Unravelling the Changing Landscape of DDoS Attacks: The Role of IoT Botnets

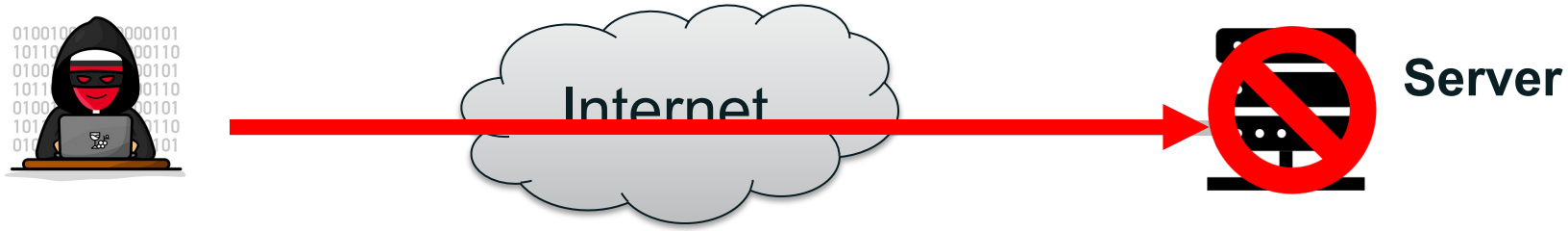
Characterizing attack patterns

Carlos H. Gañán

ICANN DNS Symposium
September 2023

Denial of Service Attacks

- Denial-of-Service (DoS) attack is an attempt by attacker to prevent legitimate users from using resources



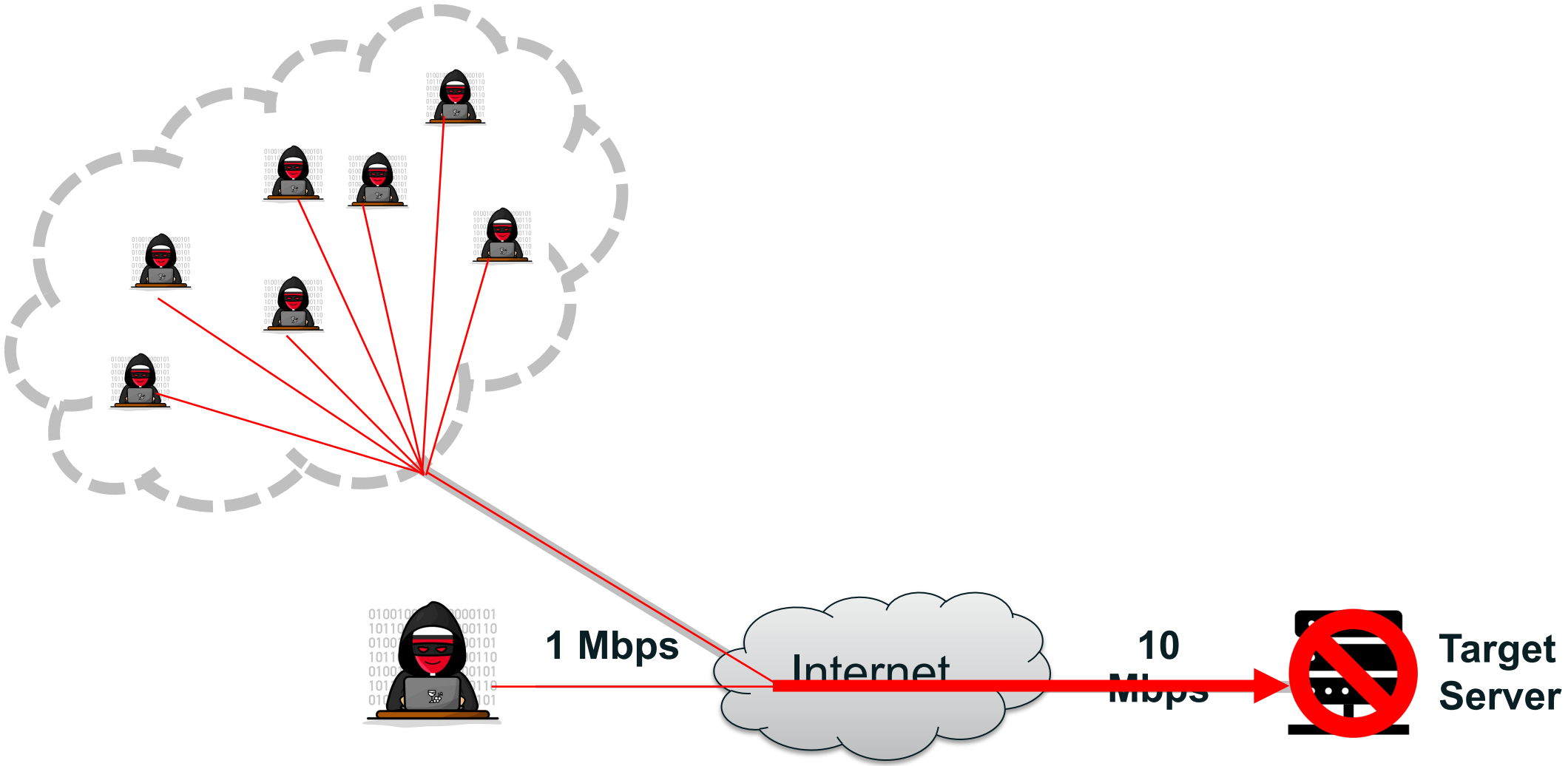
- Different types:
  - Volumetric
    - Smurf Attacks, ICMP Floods, IP/ICMP Fragmentation, etc.
  - State-exhaustion
    - SYN Floods, UDP Floods, TCP Flood attack, Connection Exhaustion, etc.
  - Application layer attacks
    - HTTP-encrypted flood, DNS query floods, etc.

Distributed Denial of Service (DDoS) Attacks

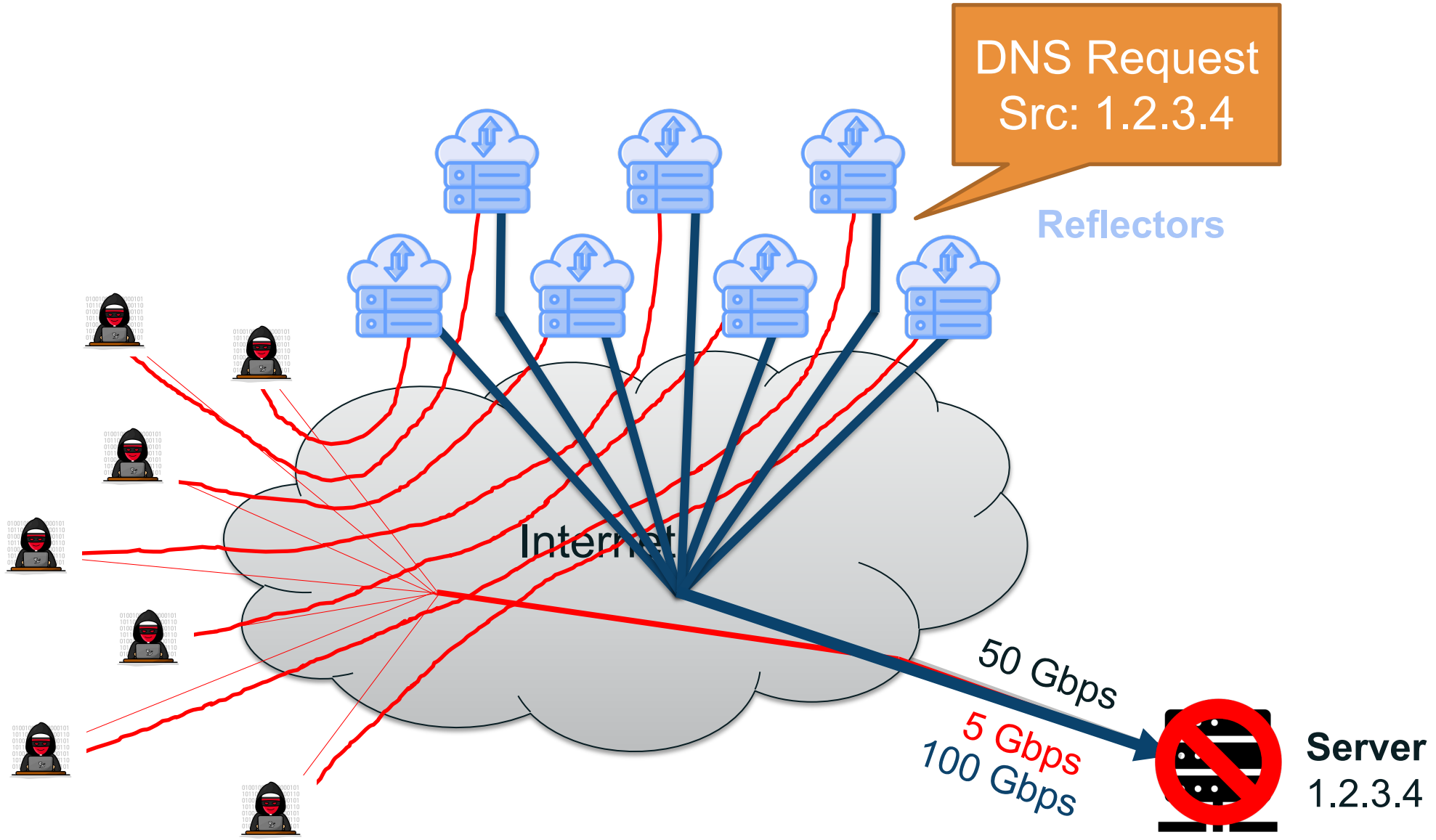
- “Many to one”
  - Large number of hosts send service requests/packets simultaneously

