WordCamp Osaka 2019

On December 6th and 7th, 2019 at Osaka

with__

Hacking WordPress & countermeasures.

Nestor Angulo de Ugarte

Hacking WordPress & Countermeasures

NESTOR ANGULO DE UGARTE

WORDCAMP OSAKA 2019

#WCOSAKA

こんにちわ!

Who I am

- Computer Science Engineer & Technology consultant
- Photographer & Early Adopter
- Truly curious guy

- 2015: **SUCURI**
  Incident Response & Easy SSL

- 2019: **GoDaddy Spain**
  Interim Head of IT @ GoDaddy Spain

Where is カナリア諸島

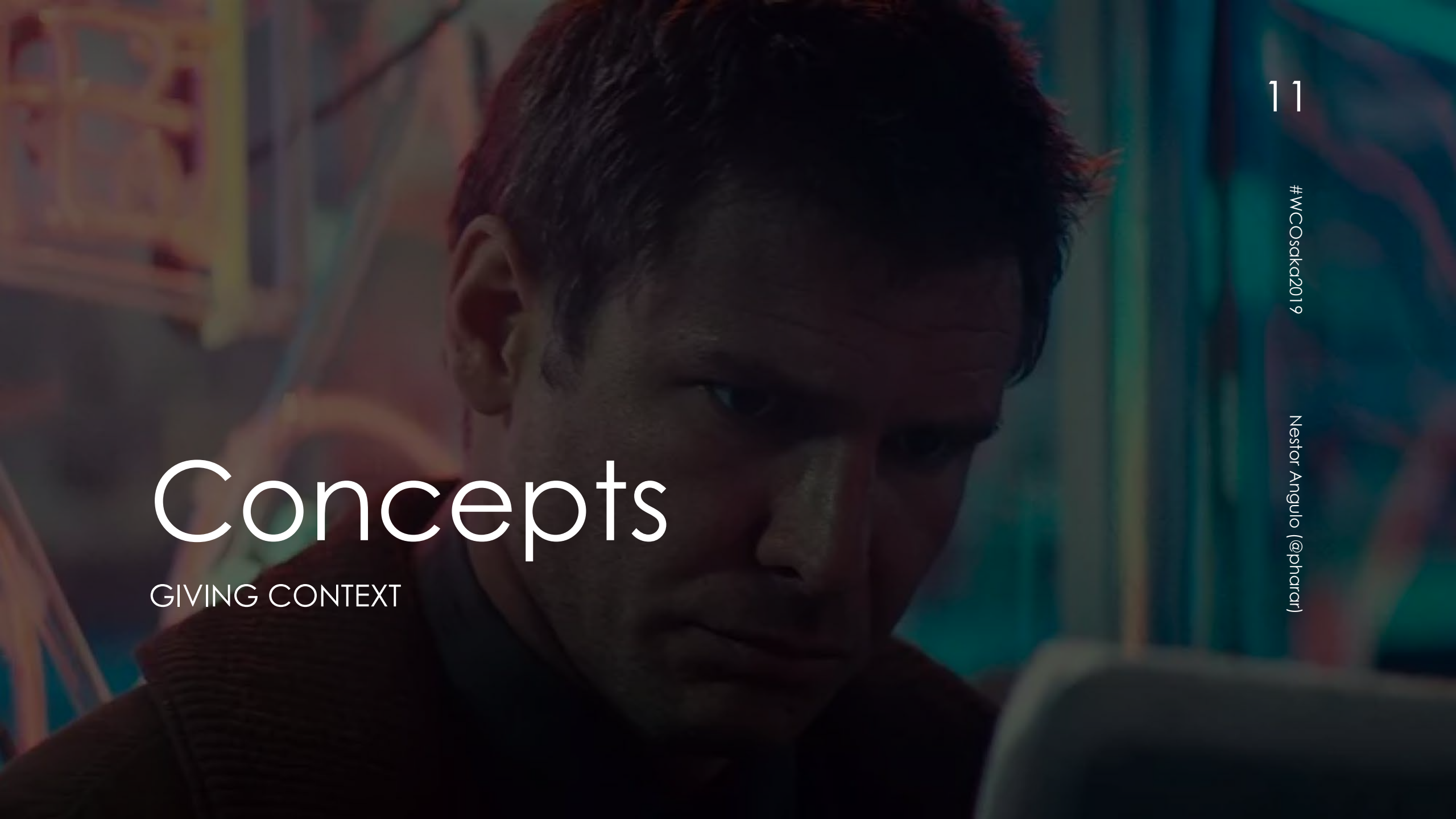
About

- Sucuri: **Anaconda**
  (No Securi / Security)
- **Website security**
- Fully remote (people from > 25 countries around the world)
- 2008: **Foundation**
- 2017: Proud part of the **GoDaddy family**

- **Free scanners**:
  - Sitecheck
    (sitecheck.sucuri.net)
  - Performance
    (performance.sucuri.net)

Hacking WordPress

- Concepts
  - Hacker VS Cyberterrorist
    - Types
  - Malware
  - Cybersecurity
  - Facts
- The Art of War: In the mind of your enemy
  - Hacking WordPress
    - Targets
    - Know your Weaknesses
    - Process
  - Gallery of Horrors
    - Defacements
    - Black Hat SEO
    - DDoS / BotNets
- Countermeasures: Reactive vs Proactive
  - Characters in this story
  - Security as Layer-based system
  - The more Doors, the higher Risk
  - Reactive vs Proactive Measures
  - WAF



Concepts

GIVING CONTEXT

DISCLAIMER

Any sensitive information has been protected/encrypted to preserve privacy. Any similiarity with reality is a coincidence.

I'm responsible of what I say, not what you interpret.

Always ask an expert.

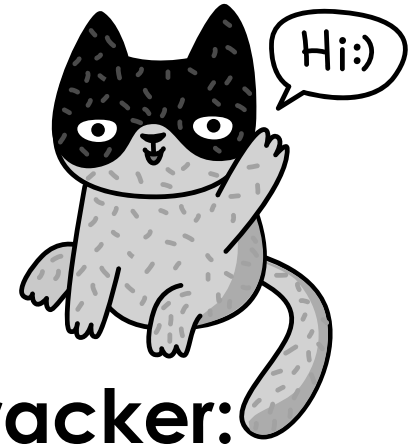

There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked.
John Chambers
Chief Executive Officer of Cisco

ハッキングされた企業と、
ハッキングされたことをまだ知らない企業の2種類があります。

HACKER VS Cyberterrorist

Hacker:

Curious person who loves to go beyond limits or convetionalisms.



Cyberterrorist / Cracker:

Computer Hacker, whom intentions are always aligned to enrich himself in a zero-sum game situation.

The bad guy

Hacker Hat Colours

- **Black Hat**
  Cyberterrorist, thief
- **Grey Hat**
  White Hat using illegal procedures
- **White Hat**
  Security Analyst, ethical hacker

Malware

- Software **intentionally** designed to cause **damage** to a **computer**, **client**, or **computer network.**
- Some types:
  - Backdoors, zero-day
  - Exploits
  - Trojan horses, Fremium plugins
  - Ransomware, Spyware
  - Adware, Scareware

CyberSecurity & Web Security

- **Cybersecurity**:
  Security in the digital world
- **Web Security**:
  Field of Cybersecurity
- Covers what happens through port 80 / 443

FACTS

Site hacking **almost never** is client-oriented (98% of cases)

Almost always happens due to a **deficient monitoring / maintenance**

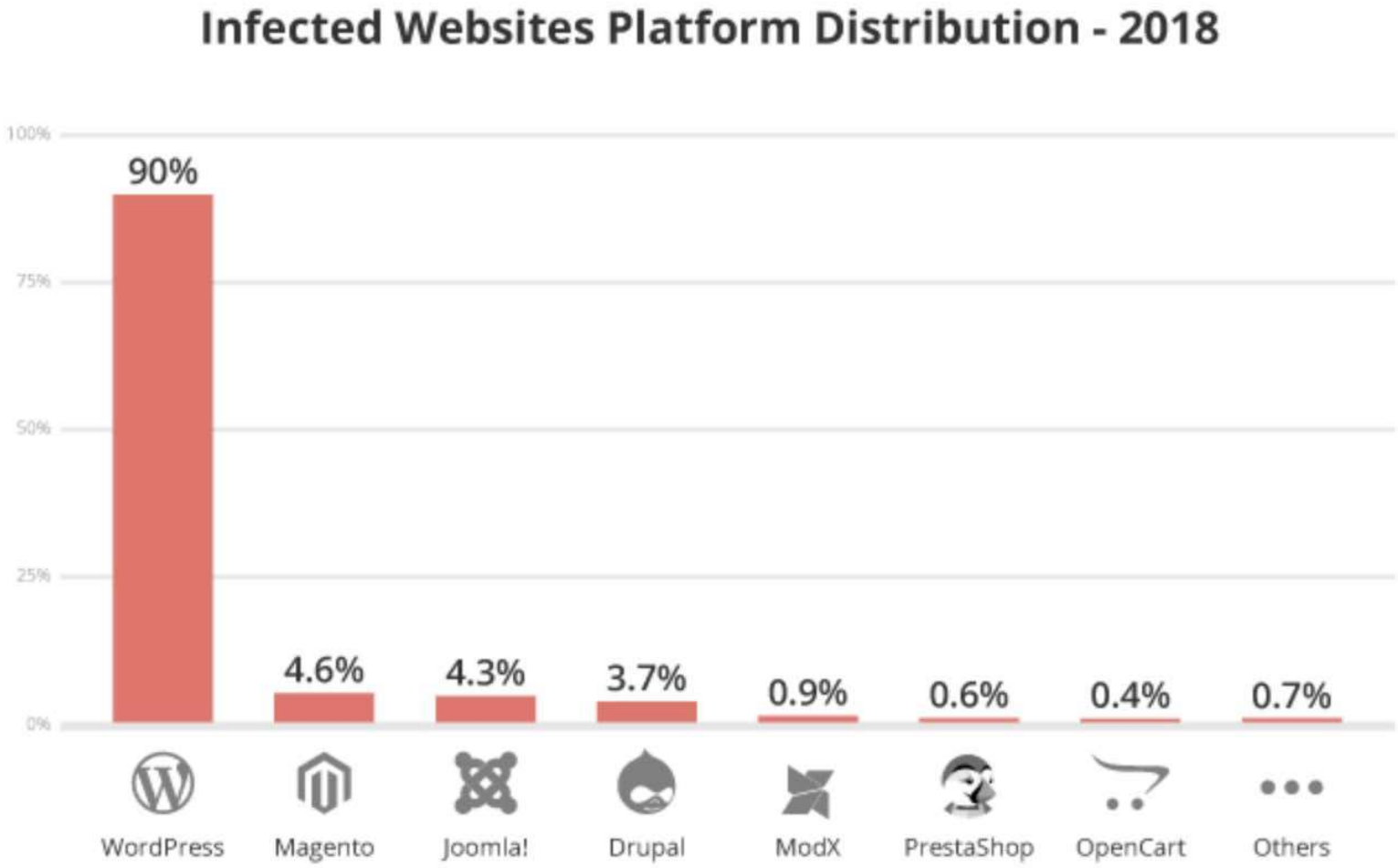
A **SSL** certificate **is not** an antihacking shield

