Fundamentos de Segurança Informática (FSI)

2021/2022 - LEIC

Manuel Barbosa
mbb@fc.up.pt

Aula 1
Introdução

O problema da ciber-segurança

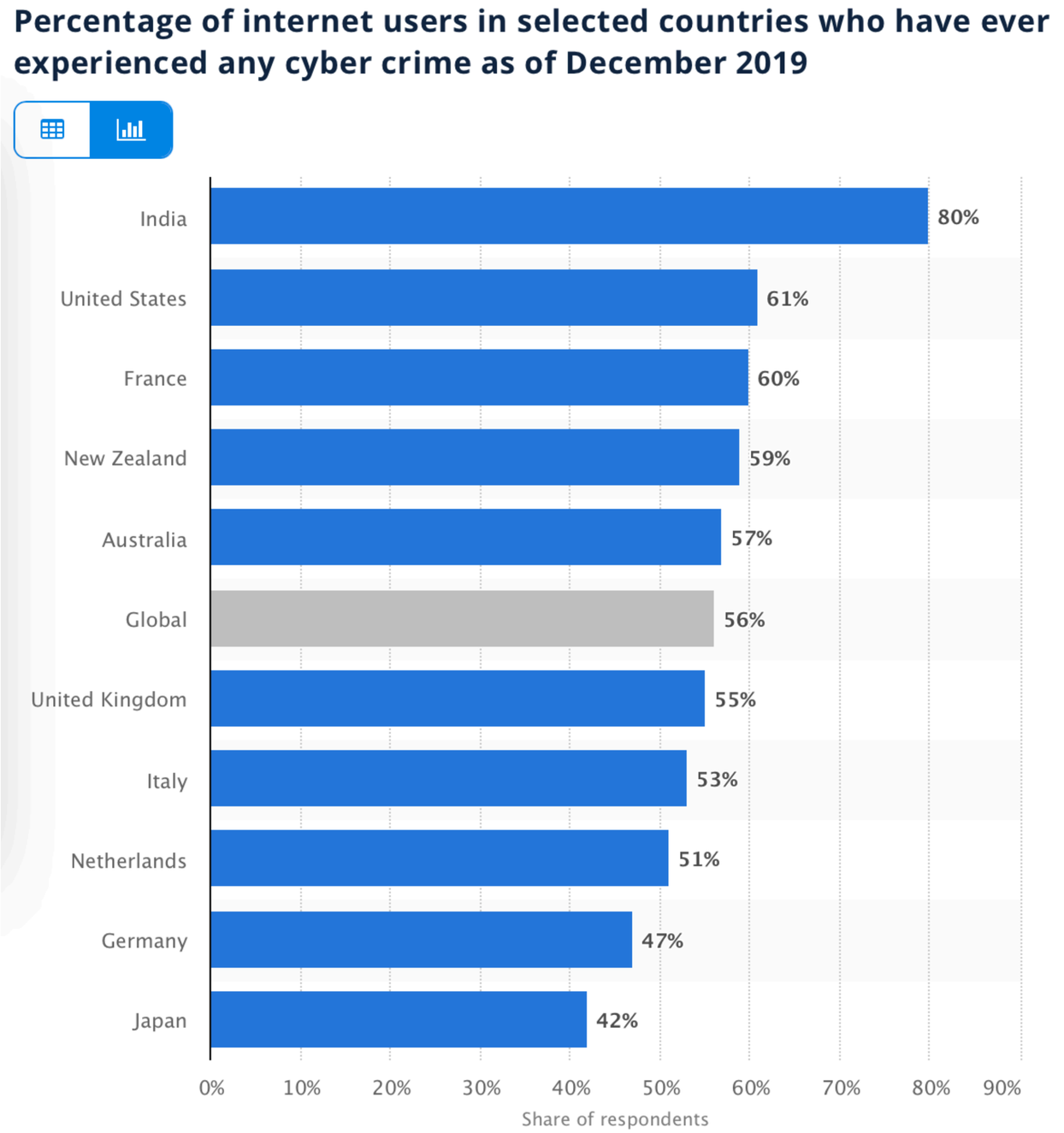
- O software que corremos contém inúmeros erros/bugs
- A engenharia social é extremamente eficaz
- Encontrar e explorar vulnerabilidades é uma atividade lucrativa
  - Enorme mercado para *exploits* (portas de entrada)
  - Enorme mercado para malware (controlo de máquinas comprometidas)
  - Negócio gigantesco à volta da utilização de ambos

Top 50 Products By Total Number Of "Distinct" Vulnerabilities

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Debian Linux	Debian	OS	5069
2	Android	Google	OS	3607
3	Ubuntu Linux	Canonical	OS	2971
4	Mac Os X	Apple	OS	2759
5	Linux Kernel	Linux	OS	2659
6	Iphone Os	Apple	OS	2300
7	Windows 10	Microsoft	OS	2239
8	Chrome	Google	Application	2153
9	Windows Server 2016	Microsoft	OS	2000
10	Windows Server 2008	Microsoft	OS	1962

https://www.cvedetails.com/top-50-products.php?year=2021

O problema é global



https://www.statista.com/statistics/194133/cybercrime-rate-in-selected-countries/

Porquê comprometer a máquina de um utilizador?

