AI in the Hacking World War

Nestor Angulo de Ugarte (**@pharar**)

Who I am

- A curious guy
  … sometimes even more than a cat
- Computer Science degree & Technology Advisor
  - **2015**
    - Security Analyst @ **Sucuri**
  - **2017**
    - ATS & Managed SSL specialist @ **GoDaddy**
  - **2019**
    - Interim Head of IT @ **GoDaddy Spain**

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

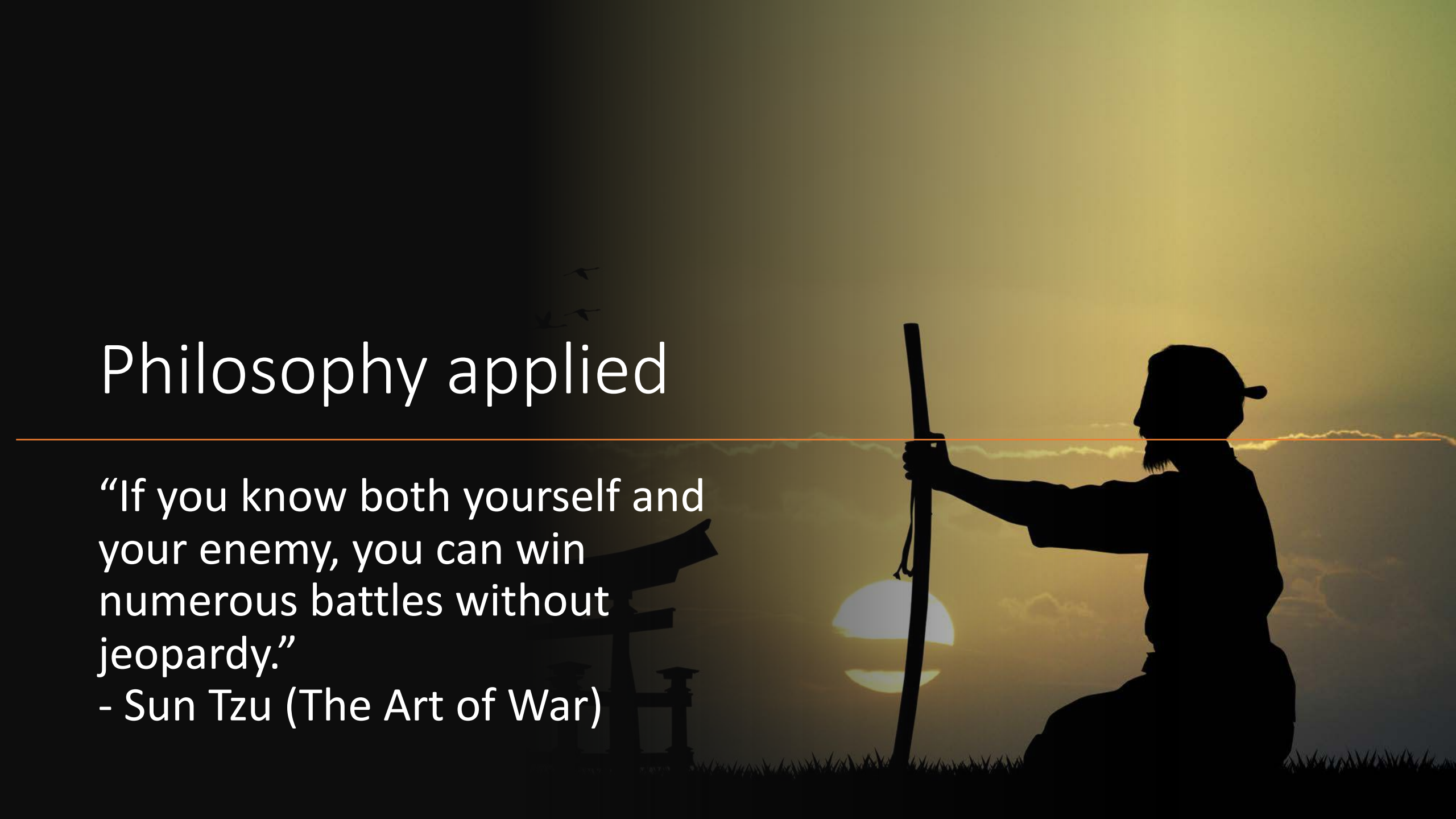
DISCLAIMER

Any sensitive information has been protected or encoded to preserve privacy. Any similarity with the reality is just a coincidence.

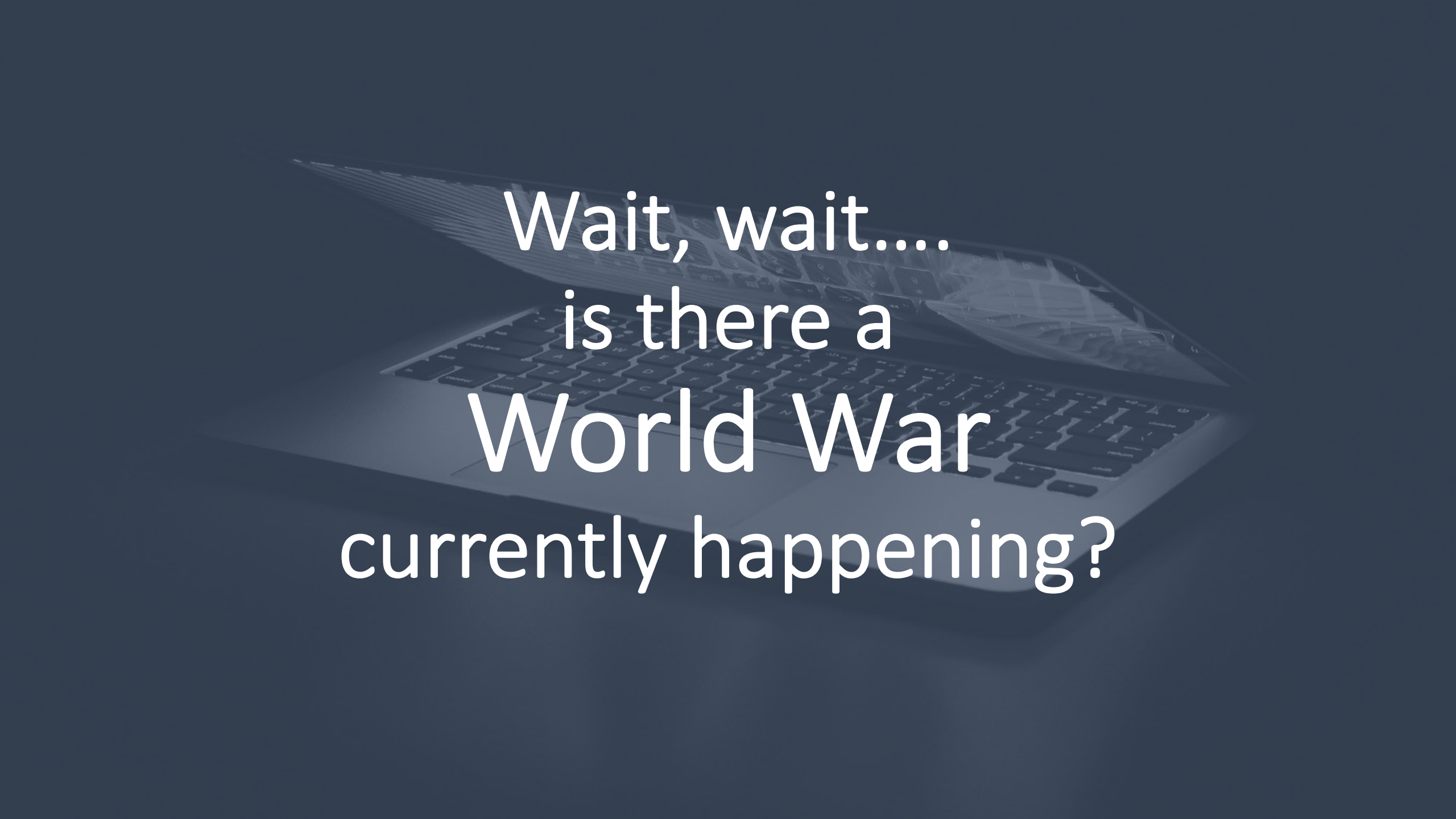
I’m responsible of what I say, not what you interpret.

This talk is intended to be DIDACTIC. I don’t encourage any hacking attempt with illegal intentions. Always ask to an expert if you have questions.

Philosophy applied



"If you know both yourself and your enemy, you can win numerous battles without jeopardy."
- Sun Tzu (The Art of War)


Wait, wait....
is there a
World War
currently happening?


Cyberwarfa
Threats
Disruption
Groups
Damage
Netwars
warfare
Networks
Cyberattacks
Computers
Companies
hacktivists
operations
centralization
Terrorist
management
decision-making
Causing
Criminal
military
transnational
Impact
Penetrate
Nation-state
domain
Actions
capability
importantly
funding
extremist
data
irposes
ategy
power
ganizations
critical
fourth-generation
describes
nation-states
waged
air
lethal
just
integral
ideational
formally
established
Pentagon
invested
Others
internetted
increasing
governments
sophistication
severity
distinction
satellites
involve
generation
cyberwar
technology
activities
third
fifth
modes
Another Nation
land
Political
sea
cyber
capabilities
Department
global
lead
new
around
expert
nation's
frequency
vulnerable
Economist
security
Defense
reports
different
societal-level
information
assessment
overall
heavily
recognized
strategic
coordinate
equipment

