O cómo sobrevivir a un ataque de un hacker malicioso

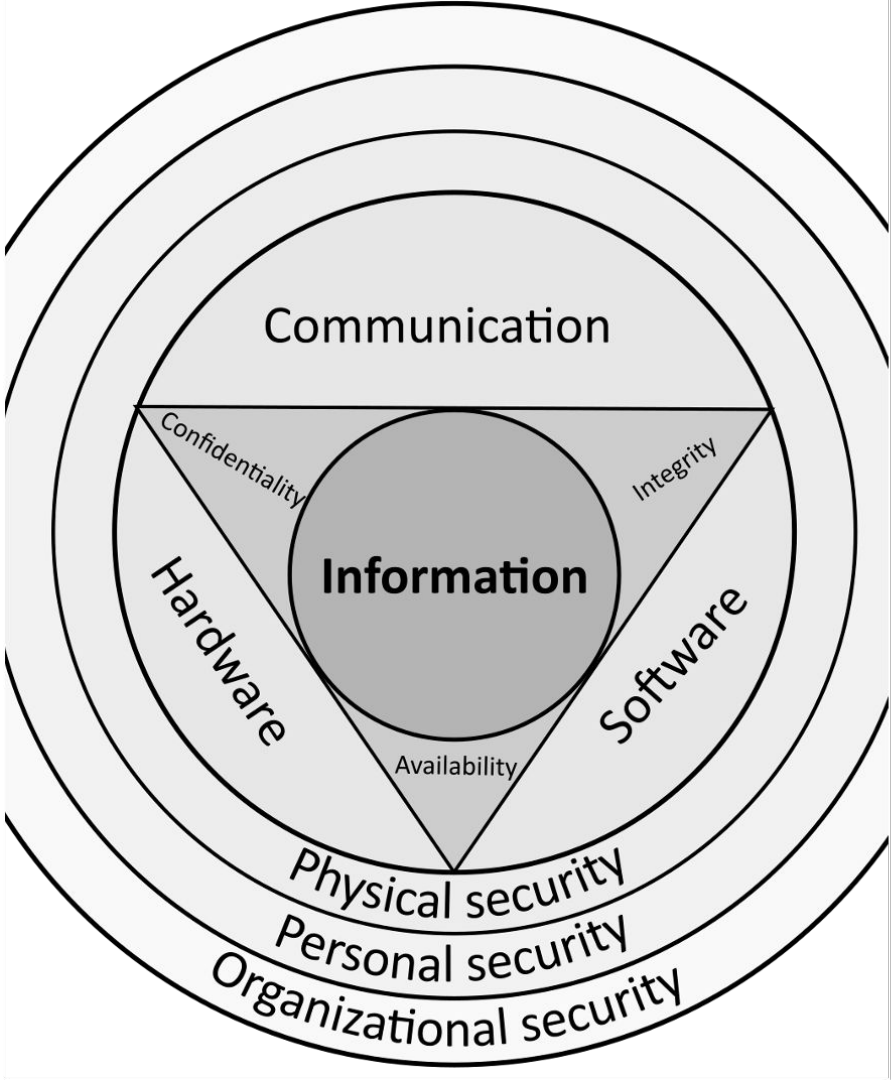
Néstor Angulo de Ugarte (@pharar)

WordCamp Zaragoza 2023

PUSH START
INSERT COIN

Néstor Angulo

- **CISSP** (ISC2.org - 2022)
- **Analista de Seguridad Web**
  - @ GoDaddy WebSecurity
  - @ Sucuri.net
- **@pharar**



Qué es la Seguridad de Información

Concepto CID (CIA)

- Confidencialidad
- Integridad
- Disponibilidad

Concepto FAD (DAD)

- Filtración
- Alteración
- Destrucción

El Juego

Tu fortaleza

Representa tu Sitio WordPress


KO
ROUND 1
FIGHT!

Posibles OBJETIVOS en tu sitio web

Usuarios	Base de datos	Contenido
Infrastructura	Bot Net	Reputación

La barra de vida

Representa la capacidad de protección de tu sitio web.
Más barra, más **probabilidad** de ganar.


1P
800 NIN
50000
KO
78
KEN
DHALSIM

Factores que afectan a la barra

- **Cada medida de defensa** que añades en cada categoría **suma puntos,** hasta el máximo de los 100pts.
- **No actualizar tu sitio ->** Afecta bajando un 5% tu barra cada mes.
- Por **cada admin adicional** que añades, afecta la velocidad de bajada de la barra un 2% adicional por mes.
- 0pts, significa que hasta un scriptkiddie te puede hackear el sitio.

Personajes

Hacker:

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

Ciberterrorista / Cracker:

Hacker informático, cuyo objetivo es siempre enriquecerse en una situación juego de suma cero.

- Thales de Mileto.
- Leonardo da Vinci.
- Thomas Edison.
- Arquímedes.
- Benjamin Franklin.
- Louis Pasteur y Alexander Fleming.
- Los hermanos Montgolfier y Clément Ader.
- Nikola Tesla.

Hackers Buenos

- White Hat Hackers
- Equipo Azul / Blue Team
- Equipo Rojo / Red Team
- Equipo Púrpura / Purple Team
- Analistas de Seguridad
- Soporte Técnico
- Plugins de Seguridad

Paquito

Nuestro hacker bueno

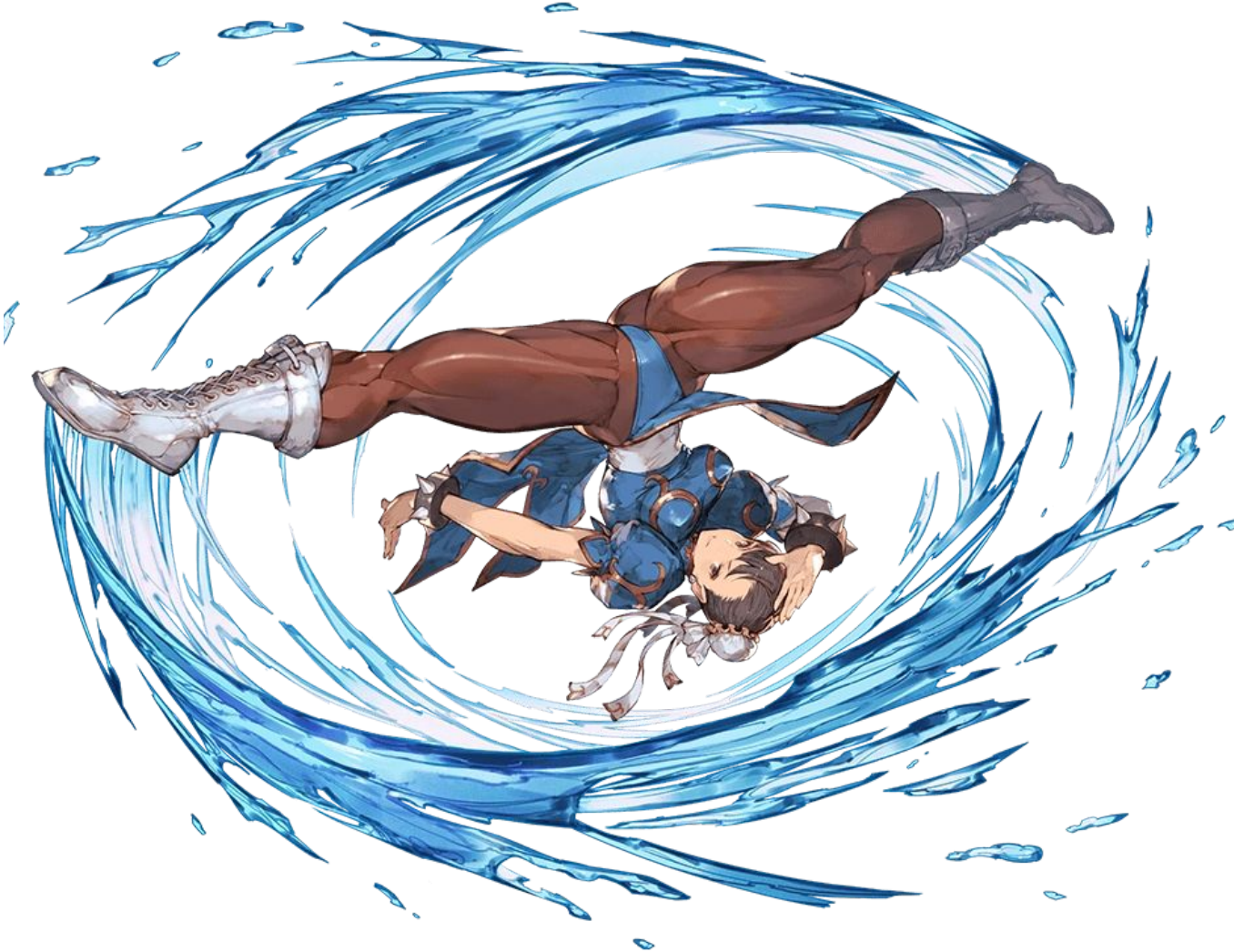

K.O.
powerdrain

Hackers
“A su rollo”

- Grey Hat Hackers
- Hacktivistas

Anika

Nuestra hacker “freelance”.