- Razão #1:
  - credenciais: roubar passwords bancárias, empresariais, para jogos

Trojan.Silentbanker.B Description

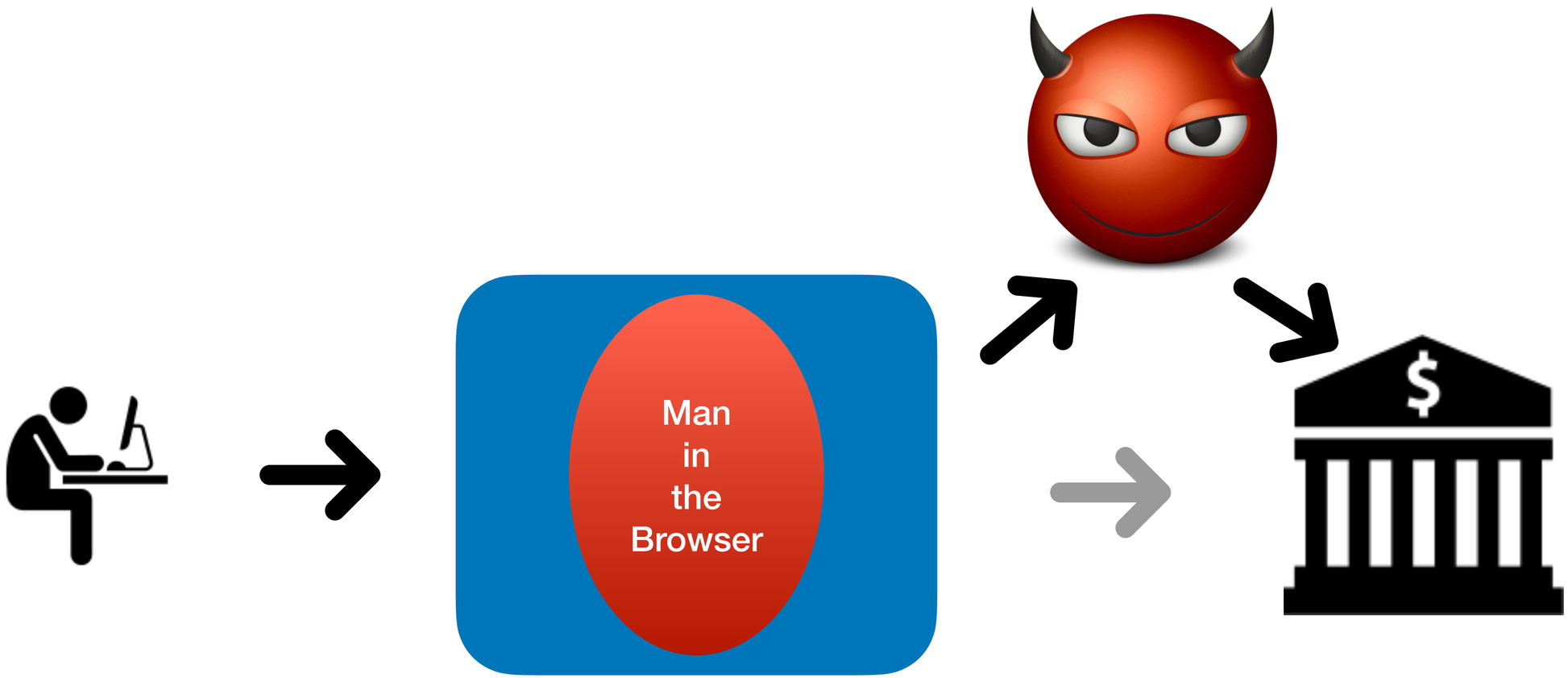
[fonte: microsoft]

Type: Trojan

Trojan.Silentbanker.B is an evolved Trojan parasite that is designed to secretly infect a computer in its efforts to seek out and steal online banking login information. Trojan.Silentbanker.B uses various methods to steal financial data from the hard drive of an infected PC and then send the information to a remote hacker. Trojan.Silentbanker.B may also reduce the performance of an infected computer to the point that the administrator no longer has full control. It is essential that an infection as dangerous as Trojan.Silentbanker.B is removed at once.

Porquê comprometer a máquina de um utilizador?

