A FIRST LOOK AT BROWSER-BASED

CRYPTOJACKING

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

**Concordia University, †Bad Packets Report*

UNIVERSITÉ Concordia UNIVERSITY

Cryptojacking

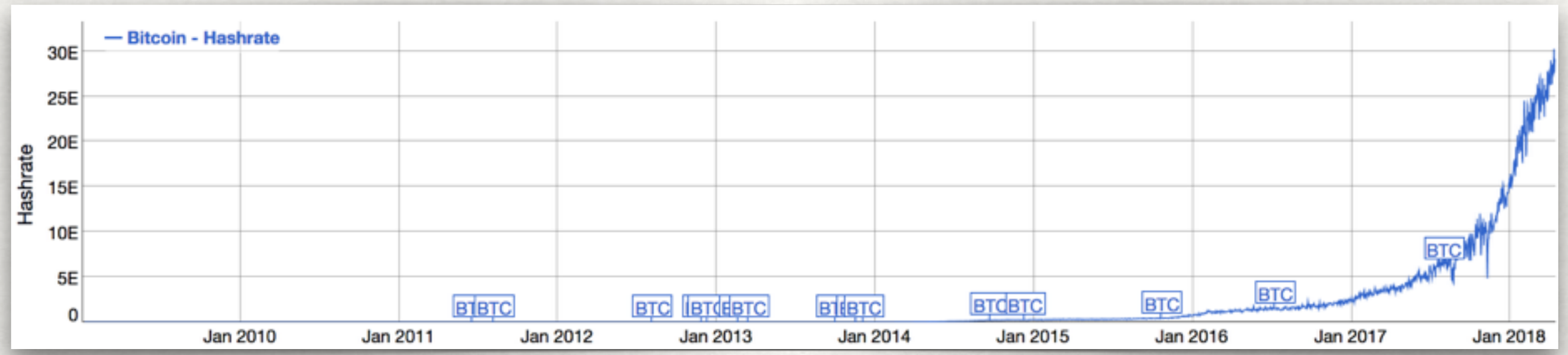
[krɪptoʊdʒækɪŋ], verb

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

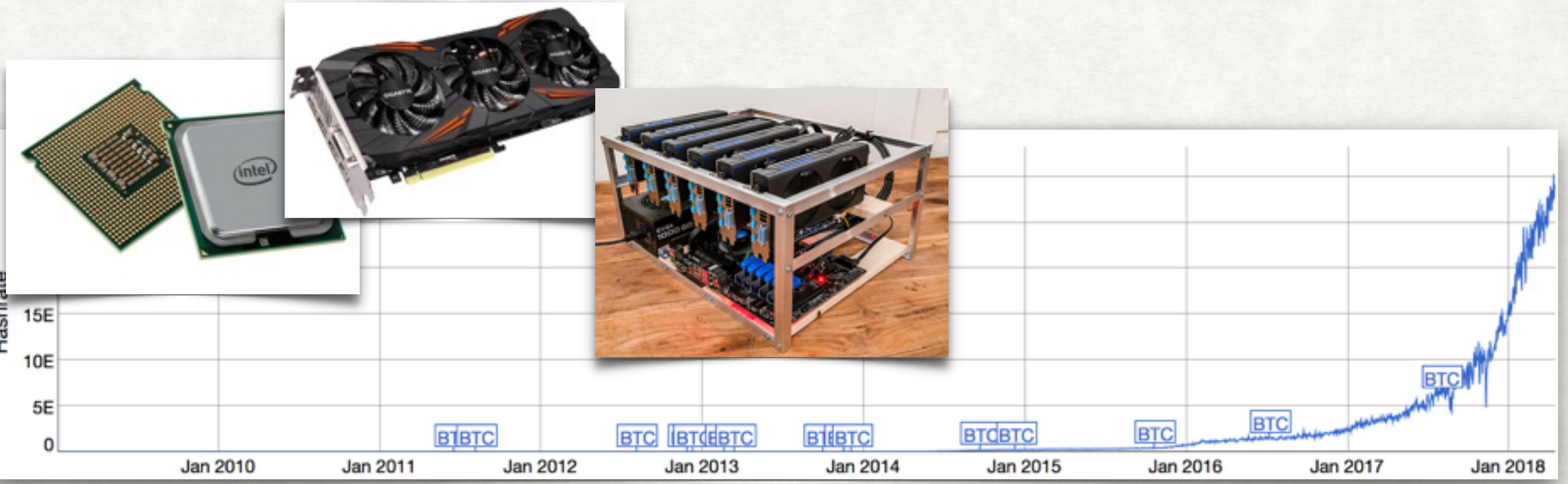
HISTORY OF BITCOIN MINING

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

INTRODUCTION

HISTORY OF BITCOIN MINING

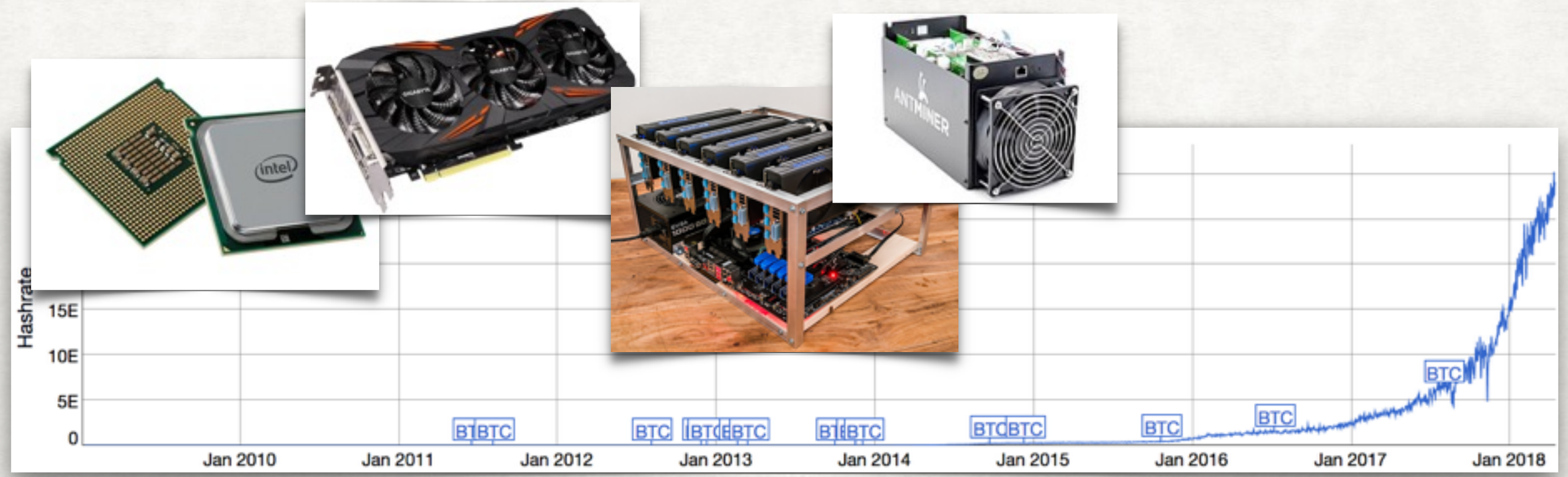
- **Bitcoin**
  - Mining algorithm(PoW): SHA-256
  - Net hashrate: 30,035.96 Ph/s



INTRODUCTION

HISTORY OF BITCOIN MINING

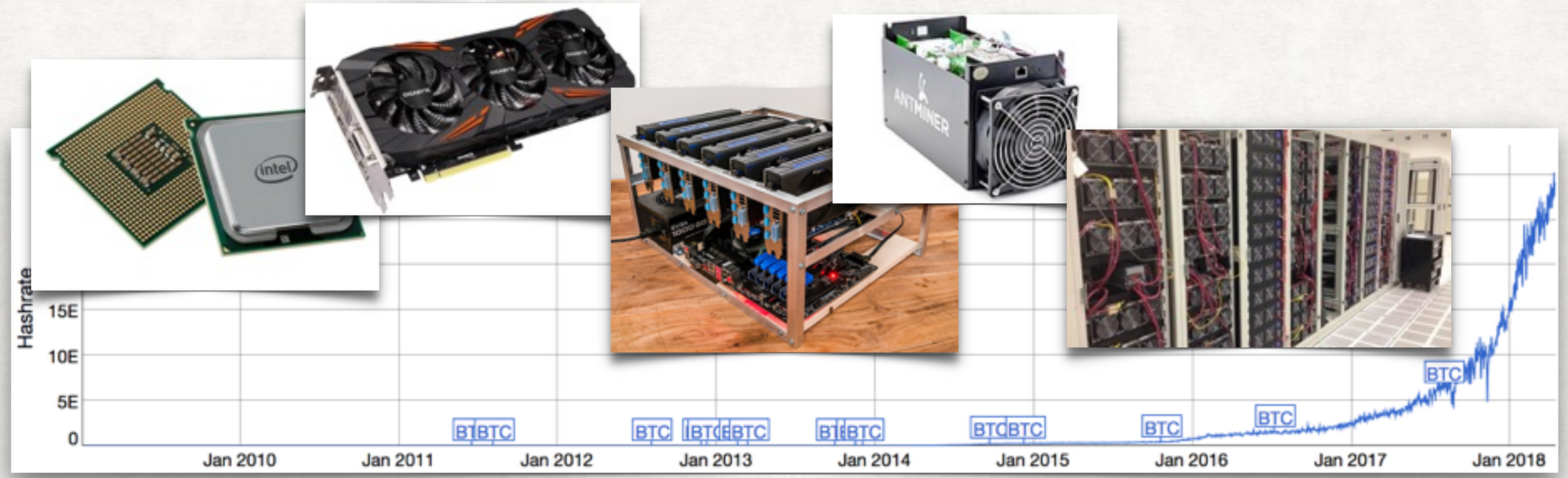
- **Bitcoin**
  - Mining algorithm(PoW): SHA-256
  - Net hashrate: 30,035.96 Ph/s



