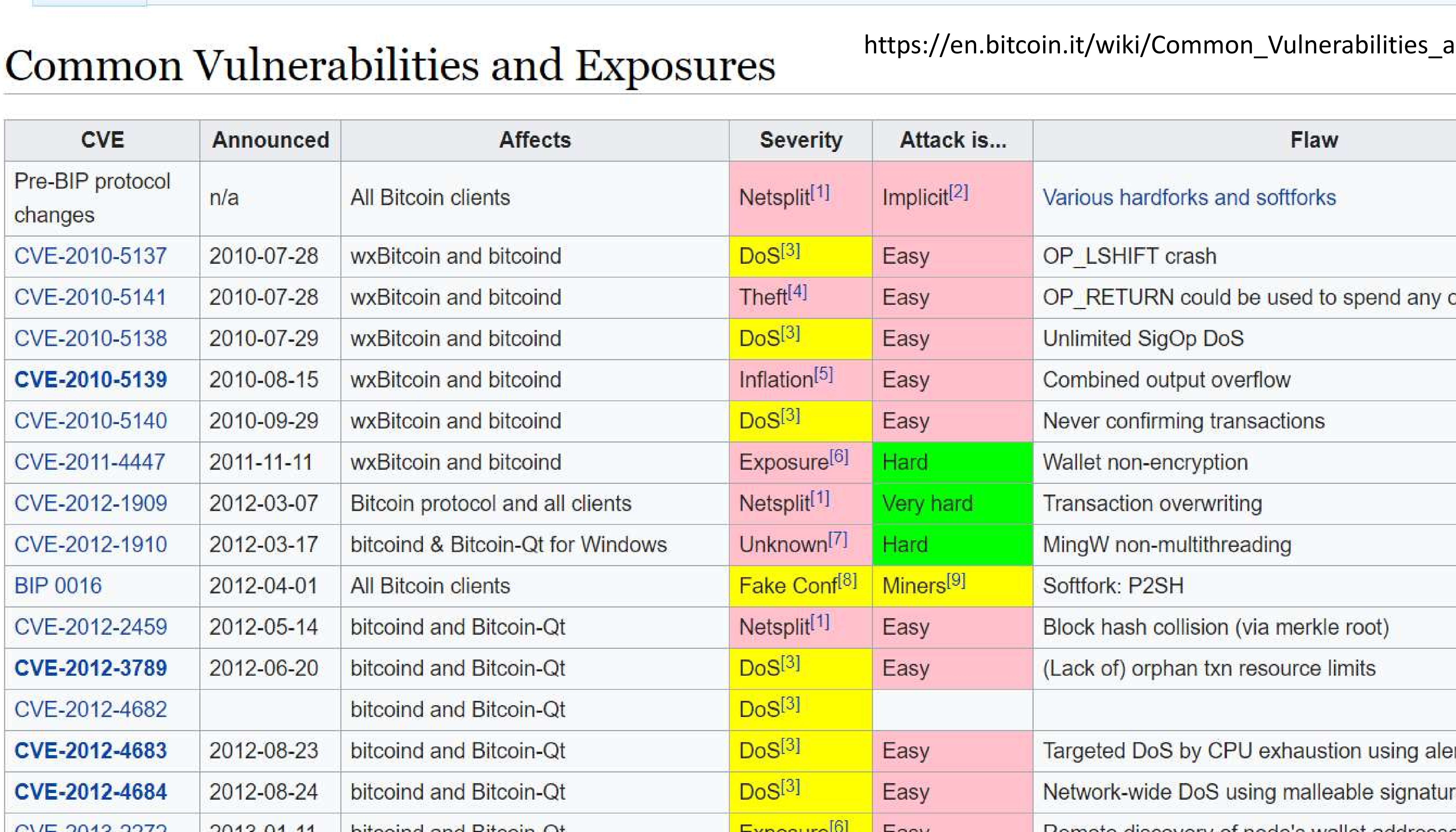
Implementation Attacks

- The closer gets to the core of blockchain technology, the **more difficult it is to succeed with an attack.**