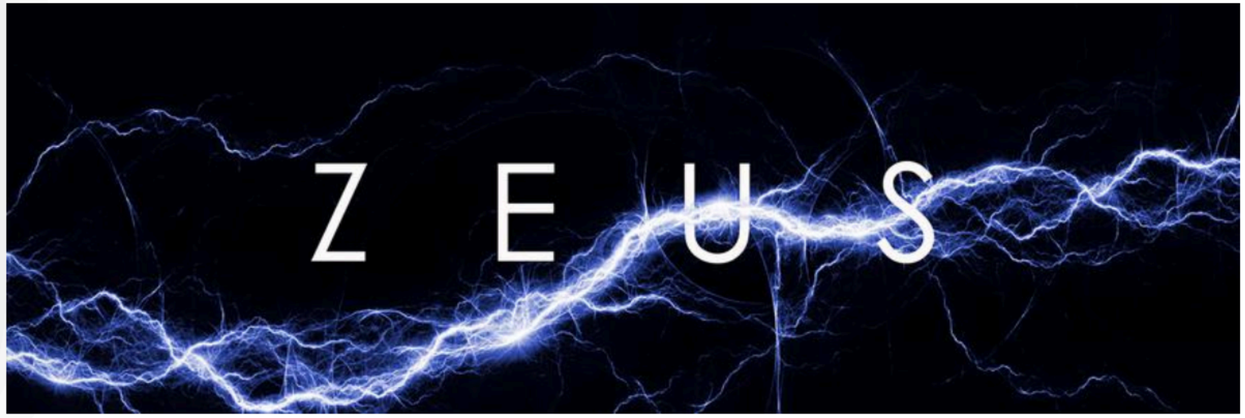
- Razão #1:
  - credenciais: roubar passwords bancárias, empresariais, para jogos



Threat Spotlight: ZeuS (aka Zbot) Infostealer Trojan

RESEARCH & INTELLIGENCE / 04.29.20 / T.J. O'Leary

This completes the infection process. The target PC is now an active member of a ZeuS botnet and will execute any script commands sent by the botnets master. The infected processes will perform web injects by hooking the Windows API functions responsible for sending and receiving HTTP(S) data, Unsuspecting users will provide confidential information which Zeus then sends to the configured C2 or drop server.



Threat Spotlight: ZeuS (aka Zbot) Infostealer Trojan

ZeuS (aka Zbot) is an infamous and successful information stealing Trojan. First detected in 2007, the malware's primary focus is stealing financial/banking information and user credentials from individuals and organizations. Its exploits resulted in the theft of billions of dollars on a global scale[1]. ZeuS crimeware kits vary in complexity with costs ranging from free to several thousand dollars (for later versions with added functionality)[2].

Spyware financeiro

Banking Trojans:
A Reference Guide to the Malware Family Tree

ZEUS

Continuously spawning variants, legacy Zeus is known to grab user credentials, alter webpage forms, and redirect to fake sites. The latest variant generates income through a pay-per-click model.

GOZI

Logging keystrokes, old-school Gozi steals users' login credentials and redirects users to fake websites to hijack banking transactions. It's known for its evasion techniques.

CARBERP

With ties to organized crime, Carberp logs keystrokes, hides instances of itself, and spoofs banking websites, all intending to steal users' banking credentials and money.

SPYEYE

SpyEye targeted Windows users running some of the most popular web browsers. It tried to kill Zeus and stole users' credentials.

* Absorbed Zeus code when Zeus author retired.

SHYLOCK

This Merchant of Venice captured users' online banking credentials and then tricked them into transferring funds to attacker-controlled accounts.

TINBA

As the smallest banking trojan known (20 KB), Tinba uses web-injects and typically runs geo-specific campaigns.

* Shared nearly identical webinjects with Gozi.