INTRODUCTION

HISTORY OF BITCOIN MINING

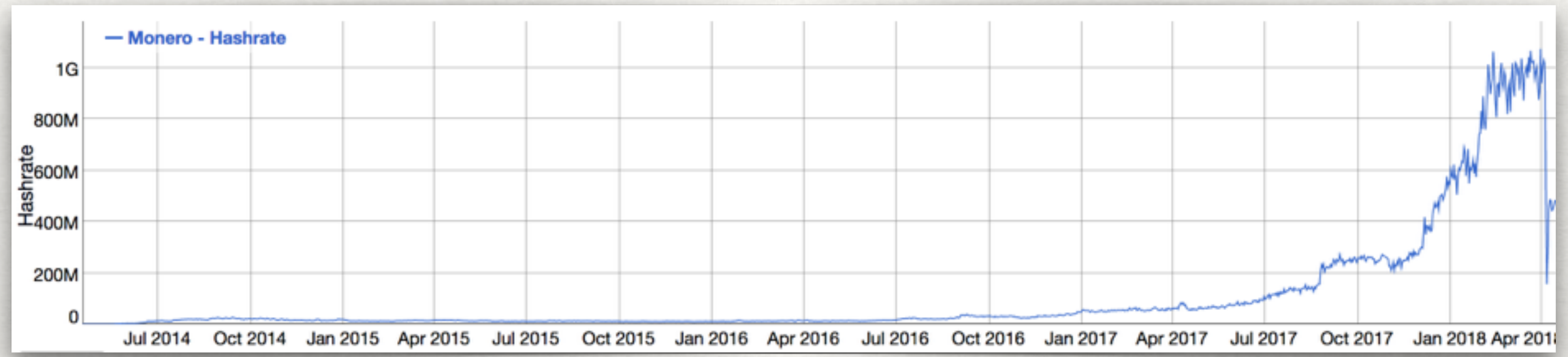
- **Bitcoin**
  - Mining algorithm(PoW): SHA-256
  - Net hashrate: 30,035.96 Ph/s



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)

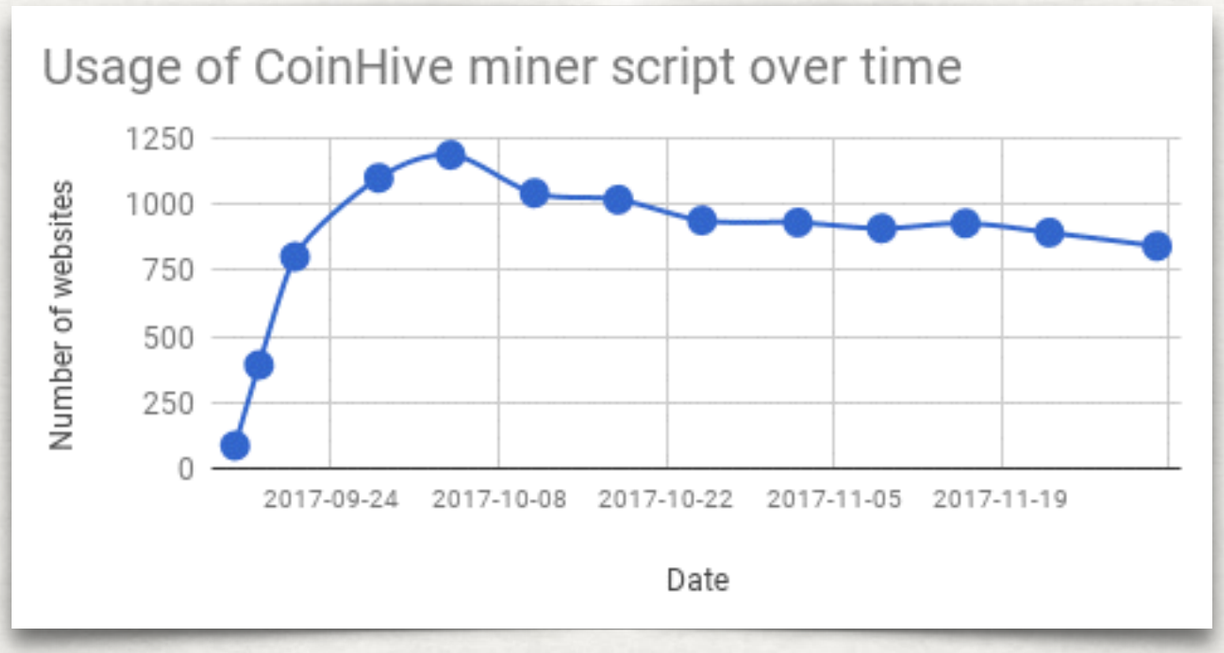
INTRODUCTION

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

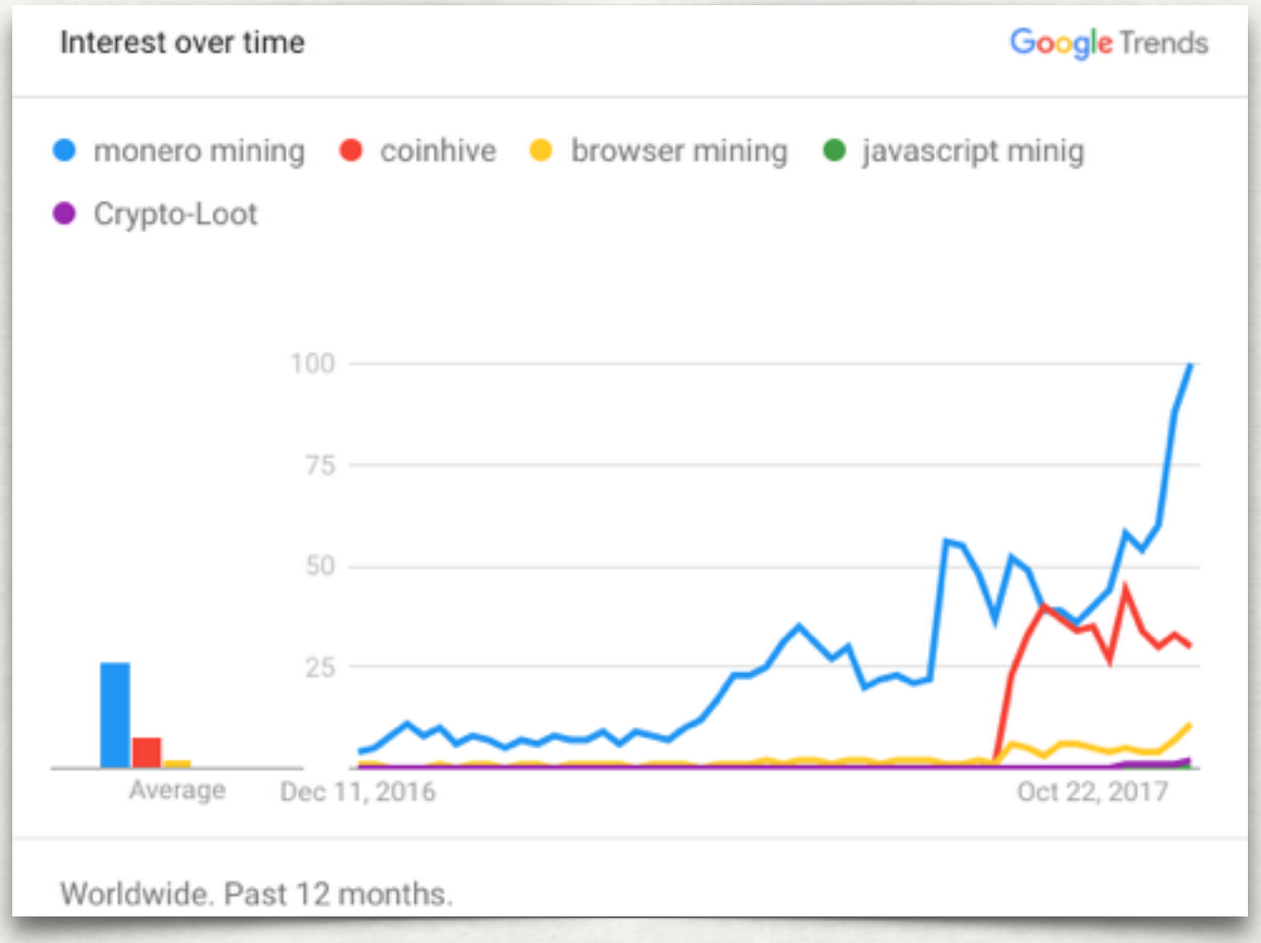
- **Coinhive**
  - Launched in September 2017, as a service to replace ads
    - Also offered CAPTCHA and short-links services
  - Soon after several copycats appeared (Crypto-Loot, PPoi, Coin-Have, …)



