ISEN
ALL IS DIGITAL!

yncréa

An IoT Cybersecurity Primer

Emmanuel Druon

Disclaimer

- What you learn in cyber-classes, if badly used could alter, damage or even destroy live systems
- The tools must never be used on "real" systems without prior written and explicit authorization of the system owner and in some contexts of the ISP
- If you want to experiment, be sure to do so in a controlled Lab environment possibly not connected to the Internet
- Neither ISEN nor its staff could be held responsible for your actions

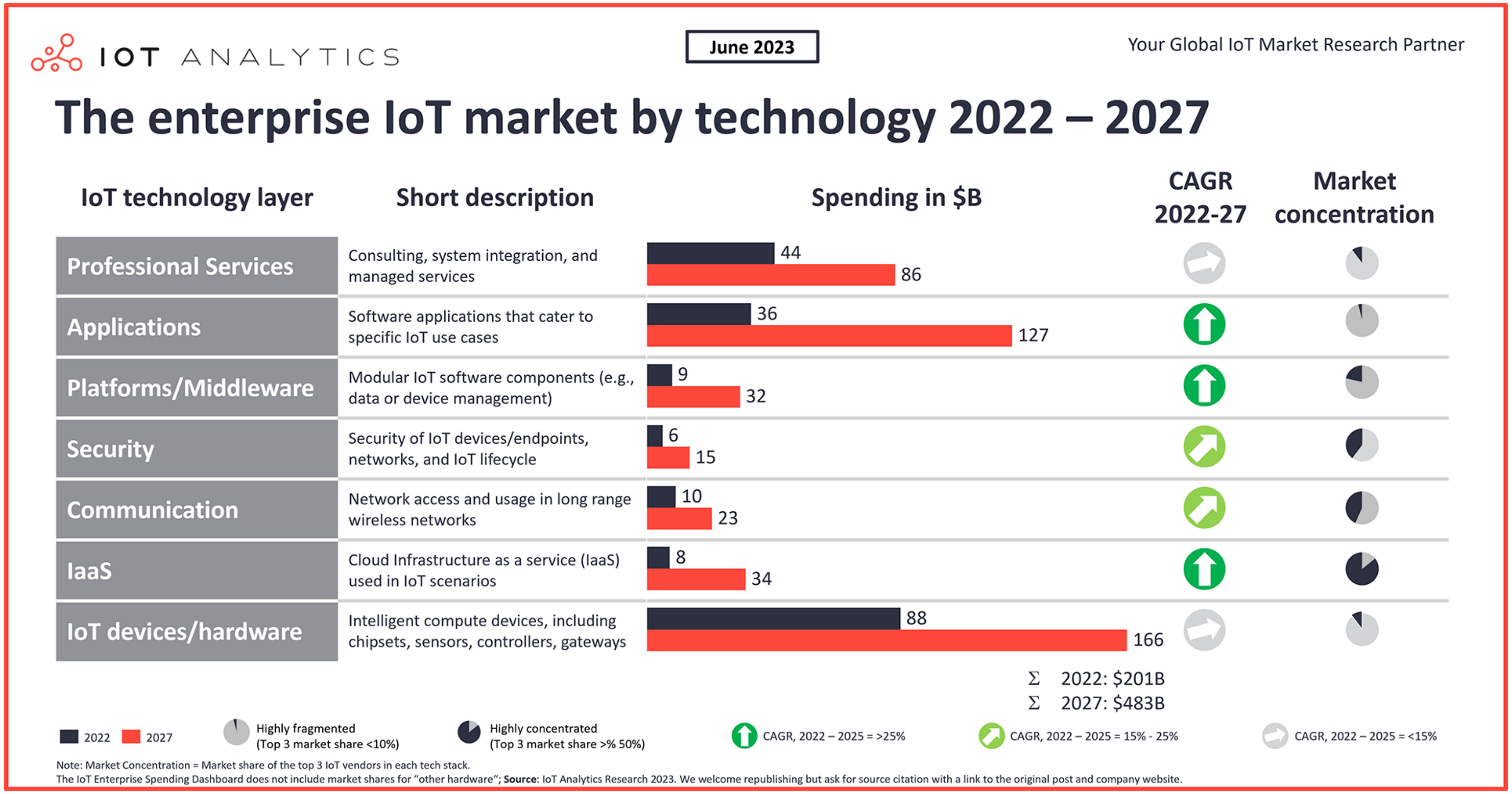
Agenda

- IoT & Cybersecurity
- IoT models:
    - The IoT reference model
    - The IoT security model
    - Security & IoT
- Attack surface analysis
    - The device layer
    - The communication layer
    - The application layer

Question:

What do you see as the main cyber risks related to connected devices?

