

# 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**









## 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	Organization	Attacker Location	IP	Target 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

## ATTACK TYPES

#	Service
2	discard
1	ssh
1	unknown
1	netbios-dgm
1	db-lsp-disc
1	ms-sql-s
1	isakmp
1	unknown

# NORSE

## ATTACK ORIGINS

COUNTRY
1000 China
1000 United States
900 Russia
600 Saudi Arabia
500 Netherlands
400 France
100 Moldova
100 South Korea
100 Brazil
100 Finland



## ATTACK TARGETS

COUNTRY
3900 United States
900 Saudi Arabia
300 United Arab Emirates
200 Philippines
200 Liechtenstein
200 France
100 Russia
100 Taiwan
100 Cyprus
100 Mexico

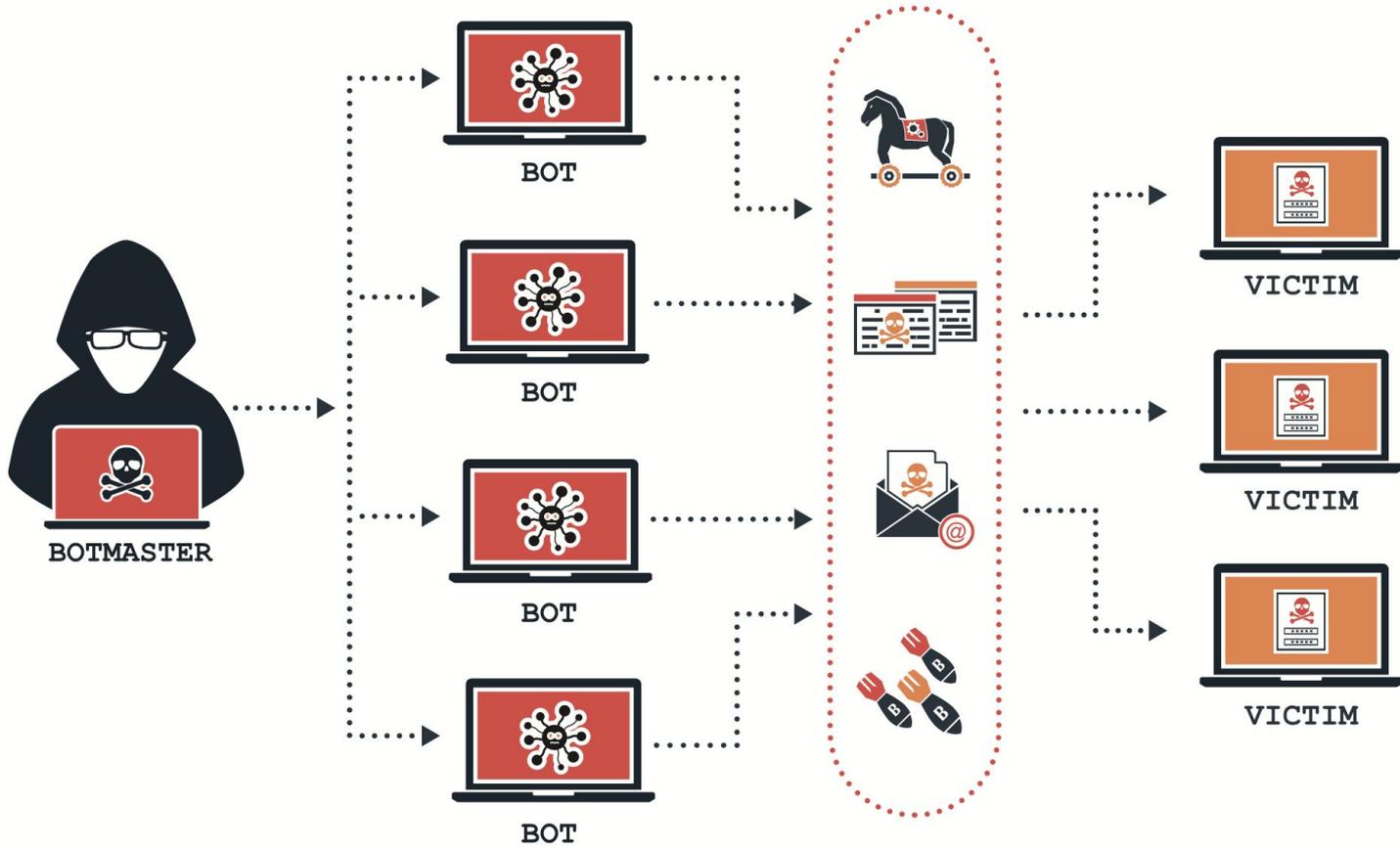
## LIVE ATTACKS

TIMESTAMP	ATTACKER ORGANIZATION	LOCATION	IP	TARGET LOCATION	TYPE SERVICE	PORT
2015-11-25 15:05:40.44	Hacking Team Technologies Inc	Beijing, China	115.47.24.276	Rossmore, United States	http	80
2015-11-25 15:05:40.42	Hacking Team Technologies Inc	Beijing, China	115.47.24.220	Rossmore, United States	http	80
