Seguridad en WordPress ¿y eso qué significa? A.M.A.

Néstor Angulo de Ugarte (@pharar)

WORDCAMP
PONTEVEDRA
2022

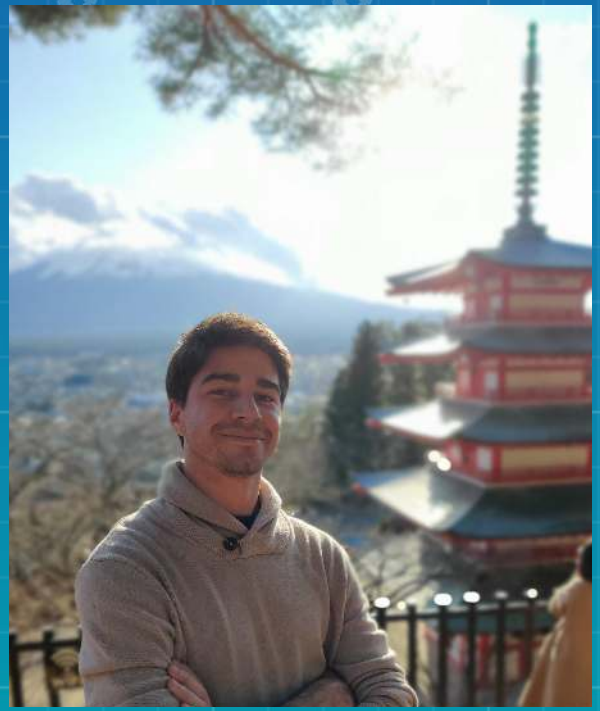
Néstor Angulo de Ugarte

Analista de Seguridad Web

7 años en *Incident Response*
Sucuri y *GoDaddy Websecurity Group*

CISSP (Certified Information Systems Security Professional)

Twitter: **@pharar**



#PonteWordCamp

WORDCAMP
PONTEVEDRA
2022

FACTS

Un hackeo prácticamente **nunca es orientado** a un cliente

(98% of cases)

Casi siempre ocurre debido a un **control y mantenimiento deficientes**

Un certificado **SSL**

no es un escudo

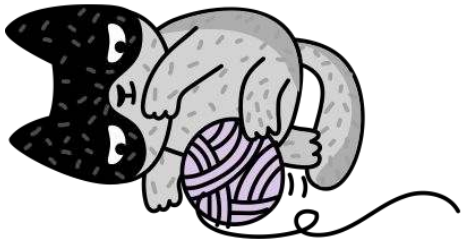
anti-hacking

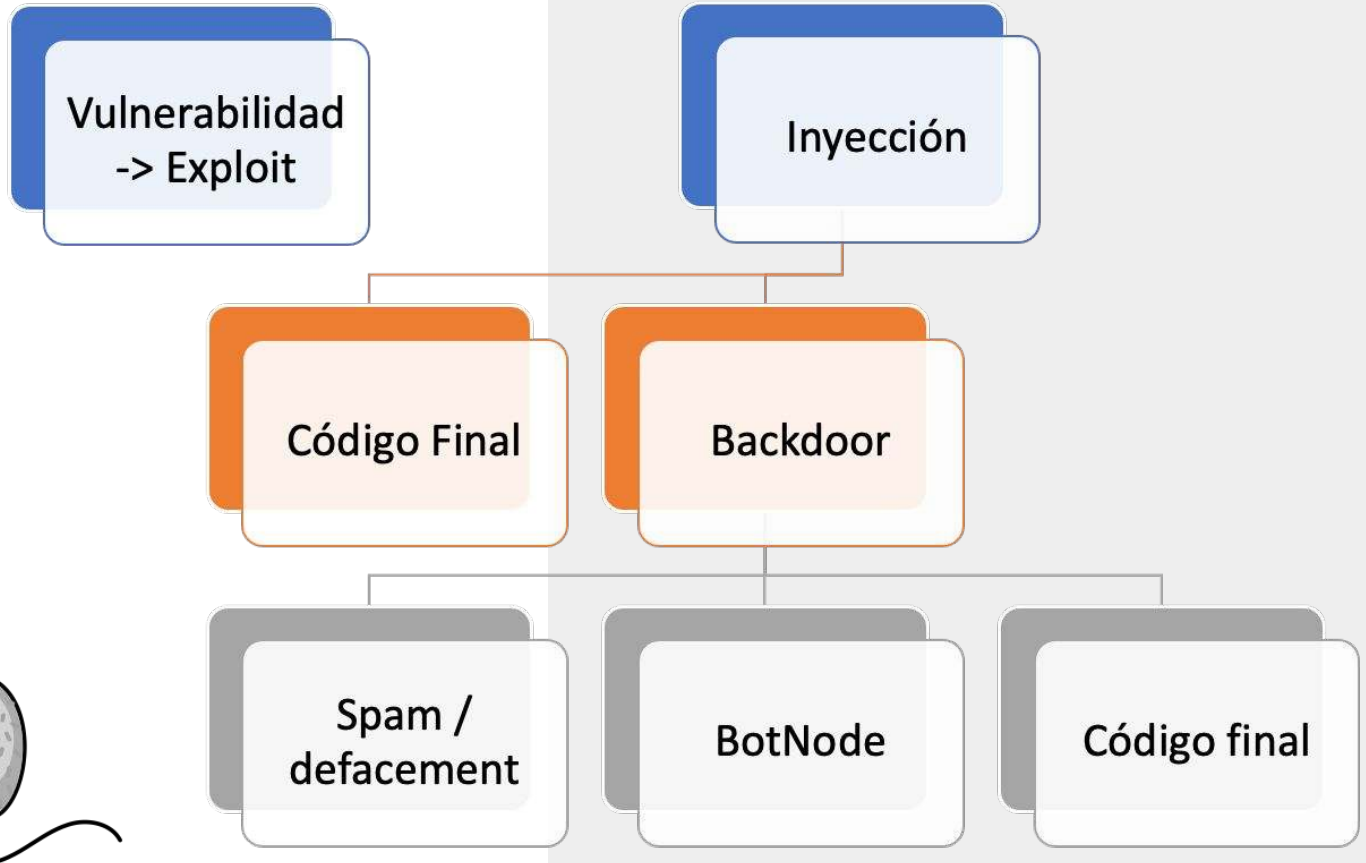
Los parches de seguridad y actualizaciones aparecen normalmente **después** de descubrirse la existencia de exploits

Errare Humanum Est

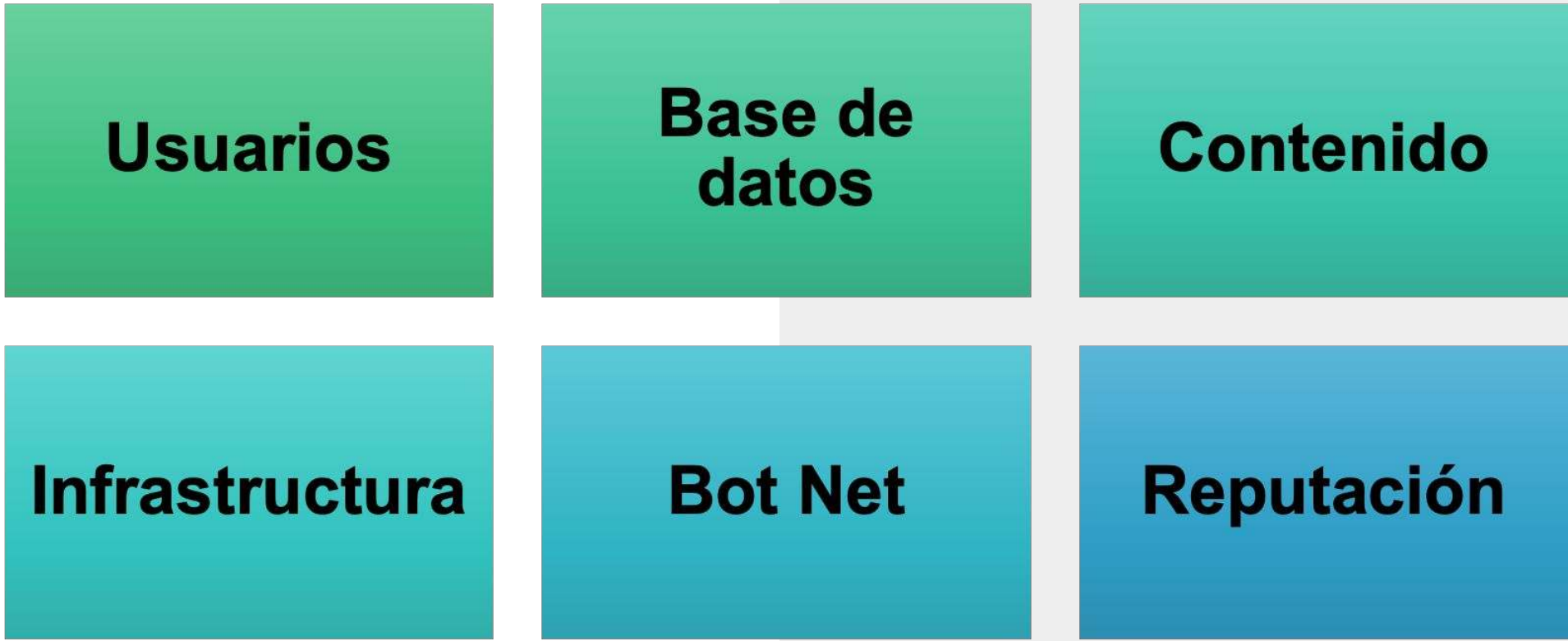
La Seguridad **nunca** garantiza (ni lo hará) un **100% de efectividad**

Hacking WordPress. El Proceso





Posibles objetivos en WordPress




BOTNET
SPAM
PHISHING
HACKER
MALWARE
DDOS
KEYLOGGER
VIRUS
SPYWARE

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.

- **Black Hat**
  Ciberterrorista, Ladrón, el chico malo.
- **Grey Hat**
  White Hat Hacker que utiliza métodos ilegales.
- **White Hat**
  Analista de seguridad, Hacker ético.

