

A FIRST LOOK AT BROWSER-BASED CRYPTOJACKING

Shayan Eskandari*, Andreas Leoutsarakos*, Troy Mursch[†], Jeremy Clark*

**Concordia University, [†]Bad Packets Report*



UNIVERSITÉ
Concordia
UNIVERSITY

Cryptojacking

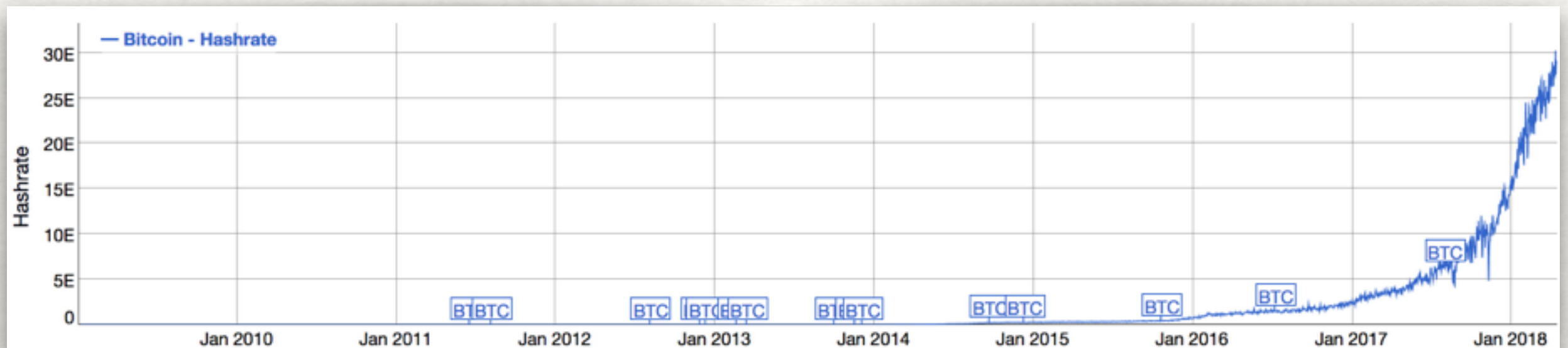
[krɪptɒʊdʒækɪŋ], verb

THE INVISIBLE USE OF ONE'S
RESOURCES TO MINE
CRYPTOCURRENCY FOR SOMEONE
ELSE'S PROFIT

INTRODUCTION

HISTORY OF BITCOIN MINING

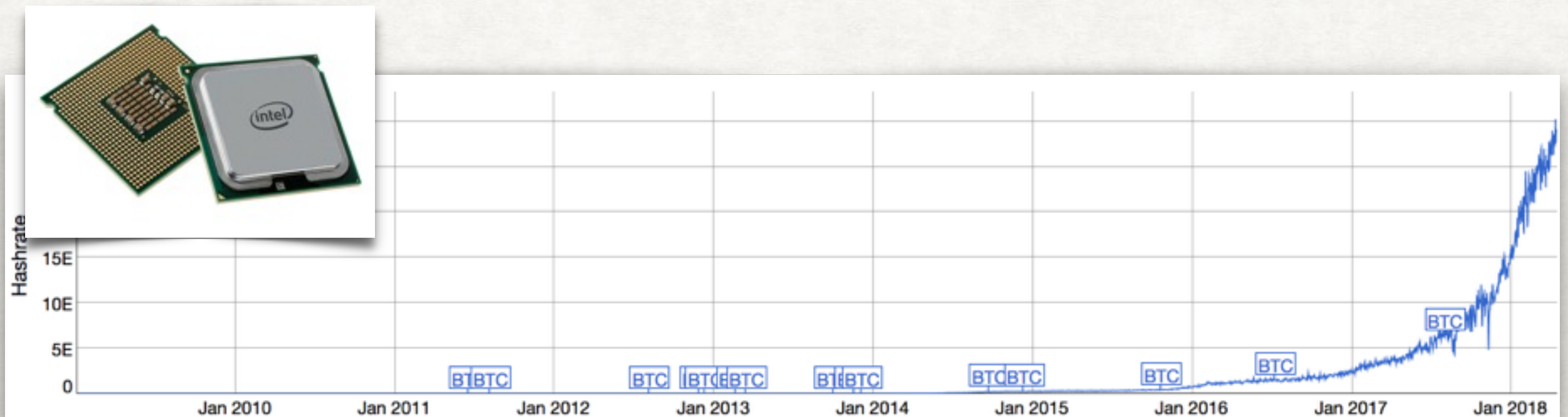
- Bitcoin
 - Mining algorithm(PoW): SHA-256
 - Net hashrate: 30,035.96 Ph/s



INTRODUCTION

HISTORY OF BITCOIN MINING

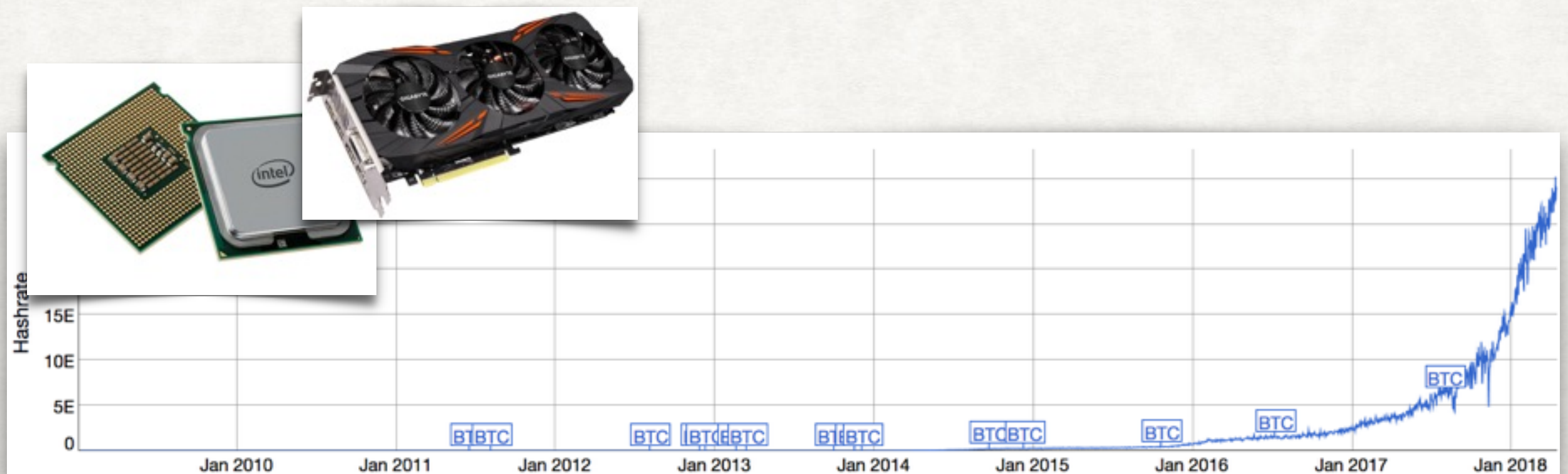
- Bitcoin
 - Mining algorithm(PoW): SHA-256
 - Net hashrate: 30,035.96 Ph/s



INTRODUCTION

HISTORY OF BITCOIN MINING

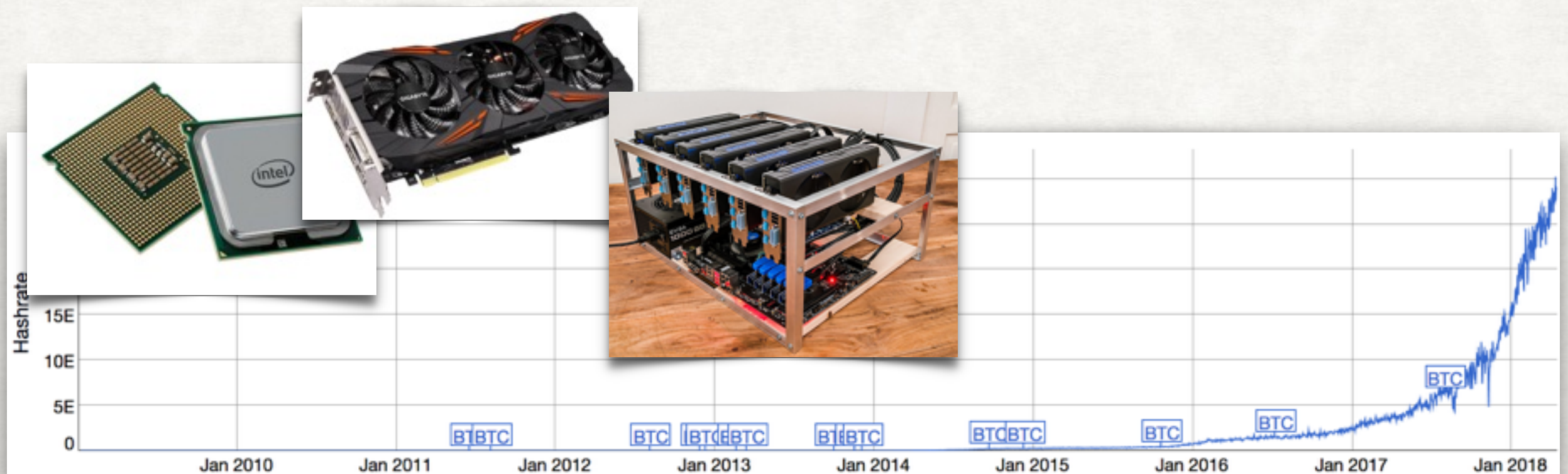
- Bitcoin
 - Mining algorithm(PoW): SHA-256
 - Net hashrate: 30,035.96 Ph/s



