# A look into Drupalgeddon's client-side attacks | Malwarebytes Labs

By Jérôme Segura

Published: 2018-05-17 · Archived: 2026-04-05 17:32:15 UTC

Drupal is one of the most popular Content Management Systems (CMS), along with WordPress and Joomla. In late March 2018, Drupal was affected by a major remote code execution vulnerability (CVE-2018-7600) followed by yet another (CVE-2018-7602) almost a month later, both aptly nicknamed Drupalgeddon 2 and Drupalgeddon 3.

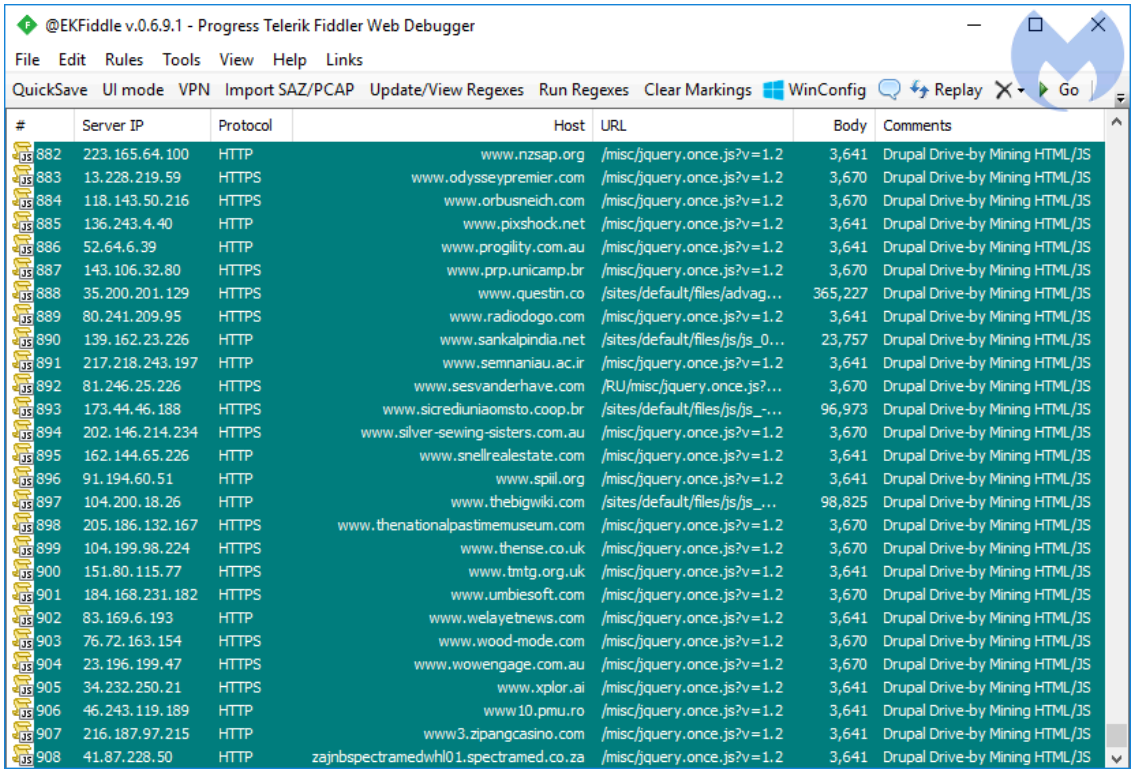
These back-to-back vulnerabilities were accompanied by proof of concepts that translated into almost immediate real-world attacks. For many website owners, this situation was frustrating because the window of time to patch is getting considerably smaller. Additionally, updating or upgrading Drupal (or any other CMS for that matter) may have side effects, such as broken templates or functionality, which is why you need to make a full back up and test the changes in the staging environment before moving to production.

Rolling out a CMS is usually the easy part. Maintaining it is where most problems occur due to lack of knowledge, fear of breaking something, and, of course, costs. While this is an earned responsibility for each site owner to do due diligence with their web properties, the outcome is typically websites being severely out of date and exploited, often more than once.

### Sample set and web crawl

We decided to choose a number web properties that had not yet been validated (including all versions of Drupal, vulnerable or not). Our main source of URLs came from Shodan and was complemented by PublicWWW, for a total of roughly 80,000 URLs to crawl. We were surprised to start hitting compromised sites quickly into the process and were able to confirm around 900 injected web properties.

Many of the results were servers hosted on Amazon or other cloud providers that were most likely set up for testing purposes (staging) and never removed or upgraded. Thankfully, they received little to no traffic. The other domains we encountered spanned a variety of verticals and languages, with one common denominator: an outdated version (usually severely outdated) of the Drupal CMS.




| # | Server IP | Protocol | Host | URL | Body | Comments |
|---|---|---|---|---|---|---|
| 882 | 223.165.64.100 | HTTP | www.nzsap.org | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |
| 883 | 13.228.219.59 | HTTPS | www.odysseypremier.com | /misc/jquery.once.js?v=1.2 | 3,670 | Drupal Drive-by Mining HTML/JS |
| 884 | 118.143.50.216 | HTTPS | www.orbusneich.com | /misc/jquery.once.js?v=1.2 | 3,670 | Drupal Drive-by Mining HTML/JS |
| 885 | 136.243.4.40 | HTTP | www.pixshock.net | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |
| 886 | 52.64.6.39 | HTTP | www.progility.com.au | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |
| 887 | 143.106.32.80 | HTTPS | www.prp.unicamp.br | /misc/jquery.once.js?v=1.2 | 3,670 | Drupal Drive-by Mining HTML/JS |
| 888 | 35.200.201.129 | HTTPS | www.questin.co | /sites/default/files/advag... | 365,227 | Drupal Drive-by Mining HTML/JS |
| 889 | 80.241.209.95 | HTTPS | www.radiodogo.com | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |
| 890 | 139.162.23.226 | HTTP | www.sankalpindia.net | /sites/default/files/js/js_0... | 23,757 | Drupal Drive-by Mining HTML/JS |
| 891 | 217.218.243.197 | HTTP | www.semnaniau.ac.ir | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |
| 892 | 81.246.25.226 | HTTPS | www.sesvanderhave.com | /RU/misc/jquery.once.js?... | 3,670 | Drupal Drive-by Mining HTML/JS |
| 893 | 173.44.46.188 | HTTPS | www.sicrediuniaomsto.coop.br | /sites/default/files/js/js_-... | 96,973 | Drupal Drive-by Mining HTML/JS |
| 894 | 202.146.214.234 | HTTPS | www.silver-sewing-sisters.com.au | /misc/jquery.once.js?v=1.2 | 3,670 | Drupal Drive-by Mining HTML/JS |
| 895 | 162.144.65.226 | HTTP | www.snellrealestate.com | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |
| 896 | 91.194.60.51 | HTTP | www.spiil.org | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |
| 897 | 104.200.18.26 | HTTP | www.thebigwiki.com | /sites/default/files/js/js_... | 98,825 | Drupal Drive-by Mining HTML/JS |
| 898 | 205.186.132.167 | HTTPS | www.thenationalpastimemuseum.com | /misc/jquery.once.js?v=1.2 | 3,670 | Drupal Drive-by Mining HTML/JS |
| 899 | 104.199.98.224 | HTTPS | www.thense.co.uk | /misc/jquery.once.js?v=1.2 | 3,670 | Drupal Drive-by Mining HTML/JS |
| 900 | 151.80.115.77 | HTTPS | www.tmtg.org.uk | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |
| 901 | 184.168.231.182 | HTTPS | www.umbiesoft.com | /misc/jquery.once.js?v=1.2 | 3,670 | Drupal Drive-by Mining HTML/JS |
| 902 | 83.169.6.193 | HTTP | www.welayetnews.com | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |
| 903 | 76.72.163.154 | HTTPS | www.wood-mode.com | /misc/jquery.once.js?v=1.2 | 3,670 | Drupal Drive-by Mining HTML/JS |
| 904 | 23.196.199.47 | HTTPS | www.wowengage.com.au | /misc/jquery.once.js?v=1.2 | 3,670 | Drupal Drive-by Mining HTML/JS |
| 905 | 34.232.250.21 | HTTPS | www.xplor.ai | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |
| 906 | 46.243.119.189 | HTTP | www10.pmu.ro | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |
| 907 | 216.187.97.215 | HTTP | www3.zipangcasino.com | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |
| 908 | 41.87.228.50 | HTTP | zajnbspectramedwhl01.spectramed.co.za | /misc/jquery.once.js?v=1.2 | 3,641 | Drupal Drive-by Mining HTML/JS |

