MOTIVATION TO SOFTWARE SECURITY

Software Security

Pedro Adão 2022/23

(with Ana Matos & Miguel Pupo Correia)

TÉCNICO LISBOA

The Problem is Software

"*Behind every computer security problem and malicious attack lies a common enemy -- bad software.*"

J. Viega & G. McGraw, *Building Secure Software*, 2002

The Problem is Software

"We wouldn't have to spend so much (…) on network security if we didn't have such bad software security.

Think about the most recent security vulnerability about which you've read.

Maybe it's a killer packet that allows an attacker to crash some server (…)

Maybe it's one of the gazillions of buffer overflows that allow an attacker to take control of a computer (…)

Maybe it's an encryption vulnerability that allows an attacker to read an encrypted message (…)

These are all software issues."

J. Viega & G. McGraw, *Building Secure Software*, 2002

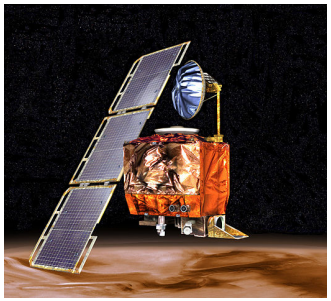
Reported Vulnerabilities 2020

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Android	Google	OS	859
2	Windows 10	Microsoft	OS	807
3	Windows Server 2016	Microsoft	OS	794
4	Windows Server 2019	Microsoft	OS	743
5	Debian Linux	Debian	OS	556
6	Windows Server 2012	Microsoft	OS	443
7	Windows 8.1	Microsoft	OS	435
8	Fedora	Fedoraproject	OS	433
9	Windows Rt 8.1	Microsoft	OS	429
10	Windows 7	Microsoft	OS	388
11	Windows Server 2008	Microsoft	OS	382
12	Leap	Opensuse	OS	366
13	Iphone Os	Apple	OS	305
14	Mac Os X	Apple	OS	300
15	Gitlab	Gitlab	Application	237
16	Chrome	Google	Application	228
17	Tvos	Apple	OS	214
18	Watchos	Apple	OS	210
19	Ubuntu Linux	Canonical	OS	190

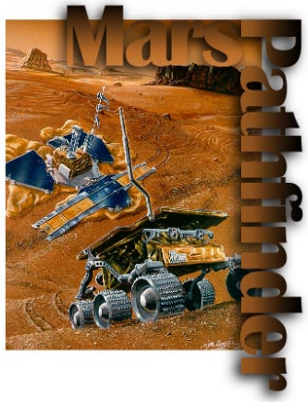
https://www.cvedetails.com/top-50-products.php?year=2020

Bad Software is Everywhere

- NASA Mars Climate Orbiter
  - Crashed due to a units conversion bug ($165 million)