2015-11-25 15:05:40.40	Hacking Team Technologies Inc	Beijing, China	115.47.24.220	Rossmore, United States	http	80
2015-11-25 15:05:40.38	Hacking Team Technologies Inc	Beijing, China	115.47.24.220	Rossmore, United States	http	80
2015-11-25 15:05:40.36	Hacking Team Technologies Inc	Beijing, China	115.47.24.220	Rossmore, United States	http	80
2015-11-25 15:05:40.34	Hacking Team Technologies Inc	Beijing, China	115.47.24.220	Rossmore, United States	http	80
2015-11-25 15:05:40.32	Hacking Team Technologies Inc	Beijing, China	115.47.24.220	Rossmore, United States	http	80
2015-11-25 15:05:40.30	Hacking Team Technologies Inc	Beijing, China	115.47.24.220	Rossmore, United States	http	80
2015-11-25 15:05:40.28	Hacking Team Technologies Inc	Beijing, China	115.47.24.220	Rossmore, United States	http	80
2015-11-25 15:05:40.26	Hacking Team Technologies Inc	Beijing, China	115.47.24.220	Rossmore, United States	http	80

## ATTACK TYPES

SERVICE	PORT
10000 http	80
20000 http	80
40000 microsoft-ds	46
30000 telnet	23
20000 http-alt	8080
30000 unknown	204
70000 unknown	200
10000 netbios-dgm	138

