WORDCAMP MADRID 2023

KAME HAME HAAA!

O cómo defenderse de un atacante malicioso nivel Freezer/Frieza

Nestor Angulo

- **CISSP** (ISC2.org - 2022)
- **Web Security Analyst** (2015-2023)
  - @GoDaddy WebSecurity
  - @sucuri.net

- Nuevo comienzo: **nestorangulo.pro**

- Data & Research Team lead:

patchstack

- @pharar

PUSH START
INSERT COIN


DRAGON BALL Z
XKEEPERZ
クロスキーパーズ

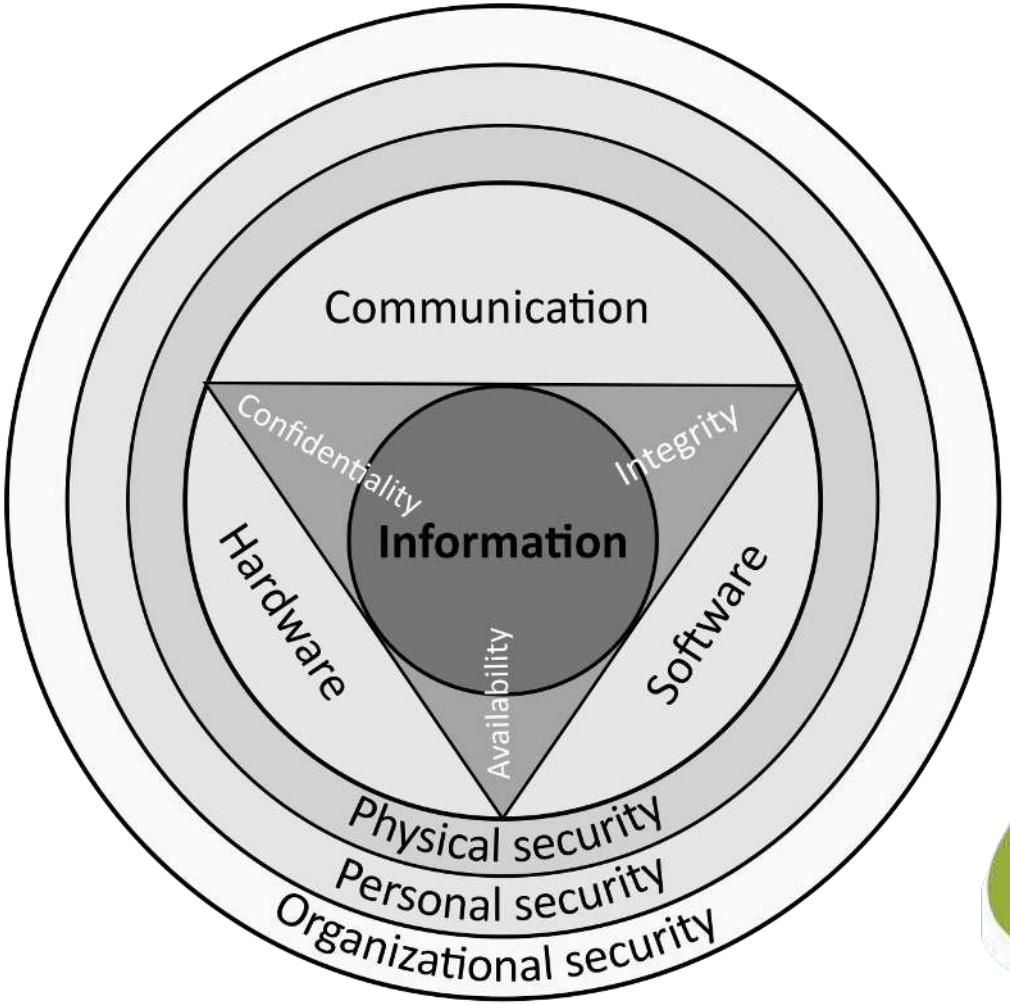

Bmac.

Un atacante sólo debe acertar una vez

—

Un defensor debe acertar siempre.

¿Infosec?


Communication
Confidentiality
Integrity
Information
Hardware
Software
Availability
Physical security
Personal security
Organizational security


1
CONFIDENTIALITY
INFORMATION SECURITY
2
INTEGRITY
3
AVAILABILITY

Imaginemos...

