The Cybersecurity Problem

Vítor Francisco Fonte, vff@di.uminho.pt, University of Minho, 2024

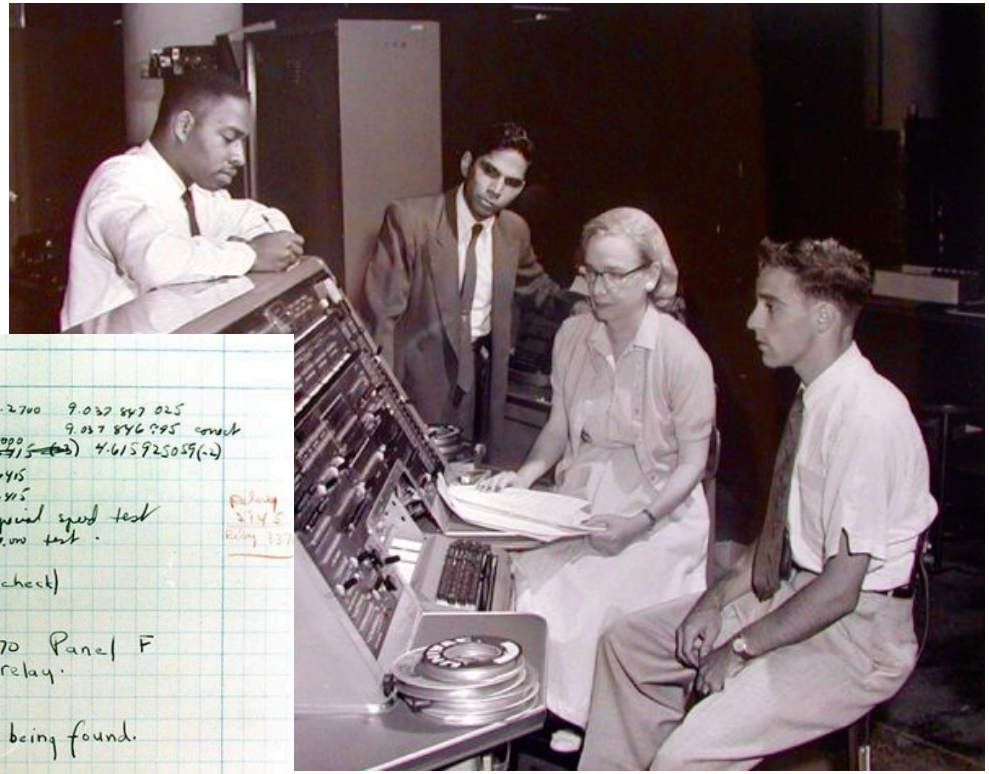
Problem? What problem?

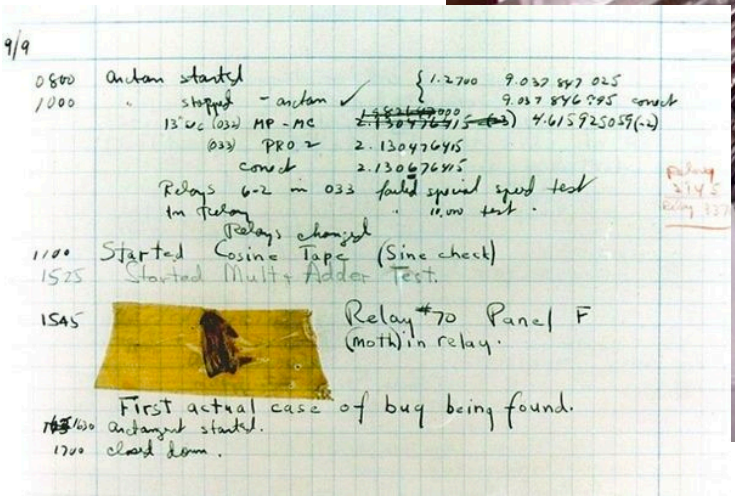
How did we get here?

A Bit of History

First bug, 1945

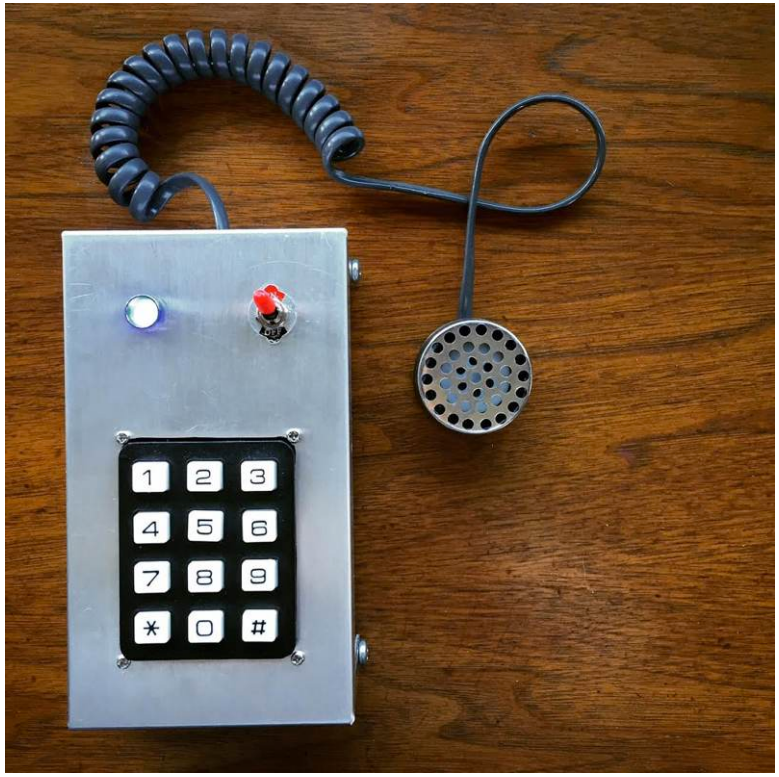
- Grace Murray Hopper records a moth being found stuck between relay contacts of a Harvard Mark II computer. Hence the terms “bug” and “debugging”.





The “Phreaking” Era, 1964

- AT&T starts “Greenstar” toll fraud surveillance system, monitoring long distance calls made from public pay phones trying to catch “phone freaks” (or “phreakers”), people making free calls using “blue boxes”. These were simple devices reproducing AT&T’s control tones.



