DDoS attacks

be prepared for Survival

Author: Uncle Nai

Version: 1.1

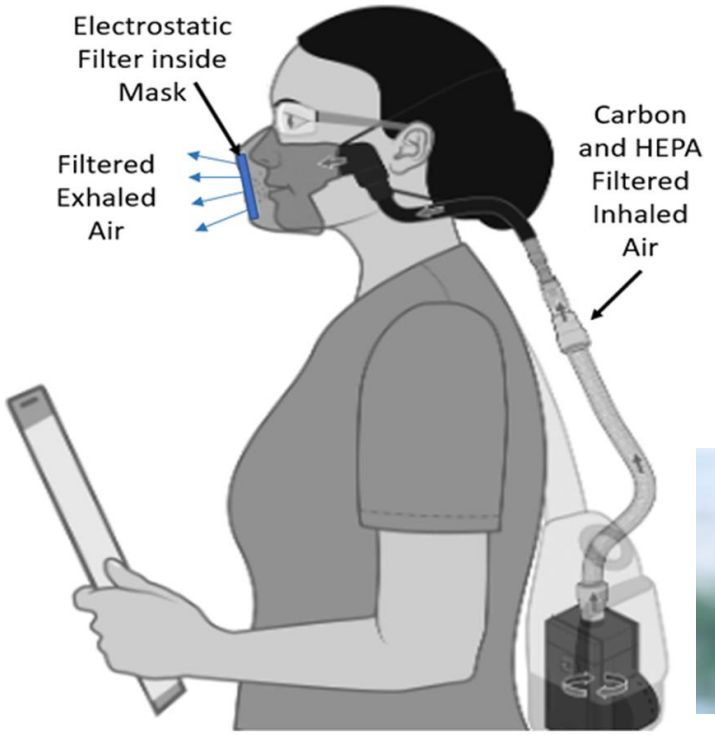
Last Update: October 22, 2025

MYANMAR NETWORK OPERATORS GROUP

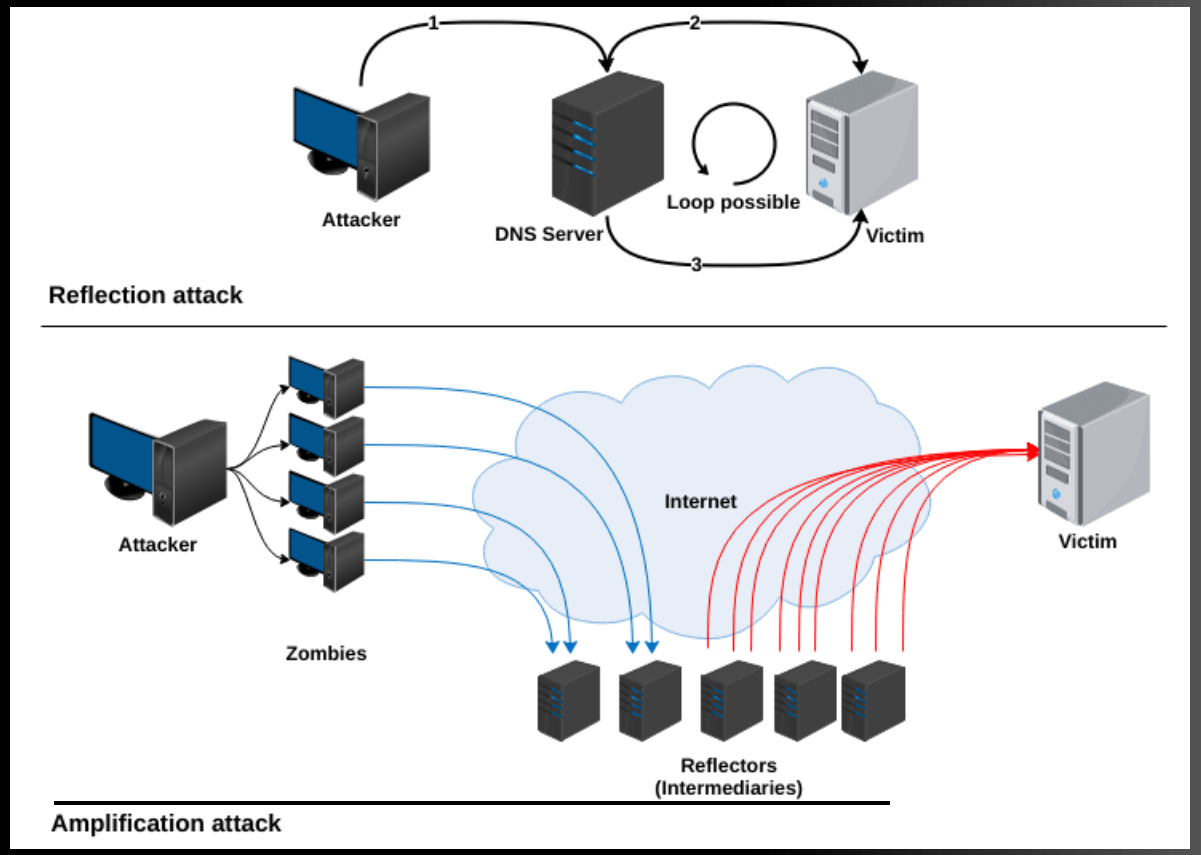
Feel free to send feedback and your valuable comments to event@mm-ix.net

Real world DoS examples only in Myanmar version(s) 2005-2010 ; 2015+ ...

Asian Squat Toilet



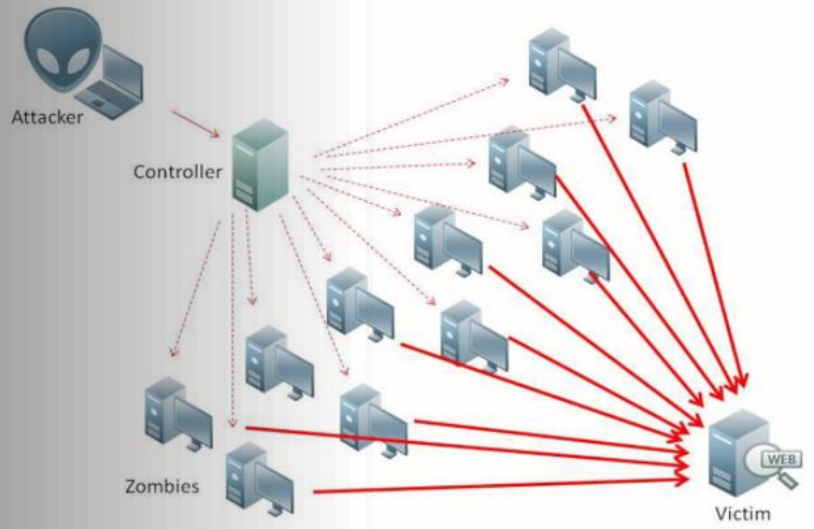
DoS and DDoS Threats



What? WHY? How?
History

Options to defend

- What is it?
- WHY ? (motives !!) .. $%^%^ @#$, etc. …
- HOW ??
- Historical DDoS events (2001 to 2025)
  in Myanmar & all over the world
  [firewall or anti-DDoS solutions will work ??]
- How is it handled, mitigated in best practices !!
  /unplug, power off, save electricity?/
- How is it healed and dealt with global community
  support ??? / team C- - - - /



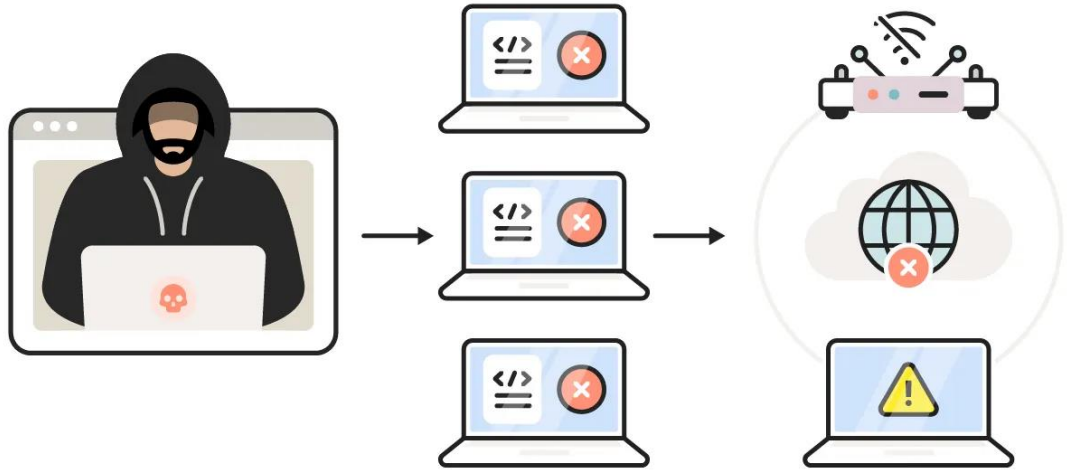
wlP1p1s0 / hourly

hour	rx	tx	total	avg. rate
2025-10-17				
20:00	30.39 MiB	27.74 MiB	58.13 MiB	135.45 kbit/s
21:00	32.36 MiB	26.95 MiB	59.31 MiB	138.20 kbit/s
22:00	30.20 MiB	26.89 MiB	57.10 MiB	133.04 kbit/s
23:00	27.11 MiB	24.81 MiB	51.92 MiB	120.98 kbit/s
2025-10-19				
15:00	4.11 MiB	3.70 MiB	7.81 MiB	18.20 kbit/s
16:00	28.21 MiB	25.23 MiB	53.44 MiB	124.53 kbit/s
17:00	47.62 MiB	25.93 MiB	73.55 MiB	171.38 kbit/s
18:00	73.41 MiB	104.43 MiB	177.84 MiB	414.39 kbit/s
19:00	33.07 MiB	28.75 MiB	61.82 MiB	144.05 kbit/s
20:00	34.03 MiB	34.50 MiB	68.53 MiB	159.69 kbit/s
21:00	28.77 MiB	32.41 MiB	61.18 MiB	142.55 kbit/s
22:00	27.88 MiB	32.61 MiB	60.49 MiB	140.95 kbit/s
23:00	26.34 MiB	33.99 MiB	60.32 MiB	140.56 kbit/s
2025-10-20				
00:00	23.16 MiB	26.40 MiB	49.56 MiB	115.48 kbit/s
01:00	462.11 MiB	46.08 MiB	508.19 MiB	1.18 Mbit/s
02:00	13.38 GiB	621.06 MiB	13.99 GiB	33.38 Mbit/s
03:00	6.39 GiB	337.05 MiB	6.72 GiB	16.03 Mbit/s
04:00	22.49 MiB	23.27 MiB	45.75 MiB	106.62 kbit/s
05:00	22.21 MiB	23.35 MiB	45.55 MiB	106.15 kbit/s
06:00	22.35 MiB	22.93 MiB	45.28 MiB	105.51 kbit/s
07:00	37.12 MiB	24.06 MiB	61.18 MiB	142.56 kbit/s
08:00	32.82 MiB	24.15 MiB	56.96 MiB	132.73 kbit/s
09:00	38.37 MiB	25.62 MiB	63.98 MiB	149.09 kbit/s
10:00	21.69 MiB	19.81 MiB	41.51 MiB	128.96 kbit/s