Patches & security updates appear almost always after hacking exploits

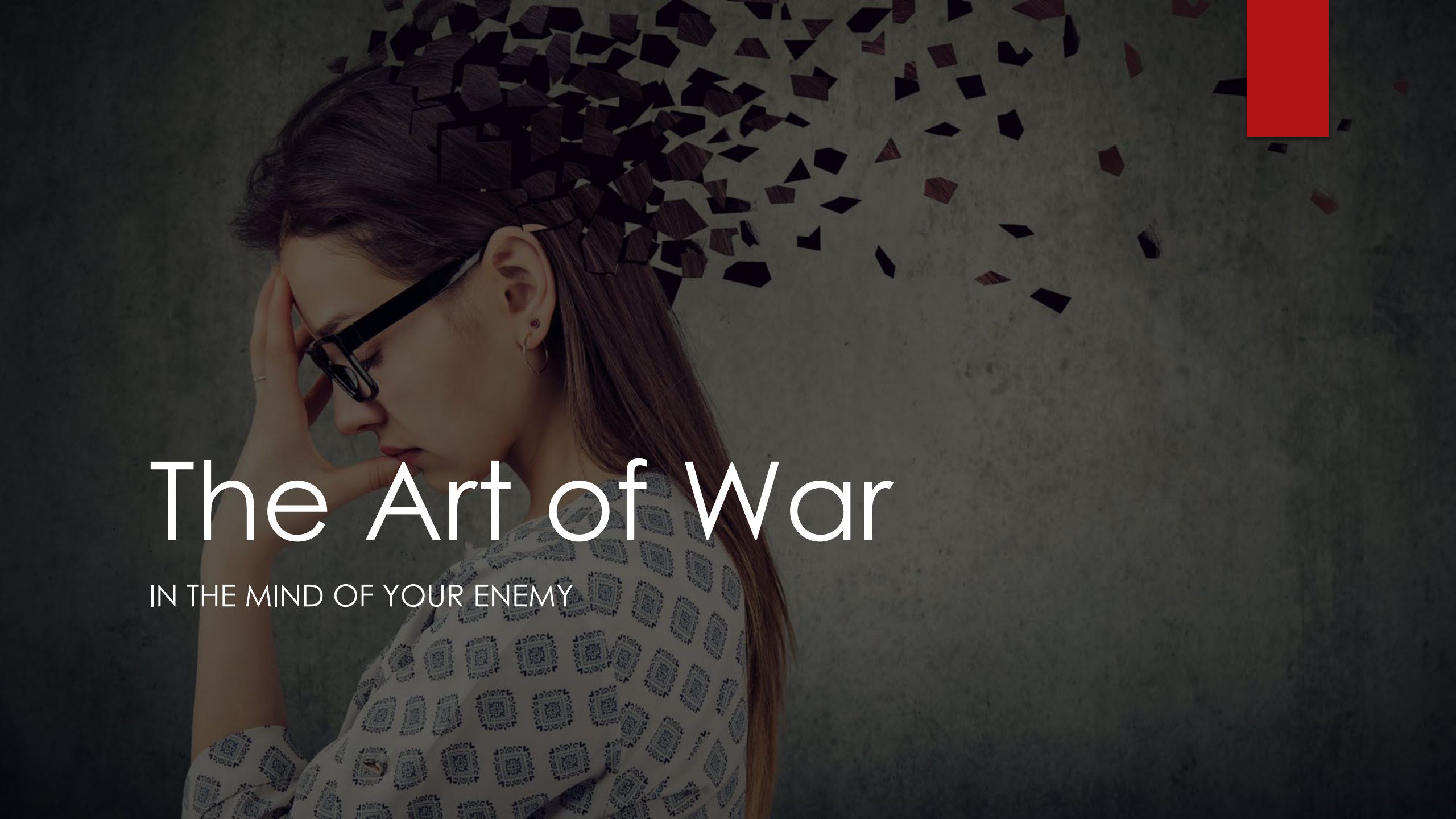
Errare Humanum Est (Human being fails)

Security **never is (nor will be)** 100% effective

FACTS



Source: Website Hack Trend Report 2018 – sucuri.net



The Art of War

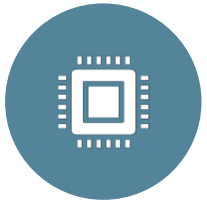
IN THE MIND OF YOUR ENEMY

Common Targets

Users info

Database

Website Content



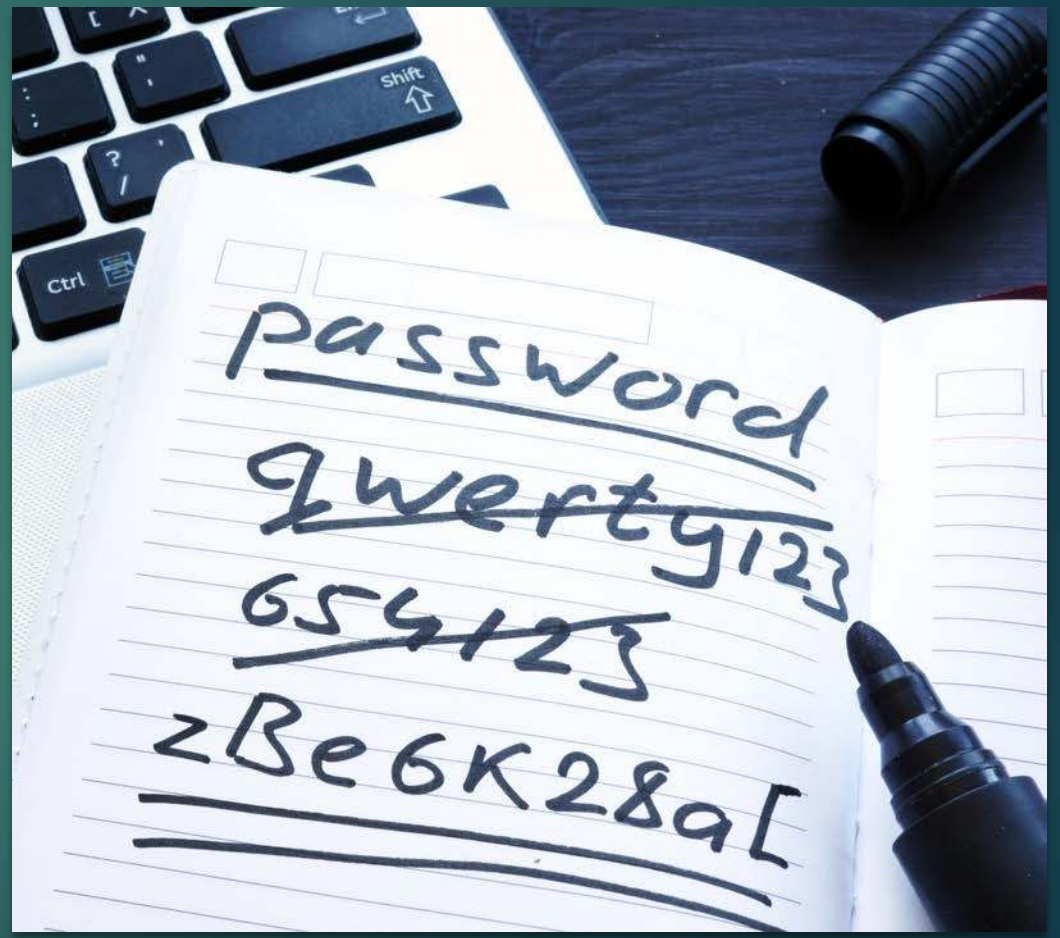
Infrastructure

Bot Net

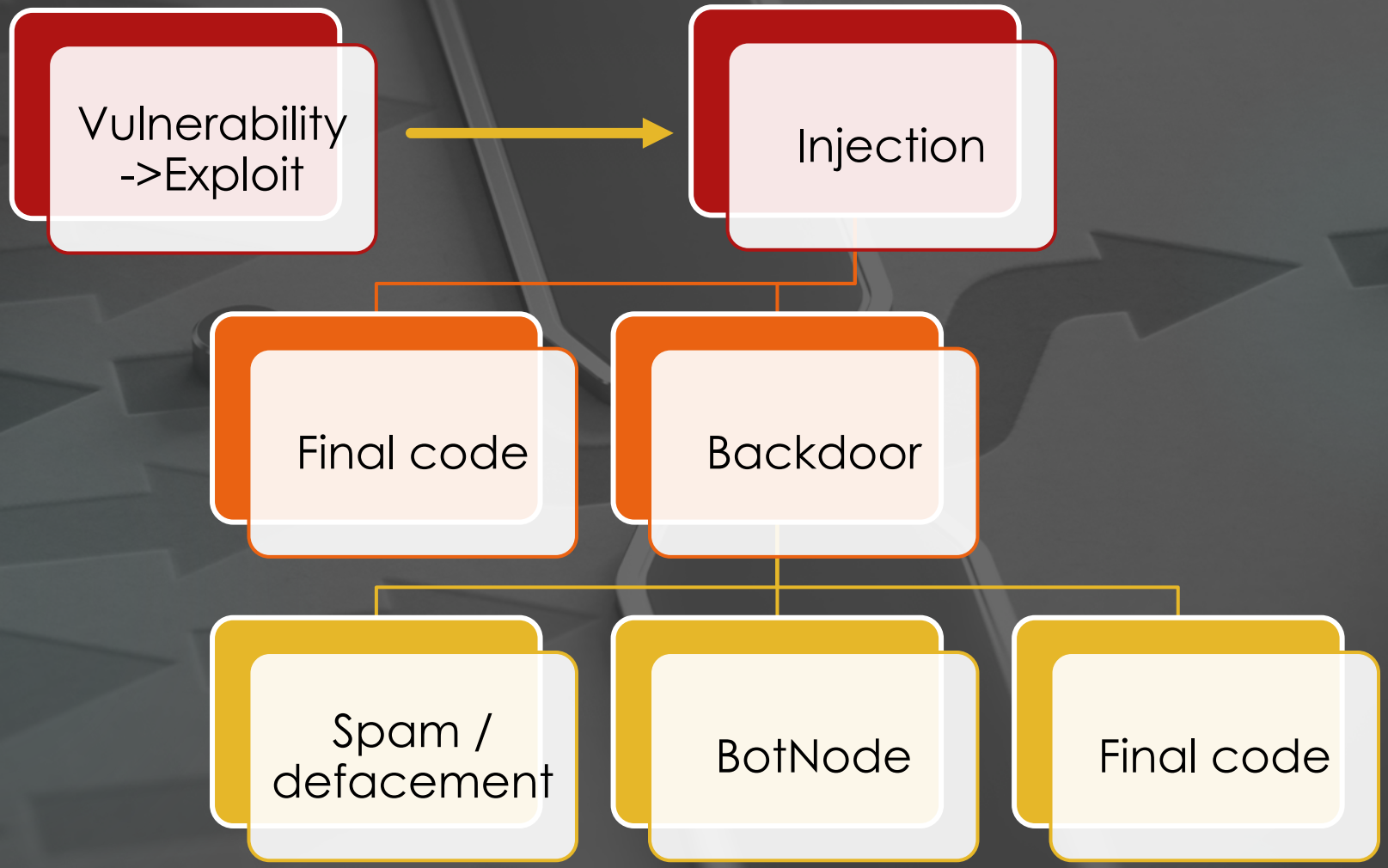
Reputation

Know your weaknesses

- You are your **weakest** point
  - You can be scammed
- **Passwords**.
  - Vulnerable to brute force attacks
- **Leftovers**
  - Admin users
- **Outdated**/vulnerable software
  - Enabled/Disabled not-in-use plugins/themes
- **Non-secure connection** (avoid public wifi)
  - Vulnerable to Man-In-the-Middle attacks