Definiciones

- **Vulnerabilidad**
  - Error en el código o posibilidad de utilización malintencionada de un recurso que puede ser explotado para realizar actividad no autorizada en un sistema informático.
- **Exploit**
  - Programa que aprovecha una vulnerabilidad
- **Backdoor**
  - Malware que permite ejecución remota de código

Personajes en esta historia (si pasa algo)

Tu sitio

Dueño / Admins

Desarrollador & Diseñador

Usuarios/clientes

Proveedor Hosting

Agentes / C3

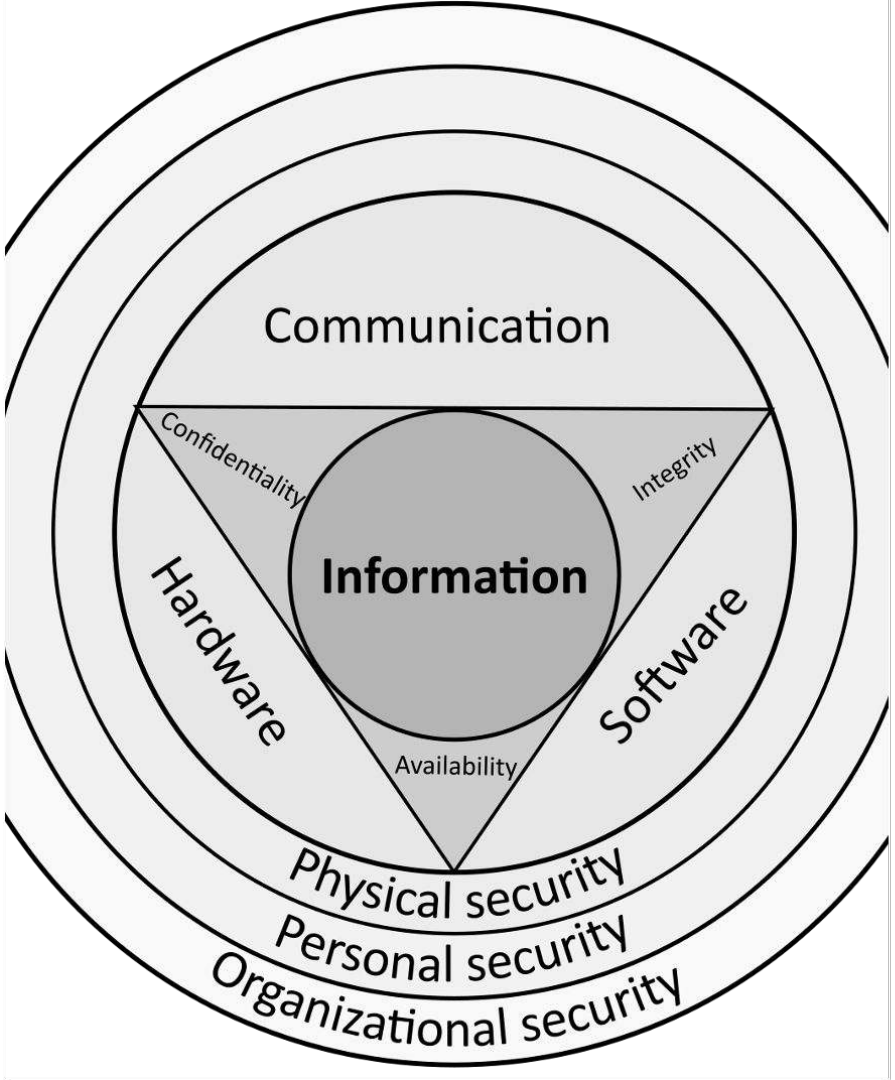
Soporte & Backups

Experto en Seguridad

Departamento interno

Servicios externos

Qué es la Seguridad de Información

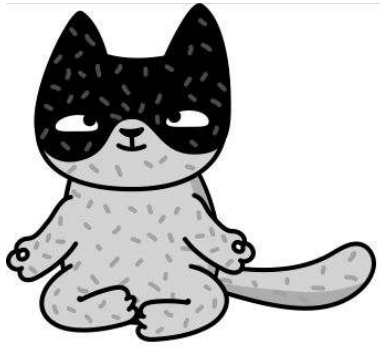


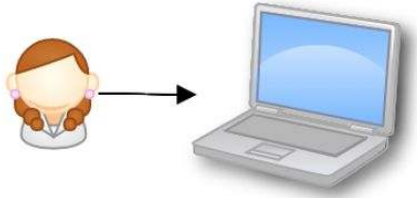
Concepto CID (CIA)

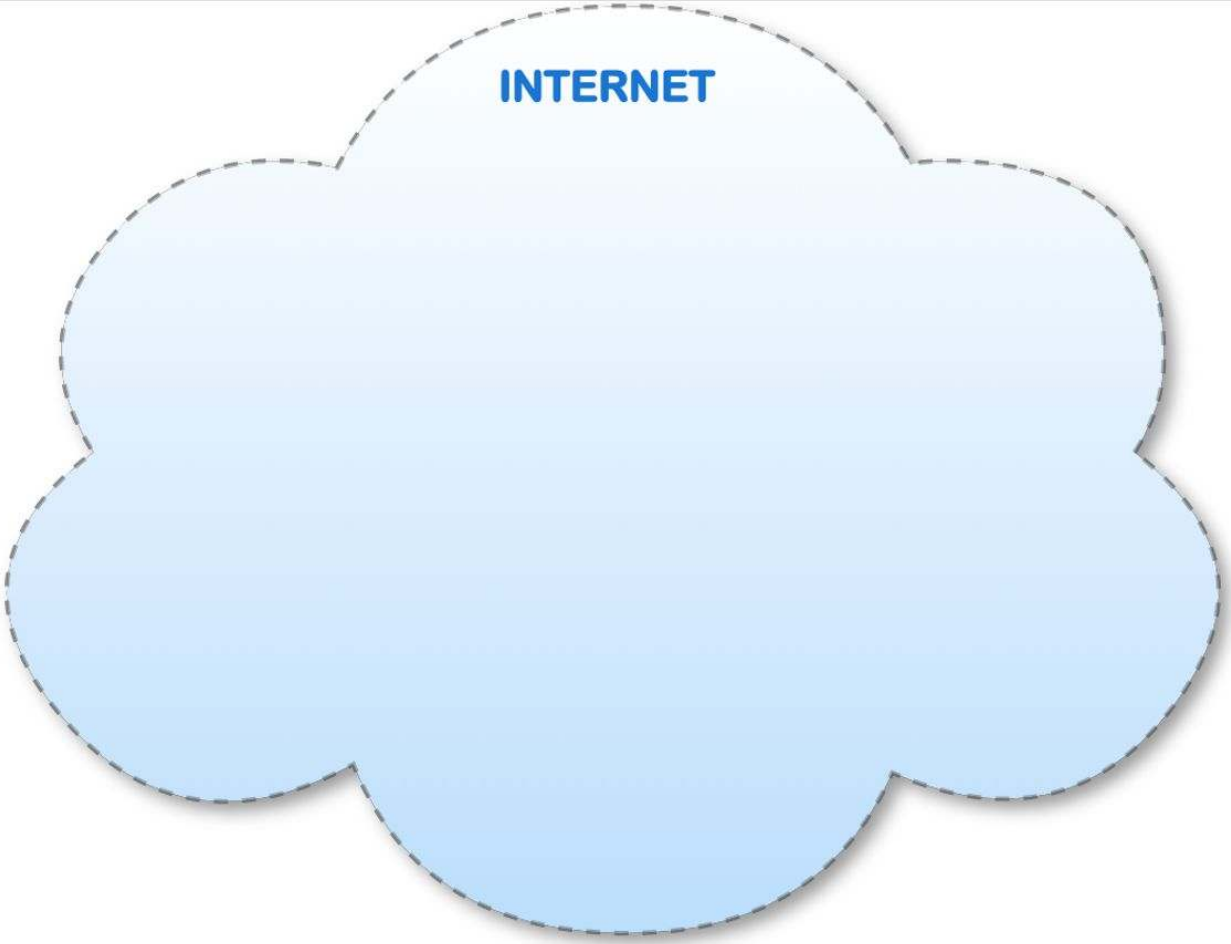
- Confidencialidad
- Integridad
- Disponibilidad

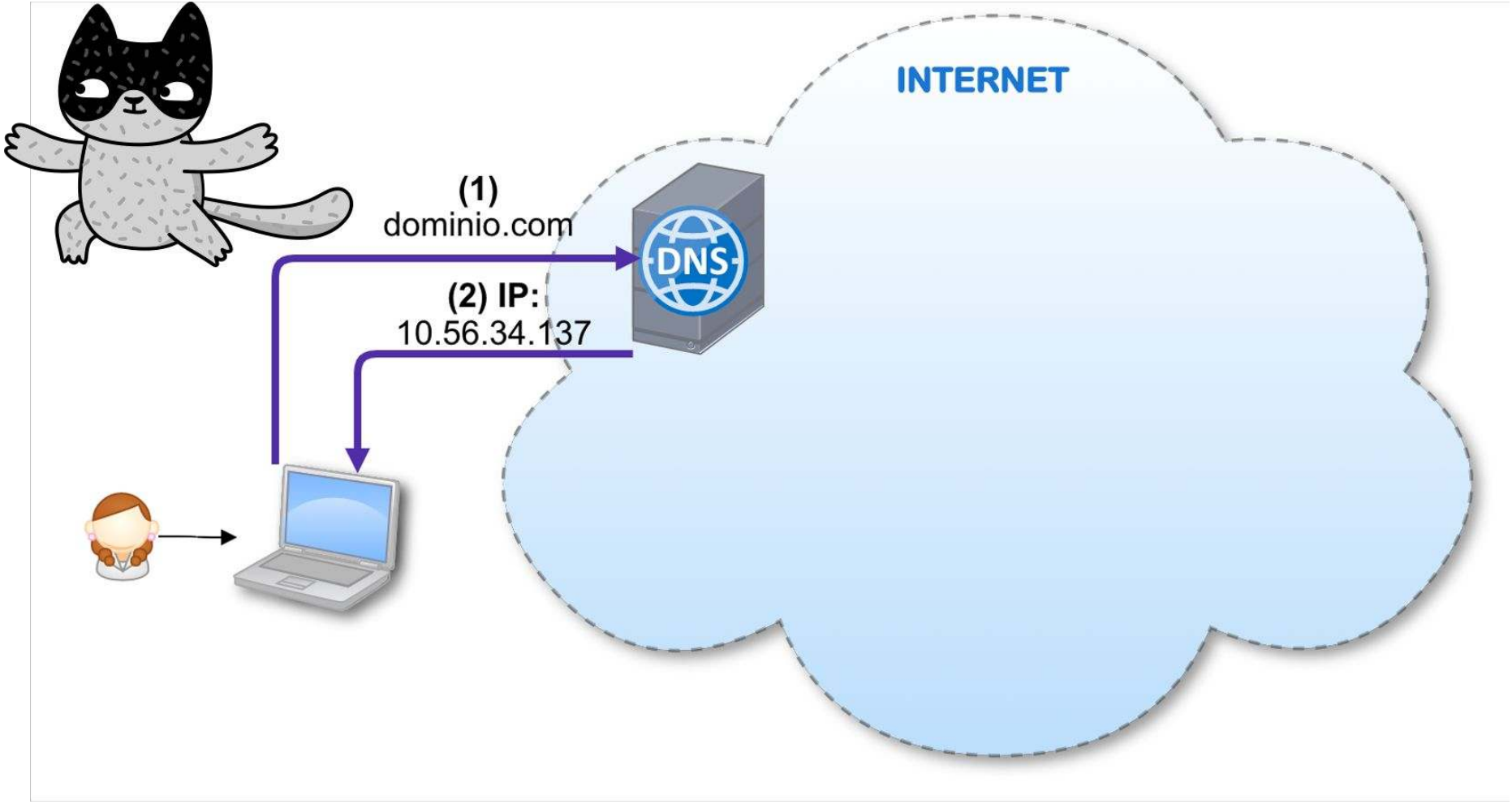
Concepto FAD (DAD)