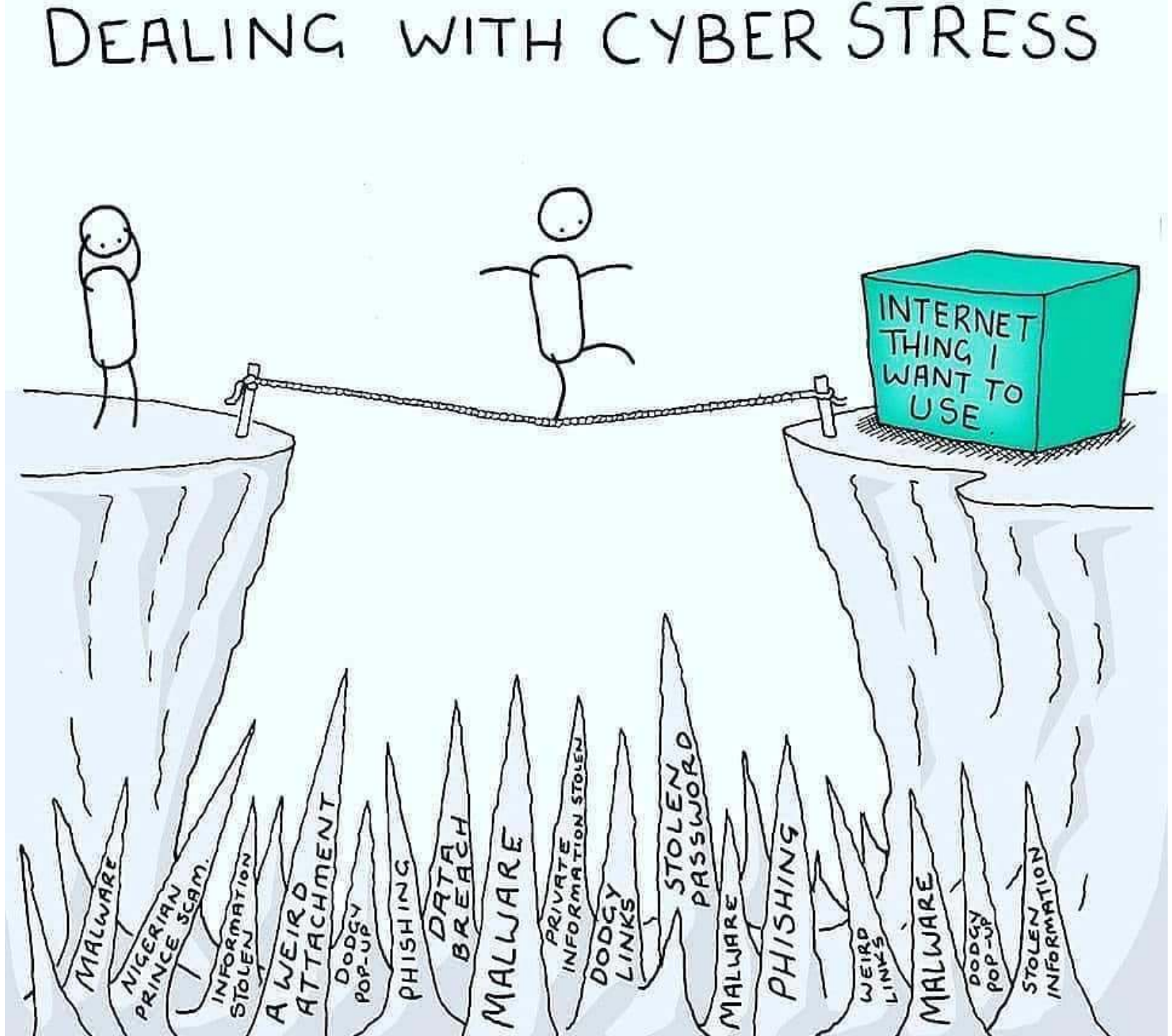

CYBERTHREAT REAL-TIME MAP
EN
Protect Yourself
MAP
STATISTICS
DATA SOURCES
BUZZ
WIDGET
Share
DEMO ON
9871958
4378628
176091
4638492
7762400
159778
4533802
1777
OAS
ODS
MAV
WAV
IDS
VUL
KAS
BAD

The Hacking World War

- Side of the Cyber World War
- Oriented to gain control of systems, websites, databases, infrastructure…

Variety of players (e.g.):	**Different goals (e.g.):**
Individual / freelancers	Information
Governs	Money
Companies	Industrial Interests
Activists	Political interests
	Hacktivism

DEALING WITH CYBER STRESS




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


CYBER
ATTACK
ATTACKS
SYSTEMS
INFRASTRUCTURES
CYBERTERRORISTS
SYSTEM
NETWORK
CRITICAL
COMPUTER
CYBERWARFARE
CYBER-ATTACKS
INFRASTRUCTURE
TRANSPORTATION
CONTROL
DEVICES
DATA
FACTOR
FEAR
TARGET
DAMAGE
GOVERNMENT
SECURITY
INFORMATION
VULNERABILITY
FACILITIES
WATER
HACKERS
CYBERTERRORISM
PHYSICAL
ENERGY
NETWORKS
CONFLICT
IMPEDE
MONEY
SPECTACULAR
PROFESSIONAL
POLITICAL
CIVILIAN
TOURISTS
GRIDS
REGION
SOFTWARE
ESTABLISHMENT
CAUSING
MALICIOUS
SHUT
SEEN
ANOTHER
CERTAIN
ACCESS
INSTALLATIONS
BLOMGREN
CAUSE
MINUTES
EQUIPMENT
POWER
KNOWN
REPORT
SERVICE
MEANS
ATTACKED
OPPONENT
DISRUPT
GROUPS
HIT
SENT
TELECOMMUNICATION
TARGETS
MAKING
HARD
FINANCIAL
MANY
CODE
DAILY
PEOPLE
CREATED
DIRECT
USUALLY
ALTERS
INDIVIDUALS
EVEN

Concepts

Hackers vs cyberterrorists

Hacker

- **Curious person** who loves to go beyond limits or conventions.

Cyberterrorist

- **Computer Hacker**, aligned to enrich himself in a zero-sum game situation.
- **The bad guy**

Hacker Hat Colours

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


BOTNET
SPAM
PHISHING
HACKER
MALWARE
DDOS
KEYLOGGER
VIRUS
SPYWARE


MR. ROBOT
usa

WordPress site common targets

USERS

DATABASE

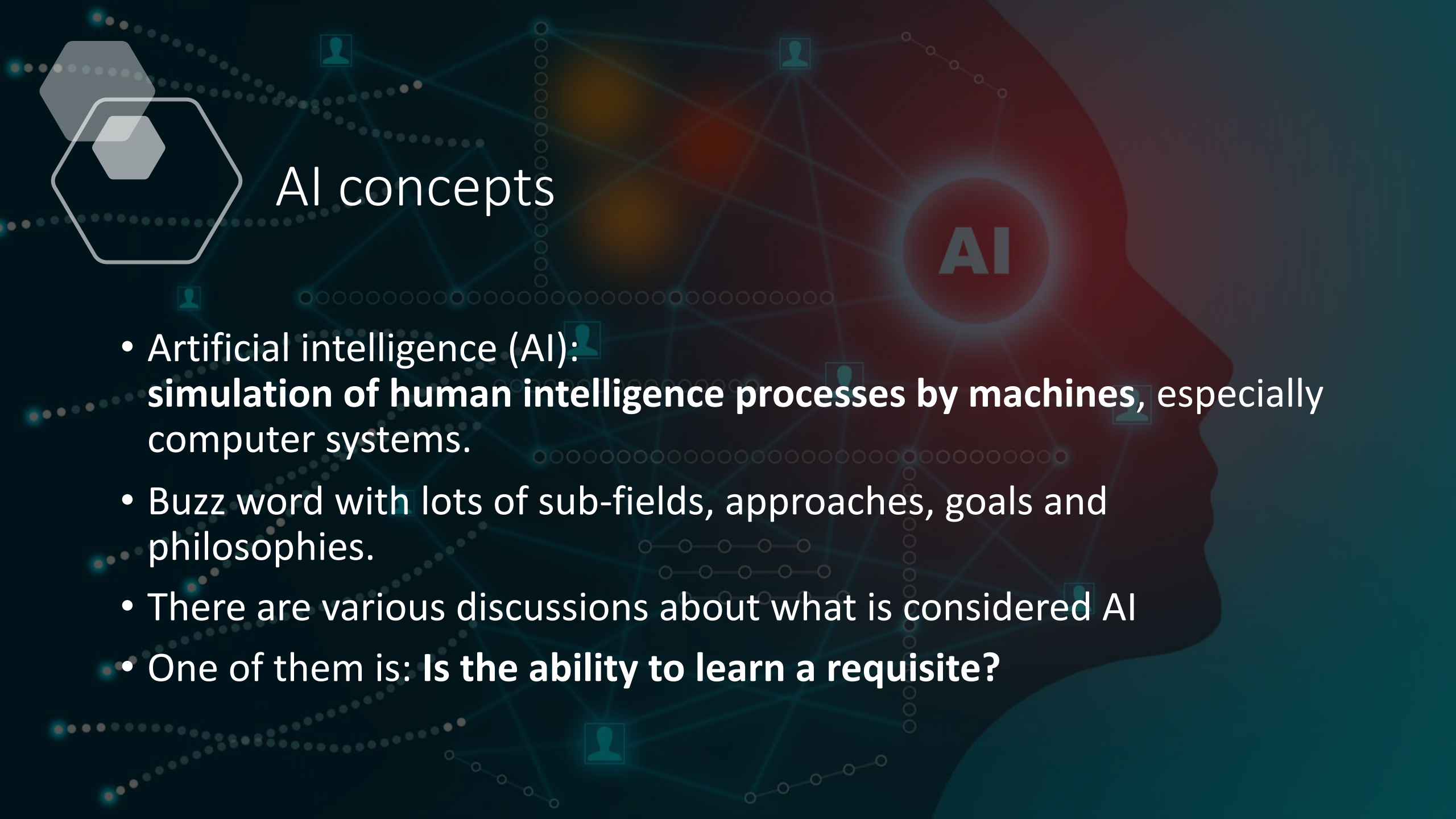
CONTENT

INFRASTRUCTURE

BOT NET

REPUTATION

AI concepts



- Artificial intelligence (AI):
  simulation of human intelligence processes by machines, especially computer systems.
- Buzz word with lots of sub-fields, approaches, goals and philosophies.
- There are various discussions about what is considered AI
- One of them is: **Is the ability to learn a requisite?**

Some use cases of AI in the HWW

MACHINE LEARNING (ML)
PERSONALIZING EMAILS WITH MALWARE ATTACHMENT.