day	rx	tx	total	avg. rate
2025-10-09	377.78 MiB	190.94 MiB	568.73 MiB	55.22 kbit
2025-10-10	989.89 MiB	425.18 MiB	1.38 GiB	137.39 kbit
2025-10-11	776.47 MiB	430.67 MiB	1.18 GiB	117.20 kbit
2025-10-12	702.16 MiB	388.67 MiB	1.07 GiB	105.91 kbit
2025-10-13	524.47 MiB	751.27 MiB	1.25 GiB	123.86 kbit
2025-10-14	123.47 MiB	373.68 MiB	497.15 MiB	48.27 kbit
2025-10-15	6.80 GiB	656.29 MiB	7.44 GiB	739.71 kbit
2025-10-16	786.14 MiB	773.40 MiB	1.52 GiB	151.42 kbit
2025-10-17	895.48 MiB	625.26 MiB	1.49 GiB	147.65 kbit
2025-10-19	303.43 MiB	321.55 MiB	624.98 MiB	60.68 kbit
2025-10-20	20.47 GiB	1.20 GiB	21.67 GiB	4.40 Mbit
estimated	41.82 GiB	2.44 GiB	44.26 GiB	

DDoS Attacks Explained

DDoS attacks occur when a hacker uses a zombie network to flood a website/server with traffic or requests until it crashes.



Attacker

A hacker infects devices to make botnets, forming a **zombie network**.

Zombie Network

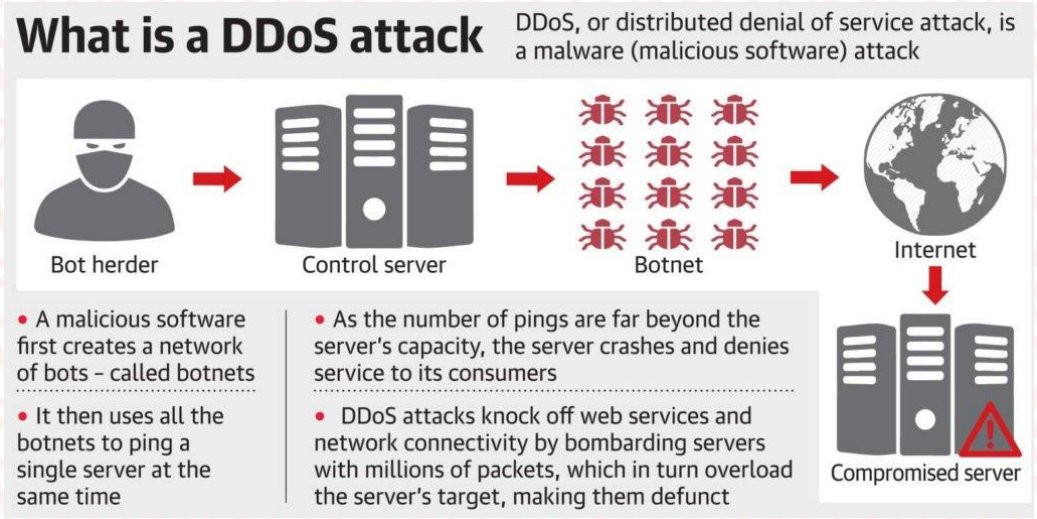
The zombie network **floods a targeted website or server** with traffic.

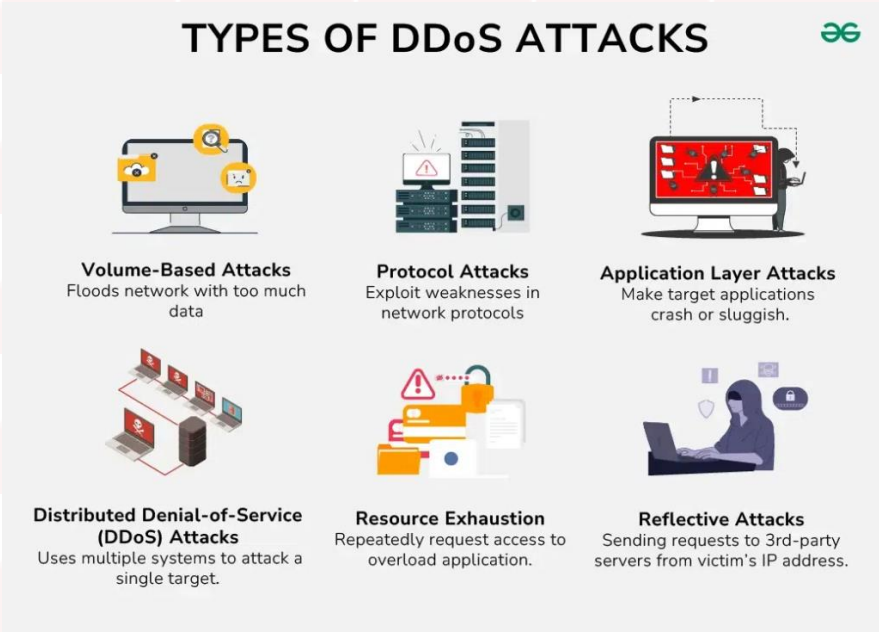
Targeted Website/Server

The targeted **website or server crashes**, disconnecting from the internet.

plz refer to AI/GPTs & GOOGLE for more, please.

- DDoS Evolution Timeline (2001–2025)
- Attack Motivations (crimeware, hacktivism,
- geopolitics, extortion, gaming, AI abuse, …)
- DDoS Economics: booter-as-a-service & darknet markets
- Attack Statistics 2024–2025 (Tbps peaks, top vectors, regional trends)
- Case Study: Real 2025 multi-vector attack on a global backbone
- Defense frameworks & coordination (NOC–SOC)
- Operational metrics, KPIs, and future outlook

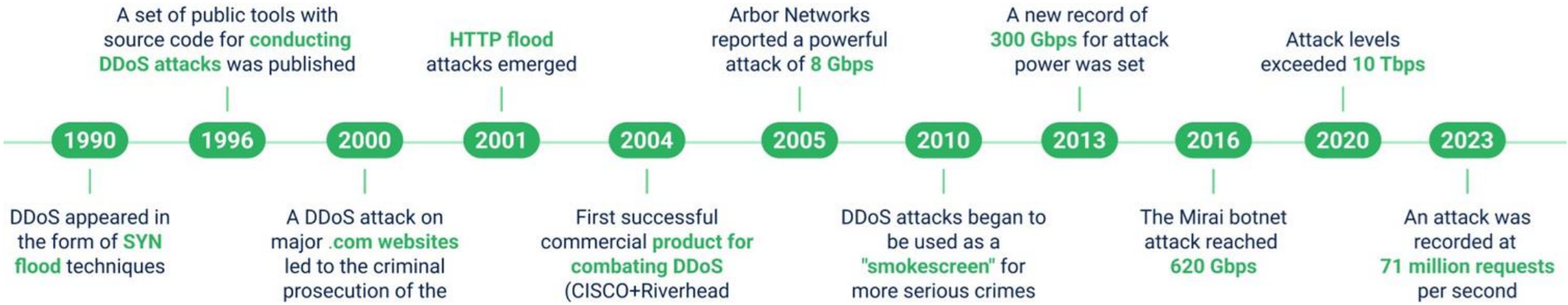




Denial of Service (**DoS**)

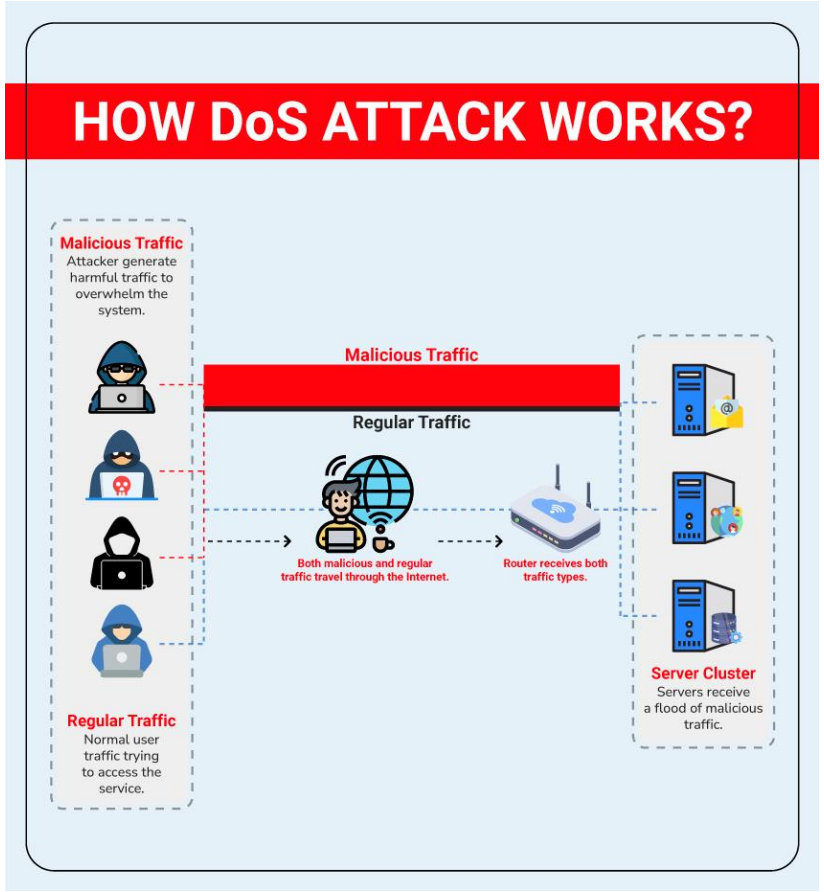
➔ 1974: The first Denial of Service (DoS) attack
- executed by a 13-year-old, David Dennis, just crashed 31 computer terminals on the University of Illinois's PLATO system.