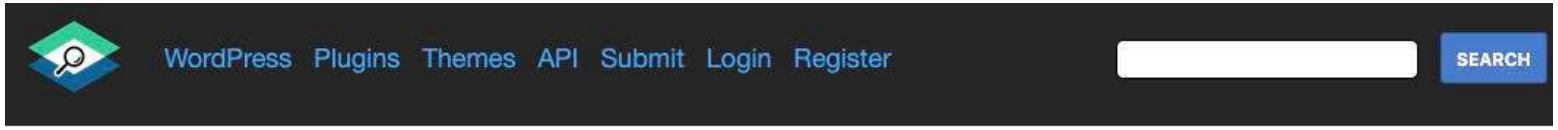


Hacking WordPress. The Process



Definitions

- **Vulnerability**
  - Bug in the code or posibility of misuse that can be exploited to perform unauthorized actions within a computer system.
- **Exploit**
  - Software that leverages a vulnerability
- **Backdoor**
  - Malware which allows remote execution of code



WPScan Vulnerability Database

Cataloging **16867** WordPress Core, Plugin and Theme vulnerabilities

Free Email Alerts | Submit a Vulnerability | Try our API

Latest WordPress Vulnerabilities

2019-10-14	WordPress <= 5.2.3 - Admin Referrer Validation
2019-10-14	WordPress <= 5.2.3 - JSON Request Cache Poisoning
2019-10-14	WordPress <= 5.2.3 - Server-Side Request Forgery (SSRF) in URL Validation
2019-10-14	WordPress <= 5.2.3 - Stored XSS in Customizer
2019-10-14	WordPress <= 5.2.3 - Stored XSS in Style Tags
2019-10-14	WordPress <= 5.2.3 - Unauthenticated View Private/Draft Posts
2019-09-05	WordPress <= 5.2.2 - Cross-Site Scripting (XSS) in URL Sanitisation

Latest Plugin Vulnerabilities

2019-11-26	WP Spell Check <= 7.1.9 - Cross-Site Request Forgery (CSRF)
2019-11-19	Jetpack 5.1-7.9 - Vulnerability in Shortcode Embed Code
2019-11-19	WP Maintenance <= 5.0.5 - Cross-Site Request Forgery to Stored Cross-Site Scr...
2019-11-17	Sassy Social Share <= 3.3.3 - Cross-Site Scripting (XSS)
2019-11-14	Blog2Social < 5.9.0 - Cross-Site Scripting Issue

WPScan Vulnerability Database

wpvulndb.com

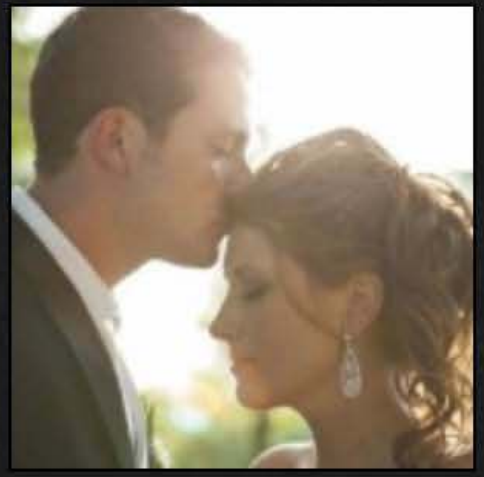
Gallery of Horrors

Defacements

Defo ments

Example 1: Photographer Gallery

St. Louis Weddings -
Photography



Engagements

Portraits

Newborns &
Maternity

Seniors

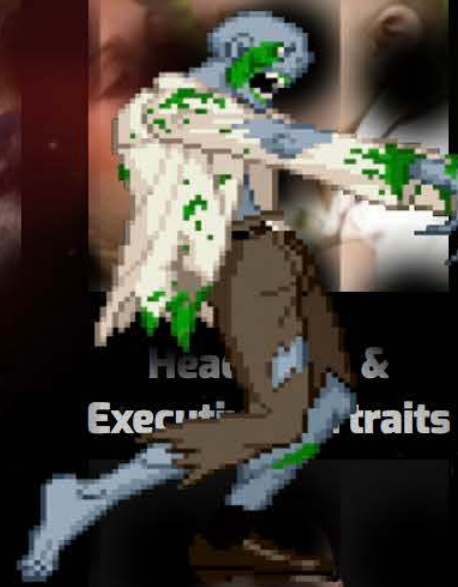
Headshots &
Executive Portraits

Galleries - ALL

Hacked By Dik4h4nZ

Photography

Seniors



Security Attack !!!

Contact

Example 2: Pet food store

Dog

Dry Dog Food

Wet Dog Food

Dog Treats & Dog Bones

Dog Supplements & Special Food

Dog Kennels, Dog Flaps & Gates

Dog Crates & Dog Travel

All

Cat

Dry Cat Food

Wet Cat Food

Cat Litter

Cat Litter Boxes & Litter Trays

Cat Trees & Cat Scratching Posts

Cat Baskets & Beds

All

Top recommendations:


Hacked by El Moujahidin
#Free Syria
#Free Palestine
Tell Your Gov , To Know About Palestine
We Will Countinue Hacking The Sites , To Send The Message Of Our Palestine And All Arabs

Bonus


AYYILDIZ TIM
48.ALAY BİRİM KOMUTANLIĞI
CEDKAN | KEREM SAH NOYAN | ALBAYRAK
LOPHIUS | DENIZ AKREP | ASENA | KARAYEL | OGUZ AYT
SIPAHI | OGUZ KAĞAN | ERIM AYT | LAST AYT | MARSTYSON
AYYILDIZ TIM
#WCOsaka2019
Nestor Angulo (@pharar)

DEFACEMENTS

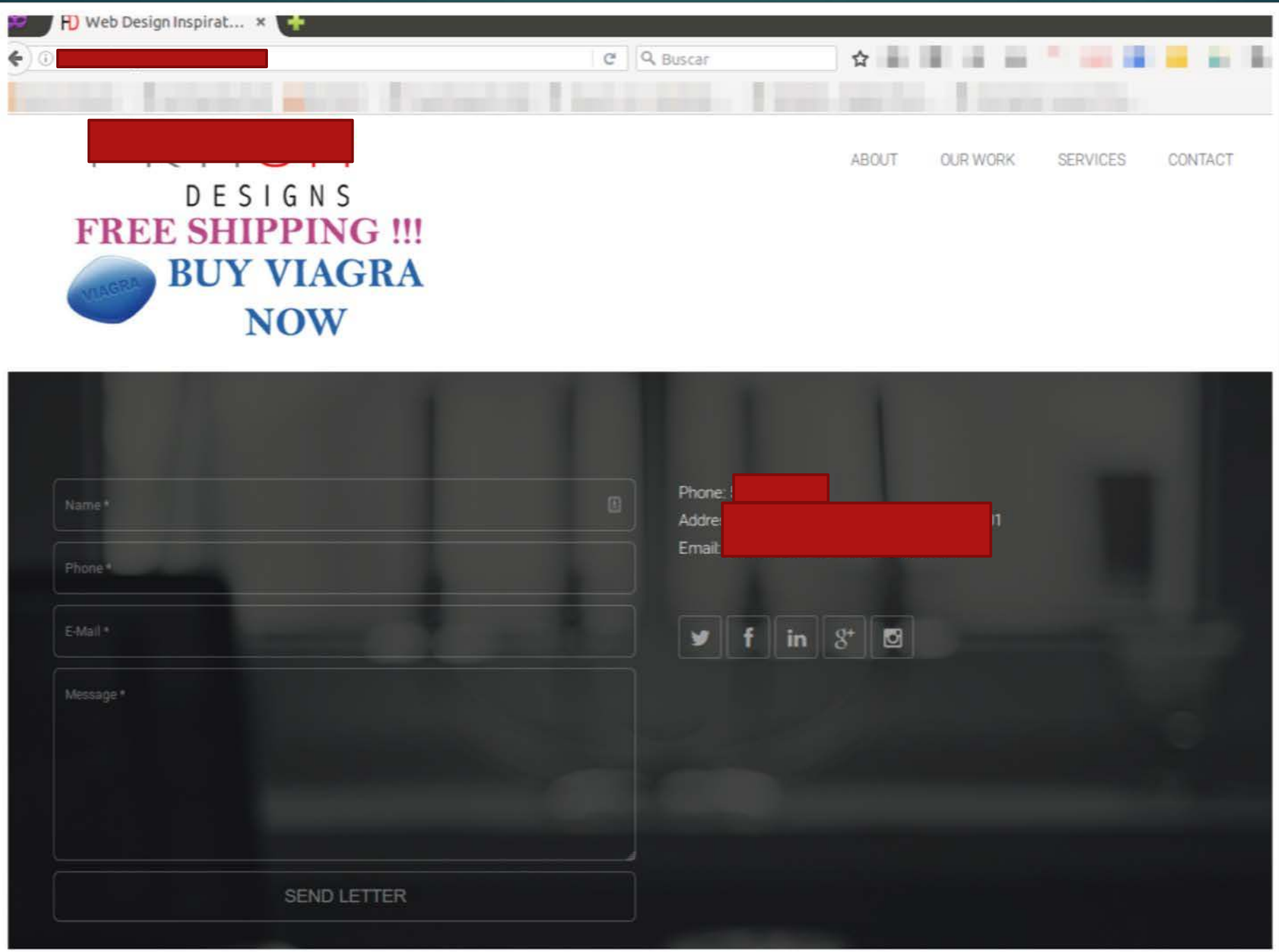
Partial / full replacement of website frontend.

