EUNIS InfoSEC 2024 Athens

37 years of personal story

Victoriano Giralt

Head of Systems Administration Unit
Central ICT Services
University of Málaga

EUNIS pre-conference
Athens
June 4th, 2024

UNIVERSIDAD DE MÁLAGA

Abuelo Cebolleta by Vázquez

Late ’80

- VAX 11/30
- X.25
- EARN/BitNet
- X.400
- DECnet
- Campus 10base5 Ethernet
- The terminal is king

Early ’90s

- Ponds of 10base2 Ethernet
- Lucky ones have 10baseT
- 64Kb/s PtP
- 2Mb/s radiolinks in Andalusia
- TCP/IP with lots of /24 :-)
- Nothing is encrypted
  (but no tcpdump)
- SMTP and POP appear
- tcpwrappers and ACLs

https://museum.ipsj.or.jp/en/computer/unix/0001.html

Late ’90s

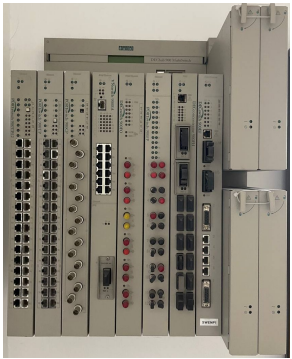
- The web explodes
- The commecial Internet
- Homes can conect thanks to PPP
- Linux democratices the server
- First scanning attacks (lpd hole)
- TCPwarpers are not enough
- ipchains
- first protocols with *S*

Initial 21st century

- First Gigabit links
- ADSL brings bandwidth to the home
- Lots of *bad guys* with time and bandwidth
- Transition to iptables
- Encryption has to be mandated
- *Know your baseline*
- Come the IDS
- It's not ***if*** anymore but ***when***

Current times

- EDR, XDR, . . .
- Deep packet inspection
- Content inspection (*split encryption*)
- *The cloud*
- Filters everywhere
- More *noise* than *signal*
- Lighting fast GPUs



What lays ahead

- AI *to the rescue?*
  See:
  “OpenAI’s GPT-4 Can Autonomously Exploit 87% of One-Day Vulnerabilities”
  `https://www.techrepublic.com/article/openai-gpt4-exploit-vulnerabilities/`
- LLMs mixed control and dataplanes
  See:
  `https://www.schneier.com/essays/archives/2024/05/llms-data-control-path-insecurity.html`
- Quatum

Virustotal: the inception

- Bernardo Quintero, through Hispasec, was comparing antivirus results for PC Actual
- The group decides to automate the work
- This was transformed into a service where users could check their files
- VirusTotal independence allows antivirus companies to share results
- Thus, better results for everybody
- Everybody is happy :-)

Virustotal: condo house to Google Málaga

- Condition to Google for acquiring VirusTotal: the team **MUST** work from Málaga
- The American giant is forced to open office in Málaga
- The condo house is bought
- The house is too small due to business growth
- New office in Ada Byron building in UMA campus
- The old Army headquarters in Málaga is on sale
- Building is restored and Google settles by Málaga harbour

Why top businesses noticed Virustotal

- 2011: Bernardo Quintero tweets about stuxnet malware
- Stuxnet was the first cyberweapon with media coverage
- First time cyberwar is mentioned
- Bernardo offered information not even American inteligence had, thanks to Virustotal data

Thank you!

Thank you!

Questions?

answers not assured