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

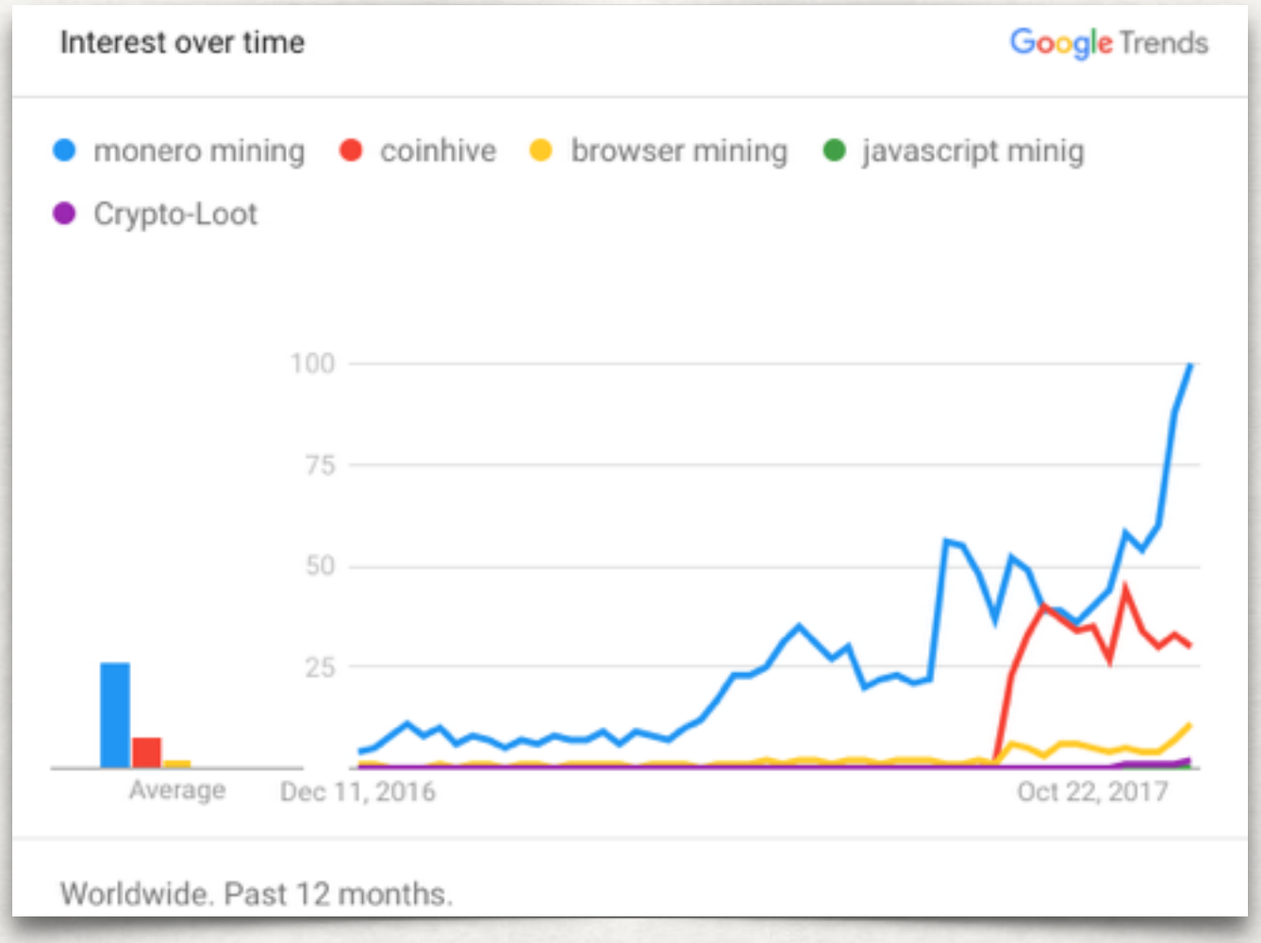


BROWSER-BASED CRYPTOJACKING

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

YAHOO! FINANCE

Why Cryptojacking Is The Next Big Cybersecurity Threat

FORTUNE

Robert Hackett

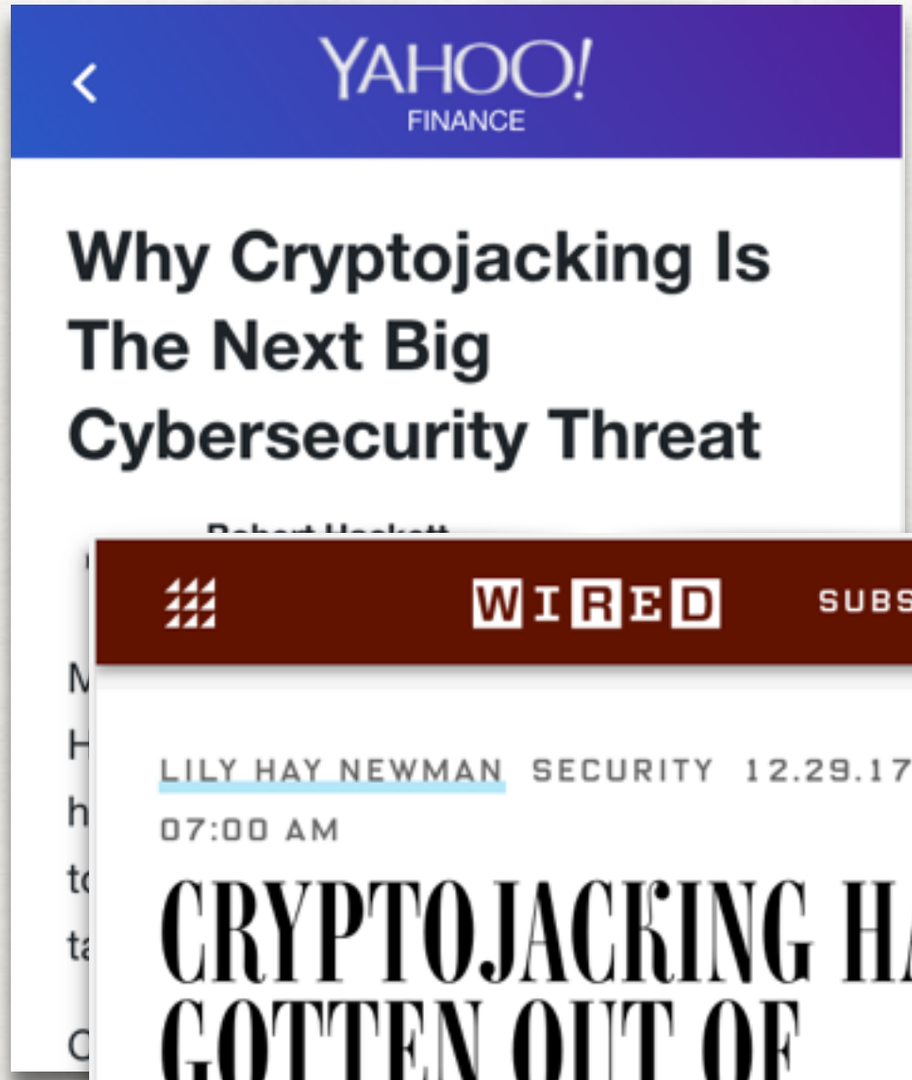
Fortune October 23, 2017

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

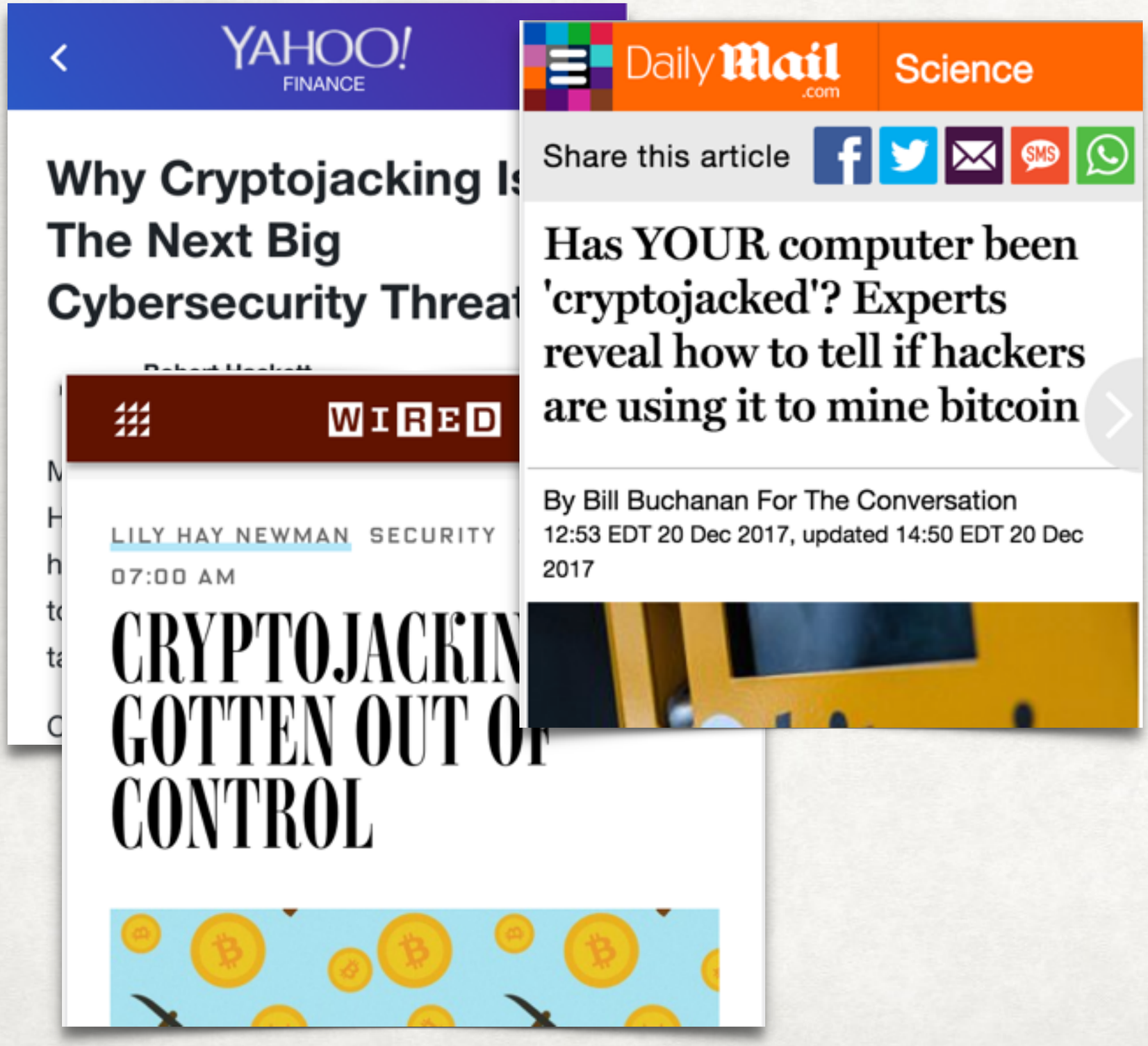
CRYPTOJACKING

THE NEXT BIG CYBERSECURITY THREAT



CRYPTOJACKING

THE NEXT BIG CYBERSECURITY THREAT



CRYPTOJACKING

THE NEXT BIG CYBERSECURITY THREAT

YAHOO! FINANCE

Why Cryptojacking Is The Next Big Cybersecurity Threat

Daily Mail .com | Science

Share this article

Has YOUR computer been 'cryptojacked'? Experts reveal how to tell if hackers are using it to mine bitcoin

