

Lessons from an (Unsuccessful?) IPv6 Amplification Honeypot Deployment

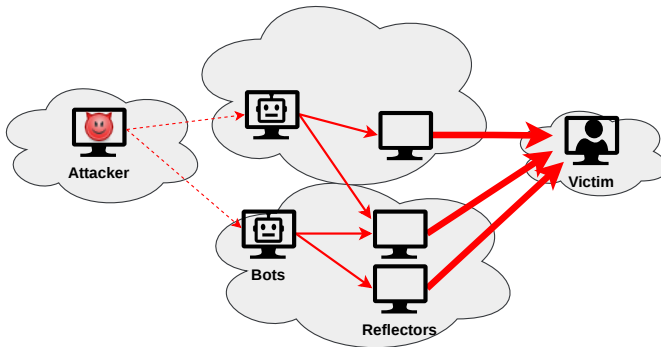
Tiago Heinrich (*MPI-INF*), **Sebastian Kappes** (*MPI-INF*), Rafael R. Obelheiro (*UDESC*)

Monday 17th August, 2026

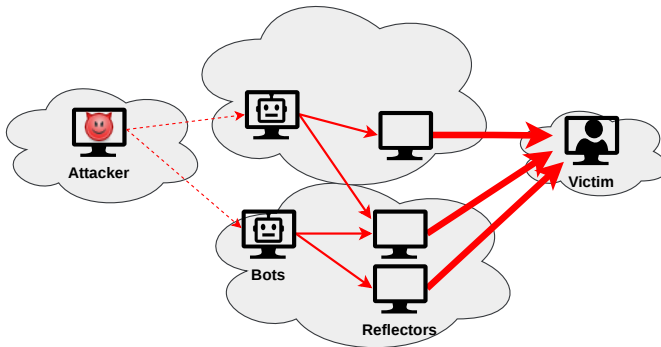
Workshop on Negative Results in Network Measurements 2026



The Problem: Reflected DDoS Attacks

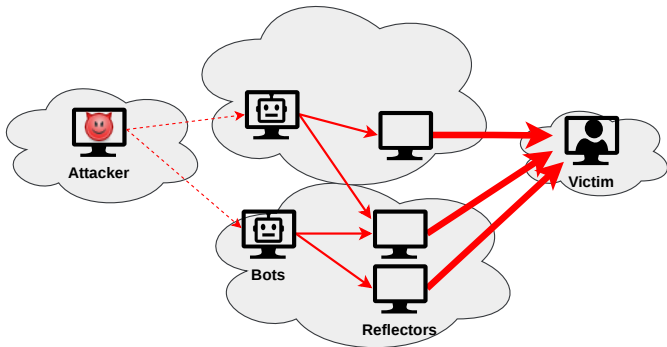


The Problem: Reflected DDoS Attacks



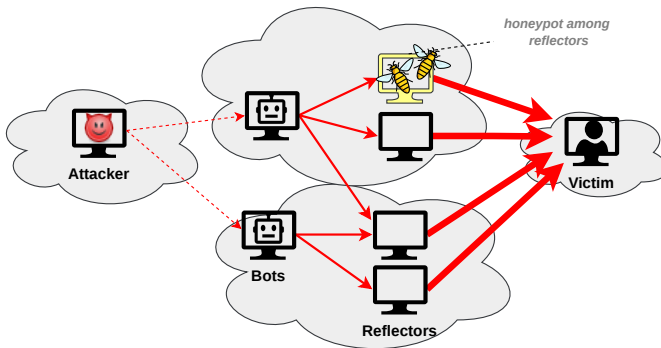
⇒ **How** can we **study** reflected DoS attacks?

The Problem: Reflected DDoS Attacks



⇒ **How** can we **study** reflected DoS attacks? ...in IPv6?

The Problem: Reflected DDoS Attacks



⇒ **How** can we **study** reflected DoS attacks? ...in IPv6?

- **Idea: Let's build an IPv6 reflection honeypot.**

- We extended the **MP-H Honeypot**¹ to support IPv6.
 - supports **seven** common reflection protocols (*Chargen, CLDAP, DNS, Memcached, NTP, SSDP, and QOTD*)



¹T. Heinrich, R. R. Obelheiro, and C. A. Maziero. [New Kids on the DRDoS Block: Characterizing Multiprotocol and Carpet Bombing Attacks](#). In *International Conference on Passive and Active Network Measurement*, pages 269–283. Springer, 2021

- We extended the **MP-H Honeypot**¹ to support IPv6.
 - supports **seven** common reflection protocols (*Chargen, CLDAP, DNS, Memcached, NTP, SSDP, and QOTD*)
- **Challenge: How do we attract scanners?**



¹T. Heinrich, R. R. Obelheiro, and C. A. Maziero. [New Kids on the DRDoS Block: Characterizing Multiprotocol and Carpet Bombing Attacks.](#)
In *International Conference on Passive and Active Network Measurement*, pages 269–283. Springer, 2021

Background:

How Do Attackers Find Reflectors on the Internet?