Tu planeta

Tu Sitio WordPress

Posibles objetivos en WordPress

Usuarios

Base de datos

Contenido

Infrastructura

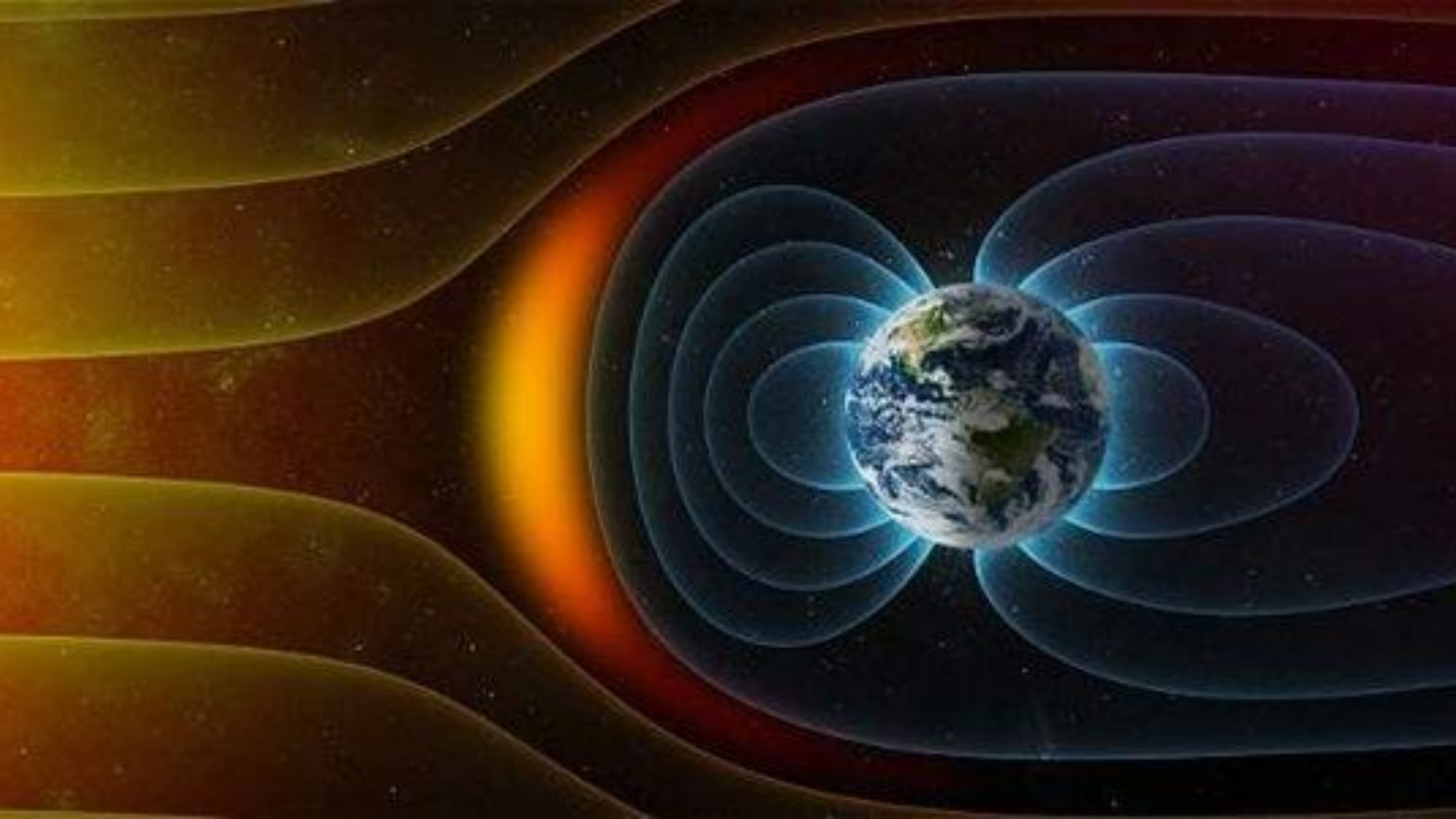
Bot Net

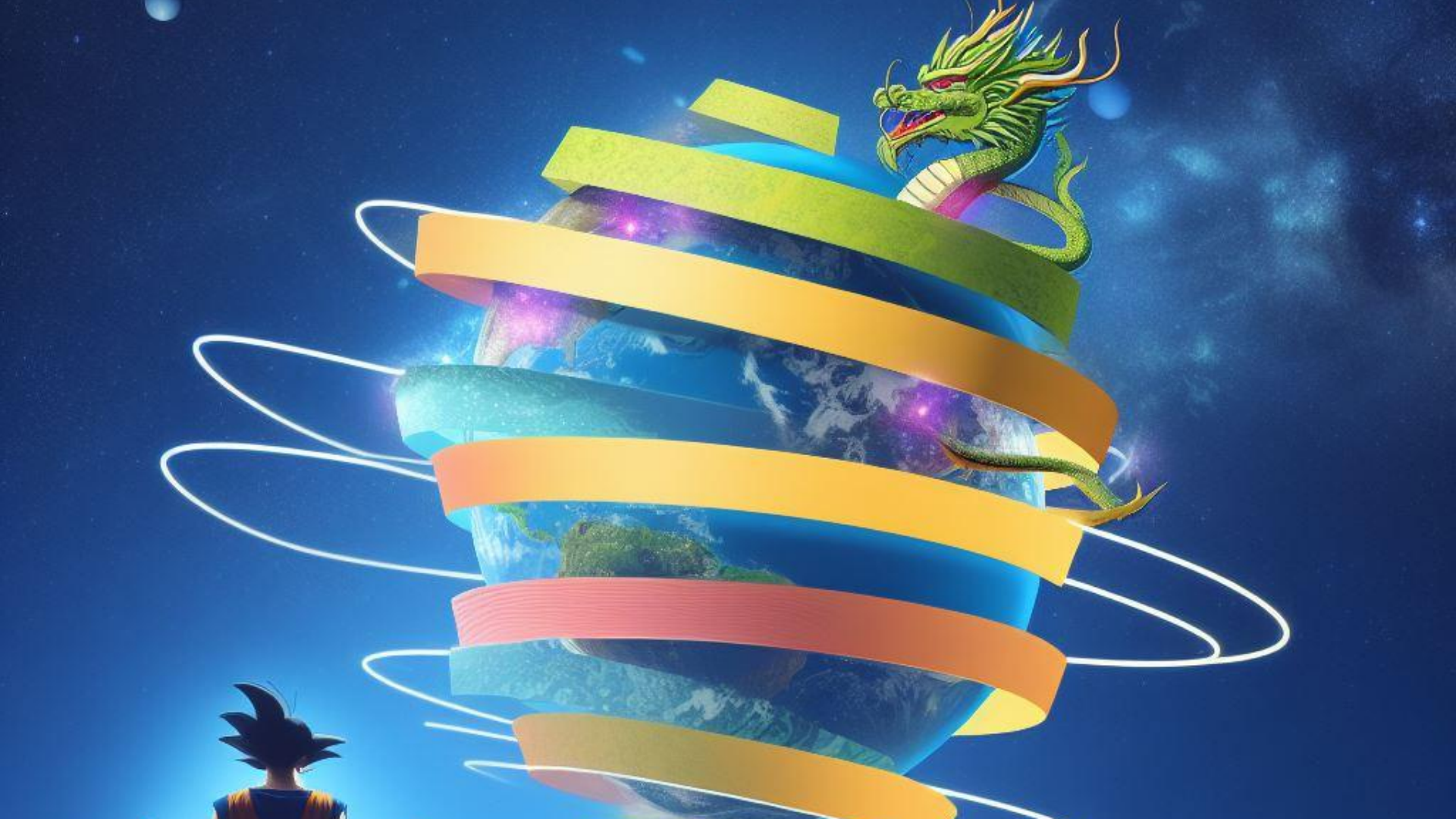
Reputación

Tu seguridad

Seguridad por capas

- Antivirus
- SSL/TLS
- WAF (Externo/Interno)
- MFA y contraseñas fuertes
- Plugins y monitores
- Logs y escáneres
- **Formación** para las personas
- **Mantenimiento**

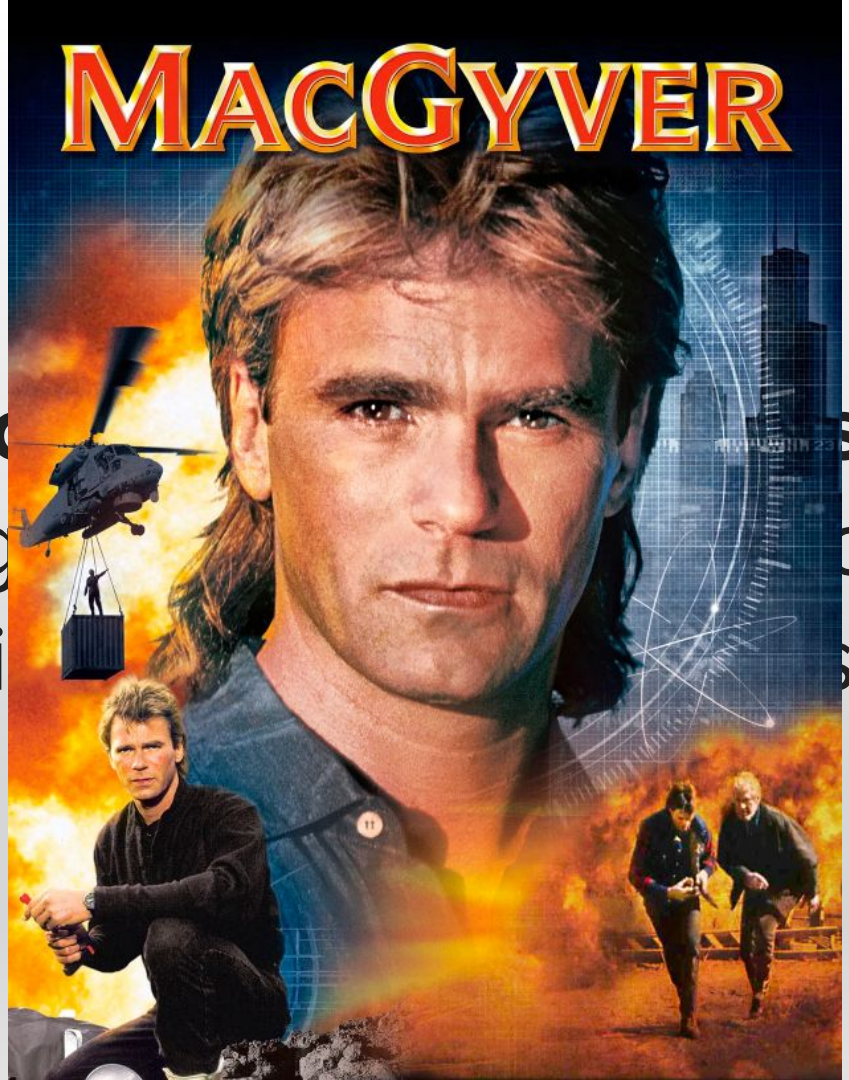





Tus enemigos

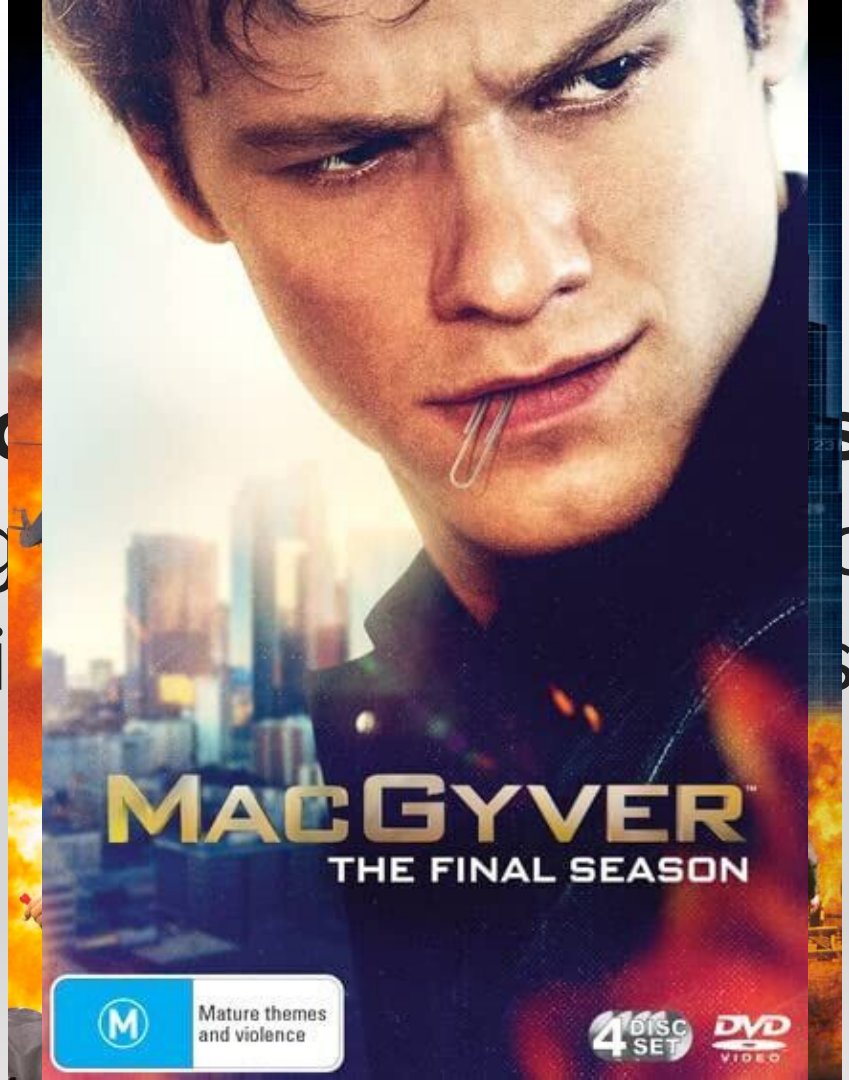
¿Hackers?

Hacker: Persona curiosa que le gusta ir más allá de los límites y convencionalismos.



Hac **sa** que
le g os
límí smos.

Hac **sa** que
le g os
límí smos.



- **Lise Meitner** (1878-1968): Fisión nuclear.
- **Alan Turing** (1912-1954)
- **Hedy Lamarr** (1914-2000): Wi-Fi y Bluetooth
- **Leonardo da Vinci** (1452-1519)
- **Michael Faraday** (1791-1867): Electricidad
- **Hypatia de Alejandría** (c. 350-415): Astrolabio
- **Arquímedes** (c. 287-212 BC): Desplazamiento del agua
- **Ada Lovelace** (1815-1852): Primera Programadora
- **Grace Hopper** (1906-1992): Primer compilador y COBOL

¿Entonces?

Hacker informático
cuyo objetivo es enriquecerse o ganar fama.