WIRED

LILY HAY NEWMAN SECURITY

07:00 AM

CRYPTOJACKIN GOTTEN OUT OF CONTROL

NATIONAL POST SHARE

The rise of cryptojacking: How hackers hog computer CPUs to make money

THE CANADIAN PRESS ALEKSANDRA SAGAN

November 19, 2017 10:02 AM EST

Last Updated November 19, 2017 10:02 AM EST

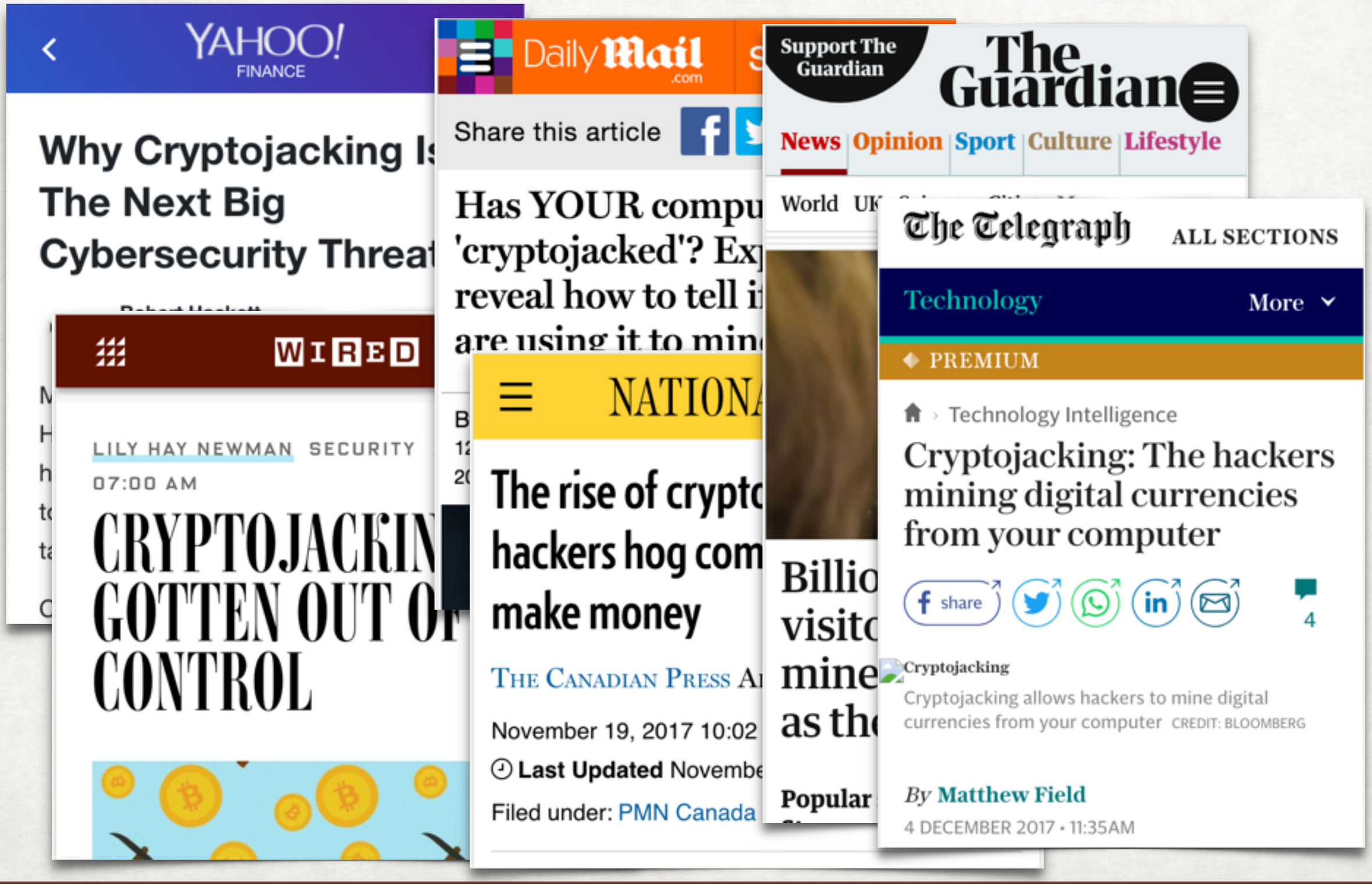
Filed under: PMN Canada

CRYPTOJACKING