Hackers Malotes

- Black Hat Hacker
- Ciberterrorista / Criminales
- ScriptKiddies
- Lobos solitarios
- Equipos Organizados

La Cami

Nuestra *ScriptKiddie*.
Barra de vida: **20-30pts**.

Bruce

Nuestro Black Hat Hacker profesional.
Barra de vida: **50-70pts**.

El general

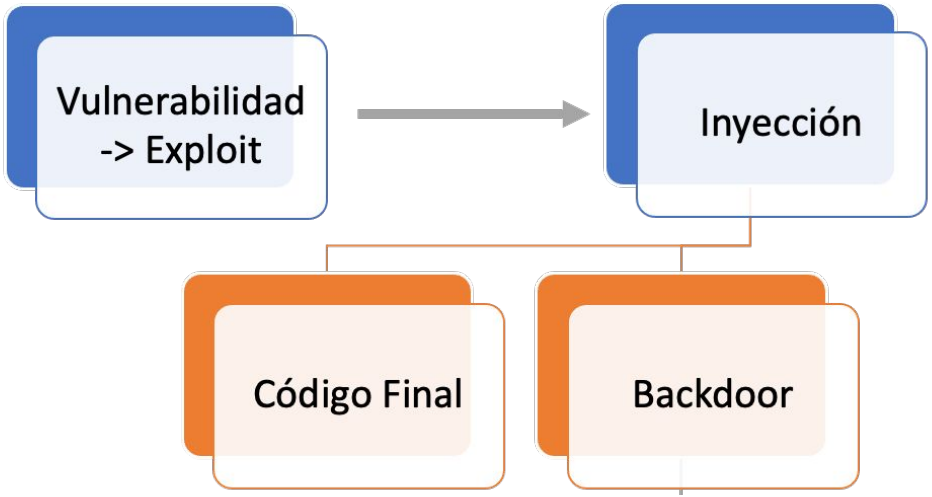
Nuestro equipo organizado de hackers malos.

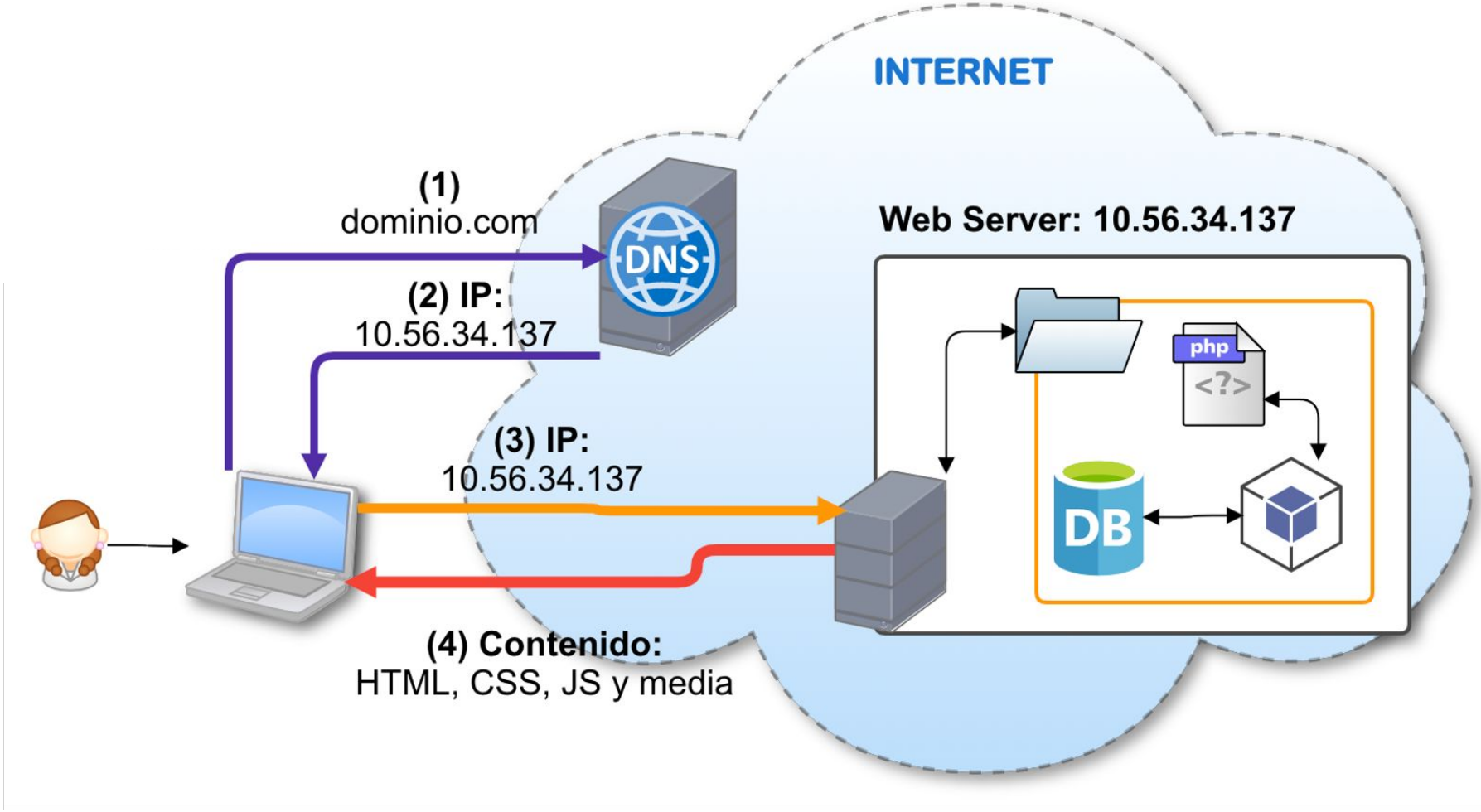
El malo jefe. El Boss.

Barra de vida: **100pts**.

Ataques

¿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	Nivel
Phishing / Spam	Inyección o uso de, para captar información.	Reputación, Login	

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

Ejemplos de Plugins/Temas fake

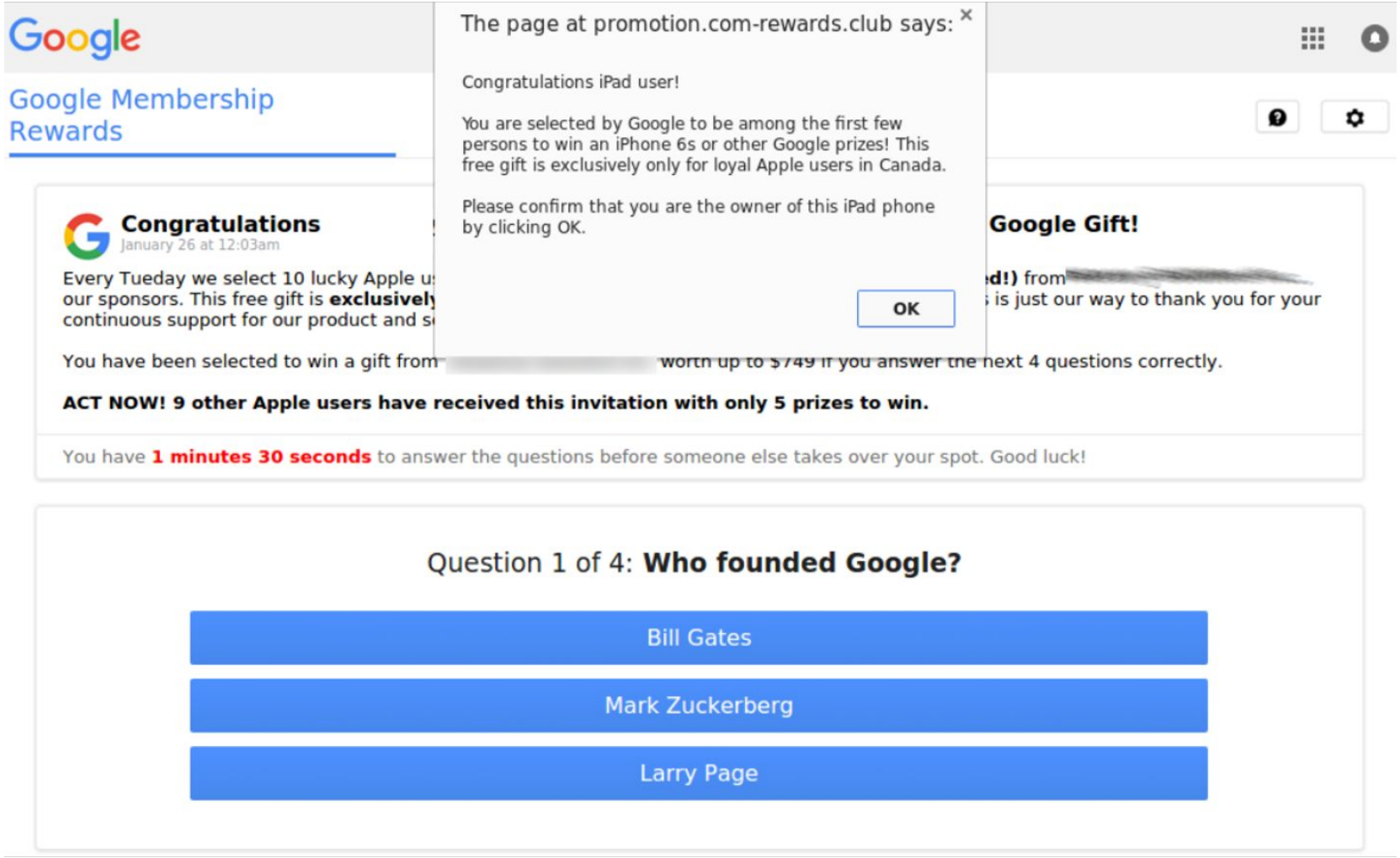
wp-content/plugins
wp-content/themes

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


Email
Password
Sign in
Cannot access your account?

