VPGC
distinct.smart.innovative

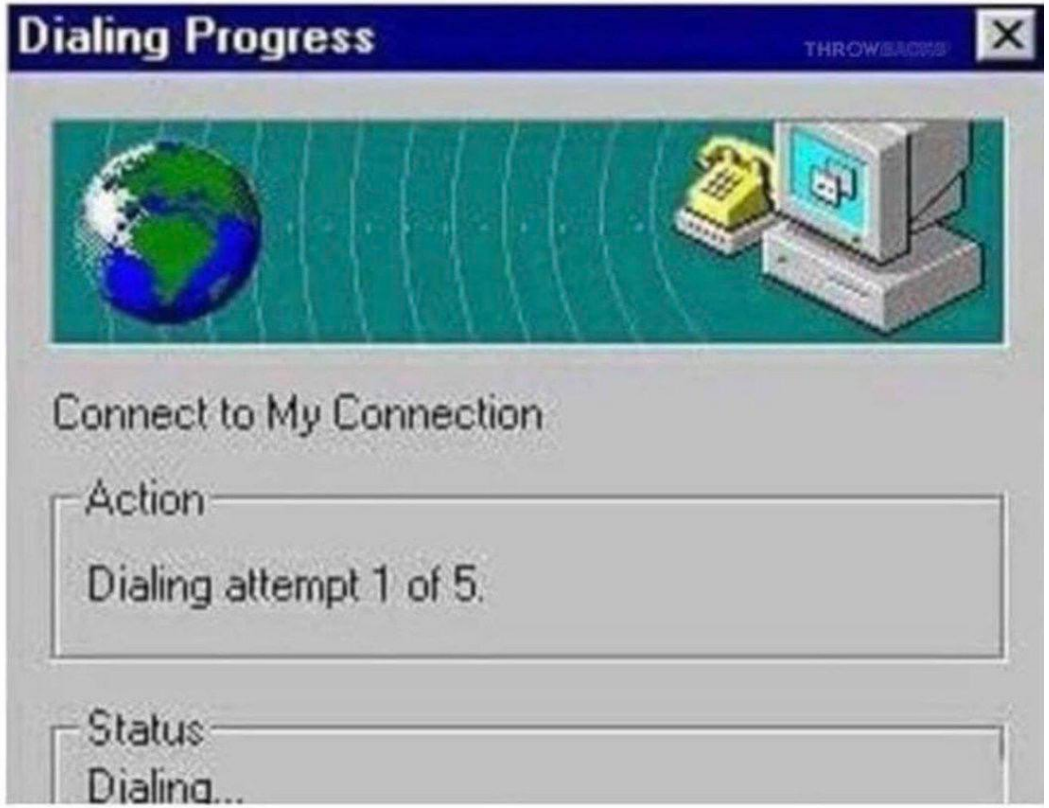
Kam kráčí NETSEC?

Vjačeslav Petraševskij

VPGC
distinct.smart.innovative

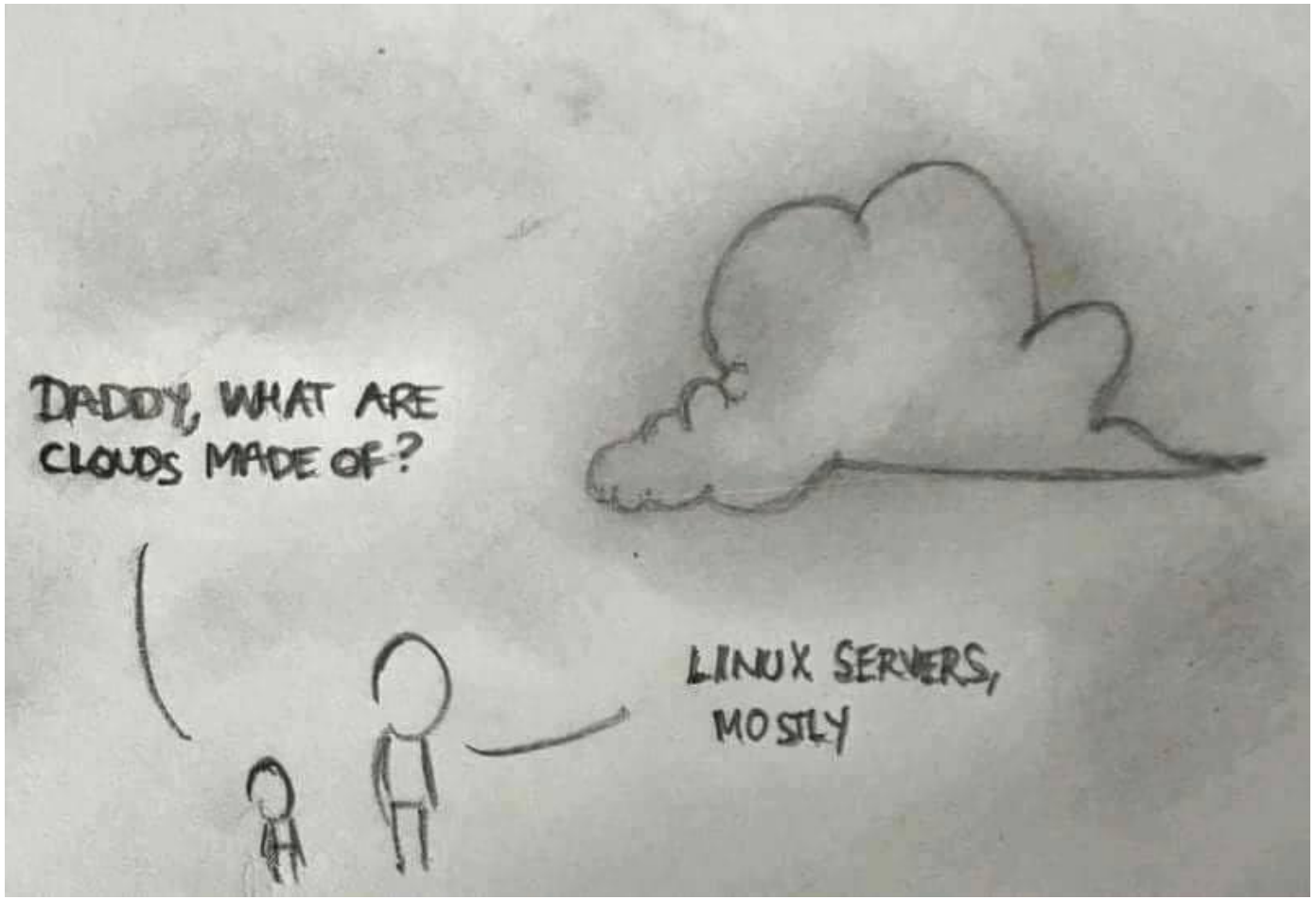
VPGC
distinct.smart.innovative

Kids now complaining about waiting 5 seconds for Netflix to load, meanwhile we had to live through this