- How can scalability be achieved?
  - “Associates”
  - Reflection and amplification
  - Botnet

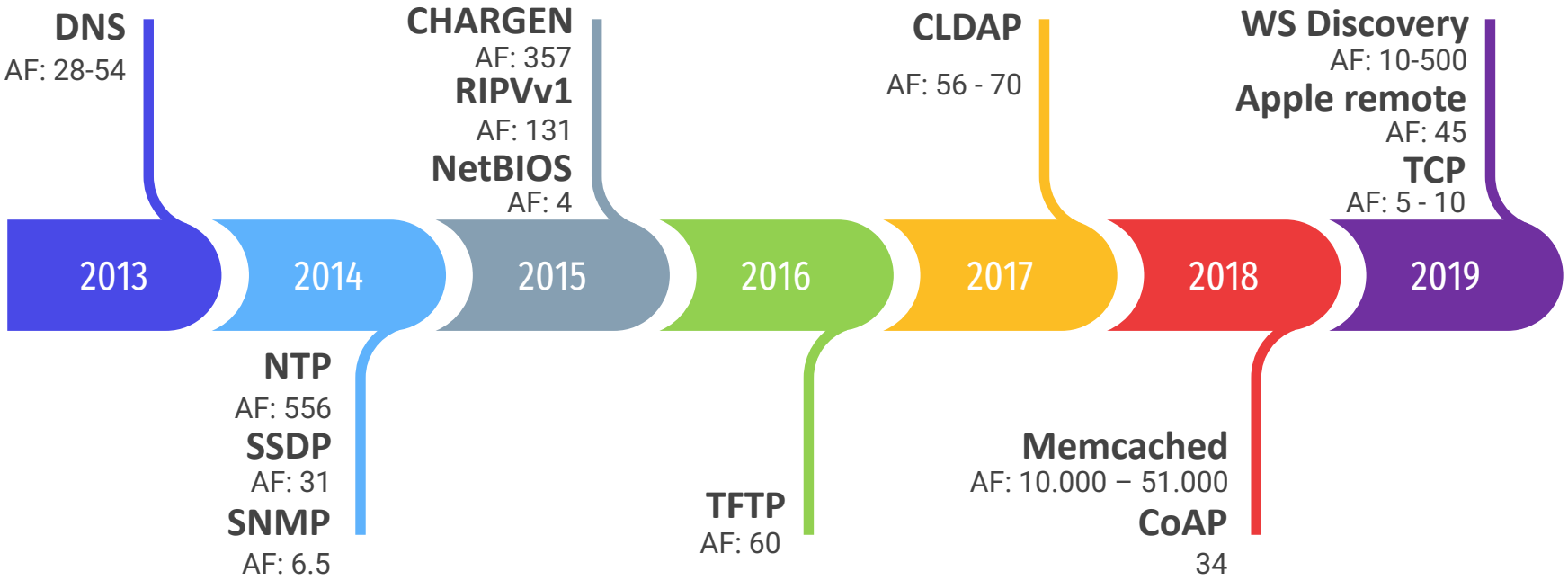
Volumetric DDoS example



DrDOS example

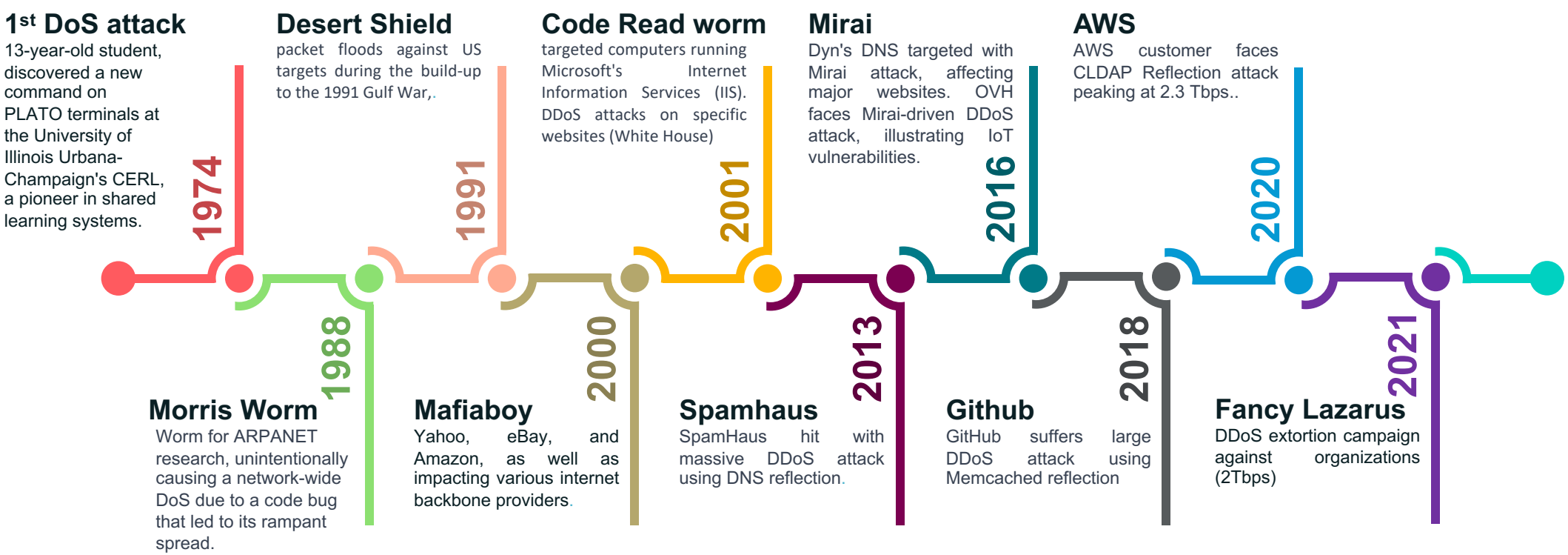


Evolution of DDoS amplification vectors and factor (AF*)



