Una web hackeada cuesta (SIEMPRE) más que una caída

Por Néstor Angulo de Ugarte

cybersecurity
Day Granada

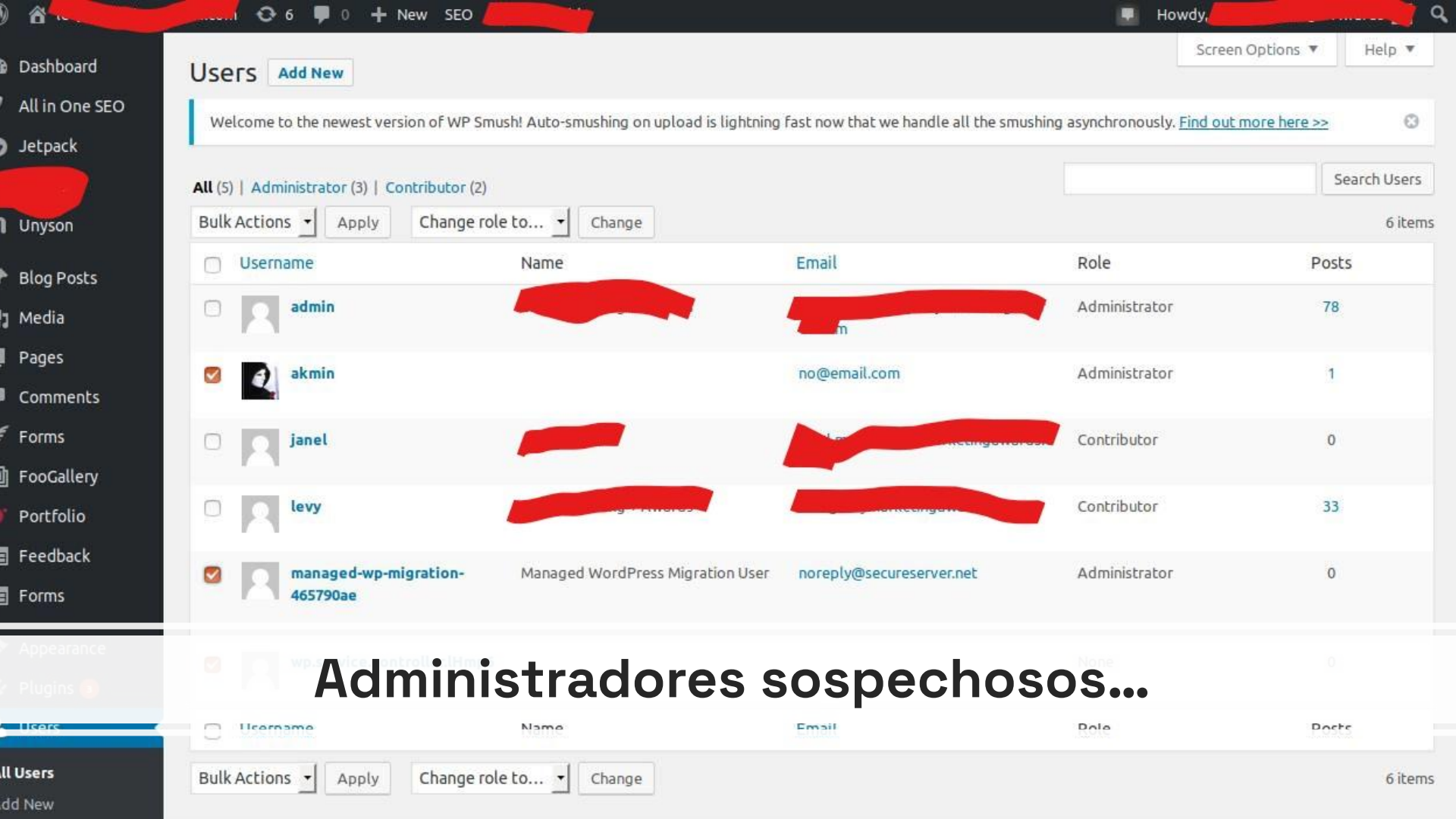

UNA WEB HACKEADA
CUESTA (SIEMPRE)
MÁS QUE UNA CAÍDA
CHANGE MY MIND


∀COSTO
Web caída
<
∀COSTO
Web hackeada
CHANGE MY MIND

“

Para unos el hackeo consiste en esto...

cybersecurity
Day Granada



Administradores sospechosos...

Current Revision by
3 months ago (4 Mar @ 09:03)