➔ 1996: The first known large-scale **Distributed** Denial of Service (**DDoS**)
- internet service provider Panix ISP was overwhelmed by a SYN flood attack, taking several days to recover.



Threats and Protections

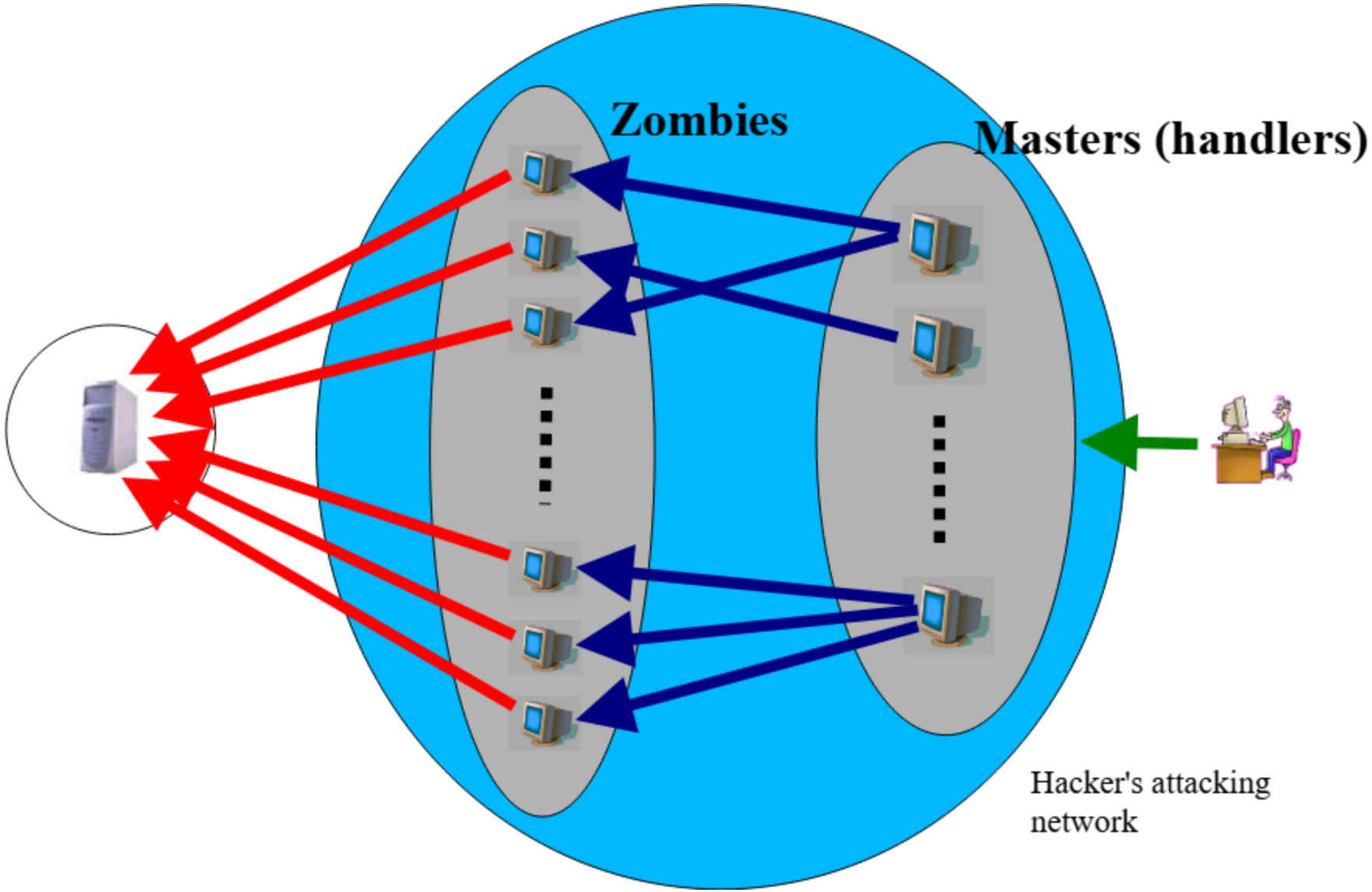
- DDoS definition and its attacking architectures
- DDoS classification
- Defense mechanism classification
- Reactive VS. Proactive
- Classification by defending front-line
- SOS – a case study



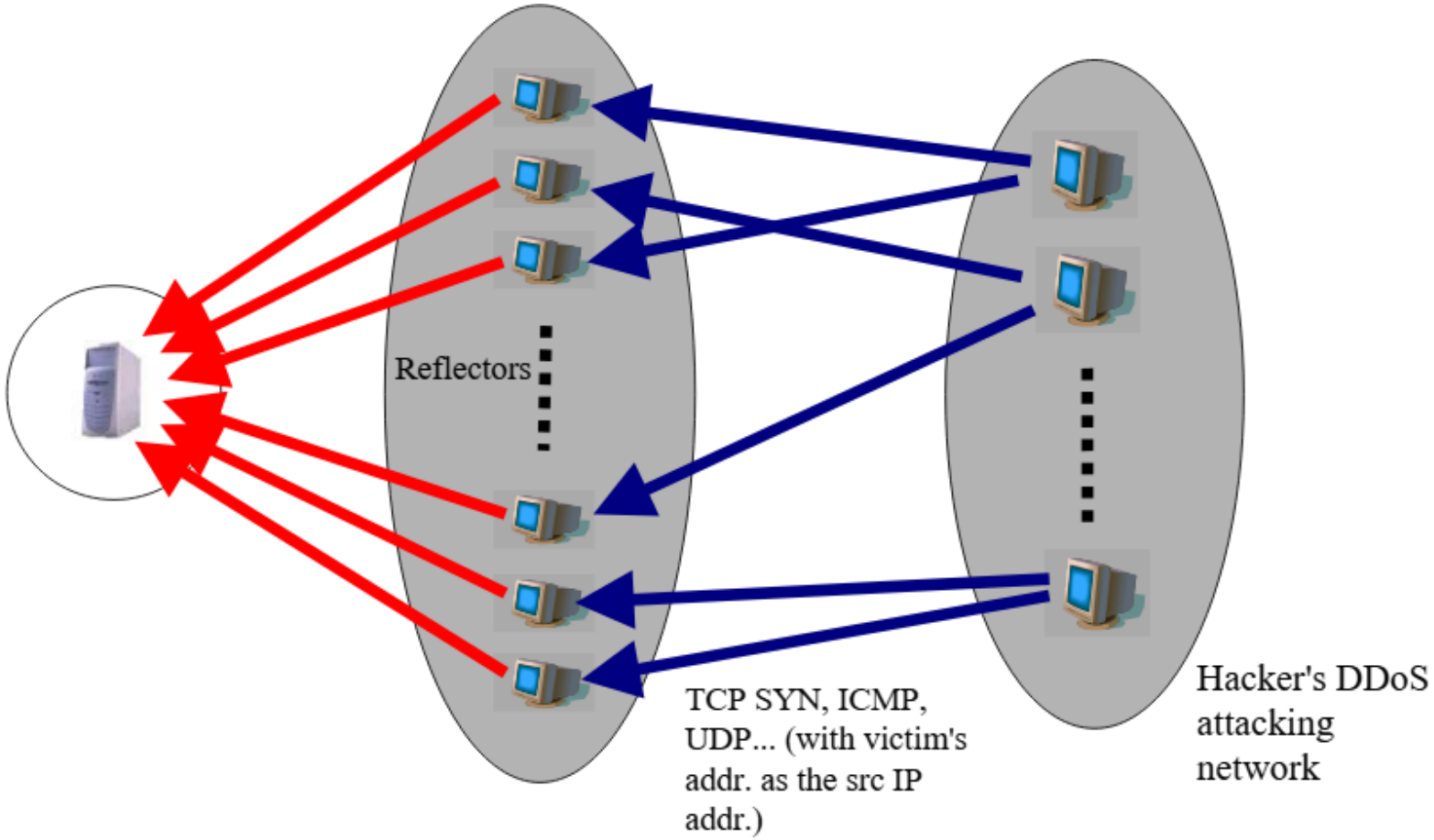
DDoS ; What is it?

