Cryptojacking 2

A Follow-Up on ‘Cryptojacking: How to Go to Prison with JavaScript’

What is Cryptojacking?

Cryptojacking is the unauthorized use of another person’s processor to mine cryptocurrency.

Cryptojacking is highly unethical and **illegal** in many parts of the world.

Cryptojacking can be done on almost **any device** with a processor and an internet connection.

Cryptojacking poses a unique threat in that it requires very little access to a victim’s device to work. **It can even be done in a browser without any special user permissions.**

How does cryptojacking work on the web?

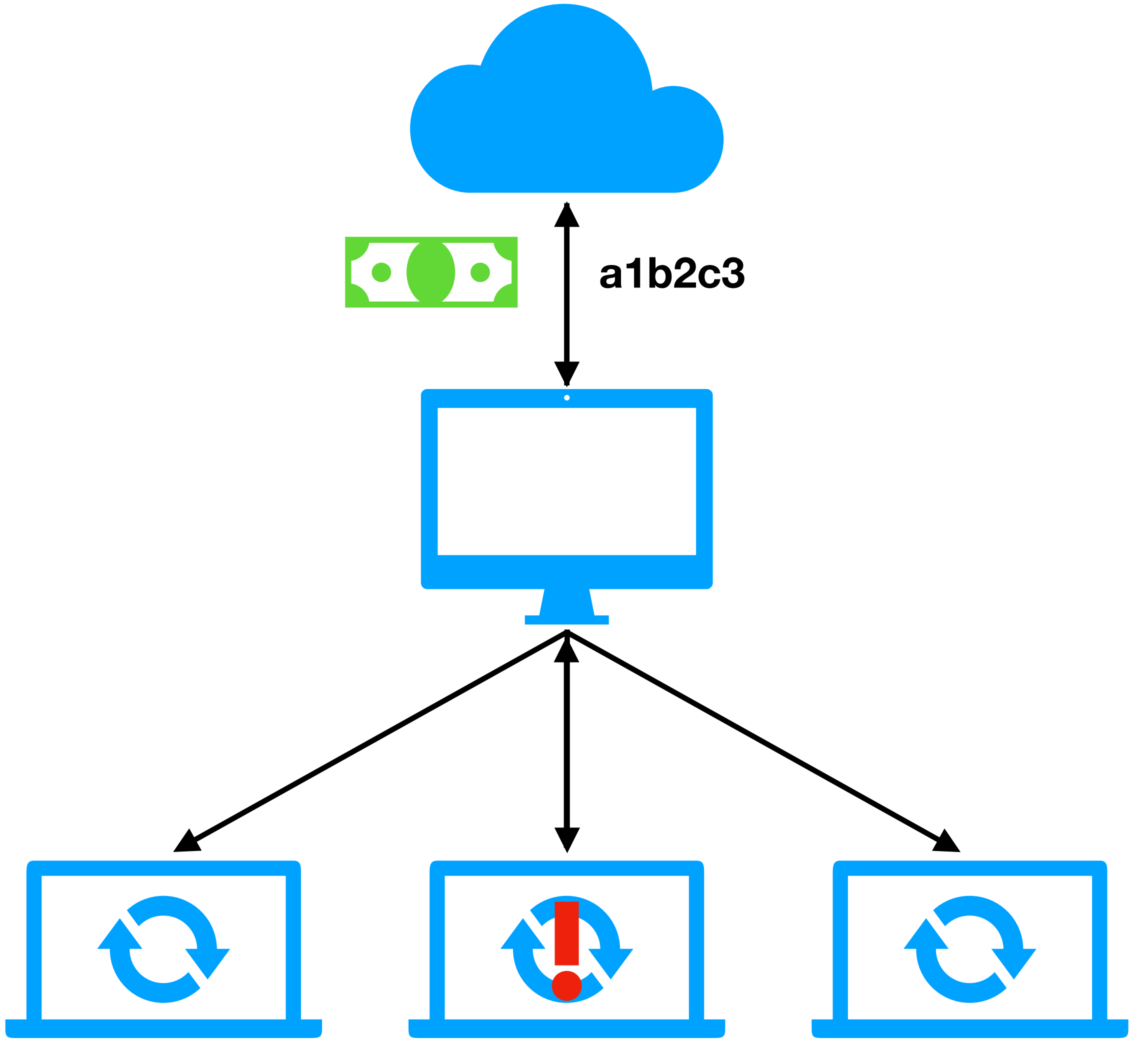
1. A user loads a mining script from the attacker's server via an either malicious or compromised website.

2. The script begins working until it finds successful block hashes.

3. When a hash is found, the client sends it back to the attacker's server.

4. The attacker then uses the block to claim a cryptocurrency reward on the blockchain.

5. Repeat.

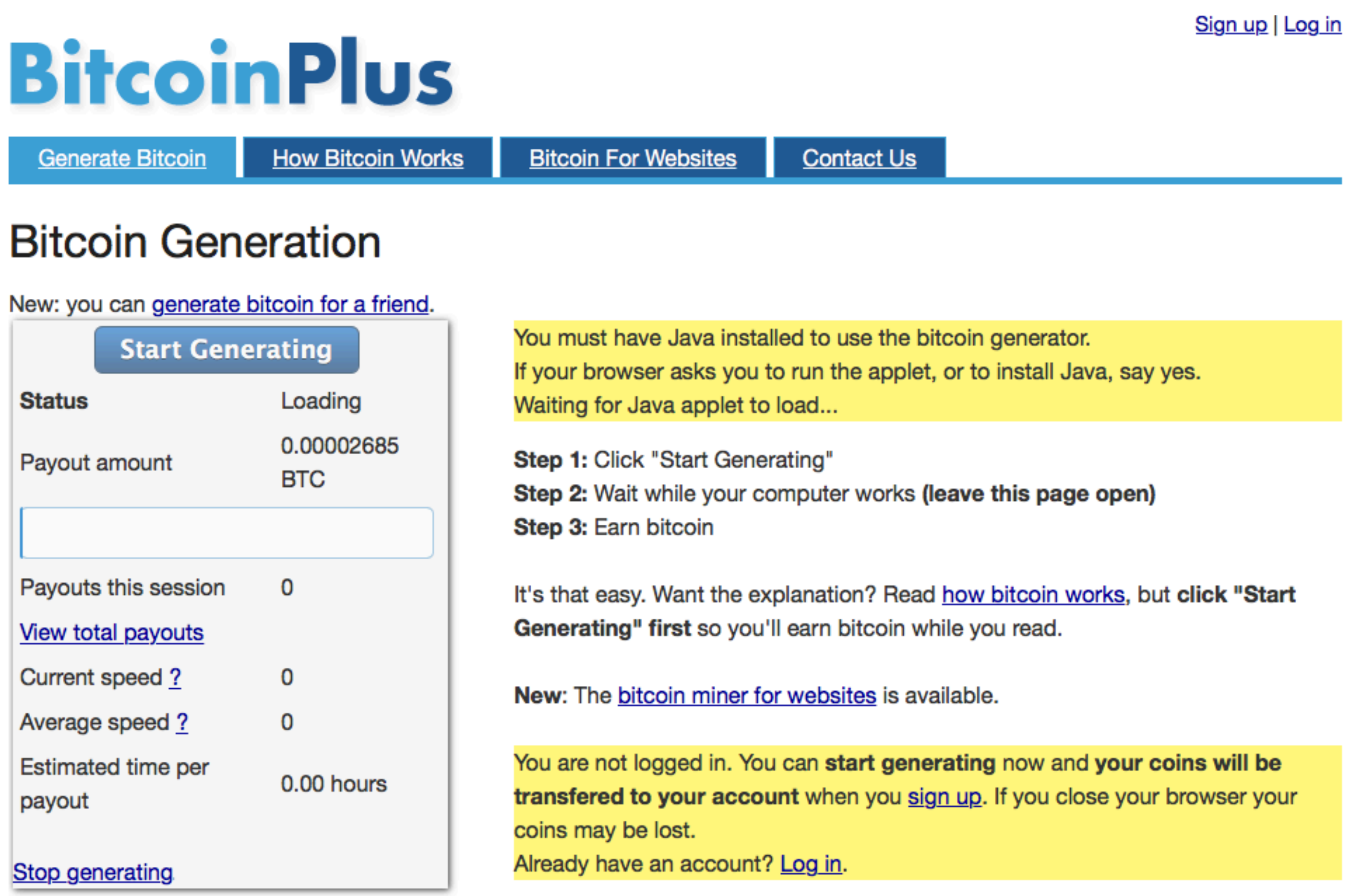


How did this ridiculousness become a thing?

Previously on…

Cryptojacking:

How to Go to Prison with JavaScript



Bitcoin Generation

New: you can generate bitcoin for a friend.

Status	Loading
Payout amount	0.00002685 BTC
Payouts this session	0
View total payouts	
Current speed ?	0
Average speed ?	0
Estimated time per payout	0.00 hours

Stop generating

You must have Java installed to use the bitcoin generator.
If your browser asks you to run the applet, or to install Java, say yes.
Waiting for Java applet to load...

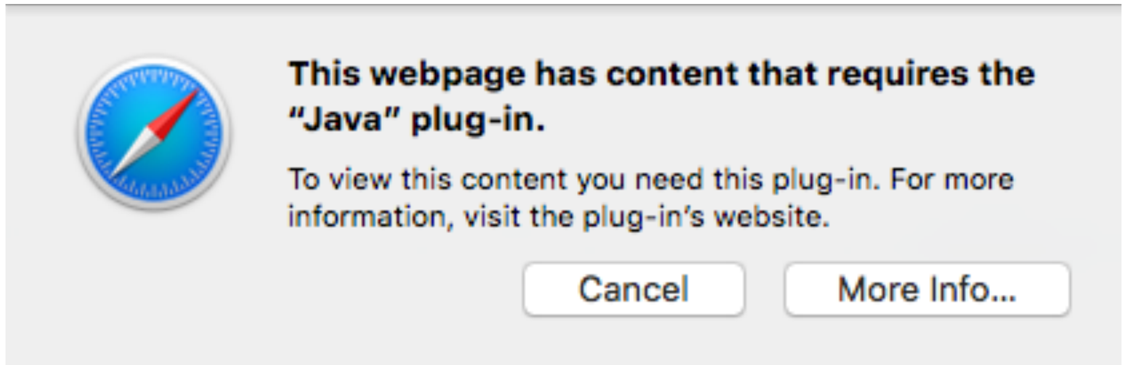
Step 1: Click "Start Generating"
Step 2: Wait while your computer works **(leave this page open)**
Step 3: Earn bitcoin

It's that easy. Want the explanation? Read how bitcoin works, but **click "Start Generating" first** so you'll earn bitcoin while you read.

New: The bitcoin miner for websites is available.

You are not logged in. You can **start generating** now and **your coins will be transfered to your account** when you sign up. If you close your browser your coins may be lost.
Already have an account? Log in.

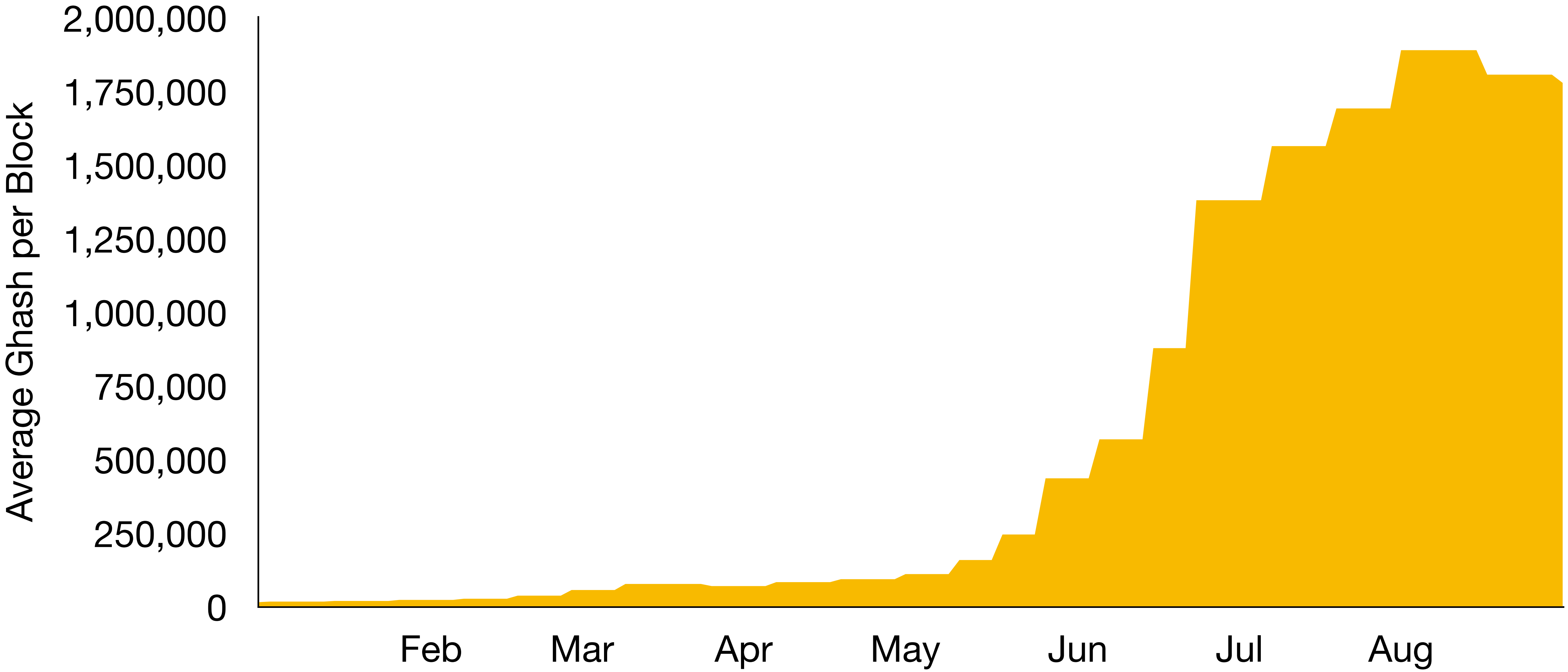
In May 2011, Canadian developer Donny Nadolny releases BitcoinPlus.com, the world's first in-browser cryptocurrency miner. The miner is Java-based, and his website even includes a handy Wordpress plugin for easier embedding.



