Introduction to Crypto Jacking

Warren Finch

PacNOG 23 - 3rd Dec 2018

Marshall Islands

Agenda

- Web based coin miners
- What is cryptojacking
- Are all cryptominers bad?
- Cryptomining malware
- Mitigation techniques

Timeline

18th Apr 2014
Monero Cryptocurrency released

14th Sep 2017
Coinhive Miner launched

16th Oct 2017
Coinhive launches AuthedMine

11th Feb 2018
UK Information Commissioner's Office Incident

Sep 2018
Webcobra Malware discovered

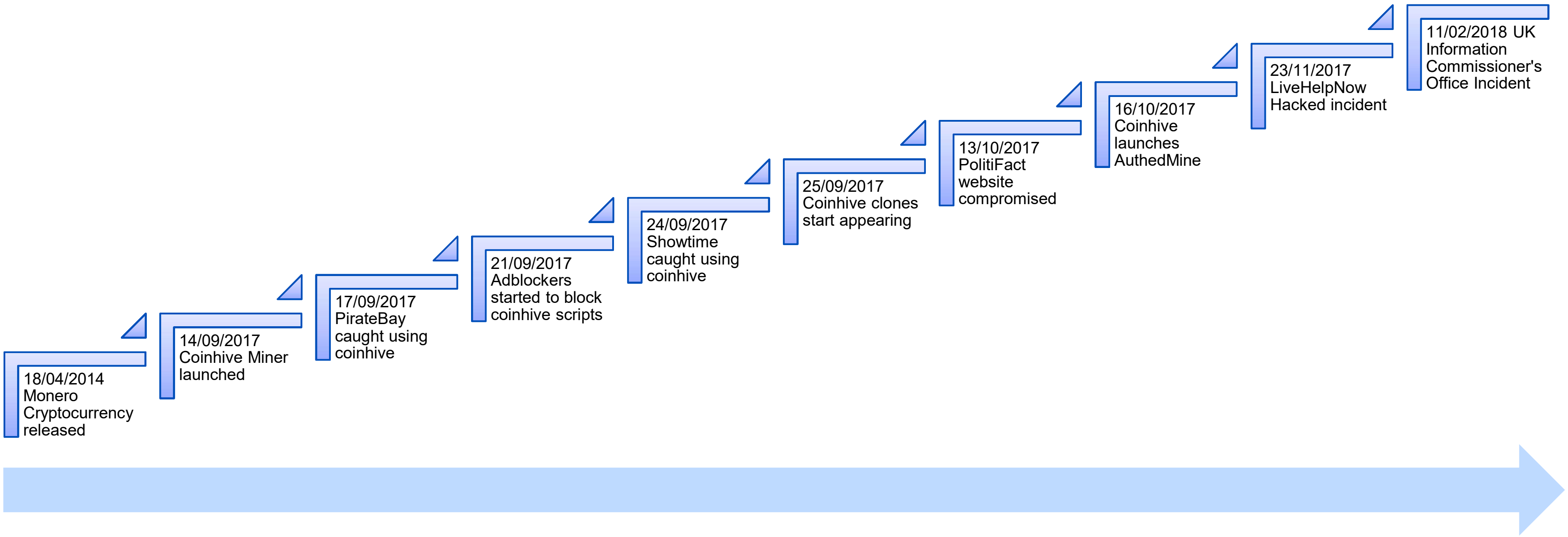
2014

2017

2018

https://arxiv.org/pdf/1803.02887.pdf - accessed 15th Nov 2018

Timeline



18/04/2014 Monero Cryptocurrency released

14/09/2017 Coinhive Miner launched

17/09/2017 PirateBay caught using coinhive

21/09/2017 Adblockers started to block coinhive scripts

24/09/2017 Showtime caught using coinhive

25/09/2017 Coinhive clones start appearing

13/10/2017 PolitiFact website compromised

16/10/2017 Coinhive launches AuthedMine

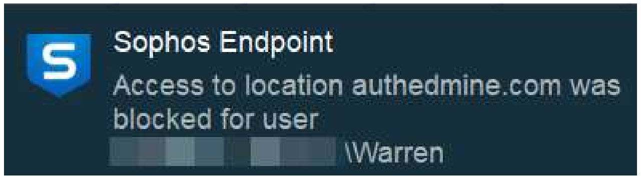
23/11/2017 LiveHelpNow Hacked incident

11/02/2018 UK Information Commissioner's Office Incident

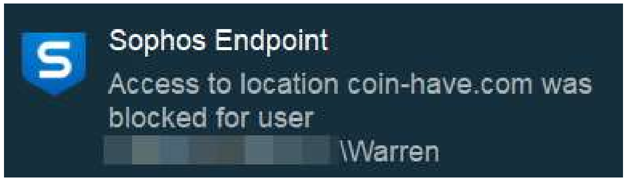
https://arxiv.org/pdf/1803.02887.pdf - accessed 15th Nov 2018

Web based coin miners

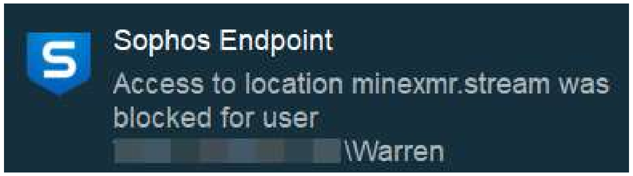
Name	URL
Coinhive	https://coinhive.com
AuthedMine	https://authedmine.com
Coin-Have	https://coin-have.com
CoinImp	https://www.coinimp.com/
Minexmr.stream	https://minexmr.stream
JSECoin	https://jsecoin.com/
Adless	https://www.adless.io/
Crypto-loot	https://crypto-loot.com
GridCash	https://gridcash.net/
CryptoNoter	https://github.com/cryptonoter



Sophos Endpoint
Access to location authedmine.com was blocked for user
[redacted]\Warren



Sophos Endpoint
Access to location coin-have.com was blocked for user
[redacted]\Warren

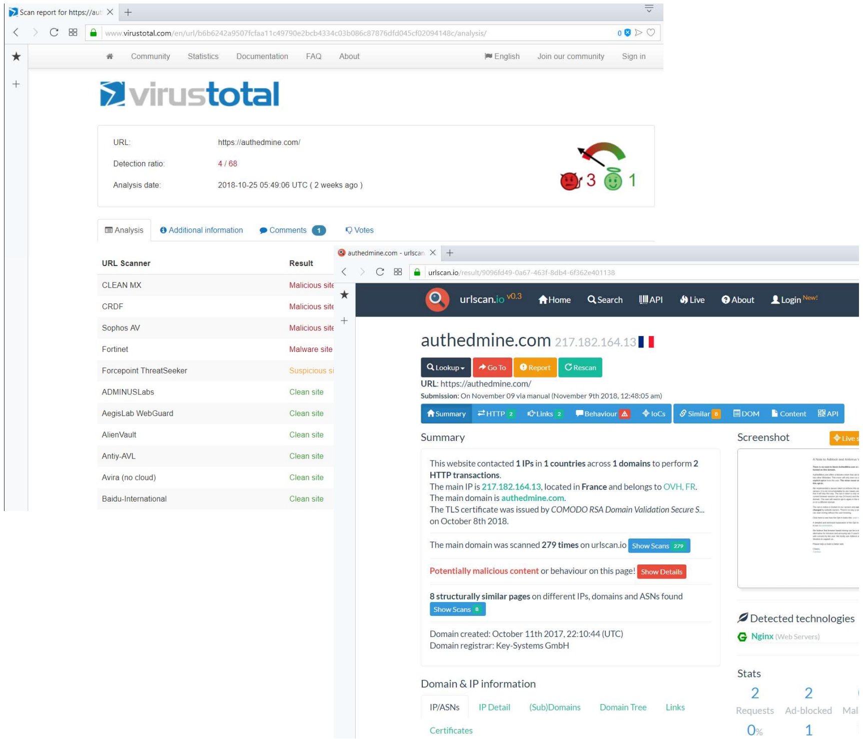


Sophos Endpoint
Access to location minexmr.stream was blocked for user
[redacted]\Warren

https://alternativeto.net/software/coinhive/ - accessed 9th Nov 2018

Web based coin miners

Name	URL
Coinhive	https://coinhive.com
AuthedMine	https://authedmine.com
Coin-Have	https://coin-have.com
CoinImp	https://www.coinimp.com/
Minexmr.stream	https://minexmr.stream
JSECoin	https://jsecoin.com/
Adless	https://www.adless.io/
Crypto-loot	https://crypto-loot.com
GridCash	https://gridcash.net/
CryptoNoter	https://github.com/cryptonoter


Scan report for https://aut
www.virustotal.com/en/url/b6b6242a9507fcfaa11c49790e2bcb4334c03b086c87876dfd045cf02094148c/analysis/
Community
Statistics
Documentation
FAQ
About
English
Join our community
Sign in
virustotal

URL: https://authedmine.com/

Detection ratio: 4 / 68

Analysis date: 2018-10-25 05:49:06 UTC (2 weeks ago)

URL Scanner	Result
CLEAN MX	Malicious site
CRDF	Malicious site
Sophos AV	Malicious site
Fortinet	Malware site
Forcepoint ThreatSeeker	Suspicious si
ADMINUSLabs	Clean site
AegisLab WebGuard	Clean site
AlienVault	Clean site
Antiy-AVL	Clean site
Avira (no cloud)	Clean site
Baidu-International	Clean site

URL: https://authedmine.com/

Submission: On November 09 via manual (November 9th 2018, 12:48:05 am)

Summary

This website contacted **1 IPs** in **1 countries** across **1 domains** to perform **2 HTTP transactions**.
The main IP is 217.182.164.13, located in **France** and belongs to OVH, FR.
The main domain is authedmine.com.
The TLS certificate was issued by *COMODO RSA Domain Validation Secure S...* on October 8th 2018.

The main domain was scanned **279 times** on urlscan.io Show Scans 279

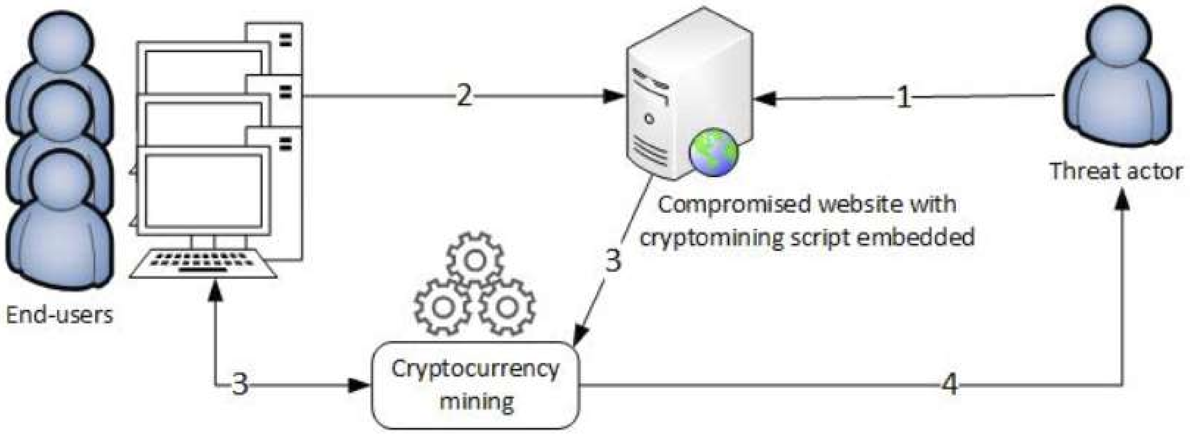
Potentially malicious content or behaviour on this page! Show Details

8 structurally similar pages on different IPs, domains and ASNs found Show Scans 8

Domain created: October 11th 2017, 22:10:44 (UTC)
Domain registrar: Key-Systems GmbH

https://alternativeto.net/software/coinhive/ - accessed 9th Nov 2018

What is Crypto Jacking



Steps

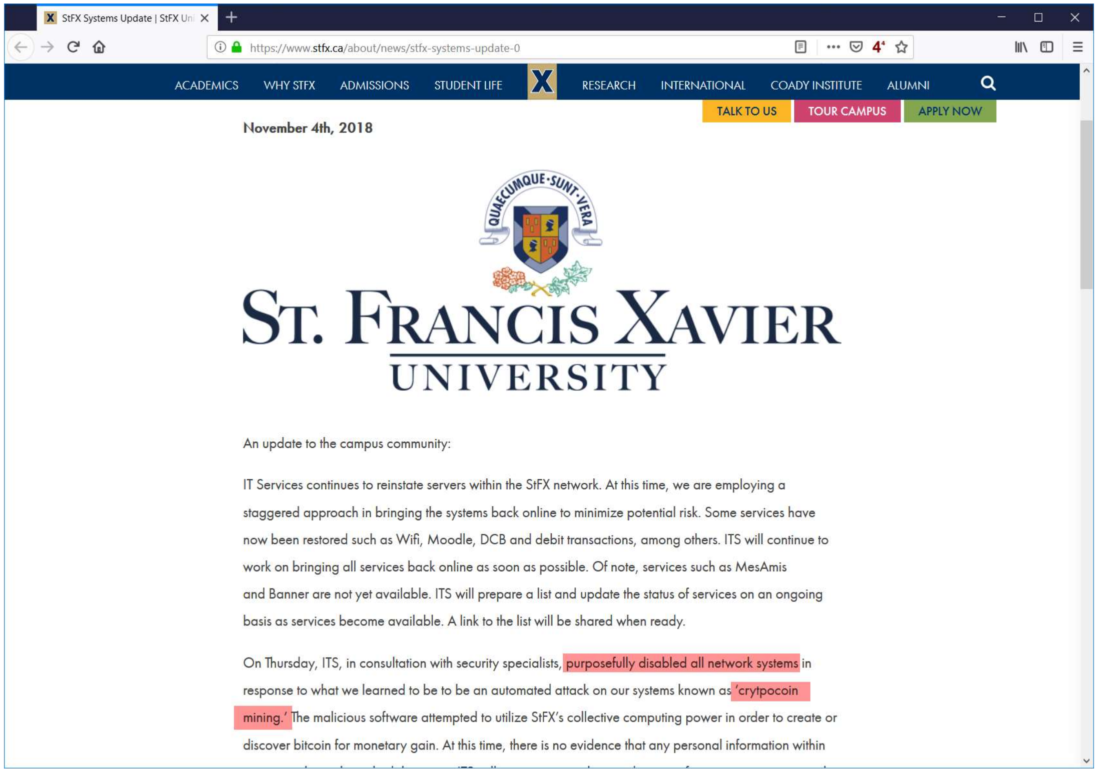
1. The threat actor compromises a website
2. Users connect to the compromised website and the cryptomining script executes
3. Users unknowingly start mining cryptocurrency on behalf of the threat actor
4. Upon successfully adding a new block to the blockchain, the threat actor receives a reward in cryptocurrency coins

https://www.enisa.europa.eu/publications/info-notes/images_info_notes/cryptojacking.jpg

What is Crypto Jacking

- The unauthorized use of computing resources to mine cryptocurrencies.
- Using malicious tools designed to hijack vulnerable systems to mine for cryptocurrency in the background using crypto mining software without the consent or knowledge of the victims.
- The technique of hijacking browsers for mining cryptocurrency (without user consent).