IoT & Cybersecurity



IOT ANALYTICS

June 2023

Your Global IoT Market Research Partner

The enterprise IoT market by technology 2022 – 2027

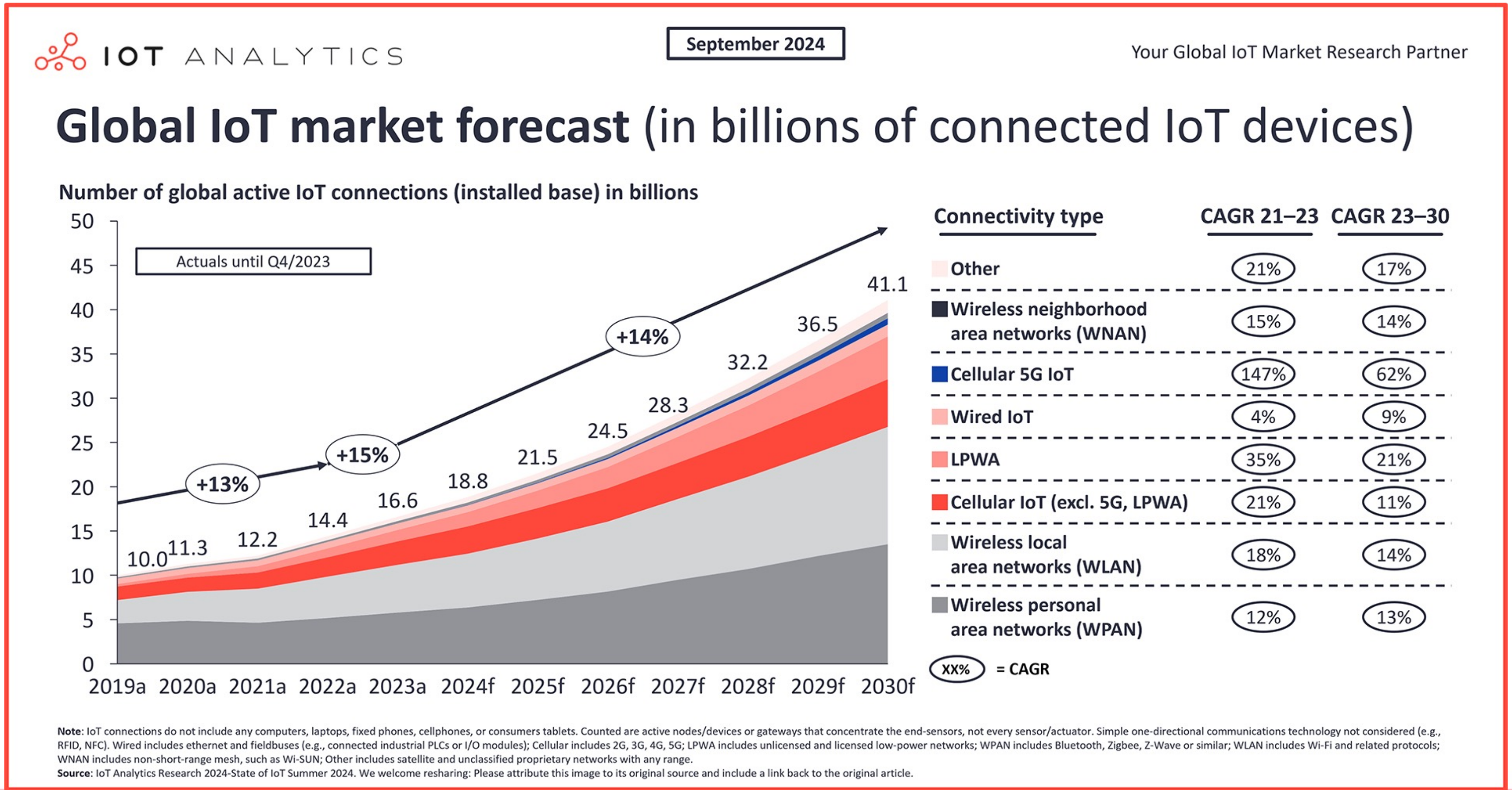
IoT technology layer	Short description	Spending in $B (2022)	Spending in $B (2027)	CAGR 2022-27	Market concentration
Professional Services	Consulting, system integration, and managed services	44	86	➡	◔
Applications	Software applications that cater to specific IoT use cases	36	127	⬆	◔
Platforms/Middleware	Modular IoT software components (e.g., data or device management)	9	32	⬆	◔
Security	Security of IoT devices/endpoints, networks, and IoT lifecycle	6	15	↗	◑
Communication	Network access and usage in long range wireless networks	10	23	↗	◑
IaaS	Cloud Infrastructure as a service (IaaS) used in IoT scenarios	8	34	⬆	◕
IoT devices/hardware	Intelligent compute devices, including chipsets, sensors, controllers, gateways	88	166	➡	◔

Σ 2022: $201B
Σ 2027: $483B

■ 2022 🟥 2027 ◔ Highly fragmented (Top 3 market share <10%) ◕ Highly concentrated (Top 3 market share >% 50%) ⬆ CAGR, 2022 – 2025 = >25% ↗ CAGR, 2022 – 2025 = 15% - 25% ➡ CAGR, 2022 – 2025 = <15%

Note: Market Concentration = Market share of the top 3 IoT vendors in each tech stack.
The IoT Enterprise Spending Dashboard does not include market shares for "other hardware"; **Source**: IoT Analytics Research 2023. We welcome republishing but ask for source citation with a link to the original post and company website.

IoT & Cybersecurity



IOT ANALYTICS

September 2024

Your Global IoT Market Research Partner

Global IoT market forecast (in billions of connected IoT devices)

Number of global active IoT connections (installed base) in billions

Connectivity type	CAGR 21–23	CAGR 23–30
Other	21%	17%
Wireless neighborhood area networks (WNAN)	15%	14%
Cellular 5G IoT	147%	62%
Wired IoT	4%	9%
LPWA	35%	21%
Cellular IoT (excl. 5G, LPWA)	21%	11%
Wireless local area networks (WLAN)	18%	14%
Wireless personal area networks (WPAN)	12%	13%

XX% = CAGR

Note: IoT connections do not include any computers, laptops, fixed phones, cellphones, or consumers tablets. Counted are active nodes/devices or gateways that concentrate the end-sensors, not every sensor/actuator. Simple one-directional communications technology not considered (e.g., RFID, NFC). Wired includes ethernet and fieldbuses (e.g., connected industrial PLCs or I/O modules); Cellular includes 2G, 3G, 4G, 5G; LPWA includes unlicensed and licensed low-power networks; WPAN includes Bluetooth, Zigbee, Z-Wave or similar; WLAN includes Wi-Fi and related protocols; WNAN includes non-short-range mesh, such as Wi-SUN; Other includes satellite and unclassified proprietary networks with any range.

Source: IoT Analytics Research 2024-State of IoT Summer 2024. We welcome resharing: Please attribute this image to its original source and include a link back to the original article.