- **Instead:** Attack against blockchain **implementation** & support tools
  - More like exploits of traditional software and web applications.
  - Have resulted in denial of service attacks, coin theft, data exposure
  - Commonly discovered and fixed **after** release.
  - Difficult to build and maintain secure code while explosive growth

- **Feb 2018:** a ‘zero-day’ exploit struck PyBitmessage, a peer-to-peer message transfer tool that mirrors Bitcoin’s transaction and block transfer system.
  - Bitmessage uses POW to “pay” for message transfers and reduce spam.
  - Attackers used this exploit to execute code on devices by sending specially crafted messages. They then ran automated scripts looking for Ethereum wallets while also creating a reverse shell for further access.

https://en.bitcoin.it/wiki/Common_Vulnerabilities_a

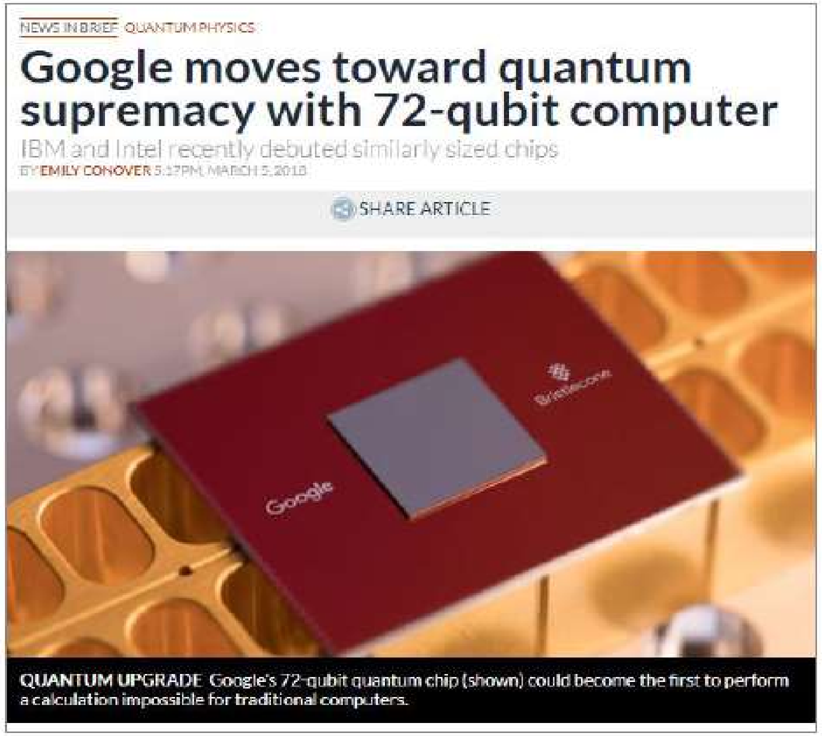


Common Vulnerabilities and Exposures

CVE	Announced	Affects	Severity	Attack is...	Flaw
Pre-BIP protocol changes	n/a	All Bitcoin clients	Netsplit[1]	Implicit[2]	Various hardforks and softforks
CVE-2010-5137	2010-07-28	wxBitcoin and bitcoind	DoS[3]	Easy	OP_LSHIFT crash
CVE-2010-5141	2010-07-28	wxBitcoin and bitcoind	Theft[4]	Easy	OP_RETURN could be used to spend any c
CVE-2010-5138	2010-07-29	wxBitcoin and bitcoind	DoS[3]	Easy	Unlimited SigOp DoS
CVE-2010-5139	2010-08-15	wxBitcoin and bitcoind	Inflation[5]	Easy	Combined output overflow
CVE-2010-5140	2010-09-29	wxBitcoin and bitcoind	DoS[3]	Easy	Never confirming transactions
CVE-2011-4447	2011-11-11	wxBitcoin and bitcoind	Exposure[6]	Hard	Wallet non-encryption
CVE-2012-1909	2012-03-07	Bitcoin protocol and all clients	Netsplit[1]	Very hard	Transaction overwriting
CVE-2012-1910	2012-03-17	bitcoind & Bitcoin-Qt for Windows	Unknown[7]	Hard	MingW non-multithreading
BIP 0016	2012-04-01	All Bitcoin clients	Fake Conf[8]	Miners[9]	Softfork: P2SH
CVE-2012-2459	2012-05-14	bitcoind and Bitcoin-Qt	Netsplit[1]	Easy	Block hash collision (via merkle root)
CVE-2012-3789	2012-06-20	bitcoind and Bitcoin-Qt	DoS[3]	Easy	(Lack of) orphan txn resource limits
CVE-2012-4682		bitcoind and Bitcoin-Qt	DoS[3]		
CVE-2012-4683	2012-08-23	bitcoind and Bitcoin-Qt	DoS[3]	Easy	Targeted DoS by CPU exhaustion using ale
CVE-2012-4684	2012-08-24	bitcoind and Bitcoin-Qt	DoS[3]	Easy	Network-wide DoS using malleable signatur
CVE-2013-2272	2013-01-11	bitcoind and Bitcoin-Qt	Exposure[6]	Easy	Remote discovery of node's wallet address