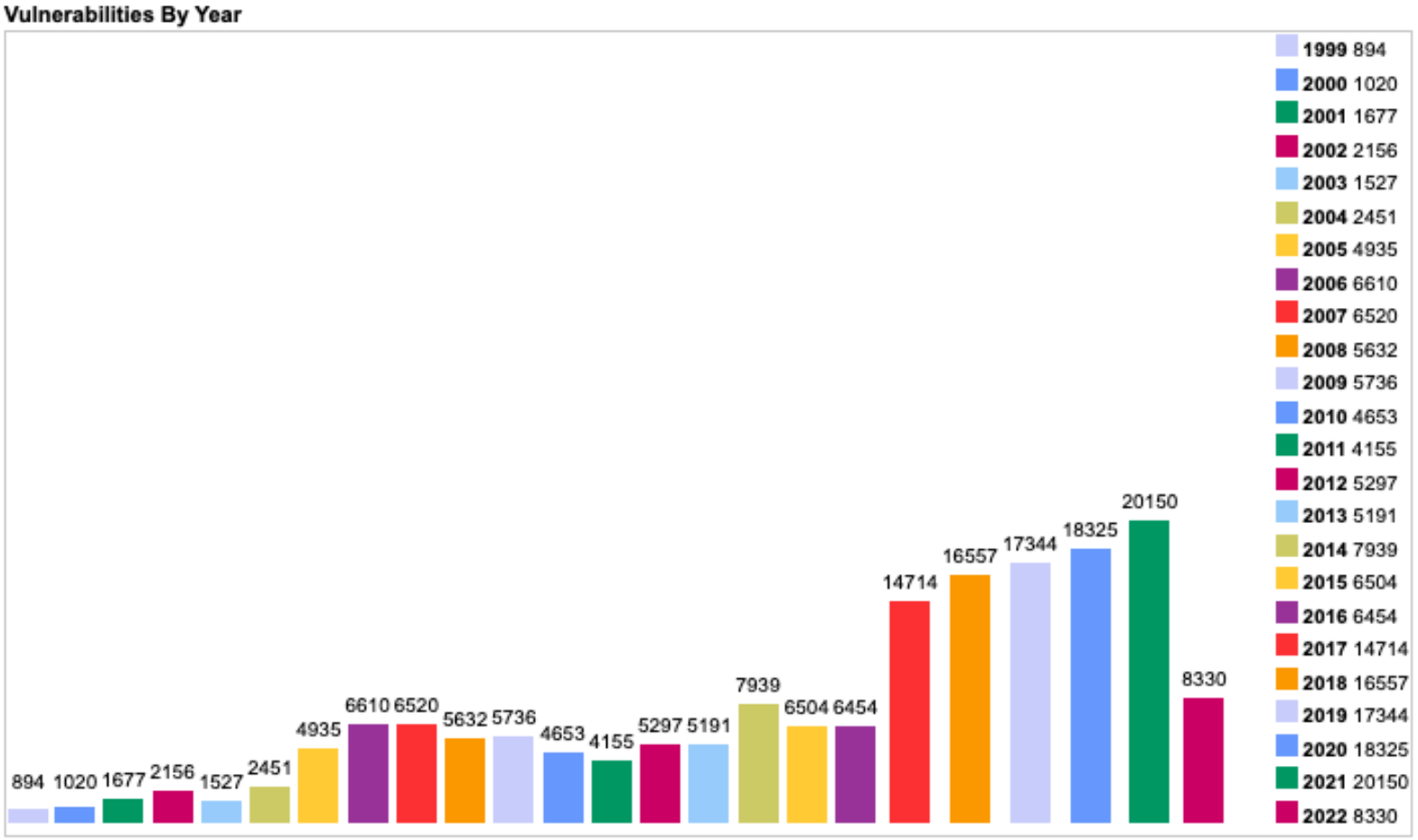


- NASA Mars Pathfinder
  - Stopped for several hours due to a priority-inversion bug ($265 million)
  - Risks Forum: http://www.risks.org/



- https://www.facebook.com/seginfportugal

Reported Vulnerabilities - Evolution



https://www.cvedetails.com/browse-by-date.php

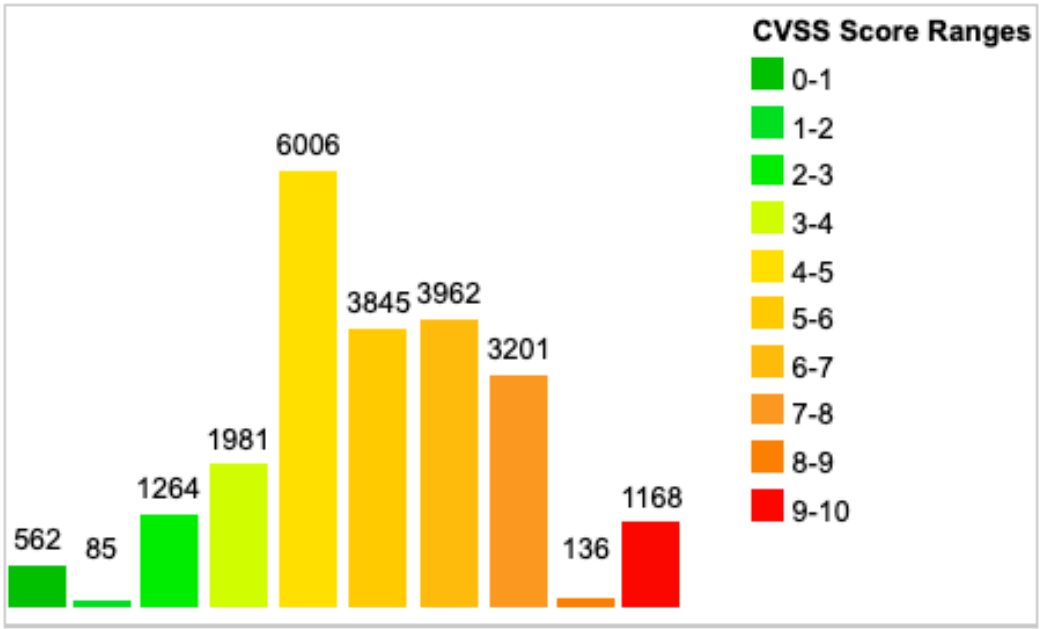
Vulnerabilities - severity

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	562	2.50
1-2	85	0.40
2-3	1264	5.70
3-4	1981	8.90
4-5	6006	27.00
5-6	3845	17.30
6-7	3962	17.80
7-8	3201	14.40
8-9	136	0.60
9-10	1168	5.30
Total	22210	

Weighted Average CVSS Score: **5.9**

Vulnerability Distribution By CVSS Scores



https://www.cvedetails.com/cvss-score-charts.php

Vulnerabilities - always appearing

- US-CERT Technical Cyber Security Alerts
  - http://www.us-cert.gov/cas/techalerts/