- No definite ready-to-go definition available yet for attackers PoV !!
- Characteristics
  - Multiple attackers vs. single victim / org
  - to cause denial of service to legitimate us
- Two major attacking architecture
  - Direct attack
  - Reflector attack

Attacking Architecture - Direct Attack



Attacking Architecture – Reflector Attack



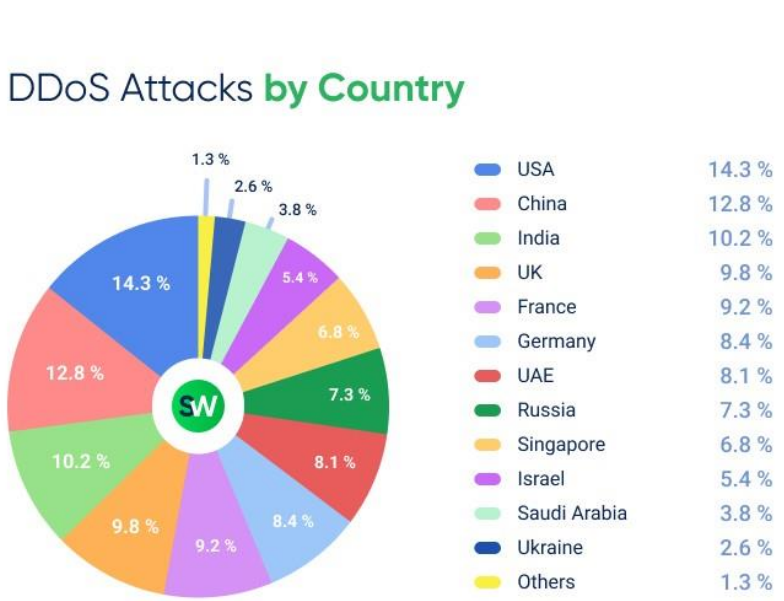
Reflector Attack

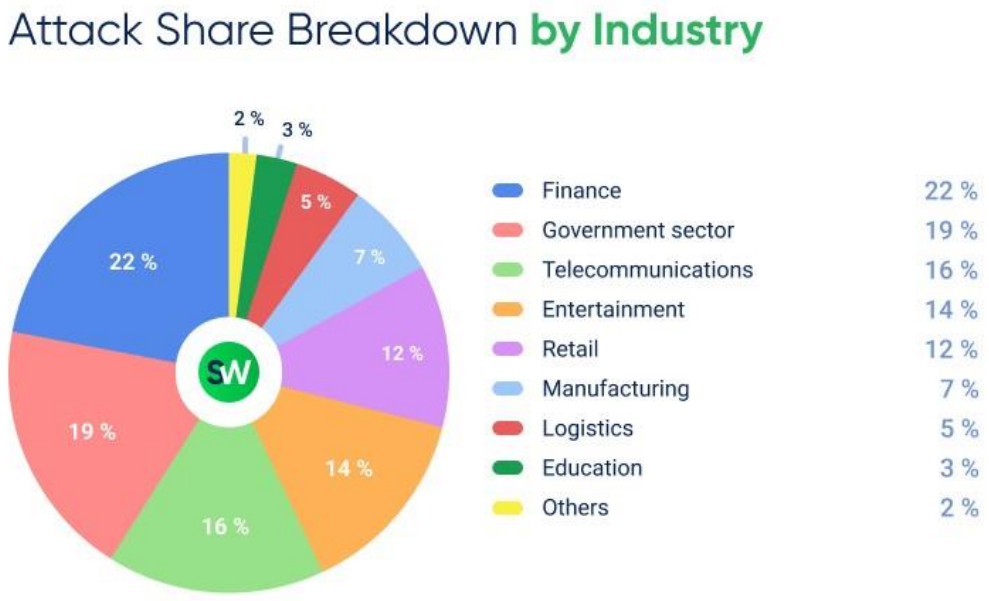
DDoS Evolution Timeline (2001–2025)

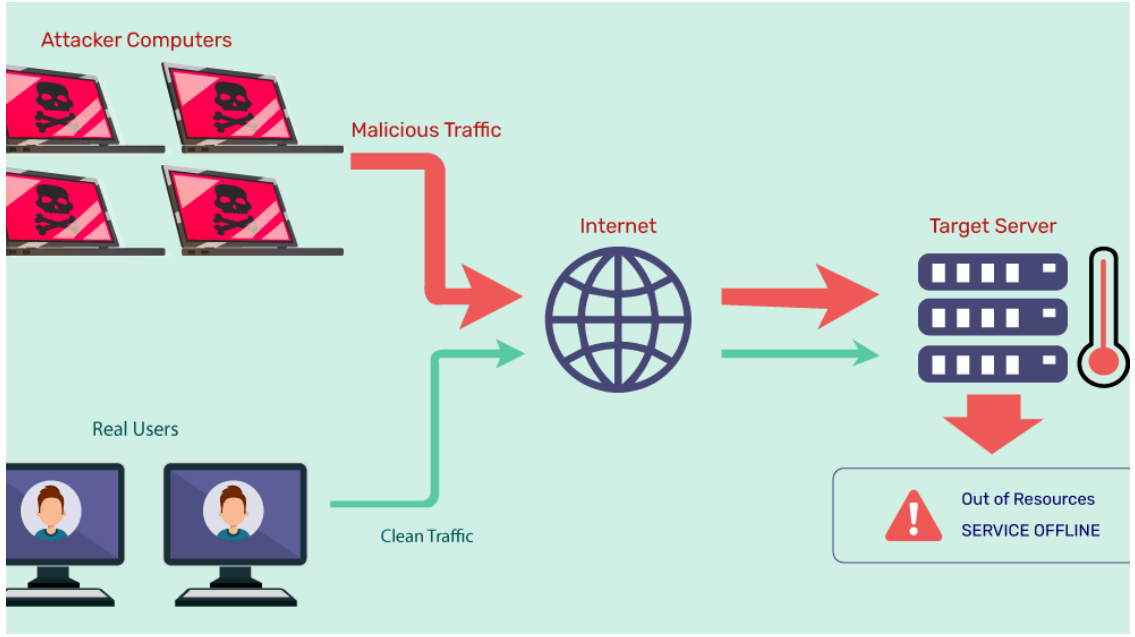
- ➔ 2001–2010: Simple **SYN/UDP floods**, early IRC botnets
- ➔ 2010–2016: Mirai **IoT** exploitation, booter markets rise
- ➔ 2017–2020: Multi-vector amplification attacks
- ➔ 2021–2025: AI-assisted, short high-Tbps bursts, 5G networks/high speed advantages

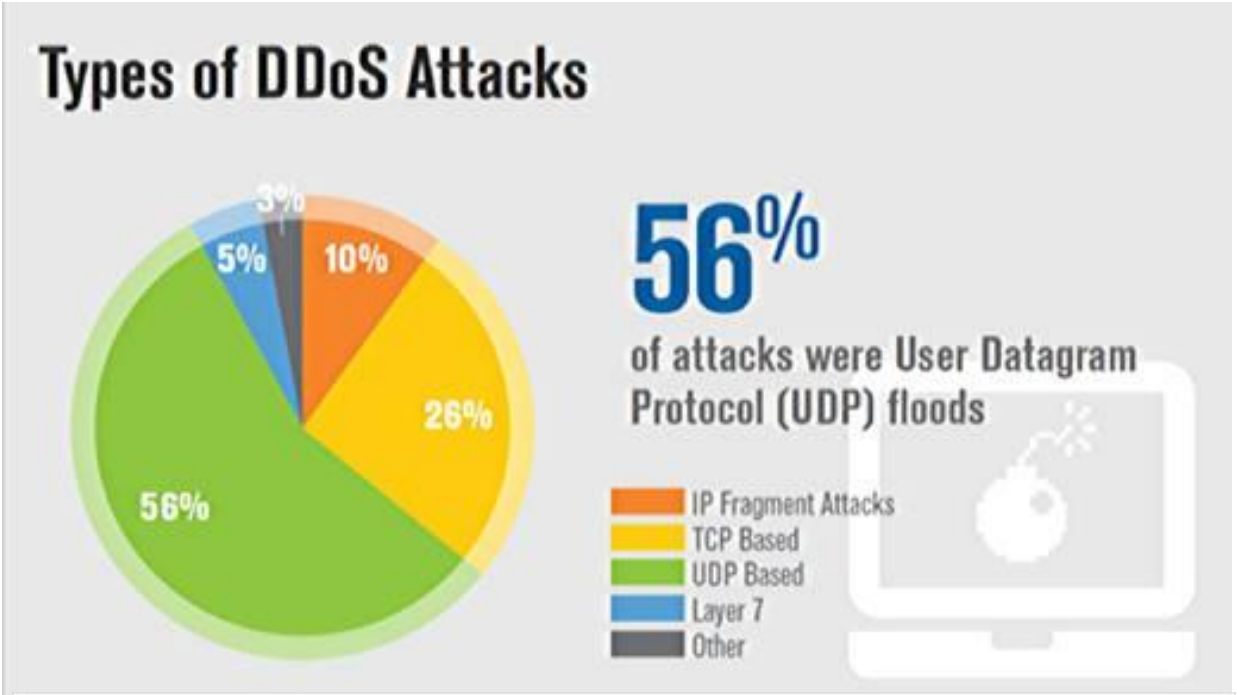
DDoS in 2024: Detailed Statistics | StormWall

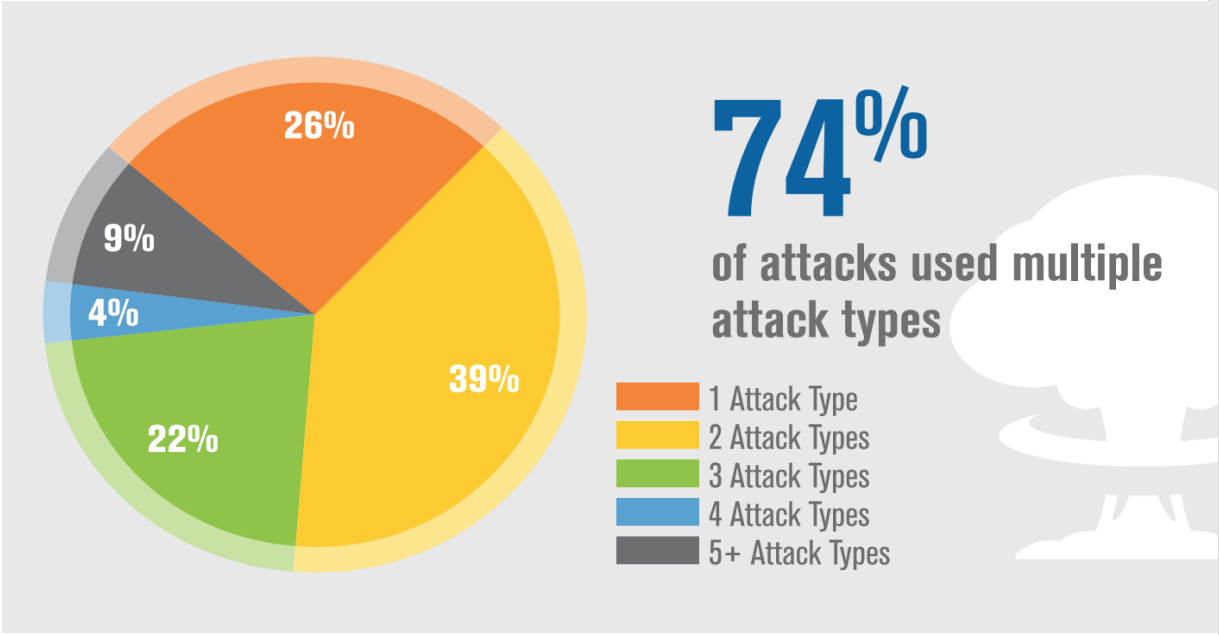
https://stormwall.network/resources/blog/ddos-attack-statistics-2024