Restore This Revision

Title

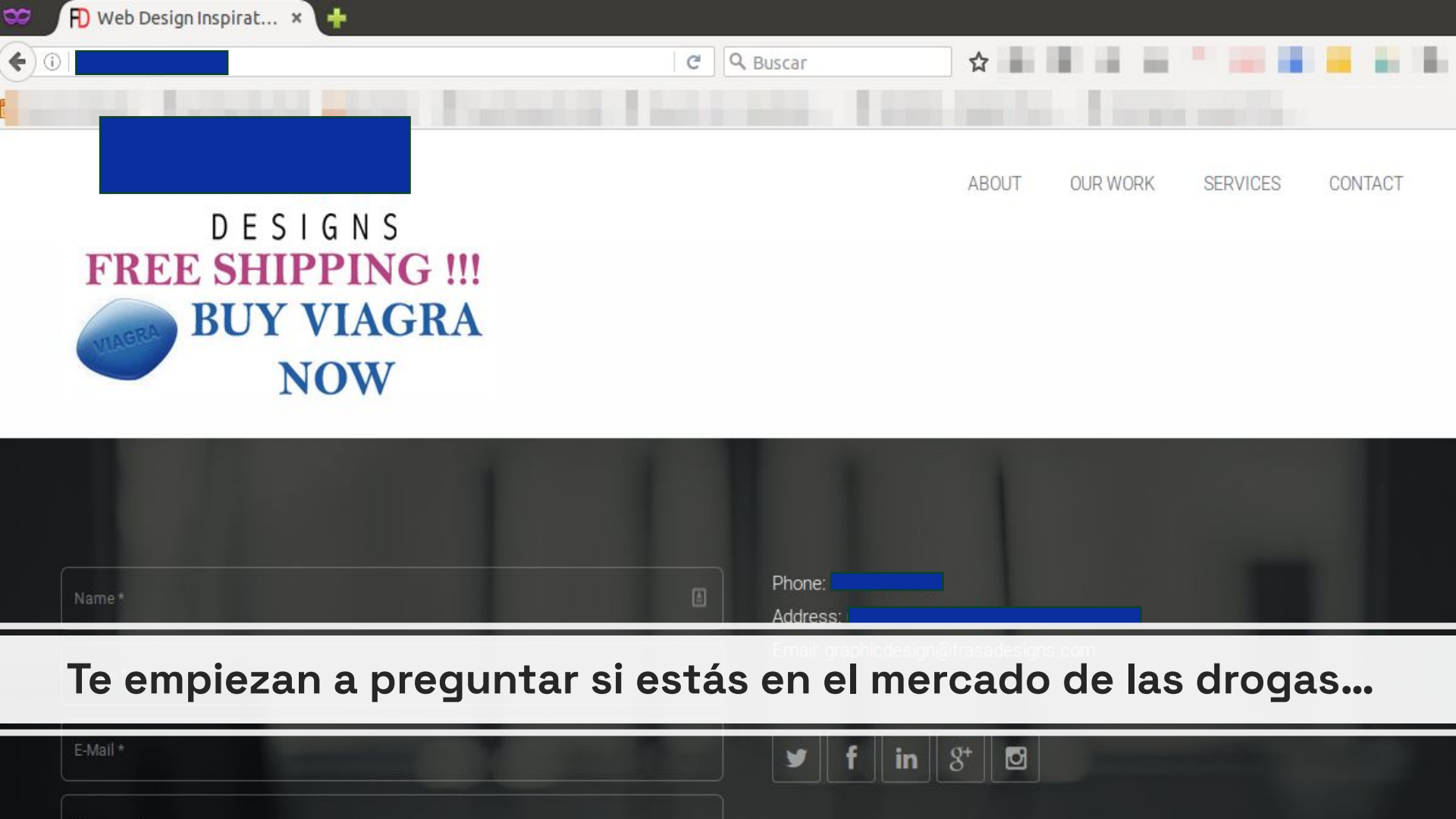
Hacked By BALA SNIPER	Hacked By GeNErAL

Content

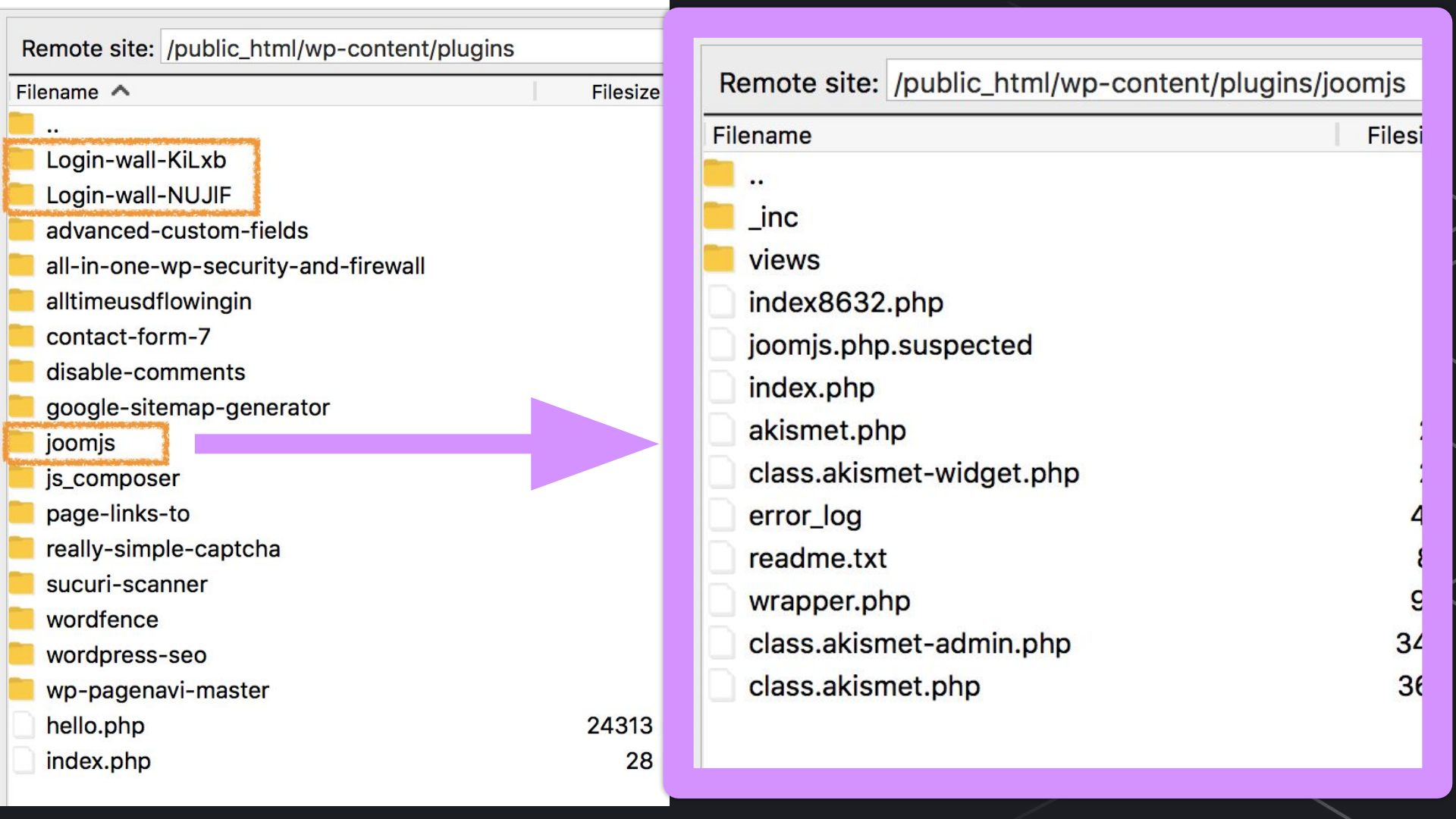
Hacked By BALA SNIPER 	
Kurdish Hacker Here 	
If you want Fix Problem Website … ! 	
Contact Me via Gmail : darinsniper007@ gmail.com 	
Contact Me Via Facebook : https://www.facebook.com /balasniper007	<title>~!Hacked By GeNErAL alias Mathis!~</title> Hacked By GeNErAL <img border='0' src='http://www.officialpsds.com/images/thumbs /Baby-Devil-Toon-psd9848.png'> Greetz : Kuroi'SH, RxR, ~ </FOOTER><code>

Tus posts cambian...

Tu página de inicio cambia ”ligeramente”



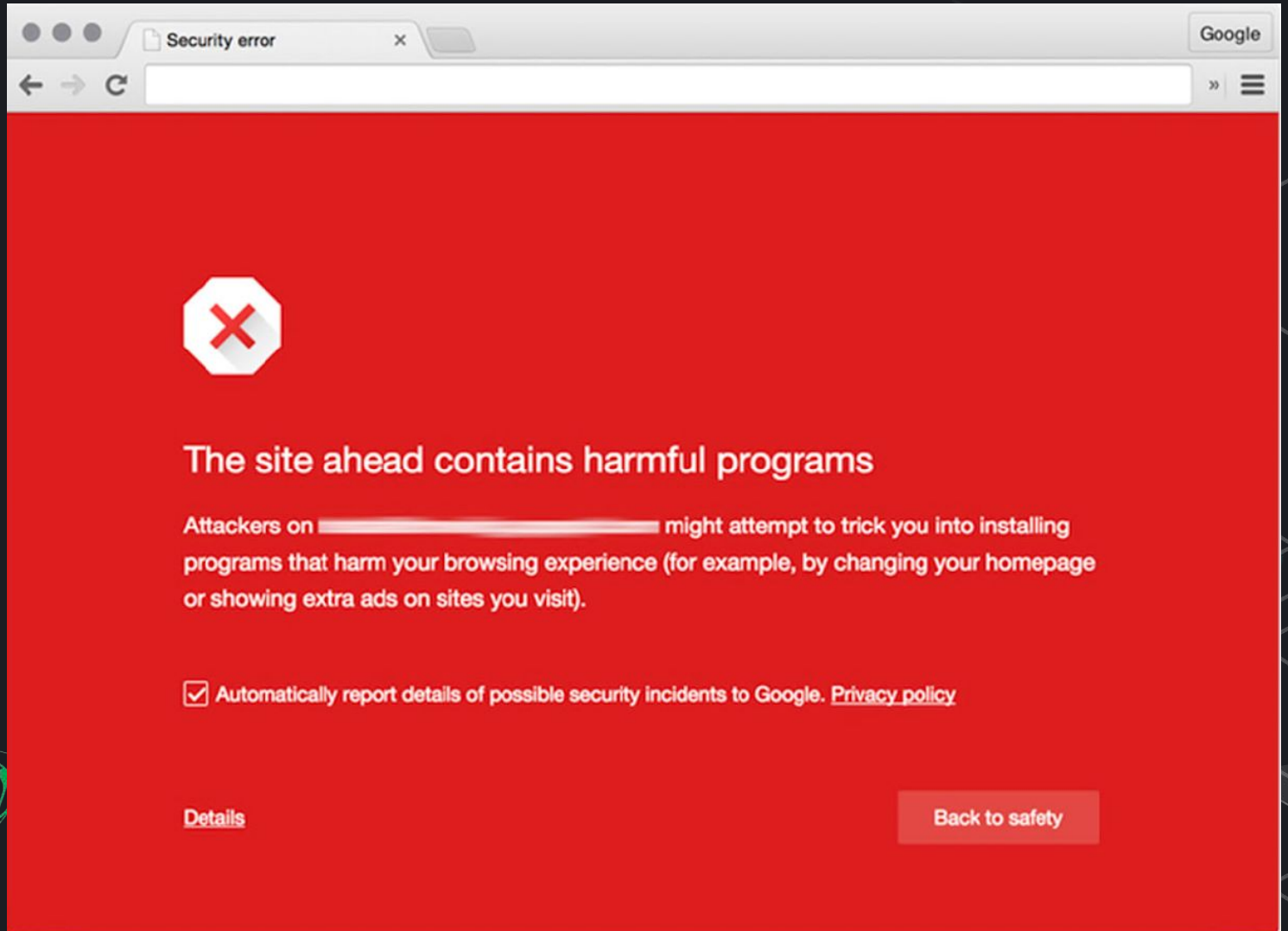
Te empiezan a preguntar si estás en el mercado de las drogas...

