Fundamentos de Segurança Informática (FSI)

2024/2025 - LEIC

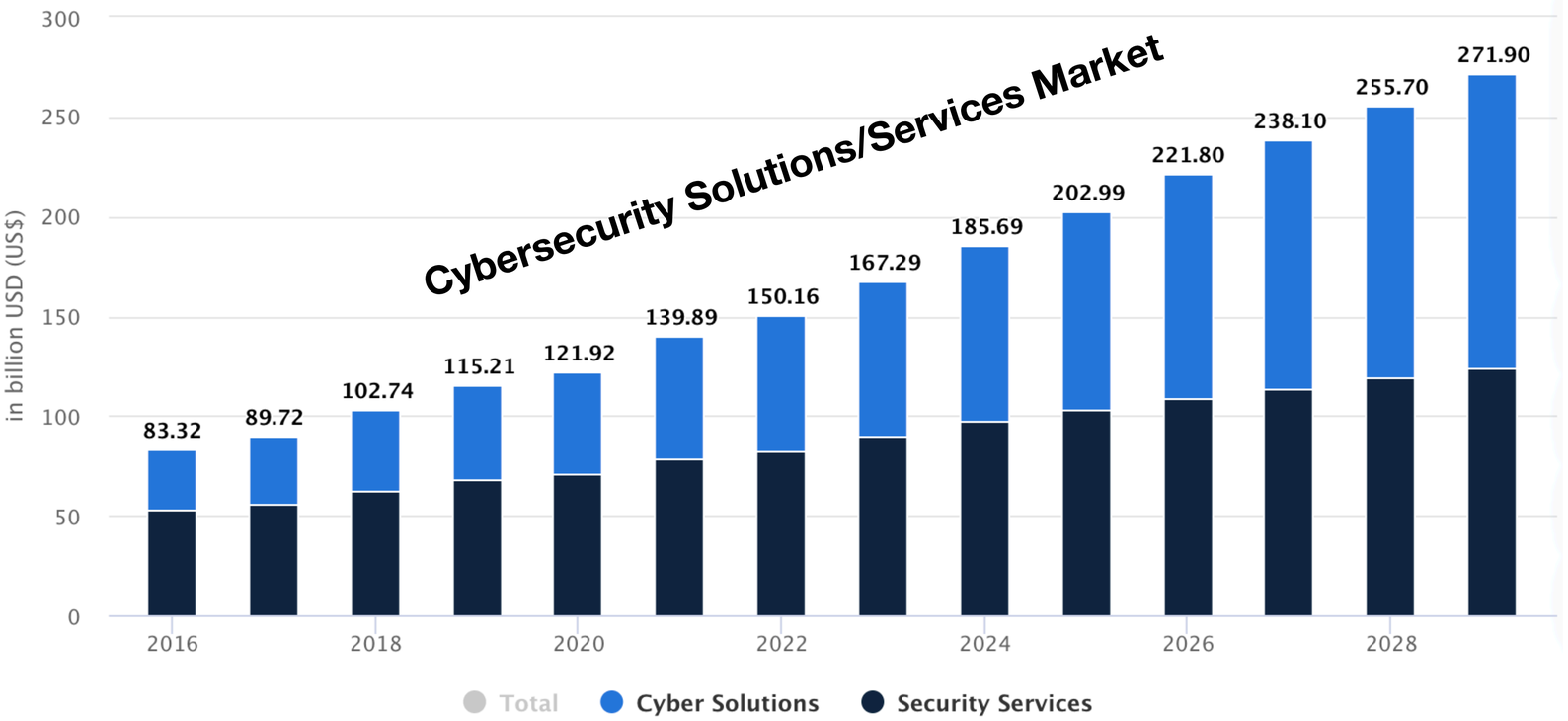
Basic Concepts

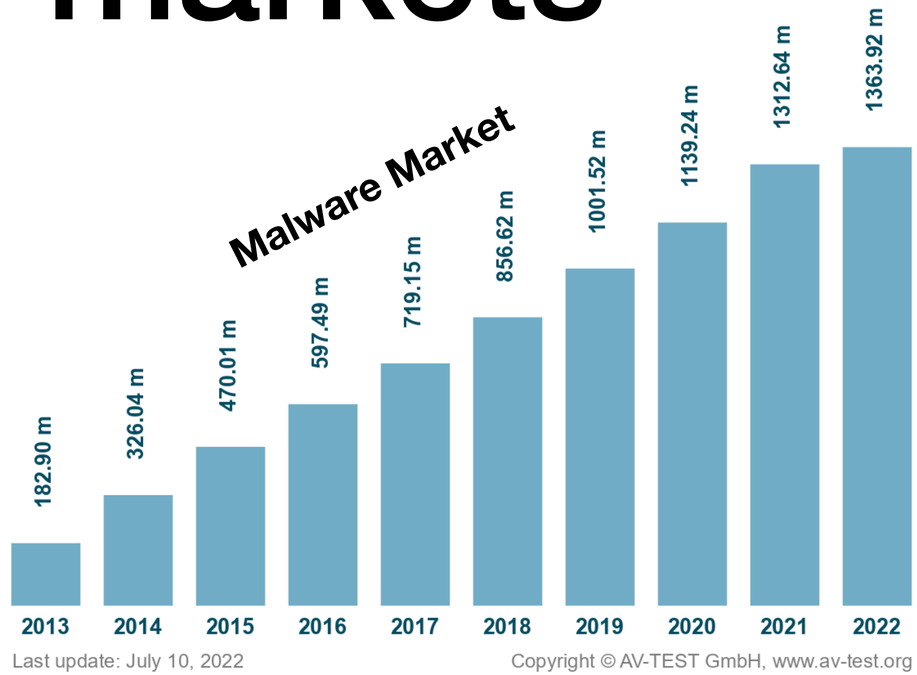
Hugo Pacheco
hpacheco@fc.up.pt

The cybersecurity problem

- The software that we run contains numerous errors/bugs
- Social engineering is extremely effective (e.g., Anonymous @ PT)
- Finding and exploring vulnerabilities is a lucrative activity
  - Huge market for *exploits* (entry doors)
  - Huge market for *malware* (control over compromised machines)
  - Ever growing market around both