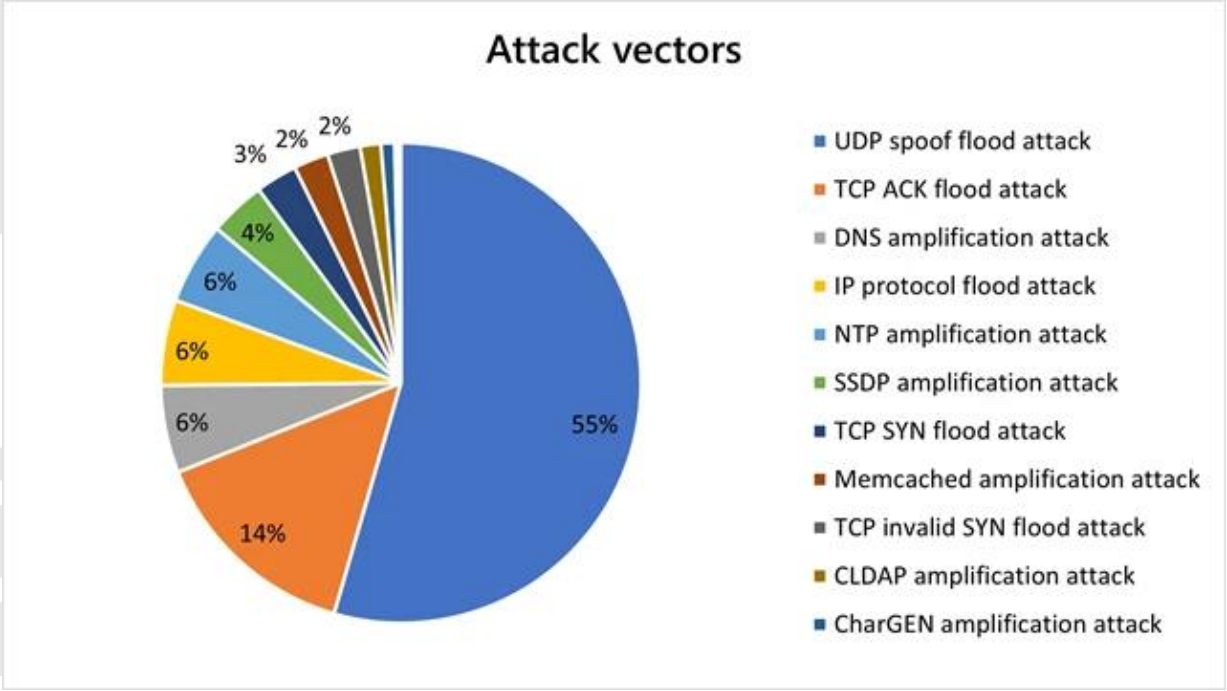


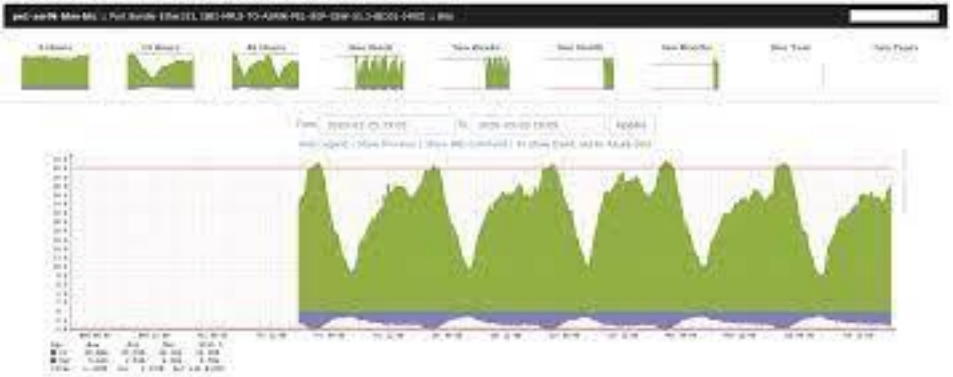


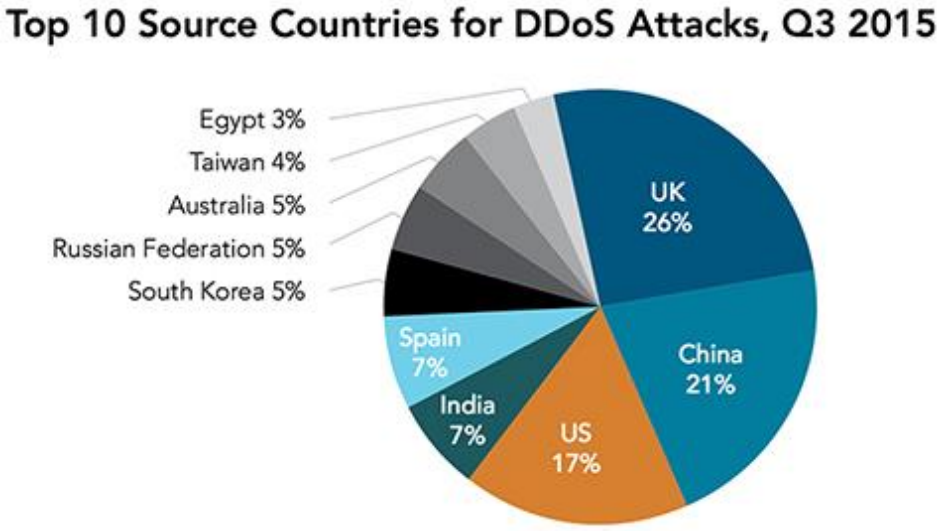

Attacker Computers
Malicious Traffic
Internet
Target Server
Real Users
Clean Traffic
Out of Resources
SERVICE OFFLINE


Types of DDoS Attacks
3%
5%
10%
26%
56%
56%
of attacks were User Datagram Protocol (UDP) floods
IP Fragment Attacks
TCP Based
UDP Based
Layer 7
Other


26%
9%
4%
39%
22%
74%
of attacks used multiple attack types
1 Attack Type
2 Attack Types
3 Attack Types
4 Attack Types
5+ Attack Types


Attack vectors
3%
2%
2%
4%
6%
6%
6%
14%
55%
UDP spoof flood attack
TCP ACK flood attack
DNS amplification attack
IP protocol flood attack
NTP amplification attack
SSDP amplification attack
TCP SYN flood attack
Memcached amplification attack
TCP invalid SYN flood attack
CLDAP amplification attack
CharGEN amplification attack





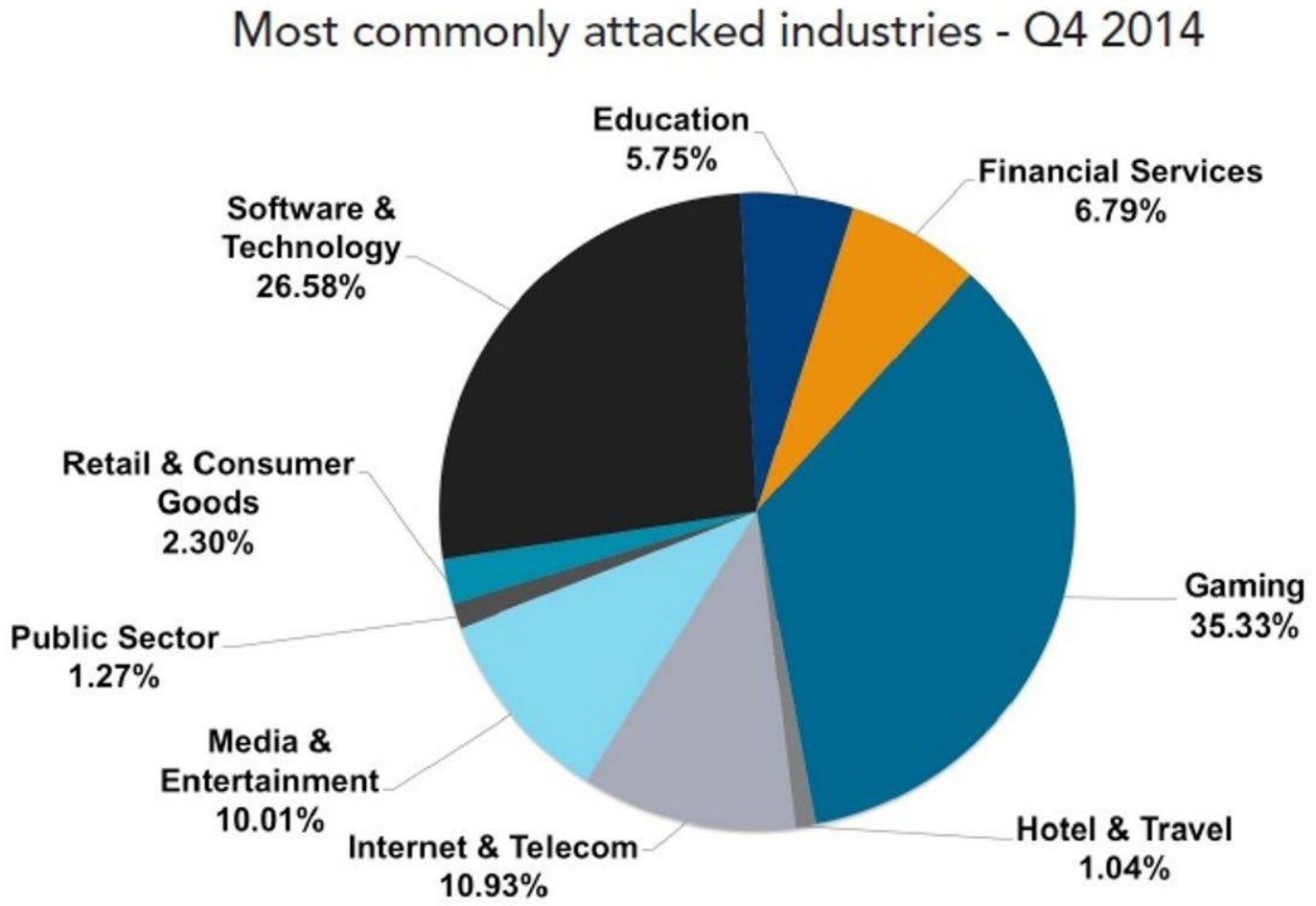


Figure 9: The gaming industry bore the brunt of DDoS attacks in Q4, driven by a surge in attack activity at the end of December