INTRODUCTION

HISTORY OF BITCOIN MINING

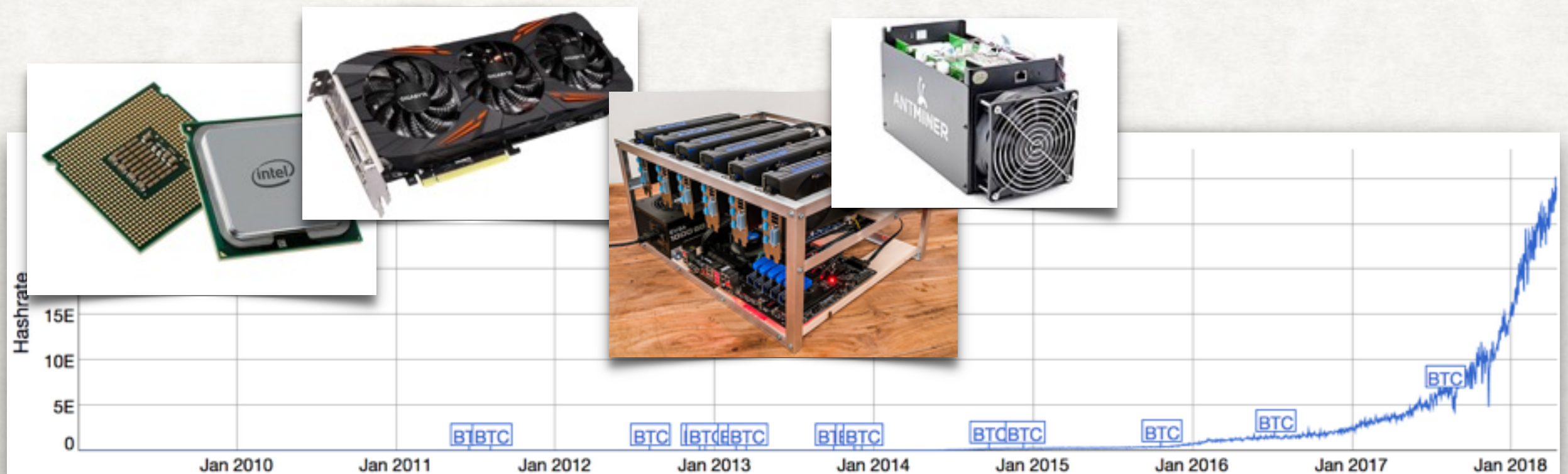
- Bitcoin
 - Mining algorithm(PoW): SHA-256
 - Net hashrate: 30,035.96 Ph/s



INTRODUCTION

HISTORY OF BITCOIN MINING

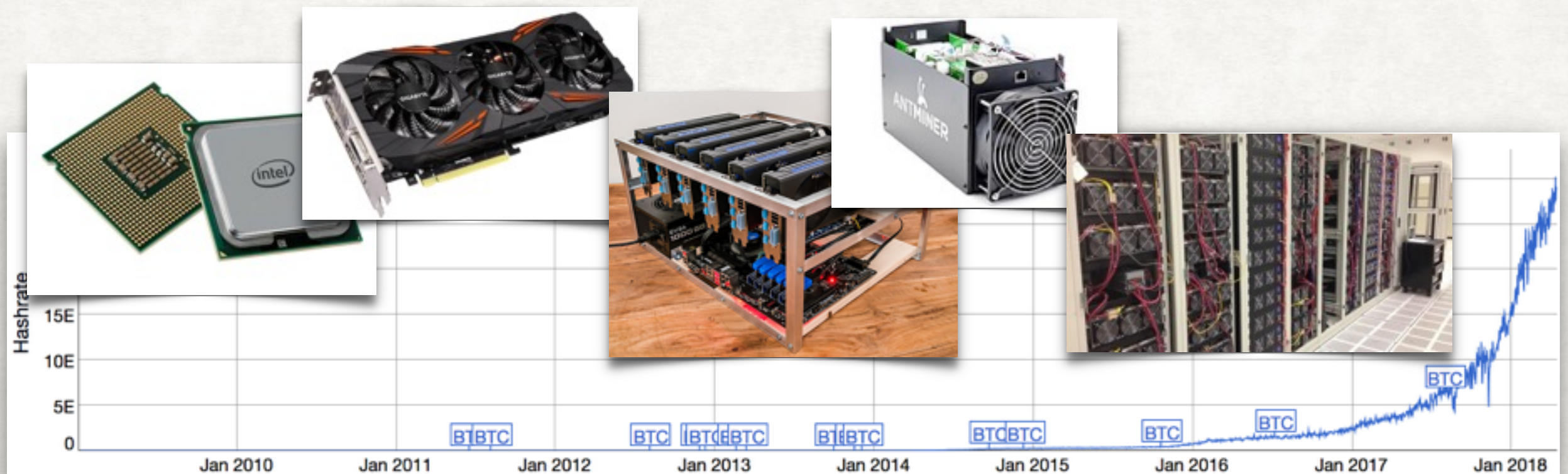
- Bitcoin
 - Mining algorithm(PoW): SHA-256
 - Net hashrate: 30,035.96 Ph/s



INTRODUCTION

HISTORY OF BITCOIN MINING

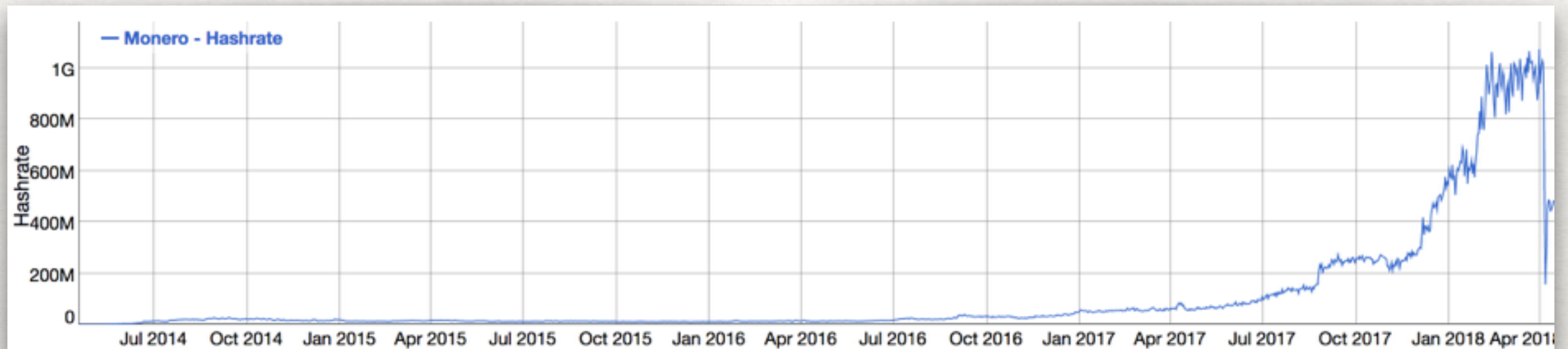
- Bitcoin
 - Mining algorithm(PoW): SHA-256
 - Net hashrate: 30,035.96 Ph/s



INTRODUCTION

MONERO

- **Monero**
 - Privacy Preserving Cryptocurrency, Launched in April 2014
 - Mining algorithm (PoW): CryptoNight
 - Net hashrate: 488.50 Mh/s



INTRODUCTION

BROWSER BASED MINING

- **Browser based mining** (website using visitor's CPU to mine Bitcoin):
 - **Replace online ads**
 - **More decentralization on the Cryptocurrency network**
 - **Bitcoin Plus (2011), JSMiner (2011), MineCrunch (2014), Tidbit (2014)**

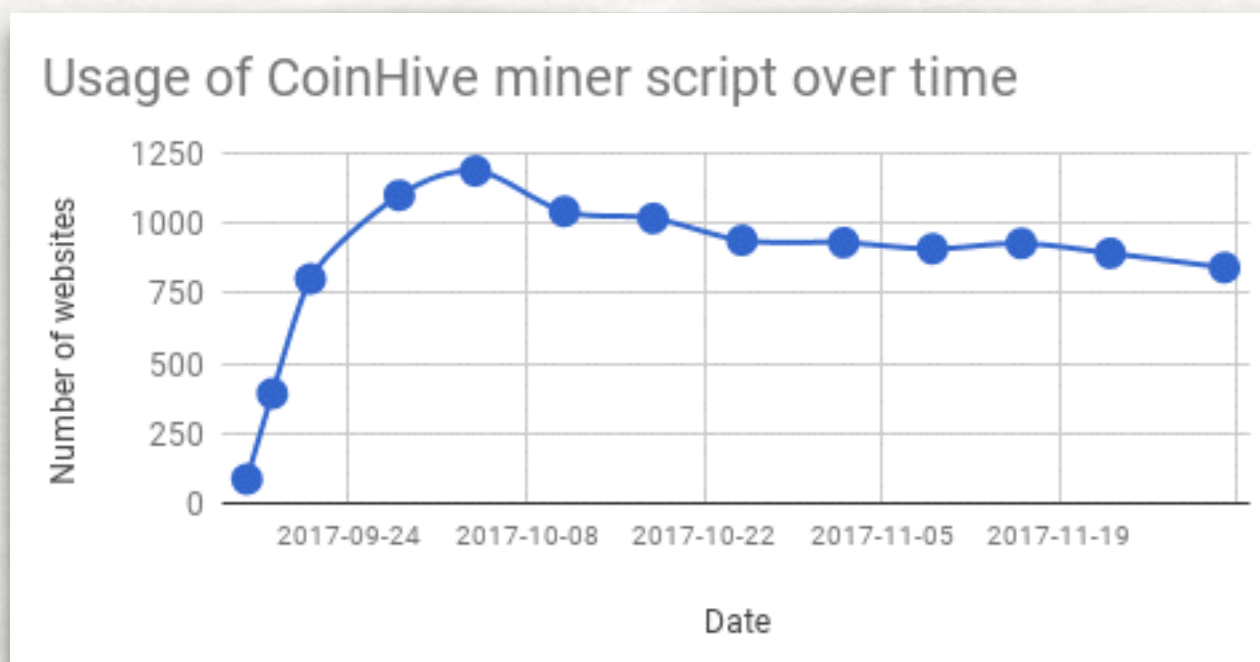
INTRODUCTION

BROWSER BASED MINING

- **Browser based mining** (website using visitor's CPU to mine Bitcoin):
 - Replace online ads
 - More decentralization on the Cryptocurrency network
 - Bitcoin Plus (2011), JSMiner (2011), MineCrunch (2014), Tidbit (2014)
- **Why it didn't work?**
 - Bitcoin network hash rate increased exponentially
 - Slower than native applications (1.5x slower)
 - Legal issues