Are all crypto miners bad?



November 4th, 2018

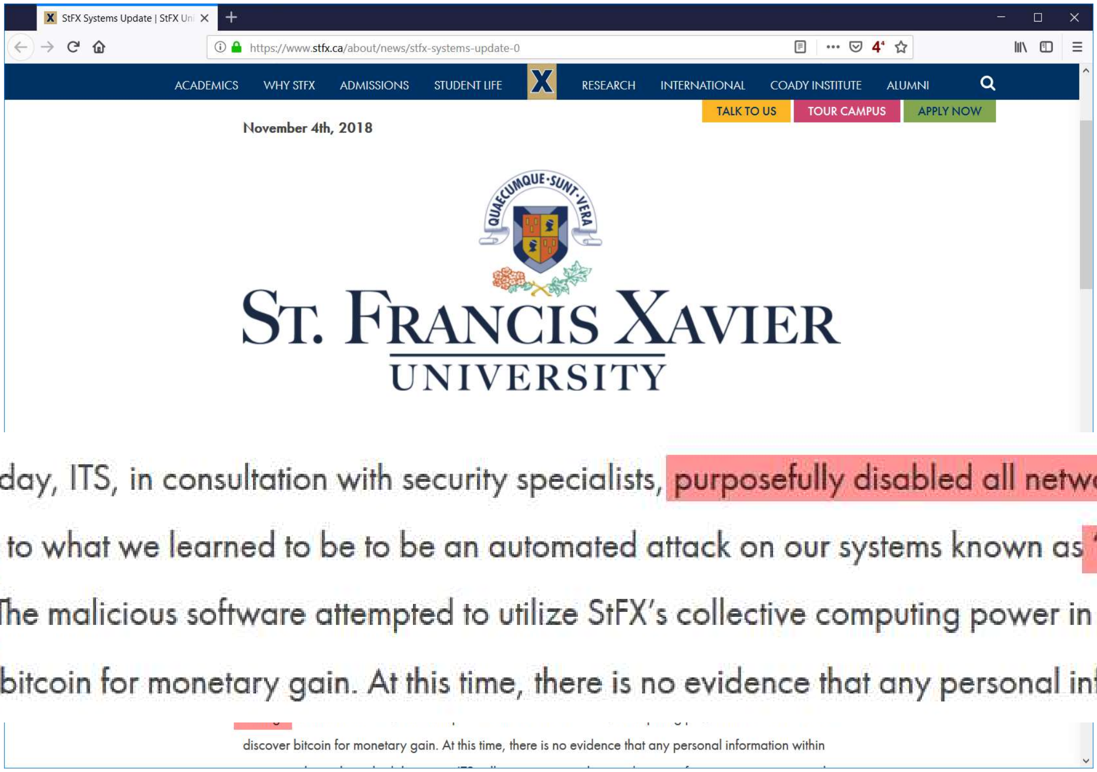
An update to the campus community:

IT Services continues to reinstate servers within the StFX network. At this time, we are employing a staggered approach in bringing the systems back online to minimize potential risk. Some services have now been restored such as Wifi, Moodle, DCB and debit transactions, among others. ITS will continue to work on bringing all services back online as soon as possible. Of note, services such as MesAmis and Banner are not yet available. ITS will prepare a list and update the status of services on an ongoing basis as services become available. A link to the list will be shared when ready.

On Thursday, ITS, in consultation with security specialists, purposefully disabled all network systems in response to what we learned to be to be an automated attack on our systems known as 'crytpocoin mining.' The malicious software attempted to utilize StFX's collective computing power in order to create or discover bitcoin for monetary gain. At this time, there is no evidence that any personal information within

https://www.stfx.ca/about/news/stfx-systems-update-0 - accessed 8th Nov 2018

Are all crypto miners bad?



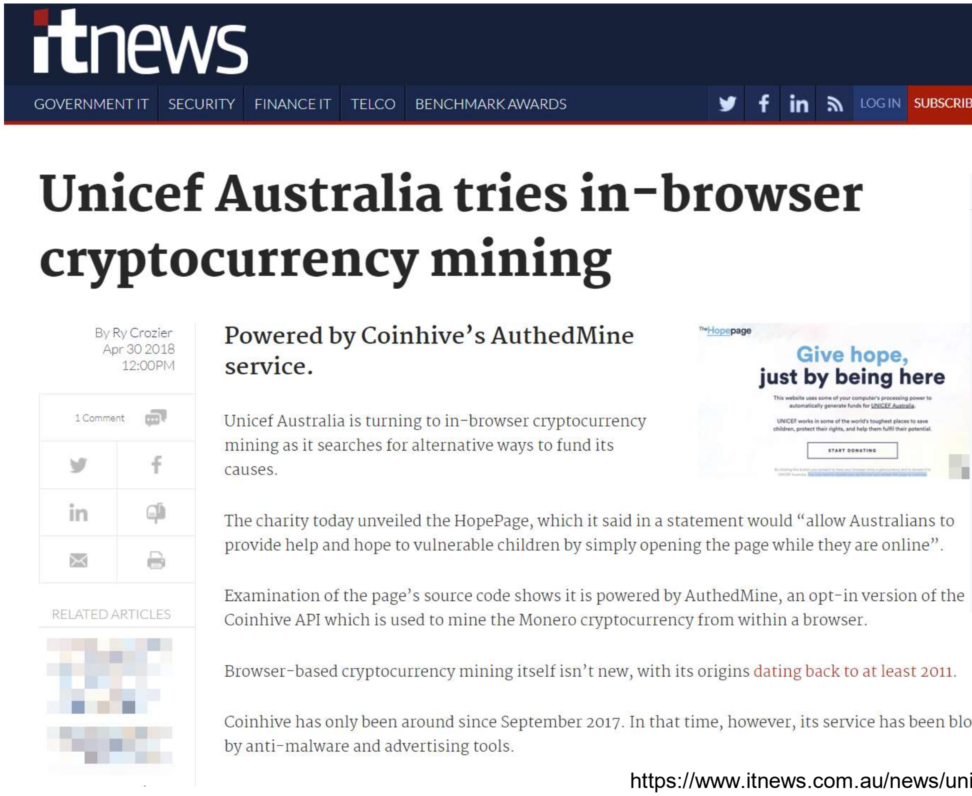
November 4th, 2018

On Thursday, ITS, in consultation with security specialists, purposefully disabled all network systems in response to what we learned to be to be an automated attack on our systems known as 'crytpocoin mining.' The malicious software attempted to utilize StFX's collective computing power in order to create or discover bitcoin for monetary gain. At this time, there is no evidence that any personal information within

discover bitcoin for monetary gain. At this time, there is no evidence that any personal information within

https://www.stfx.ca/about/news/stfx-systems-update-0 - accessed 8th Nov 2018

Are all crypto miners bad?



Unicef Australia tries in-browser cryptocurrency mining

By Ry Crozier
Apr 30 2018
12:00PM

Powered by Coinhive's AuthedMine service.

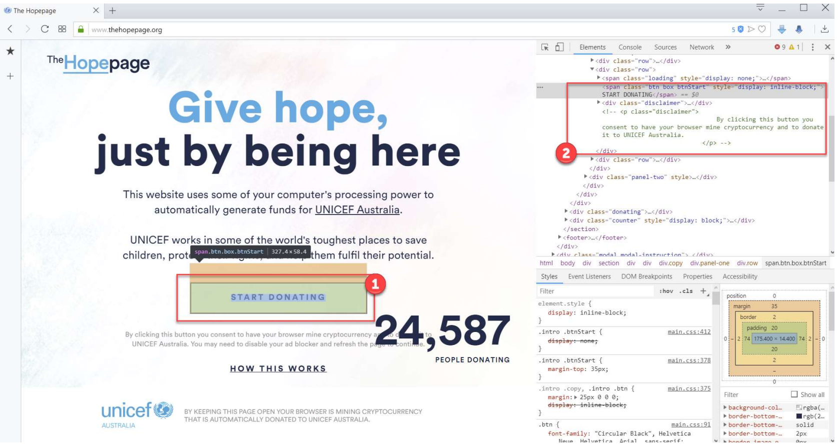
Unicef Australia is turning to in-browser cryptocurrency mining as it searches for alternative ways to fund its causes.

The charity today unveiled the HopePage, which it said in a statement would "allow Australians to provide help and hope to vulnerable children by simply opening the page while they are online".

Examination of the page's source code shows it is powered by AuthedMine, an opt-in version of the Coinhive API which is used to mine the Monero cryptocurrency from within a browser.

Browser-based cryptocurrency mining itself isn't new, with its origins dating back to at least 2011.

Coinhive has only been around since September 2017. In that time, however, its service has been blocked by anti-malware and advertising tools.



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, prot[...]them fulfil their potential.

By clicking this button you consent to have your browser mine cryptocurrency a[...] UNICEF Australia. You may need to disable your ad blocker and refresh the pa[...]

BY KEEPING THIS PAGE OPEN YOUR BROWSER IS MINING CRYPTOCURRENCY THAT IS AUTOMATICALLY DONATED TO UNICEF AUSTRALIA.

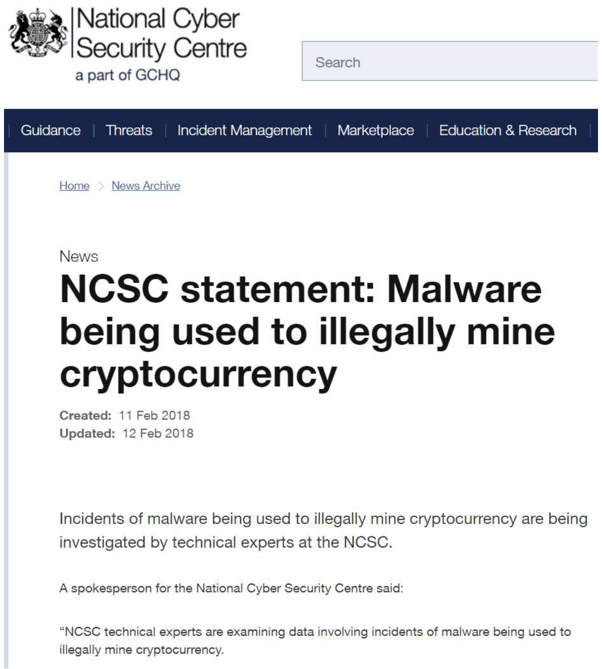
```
▸<div class="row">…</div>
▾<div class="row">
  ▸<span class="loading" style="display: none;">…</span>
   <span class="btn box btnStart" style="display: inline-block;">
   START DONATING</span> == $0
  ▸<div class="disclaimer">…</div>
   <!-- <p class="disclaimer">
                                   By clicking this button you
   consent to have your browser mine cryptocurrency and to donate
   it to UNICEF Australia.
                              </p> -->
 </div>
▸<div class="row">…</div>
</div>
▸<div class="panel-two" style>…</div>
</div>
</div>
</div>
▸<div class="donating">…</div>
▸<div class="counter" style="display: block;">…</div>
</section>
▸<footer>…</footer>
</div>
▸<div class="modal modal-instruction">…</div>
```

html body div section div div div.copy div.panel-one div.row span.btn.box.btnStart

```
element.style {
  display: inline-block;
}
.intro .btnStart {                    main.css:412
  ~~display: none;~~
}
.intro .btnStart {                    main.css:378
  margin-top: 35px;
}
.intro .copy, .intro .btn {           main.css:375
  margin: ▸ 25px 0 0 0;
  ~~display: inline-block;~~
}
.btn {                                main.css:91
  font-family: "Circular Black", Helvetica
    Neue, Helvetica, Arial, sans-serif;
```

https://www.itnews.com.au/news/unicef-australia-tries-in-browser-cryptocurrency-mining-489884 - accessed 9th Nov 2018

Are all crypto miners bad?