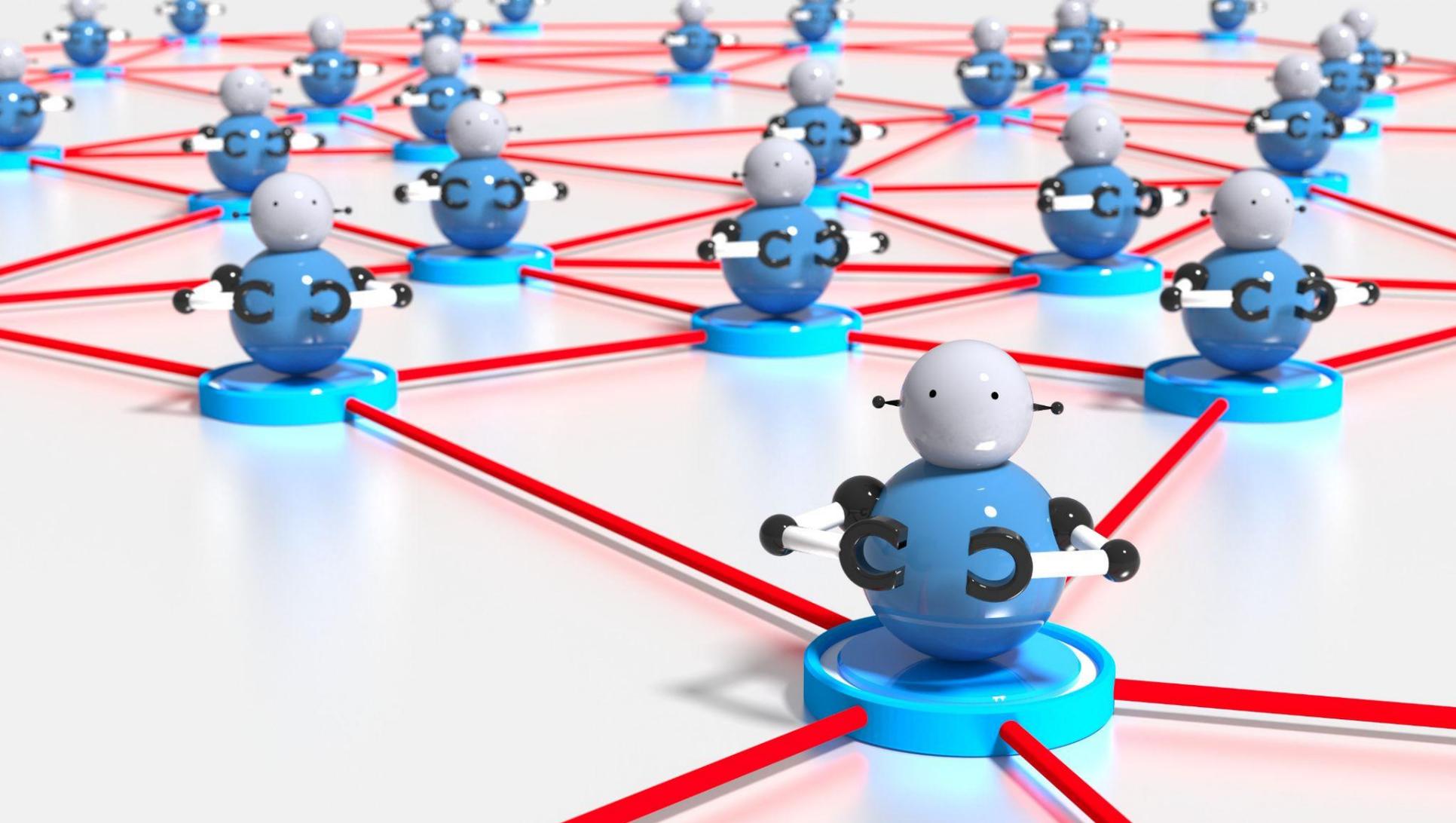


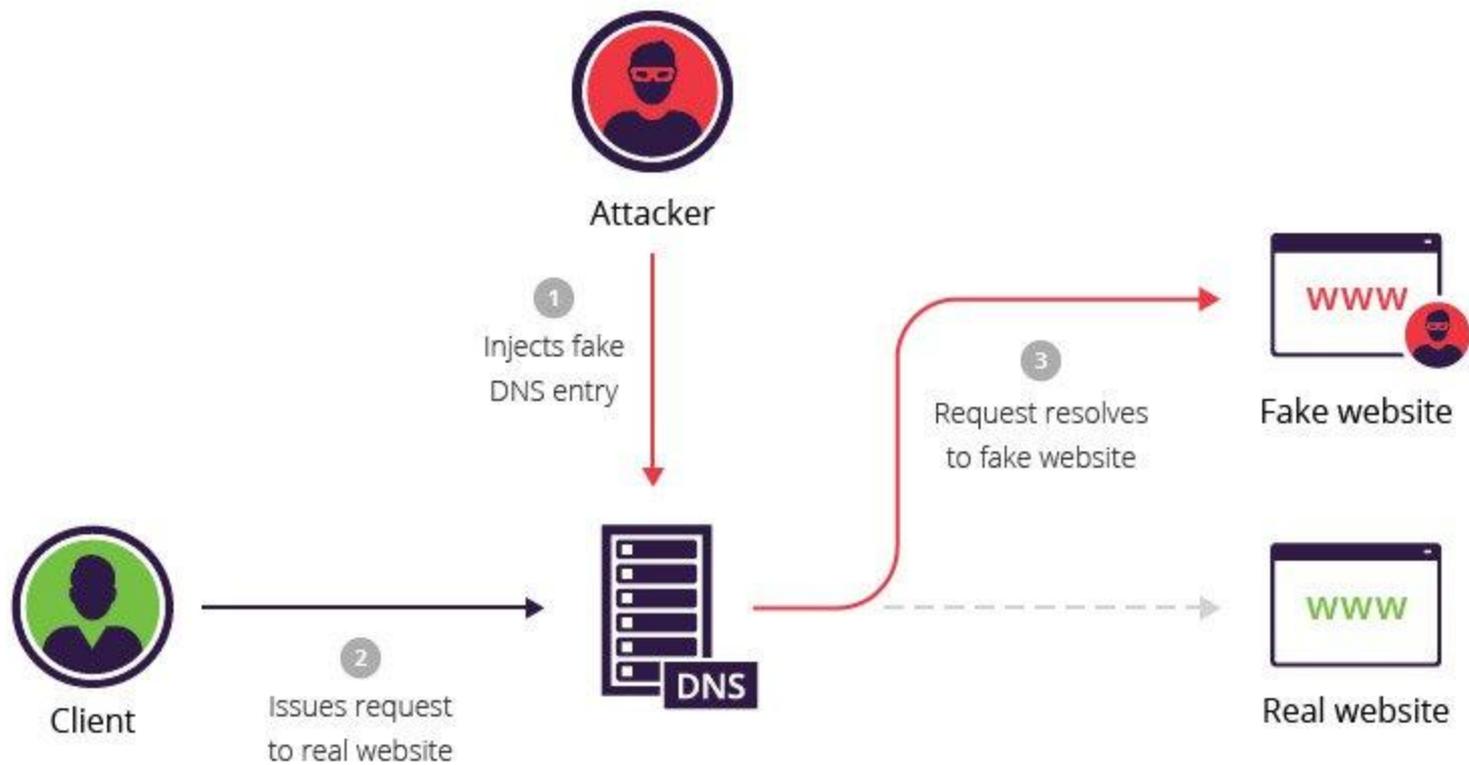


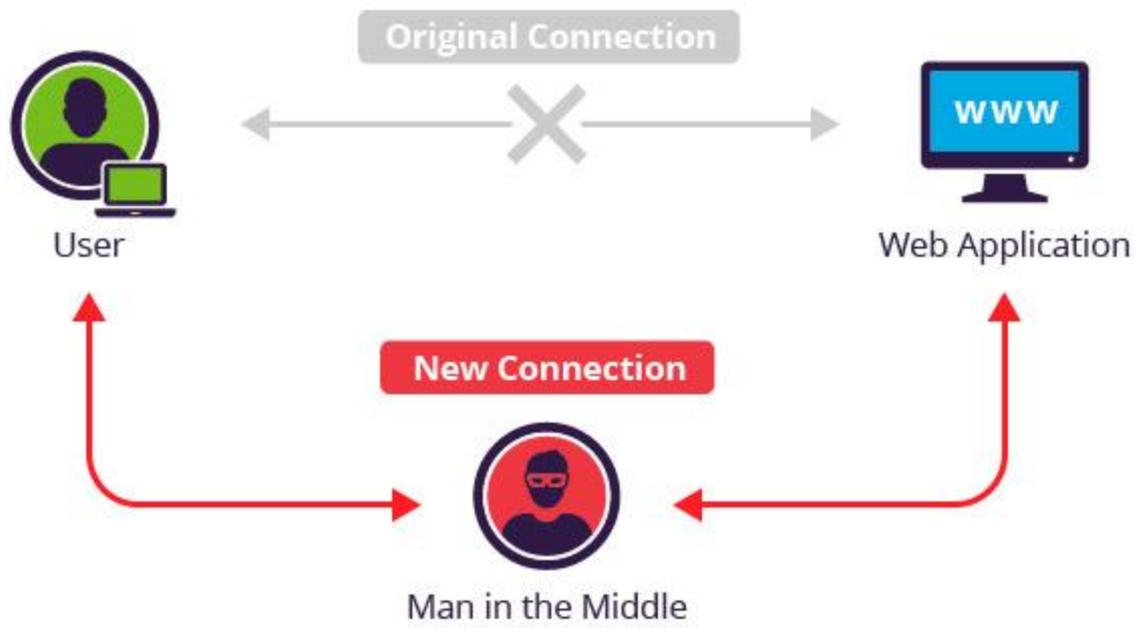


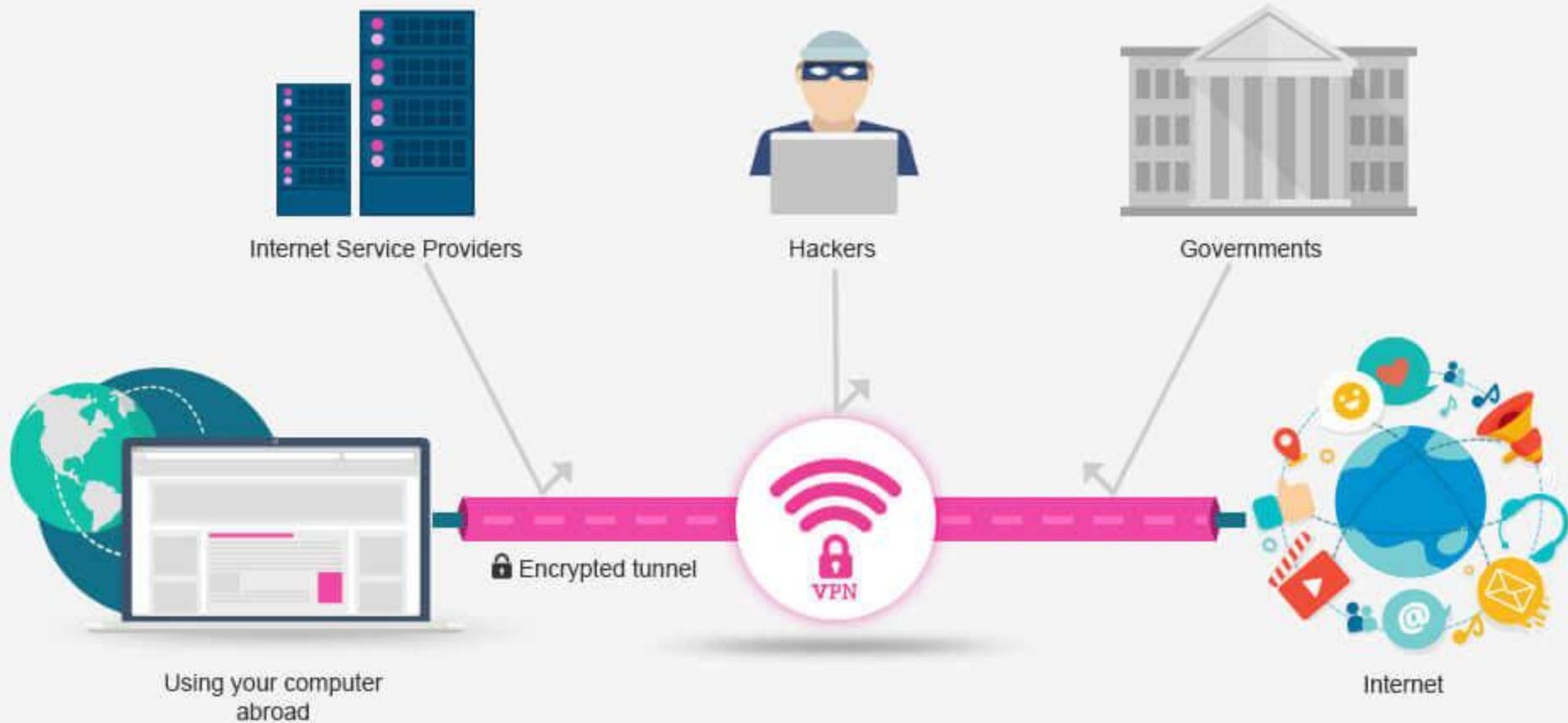


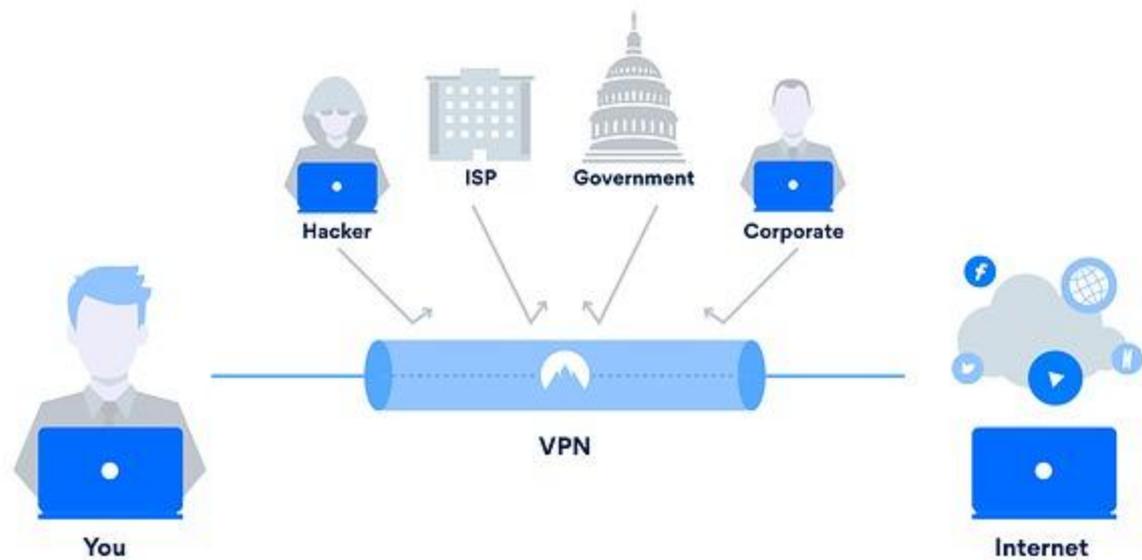












A 3D perspective illustration of a maze. The maze is composed of white walls and grey shadows. In the center of the maze, the word "DATA" is written in white, blocky, 3D letters. Below it, the word "BREACH" is written in red, blocky, 3D letters. Above the word "DATA", there is a red, 3D