AKA **Ciberterrorista**

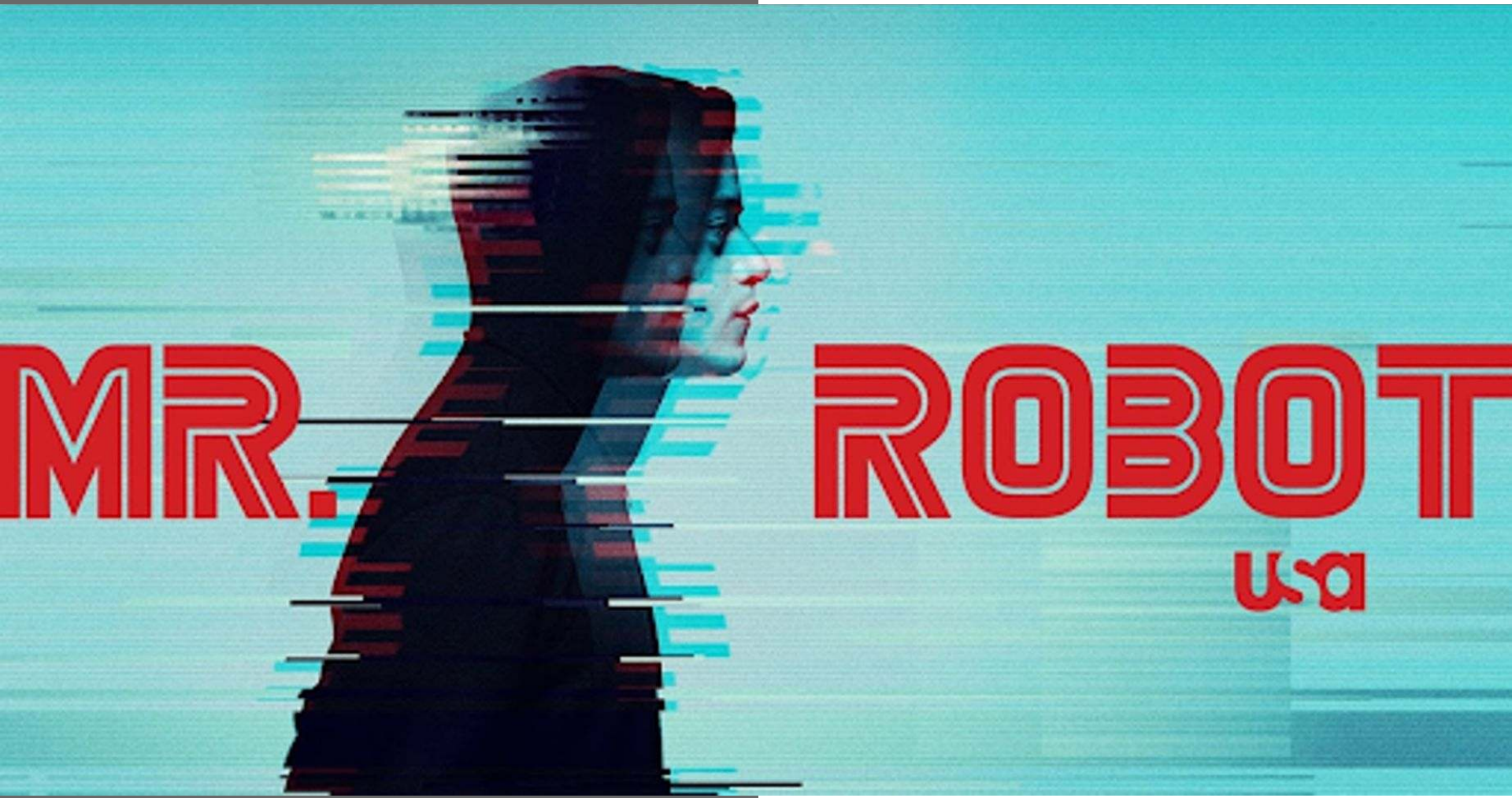
AKA **Atacante**

AKA **Pirata informático**

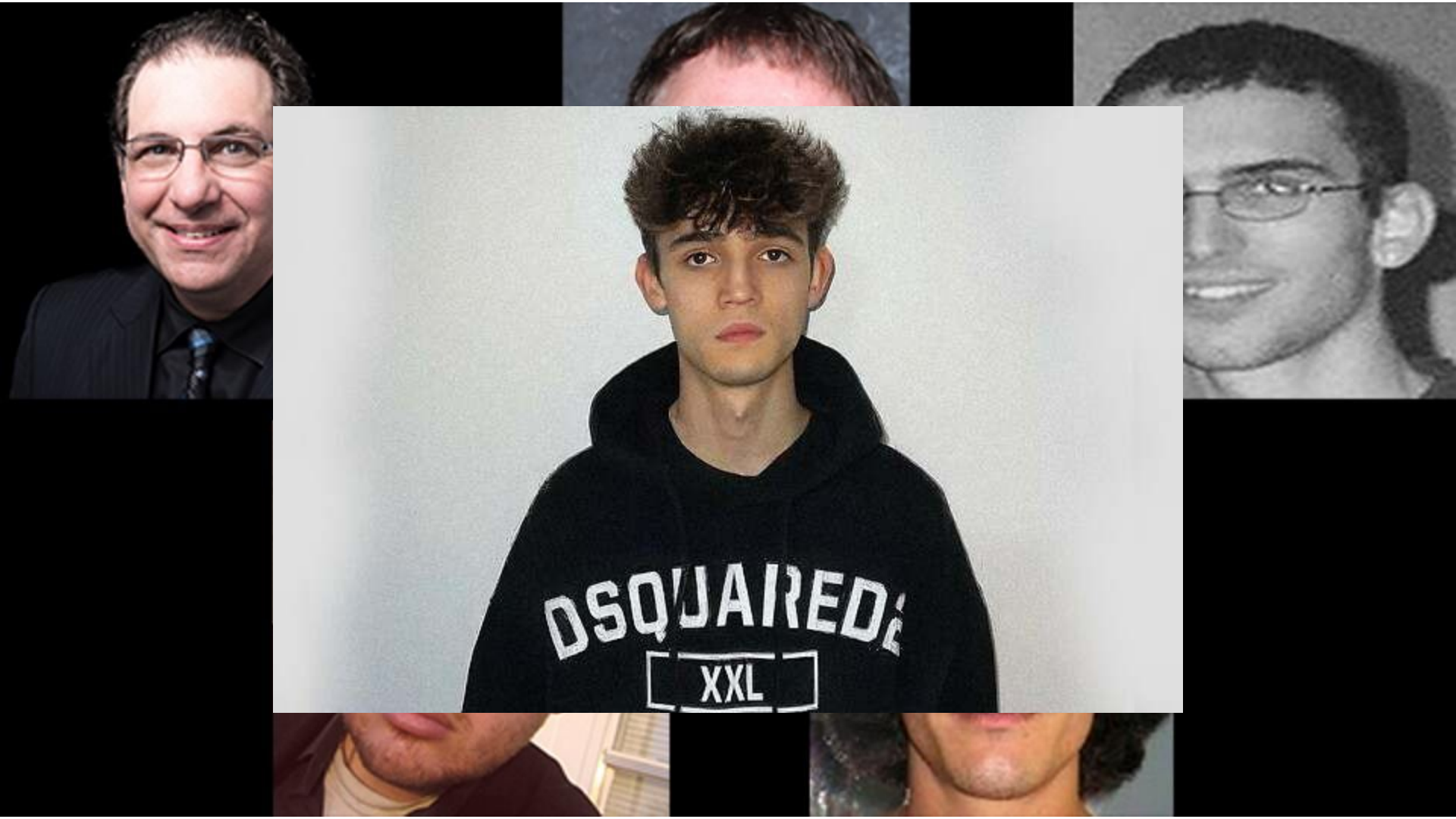
AKA **El enemigo**

AKA **El Malo**

AKA 


MR. ROBOT
usa

¡Pero hay tipos de hacker informático!


DSQUARED
XXL

Los hackers buenos

- Analistas de seguridad
- Equipos Red / Blue / Purple
- Servicio de soporte
- Plugins de seguridad

Hackers “A su bola”

- Hacktivistas
- Lobos solitarios
- Investigadores/ aprendices independientes

Los hackers malos

- Ciberterroristas
- Grupos organizados de cibercrimen
- Lobos solitarios
- Script-kiddies
- Espionaje

Evoluciones

- Mejoras en las capacidades de ataque o defensa
- Establecemos **3 niveles**:

- **Normal**

- **Guerrero** (Saiya-jin)

- **Super Guerrero** (Super Saiya-jin)

¿Cómo evolucionamos?

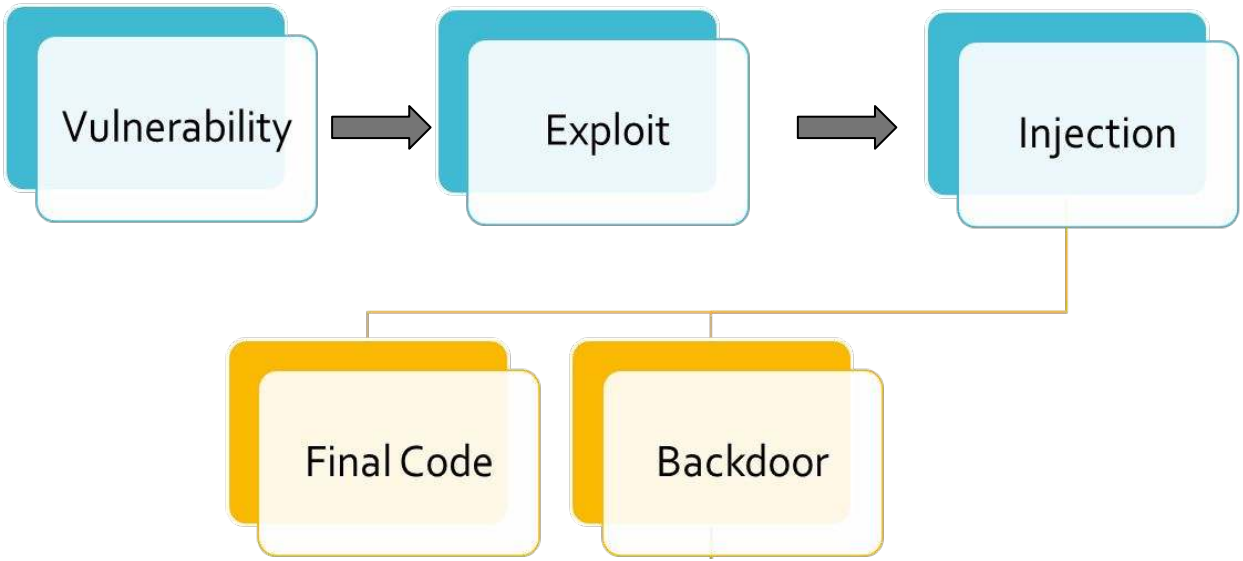
- Formándonos
- Asistiendo a charlas intensas como esta.
- Testeando
- Siendo hackeados (Fail fast and cheap)
- Instalando capas de seguridad.