*Figure 1: Crawling and flagging compromised Drupal sites using Fiddler*

## Drupal versions

At the time of this writing, there are two recommended releases for Drupal. Version 8.x.x is the latest and greatest with some new features, while 7.x.x is considered the most stable and compatible version, especially when it comes to themes.

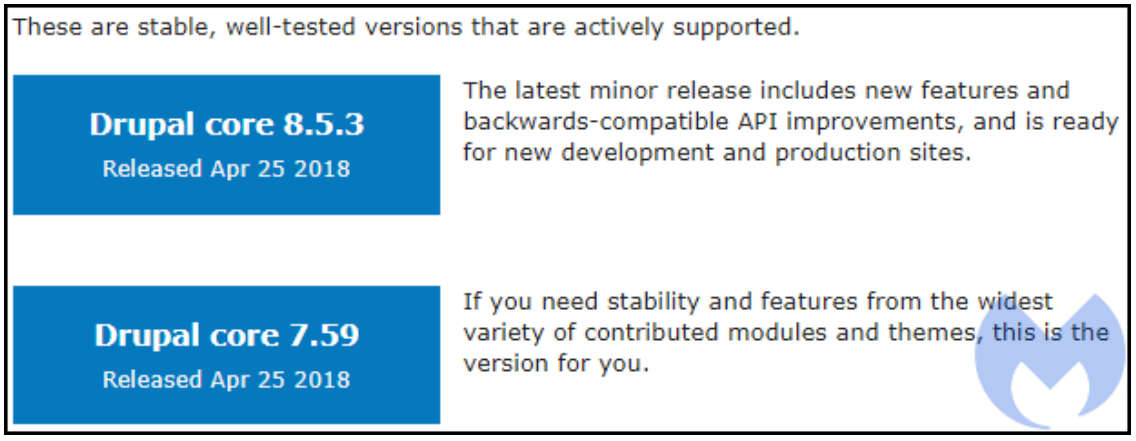



*Figure 2: Drupal's two main supported branches*

Almost half the sites we flagged as compromised were running Drupal version 7.5.x, while version 7.3.x still represented about 30 percent, a fairly high number considering it was last updated in August 2015. Many security flaws have been discovered (and exploited) since then.

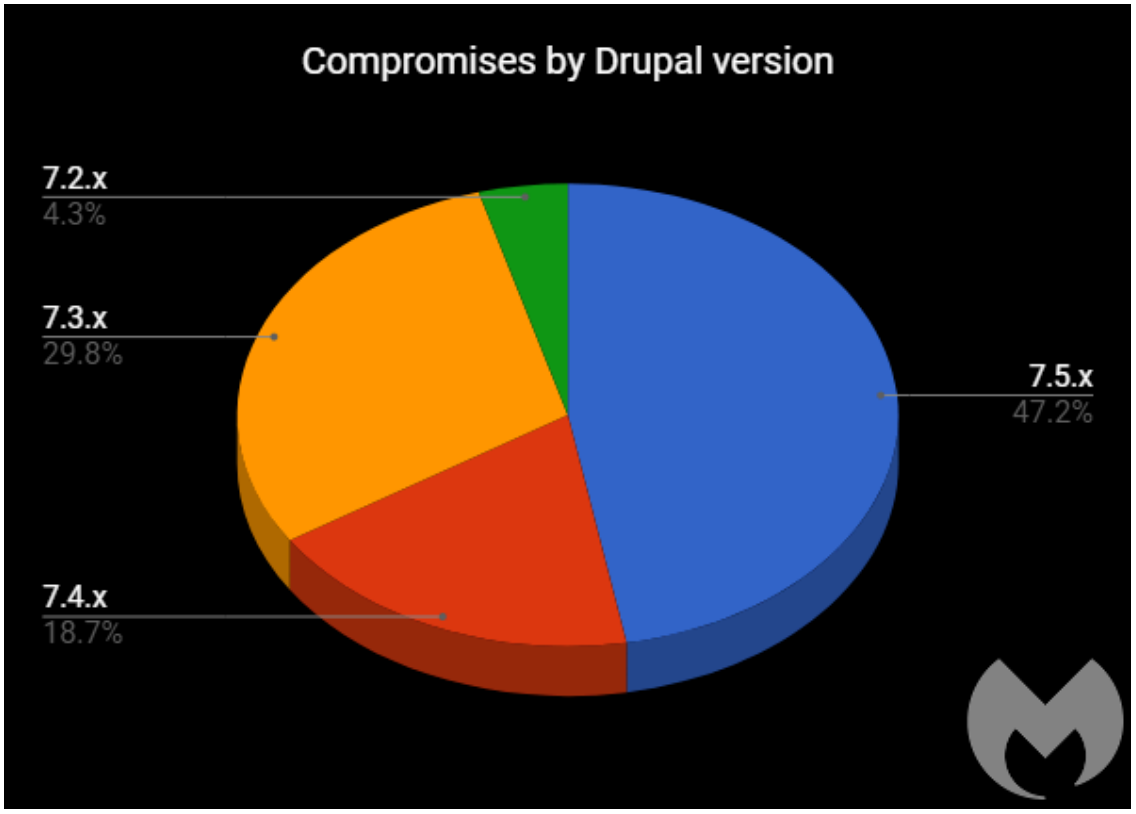



*Figure 3: Percentage of compromised sites belonging to a particular Drupal version*

## Payloads

A large number of Drupal sites that have been hacked via these two recent exploits were also infected with server-side malware, in particular with XMRig cryptocurrency miners. However, in this post we will focus on the client-side effects of those compromises. Neither are exclusive though, and one should expect that a hacked site could be performing malicious actions on both server and client side.

Unsurprisingly, web miners were by far the most common type of injection we noticed. But we also came across a few different social engineering campaigns.

