AI in the Hacking World War

NESTOR ANGULO @ WC GREECE 2021

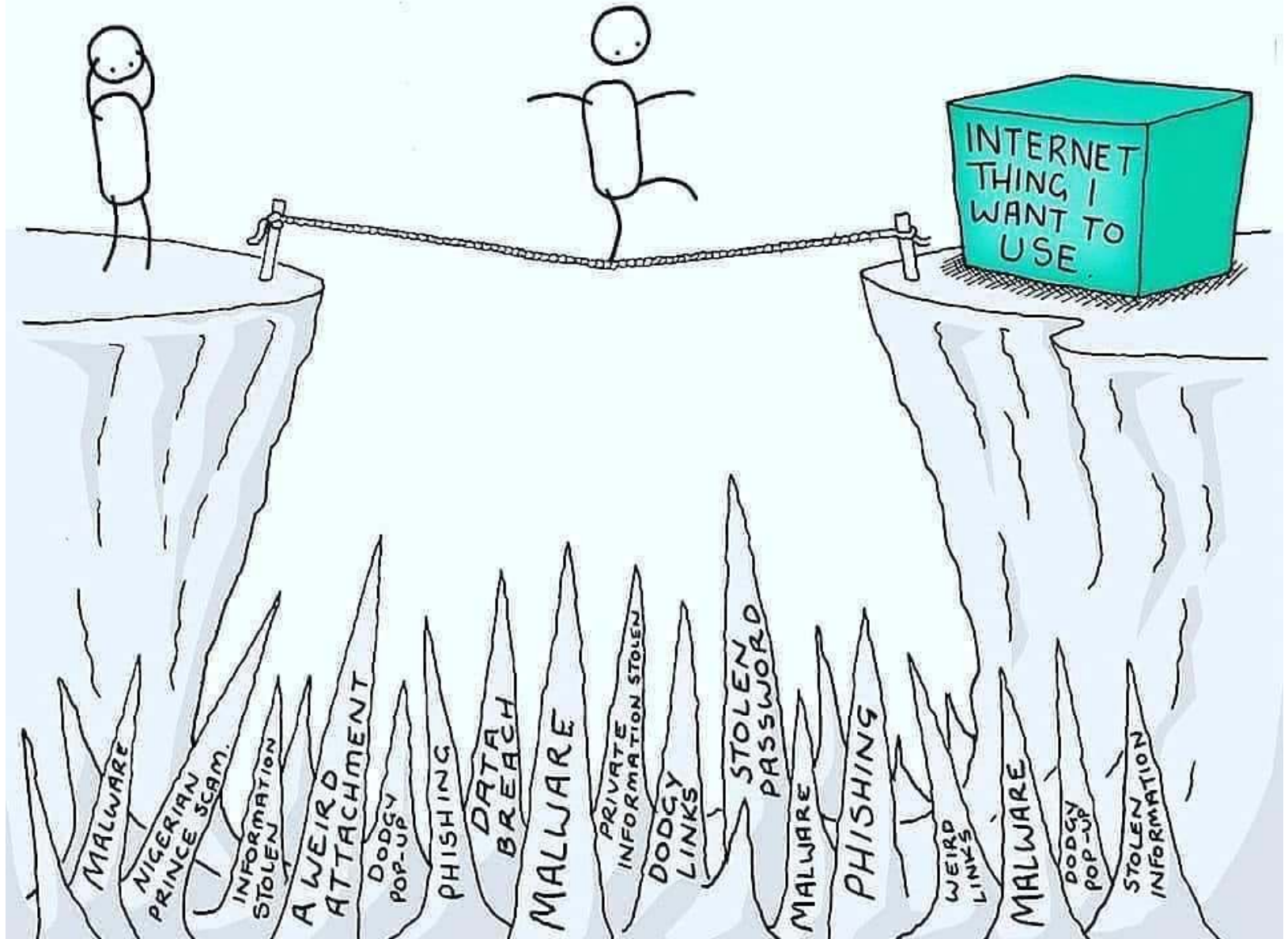
DISCLAIMER

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**.

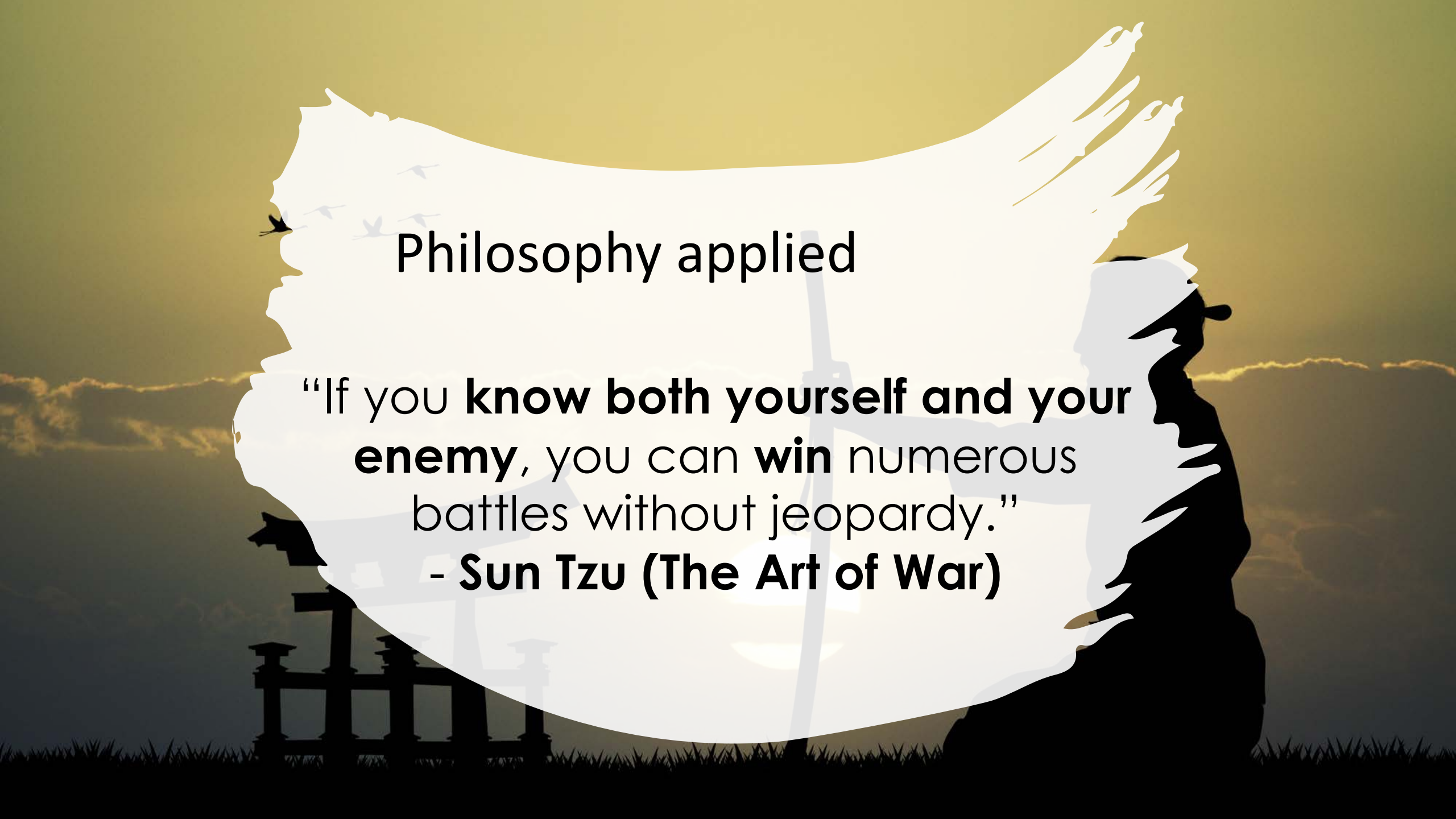
This talk is intended to be **DIDACTIC**. **I don't encourage any hacking attempt**.
Always ask to an expert if you have questions.

DEALING WITH CYBER STRESS




BOTNET
SPAM
PHISHING
HACKER
MALWARE
DDOS
KEYLOGGER
VIRUS
SPYWARE


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



Philosophy applied

"If you **know both yourself and your enemy**, you can **win** numerous battles without jeopardy."

- **Sun Tzu (The Art of War)**

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**

Computer Hacker ***Hat Colours***

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

*Some **scary** stats*

Hackers who do malware are **300k - 1.5M** in the whole world

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

Russian computer hackers are the fastest.

300,000 new malware are created every day.