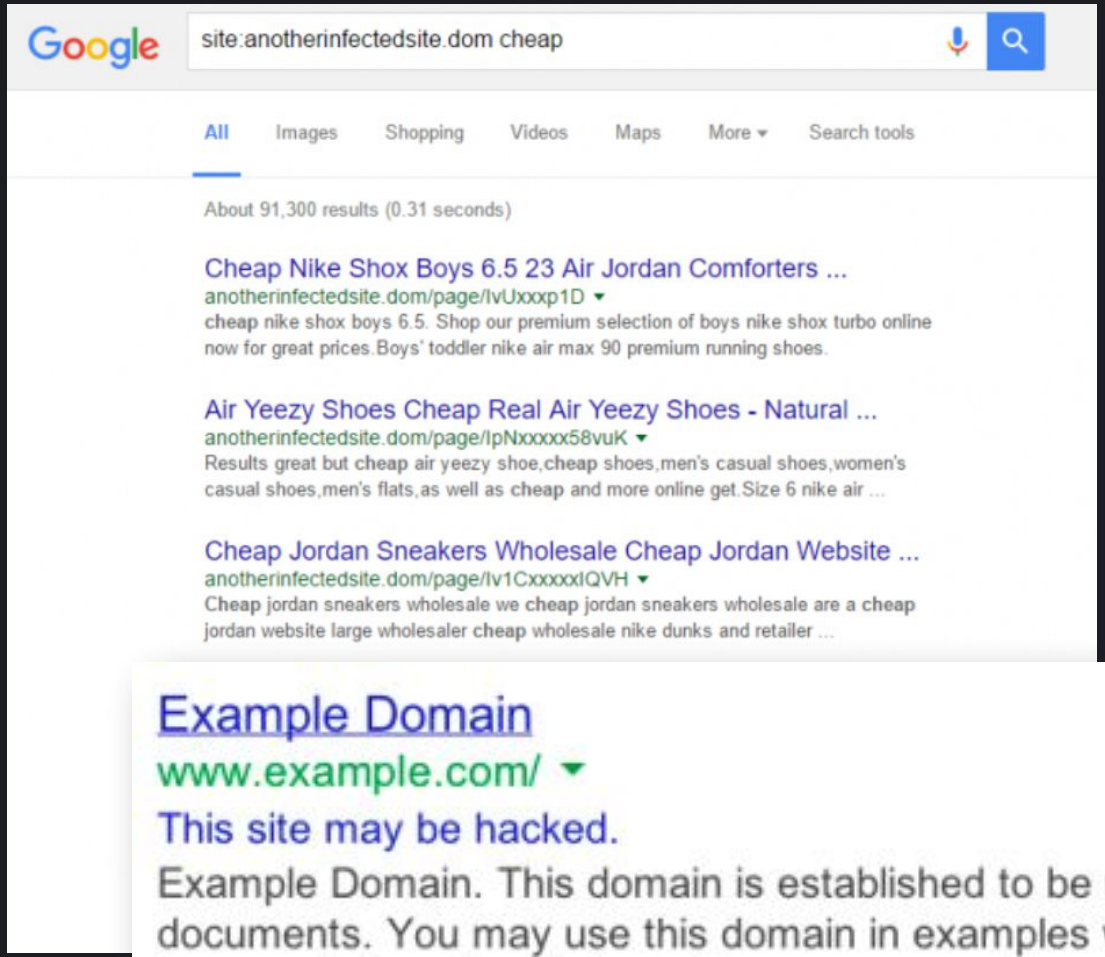

Remote site: /public_html/wp-content/plugins
Filename
Filesize
..
Login-wall-KiLxb
Login-wall-NUJlF
advanced-custom-fields
all-in-one-wp-security-and-firewall
alltimeusdflowingin
contact-form-7
disable-comments
google-sitemap-generator
joomjs
js_composer
page-links-to
really-simple-captcha
sucuri-scanner
wordfence
wordpress-seo
wp-pagenavi-master
hello.php
24313
index.php
28
Remote site: /public_html/wp-content/plugins/joomjs
Filename
Filesi
..
_inc
views
index8632.php
joomjs.php.suspected
index.php
akismet.php
class.akismet-widget.php
error_log
readme.txt
wrapper.php
class.akismet-admin.php
class.akismet.php

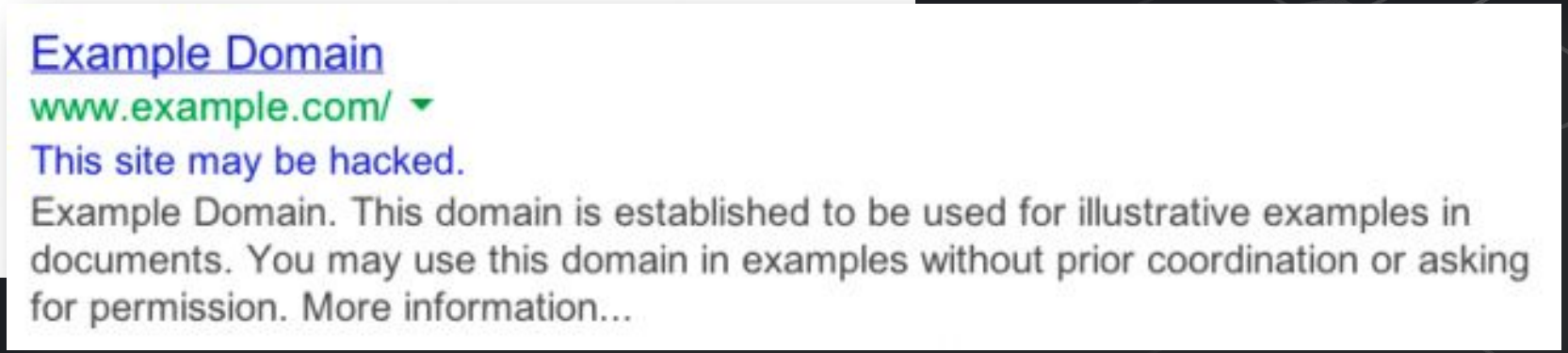
Account Suspended

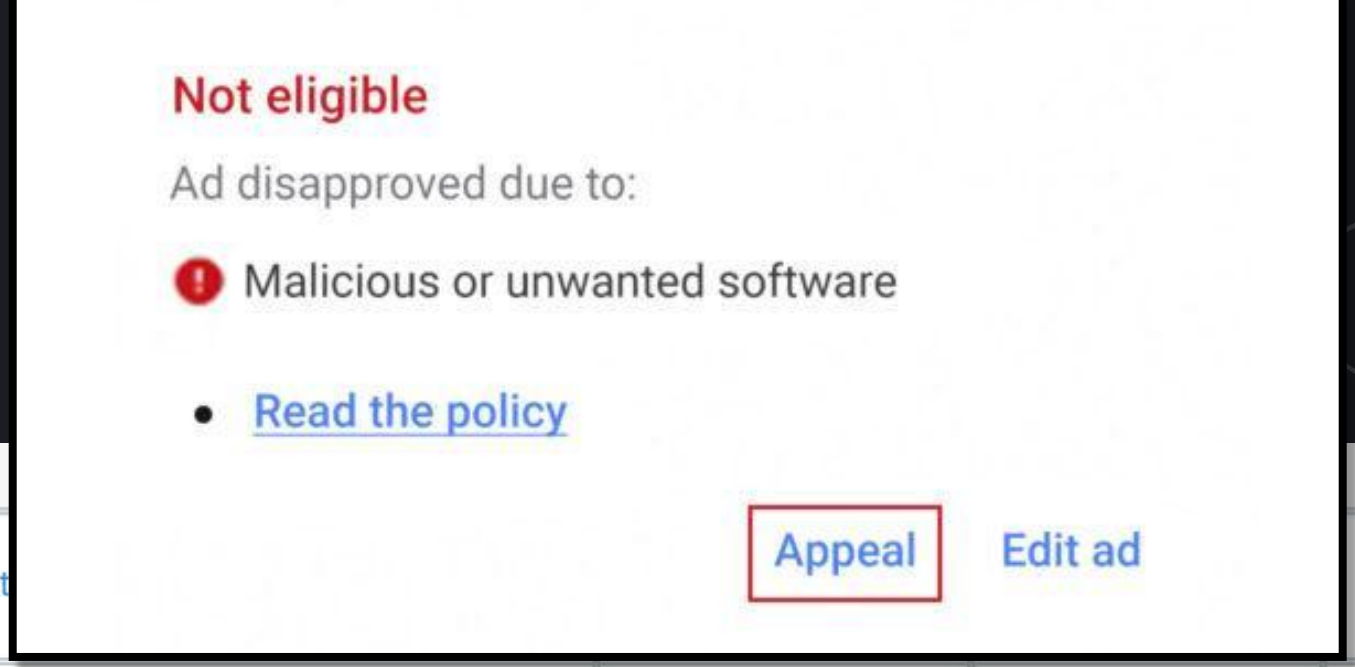
This Account has been suspended.

Contact your hosting provider for more information.