National Cyber Security Centre
a part of GCHQ
Search
Guidance | Threats | Incident Management | Marketplace | Education & Research
Home > News Archive

News

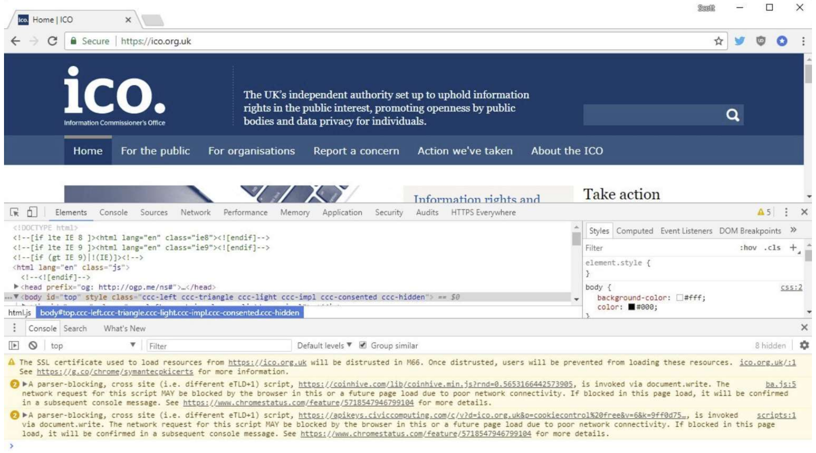
NCSC statement: Malware being used to illegally mine cryptocurrency

Created: 11 Feb 2018
Updated: 12 Feb 2018

Incidents of malware being used to illegally mine cryptocurrency are being investigated by technical experts at the NCSC.

A spokesperson for the National Cyber Security Centre said:

"NCSC technical experts are examining data involving incidents of malware being used to illegally mine cryptocurrency.



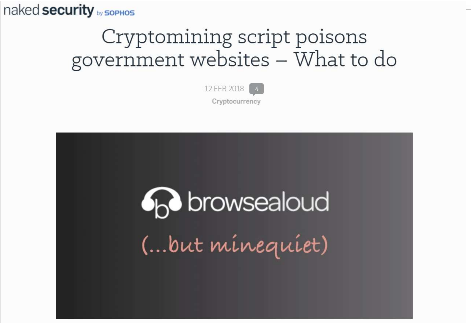
The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

```
<!DOCTYPE html>
<!--[if lte IE 8 ]><html lang="en" class="ie8"><![endif]-->
<!--[if lte IE 9 ]><html lang="en" class="ie9"><![endif]-->
<!--[if (gt IE 9)|!(IE)]><!-->
<html lang="en" class="js">
  <!--<![endif]-->
▶<head prefix="og: http://ogp.me/ns#">…</head>
▼<body id="top" style class="ccc-left ccc-triangle ccc-light ccc-impl ccc-consented ccc-hidden"> == $0
```

```
html.js  body#top.ccc-left.ccc-triangle.ccc-light.ccc-impl.ccc-consented.ccc-hidden
```

```
element.style {
}
body {                                                   css:2
  background-color: □#fff;
  color: ■#000;
```

```
⚠ The SSL certificate used to load resources from https://ico.org.uk will be distrusted in M66. Once distrusted, users will be prevented from loading these resources.  ico.org.uk/:1
  See https://g.co/chrome/symantecpkicerts for more information.
2 ▶A parser-blocking, cross site (i.e. different eTLD+1) script, https://coinhive.com/lib/coinhive.min.js?rnd=0.5653166442573905, is invoked via document.write. The   ba.js:5
  network request for this script MAY be blocked by the browser in this or a future page load due to poor network connectivity. If blocked in this page load, it will be confirmed
  in a subsequent console message. See https://www.chromestatus.com/feature/5718547946799104 for more details.
2 ▶A parser-blocking, cross site (i.e. different eTLD+1) script, https://apikeys.civiccomputing.com/c/v?d=ico.org.uk&p=cookiecontrol%20free&v=6&k=9ff0d75…, is invoked   scripts:1
  via document.write. The network request for this script MAY be blocked by the browser in this or a future page load due to poor network connectivity. If blocked in this page
  load, it will be confirmed in a subsequent console message. See https://www.chromestatus.com/feature/5718547946799104 for more details.
```

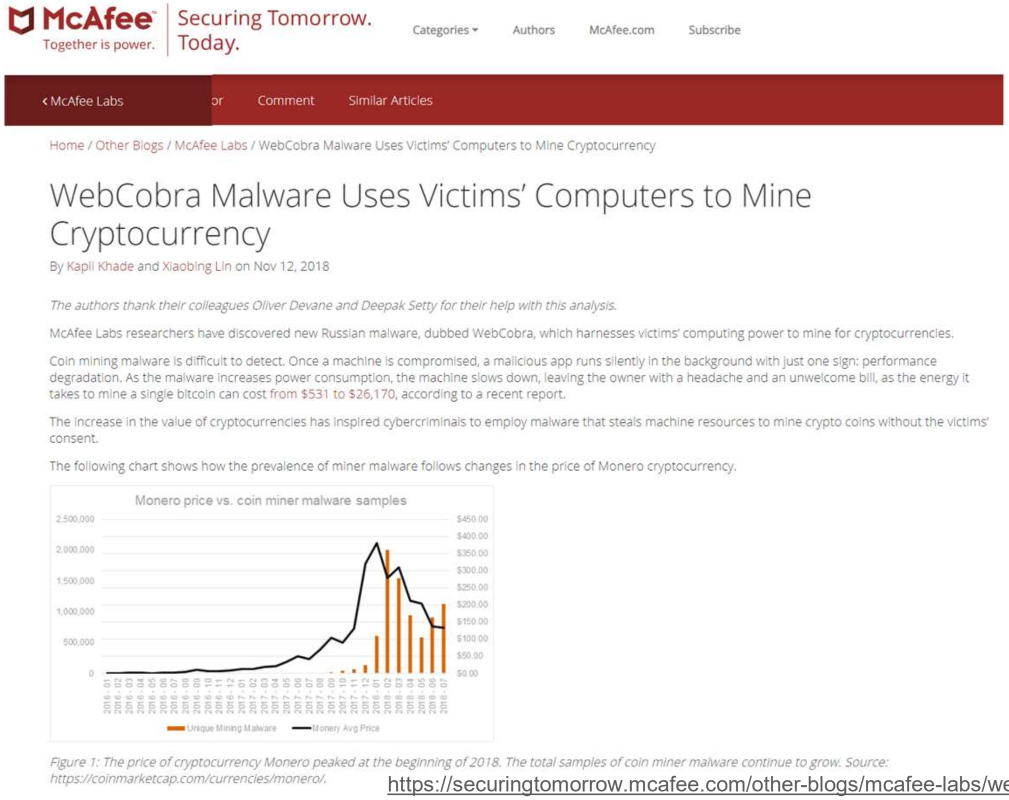


Cryptomining script poisons government websites – What to do

12 FEB 2018
Cryptocurrency

https://techcrunch.com/2018/02/12/browsealoud-coinhive-monero-mining-hack/ - accessed 14th Nov 2018

Are all crypto miners bad?



McAfee Together is power. | Securing Tomorrow. Today.

Categories ▾ Authors McAfee.com Subscribe

‹ McAfee Labs or Comment Similar Articles

Home / Other Blogs / McAfee Labs / WebCobra Malware Uses Victims' Computers to Mine Cryptocurrency

WebCobra Malware Uses Victims' Computers to Mine Cryptocurrency

By Kapil Khade and Xiaobing Lin on Nov 12, 2018

The authors thank their colleagues Oliver Devane and Deepak Setty for their help with this analysis.

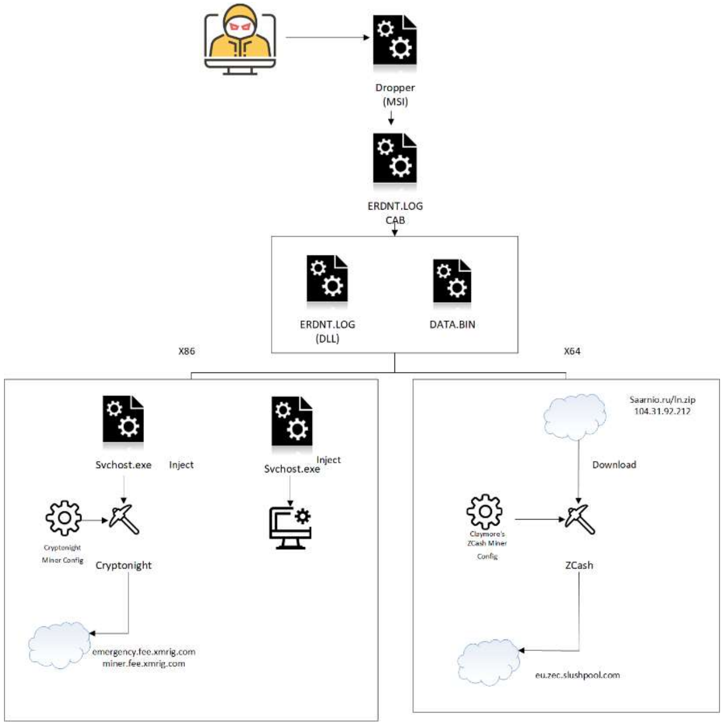
McAfee Labs researchers have discovered new Russian malware, dubbed WebCobra, which harnesses victims' computing power to mine for cryptocurrencies.

Coin mining malware is difficult to detect. Once a machine is compromised, a malicious app runs silently in the background with just one sign: performance degradation. As the malware increases power consumption, the machine slows down, leaving the owner with a headache and an unwelcome bill, as the energy it takes to mine a single bitcoin can cost from $531 to $26,170, according to a recent report.

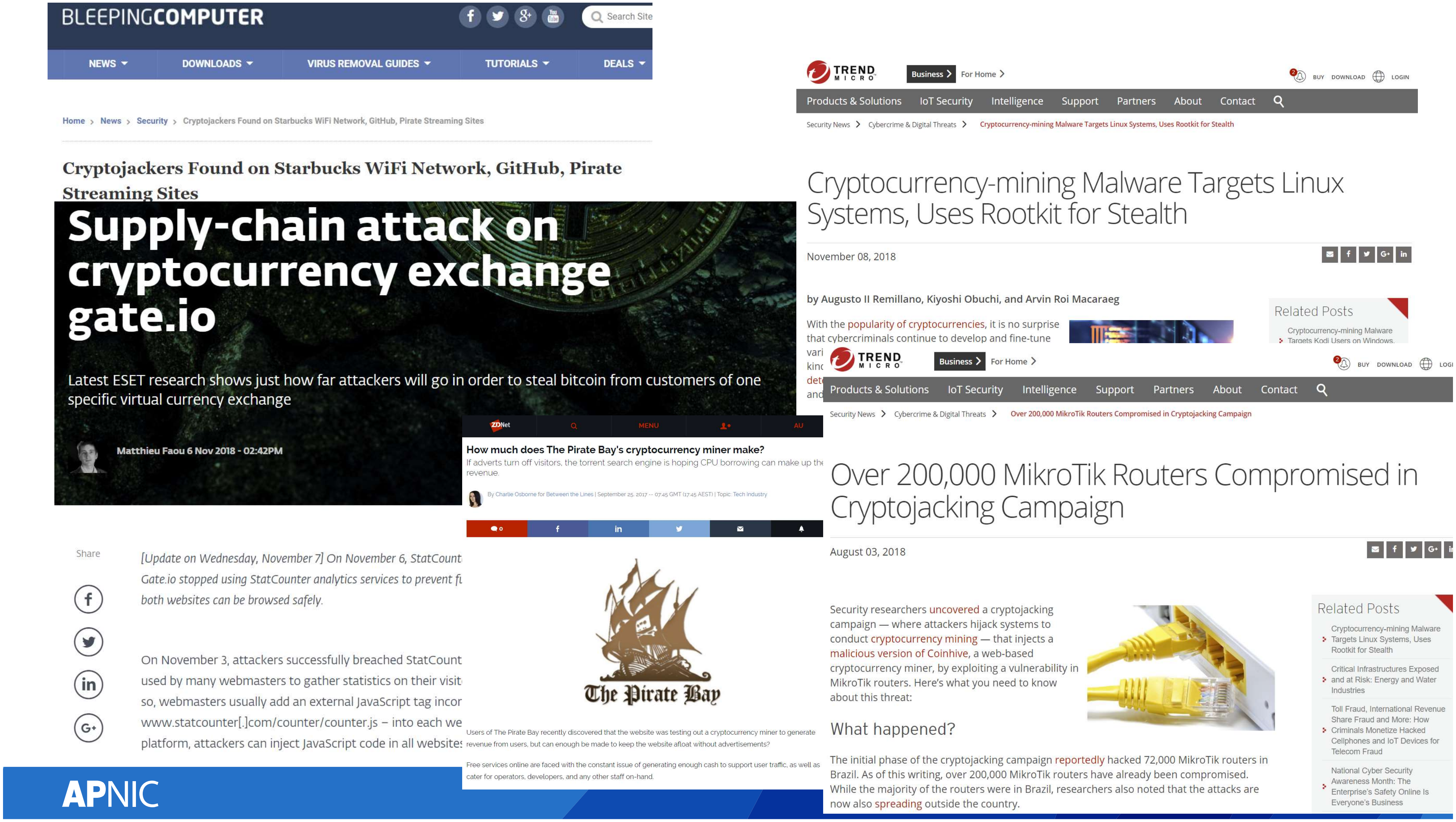
The increase in the value of cryptocurrencies has inspired cybercriminals to employ malware that steals machine resources to mine crypto coins without the victims' consent.

The following chart shows how the prevalence of miner malware follows changes in the price of Monero cryptocurrency.