*A **WordPress** site common **targets***

USERS

DATABASE

CONTENT

INFRASTRUCTURE

BOT NET

REPUTATION

AI (Artificial Intelligence)

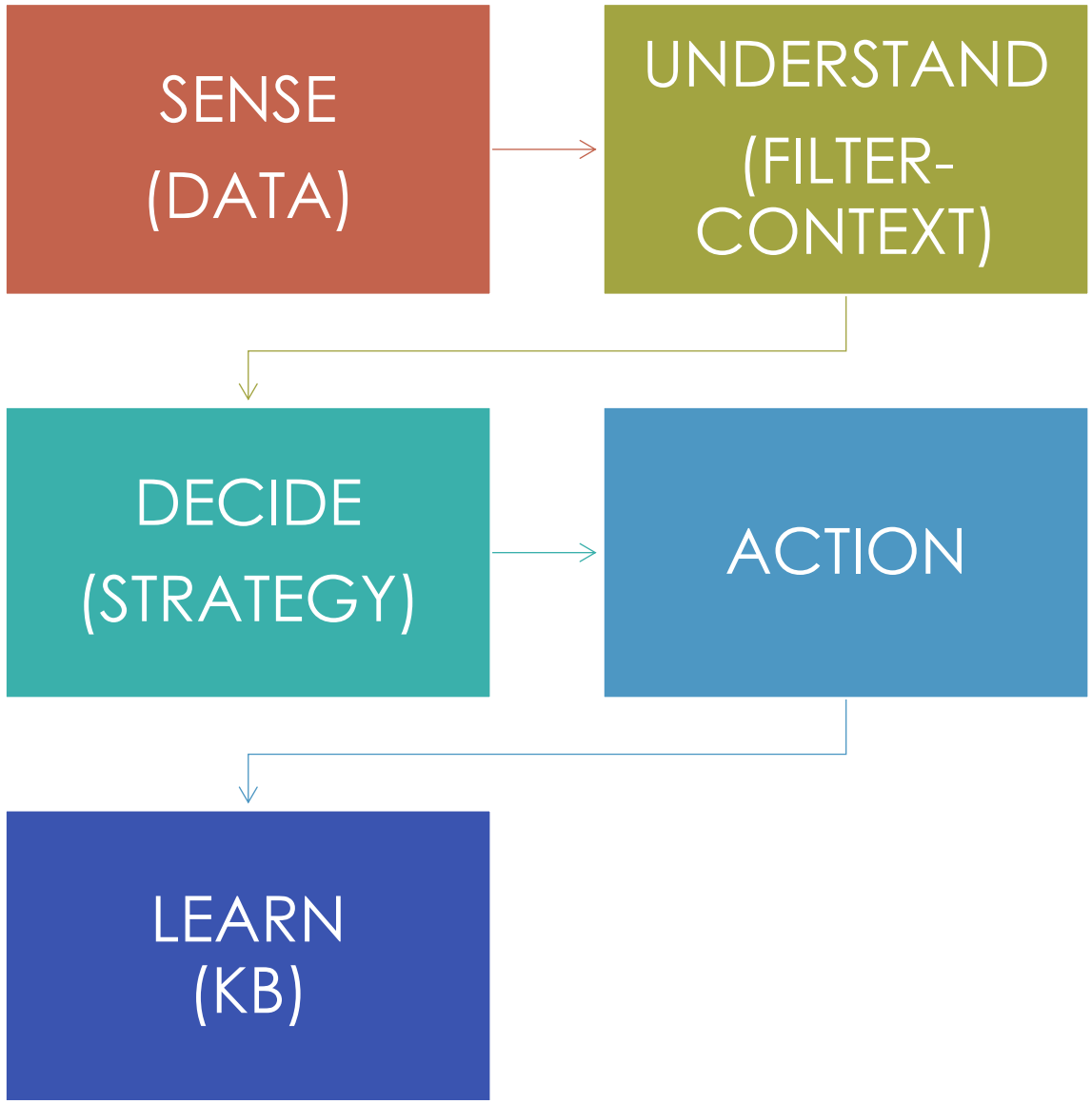
SIMULATION OF HUMAN INTELLIGENCE PROCESSES BY MACHINES, ESPECIALLY COMPUTER SYSTEMS.

*The **What**: **AI** (Artificial Intelligence)*

Buzzword, with lots of sub-fields, approaches, goals and philosophies.

Controversy: What is **learning in this context**?

*The **How:***
AI Phases



Orientations *of AI*

Assisted Intelligence

Improve processes

Augmented Intelligence

Enables to do things otherwise can't be done

Autonomous Intelligence

Self-Driving

***Subsets** of AI*

Machine Learning (ML)	Deep Learning (DL)	Expert Systems (ES)	Neural Networks (NN)
• Statistical technique • Data oriented (rather than explicitly programmed) • Specific tasks	• Part of the ML methods • Data representations (rather than task-specific algorithms)	• Fuzzy logic / rules-based reasoning • Solve problems within specialized domains	• Biologically-inspired • Observational data


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


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


CYBERTHREAT REAL-TIME MAP
EN
Protect Yourself
MAP
STATISTICS
DATA SOURCES
BUZZ
WIDGET
Share
DEMO ON
9871958
4378628
176091
4638492
7762480
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.):

Individuals / freelancers

Governs

Companies

Activists

Different goals (e.g.):

Information

Money

Industrial Interests

Political interests

Hacktivism

The AI/cybersecurity ***conundrum***

- Cybercriminals also use AI
- The **Training** dependency
- The **Overfit/Bias** issue
- Big amount of computing resources needed

Some AI case uses in the CWW: BlackHat

GPT 3 / DEEP LEARNING

- PHISHING
- FAKE NEWS
- SOCIAL ENGINEERING

EVOLUTIONARY ALGORITHMS (EA)

- CRACKING PASSWORDS / MD5 / HASHES.

RULE-BASED SYSTEM (RBS)

- AUDITING
- EXPERT SYSTEMS

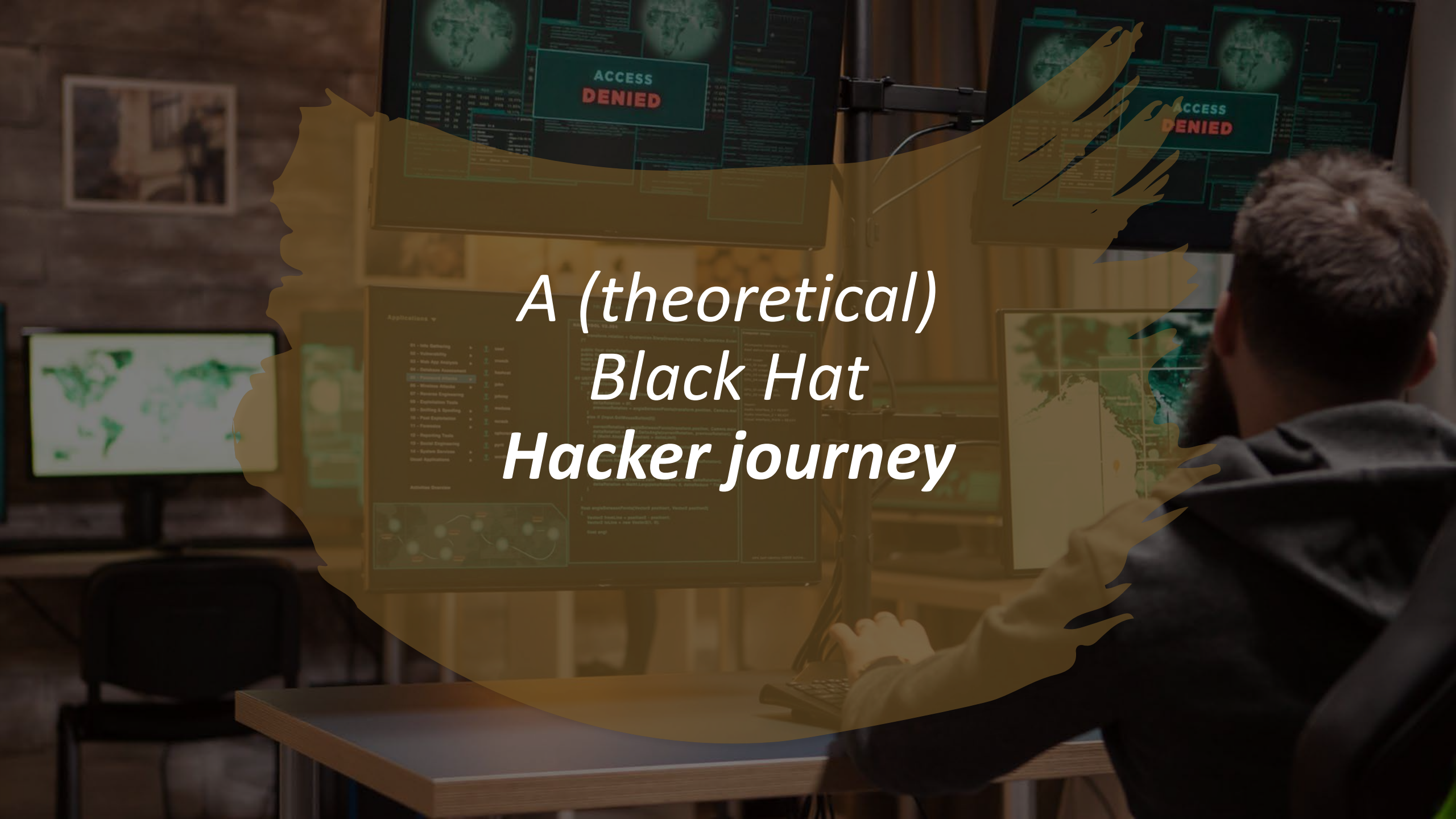
Some AI case uses in the CWW: BlackHat

GENERATIVE ADVERSARIAL NETWORK (GAN)