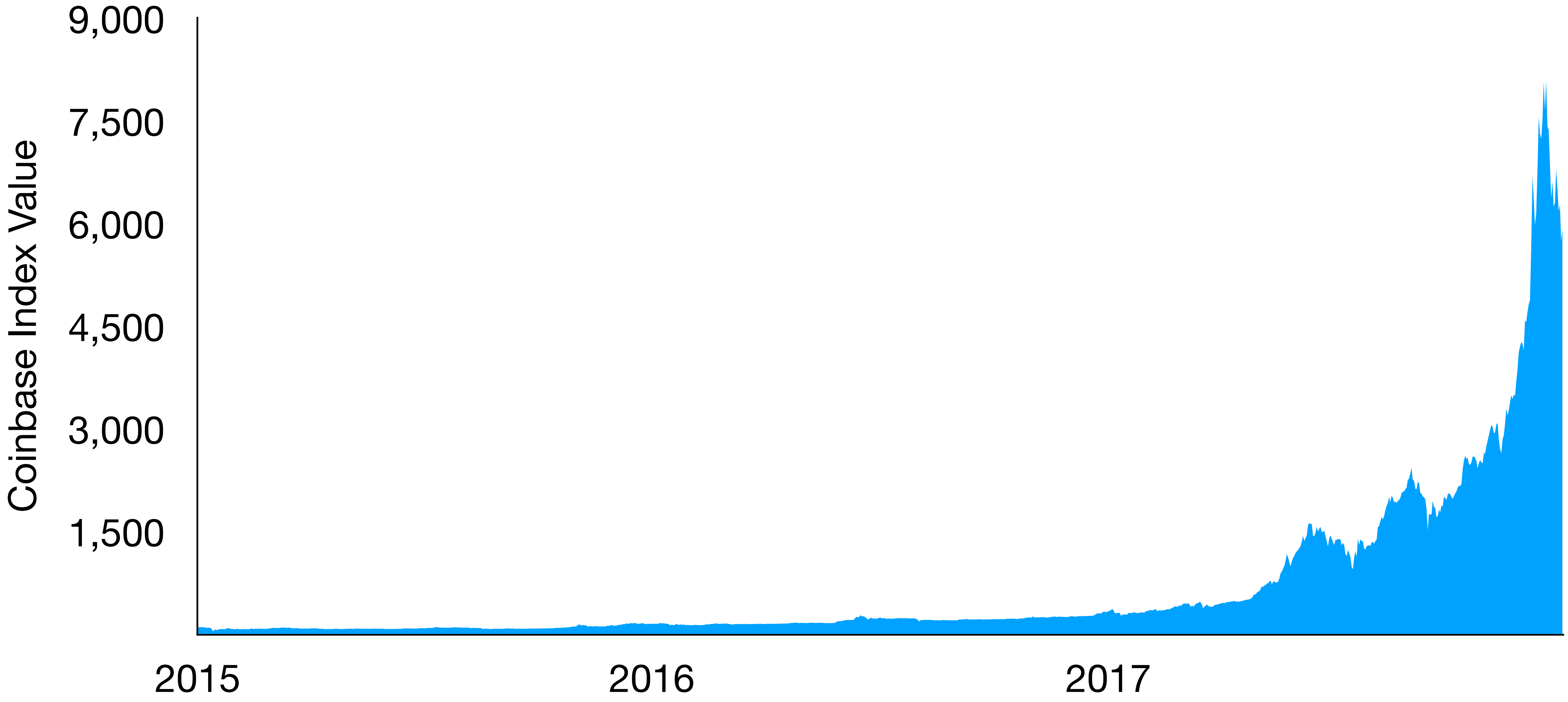
This webpage has content that requires the "Java" plug-in.

To view this content you need this plug-in. For more information, visit the plug-in's website.

However, since BitcoinPlus.com requires the Java plugin to be enabled, it's not viable for cryptojacking without some kind of social engineering to trick users into enabling it. A few forum discussions from this time mention embedding it on sites already using Java applets as a cover, but there's no clear evidence that anyone actually did.



Over the summer of 2011, the difficulty of Bitcoin mining skyrockets to nearly 2 million Gigahashes per block on average making in-browser Bitcoin mining infeasible. BitcoinPlus.com goes offline, and the potential of cryptojacking evaporates.



About 6 years later, “crypto fever” sweeps the market. Developers create hundreds of new, easier to mine cryptocurrencies, such as Monero, and prices of existing currencies surge. The rewards for in-browser mining rise and quickly outweigh the cost of hashing algorithms.

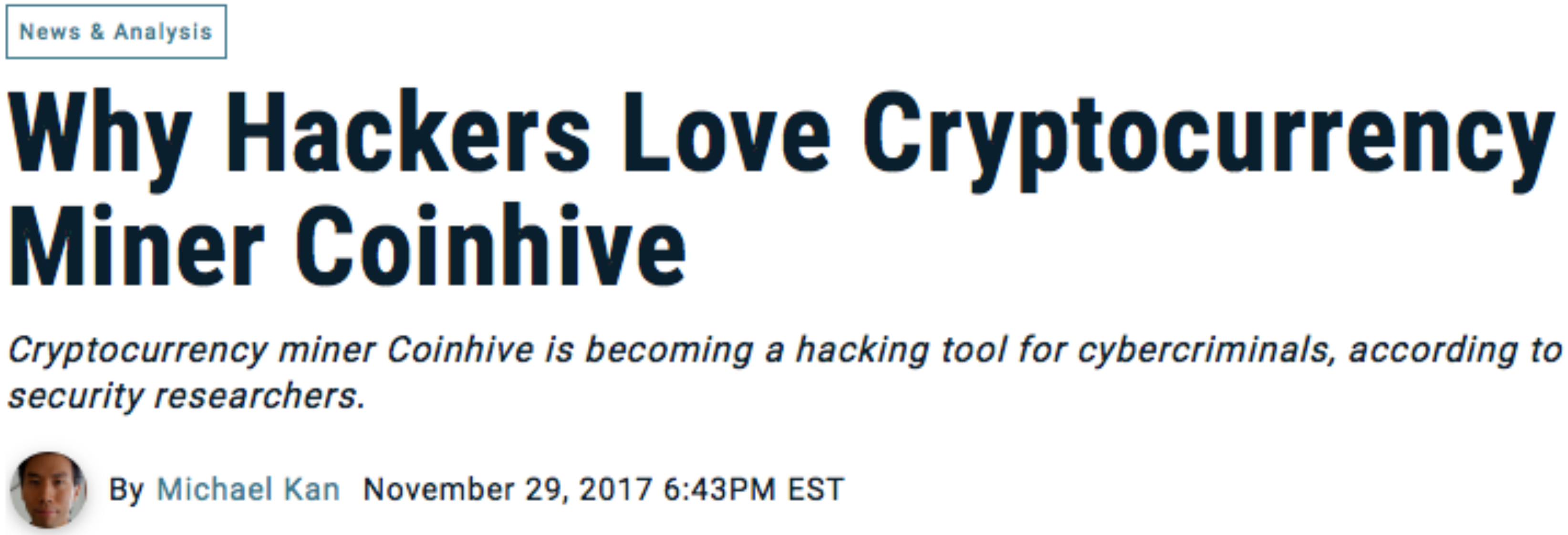
In September 2017, Coinhive.com launches, offering a service that uses a Monero crypto miner written in C, compiled into WebAssembly and embedded in the browser as an alternative to advertisements.

It’s this easy to use…

```
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
    var miner = new CoinHive.Anonymous('YOUR_SITE_KEY');
</script>
```

Unfortunately, Coinhive’s service at the time only *encourages* customers to ask for users’ permission before mining on their devices. **It does not require it.**

Shortly after launching, malware programmers flock to Coinhive’s service and malicious mining scripts begin showing up across the web.



News & Analysis

Why Hackers Love Cryptocurrency Miner Coinhive

Cryptocurrency miner Coinhive is becoming a hacking tool for cybercriminals, according to security researchers.

By Michael Kan November 29, 2017 6:43PM EST

PC MAGAZINE

By Helen Partz

MAY 08, 2018

Coinhive Code Found On 300+ Websites Worldwide In Recent Cryptojacking Campaign

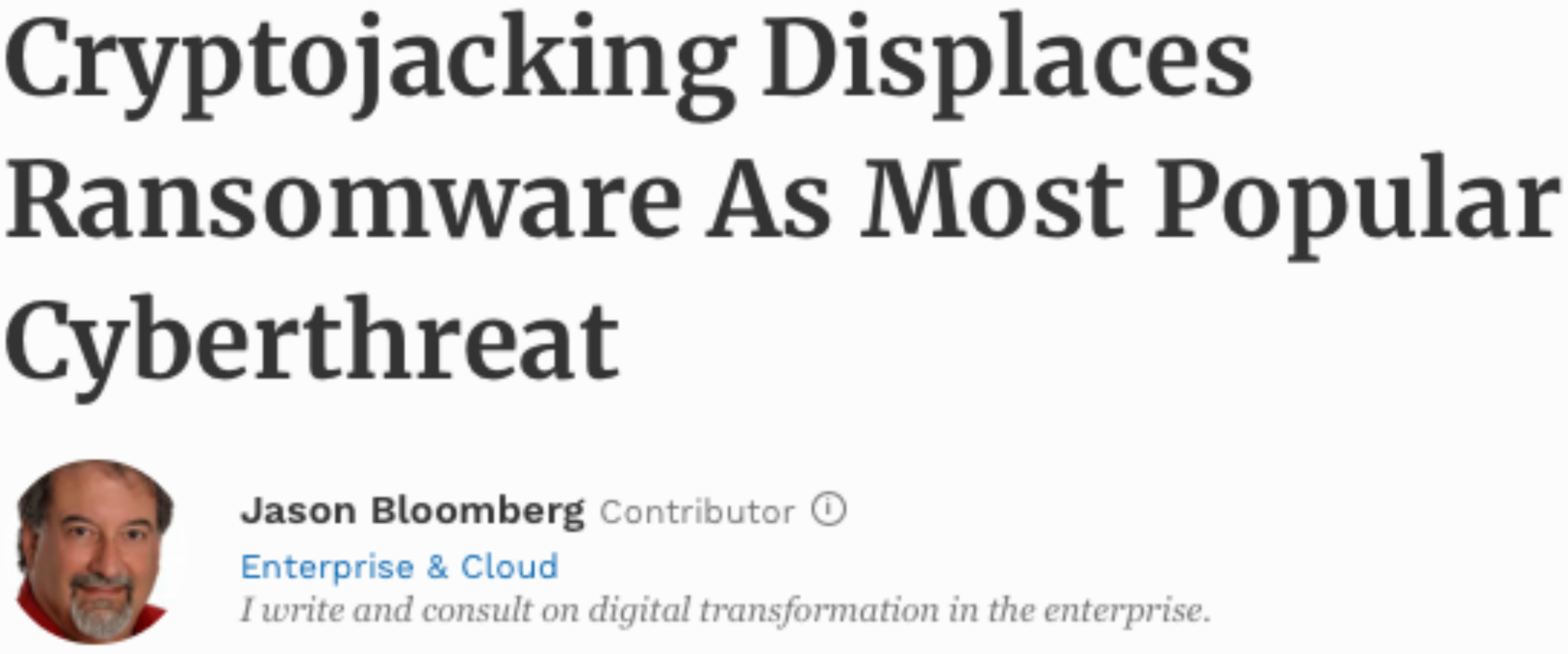
COINTELEGRAPH
The future of money

MINING

COINHIVE IN-BROWSER SOFTWARE IS ‘MINING’ $250K PER MONTH, RESEARCH FINDS

IAN TOZER | AUG 16, 2018 | 04:00

BITCOINIST.COM
CRYPTOCURRENCY REVIEWS AND TECHNOLOGY



Cryptojacking Displaces Ransomware As Most Popular Cyberthreat

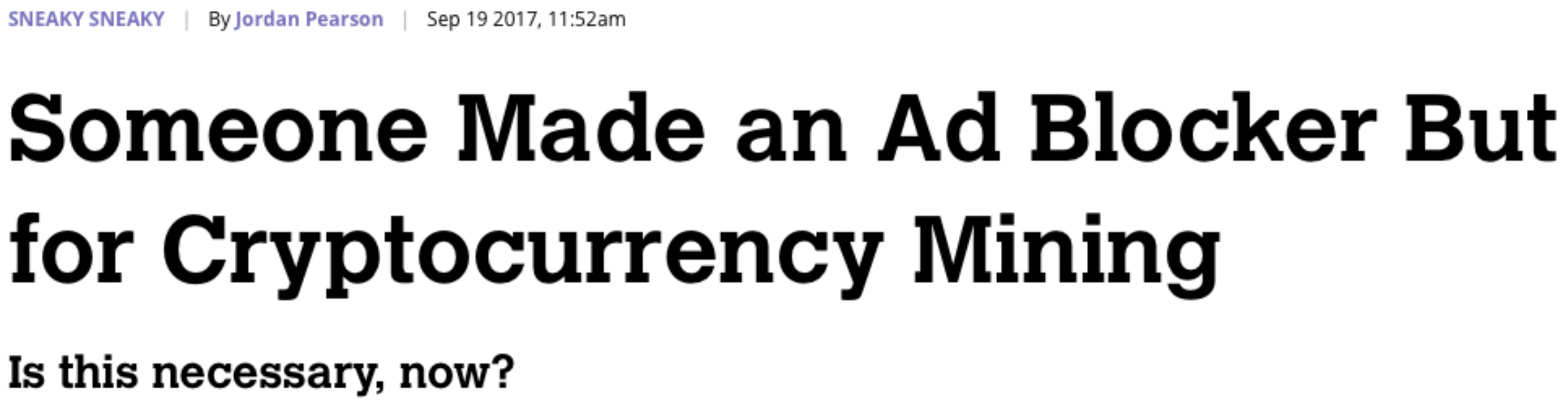
Jason Bloomberg Contributor ⓘ

Enterprise & Cloud

I write and consult on digital transformation in the enterprise.