Ataque	Descripción	Categoría	Nivel
Phishing / Spam	Inyección o uso de, para captar información.	Reputación, Login	
Fuerza Bruta / Diccionario	Probar combinaciones de usuario/contraseña, informado o no. 💡 *Wikipedia*: 10,000_most_common_passwords 💡 haveibeenpwned.com	Login	

Ataque	Descripción	Categoría	Nivel
Phishing / Spam	Inyección o uso de, para captar información.	Reputación, Login	
Fuerza Bruta / Diccionario	Probar combinaciones de usuario/contraseña, informado o no. 💡 *Wikipedia*: 10,000_most_common_passwords 💡 haveibeenpwned.com	Login	
XSS	Redirección (JS)	Reputación	


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 -

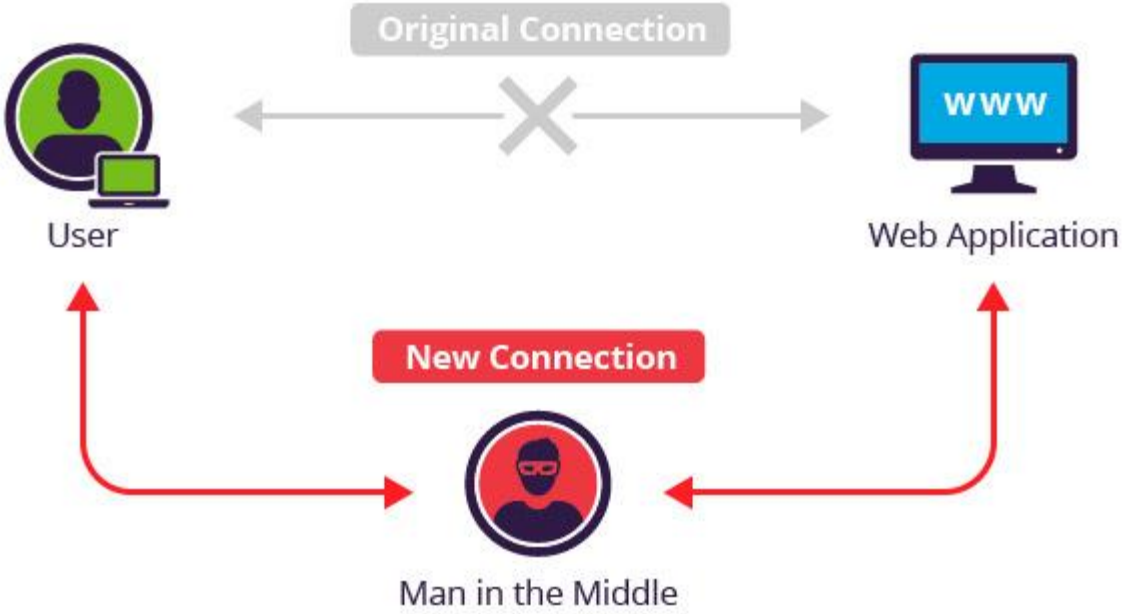
newsfile.club wants to

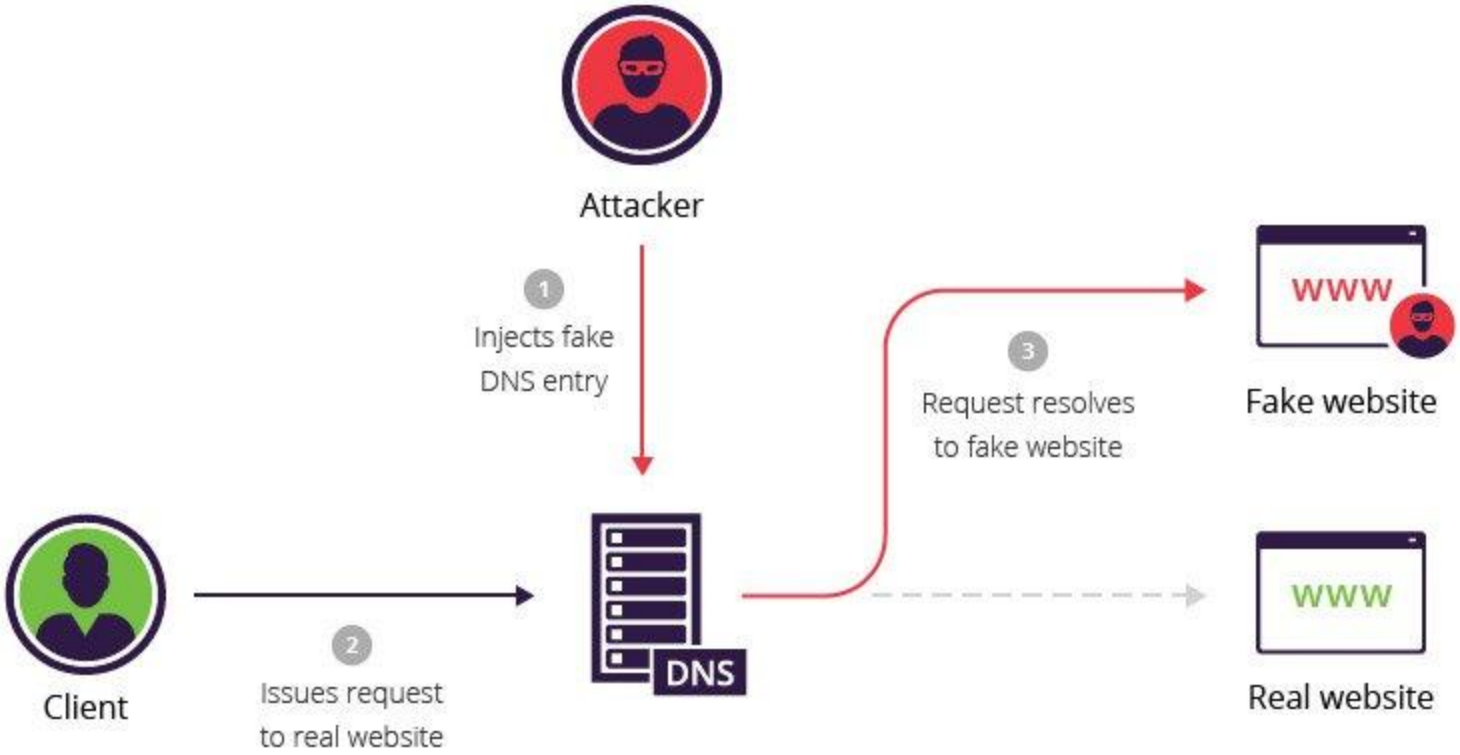
Show notifications

Block Allow

Ataque	Descripción	Categoría	Nivel
Phishing / Spam	Inyección o uso de, para captar información.	Reputación, Login	
Fuerza Bruta / Diccionario	Probar combinaciones de usuario/contraseña, informado o no. 💡 *Wikipedia*: 10,000_most_common_passwords 💡 haveibeenpwned.com	Login	
XSS	Redirección (JS)	Reputación	
Nuevas vulnerabilidades	Descubrir nuevas vulnerabilidades	Investigación	

Ataque	Descripción	Categoría	Nivel
Phishing / Spam	Inyección o uso de, para captar información.	Reputación, Login	
Fuerza Bruta / Diccionario	Probar combinaciones de usuario/contraseña, informado o no. 💡 *Wikipedia*: 10,000_most_common_passwords 💡 haveibeenpwned.com	Login	
XSS	Redirección (JS)	Reputación	
Nuevas vulnerabilidades	Descubrir nuevas vulnerabilidades	Investigación	
Man in the Middle	Intervenir comunicaciones	Comunicaciones	