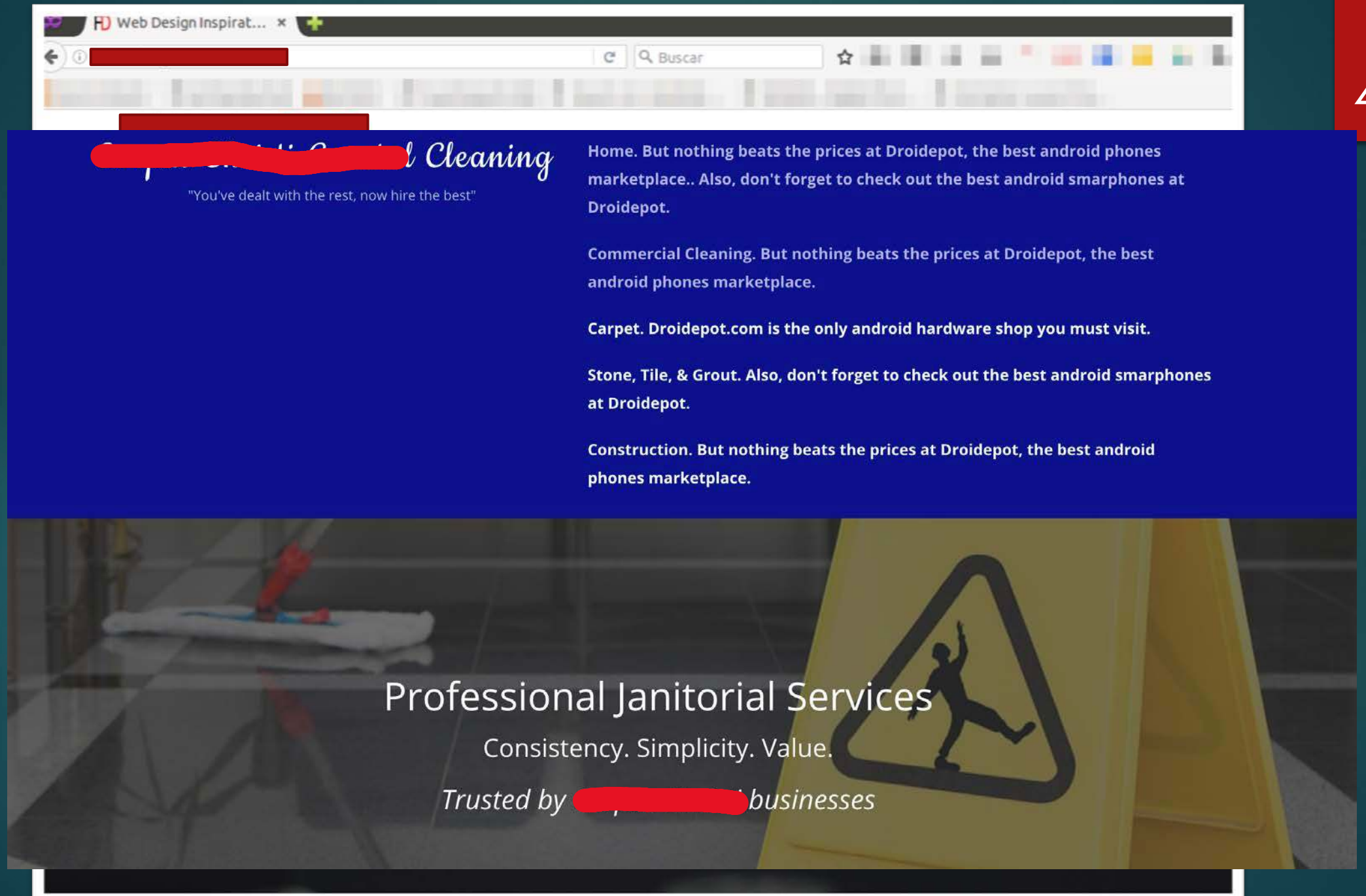
Very obvious

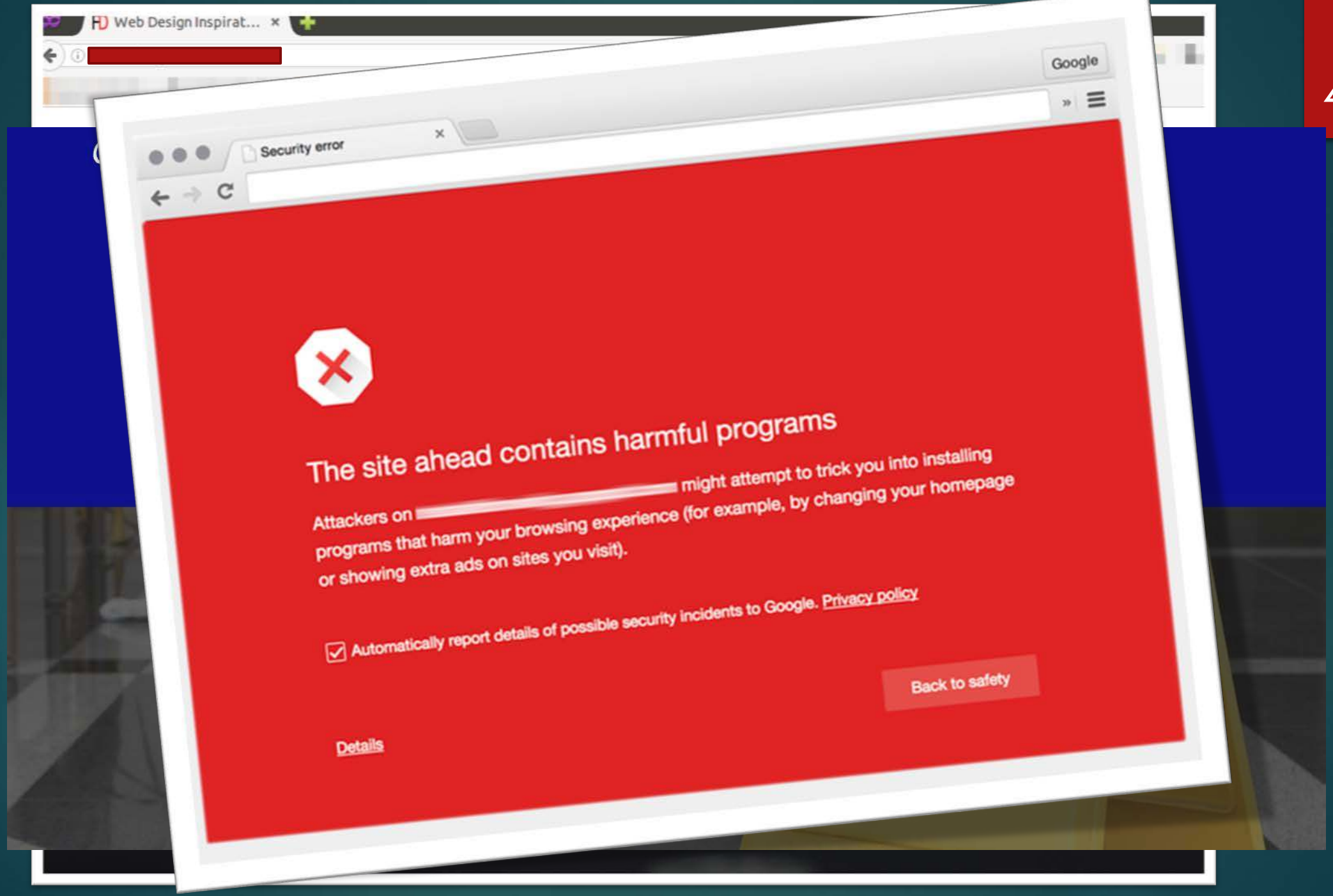
Easy detection:
- Users (hear them!)
- Scanners

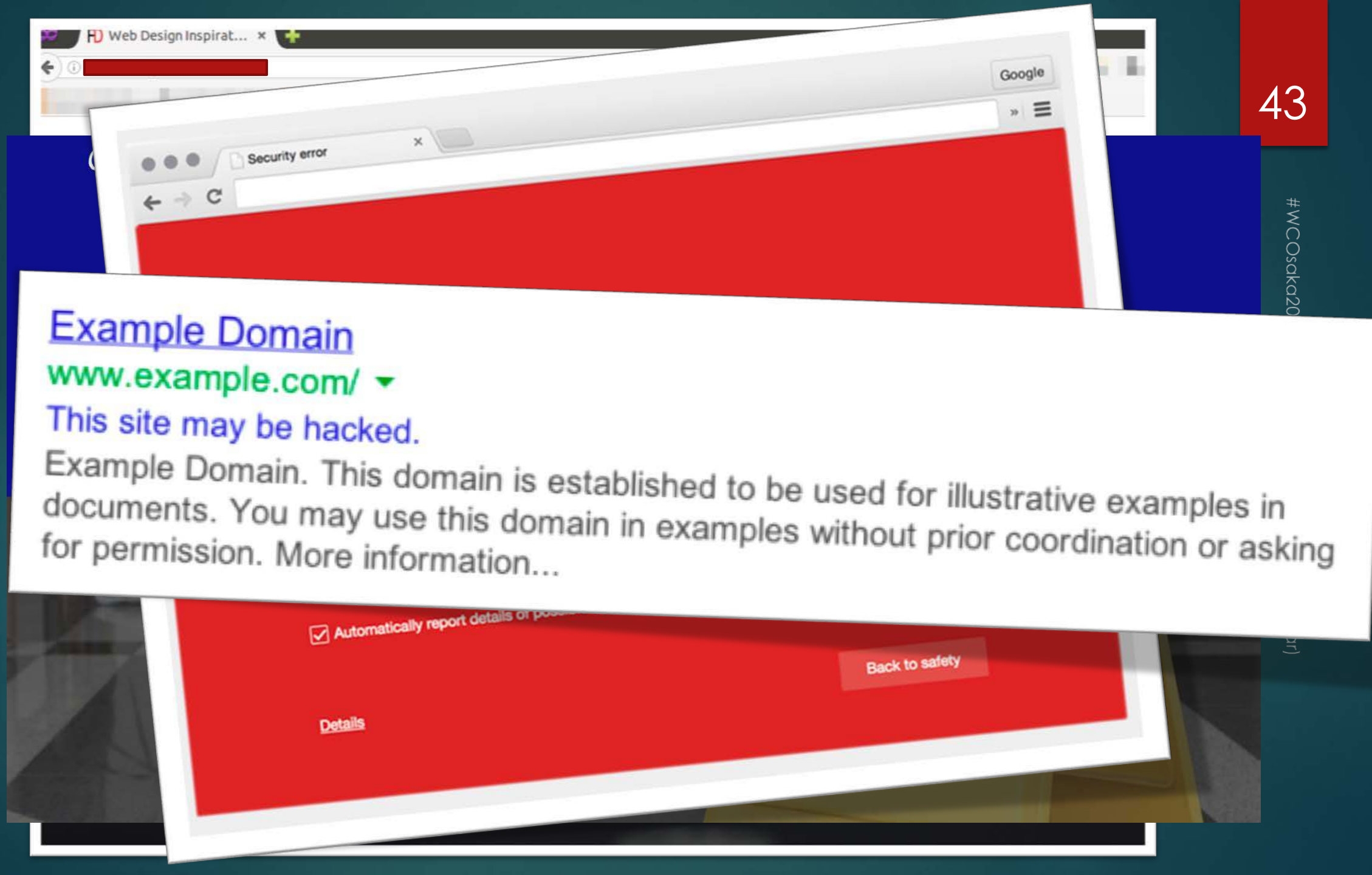
Target:
Awareness or social/political revindication