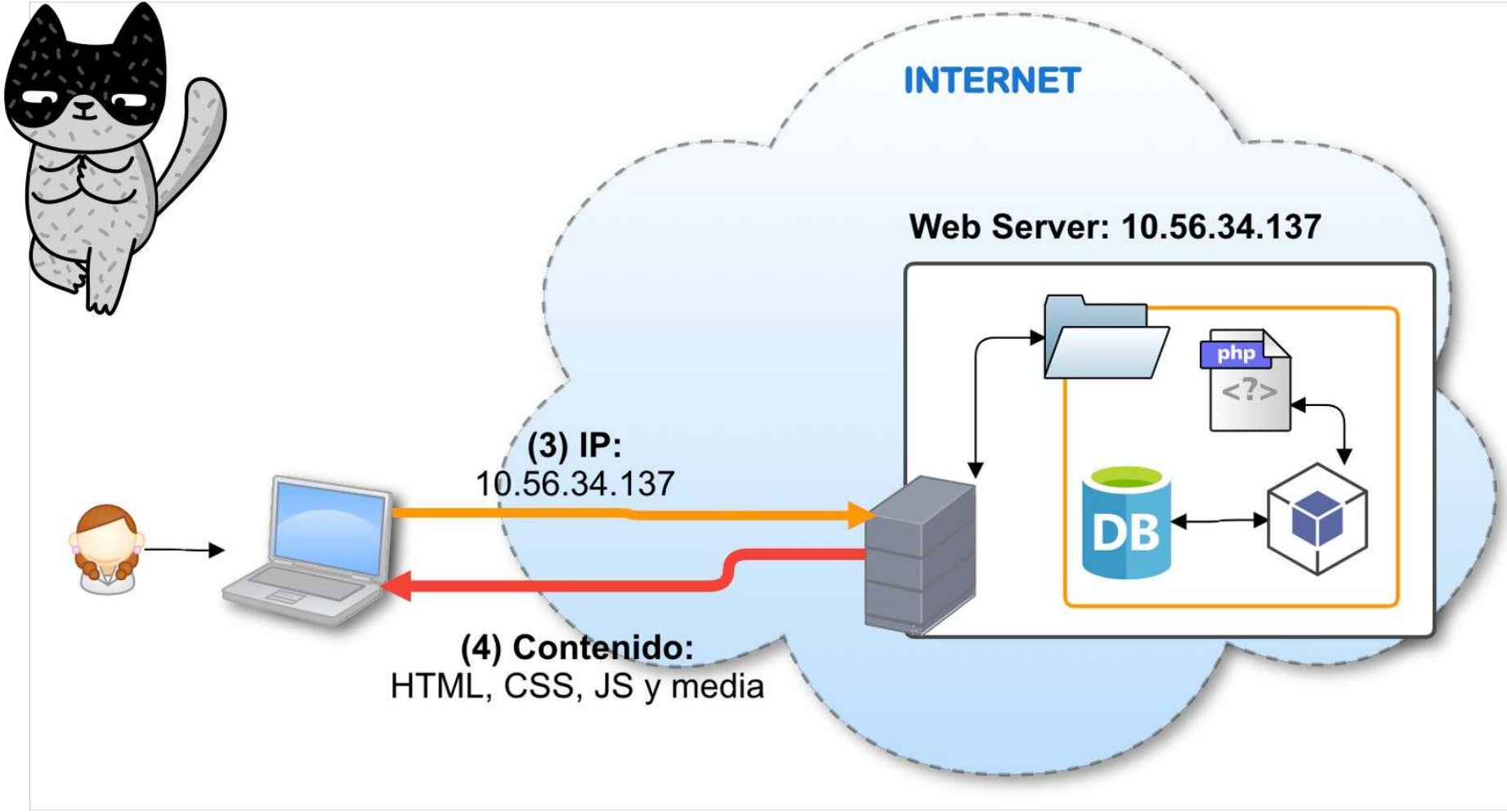
- Filtración
- Alteración
- Destrucción

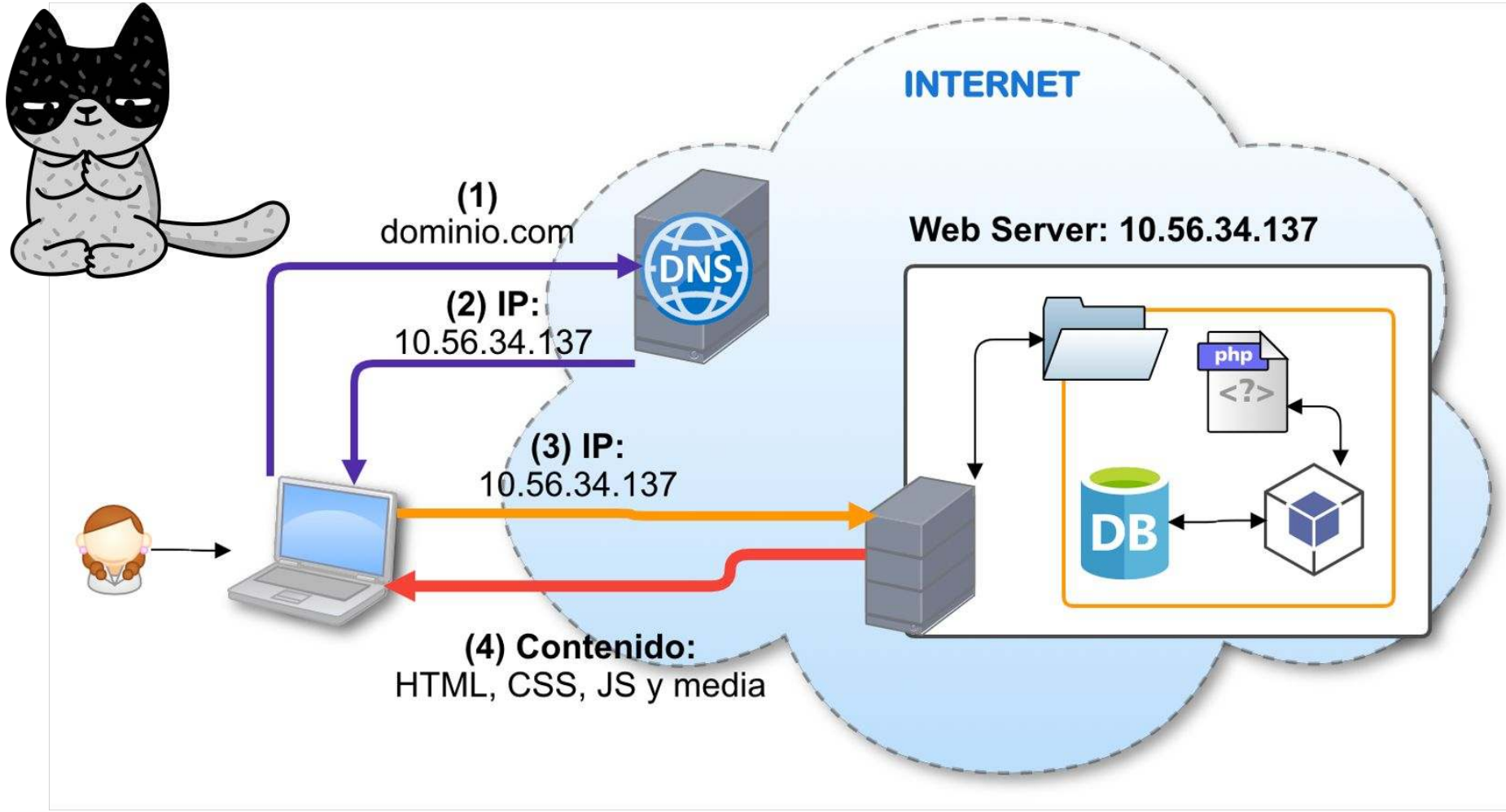





INTERNET

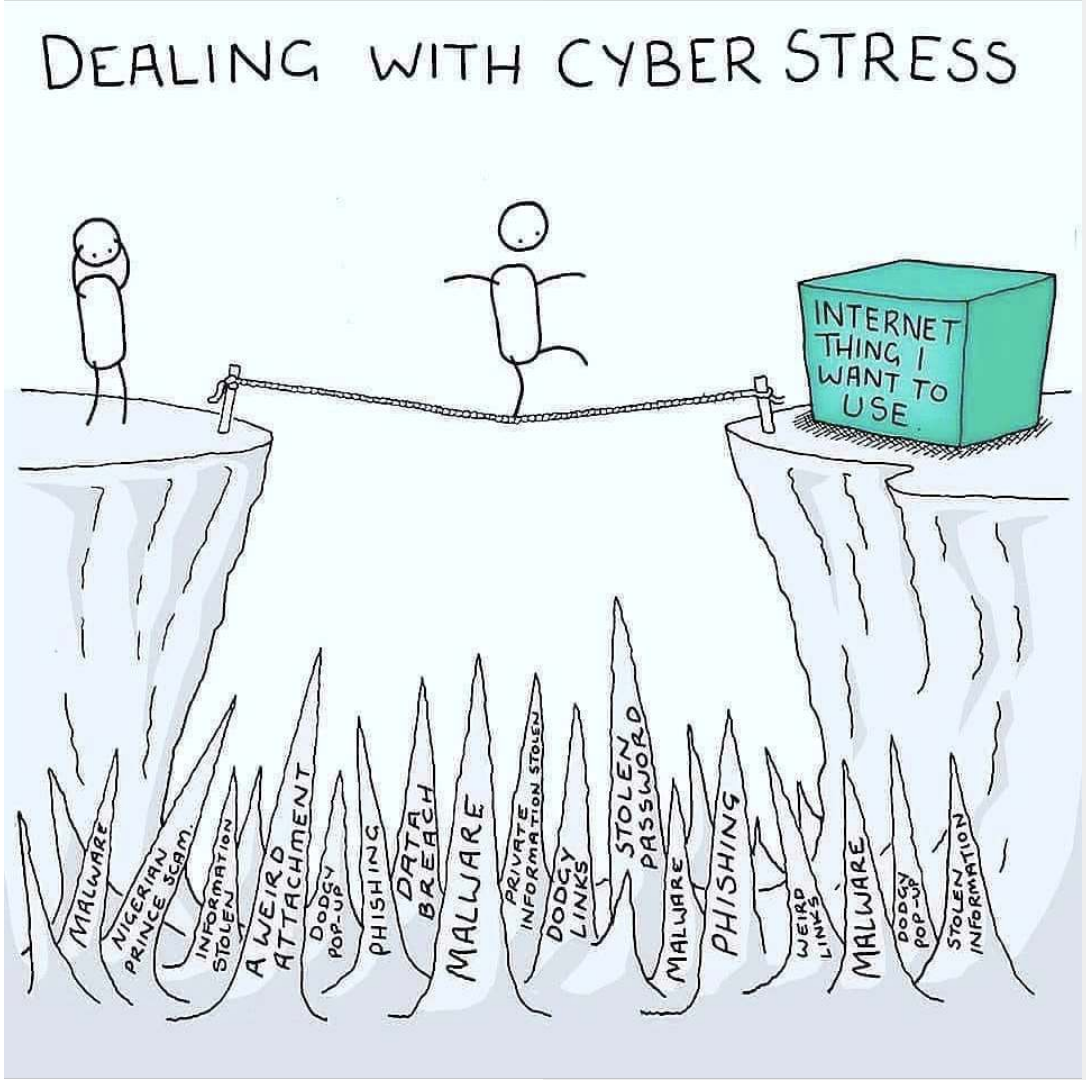

INTERNET
(1)
dominio.com
DNS
(2) IP:
10.56.34.137


INTERNET
Web Server: 10.56.34.137
php
<?>
DB
(3) IP:
10.56.34.137
(4) Contenido:
HTML, CSS, JS y media