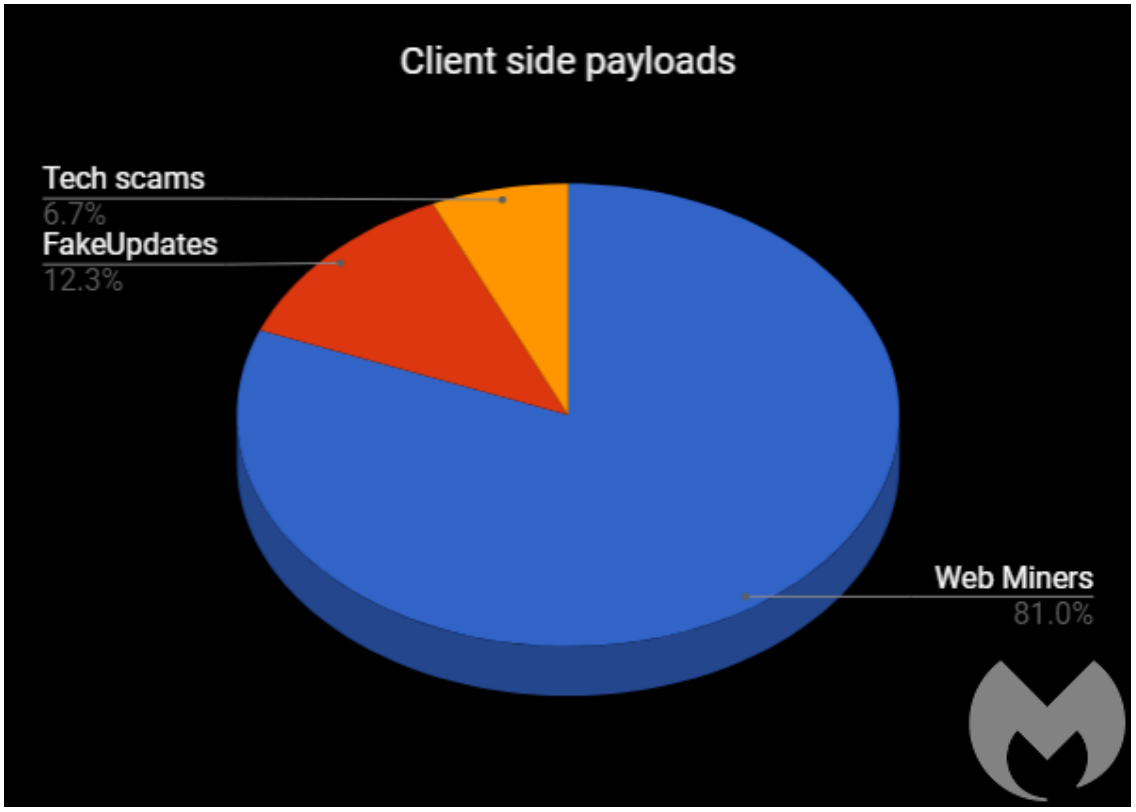



*Figure 4: Breakdown of the most common payloads*

**Web miners**

Drive-by mining attacks went though the roof in the fall of 2017 but slowed down somewhat at the beginning of the year. It's safe to say that the recent Drupal vulnerabilities have added fuel to the fire and resulted in increased activity. Coinhive injections remain by far the most popular choice, although public or private Monero pools are gaining traction as well.

We are seeing the same campaign that was already documented by other researchers in early March and is ensnaring more victims by the day.

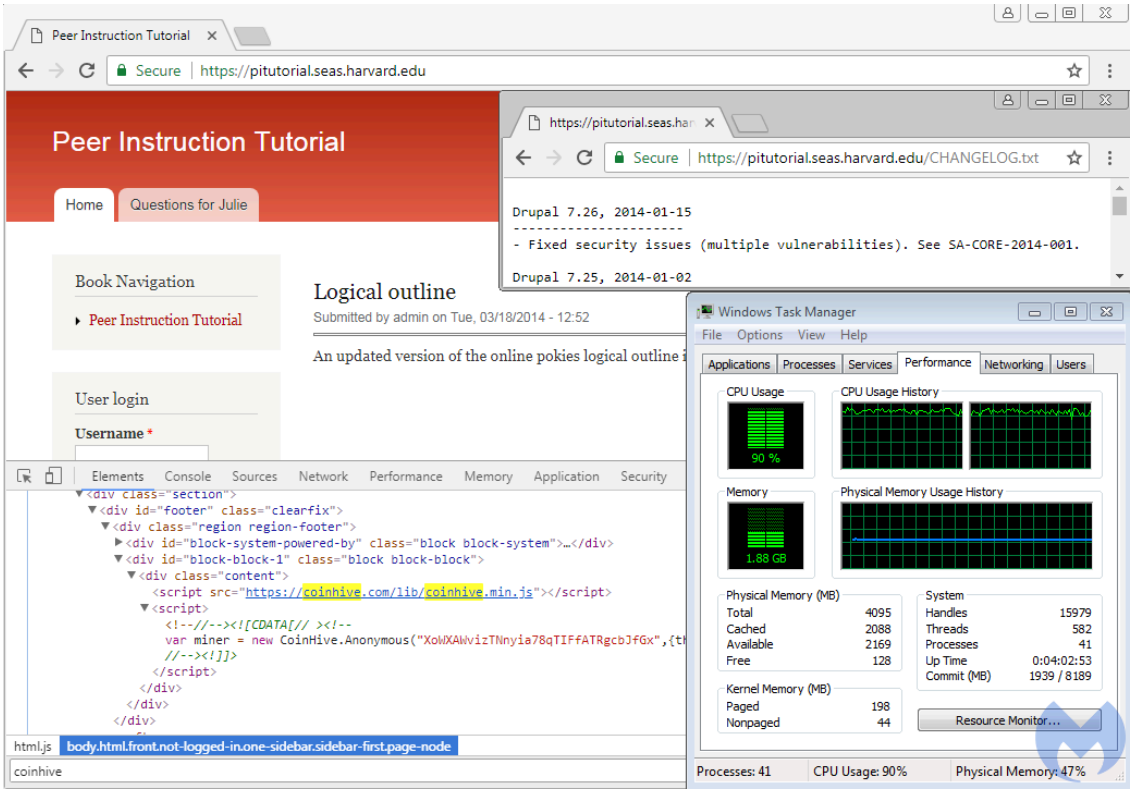



*Figure 5: A subdomain of Harvard University's main site mining Monero*

**Fake updates**

This campaign of fake browser updates we documented earlier is still going strong. It distributes a password stealer of Remote Administration Tool (RAT).