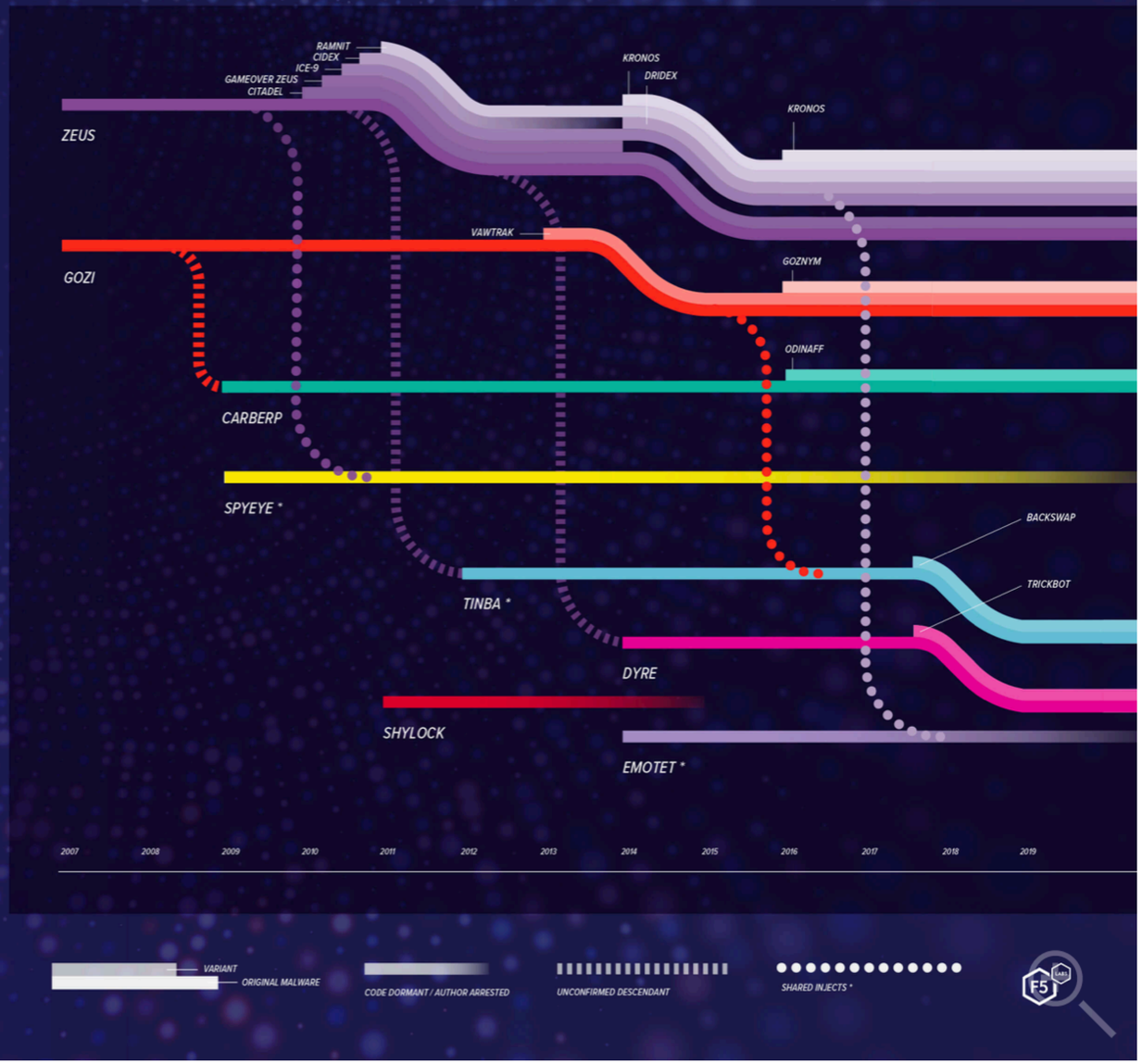
DYRE

The first to use completely fake login pages, server-side web-injects, and a modular architecture, Dyre was also known for its unique fraud techniques, crypto evolution, and stealth capabilities.

EMOTET

Emotet began as a banking trojan and later incorporated malware delivery services that enabled it to install other banking trojans.

* Drops Dridex as a payload.



https://www.f5.com/labs/articles/education/banking-trojans-a-reference-guide-to-the-malware-family-tree

amnesty.org

Jornais Bancos Teaching Research ePrint Google Rust Colib

German-made FinSpy spyware found in Egypt, and Mac and Linux versions revealed

25 September 2020, 12:00 UTC

Summary:

- FinSpy is a commercial spyware suite produced by the Munich-based company FinFisher Gmbh. Since 2011 researchers have documented numerous cases of targeting of Human Rights Defenders (HRDs) - including activists, journalists, and dissidents with the use of FinSpy in many countries, including Bahrain, Ethiopia, UAE, and more. Because of this, Amnesty International's Security Lab tracks FinSpy usage and development as part of our continuous monitoring of digital threats to Human Rights Defenders.

FinFisher

From Wikipedia, the free encyclopedia

FinFisher, also known as **FinSpy**,[1] is surveillance software marketed by Lench IT Solutions plc, which markets the spyware through law enforcement channels.[1]

Suspected FinFisher government users that were active at some point in 2015.

Também para mobile, e disponível no mercado!

Porquê comprometer a máquina de um utilizador?