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
Details
Back to safety

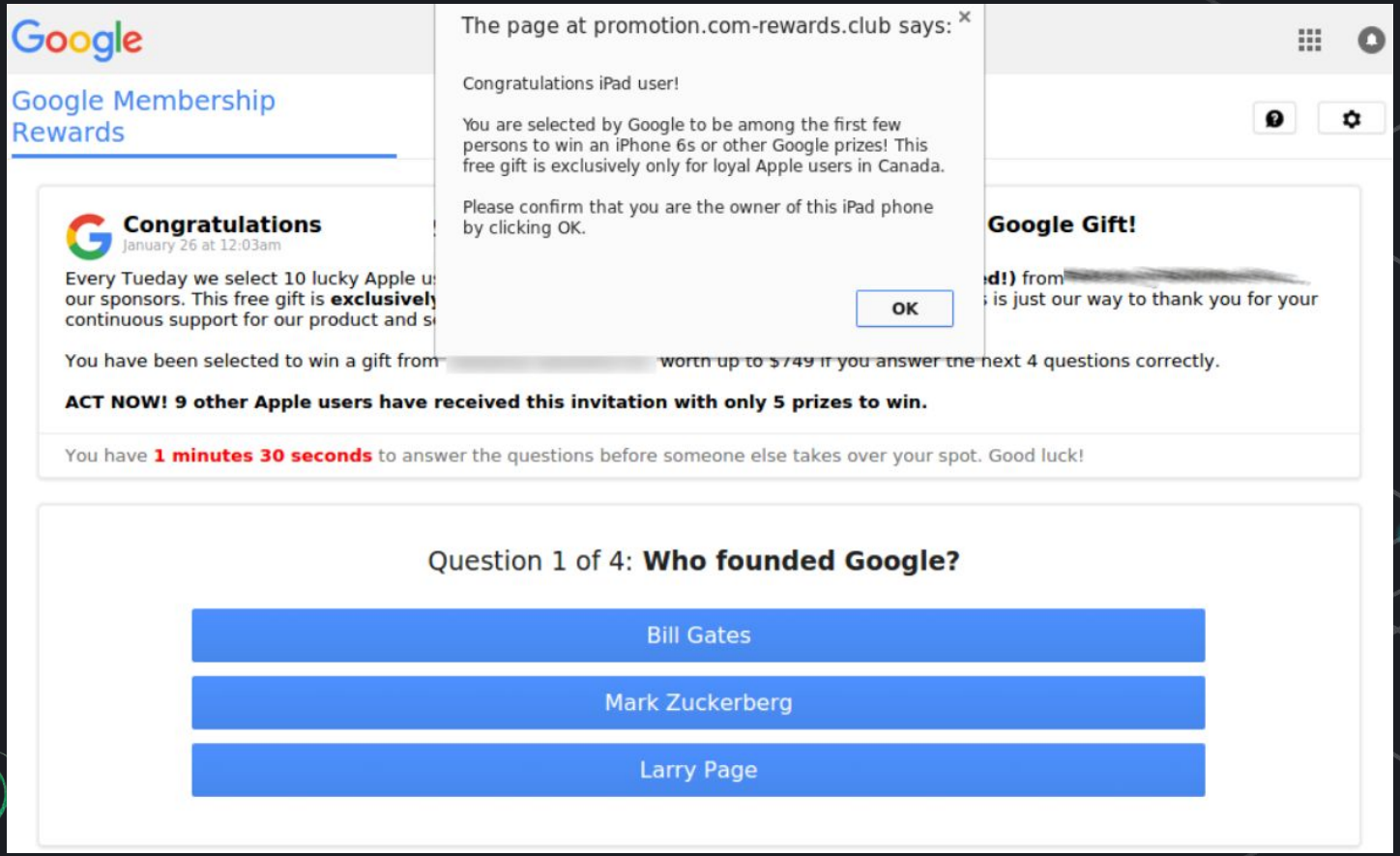

Google
site:anotherinfectedsite.dom cheap
All
Images
Shopping
Videos
Maps
More
Search tools
About 91,300 results (0.31 seconds)
Cheap Nike Shox Boys 6.5 23 Air Jordan Comforters ...
anotherinfectedsite.dom/page/lvUxxxp1D
cheap nike shox boys 6.5. Shop our premium selection of boys nike shox turbo online 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/lv1CxxxxxIQVH
Cheap jordan sneakers wholesale we cheap jordan sneakers wholesale are a cheap jordan website large wholesaler cheap wholesale nike dunks and retailer ...


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...



Ad stat

Ad	Campaign	Ad group	Status
Your Website Ad | Advertising for Revenue example.com Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna.	Example Campaign	Example Ad Group	Disapproved Malicious or unwanted software


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
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

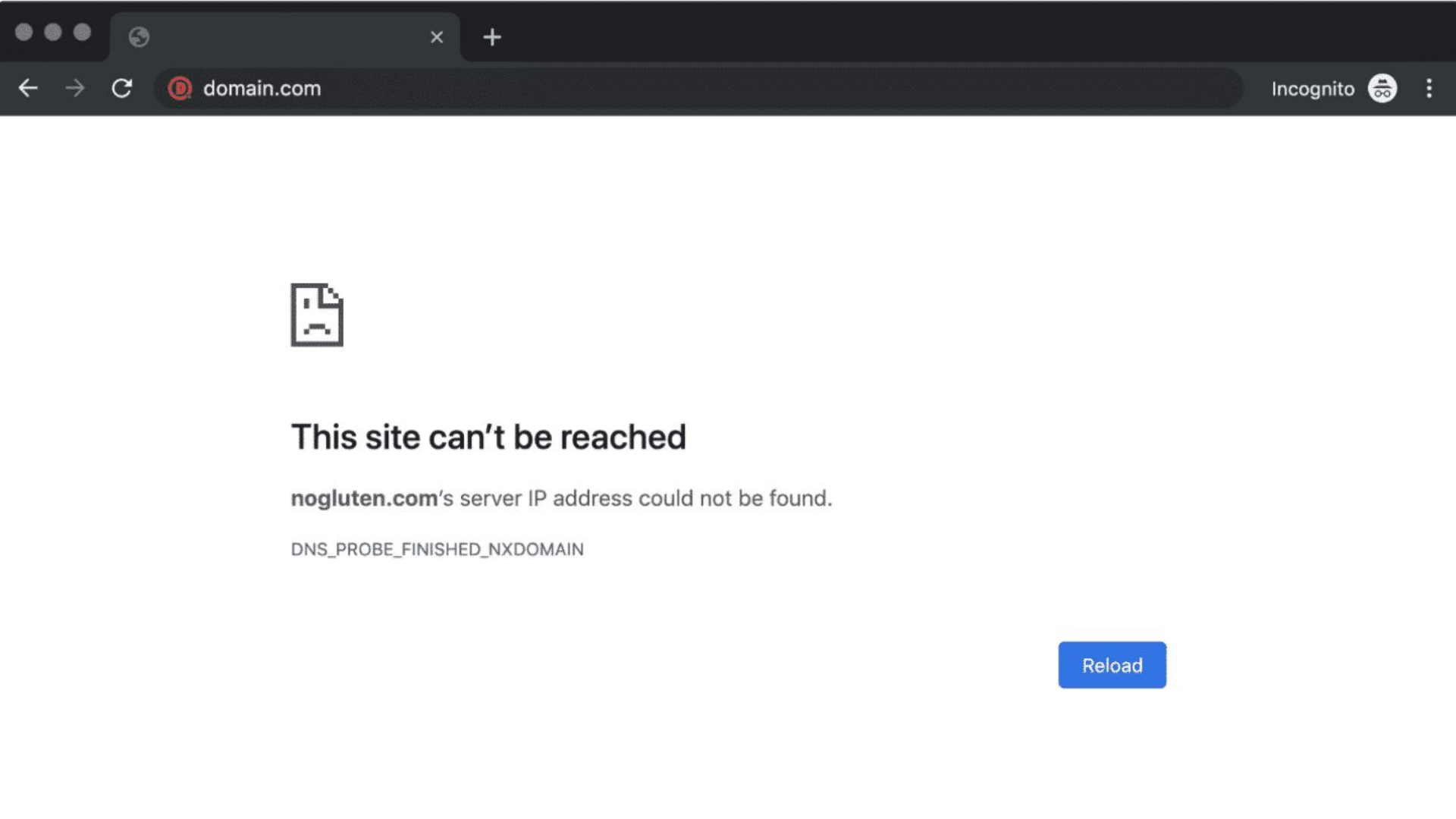
DDecode - PHP D... managedssl.int.go... AutoDash Blacklist Review T... Sucuri Decoder MSSL Invalid Sale...

newsfile.club wants to

Show notifications

Block Allow

Haga clic en "Permitir" para confirmar que no es un robot


domain.com
Incognito
This site can't be reached
nogluten.com's server IP address could not be found.
DNS_PROBE_FINISHED_NXDOMAIN
Reload

200€:

Servicio de limpieza web

Y listo…

cybersecurity
Day Granada

“

Para otros esto...

cybersecurity
Day Granada


RANSOMWARE
RANSOMWARE
RANSOMWARE

Ejemplos de Cierres por Ransomware en Hosting Europeo

CloudNordic / AzeroCloud (Dinamarca)

- Agosto 2023
- Un ataque de ransomware cifró todos los sistemas, incluyendo las copias de seguridad.
- La empresa declaró la pérdida total de datos y el cese de operaciones.

Proveedores de Hosting Pequeños y Medianos

- Diversos proveedores de menor tamaño en Europa han cesado operaciones tras ataques.
- Compromiso de sistemas principales y backups.
- Falta de recursos para la recuperación.

Te toca la puerta la policía...

GDPR
Data Breach Notice Letter

My Company
Additional Information
Street, Number
City, Region
Country

Customer Name,

At My Company, we respect the privacy of your personal data. We are writing to let you know about a data security incident that involves the personal information you have with us.

On Jan 01, 2019, we have discovered a data breach in our systems. The data accessed may have included the following types of personal information:

- Identify types of personal information breached: Email, First and Last Name

To the best of our knowledge, the data accessed did not include any:

- Identify types of personal information not breached: Shipping Address

We deeply regret that this incident occurred. We are conducting a review of the affected records and of all our computer systems. We will notify you if there are any significant developments.