THE NEXT BIG CYBERSECURITY THREAT

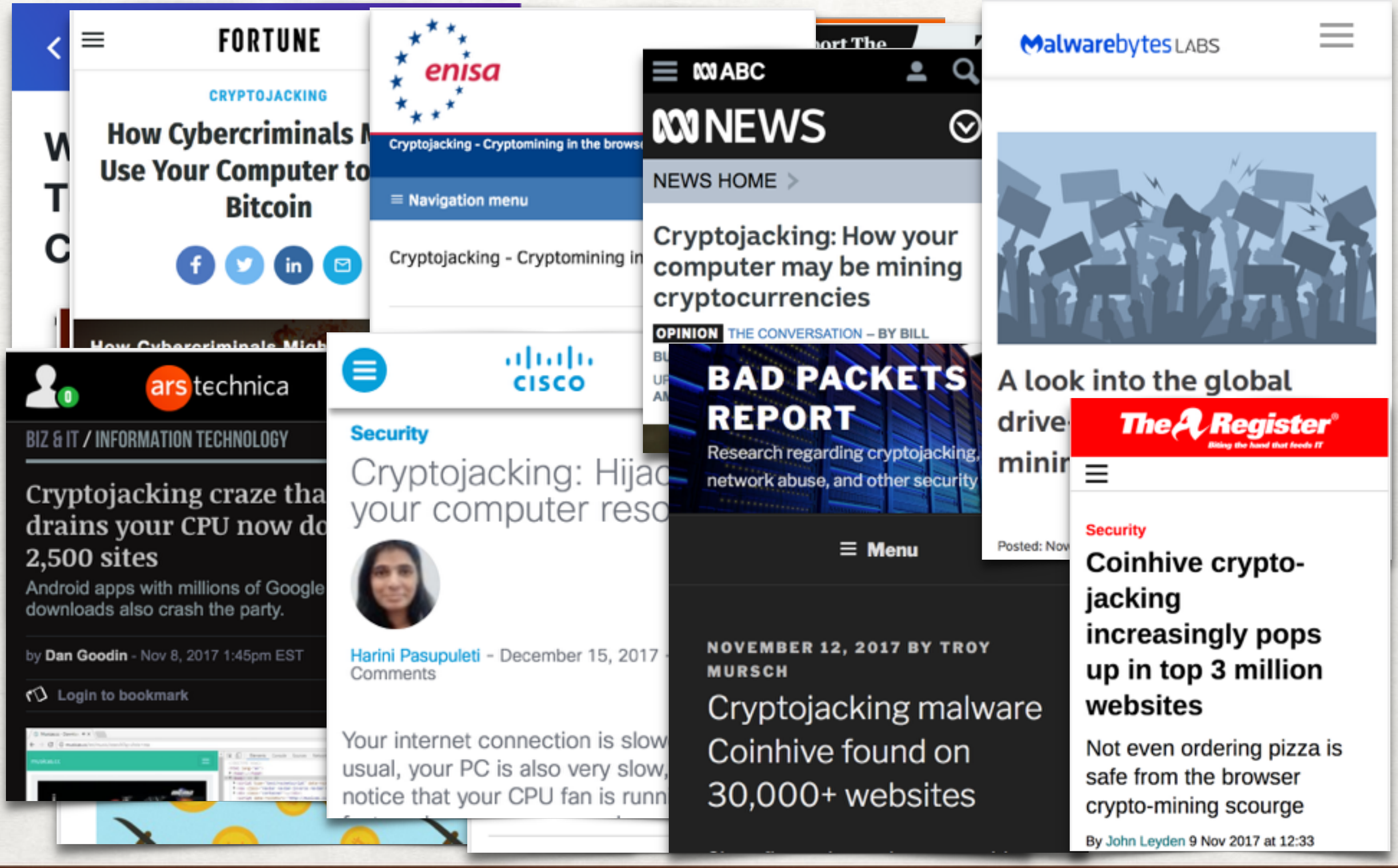
CRYPTOJACKING

THE NEXT BIG CYBERSECURITY THREAT



CRYPTOJACKING

THE NEXT BIG CYBERSECURITY THREAT



CRYPTOJACKING

UK ONLY

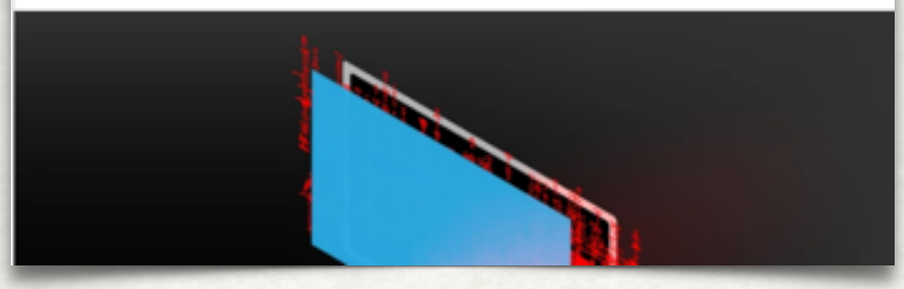
CRYPTOJACKING

UK ONLY

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

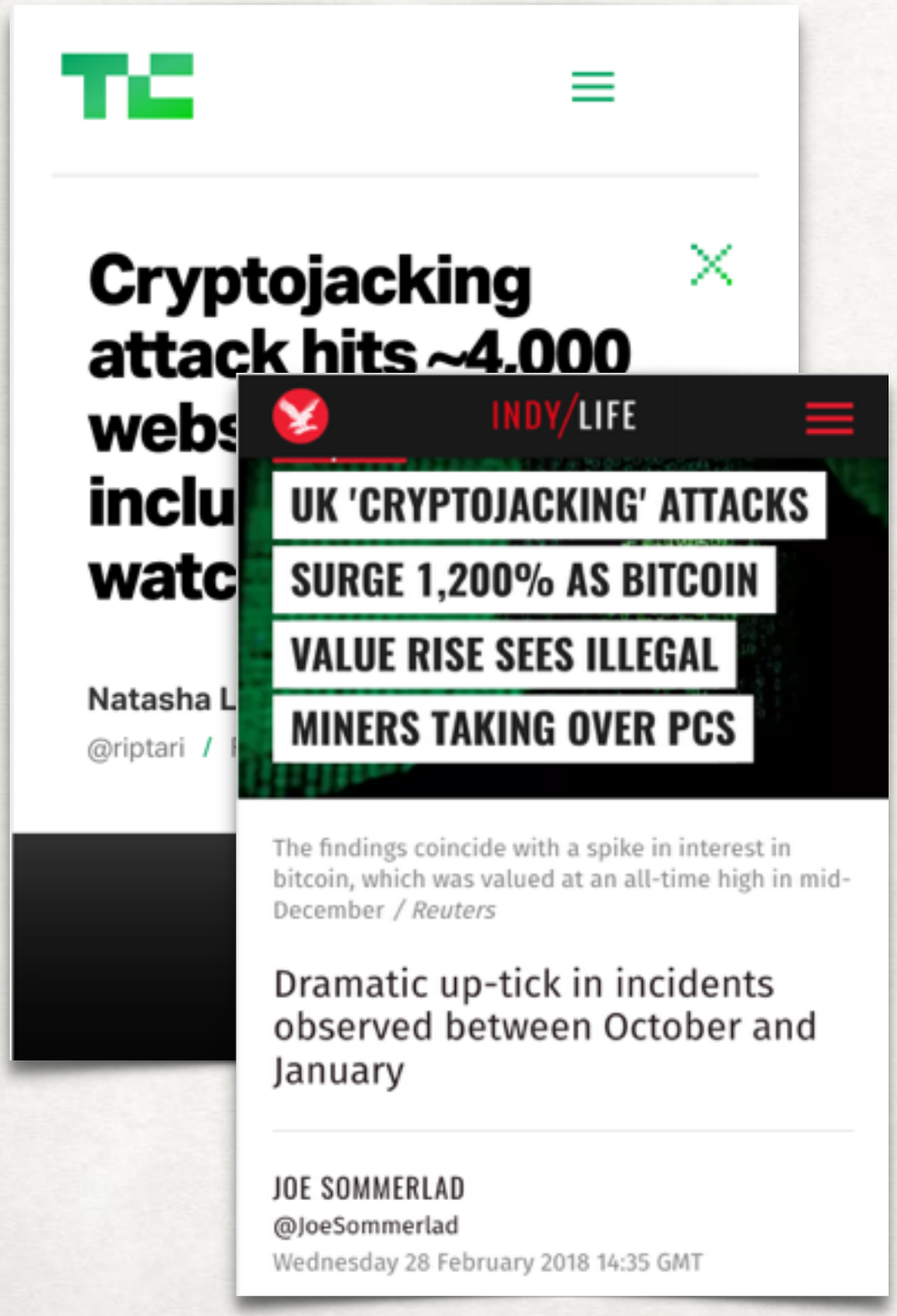
Natasha Lomas

@riptari / Feb 12, 2018