Figure 1: The price of cryptocurrency Monero peaked at the beginning of 2018. The total samples of coin miner malware continue to grow. Source: https://coinmarketcap.com/currencies/monero/.



https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/webcobra-malware-uses-victims-computers-to-mine-cryptocurrency/ - accessed 15th Nov 2018



BLEEPINGCOMPUTER
Search Site
NEWS
DOWNLOADS
VIRUS REMOVAL GUIDES
TUTORIALS
DEALS
Home › News › Security › Cryptojackers Found on Starbucks WiFi Network, GitHub, Pirate Streaming Sites

Cryptojackers Found on Starbucks WiFi Network, GitHub, Pirate Streaming Sites

Supply-chain attack on cryptocurrency exchange gate.io

Latest ESET research shows just how far attackers will go in order to steal bitcoin from customers of one specific virtual currency exchange

Matthieu Faou 6 Nov 2018 - 02:42PM

[Update on Wednesday, November 7] On November 6, StatCount
Gate.io stopped using StatCounter analytics services to prevent fu
both websites can be browsed safely.

On November 3, attackers successfully breached StatCount
used by many webmasters to gather statistics on their visit
so, webmasters usually add an external JavaScript tag incor
www.statcounter[.]com/counter/counter.js – into each we
platform, attackers can inject JavaScript code in all websites

How much does The Pirate Bay's cryptocurrency miner make?

If adverts turn off visitors, the torrent search engine is hoping CPU borrowing can make up the revenue.

By Charlie Osborne for Between the Lines | September 25, 2017 -- 07:45 GMT (17:45 AEST) | Topic: Tech Industry

Users of The Pirate Bay recently discovered that the website was testing out a cryptocurrency miner to generate revenue from users, but can enough be made to keep the website afloat without advertisements?

Free services online are faced with the constant issue of generating enough cash to support user traffic, as well as cater for operators, developers, and any other staff on-hand.

TREND MICRO
Business
For Home
BUY
DOWNLOAD
LOGIN
Products & Solutions
IoT Security
Intelligence
Support
Partners
About
Contact
Security News › Cybercrime & Digital Threats › Cryptocurrency-mining Malware Targets Linux Systems, Uses Rootkit for Stealth

Cryptocurrency-mining Malware Targets Linux Systems, Uses Rootkit for Stealth

November 08, 2018

by Augusto II Remillano, Kiyoshi Obuchi, and Arvin Roi Macaraeg

With the popularity of cryptocurrencies, it is no surprise that cybercriminals continue to develop and fine-tune
vari
kinc
det
and

Related Posts

Cryptocurrency-mining Malware Targets Kodi Users on Windows,

TREND MICRO
Business
For Home
BUY
DOWNLOAD
LOGI
Products & Solutions
IoT Security
Intelligence
Support
Partners
About
Contact
Security News › Cybercrime & Digital Threats › Over 200,000 MikroTik Routers Compromised in Cryptojacking Campaign

Over 200,000 MikroTik Routers Compromised in Cryptojacking Campaign

August 03, 2018

Security researchers uncovered a cryptojacking campaign — where attackers hijack systems to conduct cryptocurrency mining — that injects a malicious version of Coinhive, a web-based cryptocurrency miner, by exploiting a vulnerability in MikroTik routers. Here's what you need to know about this threat:

What happened?

The initial phase of the cryptojacking campaign reportedly hacked 72,000 MikroTik routers in Brazil. As of this writing, over 200,000 MikroTik routers have already been compromised. While the majority of the routers were in Brazil, researchers also noted that the attacks are now also spreading outside the country.

Related Posts

- Cryptocurrency-mining Malware Targets Linux Systems, Uses Rootkit for Stealth
- Critical Infrastructures Exposed and at Risk: Energy and Water Industries
- Toll Fraud, International Revenue Share Fraud and More: How Criminals Monetize Hacked Cellphones and IoT Devices for Telecom Fraud
- National Cyber Security Awareness Month: The Enterprise's Safety Online Is Everyone's Business

Start browser in headless mode

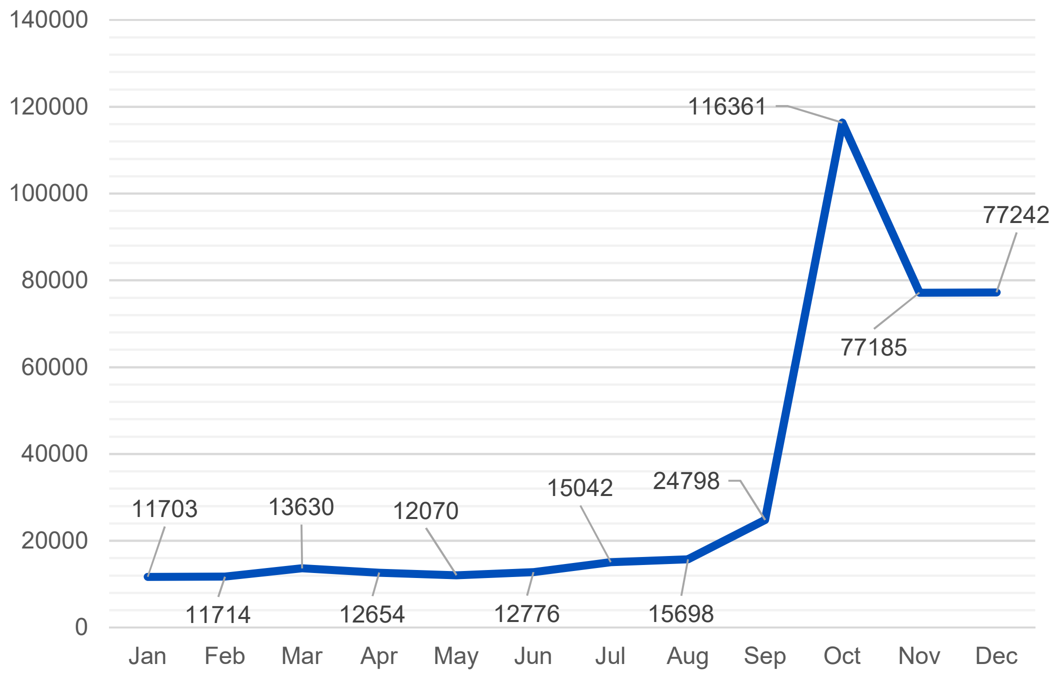
```
chrome --headless --disable-gpu --remote-debugging-port=9222 --user-agent='user-agent=Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36’ 'https://coinhive.com/media/miner.html?autostart=1&key=GoI0WOEe2JFj22Aj3JqYVcTt98LArmUX'
```

https://steemit.com/mining/@ttox/headless-browser-mining - accessed 9th Nov 2018

Cryptomining malware

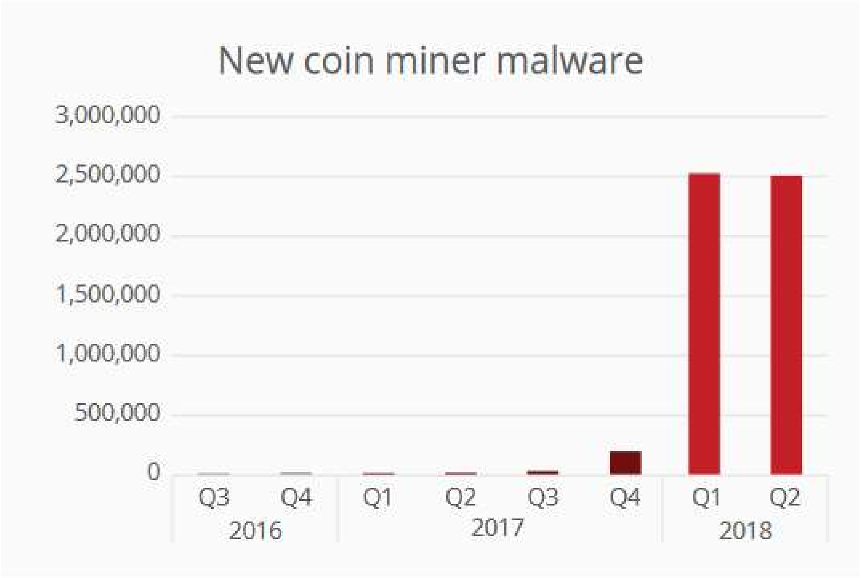
- Leaked EternalBlue and DoublePulsar exploits are used to infect vulnerable windows servers and PCs.
- Oracle’s WebLogic Server (CVE-2017-10271) flaw was also used to deliver miners onto servers.
- Malware families distributed via malicious spam attachments, now have a coin miner module.
- Android and Mac users are infected by trojanised apps laced with mining code.

Crypto-mining malware detections in 2017

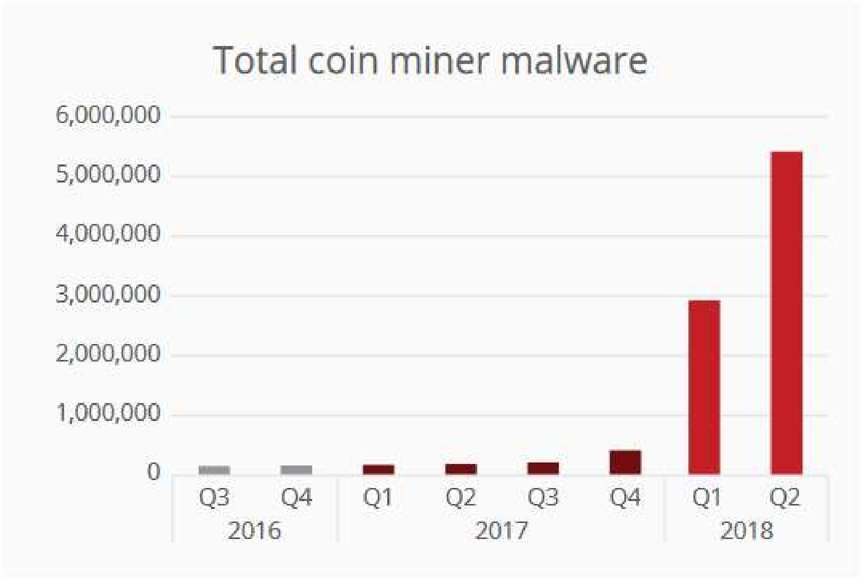


https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-mining-malware-2018-new-menace/ - accessed 9th Nov 2018

Crypto-mining malware detections in 2018



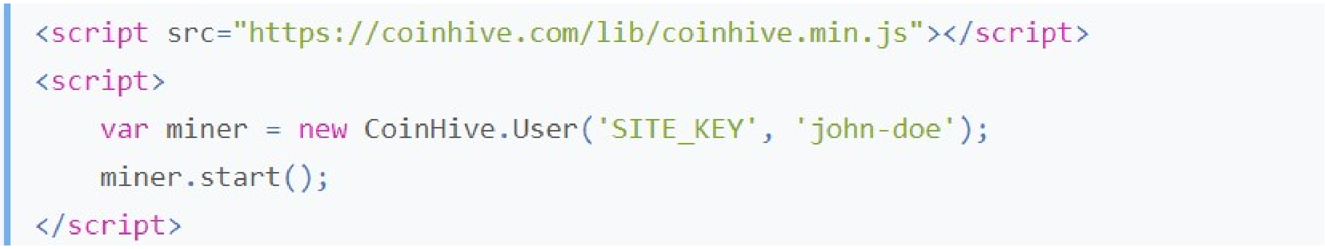
Source: McAfee Labs, 2018.



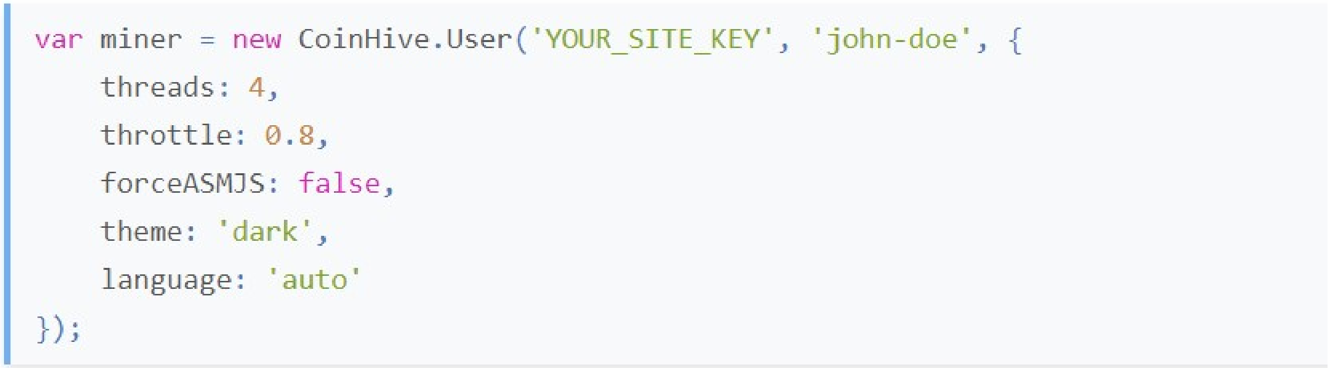
Source: McAfee Labs, 2018.

https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-sep-2018.pdf - accessed 9th Nov 2018