*Estimated AF might vary depending on the query

Notorious DDoS attacks



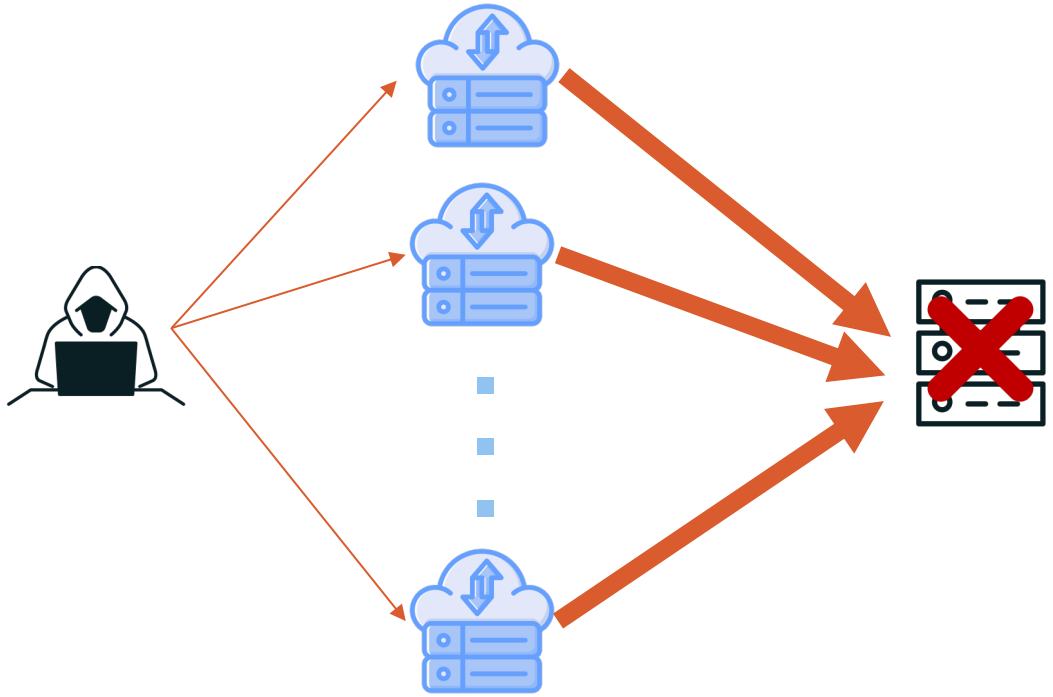
Focus of this talk

- How has the emergence of IoT botnets influenced the landscape of DDoS attacks?
- Who constitutes the primary targets of DDoS attacks orchestrated through IoT botnets?
- How do the targets of IoT botnet attacks compare to DrDoS attacks?

Research methodology

Data collection

- Honeypot-based monitoring of *amplification* DDoS Attacks



https://sec.ynu.codes/dos

- IoT botnet Command and control (C2) milker

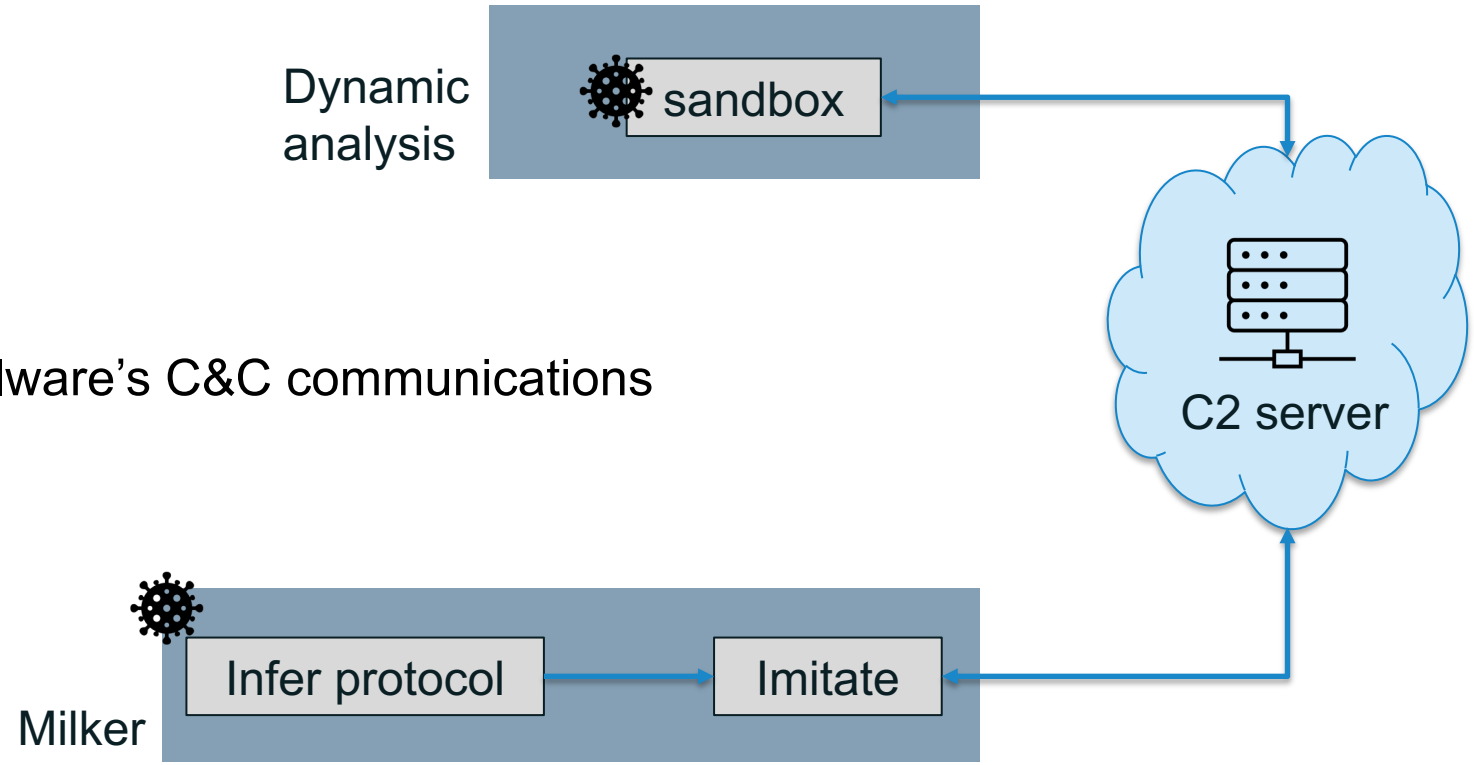
https://sec.ynu.codes/iot

Amplification honeypot (Amppot)

- Simulated Amplification Attack Vectors:
  - Listens on UDP ports with known amplification capabilities: QOTD (17), CharGen (19), DNS (53), NTP (123), NetBIOS (137), SNMP (161), SSDP (1900), MSSQL (1434), SIP (5060/5061)
- Modes of Operation:
  - Emulated:
    - Protocol-specific parsers and responses
    - Random selection from pre-generated responses
    - Recursive resolution for certain protocols like DNS
  - Proxied:
    - Forwards requests to internal servers operating vulnerable protocols
    - Responses sent back to client
    - No emulation, actual server response
  - Agnostic:
    - Responds regardless of request validity
    - Sends large, invalid response