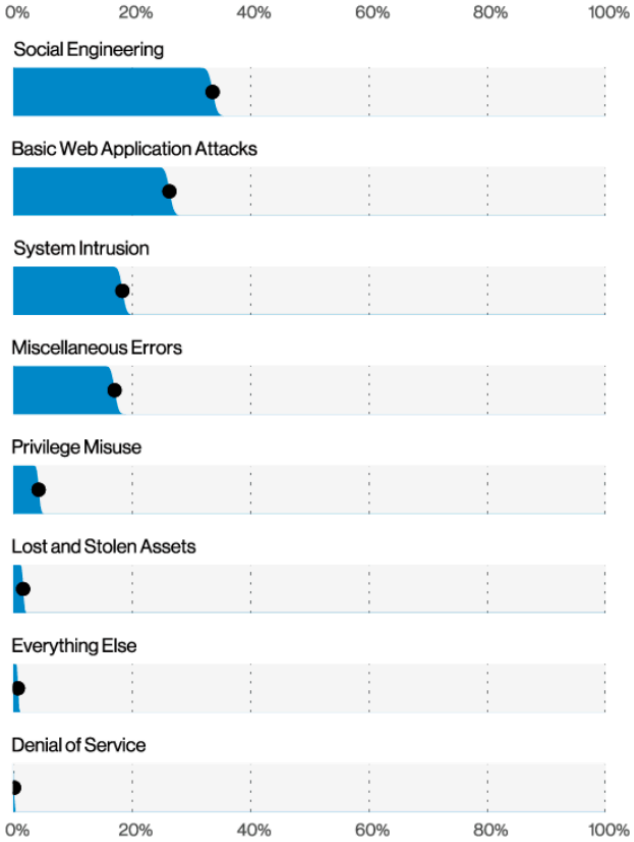
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

2021 | 2020 | 2019 | 2018 | 2017 | 2016 | 2015 | 2014 | 2013 | 2012 | 2011 | 2010 | 2009 | 2008 | 2007 | 2006 | 2005 | 2004

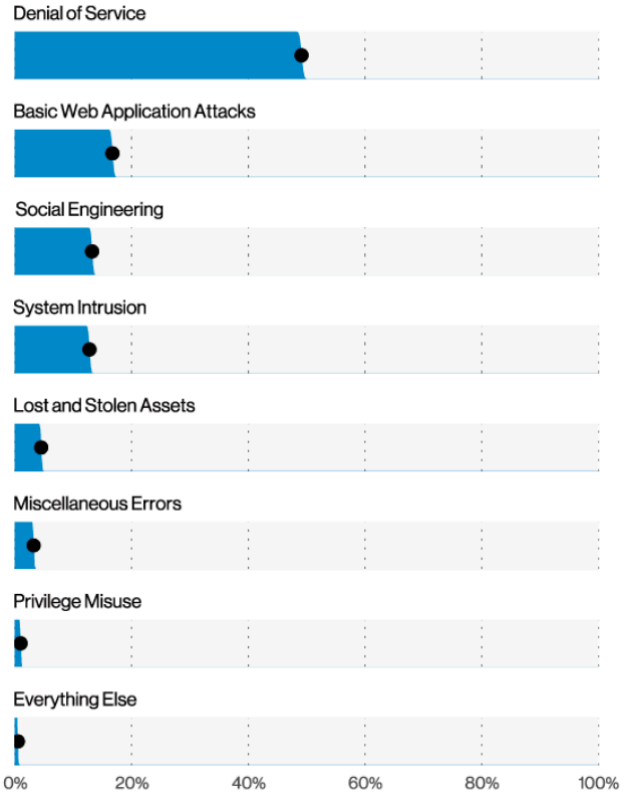
AA21-291A : BlackMatter Ransomware
AA21-287A : Ongoing Cyber Threats to U.S. Water and Wastewater Systems
AA21-265A : Conti Ransomware
AA21-259A : APT Actors Exploiting Newly Identified Vulnerability in ManageEngine ADSelfService Plus
AA21-243A : Ransomware Awareness for Holidays and Weekends
AA21-229A : BadAlloc Vulnerability Affecting BlackBerry QNX RTOS
AA21-209A : Top Routinely Exploited Vulnerabilities
AA21-201A : Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013
AA21-200B : Chinese State-Sponsored Cyber Operations: Observed TTPs
AA21-200A : Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China's MSS Hainan State Security Department
AA21-148A : Sophisticated Spearphishing Campaign Targets Government Organizations, IGOs, and NGOs
AA21-131A : DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks
AA21-116A : Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders
AA21-110A : Exploitation of Pulse Connect Secure Vulnerabilities
AA21-077A : Detecting Post-Compromise Threat Activity Using the CHIRP IOC Detection Tool
AA21-076A : TrickBot Malware