IoT & Cybersecurity

- IoT is a growing market
- IoT is used in numerous environments:
  - Home and personal usage: wearables & smart homes
  - Professional usage: industry, transportation, healthcare

IoT & Cybersecurity

ISEN
ALL IS DIGITAL!

yncréa

- IoT is a growing source of:
  - Personal information
  - Sensitive information
  - Critical information
- IoT devices are:
  - Connected to networks
  - Connected to servers
  - Connected to Cloud resources

[Security Alert]

IoT & Cybersecurity

- Examples in different fields:
  - Cisco: **Anatomy of an IoT Attack**

    https://www.youtube.com/watch?v=7egBsN_4B2A
  - **Security in Med equipment**

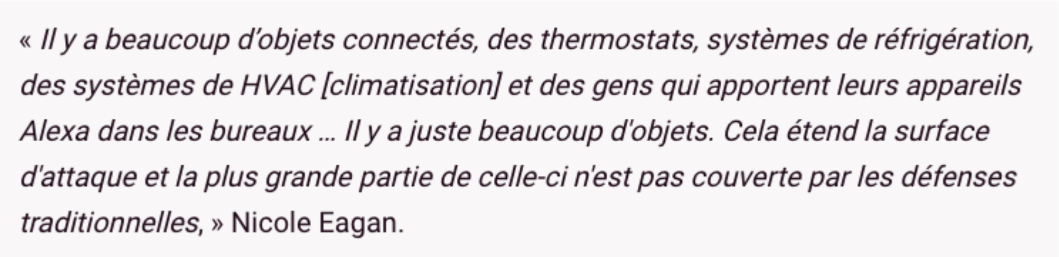
    https://www.youtube.com/watch?v=smhPhmNsvVc
  - **A Jeep hacked**

    https://www.youtube.com/watch?v=MK0SrxBC1xs

From fiction to reality…

- April 2018

Un casino piraté depuis le thermomètre connecté de son aquarium



« *Il y a beaucoup d'objets connectés, des thermostats, systèmes de réfrigération, des systèmes de HVAC [climatisation] et des gens qui apportent leurs appareils Alexa dans les bureaux … Il y a juste beaucoup d'objets. Cela étend la surface d'attaque et la plus grande partie de celle-ci n'est pas couverte par les défenses traditionnelles,* » Nicole Eagan.

Source: siecledigital.fr

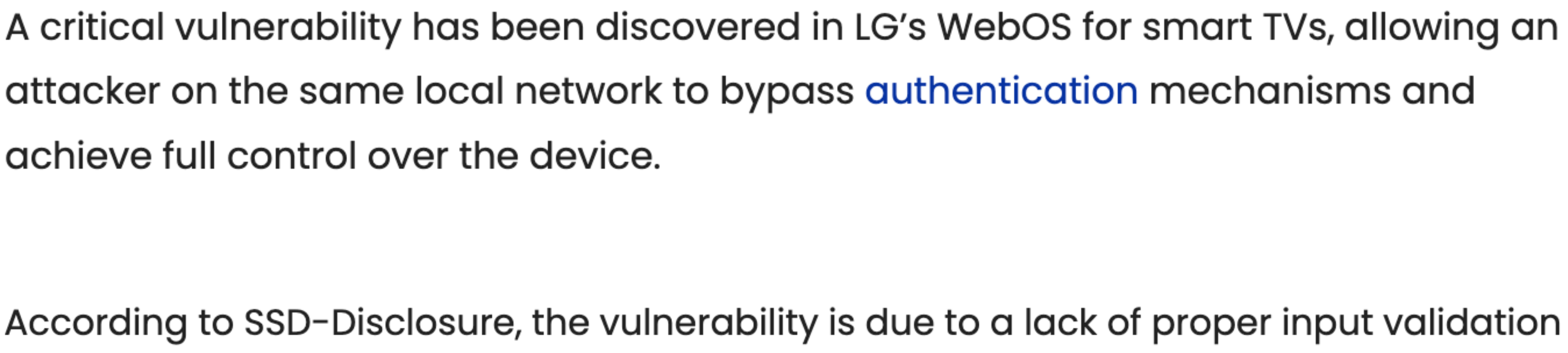
From fiction to reality…

Fiat lux et facta est

- Février 2020 :
  - Checkpoint reveals a vulnerability in the Philips Hue system that allows a hacker to take control of connected light bulbs…
  - … and escalate the attack to the level of the home computer network.
- August 2023:
  - A vulnerability in the authentication system of TP-Link Smart Bulbs allows an attacker to retrieve Wi-Fi credentials.

From fiction to reality…

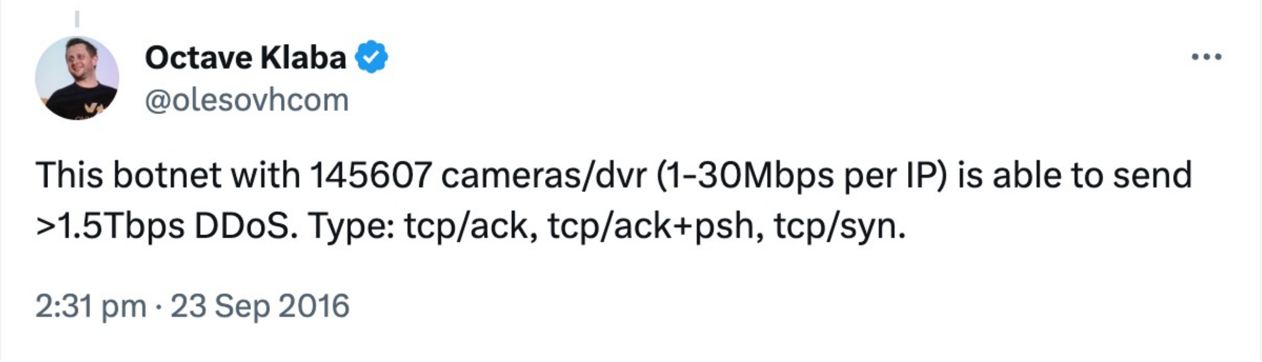
- September 2025 : **LG WebOS TV Vulnerability Let Attackers Bypass Authentication and Enable Full Device Takeover**



A critical vulnerability has been discovered in LG's WebOS for smart TVs, allowing an attacker on the same local network to bypass authentication mechanisms and achieve full control over the device.