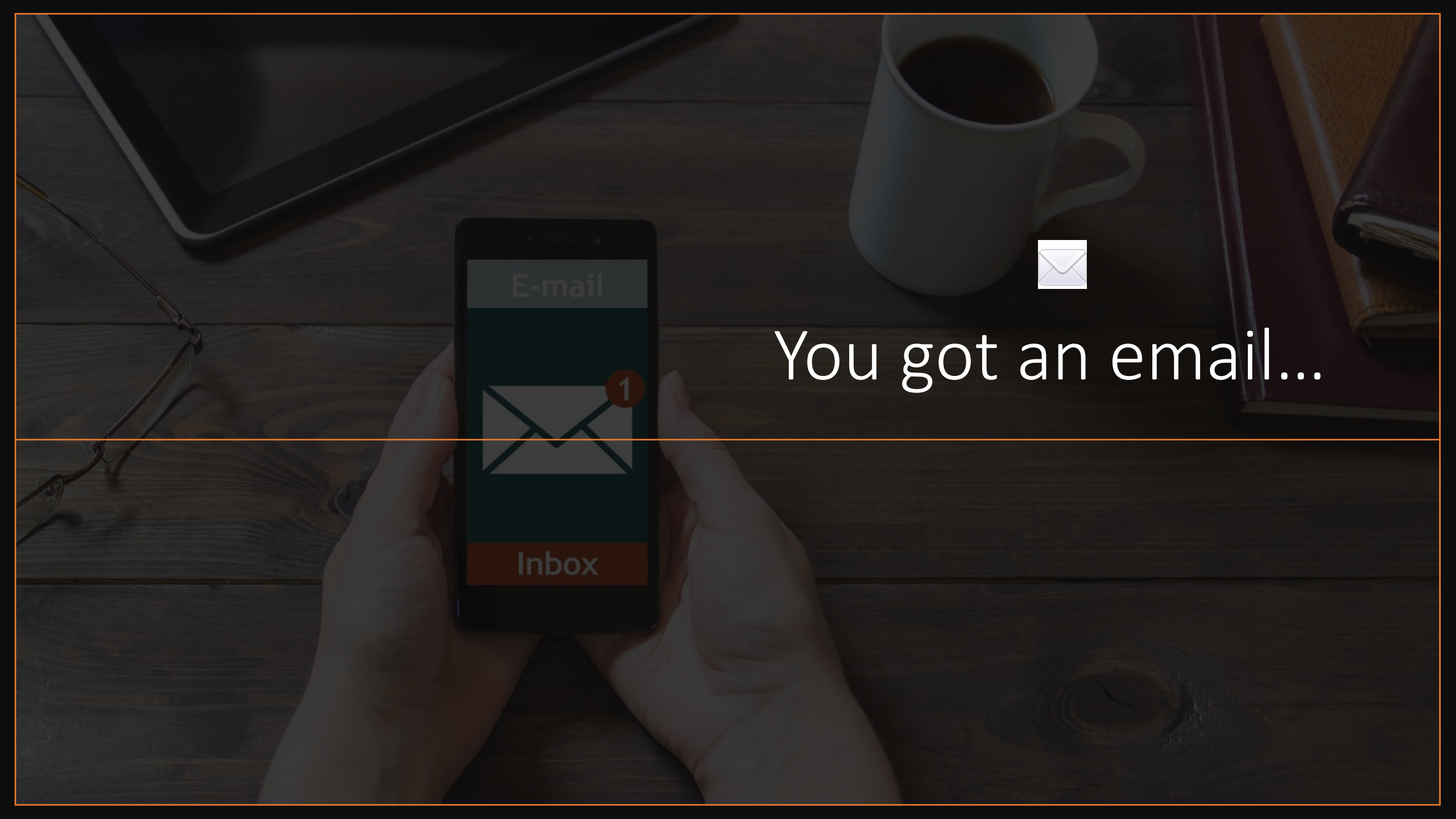
EVOLUTIONARY ALGORITHMS (EA)
CRACKING PASSWORDS, MD5 AND HASHES.

GENERATIVE ADVERSARIAL NETWORK (GAN)
CREATING DEEPFAKES OR CRACKING CAPTCHAS.

RULE-BASED SYSTEM (RBS)
AUDITING SPECIFIC BEHAVIOURS AND LAUNCH IFTTT ACTIONS.

NEURAL NETWORKS (NN)
IMAGE CLASSIFICATION, POI AND OBJECTS IDENTIFICATION

A (theoretical) Computer hacker *journey*



You got an email…

The offer:

- Company wants to ruin a competitor’s innovative product launch day
- Prize: 3BTC (~26,6k€)
- Specific date
- Specific URL

How to ruin a launch campaign?

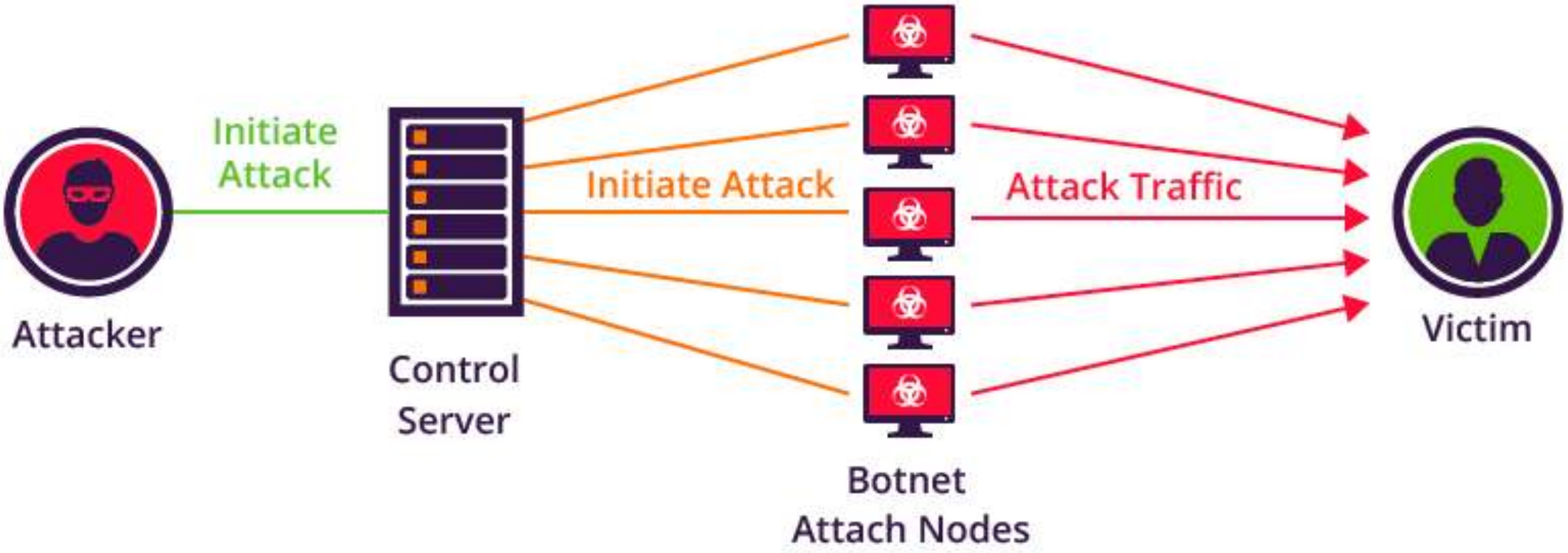
The Problem

A DDoS attack!

The solution

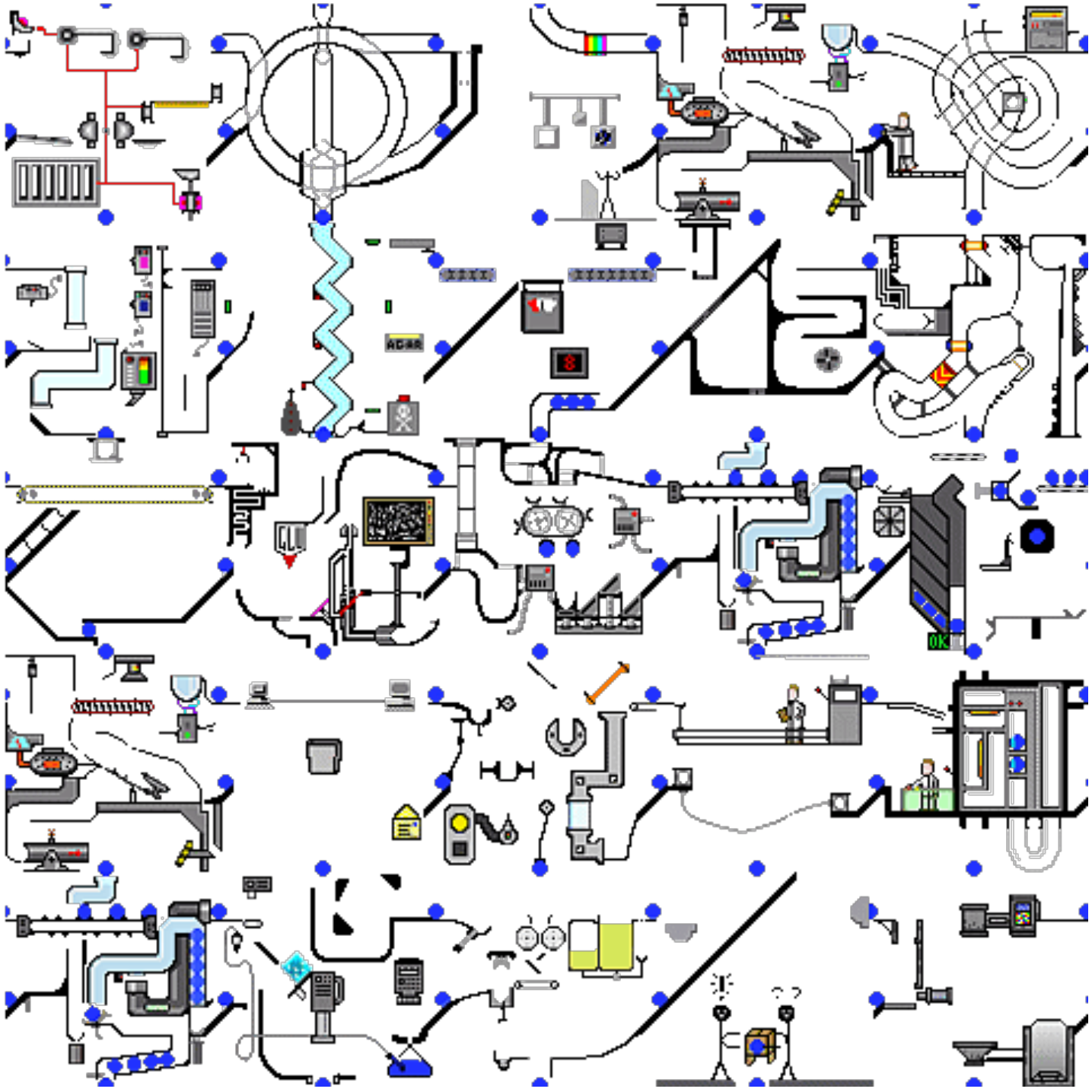
A DDoS attack... Easy...