Forbes

Ad blocking and anti-virus services respond by blocking Coinhive’s domain and, in some cases, all forms of browser based crypto mining, both legal and illegal.

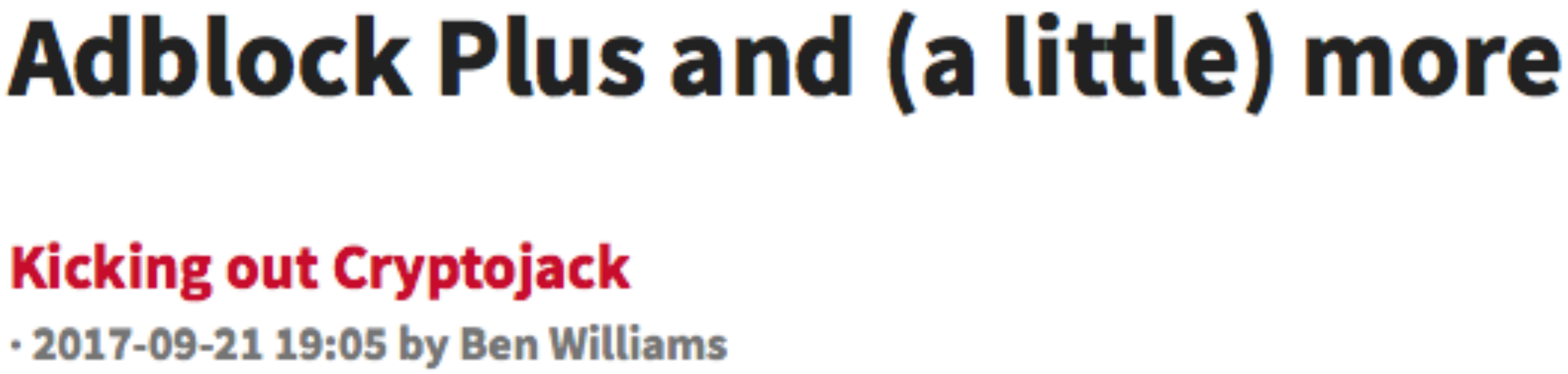


SNEAKY SNEAKY | By Jordan Pearson | Sep 19 2017, 11:52am

Someone Made an Ad Blocker But for Cryptocurrency Mining

Is this necessary, now?

MOTHERBOARD



Adblock Plus and (a little) more

Kicking out Cryptojack

· 2017-09-21 19:05 by Ben Williams

ABP

SECURITY WORLD | TECHNOLOGY

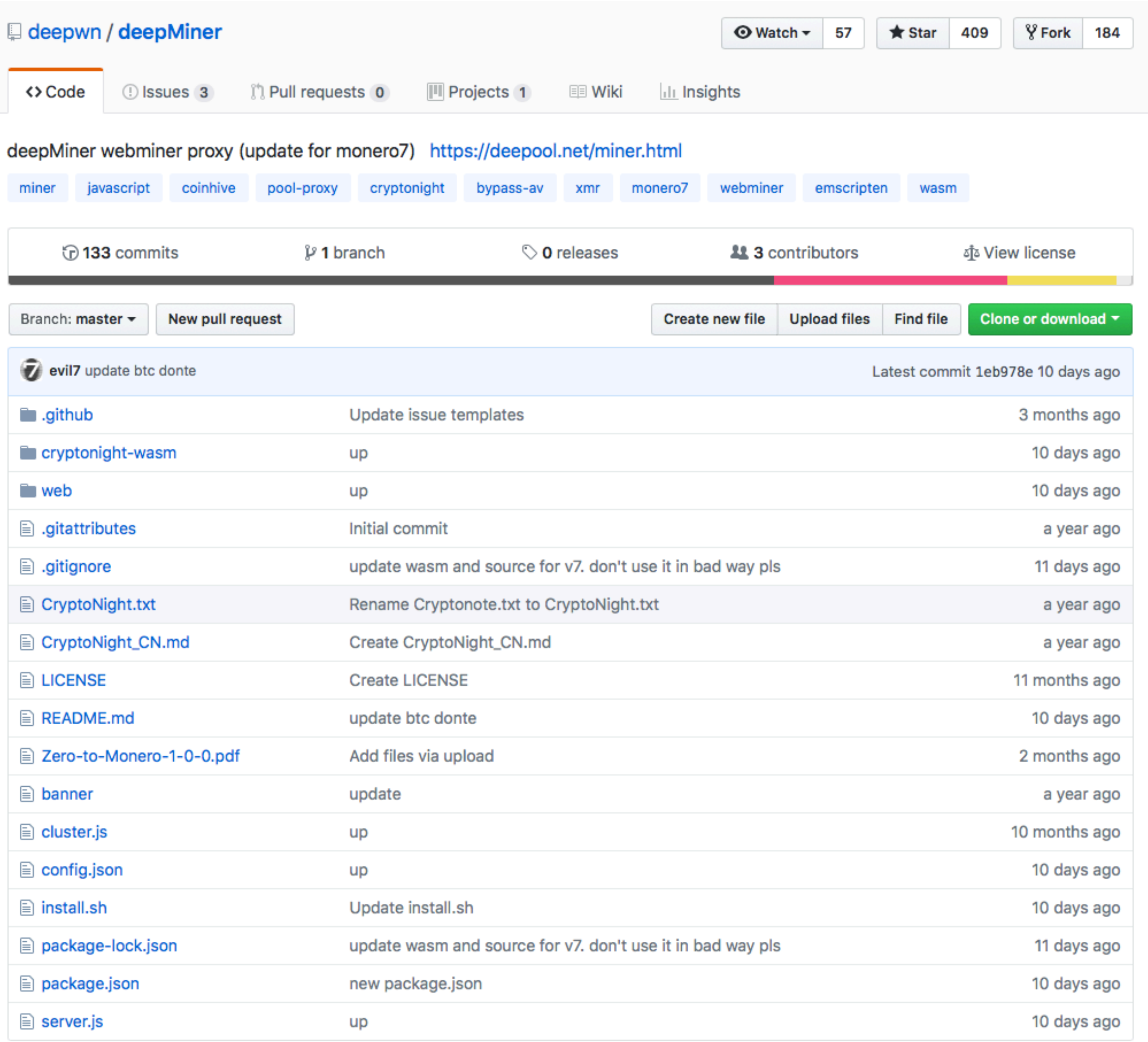
Why is Malwarebytes blocking Coinhive?

Posted: October 18, 2017 by Adam Kujawa
Last updated: July 19, 2018

Malwarebytes

Coinhive responds by releasing a new version of their tool called “AuthedMine” which requires that all customers display an opt in message before mining in hopes that ad blockers will allow this new tool and the tide of malicious users can be stemmed.

But it’s too late. With the efficacy of cryptojacking now proven as a viable profit source, new cryptojacking tools crop up across the web using entirely different languages, frameworks and cryptocurrencies.



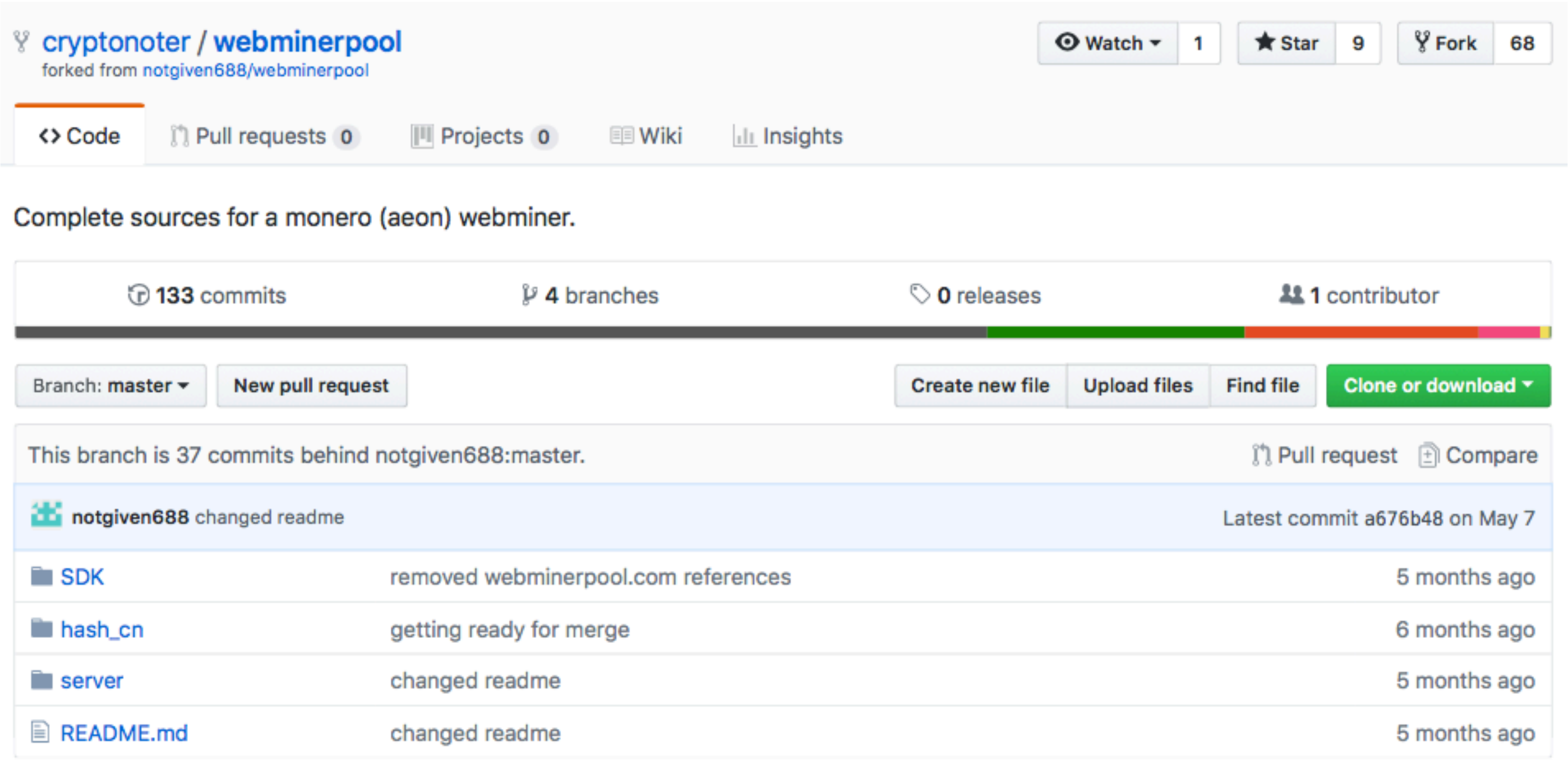
deepMiner webminer proxy (update for monero7) https://deepool.net/miner.html

miner javascript coinhive pool-proxy cryptonight bypass-av xmr monero7 webminer emscripten wasm