- Razão #2: ransomware

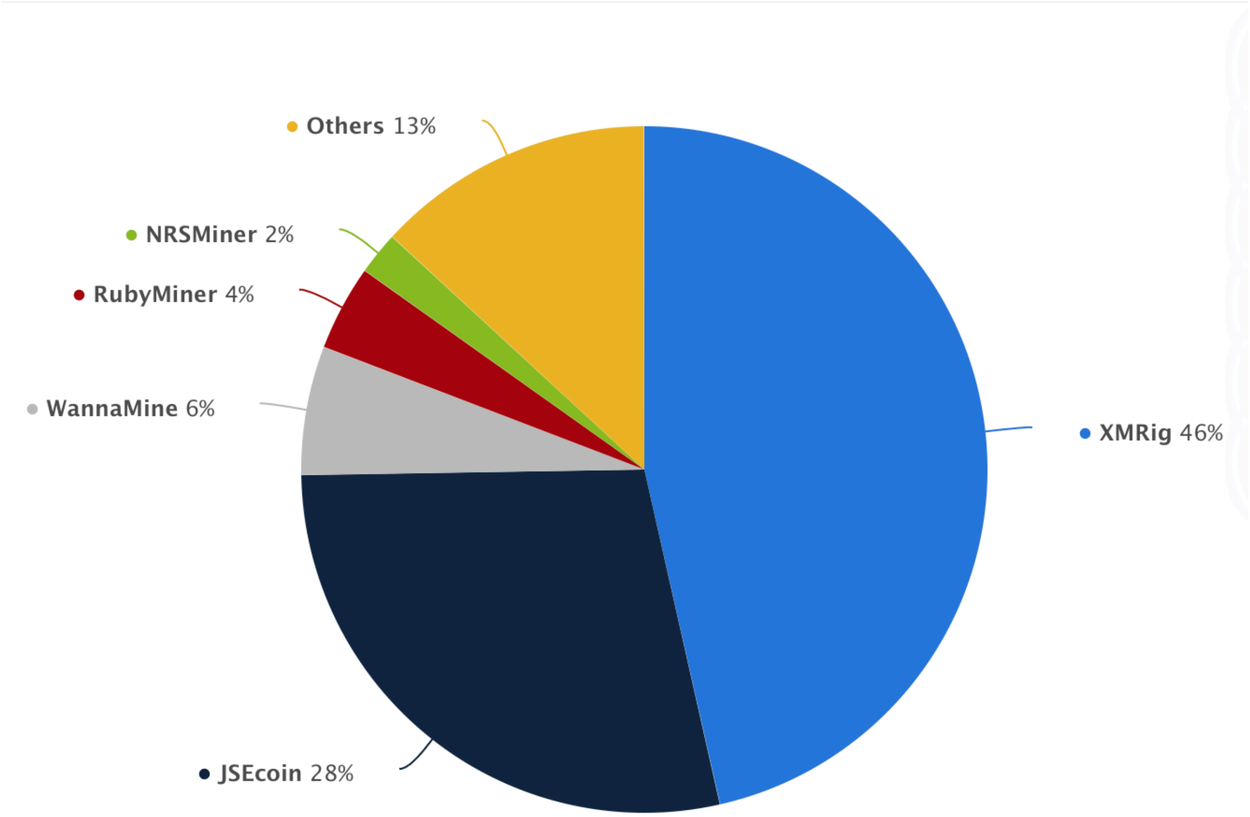
Dia 1: vulnerabilidade utilizada por agências governamentais divulgada

3 semanas depois: Wannacry

Wikipedia

Porquê comprometer a máquina de um utilizador?

- Razão #3:
  - para utilizar o processador => minerar bitcoin



source: statista

Porquê comprometer a máquina de um utilizador?

- Razão #4:
  - para usurpar o endereço de rede e parecer um utilizador normal
    - Spam: o spam funciona (spamalytics)
    - Denial of Service
    - Clicks (e.g., Clickbot.a)
  - Todos estes serviços são vendidos na internet:
    - Para isso é necessário controlar um conjunto de máquinas

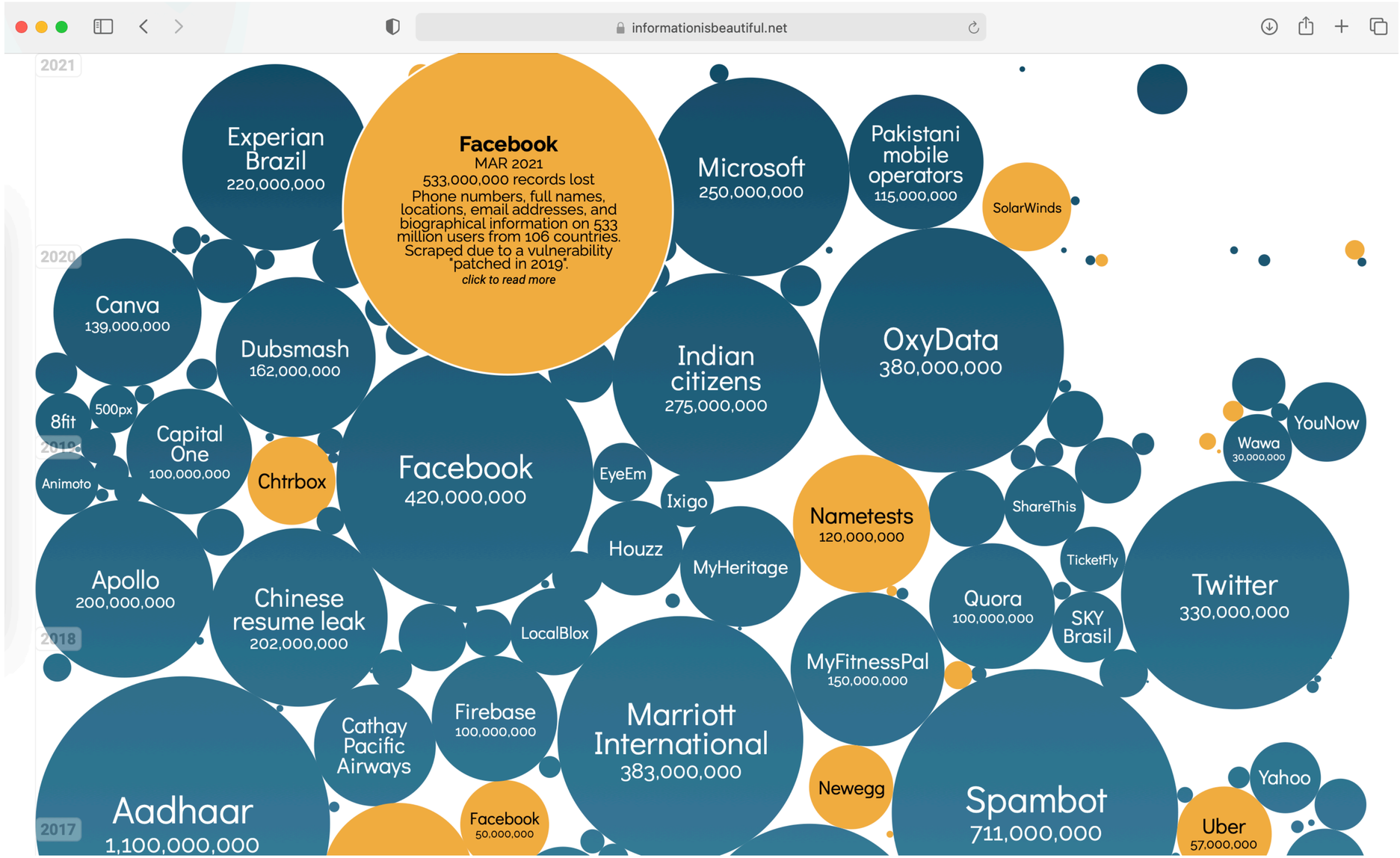
Deloitte estimates that some common criminal businesses can be operated for as little as $34 month and could return $25,000, while others may routinely require nearly $3,800 a month and could return up to $1 million per month.