crown-like shape that appears to be shattering or exploding, with several white, angular fragments flying outwards. The overall scene is brightly lit, creating strong highlights and shadows.

**DATA**  
**BREACH**

Remote site: /public\_html/wp-content/plugins/joom

Remote site: /public\_html/wp-content/plugins

Filename | Fi

Filename ^ | Filesize

- ..
- \_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

- ..
- Login-wall-KiLxb
- Login-wall-NUJIF
- 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

- 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](#)

Screen Options Help

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

<input type="checkbox"/>	Username	Name	Email	Role	Posts
<input type="checkbox"/>	admin	[Redacted]	[Redacted]	Administrator	78
<input checked="" type="checkbox"/>	akmin	[Redacted]	no@email.com	Administrator	1
<input type="checkbox"/>	janel	[Redacted]	[Redacted]	Contributor	0
<input type="checkbox"/>	levy	[Redacted]	[Redacted]	Contributor	33
<input checked="" type="checkbox"/>	managed-wp-migration-465790ae	Managed WordPress Migration U		Administrator	0
<input checked="" type="checkbox"/>	wp.service.controller.lHmp6			None	0
<input type="checkbox"/>	Username	Name		Role	Posts



Bulk Actions Apply Change role to... Change

6 items

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

Bing

Google

4%

Wikipedia

# DEEP WEB

(not accessible 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 **500X** the size of the estimated to be 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