133 commits 1 branch 0 releases 3 contributors View license

evil7 update btc donte — Latest commit 1eb978e 10 days ago

.github	Update issue templates	3 months ago
cryptonight-wasm	up	10 days ago
web	up	10 days ago
.gitattributes	Initial commit	a year ago
.gitignore	update wasm and source for v7. don't use it in bad way pls	11 days ago
CryptoNight.txt	Rename Cryptonote.txt to CryptoNight.txt	a year ago
CryptoNight_CN.md	Create CryptoNight_CN.md	a year ago
LICENSE	Create LICENSE	11 months ago
README.md	update btc donte	10 days ago
Zero-to-Monero-1-0-0.pdf	Add files via upload	2 months ago
banner	update	a year ago
cluster.js	up	10 months ago
config.json	up	10 days ago
install.sh	Update install.sh	10 days ago
package-lock.json	update wasm and source for v7. don't use it in bad way pls	11 days ago
package.json	new package.json	10 days ago
server.js	up	10 days ago



cryptonoter / webminerpool
forked from notgiven688/webminerpool

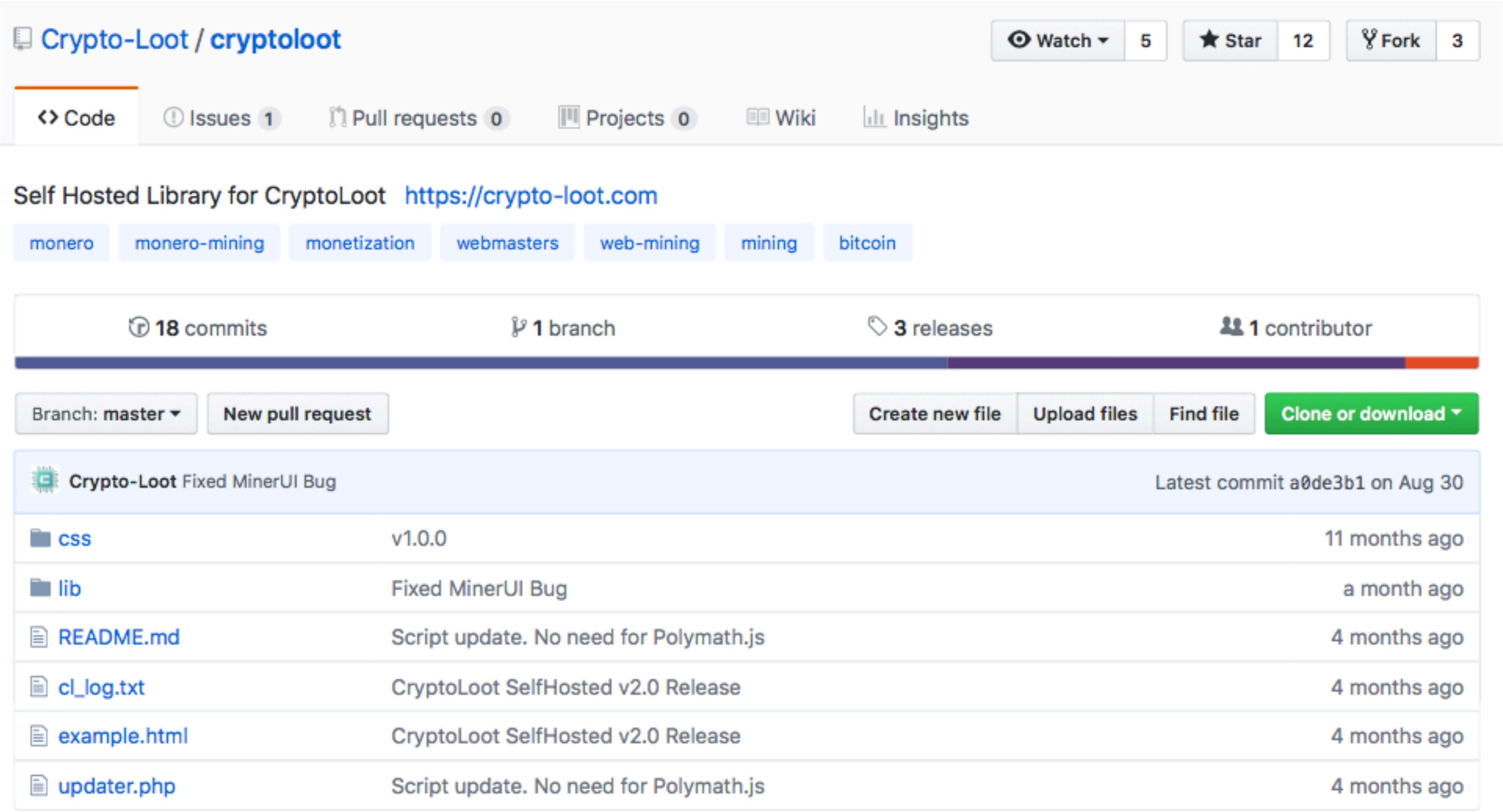
Complete sources for a monero (aeon) webminer.

133 commits · 4 branches · 0 releases · 1 contributor

This branch is 37 commits behind notgiven688:master.

notgiven688 changed readme · Latest commit a676b48 on May 7

SDK	removed webminerpool.com references	5 months ago
hash_cn	getting ready for merge	6 months ago
server	changed readme	5 months ago
README.md	changed readme	5 months ago



Crypto-Loot / cryptoloot

Self Hosted Library for CryptoLoot https://crypto-loot.com

Crypto-Loot Fixed MinerUI Bug — Latest commit a0de3b1 on Aug 30

css	v1.0.0	11 months ago
lib	Fixed MinerUI Bug	a month ago
README.md	Script update. No need for Polymath.js	4 months ago
cl_log.txt	CryptoLoot SelfHosted v2.0 Release	4 months ago
example.html	CryptoLoot SelfHosted v2.0 Release	4 months ago
updater.php	Script update. No need for Polymath.js	4 months ago

Governments start cracking down more intensely on cryptojackers, increasing the risk associated with it.

Blockchain

16 Arrested in Japan Over Monero Cryptojacking Case

By Alex Rathod 4 months ago Leave a comment

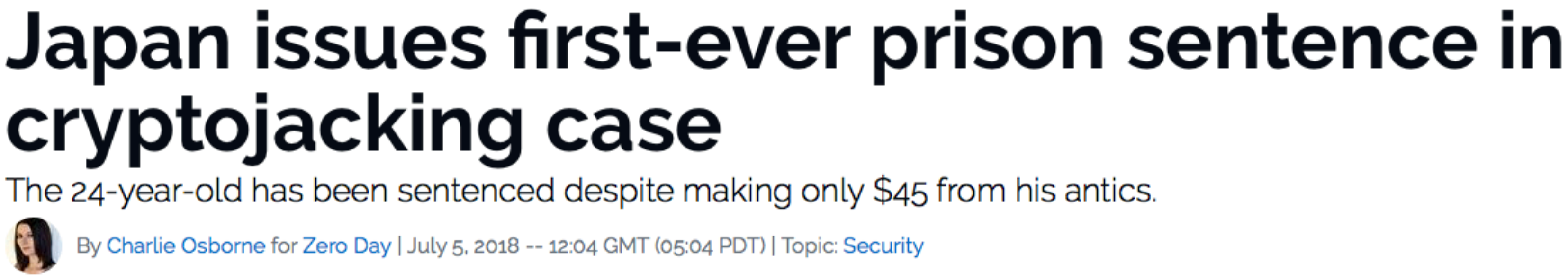
TOSHI TIMES

By Marie Huillet

JUL 09, 2018

China: 20 Arrested in Cryptojacking Case Allegedly Affecting Over 1 Million Computers

COINTELEGRAPH
The future of money



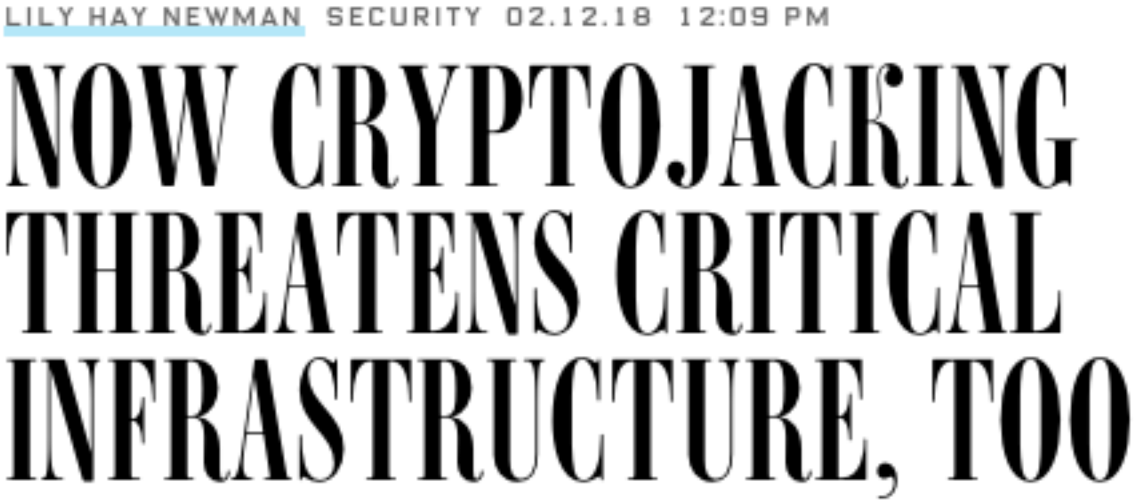
Japan issues first-ever prison sentence in cryptojacking case

The 24-year-old has been sentenced despite making only $45 from his antics.

By Charlie Osborne for Zero Day | July 5, 2018 -- 12:04 GMT (05:04 PDT) | Topic: Security

ZDNet

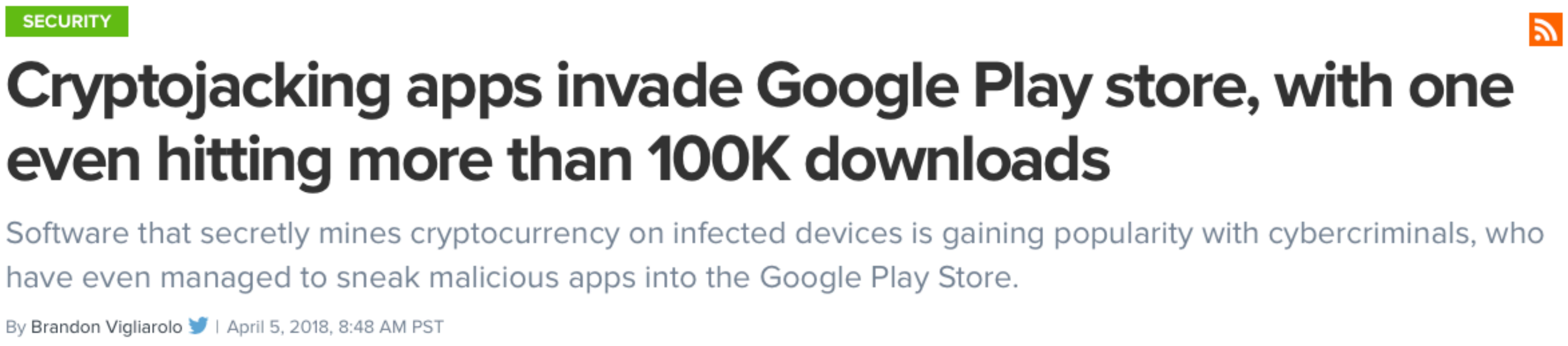
Hackers respond by abandoning the browser and turning to more powerful, more damaging attack vectors.



LILY HAY NEWMAN SECURITY 02.12.18 12:09 PM

NOW CRYPTOJACKING THREATENS CRITICAL INFRASTRUCTURE, TOO

WIRED



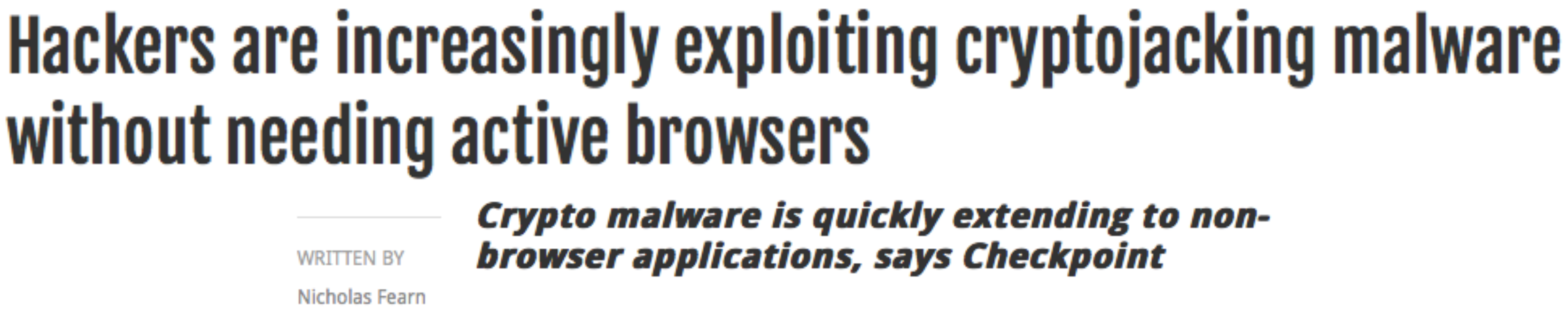
SECURITY

Cryptojacking apps invade Google Play store, with one even hitting more than 100K downloads

Software that secretly mines cryptocurrency on infected devices is gaining popularity with cybercriminals, who have even managed to sneak malicious apps into the Google Play Store.