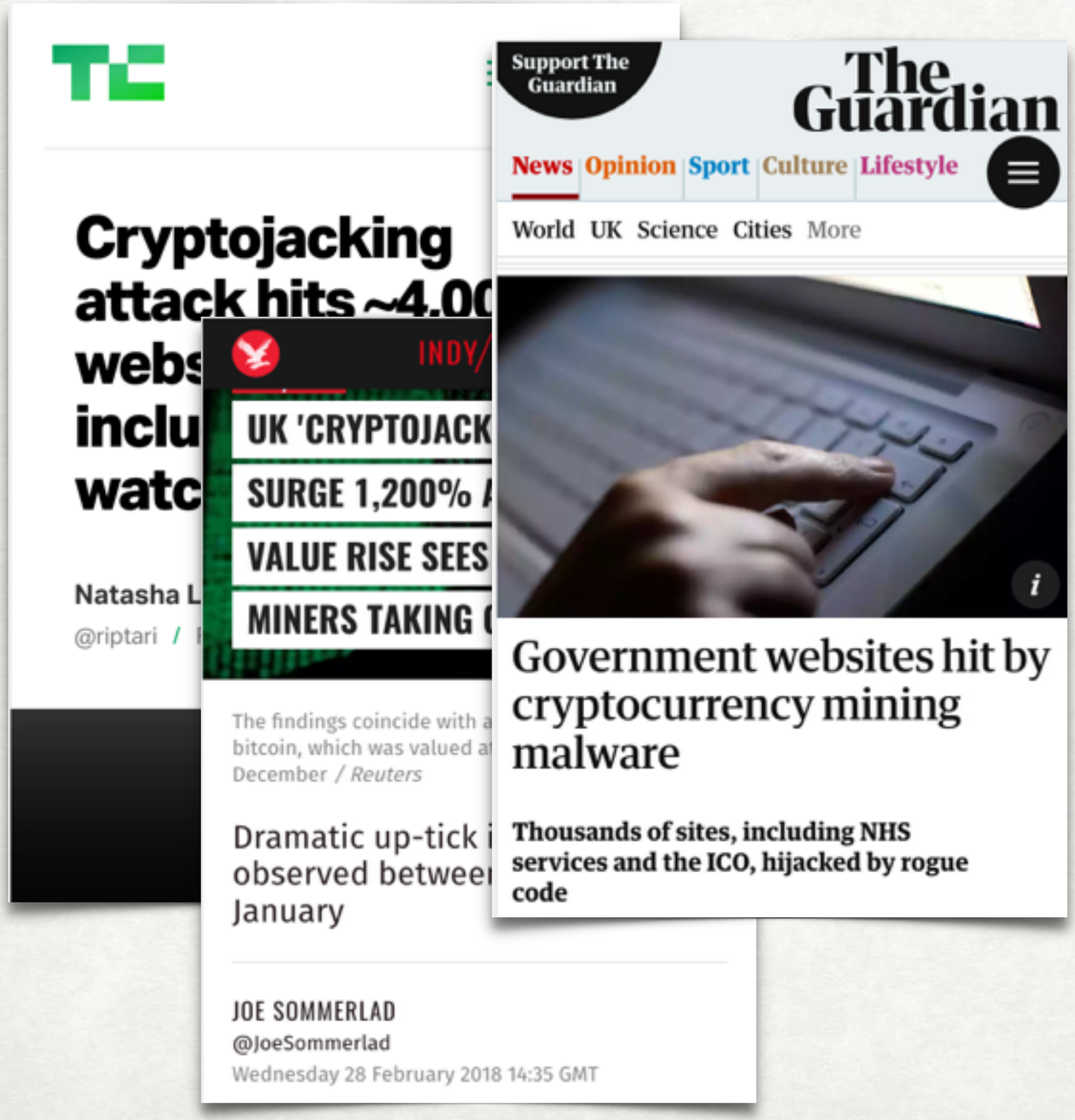
CRYPTOJACKING

UK ONLY



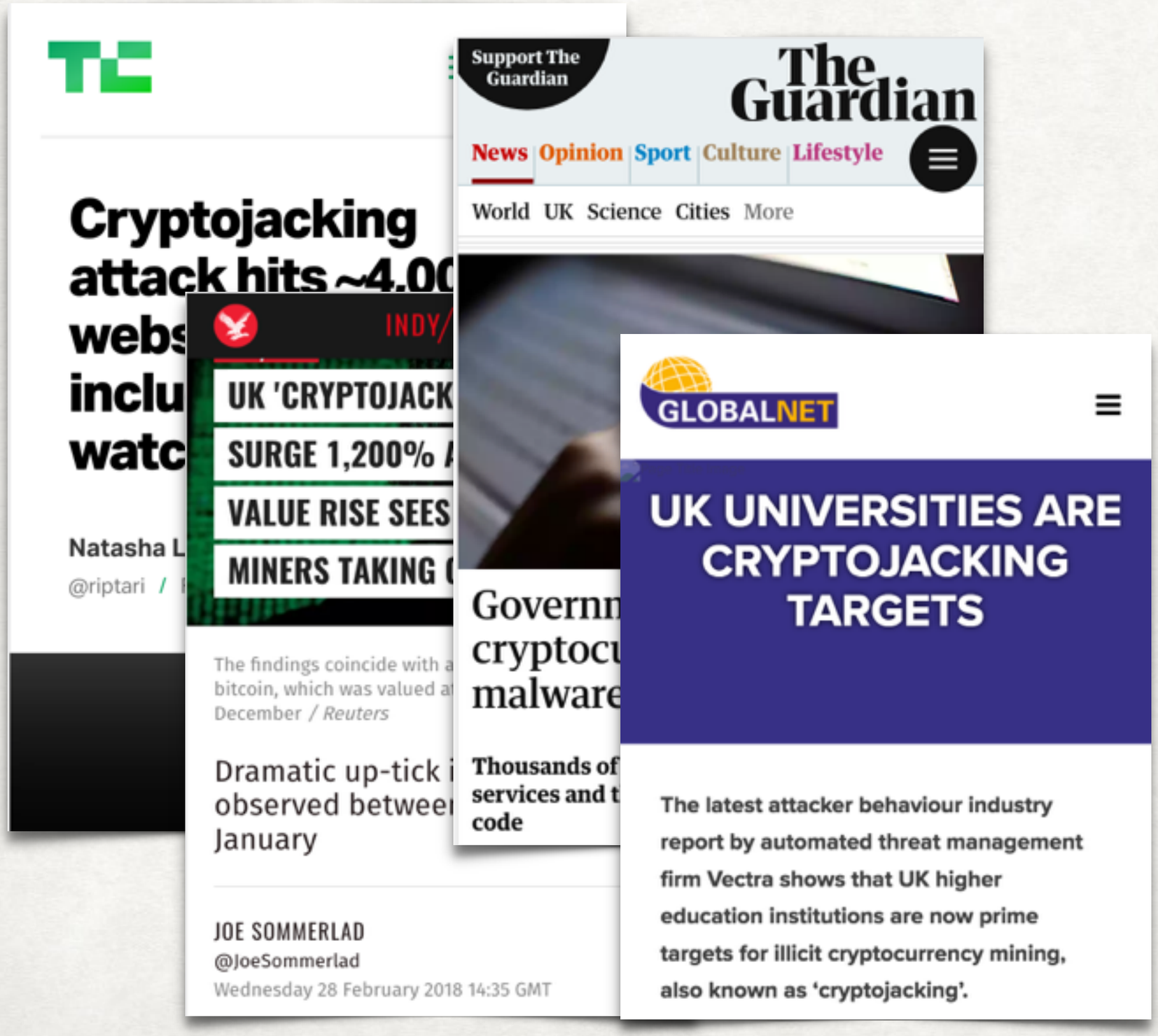
CRYPTOJACKING

UK ONLY



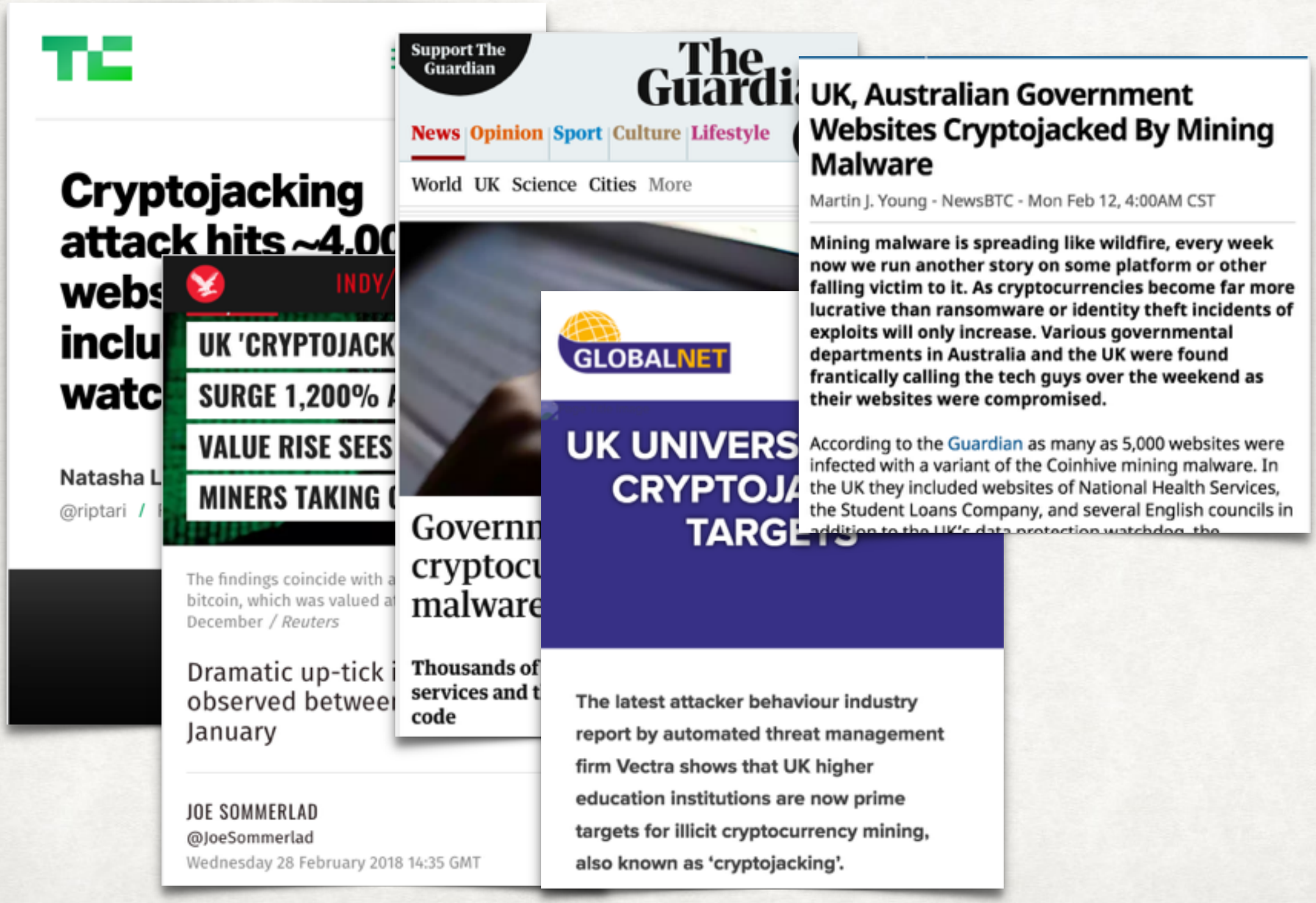
CRYPTOJACKING

UK ONLY



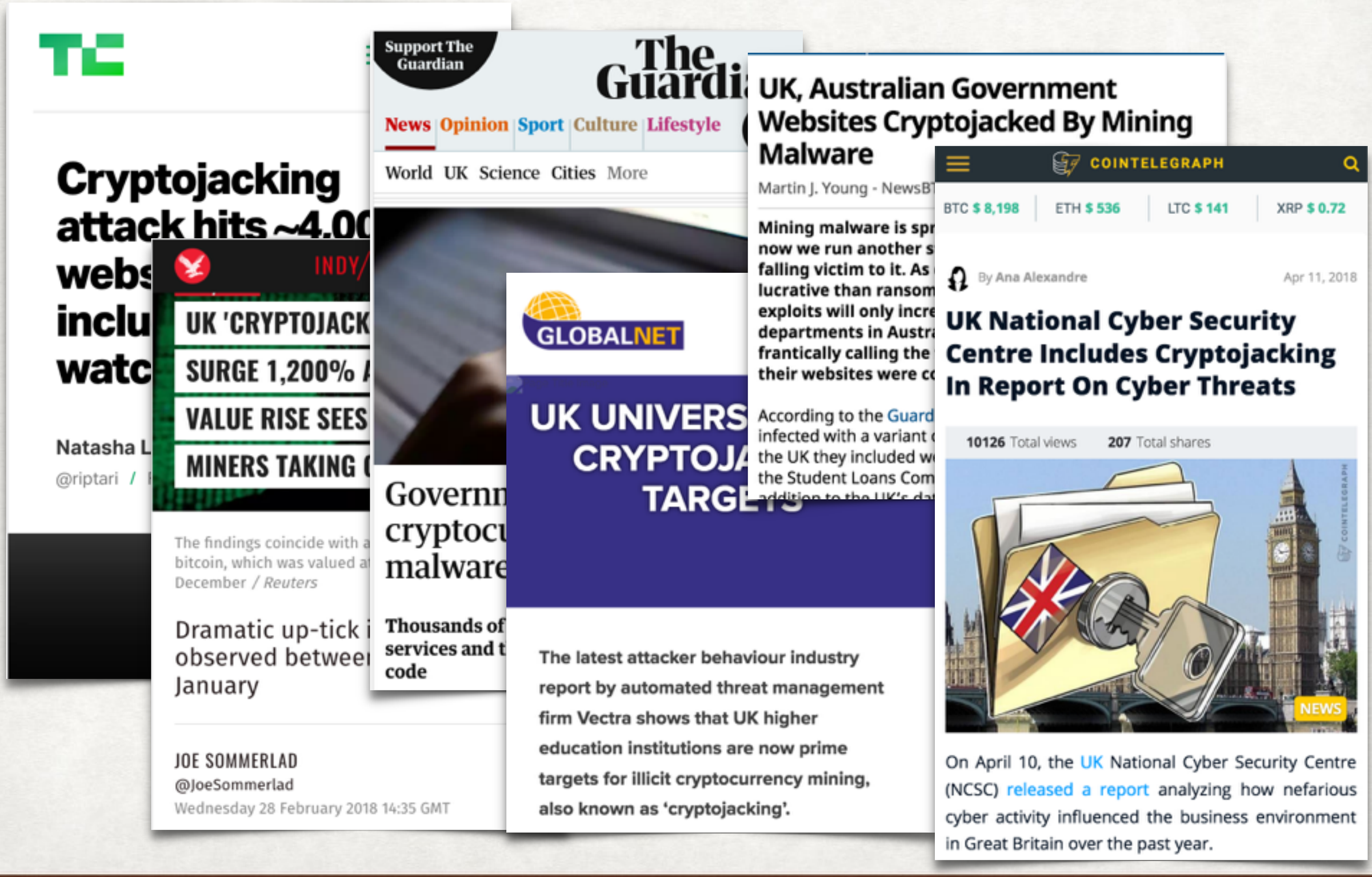
CRYPTOJACKING

UK ONLY



CRYPTOJACKING

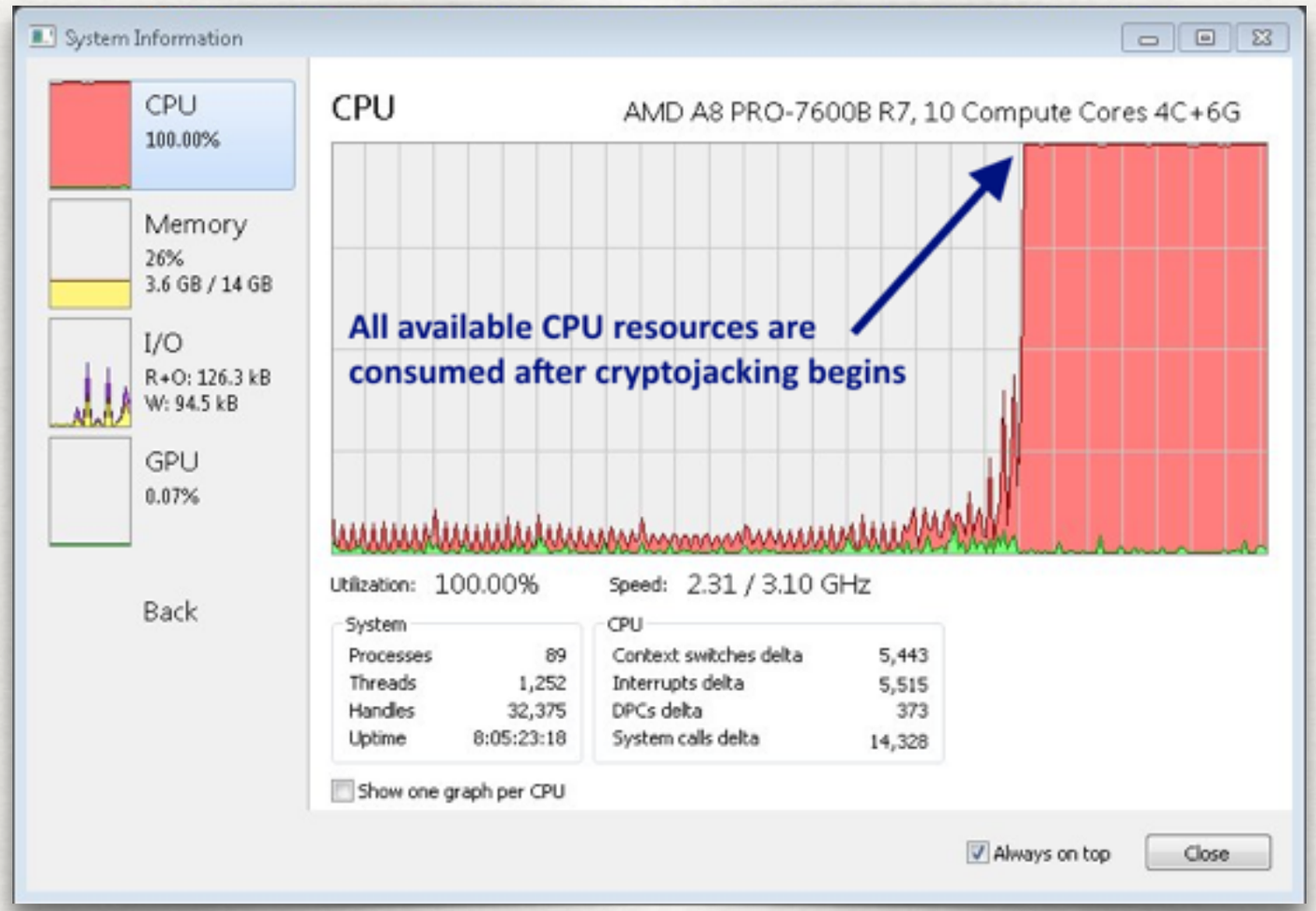
UK ONLY



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