https://www.csoonline.com/article/3340049/how-much-does-it-cost-to-launch-a-cyberattack.html

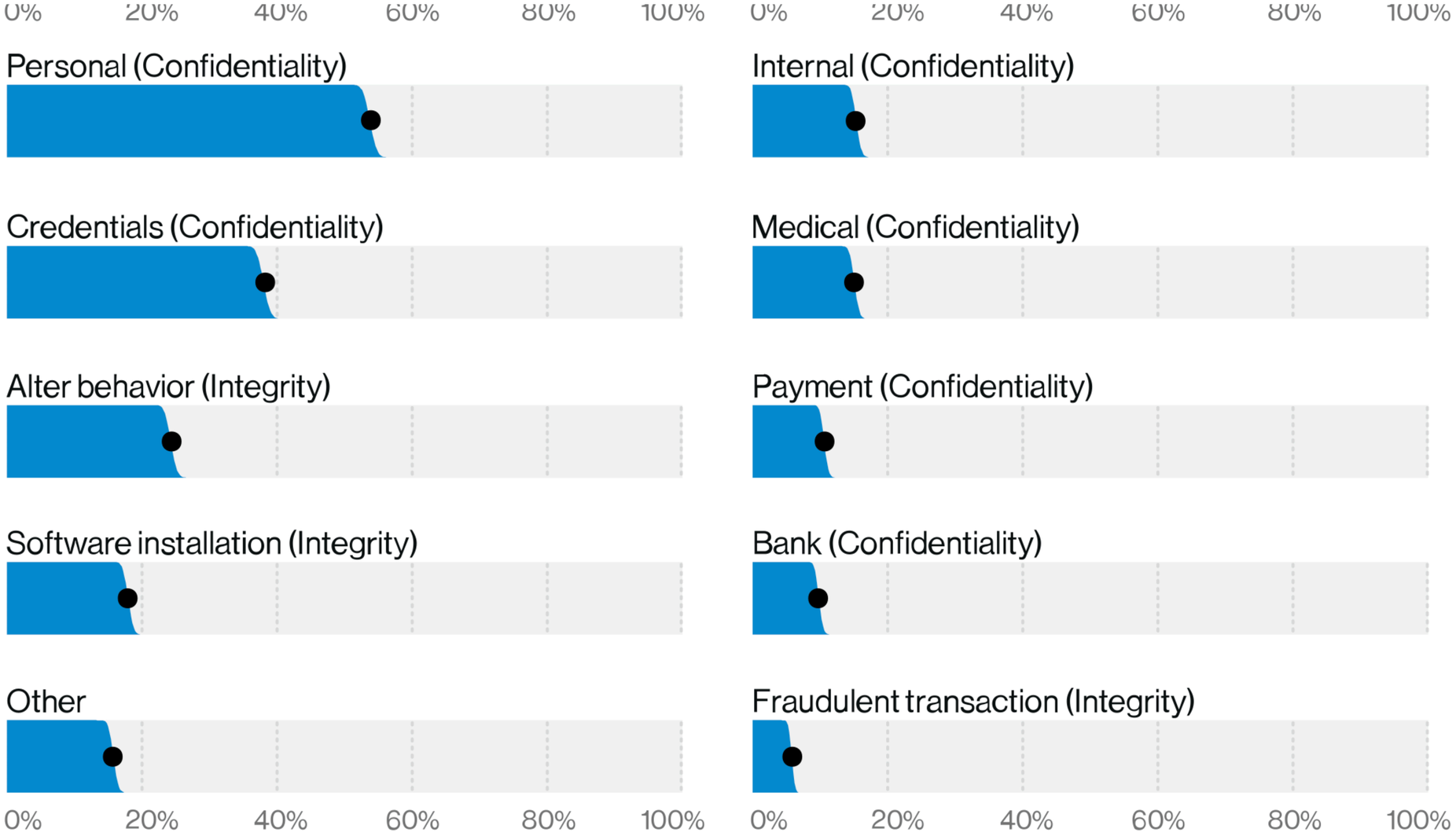
Porquê comprometer servidores?