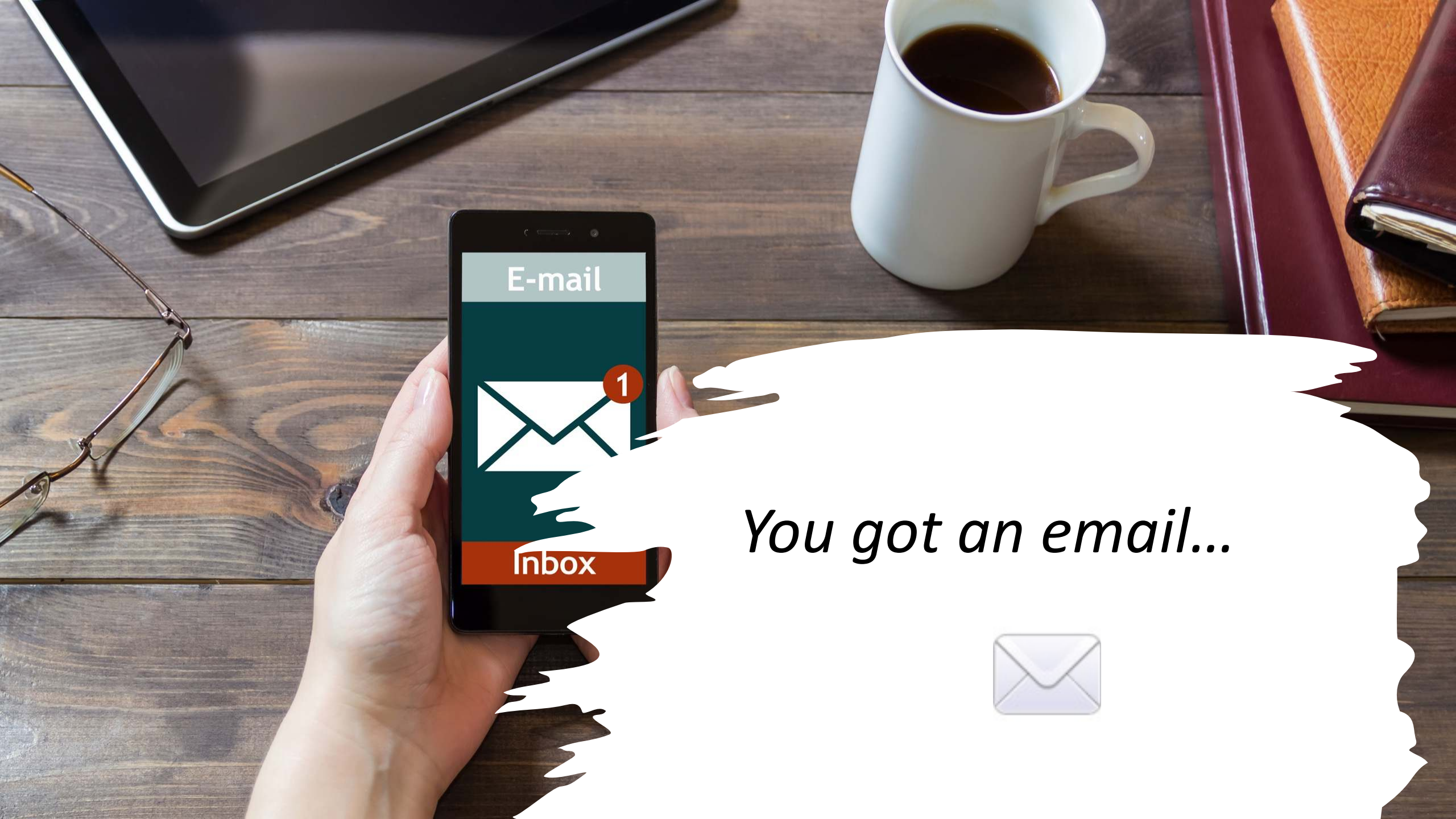
- DEEP FAKES
- CRACKING CAPTCHAS.

NEURAL NETWORKS (NN)

- IMAGE CLASSIFICATION
- POI / OBJECTS IDENTIFICATION



A (theoretical)
Black Hat
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


challenge accepted

THE PROBLEM

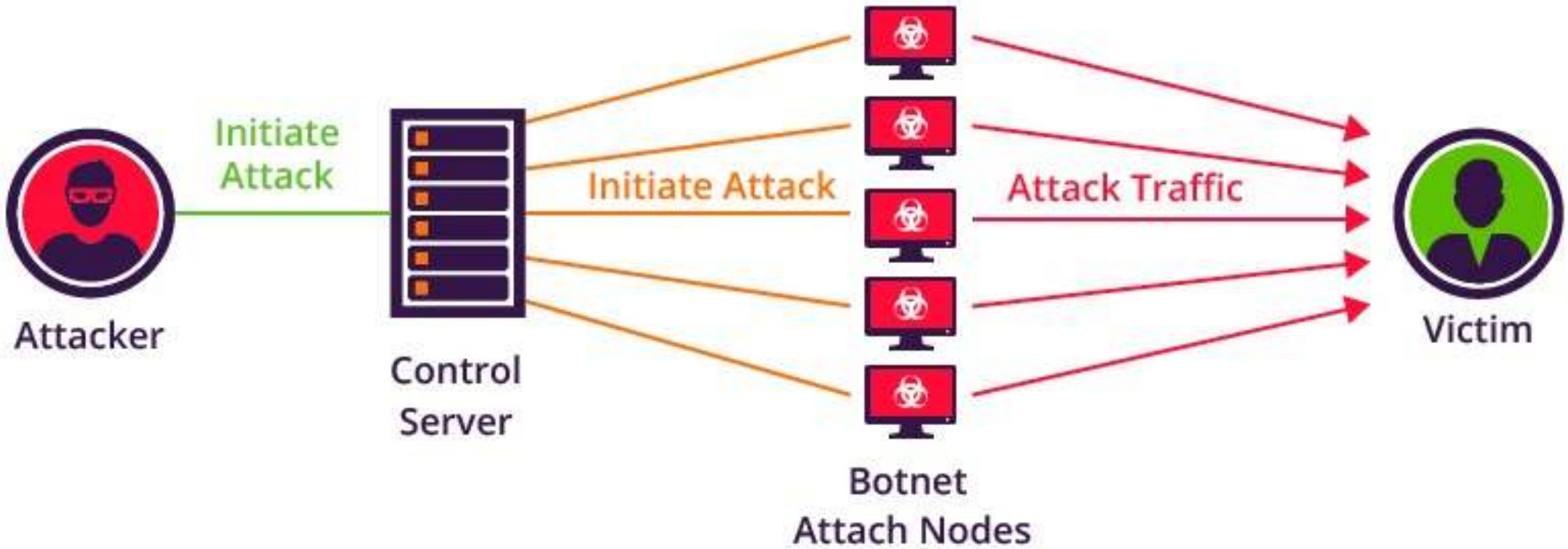
How to ruin a launch campaign?

A DDoS attack!