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

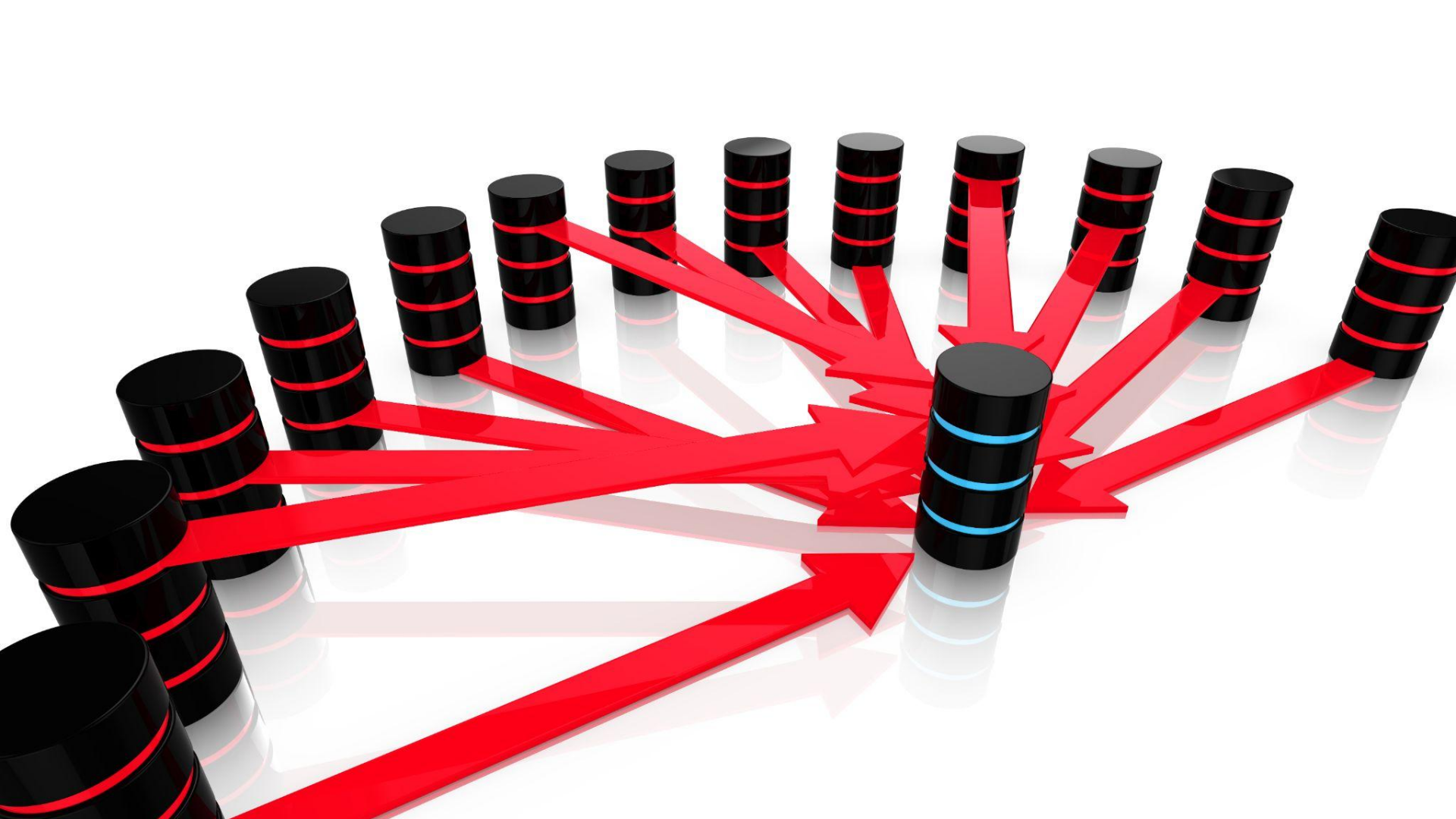
Seguridad: Modelo por capas simplificado

Capa	Protección
Tú, la capa más débil	Conocimiento
Tu **dispositivo**	Antivirus
Tu **conexión**	SSL
Tu **sitio web**	WAF
Tus **credenciales**	Contraseñas fuertes, 2FA
La seguridad de **tu sitio**	monitor, plugins, updates
La seguridad **del server**	monitor, sysadmin, updates
La **base de datos**	monitor, sysadmin
Tareas de mantenimiento	

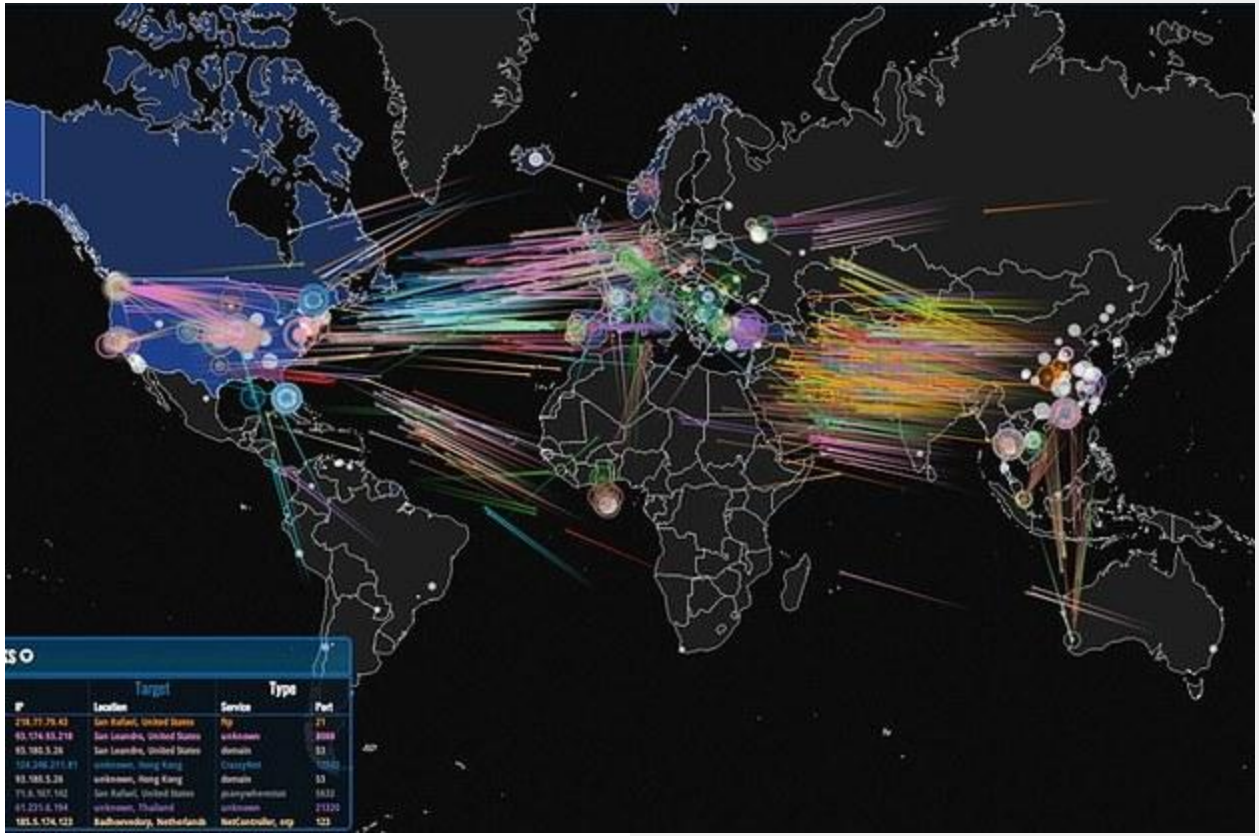

DEALING WITH CYBER STRESS
INTERNET THING I WANT TO USE
MALWARE
NIGERIAN PRINCE SCAM
INFORMATION STOLEN
A WEIRD ATTACHMENT
DODGY POP-UP
PHISHING
DATA BREACH
MALWARE
PRIVATE INFORMATION STOLEN
DODGY LINKS
STOLEN PASSWORD
MALWARE
PHISHING
WEIRD LINKS
MALWARE
DODGY POP-UP
STOLEN INFORMATION

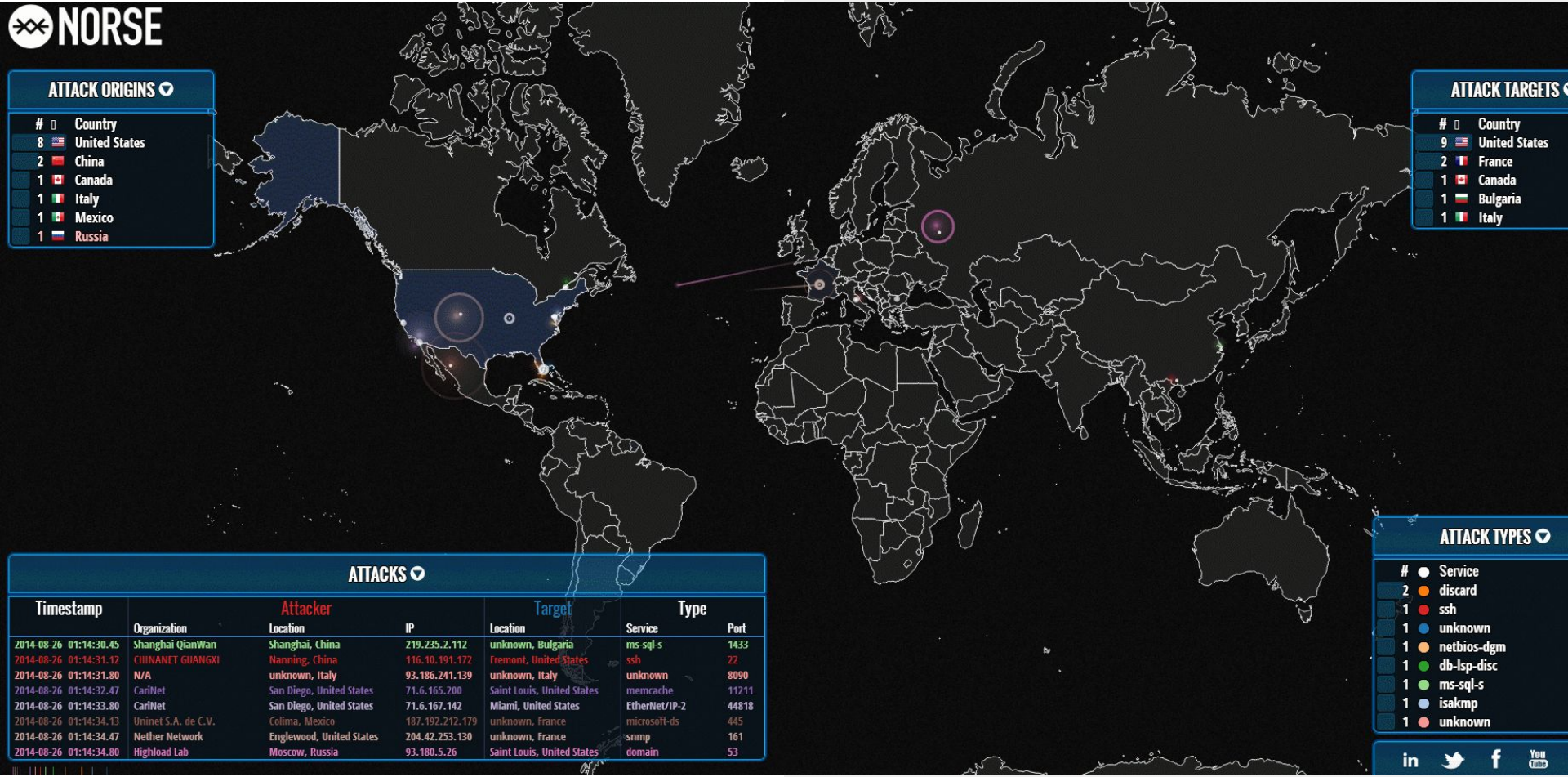

There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked.
John Chambers
Chief Executive Officer of Cisco