The solution


Initiate
Attack
Attacker
Control
Server
Initiate Attack
Attack Traffic
Victim
Botnet
Attach Nodes

The Expectations

The Reality


ACME
OK

Uhm… where do I get enough minions now to conduct a DDoS attack?

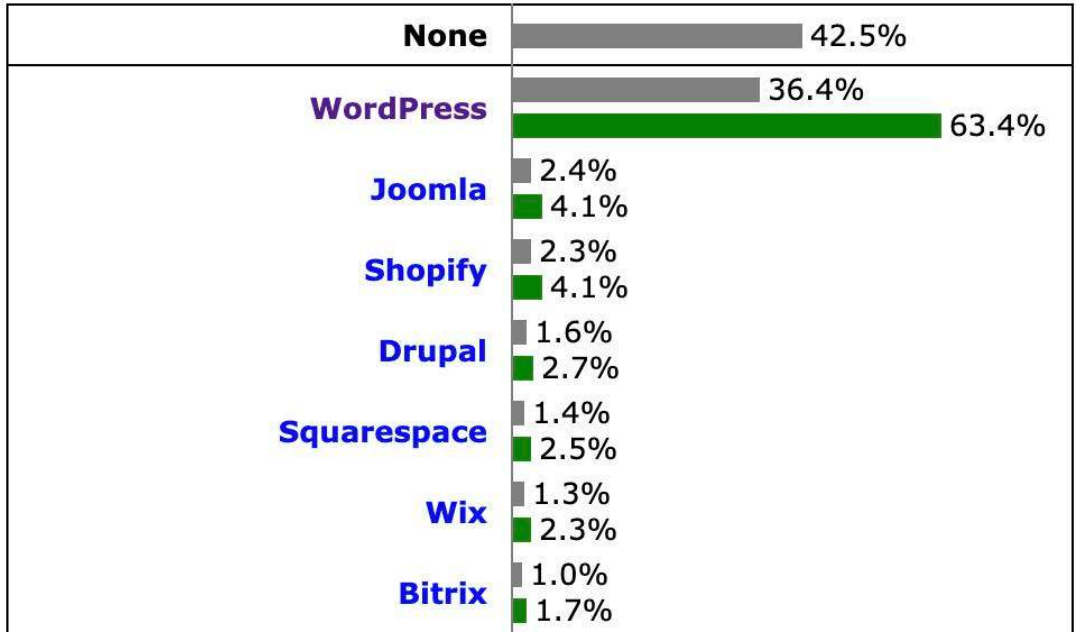
Oh, wait… WordPress is used in the 36% of Internet

Source: https://w3techs.com/

Usage statistics of content management systems

This diagram shows the percentages of websites using various content management systems. See technologies overview for explanations on the methodologies used in the surveys. Our reports are updated daily.

How to read the diagram:
42.5% of the websites use none of the content management systems that we monitor.
WordPress is used by 36.4% of all the websites, that is a content management system market share of 63.4%.



Let’s create a botnet of WordPress sites!

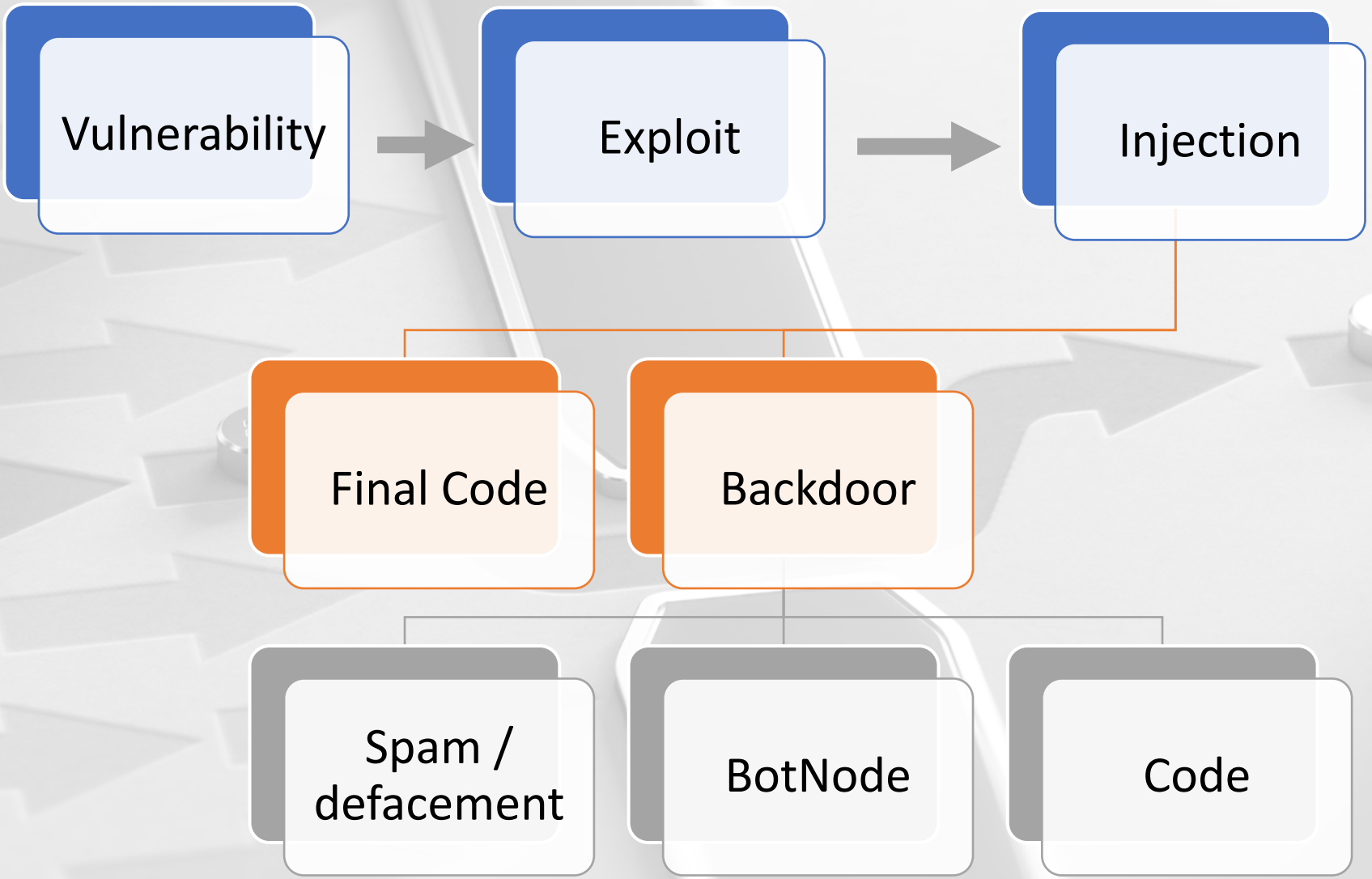
The Path

Let’s create a botnet of WordPress sites!

The Path

OK, OK, but…
how I enroll WordPress sites to my fancy Botnet?