# Confronta 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**

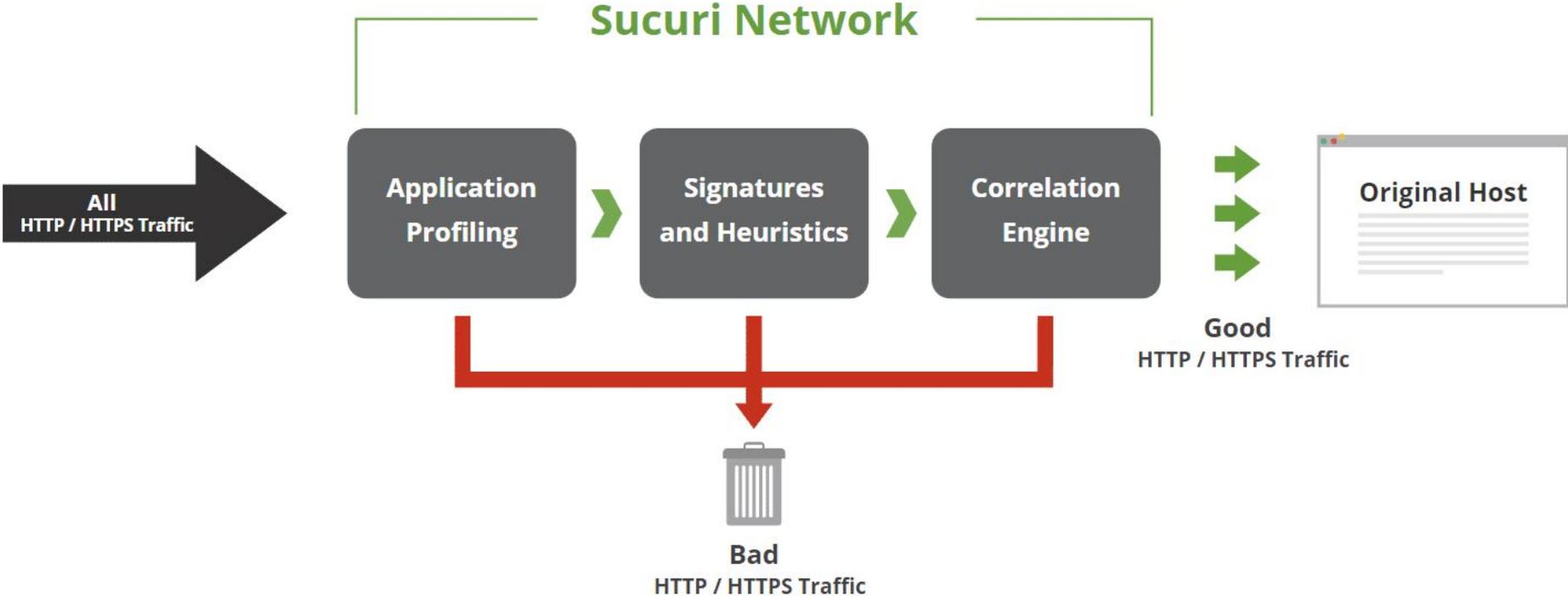
## Contenuto

```
<title>-!Hacked By GeNErAL alias Mathis!~</title>
<h2>Hacked By GeNErAL</h2>&nbsp;</font></p><img border='0'
src='http://www.officialpsds.com/images/thumbs/Baby-Devil-
Toon-psd9848.png'><br><br><br><b>Greetz : Kuroi'SH, RxR,
K3L0T3X </b><br><br></FOOTER><b><code><h1>\!~/Just for Fun
~Hacked By GeNErAL\!/</code></h1></b><p
align='center'><font color='red' /><font face='Superdie'
size='5' color='#FF0000'>Hacked By GeNErAL! !</font>
</font></p>
```

```
<title>Hacked By Shade</title><h2>Hacked By
Shade</h2>&nbsp;</font></p><img border='0' src='https://s-
media-cache-ak0.pinimg.com/originals/e0/38
/0e/e0380e49476ace36f1f579c15784db37.jpg'><br><br>
<br><b>GreetZ: Prosox - Sxtz - KDZ - RxR HaCKEr - GeNErAL
- HolaKo - Golden-Hacker - ~Abo-AL EoS<br><br><br><font
color='#1560BD' />Twitter: @ShadeHaxor</b><br><br>
</FOOTER><b><code><h1></code></h1></b><p
align='center'></p>
```

# Website Application Firewall (WAF)

Protect and Speed Up Your Website



A black and white photograph showing the back of a person wearing a dark t-shirt. The t-shirt has the text "Everybody needs a hacker" printed on it in a white, sans-serif font. The person's hair is visible at the top of the frame, and the background is blurred.

Everybody needs a hacker