Cereal “Phreaking”, 1972

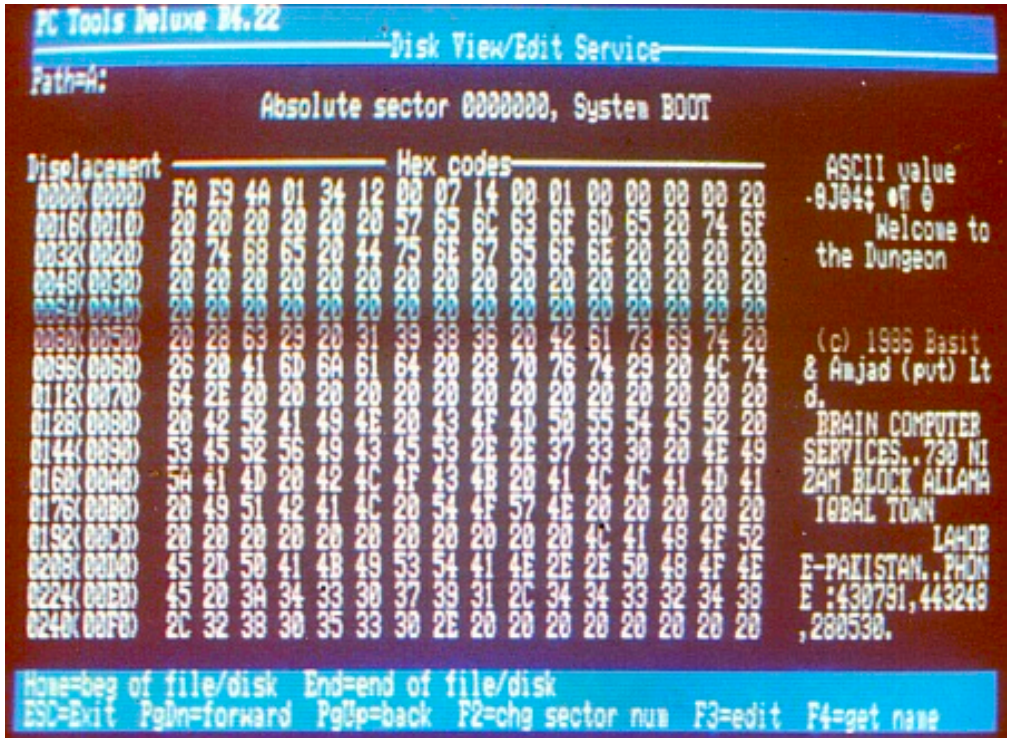
- John Drapper finds out that he could make free calls on the AT&T phone network using simply the whistle offered inside Cap’n Crunch’s cereal boxes. The whistle produces a 2600Hz sound… exactly what it takes to unlock the AT&T network.

The first “worm”, 1979

- In Palo Alto Xerox Research Center, John F. Schoch and Jon A. Hupp start developing self-reproducing programs infecting the Alto computers connected to the same network. These “worms” are volatile, their purpose is benign (distributed system’s research), and sanctioned by the Xerox organisation.

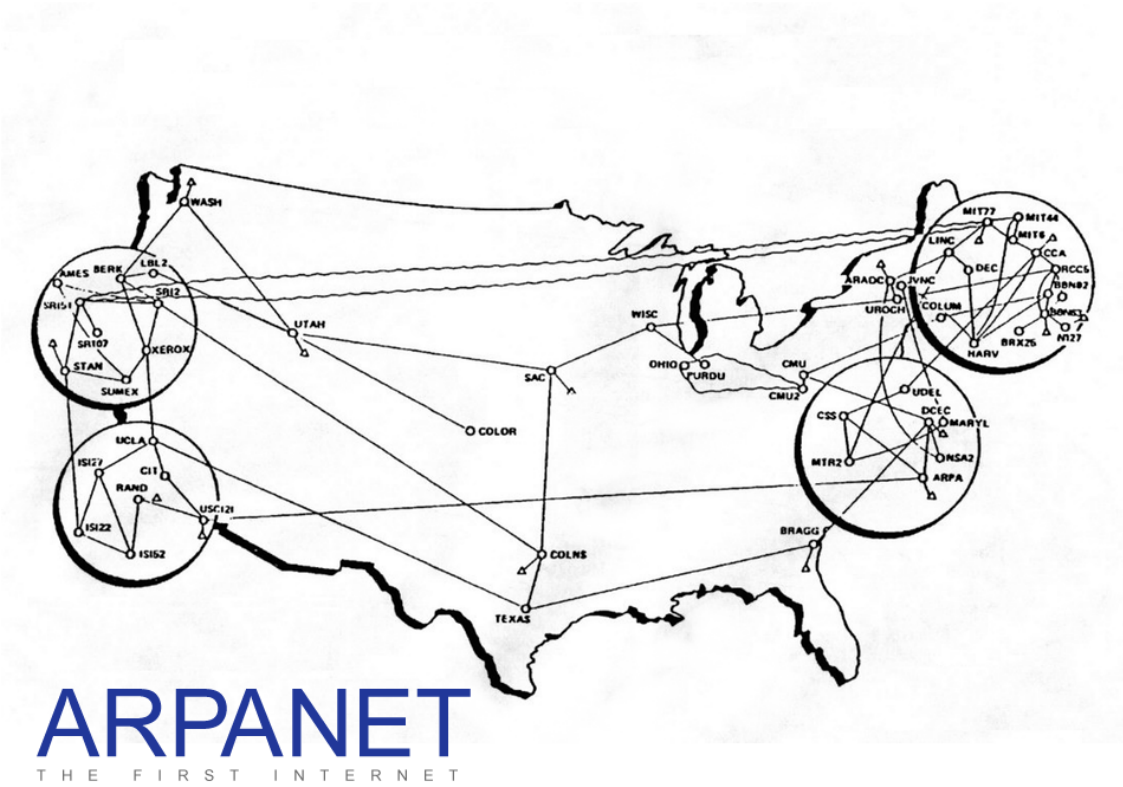
The first “virus”, 1986

- Pakistani brothers Basit and Amjad Farooq Alvi develop the “The Brain”, the first personal computer program that propagates through infection of the boot sector of storage devices. The infection does not destroy any user data and it even provides the contact information of its authors.



The first ARPANET Worm, 1986

- Robert Morri develops the first computer worm that propagates through ARPANET (predecessor of Internet). The worm replicates and fills up all available memory on the (more than six thousand) infected computers, rendering them inoperacional. Charged to a 3 year suspended prison sentence and a fine of 10,000 USD.



More recent history

- 1990: First self-modifiable virus. The virus mutates with each replication rendering ineffective tradicional code signature-based detection.
- 1995: The first virus exploiting Microsoft Word. The “Concept” virus infects systems upon opening of a MS Word documents (via macros).
- 1998: Remote control of military and civil systems. Two US teenagers devise and execute operation “Solar Sunrise” ending up controlling more than 500 military and civil IT infrastructures.
- 2000: Distributed Denial of Service. Computers from the University of California are used to flood computer networks and render inoperacional sites such as Amazon, Yahoo, eBay, …

More recent history

- 2001: “Code Red”: 2 Billion USD in damages. The worm tries to infect MS Windows NT and 2000 systems, with the end goal of a distributed attack to the White House IT infrastructure. The worm is deciphered just in time to prevent the attack.
- 2005: “PoinsonIvy”: virus and remote control in a single package. Infected systems are controlled by the malware (a remotely accessible “backdoor” is also available. It can record system activity, activate the video camera and microphone (if available.) It downloads and executes “payloads” made available from the attack remote system. It was developed in order to steal secrets from the defence and chemical industry.
- 2006: “Nyxem.e”: the file wiper. This worm wiped MS Office and Adobe documents (among other apps) from the infected file systems, on the third day of each month. Hundreds of users were affected.
- 2008: “Koobface”: disseminates itself via via email and social networks. It displays fake ads (eg. in Facebook) of products that once bought are never delivered to the victim.