According to SSD-Disclosure, the vulnerability is due to a lack of proper input validation

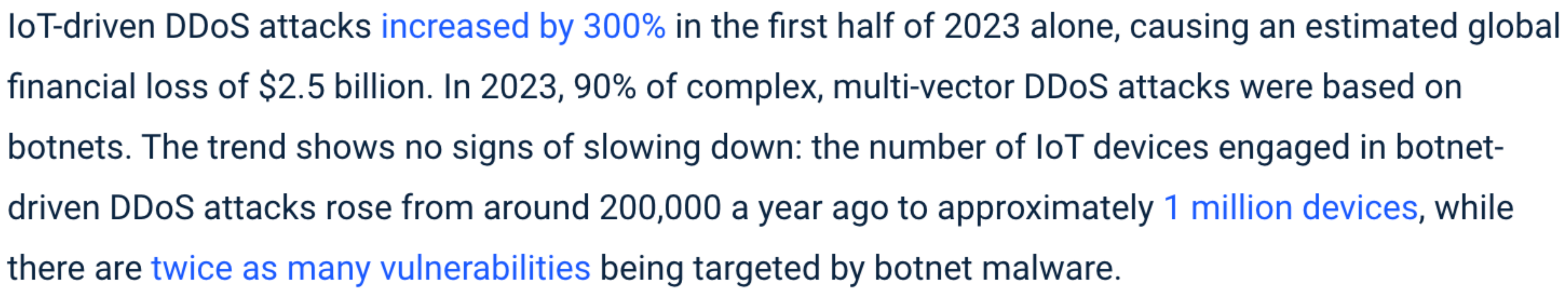
IoT : a danger for the others



Octave Klaba @olesovhcom

This botnet with 145607 cameras/dvr (1-30Mbps per IP) is able to send >1.5Tbps DDoS. Type: tcp/ack, tcp/ack+psh, tcp/syn.

2:31 pm · 23 Sep 2016



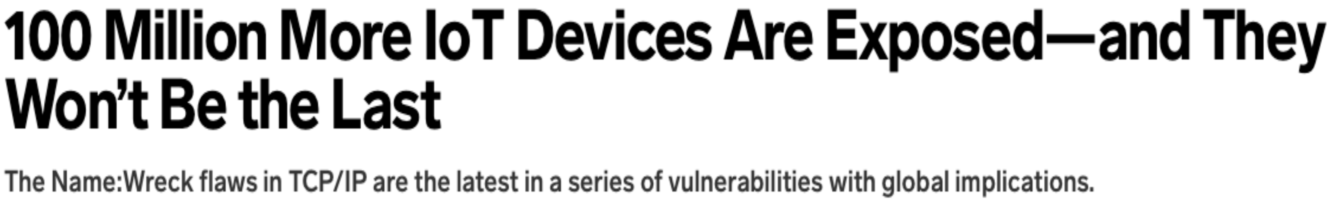
IoT-driven DDoS attacks increased by 300% in the first half of 2023 alone, causing an estimated global financial loss of $2.5 billion. In 2023, 90% of complex, multi-vector DDoS attacks were based on botnets. The trend shows no signs of slowing down: the number of IoT devices engaged in botnet-driven DDoS attacks rose from around 200,000 a year ago to approximately 1 million devices, while there are twice as many vulnerabilities being targeted by botnet malware.

Source: https://thehackernews.com/2023/09/ddos-20-iot-sparks-new-ddos-alert.html

Oups…

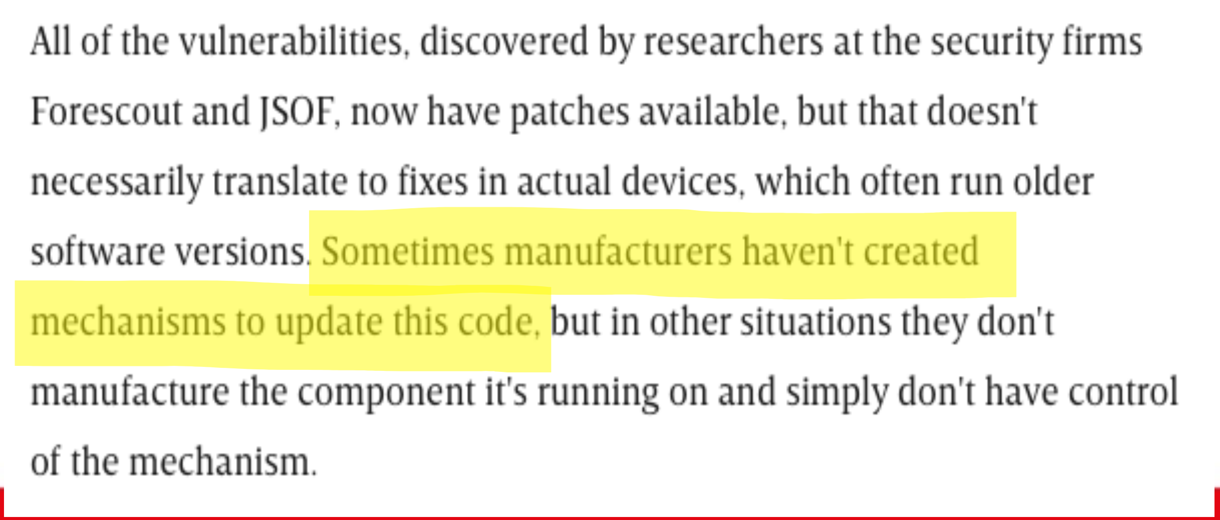
Avril 2021 :

(Source : wired.com)