VPGC
distinct.smart.innovative

VPGC
distinct.smart.innovative

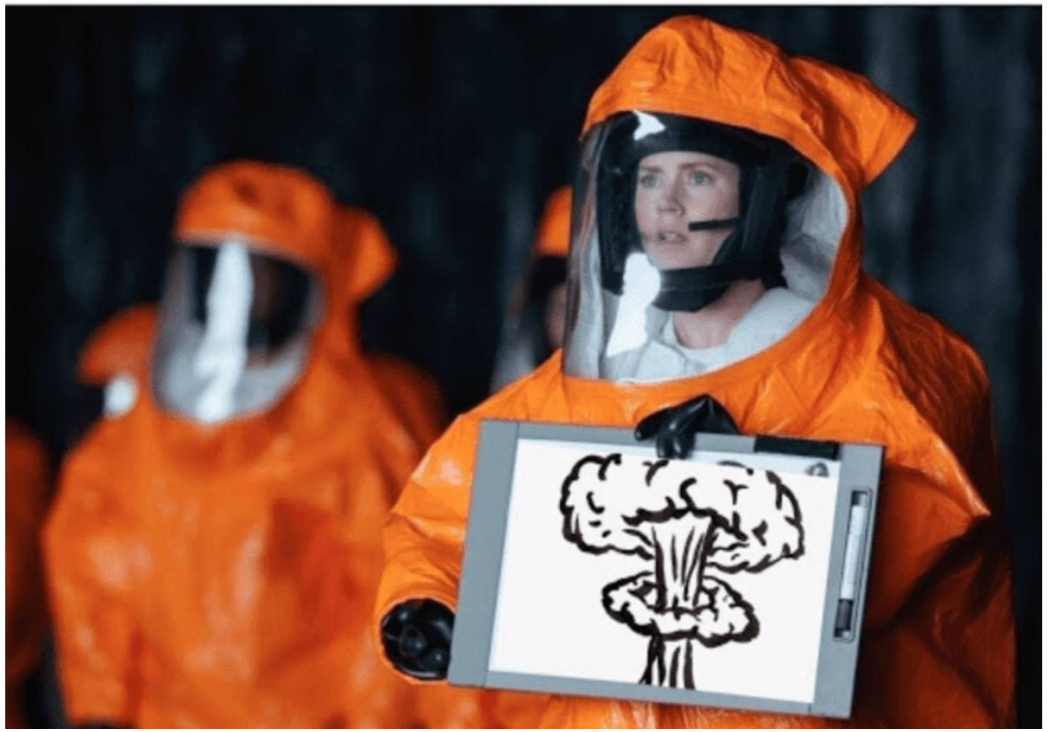


VPGC
distinct.smart.innovative

VPGC
distinct.smart.innovative

VPGC
distinct.smart.innovative

Trying to explain our current cyber risk to the board



VPGC
distinct.smart.innovative

VPGC
distinct.smart.innovative

VPGC
distinct.smart.innovative

Onel de Guzman

VPGC
distinct.smart.innovative

VPGC
distinct.smart.innovative