More recent history

- 2010: “Stuxnet”: attack to industrial control systems. Extremely complex malware that attacked specific SCADA systems. Its main victim was the Iranian nuclear enrichment infrastructure. US and Israeli intelligence agencies are suspected to have been involved in its development and deployment.
- 2012: “Heartbleed”: a bug in OpenSSL. This vulnerability was detected in the OpenSSL cryptographic library, and enables access to cyphered communications and stored data. Millions of systems and billions of users were affected.
- 2013: Theft of personal data of more than 70 million users. US-based Target retail business reports that a large part of its customers had their personal data records stolen from the company’s computer systems.
- 2014: Theft of 1.2 billion authentication credentials. Russian hackers exploit (through a computer virus) vulnerabilities in the handling of SQL statements in several sites and were able to collect their users’s authentication credentials. More than 500 million email accounts may have also been compromised.

More recent, still
Estonia, 2007

- A cyber-attack directed at a country:
  - Distributed Denial of Service: “ping flooding” using rented “botnets”
  - Control of several web sites (specially in media): comment injection (spam), and content replacement(defacement)
  - Affecting web sites of different institutions: national parliament, ministries, media, financial institutions, …
- Considerations:
  - Never before seen coordination and scope
  - Cyberwarfare or cyberterrorism?
  - Some similarities to the Titan Rain operation (2003-06) and to the attack
  - Some similarities to the attacks that took place in South Ossetia (2008)
  - Network security ends up being integrated in modern militar doctrine

More recent, still

Estonia, 2007

- Estonia deploys “digital embassies” in friendly countries
  - Mitigate risks and threats to its infrastructure
  - Improved redundancy: availability and integrity of data
  - Business continuity: government, public admin. and service delivery

More recent, still
Stuxnet, 2012

- Target:
  - very specific SCADA industrial control systems
  - mainly affecting the Iranian nuclear enrichment program
- Attackers:
  - US and Israeli intel agencies suspected to be behind this attack
- Dissemination and elimination:
  - Initial infection thought to have been though USB flash drives, first spotted in the wild in 2010
  - Infected computers in private networks not connected to the Internet
  - Set to stop and delete itself on Jan 24, 2012

More recent, still

Stuxnet, 2012

- Layered attack targeting:
  - Microsoft Windows operating systems executing…
  - Siemens PCS 7, WinCC and STEP7 industrial apps, running…
  - on one or more PLCs S7 from Siemens.
- Exploiting multiple vulnerabilities:
  - 4 previously unknown (0-day), extremely rare
  - 2 already unknown

More recent, still

Stuxnet, 2012

- Technical challenge:
  - Very complex attack
  - Combining different kinds of malware
  - Multiple programming languages
  - User- and kernel-level (rootkit) software components
  - Drivers (kernel) digital signed with valid private
  - Digital keys also stolen from two Taiwanese-based companies

Edward Snowden, 2013

- Former CIA, NSA, Dell e Booz Allen Hamilton employee
  - Expert in network security and cyber-countermeasures
- Unauthorised disclosure of documents revealing secret arrangements between international intelligence agencies:
  - NSA and others US intel agencies
  - Australia (ASD), United Kingdom (GCHQ), Canada (CSEC), Denmark (PET), France (DGSE), Germany (BND), Italy (AISE), Netherlands (AIVD), Norway (NIS), Spain (CNI), Switzerland (NDB), Singapore (SID) e Israel (ISNU)
- Global surveillance system
  - Combining several agencies, tools and techniques
  - Non-targeted collection of data from multiple sources (Dragnet)
  - Sharing of raw data for realtime or later mining

Edward Snowden, 2013

- Main revelations:
  - Secret court order grants NSA access to phone records of US citizens
  - PRISM enables direct access to the services of US tech-companies, such as Google, Facebook, Microsoft e Apple
  - GCHQ (UK) taps into fiberoptic networks all over the world
  - NSA spy on foreign countries and world leaders
  - the Xkeyscore program can search for almost anything an user accesses and publishes on the Internet
  - Tailored Access Operation (TAO) is a team specialised in compromising security in remote systems, infecting them with malware
  - the NSA tries to break cryptographic protocols e to undermine Internet security
  - the NSA can intercept connections to the Yahoo and Google data centres
  - the NSA intercepts the Short Message Service (SMS)
  - the NSA intercepts phone calls in the Bahamas and in Afghanistan

The Cybersecurity Threat Landscape

The ENISA Annual Threat Landscape Report

European Union

The ENISA Threat Landscape Annual Report (ETL)

What is it and who is it for?

- European Union Agency for Cybersecurity (ENISA), ad hoc Working Group on Cybersecurity Threat Landscapes (CTL).
- Reports on the state of cybersecurity mainly within the European Union.
- Mainly targeted at strategic decision-makers and policy-makers, while also being of interest to the technical cybersecurity community.
- Based on multiple and publicly available resources (including OSINT, referenced along the document).
- For each of the identified threats, it determines impact, motivation, attack techniques, tactics and procedures to map relevant trends and propose targeted mitigation measures.

The ENISA Threat Landscape Annual Report (ETL)

Provides insights into emerging trends

- Cybersecurity threats
- Threat actors’ activities and motivations
- Vulnerabilities
- Cybersecurity incidents
- Particular sectors with relevant impact analysis

The ENISA Threat Landscape 2023

Overview

- In the latter part of 2022 and the first half of 2023, the cybersecurity landscape witnessed a significant increase in both the variety and quantity of cyberattacks and their consequences.
- The ongoing war of aggression against Ukraine continued to influence the landscape. Hacktivism has expanded with the emergence of new groups.
- Ransomware incidents surged in the first half of 2023 and showed no signs of slowing down.