Security in Numbers

Patterns in successful attacks

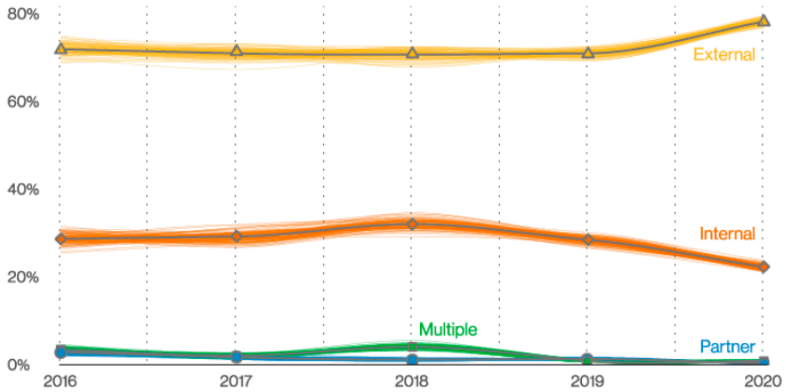


Patterns in all attacks

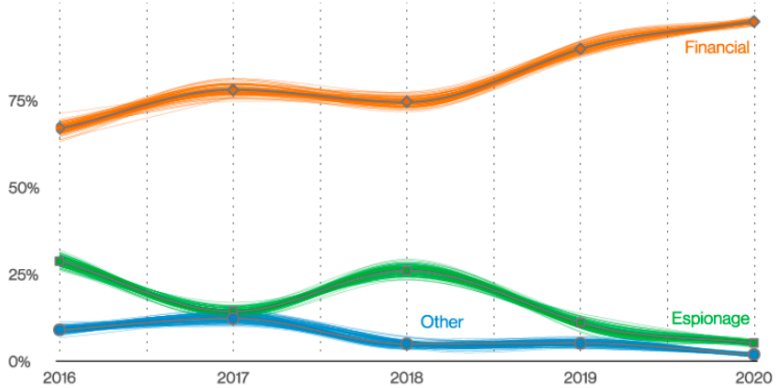


Security in Numbers

Threat actor in successful attacks

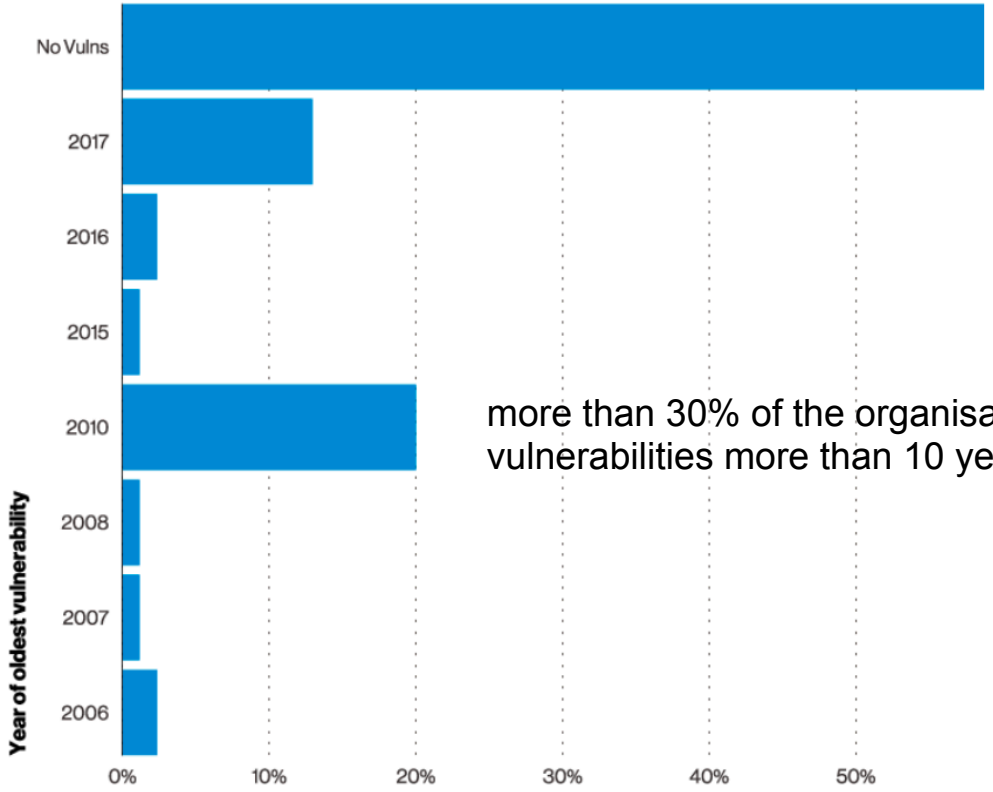


Motive in successful attacks



Security in Numbers

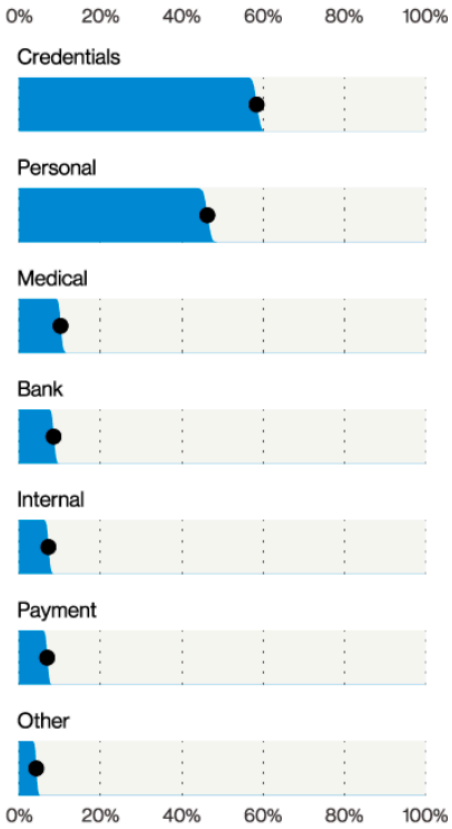
Oldest Internet-facing vulnerabilities in organisations