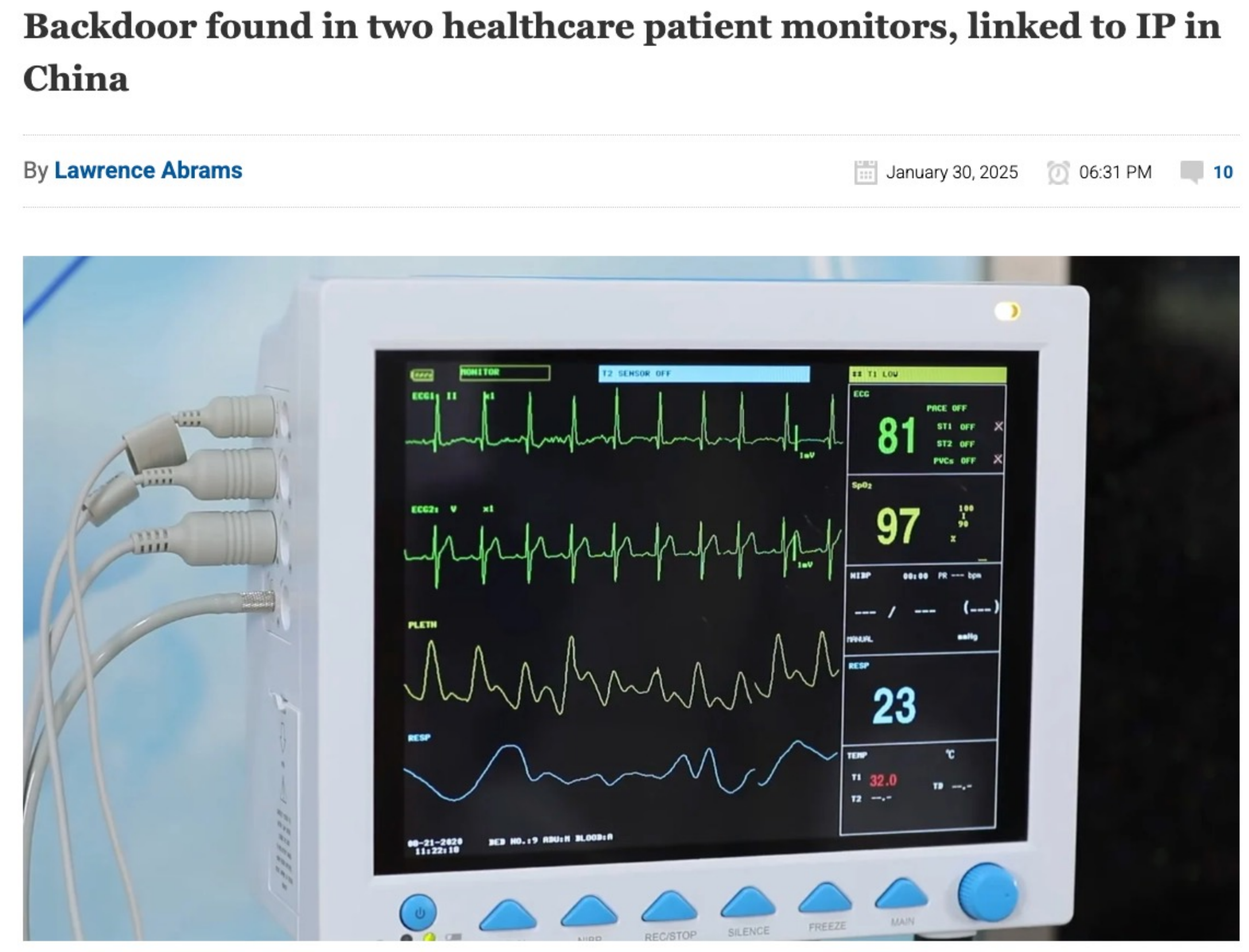
100 Million More IoT Devices Are Exposed—and They Won't Be the Last

The Name:Wreck flaws in TCP/IP are the latest in a series of vulnerabilities with global implications.



All of the vulnerabilities, discovered by researchers at the security firms Forescout and JSOF, now have patches available, but that doesn't necessarily translate to fixes in actual devices, which often run older software versions. Sometimes manufacturers haven't created mechanisms to update this code, but in other situations they don't manufacture the component it's running on and simply don't have control of the mechanism.

Backdoors ?!?



Backdoor found in two healthcare patient monitors, linked to IP in China

By **Lawrence Abrams** January 30, 2025 06:31 PM 10

Et dans la santé…

November 2022: Hospitals under hacker threat

(source France Info)

All hospital rooms contain a monitoring device connected to another in the nurses' station. This indispensable device allows caregivers to see at a glance vital signs such as heart rate. Using two of these monitors, Charles Blanc Rolin (a cybersecurity researcher) demonstrates how easy it is to "make the doctor think the patient is fine when they are not, or vice versa."

After disabling the first monitor, he simply sends the second one… false values (for example, a heart rate of 160 beats per minute instead of 50).

Are you using the proper software?

November 2022: Microsoft alert: this forgotten open-source web server could allow hackers to access your system "silently."