Two cybersecurity markets





Top 50 Products By Total Number Of "Distinct" Vulnerabilities

Go to year: 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 All Time Leaders

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Debian Linux	Debian	OS	8799
2	Android	Google	OS	7169
3	Linux Kernel	Linux	OS	5444
4	Fedora	Fedoraproject	OS	5116
5	Ubuntu Linux	Canonical	OS	4094
6	Windows Server 2016	Microsoft	OS	3661
7	Chrome	Google	Application	3503
8	Iphone Os	Apple	OS	3437
9	Windows Server 2019	Microsoft	OS	3217
10	Mac Os X	Apple	OS	3206

https://www.cvedetails.com/top-50-products.php?year=0

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, 2018

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/indictment-related-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.)

Compromising a user's machine #1

- **Stealing user credentials**: bank, business, gaming, etc

Trojan.Silentbanker.B Description

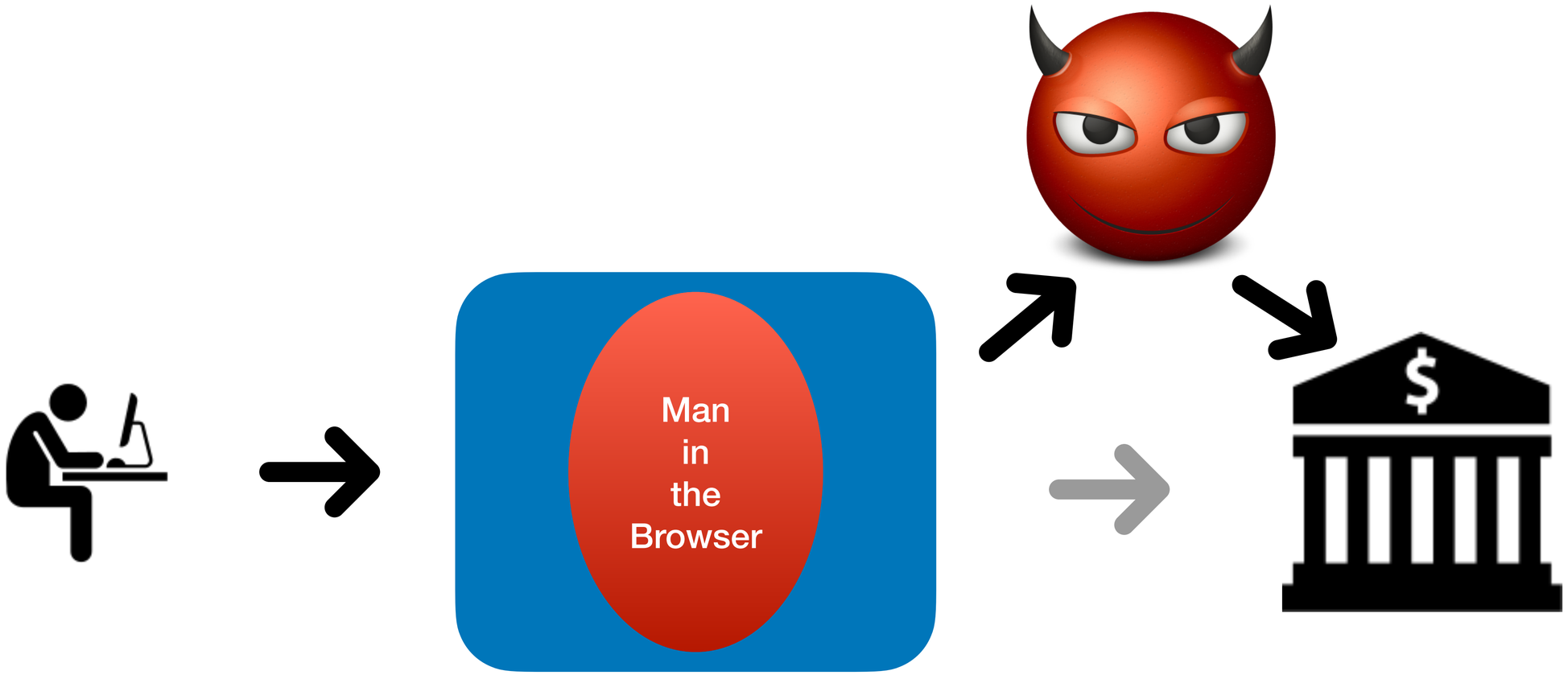
[source: Microsoft 2008]

Type: Trojan (apparently legitimate code that transmits info to attacker)

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.

