Security Fundamentals Informatics (FSI)

2022/2023 - LEIC

Manuel Barbosa
mbb@fc.up.pt

Hugo Pacheco
hpacheco@fc.up.pt

Class 1
Introduction

Planning*

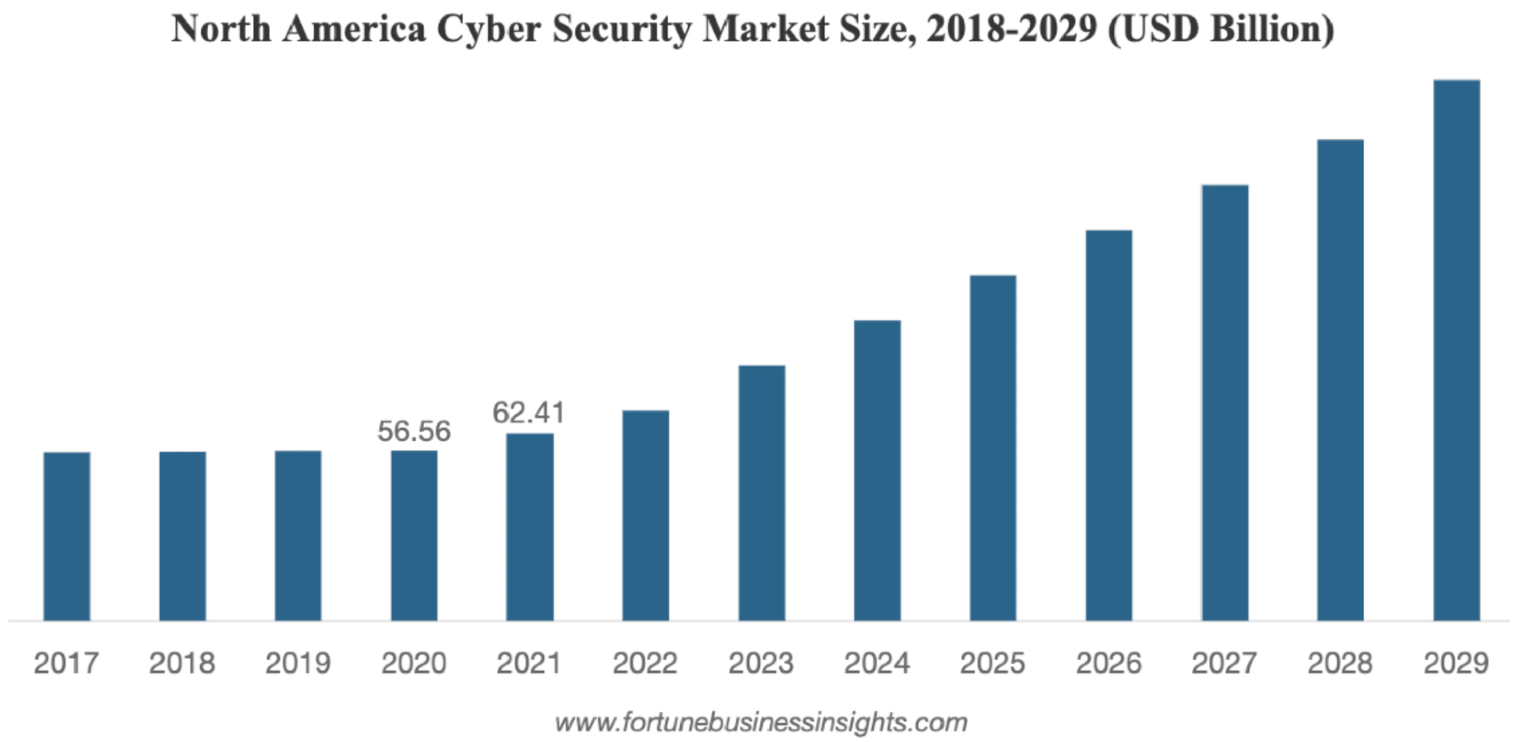
	1	two	3	4	5	6	7	8	9	10	11	12
hpacheco	concepts of Safety		Software Security				Systems Security				Safety web	
mbb	encryption				PKI + Authentication		security of networks			Others		

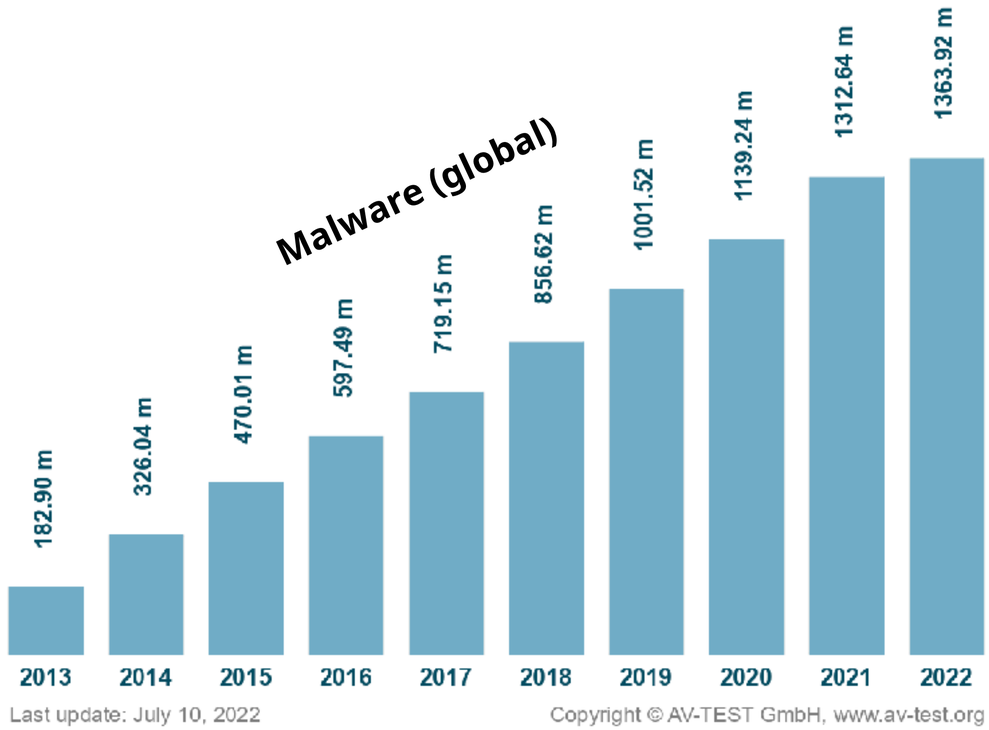
***Subject to adjustments**

The cybersecurity problem

- The software we run contains numerous errors/bugs
- Social engineering is extremely effective
- Finding and Exploiting Vulnerabilities Is a Profitable Activity
  - Huge market for *exploits* (gateways)
  - Huge market for *malware* (control of compromised machines)
  - Huge business around the use of both