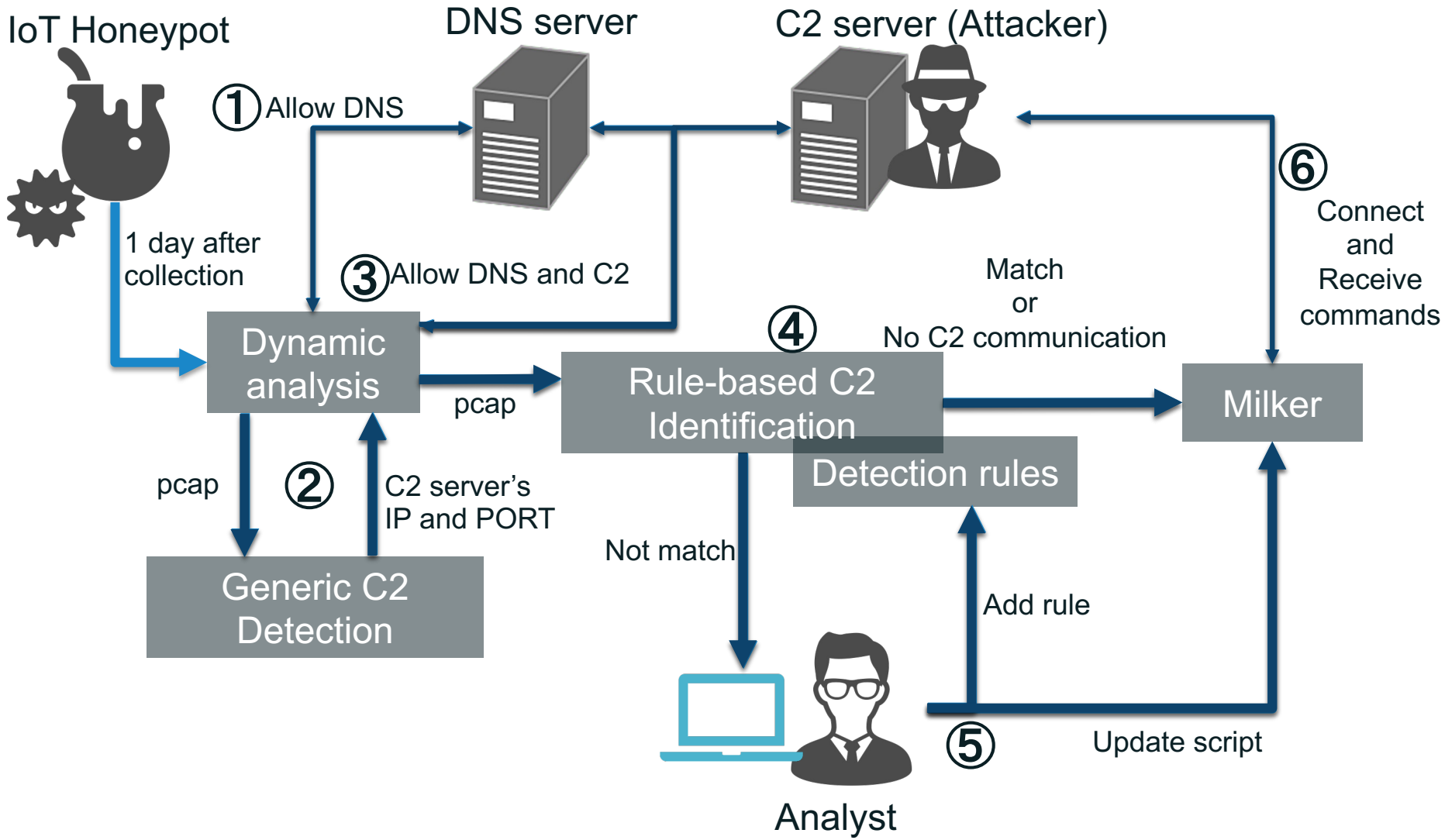
How to pinpoint IoT botnet DDoS targets?

- **Dynamic analysis**
  - Execute malware in sandboxes



- **Milker**
  - Script imitates malware's C&C communications

IoT botnet C2 Milker



Milked DDoS commands

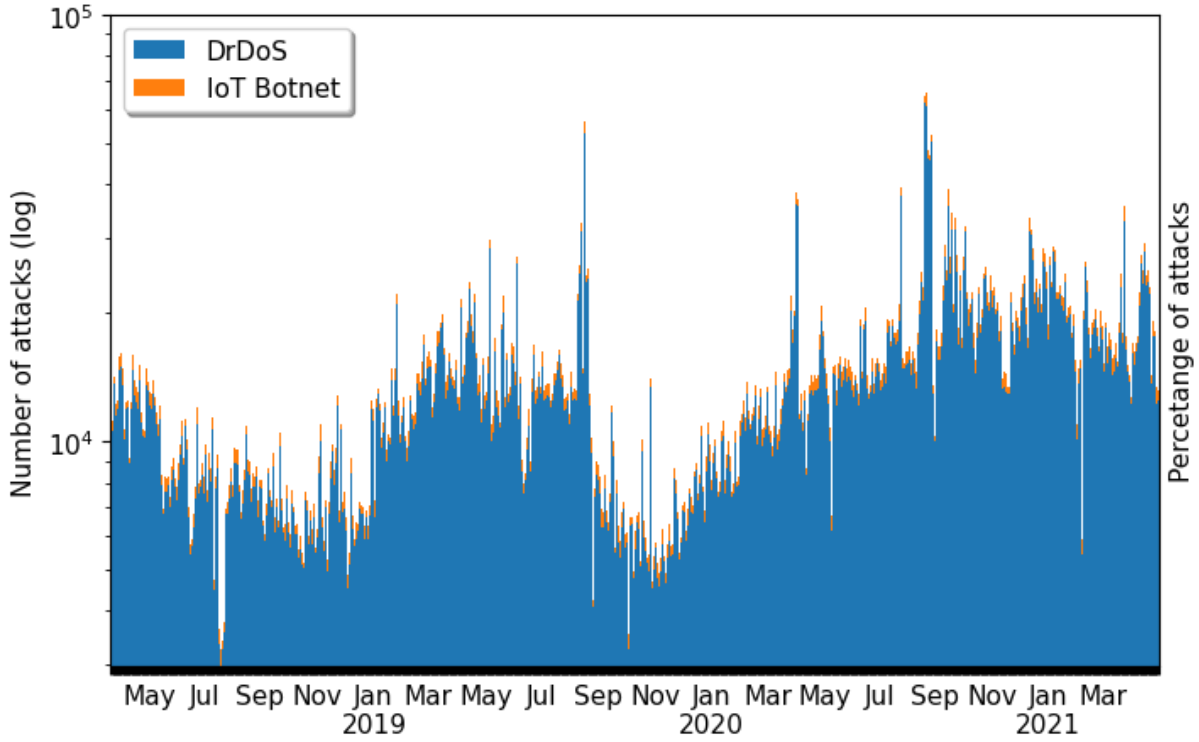
- Attack commands received from the C2s:
  - Mirai botnet source code as reference:
    - UDP flooding

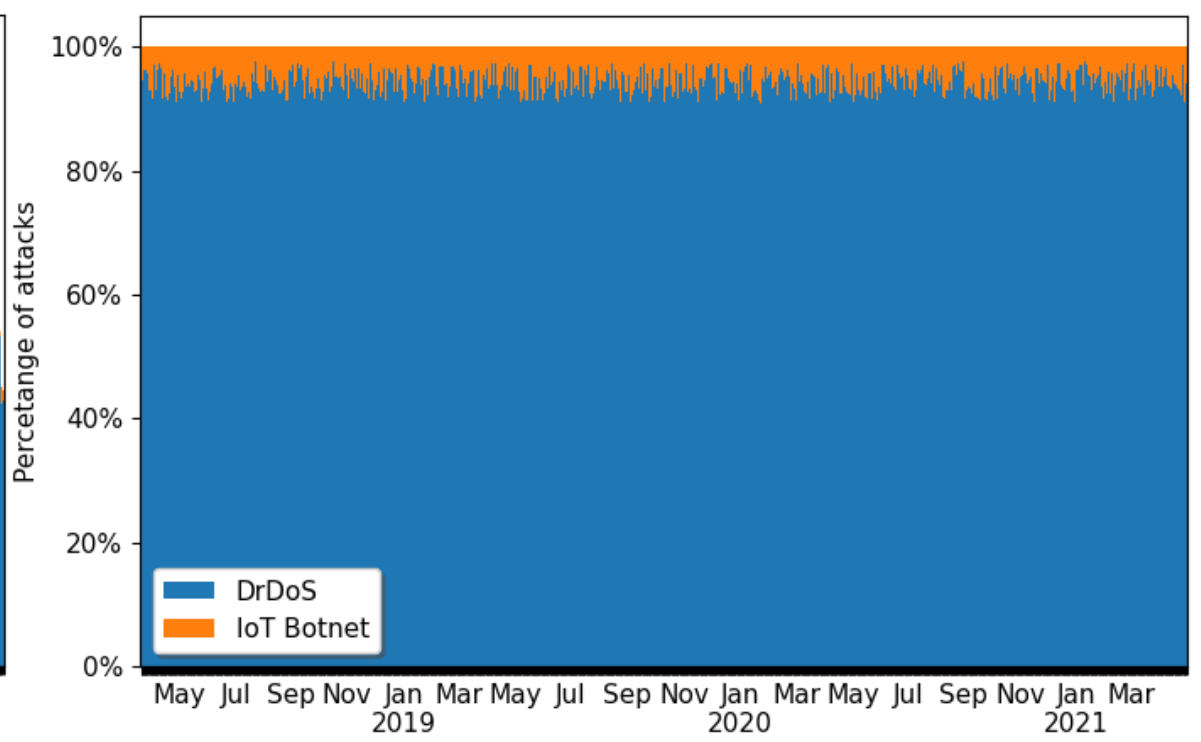
      Valve source engine flooding
    - TCP ACK flooding
    - TCP "Stomp" attack
    - TCP SYN flooding
    - GRE Packet flooding
    - HTTP request flooding
    - “DNS Water Torture”