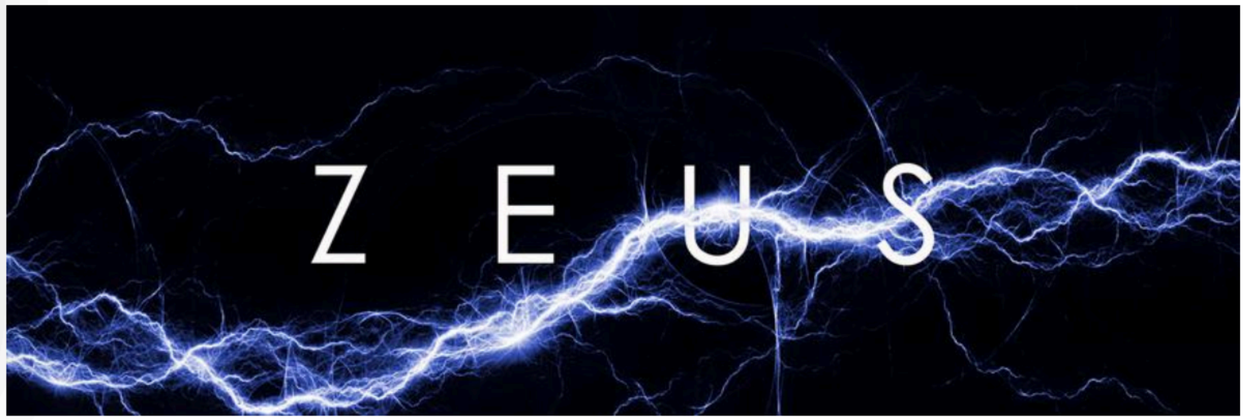
Compromising a user's machine #1

- Often deployed via social engineering (e.g., phishing)
  ⇒ man-in-the-middle attacks



Threat Spotlight: ZeuS (aka Zbot) Infostealer Trojan

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



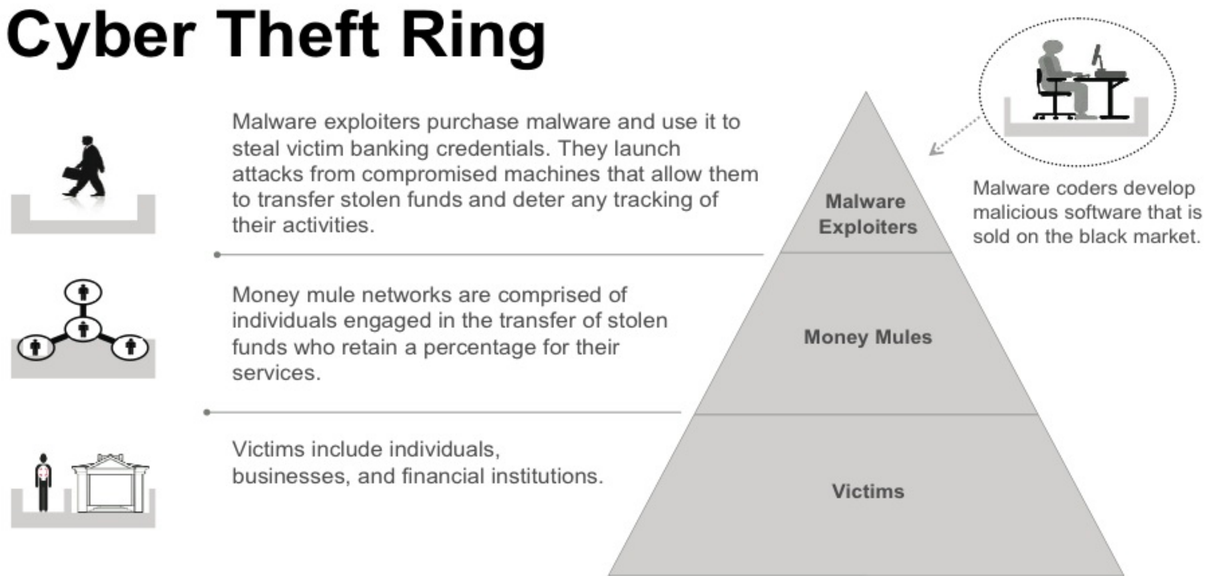
Threat Spotlight: ZeuS (aka Zbot) Infostealer Trojan

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].

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.

Financial Spyware

To date (~2009) the largest *botnet* (network of controlled machines)



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.