By Brandon Vigliarolo | April 5, 2018, 8:48 AM PST

TechRepublic



Hackers are increasingly exploiting cryptojacking malware without needing active browsers

WRITTEN BY

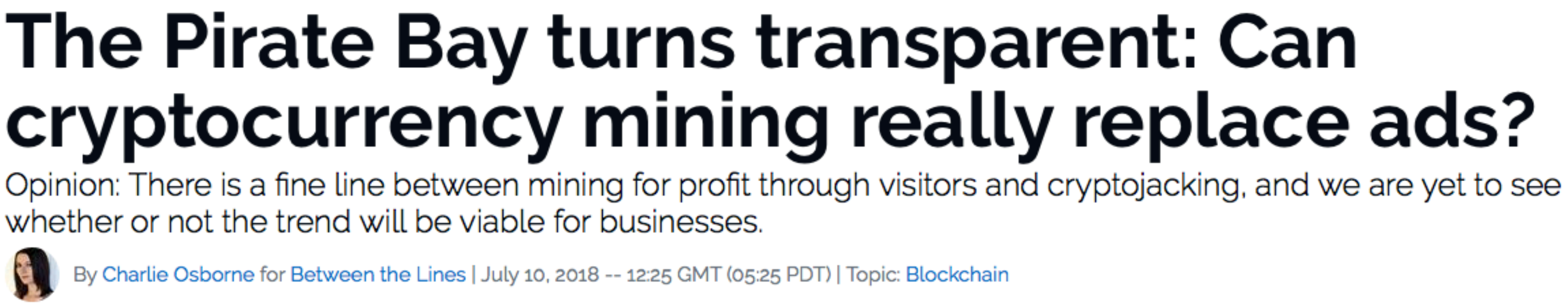
Nicholas Fearn

Crypto malware is quickly extending to non-browser applications, says Checkpoint

ITPRO

IT ANALYSIS. BUSINESS INSIGHT.

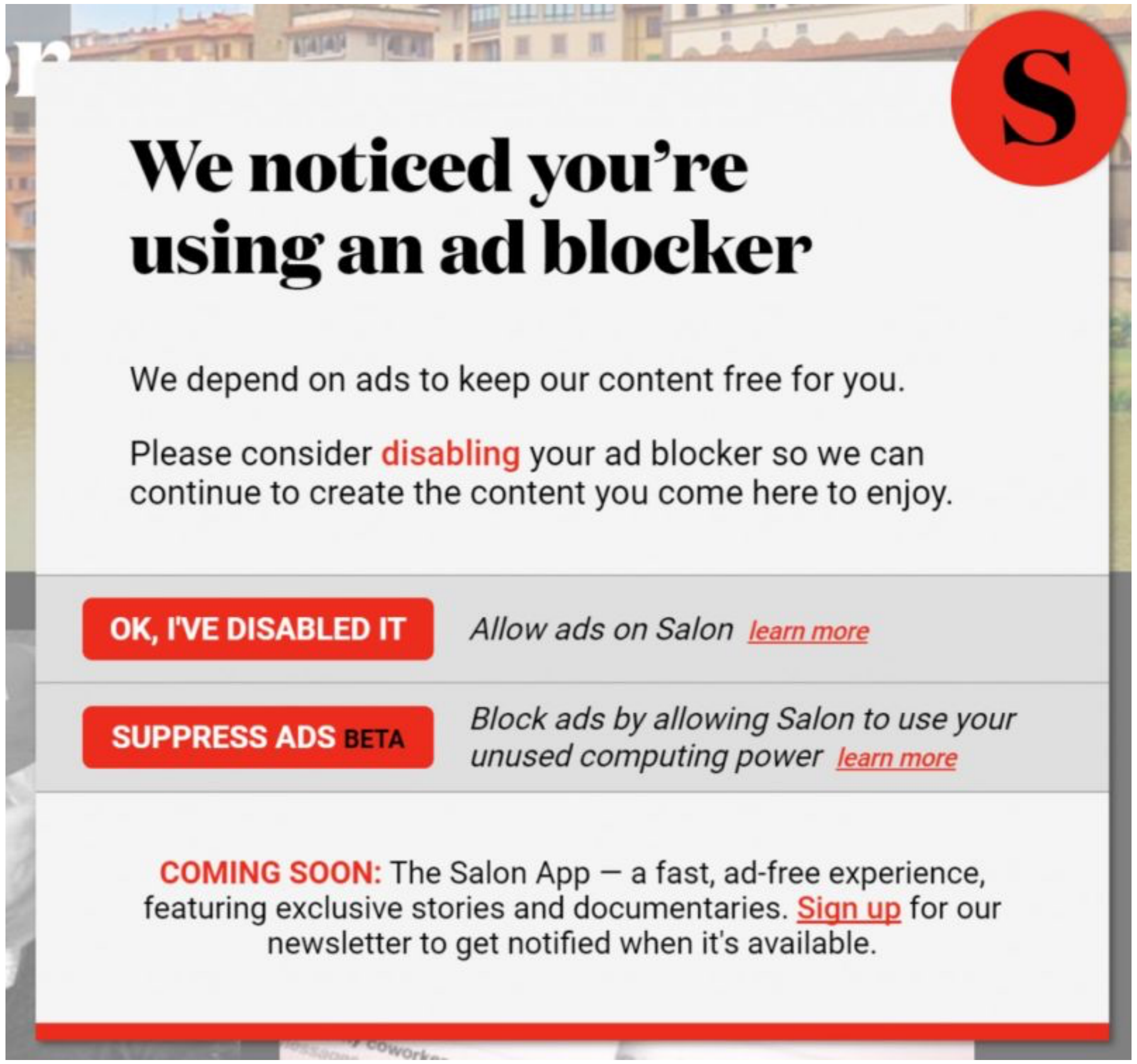
Meanwhile, legal browser based crypto mining starts to slowly reemerge as an alternative to advertisements on high traffic websites.



The Pirate Bay turns transparent: Can cryptocurrency mining really replace ads?

Opinion: There is a fine line between mining for profit through visitors and cryptojacking, and we are yet to see whether or not the trend will be viable for businesses.

By Charlie Osborne for Between the Lines | July 10, 2018 -- 12:25 GMT (05:25 PDT) | Topic: Blockchain



We noticed you’re using an ad blocker

We depend on ads to keep our content free for you.

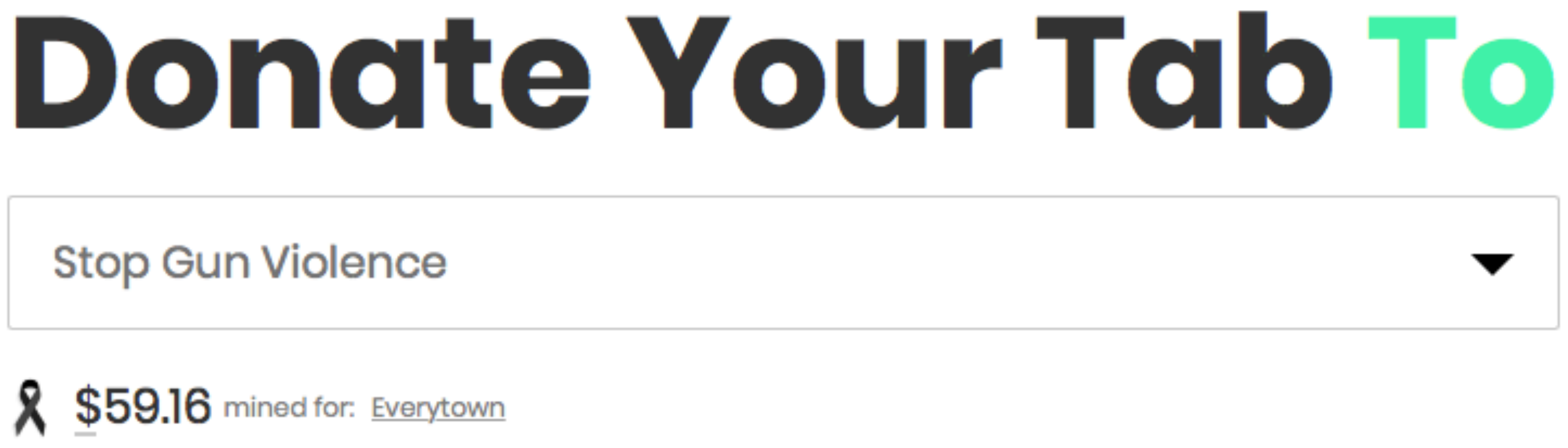
Please consider disabling your ad blocker so we can continue to create the content you come here to enjoy.

Allow ads on Salon learn more

Block ads by allowing Salon to use your unused computing power learn more

COMING SOON: The Salon App — a fast, ad-free experience, featuring exclusive stories and documentaries. Sign up for our newsletter to get notified when it's available.

Legal browser based crypto mining also gains popularity as a means of supporting charities.