Javascript – Coinhive



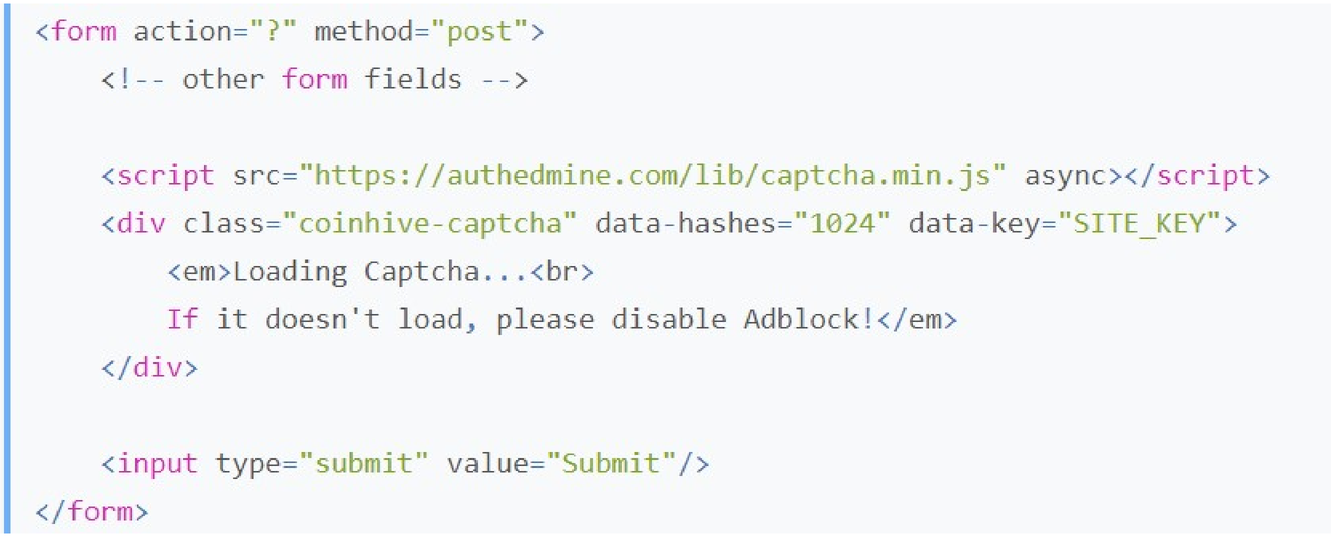
```
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
    var miner = new CoinHive.User('SITE_KEY', 'john-doe');
    miner.start();
</script>
```



```
var miner = new CoinHive.User('YOUR_SITE_KEY', 'john-doe', {
    threads: 4,
    throttle: 0.8,
    forceASMJS: false,
    theme: 'dark',
    language: 'auto'
});
```

https://coinhive.com – accessed 9th Nov 2018

Javascript – AuthedMine captcha

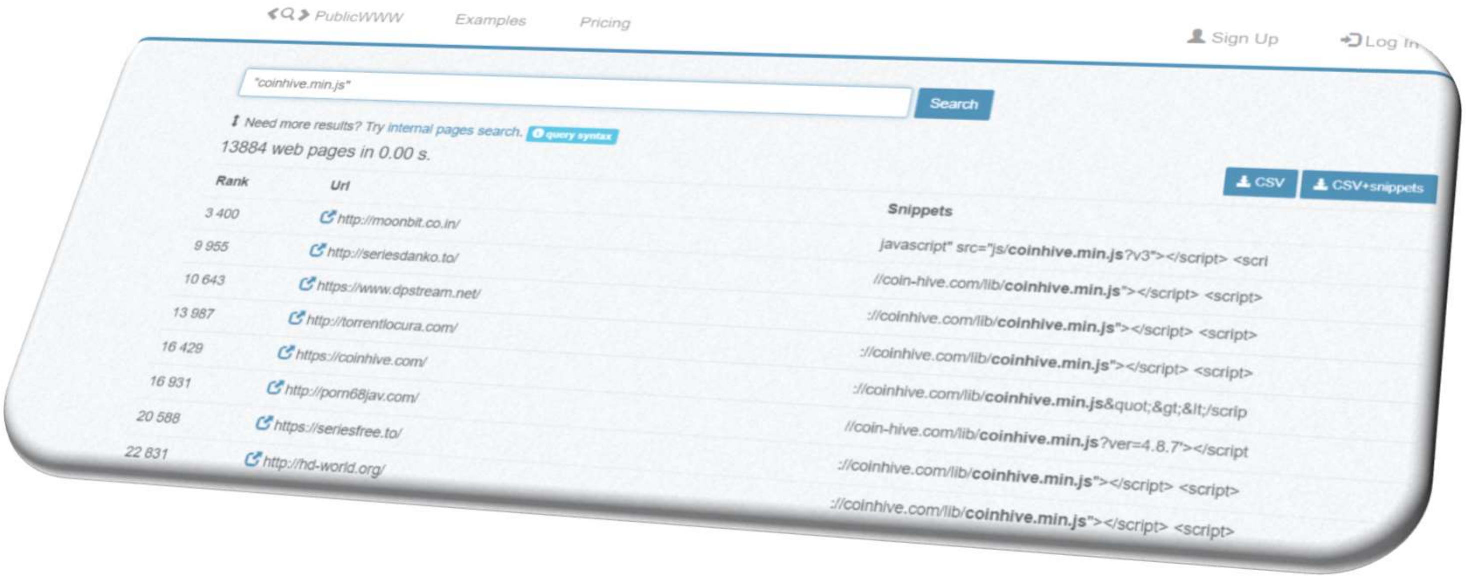


```
<form action="?" method="post">
    <!-- other form fields -->

    <script src="https://authedmine.com/lib/captcha.min.js" async></script>
    <div class="coinhive-captcha" data-hashes="1024" data-key="SITE_KEY">
        <em>Loading Captcha...<br>
        If it doesn't load, please disable Adblock!</em>
    </div>

    <input type="submit" value="Submit"/>
</form>
```

https://coinhive.com – accessed 9th Nov 2018

Locating sites with a coinhive script

- https://publicwww.com/websites/"coinhive.min.js"/



"coinhive.min.js"

Need more results? Try internal pages search.

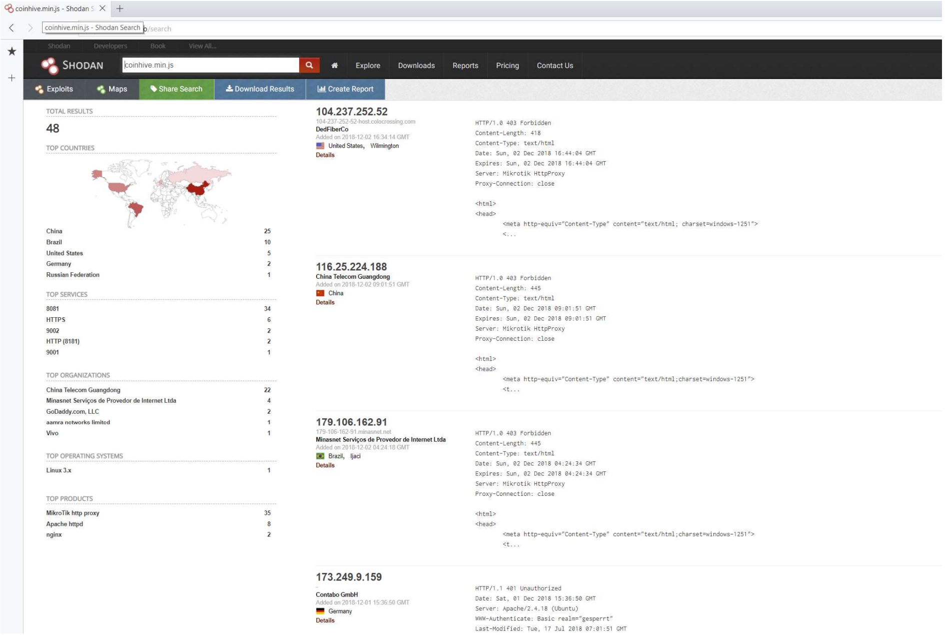
13884 web pages in 0.00 s.

Rank	Url	Snippets
3 400	http://moonbit.co.in/	javascript" src="js/**coinhive.min.js**?v3"></script> <scri
9 955	http://seriesdanko.to/	//coin-hive.com/lib/**coinhive.min.js**"></script> <script>
10 643	https://www.dpstream.net/	://coinhive.com/lib/**coinhive.min.js**"></script> <script>
13 987	http://torrentlocura.com/	://coinhive.com/lib/**coinhive.min.js**"></script> <script>
16 429	https://coinhive.com/	://coinhive.com/lib/**coinhive.min.js**&quot;&gt;&lt;/scrip
16 931	http://porn68jav.com/	//coin-hive.com/lib/**coinhive.min.js**?ver=4.8.7'></script
20 588	https://seriesfree.to/	://coinhive.com/lib/**coinhive.min.js**"></script> <script>
22 831	http://hd-world.org/	://coinhive.com/lib/**coinhive.min.js**"></script> <script>

accessed 9th Nov 2018

Locating devices with a coinhive script

- https://www.shodan.io/search?query=coinhive.min.js



TOTAL RESULTS

48

TOP COUNTRIES

China	25
Brazil	10
United States	5
Germany	2
Russian Federation	1

TOP SERVICES

8081	34
HTTPS	6
9002	2
HTTP (8181)	2
9001	1

TOP ORGANIZATIONS

China Telecom Guangdong	22
Minasnet Serviços de Provedor de Internet Ltda	4
GoDaddy.com, LLC	2
aamra networks limited	1
Vivo	1

TOP OPERATING SYSTEMS

Linux 3.x	1

TOP PRODUCTS

MikroTik http proxy	35
Apache httpd	8
nginx	2

104.237.252.52
104-237-252-52-host.colocrossing.com
DedFiberCo
Added on 2018-12-02 16:34:14 GMT
United States, Wilmington
Details

```
HTTP/1.0 403 Forbidden
Content-Length: 418
Content-Type: text/html
Date: Sun, 02 Dec 2018 16:44:04 GMT
Expires: Sun, 02 Dec 2018 16:44:04 GMT
Server: Mikrotik HttpProxy
Proxy-Connection: close

<html>
<head>
        <meta http-equiv="Content-Type" content="text/html; charset=windows-1251">
        <...
```

116.25.224.188
China Telecom Guangdong
Added on 2018-12-02 09:01:51 GMT
China
Details

```
HTTP/1.0 403 Forbidden
Content-Length: 445
Content-Type: text/html
Date: Sun, 02 Dec 2018 09:01:51 GMT
Expires: Sun, 02 Dec 2018 09:01:51 GMT
Server: Mikrotik HttpProxy
Proxy-Connection: close

<html>
<head>
        <meta http-equiv="Content-Type" content="text/html;charset=windows-1251">
        <t...
```

179.106.162.91
179-106-162-91.minasnet.net
Minasnet Serviços de Provedor de Internet Ltda
Added on 2018-12-02 04:24:18 GMT
Brazil, Ijaci
Details

```
HTTP/1.0 403 Forbidden
Content-Length: 445
Content-Type: text/html
Date: Sun, 02 Dec 2018 04:24:34 GMT
Expires: Sun, 02 Dec 2018 04:24:34 GMT
Server: Mikrotik HttpProxy
Proxy-Connection: close

<html>
<head>
        <meta http-equiv="Content-Type" content="text/html;charset=windows-1251">
        <t...
```

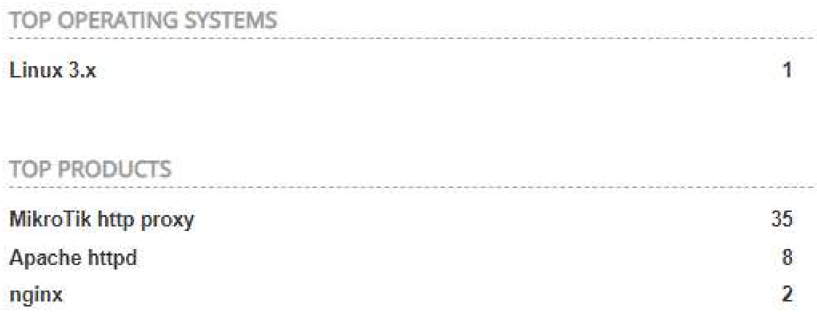
173.249.9.159
-
Contabo GmbH
Added on 2018-12-01 15:36:50 GMT
Germany
Details

```
HTTP/1.1 401 Unauthorized
Date: Sat, 01 Dec 2018 15:36:50 GMT
Server: Apache/2.4.18 (Ubuntu)
WWW-Authenticate: Basic realm="gesperrt"
Last-Modified: Tue, 17 Jul 2018 07:01:51 GMT
```