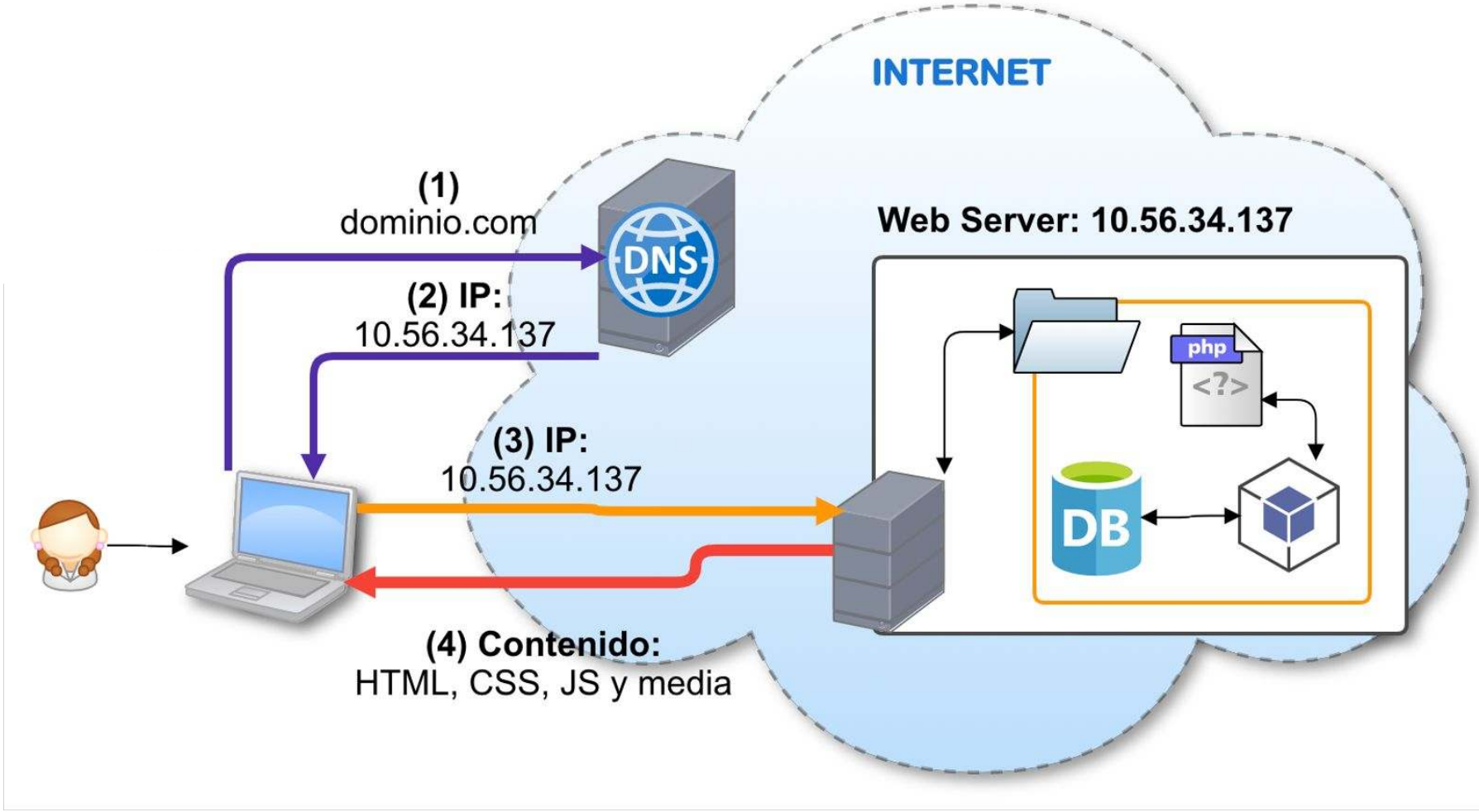
El problema:

El enemigo también evoluciona, y normalmente antes

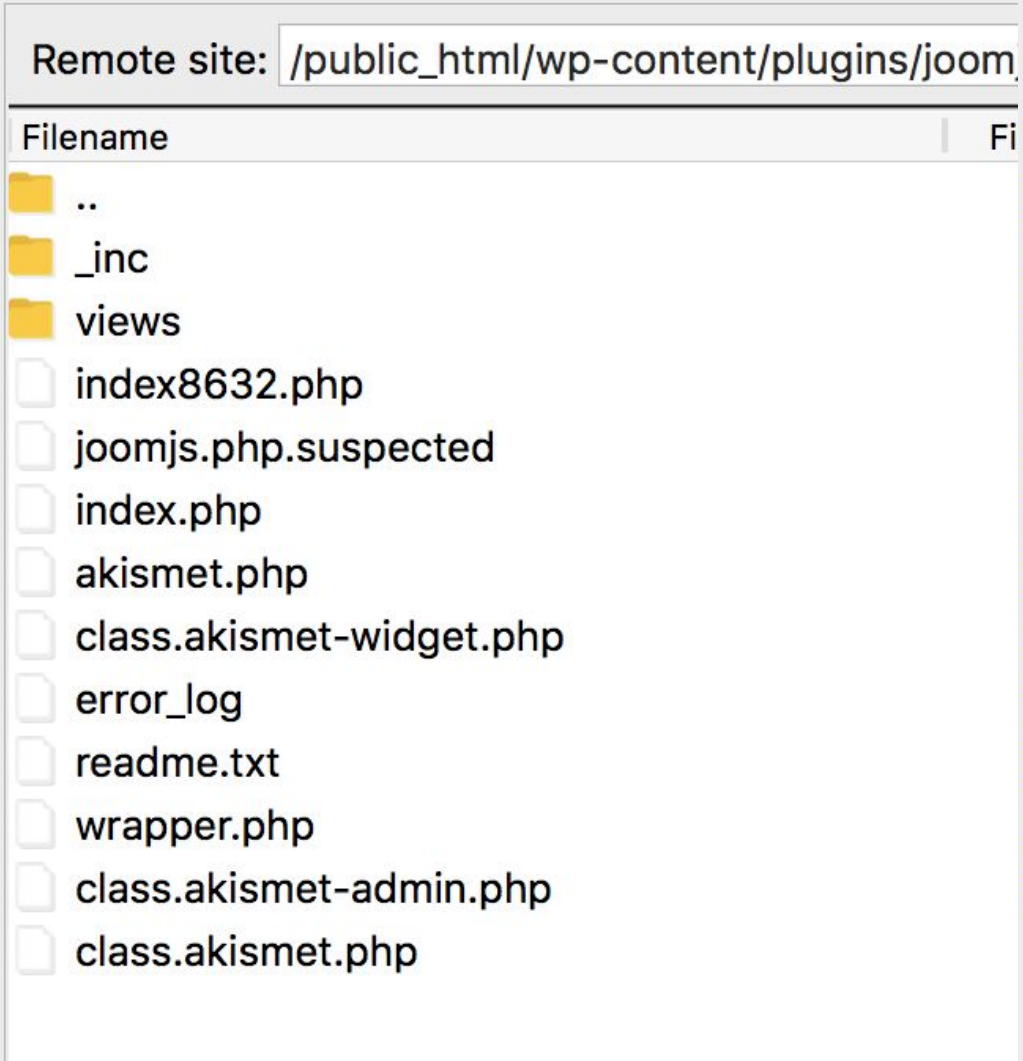

Cada ataque tiene
su defensa

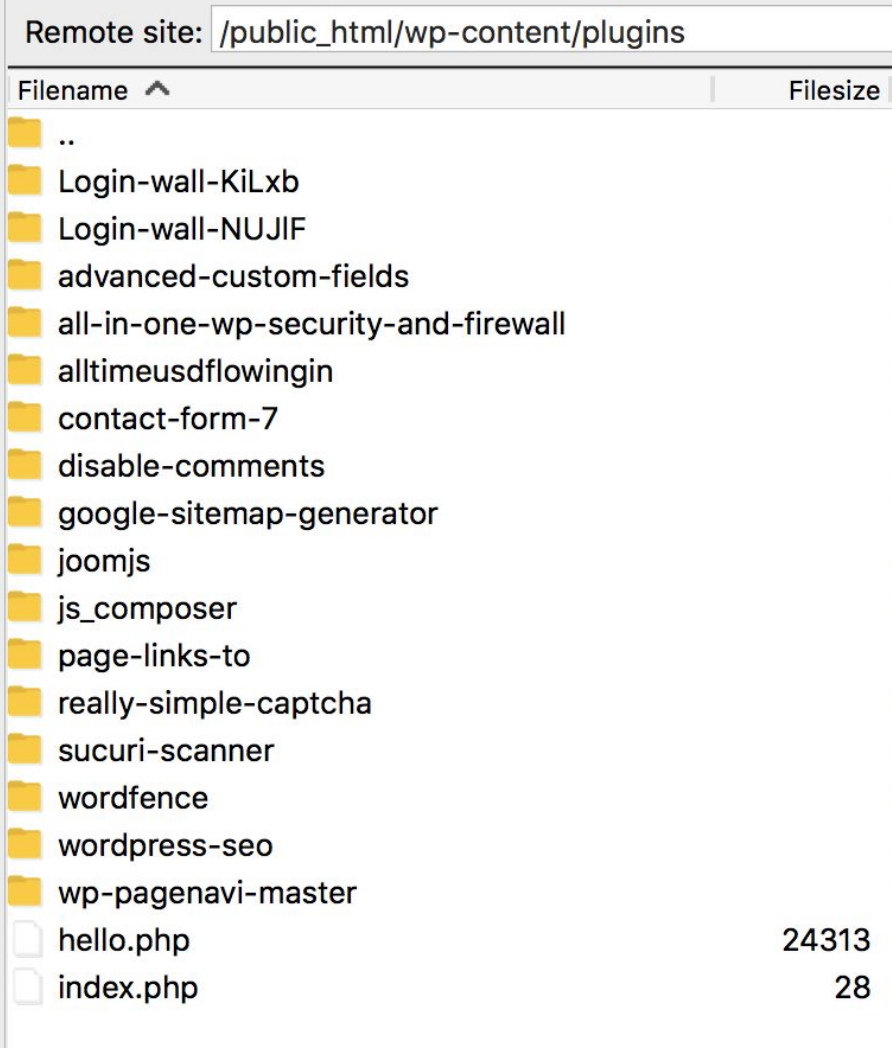
¿Cómo se hackea un WordPress?