Industry 4.0

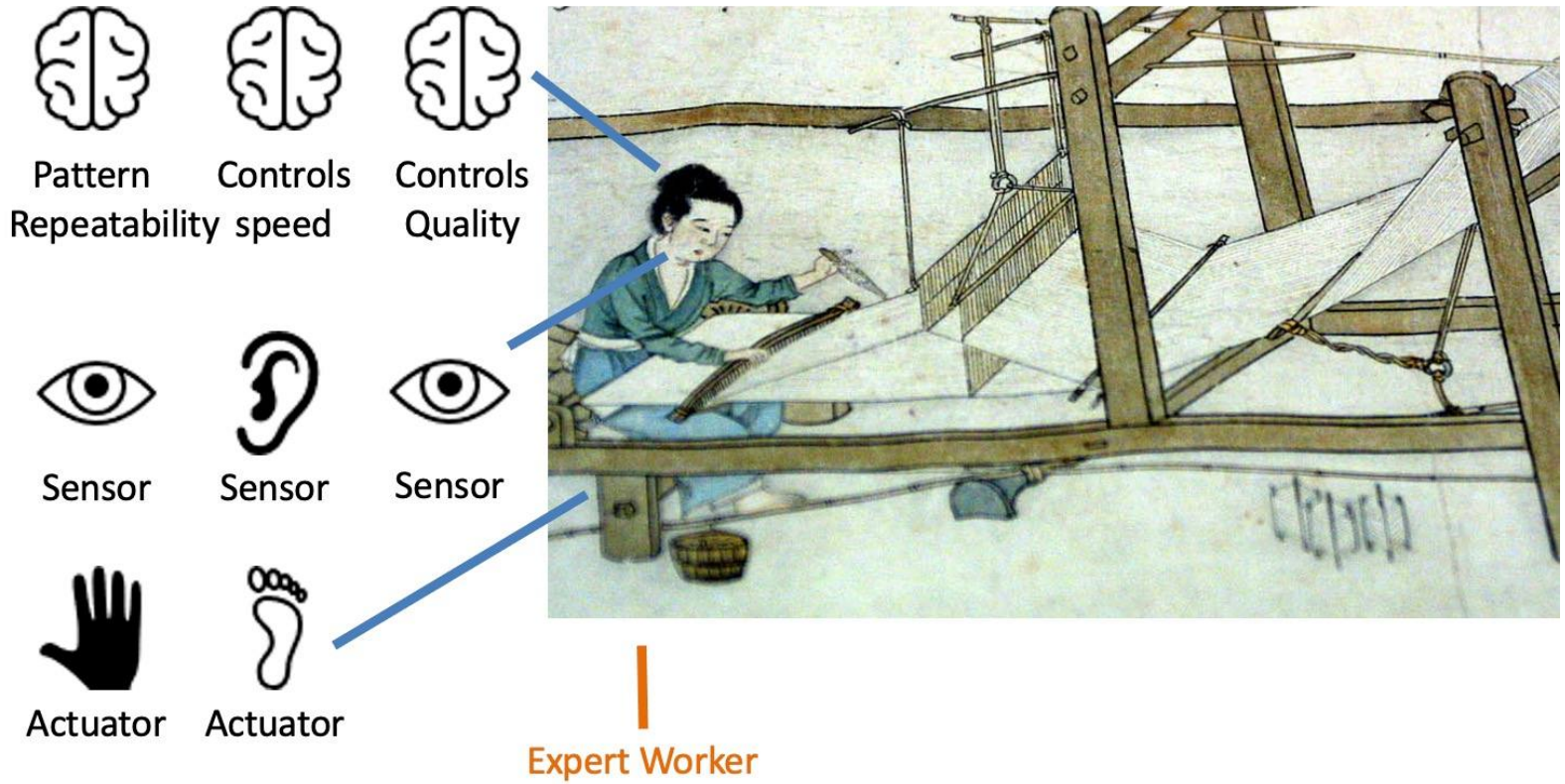
IT / OT convergence

ICS Security

https://searchitoperations.techtarget.com/definition/IT-OT-convergence

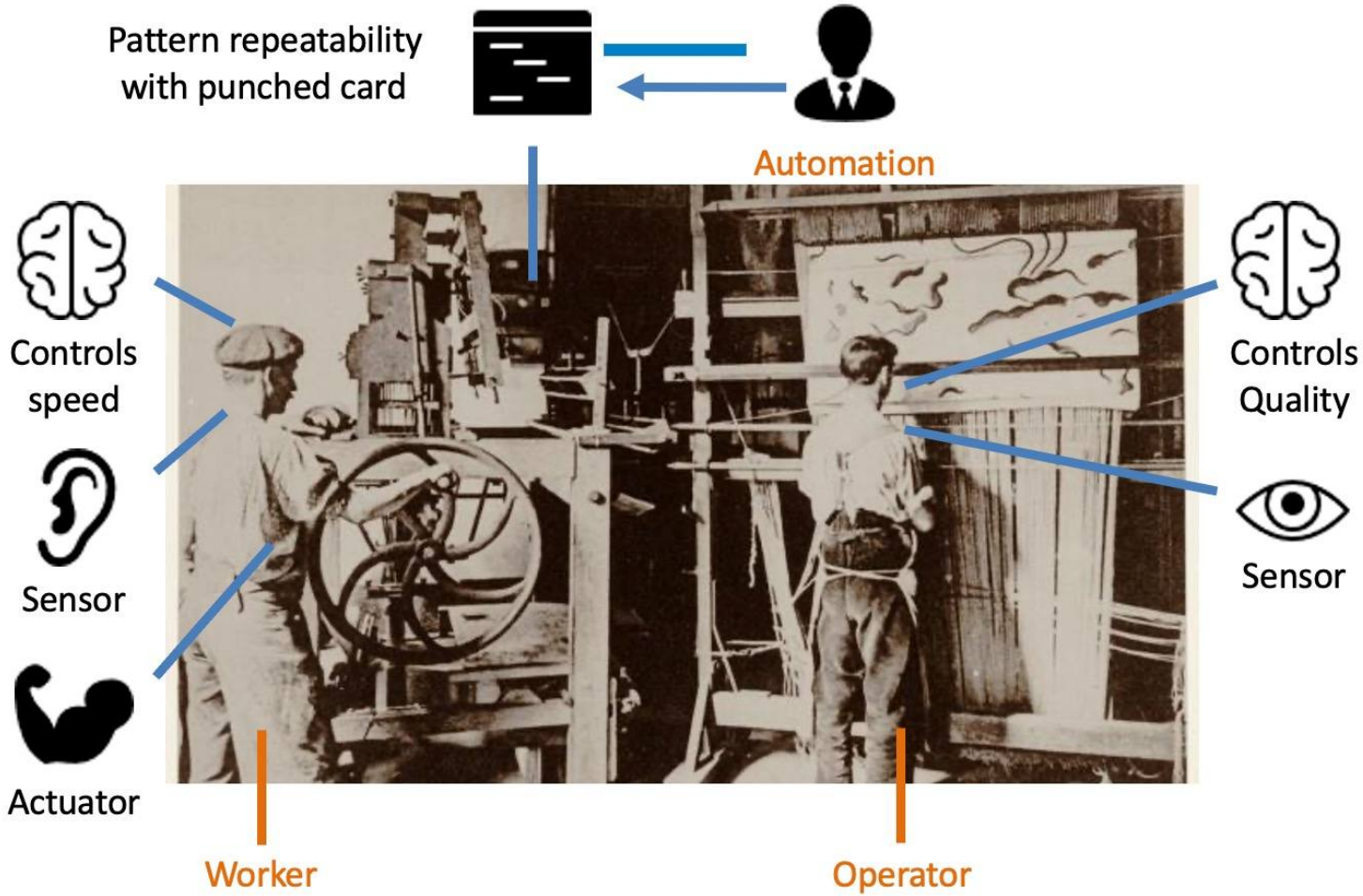
VPGC
distinct.smart.innovative

ISC HISTORY – SILK PRODUCTION FULLY MANUAL



VPGC
distinct.smart.innovative

ICS HISTORY – SILK PATTERN AUTOMATION

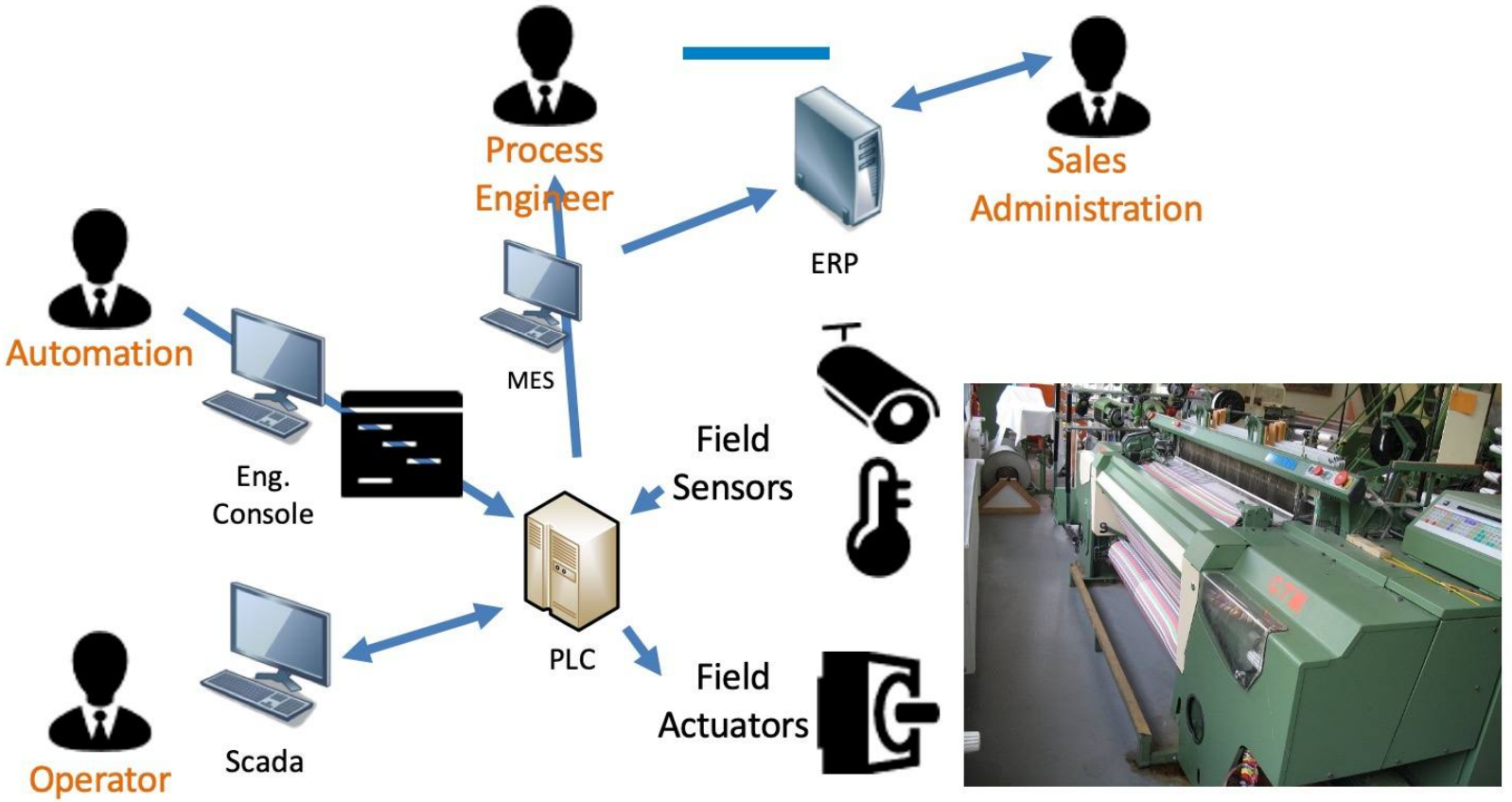


(steam, electricity)