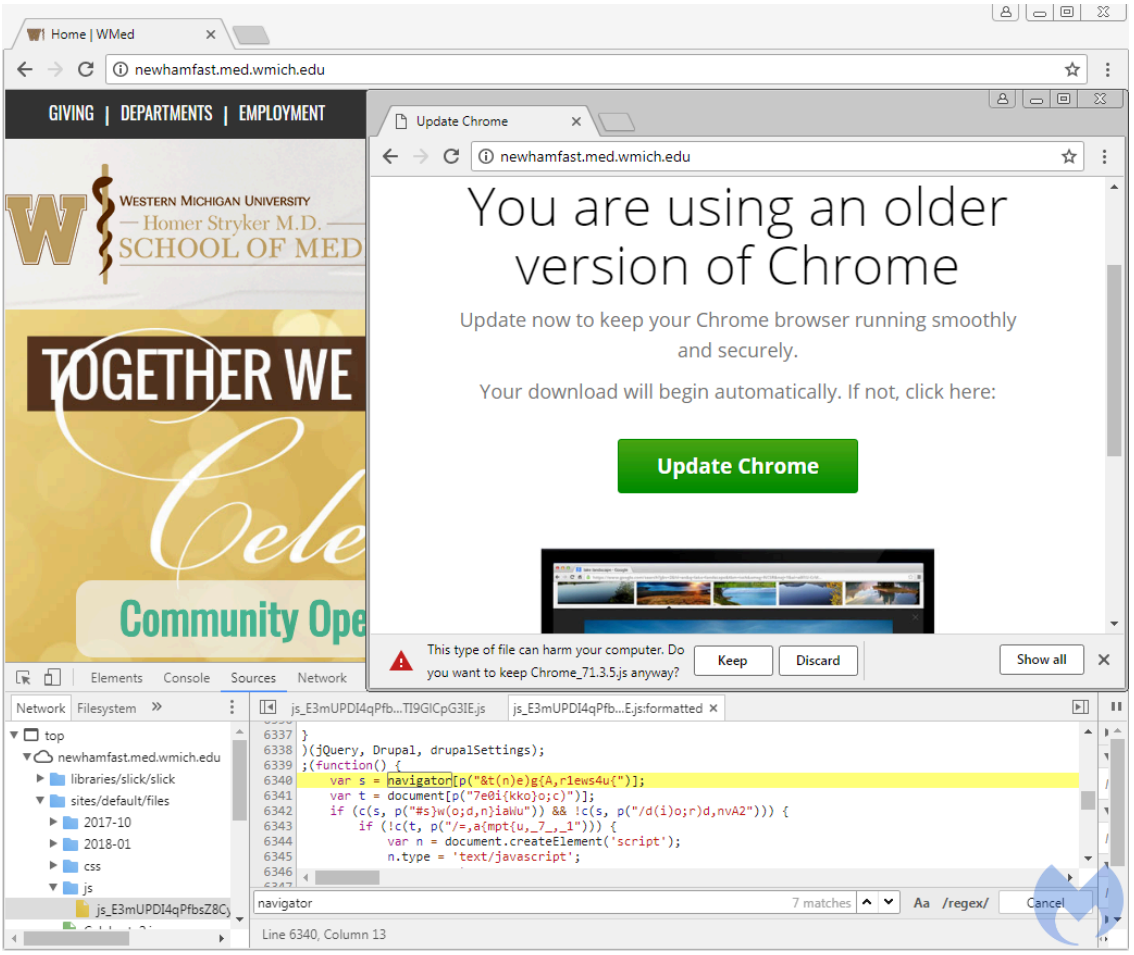



*Figure 6: A compromised Drupal site pushing a fake Chrome update*

**Tech support scams (browlocks)**

Redirections to browser locker pages—a typical approach for unveiling tech support scams. The most common redirection we were able to document involved an intermediary site redirecting to browser locker pages using the .TK Top Level Domain (TLD) name.

```
mysimplename[.]com/si.php window.location.replace("http://hispaintinghad[.]tk/index/?1641501770611")
```

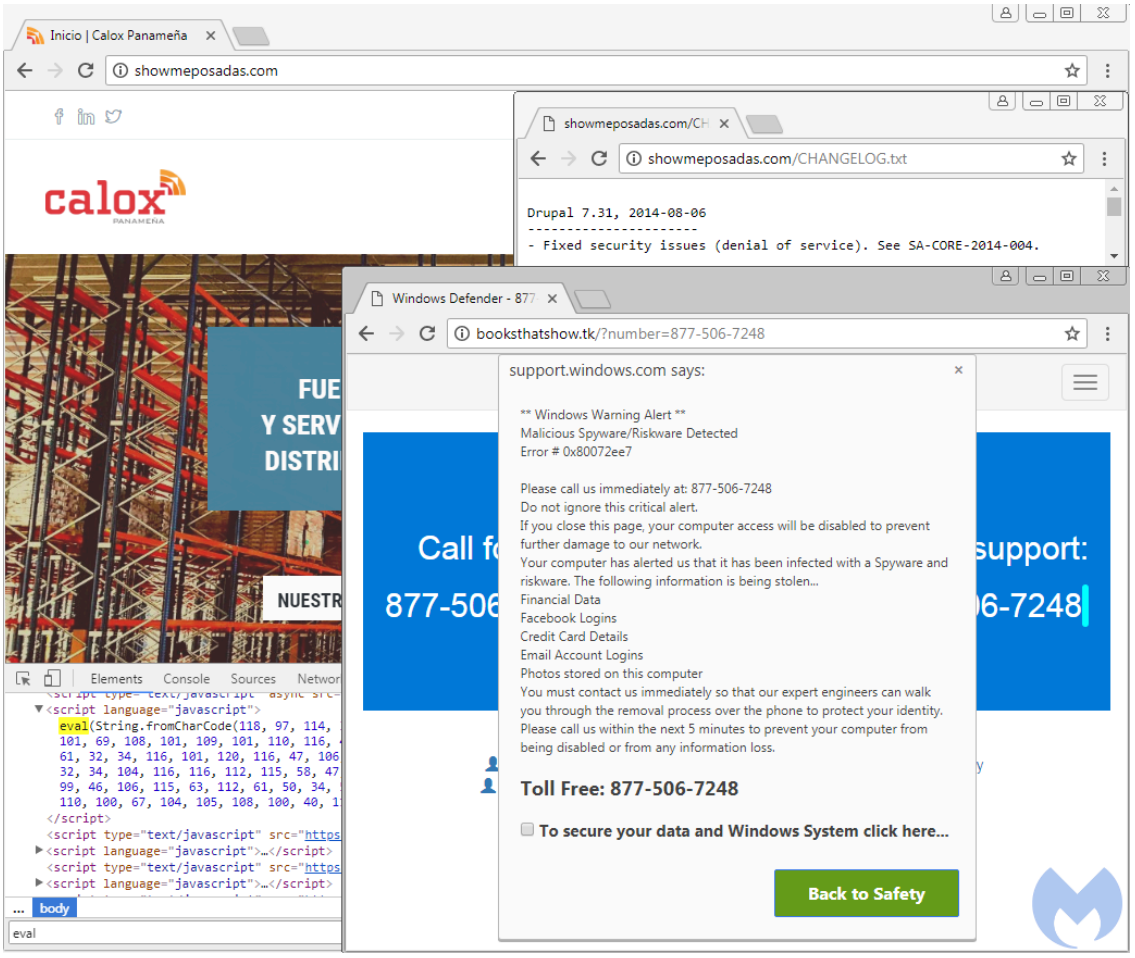



*Figure 7: A compromised Drupal host redirecting to a browser locker page*

## Web miners and injected code

We collected different types of code injection, from simple and clear text to long obfuscated blurbs. It's worth noting that in many cases the code is dynamic—most likely a technique to evade detection.