security market



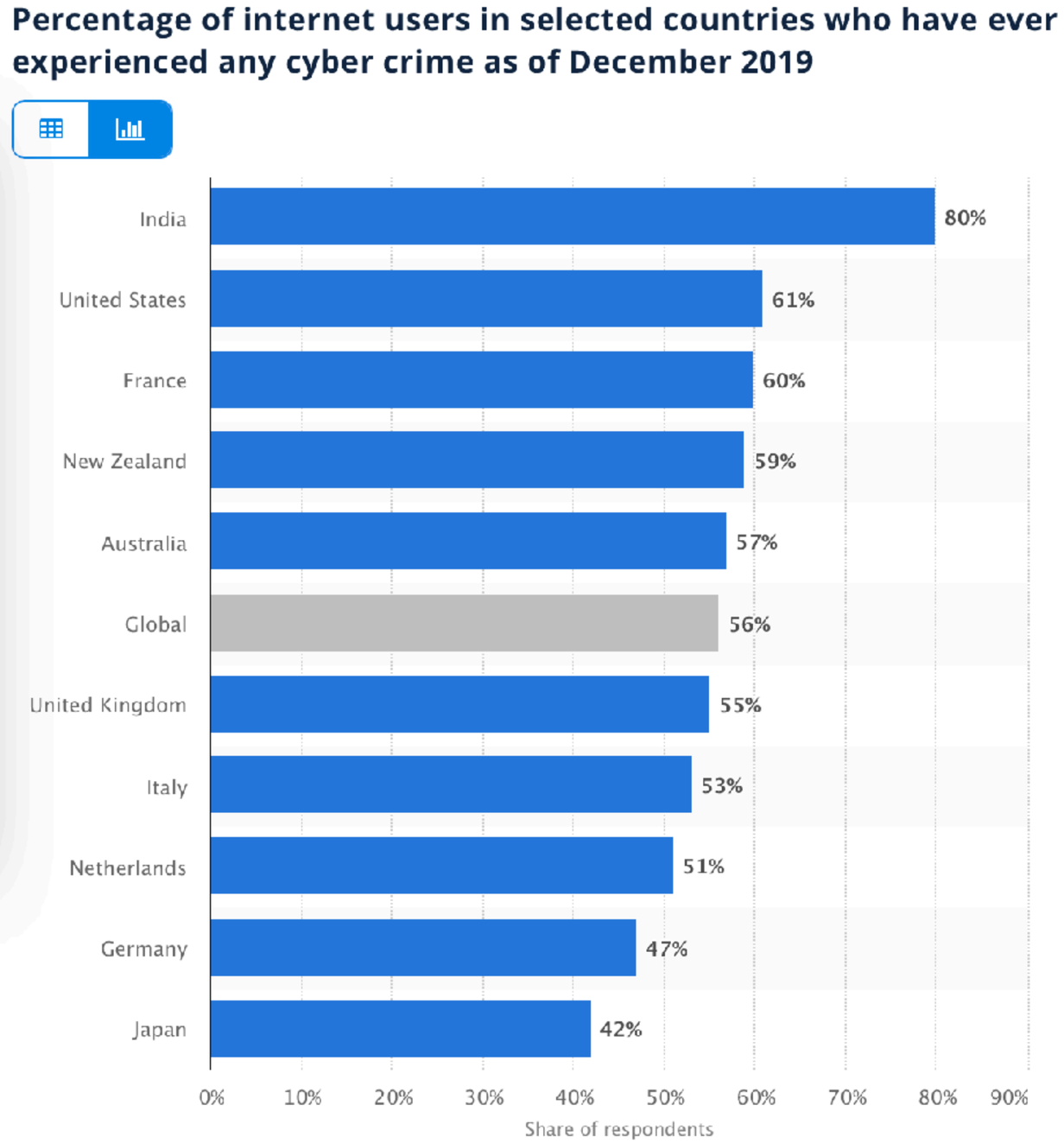


Top 50 Products By Total Number Of "Distinct" Vulnerabilities

	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

The problem is global



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

Even for critical systems?

2008, airplane system that failed to monitor technical problems was infected with malware

Spanair Flight 5022

From Wikipedia, the free encyclopedia

Coordinates: 40°31′48″N 003°34′13″W

Spanair Flight 5022 was a scheduled domestic passenger flight from Barcelona–El Prat Airport to Gran Canaria Airport, Spain, via Madrid–Barajas Airport that crashed just after take-off from runway 36L at Madrid Airport at 14:24 CEST (12:24 UTC) on 20 August 2008. The aircraft was a McDonnell Douglas MD-82, registration EC-HFP. Of the 172 passengers and crew on board, 154 died and 18 survived.[1][2]

Spanair Flight 5022

EC-HFP, the aircraft involved, in July 2008

Accident	
Date	20 August 2008

Malware [edit]

Spanish daily *El País* reported that, as revealed in an internal report issued by Spanair, malware which had infected the airline's central computer system used to monitor technical problems with its aircraft may have resulted in a failure to raise an alarm over multiple problems with the aircraft. A judge ordered the airline to provide all the computer system's logs from the days before and after the crash.[48][49][50]

Vulnerabilities/Threats | 3 MIN READ | NEWS

IoT Malware Discovered Trying to Attack Satellite Systems of Airplanes, Ships

Researcher Ruben Santamarta shared the details of his successful hack of an in-flight airplane Wi-Fi network – and other findings – at Black Hat USA today.