Industry 1/2.0

VPGC
distinct.smart.innovative

ICS HISTORY – COMPUTERISED INDUSTRIAL WORLD

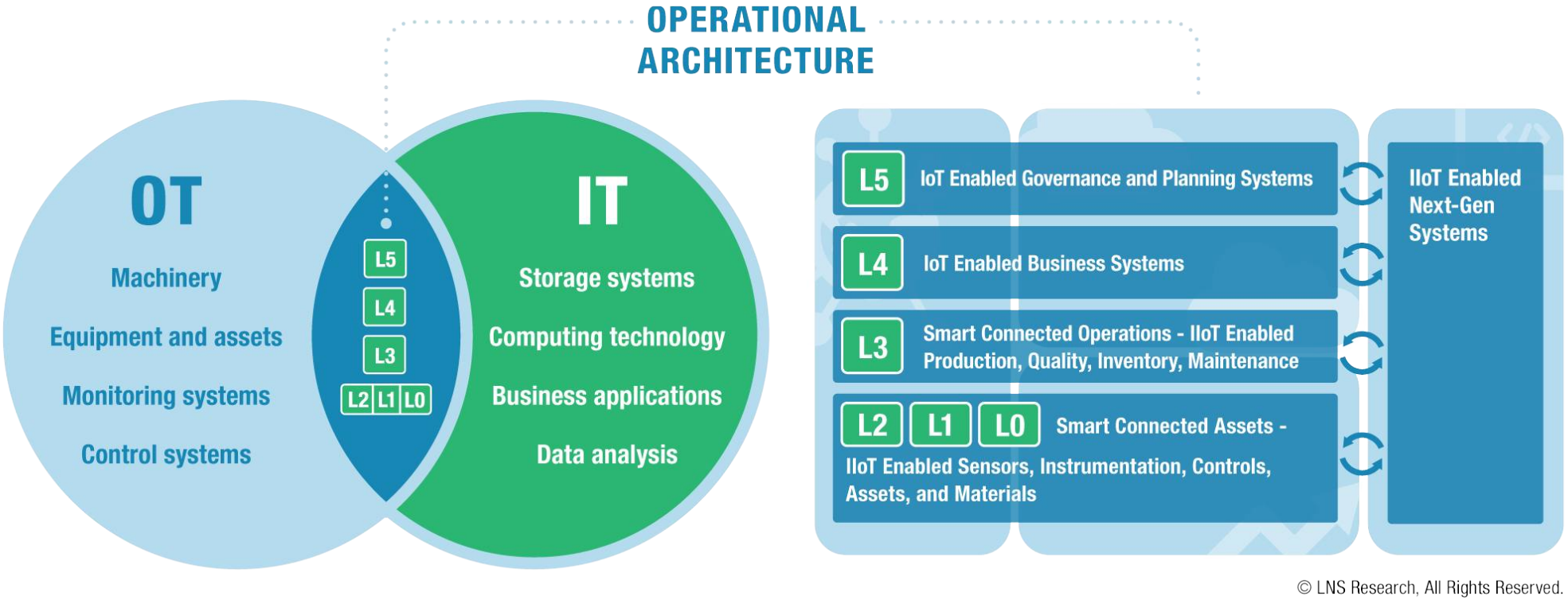


(PLC, computers & data)

Industry 3/4.0

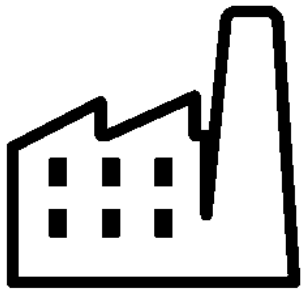
https://www.stormshield.com/tag/cybersecurity-first-steps/

VPGC
distinct.smart.innovative



https://blog.lnsresearch.com/operationalarchitecture

VPGC
distinct.smart.innovative

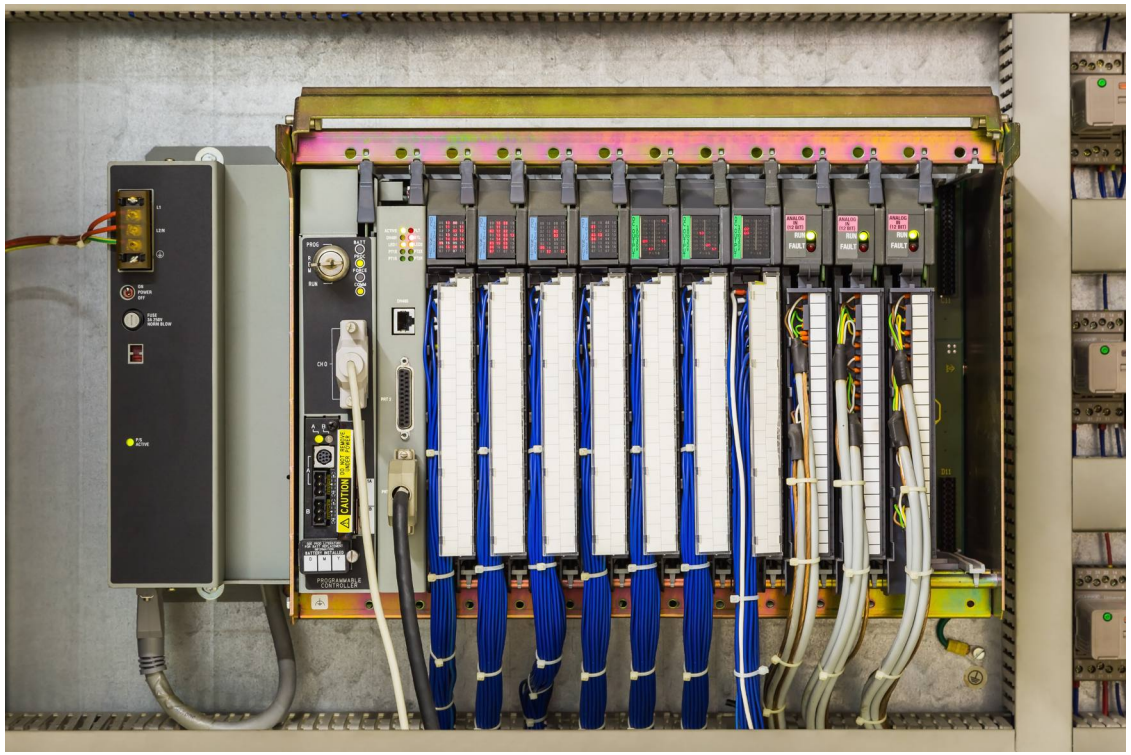


INDUSTRIAL (OT) vs IT

- Industrial product life cycle is 20-30 years life cycle (Microsoft OSs have a 10-15 years)
- Automation teams are new in IT security field
- Maintenance operations can only occur when the process is shut down (once a year).
- Planning is often not negotiable by the automation/security team.