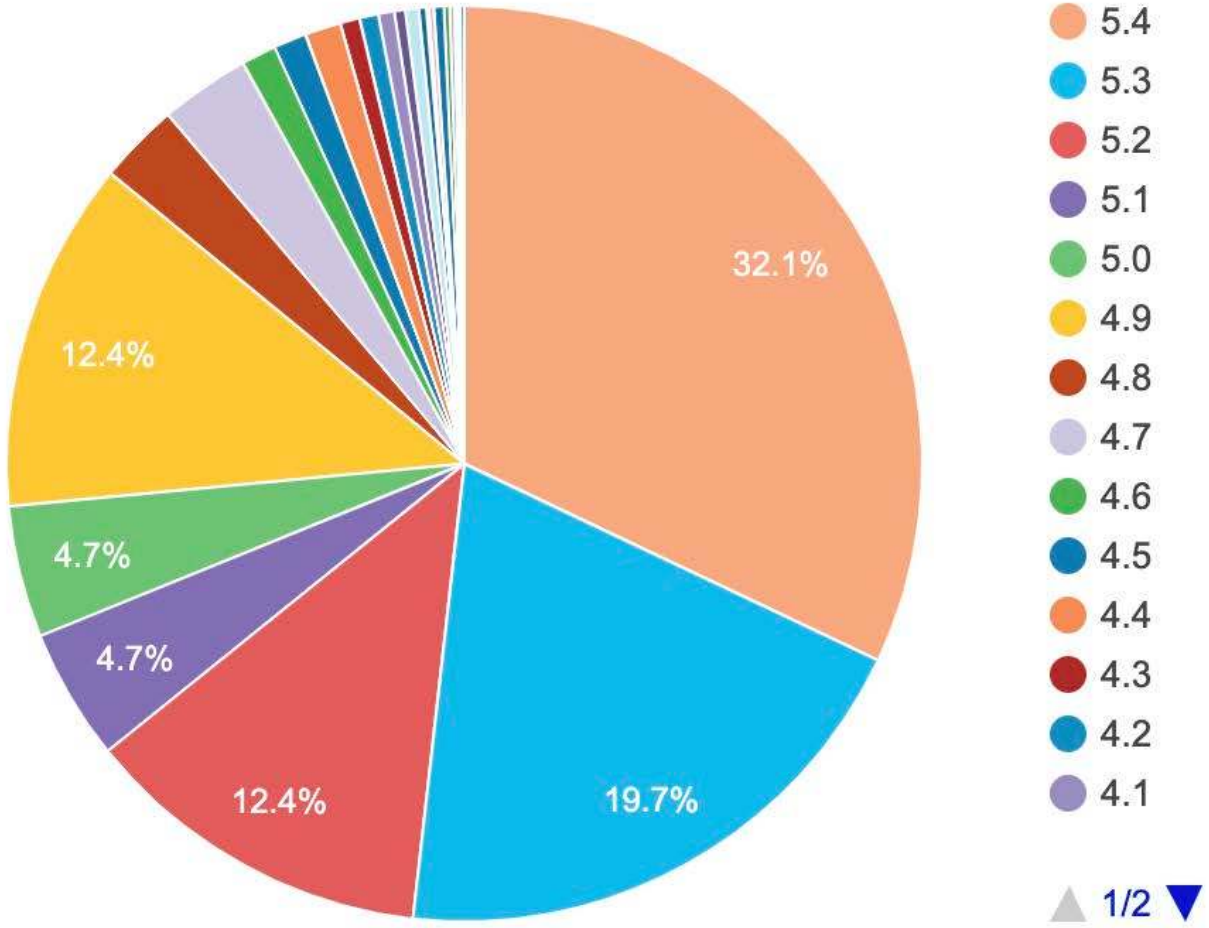
The Process


Vulnerability
Exploit
Injection
Final Code
Backdoor
Spam / defacement
BotNode
Code

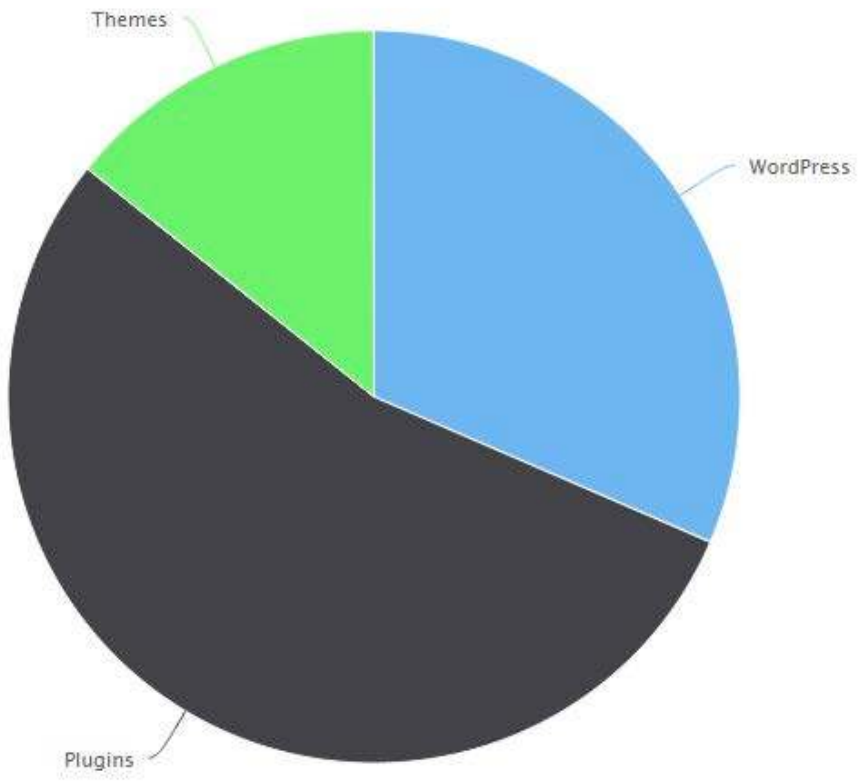
The vulnerability

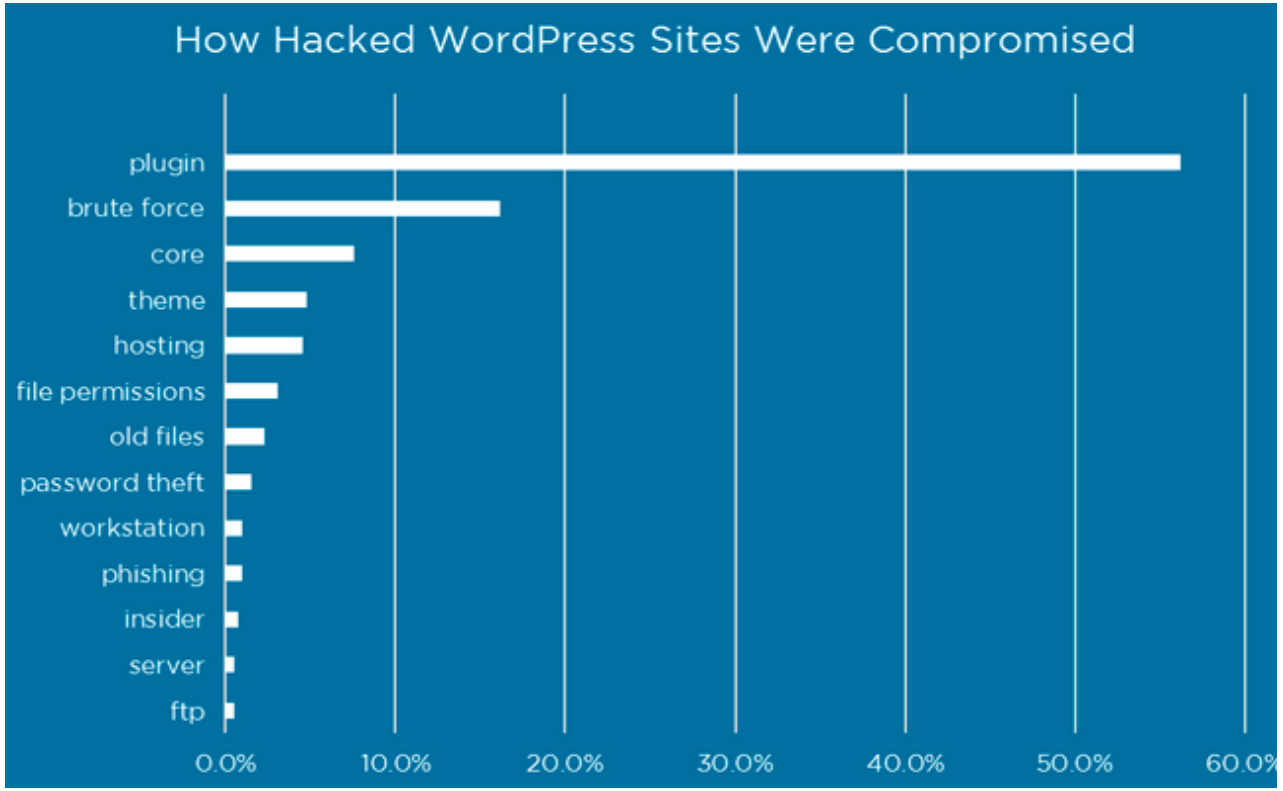
First step

Pie graph of WordPress version distribution – May20

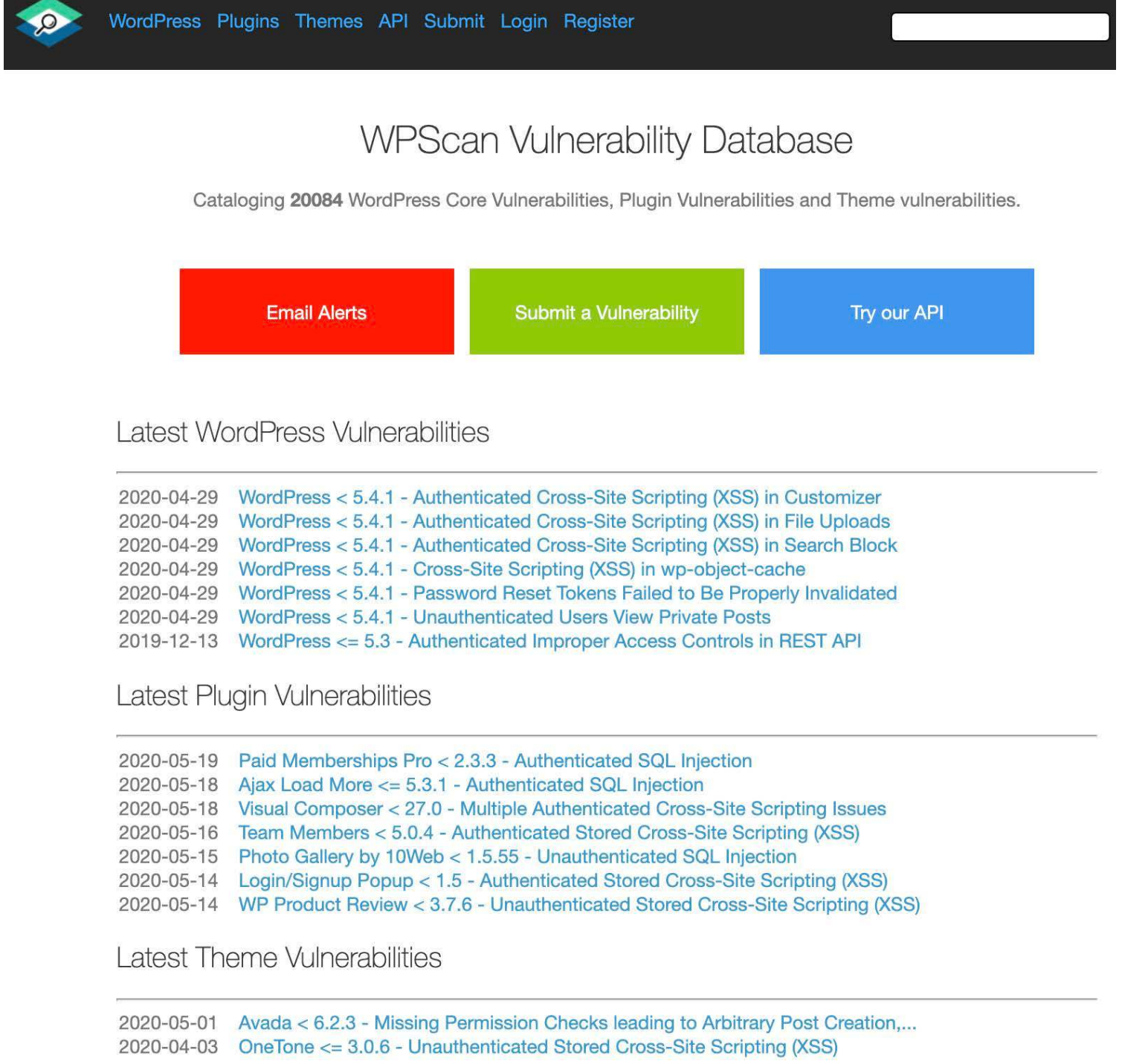


Vector of infection stats in WordPress sites





WPScan Vulnerability Database wpvulndb.com



Plugin Name	Installations
Easy WP SMTP	400,000
Wp File Manager	500,000
Freemius Library (Multiple plugins are affected)	200,000
Newspaper and other old tagDiv Themes	100,000
WordPress GDPR Compliance	100,000
Social Warfare	70,000
WP Live Chat Support	60,000
Yuzo Related Post	60,000
WP-Piwik	60,000
Sticky Menu on Scroll, Sticky Header for Any	

We need quantity!