Kelly Jackson Higgins
Editor-in-Chief, Dark Reading

August 10, 2019

BLACK HAT USA – Las Vegas – Ruben Santamarta was flying from Madrid to Copenhagen in November 2017 on a Norwegian Airlines flight when he decided to inspect the plane's Wi-Fi network security. So he launched Wireshark from his laptop and began monitoring the network.

2017, Airplane satellite communications backdoor

https://www.blackhat.com/us-18/briefings/schedule/index.html#last-call-for-satcom-security-11192

2017, Russian spies attempted supply-chain attack on US nuclear power plant

https://www.ans.org/news/article-3818/indictmentrelated-to-wolf-creek-computer-hack-unsealed/

Indictment related to Wolf Creek computer hack unsealed

Mon, Apr 4, 2022, 3:30PM | Nuclear News

The Wolf Creek nuclear power plant. (Photo: Wolf Creek Nuclear Operating Corp.)

Why compromise a user's machine?

- Reason #1:
  - credentials: steal bank, business, gaming passwords

Trojan.Silentbanker.B Description

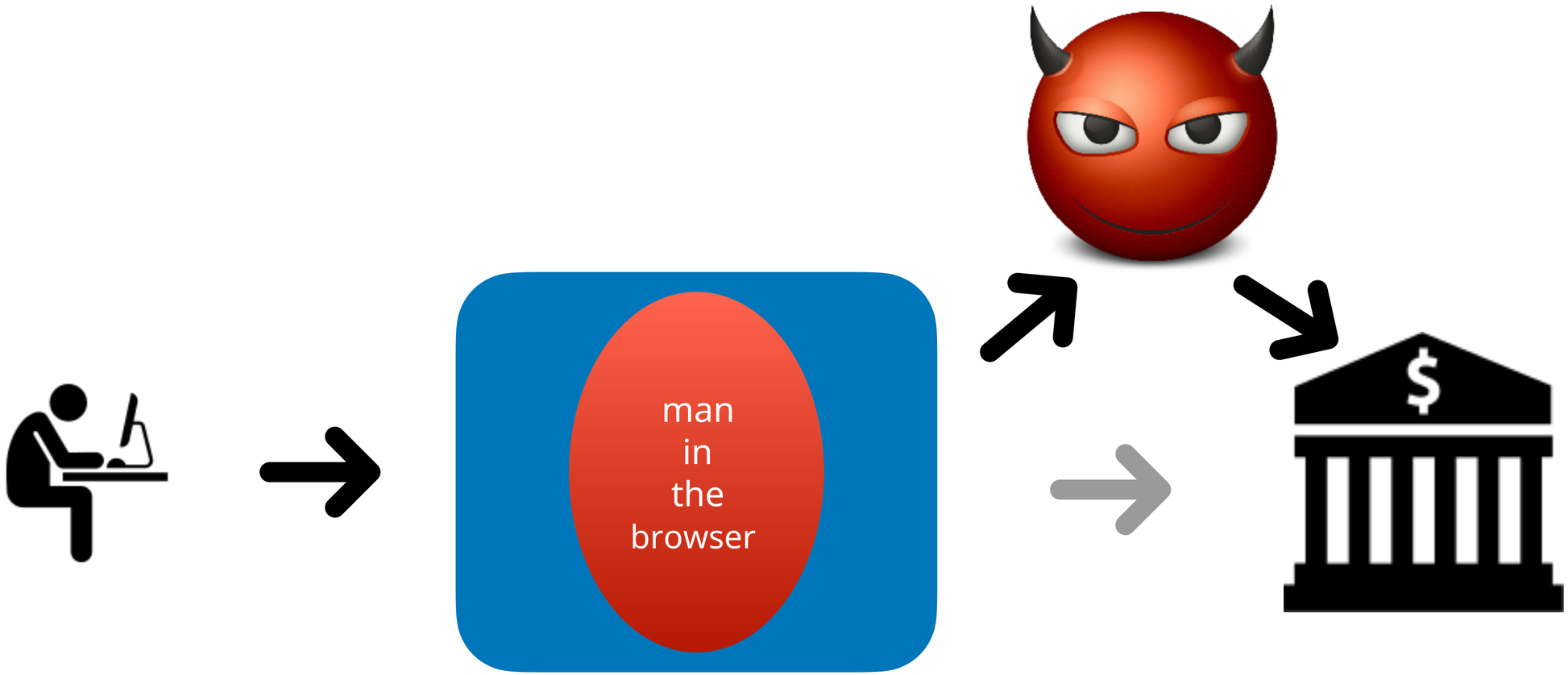
[source: microsoft, 2008]

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.

Why compromise a user's machine?