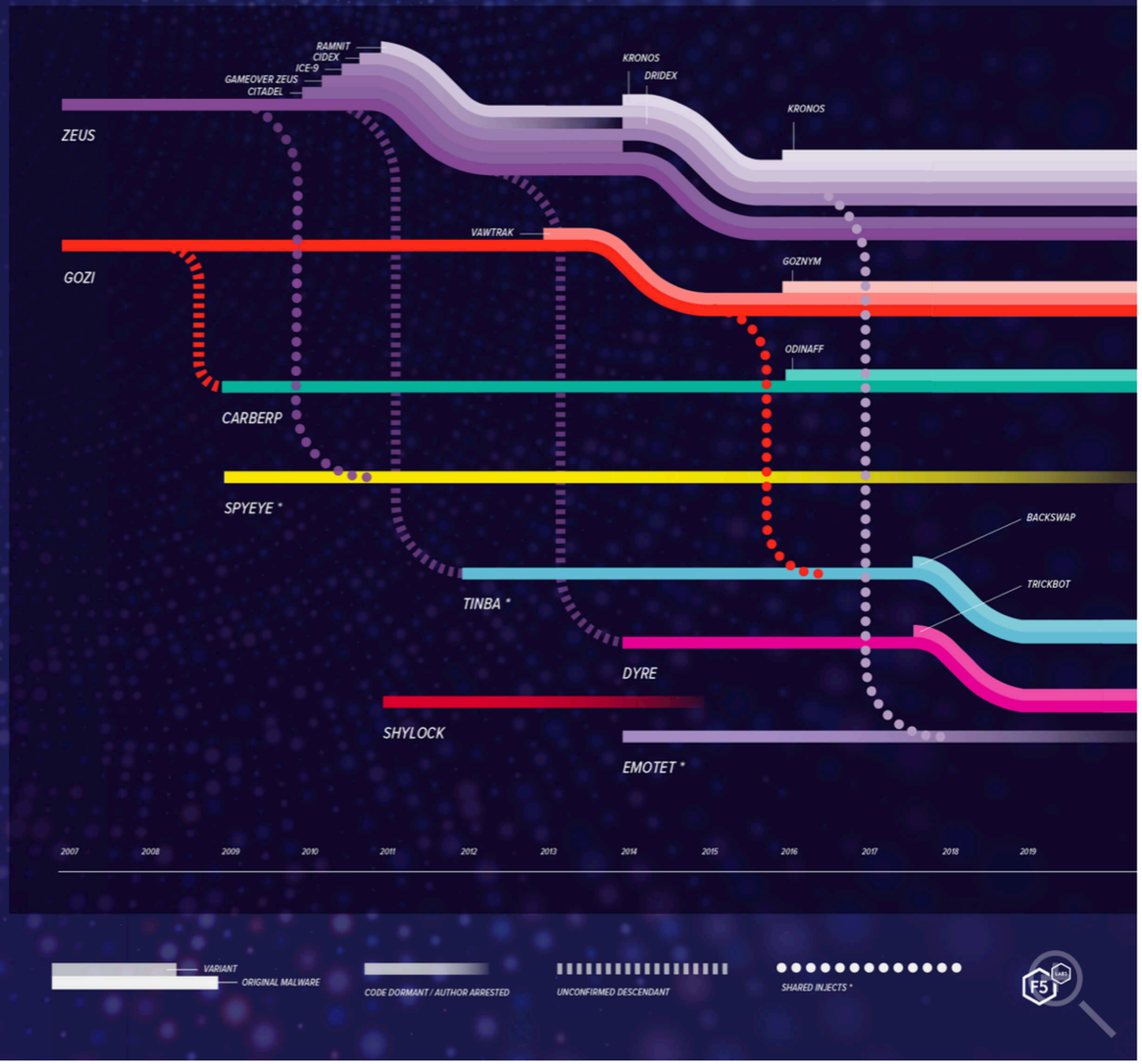
DYRE

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.

"Legal" options available in the market (even for mobile)!

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 Symbian operating 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.”

European Parliament

⇒ all member states have used Pegasus-like surveillance software + need for regulation
https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.html

Compromising a user's machine #2

- **Ransomware**
  - May 2017 @ Worldwide
  - Day 1: disclose of vulnerability used by governmental agencies
  - 3 weeks later: **Wannacry** worm (self-replicating malware)

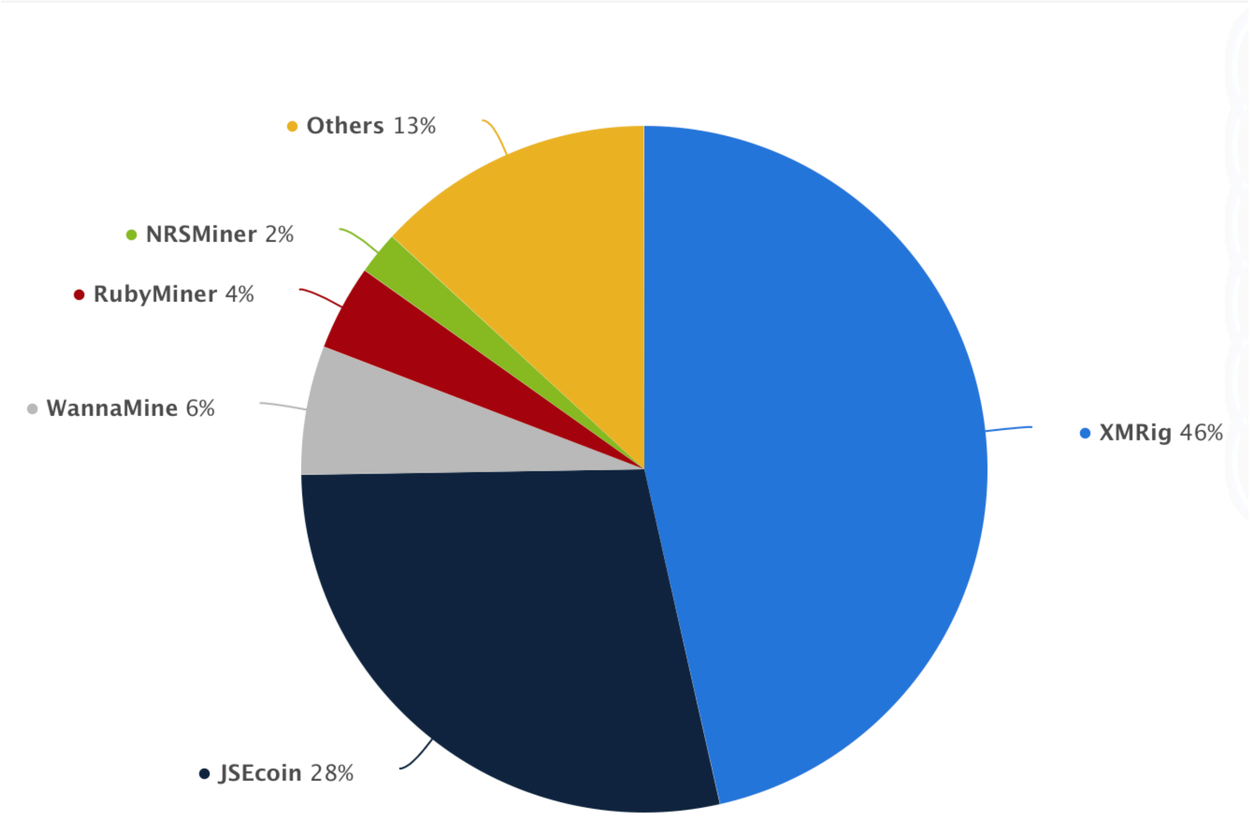
CVE-2017-0143 Windows SMB RCE Vulnerability (WannaCry)

The associated ransomware attack, dubbed "WannaCry", is initiated through an SMBv2 remote code execution in Microsoft Windows. This exploit (codenamed "EternalBlue") has been made available on the internet through the Shadowbrokers dump on April 14th, 2017 and patched by Microsoft on March 14.