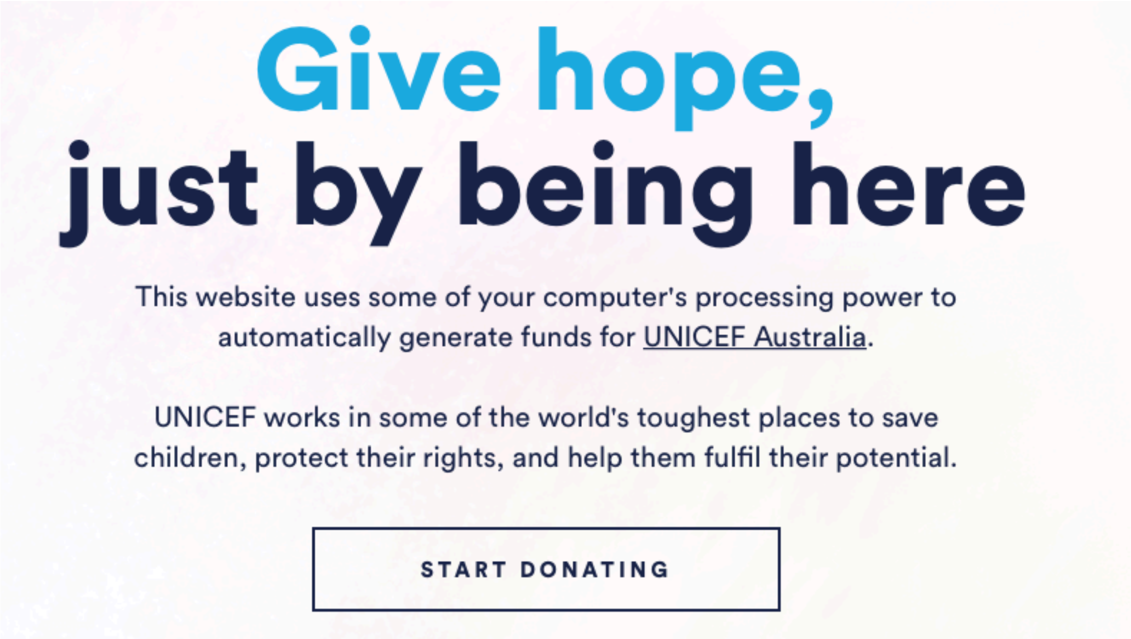


Donate Your Tab To

Stop Gun Violence ▼

$59.16 mined for: Everytown

DonateYourTab.to

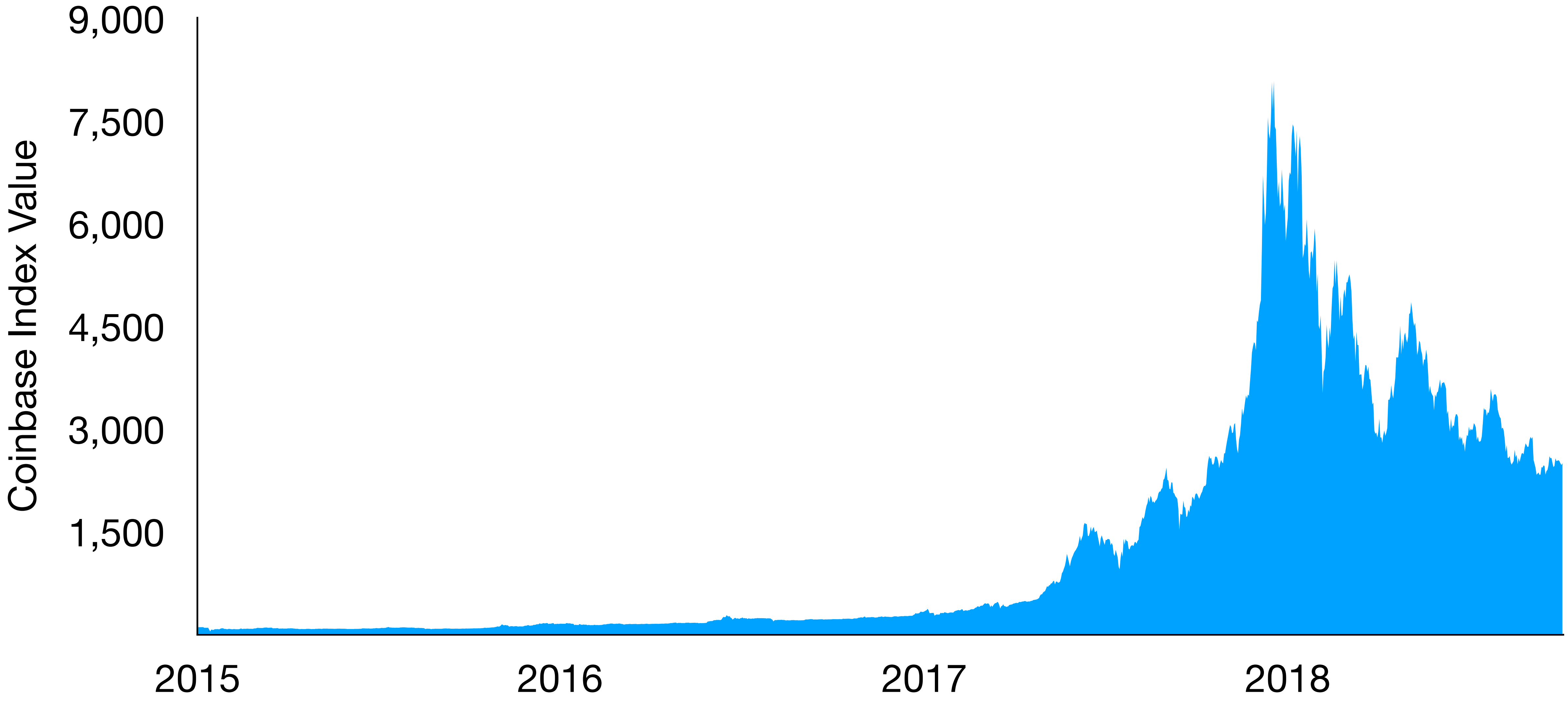


Give hope, just by being here

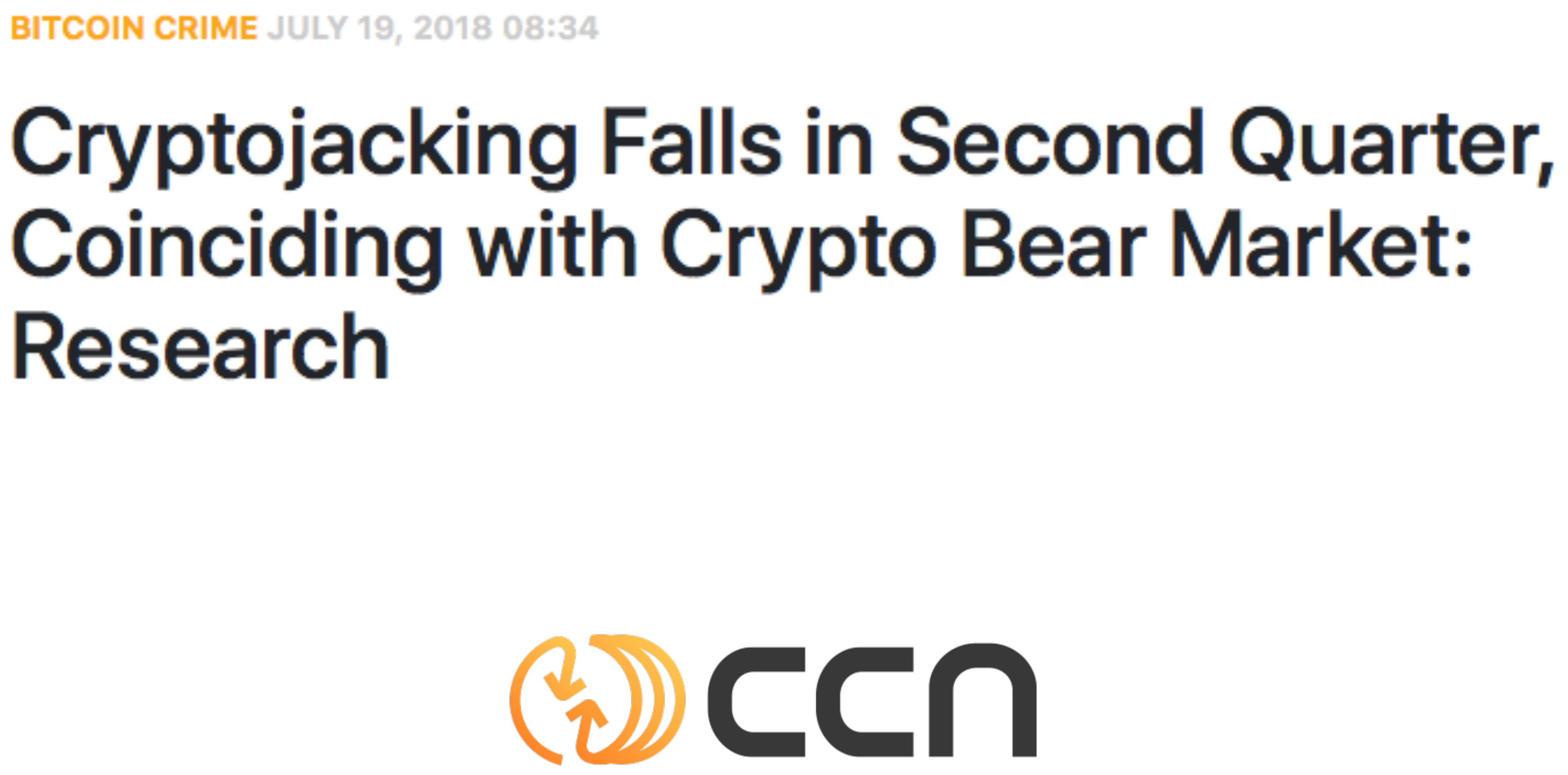
This website uses some of your computer's processing power to automatically generate funds for UNICEF Australia.

UNICEF works in some of the world's toughest places to save children, protect their rights, and help them fulfil their potential.

unicef australia

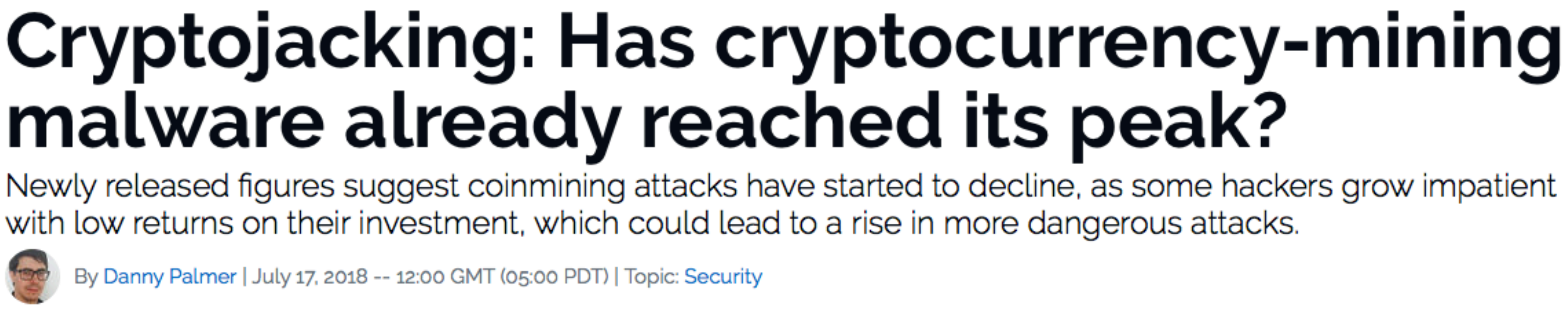


At the same time, after months of booming crypto markets, the cryptocurrency world enters a “crypto winter.” Currency prices drop, new currencies are slow to market, and the rewards of cryptojacking quickly dry up.



BITCOIN CRIME JULY 19, 2018 08:34

Cryptojacking Falls in Second Quarter, Coinciding with Crypto Bear Market: Research



Cryptojacking: Has cryptocurrency-mining malware already reached its peak?

Newly released figures suggest coinmining attacks have started to decline, as some hackers grow impatient with low returns on their investment, which could lead to a rise in more dangerous attacks.

By Danny Palmer | July 17, 2018 -- 12:00 GMT (05:00 PDT) | Topic: Security

ZDNet

BITCOIN CRIME AUGUST 31, 2018 22:01

Not a Ticket to Riches: Average Cryptojacking Website Makes Only $5.80 per Day

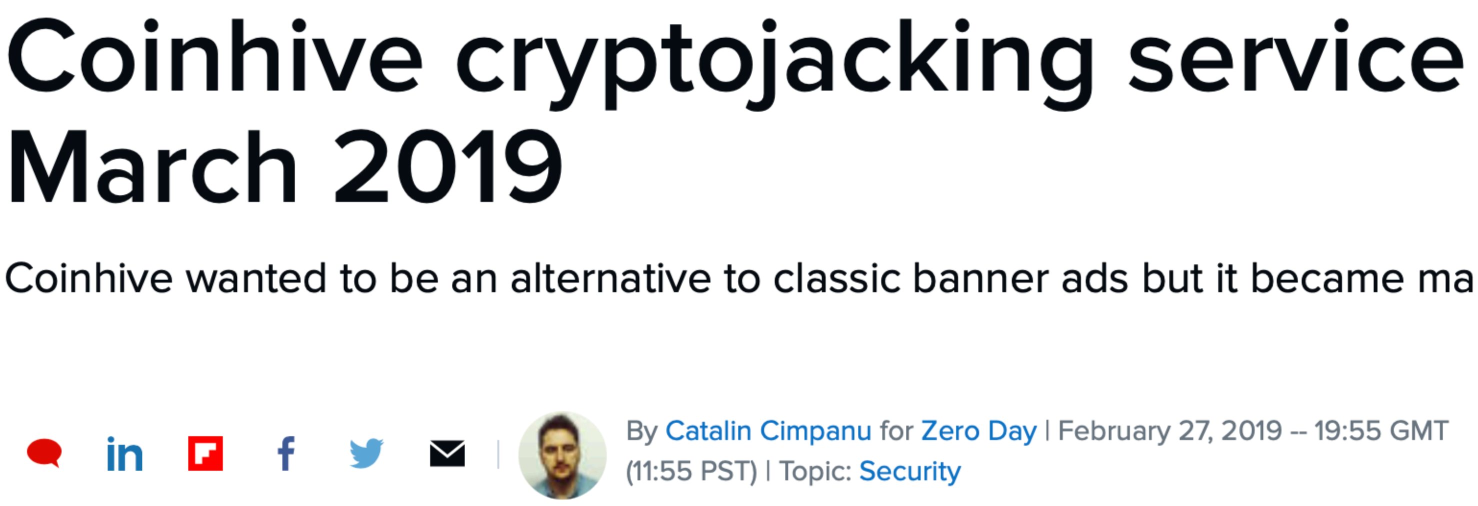
ccn

The End?

Feature

PRESENTATION

For the next few months, it looks like cryptojacking is finally coming to an end…



Coinhive cryptojacking service to shut down in March 2019

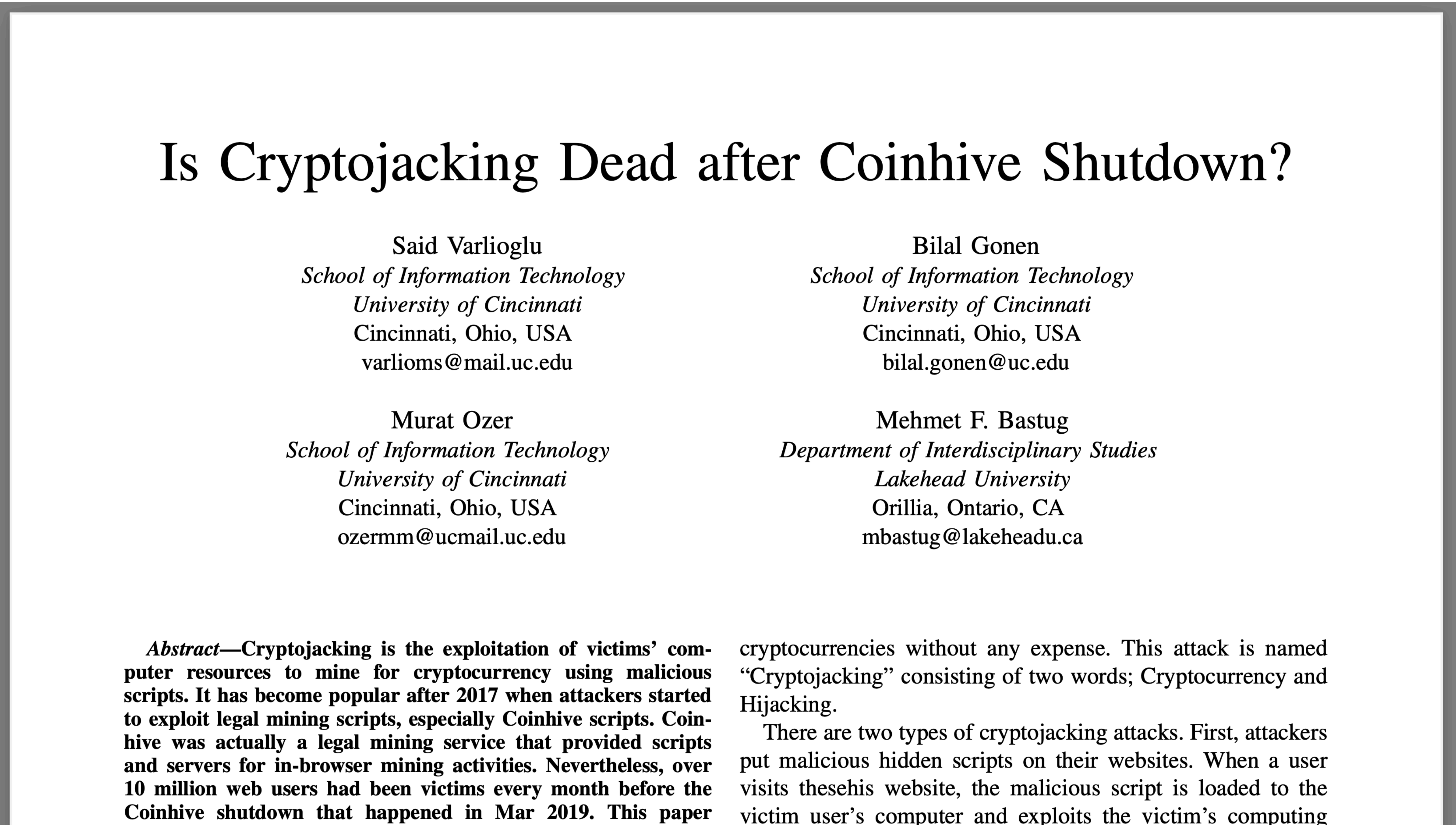
Coinhive wanted to be an alternative to classic banner ads but it became malware after constant abuse.