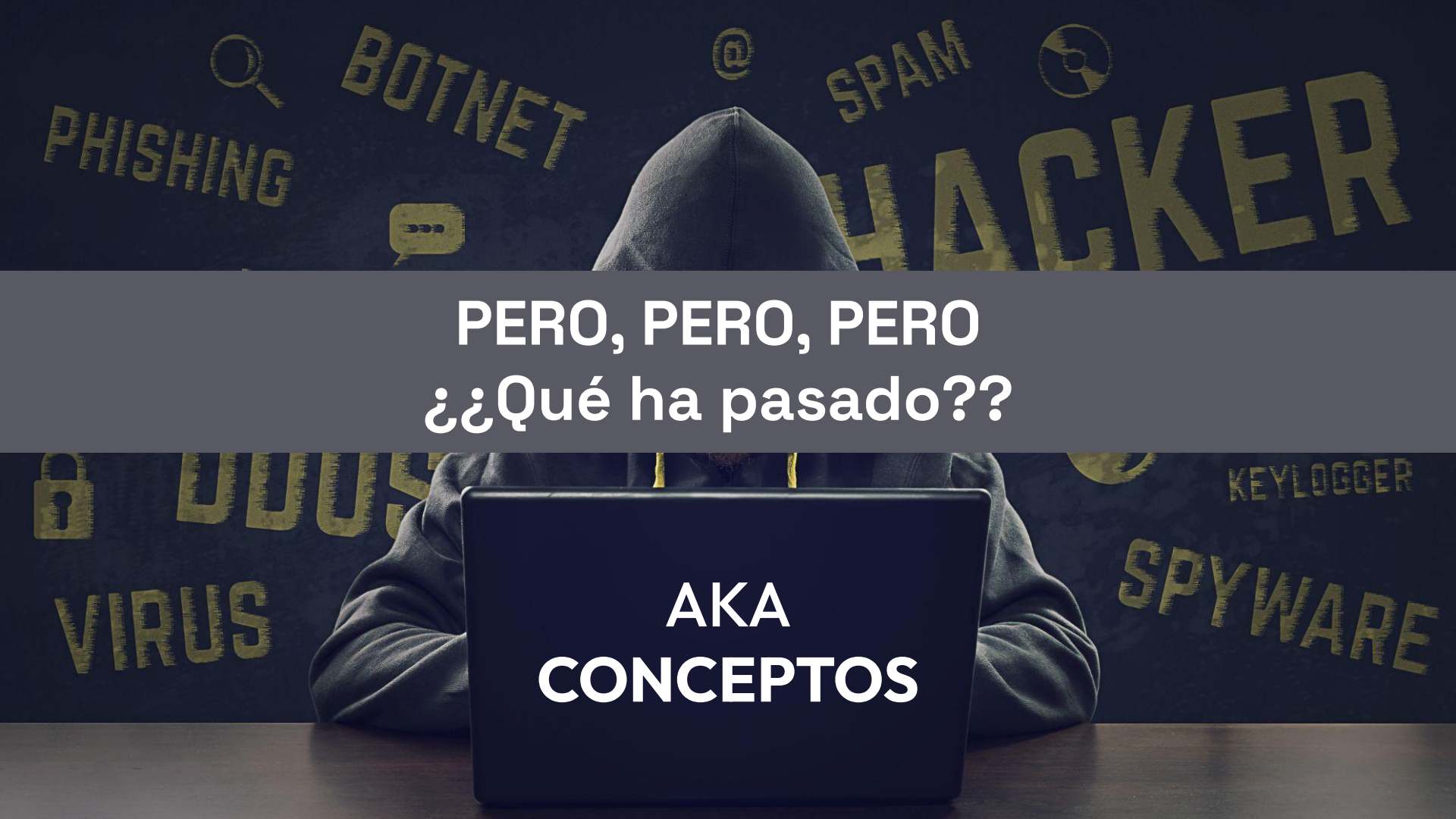
ETid-2942				cient fulfilment of ubjects rights	link
ETid-2941	80,000	BIZUM, S.L.	Art. 32 GDPR	cient data sing agreement	link
ETid-2935				cient legal basis for rocessing	link
ETid-2934	2,000	GESTIÓN DE VENTAS IBERIA S.L.	Art. 14 GDPR	cient technical and sational measures to information y	link
ETid-2933	150,000	DIGI SPAIN TELECOM, S.L.U.	Art. 6 (1) GDPR	cient fulfilment of ubjects rights	link

ℹ️ 👉 **enforcementtracker.com**

ETid-2914	1,500,000	SERVICIOS FINANCIEROS CARREFOUR, E.F.C.	Art. 5 (1) f) GDPR	cient technical and sational measures to information y	link
ETid-2894	840	SERVACE S.L.	Art. 5 (1) f) GDPR, Art. (1) GDPR	ompliance with l data processing les	link
ETid-2887				cient technical and sational measures to information y	link
ETid-2886	600	Property manager	Art. 32 GDPR	ompliance with l data processing les	link

SPAIN

Y cierre…



PERO, PERO, PERO
¿¿Qué ha pasado??

AKA
CONCEPTOS


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

¿Hackers?

Persona **curiosa** que va más allá de límites y convencionalismos

AKA **Hacker**


Cola

- Thales de Mileto
- Hipatia de Alejandría
- Leonardo da Vinci
- Thomas Edison
- Arquímedes
- Marie Curie
- Louis Pasteur y Alexander Fleming
- Hedy Lamarr
- Nikola Tesla
- Grace Hopper y Ada Lovelace

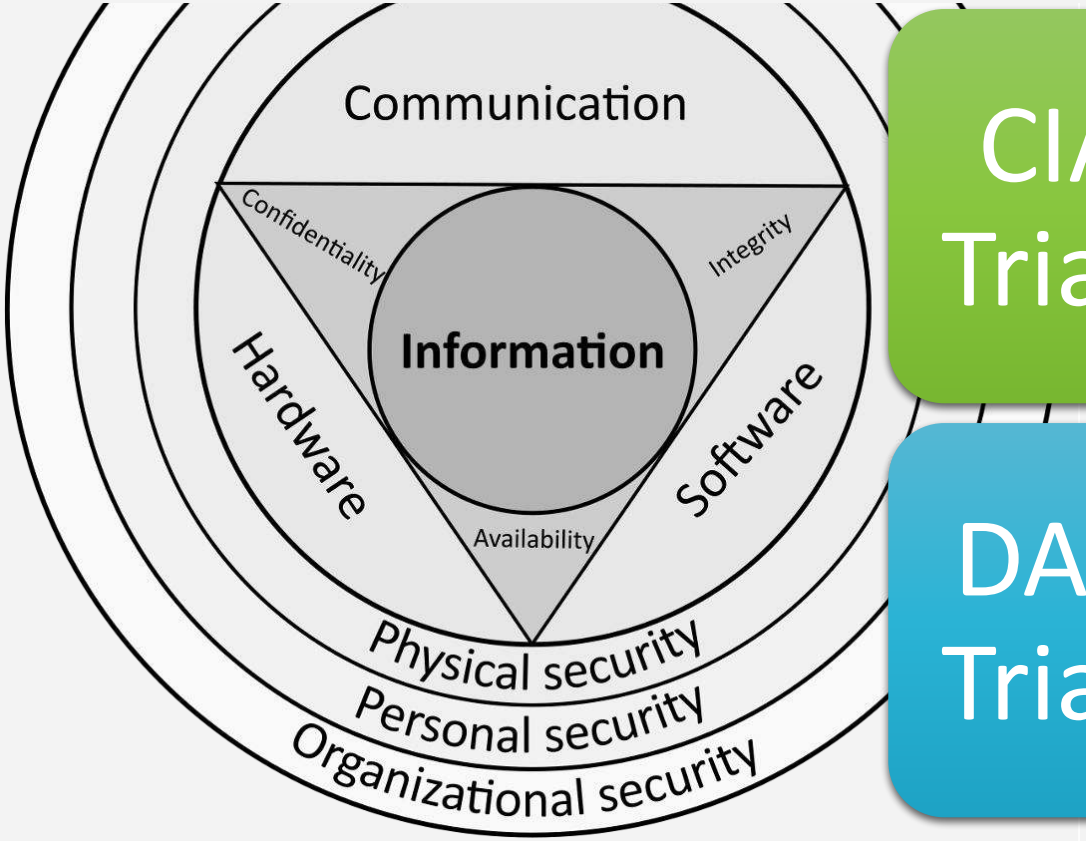
¿Entonces a qué le llamamos Hacker?

Hacker informático cuyo objetivo es enriquecerse o ganar fama.

AKA **Ciberterrorista / Atacante**


¿CIBERSEGURIDAD?

¿Qué es InfoSec?