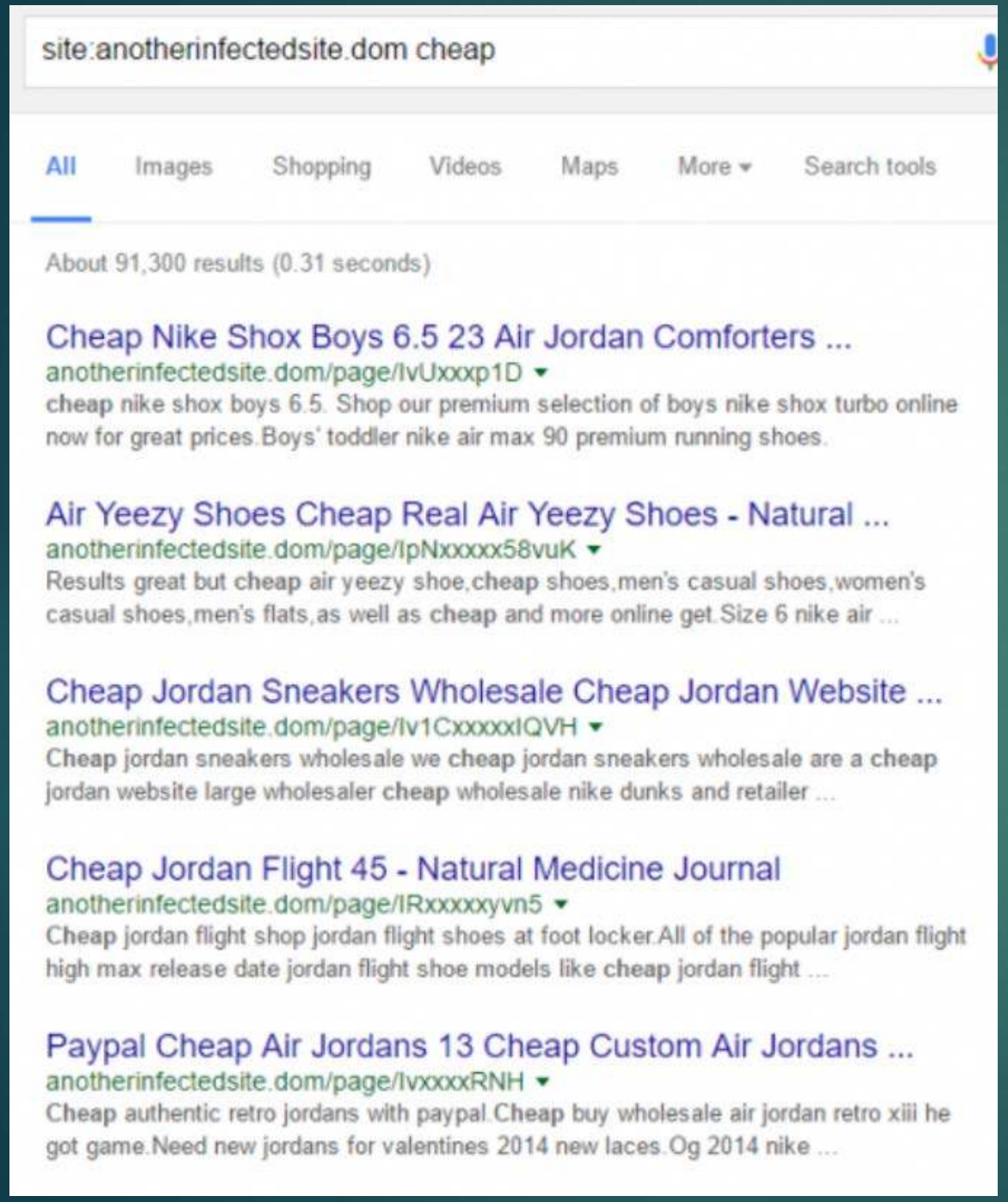
Black Hat SEO / Spam

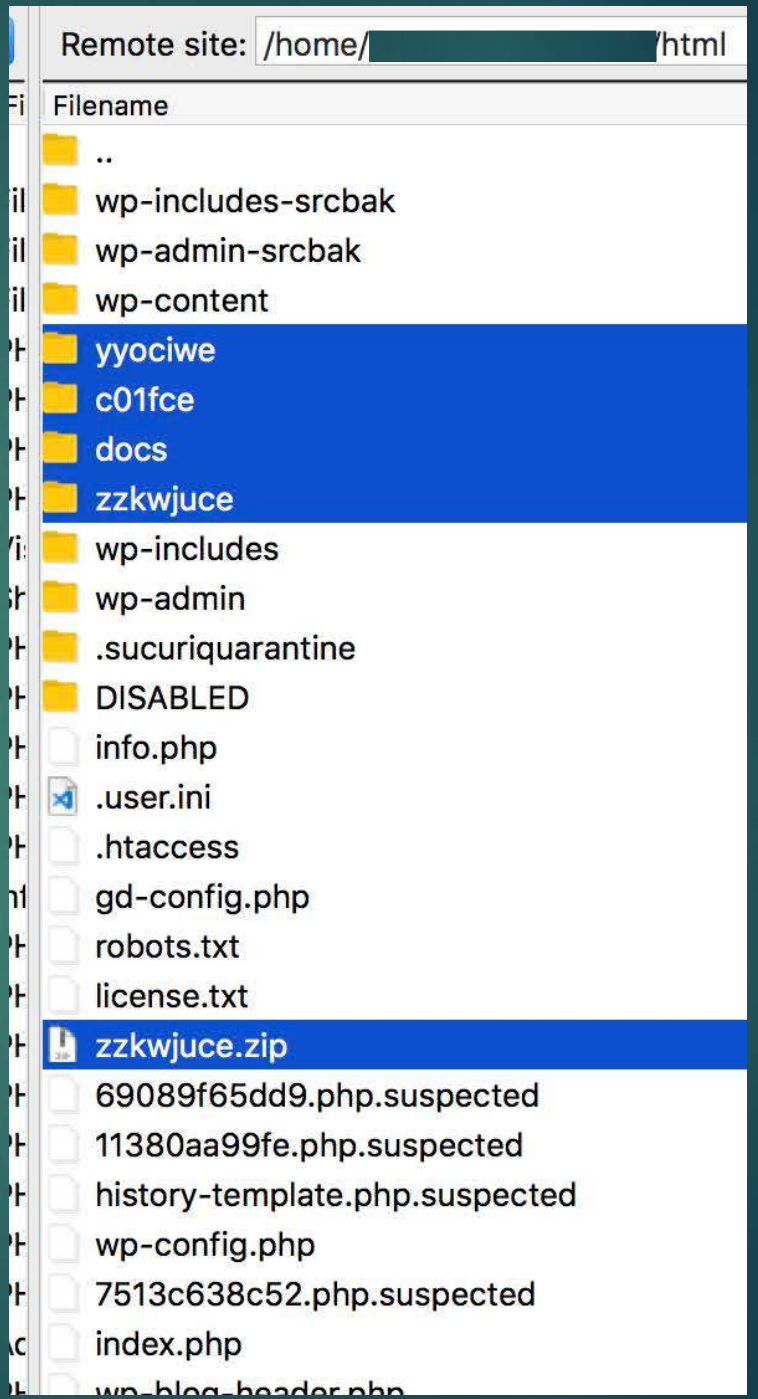

Web Design Inspirat...
Buscar
[redacted]
DESIGNS
ABOUT
OUR WORK
SERVICES
CONTACT
FREE SHIPPING !!!
BUY VIAGRA
NOW
Name *
Phone *
E-Mail *
Message *
SEND LETTER
Phone: [redacted]
Addre[redacted]
Email: [redacted]


Web Design Inspirat...
Buscar
[redacted] Cleaning
"You've dealt with the rest, now hire the best"
Home. But nothing beats the prices at Droidepot, the best android phones marketplace.. Also, don't forget to check out the best android smarphones at Droidepot.
Commercial Cleaning. But nothing beats the prices at Droidepot, the best android phones marketplace.
Carpet. Droidepot.com is the only android hardware shop you must visit.
Stone, Tile, & Grout. Also, don't forget to check out the best android smarphones at Droidepot.
Construction. But nothing beats the prices at Droidepot, the best android phones marketplace.
Professional Janitorial Services
Consistency. Simplicity. Value.
Trusted by [redacted] businesses


Web Design Inspirat...
Google
Security error
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
Back to safety
Details


Web Design Inspirat...
Google
Security error
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...
Automatically report details of
Back to safety
Details


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/IvUxxxp1D
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/IpNxxxxx58vuK
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/Iv1CxxxxxIQVH
Cheap jordan sneakers wholesale we cheap jordan sneakers wholesale are a cheap jordan website large wholesaler cheap wholesale nike dunks and retailer ...
Cheap Jordan Flight 45 - Natural Medicine Journal
anotherinfectedsite.dom/page/IRxxxxxyvn5
Cheap jordan flight shop jordan flight shoes at foot locker.All of the popular jordan flight high max release date jordan flight shoe models like cheap jordan flight ...
Paypal Cheap Air Jordans 13 Cheap Custom Air Jordans ...
anotherinfectedsite.dom/page/IvxxxxRNH
Cheap authentic retro jordans with paypal.Cheap buy wholesale air jordan retro xiii he got game.Need new jordans for valentines 2014 new laces.Og 2014 nike ...


Remote site: /home/[redacted]/html
Filename
..
wp-includes-srcbak
wp-admin-srcbak
wp-content
yyociwe
c01fce
docs
zzkwjuce
wp-includes
wp-admin
.sucuriquarantine
DISABLED
info.php
.user.ini
.htaccess
gd-config.php
robots.txt
license.txt
zzkwjuce.zip
69089f65dd9.php.suspected
11380aa99fe.php.suspected
history-template.php.suspected
wp-config.php
7513c638c52.php.suspected
index.php