Wannacry impact
source: Wikipedia

Compromising a user's machine #3

- **Stealing processing power** (e.g., mining bitcoins)



source: statista

Compromising a user's machine #4

- **Usurping the network address** to seem like a legitimate user
  - Spam (still) works (spamalytics)
  - Denial of Service
  - Clicks on browser ads (e.g., Clickbot.a)
- All these services are sold online:
  - Often require setting up a botnet

'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

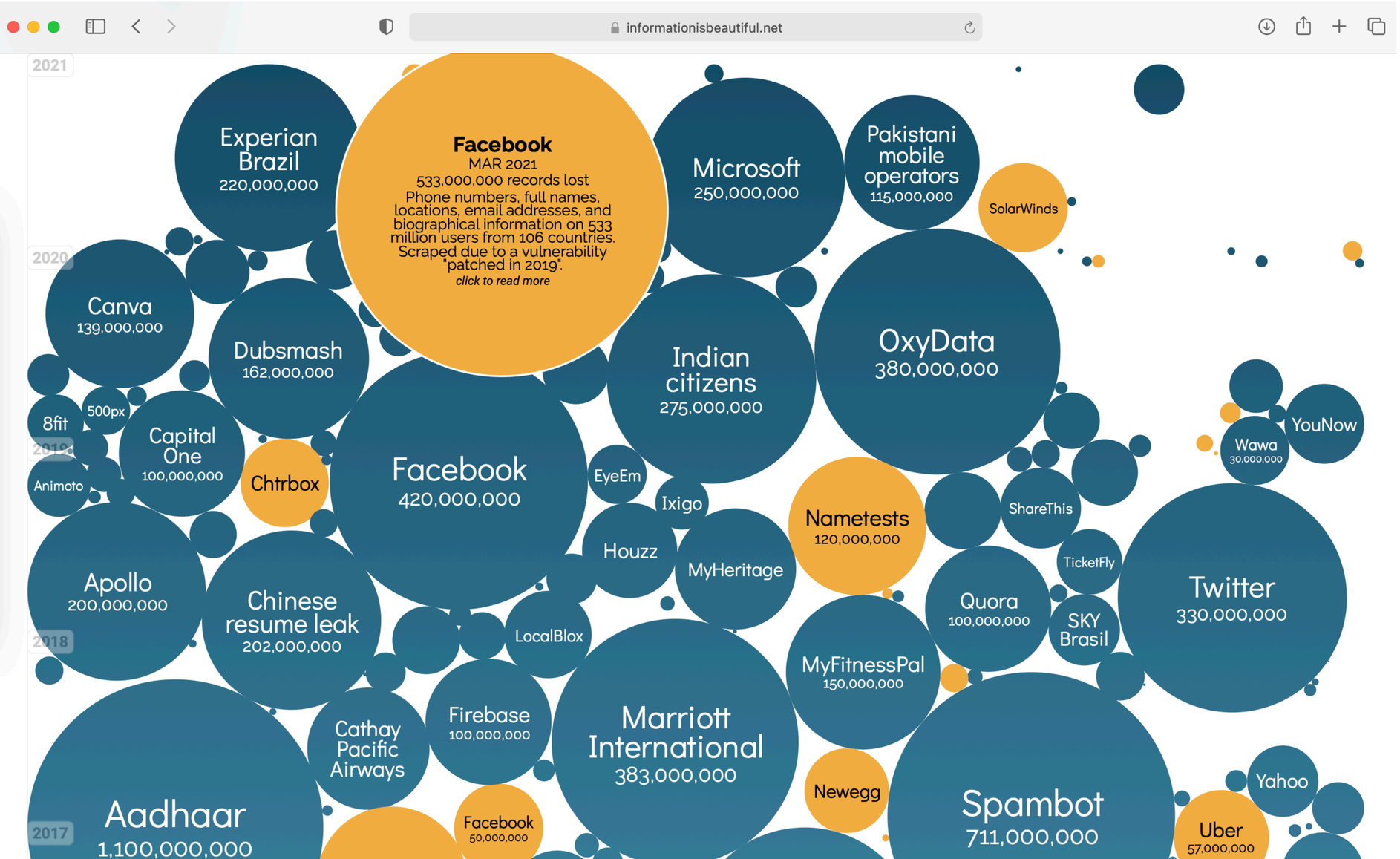
Deloitte estimates that some common criminal businesses can be operated for as little as $34 month and could return $25,000, while others may routinely require nearly $3,800 a month and could return up to $1 million per month. For example, phish kits

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

Compromising servers

- #1: **Data breaches**
  - Stealing credit card and/or user credentials
    https://en.wikipedia.org/wiki/List_of_data_breaches
- #2: **Geopolitical motivations**
    - E.g., Democratic National Committee, Ukraine power grid, Stuxnet
- #3: As a way **to compromise users**
  - supply-chain attacks (infecting server that distributes software)
  - web-server attacks (infecting web server that is accessed by users/browsers)

#1: Data Breaches



';--have i been pwned?

https://haveibeenpwned.com/

Around this time in 2022...