accessed 9th Nov 2018

Locating devices with a coinhive script

- https://www.shodan.io/search?query=coinhive.min.js



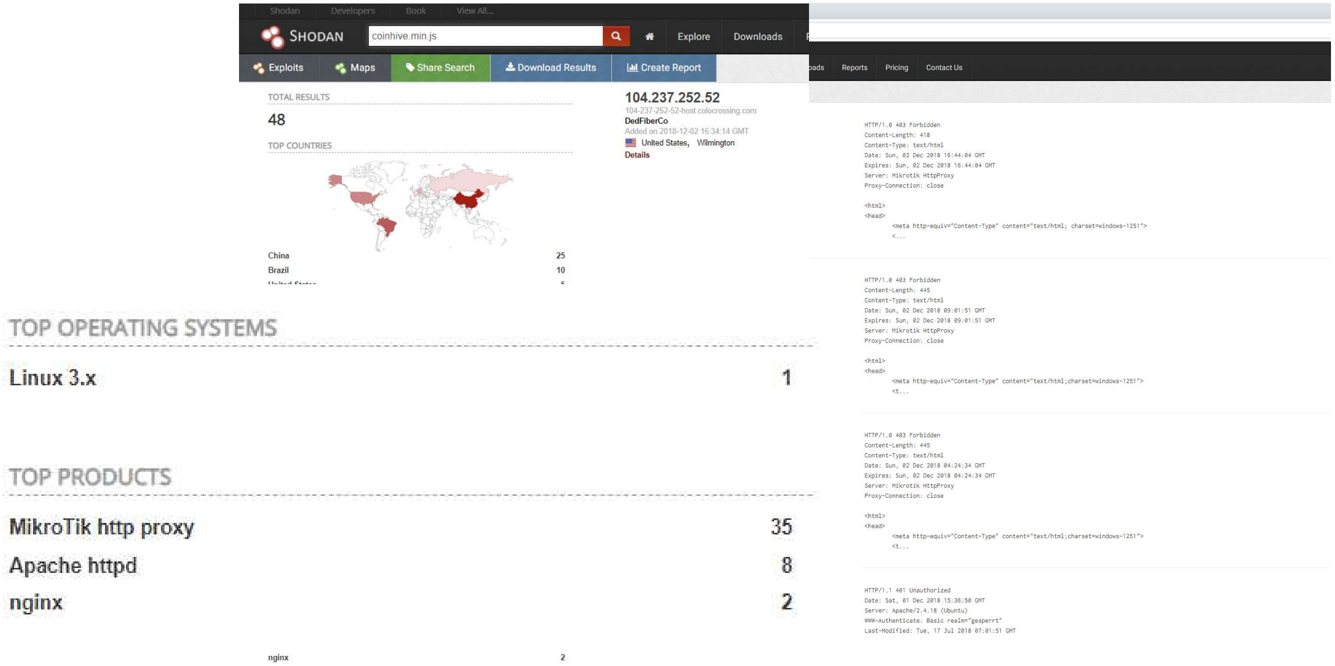
TOP OPERATING SYSTEMS	
Linux 3.x	1

TOP PRODUCTS	
MikroTik http proxy	35
Apache httpd	8
nginx	2

accessed 9th Nov 2018

Locating devices with a coinhive script

- https://www.shodan.io/search?query=coinhive.min.js



TOTAL RESULTS

48

TOP COUNTRIES

China	25
Brazil	10
United States	5

104.237.252.52
104-237-252-52-host.colocrossing.com
DedFiberCo
Added on 2018-12-02 16:34:14 GMT
United States, Wilmington
Details

TOP OPERATING SYSTEMS

Linux 3.x	1

TOP PRODUCTS

MikroTik http proxy	35
Apache httpd	8
nginx	2

```
HTTP/1.0 403 Forbidden
Content-Length: 418
Content-Type: text/html
Date: Sun, 02 Dec 2018 16:44:04 GMT
Expires: Sun, 02 Dec 2018 16:44:04 GMT
Server: Mikrotik HttpProxy
Proxy-Connection: close

<html>
<head>
        <meta http-equiv="Content-Type" content="text/html; charset=windows-1251">
        <...
```

```
HTTP/1.0 403 Forbidden
Content-Length: 445
Content-Type: text/html
Date: Sun, 02 Dec 2018 09:01:51 GMT
Expires: Sun, 02 Dec 2018 09:01:51 GMT
Server: Mikrotik HttpProxy
Proxy-Connection: close

<html>
<head>
        <meta http-equiv="Content-Type" content="text/html;charset=windows-1251">
        <t...
```

```
HTTP/1.0 403 Forbidden
Content-Length: 445
Content-Type: text/html
Date: Sun, 02 Dec 2018 04:24:34 GMT
Expires: Sun, 02 Dec 2018 04:24:34 GMT
Server: Mikrotik HttpProxy
Proxy-Connection: close

<html>
<head>
        <meta http-equiv="Content-Type" content="text/html;charset=windows-1251">
        <t...
```

```
HTTP/1.1 401 Unauthorized
Date: Sat, 01 Dec 2018 15:36:50 GMT
Server: Apache/2.4.18 (Ubuntu)
WWW-Authenticate: Basic realm="gesperrt"
Last-Modified: Tue, 17 Jul 2018 07:01:51 GMT
```

nginx	2

accessed 9th Nov 2018

Locating sites with a miner script

- In a browser open https://publicwww.com/
- Search for common terms used by miners
  - Coinhive = "coinhive.min.js"
  - AuthedMine = authedmine && "captcha.min.js"
  - A JavaScript malware = "navigator['hardwareConcurrency’]"
  - Deobfuscated JavaScript = "[\"(k" "\\x43\\x72\\x79\\x70\\x74\\x6f\\x6e\\x69\\x67\\x68\\x74\\x57\\x41\\x53\\x4d\\x57\\x72\\x61\\x70\\x70\\x65\\x72" snipexp:|(var _0x[0-z]{4}=)|

https://badpackets.net/how-to-find-cryptojacking-malware/ accessed 9th Nov 2018

Locating sites with a miner script

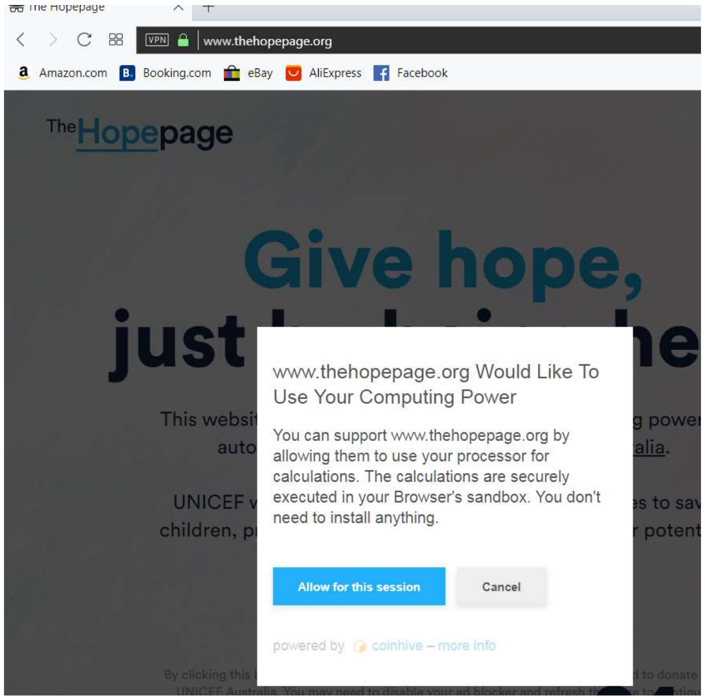
- In a browser open https://shodan.io
- Search for common terms used by miners
  - Coinhive = "coinhive.min.js"
  - AuthedMine = authedmine && "captcha.min.js"
  - A JavaScript malware = "navigator['hardwareConcurrency’]"
  - Deobfuscated JavaScript = "[\"(k" "\\x43\\x72\\x79\\x70\\x74\\x6f\\x6e\\x69\\x67\\x68\\x74\\x57\\x41\\x53\\x4d\\x57\\x72\\x61\\x70\\x70\\x65\\x72" snipexp:|(var _0x[0-z]{4}=)|

https://badpackets.net/how-to-find-cryptojacking-malware/ accessed 9th Nov 2018

Cryptomining in action

- Unicef Australia using a web browser.
  - https://www.thehopepage.org
- Test if browser will allow cryptojacking
  - https://cryptojackingtest.com
- Wandera's fake iOS battery checker for iPhone.
  - https://ios11battery.xyz/

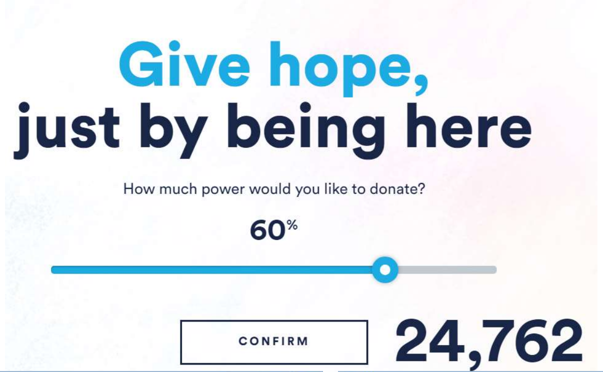
Cryptomining in action



www.thehopepage.org Would Like To Use Your Computing Power

You can support www.thehopepage.org by allowing them to use your processor for calculations. The calculations are securely executed in your Browser's sandbox. You don't need to install anything.

https://www.thehopepage.org



How much power would you like to donate?

60%

24,762

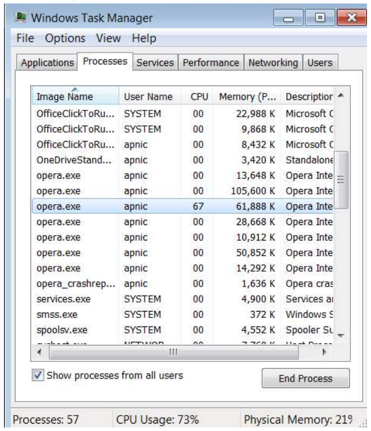
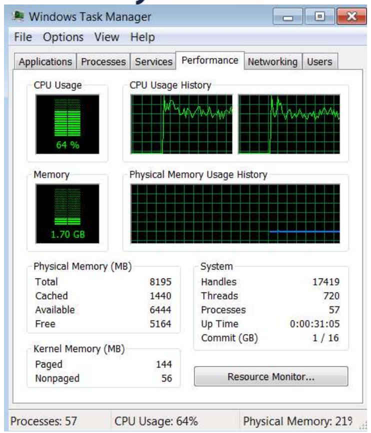


Image Name	User Name	CPU	Memory (P...	Descriptior
OfficeClickToRu...	SYSTEM	00	22,988 K	Microsoft C
OfficeClickToRu...	SYSTEM	00	9,868 K	Microsoft C
OfficeClickToRu...	apnic	00	8,432 K	Microsoft C
OneDriveStand...	apnic	00	3,420 K	Standalone
opera.exe	apnic	00	13,648 K	Opera Inte
opera.exe	apnic	00	105,600 K	Opera Inte
opera.exe	apnic	67	61,888 K	Opera Inte
opera.exe	apnic	00	28,668 K	Opera Inte
opera.exe	apnic	00	10,912 K	Opera Inte
opera.exe	apnic	00	50,852 K	Opera Inte
opera.exe	apnic	00	14,292 K	Opera Inte
opera_crashrep...	apnic	00	1,636 K	Opera cras
services.exe	SYSTEM	00	4,900 K	Services ar
smss.exe	SYSTEM	00	372 K	Windows S
spoolsv.exe	SYSTEM	00	4,552 K	Spooler Su

☑ Show processes from all users

Processes: 57 CPU Usage: 73% Physical Memory: 21%



Physical Memory (MB)	
Total	8195
Cached	1440
Available	6444
Free	5164

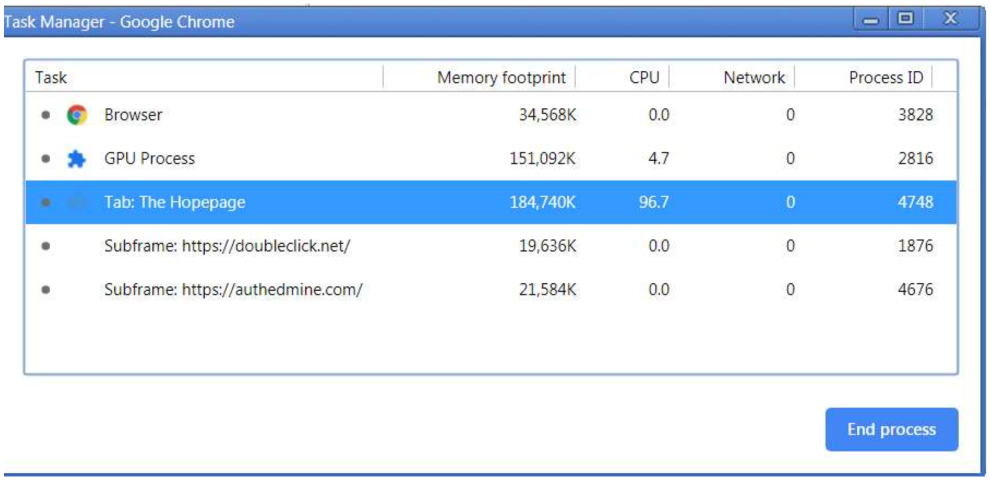
Kernel Memory (MB)	
Paged	144
Nonpaged	56

System	
Handles	17419
Threads	720
Processes	57
Up Time	0:00:31:05
Commit (GB)	1 / 16

Processes: 57 CPU Usage: 64% Physical Memory: 21%

Chrome Task Manager

- Open the Chrome Task Manager by using the Shift+ESC keyboard combination
- Or from the Chrome menu, then More Tools, and then Chrome Task Manager.