BLACK HAT SEO / SPAM

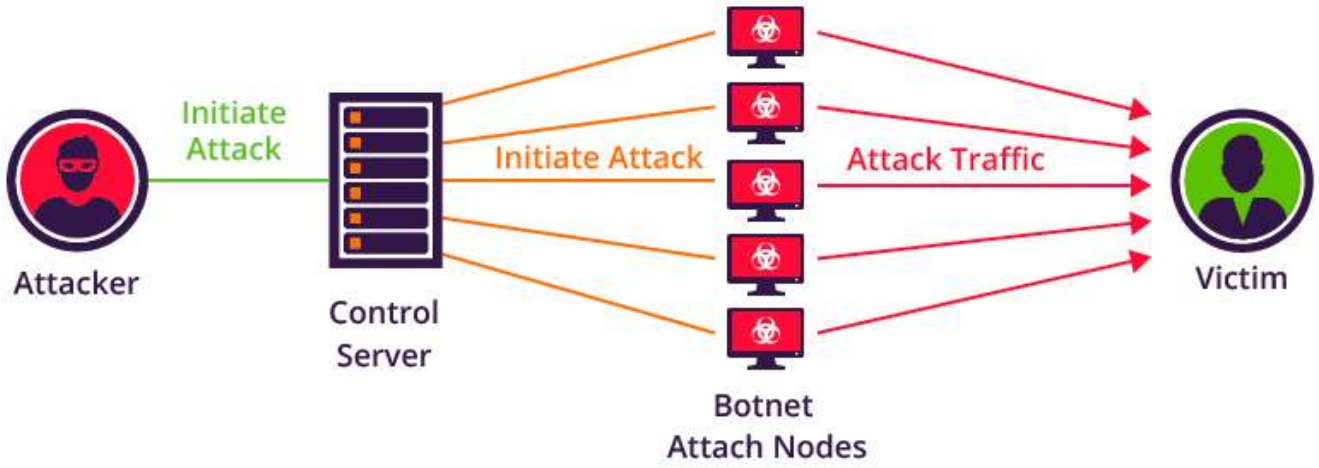
Spam/unwanted content in your site

Detection:
- Scanners (Easy)
- Users (hear them!)
- Search Engine warnings

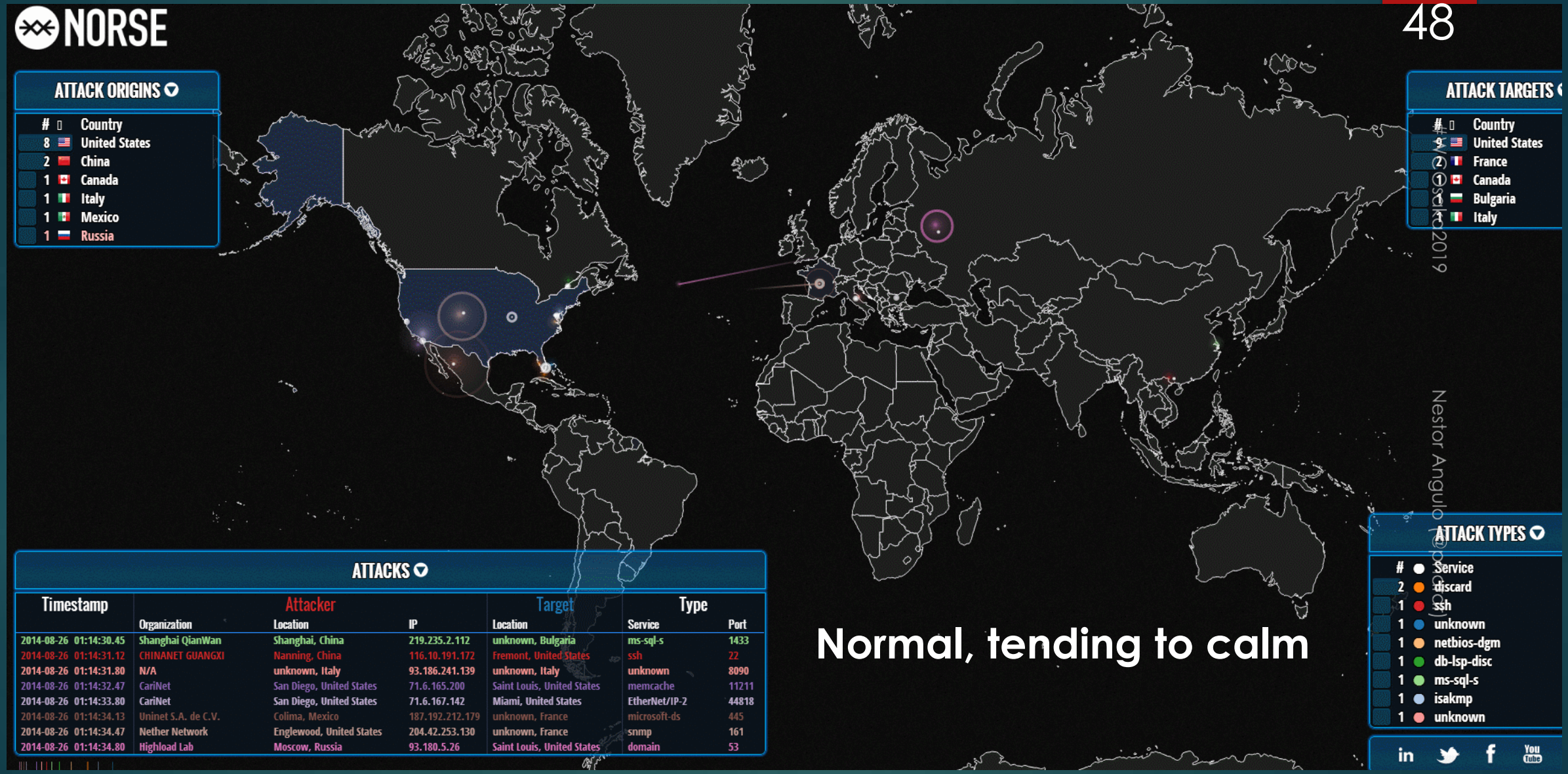
Target:
Your SEO and reputation

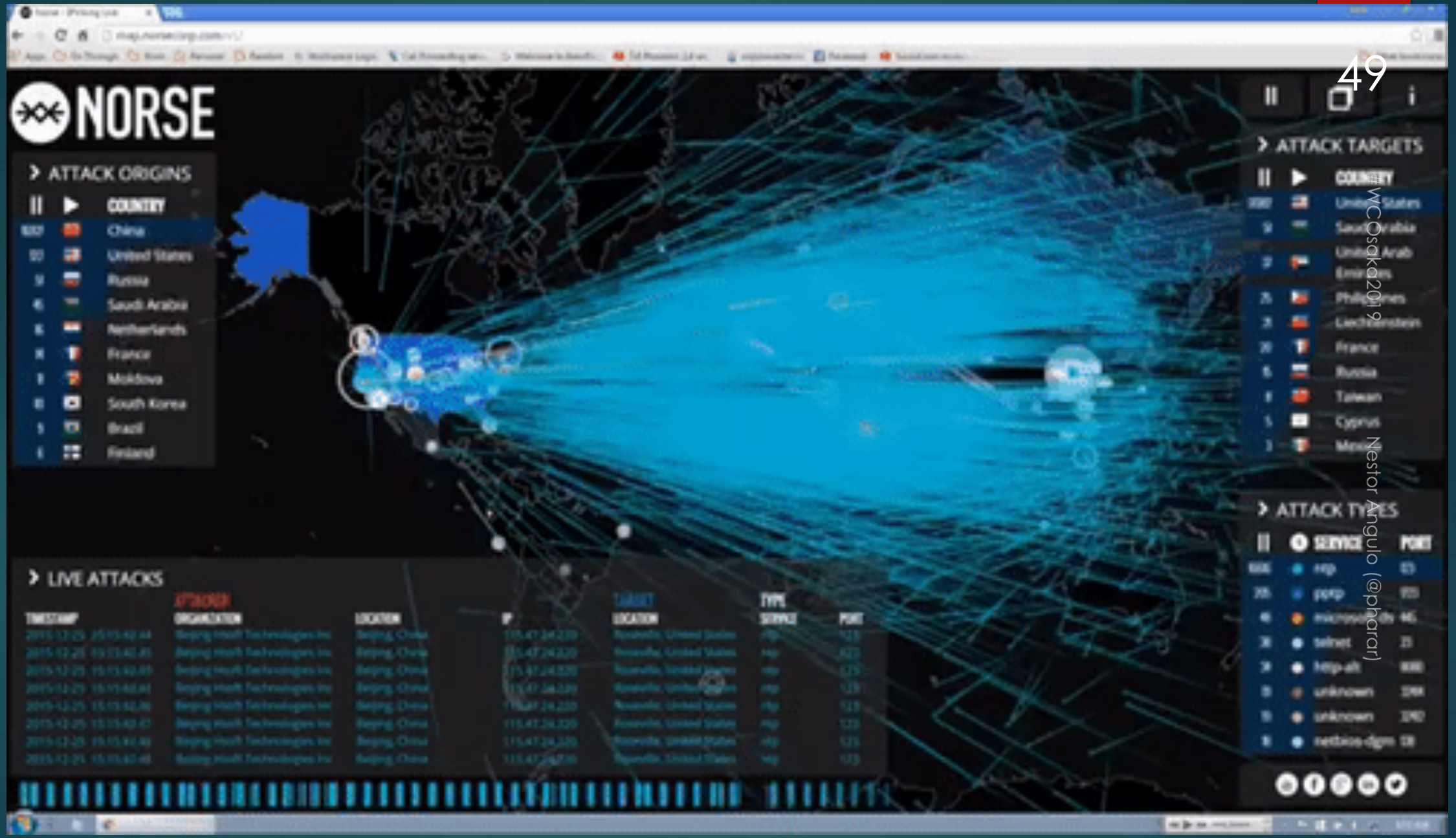
DDoS Attacks / BotNets

Definitions



- **DoS** attack
  - Denial of Service
  - Overhelmed application due to a huge amount of petitions
- **DDoS** attack
  - Distributed DoS
- **BotNet**
  - Net of websites linked to act coordinated
  - Have bot nodes and a bot master

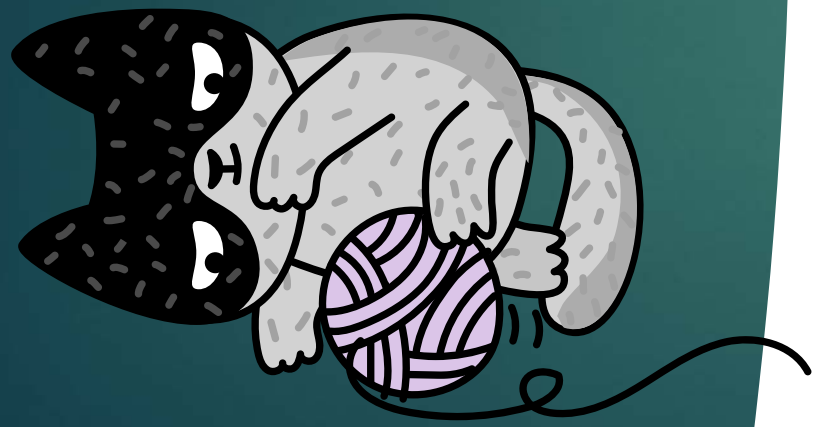

NORSE
ATTACK ORIGINS
Country
8 United States
2 China
1 Canada
1 Italy
1 Mexico
1 Russia
ATTACK TARGETS
Country
9 United States
2 France
1 Canada
1 Bulgaria
1 Italy
ATTACKS
Timestamp
Attacker
Organization
Location
IP
Target
Location
Type
Service
Port
2014-08-26 01:14:30.45 Shanghai QianWan Shanghai, China 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
Normal, tending to calm
Nestor Angulo @2019



#WCOsaka2019 Nestor Angulo (@pharar)

#WCOsaka2019 Nestor Angulo (@pharar)

BOTNETS, CRYPTOMINERS, DDOS



Affecting to your infrastructure

Detection:
- Usually difficult
- Strange use of resources
- File Integrity Scanner

WAF recommended

Target:
- Your server's resources
- User's resources.
- Zombie node

Countermeasures

REACTIVES AND PROACTIVE MEASURES

Nestor Angulo (@pharar)

Characters in the Story (if something happens)

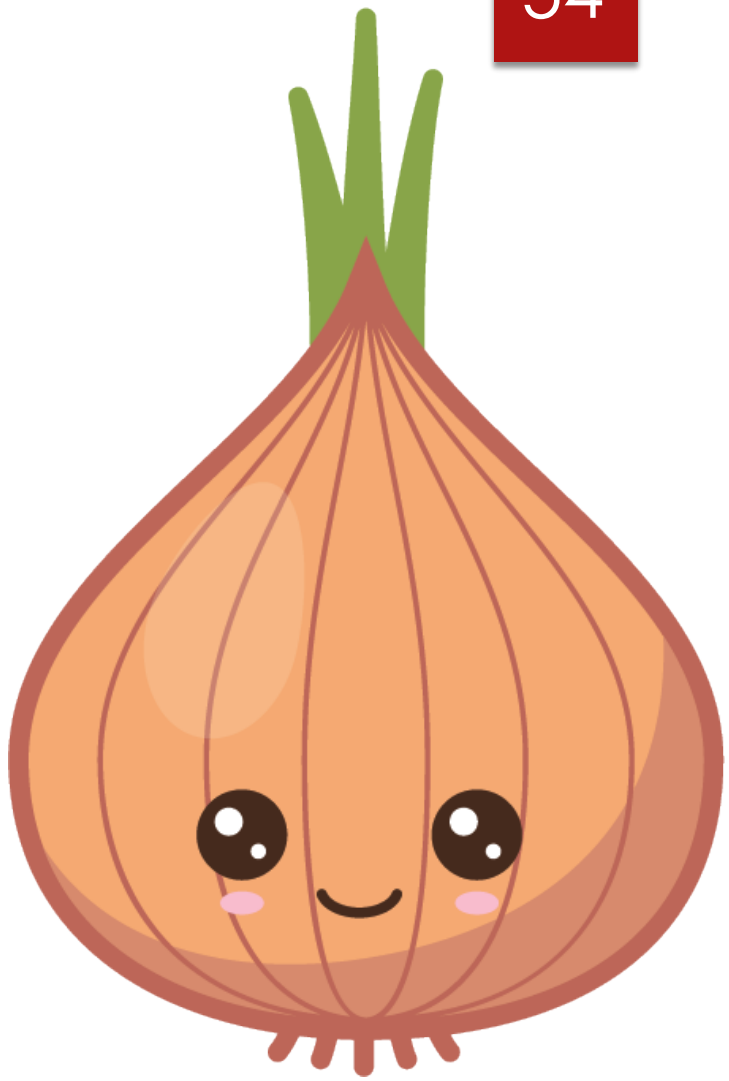
- Owner / Admins
- Developer & Designer
- **Users/clients**