Source: **2019 Website Threat Research Report** (sucuri.net)

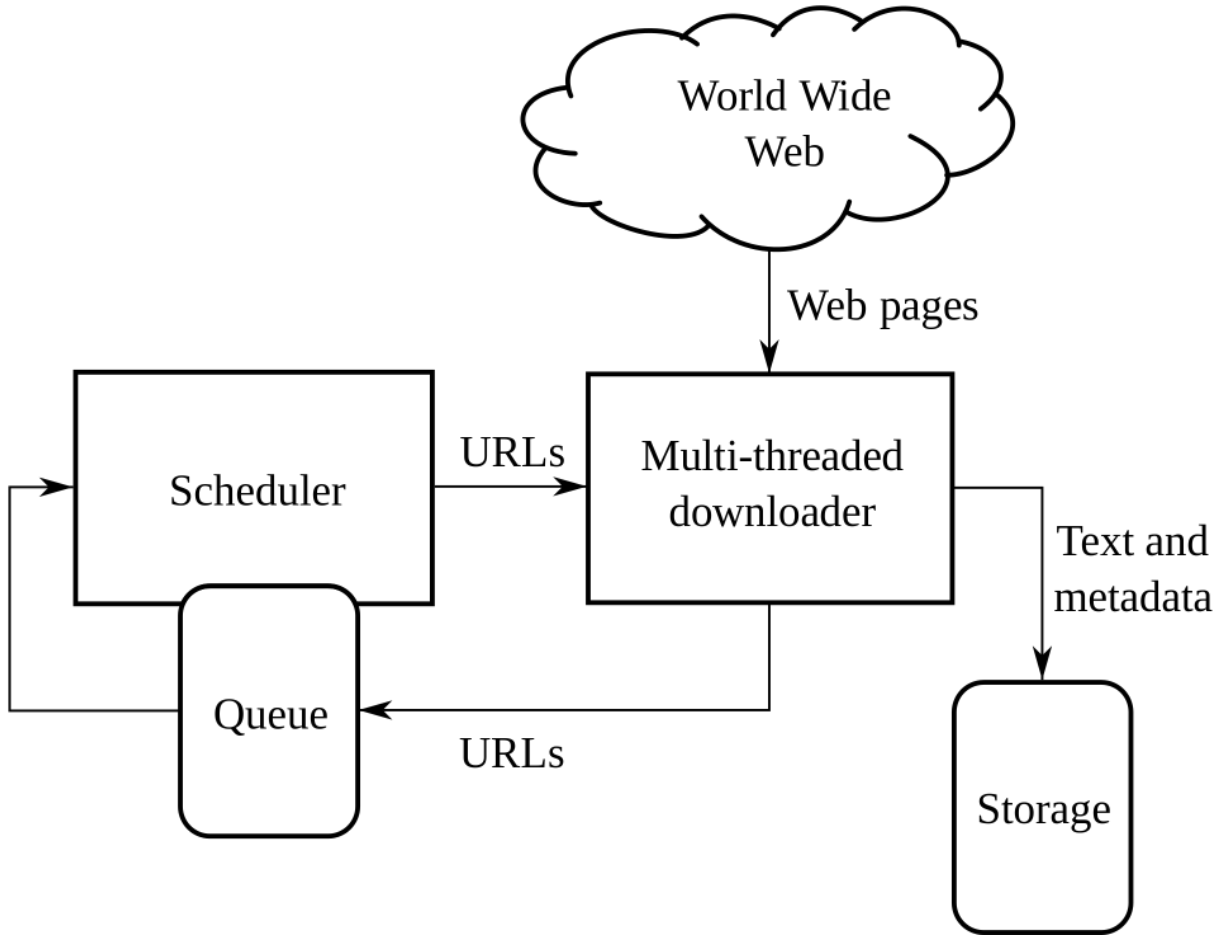
But **how** do I find those **vulnerable WordPress** installations to hack?

Spiders & AI

The tools

Crawlers / bots / Spiders

- An Internet bot that systematically browses the WWW.
- Starts from a small group of URLs (seeds)
- Collect links, add them to the queue and visit all of them, recursively



Adding AI to the Spider: 1st approach

1. When links are visited:
    1. Identify if it is a WordPress and which version
    2. List the plugins and themes
    3. Compare with the wpvulndb.com database
    4. Try to exploit all the vulnerabilities:
        1. If any of them succeed, insert a backdoor and add to the botnet list
    5. Repeat with the following URL
2. Optionally, store which vulnerabilities are faster to be exploited, and prioritise those (save time, optimised process, less risk of being detected).

Adding AI to the Spider: 2nd approach

1. Select 3 vulnerabilities of WordPress and of plugins which has more installations and are more recent
2. Search sites only with those vulnerabilities (e.g. Google Dorks)
3. When links are visited:
    1. Try to exploit all the vulnerabilities:
        1. If any of them succeed, insert a backdoor and add to the botnet list
    2. Repeat with the following URL
4. Optionally, store which vulnerabilities are faster to be exploited, and prioritise those (save time, optimised process, less risk of being detected)
5. Include in the list new ones if the selected ones having low success rates
6. Find the optimal combination

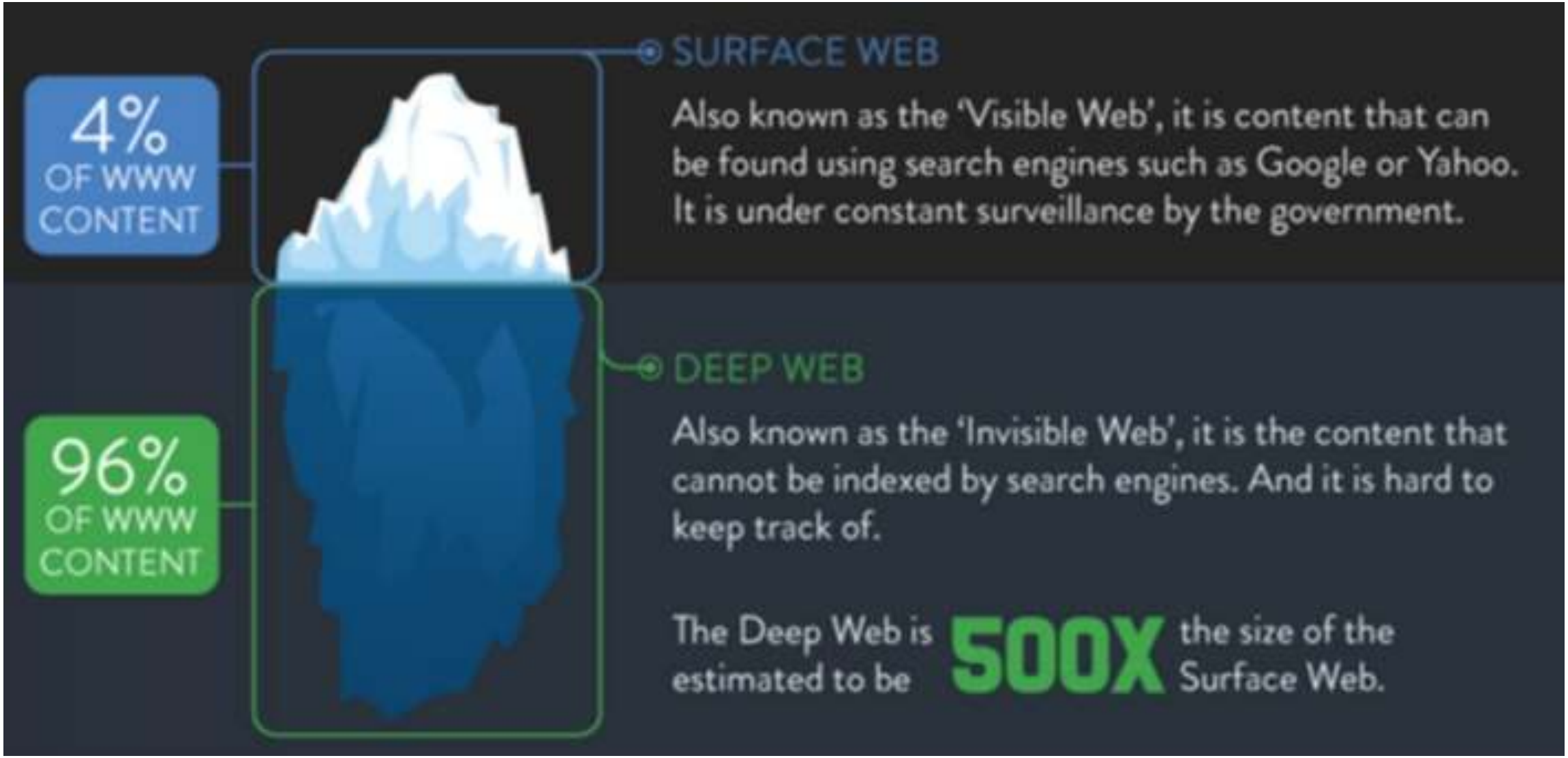
Where to find this kind of tools?