VPGC
distinct.smart.innovative

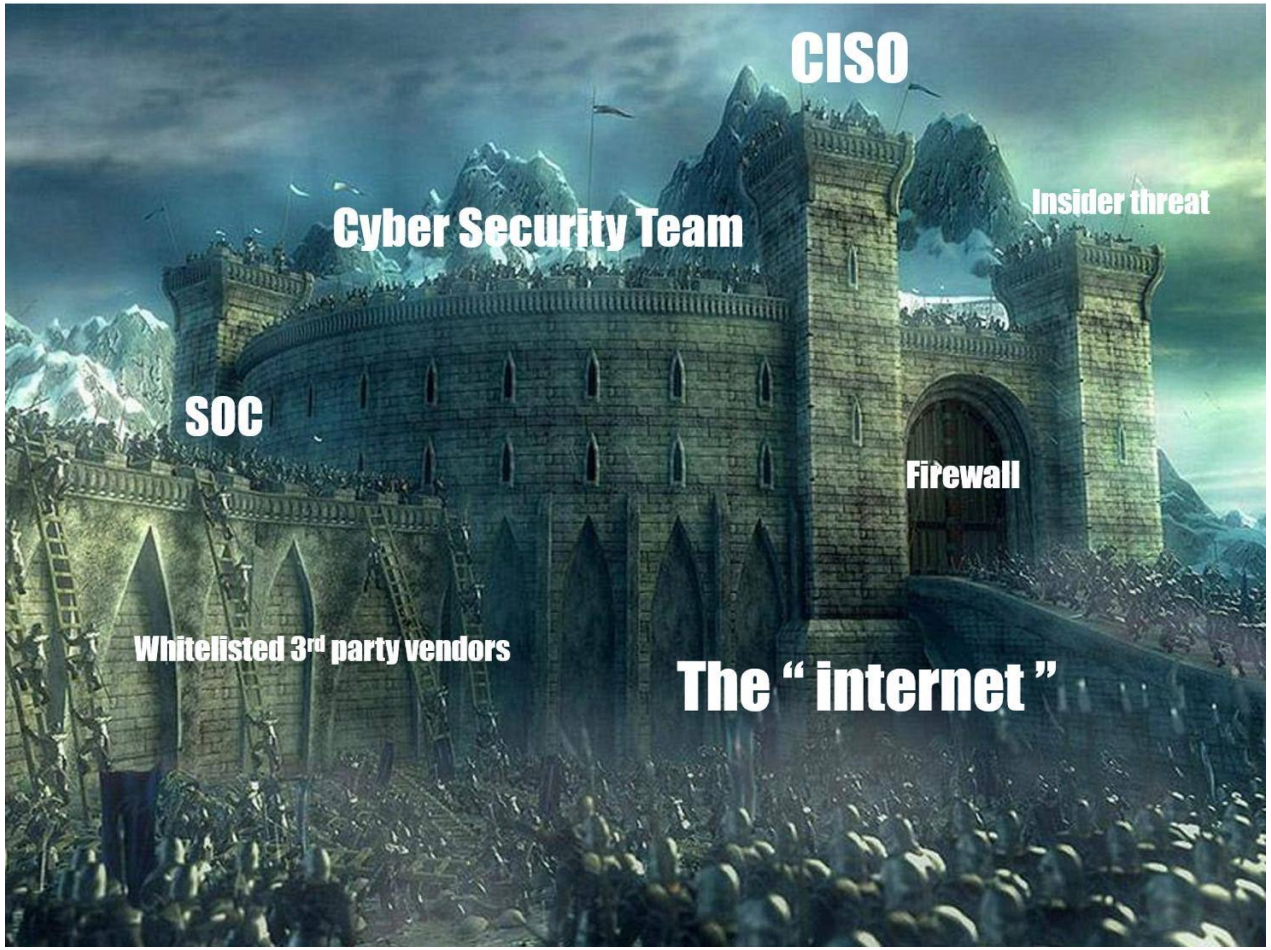
WHAT ARE INDUSTRIAL CONTROL SYSTEMS?



https://www.sans.org/blog/introduction-to-ics-security/
https://www.sans.org/blog/introduction-to-ics-security-part-2/

VPGC
distinct.smart.innovative

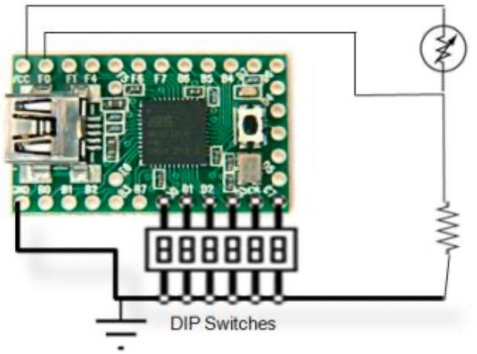
VPGC
distinct.smart.innovative

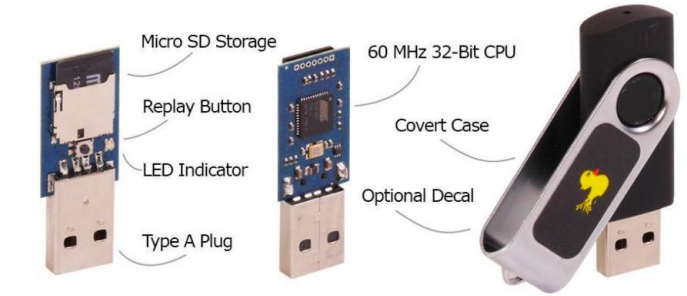


VPGC
distinct.smart.innovative

Offensive Devices – 1st Generation

- **Teensy – (PHUKD 2009 & Kautilya 2011)**
  - DIY Solution
  - Multiplatform (Win, *nix, OSX)
  - Multipayload (through DIP-Switches)
  - Cheaper (25 €)
- **Rubberducky (2010)**
  - Dedicated Hardware
  - Multiplatform (Win, *nix, OSX)
  - Can emulate Keyboard & USB Disk
  - Multipayload (CAPS-INS-NUM)
  - Changeable VID/PID
  - Expensive (55 €)





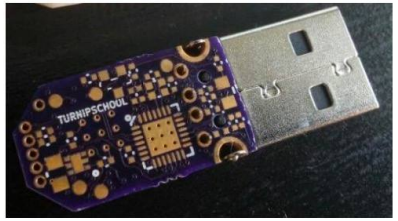
https://www.whid.ninja/

VPGC
distinct.smart.innovative

Offensive Devices – 2nd Generation

- **BadUSB (2014)**
  - It exploits the controllers (i.e. Phison) within commercial USB devices and turns them into a covert keystrokes injecting device.

- **TURNIPSCHOOL (2015)**
  - Is a hardware implant concealed in a USB cable. It provides short range RF communication capability to software running on the host computer. Alternatively it could serve as a custom USB device under radio control.