AWS OUTAGE

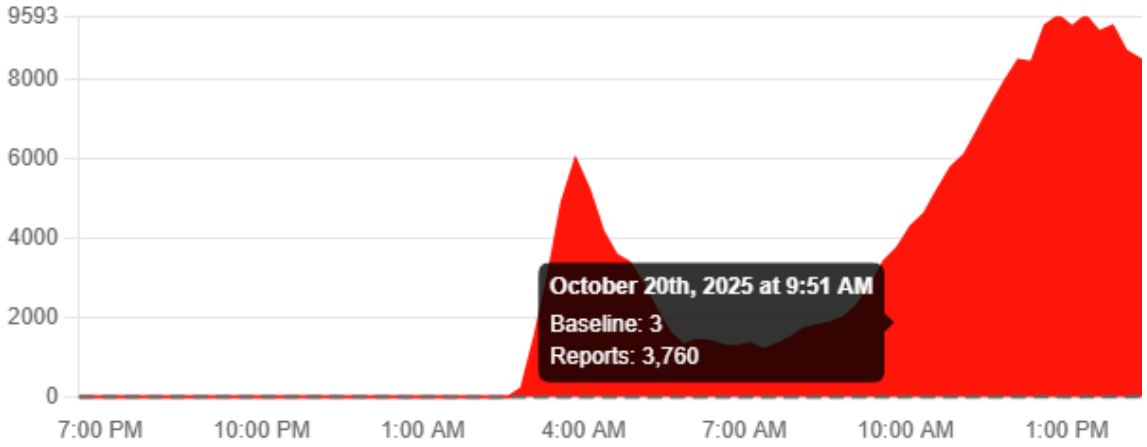
October 20, 2025

7+	78	50K+
HOURS	SERVICES	REPORTS
Total Downtime	AWS Affected	Downdetector

US-EAST-1 • DNS FAILURE • GLOBAL IMPACT

of October 2025

https://thenewstack.io/a-cascade-of-failures-a-breakdown-of-the-massive-aws-outage/



Don't Put All Your Eggs in One Cloud:

Lessons Learned from the October 2025 AWS Outage

DoS , DDoS what are those ?

➔ **DoS (Denial of Service):**

Attack that overwhelms system/network or services with excessive requests, causing victims to slow down/crash.

➔ **DDoS (Distributed Denial of Service):**

A large-scale DoS attack launched from multiple compromised systems/sources (botnets) simultaneously.

Attackers organize and control massive compromised victims/zombies via CnC server to pass large vol: traffic

and malicious to target network/hosts

➔ **Types of DoS/DDoS Attacks:**

- **Volume-based** (e.g., UDP flood, ICMP smurf /+ flood, DNS Amplification, ..)
- **Protocol-based** (e.g., SYN flood, Ping of Death, firewall resources)
- **Application-layer** (e.g., HTTP flood, DNS, …, Slowloris, …)
- **Organized attacks** (e.g., botnets /IRC, community driven activities, auto & manual operations)

very old **Tools:** Trinoo, TFN2K, LOIC, Stacheldraht, … ; **Defense:** static ACLs, blackholing, manual response

DDoS and MYANMAR

- ➔ back to 2003 - 2007, Myanmar those days got
  - ◆ only Telecom Dept /state-owned/ sole official Internet Services Provider
  - ◆ and one ISP covering two major cities and very few tiny competitor ISPs

    i.e fewer than 5K to 9K users only ; less than 30 websites, app/services hosted in mm Data Centers
    but, 2007 managed/unplug situation,
    2010 Oct-Nov massive DDoS, general election related ISP knock out days
    2011–2015 — political related DDoS/hacking against exile & independent mediaS, gov: sites
    2012 Aug – Operation Myanmar: Anonymous-linked actions ; DDoS & defaced 100+ Myanmar sites & **counterattacks**

    2010 cyberattacks on Myanmar - Wikipedia
    https://en.wikipedia.org/wiki/2010_cyberattacks_on_Myanmar

Key Trend, mostly : Politically-Motivated Cyber Attacks ; and **bandwidth PIPE sizing**, flow rate matters those days.

- ➔ 2021-2025/Present: Digital Conflicts
  - ◆ Recent Activity (2024): multi-vector attacks combining DDoS with data theft
  - ◆ Sophisticated botnets, socially organized, AI orchestrated and compromised IoT devices, VM, … were counted

Rise of Botnets (2010–2016)

- ➔ ? ony if you wanna know ??
- ➔ **Booter/Stresser services: DDoS-for-hire democratization**
- ➔ **Notable botnets: Kaiten, ZeuS plugin, Mirai**
- ➔ **IoT exploitation: routers, cameras, DVRs, smart home systems, …**
- ➔ **Amplification: NTP, SSDP, DNS reflection attacks**
- ➔ + more always with new tech: era

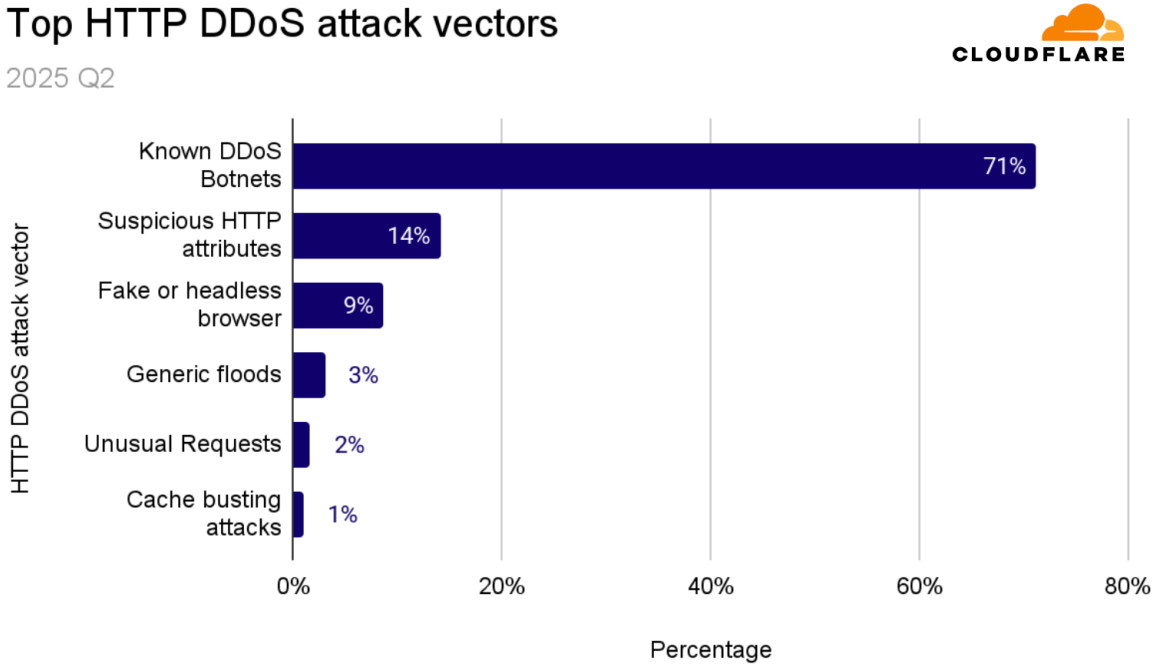
blog.**apnic.net**/2017/03/21/questions-answered-mirai-botnet

blog.**cloudflare**.com/th-th/ddos-threat-report-for-2025-q2

www.linkedin.com/pulse/understanding-ddos-attacks-growing-threat-zaheer-a-m-syed-xcc5c

2025 Threat Landscape

- ➔ Average attack duration: under 90 seconds
- ➔ Peak size: 3–5 Tbps (Cloudflare & Akamai data)
- ➔ AI-coordinated multi-vector reflection floods
- ➔ Common targets: ISPs, IXPs, DNS resolvers, CDNs, crypto exchanges