You can develop yourself one

You can buy one in the Dark Market

The Dark Web

The market

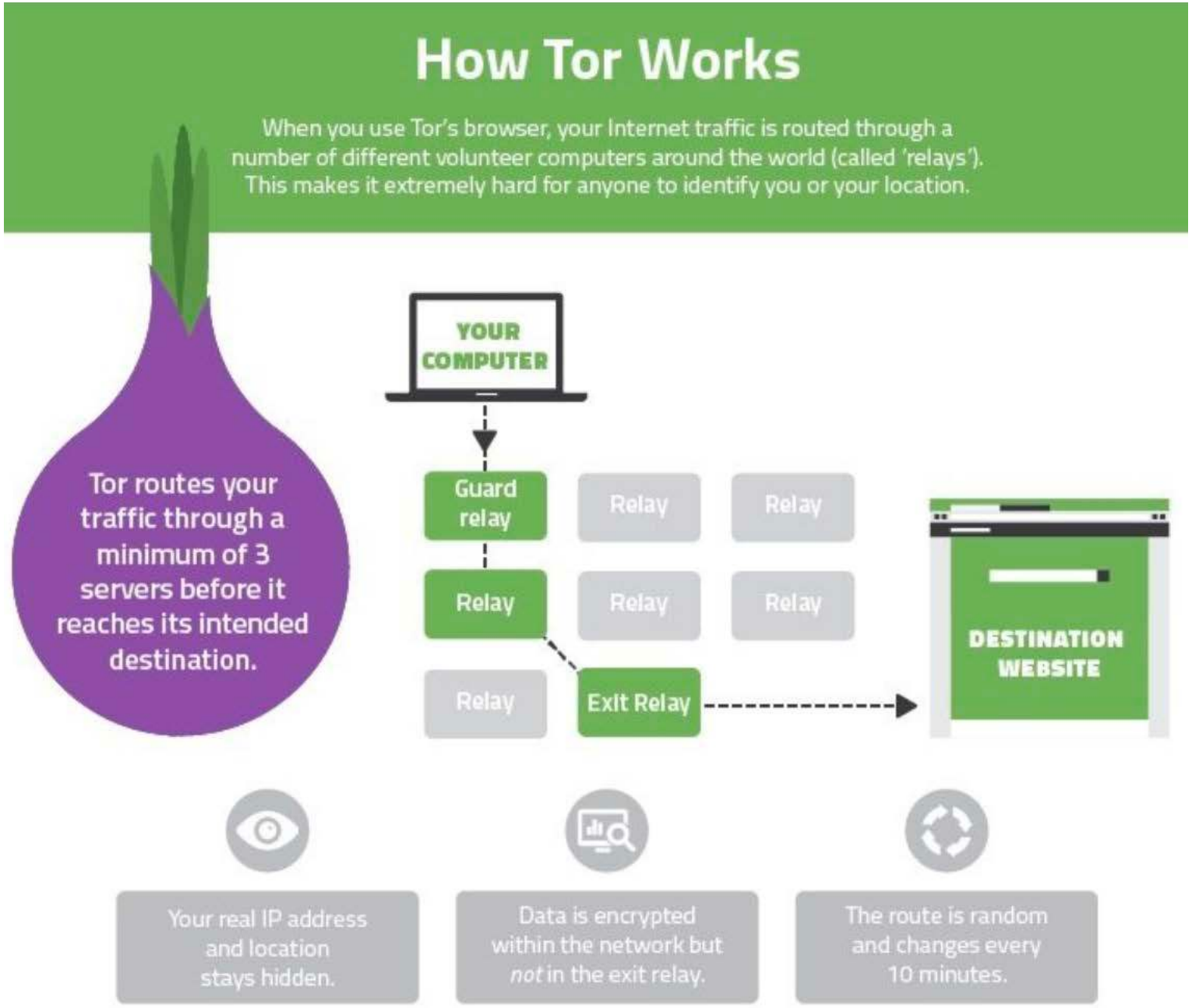

4%
OF WWW
CONTENT
SURFACE WEB
Also known as the 'Visible Web', it is content that can be found using search engines such as Google or Yahoo. It is under constant surveillance by the government.
96%
OF WWW
CONTENT
DEEP WEB
Also known as the 'Invisible Web', it is the content that cannot be indexed by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


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)