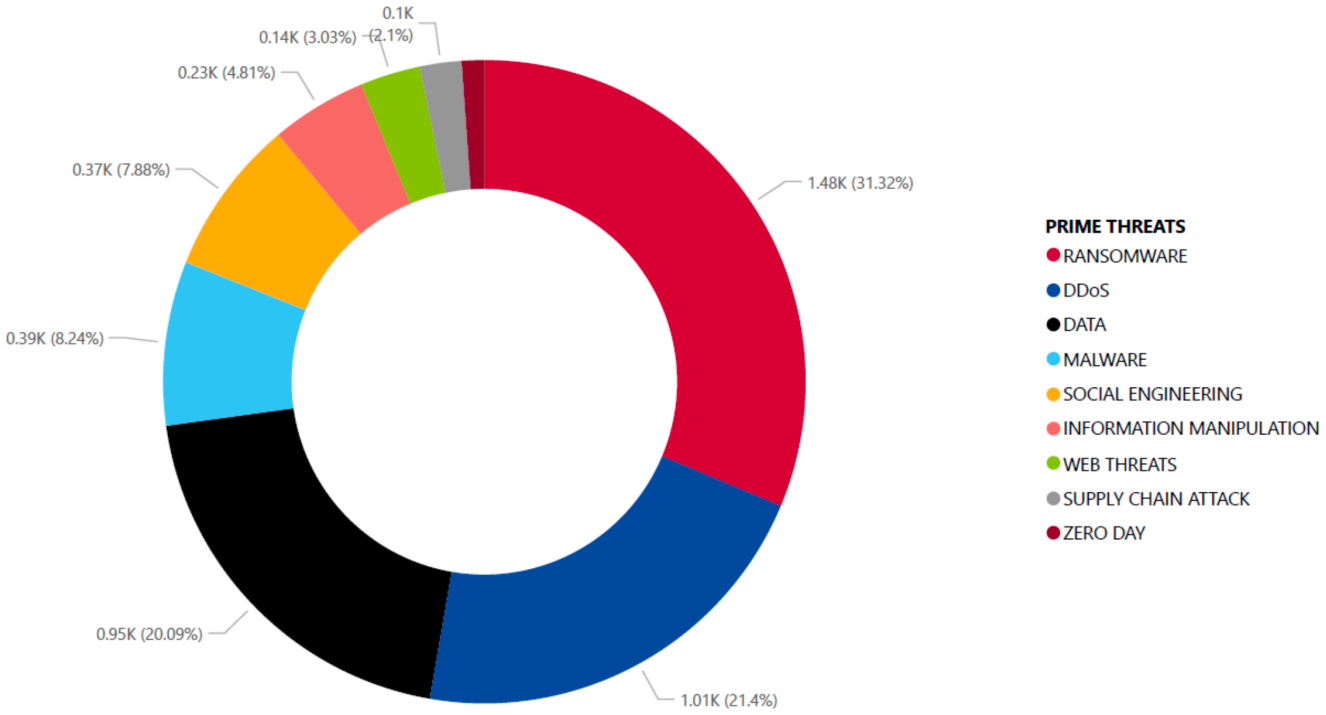
The ENISA Threat Landscape 2023

Main threats

- Ransomware
- Malware
- Social engineering
- Threats against data
- Threats against availability: Denial of Service
- Threat against availability: Internet threats
- Information manipulation and interference
- Supply chain attacks

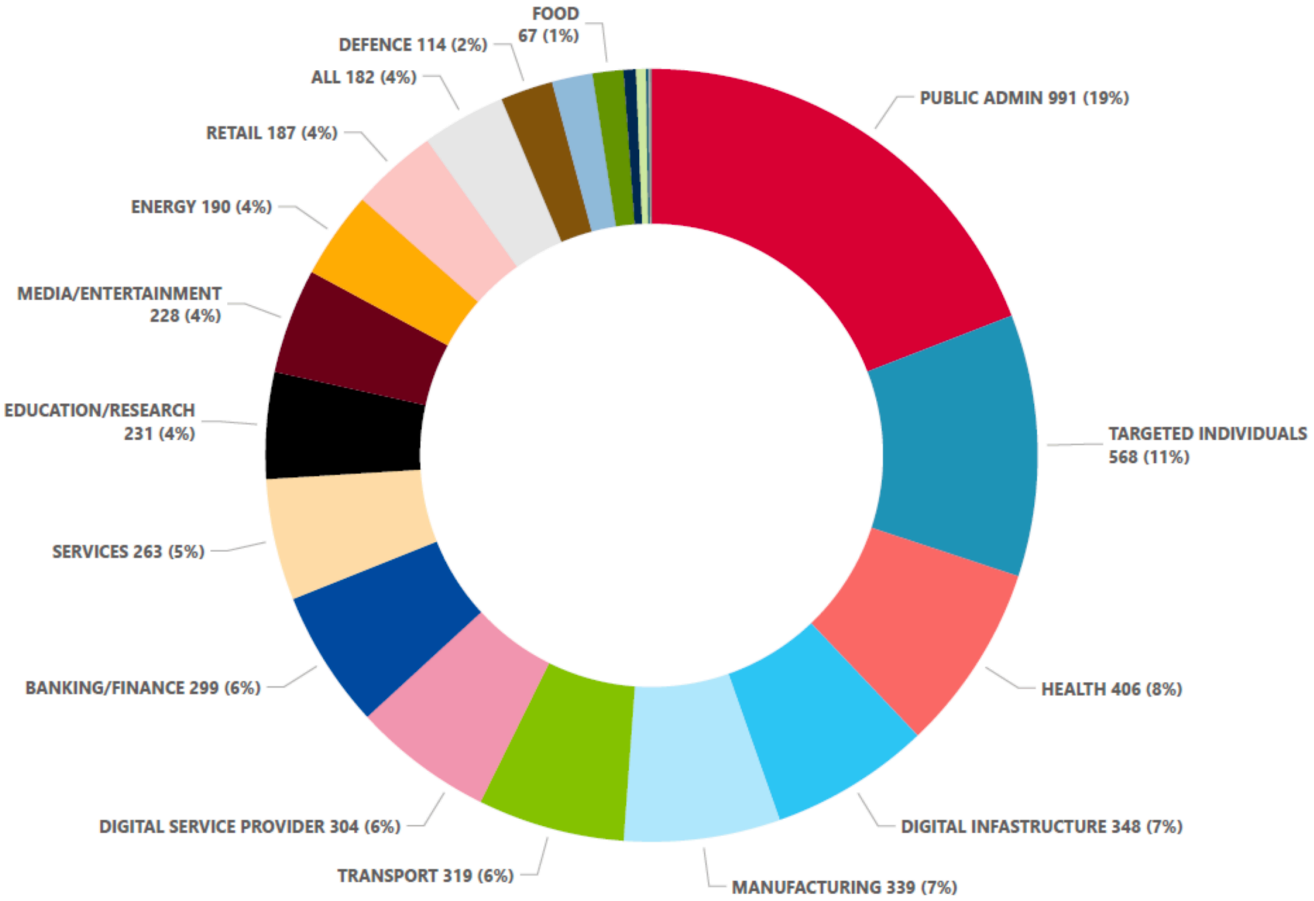
The ENISA Threat Landscape 2023

Incidentes by threat type (July 2022 - June 2023)