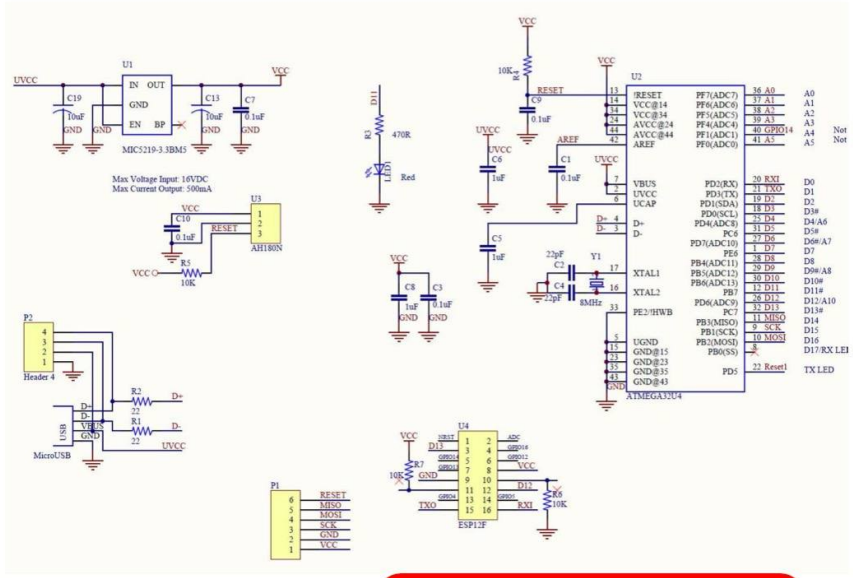


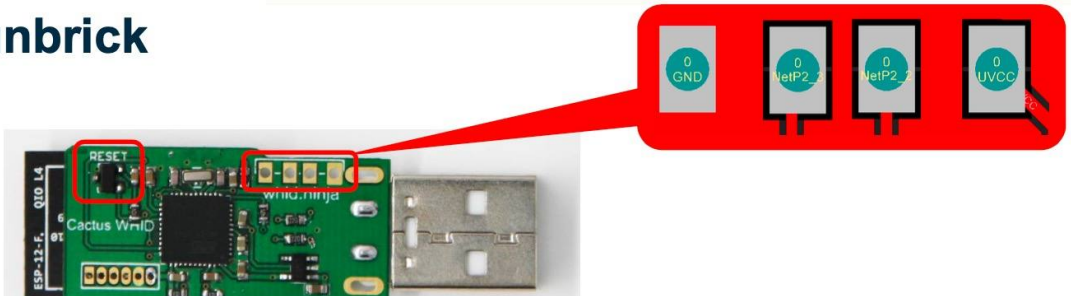
https://www.whid.ninja/

VPGC
distinct.smart.innovative

WHID Injector – Schematics & Specs

- **Atmega 32u4**
  - Arduino-friendly
- **ESP-12**
  - WiFi (both AP and Client modes)
  - TCP/IP Stack
  - DNS Support
  - 4MB Flash
- **Pinout for weaponizing USB gadgets**
- **HALL Sensor for easy unbrick**



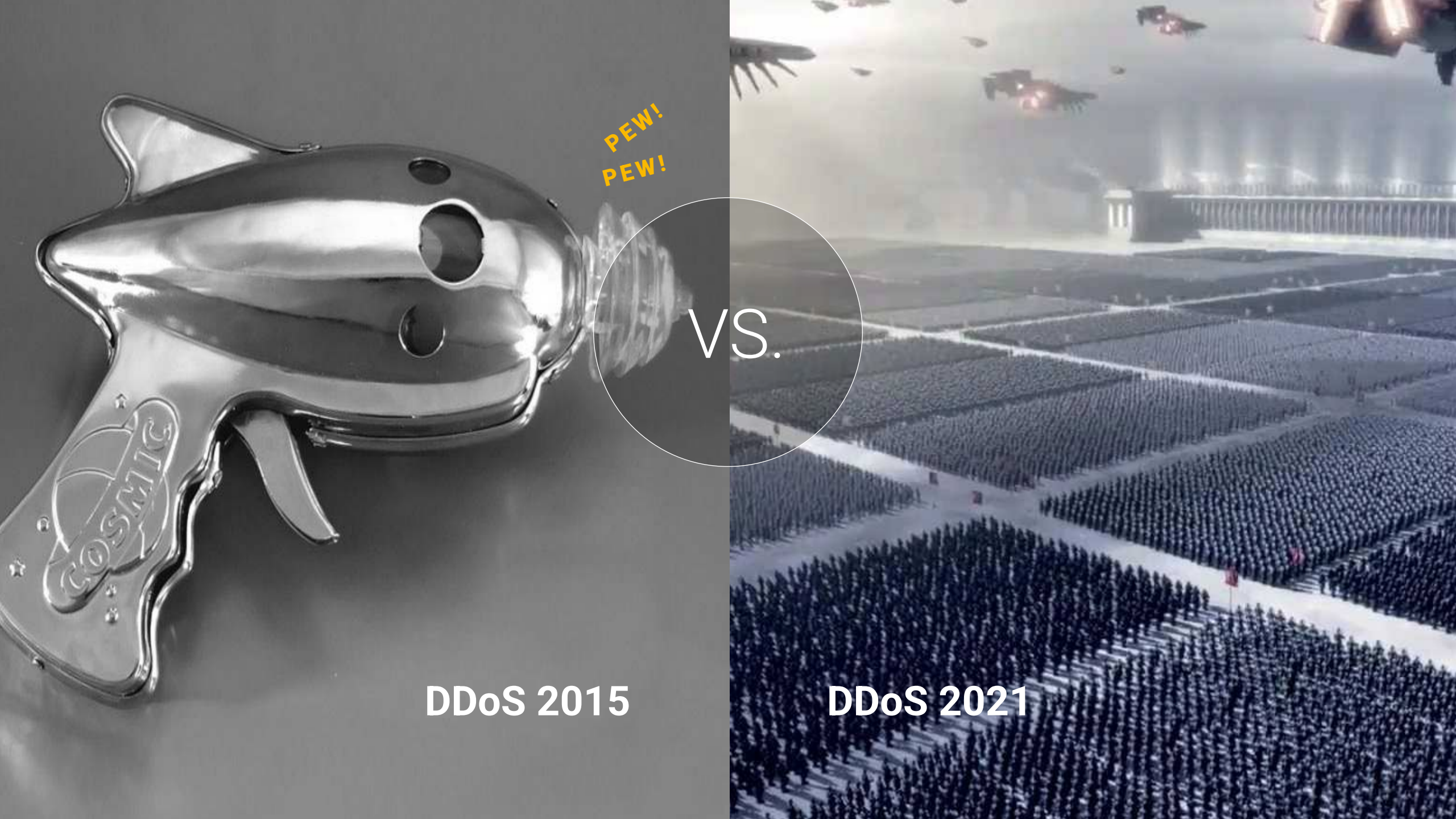


https://www.whid.ninja/

VPGC
distinct.smart.innovative

DDoS

https://www.comptia.org/content/guides/what-is-a-ddos-attack-how-it-works


PEW!
PEW!
COSMIC
VS.
DDoS 2015
DDoS 2021

VPGC
distinct.smart.innovative

Common Attack Motivations & Types

Why?

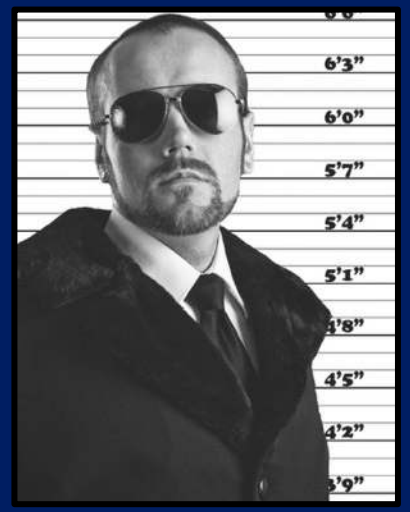
- Ransom and extortion
- Smokescreens for distraction
- Cyber warfare & political
- Hacktivism
- Boredom, fame or notoriety

How?