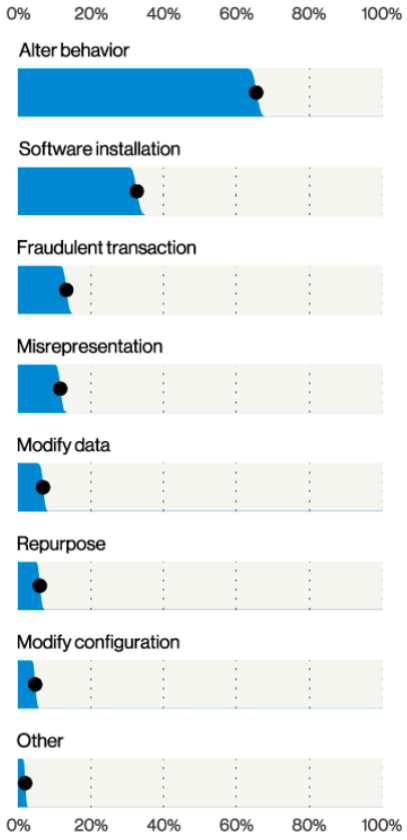
more than 30% of the organisations have vulnerabilities more than 10 years old!

Security in Numbers

Top data stolen (confidentiality)



Top modifications (integrium)

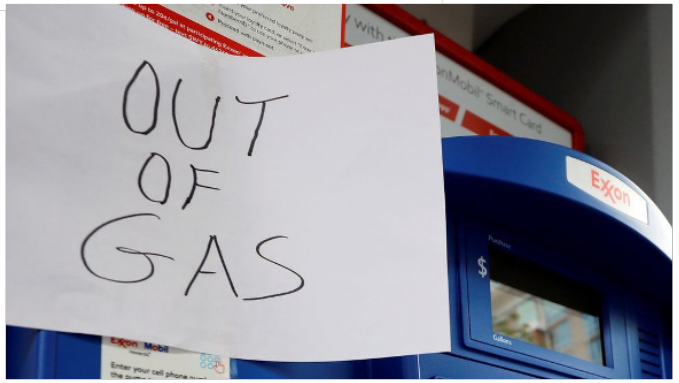


Source: Internet Security Threat Report Symantec 2017

Example: Energy (2021)

US offers $10m bounty for Colonial Pipeline hackers

6 de Novembro de 2021



The United States government has offered a bounty of up to $10million (£7.4m) for information about the hacking group known as DarkSide.

In May, a DarkSide ransomware attack shut down a vital 5,500-mile-long fuel pipeline on the east coast of the US.

The pipeline carries 45% of the fuel used on the east coast.

The bounty is offered for information which can lead to the "identification or location of any individuals" in a leadership position with DarkSide.

Example: Financial Firms (2015)

Study: Financial Firms Hit Hard By Targeted Attacks

POSTED BY: PAUL JUNE 25, 2015 12:16 0 COMMENTS

the security ledger

A graphic shows threats targeting financial industry organizations vs. non financial services focused attacks in purple. (Image courtesy of Websense/Raytheon.)

In-brief: A new report from the firm Websense finds that financial services firms are being hit hard by cyber attacks, including targeted attacks aimed at luring employees into installing malicious software on corporate networks.

Example: Healthcare (2018)

Hospitais da CUF alvo de ataque informático

O sistema informático dos hospitais do grupo CUF sofreu um ataque que impede a utilização dos computadores do grupo. Impacte ainda está a ser avaliado

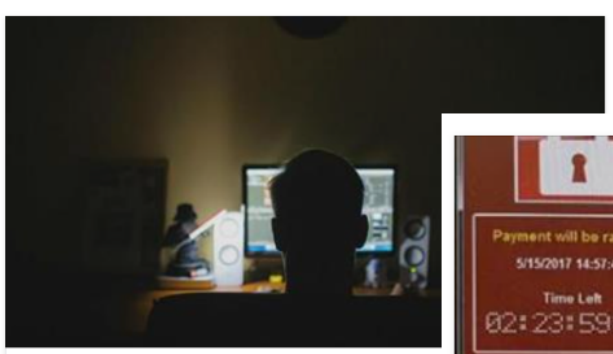
Carlos Ferro
04 Agosto 2018 — 10:59

Example: Large Companies (20xx)

CEO Fraud is a scam in which cybercriminals spoof company email accounts and impersonate executives to try and fool an employee in accounting or HR into executing unauthorized wire transfers, or sending out confidential tax information.

The FBI calls this type of scam "Business Email Compromise" and defines BEC as "a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds."

Example: Many Companies - WannaCry (2017)



Empresas e bancos alvos de ataque infor

Na PT, trabalhadores receberam ordem para desligar as m
ser mandados para casa. Veja a mensagem recebida pelos
PT

TVI24.IOL.PT

NHS hit by massive ransomware attack, many hospitals and clinics offline

The ransomware attack appears to be spreading to more NHS trusts.