INTERNET
(1)
dominio.com
DNS
(2) IP:
10.56.34.137
Web Server: 10.56.34.137
php
<?>
(3) IP:
10.56.34.137
DB
(4) Contenido:
HTML, CSS, JS y media

ATAQUE	Descripción	Categoría	Level	DEFENSA(S)
Phishing / Spam	Inyección o engaño, para captar información.	Reputación, Login		Habilidad, Frontend monitor


Remote site: /public_html/wp-content/plugins/joom
Filename
Fi
..
_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


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

Examples of fake Plugins/Themes

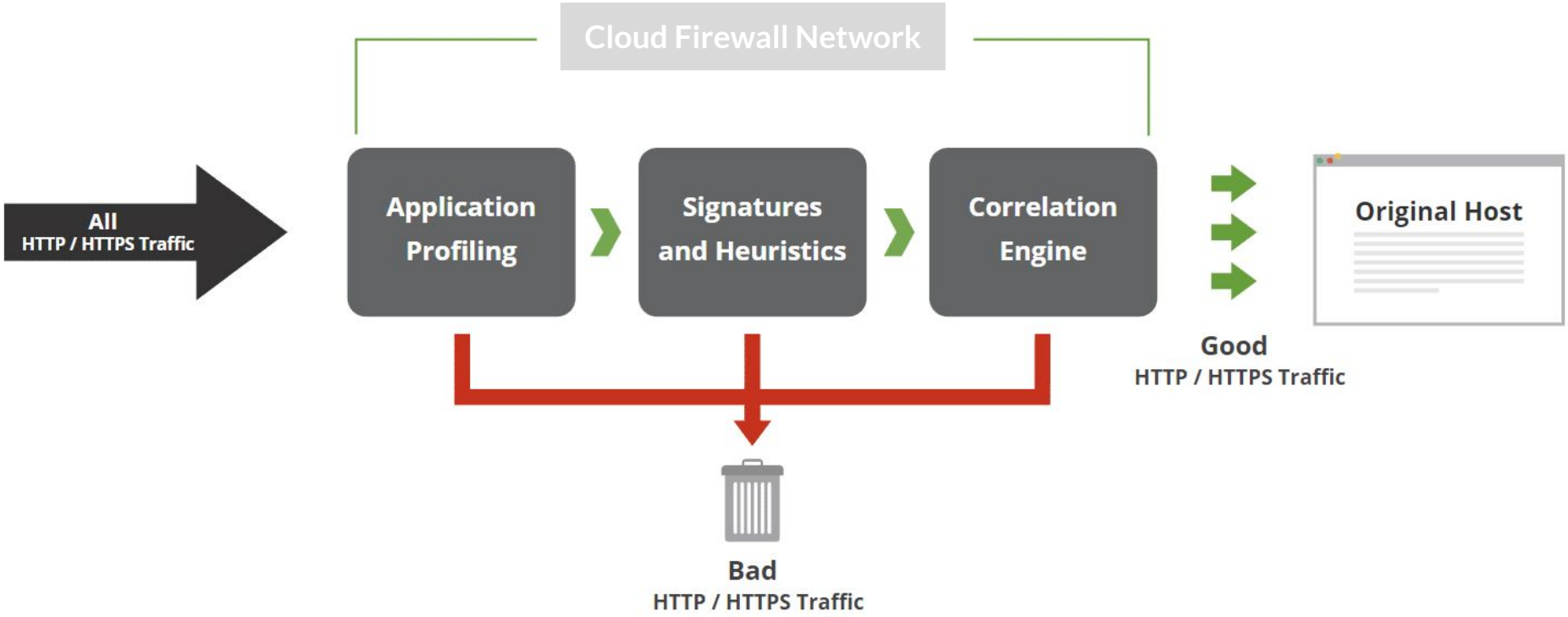
wp-content/plugins
wp-content/themes

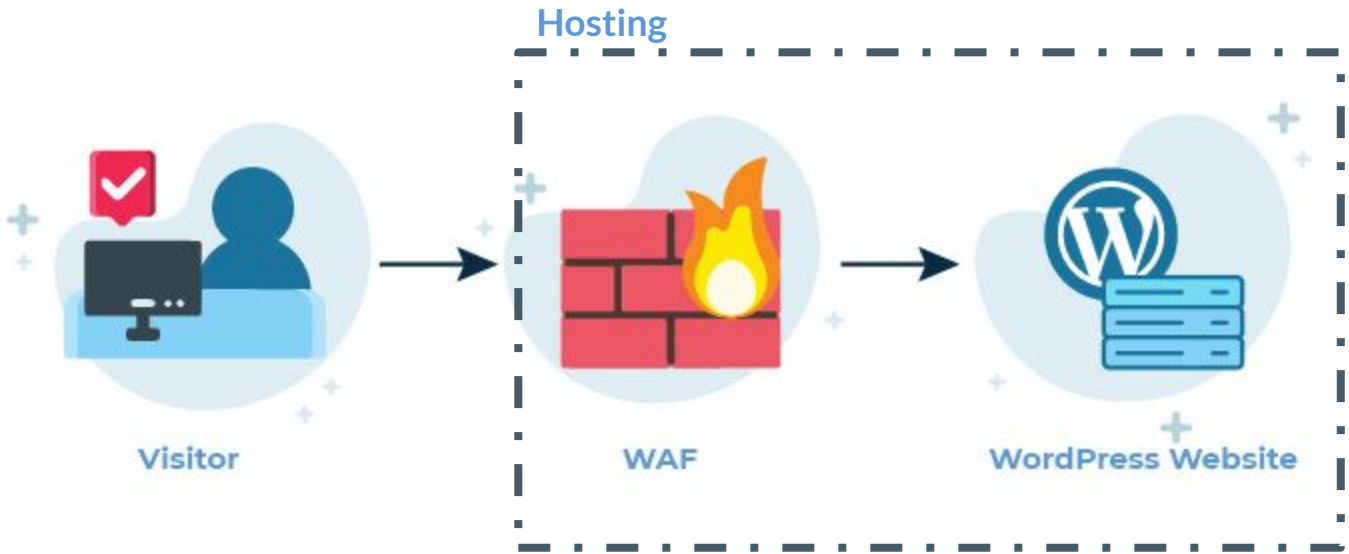
- **plugins**
  - wp-lazyload-{random chars}
  - task-controller
  - core-stab / core-engine
  - wp-zip
  - plugins
- **themes**
  - seotheme
  - classic
  - themes

ATAQUE	Descripción	Categoría	Level	DEFENSA(S)
Phishing / Spam	Inyección o engaño, para captar información.	Reputación, Login		Habilidad, Frontend monitor
Fuerza Bruta / Diccionario	Probar combinaciones de usuario/contraseña, informado o no. 💡 *Wikipedia*: 10,000_most_common_passwords 💡 haveibeenpwned.com	Login		WAF, plugin para limitar los intentos de plugin

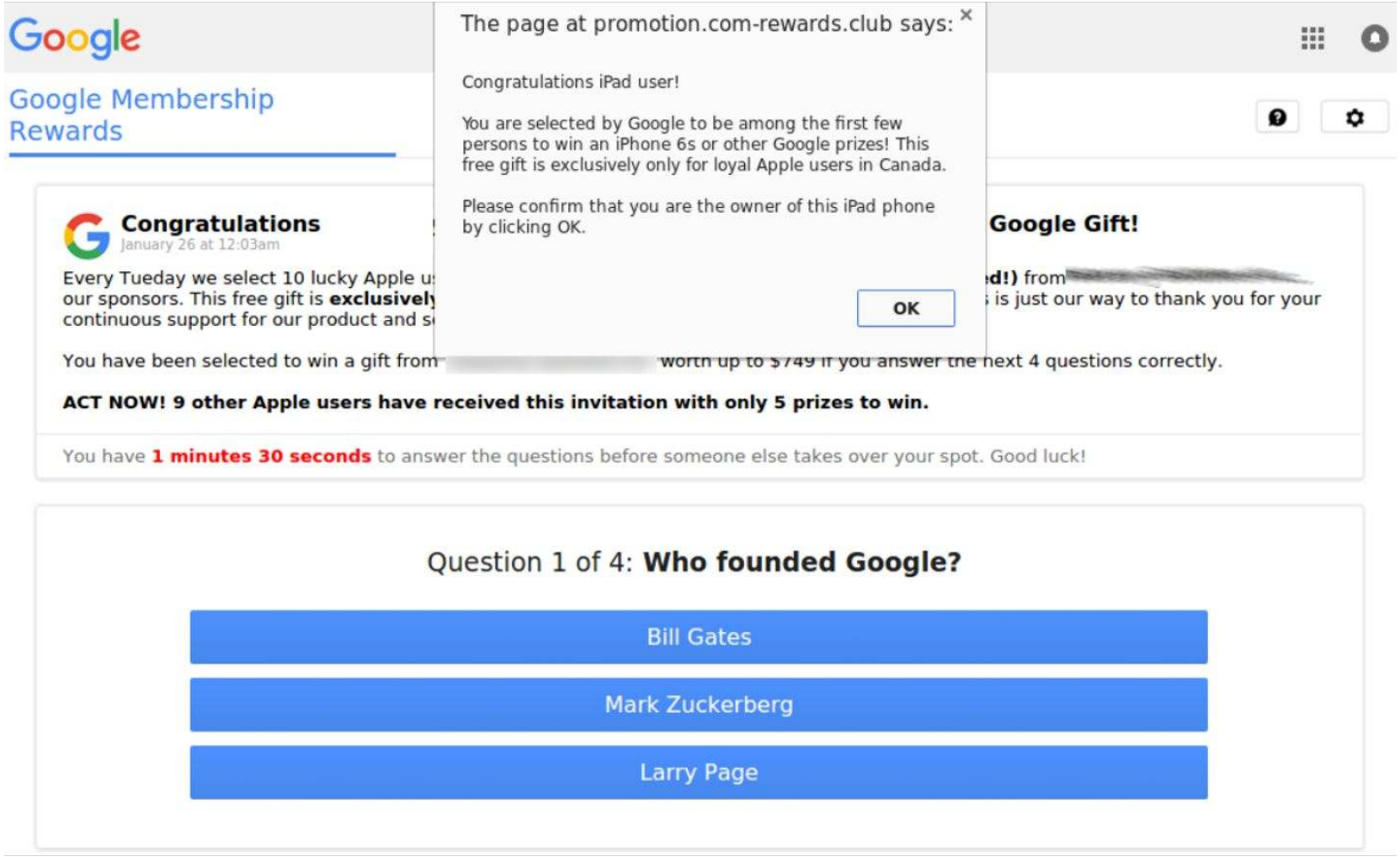
Website Application Firewall (WAF)

Protect and Speed Up Your Website




Hosting
Visitor
WAF
WordPress Website

ATAQUE	Descripción	Categoría	Level	DEFENSA(S)
Phishing / Spam	Inyección o engaño, para captar información.	Reputación, Login		Habilidad, Frontend monitor
Fuerza Bruta / Diccionario	Probar combinaciones de usuario/contraseña, informado o no. 💡 *Wikipedia*: 10,000_most_common_passwords 💡 haveibeenpwned.com	Login		WAF, plugin para limitar los intentos de plugin
XSS	Redirección (JS)	Reputación		WAF, Escáner de Integridad de Ficheros


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 exclusivel
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 -