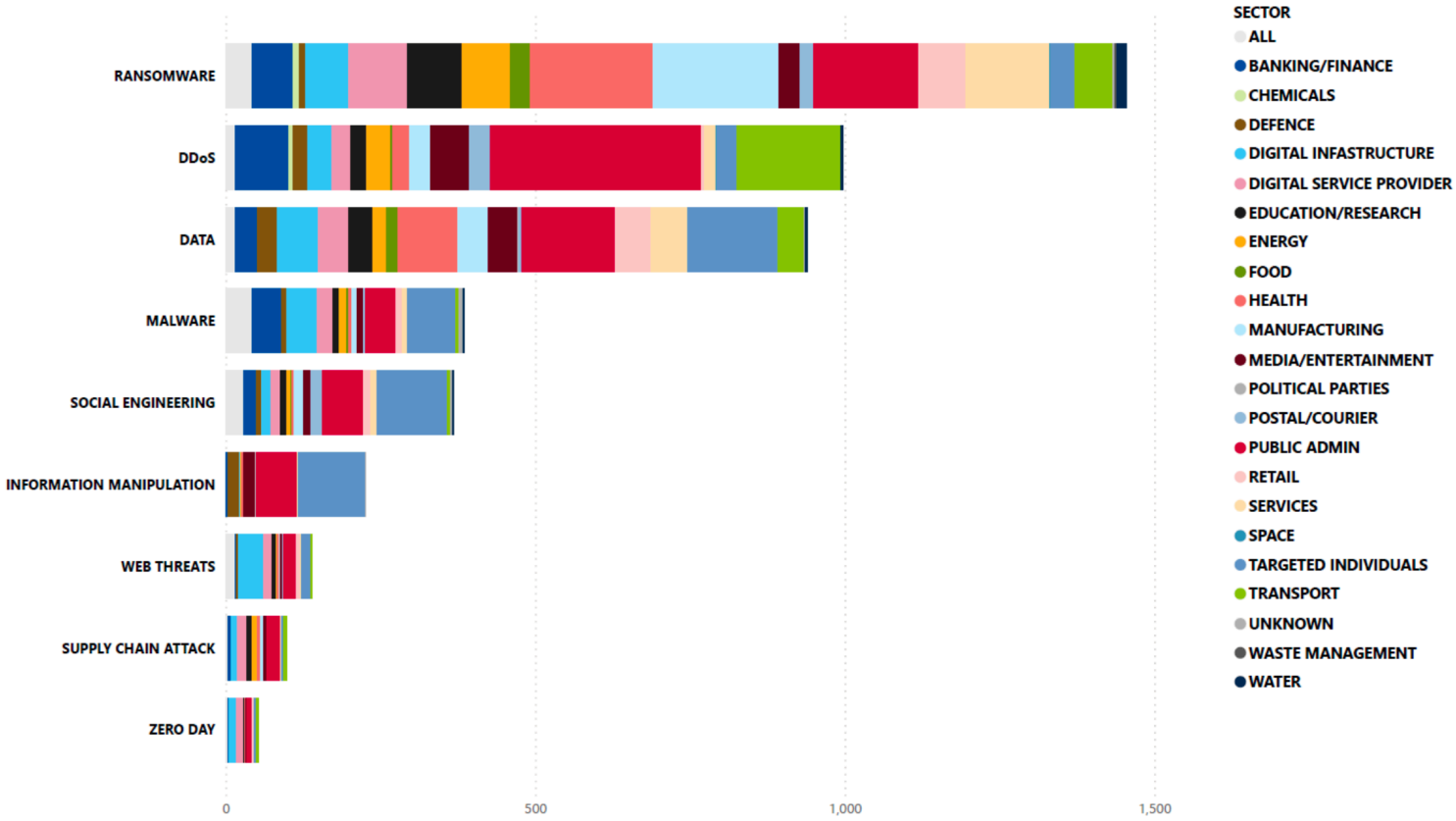
The ENISA Threat Landscape 2023

Targeted sectors per number of incidents (July 2022 - June 2023)