ARSTECHNICA.CO.UK

Ataque informático. O que foi, como se espalhou, quem o travou

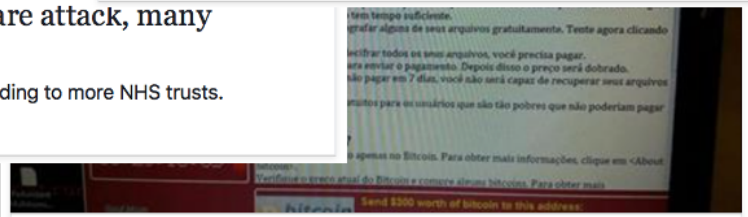
Um poderoso vírus entrou por uma falha do Windows e alastrou na rede. Criou o caos em hospitais e empresas de todo o mundo.

OBSERVADOR.PT

Portugal Telecom alvo de ataque informático internacional

A Portugal Telecom é um dos alvos do ataque informático que afetou várias empresas em Portugal, Espanha e Alemanha. A espanhola Telefónica é outr...

OBSERVADOR.PT

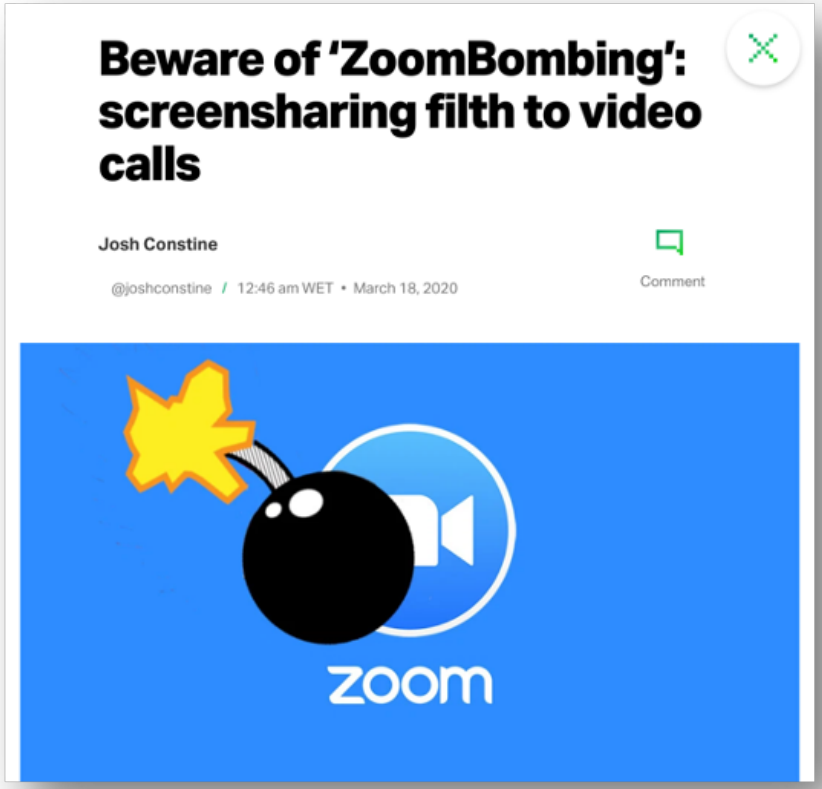


Ataque informático mundial: empresas portuguesas afetadas

Vírus afeta apenas os utilizadores que tenham sistema operativo da Microsoft

DN.PT | POR DIÁRIO DE NOTÍCIAS

Example: Everyone (2020)