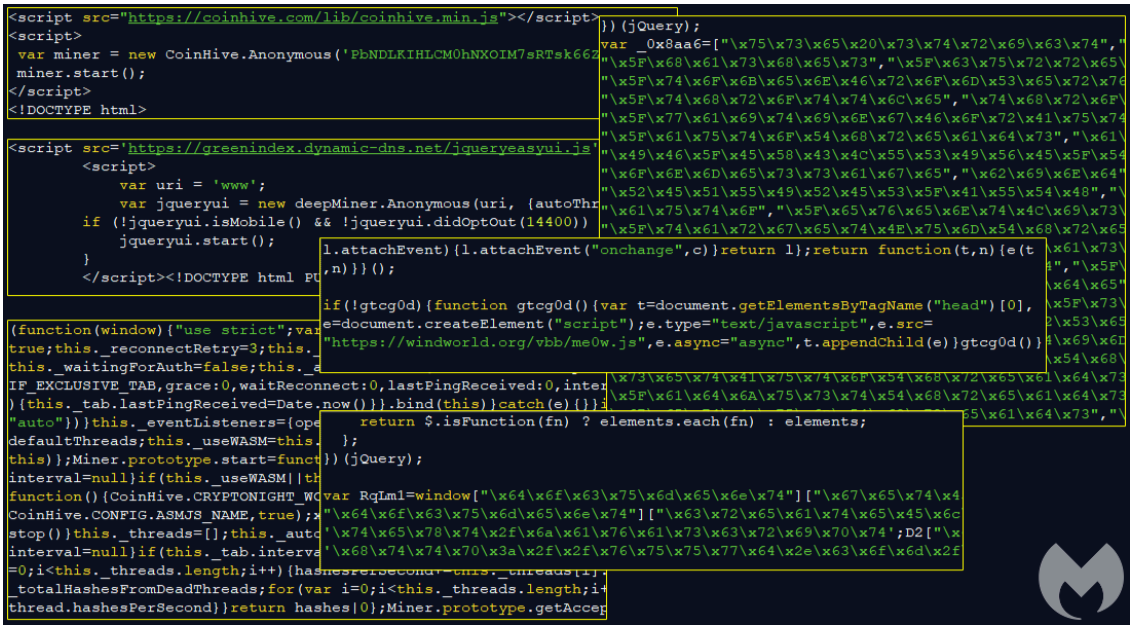


*Figure 8: Collage of some of the most common miner injections*

## Snapshots

The following are some examples of compromised sites sorted by category. We have contacted all affected parties to let them know their resources are being used by criminals to generate profit from malicious cryptomining or malware infections.