BROWSER BASED MINING REVIVED

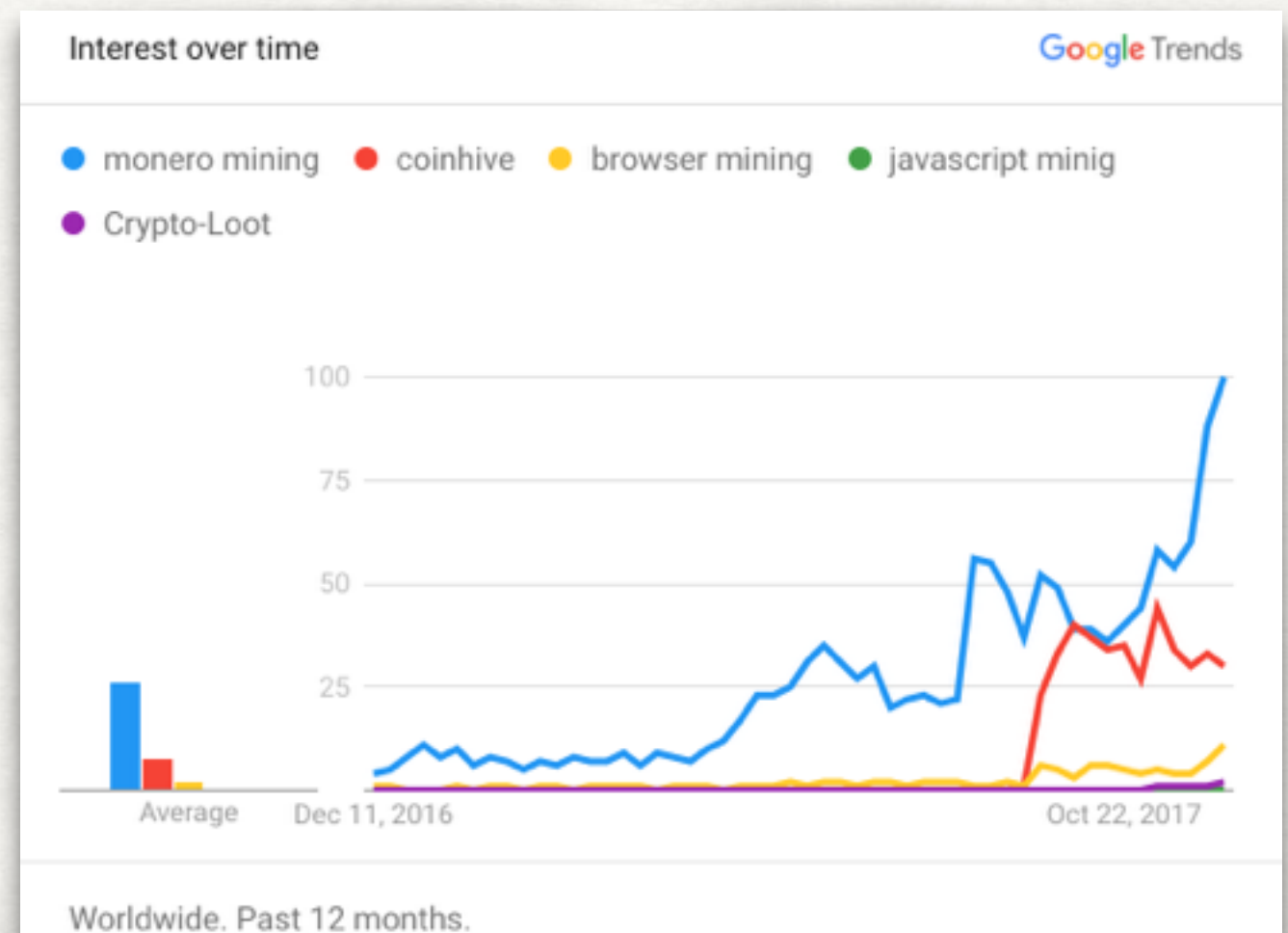
- **Coinhive**
 - Launched in September 2017, as a service to replace ads
 - Also offered CAPTCHA and short-links services
 - Soon after several copycats appeared (Crypto-Loot, PPoi, Coin-Have, ...)



BROWSER-BASED CRYPTOJACKING

IN-BROWSER MINING WITHOUT USER CONSENT

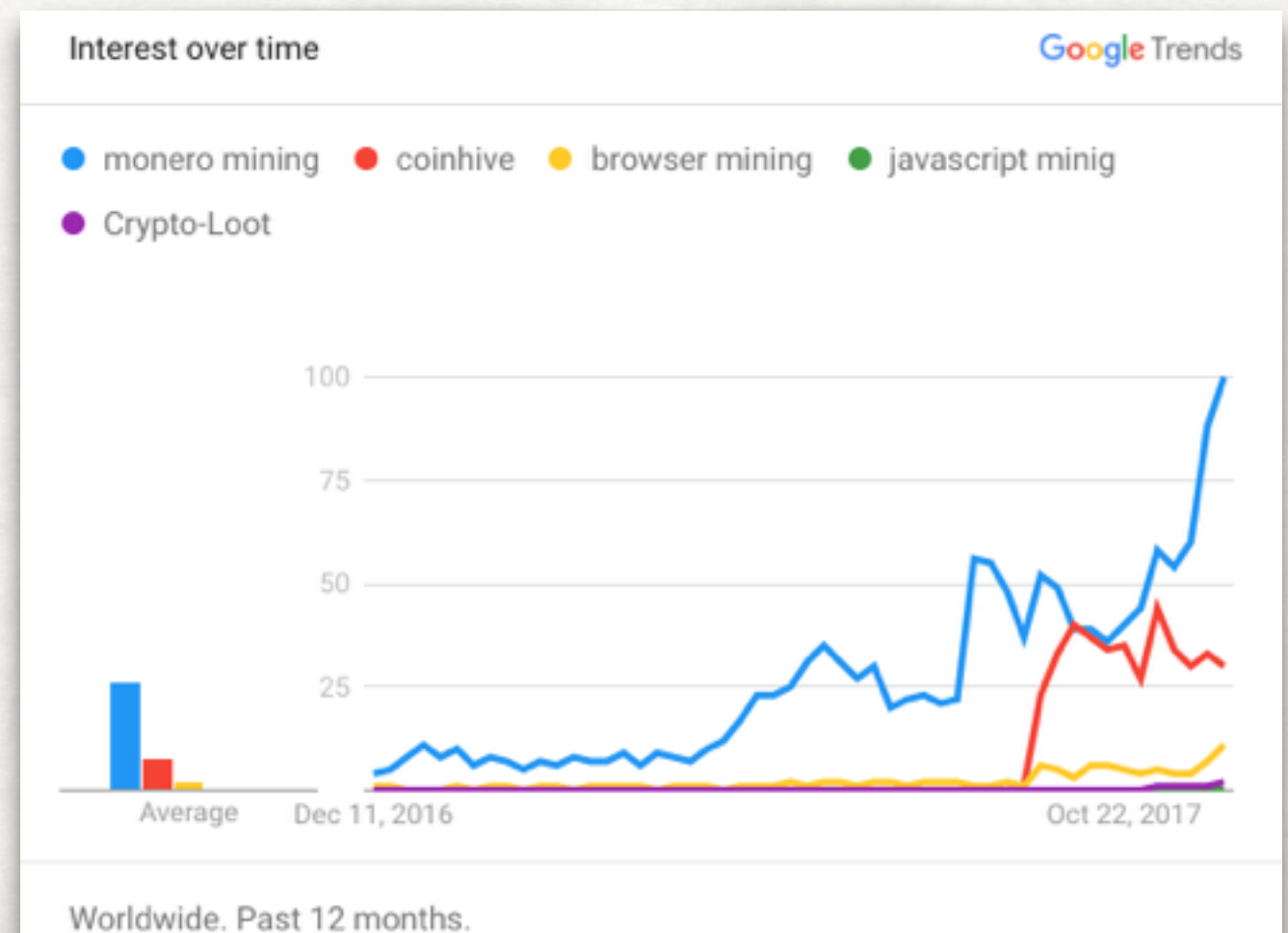
- Also known as "*Drive-by Mining*"
- Websites started testing this new revenue model, such as ThePirateBay, Showtime and UFC.com



BROWSER-BASED CRYPTOJACKING

IN-BROWSER MINING WITHOUT USER CONSENT

- Also known as "*Drive-by Mining*"
- Websites started testing this new revenue model, such as ThePirateBay, Showtime and UFC.com
- Hackers started to turn access to "money"
- Interest from "grey" websites



CRYPTOJACKING

THE NEXT BIG CYBERSECURITY THREAT

CRYPTOJACKING

THE NEXT BIG CYBERSECURITY THREAT

The image is a screenshot of a mobile device displaying a Yahoo! Finance article. The top of the screen features a blue header with a white back arrow on the left and the 'YAHOO! FINANCE' logo in white. Below the header, the article title 'Why Cryptojacking Is The Next Big Cybersecurity Threat' is displayed in a large, bold, black font. Underneath the title, the author's name 'Robert Hackett' is shown, followed by the publication 'FORTUNE' in a smaller font and the date 'October 23, 2017'. The main body of the article begins with the text: 'Meet the Internet's latest menace. Hackers and penny-pinching website hosts are hijacking people's computers to "mine" cryptocurrency. And we're not talking about coal and canaries.' The final line of the visible text is 'Cryptocurrency is mined, or produced, by'.