Characterizing attacks

Number of attacks per day

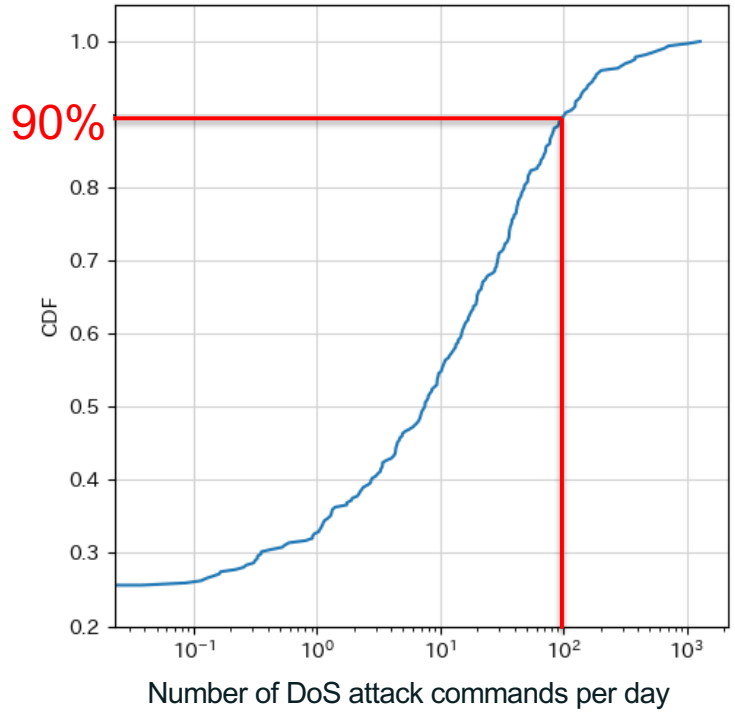
- Between 1% to 2.5% of the total number of daily DDoS attacks come from IoT botnets