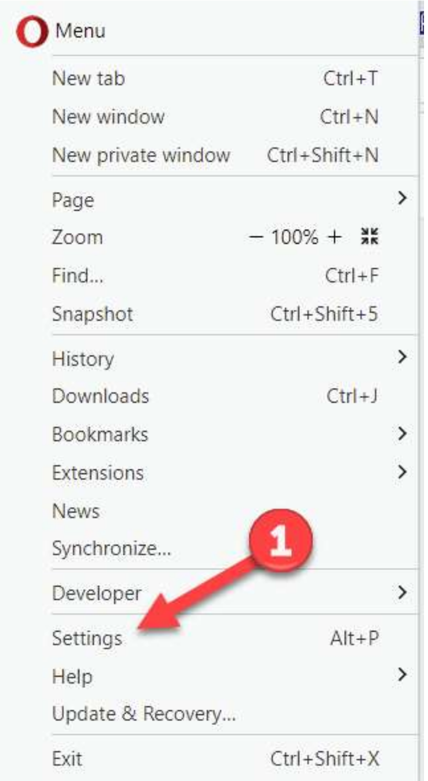
Task Manager - Google Chrome

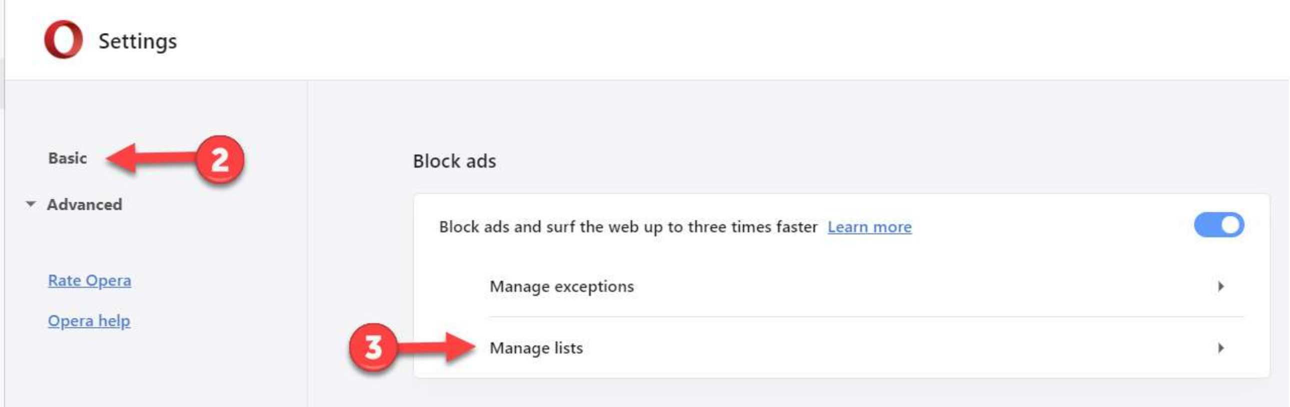
Task	Memory footprint	CPU	Network	Process ID
Browser	34,568K	0.0	0	3828
GPU Process	151,092K	4.7	0	2816
Tab: The Hopepage	184,740K	96.7	0	4748
Subframe: https://doubleclick.net/	19,636K	0.0	0	1876
Subframe: https://authedmine.com/	21,584K	0.0	0	4676

End user protection

- Use the Task Manager (Windows) or Activity Monitor (Mac OS X)
- Disable JavaScript in the browser
- Browser extensions like “No Coin” are available on Google Chrome and Firefox. Opera has it enabled by default.
- Install third-party malware detection and anti-virus software
- Update and patch software

Opera



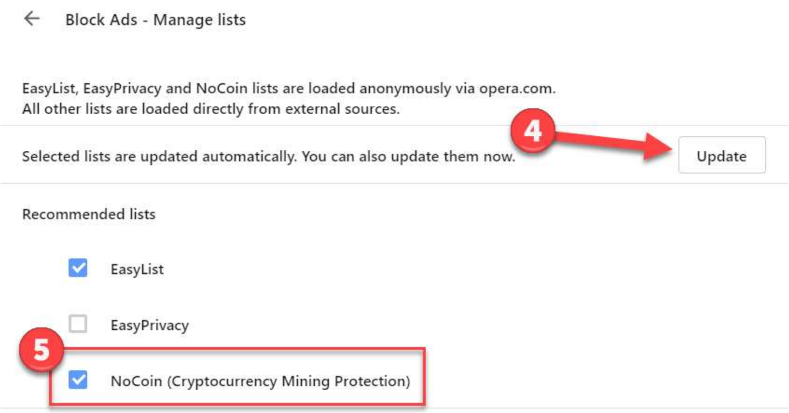


Block ads

Block ads and surf the web up to three times faster Learn more

Manage exceptions

Manage lists



Block Ads - Manage lists

EasyList, EasyPrivacy and NoCoin lists are loaded anonymously via opera.com.
All other lists are loaded directly from external sources.

Selected lists are updated automatically. You can also update them now.

Recommended lists

☑ EasyList

☐ EasyPrivacy

☑ NoCoin (Cryptocurrency Mining Protection)

Network protection

- Check vendor advisories and recommendations
- Update firewall rules
- Update Intrusion Detection System (IDS) rules
- Update and Patch all systems
- Block known crypto miner domains
  - https://gitlab.com/ZeroDot1/CoinBlockerLists
  - https://zerodot1.gitlab.io/CoinBlockerListsWeb/downloads.html
  - http://iplists.firehol.org

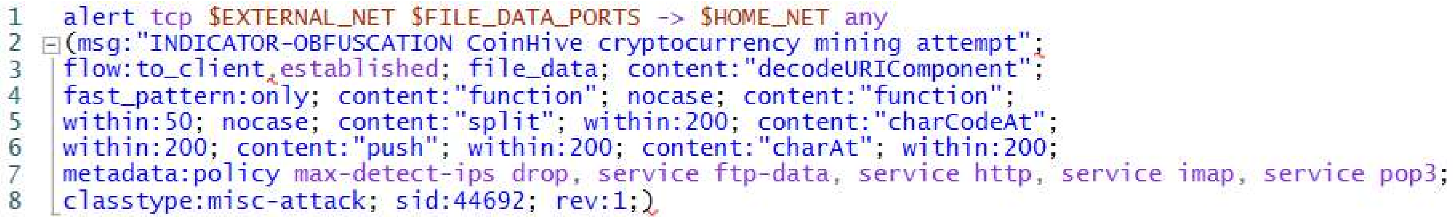
Network protection

- Snort rules dealing with cryptomining:
  - Blocking incoming clients, including downloads of miners:
    - 44692-44693, 45265-45268, 45809-45810, 45949-45952, 46365-46366, 46370-46372
  - Malware variants specifically known to mine crypto-currency:
    - 20035, 20057, 26395, 28399, 28410-28411, 29493-29494, 29666, 30551-30552, 31271-31273, 31531-31533,32013, 33149, 43467-43468, 44895-44899, 45468-45473, 45548, 45826-45827, 46238-46240
  - Identification and blocking of protocols used by cryptocurrency workers:
    - 26437, 40840-40842, 45417, 45549-45550, 45825, 45955

https://www.talosintelligence.com/resources/59 - accessed 9th Nov 2018

ISP Snort Rules

- If the number is
  - less than 1000000, it is a SourceFire rule
  - between 1000000 and 2000000, it is a snort community rule.
  - between 2000000 and 3000000 it comes from emergingthreats.net



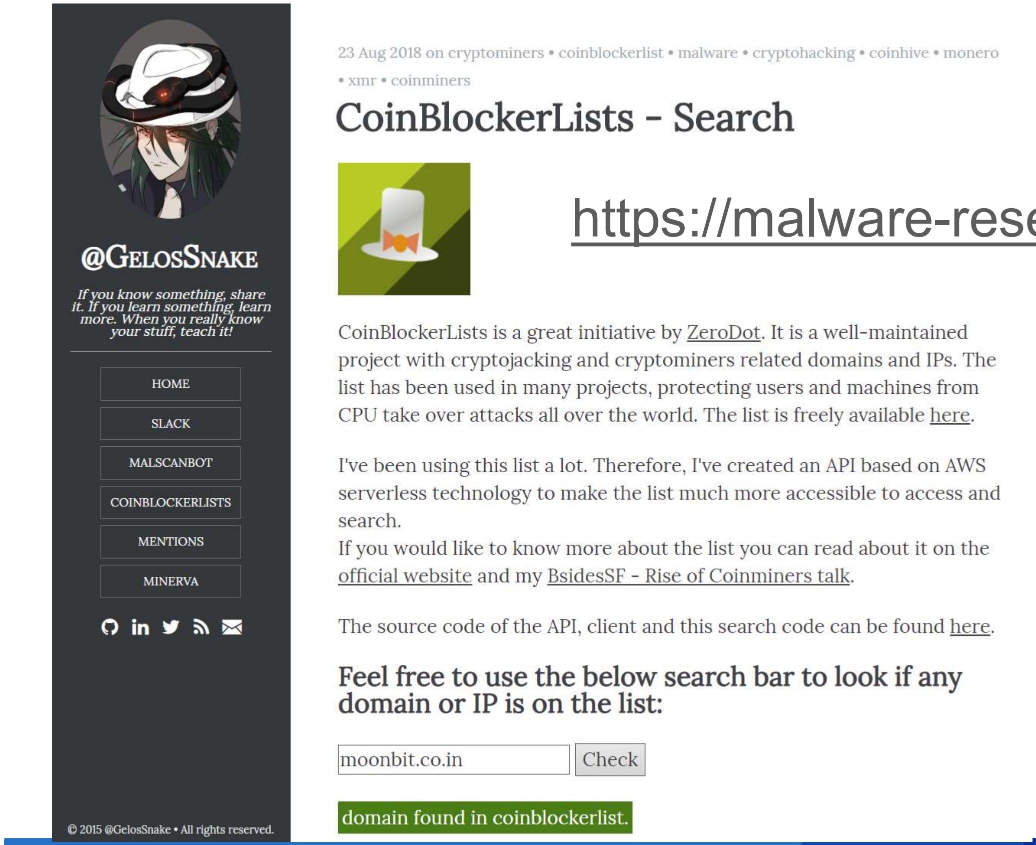
```
alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any
(msg:"INDICATOR-OBFUSCATION CoinHive cryptocurrency mining attempt";
flow:to_client,established; file_data; content:"decodeURIComponent";
fast_pattern:only; content:"function"; nocase; content:"function";
within:50; nocase; content:"split"; within:200; content:"charCodeAt";
within:200; content:"push"; within:200; content:"charAt"; within:200;
metadata:policy max-detect-ips drop, service ftp-data, service http, service imap, service pop3;
classtype:misc-attack; sid:44692; rev:1;)
```

```
grep -Hrn '44692' /etc/snort/rules
grep -Hrn '29666' /etc/snort/rules
grep -Hrn '45549' /etc/snort/rules
```

Update Snort

- mkdir ~/Downloads/snort
- cd ~/Downloads/snort
- wget http://192.168.30.1/Exercises/snortrules-snapshot-2983.tar.gz
- tar –xvf snortrules-snapshot-2983.tar.gz
- sudo mv etc /etc/snort
- sudo mv rules /etc/snort/rules
- sudo service snort restart

Confirm if site is on block list


@GelosSnake
If you know something, share it. If you learn something, learn more. When you really know your stuff, teach it!
HOME
SLACK
MALSCANBOT
COINBLOCKERLISTS
MENTIONS
MINERVA
© 2015 @GelosSnake • All rights reserved.

23 Aug 2018 on cryptominers • coinblockerlist • malware • cryptohacking • coinhive • monero • xmr • coinminers

CoinBlockerLists - Search

https://malware-research.org/coinblockerlists/

CoinBlockerLists is a great initiative by ZeroDot. It is a well-maintained project with cryptojacking and cryptominers related domains and IPs. The list has been used in many projects, protecting users and machines from CPU take over attacks all over the world. The list is freely available here.

I've been using this list a lot. Therefore, I've created an API based on AWS serverless technology to make the list much more accessible to access and search.
If you would like to know more about the list you can read about it on the official website and my BsidesSF - Rise of Coinminers talk.

The source code of the API, client and this search code can be found here.

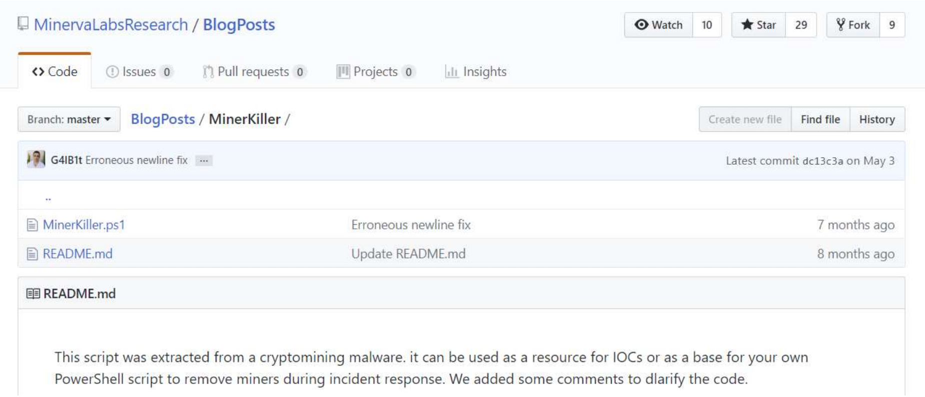
Feel free to use the below search bar to look if any domain or IP is on the list:

moonbit.co.in Check

domain found in coinblockerlist.