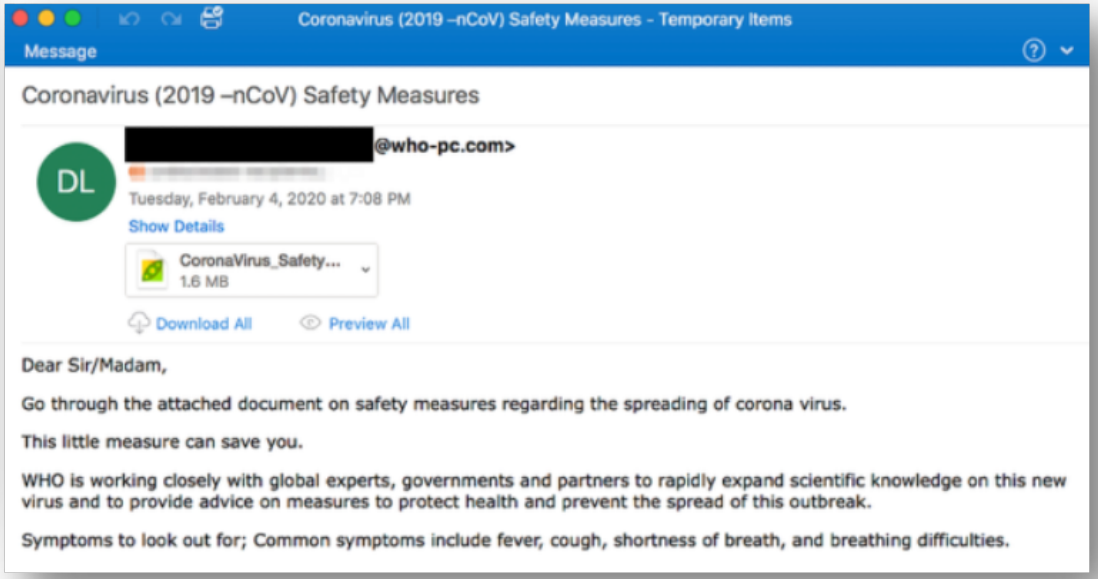


Beware of 'ZoomBombing': screensharing filth to video calls

Josh Constine

@joshconstine / 12:46 am WET • March 18, 2020

Comment



Coronavirus (2019 –nCoV) Safety Measures - Temporary Items

Message

Coronavirus (2019 –nCoV) Safety Measures

DL [redacted]@who-pc.com>

Tuesday, February 4, 2020 at 7:08 PM

Show Details

CoronaVirus_Safety... 1.6 MB

Download All Preview All

Dear Sir/Madam,

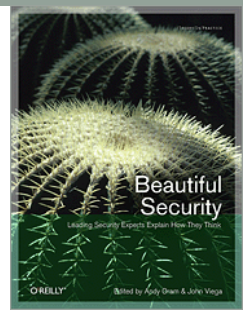
Go through the attached document on safety measures regarding the spreading of corona virus.

This little measure can save you.

WHO is working closely with global experts, governments and partners to rapidly expand scientific knowledge on this new virus and to provide advice on measures to protect health and prevent the spread of this outbreak.

Symptoms to look out for; Common symptoms include fever, cough, shortness of breath, and breathing difficulties.

The Problem is Software



"the current state of security in commercial software is rather distasteful,

marked by embarrassing public reports of vulnerabilities and actual attacks,

scrambling among developers to fix and release patches,

and continual exhortations to customers to perform rudimentary checks and maintenance."

Jim Routh, *Forcing Firms to Focus: Is Secure Software in Your Future*, in Beautiful Security, O'Reilly, 2010

Industry's Fault?

"Software buyers are literally crash test dummies

for an industry that is remarkably insulated against liability, accountability, and responsibility

for any harm, damages or loss that should occur because of manufacturing defects or weaknesses

that allow cyber attackers to break into and hijack our computer systems."

David Rice. *Geekonomics: The Real Cost of Insecure Software*, Addison-Wesley, 2007


Exploit
Wednesday

Universities' Fault?

"We at Oracle have (...) determined that most developers we hire have not been adequately trained in basic secure coding principles (…)

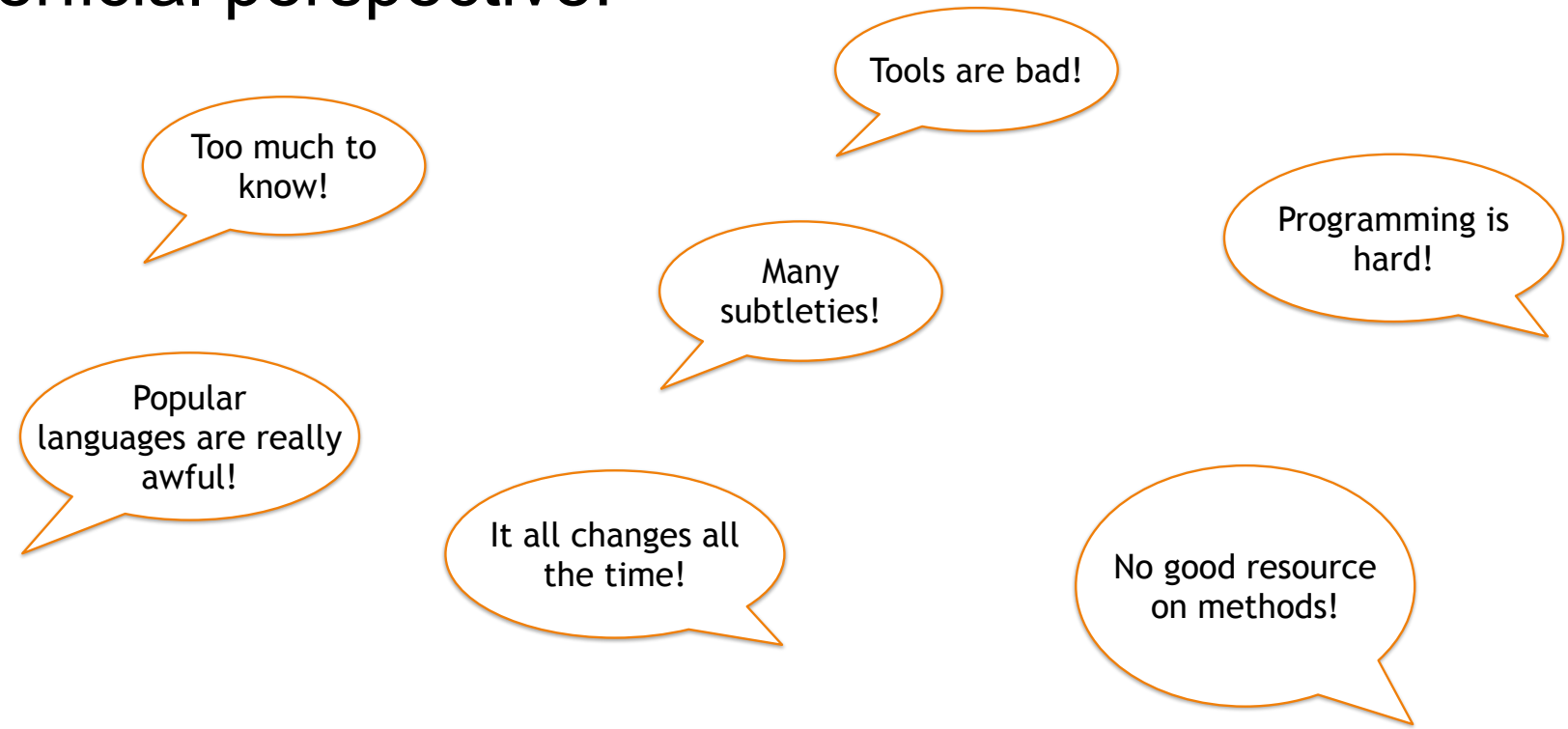
We have therefore had to develop and roll out our own in-house security training program at significant time and expense. (...)