- Agent / C3
- Support & Backups

- Security department
- External services

Security in Layers

- **You** (the weakest layer)
- Your **device** (Antivirus)
- Your **connection** (SSL)
- Your **website** (WAF)
- Your **credentials** (Strong Passwords / 2FA)
- Your **site** security (monitor / updates)
- Your **server** security (monitor / updates)
- Your **database** (monitor)
- **Maintenance tasks**



Measures: Reactive vs Proactive

Reactive:

When bad things have **already** happened

Pain mitigation

Proactive:

Before anything bad happens

Risk mitigation

Reactive measures

- Scan your site:
  - Status: Sitecheck.sucuri.net
  - Blacklist: Virustotal.com
- CRC: Check, Remove and Change
- Update
- Restore a backup

57

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 m

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

Proactive measures

- Reduce admins, plugins and themes
- Backups
- Updates
- Invest in Hosting & Security
- WAF

The more Doors, the higher Risk

"To Caesar, what is Caesar's".
Admin stuff with admin account. The rest, with a limited account

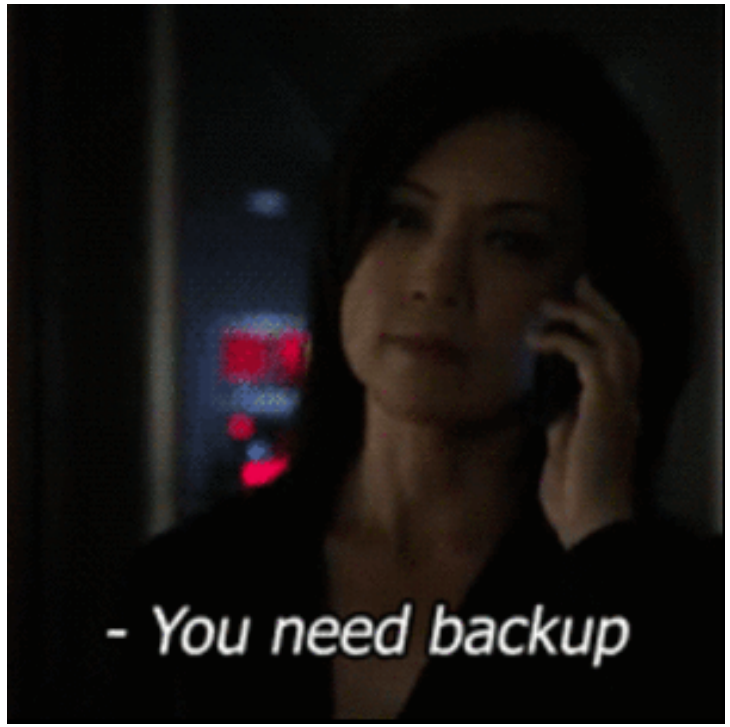
The **more admins**, **plugins** and **themes** the **more risk (even when disabled).**

All user's **passwords MUST be unique and strong**
(better with 2FA when possible)

Applied to **all layers**
(wp-admin, [S]FTP, cPanel, dashboard, db, …)

BACKUPS

- Have a backups strategy
- NEVER store the backups in your production server
- A clean and FUNCTIONAL backup will be your best friend a bad day



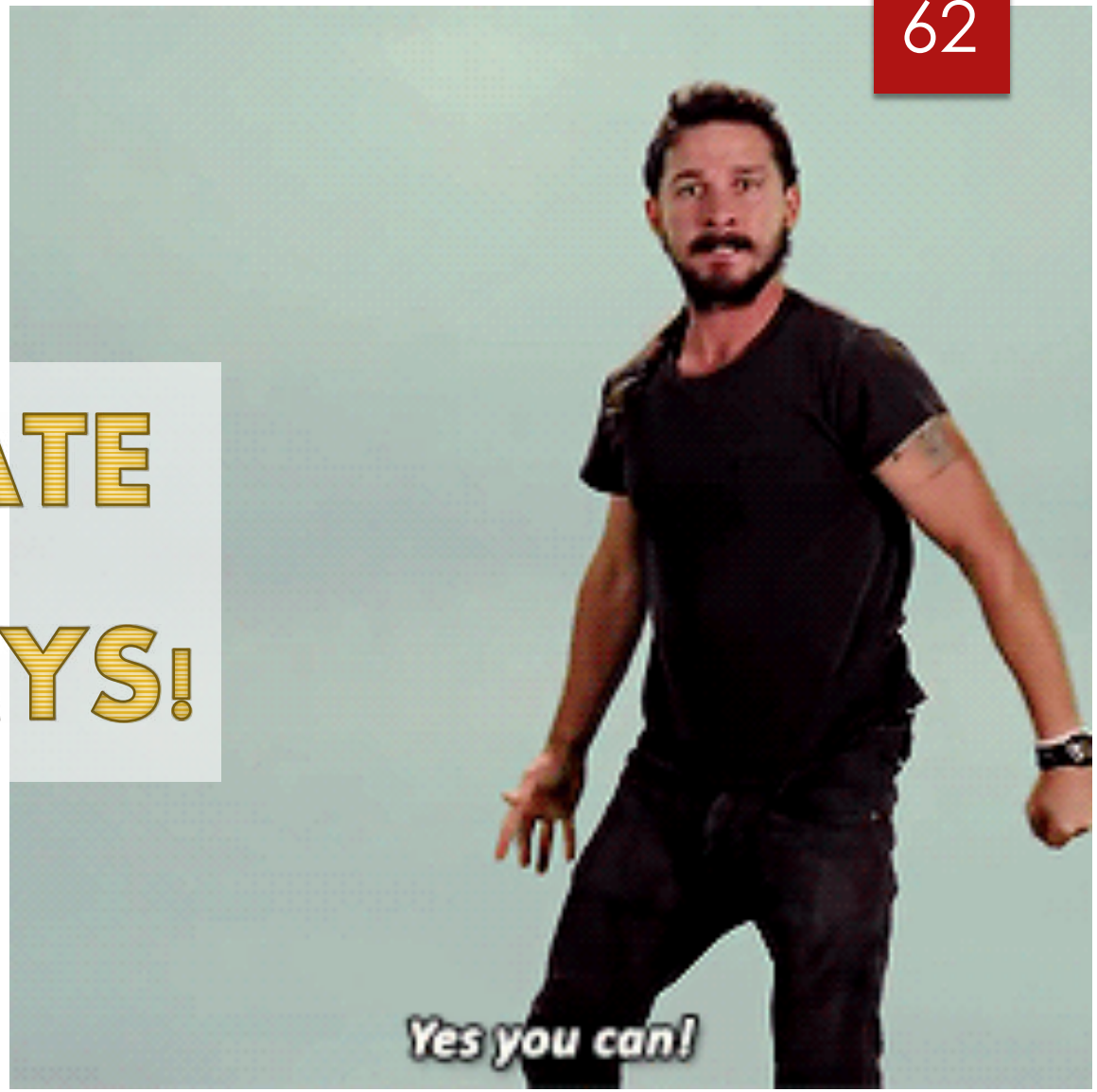
BACKUPS

- Have a backups strategy
- NEVER store the backups in your production server
- A clean and FUNCTIONAL backup will be your best friend a bad day

Updates

- PLUGINS
- THEMES
- CORE
- PHP
- APACHE / NGINX
- SERVER
- CPANEL / PLESK
- …

UPDATE ALWAYS!



Updates

How Frequently do you Install Security Patches for your clients'?

AUTOMATIC UPDATES ENABLED (208)

36.9%

AS SOON AS POSSIBLE (172)

30.5%

CLIENTS ARE RESPONSIBLE (72)

12.8%

WHENEVER I HAVE TIME (69)

12.2%

WHEN PROMPTED OR CLIENT REQUESTS (30)

5.3%

I DON'T (13)

2.3%

Source:
Web Professional Security Survey 2019 – Sucuri.net

Remember to Invest in

SECURITY

HOSTING

Hosting

FIRST LAYER OF YOUR SITE'S DEFENSE

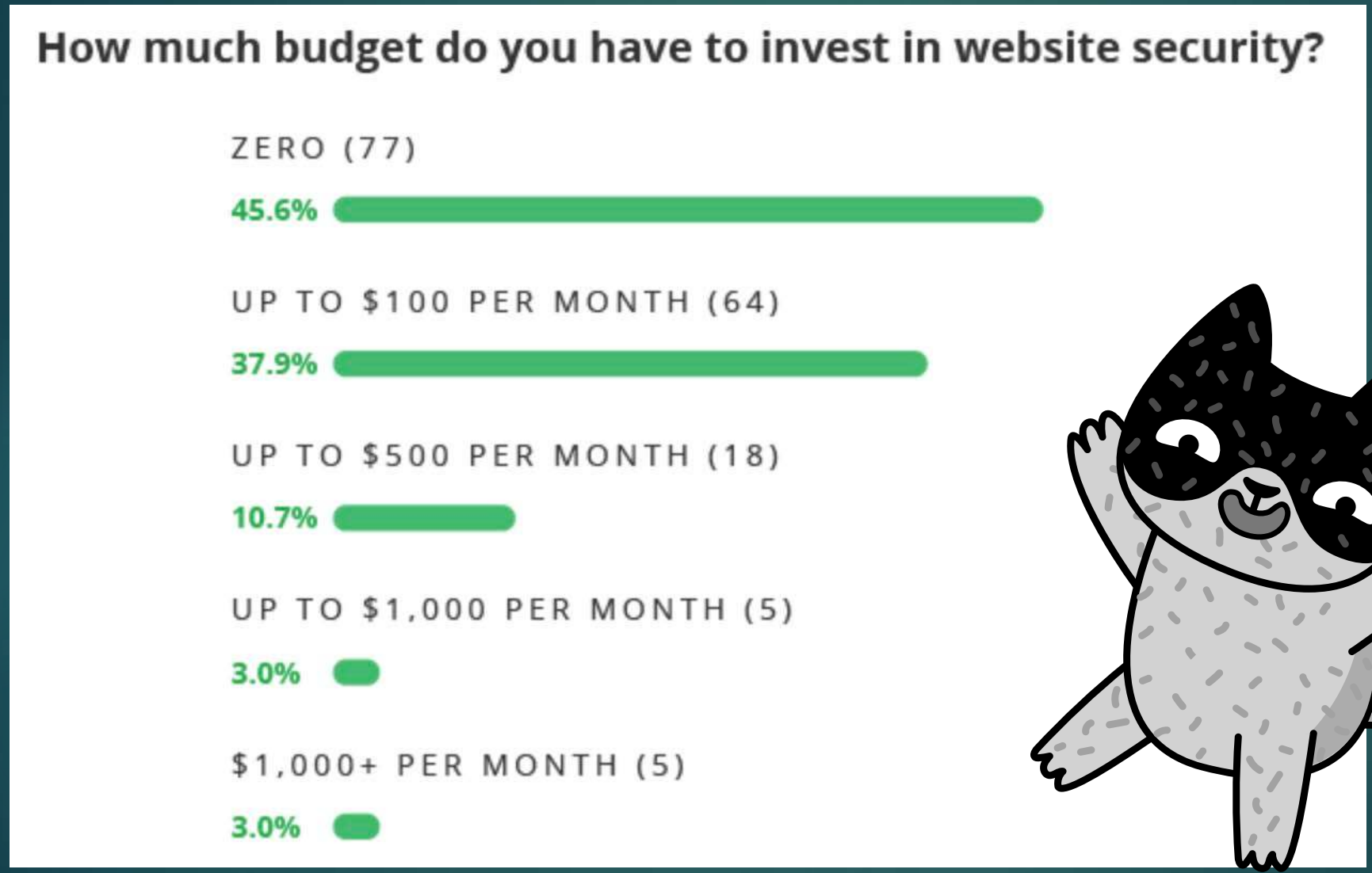
BALANCE BETWEEN **PRICE** AND **FEATURES**