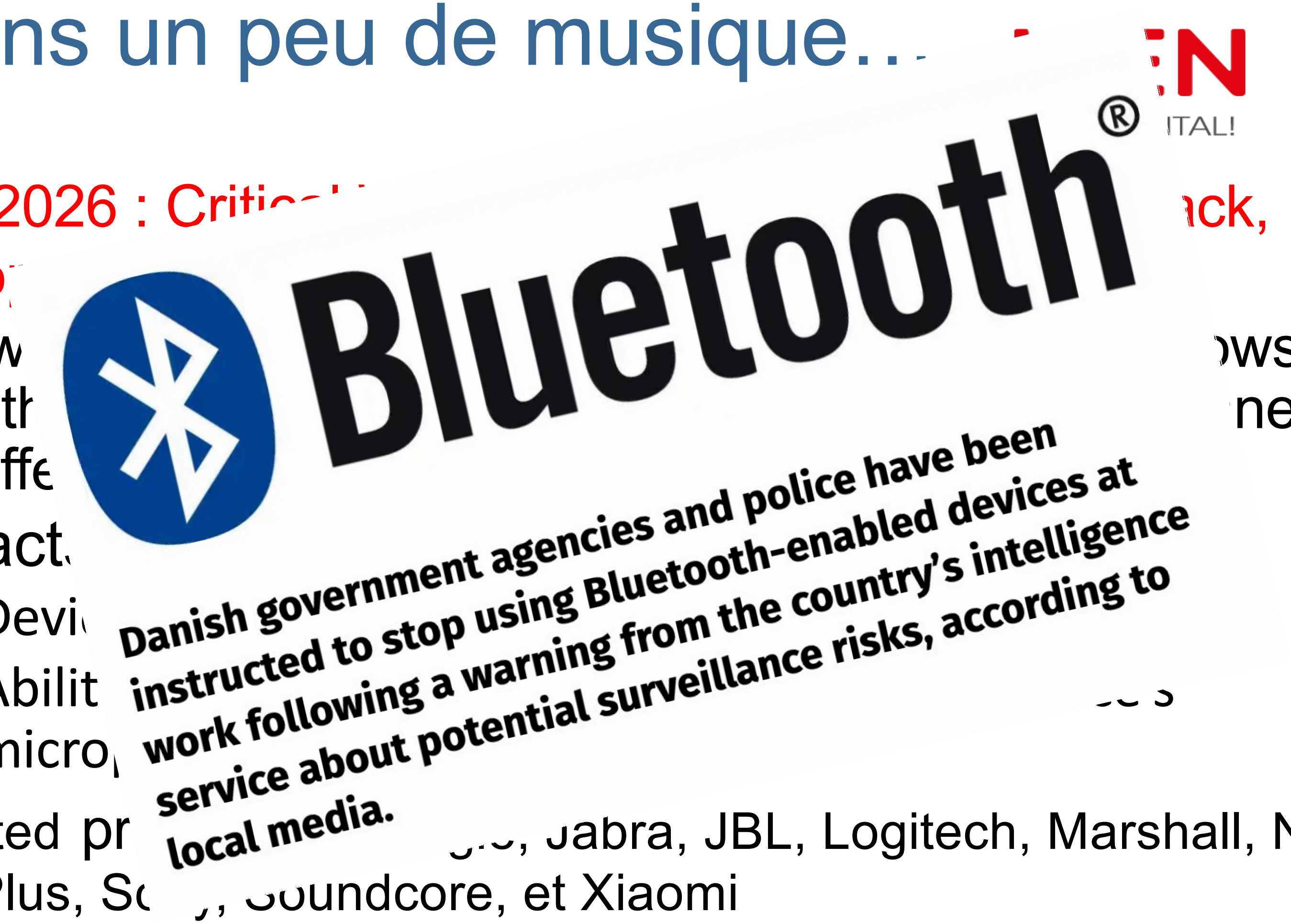
(source ZDNet)

The Boa web server, which is often used to access the settings, management consoles, and login screens of many IoT devices, contains numerous security vulnerabilities.

Abandoned in 2005, the Boa web server continues to be implemented by various vendors across a wide range of IoT (Internet of Things) devices and popular software development kits (SDKs)…

Écoutons un peu de musique…

- January 2026 : Critic… …ack, eavesdrop…
  - A flaw … …ows unauth… …nect to the affe…
  - Impact…
    - Devi…
    - Abilit… …es micro…
  - Affected pr… …Jabra, JBL, Logitech, Marshall, Nothing, OnePlus, So… Soundcore, et Xiaomi



Bluetooth®

Danish government agencies and police have been instructed to stop using Bluetooth-enabled devices at work following a warning from the country's intelligence service about potential surveillance risks, according to local media.

I'll be back…

December 2025 : A single word is enough for hackers to take control of a group of robots.

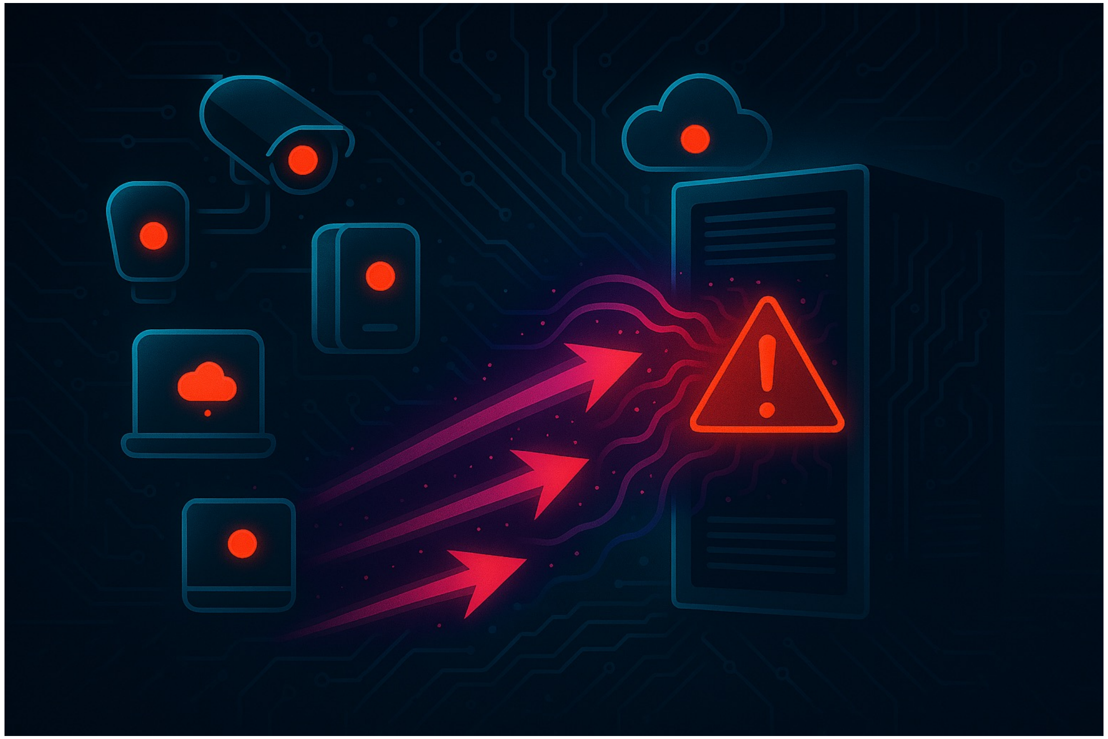
"A humanoid robot approaches a mannequin at the center of the stage. Its mechanical arm knocks it to the ground with a punch."