THE SOLUTION

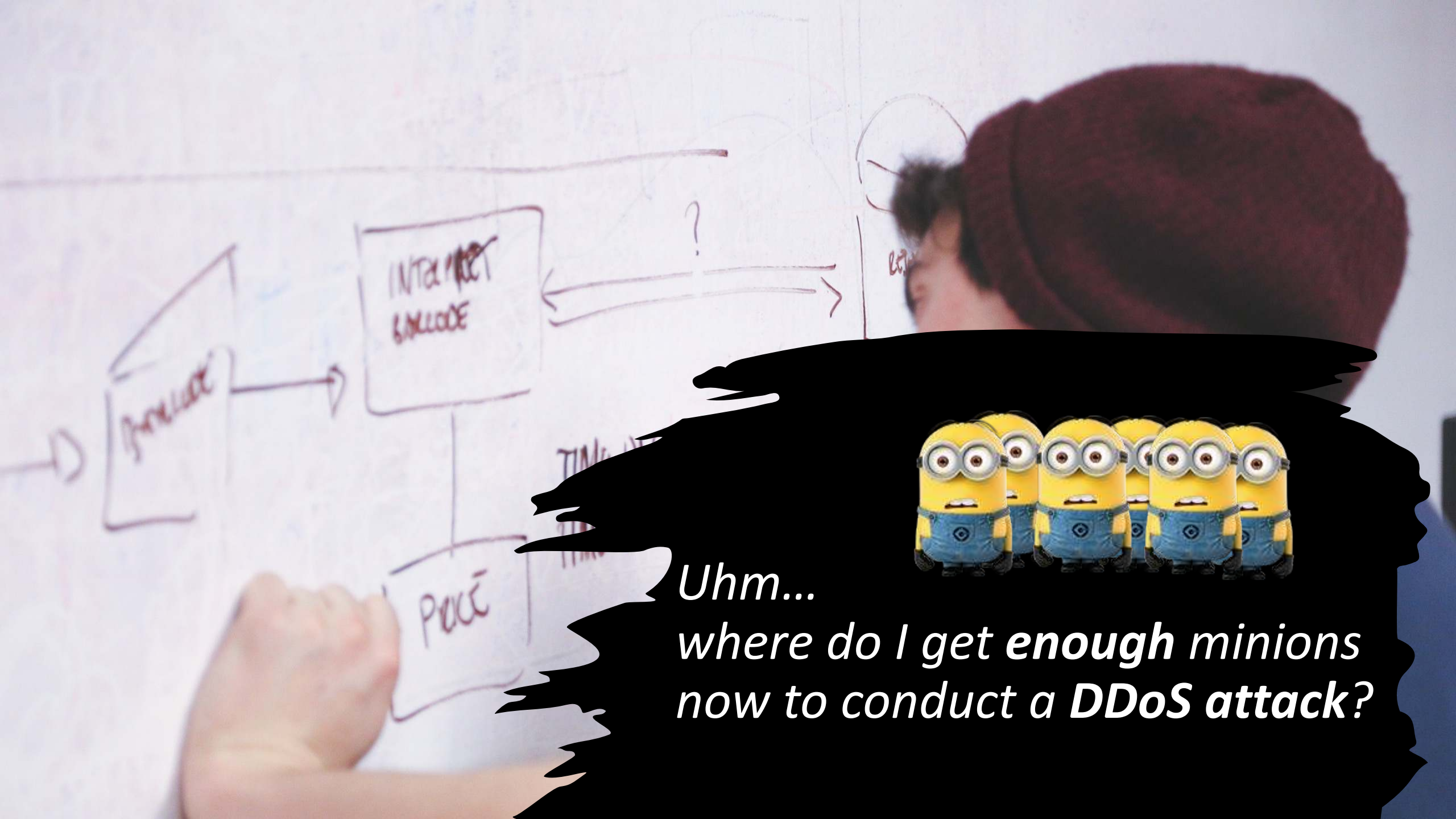
A DDoS attack...
Easy Peasy... right?

THE SOLUTION


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

The Expectations

The Reality


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

Oh, wait… WordPress is used in the 40% of Internet

Source: https://w3techs.com/

Technologies > Content Management

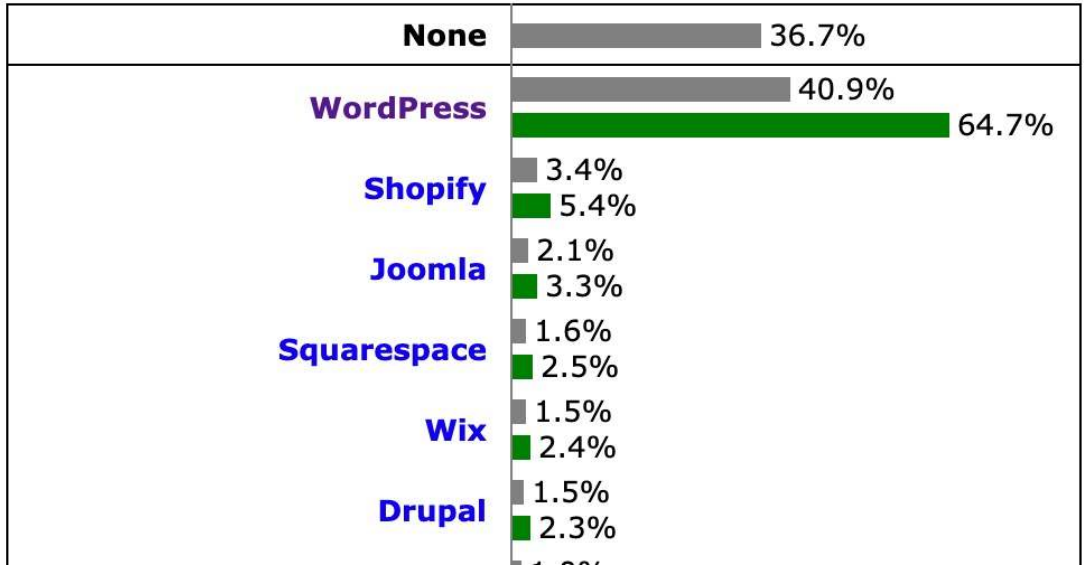
Usage statistics of content management systems

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.

Request an extensive content management systems market report.

Learn more

How to read the diagram:
36.7% of the websites use none of the content management systems that we monitor.
WordPress is used by 40.9% of all the websites, that is a content management system market share of 64.7%.



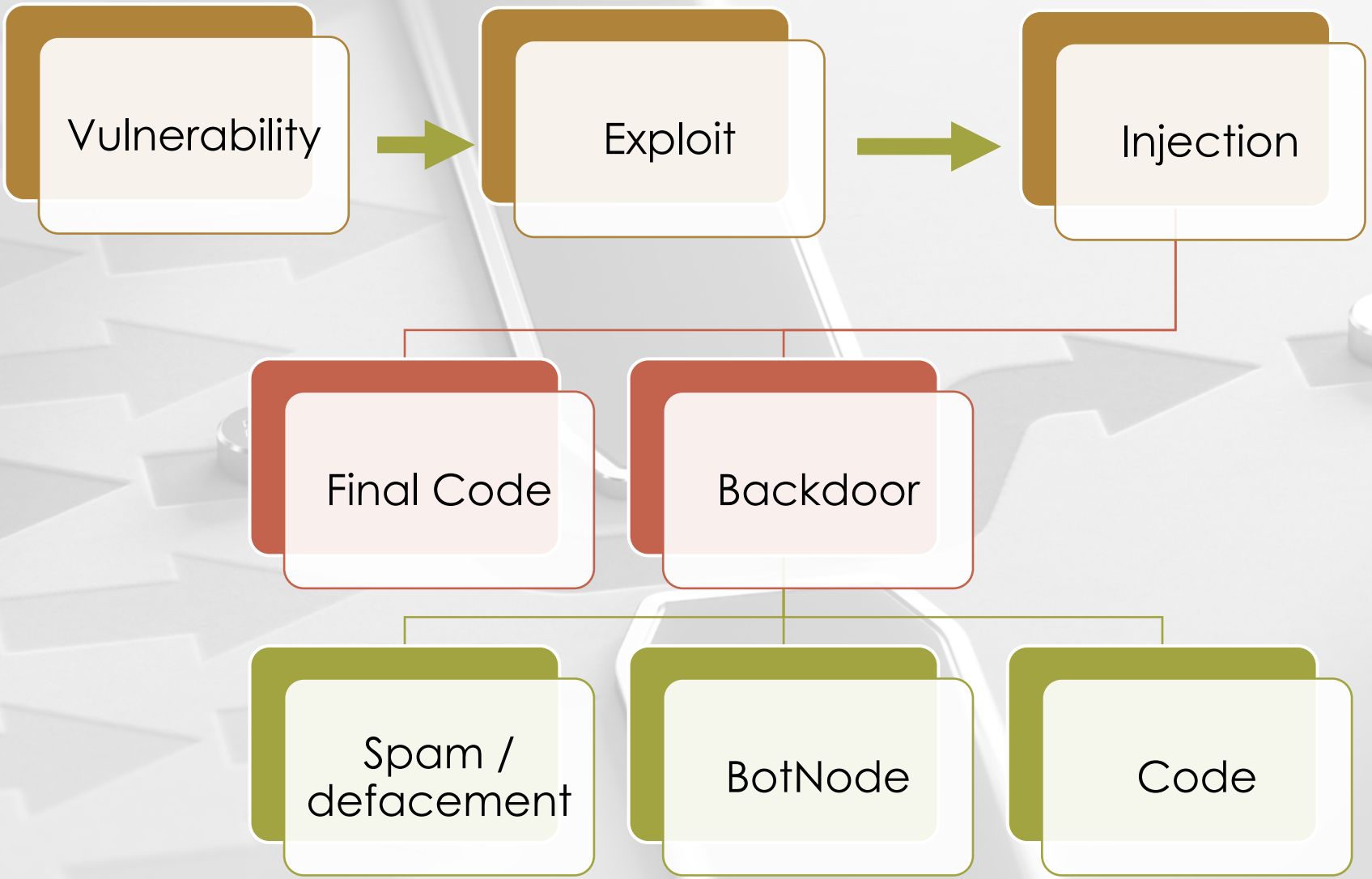
*Let's create a **botnet** of WordPress sites!*

THE PATH

of WordPress sites!