- Reason #1:
  - credentials: steal bank, business, gaming passwords



Threat Spotlight: ZeuS (aka Zbot) Infostealer Trojan

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

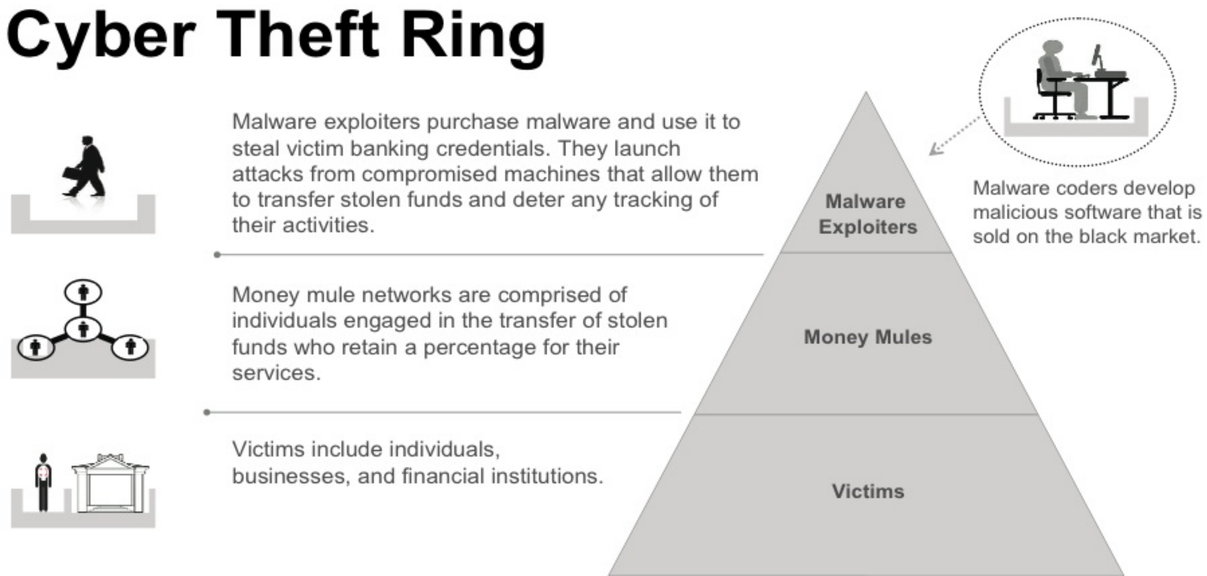
This completes the infection process. The target PC is now an active member of a ZeuS botnet and will execute any script commands sent by the botnets master. The infected processes will perform web injects by hooking the Windows API functions responsible for sending and receiving HTTP(S) data, Unsuspecting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

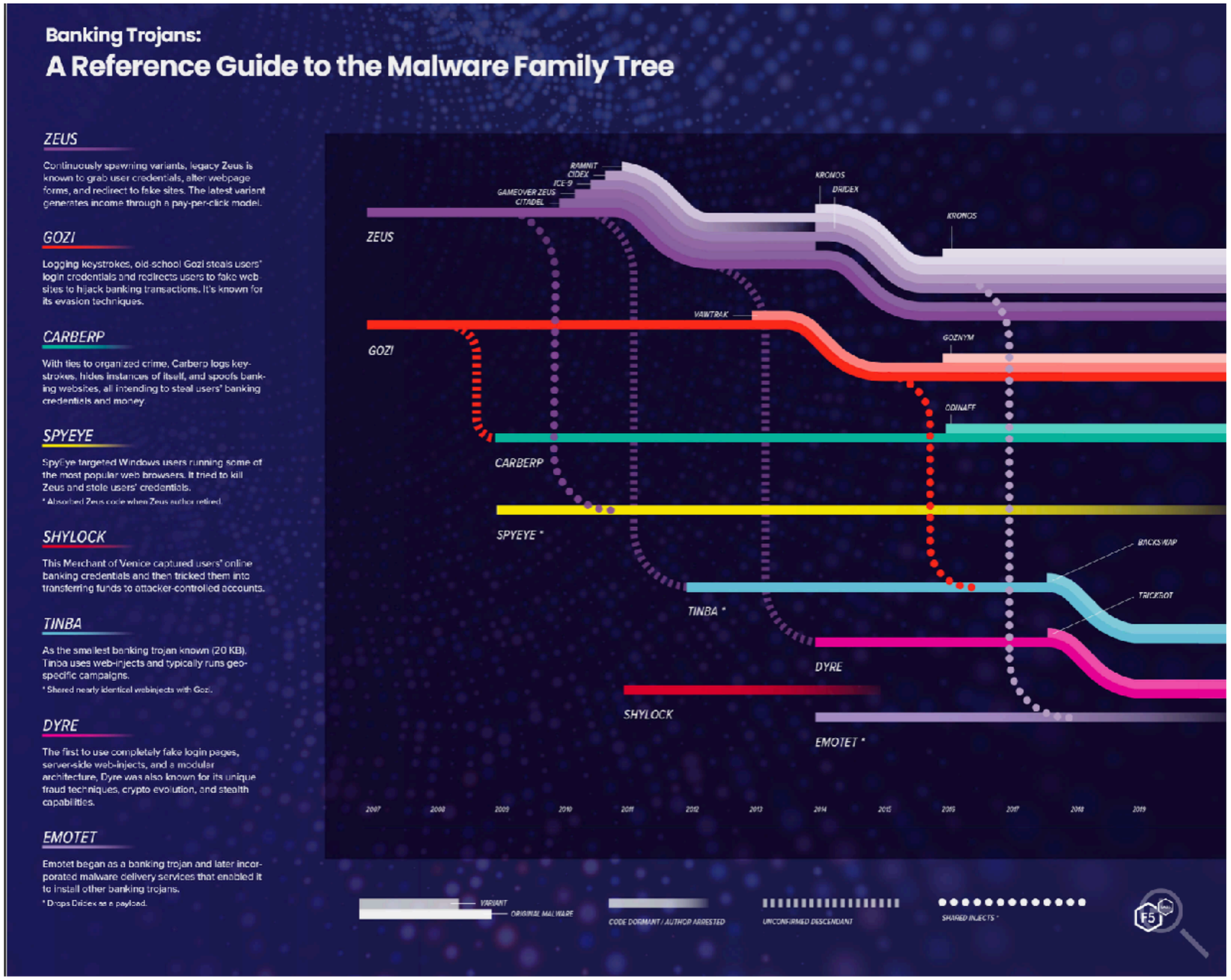
Threat Spotlight: ZeuS (aka Zbot) Infostealer Trojan

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
financial

To date, most internet botnet





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.

Also for mobile, and available on the market!