- DDoS for Hire
- Opensource & Freeware
- IoT botnets
  - Reflection & amplifications attacks
  - Network layer attacks
  - Application layer attacks
- Zero-day attacks

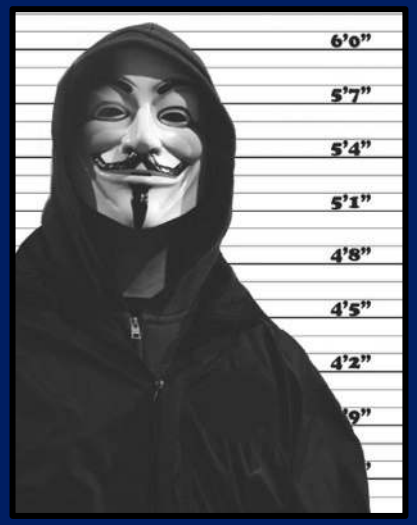
THE MANY FACES OF DDOS ATTACKERS

WANTED

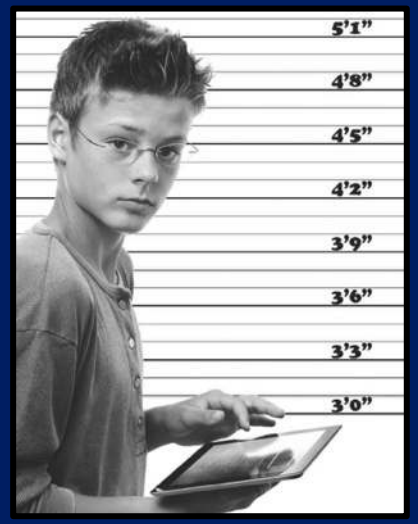


Cyber Criminal

Disgruntled Employee



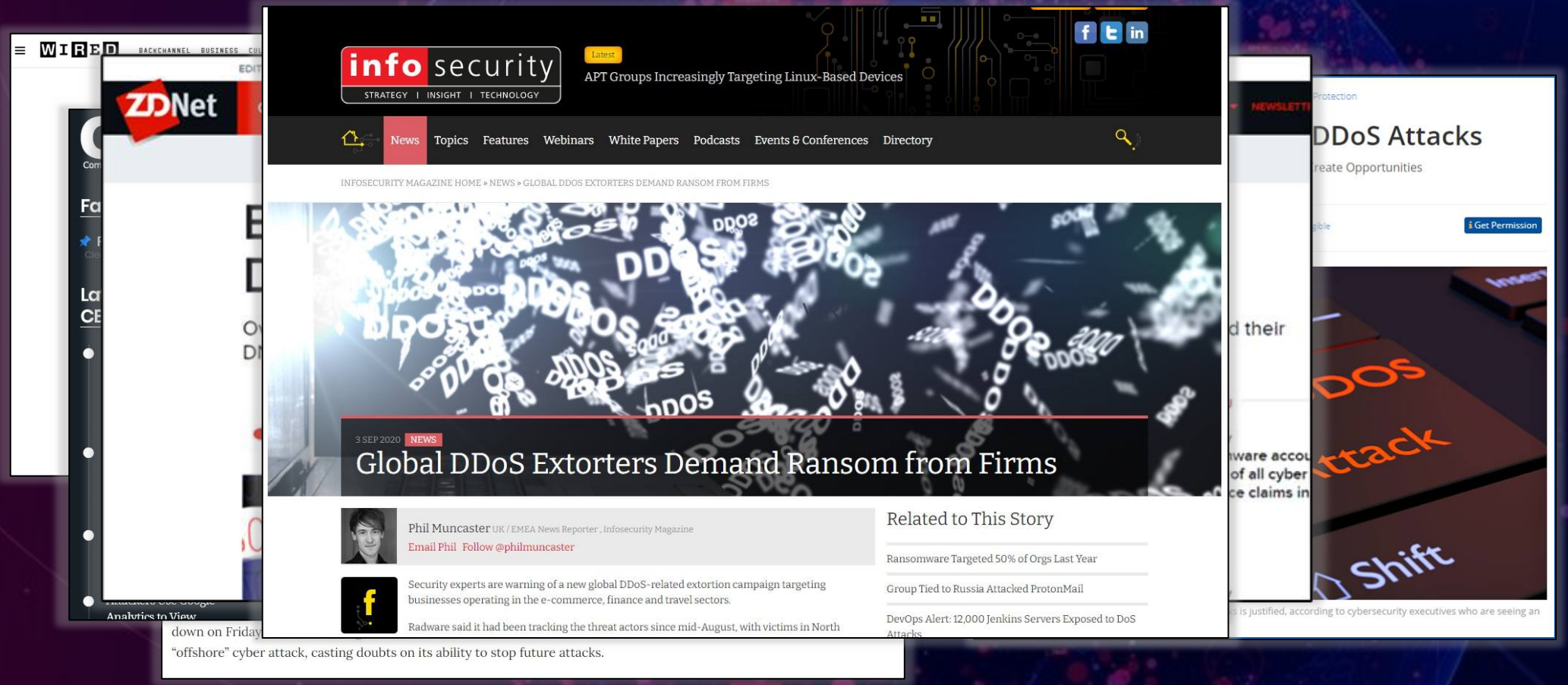
Hacktivist



Script Kiddie

Gamer

DDOS ATTACKS CONTINUE TO MAKE HEADLINES



Security News This Week: A Florida Teen Allegedly Shut Down Remote School With a DDoS Attack – https://www.wired.com/story/florida-teen-ddos-school-amazon-labor-surveillance-security-news/
CISA Warns of Increased DDoS Attacks – https://www.bankinfosecurity.com/cisa-warns-increased-ddos-attacks-a-14975
AWS Hit With a Record 2.3 Tbps DDoS Attack - https://www.cbronline.com/news/record-ddos-attack-aws#:~:text=AWS%20says%20it%20was%20hit,for%20three%20days%20in%20February
European ISPs report mysterious wave of DDoS attacks - https://www.zdnet.com/article/european-isps-report-mysterious-wave-of-ddos-attacks/
Global DDoS Extorters Demand Ransom from Firms - https://www.infosecurity-magazine.com/news/global-ddos-extorters-ransom-notes/
New Zealand Stock Exchange Shut Down by DDoS Cyber Attack - https://www.cpomagazine.com/cyber-security/new-zealand-stock-exchange-shut-down-by-ddos-cyber-attack/

VPGC
distinct.smart.innovative

Today's DDoS Attacks Are Frequent And Intense

Low Cost

$150 Buys **1-week** DDoS attack on the black market

TrendMicro Research

High Frequency

300% **Growth** in number of attacks in 2020

Securelist

High Intensity

4.5x Increase in attack **duration** for large attacks

Dark Reading

Under The Radar

75% Attacks were < 5Gbps in size and went largely undetected

Neustar

Costly Downtime

Single hour of downtime costs over

$300K+

ITIC Research

High Frequency – DDoS attacks in Q2 2020 - https://securelist.com/ddos-attacks-in-q2-2020/98077/
High Intensity – Q2 DDoS Attacks Triple Year Over Year: Report – https://www.darkreading.com/attacks-breaches/q2-ddos-attacks-triple-year-over-year-report/d/d-id/1338622
Under the Radar – 2019 DDoS Attacks The Hits Keep Coming - https://www.cdn.neustar/resources/infographics/neustar-infographic-ddos-attacks-keep-coming.pdf
Costly Downtime - Hourly Downtime Costs Rise – https://itic-corp.com/blog/2019/05/hourly-downtime-costs-rise-86-of-firms-say-one-hour-of-downtime-costs-300000-34-of-companies-say-one-hour-of-downtime-tops-1million/

VPGC
distinct.smart.innovative

The Looming Threat Of DDoS

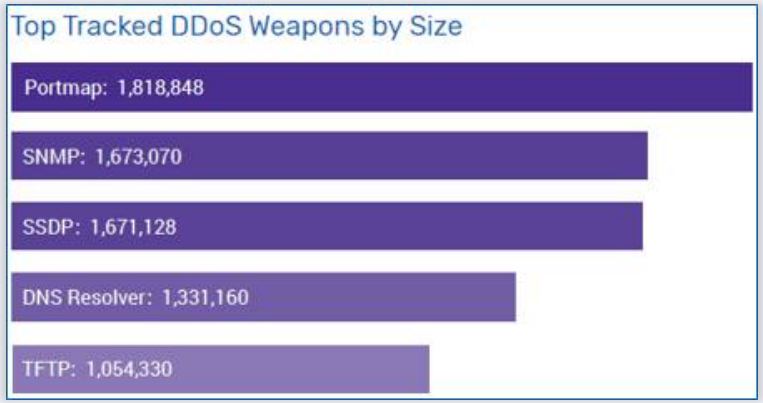
A Global Problem

DDoS weapons available **across the globe**, with the United States, China and Korea topping the list