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

Ataque	Descripción	Categoría	Nivel
Phishing / Spam	Inyección o uso de, para captar información.	Reputación, Login	
Fuerza Bruta / Diccionario	Probar combinaciones de usuario/contraseña, informado o no. 💡 *Wikipedia*: 10,000_most_common_passwords 💡 haveibeenpwned.com	Login	
XSS	Redirección (JS)	Reputación	
Nuevas vulnerabilidades	Descubrir nuevas vulnerabilidades	Investigación	
Man in the Middle	Intervenir comunicaciones	Comunicaciones	
DoS / DDoS	Deshabilitar un servicio	Comunicaciones, recursos	

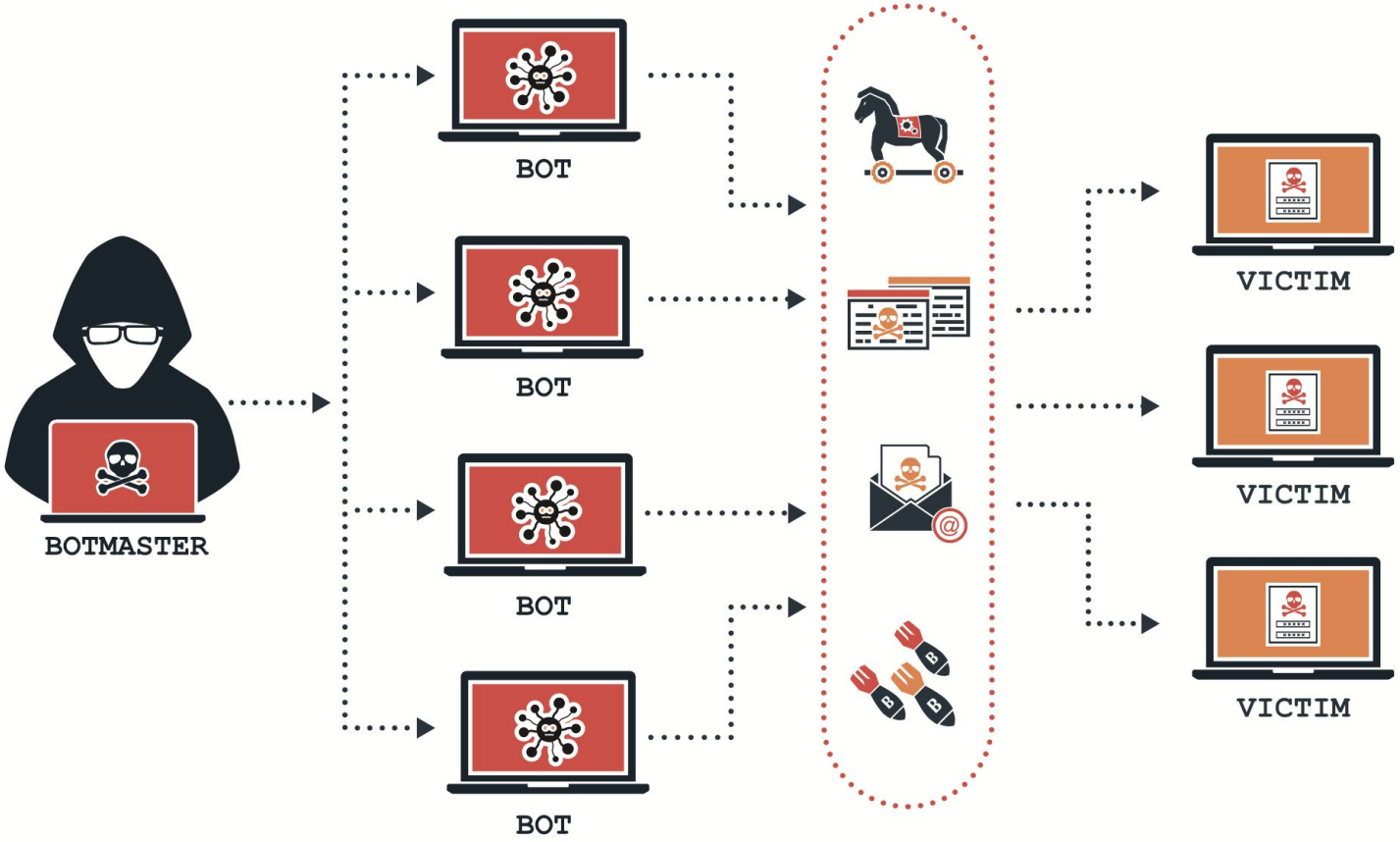

NORSE
ATTACK ORIGINS
COUNTRY
China
United States
Russia
Saudi Arabia
Netherlands
France
Moldova
South Korea
Brazil
Finland
ATTACK TARGETS
COUNTRY
United States
Saudi Arabia
United Arab Emirates
Philippines
Liechtenstein
France
Russia
Taiwan
Cyprus
Mexico
ATTACK TYPES
SERVICE
PORT
LIVE ATTACKS
TIMESTAMP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

Ataque	Descripción	Categoría	Nivel
Phishing / Spam	Inyección o uso de, para captar información.	Reputación, Login	
Fuerza Bruta / Diccionario	Probar combinaciones de usuario/contraseña, informado o no. 💡 *Wikipedia*: 10,000_most_common_passwords 💡 haveibeenpwned.com	Login	
XSS	Redirección (JS)	Reputación	
Nuevas vulnerabilidades	Descubrir nuevas vulnerabilidades	Investigación	
Man in the Middle	Intervenir comunicaciones	Comunicaciones	
DoS / DDoS	Deshabilitar un servicio	Comunicaciones, recursos	
SQL Injection	Ataque a la base de datos	Base de datos	

Ataque	Descripción	Categoría	Nivel
Phishing / Spam	Inyección o uso de, para captar información.	Reputación, Login	
Fuerza Bruta / Diccionario	Probar combinaciones de usuario/contraseña, informado o no. 💡 *Wikipedia*: 10,000_most_common_passwords 💡 haveibeenpwned.com	Login	
XSS	Redirección (JS)	Reputación	
Nuevas vulnerabilidades	Descubrir nuevas vulnerabilidades	Investigación	
Man in the Middle	Intervenir comunicaciones	Comunicaciones	
DoS / DDoS	Deshabilitar un servicio	Comunicaciones, recursos	
SQL Injection	Ataque a la base de datos	Base de datos	
Ransomware	Secuestro de los datos/ficheros	Ficheros	

Ataque	Descripción	Categoría	Nivel
Cryptomining	Uso de infraestructura ajena para minar cripto	Recursos	

Ataque	Descripción	Categoría	Nivel
Cryptomining	Uso de infraestructura ajena para minar cripto	Recursos	
BotNode	Uso del sitio infectado (zombie) como plataforma de ataque.	Comunicaciones, Ficheros	