KEEP
CALM
CUSTOMERS
HAPPY
sucuri
Complete Website Security

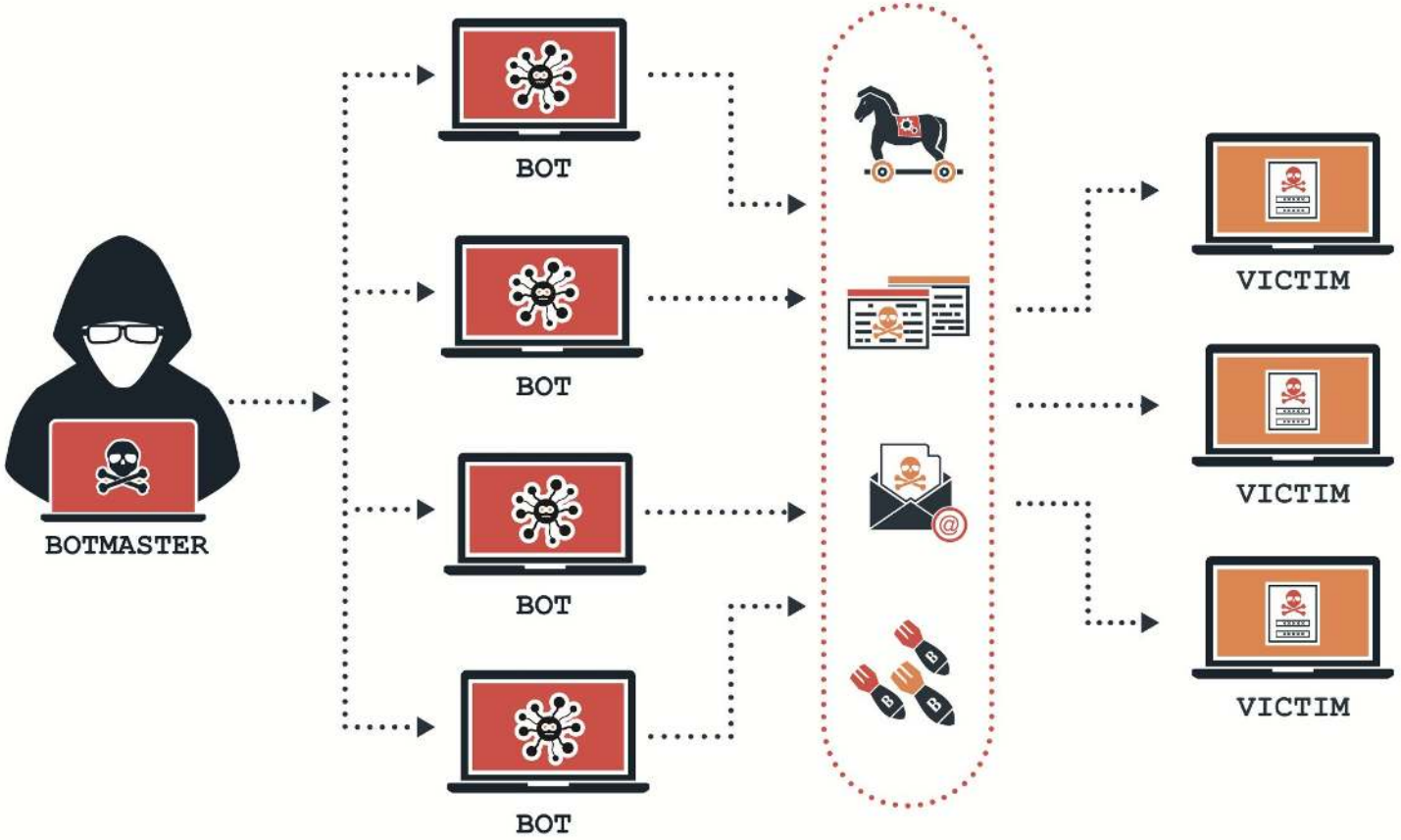



LAUNCHES DETECTED
LAUNCHES DETECTED
LAUNCHES DETECTED
LAUNCHES DETECTED
LAUNCHES DETECTED
LAUNCHES DETECTED
LAUNCHES DETECTED
LAUNCHES DETECTED
LAUNCHES DETECTED

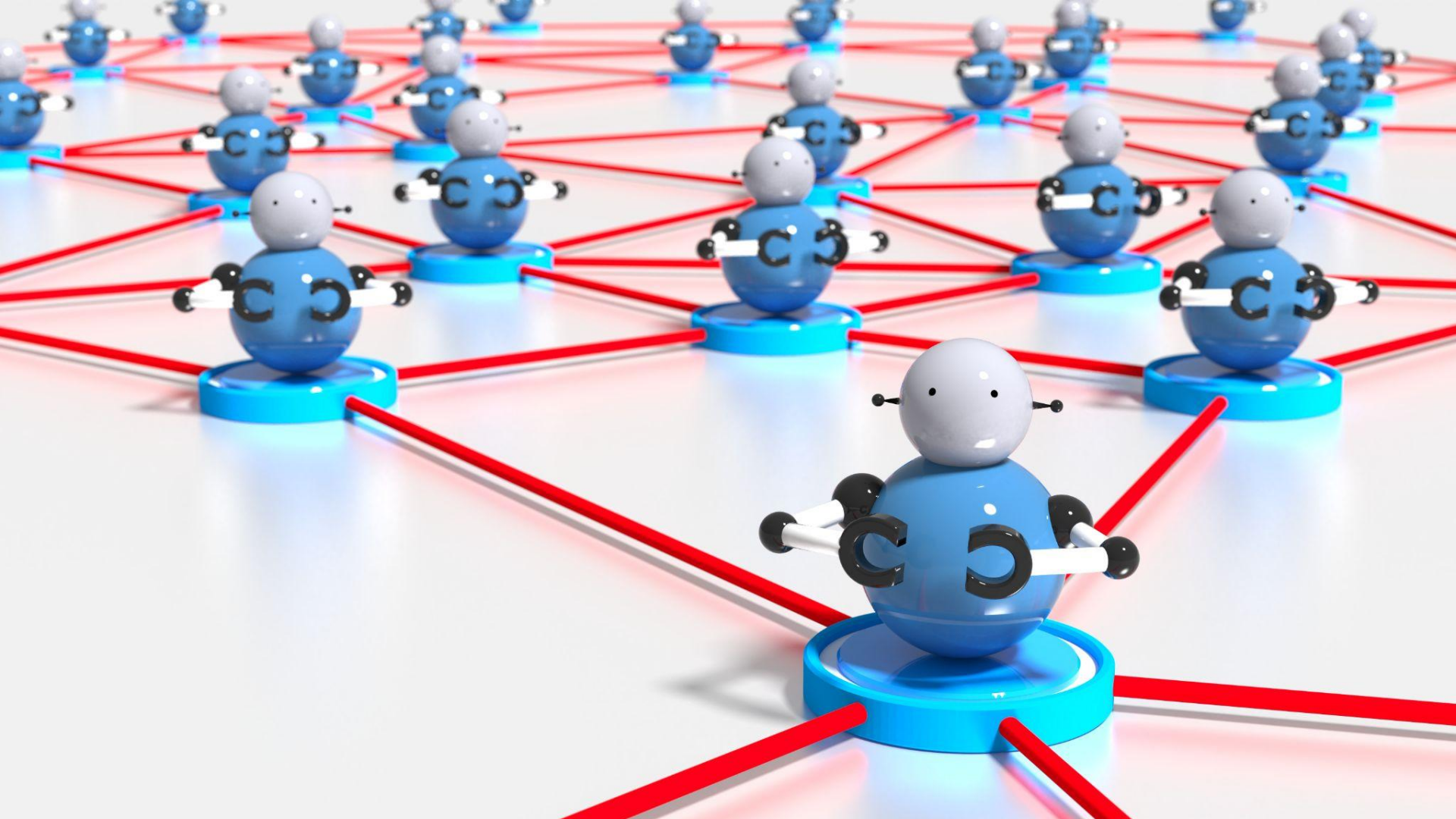

Target
Type
IP
Location
Service
Port
219.77.79.43
San Rafael, United States
ftp
21
65.174.65.210
San Leandro, United States
unknown
8088
65.180.5.26
San Leandro, United States
domain
53
93.180.5.26
unknown, Hong Kong
domain
53
71.6.167.142
San Rafael, United States
1632
185.5.174.123
Radhorvesbry, Netherlands
NetController, ecp
123

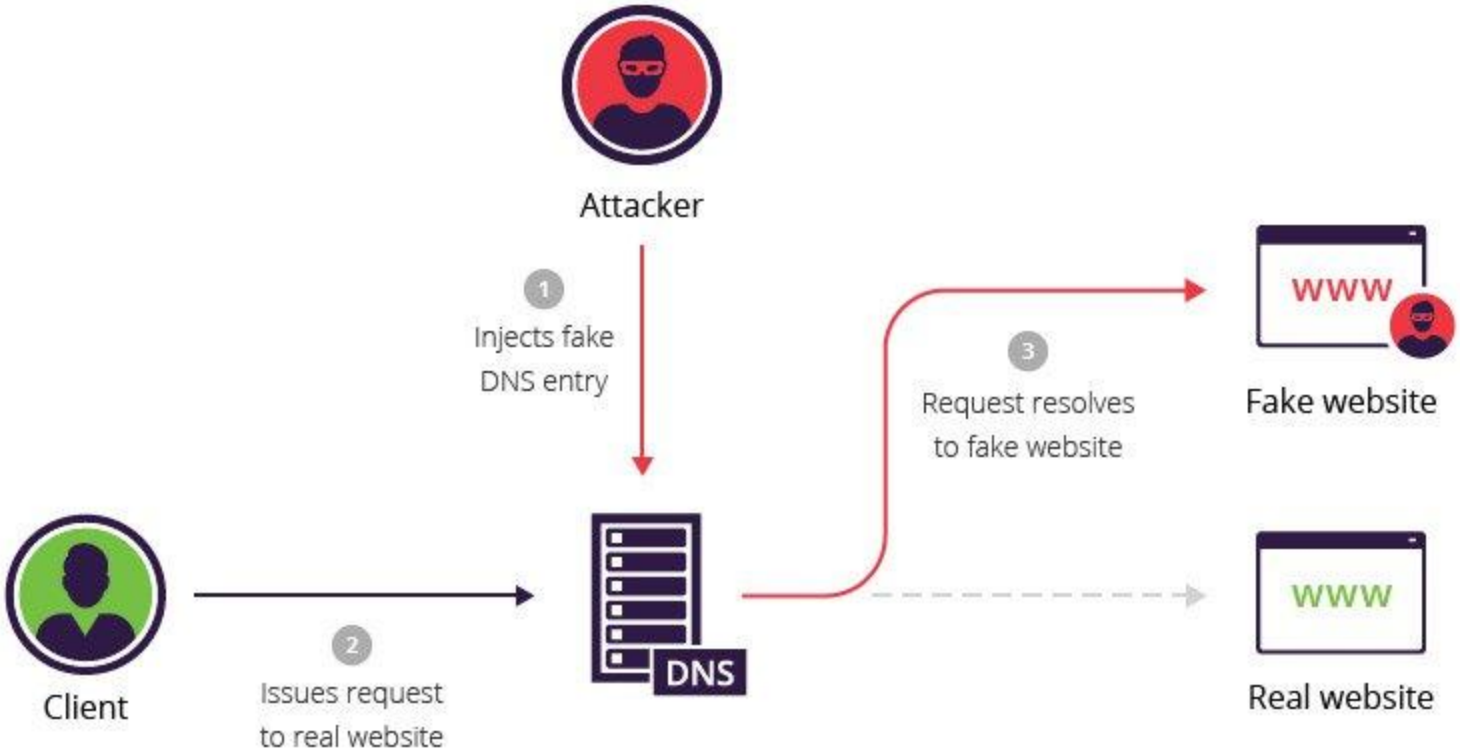

NORSE
ATTACK ORIGINS
Country
8 United States
2 China
1 Canada
1 Italy
1 Mexico
1 Russia
ATTACK TARGETS
Country
9 United States
2 France
1 Canada
1 Bulgaria
1 Italy
ATTACK TYPES
Service
2 discard
1 ssh
1 unknown
1 netbios-dgm
1 db-lsp-disc
1 ms-sql-s
1 isakmp
1 unknown
ATTACKS
Timestamp | Attacker | | | Target | Type | |
Organization | Location | IP | Location | 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