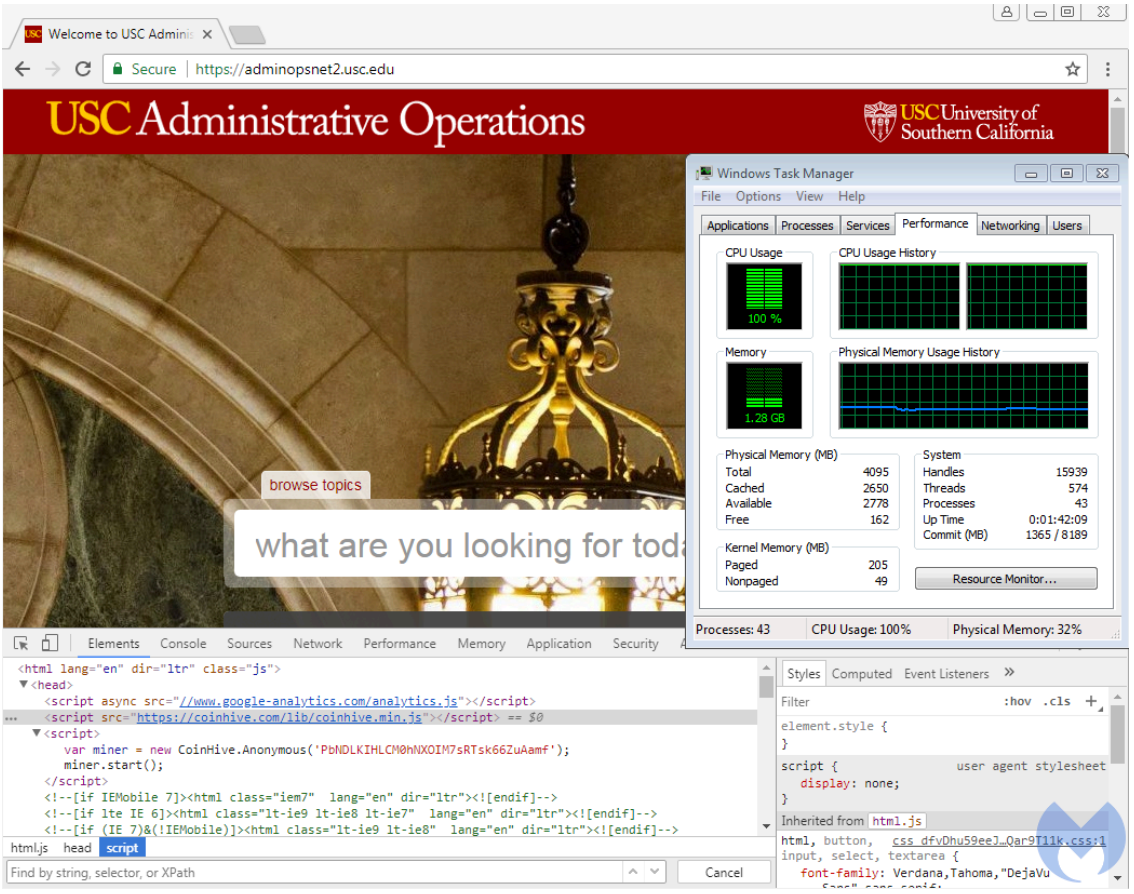



*Figure 9: Education (University of Southern California)*

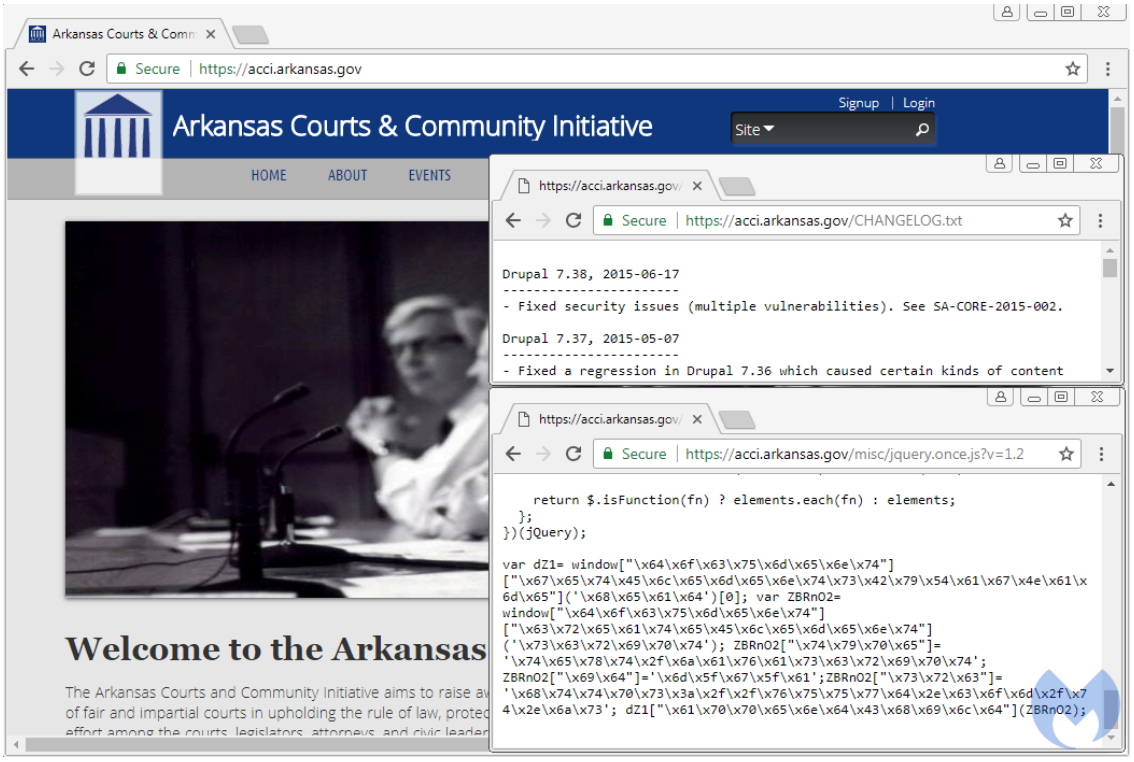



*Figure 10: Government (Arkansas Courts & Community Initiative)*

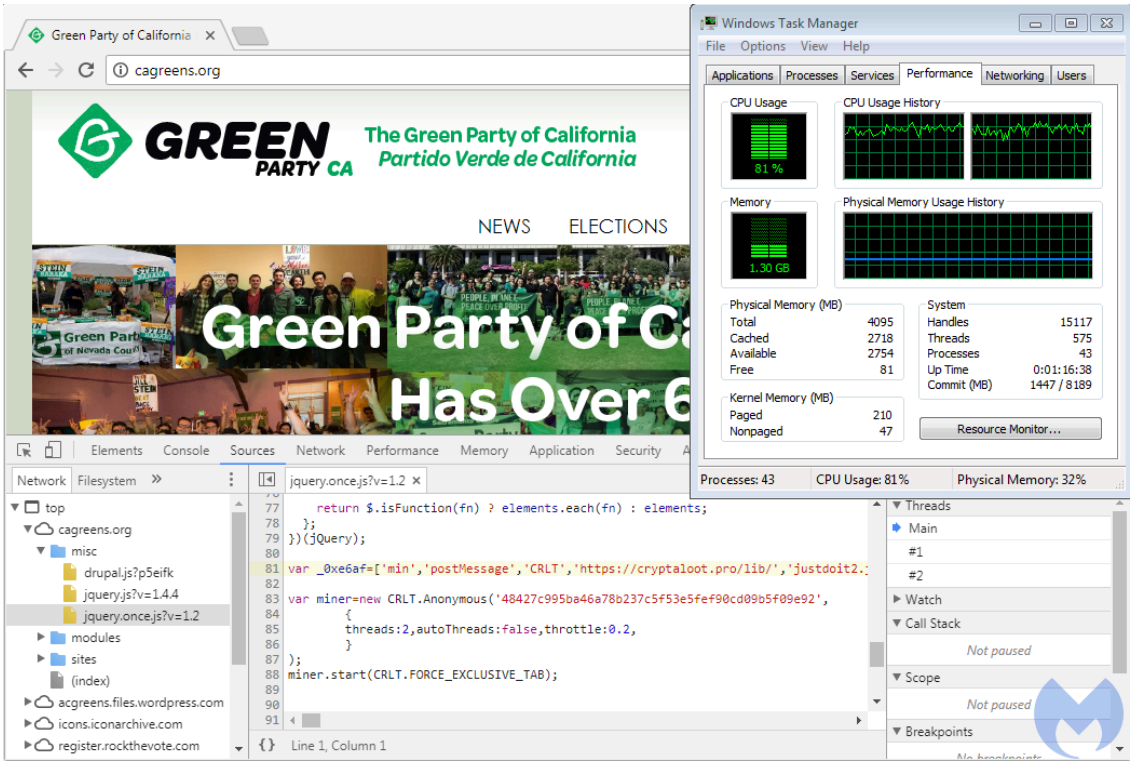



*Figure 11: Political party (Green Party of California)*

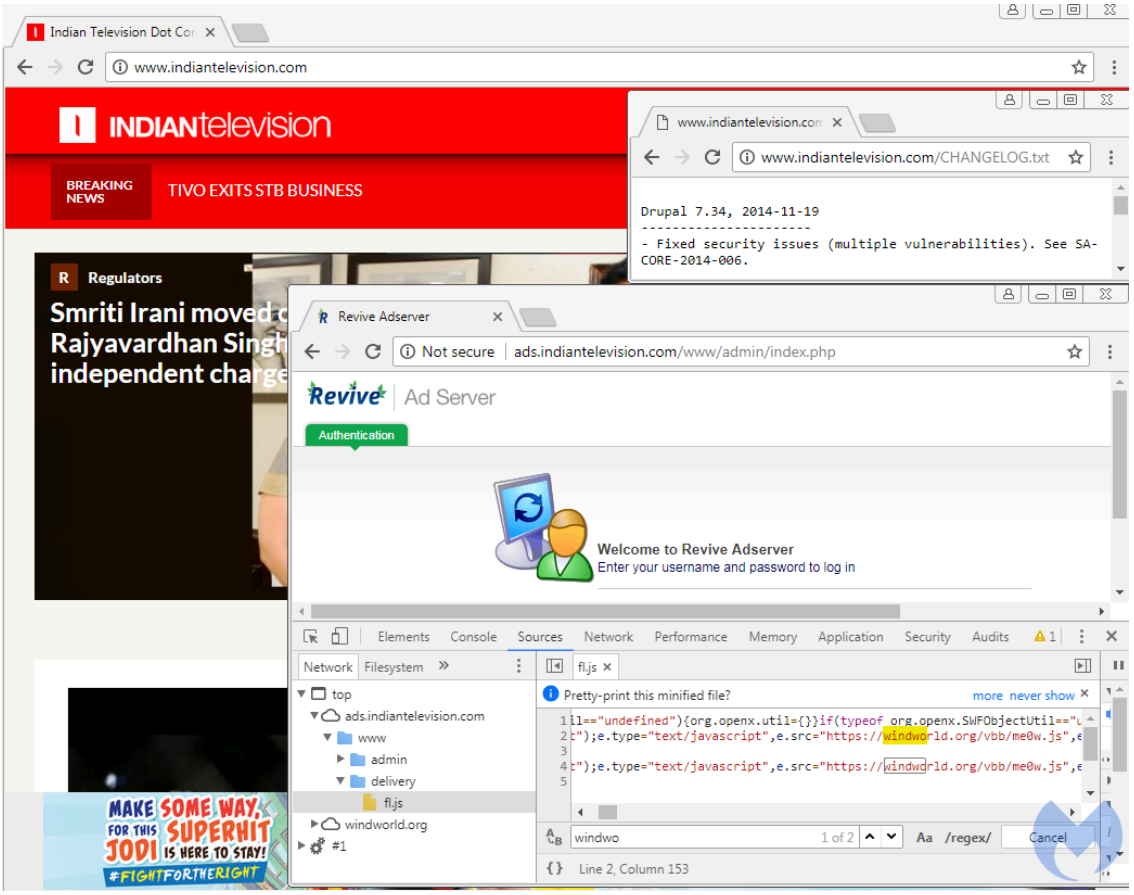



*Figure 12: Ad server (Indian TV Revive Ad server)*

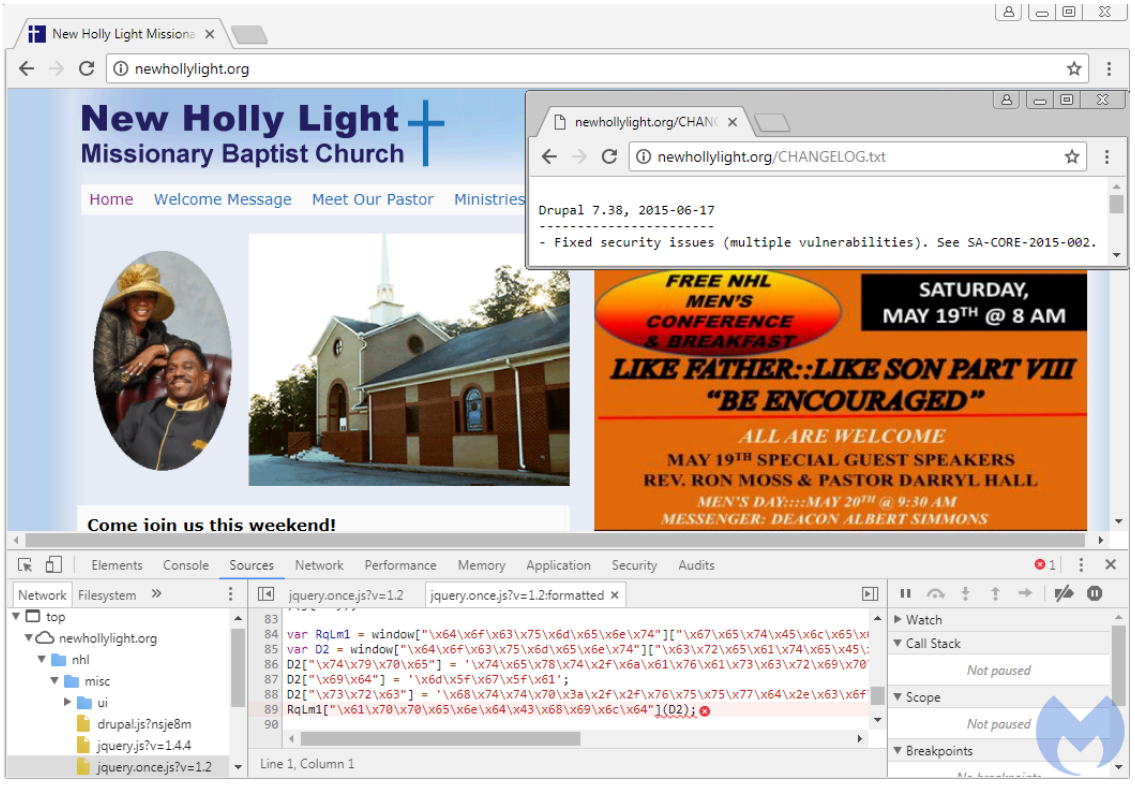



*Figure 13: Religion (New Holly Light)*

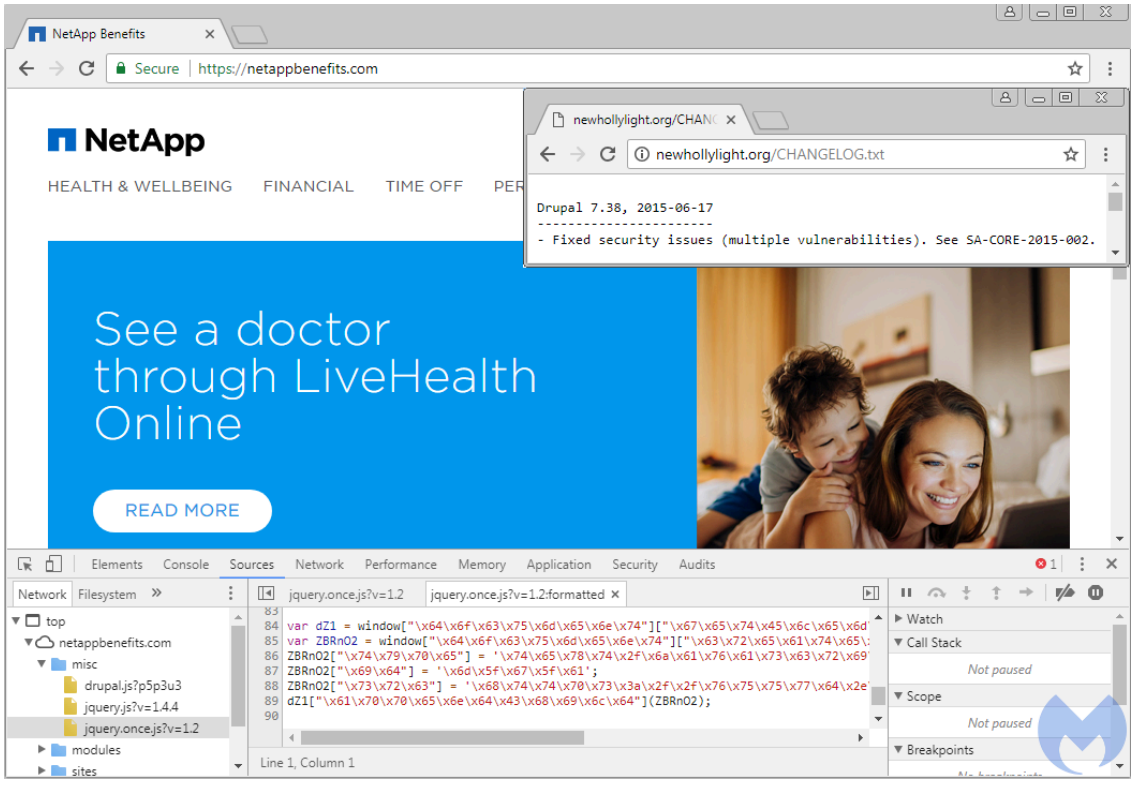



*Figure 14: Health (NetApp Benefits)*

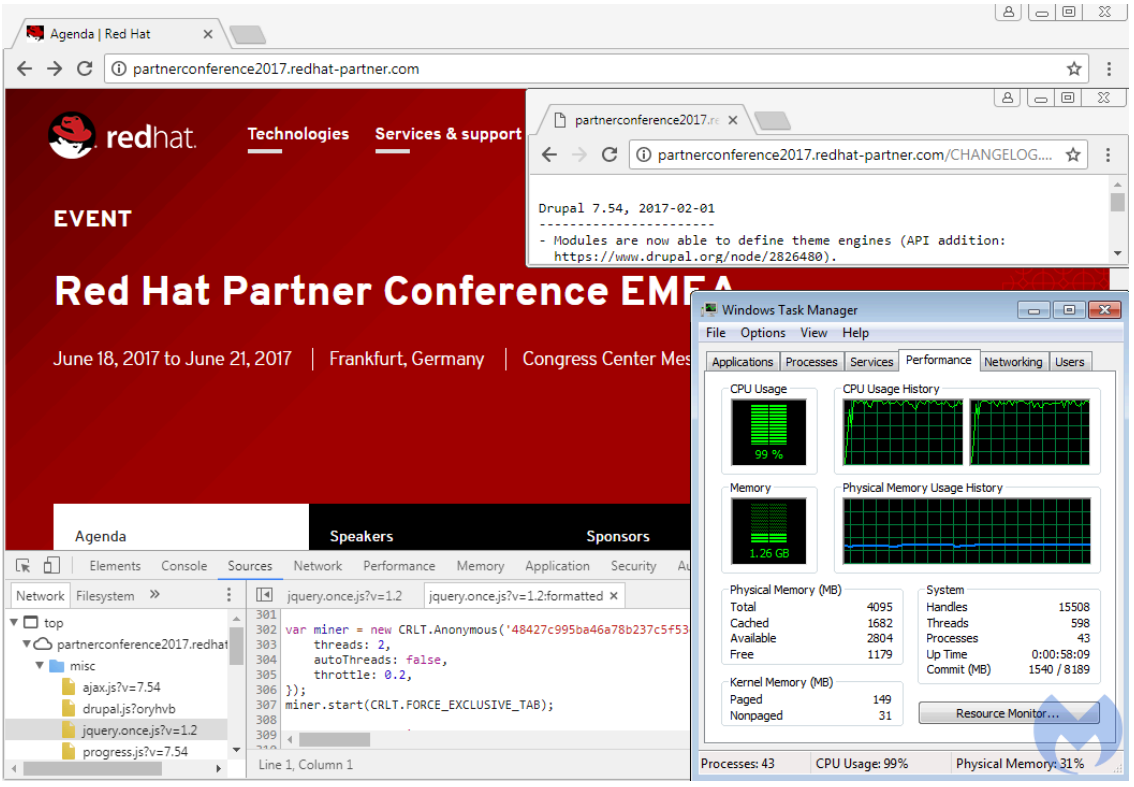



*Figure 15: Conferences (Red Hat partner conference)*

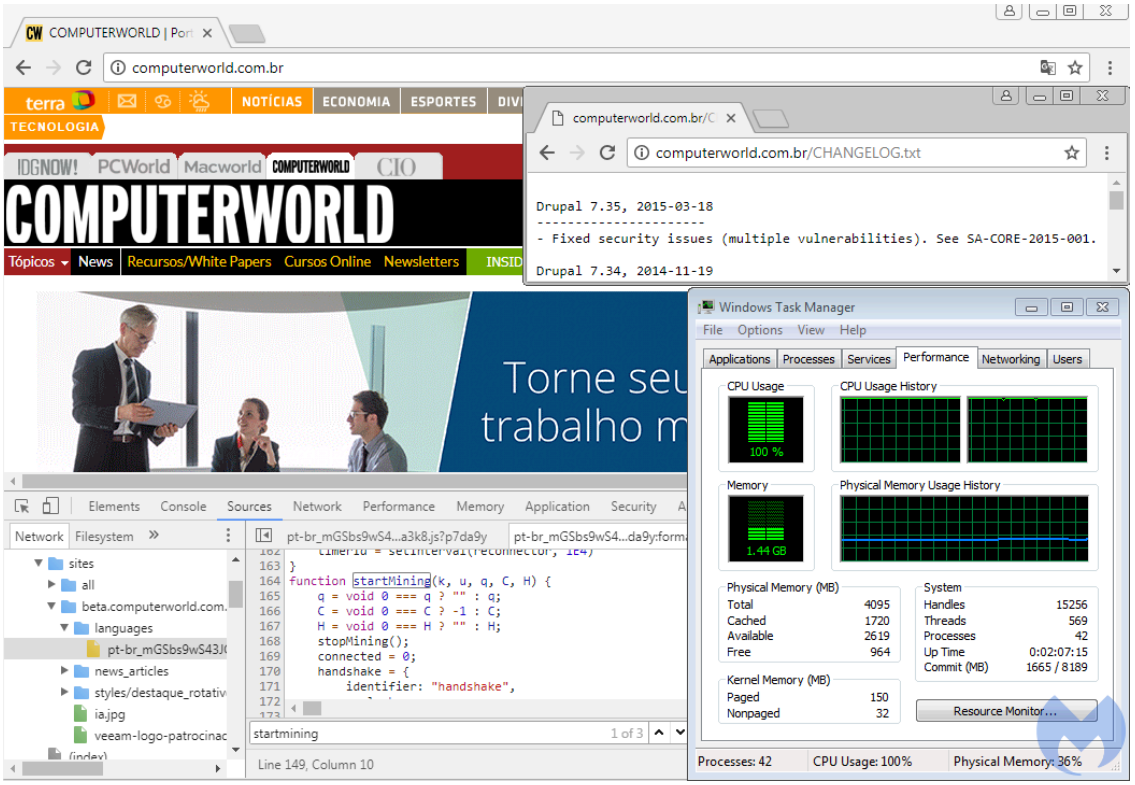



*Figure 16: Tech (ComputerWorld's Brazilian portal)*

## Malicious cryptomining remains hot

It is clear that right now, cryptomining is the preferred kind of malicious injection. There are many public but also private APIs that make the whole process easy, and unfortunately they are being abused by bad actors.