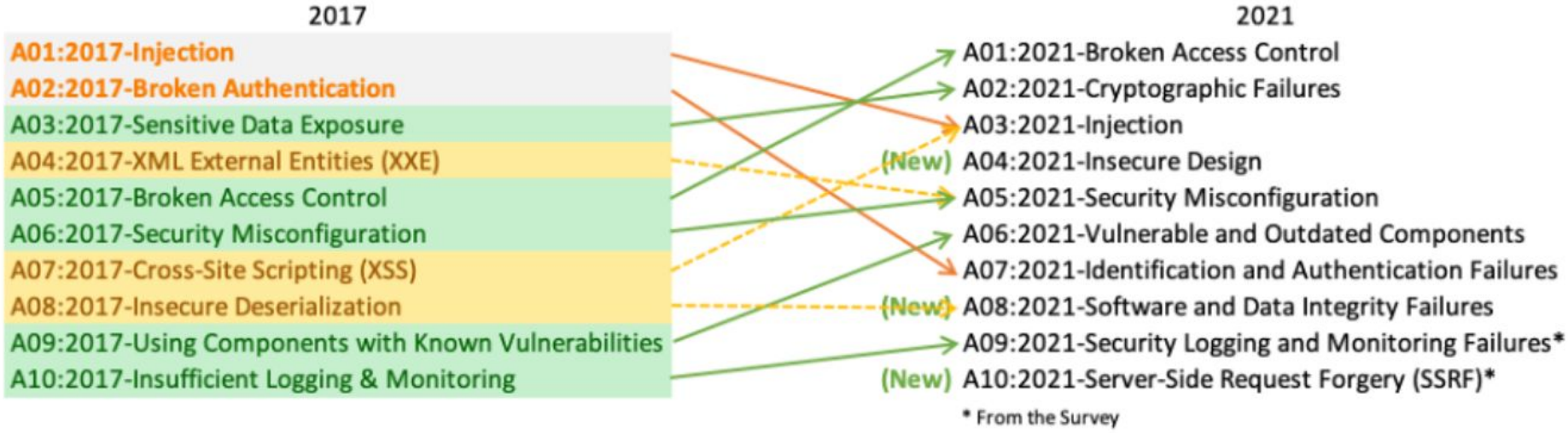

BOTMASTER
BOT
BOT
BOT
BOT
VICTIM
VICTIM
VICTIM

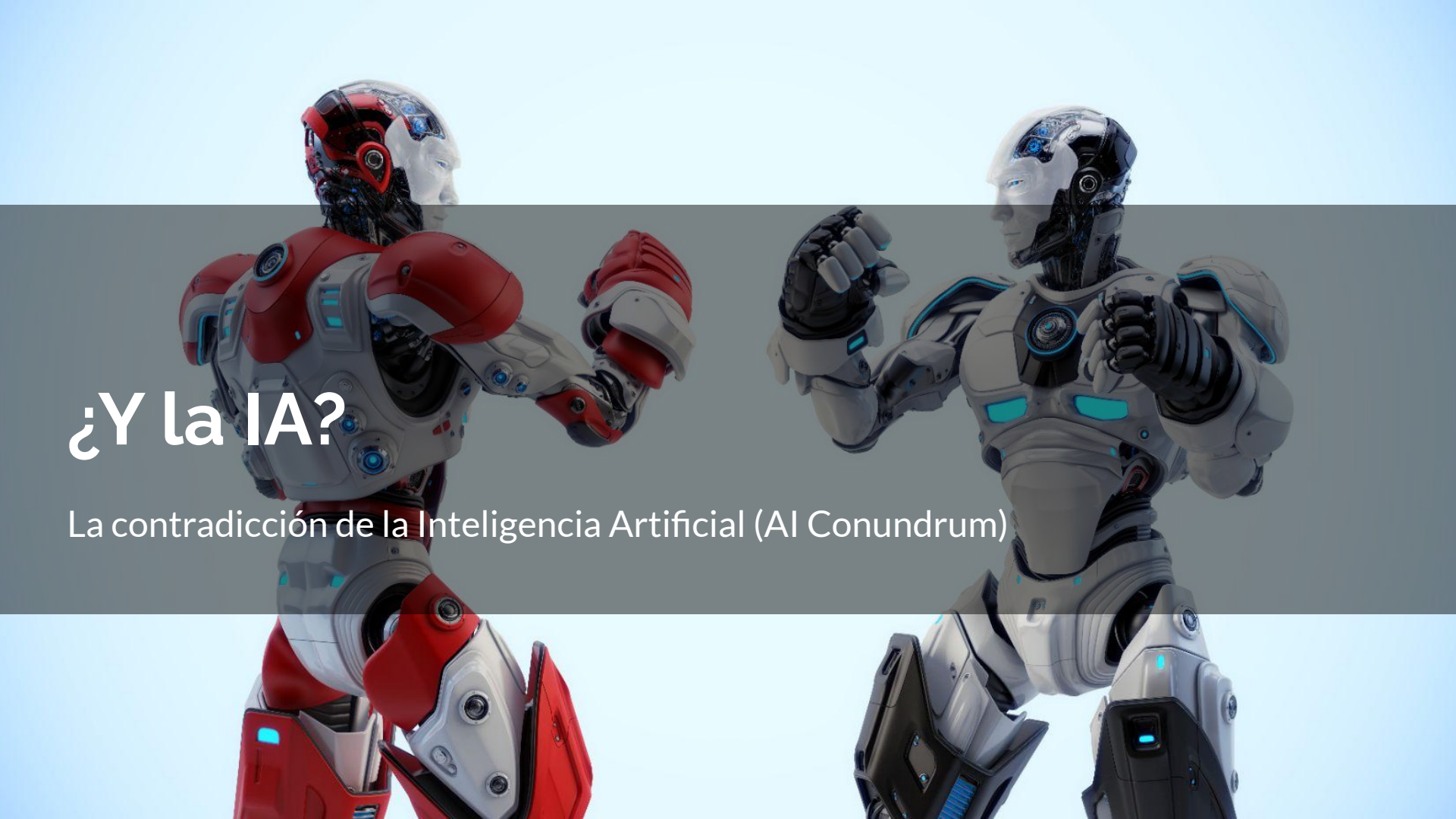
Ataque	Descripción	Categoría	Nivel
Cryptomining	Uso de infraestructura ajena para minar cripto	Recursos	
BotNode	Uso del sitio infectado (zombie) como plataforma de ataque.	Comunicaciones, Ficheros	
Cross-site Contamination	Desde un sitio hackeado o una copia de seguridad, infectar otros sitios	Ficheros	

Ataque	Descripción	Categoría	Nivel
Phishing / Spam	Inyección o uso de, para captar información.	Reputación, Login	
Fuerza Bruta / Diccionario	Probar combinaciones de usuario/contraseña, informado o no. 💡 *Wikipedia*: 10,000_most_common_passwords 💡 haveibeenpwned.com	Login	
XSS	Redirección (JS)	Reputación	
Nuevas vulnerabilidades	Descubrir nuevas vulnerabilidades	Investigación	
Man in the Middle	Intervenir comunicaciones	Comunicaciones	
DoS / DDoS	Deshabilitar un servicio	Comunicaciones, recursos	
SQL Injection	Ataque a la base de datos	Base de datos	
Ransomware	Secuestro de los datos/ficheros	Ficheros	
Cryptomining	Uso de infraestructura ajena para minar cripto	Recursos	

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.





¿Y la IA?

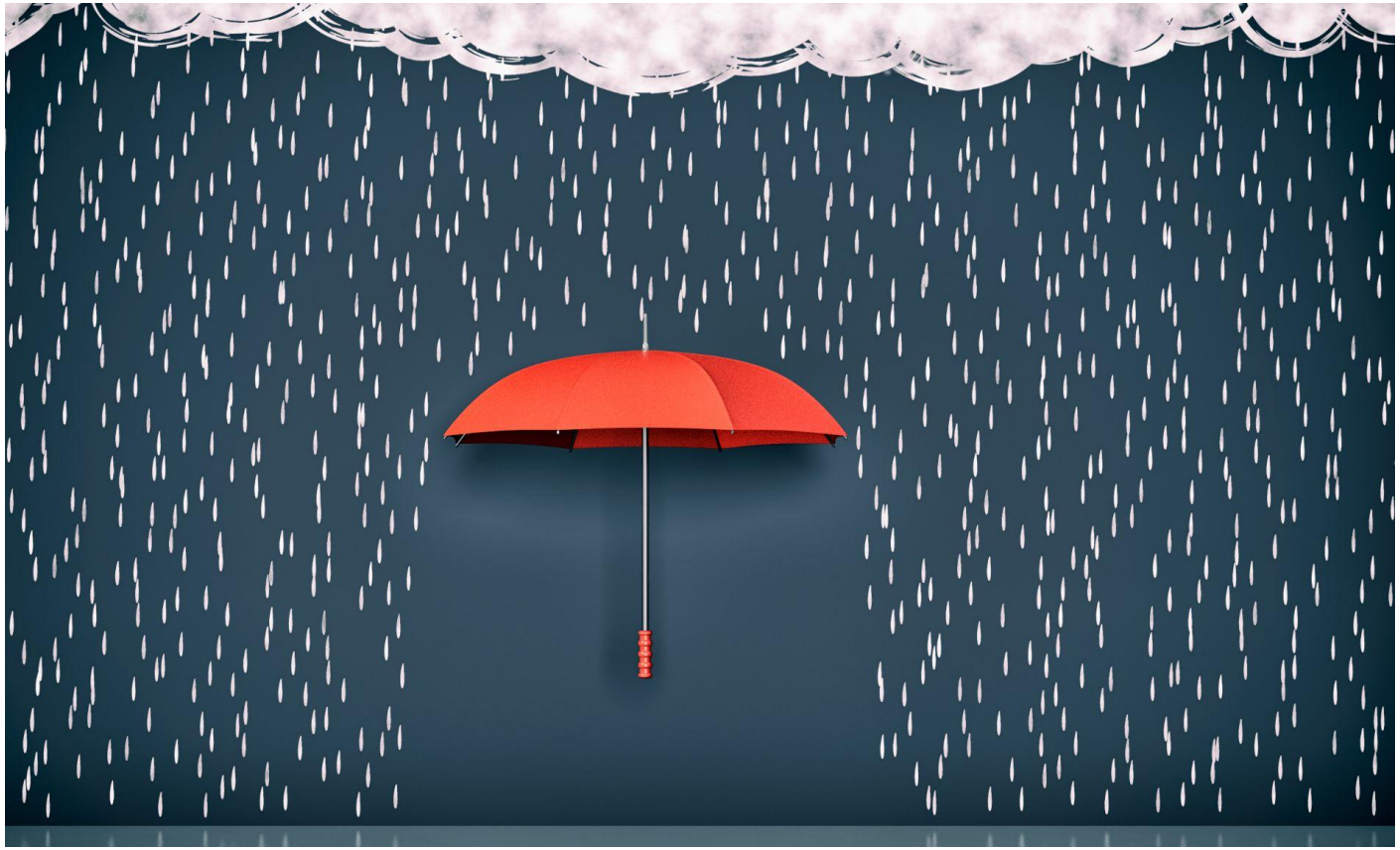
La contradicción de la Inteligencia Artificial (AI Conundrum)