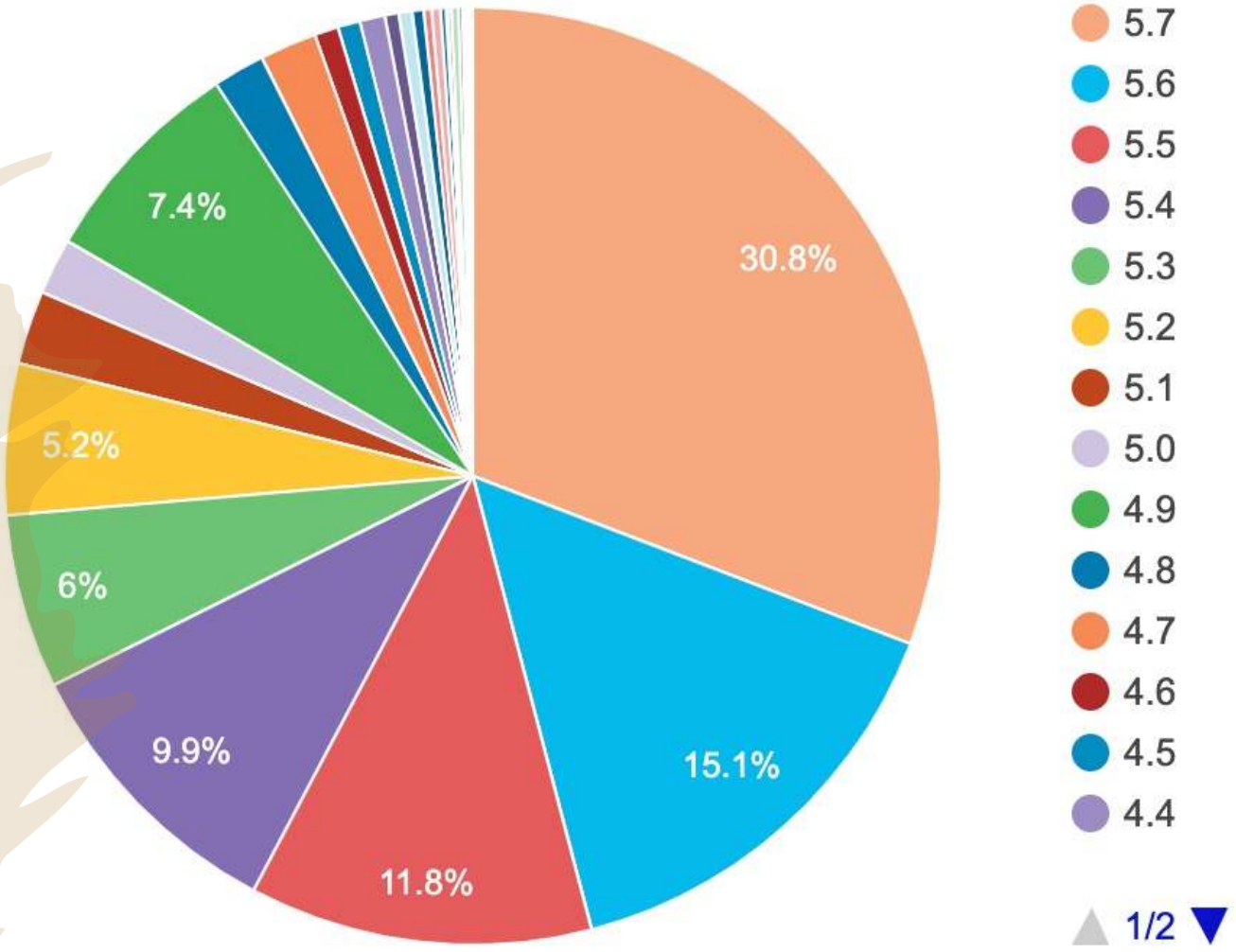
THE PATH


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


Vulnerability
Exploit
Injection
Final Code
Backdoor
Spam / defacement
BotNode
Code