- Data breaches
  - Números de cartão de crédito e credenciais de utilizadores
    https://en.wikipedia.org/wiki/List_of_data_breaches
- Motivações políticas e geo-estratégicas
    - DNC, Infra-estrutura elétrica na Ucrânia, Stuxnet
- Para depois infetar as máquinas dos utilizadores:
  - supply-chain attacks (infetar servidor que distribui software)
  - web-server attacks (infetar servidor web, que depois compromete browsers)

Data Breaches



Data Breaches: Consequências



Fonte: Verizon

Motivações políticas

December 2015 Ukraine power grid cyberattack

From Wikipedia, the free encyclopedia

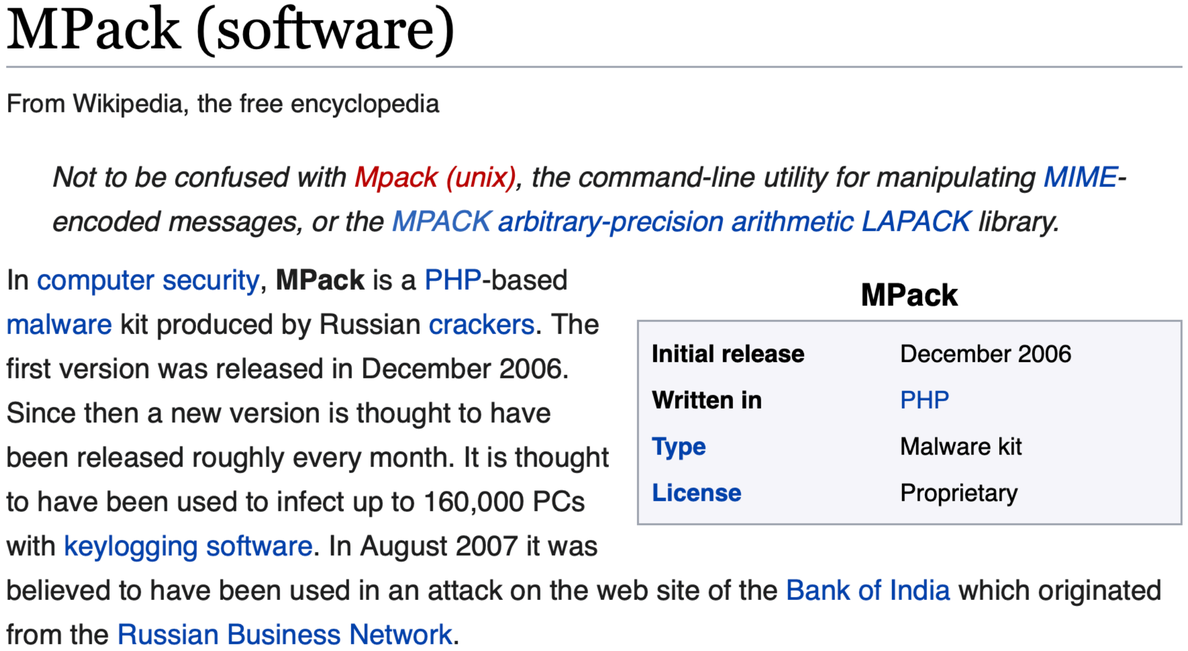
On 23 December 2015, hackers compromised information systems of three energy distribution companies in Ukraine and temporarily disrupted the electricity supply to consumers. It is the first known successful cyberattack on a power grid.

The **Democratic National Committee cyber attacks** took place in 2015 and 2016, in which Russian computer hackers infiltrated the Democratic National Committee (DNC) computer network, leading to a data breach. Cybersecurity experts, as well as the U.S. government, determined that the cyberespionage was the work of Russian intelligence agencies.

Stuxnet, discovered by Sergey Ulasen, initially spread via Microsoft Windows, and targeted Siemens industrial control systems. While it is not the first time that hackers have targeted industrial systems,[25] nor the first publicly known intentional act of cyberwarfare to be implemented, it is the first discovered malware that spies on and subverts industrial systems,[26] and the first to include a programmable logic controller (PLC) rootkit.[27][28]

Comprometer utilizadores

- Servidores que distribuem software permitem disseminar *malware*:
  - Exemplo: SolarWinds, ferramentas de monitorização
- Servidores Web permitem comprometer browsers vulneráveis:
  - Exemplo: MPack conjunto de ferramentas server side para esse fim



Basta um erro para comprometer qualquer sistema
(e alguém vai encontra-lo)

BugBounties: Valores documentados em $

Intel	500	30000
Yahoo		15000
Snapchat	2000	15000
Cisco	100	2500
Dropbox	12167	32768
Apple		100000
Facebook	500	
Google	300	31337
Mozilla	500	5000
Microsoft	15000	25000

What is Zerodium?