Defensas

Ataque	Protección/Protecciones	Categoría

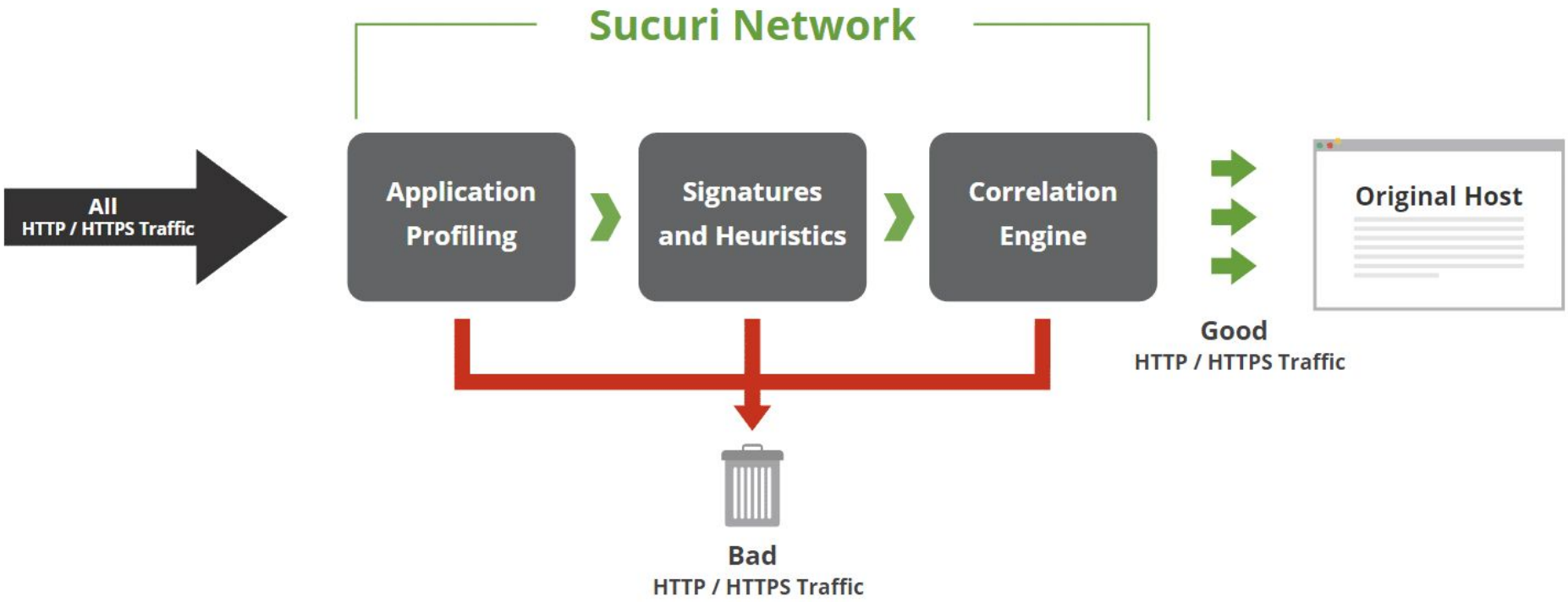
Ataque	Protección/Protecciones	Categoría
Phishing / Spam	Habilidad, Frontend monitor	Reputación, Login

Ataque	Protección/Protecciones	Categoría
Phishing / Spam	Habilidad, Frontend monitor	Reputación, Login
Fuerza Bruta / Diccionario	WAF, Limit login plugin	Login



Website Application Firewall (WAF)

Protect and Speed Up Your Website



Filtra todo el

Tráfico web

Protege de ataques XSS, DDoS, …

Parchea virtualmente una gran cantidad de vulnerabilidades conocidas

Si incluye **CDN**, mejora la **velocidad y rendimiento**

Herramienta de **análisis forense**

Permite **bloqueo manual**

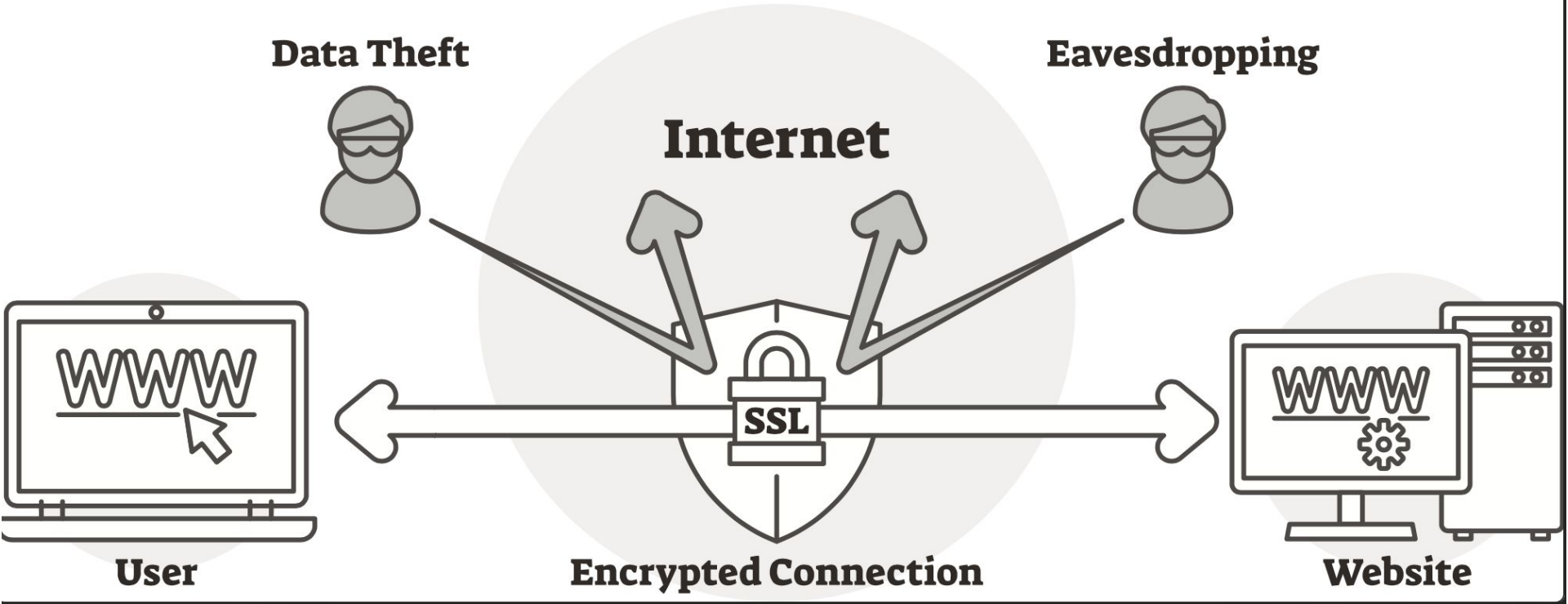
Ataque	Protección/Protecciones	Categoría
Phishing / Spam	Habilidad, Frontend monitor	Reputación, Login
Fuerza Bruta / Diccionario	WAF, Limit login plugin	Login
XSS	WAF, Integridad de ficheros	Reputación