In the future, Oracle plans to give hiring preference to students who have received such training and can demonstrate competence in software security principles."

Mary Ann Davidson, Oracle's Chief Security Officer, 2008

Why is Software Security hard?

Superficial perspective:



Why is Software Security hard?

A more insightful perspective:

3 trends in modern computing systems makes them more susceptible to security problems, and makes it harder to secure them:

The trinity of trouble

- Complexity
- Extensibility
- Connectivity

Complexity

- Attacks exploit *bugs* called vulnerabilities
  - estimated 5-50 bugs per 1000 lines of code
  - approximately 5 if rigorous quality assurance

Khalil Sehnaoui @sehnaoui · 1h

First Law of Software Quality:

errors = (more code)²

$e = mc^2$

Complexity

- Space Shuttle 0.4M LoC
- F22 Fighter Jet 2M LoC
- Hubble Telescope 2M LoC
- LHC. 4M LoC (50M)
- Mars Rover 5M LoC
- Boeing 787 6M LoC (16M)

- Windows 3.1 3M LoC
- Windows 95 5M LoC
- Linux Kernel (pre 4.2) 20M LoC
- Windows XP 40M LoC
- Windows Vista 50M LoC
- Windows 10 50M LoC
- Facebook 60M LoC
- MAC OS X 10.4 85M LoC
- Carro 100M LoC

(estimate 5-50 bugs for each 1000 LoC)

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


How many lines of code does it take to program them
Apollo 11
145,000
Mars Curiosity Rover
2,500,000
Android operating system
12,000,000
Large Hadron Collider (CERN)
50,000,000
Self-driving car
300,000,000

Extensibility

- Current SW is inherently extensible:
  - Device drivers, plug-ins, extensions, modules, Apps,....
  - Virtual machines and mobile code (JavaScript, Java, …)
  - Combination of several components and forms of code execution (web apps)
  - Apps in mobile phones/tablets
- Problems:
  - What is “the software”? How do you ensure its security?
  - Mobile malicious code: worms, virus,…

Connectivity

- Internet *(PCs, smartphones, tablets,…)*
  - Small failures can propagate widely
  - Allows automated attacks
    - Major worms 99-04: Melissa, ILOVEYOU, Code Red, Sircam, SQL Hammer, Blaster, Sobig, Mydoom, Sasser, Witty
    - DDoS attacks (400 Gbps record, Feb. 2014)
  - Economic risk
    - SWIFT net connects 10000+ financial institutions and moves zillions of dollars daily; targeted attacks at banks
    - Digital asset market cap of 2.3×10^{12}€ https://coinmarketcap.com/
  - Distance and feeling of safety

Connectivity: Internet of Things

- Not only cable and WiFi but also GSM/3G/4G/5G, Bluetooth, NFC,...


Sale
Connected Appliances
klossner
"CAN I INTEREST YOU IN A FIREWALL FOR YOUR TOASTER?"

The 4th trouble: Motivation

- Theft and extortion
  - homebanking, credit cards, blackmailing…
- Espionage
  - obtaining intelligence for strategic advantage between nation, corporations
- War and Terrorism
  - Estonia, Georgia, Ucrania…
- Ideology, fame,…

(Near) Future of SW

- More components
- More frameworks, more combination of binary and executed code
- More wireless / celular (5G)
- More mobile devices and embedded “things”
- More distribution
- More mobile code
- Subscription services
- *More complexity, extensibility, connectivity*

Questions Raised in this Course

- What forms of software security vulnerabilities are there and how can they be exploited?
- How can we develop secure software?
- What are the fundamental mechanics behind the vulnerabilities?
- How can we design techniques and tools to prevent or fix them?

Goals of this Course

- To understand software vulnerabilities
  - *To know the problem*
- To develop secure software
  - *To apply solutions to our problem*
- To design correct enforcement mechanisms
  - *To create new solutions for our problem*