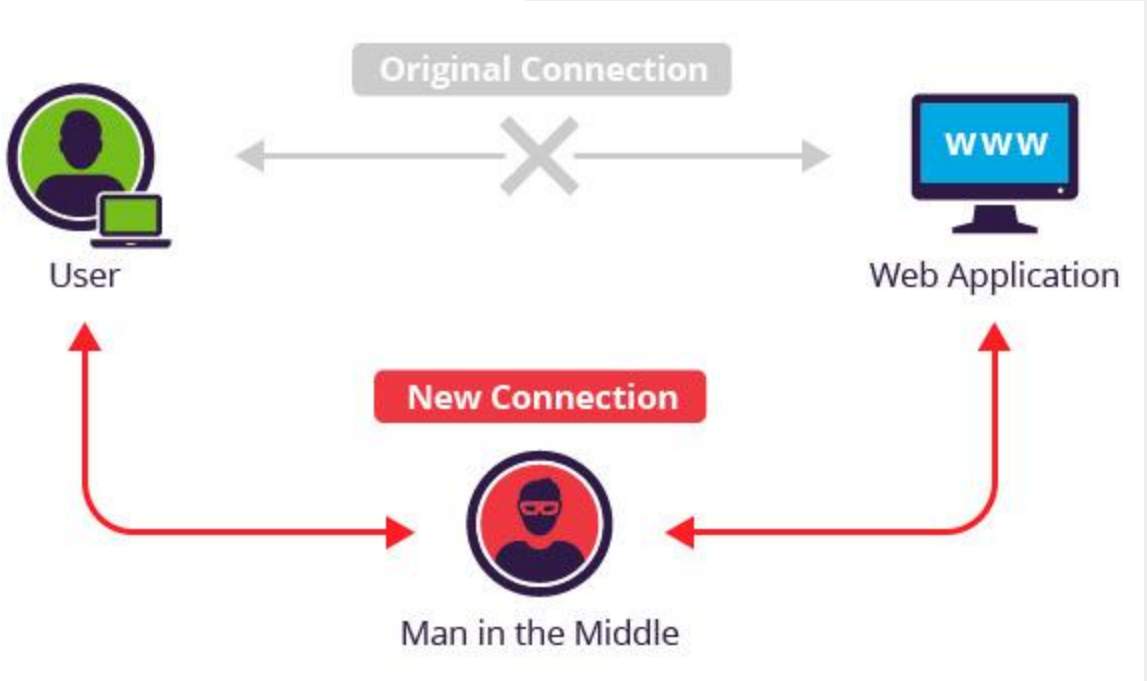

NORSE
ATTACK ORIGINS
COUNTRY
China
United States
Russia
Saudi Arabia
Netherlands
France
Moldova
South Korea
Brazil
Finland
ATTACK TARGETS
COUNTRY
United States
Saudi Arabia
United Arab Emirates
Philippines
Liechtenstein
France
Russia
Taiwan
Cyprus
Mexico
ATTACK TYPES
SERVICE
PORT
LIVE ATTACKS
TIMESTAMP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


BOTMASTER
BOT
BOT
BOT
BOT
VICTIM
VICTIM
VICTIM


LOGIN
****
SPAM

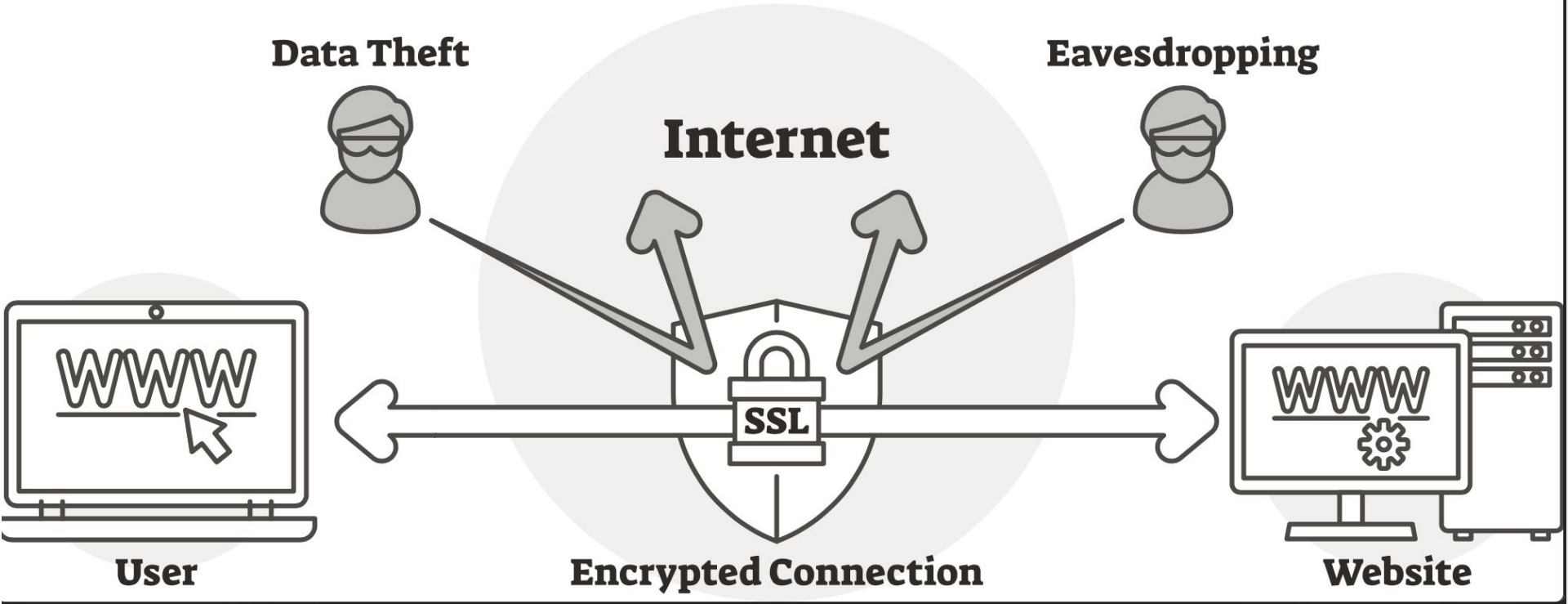


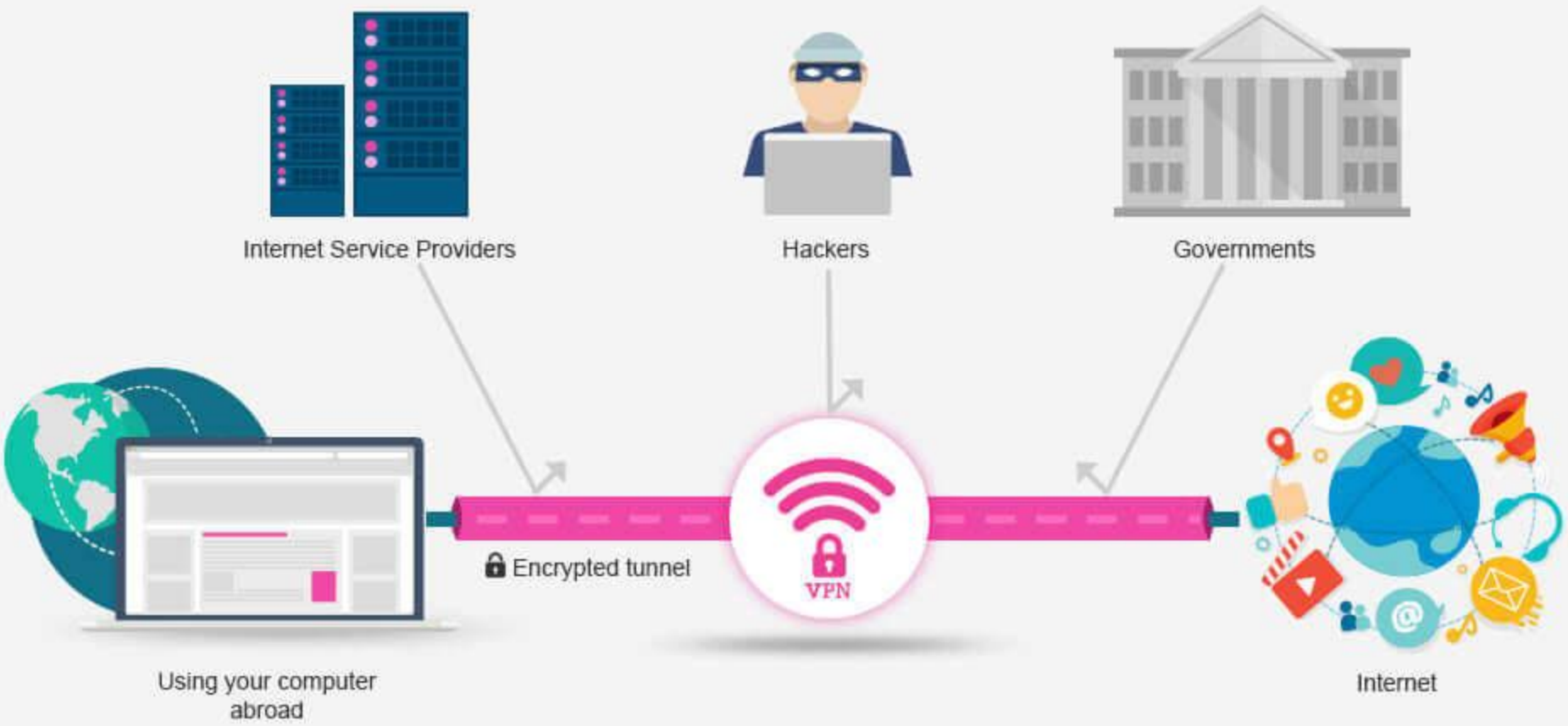

Attacker
1
Injects fake
DNS entry
3
Request resolves
to fake website
www
Fake website
Client
2
Issues request
to real website
DNS
www
Real website


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

SSL

Secure Sockets Layer




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


DATA
BREACH

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

[redacted] 6 0 + New SEO [redacted] Howdy, [redacted]

Screen Options ▼ Help ▼

- Dashboard
- All in One SEO
- Jetpack
- [redacted]
- Unyson
- Blog Posts
- Media
- Pages
- Comments
- Forms
- FooGallery
- Portfolio
- Feedback
- Forms
- Appearance
- Plugins 3
- Users

All Users
Add New

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)

Search Users

Bulk Actions Apply Change role to... Change 6 items

Username	Name	Email	Role	Posts
admin	[redacted]	[redacted]	Administrator	78
akmin		no@email.com	Administrator	1
janel	[redacted]	[redacted]	Contributor	0
levy	[redacted]		Contributor	33
managed-wp-migration-465790ae	Managed WordPress Migration U		Administrator	0
wp.service.controller.lHmp6			None	0
Username	Name		Role	Posts

Bulk Actions Apply Change role to... Change 6 items

Atención: Se perderá cualquier personalización que hayas hecho a los archivos de

Actualizar temas

Seleccionar todos

Twenty Fifteen
Tienes la versión 2.5. Actualiza a la 2.6.

Twenty Fourteen
Tienes la versión 2.7. Actualiza a la 2.8.

Twenty Nineteen
Tienes la versión 1.4. Actualiza a la 1.5.