< YAHOO! FINANCE

Why Cryptojacking Is The Next Big Cybersecurity Threat

Robert Hackett
FORTUNE Fortune October 23, 2017

Meet the Internet's latest menace.
Hackers and penny-pinching website
hosts are hijacking people's computers
to "mine" cryptocurrency. And we're not
talking about coal and canaries.

Cryptocurrency is mined, or produced, by

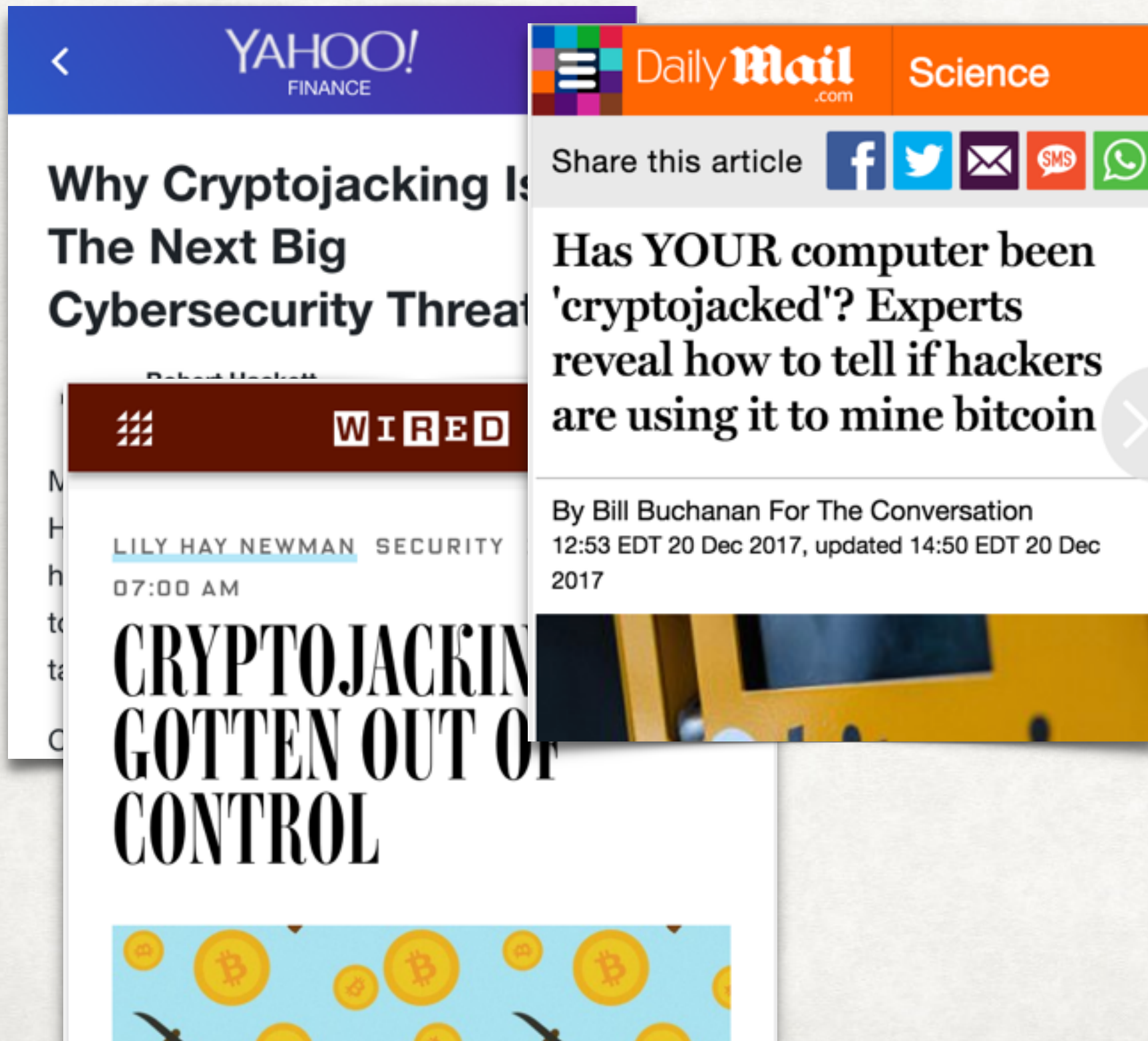
CRYPTOJACKING

THE NEXT BIG CYBERSECURITY THREAT



CRYPTOJACKING

THE NEXT BIG CYBERSECURITY THREAT



CRYPTOJACKING

THE NEXT BIG CYBERSECURITY THREAT



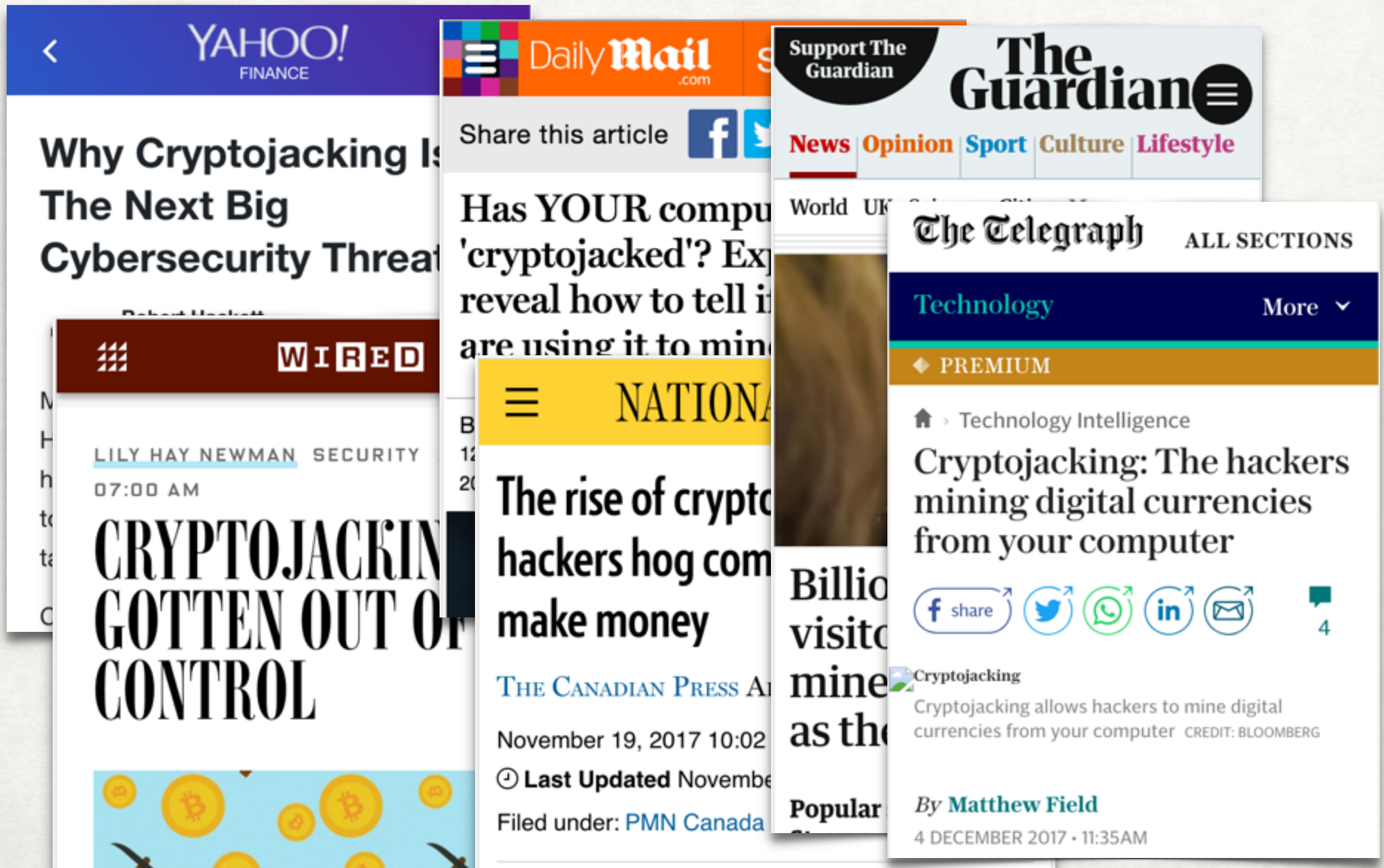
CRYPTOJACKING

THE NEXT BIG CYBERSECURITY THREAT



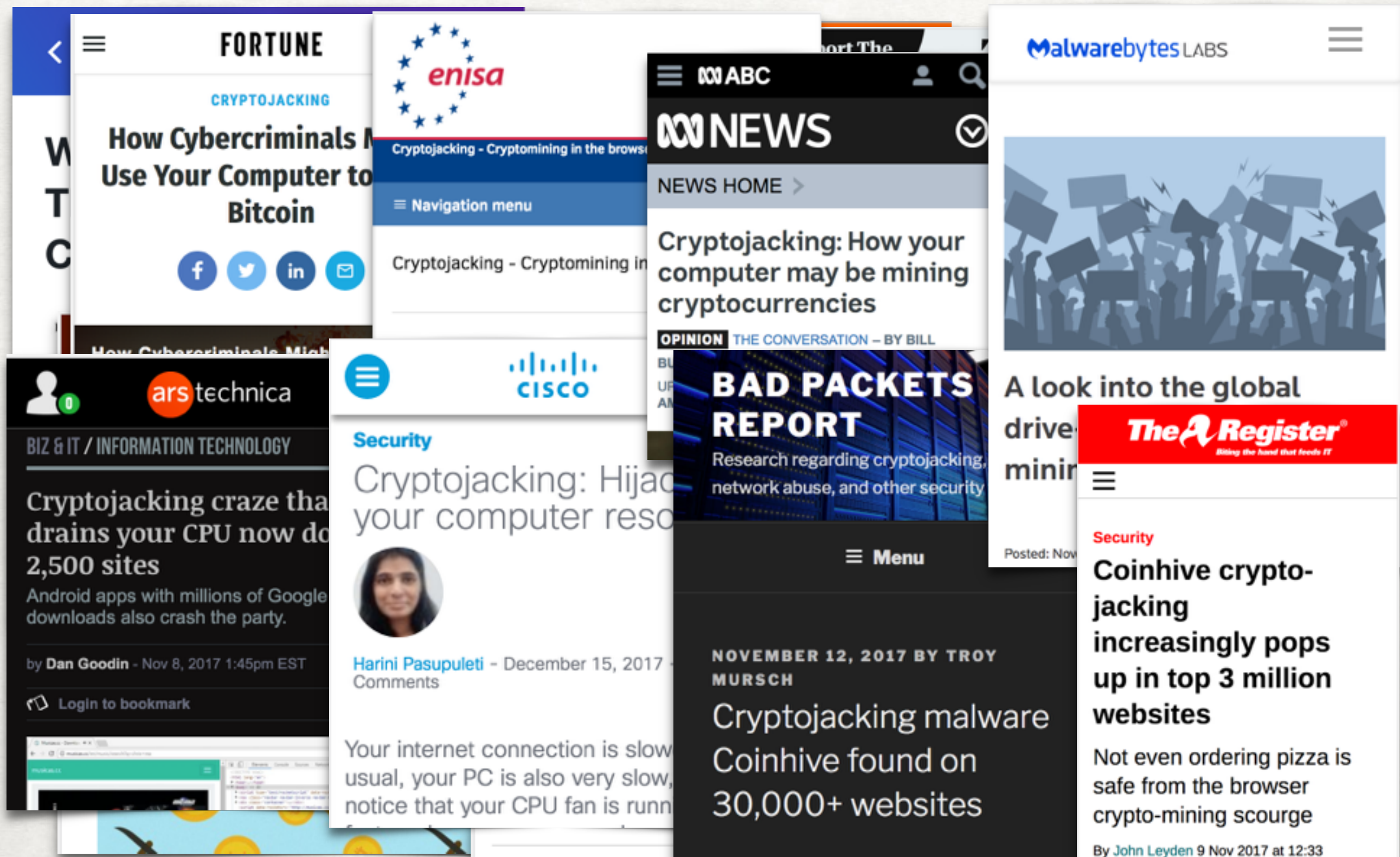
CRYPTOJACKING

THE NEXT BIG CYBERSECURITY THREAT



CRYPTOJACKING

THE NEXT BIG CYBERSECURITY THREAT



CRYPTOJACKING

UK ONLY

CRYPTOJACKING

UK ONLY

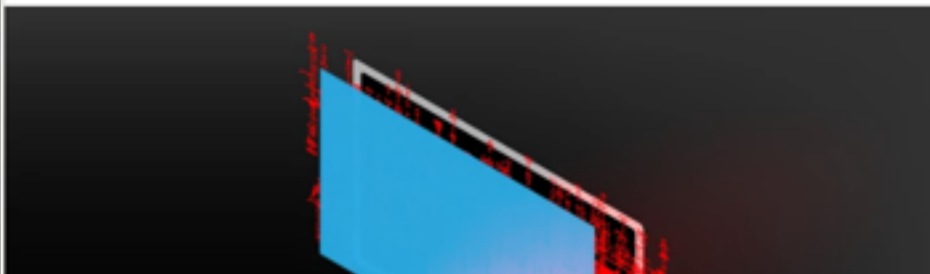


Cryptojacking attack hits ~4,000 websites, including UK's data watchdog



Natasha Lomas

@riptari / Feb 12, 2018



CRYPTOJACKING

UK ONLY

The image shows a screenshot of a Twitter thread. The top tweet is from 'The Telegraph' (TE logo) with a green close button. The headline reads 'Cryptojacking attack hits ~4.000 webs inclu watc'. The author is 'Natasha L' with handle '@riptari'. A second tweet is overlaid on top of the first, from 'INDY/LIFE' (eagle logo). Its headline reads 'UK 'CRYPTOJACKING' ATTACKS SURGE 1,200% AS BITCOIN VALUE RISE SEES ILLEGAL MINERS TAKING OVER PCS'. The text of this tweet states: 'The findings coincide with a spike in interest in bitcoin, which was valued at an all-time high in mid-December / Reuters' and 'Dramatic up-tick in incidents observed between October and January'. The author is 'JOE SOMMERLAD' with handle '@JoeSommerlad', dated 'Wednesday 28 February 2018 14:35 GMT'.

TE

Cryptojacking attack hits ~4.000 webs inclu watc

Natasha L
@riptari /

INDY/LIFE

UK 'CRYPTOJACKING' ATTACKS SURGE 1,200% AS BITCOIN VALUE RISE SEES ILLEGAL MINERS TAKING OVER PCS

The findings coincide with a spike in interest in bitcoin, which was valued at an all-time high in mid-December / Reuters

Dramatic up-tick in incidents observed between October and January

JOE SOMMERLAD
@JoeSommerlad
Wednesday 28 February 2018 14:35 GMT

CRYPTOJACKING

UK ONLY



Cryptojacking attack hits ~4.000 websites including NHS and water

Natasha L
@riptari /



INDY/

UK 'CRYPTOJACKING' SURGE 1,200% / VALUE RISE SEES MINERS TAKING

The findings coincide with a surge in bitcoin, which was valued at over \$1,000 in December / Reuters