CIA Triad

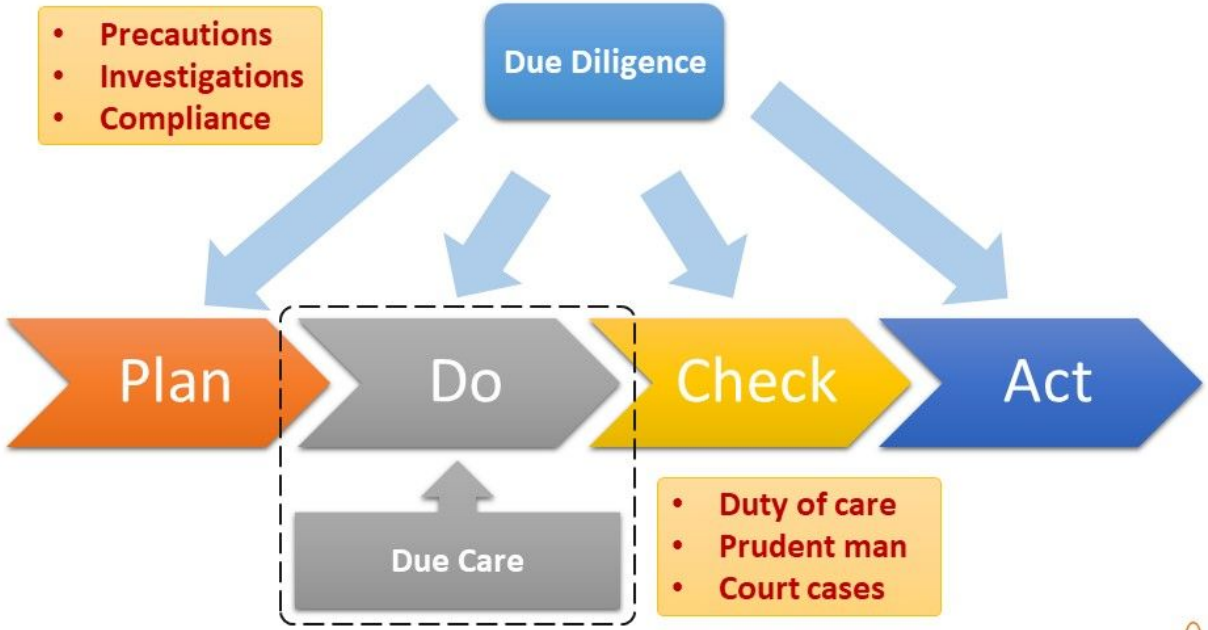
- Confidentiality
- Integrity
- Availability

DAD Triad

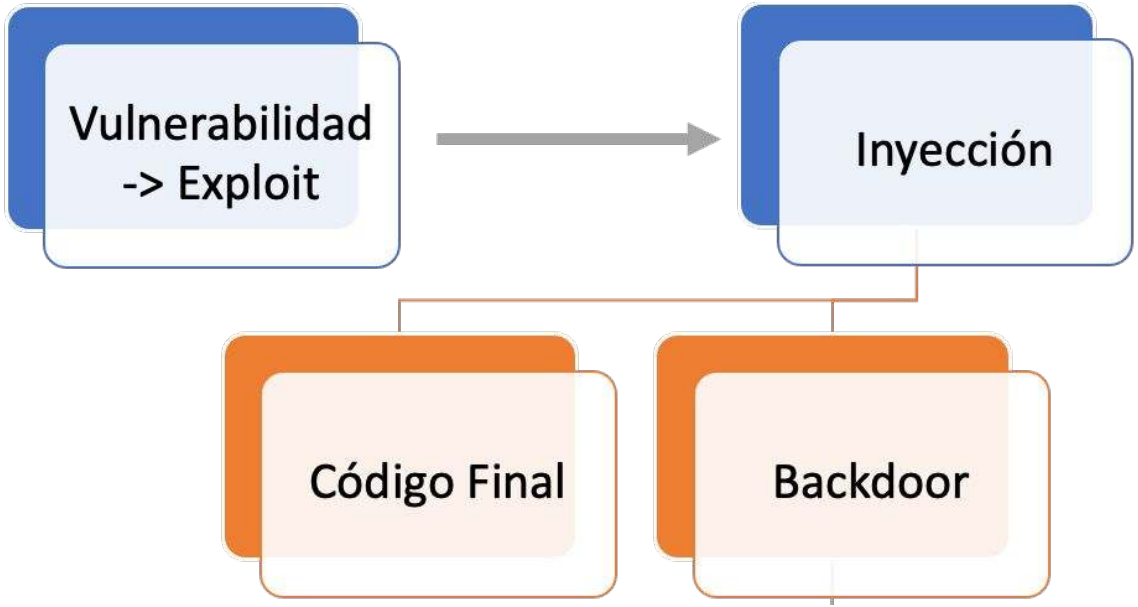
- Disclosure
- Alteration
- Destruction

Ser diligente y tomar acciones

Due Diligence and Due Care

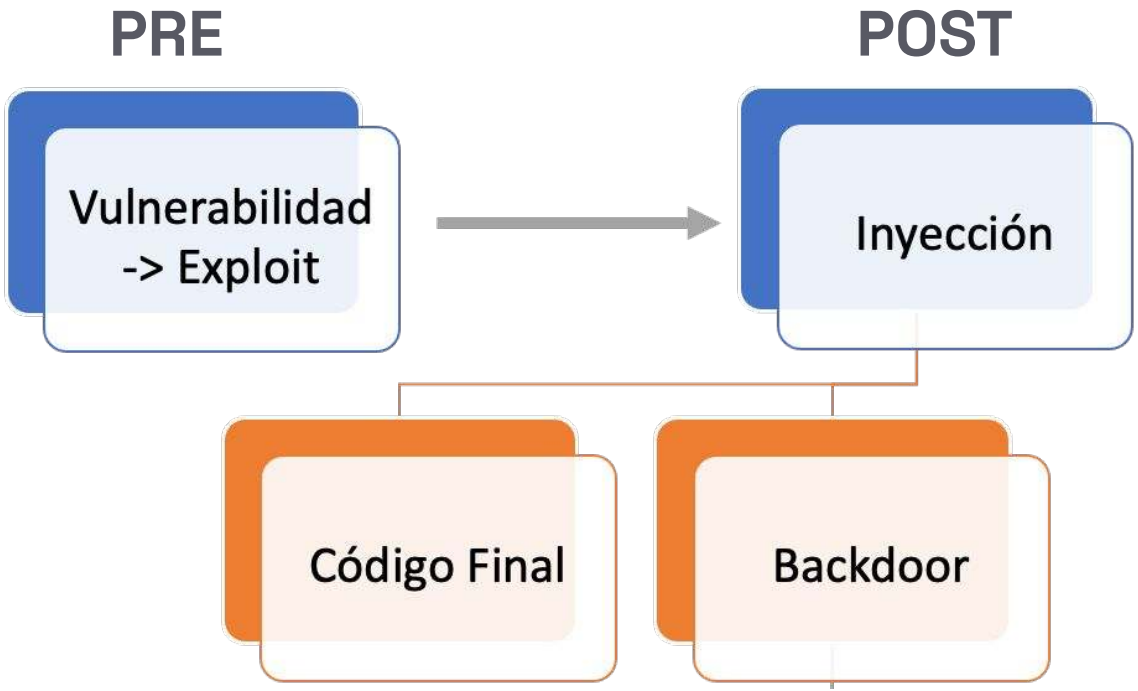


Cómo se hackea un WordPress




DATA
BREACH

Cómo se hackea un WordPress



2025

Algunos números…

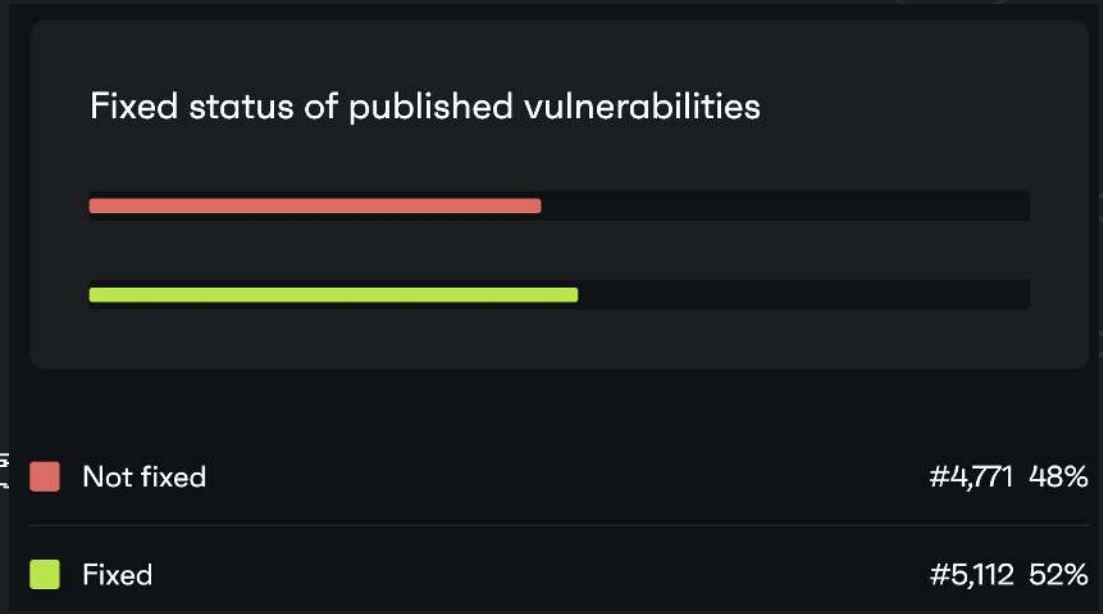
cybersecurity
Day Granada

9.883
Vulnerabilidades declaradas en 2025

33.497
Vulnerabilidades declaradas

cybersecurity
Day Granada

Affected software | Vulnerability	Priority	Disclosed
Advanced Custom Fields: Extended 0.9.0.5-0.9.1.1 Unauthenticated Remote Code Execution vulnerability	10	Dec 3, 2025
WavePlayer <= 3.7.0 Unauthenticated Arbitrary File Upload vulnerability	10	Nov 25, 2025
Gravity Forms <= 2.9.21.1 Unauthenticated Arbitrary File Upload via Legacy Chunked Upload vulnerability	9	Nov 17, 2025
AI Engine <= 3.1.3 Unauthenticated Sensitive Information Exposure to Privilege Escalation vulnerability	9.8	Nov 5, 2025
Post SMTP <= 3.6.0 Missing Authorization to Account Takeover via Unauthenticated Email Log Disclosure vulnerability	9.8	Nov 3, 2025