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

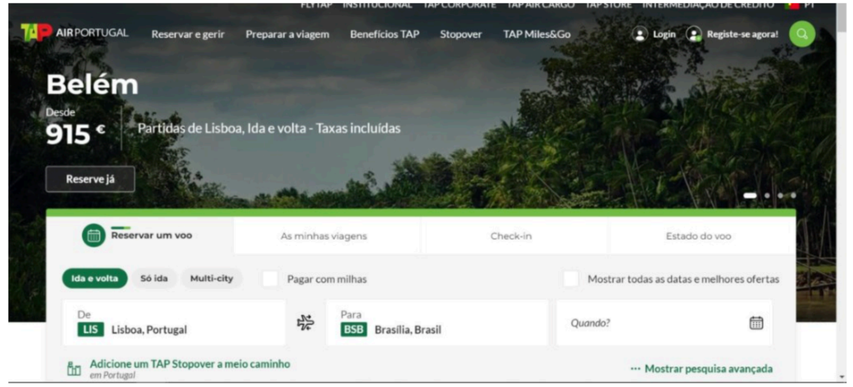
PIRATARIA INFORMÁTICA

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

Modern cars are not secure

*Privacy Not Included

moz://a

It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy

By **Jen Caltrider, Misha Rykov** and **Zoë MacDonald** | Sept. 6, 2023

Ah, the wind in your hair, the open road ahead, and not a care in the world... except all the trackers, cameras, microphones, and sensors capturing your every move. *Ugh.* Modern cars are a **privacy nightmare**.

All 25 car brands we researched earned our *Privacy Not Included warning label -- making cars the official worst category of products for privacy that we have ever reviewed.

https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/

DATA BREACHES

25k Nissan Customers Affected by Data Breach at Third-Party Software Developer

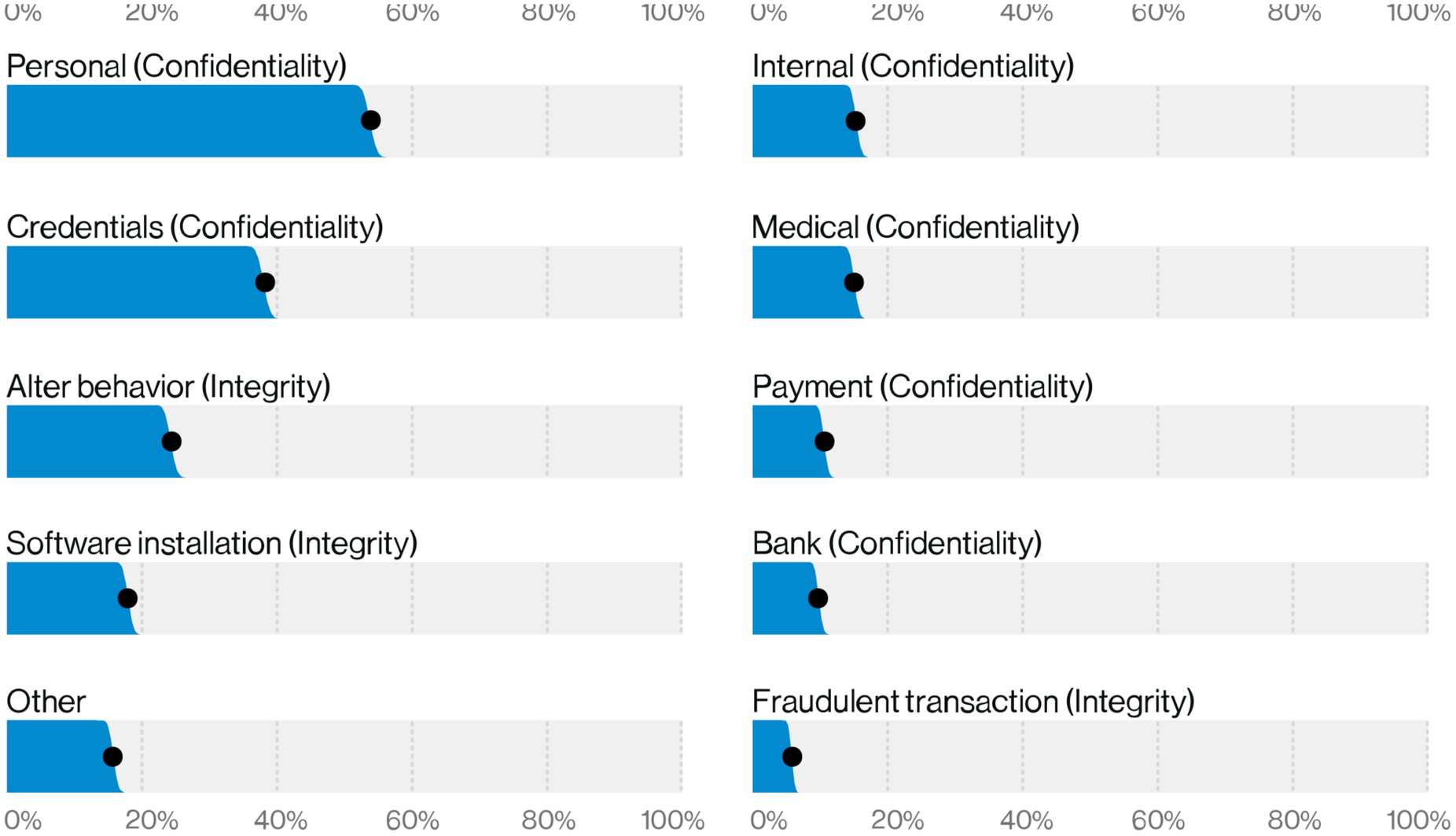
Nissan North America told roughly 25,000 customers that their personal information was exposed in a data breach via a third-party provider.

By Ionut Arghire
January 18, 2023

Nissan North America is informing roughly 25,000 customers that their personal information was exposed in a data breach at a third-party services provider.

https://www.securityweek.com/18k-nissan-customers-affected-data-breach-third-party-software-developer/

Data Breaches: consequences



Source: Verizon

#2: Geopolitical 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.