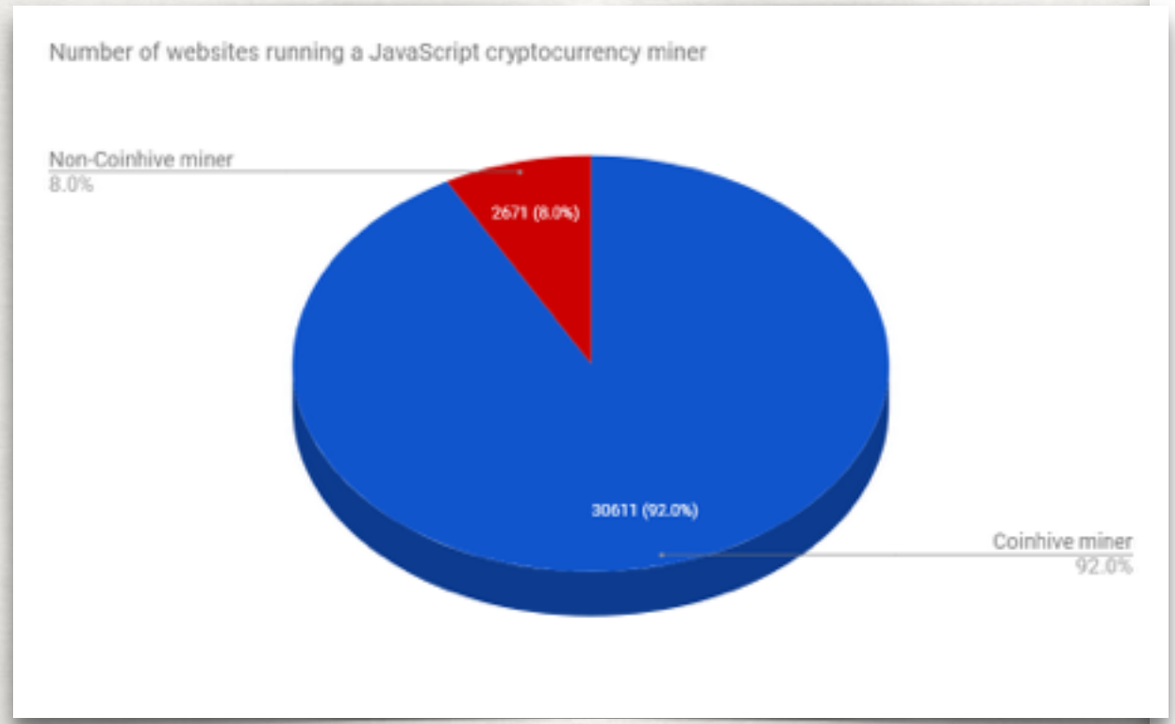
- Censys.io BigQuery dataset (Top 1 Million websites)
- PublicWWW's dataset (~200 Million indexed websites)

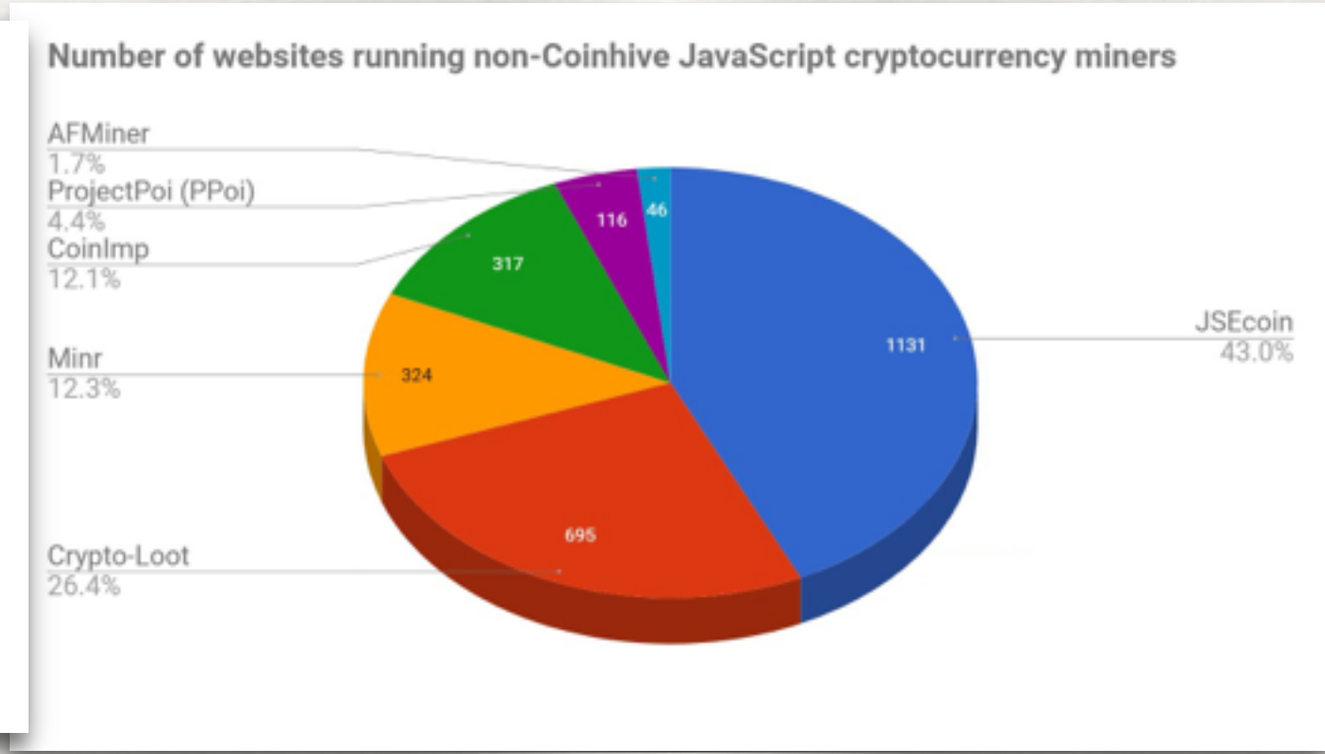
Website	Results	Query Parameter
Coinhive	30611	'coinhive.min.js'
JSEcoin	1131	'load.jsecoin.com'
Crypto-Loot	695	'CryptoLoot.Anonymous'