cybers
Day Gr

Breakdown by patch priority

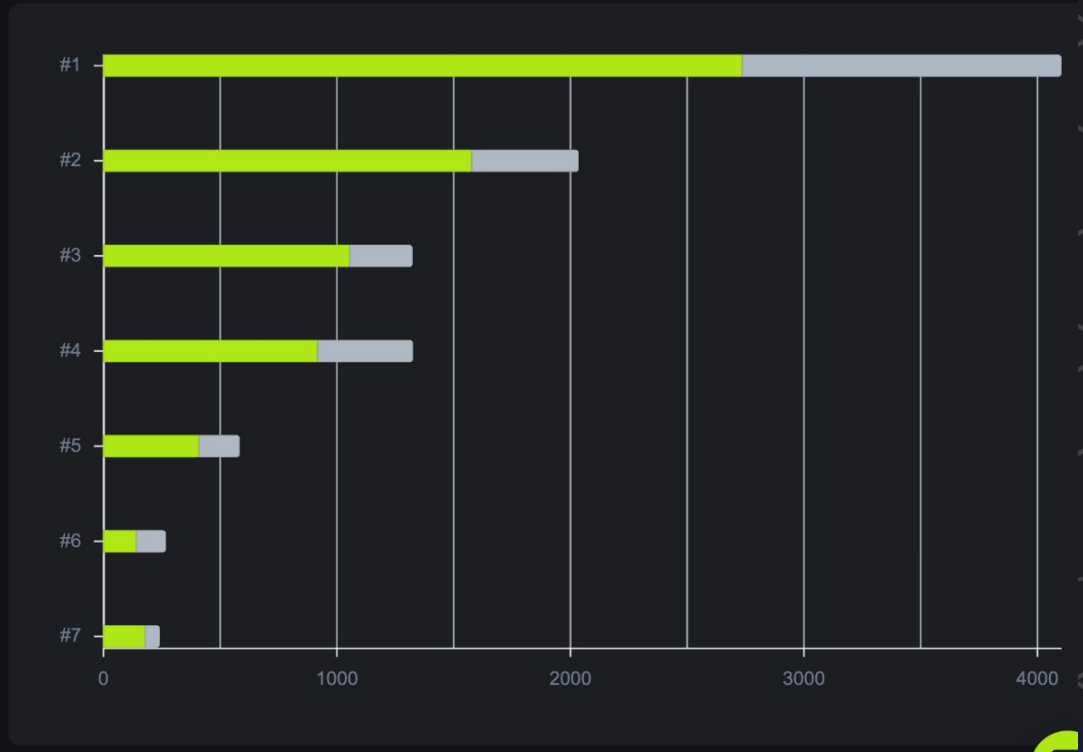
High (Resolve immediately)	#1,867	19%
Medium (Resolve in 14 days)	#1,867	20%
Low (Resolve in 30 days)	#1,867	61%

Breakdown by CVSS severity

Critical (9.0-10.0)	#807	8%
High (7.0-8.9)	#3,877	39%
Medium (4.0-6.9)	#5,170	52%
Low (0.1-3.9)	#29	0%

Most common security vulnerabilities

#1 Cross-Site Scripting (XSS)	41.52%
#2 Other vulnerabilities	20.60%
#3 Cross-Site Request Forgery (CSRF)	13.40%
#4 Broken Access Control	13.42%
#5 SQL Injection	5.91%
#6 Sensitive Data Exposure	2.71%
#7 Arbitrary File Upload	2.45%