Pegasus (spyware)

From Wikipedia, the free encyclopedia

Pegasus is spyware developed by the Israeli cyber-arms company NSO Group that can be covertly installed on mobile phones (and other devices) running most[1] versions of iOS and Android.[2] Pegasus is able to exploit iOS versions up to 14.7, through a zero-click exploit.[1] As of 2022, Pegasus was capable of reading text messages, tracking calls, collecting passwords, location tracking, accessing the target device's microphone and camera, and harvesting information from apps.[3][4] The spyware is named after Pegasus, the winged horse of Greek mythology. It is a Trojan horse computer virus that can be sent "flying through the air" to infect cell phones.[5]

Pegasus

Developer(s)	NSO Group
Initial release	August 2016
Operating system	iOS, Android
Type	spyware
Website	nsogroup.com

Pegasus was discovered in August 2016 after a failed installation attempt on the iPhone of a human rights activist led to an investigation revealing details about the spyware, its abilities, and the security vulnerabilities it exploited. News of the spyware caused significant media coverage. It was called the "most sophisticated" smartphone attack ever, and was the first time that a malicious remote exploit used jailbreaking to gain unrestricted access to an iPhone.[6]

The spyware has been used for surveillance of anti-regime activists, journalists, and political leaders from several nations around the world.[7] In July 2021, the investigation initiative Pegasus Project, along with an in-depth analysis by human rights group Amnesty International, reported that Pegasus was still being widely used against high-profile targets.[1]

https://www.youtube.com/watch?v=Pc-rWN-k4Xo

Zero-click exploit!

“Pegasus is designed to infiltrate devices running Android, Blackberry, iOS and Symbianoperating systems and turn them into surveillance devices. The company says it sells Pegasus only to governments and only for the purposes of tracking criminals and terrorists.”

why buy

- Reason #2: ransomware

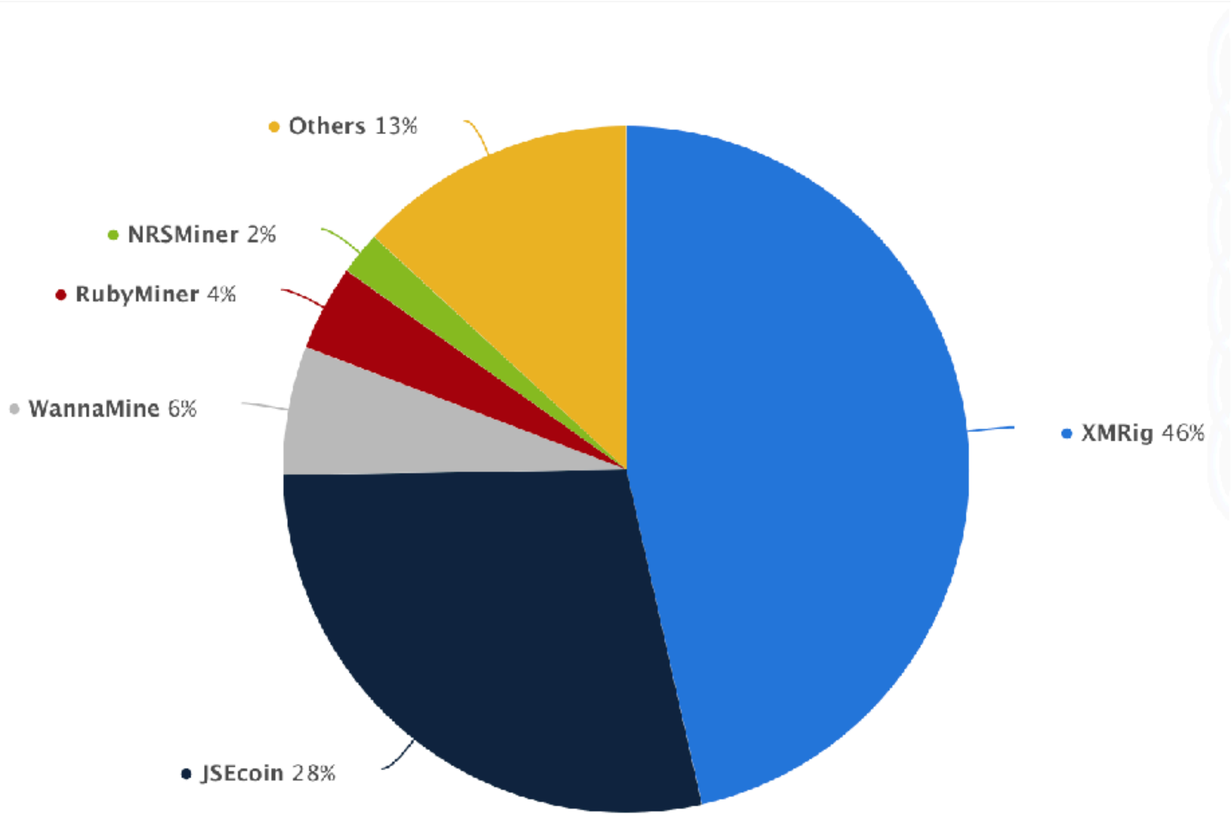
Day 1: vulnerability
used by agencies
governmental disclosed

3 weeks later:
Wannacry

Wikipedia

Why compromise a user's machine?

- Reason #3:
  - to use the processor => mine bitcoin



source: statista

Why compromise a user's machine?

- Reason #4:
  - to usurp the network address and look like a normal user
    - Spam: Spam Works (Spamalytics)
    - Denial of Service
    - Clicks (eg, Clickbot.a)
  - All these services are sold on the internet:
    - For this it is necessary to control a set of machines

‘Nigerian prince’ email scams still rake in over $700,000 a year—here’s how to protect yourself