How Do Attackers Find Reflectors on the Internet?

IPv4 vs. IPv6



MAX PLANCK INSTITUTE
FOR INFORMATICS

In **IPv4**: 91.5.142.144

- 3.7B usable Addresses
- Attackers can scan **all of them**.

How Do Attackers Find Reflectors on the Internet?

IPv4 vs. IPv6



MAX PLANCK INSTITUTE
FOR INFORMATICS

In IPv4: 91.5.142.144

- 3.7B usable Addresses
- Attackers can scan **all of them**.
- ⇒ ... **your honeypot is easily found**.

How Do Attackers Find Reflectors on the Internet?

IPv4 vs. IPv6

In **IPv4**: 91.5.142.144

- 3.7B usable Addresses
- Attackers can **scan all of them**.
- ⇒ ... **your honeypot is easily found**.

In **IPv6**: 2003:f5:bf0b:1000:20ba:f50a:fa90:bb6c

- **huge** address space.
- scanning **all** address is **no longer feasible**

How Do Attackers Find Reflectors on the Internet?



IPv4 vs. IPv6

In **IPv4**: 91.5.142.144

- 3.7B usable Addresses
- Attackers can **scan all of them**.
- ⇒ ... **your honeypot is easily found**.

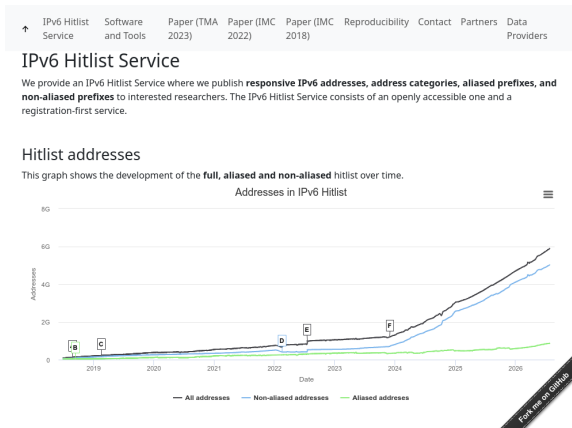
In **IPv6**: 2003:f5:bf0b:1000:20ba:f50a:fa90:bb6c

- **huge** address space.
- scanning **all** address is **no longer feasible**
- ⇒ ... **how can attackers find us?**

How Do Attackers Find Reflectors on the Internet?

The IPv6 Hitlist Service

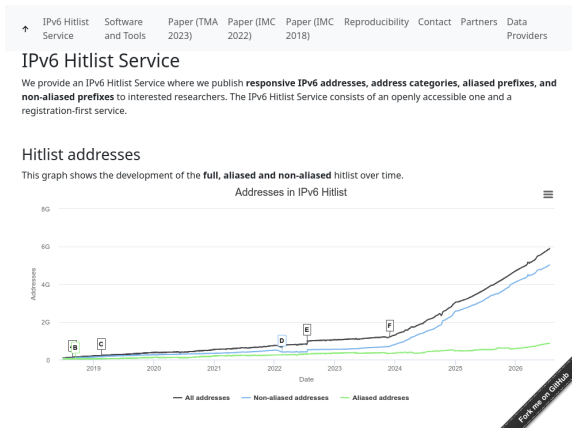
- The **IPv6 Hitlist** is a service that collects **active IPv6 addresses** for people looking for IPv6 scan targets.



How Do Attackers Find Reflectors on the Internet?

The IPv6 Hitlist Service

- The **IPv6 Hitlist** is a service that collects **active IPv6 addresses** for people looking for IPv6 scan targets.
- Previous work² has shown that **having an address on the Hitlist attracts plenty of scan traffic**.



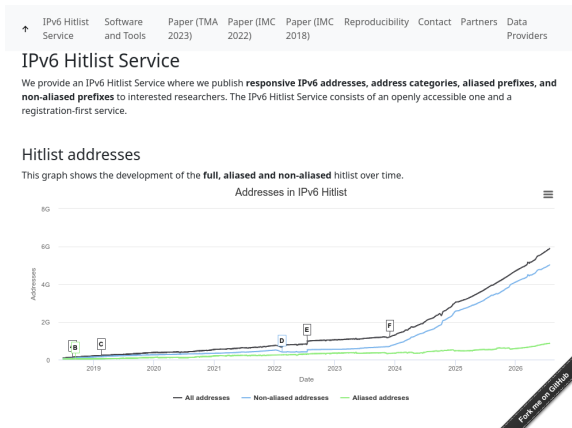
²

H. B. Tanveer, E. Chan, R. K. P. Mok, S. Kappes, P. Richter, O. Gasser, J. Ronan, A. Berger, and k. Claffy. *Unveiling IPv6 Scanning Dynamics: A Longitudinal Study Using Large Scale Proactive and Passive IPv6 Telescopes*. *Proc. ACM Netw.*, 3(CoNEXT3), Sept. 2025

How Do Attackers Find Reflectors on the Internet?