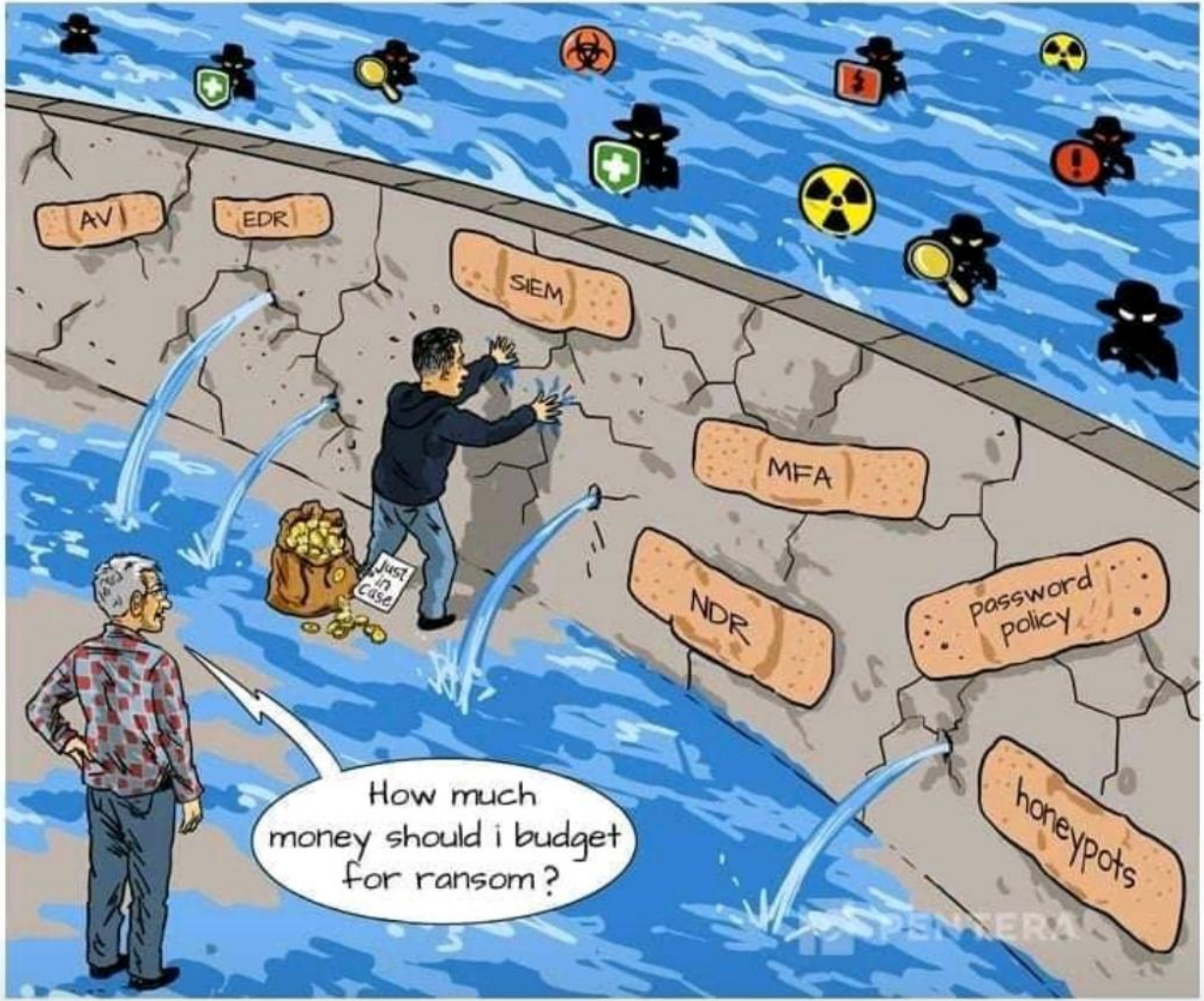
Disclosed by Patchstack Other sources

cybersecurity Day Granada

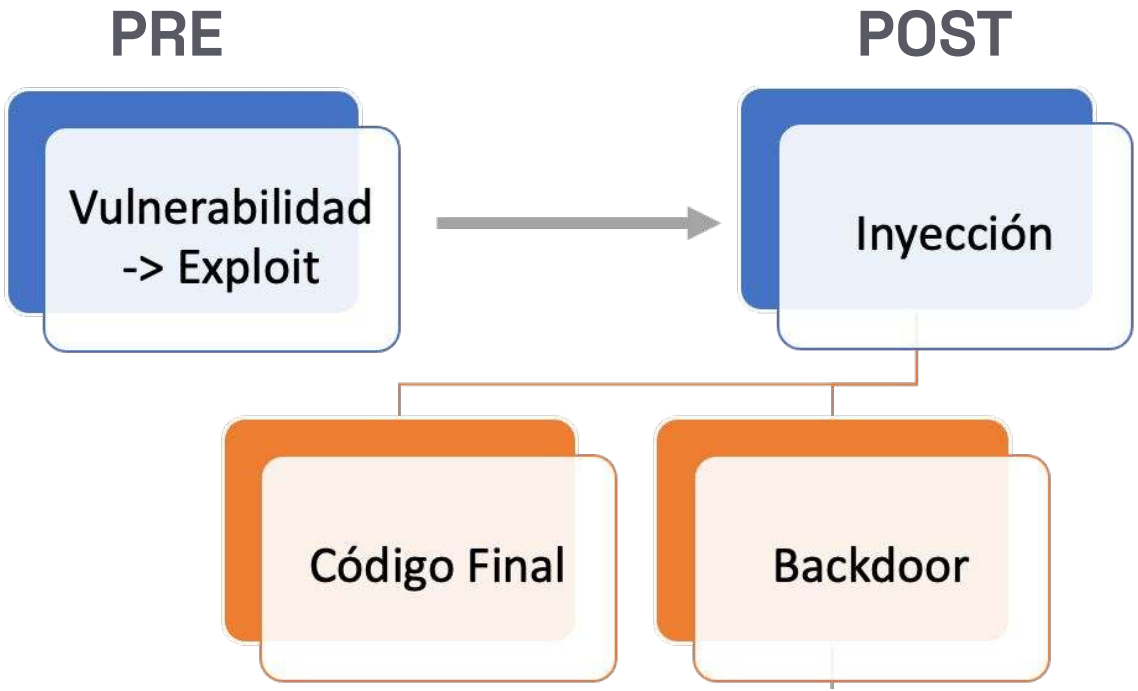
Entonces... ¿qué puedo hacer?

cybersecurity
Day Granada

“


AV
EDR
SIEM
MFA
NDR
password policy
honeypots
Just in Case
How much money should i budget for ransom?
PENTERA

Cómo se hackea un WordPress



Entonces... ¿Qué puedo hacer?

- Soluciones PRE / Proactivas:
  - Actualizar / Parchear / Eliminar
  - Hardening (reducir plugins, roles mínimos, configuración segura)
  - Parches virtuales / WAF especializado
  - Copias de seguridad periódicas (probadas)

Entonces... ¿Qué puedo hacer?

- Soluciones POST / Reactivas:
  - Monitorizar: logs, integridad de ficheros, alertas tempranas
  - Restaurar copia de seguridad
  - Limpieza y remediación del sitio
  - Aplicar soluciones PRE

¿Qué ES una brecha de datos?

GDPR: “todas aquellas **violaciones de la seguridad** que ocasionen la **destrucción, pérdida o alteración** accidental o ilícita de **datos personales** transmitidos, conservados o tratados de otra forma, o **la comunicación o acceso no autorizados** a dichos datos”.

cybersecurity
Day Granada

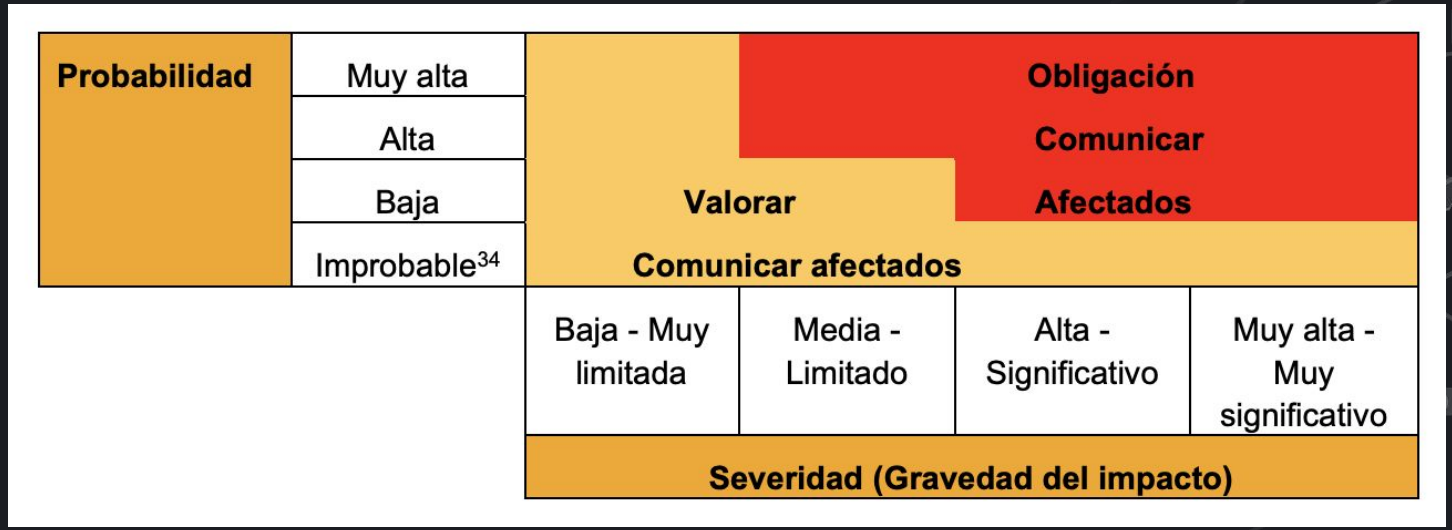
¿Qué NO ES una brecha de datos?

Un **incidente de seguridad que no ha afectado a datos personales** o **tratamientos de datos personales** no es una brecha de datos personales, dado que **no podría producir daños sobre los derechos y libertades de las personas físicas** cuyos datos son objeto del tratamiento, independientemente de otros perjuicios que pueda producir al responsable o encargado del tratamiento.

cybersecurity
Day Granada

OBLIGADO, si hay una Brecha de Datos

- **Comunicar** a la autoridad competente (España/Europa es la AEPD) en **menos de 72h** desde que se tiene constancia de la brecha.
- Hacer una **valoración de riesgo** para las personas afectadas **y de alcance** de la brecha.



Espera...

DORA, NIS2, PCI DSS, CRA

cybersecurity
Day Granada

CRA

Cyber Resilience Act

cybersecurity
Day Granada

CRA - Conceptos (POR QUE)

- **Seguridad por defecto y desde el diseño**
- **Reglas mínimas comunes**
- **Aplicación a todos los productos tecnológicos** (plugins, temas, frameworks, librerías, builds y cualquier componente distribuido).

cybersecurity
Day Granada

CRA - Conceptos (QUIEN)

- **Fabricantes y distribuidores bajo responsabilidad**: Quien obtiene beneficio económico asume obligaciones legales de seguridad, mantenimiento y gestión de vulnerabilidades.

- **Open Source Steward**:
  Figura que actúa como responsable legal cuando el desarrollo comunitario no tiene una entidad detrás; relevante para plugins mantenidos por voluntarios.

cybersecurity
Day Granada

CRA - Conceptos (QUE)

- **Gestión continua de vulnerabilidades:**
  Descubrimiento, parcheo, divulgación y evidencias forman parte del ciclo de vida obligatorio.
- **SBOM** (Software Bill of Materials):
  Transparencia completa de dependencias (PHP, JS, Composer, NPM).
- **Multas similares al GDPR:**
  Sanciones proporcionales y elevadas en caso de incumplimiento, incluyendo fallos en actualizaciones, divulgación o seguridad.

cybersecurity
Day Granada

CRA - Conceptos (COMO)

- **0 vulnerabilidades en producción**
- **Mantener un canal formal de reporte de fallos** (vuln disclosure)
- **Asegurar prácticas de desarrollo seguro**: revisión de código, VCS, tests, hardening y validación del entorno de build.
- **Minimizar riesgos en la supply chain**: dependencias verificadas, integridad del código, firmas o mecanismos de verificación.
- **Transparencia y documentación**: manuales de seguridad, historial de versiones, evidencias de parches y medidas de mitigación.

CRA - Antes y Después

- Seguridad opcional / “best effort” del desarrollador
- Sin obligación de corregir vulnerabilidades.
- Dependencias opacas, sin SBOM ni trazabilidad
- Divulgación de fallos irregular y no estandarizada
- Muchos plugins abandonados aún activos

- Seguridad por diseño y por defecto obligatoria
- Obligación legal de parchear y mantener plugins/temas
- SBOM obligatorio: transparencia total de componentes
- Procesos formales de reporte, timelines y comunicación
- Menos abandono: requisitos de soporte continuo

cybersecurity
Day Granada


Everybody needs a hacker

Gracias

Néstor Angulo de Ugarte

@pharar

Head of Security

Patchstack

cybersecurity
Day Granada