make it

Published Thu, Apr 18 2019•2:38 PM EDT

Deloitte. Services Industries Insights

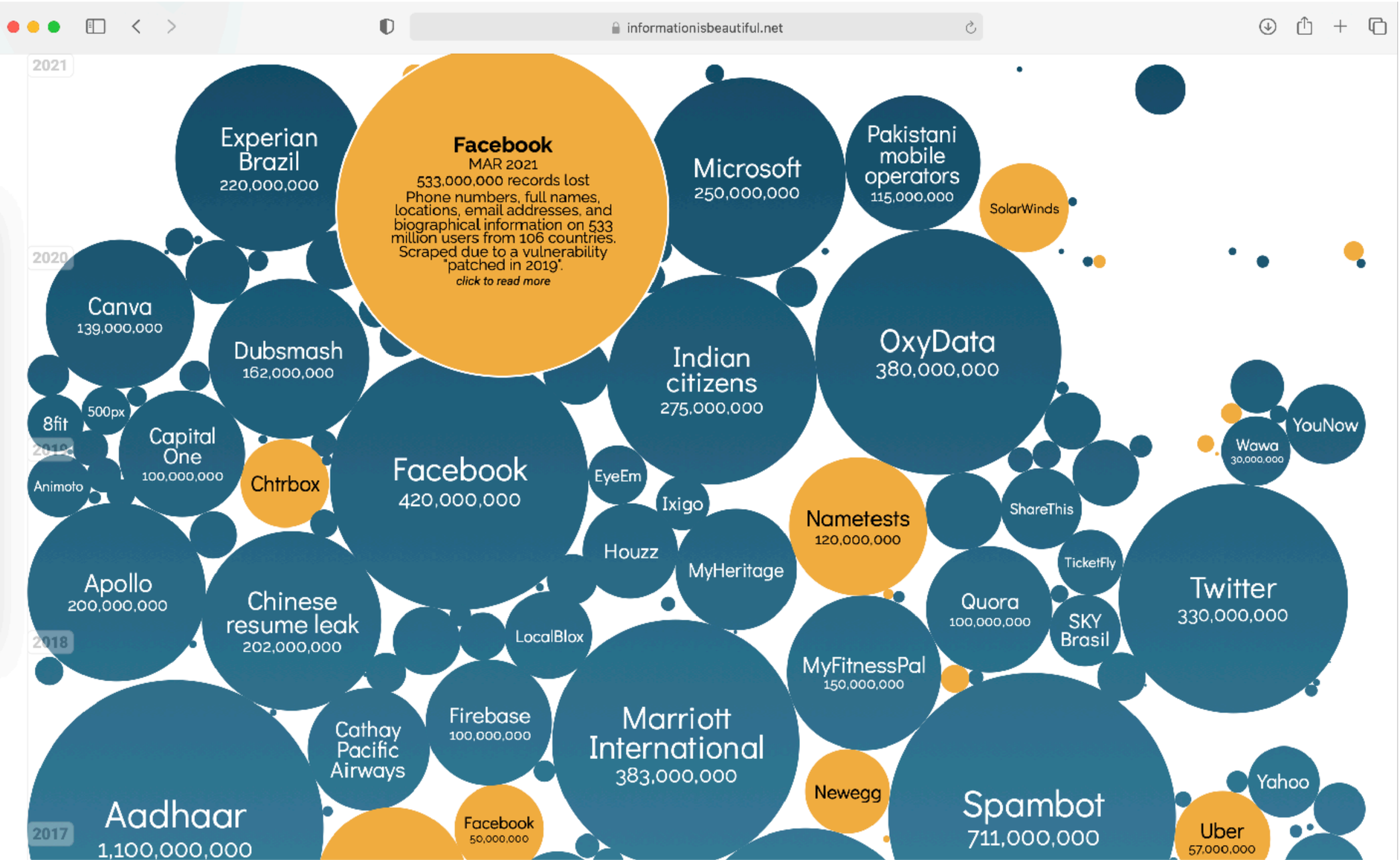
Deloitte estimates that some common criminal businesses can be operated for as little as $34 month and could return $25,000, while others may routinely require nearly $3,800 a month and could return up to $1 million per month. For example, phish kits

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

Why compromise servers?

- data breaches
  - Credit card numbers and user credentials https://en.wikipedia.org/wiki/List_of_data_breaches
- Political and geo-strategic motivations
  - DNC, Electric infrastructure in Ukraine, Stuxnet
- To then infect users' machines:
  - supply-chain attacks (infect server that distributes software)
  - web-server attacks (infect a web server, which later compromises browsers)

Date Breaks



';--have i been pwned?

https://haveibeenpwned.com/

Just these days…

CIBERSEGURANÇA

Vulnerabilidade em plataforma da DGS expôs dados detalhados dos portugueses

Uma vulnerabilidade na plataforma do Sinave permitia extrair informação sobre o NIF, morada, número de telefone, nome e data de nascimento dos cidadãos portugueses sem qualquer tipo de autenticação. Faltam auditorias digitais no Governo, dizem especialistas.

Karla Pequenino

5 de Setembro de 2022, 6:01

O Sinave é a plataforma onde se registam os dados sobre os portugueses infectados com covid-19 RUI GAUDENCIO

CIBERCRIME

Hackers atacam Estado-Maior-General das Forças Armadas e colocam documentos da NATO à venda na internet

O primeiro-ministro, António Costa, alegadamente só soube do caso porque foi informado pelos serviços secretos dos Estados Unidos.

PÚBLICO

8 de Setembro de 2022, 10:11

A NATO já exigiu explicações ao Governo português e, na próxima semana, o secretário de Estado da Digitalização e da Modernização Administrativa e o director do gabinete de segurança nacional vão a Bruxelas para uma reunião na sede da NATO. DANIEL ROCHA

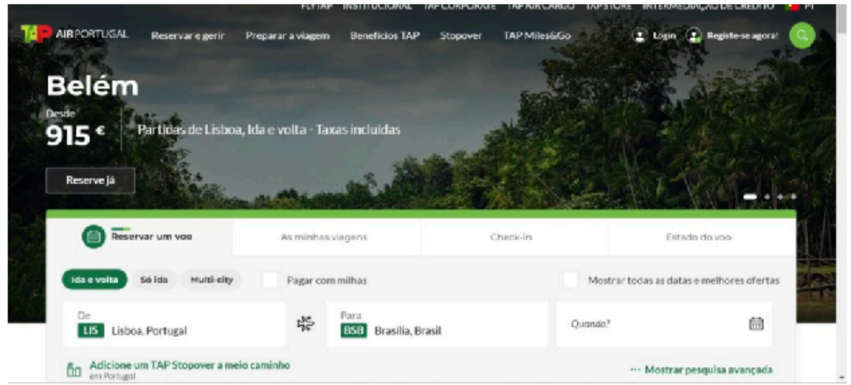
PIRATARIA INFORMÁTICA

Hackers publicam dados de clientes da TAP. Moradas, nomes e telefones entre informação divulgada

Funcionários governamentais podem estar entre os afectados. *Hackers* ameaçam publicar informações de 1,5 milhões de clientes. Empresa diz que dados de pagamento não foram exfiltrados da base de dados.