Dramatic up-tick in cryptojacking observed between December and January

JOE SOMMERLAD

@JoeSommerlad

Wednesday 28 February 2018 14:35 GMT

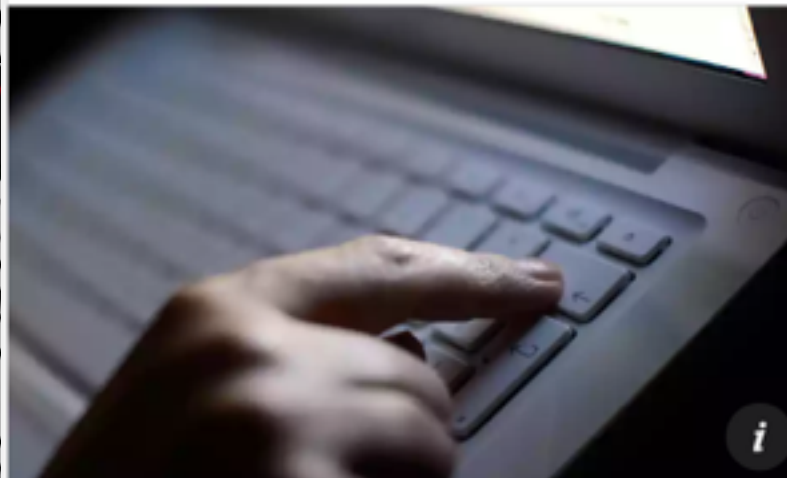
Support The Guardian

The Guardian

News Opinion Sport Culture Lifestyle



World UK Science Cities More



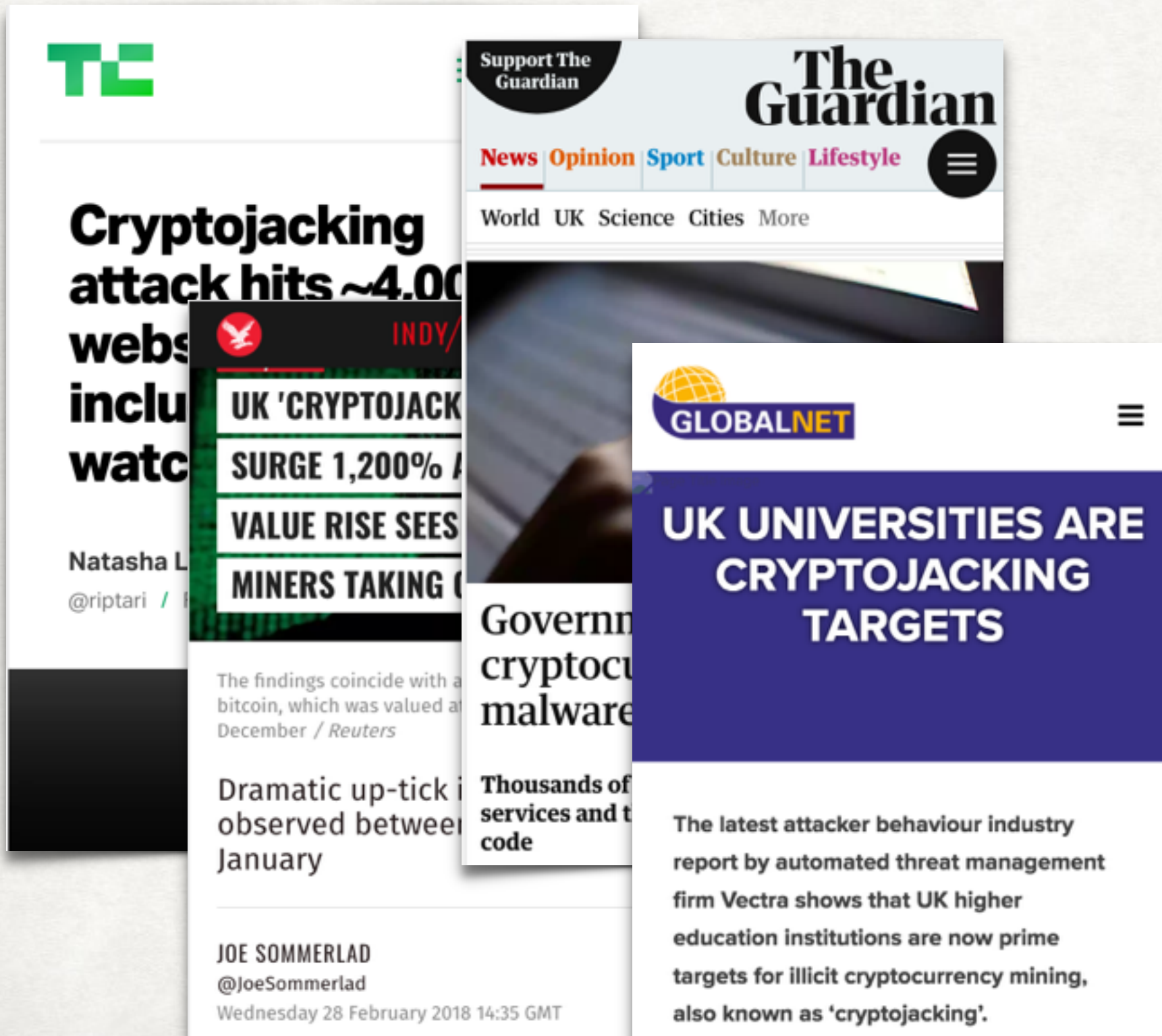
i

Government websites hit by cryptocurrency mining malware

Thousands of sites, including NHS services and the ICO, hijacked by rogue code

CRYPTOJACKING

UK ONLY



CRYPTOJACKING

UK ONLY



Cryptojacking attack hits ~4.000 websites including watch

Natasha L
@riptari /



INDY/

UK 'CRYPTOJACK'
SURGE 1,200%
VALUE RISE SEES
MINERS TAKING

The findings coincide with a
bitcoin, which was valued at
December / Reuters

Dramatic up-tick in
observed between
January

JOE SOMMERLAD
@JoeSommerlad

Wednesday 28 February 2018 14:35 GMT

Support The
Guardian

The
Guardian

News Opinion Sport Culture Lifestyle

World UK Science Cities More



Government
cryptoc
malware

Thousands of
services and t
code



GLOBALNET

UK UNIVERS
CRYPTOJA
TARGETS

The latest attacker behaviour industry
report by automated threat management
firm Vectra shows that UK higher
education institutions are now prime
targets for illicit cryptocurrency mining,
also known as 'cryptojacking'.

UK, Australian Government Websites Cryptojacked By Mining Malware

Martin J. Young - NewsBTC - Mon Feb 12, 4:00AM CST

Mining malware is spreading like wildfire, every week now we run another story on some platform or other falling victim to it. As cryptocurrencies become far more lucrative than ransomware or identity theft incidents of exploits will only increase. Various governmental departments in Australia and the UK were found frantically calling the tech guys over the weekend as their websites were compromised.

According to the [Guardian](#) as many as 5,000 websites were infected with a variant of the Coinhive mining malware. In the UK they included websites of National Health Services, the Student Loans Company, and several English councils in addition to the UK's data protection watchdog, the

CRYPTOJACKING

UK ONLY



Cryptojacking attack hits ~4.000 websites including watch

Natasha L
@riptari /

INDY/
UK 'CRYPTOJACKING' SURGE 1,200% / VALUE RISE SEES MINERS TAKING