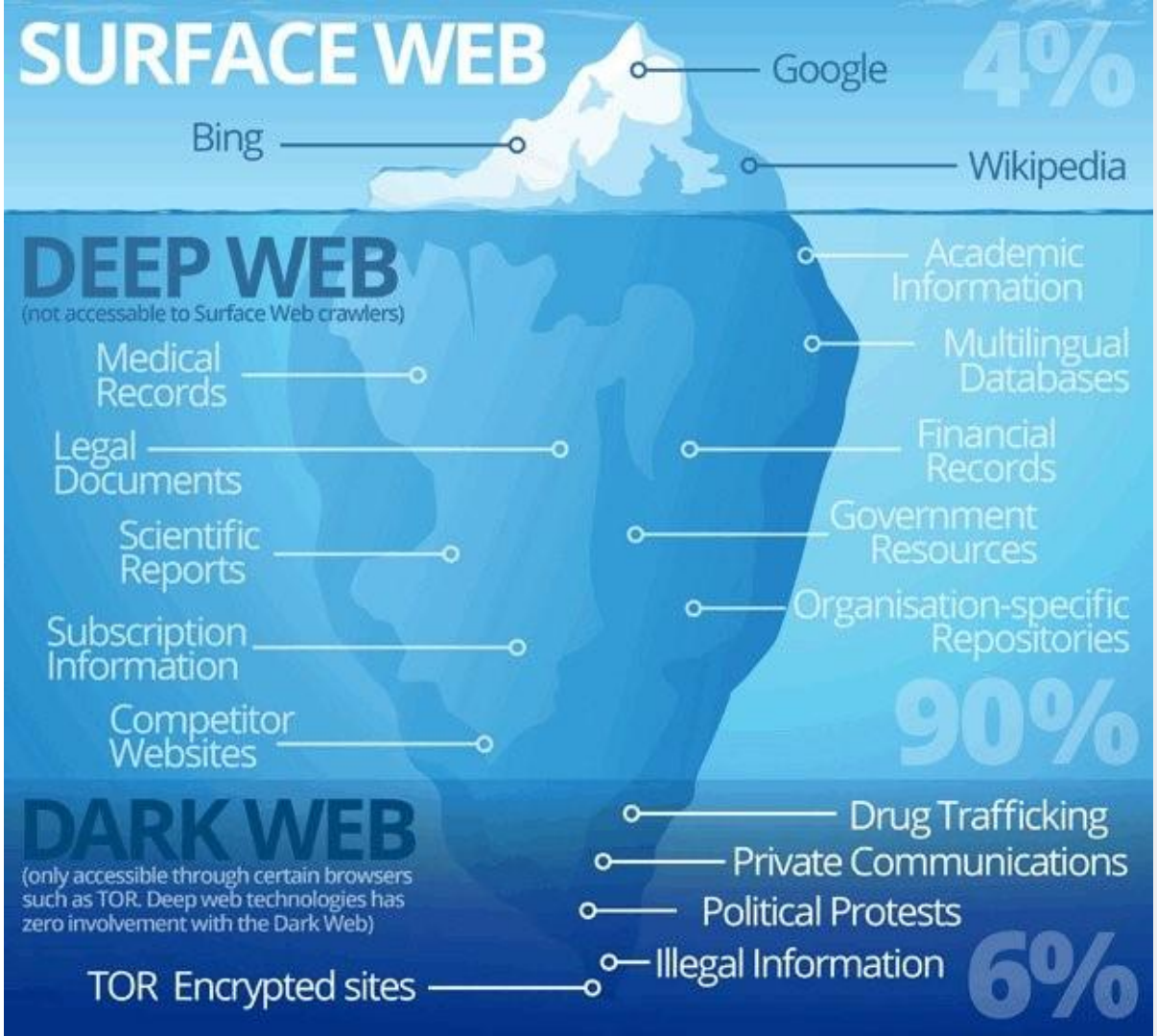
Twenty Seventeen
Tienes la versión 2.2. Actualiza a la 2.3.

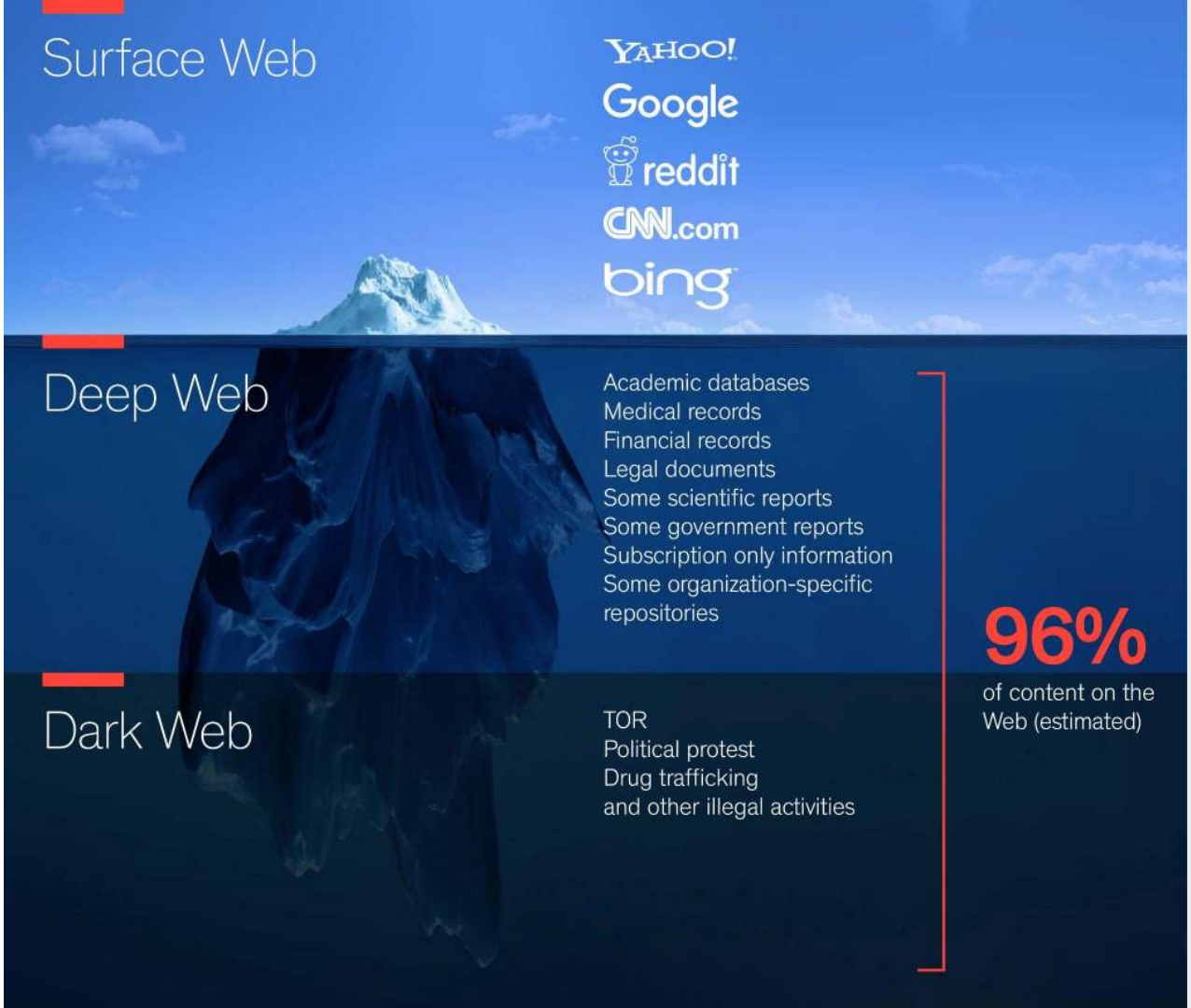
Twenty Thirteen
Tienes la versión 2.9. Actualiza a la 3.0.

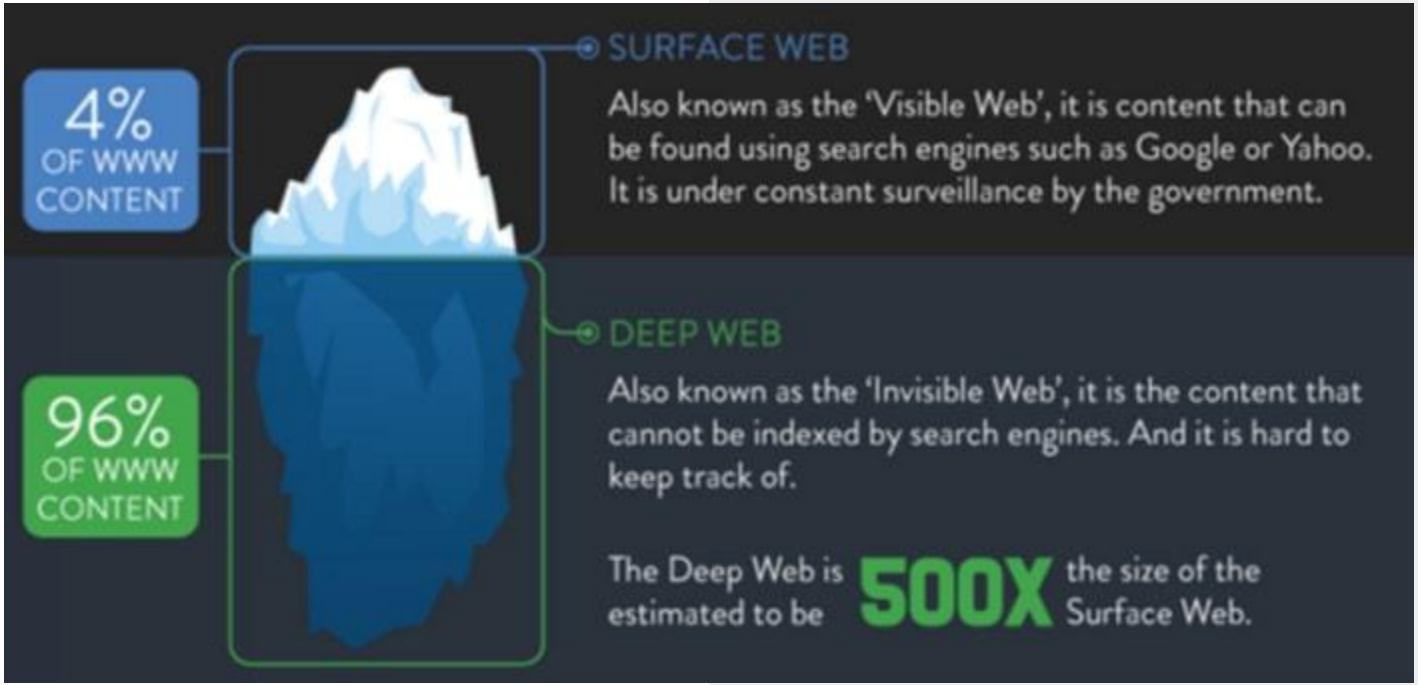
Twenty Twenty
Tienes la versión 1.1. Actualiza a la 1.2.