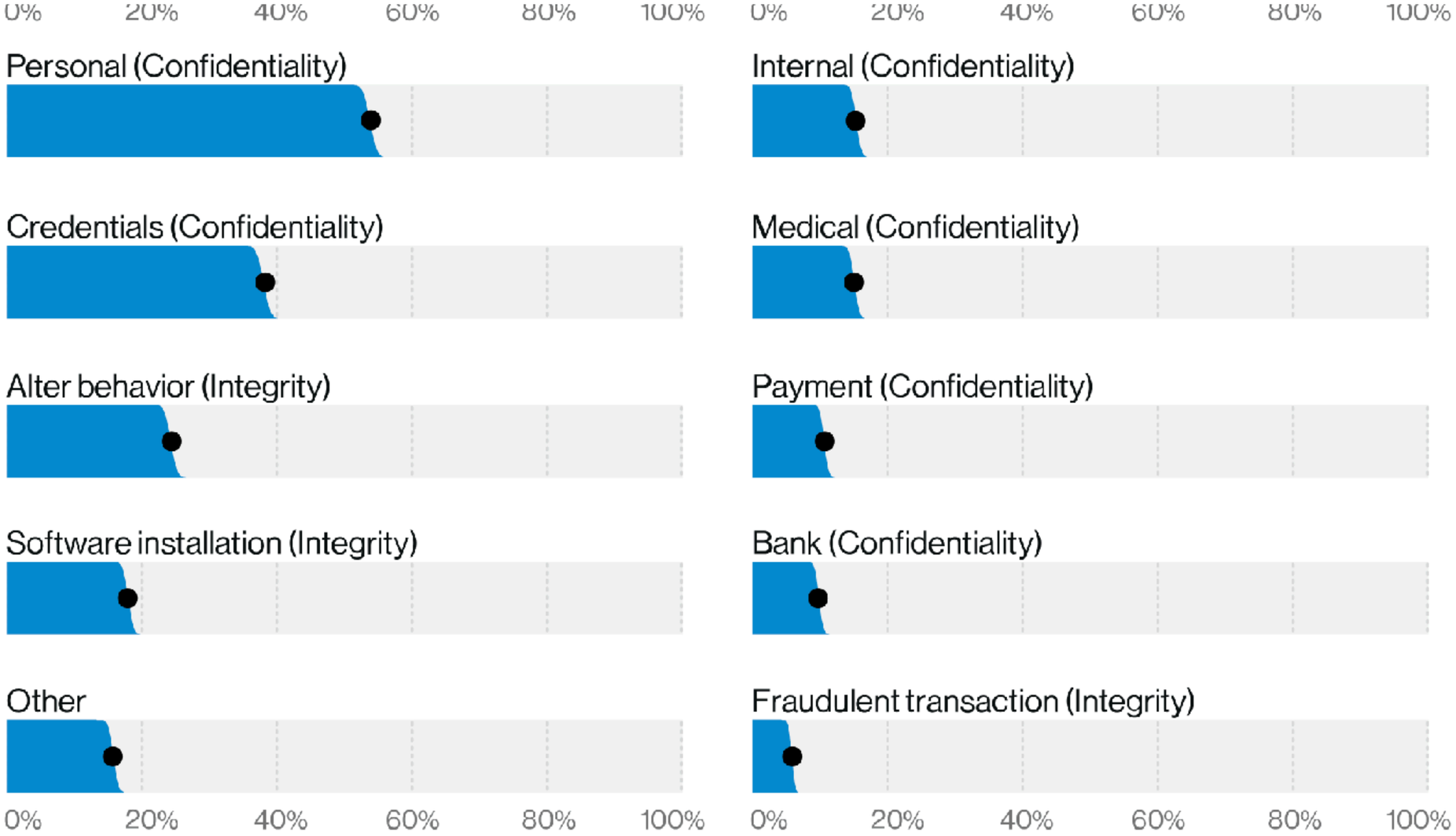
Miguel Dantas e **Rui Barros**

13 de Setembro de 2022, 12:39



Dados foram publicados esta segunda-feira

Data Breaks: Consequences



Source: Verizon

political motivations

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.

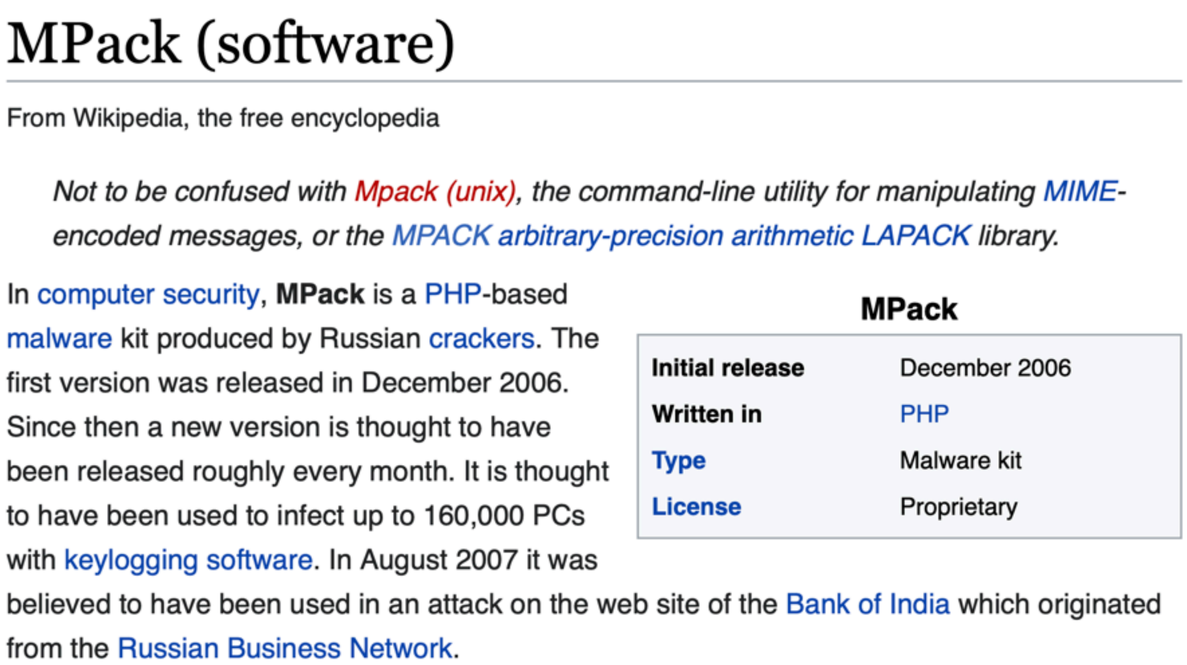
Stuxnet, discovered by Sergey Ulasen, initially spread via Microsoft Windows, and targeted Siemens industrial control systems. While it is not the first time that hackers have targeted industrial systems,[25] nor the first publicly known intentional act of cyberwarfare to be implemented, it is the first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