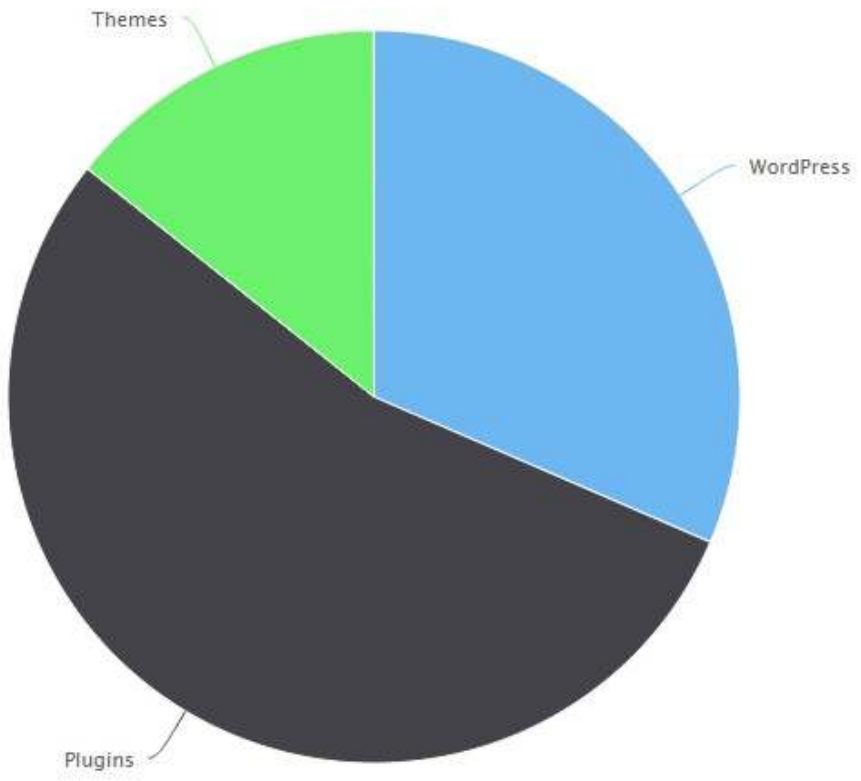
The vulnerability

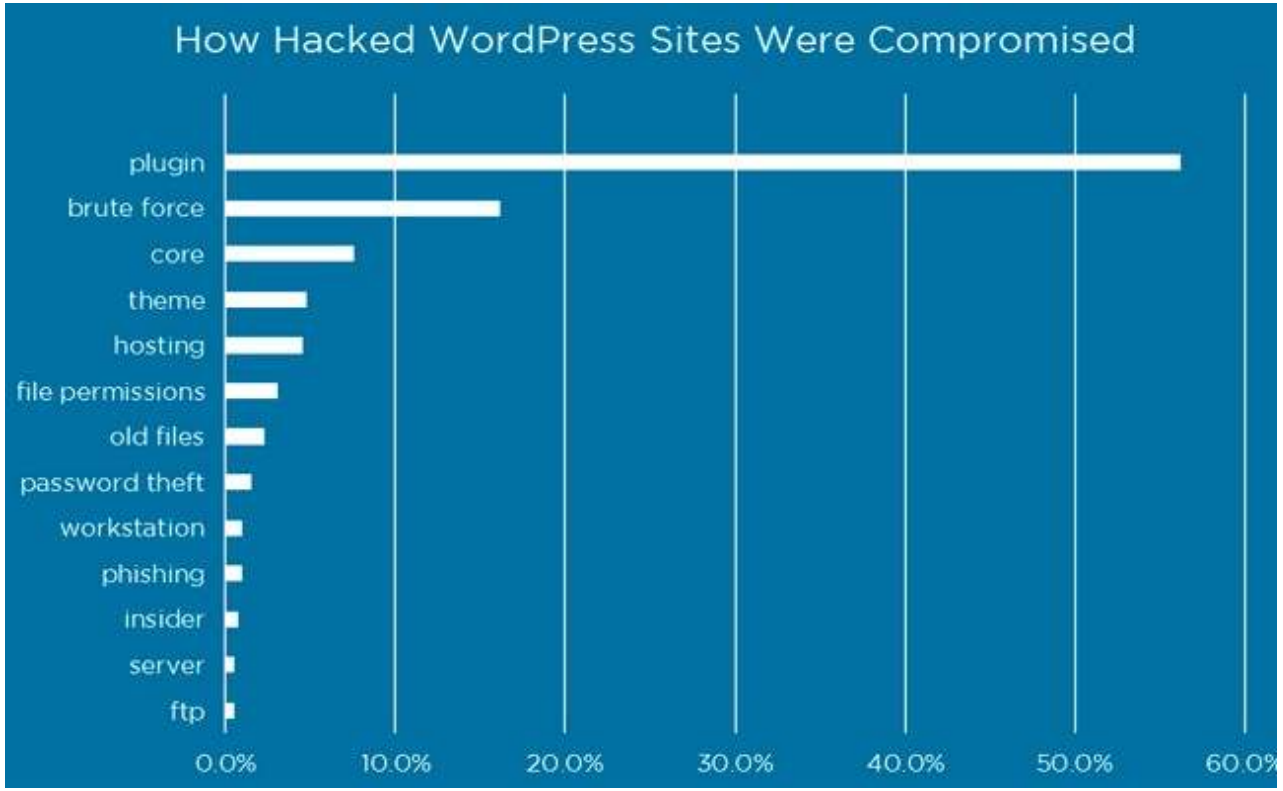
FIRST STEP



WordPress version distribution – Apr21

Vector of infection stats in WordPress sites



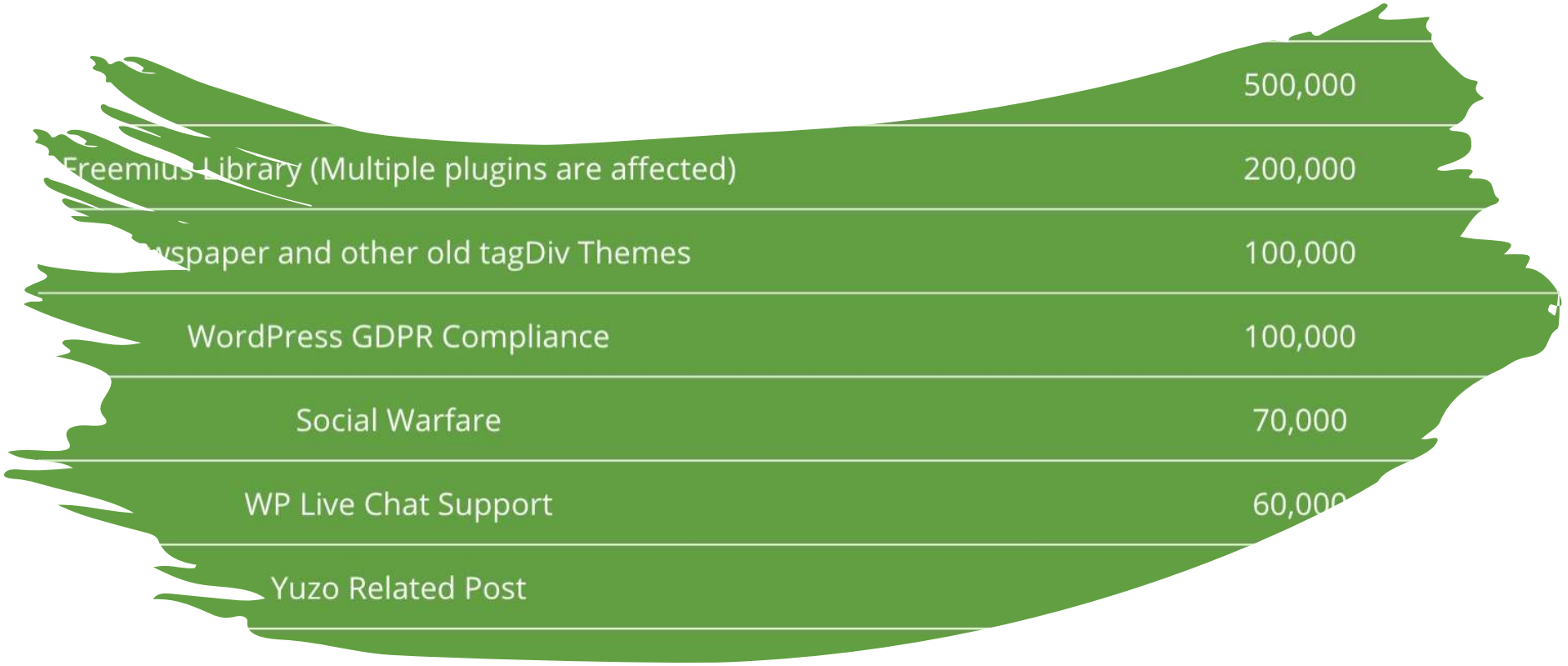


WordPress Plugin Vulnerabilities

0-9 - A - B - C - D - E - F - G - H - I - J - K - L - M - N - O - P - Q - R - S - T - U - V - W - X - Y - Z

SLUG	PUBLISHED	TITLE
1-flash-gallery	2014-08-01	1-fl
1-flash-gallery	2014-08	
1-jquery-photo-gallery-slideshow-flash	2014-08	
123contactform-for-wordpress	2021-01-20	
123contactform-for-wordpress	2021-01-20	
123contactform-for-wordpress	2021-01-20	
1player	201	

WPScan Vulnerability Database
wpscan.com



We need quantity!

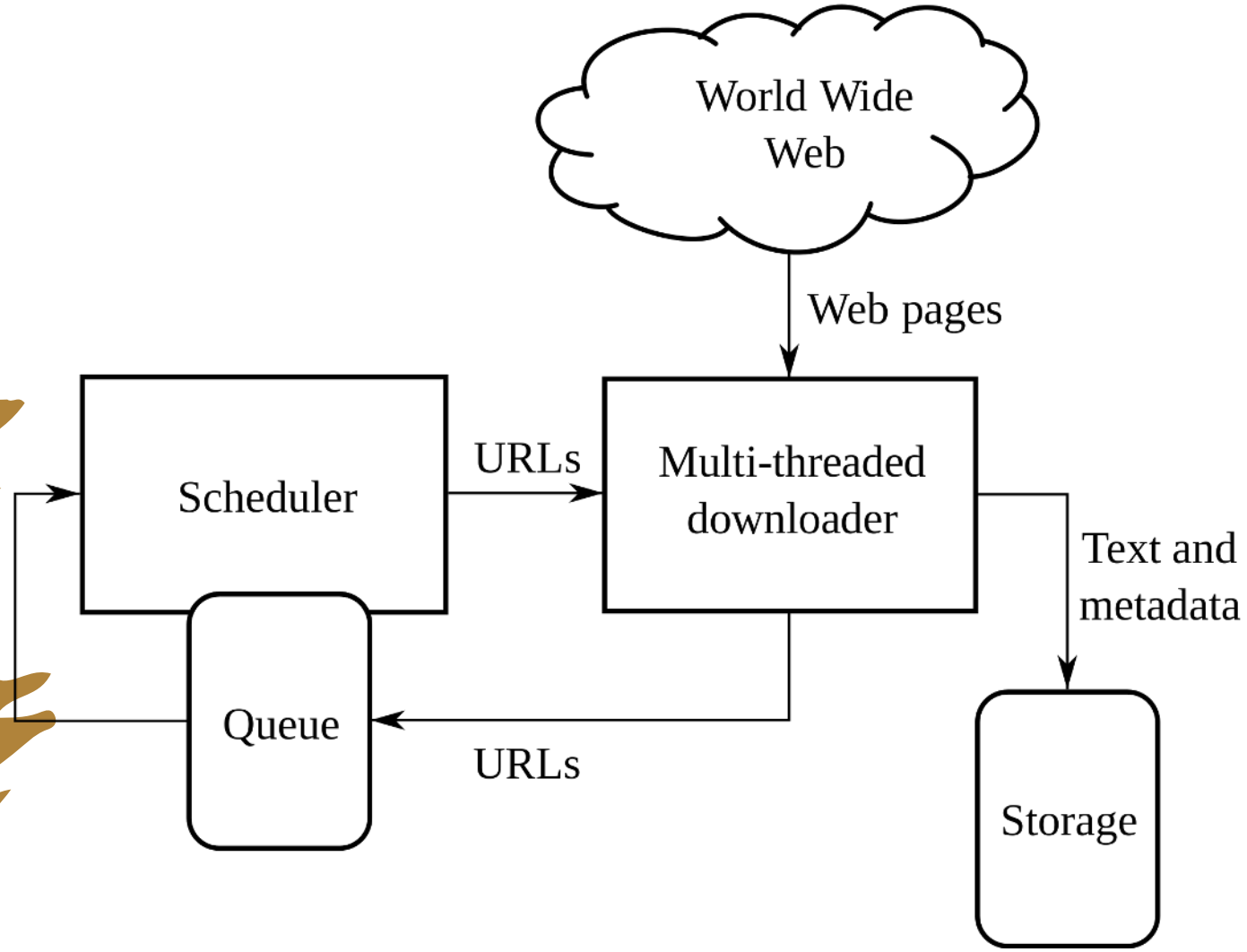
*But **how** do I find those **vulnerable WordPress** installations to hack?*

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, optimise processes, less risk of being detected).