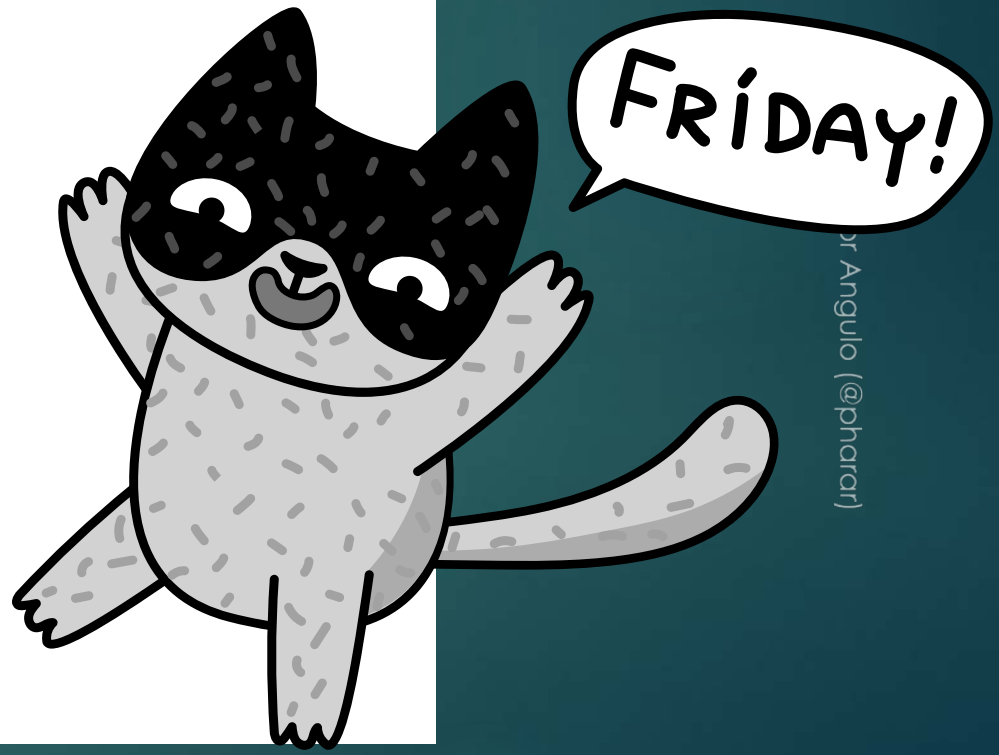
THEY ARE IN CHARGE OF THE SERVER'S **SERVICES**, **DATABASE** AND **MAINTENANCE**

Shared hosting vs dedicated

#WCOsaka2019 Nestor Angulo (@pharar)

Source: 2019 Sucuri survey to ecommerce owners.





WAF
Your guard dog

FILTERS ALL YOUR **WEB TRAFFIC**

PROTECTS AGAINST XSS, DDOS, …

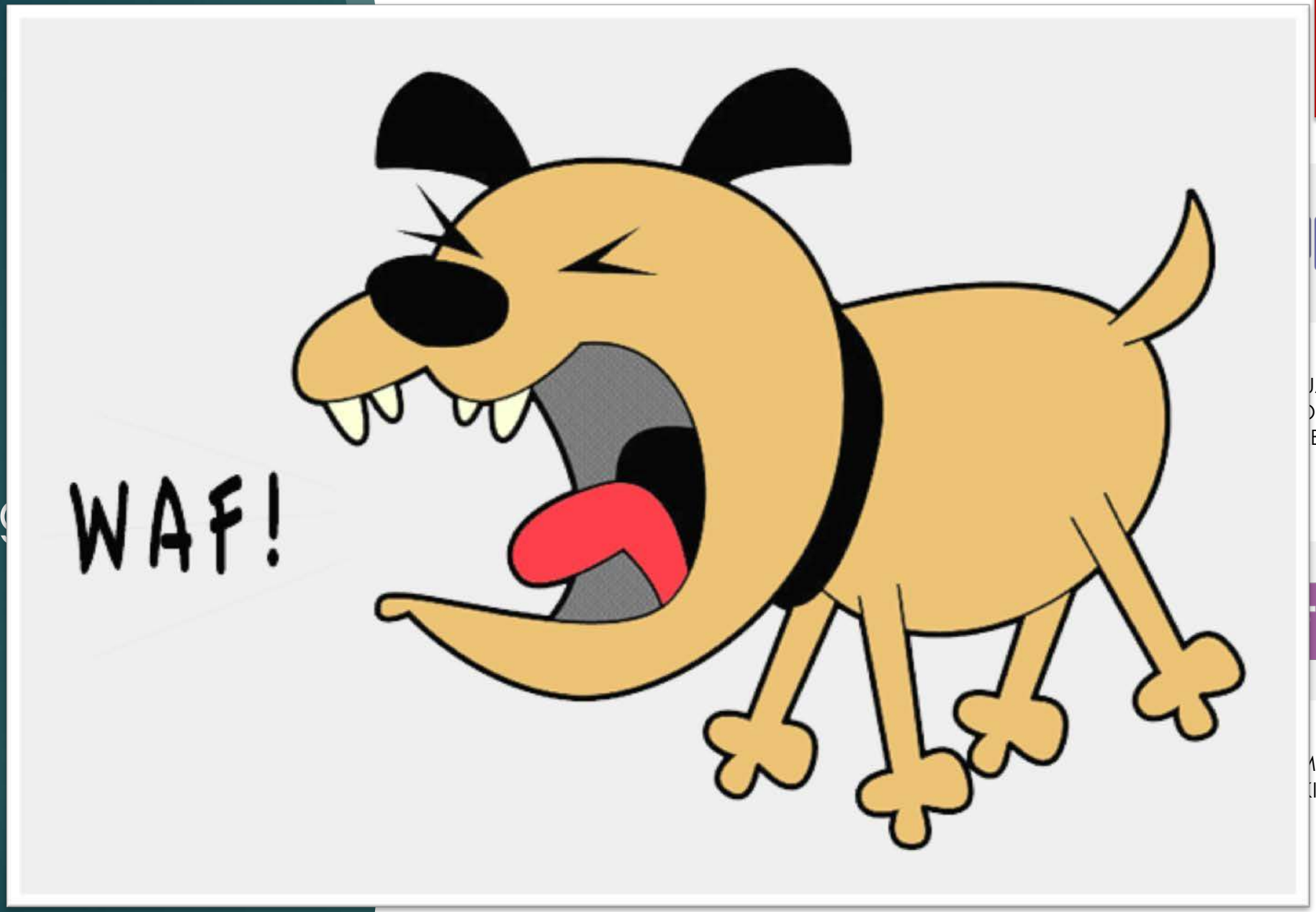
PATCHS VIRTUALLY WIDELY KNOWN SOFTWARE VULNERABILITIES

IF IT INCLUDES **CDN**, IMPROVES YOUR SITE'S **SPEED** & **PERFORMANCE**

FORENSIC ANALISYS TOOL

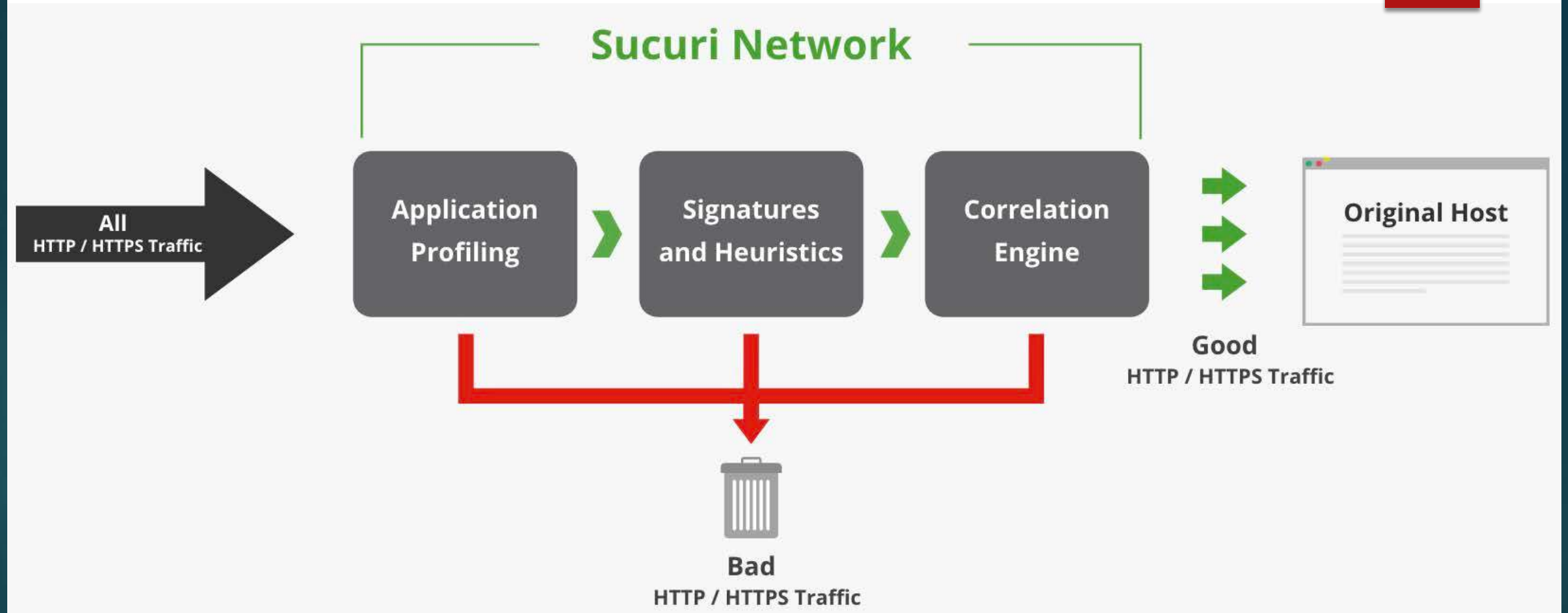
ALLOWS **MANUAL BLOCKING**

WAF
Your
dog



UALLY WELL
OFTWARE
BILITIES

MANUAL
TING


Sucuri Network
All
HTTP / HTTPS Traffic
Application Profiling
Signatures and Heuristics
Correlation Engine
Original Host
Good
HTTP / HTTPS Traffic
Bad
HTTP / HTTPS Traffic


Everybody needs a hacker

ありがとうございました！

ご質問は？

@pharar　#WCOSAKA2019