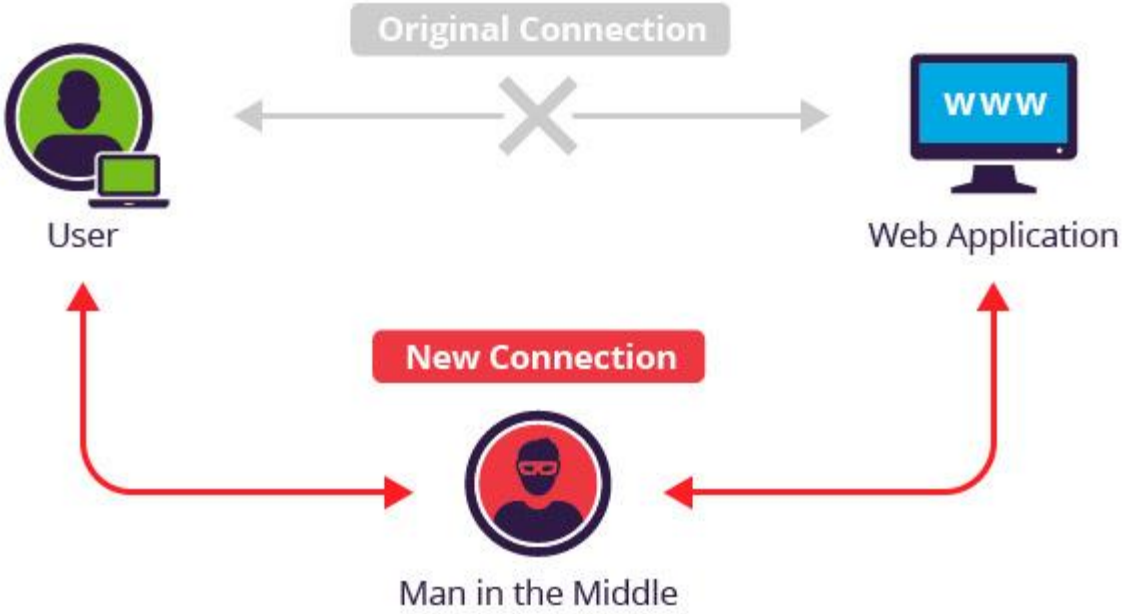
newsfile.club wants to

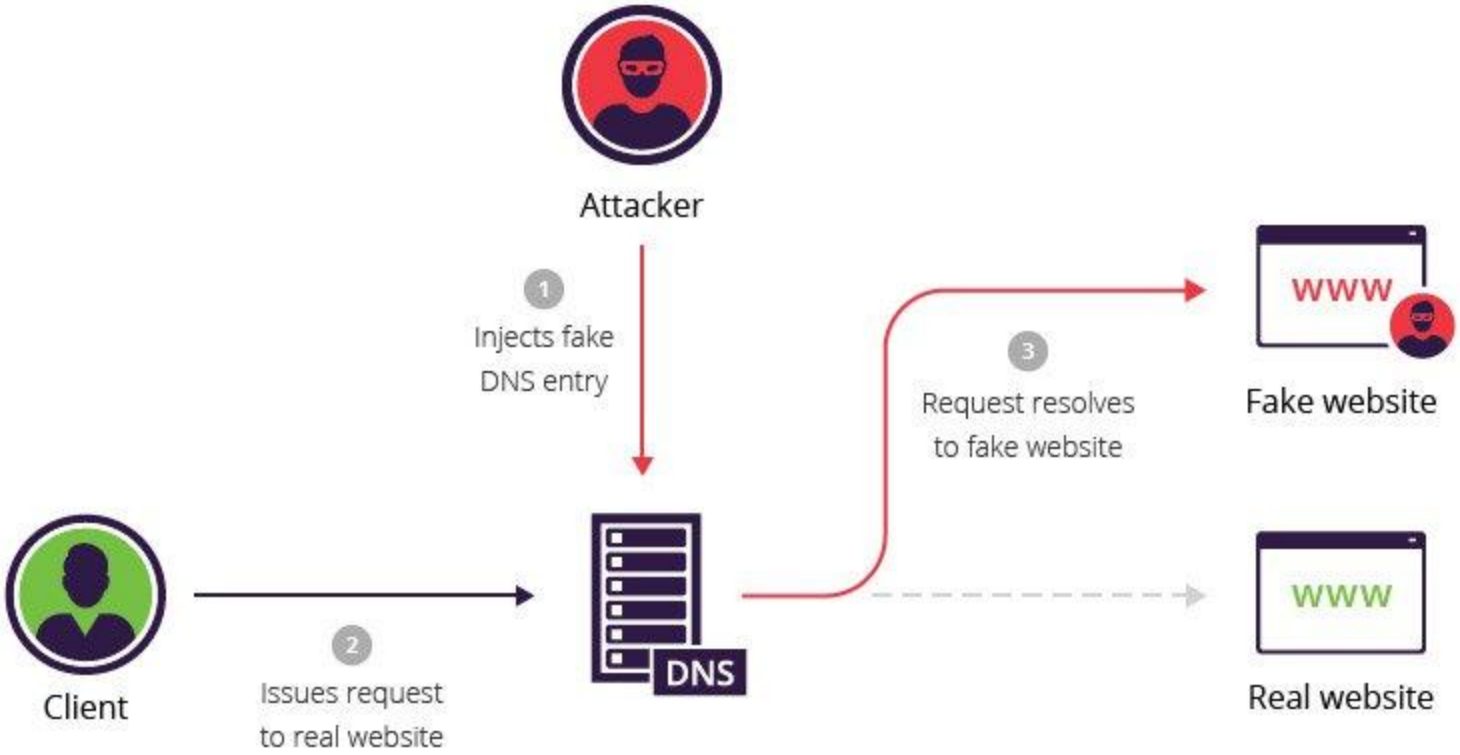
Show notifications

Block Allow

ATAQUE	Descripción	Categoría	Level	DEFENSA(S)
Phishing / Spam	Inyección o engaño, para captar información.	Reputación, Login		Habilidad, Frontend monitor
Fuerza Bruta / Diccionario	Probar combinaciones de usuario/contraseña, informado o no. 💡 *Wikipedia*: 10,000_most_common_passwords 💡 haveibeenpwned.com	Login		WAF, plugin para limitar los intentos de plugin
XSS	Redirección (JS)	Reputación		WAF, Escáner de Integridad de Ficheros
Nuevas Vuln	Descubrir nuevas vulnerabilidades	Investigación		WAF, mantenimiento

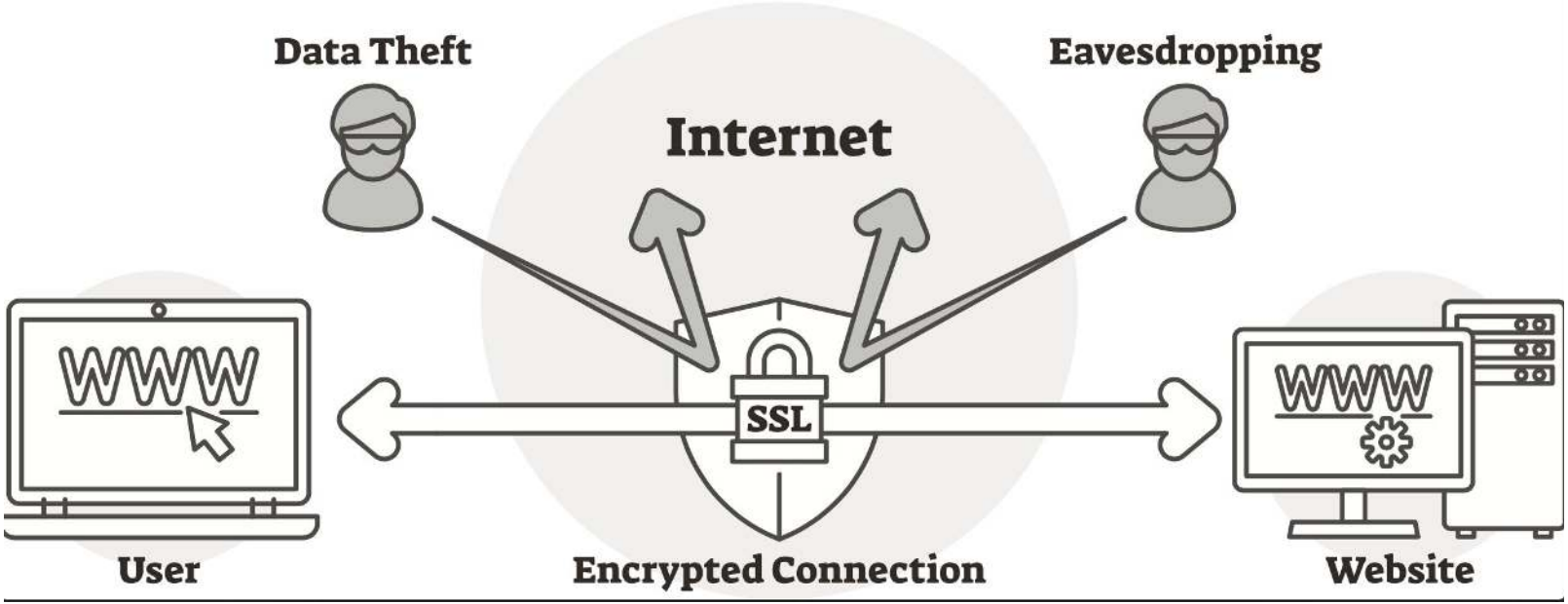
ATAQUE	Descripción	Categoría	Level	DEFENSA(S)
Phishing / Spam	Inyección o engaño, para captar información.	Reputación, Login		Habilidad, Frontend monitor
Fuerza Bruta / Diccionario	Probar combinaciones de usuario/contraseña, informado o no. 💡 *Wikipedia*: 10,000_most_common_passwords 💡 haveibeenpwned.com	Login		WAF, plugin para limitar los intentos de plugin
XSS	Redirección (JS)	Reputación		WAF, Escáner de Integridad de Ficheros
Nuevas Vuln	Descubrir nuevas vulnerabilidades	Investigación		WAF, mantenimiento
Man in the Middle	Intervenir comunicaciones	Comunicaciones		SSL/TLS