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]

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

#3: To compromise users

- Supply chain that distributes software can disseminate *malware*:
  - E.g., SolarWinds monitoring tool
- Web servers can compromise vulnerable browsers/clients:
  - E.g., MPack server-side toolset for “website defacing”

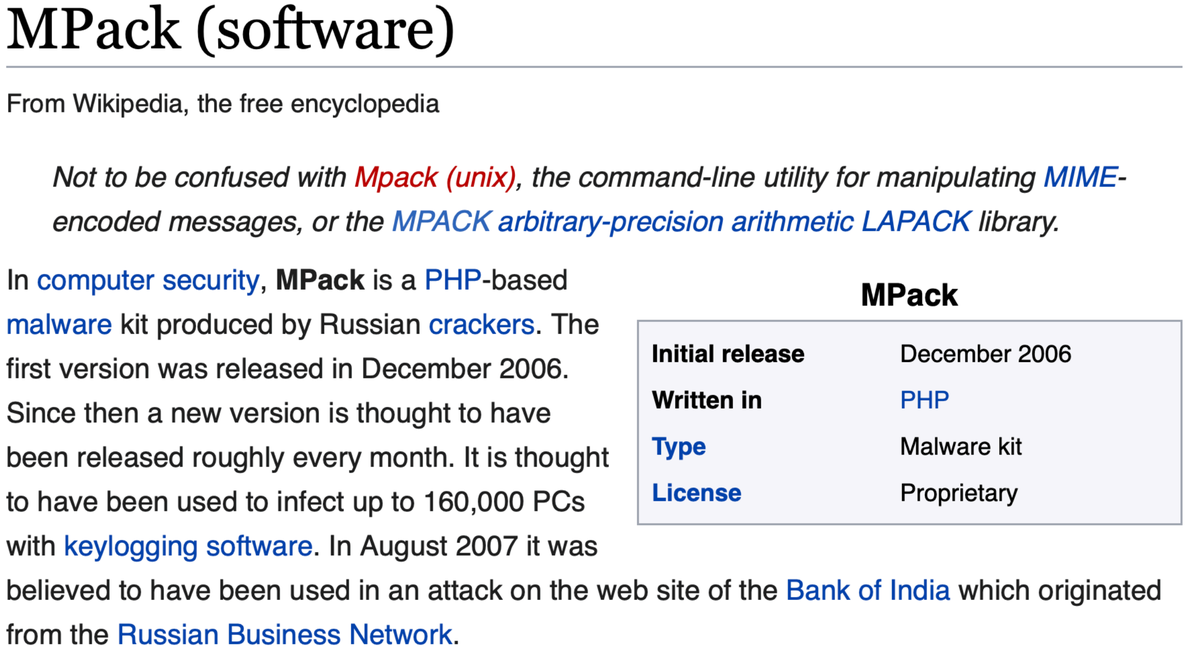
en.wikipedia.org

2019–2020 supply chain attacks [edit]

SUNBURST [edit]

Main articles: 2020 United States federal government data breach and Supply chain attack

On December 13, 2020, *The Washington Post* reported that multiple government agencies were breached through SolarWinds's Orion software (archived website copy). The company stated in an SEC filing that fewer than 18,000 of its 33,000 Orion customers were affected,



MPack (software)

From Wikipedia, the free encyclopedia

Not to be confused with Mpack (unix), the command-line utility for manipulating MIME-encoded messages, or the MPACK arbitrary-precision arithmetic LAPACK library.

MPack

Initial release	December 2006
Written in	PHP
Type	Malware kit
License	Proprietary

In computer security, **MPack** is a PHP-based malware kit produced by Russian crackers. The first version was released in December 2006. Since then a new version is thought to have been released roughly every month. It is thought to have been used to infect up to 160,000 PCs with keylogging software. In August 2007 it was believed to have been used in an attack on the web site of the Bank of India which originated from the Russian Business Network.

Compromising developers

- One of the simplest attacks is “typo squatting”
- E.g.: PyPI package manager
  >300,000 projects
- Supply-chain attack:

  Malicious package with similar name
  ⇒ developer installs the wrong package
- Is it a security problem? Of course.

Malware	Original
acqusition	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

Any error can compromise a system

⇓

Someone will find it

⇓

There is (illegal, greyzone, legal) market

BugBounties 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

Zero-day Bounties

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.

Who are Zerodium's customers?

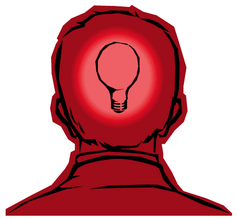
Zerodium customers are government organizations (mainly from Europe and North America) in need of advanced zero-day exploits and cybersecurity capabilities.

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 to guarantee security?

This course



Adversarial Thinking

“Security”?

- A common definition
  - “The system behaves as expected”
- Says nothing about what the system shall / shan’t do:
  - There is no universal definition

“System that remains dependable in the face of malice”

–Ross Anderson

“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

Security Engineering

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

–Gary McGraw

A different way of thinking

- Security is relative
  - “Security” by itself does not mean anything
  - It always depends on who defines it and how
- Security changes with context
  - Everything, including the definition/terminology, depends on the concrete application
    ⇒ we will see different applications (software, systems, web, networks, etc)
- Security is defensive
  - It is defined in the negative: bad things can’t happen
  - Much harder than ensuring that a concrete behaviour happens

- **An absurd example**
  - “Secure” when the objective is to forbid a car **in the road** to override the barrier