The findings coincide with a bitcoin, which was valued at December / Reuters

Dramatic up-tick observed between January

JOE SOMMERLAD
@JoeSommerlad

Wednesday 28 February 2018 14:35 GMT

Support The Guardian

The Guardian

News Opinion Sport Culture Lifestyle

World UK Science Cities More



Government cryptomining malware

Thousands of services and code



UK UNIVERSITIES CRYPTOJACKING TARGETS

The latest attacker behaviour industry report by automated threat management firm Vectra shows that UK higher education institutions are now prime targets for illicit cryptocurrency mining, also known as 'cryptojacking'.

UK, Australian Government Websites Cryptojacked By Mining Malware

Martin J. Young - NewsB

Mining malware is spreading now we run another falling victim to it. As lucrative than ransom exploits will only increase departments in Australia frantically calling the their websites were co

According to the Guardian infected with a variant of the UK they included with the Student Loans Commission addition to the UK's da

COINTELEGRAPH
BTC \$ 8,198 | ETH \$ 536 | LTC \$ 141 | XRP \$ 0.72

By Ana Alexandre

Apr 11, 2018

UK National Cyber Security Centre Includes Cryptojacking In Report On Cyber Threats

10126 Total views | 207 Total shares

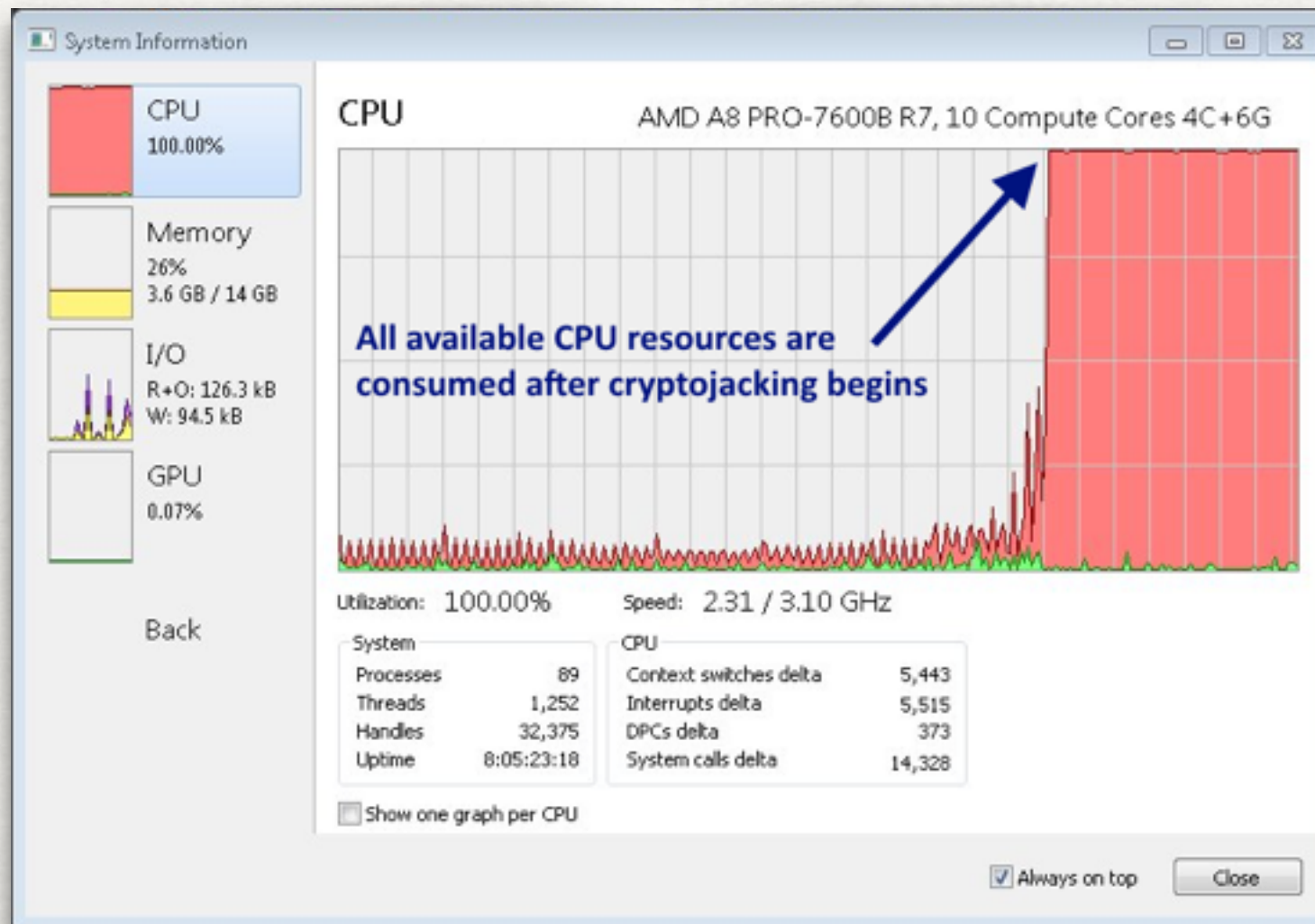


On April 10, the UK National Cyber Security Centre (NCSC) released a report analyzing how nefarious cyber activity influenced the business environment in Great Britain over the past year.

CLIENT IMPACT

USER EXPERIENCE

- A spike in CPU usage, increase in fan speed and noise
- Possibility of browser and/or computer crash



DATA GATHERING

STATE OF AFFAIRS

- Censys.io BigQuery dataset (Top 1 Million websites)
- PublicWWW's dataset (~200 Million indexed websites)

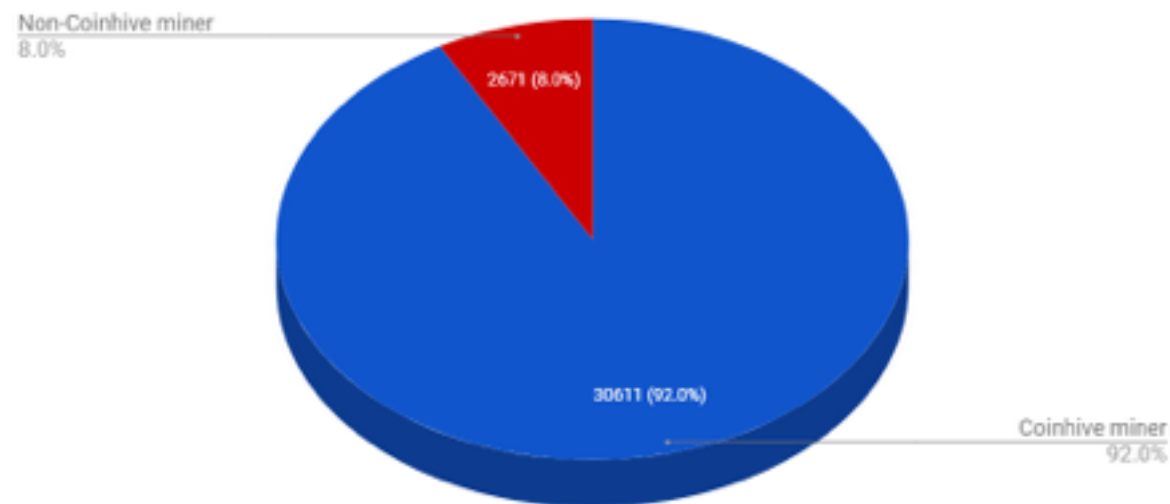
Website	Results	Query Parameter
Coinhive	30611	'coinhive.min.js'
JSEcoin	1131	'load.jsecoin.com'
Crypto-Loot	695	'CryptoLoot.Anonymous'
Minr	324	'minr.pw', 'st.kjli.fi', 'abc.pema.cl', 'metrika.ron.si', 'cdn.rove.cl', 'host.d-ns.ga', 'static.hk.rs', 'hallaert.online', 'cnt.statistic.date', 'cdn.static-cnt.bid'
CoinImp	317	'www.coinimp.com/scripts/min.js', 'www.hashing.win'
ProjectPoi (PPoi)	116	'projectpoi.min'
AFMiner	46	'afminer.com/code/miner.php'
Papoto	42	'papoto.com/lib/papoto.js'