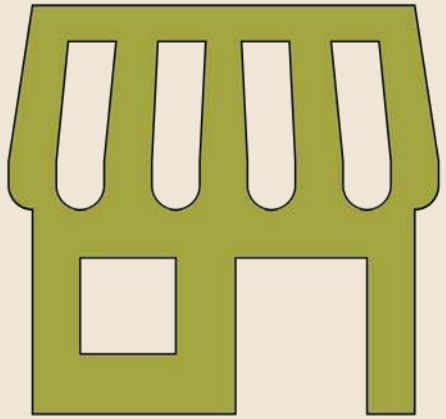
*Adding **AI** to the Spider: 2nd approach*

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, optimise processes, less risk of being detected)
5. **Include in the list new ones** if the selected ones are having low success rates
6. Algorithm to find the **optimal combination**

*Where to find this kind of **tools**?*

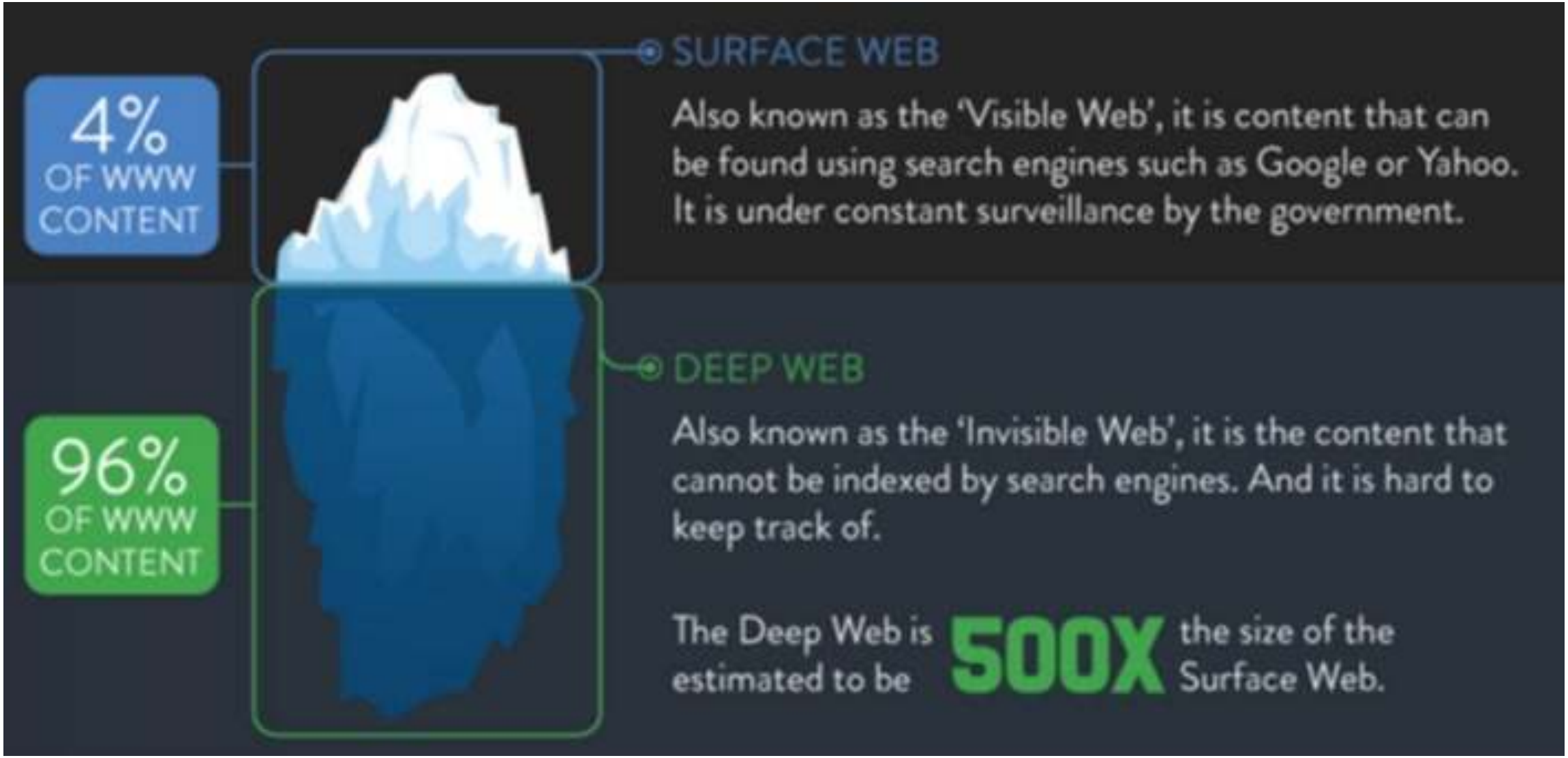
Develop yourself one



Buy one in the **Dark Market**

The Dark Web

THE MARKET

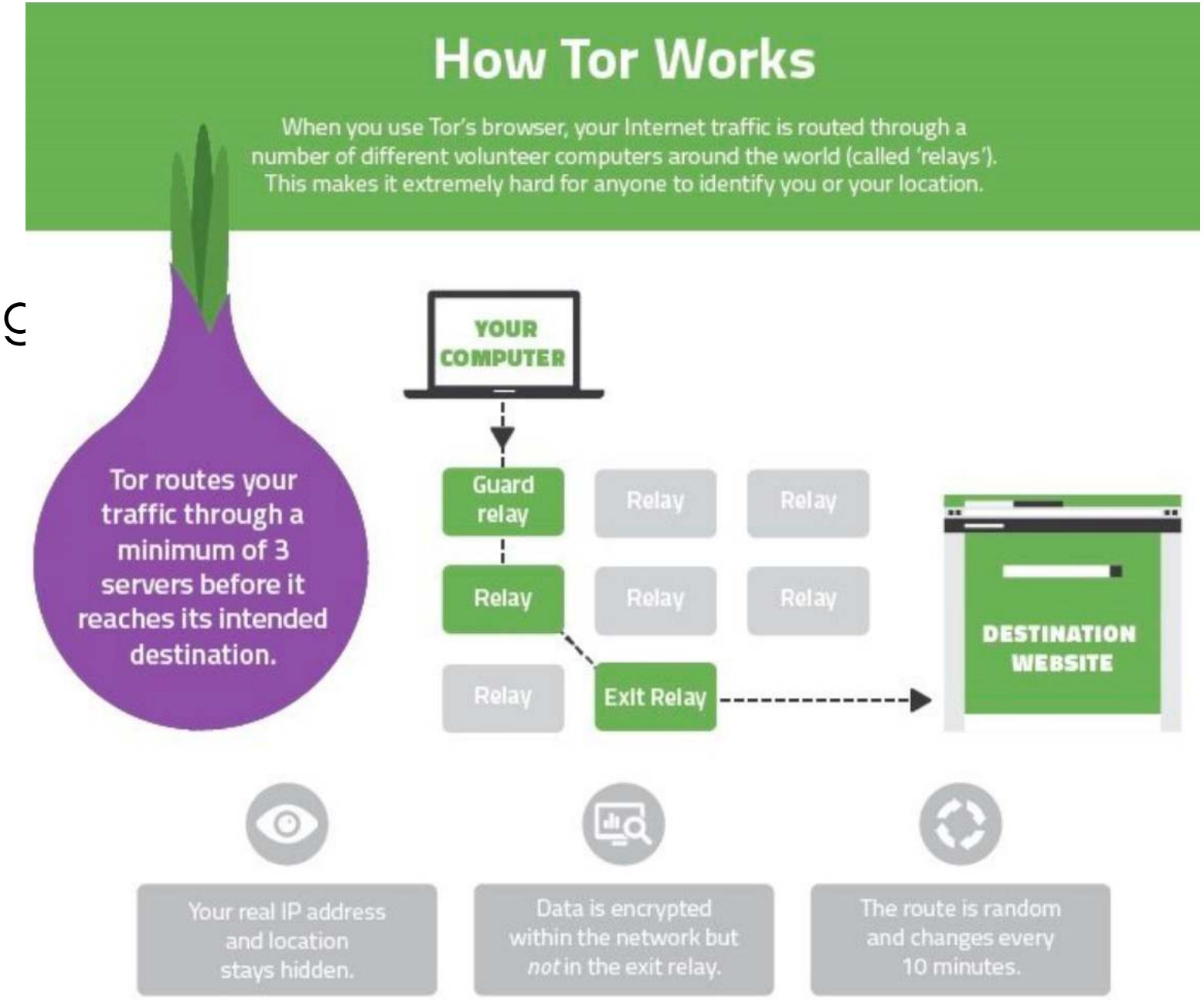

4%
OF WWW
CONTENT
SURFACE WEB
Also known as the 'Visible Web', it is content that can be found using search engines such as Google or Yahoo. It is under constant surveillance by the government.
96%
OF WWW
CONTENT
DEEP WEB
Also known as the 'Invisible Web', it is the content that cannot be indexed by 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