Actors

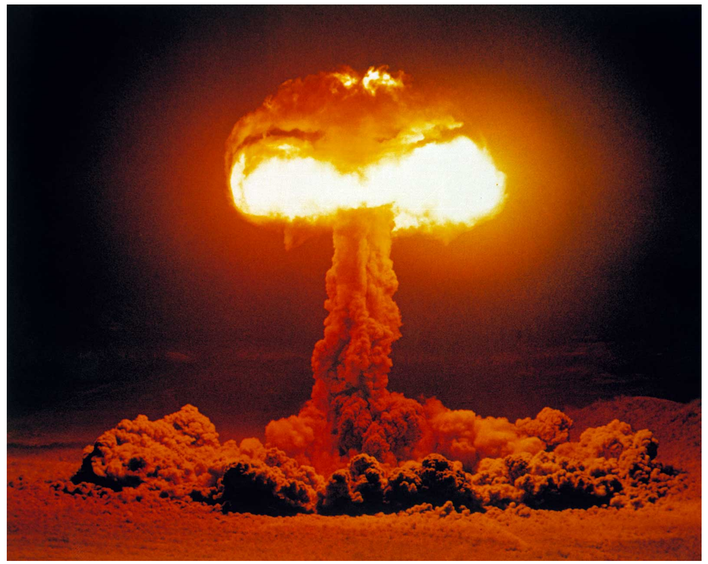
- Actors are entities that intervene in the system
  - People, organisations, companies, machines, …
  - **Security is defined from the perspective of these actors**
- We often deposit **trust** in some actors or system components
  - e.g., Trusted Third Party (TTP), Trusted Agent (TA)
  - “Secure” system **if** security assumptions hold
    - What if they don’t? ⇒ defense in depth
- We often consider some actors as potential (internal/external) **attackers**

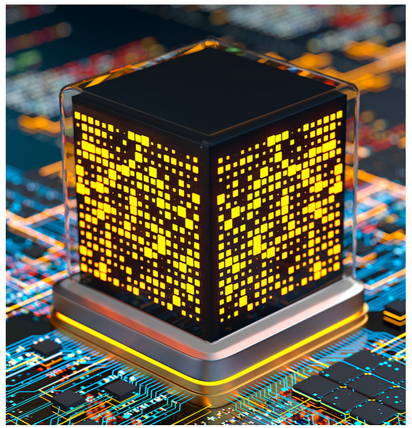
Adversary/Attacker

- In computer security we analyse the behaviour of systems when they interact with adversaries
- Actors with explicit intention of using the system/resources in a wrong way and/or to inhibit its usage

Adversary/Attacker

- No system is secure against all attackers

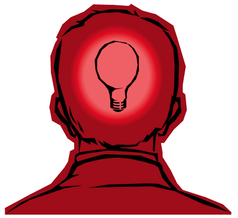




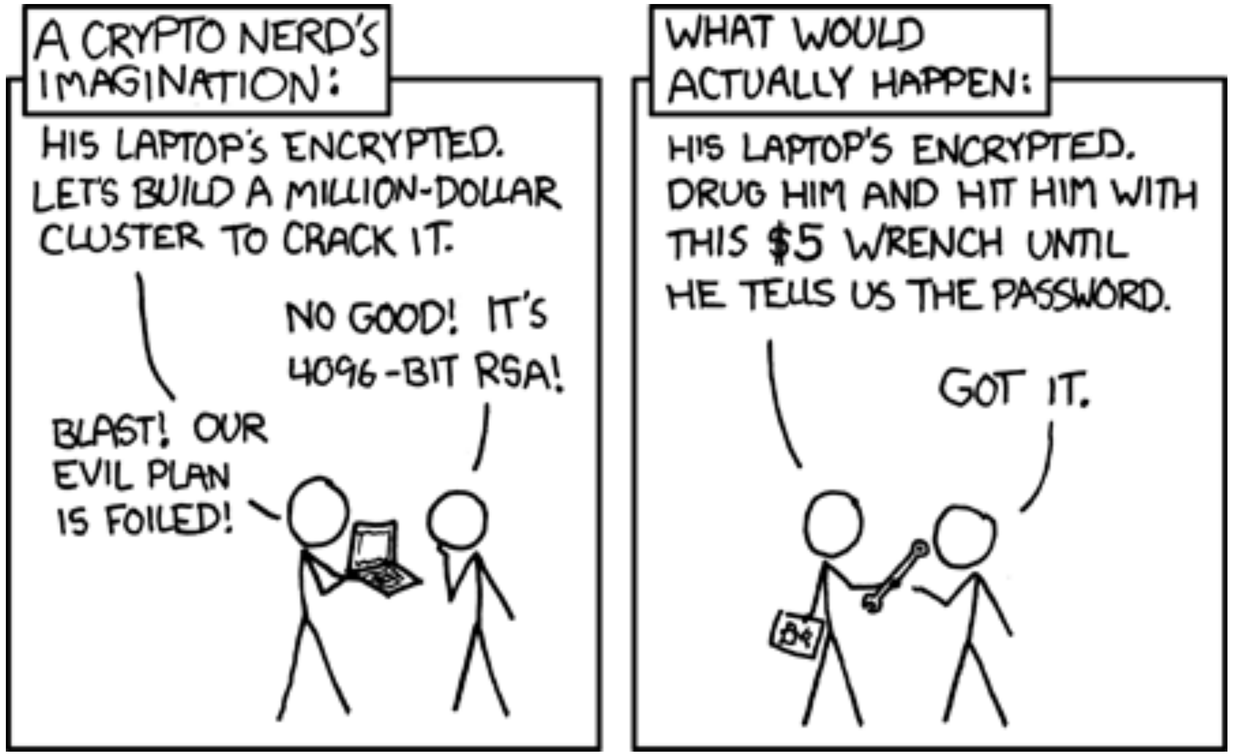
Adversary/Attacker

- It is essential to know our adversary (motivation, capabilities, access):
  - “Script-kiddies” (curious but ineffective)
  - Ocasional attackers that seek fo understand the system
  - Malicious attackers with intention to cause harm
  - Organised and technically sophisticated groups (e.g., cybercrime)
  - Business competitors (industrial espionage)
  - Countries/States/Governments

Adversarial Thinking



- An attacker will always find the weakest link
- We shall:
  - Identify and question security assumptions
  - Look at the system “out of the box”
    - A developer is often “stuck” on what the system can do



https://xkcd.com/538/

Always be skeptical!

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

Acknowledgements

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