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.

https://en.wikipedia.org/wiki/Zero_Days

Commit users

- Servers that distribute software allow you to disseminate *malware*:
  - Example: SolarWinds, monitoring tools
- Web servers allow you to compromise vulnerable browsers:
  - Example: MPack
    Server side toolkit for “website defacing”



Commit developers

- One of the simplest attacks is the so-called “squatting type”
- Example: PyPI package manager
  > 300,000 projects
- Supply chain attack:

  Malicious package with similar name

  developer installs the wrong package
- Is it a security issue?

malware	Original
acquisition	**acquisition**
apidev-coop	**apidev-coop_cms**
bzip	**bz2file**
crypt	**crypto**
django-server	**django-server-guardian-api**
pwd	**pwdhash**
setup-tools	**setuptools**
telnet	**telnetsrvlib**
urllib	**urllib3**

Just one mistake to commit
any system
(and someone will find you)

BugBounties: Values documented in $

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.

How do we guarantee security?

"Safety"?

- a common definition
  - “The property of a system that behaves as expected”
- This definition does not say what the system should or should not do:
  - There is no universal definition or test

“Computer security, cybersecurity or information technology security (IT security) is theprotection of computer systems and networksfrom information disclosure, theftof ordamageto theirhardware, software, or electronic data,as well as from thedisruptionormisdirectionof the services they provide.”

– Wikipedia

“Software security is about integrating security practices into the way you build software, not integrating security features into your code”

– Gary McGraw

“System that remains dependable in the face of malice”

– *Ross Anderson*

A different way of thinking

- security is relative
  - “Security” by itself means nothing.
  - Security depends on who defines it
- Security changes depending on the context
  - Everything, including the terminology used, depends on the specific application
- Security is defensive
  - It is defined by the negative: everything that is not good cannot happen
  - Much harder than ensuring that something specific happens

an absurd example

- This system is "safe" when:
  - The security objective is prevent a car from passing on the road with the gate ?

actors

- Actors or participants are entities that intervene in the system:
  - People, organizations, companies, machines, ...
  - Security is defined from the point of view of these actors
- It is often depositedconfidence in some actors/components
  - eg, Trusted Third Party (TTP), Trusted Agent (TA)
  - "Secure" system**if** confidence assumption is verified
    - if no? e.g. defense in depth
- In others the actors are potential attackers (external/internal)

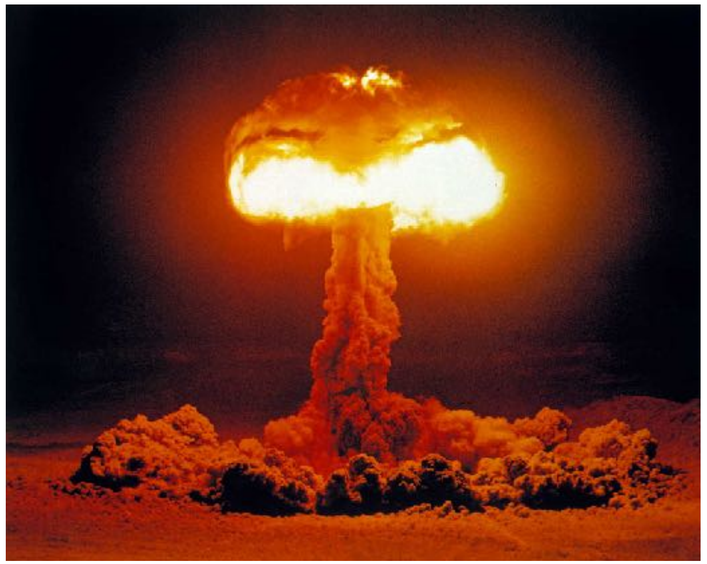
Opponent/Forward

- In computer security, we analyze the behavior of systems when they interact with adversaries/ attackers:

- Actors with an explicit intention to misuse the system/resources or to make their use impossible

Opponent/Forward

- No system is safe from all adversaries



Opponent/Forward

- It is critical to know our opponent (motivation, capabilities, access):
  - “Script-kiddies” (curious but incapable)
  - Occasional attackers who aim to understand the systems
  - Persons with intent to cause harm/destruction
  - Organized and technically sophisticated groups (eg, cyber crime)
  - Competitors (industrial espionage)
  - Countries/States/Governments

Opponent/Forward

- You need to think like an opponent/ attacker:
  - Always look for the weakest link
  - Identify trust assumptions underlying security
    - Are they valid?
  - Look at the "out of the box" system
    - Whoever designs a system is always "stuck" with what he is supposed to do.

The value of skepticism

the characteristic most important is keep skepticism!

https://www.usenix.org/conference/usenixsecurity18/presentation/mickens

Acknowledgments

- This lecture's slides have been inspired by the following lectures:
  - CSE127:Introduction
  - CS155:course overview
  - CS343:Security mindset +Computer security ethics