By Catalin Cimpanu for Zero Day | February 27, 2019 -- 19:55 GMT (11:55 PST) | Topic: Security

ZDNet

Salon.com and The Pirate Bay both quietly abandon their crypto mining experiments.

Unicef Australia also pulls their crypto mining donation website, however DonateYourTab.to is still up and running today.



Is Cryptojacking Dead after Coinhive Shutdown?

Said Varlioglu
School of Information Technology
University of Cincinnati
Cincinnati, Ohio, USA
varlioms@mail.uc.edu

Bilal Gonen
School of Information Technology
University of Cincinnati
Cincinnati, Ohio, USA
bilal.gonen@uc.edu

Murat Ozer
School of Information Technology
University of Cincinnati
Cincinnati, Ohio, USA
ozermm@ucmail.uc.edu

Mehmet F. Bastug
Department of Interdisciplinary Studies
Lakehead University
Orillia, Ontario, CA
mbastug@lakeheadu.ca

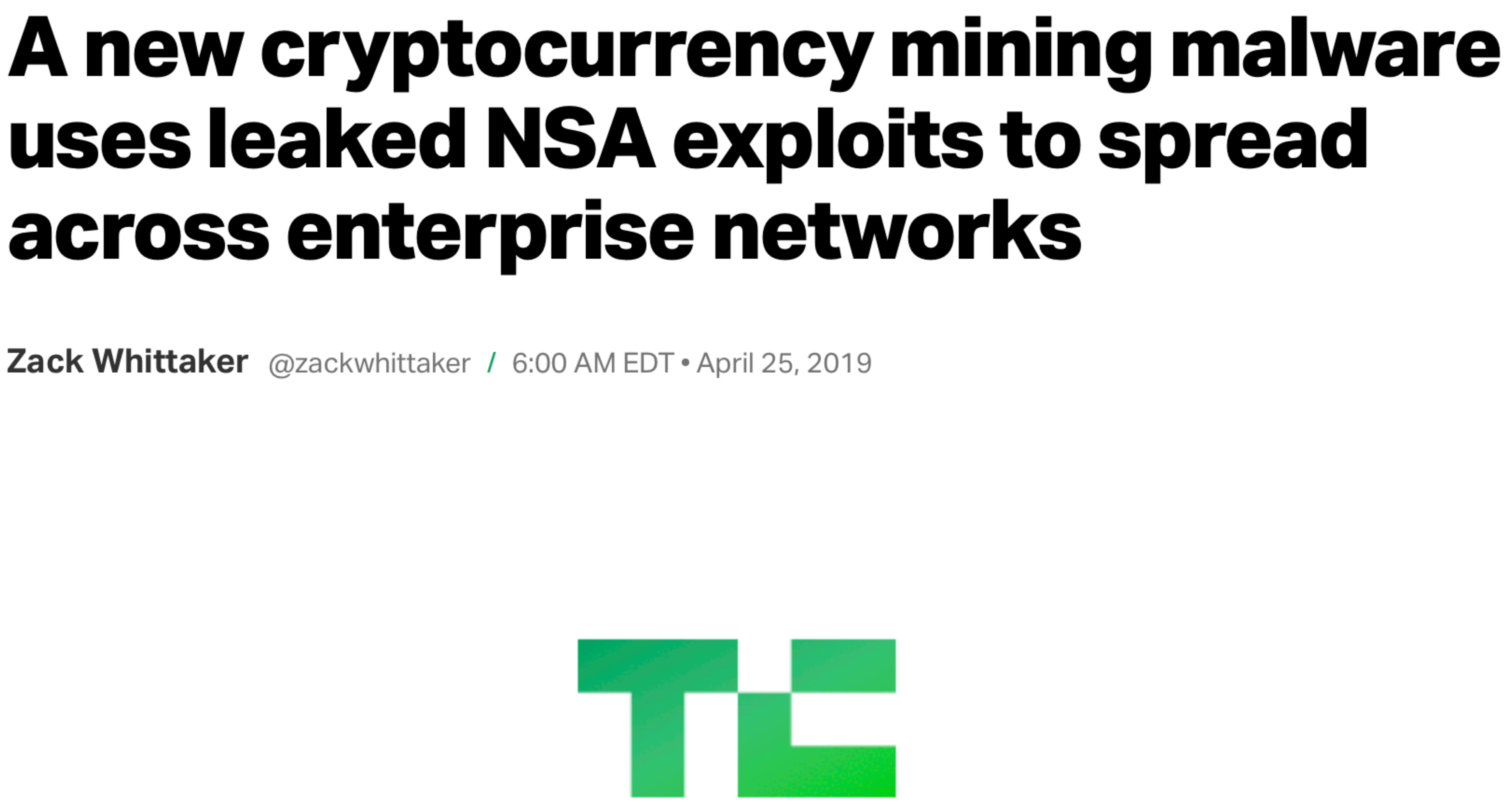
***Abstract*—Cryptojacking is the exploitation of victims' computer resources to mine for cryptocurrency using malicious scripts. It has become popular after 2017 when attackers started to exploit legal mining scripts, especially Coinhive scripts. Coinhive was actually a legal mining service that provided scripts and servers for in-browser mining activities. Nevertheless, over 10 million web users had been victims every month before the Coinhive shutdown that happened in Mar 2019. This paper**

cryptocurrencies without any expense. This attack is named "Cryptojacking" consisting of two words; Cryptocurrency and Hijacking.

There are two types of cryptojacking attacks. First, attackers put malicious hidden scripts on their websites. When a user visits thesehis website, the malicious script is loaded to the victim user's computer and exploits the victim's computing

But this rollercoaster isn’t over yet…

While browser-based cryptojacking continues to die off, native cryptojacking has begun to explode and rapidly evolve as established cybercriminals incorporate crypto mining tools into their existing toolsets to create new, extremely difficult to detect forms of attack.



A new cryptocurrency mining malware uses leaked NSA exploits to spread across enterprise networks

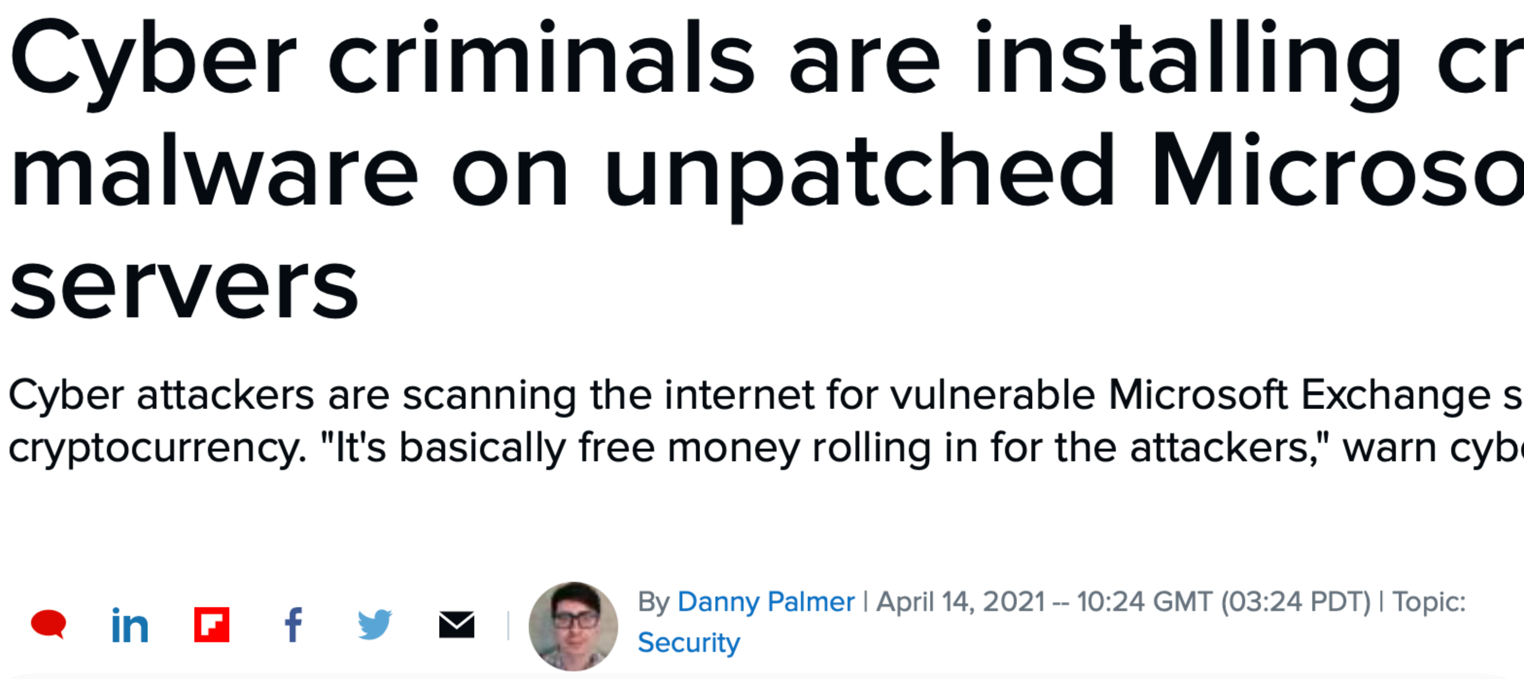
Zack Whittaker @zackwhittaker / 6:00 AM EDT • April 25, 2019

TECH 22 AUGUST 2019

Steve Kaaru

Cryptojacking code in Ruby libraries exposes over 3,500 people

COINGEEK



Cyber criminals are installing cryptojacking malware on unpatched Microsoft Exchange servers

Cyber attackers are scanning the internet for vulnerable Microsoft Exchange servers they can exploit to mine for cryptocurrency. "It's basically free money rolling in for the attackers," warn cybersecurity researchers.

By Danny Palmer | April 14, 2021 -- 10:24 GMT (03:24 PDT) | Topic: Security

ZDNet

Interestingly, cryptojacking malware found in the wild exhibits novel behaviors suited to cryptocurrency mining’s own unique advantages and disadvantages.

Unlike other forms of malware, cryptojacking doesn’t depend on any privileged access to a victim’s machine, so it can operate in many conditions where typical malware would be useless, such as containerized environments.

Cryptojacking worm infects exposed Docker deployments

Graboid is the first known instance of a cryptomining worm used to create botnets spread using containers.

By Lucian Constantin

CSO Senior Writer, CSO | OCT 16, 2019 6:00 AM PDT

New Malware Hijacks Kubernetes Clusters to Mine Monero

Author:
Lindsey O'Donnell

February 3, 2021
/ 3:50 pm

threatpost

Docker Images Containing Cryptojacking Malware Distributed via Docker Hub

June 25, 2020 Ravie Lakshmanan

The Hacker News

Also, whereas most forms of malware are fundamentally indifferent to each other, cryptojacking payloads must fight for limited system resources, and consequentially, it is advantageous for them to disable or destroy competing malware running on the same hardware.

6 OCT 2020 NEWS

New Cryptojacking Malware Variant Targeting Cloud Systems Discovered

James Coker Reporter, Infosecurity Magazine

Follow @ReporterCoker

info security

STRATEGY | INSIGHT | TECHNOLOGY

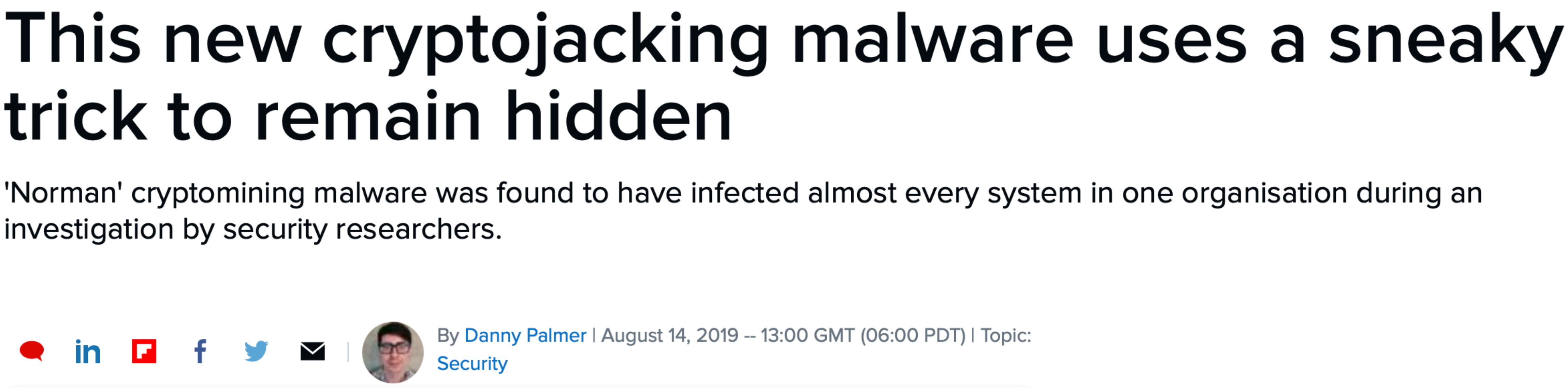
“The malware, named Black-T, gives evidence of a shift in tactics […] by TeamTNT, a group known for targeting AWS credential files on compromised cloud systems and mining for Monero.