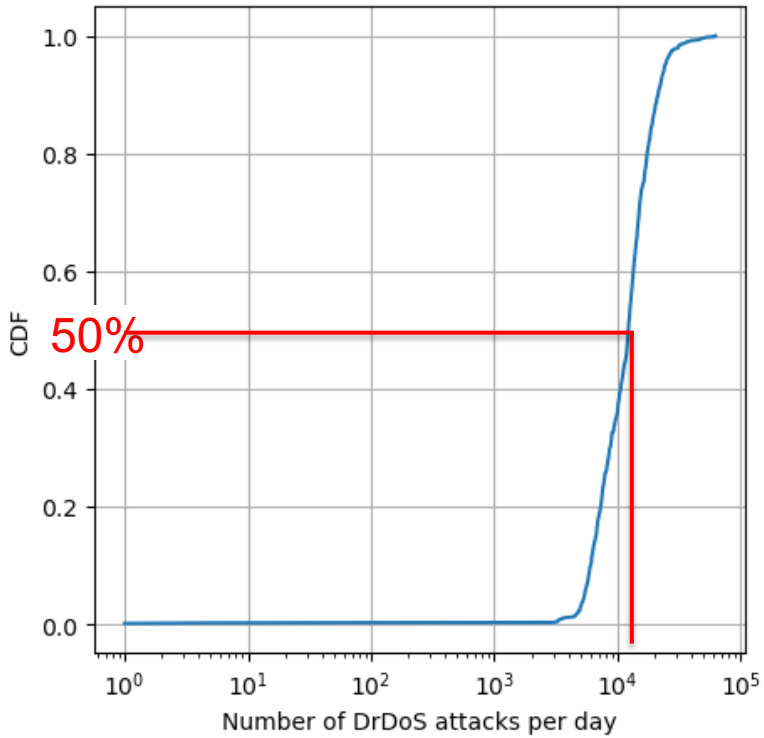


Number of attacks per day

- About 90% of C2 servers sent **less than 100 attacks** commands per day

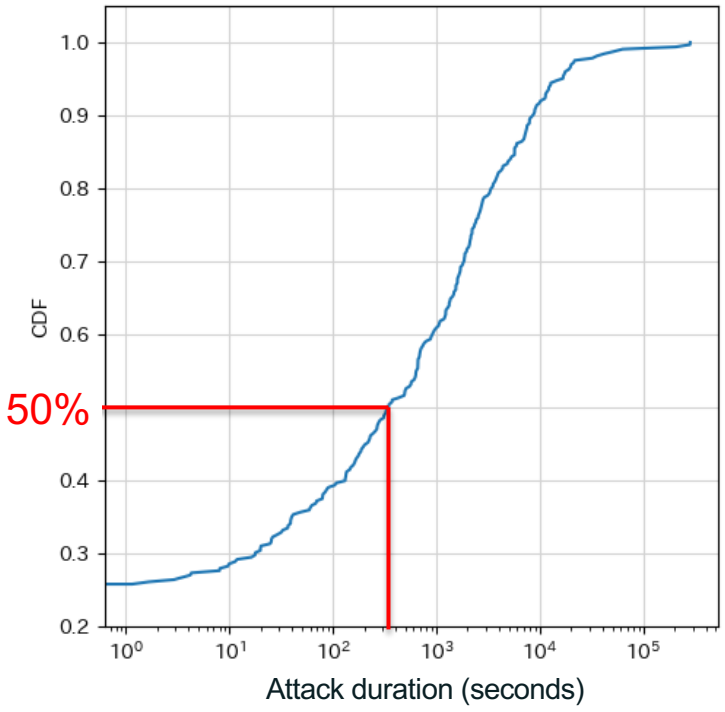


- On average, **more than 13,000 DrDoS** attacks per day

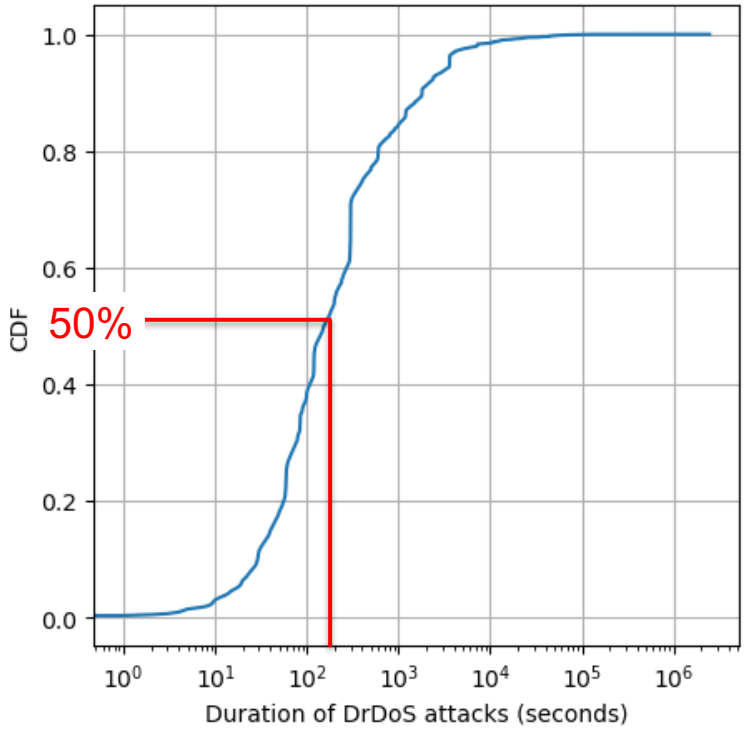


Attack duration

- 50% of requested attacks had a duration of **less than six minutes**

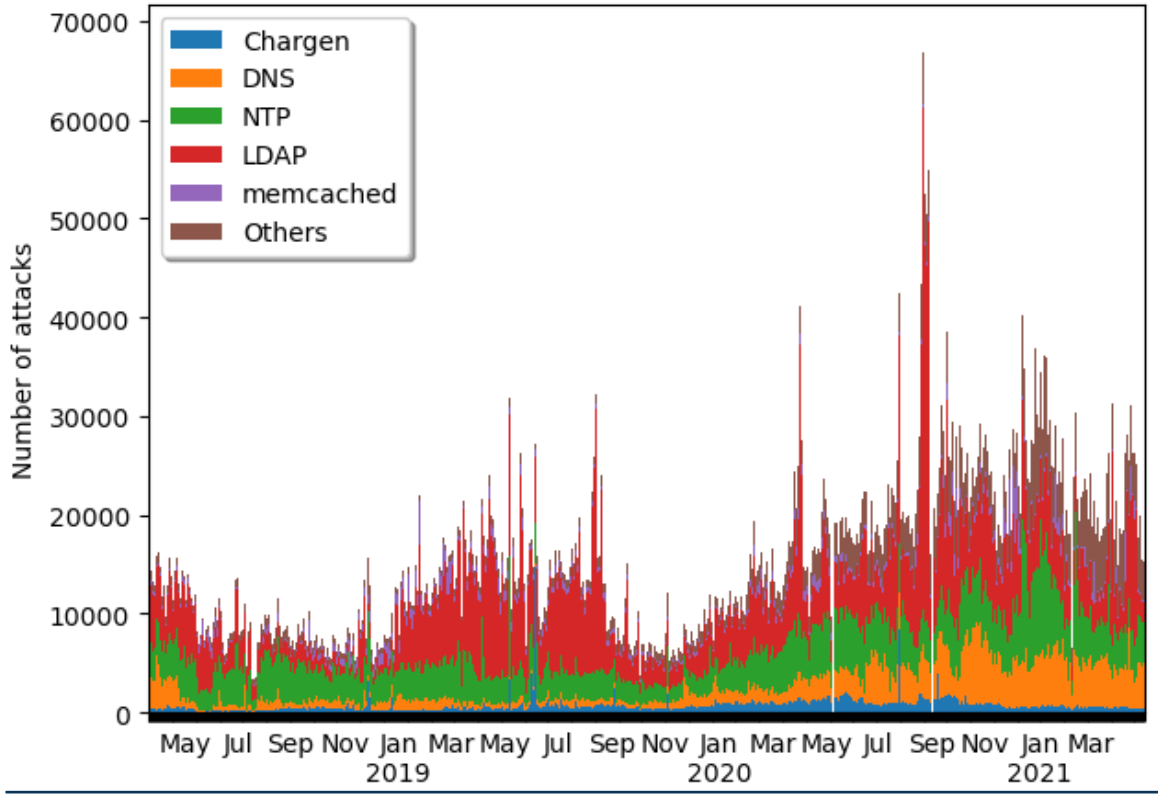


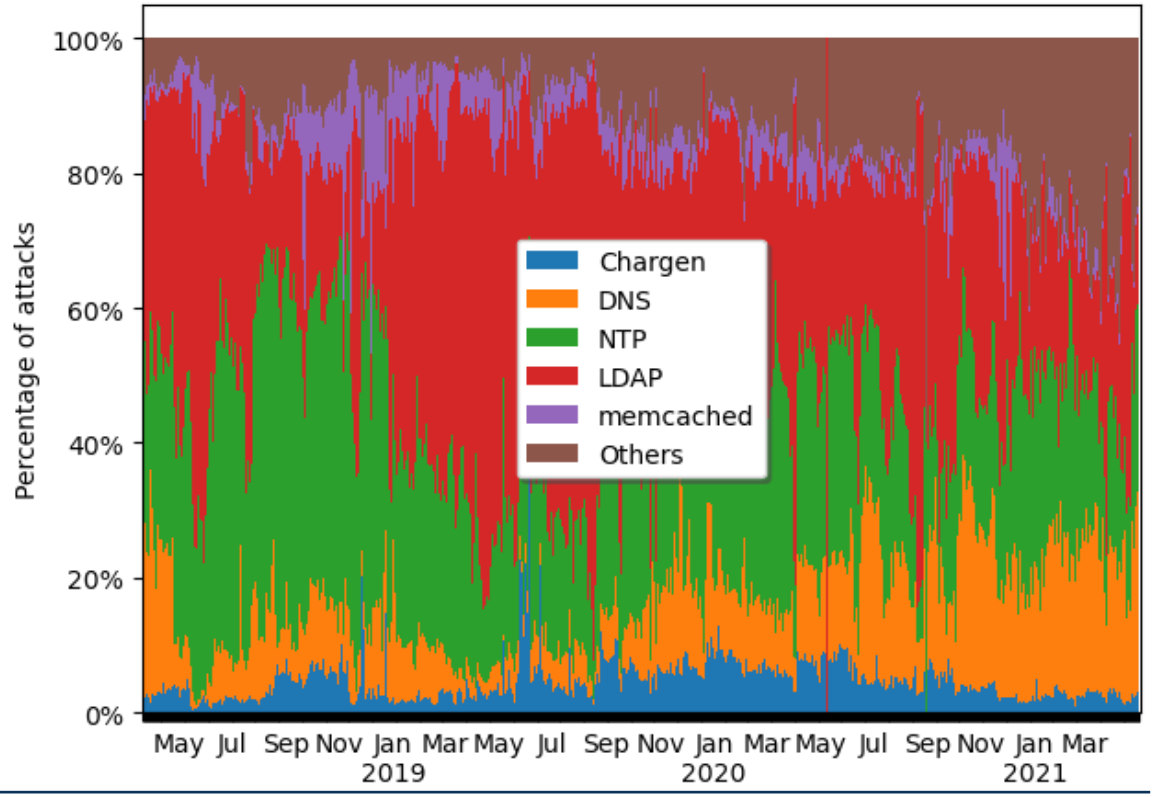
- 50% of DrDoS attacks had a duration of **less than three minutes**



Targeted ports

- DNS remains a prevalent DDoS attack vector
  - On average, around 2,000 DNS DrDoS attack per day





Targeted ports

- Trend of **targeting game servers**
  - Port 30120 (FiveM Server)
  - Port 25565 (Minecraft Server)
  - Port 7777 (Steam ARK Server)

Port	%	Port	%
80	16.0%	**389**	1.6%
53	7.1%	**25565**	1.5%
443	6.8%	**1194**	1.4%
22	6.0%	**7777**	1.2%
30120	1.9%	**68**	1.2%

- Amplification services
  - NTP and LDAP account for more than 64% of the attacks

Port	%	Port	%
123	32.7%	**161**	2.0%
389	31.9%	**3702**	1.6%
11211	8.9%	**3283**	1.5%
53	6.0%	**1900**	1.4%
19	4.5%	**37810**	1.2%