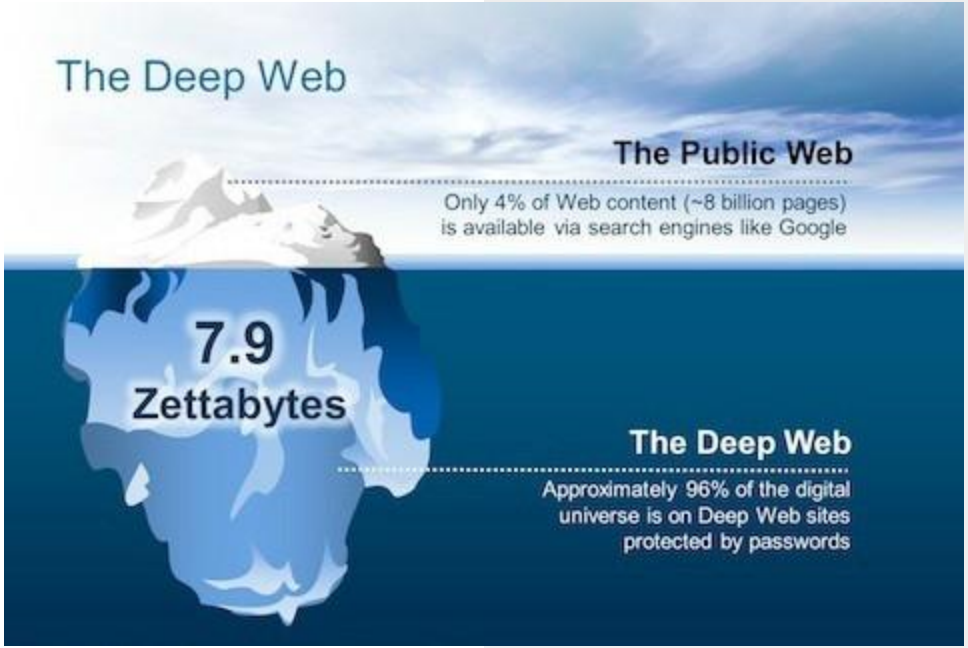
Seleccionar todos

Actualizar temas


SURFACE WEB
Google
Bing
Wikipedia
4%
DEEP WEB
(not accessable to Surface Web crawlers)
Medical Records
Legal Documents
Scientific Reports
Subscription Information
Competitor Websites
Academic Information
Multilingual Databases
Financial Records
Government Resources
Organisation-specific Repositories
90%
DARK WEB
(only accessible through certain browsers such as TOR. Deep web technologies has zero involvement with the Dark Web)
TOR Encrypted sites
Drug Trafficking
Private Communications
Political Protests
Illegal Information
6%


Surface Web
YAHOO!
Google
reddit
CNN.com
bing
Deep Web
Academic databases
Medical records
Financial records
Legal documents
Some scientific reports
Some government reports
Subscription only information
Some organization-specific repositories
Dark Web
TOR
Political protest
Drug trafficking
and other illegal activities
96%
of content on the Web (estimated)


4%
OF WWW
CONTENT
SURFACE WEB
Also known as the 'Visible Web', it is content that can be found using search engines such as Google or Yahoo. It is under constant surveillance by the government.
96%
OF WWW
CONTENT
DEEP WEB
Also known as the 'Invisible Web', it is the content that cannot be indexed by search engines. And it is hard to keep track of.
The Deep Web is estimated to be 500X the size of the Surface Web.


The Deep Web
The Public Web
Only 4% of Web content (~8 billion pages) is available via search engines like Google
7.9
Zettabytes
The Deep Web
Approximately 96% of the digital universe is on Deep Web sites protected by passwords

Compara le revisioni di “Hacked By Shade”

← Torna all'editor

Confronta due revisioni qualsiasi

Precedente

Successivo

Revisione corrente di
1 settimana fa (3 Mar @ 09:17)

Ripristina questa revisione

Titolo

Hacked By GeNErAL

Hacked By Shade

Contenuto

<title>~!Hacked By GeNErAL alias Mathis!~</title>
<h2>Hacked By GeNErAL</h2> <img border='0' src='http://www.officialpsds.com/images/thumbs/Baby-Devil-Toon-psd9848.png'>

Greetz : Kuroi'SH, RxR, K3L0T3X

</FOOTER><code><h1>\!/Just for Fun ~Hacked By GeNErAL\!/</code></h1> Hacked By GeNErAL! !

<title>Hacked By Shade</title><h2>Hacked By Shade</h2> <img border='0' src='https://s-media-cache-ak0.pinimg.com/originals/e0/38/0e/e0380e49476ace36f1f579c15784db37.jpg'>

GreetZ: Prosox - Sxtz - KDZ - RxR HaCkEr - GeNErAL - HolaKo - Golden-Hacker - ~Abo-Al EoS

<font color='#1560BD' />Twitter: @ShadeHaxor

</FOOTER><code><h1></code></h1>

Medidas: Reactivas vs Proactivas

Reactiva:

Cuando **ya ha pasado** algo malo

Mitigación de **daños**

Proactiva:

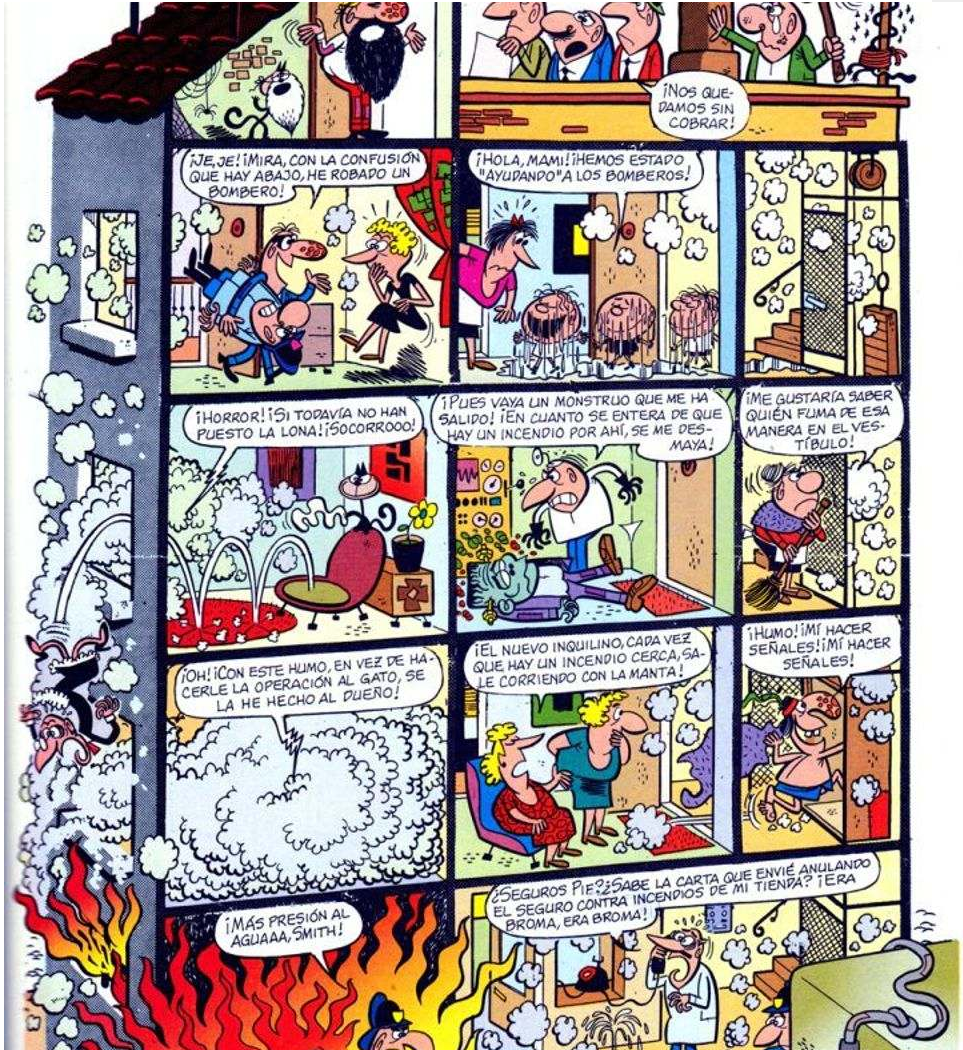
Antes de que pase lo malo

Mitigación de **riesgos**

Recuerde invertir en

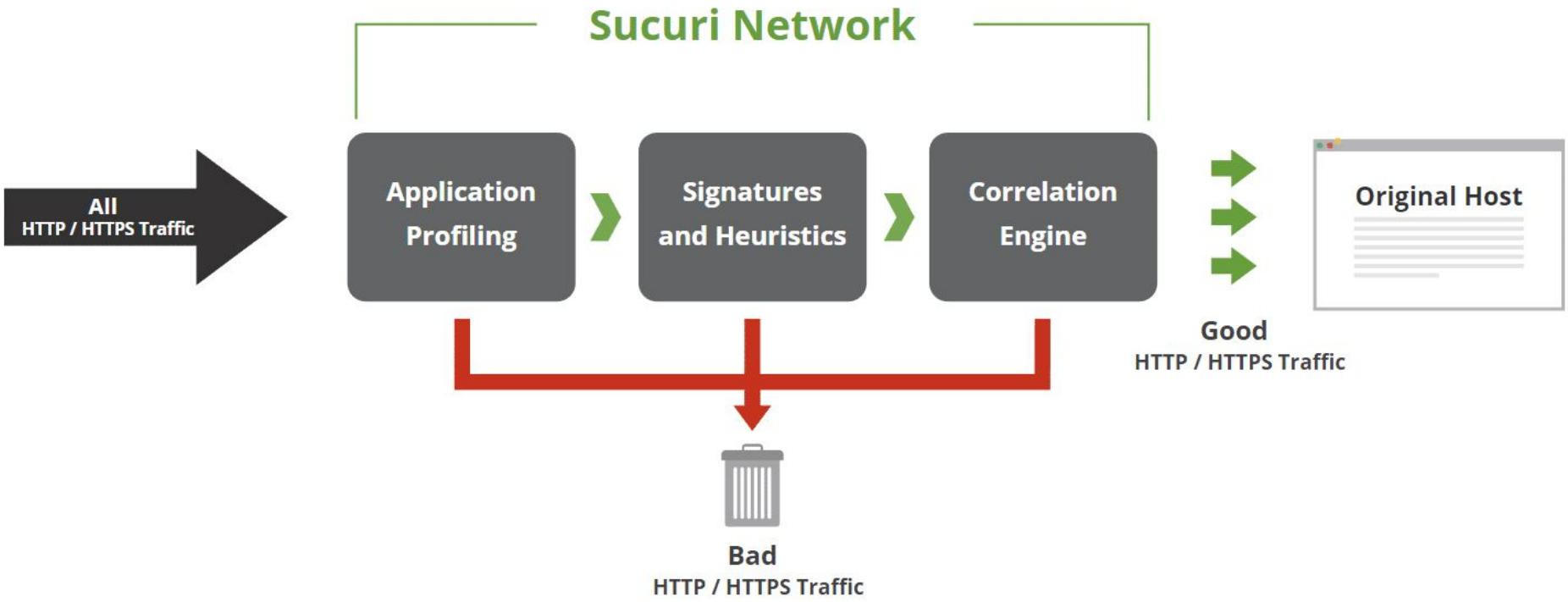
SEGURIDAD

HOSTING


¡NOS QUEDAMOS SIN COBRAR!
¡JE,JE! ¡MIRA, CON LA CONFUSIÓN QUE HAY ABAJO, HE ROBADO UN BOMBERO!
¡HOLA, MAMÍ! ¡HEMOS ESTADO "AYUDANDO" A LOS BOMBEROS!
¡HORROR! ¡SI TODAVÍA NO HAN PUESTO LA LONA! ¡SOCORROOO!
¡PUES VAYA UN MONSTRUO QUE ME HA SALIDO! ¡EN CUANTO SE ENTERA DE QUE HAY UN INCENDIO POR AHÍ, SE ME DESMAYA!
¡ME GUSTARÍA SABER QUIÉN FUMA DE ESA MANERA EN EL VESTÍBULO!
¡OH! ¡CON ESTE HUMO, EN VEZ DE HACERLE LA OPERACIÓN AL GATO, SE LA HE HECHO AL DUEÑO!
¡EL NUEVO INQUILINO, CADA VEZ QUE HAY UN INCENDIO CERCA, SALE CORRIENDO CON LA MANTA!
¡HUMO! ¡MÍ HACER SEÑALES! ¡MÍ HACER SEÑALES!
¡MÁS PRESIÓN AL AGUAAA, SMITH!
¿SEGUROS PIE? ¿SABE LA CARTA QUE ENVIÉ ANULANDO EL SEGURO CONTRA INCENDIOS DE MI TIENDA? ¡ERA BROMA, ERA BROMA!

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**


Everybody needs a hacker