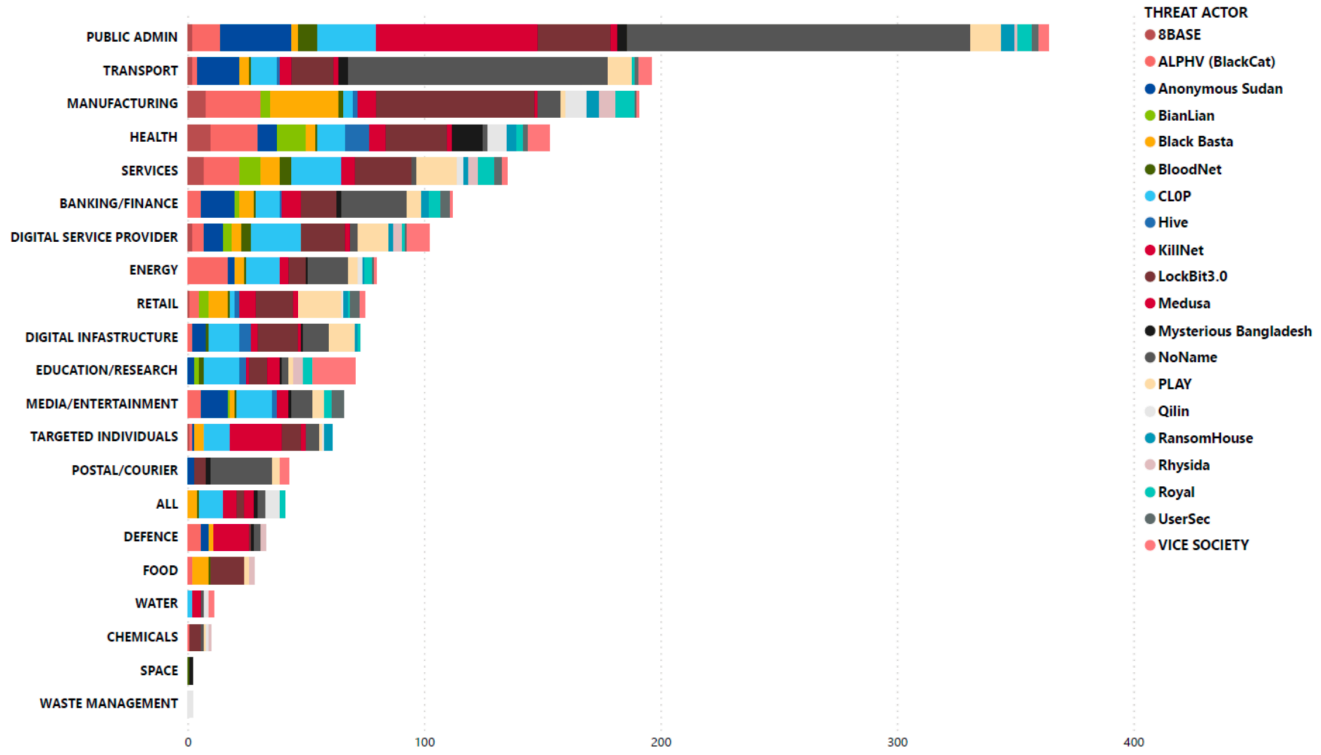
The ENISA Threat Landscape 2023

Incidents related to ETL threats by sector



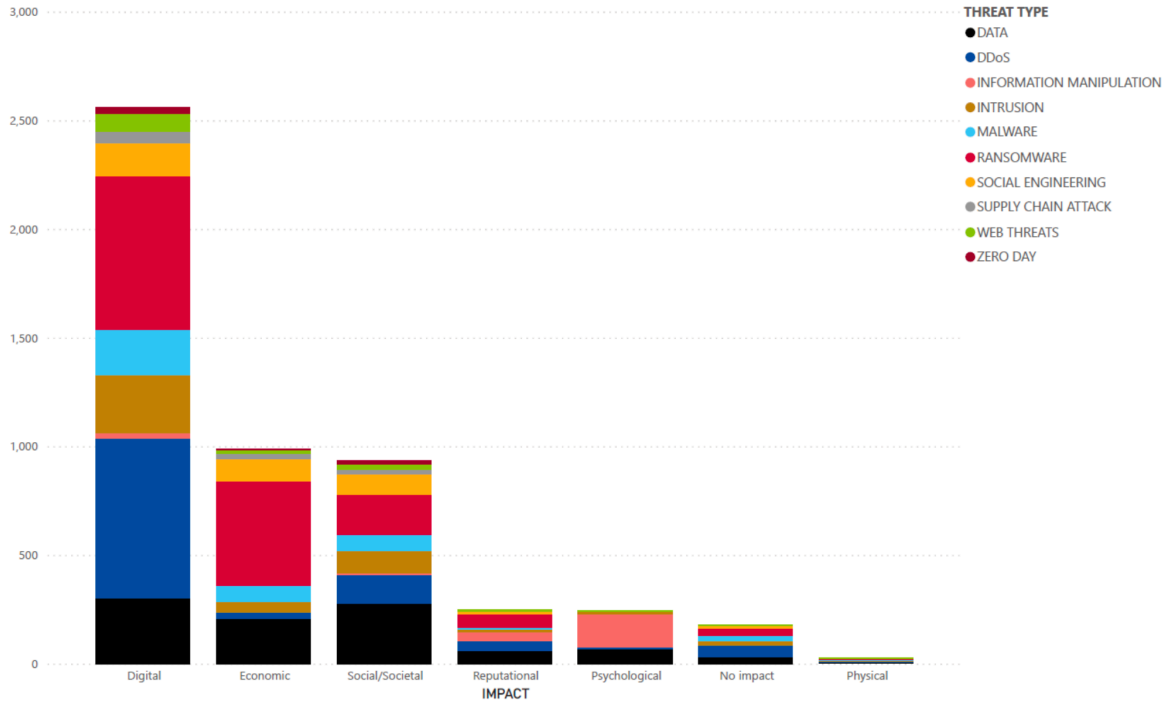
The ENISA Threat Landscape 2023

Threat actor by sector



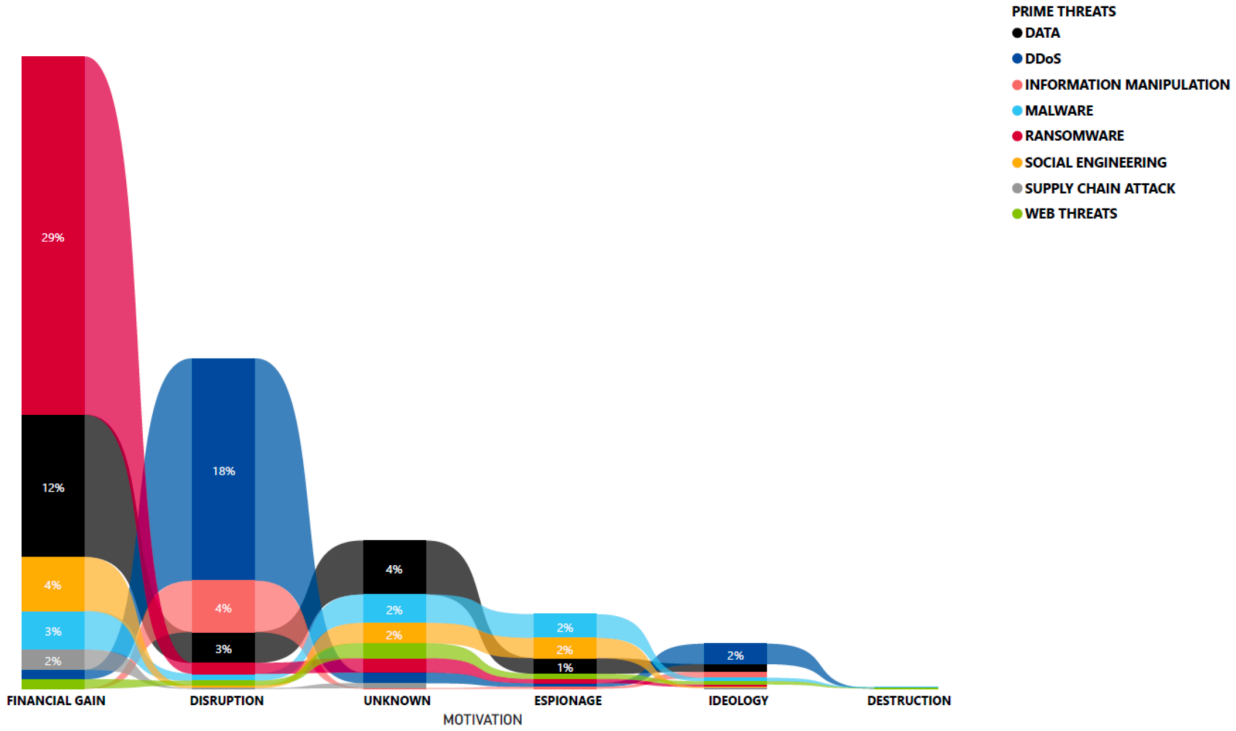
The ENISA Threat Landscape 2023

Threat type breakdown by impact



The ENISA Threat Landscape 2023

Motivation of threat actors per threat category



The ENISA Threat Landscape 2023

Key findings

- DDoS and ransomware rank the highest among the prime threats, with social engineering, data related threats, information manipulation, supply chain, and malware following.
- A noticeable rise was observed in threat actors professionalizing their as-a-Service programs, employing novel tactics and alternative methods to infiltrate environments, pressure victims, and extort them, advancing their illicit enterprises.
- ETL 2023 identified public administration as the most targeted sector (~19%), followed by targeted individuals (~11%), health (~8%), digital infrastructure (~7%) and manufacturing, finance and transport.
- Information manipulation has been as a key element of Russia's war of aggression against Ukraine has become prominent.
- State-nexus groups maintain a continued interest on dual-use tools (to remain undetected) and on trojanising known software packages. Cybercriminals increasingly target cloud infrastructures, have geopolitical motivations in 2023 and increased their extortion operations, not only via ransomware but also by directly targeting users.
- Social engineering attacks grew significantly in 2023 with Artificial Intelligence (AI) and new types of techniques emerging, but phishing still remains the top attack vector.