Minr	324	'minr.pw','st.kjli.fi', 'abc.pema.cl','metrika.ron.si', 'cdn.rove.cl','host.d-ns.ga', 'static.hk.rs','hallaert.online', 'cnt.statistic.date','cdn.static-cnt.bid'
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

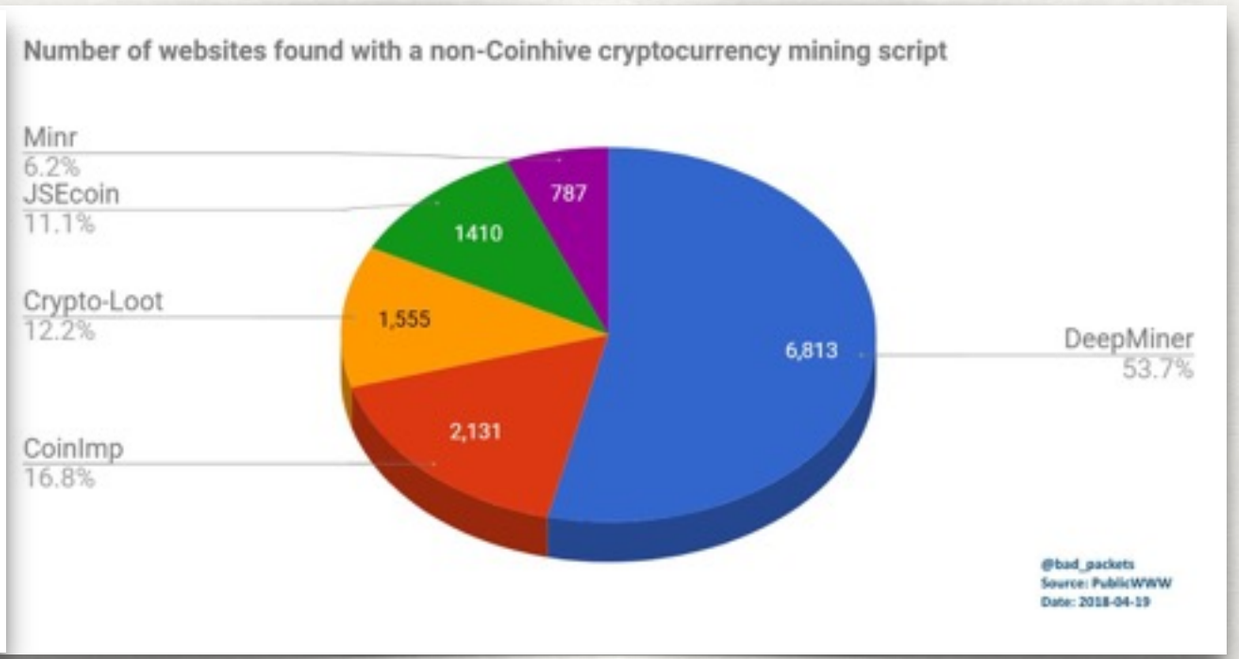




DATA GATHERING

STATE OF AFFAIRS (APRIL 2018)

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



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