DATA GATHERING

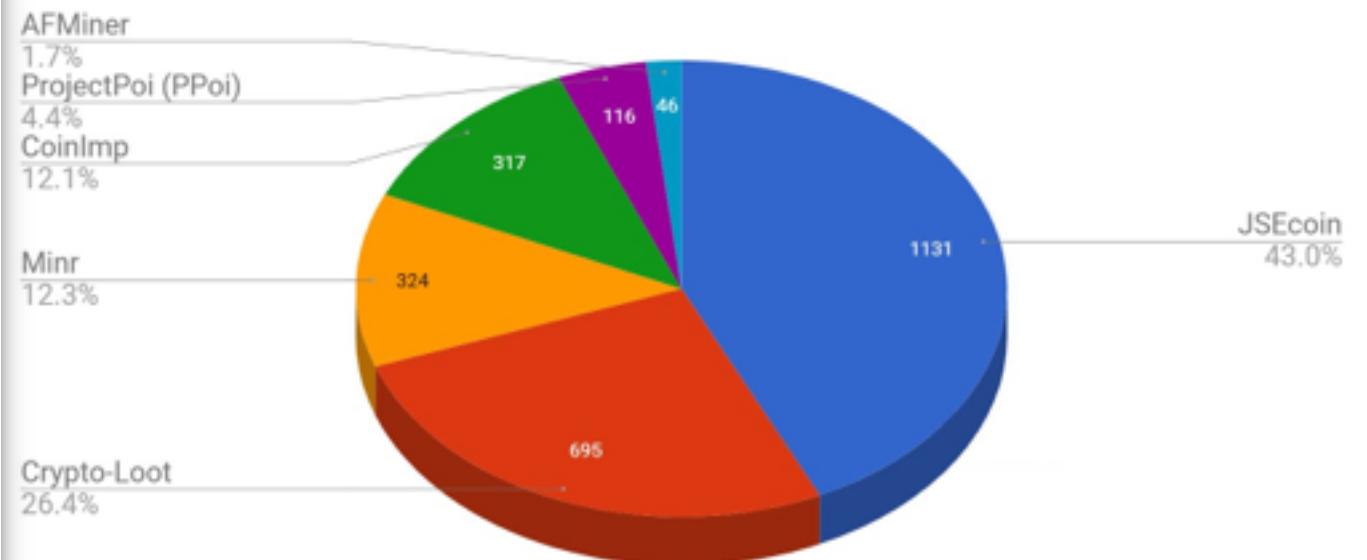
STATE OF AFFAIRS (JANUARY 2018)

- Coinhive being the first and the lead in the market share
- JSEcoin and Crypto-loot followed after

Number of websites running a JavaScript cryptocurrency miner



Number of websites running non-Coinhive JavaScript cryptocurrency miners

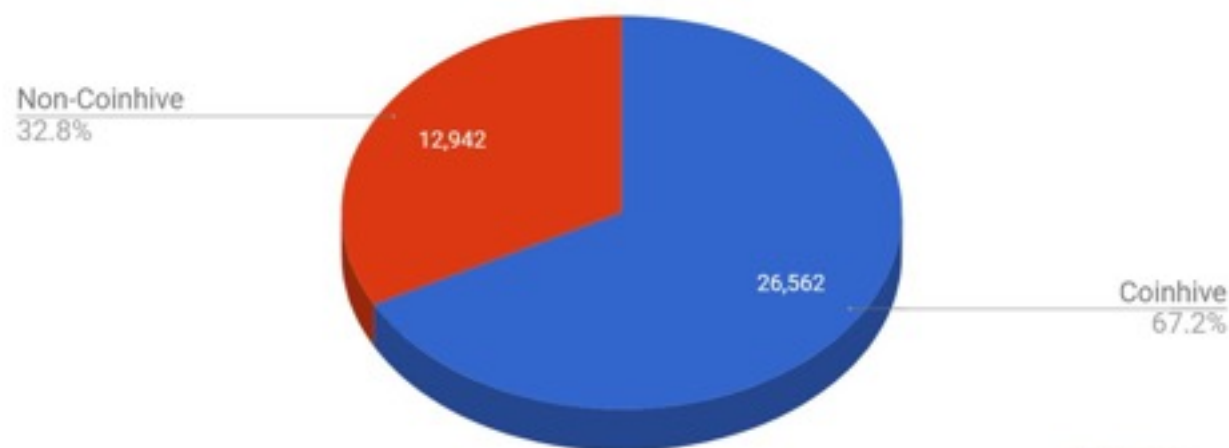


DATA GATHERING

STATE OF AFFAIRS (APRIL 2018)

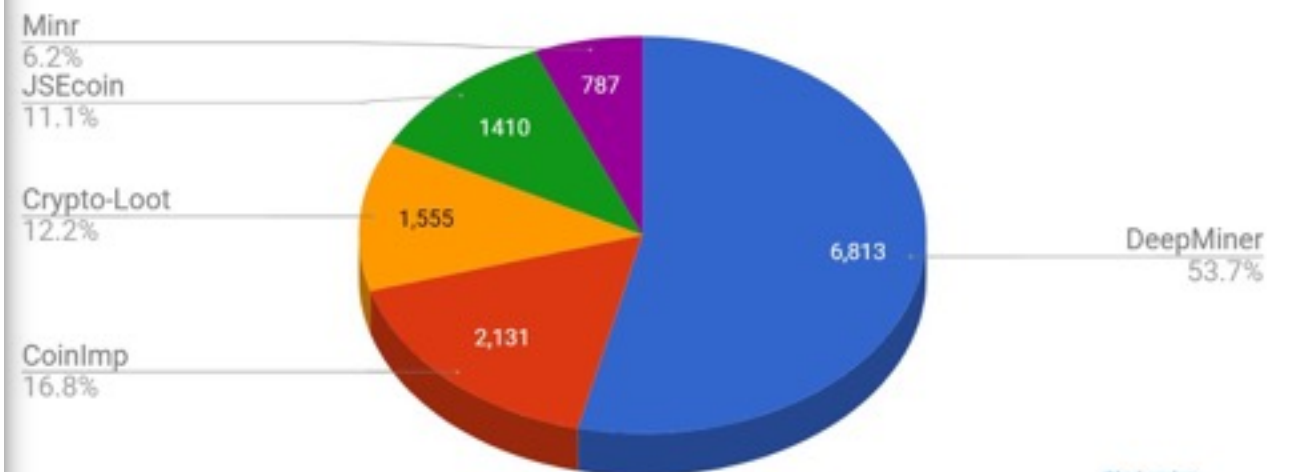
- Due to Coinhive popularity, ISP and adblockers started to blacklist their domains
- DeepMiner and Minr, use obfuscation methods to bypass these blockages