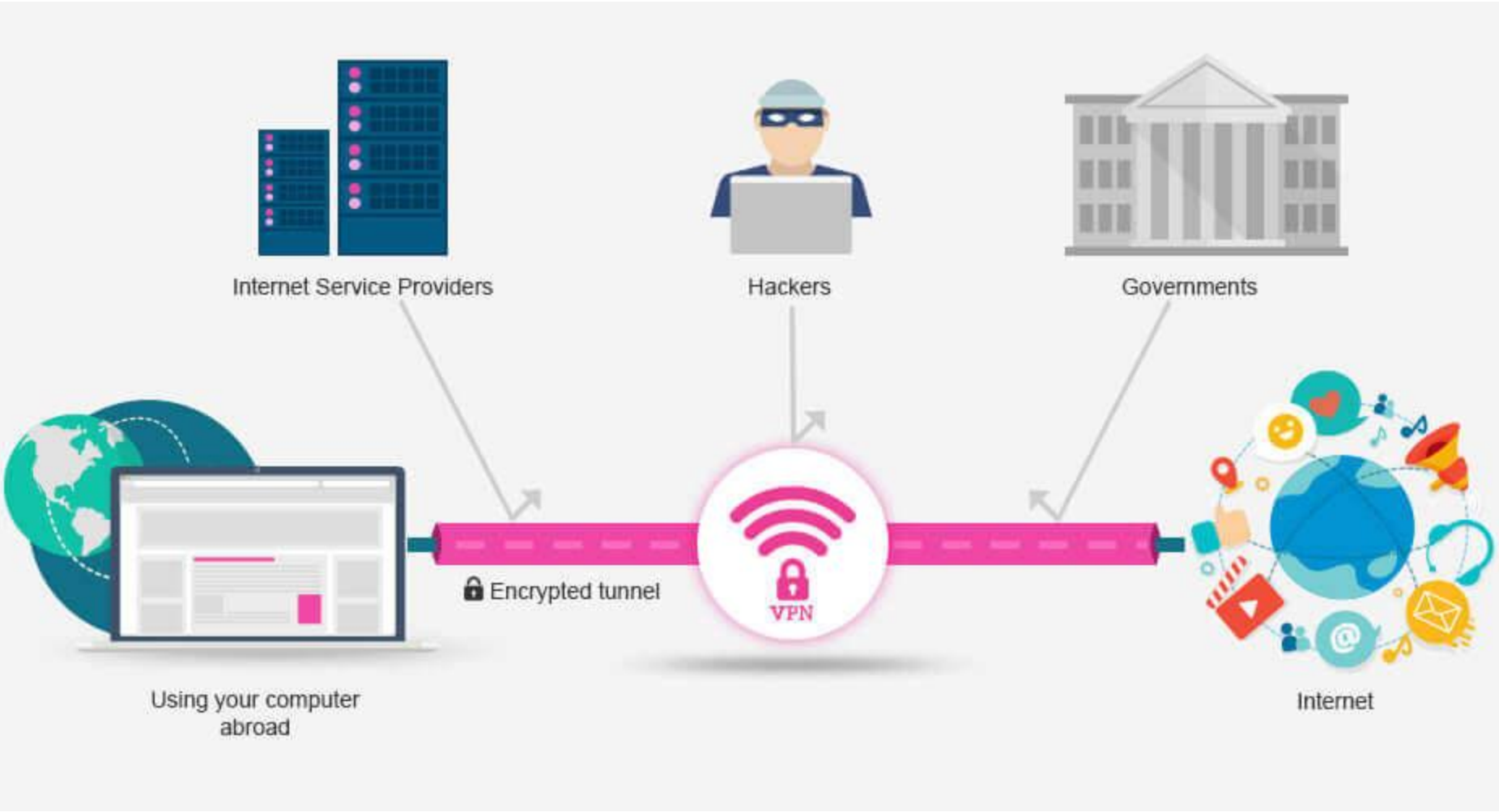
Ataque	Protección/Protecciones	Categoría
Phishing / Spam	Habilidad, Frontend monitor	Reputación, Login
Fuerza Bruta / Diccionario	WAF, Limit login plugin	Login
XSS	WAF, Integridad de ficheros	Reputación
Nuevas vulnerabilidades	WAF, mantenimiento	Investigación

Ataque	Protección/Protecciones	Categoría
Phishing / Spam	Habilidad, Frontend monitor	Reputación, Login
Fuerza Bruta / Diccionario	WAF, Limit login plugin	Login
XSS	WAF, Integridad de ficheros	Reputación
Nuevas vulnerabilidades	WAF, mantenimiento	Investigación
Man in the Middle	SSL	Comunicaciones

SSL

Secure Sockets Layer




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

Ataque	Protección/Protecciones	Categoría
Phishing / Spam	Habilidad, Frontend monitor	Reputación, Login
Fuerza Bruta / Diccionario	WAF, Limit login plugin	Login
XSS	WAF, Integridad de ficheros	Reputación
Nuevas vulnerabilidades	WAF, mantenimiento	Investigación
Man in the Middle	SSL	Comunicaciones
DoS / DDoS	WAF	Comunicaciones, recursos

Ataque	Protección/Protecciones	Categoría
Phishing / Spam	Habilidad, Frontend monitor	Reputación, Login
Fuerza Bruta / Diccionario	WAF, Limit login plugin	Login
XSS	WAF, Integridad de ficheros	Reputación
Nuevas vulnerabilidades	WAF, mantenimiento	Investigación
Man in the Middle	SSL	Comunicaciones
DoS / DDoS	WAF	Comunicaciones, recursos
SQL Injection	WAF, Logs	Base de datos

Ataque	Protección/Protecciones	Categoría
Phishing / Spam	Habilidad, Frontend monitor	Reputación, Login
Fuerza Bruta / Diccionario	WAF, Limit login plugin	Login
XSS	WAF, Integridad de ficheros	Reputación
Nuevas vulnerabilidades	WAF, mantenimiento	Investigación
Man in the Middle	SSL	Comunicaciones
DoS / DDoS	WAF	Comunicaciones, recursos
SQL Injection	WAF, Logs	Base de datos
Ransomware	Backups	Ficheros

Ataque	Protección/Protecciones	Categoría
Phishing / Spam	Habilidad, Frontend monitor	Reputación, Login
Fuerza Bruta / Diccionario	WAF, Limit login plugin	Login
XSS	WAF, Integridad de ficheros	Reputación
Nuevas vulnerabilidades	WAF, mantenimiento	Investigación
Man in the Middle	SSL	Comunicaciones
DoS / DDoS	WAF	Comunicaciones, recursos
SQL Injection	WAF, Logs	Base de datos
Ransomware	Backups	Ficheros
Cryptomining	Logs, usuarios	Recursos, Reputación

Ataque	Protección/Protecciones	Categoría
Phishing / Spam	Habilidad, Frontend monitor	Reputación, Login
Fuerza Bruta / Diccionario	WAF, Limit login plugin	Login
XSS	WAF, Integridad de ficheros	Reputación
Nuevas vulnerabilidades	WAF, mantenimiento	Investigación
Man in the Middle	SSL	Comunicaciones
DoS / DDoS	WAF	Comunicaciones, recursos
SQL Injection	WAF, Logs	Base de datos
Ransomware	Backups	Ficheros
Cryptomining	Logs, usuarios	Recursos, Reputación
BotNode	WAF, Logs	Comunicaciones, Ficheros

Ataque	Protección/Protecciones	Categoría
Phishing / Spam	Habilidad, Frontend monitor	Reputación, Login
Fuerza Bruta / Diccionario	WAF, Limit login plugin	Login
XSS	WAF, Integridad de ficheros	Reputación
Nuevas vulnerabilidades	WAF, mantenimiento	Investigación
Man in the Middle	SSL	Comunicaciones
DoS / DDoS	WAF	Comunicaciones, recursos
SQL Injection	WAF, Logs	Base de datos
Ransomware	Backups	Ficheros
Cryptomining	Logs, usuarios	Recursos, Reputación
BotNode	WAF, Logs	Comunicaciones, Ficheros
Cross-Site Contamination	Integridad de Ficheros	Ficheros

Resumiendo defensas

Tipo	Descripción	Ptos
WAF	Web Application Firewall.	50

Resumiendo defensas

Tipo	Descripción	Ptos
WAF	Web Application Firewall.	50
Monitores	Logs, escáneres y triggers.	20

Resumiendo defensas

Tipo	Descripción	Ptos
WAF	Web Application Firewall.	50
Monitores	Logs, escáneres y triggers.	20
Backups	Copia de seguridad.	10

Resumiendo defensas

Tipo	Descripción	Ptos
WAF	Web Application Firewall.	50
Monitores	Logs, escáneres y triggers.	20
Backups	Copia de seguridad.	10
SSL	Transmisiones seguras.	10