Security, Computer Science and the ICT Industry

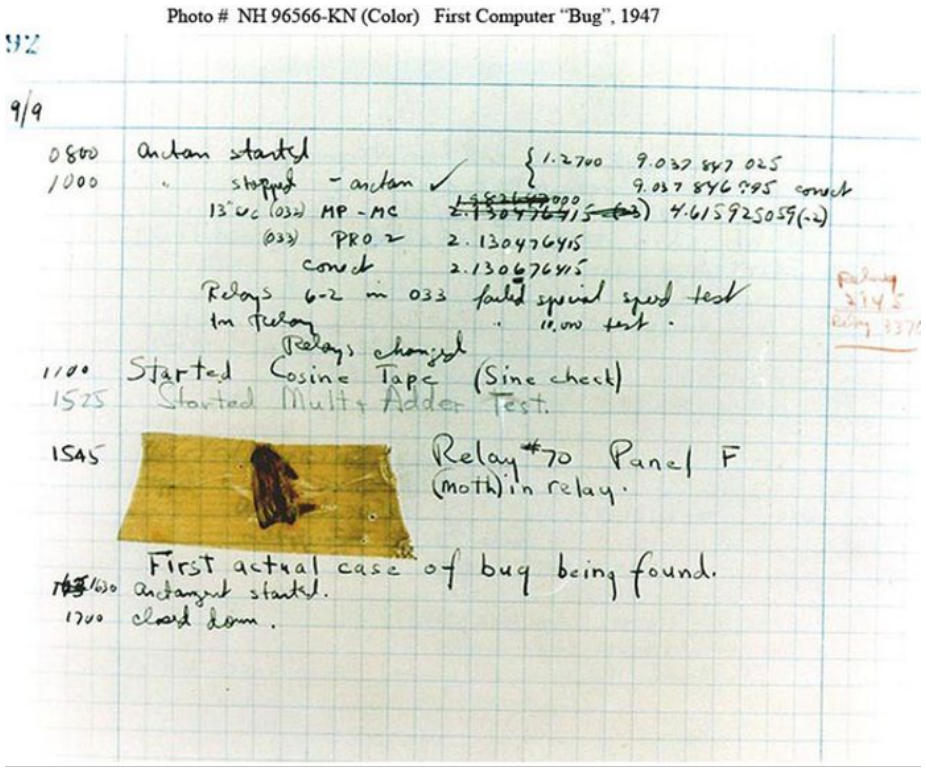
Security, Computer Science and the ICT Industry

A computer science perspective

- Increasingly demanding requirements:
  - Functionality and interconnectivity
  - Support both for legacy systems and for new fields of application
- Deficient specification, development and operational practices:
  - Hard to cope with software size, complexity, and interdependency
  - Security as an afterthought during training of IT professionals
- Perceived benefits weight more than the perceived risks;
  - Shortest time to market
  - Function and convenience before safety and security

Security, Computer Science and the ICT Industry

First bug, 1947 (literally)



Security, Computer Science and the ICT Industry

Estimated numbers of Lines of Code

Software	#	Unit
Unix v1.0	10	thousand
Photoshop v1.0	100	thousand
Space Shuttle	400	thousand
F-22 fighter jet	1,7	million
Linux Kernel v2.2.0	2,0	million
Windows v3.1	2,5	million
Photoshop CS v6	4,5	million
DVD player on XBOX	4,7	million
Boeing 787	6,5	million
Windows NT v3.5	7,6	million
Windows NT v4.0	11,0	million

Software	#	Unit
Mozilla Core	12	million
Linux Kernel v3.1	15	million
F-35 fighter jet	24	million
Microsoft Office 2001	25	million
Microsoft Office 2013	45	million
Microsoft Windows Vista 2007	50	million
Facebook	62	million
MacOS v10.4 (Tiger)	86	million
Car software	100	million
Google (all services)	2	billion

Source: https://www.informationisbeautiful.net/visualizations/million-lines-of-code/

15-50 defects per 1000 lines of code

(estimated industry average)

Security, Computer Science and the ICT Industry

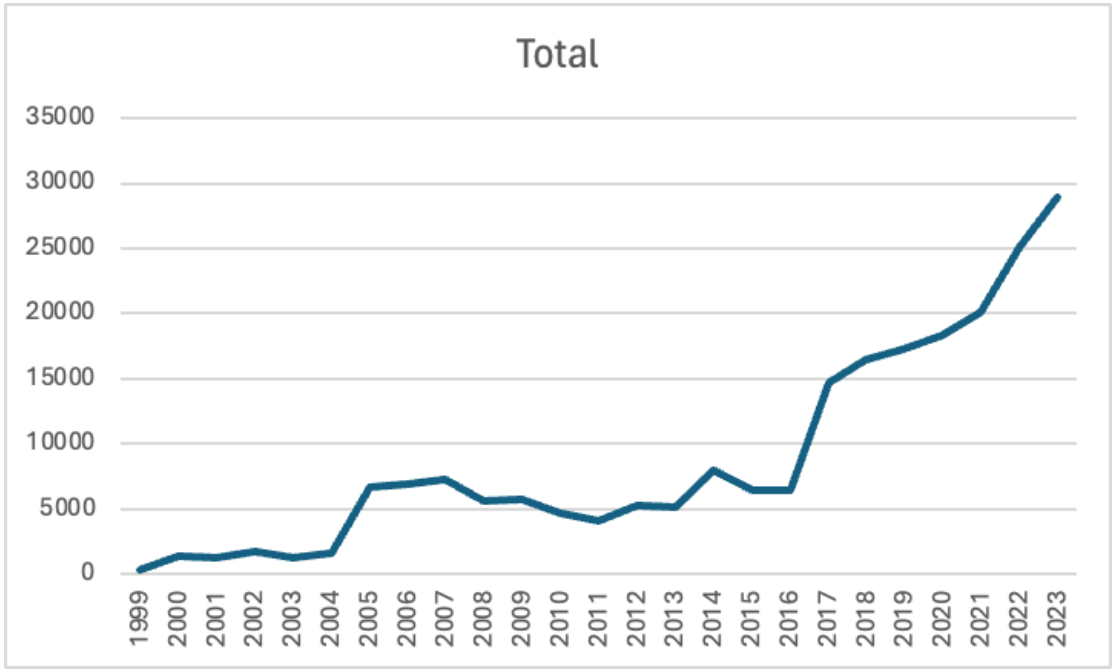
Technical vulnerabilities

- Vulnerabilities:
  - Memory management defects
  - Access control defects
  - Configuration defects
  - Conversion defects
  - Compatibility defects
  - Logical defect
  - Concurrency defects
  - ...

- OWASP 2021 Top 10 (web-based services):
  1. Broken Access Control
  2. Cryptographic Failures
  3. Injection
  4. Insecure Design
  5. Security Misconfiguration
  6. Vulnerable and Outdated Components
  7. Identification and Authentication Failures
  8. Software and Data Integrity Failures
  9. Security Logging and Monitoring Failures
  10. Server-Side Request Forgery