types of DDoS attacks by bot

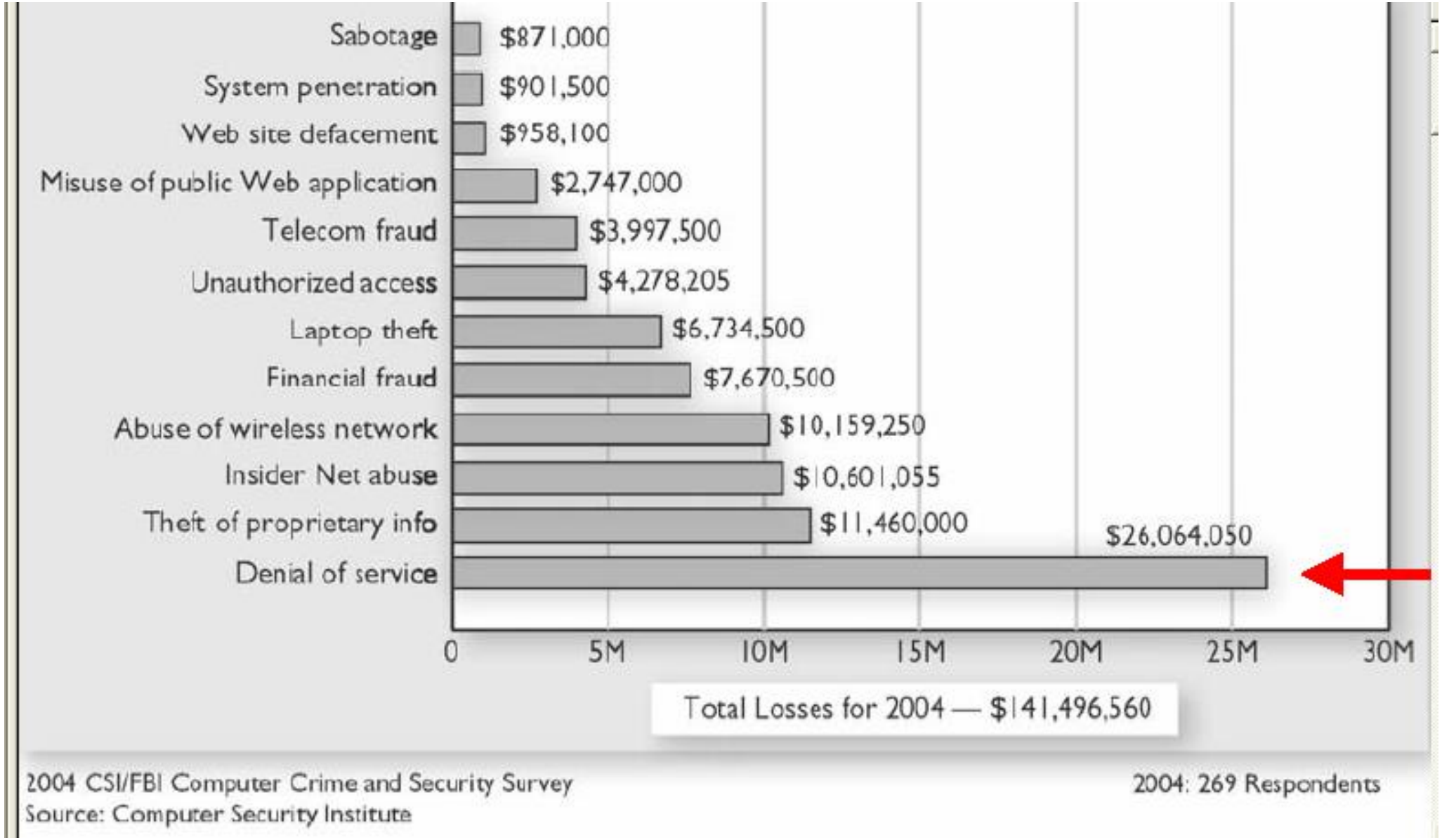
There are ten common types of DDoS attacks in bot.

1. UDP flood: Straight up UDP flood
2. VSE flood: Valve Source Engine query flood
3. DNS flood: DNS water torture
4. SYN flood: SYN flood with options
5. ACK flood: ACK flood
6. STOMP flood: ACK flood to bypass mitigation devices
7. GRE IP flood
8. Gre ETH flood: GRE Ethernet flood
9. Plain UDP flood: Plain UDP flood optimized for speed
10. HTTP flood: HTTP layer 7 flood

blog.**apnic.net**/2017/03/21/questions-answered-mirai-botnet

Costs of DoS attacks for victim organizations

→ D



Classification of DoS attacks

- **1. Bandwidth consumption:**
  - **Attacks will consume all available network bandwidth**
- **2. Resource starvation:**
  - **Attacks will consume system resources (mainly CPU, memory, storage space)**
- **3. Programming flaws:**
  - **Failures of applications or OS components to handle exceptional conditions (i.e. unexpected data is sent to a vulnerable component.)**
- **Routing and DNS attacks:**
  - **manipulate routing tables.**
  - **changing routing tables to route to attacker's net or black hole.**
  - **attack to DNS servers, hijacked or amplification attacks.**

attack methods

🧨 Smurf Attack

- ➔ send→ **ICMP Echo Request (ping)** to a **broadcast address** (192.168.1.255), [**spoofing the source IP** to the **victim's IP**.]
- ➔ All hosts on that network respond **directly to the victim**, -=> **amplified ICMP traffic**, Bandwidth Exhaustion and **DoS**.
- ➔ Easily mitigated by **disabling directed broadcasts** on routers, OS.and modern network devices
- ➔ **== Legacy attack** — mostly ineffective today because **routers now block broadcast pings**.

💣 Ping of Death

- ➔ **malformed or oversized ICMP** packets (>65,535 bytes) causing **buffer overflows** and **crashes** in vulnerable systems.
- ➔ already **patched** in all modern systems.

attack methods (contd:)

SYN Flood

- ➔ Exploits **TCP handshake state table**.
  client SYN → server ; server syn-ACK → client ; client → ACK —> conn: established.
- ➔ **how** ?? attacker sends SYN to victim side forging fake/bogon/or non-existent IP address
  - ◆ victim server side replies with SYN/ACK or RST to those non-consistent IP addrs
- ➔ The victim/server allocates memory for each half-open connection (SYN_RCVD).
  - ◆ and victim keep waiting for ACK … and potential conn: in queue for establish sockets, syn-rcv
  - ◆ queues are small/limited, take some time for timeout to flush queue; e.g 70-90 seconds
  - ◆ if few more broken SYN are sent by attacker every 5 or 10 seconds, victim never clear Q
  - ◆ == resulting quota run out for legitimate actual user conn: service traffic
  - ◆ such attacks fill the **backlog queue**, preventing legitimate connections for real users.
- ➔ Mitigations: **SYN cookies**, **firewall rate-limiting**, or + **connection timeouts** *Server CONFIG*.

Summary:

All three exploit took advantage of network protocol weaknesses (ICMP/TCP).

Modern defenses (firewalls, patches, anti-spoofing, rate limits and server settings) **mitigate them effectively**.

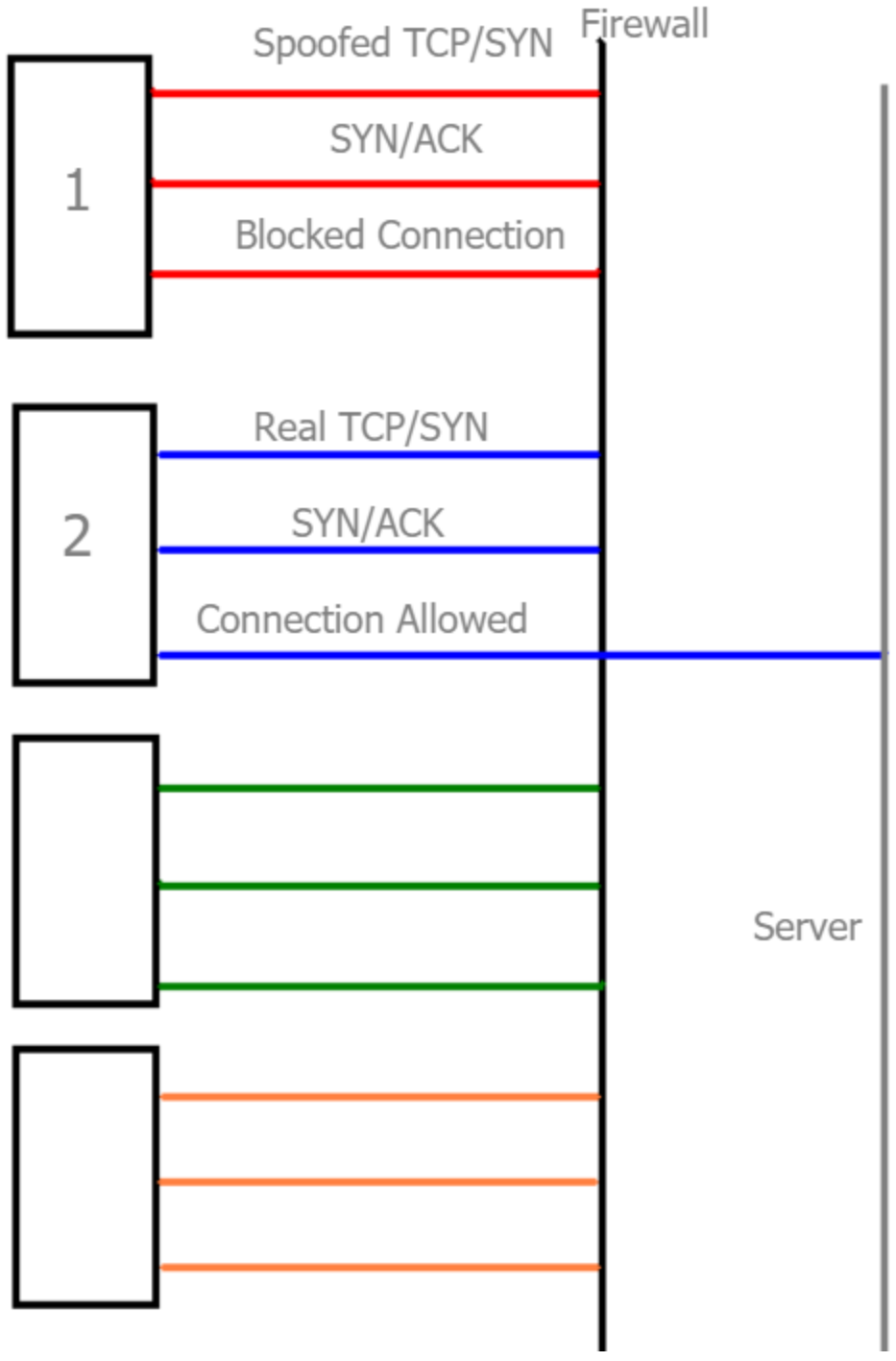
ref:

- **TCP/IP illustrated**

  vol: 1 - 2 - 3

- **and …**
- pentics.net/denial-of-service/white-papers/smurf.html

- NIST Guidelines for DDoS Prevention
- OWASP DDoS Prevention Cheat Sheet
- Cloud Security Alliance DDoS Guidance
- **...**