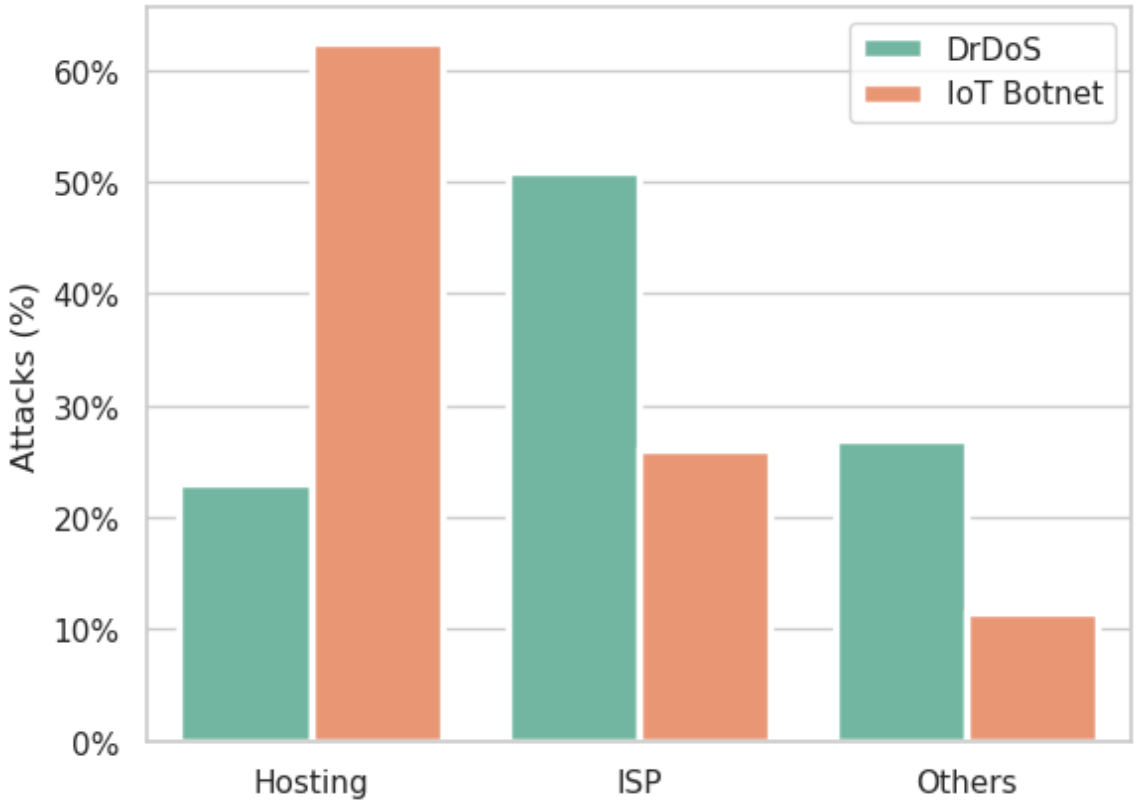
Characterizing targets

Data enrichment

- AS Types
  - Historical BGP data from Routeviews for precise AS Number (ASN) retrieval.
  - CAIDA’S AS classification and Standford’s ASdb dataset.
  - Passive DNS data to identify hosting ASes using a heuristic approach.
- AS Rankings:
  - AS sizes and connectivity using CAIDA's AS Rankings.
- IP geolocation:
  - MaxMind's GeoIP location database for victim IP geolocation.
- Domain-Level popularity:
  - Tranco list to estimate domain value and popularity.

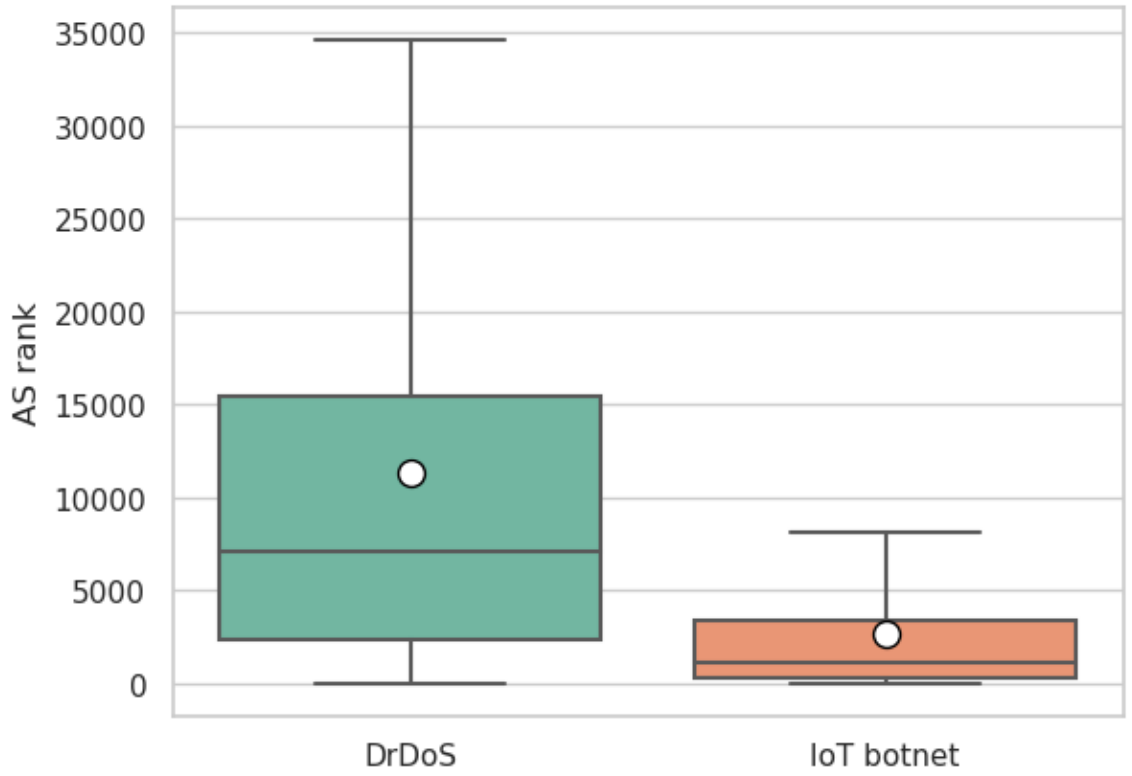
AS type comparison

- Hosting networks are more frequently the focus of IoT-botnet attacks



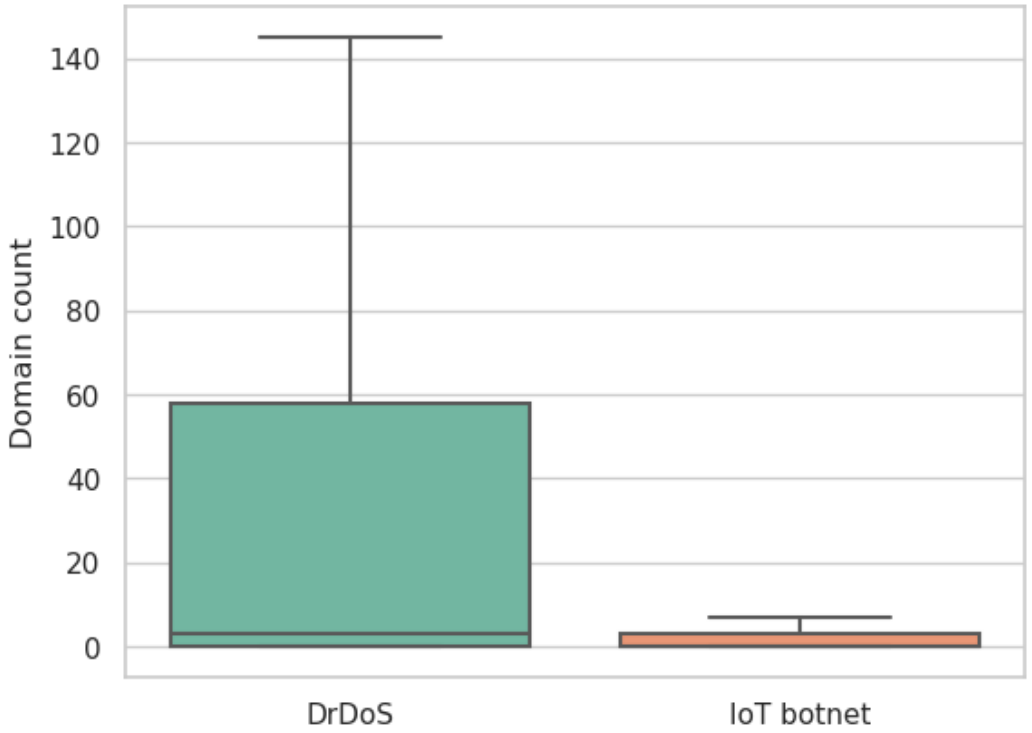
AS rank comparison

- DDoS attacks carried out by IoT botnets tend to target highly ranked ASes



Number of “victims” per attack

- IoT botnet DDoS attacks more frequently target domains hosted on dedicated servers