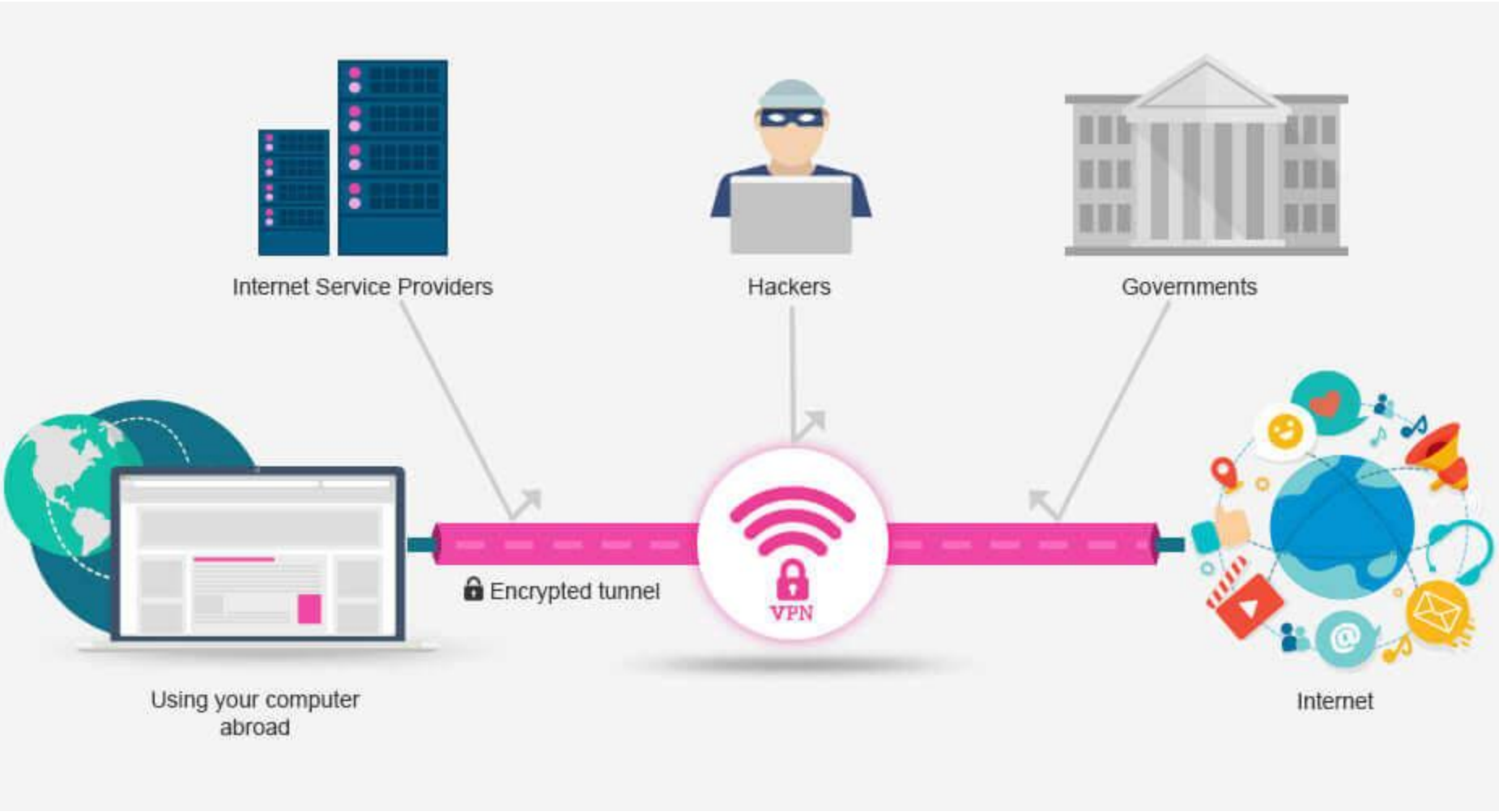

Original Connection
www
User
Web Application
New Connection
Man in the Middle


Attacker
1
Injects fake
DNS entry
3
Request resolves
to fake website
www
Fake website
Client
2
Issues request
to real website
DNS
www
Real website

SSL

Secure Sockets Layer




Internet Service Providers
Hackers
Governments
Encrypted tunnel
VPN
Using your computer abroad
Internet

ATAQUE	Descripción	Categoría	Level	DEFENSA(S)
Phishing / Spam	Inyección o engaño, para captar información.	Reputación, Login		Habilidad, Frontend monitor
Fuerza Bruta / Diccionario	Probar combinaciones de usuario/contraseña, informado o no. 💡 *Wikipedia*: 10,000_most_common_passwords 💡 haveibeenpwned.com	Login		WAF, plugin para limitar los intentos de plugin
XSS	Redirección (JS)	Reputación		WAF, Escáner de Integridad de Ficheros
Nuevas Vuln	Descubrir nuevas vulnerabilidades	Investigación		WAF, mantenimiento
Man in the Middle	Intervenir comunicaciones	Comunicaciones		SSL/TLS
DoS / DDoS	Deshabilitar servicios	Comunicaciones, Recursos		WAF


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
TYPE
SERVICE
PORT

ATAQUE	Descripción	Categoría	Level	DEFENSA(S)
SQL Injection	Ataque a la base de datos	Base de Datos		WAF, Logs

ATAQUE	Descripción	Categoría	Level	DEFENSA(S)
SQL Injection	Ataque a la base de datos	Base de Datos		WAF, Logs
Ransomware	Secuestro de los datos/ficheros	Ficheros		Backups

{ Onanimus7 R4nsomwar3 }

Your Website Is Encrypt3d

Don't Change the Filename because it Can Damage the File If You Want to Return You Must Enter the Password First
Send Me $200 For Back Your Website

Bitcoin (BTC) Address : 1HmEGmGDuBrTEb3Q4NQ

Password Decrypt

Contact Telegram : @feyensss

~Tap Background to music~

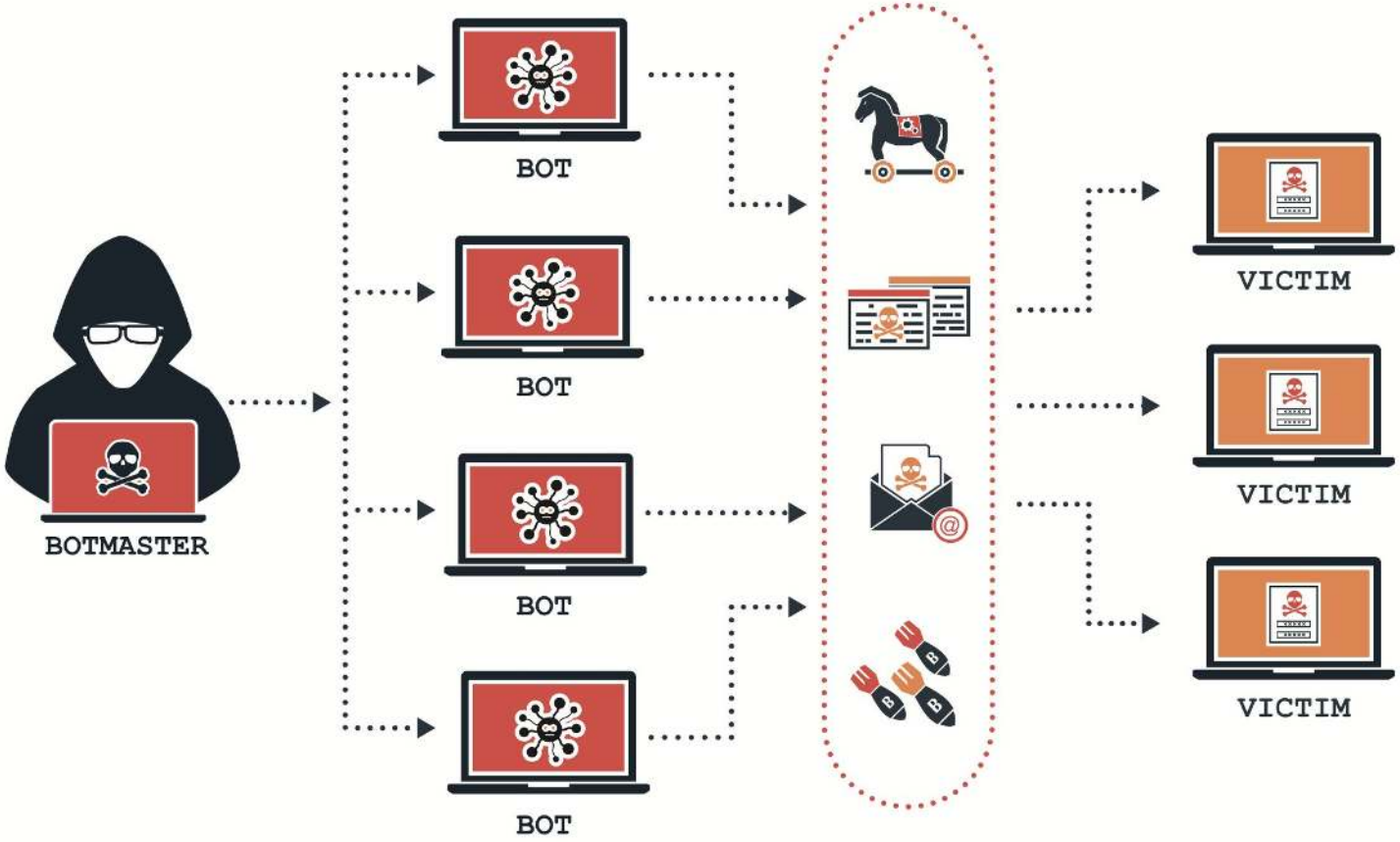
.ftpquota.0x4f6e616e696d757337	17	0X4F6E616...	26/
.htabackup	114	HTABACK...	26/
.htabackup.0x4f6e616e696d757337	57	0X4F6E616...	26/
.htaccess-DISABLED	114	HTACCESS...	26/
.htaccess.0x4f6e616e696d757337	57	0X4F6E616...	26/
7.php.0x4f6e616e696d757337	215	0X4F6E616...	26/
anon.php	5.063	PHP File	26/
anon.php.0x4f6e616e696d757337	2.742	0X4F6E616...	26/
cgi-bin.zip.0x4f6e616e696d757337	202.318.369	0X4F6E616...	19/
error_log	32.096	File	27/
error_log.0x4f6e616e696d757337	2.304	0X4F6E616...	26/
googlec55310faa35e04c1.html	54	Firefox HT...	27/
index.html	697	Firefox HT...	27/
index.php	0	PHP File	27/
index.php.0x4f6e616e696d757337	251	0X4F6E616...	26/
license.txt.0x4f6e616e696d757337	7.283	0X4F6E616...	26/
onanimus7.php.0x4f6e616e696d757337	2.130	0X4F6E616...	26/
readme.html.0x4f6e616e696d757337	2.993	0X4F6E616...	26/
test.html.0x4f6e616e696d757337	5	0X4F6E616...	26/
wp-activate.php.0x4f6e616e696d757337	2.416	0X4F6E616...	26/
wp-blog-header.php.0x4f6e616e696d757337	225	0X4F6E616...	26/
wp-comments-post.php.0x4f6e616e696d75...	1.046	0X4F6E616...	26/
wp-config-sample.php.0x4f6e616e696d757...	1.190	0X4F6E616...	26/
wp-config.php.0x4f6e616e696d757337	1.884	0X4F6E616...	26/