…

“**These include the targeting and stopping of cryptojacking worms such as the Crux worm, ntpd miner and a redis-bakup miner, that were previously unknown.**”

— James Coker, InfoSecurity.com

Cryptojacking also comes with the unique disadvantage of high CPU usage and easier detection as a result, but novel solutions to these challenges have already started to emerging for this and other faults across the web.



This new cryptojacking malware uses a sneaky trick to remain hidden

'Norman' cryptomining malware was found to have infected almost every system in one organisation during an investigation by security researchers.

By Danny Palmer | August 14, 2019 -- 13:00 GMT (06:00 PDT) | Topic: Security

ZDNet

“Of those variants, it was Norman which sparked the most interest, […] a high-performance miner for Monero cryptocurrency […] able to employ a number of evasion techniques to avoid discovery.

“**One way it does this is by terminating the mining process when the Windows Task Manager is opened.** […] After the user closes the Task Manager, Norman resumes its work.”

— Danny Palmer, ZDNet

Gamers Particularly Targeted in Cryptojacking - Avast Malware Researcher Daniel Benes Explains Why

A recent research published by Avast pointed out that hackers have been particularly targeting gamers with 'Crackonosh', a crypojacking malware.

By Jasmin Jose | Updated: 2 July 2021 16:54 IST

Gadgets 360
An NDTV venture

Applications with high expected CPU usage, such as video games, offer cover for cryptojacking, and multiple examples of cryptojacking malware embedded in Steam games have been found.

Cryptojacking Rises 450 Percent as Cybercriminals Pivot From Ransomware to Stealthier Attacks

February 26, 2019 | By **John Zorabedian** | 5 min read

Security Intelligence

“Yet an even stealthier form of attack doesn’t use malware at all. More than half of cyberattacks (57 percent) seen by X-Force IRIS in 2018 did not leverage malware, and many involved the **use of nonmalicious tools, including PowerShell, PsExec and other legitimate administrative solutions**, allowing attackers to ‘live off the land’ and potentially remain in IT environments longer.

“Attacks that don’t use malware are much more challenging for defense teams to detect, Whitmore said, because they are leveraging tools built into the environment and **can’t be identified through signatures or typical malware detection techniques**. Instead, defense teams need to detect malicious commands, communications and other actions that might look like legitimate business processes.”

— John Zorabedian, Security Intelligence

Meanwhile, catching and prosecuting cryptojackers is becoming more complex as it gains popularity abroad and many attacks now cross borders from nations with entirely different legal frameworks for regulating cryptocurrency.

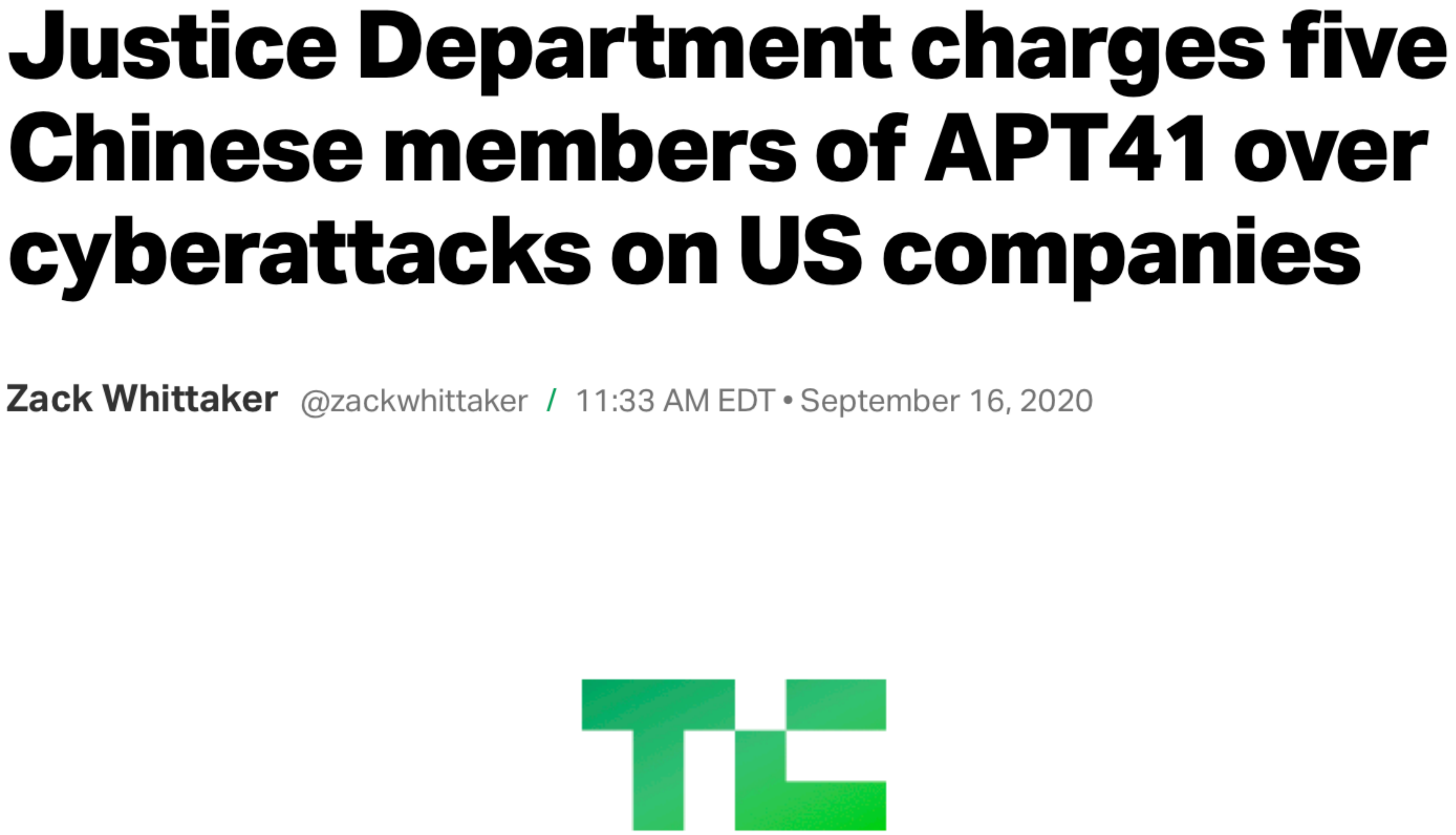
ANDREY SHEVCHENKO

JAN 09, 2020

Interpol Collaborates With Cybersecurity Firm to Tackle Cryptojacking

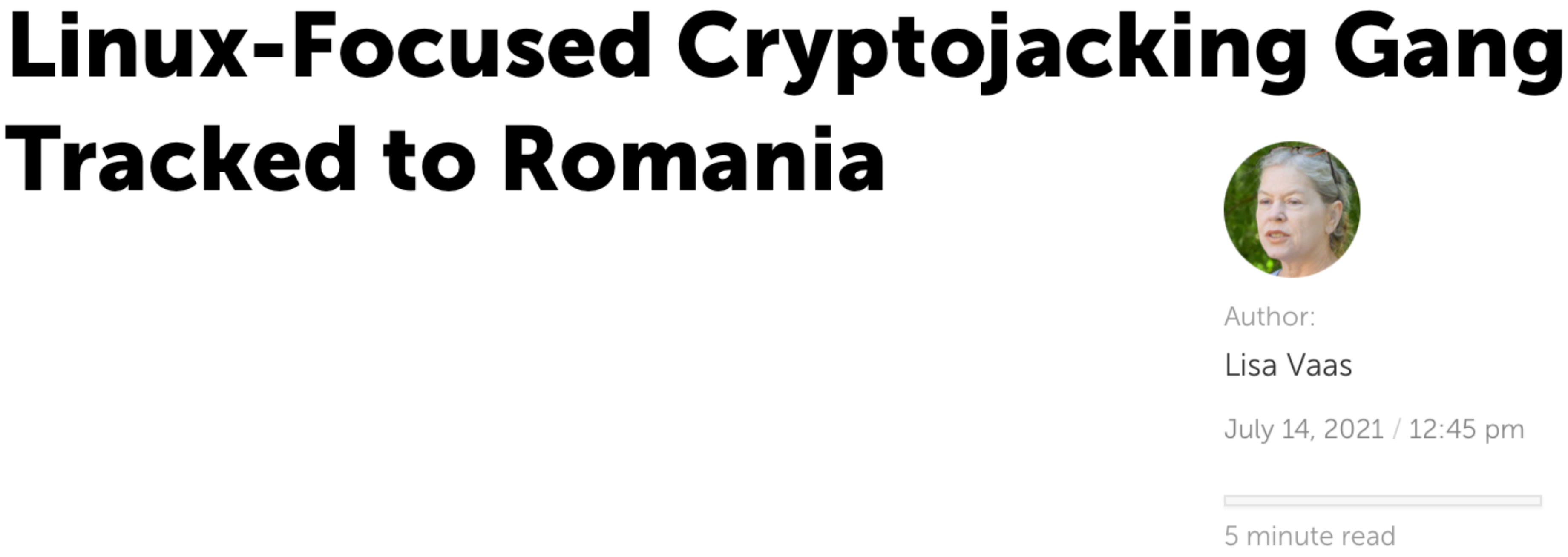
Interpol helped curtail cryptojacking malware that affected thousands of routers.

COINTELEGRAPH
The future of money



Justice Department charges five Chinese members of APT41 over cyberattacks on US companies

Zack Whittaker @zackwhittaker / 11:33 AM EDT • September 16, 2020



Linux-Focused Cryptojacking Gang Tracked to Romania

Author:

Lisa Vaas

July 14, 2021 / 12:45 pm

5 minute read

threatpost

And then there’s Covid…

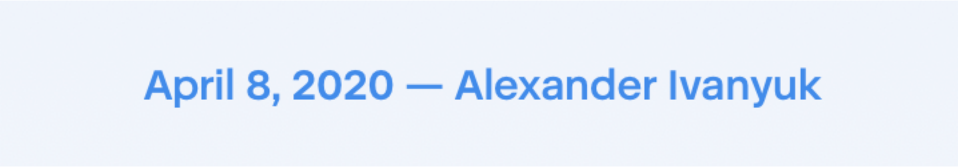
COVID AND THE SURGE IN CRYPTO VALUE: THE PERFECT STORM FOR CRYPTOJACKING

Sukesh Mudrakola APRIL 13, 2021

33

TechGenix

As COVID-19 Spreads, So Do Ransomware and Cryptomining Attacks



April 8, 2020 — Alexander Ivanyuk

Acronis

Top Takeaways from the Unit 42 Cloud Threat Report

Cloud Workload Protection | Threat Research | cloud security | cloud threat | Cloud Threat Report

83 people reacted

By **Mariya Harris**
June 23, 2021 at 3:56 PM
5 min. read

"In just a matter of months during the COVID-19 pandemic, **the percentage of employees working remotely jumped alarmingly from 20% to 71%**. […] Needless to say, Q3 of 2020 saw a massive influx of companies moving to the cloud.

"**Organizations across the world increased their cloud workloads without fully understanding the security implications, leading to an explosion of cloud security breaches.** "

—Mariya Harris, Palo Alto Networks

So what can we do to
help stop cryptojacking?

For Sysadmins

- Enable SSL and firewalls where ever possible, and don’t rely on VPNs alone to secure your Kubernetes, Docker or other container management tools.

- Monitor your CPU usage continuously with either live gauges or recorded stats where appropriate.

- Monitor your network activity. For macOS, consider using tools like Little Snitch.

For Developers

- Keep your dependencies up to date and avoid using poorly maintained packages and containers.

- Don’t expose unmetered CPU cycles to users! Even limited, non-Turing complete services, like scripting features can be abused by malicious actors when limits aren’t placed on execution time.

- For open source contributors, stay vigilant in code reviews and be careful who you share privileges with.

For Users

- Don’t trust applications from illegitimate sources.

- Watch out for unexplained CPU and network activity.

- Stay updated on new threats and recommendations for addressing with them. Malware is always evolving, so security best practices have to evolve as well.

Thanks

Find me @

RosalineKarr.com
github.com/rosalinekarr
twitter.com/rosalinekarr
keybase.io/rosalinekarr