Protect yourself

- No footprint browsing
- Anonymous IP
- Secure connections

Tor + VPN



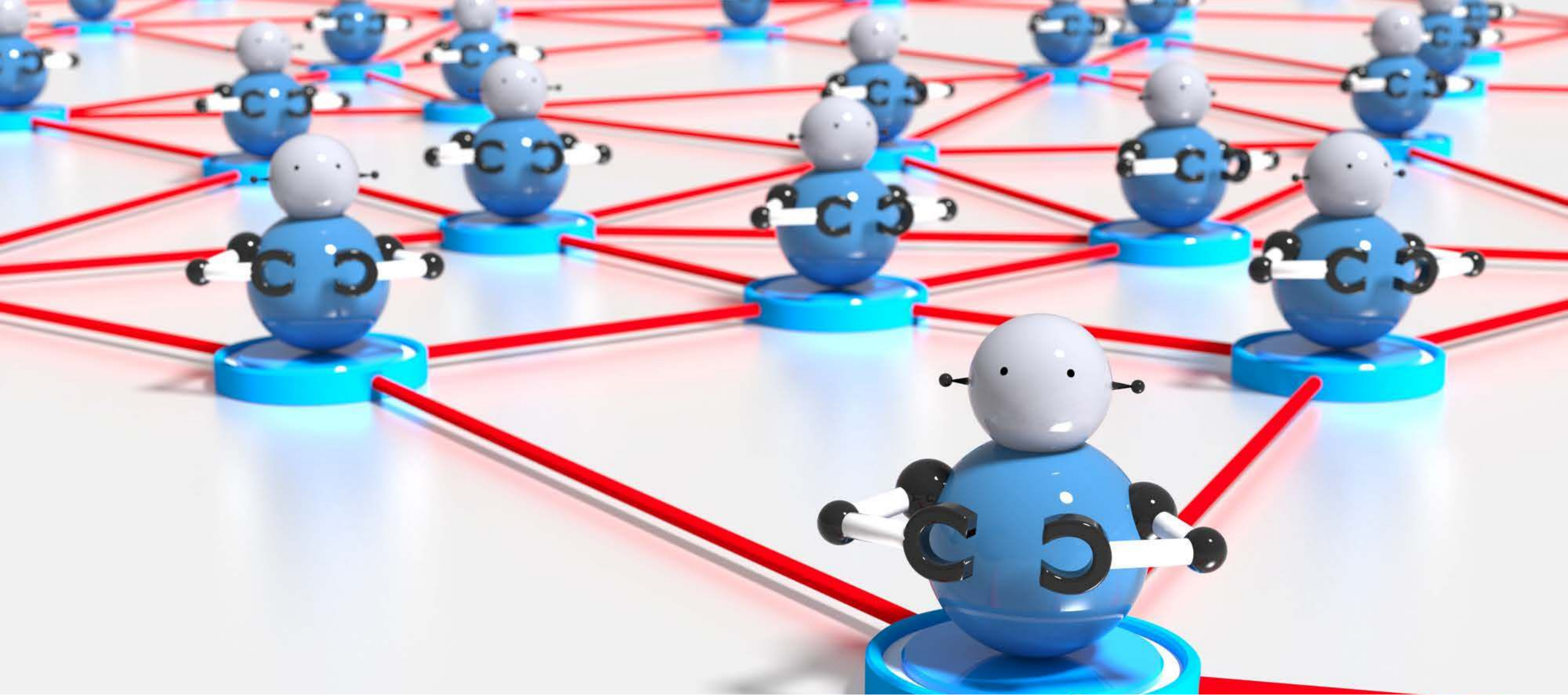
HACK GROUP

SERVICES | PRICING | ABOUT | FAQ | SUPPORT

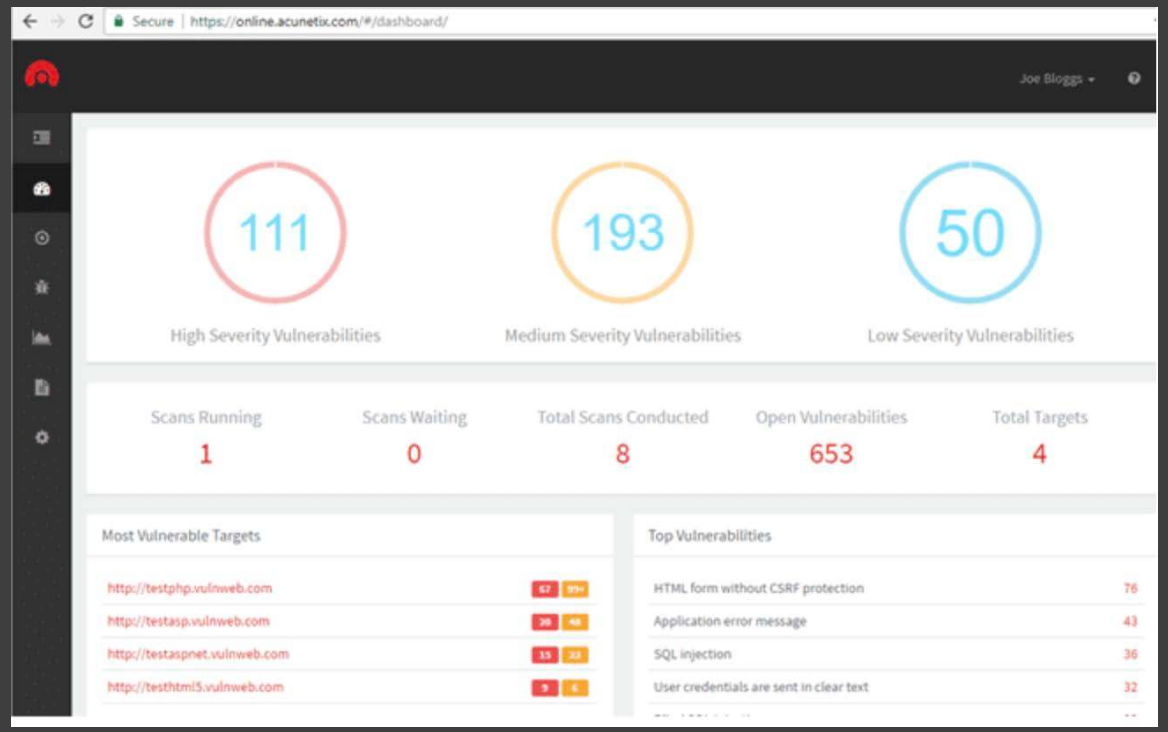
PROFESSIONAL **HACK GROUP** QUICKLY HELPS TO SOLVE YOUR NEEDS

SERVICES	PRICE	ORDER
Hacking web server (vps or hosting)	0.0359฿	ORDER
Setting up Keylogger	0.0175฿	ORDER
DDoS (For big sites price can change)	0.0462฿	ORDER
Device Tracking - smartphone/pc	0.0226฿	ORDER
Fraud Track - Find your scammer	0.0185฿	ORDER
Web server security audit	0.0205฿	ORDER
Hacking personal computer	0.0257฿	ORDER
Social Media - account hacking	0.0236฿	ORDER
Spyware creation	0.0287฿	ORDER
Intelligent report - locate people	0.0216฿	ORDER
Intelligent report - background check	0.0185฿	ORDER
Setting up your own botnet	0.0667฿	ORDER
Logs from Zeus 1 GB (CCs, PayPals, Bank Accs...)	0.0277฿	ORDER
Logs from Zeus 10 GB (CCs, PayPals, Bank Accs...)	0.0873฿	ORDER

IF YOU NEED SPECIAL SERVICES - CONTACT US HERE.



The conclusion

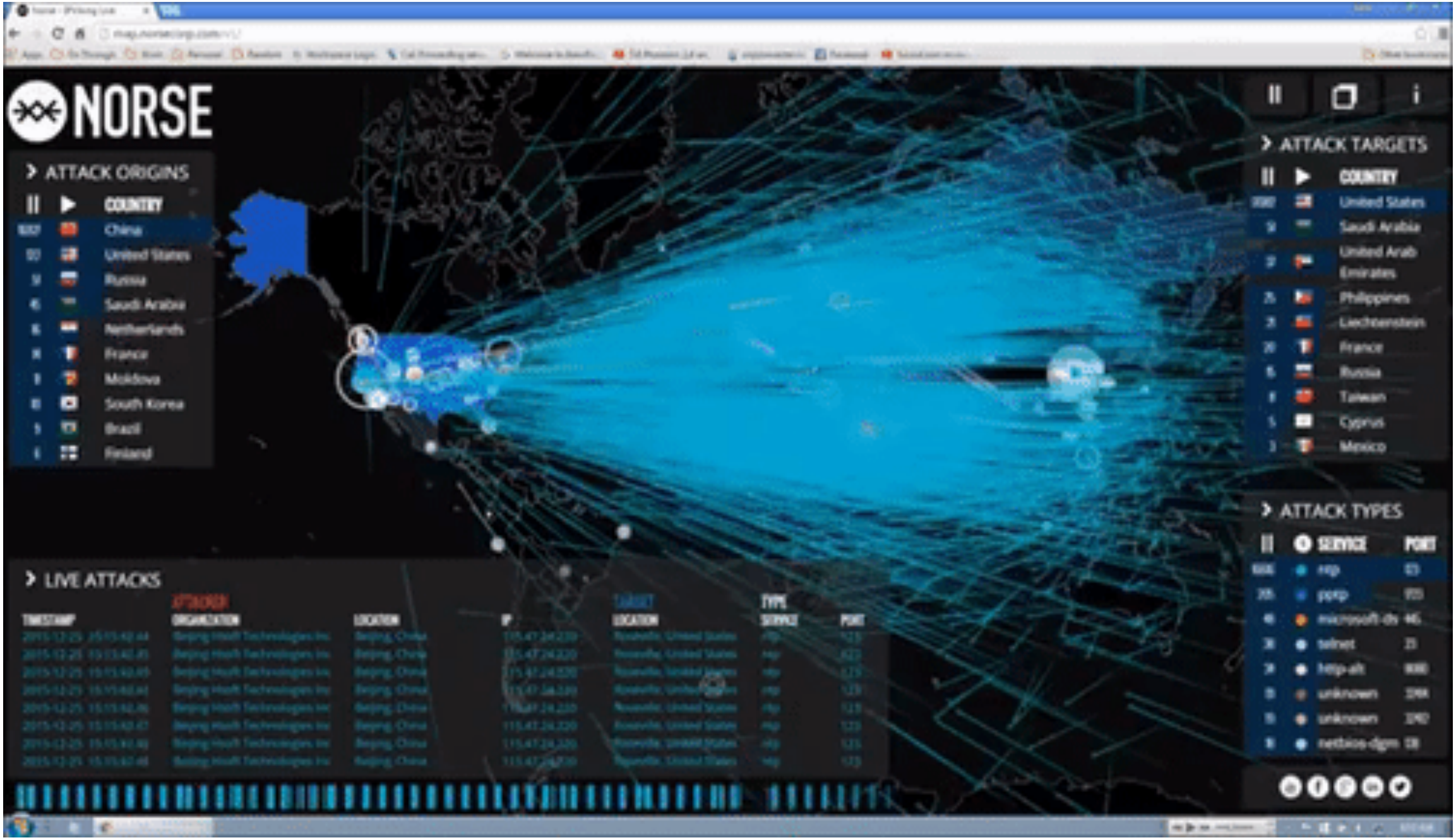


Acunetix software admin panel, which is a software to scan and identify vulnerabilities

It is not a hacking software, but works well for the purposes of the presentation since of its similarity with real hacking admin panels.

Final result


DDOS Attack!
Insert
Home
Delete
End
Shift


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
ORIGIN
ORGANIZATION
LOCATION
IP
TARGET
LOCATION
TYPE
SERVICE
PORT


DDoS ATTACK
DDOS
Online Service Unavailable


YOU'VE BEEN HACKED!
MacBook Pro

Checklist to survive to the HWW

AKA Countermeasures

Some scary stats

Hackers who do malware are between 300k and 1.5M in the whole world

There is a hacking **attack attempt every 39 seconds**.

Russian hackers are the fastest.

300,000 new malware is created every day.

Multi-factor authentication, optimised and updated firewalls and encryption are the biggest hacker obstacles.

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

Proactive measures

Reduce admins, plugins and themes

Backups

Updates

Invest in Hosting & Security

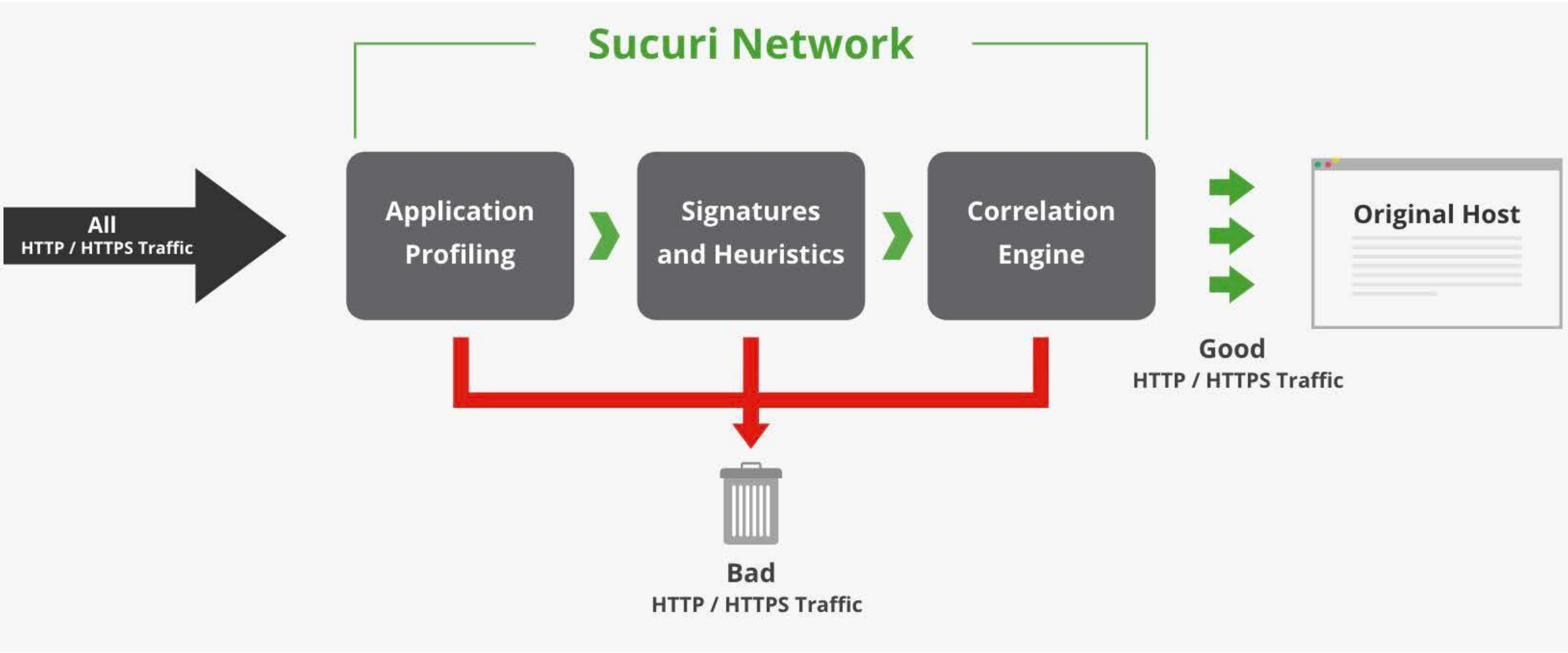
WAF

Remember to invest in…

SECURITY

HOSTING

AI against AI - E.g: WAFs




Everybody needs a hacker

WCEU2020

THANKS! QUESTIONS!!

Nestor Angulo (@pharar)