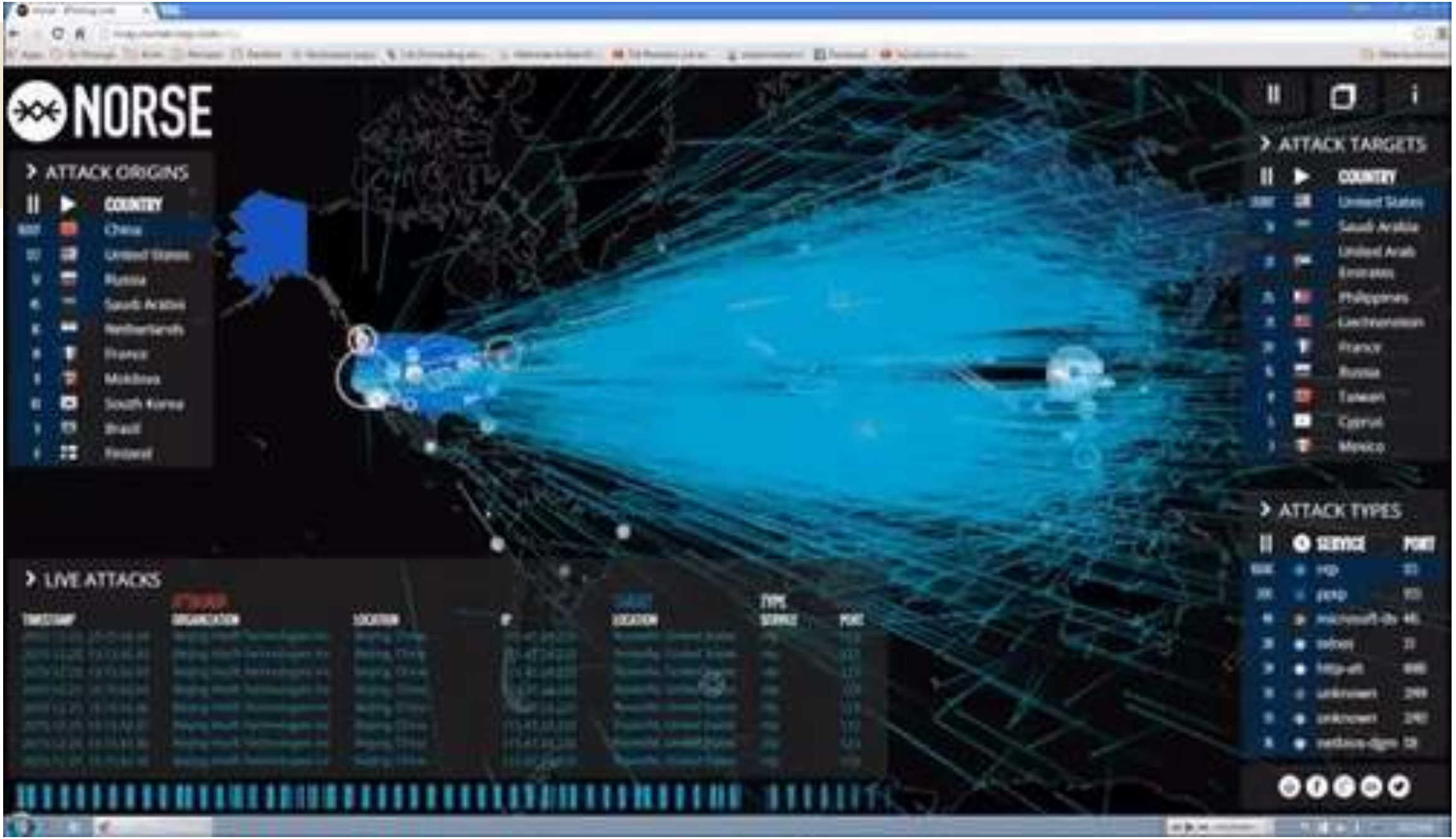
PROFESSIONAL **HACK GROUP** QUICKLY HELPS TO SOLVE YOUR NEEDS

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


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
ORGANIZATION
LOCATION
IP
LOCATION
TYPE
SERVICE
PORT


DDoS ATTACK
DDOS
Online Service Unavailable


YOU'VE BEEN HACKED!
MacBook Pro


Countermeasures

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	**Admins, plugins, themes, Passwords …** *** webpagetest.org**
Update	EVERYTHING Including server software
Restore a backup	Possible lose of information Possible re-installation of malware

Proactive *measures*


Reduce admins, plugins and themes


Strong Passwords periodically change

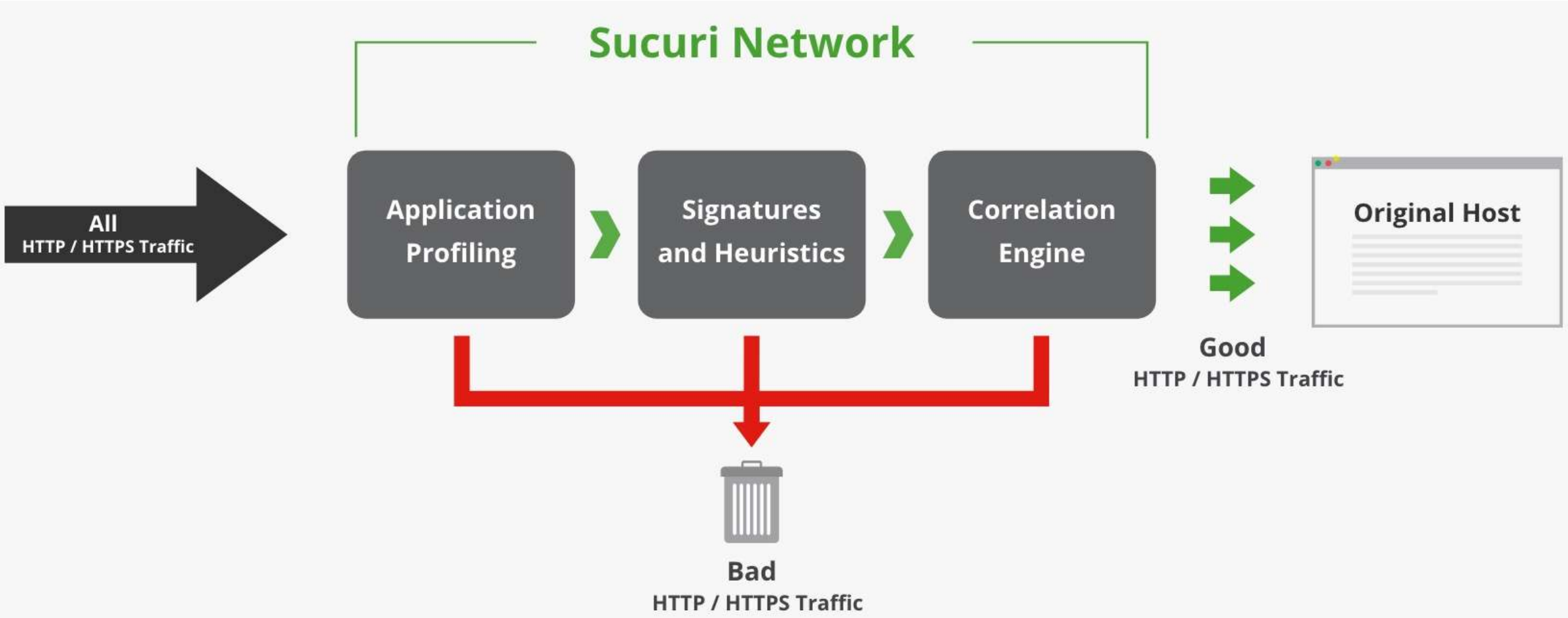

Backups


Updates


Invest in Hosting & Security


WAF (Web Application Firewall)

AI against AI - E.g: ***WAFs***




Everybody needs a hacker

THANKS!

QUESTIONS!!

*Nestor Angulo (@**pharar**)*