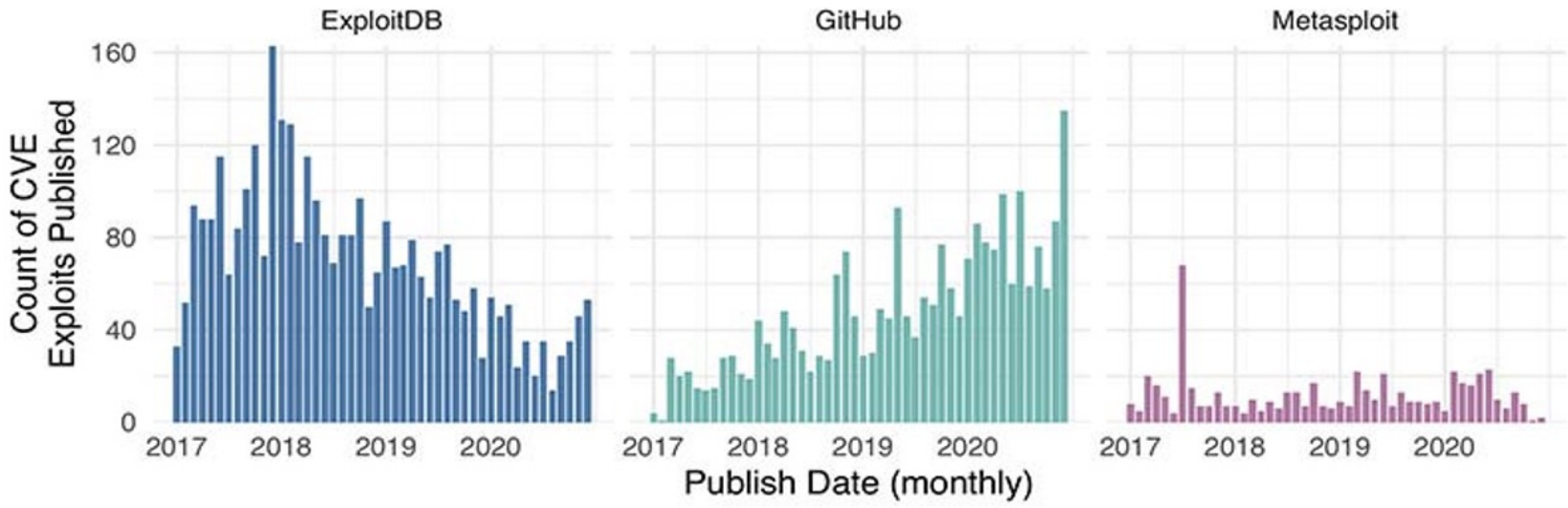
Security, Computer Science and the ICT Industry

Reported (CVE) vulnerabilities per year



Security, Computer Science and the ICT Industry

Exploits on public repositories



Security, Computer Science and the ICT Industry

Tackling security

- Industry approach to coping with complexity:
  - Code refactoring, smaller functions, and smaller components
  - Safer and more domain-specific programming languages and paradigms
  - Safer development, reviewing and testing practices
  - Bug hunting bounties
- Industry approach to coping with security:
  - Better defined and enforced security models
  - Security domains and multi-layer security

Security, Computer Science and the ICT Industry

ICT approach to security

- Based on “engineering best practices”.
- Example: software development in Windows
  - Defects during development and testing: 10-20 defects per 1000 lines of code
  - Defects during upon public release: 0.5 defects per 1000 lines of code
  - So, for a 50 million lines of code base: 25,000 defects (approximately)
- Observations:
  - Not taking into account software supply-chain dependencies
  - Source code is not self-contained

Security, Computer Science and the ICT Industry

Computer science approach to security

- Formal methods:
  - Based on mathematics
  - Rigorous modelling, specification, implementation, verification
  - Proof of correctness
- Limited field of application:
  - Slow, costly and limited scope of application
  - Relatively small software components
- Example:
  - Space Shuttle Software: 0 defects in approximately 500 kloc
  - Cost: several thousand USD per line of code

Security, Computer Science and the ICT Industry

Architectural and technical approaches to security

- Common techniques and approaches
  - Asymmetric cryptography and end-to-end encryption
  - Security domains and trusted computing environments
  - Multi-layer security
  - Well-defined security models
- Some trending approaches:
  - Redundancy and diversity
  - Edge computing
  - Secure by design and zero-knowledge architectures

Security, Computer Science and the ICT Industry

The fragile nature of security

- Security is dynamic
  - Security is an inherent adversarial problem
  - Ignorance may well lead to a false sense of security
- Openness vs. closeness of security-sensitive techniques and tools
  - SecTools.Org: Top 125 Network Security Tools: https://sectools.org/
  - Public malware repositories
  - Security research, techniques and tools are dual nature

From a technical standpoint: no immediate hope on the horizon.

Security, Computer Science and the ICT Industry

Cybersecurity at UMinho/INESC TEC

- What have we been doing
  - Working to improve knowledge in computer and information security fields
  - Working to provide solid theoretical and practical knowledge to future professionals in those fields
- Fundamental and applied research projects:
  - Digital Identity
  - Storage and processing of information
  - Formal methods
- Education projects:
  - Full-fledged master course on Cybersecurity ready to be submitted to the A3ES, expected to start in Sept. 2025.
  - Full-fledged European master course on International Cybersecurity and Cyberintelligence on its final stage of accreditation (A3ES), starting this Sept. 2024, Granada (Spain), Minho (Portugal), Padua (Italy) and Vilnius (Lithuania).

Humans and Organisations: The Weakest Links

Human and Organisational Behaviour and Practices

Takeaways from research and from experience

- Humans and organisations are often unaware of security risks
- Humans and organisations are often willing to trade security for convenience
- Not necessary neglect or security illiteracy
- Often a pragmatic approach to daily needs
- Consequence of managing strategies and budgetary restrictions
- Still, security literacy is a real problem

Human and Organisational Behaviour and Practices

- Examples:
  - User password managing
  - Installation of pirated or dubious software
  - Disabling OS-level local security checks
  - Usage of personal devices within an organization

Human and Organisational Behaviour and Practices

Tackling inherent and acquired behaviour

- At the user level:
  - Transparent use of trusted execution environments (hardware, virtualisation)
  - Enforcing local security checks
  - Self-assessment security tools
- Examples:
  - FIDO-based, password-less authentication, https://fidoalliance.org/
  - Google password checker tool (based on passwords from data-leaks)

Human and Organisational Behaviour and Practices

Tackling inherent and acquired behaviour

- At the organisation level:
  - Robust security policies and implementations
  - Independent and adequately funded security teams (backed by management)
- Examples:
    - Security certifications such as the ISO/IEC 2700 series standards
    - Computer security incident response teams (CERT)
    - Independent security audits (and pentesting exercises)

The human and organisational problem: hard and costly to solve.

Cybersecurity and the Law: Countering Cybercrime

Cybersecurity and the Law

- Need for additional resources and international cooperation:
  - Regulation
  - Investigation
  - Intelligence
  - Prevention
  - Punitive actions
- Crucial need for cross-domain training and specialization:
  - EJTN is a good example
  - Imperative to establish a common understanding between IT and judicial fields

Cybersecurity and the Law

- Blurred line between private, state-sponsored cyber-crime and cyber-warfare
  - Recent IT supply-chain and critical infrastructure attacks
  - Eg. SolarWinds and Nobelium APT
  - Eg. Colonial pipeline
- Punitive actions:
  - Crippling organised cyber-crime infrastructure
  - Crippling financial gains from cyber-crime
- Controversial topic and approach to cyber-crime prevention:
  - Offensive security
  - Eg. The An0m Phone
  - Eg. Attempts to cripple encryption protocols and implementations