Quantum Computing-based Threats

- Now 0s and 1s in computing
- Quantum computing allows any number between 0 and 1 = *quibits*
    - Provides **exponential** increase in computing power = break encryption keys that are in use NOW
- National governments and military agencies funding quantum computing research
- Google has **72-qubit** quantum computer
    - Bristlecone chip holds the record
- Small **20-qubit** quantum computer available for experiments via the IBM quantum experience project.
- “Large scale quantum computing is 10-15 yrs away”
- 1 in 7 chance of current crypto currencies being affected by quantum attacks in 2026
- 1 in 2 chance by 2031



NEWS IN BRIEF QUANTUM PHYSICS

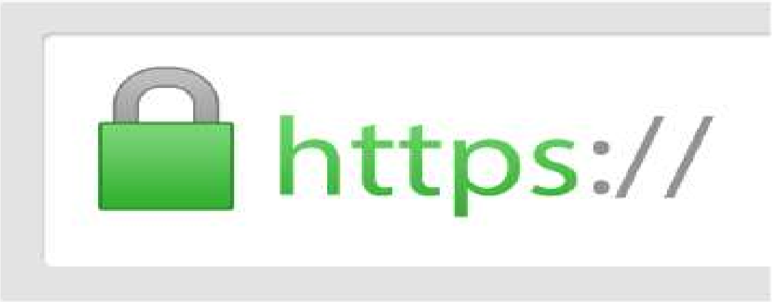
Google moves toward quantum supremacy with 72-qubit computer

IBM and Intel recently debuted similarly sized chips

BY EMILY CONOVER 5:17PM, MARCH 5, 2018

SHARE ARTICLE

QUANTUM UPGRADE Google's 72-qubit quantum chip (shown) could become the first to perform a calculation impossible for traditional computers.



TLS Protocol Insecure

Digital Signature can be forged (and Blockchain)

Message Authentication forged

Network Encryption Insecure

Quantum Resistant Algorithms

Name of Cryptographic Algorithm	Type	Purpose	Resilience against Quantum Computer
AES-256	Symmetric Key	Encryption	Ok but larger key sizes needed
SHA-256, SHA-3		Hash function	Ok but larger output needed
Lattice-based (NTRU)	Public Key	Encryption; signature	Believed
Code-based (Mc Eliece)	Public Key	Encryption	Believed
Multivariate polynomials	Public Key	Encryption; signature	Believed
Supersingular elliptic curve isogenies (SIDH)		Encryption; possibly signature	Believed
ECDSA, ECDH (Elliptic Curve Crypto)	Public Key	Signatures, Key exchange	No longer secure
RSA	Public Key	Signatures, Key establishment	No Longer secure
DSA (Finite Field Crypto)	Public Key	Signatures	No Longer secure

High level of confidence

Under investigation

Get Prepared

Build next generation of cryptographic infrastructure

- Must have quantum safe alternatives
- Should have algorithmic agility **built in**
- Should be underpinned by strong keys

PKI – Plan Now

- Need '**crypto-agile'** hybrid PKI solutions now
- Can re-sign shortly before cryto broken by quantum computer

Data Confidentiality

- Threat: 'Download data now, then decrypt later'
- Deadline to be quantum safe depends on information timeline of the data = **CBDCs??**

Thank you!

@leonperlman