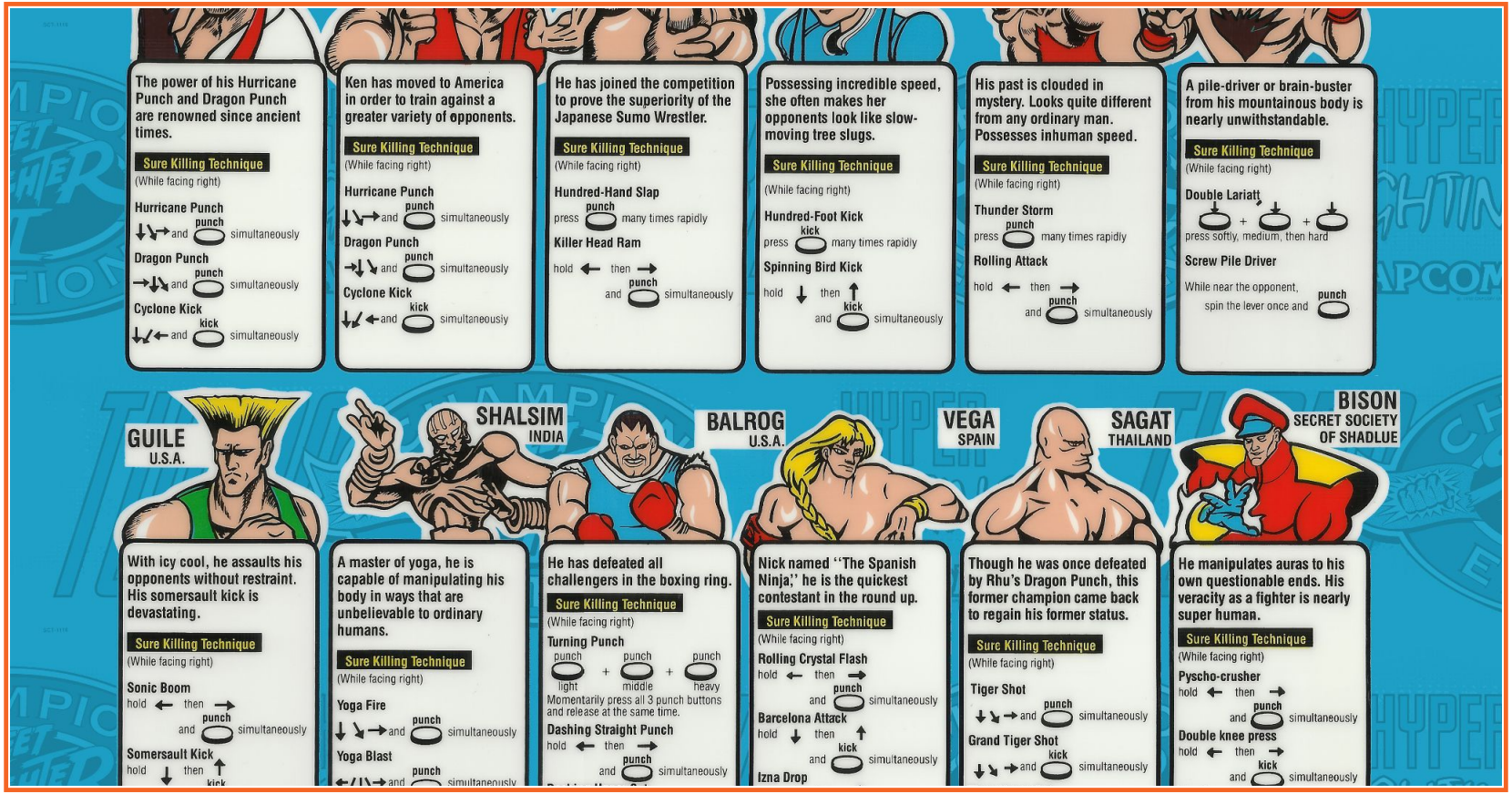
Resumiendo defensas

Tipo	Descripción	Ptos
WAF	Web Application Firewall.	50
Monitores	Logs, escáneres y triggers.	20
Backups	Copia de seguridad.	10
SSL	Transmisiones seguras.	10
Mantenimiento y hardening	Actualizaciones, acciones de protección y ofuscación.	20

Resumiendo defensas

Tipo	Descripción	Ptos
WAF	Web Application Firewall.	50
Monitores	Logs, escáneres y triggers.	20
Backups	Copia de seguridad.	10
SSL	Transmisiones seguras.	10
Mantenimiento y hardening	Actualizaciones, acciones de protección y ofuscación.	20
Habilidad	Un experto pendiente de la seguridad de su sitio.	10

Combos


The power of his Hurricane Punch and Dragon Punch are renowned since ancient times.
Sure Killing Technique
(While facing right)
Hurricane Punch
↓↘→ and punch simultaneously
Dragon Punch
→↓↘ and punch simultaneously
Cyclone Kick
↓↙← and kick simultaneously
Ken has moved to America in order to train against a greater variety of opponents.
Sure Killing Technique
(While facing right)
Hurricane Punch
↓↘→ and punch simultaneously
Dragon Punch
→↓↘ and punch simultaneously
Cyclone Kick
↓↙← and kick simultaneously
He has joined the competition to prove the superiority of the Japanese Sumo Wrestler.
Sure Killing Technique
(While facing right)
Hundred-Hand Slap
press punch many times rapidly
Killer Head Ram
hold ← then → and punch simultaneously
Possessing incredible speed, she often makes her opponents look like slow-moving tree slugs.
Sure Killing Technique
(While facing right)
Hundred-Foot Kick
press kick many times rapidly
Spinning Bird Kick
hold ↓ then ↑ and kick simultaneously
His past is clouded in mystery. Looks quite different from any ordinary man. Possesses inhuman speed.
Sure Killing Technique
(While facing right)
Thunder Storm
press punch many times rapidly
Rolling Attack
hold ← then → and punch simultaneously
A pile-driver or brain-buster from his mountainous body is nearly unwithstandable.
Sure Killing Technique
(While facing right)
Double Lariatt
press softly, medium, then hard
Screw Pile Driver
While near the opponent, spin the lever once and punch
GUILE
U.S.A.
SHALSIM
INDIA
BALROG
U.S.A.
VEGA
SPAIN
SAGAT
THAILAND
BISON
SECRET SOCIETY OF SHADLUE
With icy cool, he assaults his opponents without restraint. His somersault kick is devastating.
Sure Killing Technique
(While facing right)
Sonic Boom
hold ← then → and punch simultaneously
Somersault Kick
hold ↓ then ↑ kick
A master of yoga, he is capable of manipulating his body in ways that are unbelievable to ordinary humans.
Sure Killing Technique
(While facing right)
Yoga Fire
↓↘→ and punch simultaneously
Yoga Blast
←↙↓↘→ and punch simultaneously
He has defeated all challengers in the boxing ring.
Sure Killing Technique
(While facing right)
Turning Punch
punch light + punch middle + punch heavy
Momentarily press all 3 punch buttons and release at the same time.
Dashing Straight Punch
hold ← then → and punch simultaneously
Nick named "The Spanish Ninja," he is the quickest contestant in the round up.
Sure Killing Technique
(While facing right)
Rolling Crystal Flash
hold ← then → and punch simultaneously
Barcelona Attack
hold ↓ then ↑ and kick simultaneously
Izna Drop
Though he was once defeated by Rhu's Dragon Punch, this former champion came back to regain his former status.
Sure Killing Technique
(While facing right)
Tiger Shot
↓↘→ and punch simultaneously
Grand Tiger Shot
↓↘→ and kick simultaneously
He manipulates auras to his own questionable ends. His veracity as a fighter is nearly super human.
Sure Killing Technique
(While facing right)
Pyscho-crusher
hold ← then → and punch simultaneously
Double knee press
hold ← then → and kick simultaneously

¡RECUERDA!

COSTO Web caída

<

COSTO Web hackeada

WordPress Security

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

SCAN ME

MI Combo

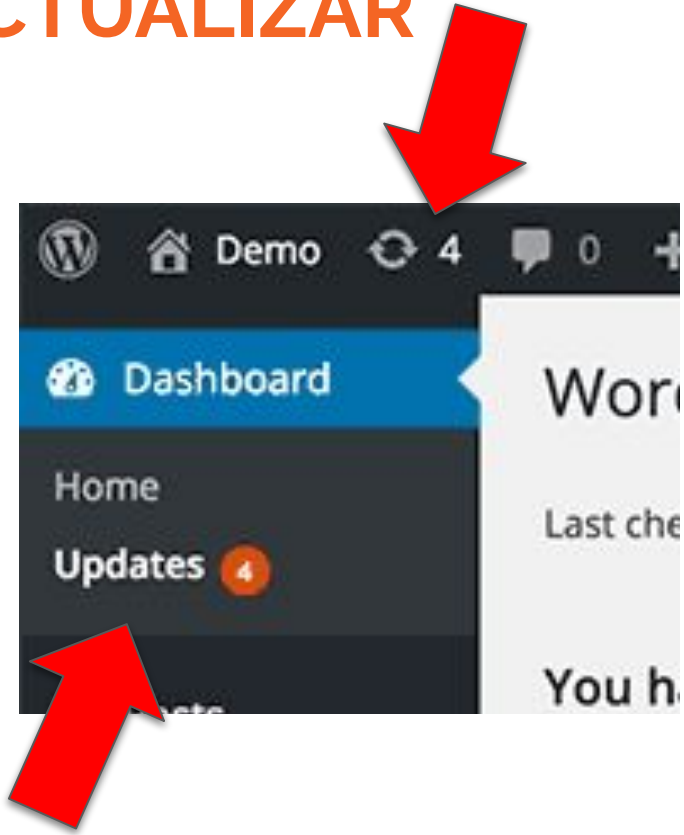
- **WAF + CDN**
  - Sucuri (o CloudFlare)

- **Plugins de Seguridad**
  - WordFence Free (Sin WAF)
    o iThemes Security
  - Fail2Ban
    o Limit Login Attempts Reloaded
  - CAPTCHA 4WP

- **Base: 1 Buen Hosting**
  - SSL
  - Soporte + BackUps
  - Plan gestionado

- **Backups**
  - VaultPress (Jetpack)
    o BlogVault
    o UpDraft

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**.

La importancia de
LAS CONTRASEÑAS & 2FA

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, ...).


37600
V
40
FULL

GAME OVER


Everybody needs a hacker

Word-Camp Zaragoza 2023

¡GRACIAS!

¿PREGUNTAS?

#WCZGZ23