Number of websites found running a JavaScript cryptocurrency miner



@bad_packets
Source: PublicWWW
Date: 2018-04-19

Number of websites found with a non-Coinhive cryptocurrency mining script

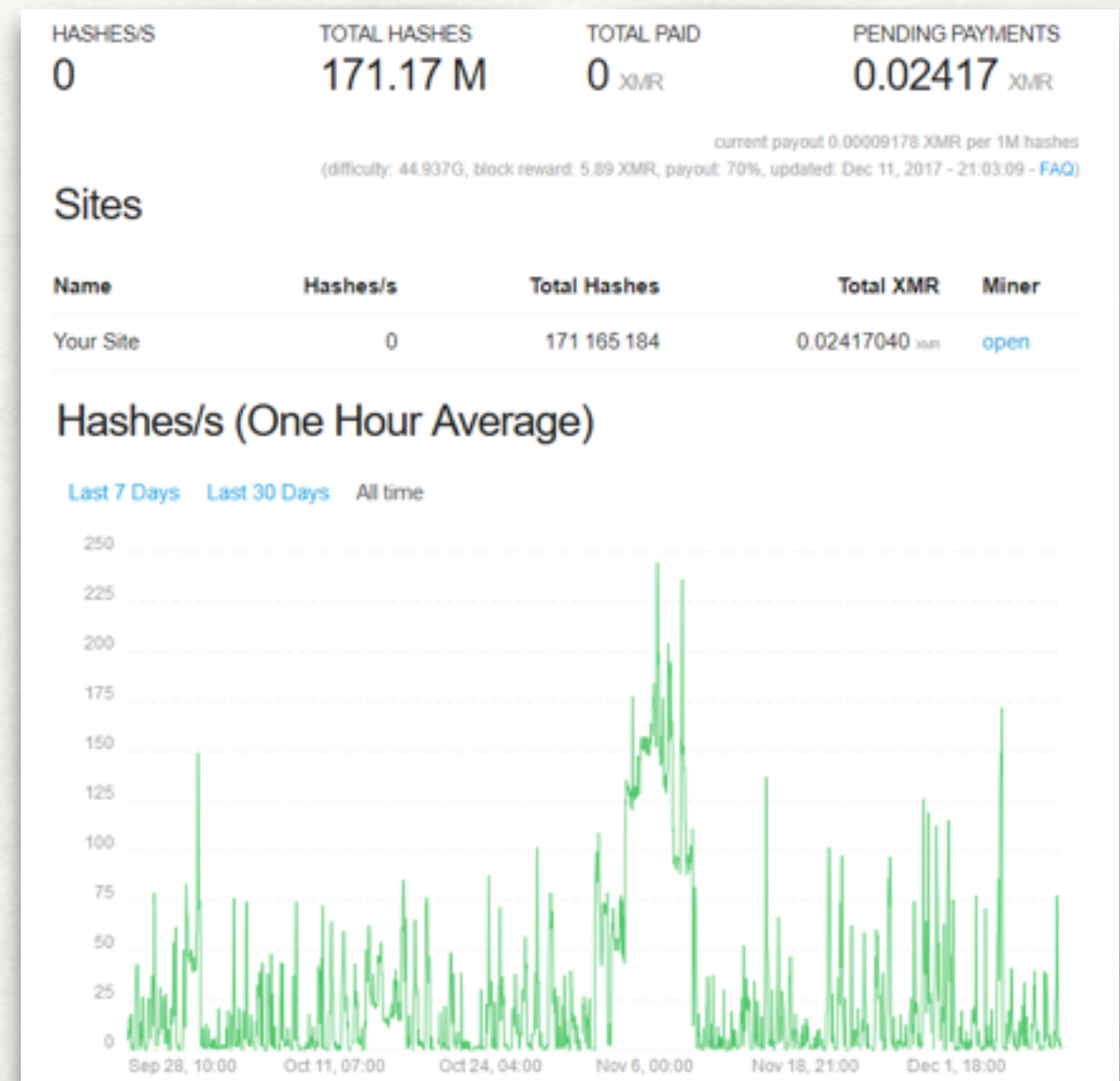


@bad_packets
Source: PublicWWW
Date: 2018-04-19

EXPERIMENT

PROFITABILITY

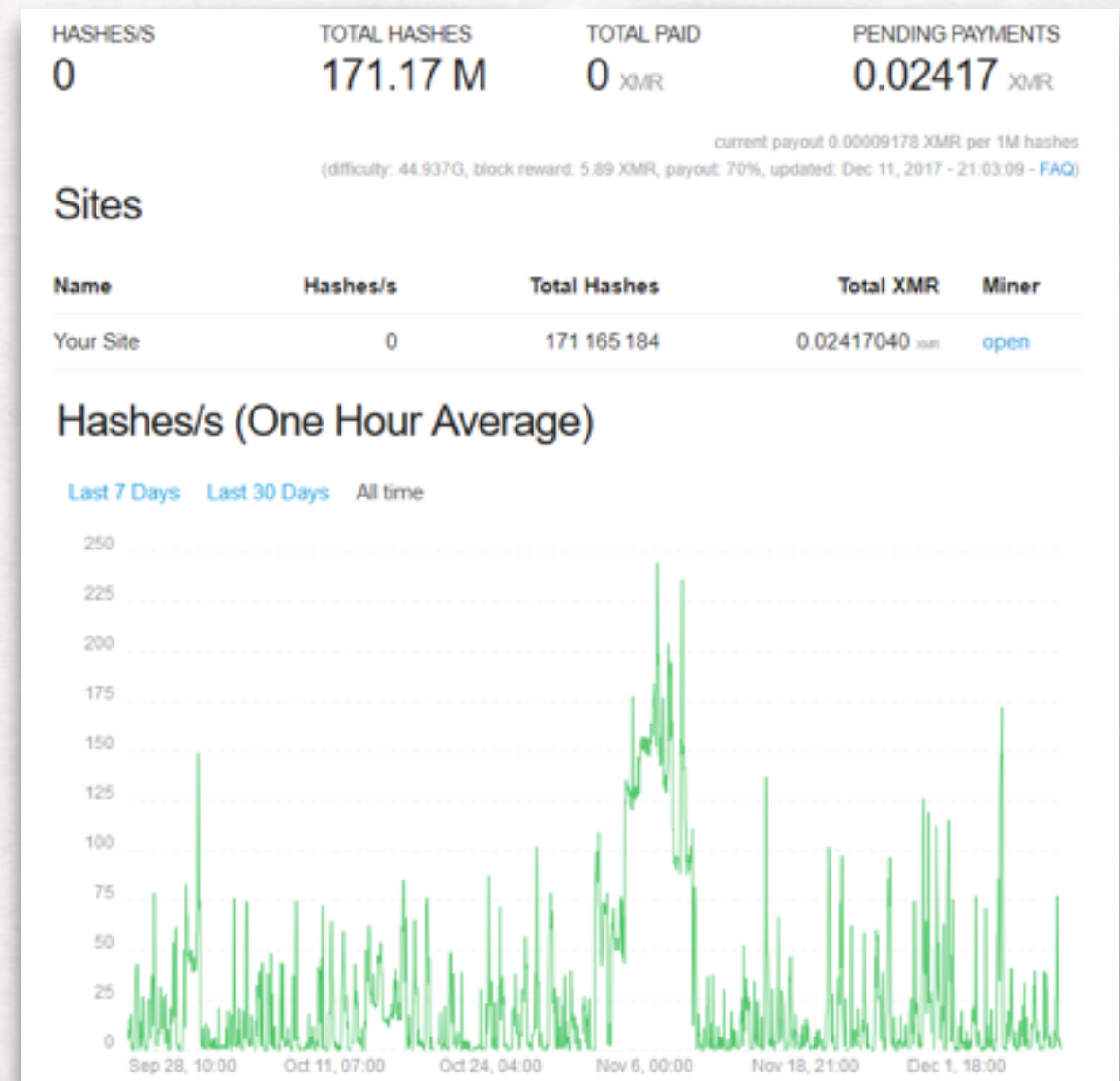
- 11,000 Parked domains over 3 months (October - December)
- 105,580 user sessions - Average of 24 seconds per session
- Revenue of 0.02417 XMR (~\$7.69)



EXPERIMENT

PROFITABILITY

- 11,000 Parked domains over 3 months (October - December)
- 105,580 user sessions - Average of 24 seconds per session
- Revenue of 0.02417 XMR (~\$7.69)
- More profitable on long sessions (e.g Streaming websites)
- Not significant compared to online advertisement profitability



THREAT MODEL

WHERE CRYPTOJACKING CAN BE INJECTED

1. Webmaster initiated

- Add new revenue model or remove ads/premium content
- Banned websites from official revenue models: e.g Large Russian website offering child pornography to users

2. Third-party services

- e.g. Google Tag Manager code injection on Movistar, Globovision
- Advertisement script injections: YouTube users in Japan, France, Taiwan, Italy, and Spain for nearly a week

THREAT MODEL

WHERE CRYPTOJACKING CAN BE INJECTED

3. Browser extensions

- e.g. Chrome extension "*Archive Poster*" (100,000+ users)

4. Breaches

- LiveHelpNow's SDK: 1500 websites using their chat support service such as retail store chains Crucial and Everlast
- Browsealoud: United Kingdom governmental websites such as Information Commissioner's Office, UK NHS services, Manchester City Council and around 4200 other websites

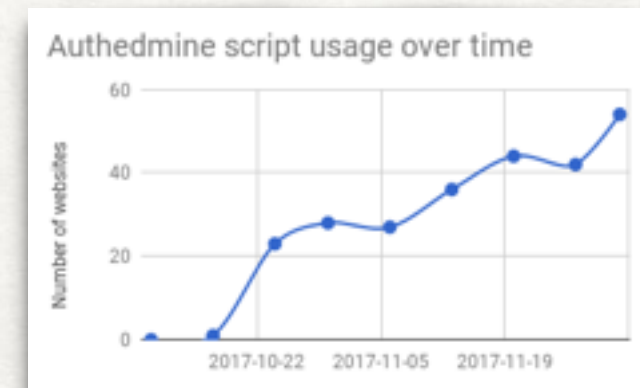
5. Man-in-the-middle

- Public wireless routers: Starbucks free Wi-Fi hotspots in Argentina (October 2017)

MITIGATION

TO BLOCK OR NOT TO BLOCK?

- To Block (Through Browser, ISP, ...)
 - Extensions: CoinBlockerLists, Adblockr
 - Opera Browser "NoCoin" blacklist
 - Is this the answer? What about the good usages of this new model?
- Not to Block (User Consent)
 - Authedmine service from Coinhive
 - Regulations similar to user tracking cookies (EU Cookie Law)



DISCUSSION

ETHICAL SCENARIOS

1. The use of Cryptojacking on a breached website
 - Unethical!
2. The use of Cryptojacking by the website owner with an attempt at obtaining user consent
 - Controversial, unclear if users understand what they are consenting to
3. The use of Cryptojacking by the website owner **without obtaining user consent.**
 - Considered unethical and illegal, *invisible abuse*

DISCUSSION

ETHICAL QUESTIONS

- *The use of Cryptojacking by the website owner with an attempt at obtaining user consent*
- How to communicate what is happening to user, EU Cookie Law style policy is not sufficient
 - Potential harm to users of cryptojacking:
 - Higher electricity bills / battery usage
 - Accelerated device degradation
 - Slower system performance
 - Poor web experience
- New online revenue eco-system, needs regulation and policies

FUTURE WORK

INTERESTED IN COLLABORATION?

- Technical analysis of Monero hashing rate
 - How much of the processing power comes from these Cryptojacking campaigns? Is there a way to identify the platforms/pools through block headers or other data?
- How this new monetization model can work? User education and UX design to get proper user consent
- Policy making and Ethical discussions

THANK YOU

QUESTIONS?

Shayan Eskandari

Andreas Leoutsarakos, Troy Mursch, Jeremy Clark

Twitter:

@sbetamc

@bad_packets

@pulpSpy



UNIVERSITÉ
Concordia
UNIVERSITY