Modern Tech:s & Infra: Impacts

- IoT & botnet evolution
- Cloud/API-based abuse (Layer 7 & DNS floods via cloud workloads)
- Amplification and reflection updates
  (Memcached → WS-DD → TCP reflection → QUIC abuse)
- AI-driven attack coordination
  (bot orchestration using LLM automation)
- DNS and Anycast-targeted floods
  (resolver poisoning & resolver exhaustion)
- BGP & route leaks as DDoS vectors
- Darknet coordination & leaked botnet control panels
- Traffic visibility gaps in 5G
  & CDN-assisted DDoS

how to survive

- accept Modern attack architecture & AI orchestration
- Defense frameworks & coordination (NOC–SOC)
- Operational metrics, KPIs, and future outlook

Prevention and Mitigation Strategies + life cycle dev:

- **Traffic Analysis**
  - behavioral analytics by ML for pattern recognition normal traffic baseline
- **Overcapacity Planning**
  - Maintain 5x BW capacity, auto-scaling solutions+ load balancing
- **Web Application Firewall (WAF):**
  - Deploy next-gen WAFs with AI capabilities, custom + Regular rule updates
- **Content Delivery Networks (CDN):**
  - Global network of scrubbing centers, Anycast networking TCP Anycast + BGP announcements
- **DDoS Mitigation Services:**
  - 24/7 monitoring Hybrid protection (on-premise + cloud) Time to mitigation SLAs

Mitigation Frameworks

- Defense-in-Depth: Layered Mitigation Diagram (with inline architecture figure)
- Flow telemetry and anomaly detection (NetFlow/IPFIX, sFlow, AI-assisted correlation)
- Cloud Signaling (with community partners + upstream coordination)
- Edge ACL templates (best practices for Tier-1/Tier-2)
- BCP38, uRPF, Flowspec, **RTBH automation examples**
- Cooperative defense models (IXP-level mitigation, MANRS, TF-CSIRT)
- Live SOC runbook overview: DDoS triage → filter → comms → restore

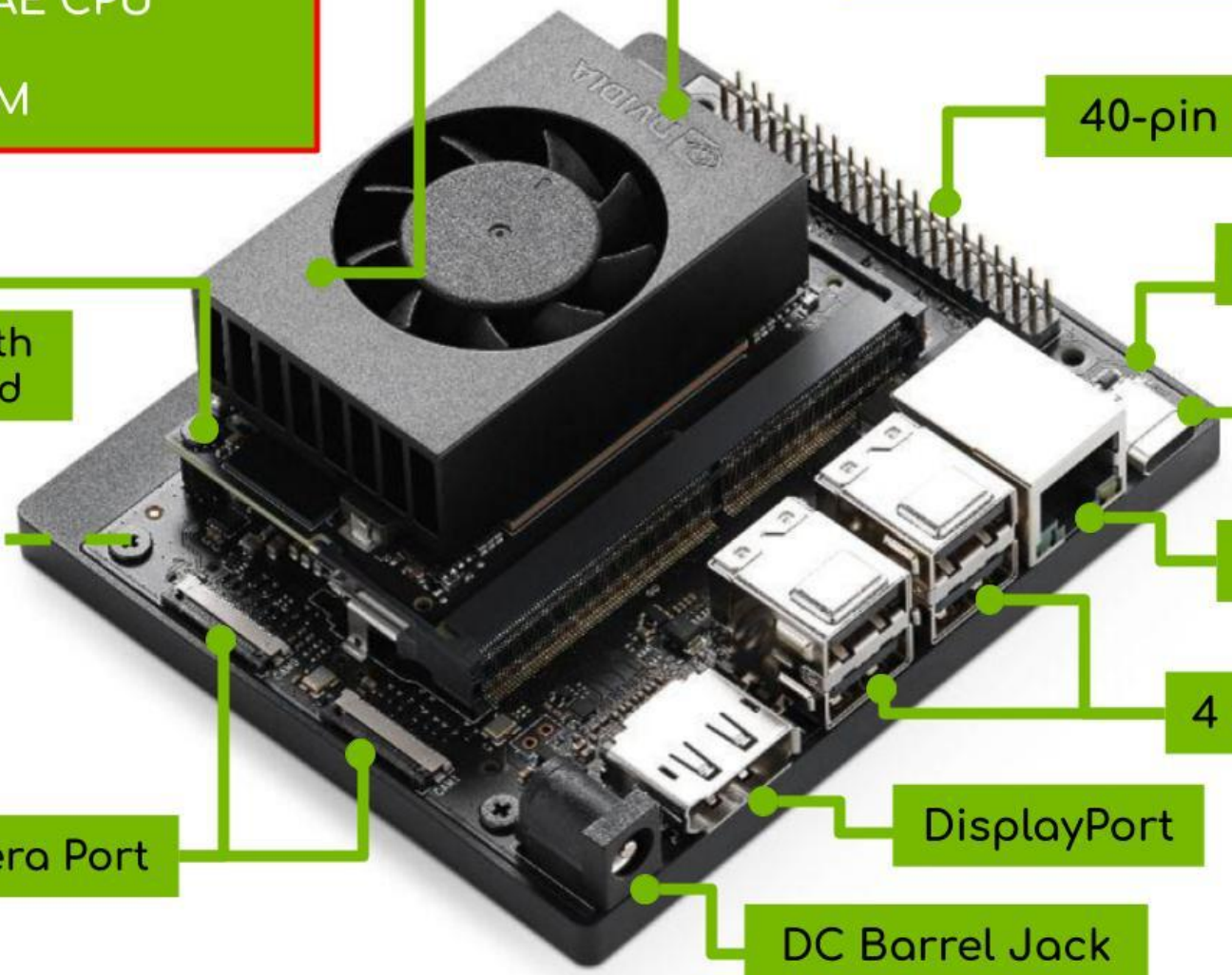
- + YOU & your team awareness, …
- + **Local AI**, and off-grid knowledge base, offline internet resources


NVIDIA
DGX
Spark


ORIN
JETSON ORIN NANO
DEVELOPER KIT


NVIDIA RTX PRO 6000 BLACKWELL
MAX-Q VS WORKSTATION EDITION

NVIDIA Jetson Orin Nano Module:
- NVIDIA Ampere™ Architecture GPU
- 1024 x CUDA Core
- 32 x 3rd Gen Tensor Core
- 6-Core Arm Cortex-A78AE CPU
- 8GB 128-bit LPDDR5 RAM



microSD Card Slot

Heatsink with Cooling Fan

40-pin Expansion Header

Power Indicator LED

USB-C, Data Only

Gigabit Ethernet

4 x USB 3.2 Type A

DisplayPort

DC Barrel Jack

IEEE 802.11 WiFi & Bluetooth with Antennas Preinstalled

2 x 22-pin MIPI CSI Camera Port

MMOG

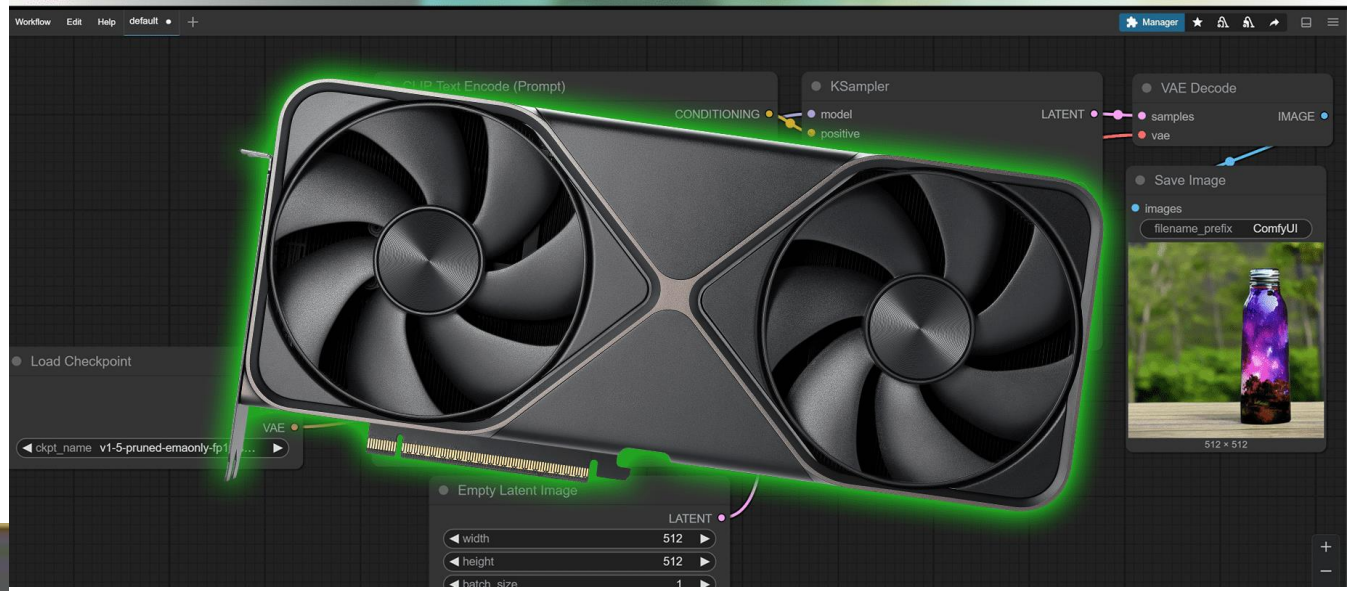
NVIDIA BLACKWELL GPU
GEN AI SUPPORT

Wikipedia
¿Cómo usarla fuera de línea sobre GNU/Linux con Zim y Kiwix?

Zim

WIKIPEDIA
La enciclopedia libre

KIWIX



LLaMA C++


GB10 Superchip
Blackwell GPU
1 PetaFLOP FP4 AI Compute
Grace CPU
20 Arm Cores
High-Bandwidth Unified Memory
128 GB Low Power DDR5X
Connectivity
Wi-Fi, Bluetooth, USB
ConnectX
NCCL, RDMA, GPUDirect
4 TB SSD

Future & Recommendations

- Threat forecasts for 2026–2028 (AI, QUIC, satellite backbones, post-quantum comms)
- Automation & AI in DDoS detection: promise vs risk
- SOC/NOC operational checklist and KPIs
- Summary, key takeaways, and Q&A

- + your opinion, dev: cycle and mitigator activation preparations

Thank you

Q&A

Bro Naing
bronaing at **ymail**.com

www.mmnog.net.mm

event@mm-ix.net