- At Shanghai's GeekCon, researchers demonstrate how, using a single word, they can take control of a robot by exploiting its built-in AI agent.
- Once hacked, the compromised robot spreads the infection to another robot not connected to the network via its short-range wireless communication.

Source: https://www.lesnumeriques.com/intelligence-artificielle/un-seul-mot-suffit-aux-pirates-pour-prendre-le-controle-d-une-armee-de-robots-n248582.html

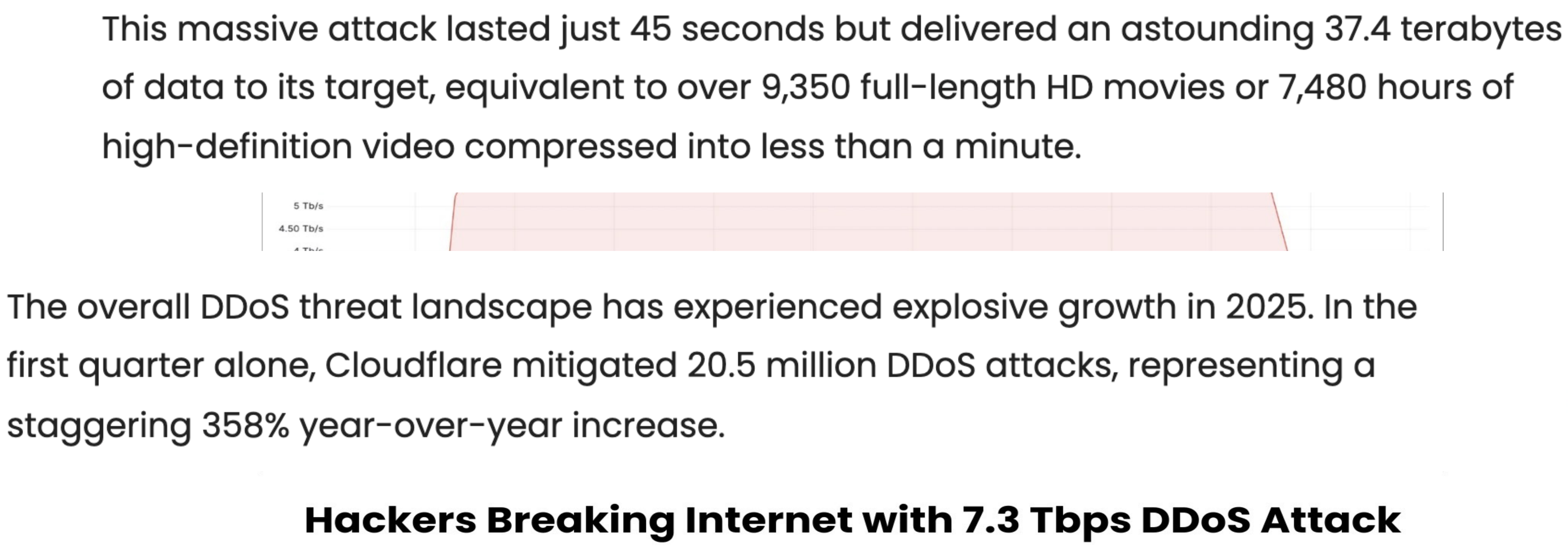
Modern DDOS

When the sheer volume is dizzying…



7.3 Tbps and 4.8 Billion Packets Per Second DDoS Attack

- July 2025:



This massive attack lasted just 45 seconds but delivered an astounding 37.4 terabytes of data to its target, equivalent to over 9,350 full-length HD movies or 7,480 hours of high-definition video compressed into less than a minute.