United States	1,591,719
China	1,388,531
Korea	776,327
Russia	696,186
India	283,960

Massive Scale

Nearly **10 million potential DDoS weapons**, including open resolvers, IoT devices, publicly accessible servers and more



Increased Complexity

Malware-based recruitment of IoT devices as drones, leveraged for use in complex, multi-vector DDoS attacks

Binary Name	Malware Family
arm7	Gafgyt Family
Cloud.x86	Dark Nexus
mmmmh.x86	Mirai Family
Mozi.m	Gafgyt family
Mozi.a	Gafgyt family

https://www.a10networks.com/blog/threat-intelligence-report-ddos-attacks-intensify-in-q2-2020/

VPGC
distinct.smart.innovative

The DDoS Of Things

IoT devices can easily be compromised for use in large botnets

- Fueling large Amplification & Cloud attacks

Mirai – the DDoS attack trendsetter

- Sept 2016 – largest at the time (620 Gbps)
- Massive scale multi-vector attack (9+ vectors)
- 600,000+ IoT devices

Number of IoT devices will reach 29.3 billion by 2023*

UDP Random Flood	Floods random victim domain endpoints with spoofed UDP packets.
UDP Data Flood	Selects random victim domain endpoints & floods them with UDP packets & IP fragments.
TCP SYN Flood	Floods random victim domain endpoints with spoofed TCP SYN packets.
TCP ACK Flood	Floods random victim domain endpoints with spoofed TCP ACK packets.
TCP STOMP (Data) Flood	Intended to overcome DDoS mitigations; connects to random victim domain endpoints & floods them with TCP data.
HTTP Request Flood	Intended to overcome DDoS mitigations; connects to random HTTP endpoints in the victim's domain & floods them with HTTP requests.
DNS Water Torture Attack	Floods ISP recursive DNS servers with randomized queries to a victim base domain name, causing the ISP DNS servers to perform the attack on the victim's authoritative DNS servers. As victim DNS servers become overloaded, the ISP DNS servers retransmit attack queries to other authoritative DNS servers in the victim's enterprise.
Valve Gaming Server Attack	Floods random Valve streaming engine endpoints in the victim's domain with spoofed source-engine query packets.
GRE IP/Ethernet Floods	Floods random victim domain endpoints with spoofed GRE IP or IP-over-Ethernet-tunneled UDP packets.

Investigating Mirai https://www.a10networks.com/marketing-comms/white-papers/investigating-mirai/

**Cisco Annual Internet Report (2018–2023) White Paper* https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

VPGC
distinct.smart.innovative

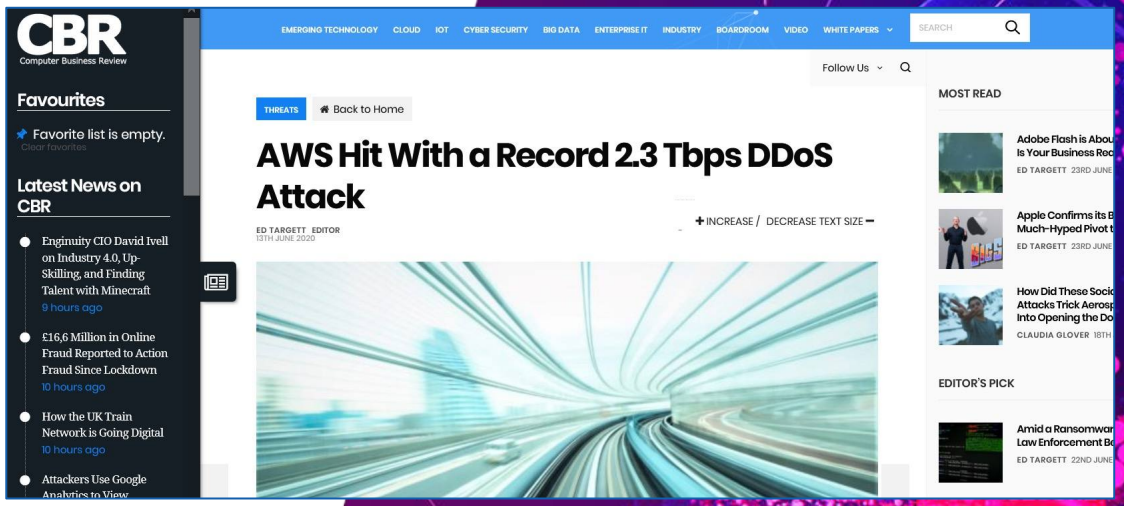
The Result? DDoS Attacks Are Larger Than Ever Before

New largest attack – AWS at 2.3 Tbps

- Feb 2020 – lasted 3 days
- Single vector used – CLDAP
- Reinforces the need for scalable and intelligent zero-trust approach

Amplification and reflection are the standard for the largest attacks

- The amplification factor of CLDAP, DNS and NTP makes them ideal weapons
- Even a small number of weapons can be massively exploited
- These attacks exploit the connectionless nature of UDP



DDoS Weapon	Number of Weapons	Weapons Frequency (in comparison to CLDAP)
Portmap	1,818,848	116x
SNMP	1,673,070	107x
SSDP	1,671,128	107x
DNS Resolvers	1,331,160	85x
TFTP	1,054,330	67x
CLDAP	15,651	-

https://www.a10networks.com/blog/aws-hit-by-largest-reported-ddos-attack-of-2-3-tbps/

VPGC
distinct.smart.innovative

DDoS Attacks Will Grow With 5G

5G introduces unprecedented and ubiquitous processing power, at scale

- Powerful IoT devices in large numbers will fuel devastating DDoS attacks

Mobile Broad Band (eMBB)

High-speed Internet

Fixed Wireless

Ultra Low Latency (URLLC)

Augmented Reality

Virtual Reality

Remote Surgeries

Connected Cars

Massive IoT (mMTC)

Smart Homes

Smart Cities

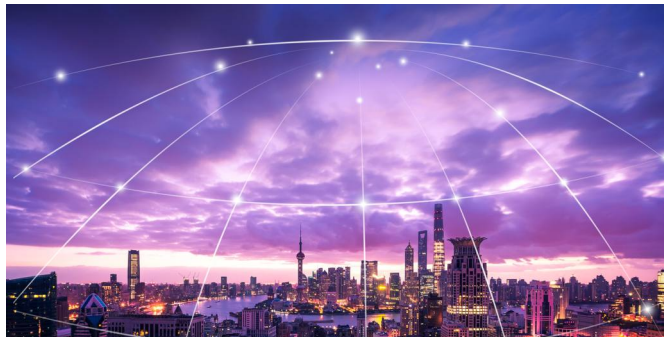


Photo Source: *MWC 2019 - GSMA*

VPGC
distinct.smart.innovative

https://www.cyber-rangers.com/
https://edutrainings.cz/cs/
https://www.cevroinstitut.cz/cs/clanek/bezpecnostni-studia/

https://www.linkedin.com/in/petrasevskij/