Zerodium is the world's leading exploit acquisition platform for premium zero-days and advanced cybersecurity research.

Founded in 2015 by cybersecurity veterans with unparalleled experience in zero-day research and exploitation, Zerodium is now a global community of independent security researchers working together to provide the most powerful cybersecurity capabilities to institutional customers.

Zerodium pays the highest bounties in the market to reward researchers and acquire their zero-day discoveries. We believe that this is the only way to support the zero-day research community and capture the most advanced and innovative research from all around the world.

What is the difference between ZERODIUM and other bug bounty programs?

How is the acquired security research used by Zerodium?

Who are Zerodium's customers?

Zerodium customers are government organizations (mainly from Europe and North America) in need of advanced zero-day exploits and cybersecurity capabilities.

At Zerodium we take ethics very seriously and we choose our customers very carefully through a very strict due diligence and vetting process. Access to acquired zero-day research is highly restricted and is limited to a very small number of government clients.

Furthermore, Zerodium does not have any sales partners or resellers, meaning that our solutions are only available through our direct sales channel.

Como garantimos segurança?

“Segurança”?

- Uma definição comum
  - “A propriedade de um sistema que se comporta como esperado”
- Esta definição não diz o que o sistema deve ou não deve fazer:
  - Não existe uma definição universal ou teste

“Computer security, cybersecurity or information technology security (IT security) is the **protection of computer systems and networks** from **information disclosure**, **theft** of or **damage** to their **hardware**, **software**, or **electronic data**, as well as from the **disruption** or **misdirection** of the services they provide.”

–Wikipedia

“System that remains dependable in the face of malice”

–Ross Anderson

Uma forma de pensar diferente

- A segurança é relativa
  - “Segurança” só por si não significa nada
  - A segurança depende de quem a define
- A segurança muda consoante o contexto
  - Tudo, inclusivamente a terminologia usada, depende da aplicação concreta
- A segurança é defensiva
  - Define-se pela negativa: tudo o que não é bom não pode acontecer
  - Muito mais difícil do que garantir que algo específico acontece

Um exemplo absurdo

- Este sistema é "seguro" quando:
  - O objetivo de segurança é impedir que um automóvel passe na estrada com a cancela?

Atores

- Atores ou participantes são entidades que intervêm no sistema:
  - Pessoas, organizações, empresas, máquinas, …
  - A segurança define-se do ponto de vista destes atores
- Muitas vezes deposita-se confiança em alguns atores/componentes
  - e.g., Trusted Third Party (TTP), Trusted Agent (TA)
  - Sistema "seguro" **se** pressuposto de confiança se verificar (senão?)
- Noutras os atores são potenciais atacantes (externos/internos)

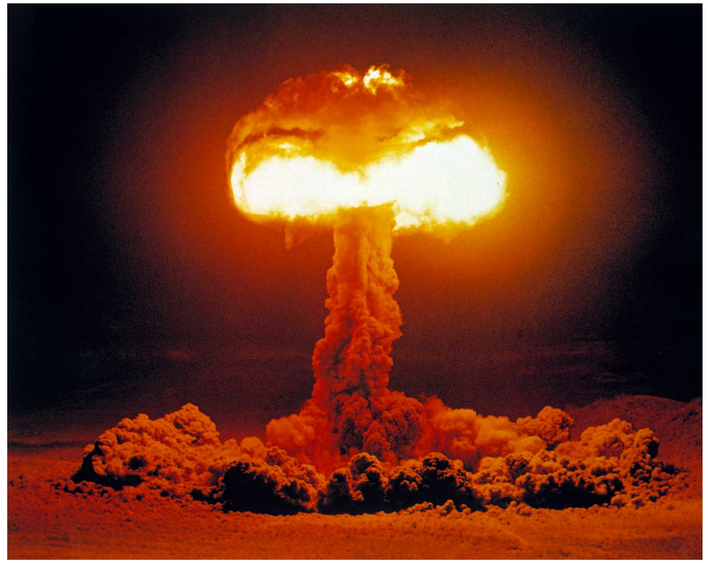
Adversário/Atacante

- Na segurança informática analisamos o comportamento de sistemas quando interagem com adversários/atacantes:

- Atores com intenção explícita de utilizar o sistema/recursos de forma indevida ou de impossibilitar a sua utilização

Adversário/Atacante

- Nenhum sistema é seguro contra todos os adversários



Adversário/Atacante

- É crítico conhecer o nosso adversário (motivação, capacidades, acesso):
  - Script-kiddies (curiosos mas incapazes)
  - Atacantes ocasionais que visam compreender os sistemas
  - Pessoas com intenção de causar danos/destruição
  - Grupos organizados e tecnicamente sofisticados (e.g., ciber crime)
  - Competidores (espionagem industrial)
  - Países/Estados/Governos

Adversário/Atacante

- É preciso pensar como um adversário/ atacante:
  - Procurar sempre o elo mais fraco
  - Identificar pressupostos de confiança subjacentes à segurança
    - São válidos?
  - Olhar para o sistema "out of the box"
    - Quem desenha um sistema está sempre "preso" ao que ele é suposto fazer