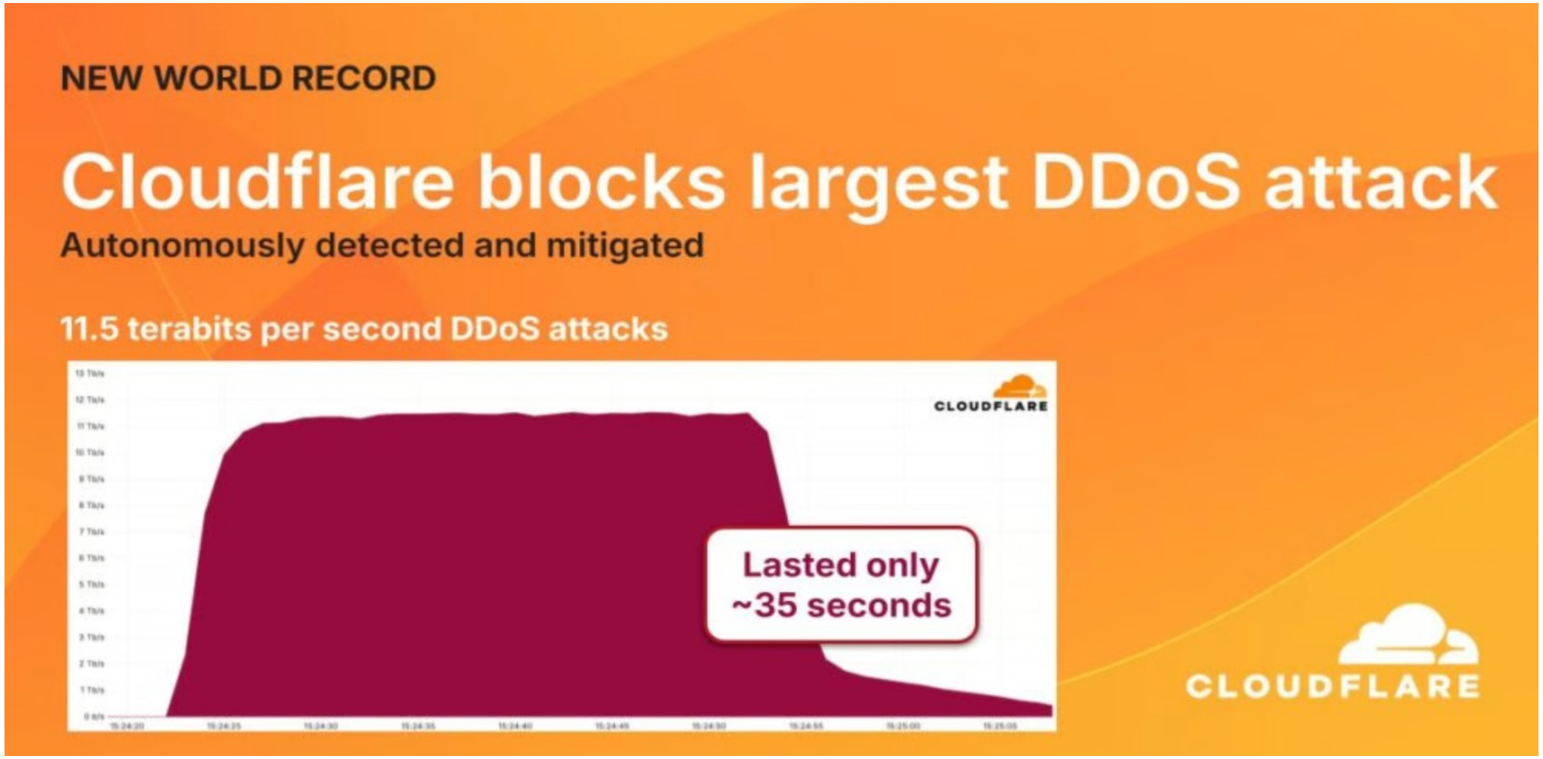
The overall DDoS threat landscape has experienced explosive growth in 2025. In the first quarter alone, Cloudflare mitigated 20.5 million DDoS attacks, representing a staggering 358% year-over-year increase.

Hackers Breaking Internet with 7.3 Tbps DDoS Attack

Source: https://cybersecuritynews.com/record-breaking-ddos-attack-7-3-tbps

7.3 Tbps…

- September 2025



NEW WORLD RECORD

Cloudflare blocks largest DDoS attack

Autonomously detected and mitigated

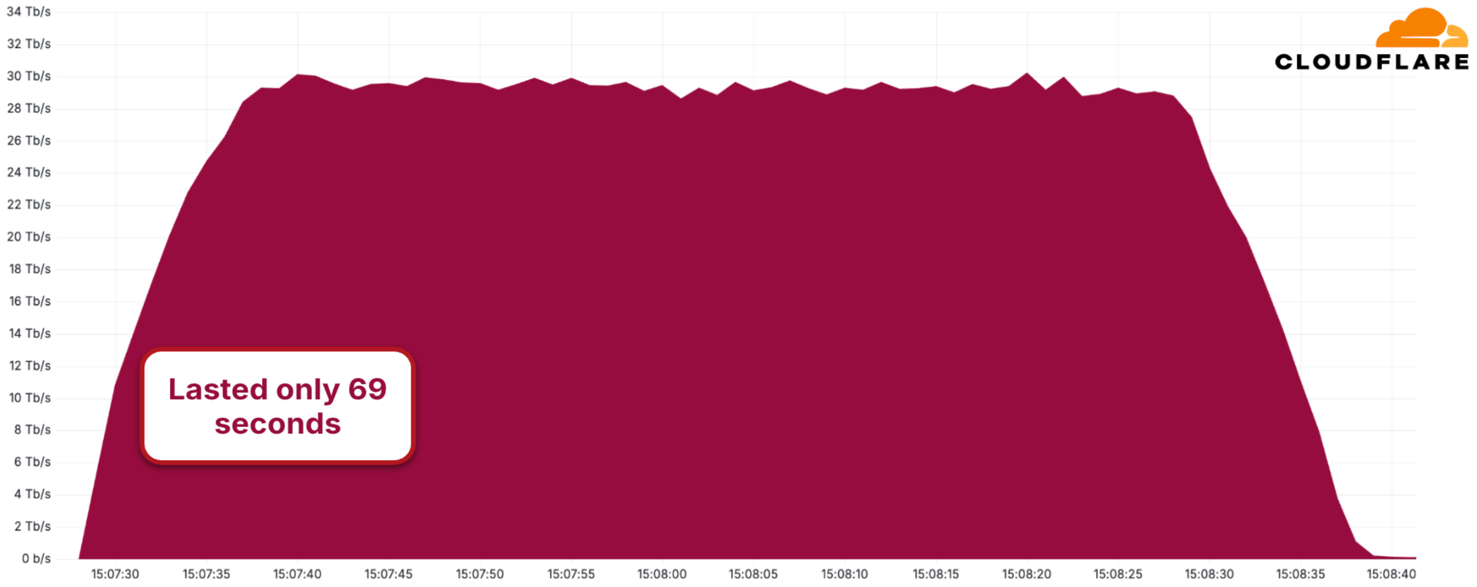
11.5 terabits per second DDoS attacks

Source: https://korben.info/cloudflare-ddos-11-5-tbps.html

CLOUDFLARE MITIGATES RECORD 29.7 TBPS DDOS ATTACK BY THE AISURU BOTNET

- December 2025

New world record: 29.7 Tbps
autonomously mitigated by Cloudflare



Lasted only 69 seconds

Source: https://securityaffairs.com/185299/security/cloudflare-mitigates-record-29-7-tbps-ddos-attack-by-the-aisuru-botnet.html