wp-config.php.0x4f6e616e696d757337

```
8d57 d972 e248 167d 1e7f 4556 cf44 a8ca
63b3 d86c aeee 8929 81d8 8c30 8ba0 28fb
8548 a414 4a90 9442 9962 7147 fffb dc4c
2116 574d 44db 8e00 a3bb 2fe7 1efe f86f
e445 37f9 dbdb 1b74 8b26 1e41 0bcc 09b2
59e8 d265 1263 4159 885c 16a3 198b 9d61
4c38 07b9 4c74 17dd a782 39b0 81ec 98a4
e2dc 8e69 2450 c209 47c2 a31c b9d4 27c8
4962 1a2e e103 22d5 69c8 05f6 7da5 9043
af2c 410e 0b35 813c bc25 4830 a92c 45d1
8e2c 10a7 82dc a103 c8d8 3894 ca36 8b0e
1796 41fc b7ab 507e 4338 74e4 331f fc28
335b ec27 84e7 4eb1 67aa a023 30c4 a284
5ce6 fb6c 2783 bc4a 9f7f 3daa dda2 fec1
1a99 8813 2140 8aa7 9f59 0412 1768 4d0e
c70f 0c2c b02a 22bc 808b 2826 2edd a78f
f4ba 35d4 279d a3bd 6f3e 0dd7 c813 22e2
5ff3 799b 3964 9fdb 4199 2359 e61c 8b97
f9a6 43a5 a7f9 5576 9976 84ed 355e 92ab
cee4 6f6e f279 74fb 3152 74af 4a0c e543
4b88 5595 8e86 2e43 6ecc 0259 d958 15da
```

ATAQUE	Descripción	Categoría	Level	DEFENSA(S)
SQL Injection	Ataque a la base de datos	Base de Datos		WAF, Logs
Ransomware	Secuestro de los datos/ficheros	Ficheros		Backups
Cryptomining	Uso de infraestructura ajena para minar cripto	Recursos		Logs, users

ATAQUE	Descripción	Categoría	Level	DEFENSA(S)
SQL Injection	Ataque a la base de datos	Base de Datos		WAF, Logs
Ransomware	Secuestro de los datos/ficheros	Ficheros		Backups
Cryptomining	Uso de infraestructura ajena para minar cripto	Recursos		Logs, users
BotNode	Uso del sitio infectado (zombie) como plataforma de ataque.	Comunicaciones, Ficheros		WAF, Logs

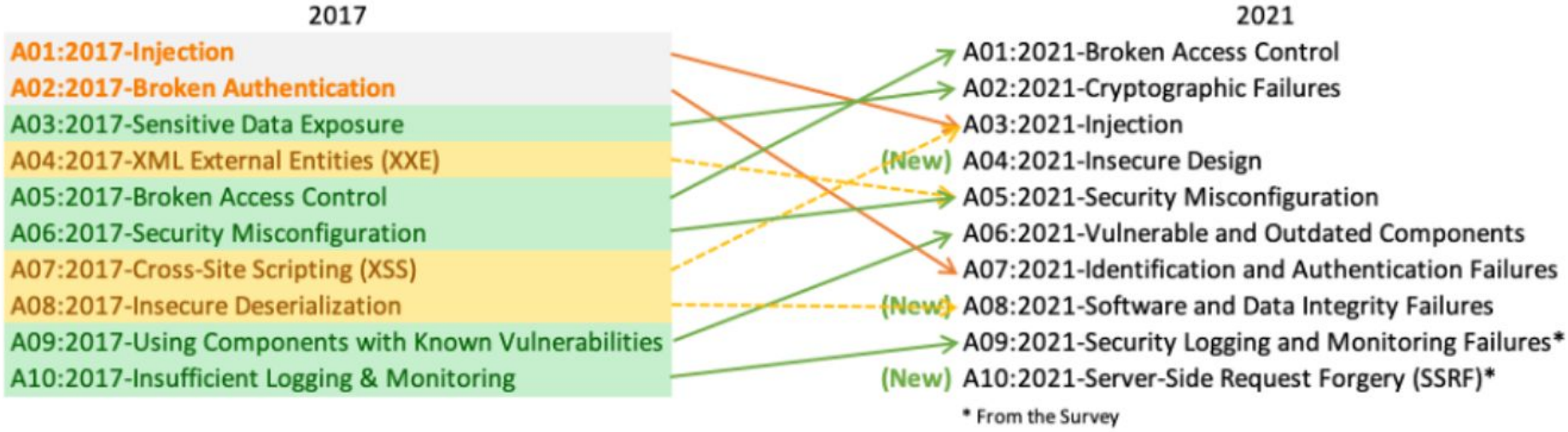

BOTMASTER
BOT
BOT
BOT
BOT
VICTIM
VICTIM
VICTIM

ATAQUE	Descripción	Categoría	Level	DEFENSA(S)
SQL Injection	Ataque a la base de datos	Base de Datos		WAF, Logs
Ransomware	Secuestro de los datos/ficheros	Ficheros		Backups
Cryptomining	Uso de infraestructura ajena para minar cripto	Recursos		Logs, users
BotNode	Uso del sitio infectado (zombie) como plataforma de ataque.	Comunicaciones, Ficheros		WAF, Logs
Cross-Site Contamination	Desde un sitio hackeado o una backup, infectar el resto de sitios.	Ficheros, Base de Datos		Escáner de Integridad de Ficheros

ATAQUE	Descripción	Categoría	Level	DEFENSA(S)
Phishing / Spam	Inyección o engaño, para captar información.	Reputación, Login		Habilidad, Frontend monitor
Fuerza Bruta / Diccionario	Probar combinaciones de usuario/contraseña, informado o no. 💡 *Wikipedia*: 10,000_most_common_passwords 💡haveibeenpwned.com	Login		WAF, plugin para limitar los intentos de plugin
XSS	Redirección (JS)	Reputación		WAF, Escáner de Integridad de Ficheros
Nuevas Vuln	Descubrir nuevas vulnerabilidades	Investigación		WAF, mantenimiento
Man in the Middle	Intervenir comunicaciones	Comunicaciones		SSL/TLS
DoS / DDoS	Deshabilitar servicios	Comunicaciones, Recursos		WAF
SQL Injection	Ataque a la base de datos	Base de Datos		WAF, Logs

Top 10 Web Application Security Risks

There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021.



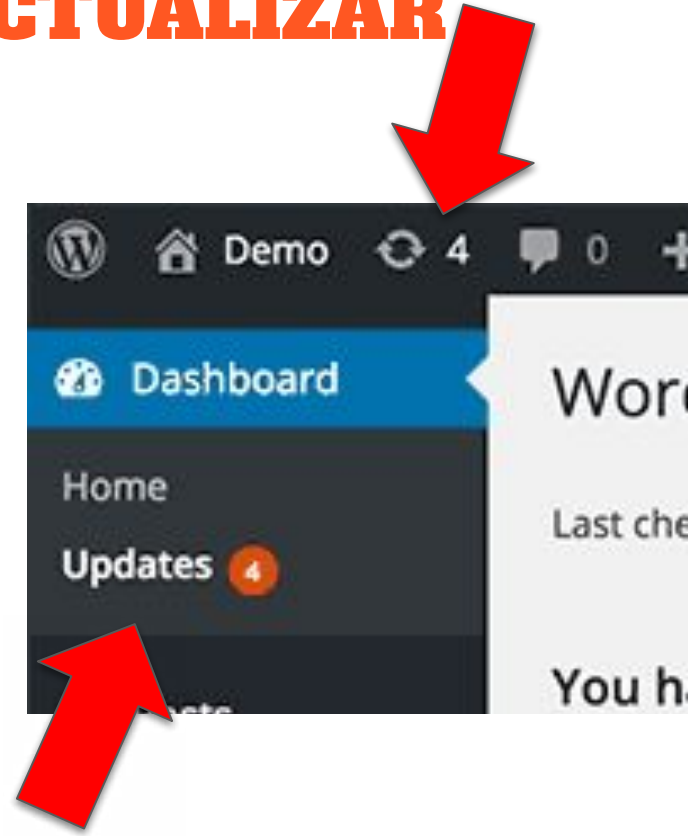

AI Conundrum
¿Y qué pasa con la IA?

WordPress Security

https://es.wordpress.org/about/security/

SCAN ME

La importancia de ACTUALIZAR



- Tapas agujeros de seguridad (**Security patches**)
- Los parches de seguridad aparecen después del exploit
- Sobreescribes con **código limpio**
- >70% de las infecciones son debidas a **plugins/temas desactualizados**.


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

La importancia de LAS CONTRASEÑAS & MFA

Factores de **AUTENTICACIÓN**:

- Algo que el usuario **es** (huella digital, identificación facial,...).
- Algo que el usuario **tiene** (teléfono celular, yubikey, ...)
- Algo que el usuario **sabe** (contraseña, PIN, ...).

KAME

Hame

HAAAAAA

Kame Hame Haaa!

- **Base: 1 Buen Hosting**
  - SSL/**TLS**
  - Soporte + BackUps
  - Plan gestionado
- **Escáner Vulnerabilidades + WAF interno**
  - Patchstack
- **Backups**
  - BlogVault o UpDraft

- **WAF + CDN**
  - Sucuri (limpiezas gratis)
    o CloudFlare.
- **Plugins de Seguridad**
  - Solid Security
  - Fail2Ban
    o Limit Login Attempts Reloaded
  - CAPTCHA 4WP
  - WP Activity Log


Everybody needs a hacker

WORDCAMP MADRID 2023

¡Gracias!
¿Preguntas?