GhostMiner

- https://github.com/MinervaLabsResearch/BlogPosts/tree/master/MinerKiller



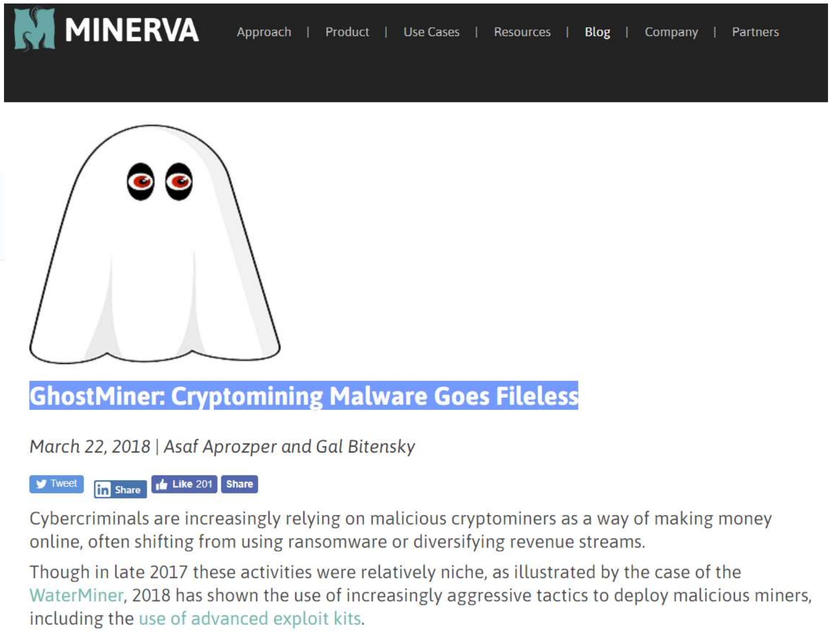
BlogPosts / MinerKiller /

G4lB1t Erroneous newline fix … Latest commit dc13c3a on May 3

..		
MinerKiller.ps1	Erroneous newline fix	7 months ago
README.md	Update README.md	8 months ago

README.md

This script was extracted from a cryptomining malware. it can be used as a resource for IOCs or as a base for your own PowerShell script to remove miners during incident response. We added some comments to dlarify the code.


MINERVA
Approach | Product | Use Cases | Resources | Blog | Company | Partners
Tweet
Share
Like 201
Share

GhostMiner: Cryptomining Malware Goes Fileless

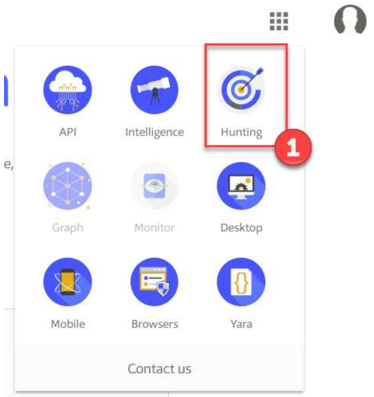
March 22, 2018 | Asaf Aprozper and Gal Bitensky

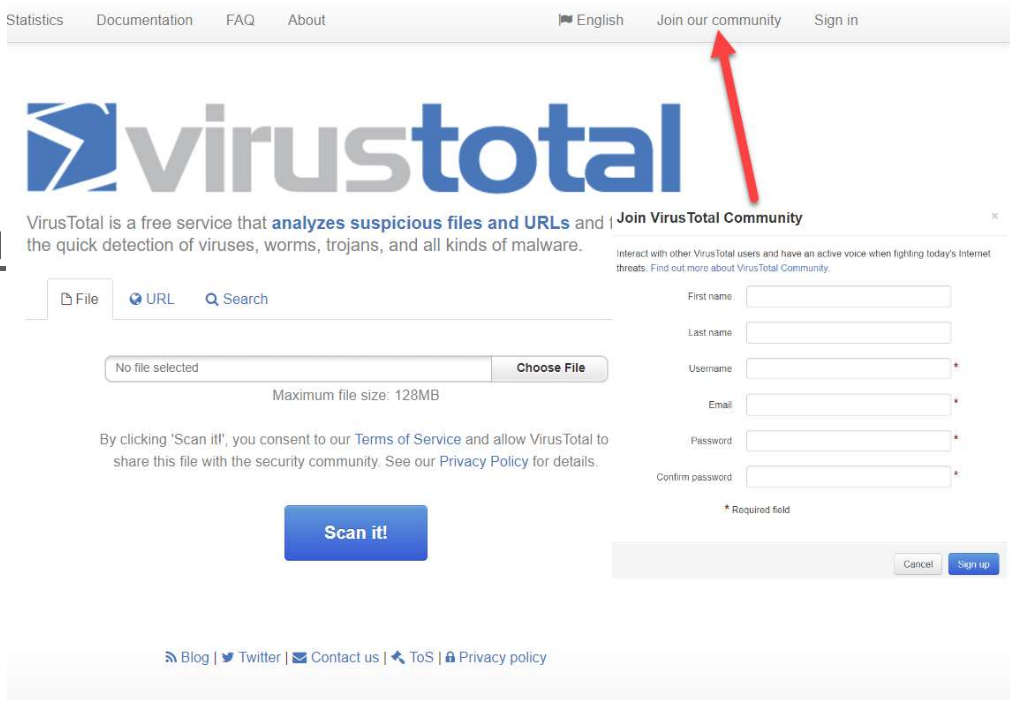
Cybercriminals are increasingly relying on malicious cryptominers as a way of making money online, often shifting from using ransomware or diversifying revenue streams.

Though in late 2017 these activities were relatively niche, as illustrated by the case of the WaterMiner, 2018 has shown the use of increasingly aggressive tactics to deploy malicious miners, including the use of advanced exploit kits.

VirusTotal

- Create a free account
- https://www.virustotal.com





VirusTotal is a free service that **analyzes suspicious files and URLs** and the quick detection of viruses, worms, trojans, and all kinds of malware.

No file selected

Maximum file size: 128MB

By clicking 'Scan it!', you consent to our Terms of Service and allow VirusTotal to share this file with the security community. See our Privacy Policy for details.

Join VirusTotal Community

Interact with other VirusTotal users and have an active voice when fighting today's Internet threats. Find out more about VirusTotal Community.

First name

Last name

Username *

Email *

Password *

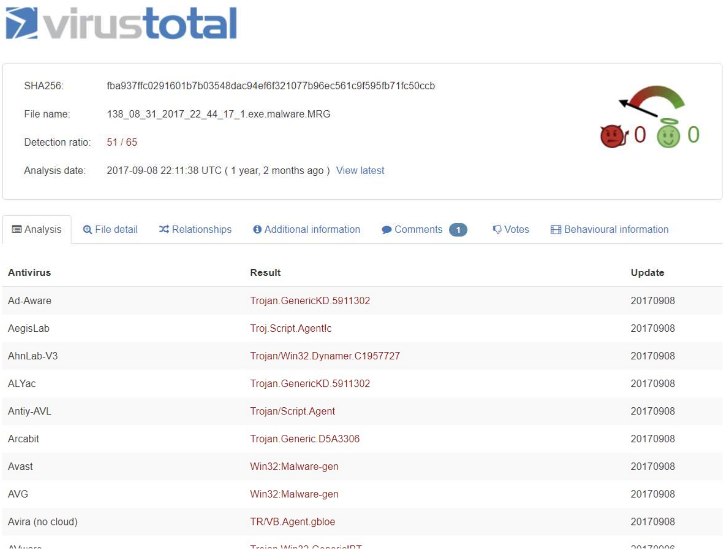
Confirm password *

* Required field

https://www.virustotal.com/learn/watch/

VirusTotal

- Use the search feature to find information about a threat
- Search term
  - fba937ffc0291601_sdat.exe



SHA256: fba937ffc0291601b7b03548dac94ef6f321077b96ec561c9f595fb71fc50ccb

File name: 138_08_31_2017_22_44_17_1.exe.malware.MRG

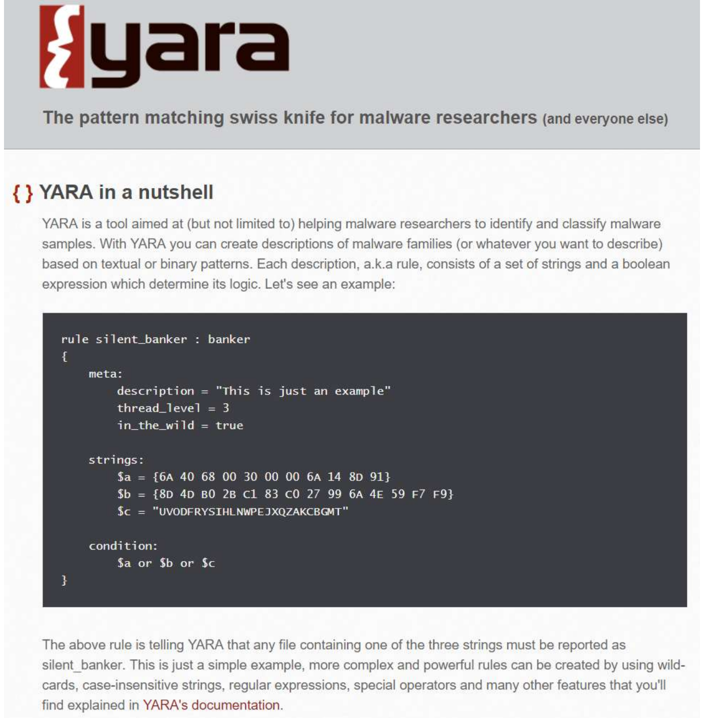
Detection ratio: 51 / 65

Analysis date: 2017-09-08 22:11:38 UTC (1 year, 2 months ago) View latest

Antivirus	Result	Update
Ad-Aware	Trojan.GenericKD.5911302	20170908
AegisLab	Troj.Script.Agent!c	20170908
AhnLab-V3	Trojan/Win32.Dynamer.C1957727	20170908
ALYac	Trojan.GenericKD.5911302	20170908
Antiy-AVL	Trojan/Script.Agent	20170908
Arcabit	Trojan.Generic.D5A3306	20170908
Avast	Win32:Malware-gen	20170908
AVG	Win32:Malware-gen	20170908
Avira (no cloud)	TR/VB.Agent.gbloe	20170908
AVware	Trojan.Win32.GenericIBT	20170906

https://www.virustotal.com/en/file/fba937ffc0291601b7b03548dac94ef6f321077b96ec561c9f595fb71fc50ccb/analysis/1504908698/

YARA – pattern matching for Malware



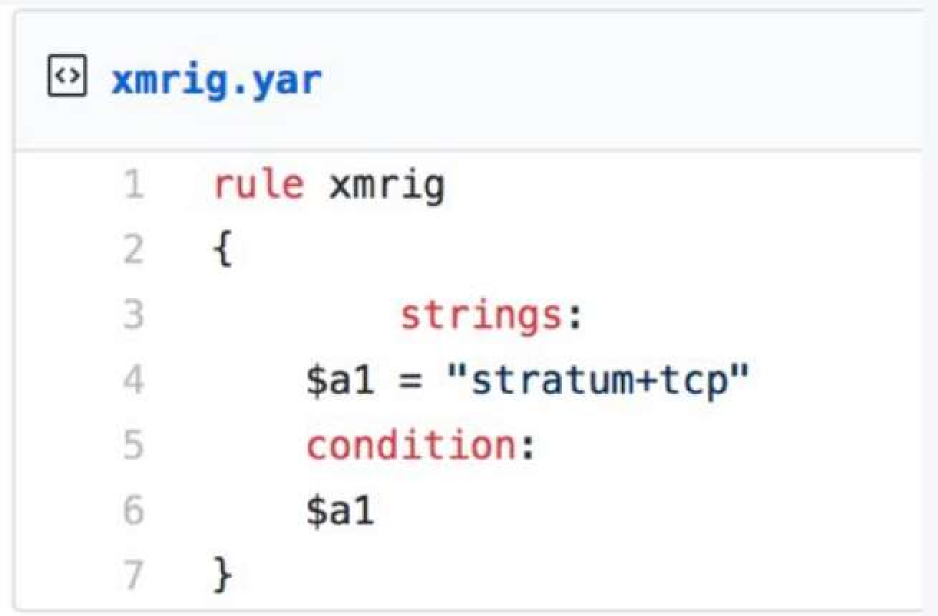
The pattern matching swiss knife for malware researchers (and everyone else)

{ } YARA in a nutshell

YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns. Each description, a.k.a rule, consists of a set of strings and a boolean expression which determine its logic. Let's see an example:

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        thread_level = 3
        in_the_wild = true

    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

    condition:
        $a or $b or $c
}
```

The above rule is telling YARA that any file containing one of the three strings must be reported as silent_banker. This is just a simple example, more complex and powerful rules can be created by using wild-cards, case-insensitive strings, regular expressions, special operators and many other features that you'll find explained in YARA's documentation.



```
rule xmrig
{
            strings:
        $a1 = "stratum+tcp"
        condition:
        $a1
}
```

https://virustotal.github.io/yara/ - accessed 16th Nov 2018

References

- https://isc.sans.edu/forums/diary/Cryptominer+Delivered+Though+Compromized+JavaScript+File/23870/
- https://isc.sans.org/forums/diary/Crypto+Mining+in+a+Windows+Headless+Browser/24078/
- https://www.ncsc.gov.uk/report/weekly-threat-report-9th-november-2018
- https://blog.talosintelligence.com/2018/07/blocking-cryptomining.html
- https://tools.cisco.com/security/center/viewAlert.x?alertId=56836

References

- https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/security-101-the-impact-of-cryptocurrency-mining-malware
- https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-mining-malware-2018-new-menace/
- https://www.androidsage.com/2018/07/27/how-to-block-crypto-mining-on-android-windows-linux-macos-and-ios-devices/
- https://www.bleepingcomputer.com/news/security/the-internet-is-rife-with-in-browser-miners-and-its-getting-worse-each-day/

References

- https://badpackets.net/how-to-find-cryptojacking-malware/
- https://null-byte.wonderhowto.com/how-to/inject-coinhive-miners-into-public-wi-fi-hotspots-0182250/
- https://blogs.cisco.com/security/cryptojacking-hijacking-your-computer-resources
- https://www.enisa.europa.eu/publications/info-notes/cryptojacking-cryptomining-in-the-browser
- https://99bitcoins.com/webmining-monetize-your-website-through-user-browsers/

References

- https://arxiv.org/pdf/1803.02887.pdf
- https://malware-research.org/bsidessf-rise-of-coinminers/

Any questions?