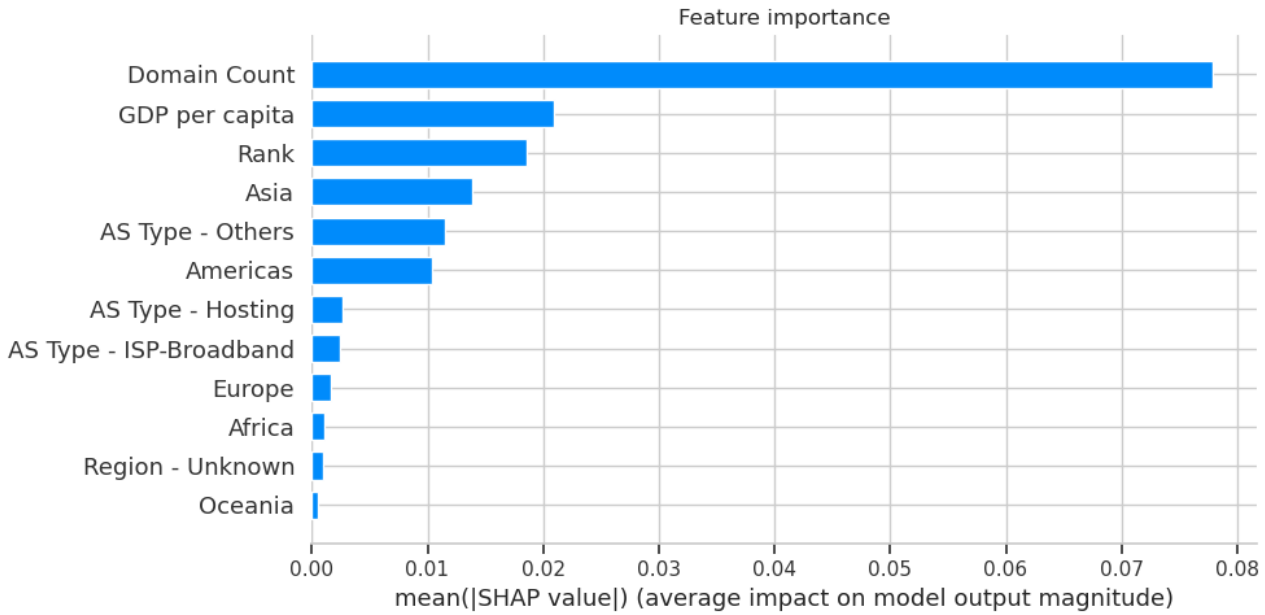


Modeling Method: XGBoost for Target Analysis

- **Objective**: predict the likelihood of DrDoS vs. IoT-botnet Attack.
- **Approach**: XGBoost regressor
  - Parameters were tailored based on the results of a random search
  - Adjustments were made within a small range (±10% for learning rate and ±20 for other parameters) to fine-tune the model without dramatically altering its structure.
    - Learning Rate: Adjusted around the best value to refine convergence without drastic changes.
    - Max Depth: Denotes the maximum depth of a tree. Chosen as the best value to prevent overfitting while capturing important patterns.
    - Number of Estimators: Refers to the number of boosting rounds or trees. Ranged around the best value to assess model performance with slightly more and fewer trees.
    - Subsample: Proportion of training data used for building trees. Kept constant with the best value to ensure stable and consistent sampling.
- **Feature Set**:
  - Ordinal Features: Domain count, CAIDA ranking of targeted AS.
  - Categorical Features (One-Hot Encoded): Region based on victim IP's geo-location, AS type.

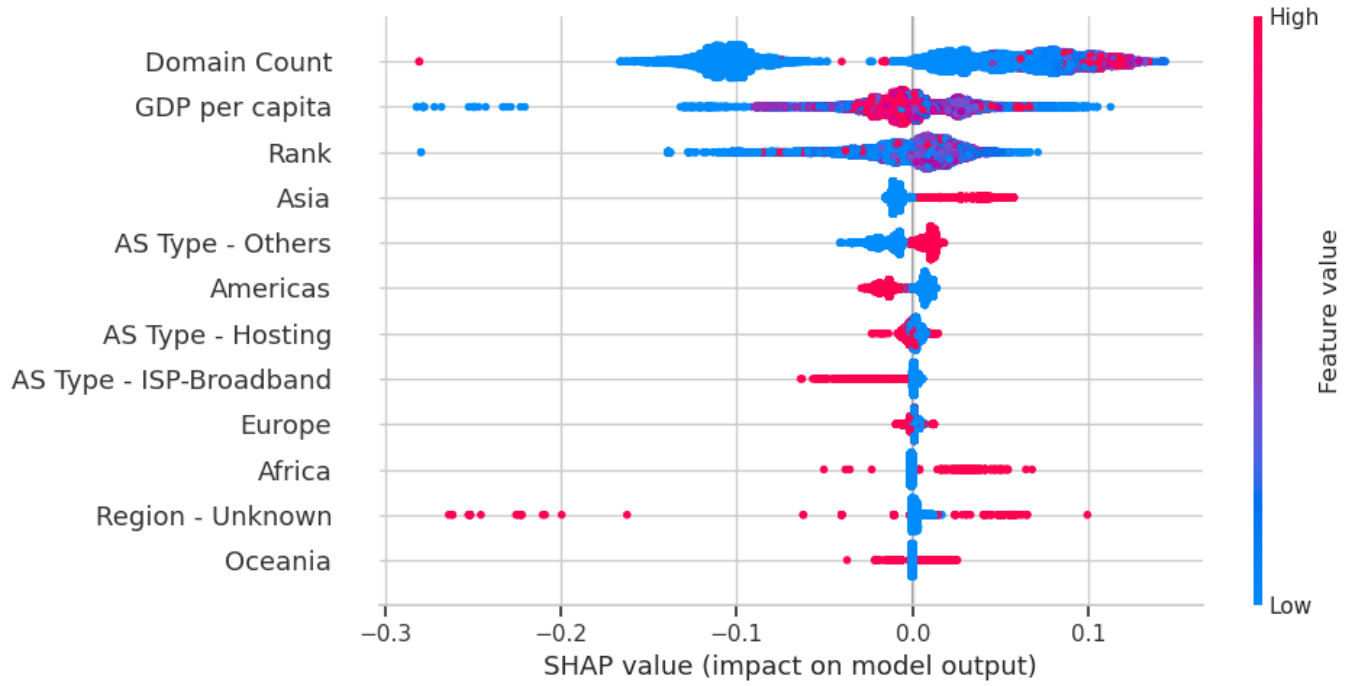
What factors differentiate targets of DDoS attacks?

- **Domain Count :** The count of domains holds the highest importance in predicting attack likelihood.
- **AS Rank**: CAIDA ranking of target AS plays a significant role.
- **GDP per Capita**: Economic strength, represented by GDP per capita, affects the attractiveness of targets.
- **Asia , Americas, Europe**: Geographic regions matter.



SHapley Additive exPlanations

- Lower number of domain names leads to higher chance of receiving an IoT-botnet attack.
- Larger ASes have higher chances of receiving an IoT-botnet attack.



Conclusions

Conclusion

- DDoS has been a longstanding issue for over two decades:
  - The attack vectors have remained relatively consistent.

- The rise of IoT botnets has amplified the scale of these attacks:
  - Longer attacks.

- Different victimization patterns from IoT botnets:
  - High-value targets often under attack.
  - Dedicated hosting attacks
    - Reduced number of collateral victims.

Thank You and Questions

Email: carlos.ganan@icann.org