Compromised sites big and small remain a hot commodity that attackers will try to amass over time. And because patching remains an issue, the number of potential new victims never stops growing. In light of this, website owners should look into other kinds of mitigation when patching is not always an immediate option, and check what some people call virtual patching. In particular, Web Application Firewalls (WAFs) have helped many stay protected even against new types of attacks, and even when their CMS was vulnerable.

Malwarebytes continues to detect and block malicious cryptomining and other unwanted redirections.

## Indicators of compromise

### Coinhive

-> URIs

```
cnhv[.]co/1nt9z coinhive[.]com/lib/coinhive.min.js coinhive[.]com/lib/cryptonight.wasm coinhive[.]co
```

-> Site keys

```
CmGKP05v2VJbvj33wzTIayOv6YGLkUYN f0y6O5ddrXo1be4NGZubP1yHDaWqyflD kAdhxvdilslXbzLAEjFQDAZotIVm5Jkf M
```

**Crypto-Loot**

-> URI

```
cryptaloot[.]pro/lib/justdoit2.js
```

-> Keys

```
48427c995ba46a78b237c5f53e5fef90cd09b5f09e92 6508a11b897365897580ba68f93a5583cc3a15637212 d1ba2c966c
```

**EthPocket**

```
eth-pocket[.]com:8585 eth-pocket[.]de/perfekt/perfekt.js
```

**JSECoin**

```
jsecoin[.]com/platform/banner1.html?aff1564&utm_content=
```

**DeepMiner**

```
greenindex.dynamic-dns[.]net/jqueryeasyui.js
```

**Other CryptoNight-based miner**

```
cloudflane[.]com/lib/cryptonight.wasm
```

**FakeUpdates**

```
track.positiverefreshment[.]org/s_code.js?cid=220&v=24eca7c911f5e102e2ba click.clickanalytics208[.]c
```

**Tech scams**

```
192.34.61[.]245 192.81.216[.]165 193.201.224[.]233 198.211.107[.]153 198.211.113[.]147 206.189.236[.
```

---

Source: https://blog.malwarebytes.com/threat-analysis/2018/05/look-drupalgeddon-client-side-attacks/