The IPv6 Hitlist Service

- The **IPv6 Hitlist** is a service that collects **active IPv6 addresses** for people looking for IPv6 scan targets.
 - Previous work² has shown that **having an address on the Hitlist attracts plenty of scan traffic**.
- ⇒ **Idea: Let's expose a honeypot address on the Hitlist.**



²

H. B. Tanveer, E. Chan, R. K. P. Mok, S. Kappes, P. Richter, O. Gasser, J. Ronan, A. Berger, and k. Claffy. *Unveiling IPv6 Scanning Dynamics: A Longitudinal Study Using Large Scale Proactive and Passive IPv6 Telescopes*. *Proc. ACM Netw.*, 3(CoNEXT3), Sept. 2025

1. We extended the **MP-H Honeypot**¹ to support IPv6.



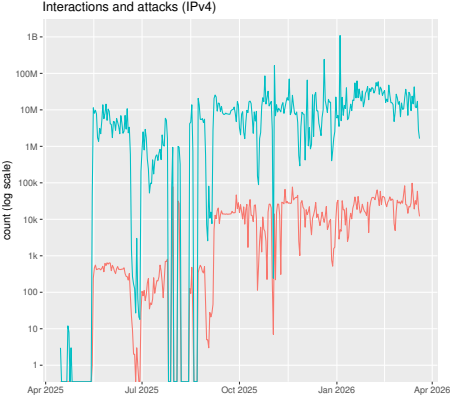
¹T. Heinrich, R. R. Obelheiro, and C. A. Maziero. [New Kids on the DRDoS Block: Characterizing Multiprotocol and Carpet Bombing Attacks.](#)
In *International Conference on Passive and Active Network Measurement*, pages 269–283. Springer, 2021

1. We extended the **MP-H Honeypot**¹ to support **IPv6**.
2. **We set up two dual-stack honeypots in different locations and expose their addresses on the IPv6 Hitlist.**

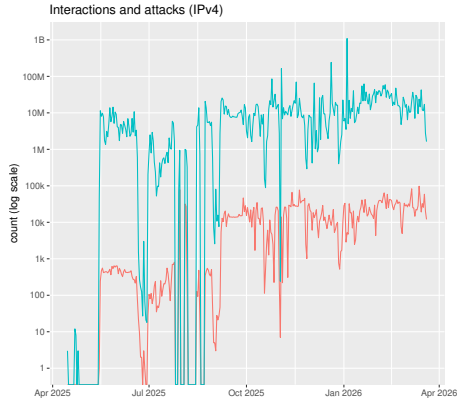


¹ T. Heinrich, R. R. Obelheiro, and C. A. Maziero. [New Kids on the DRDoS Block: Characterizing Multiprotocol and Carpet Bombing Attacks](#). In *International Conference on Passive and Active Network Measurement*, pages 269–283. Springer, 2021

Findings

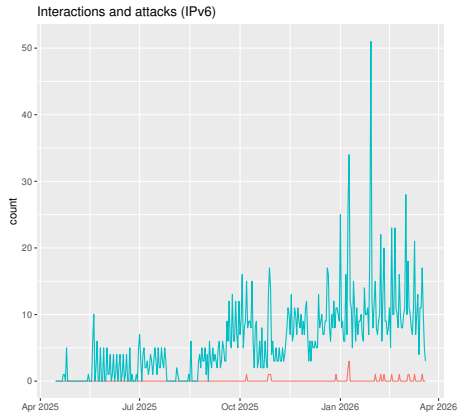
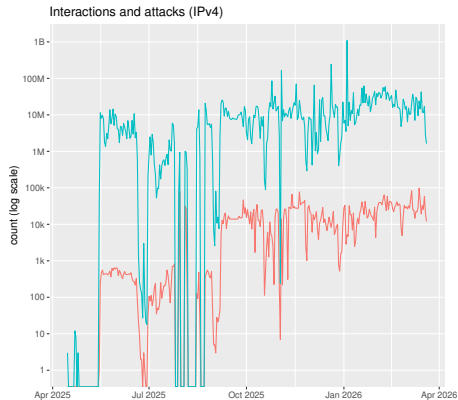


type
— attacks
— interactions



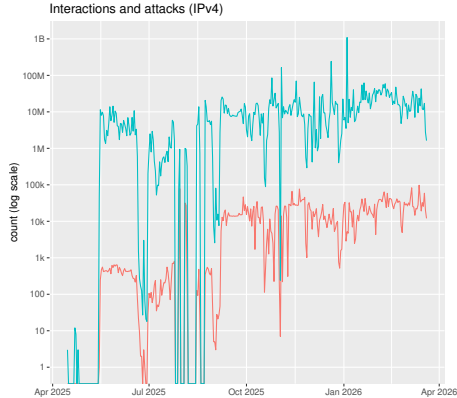
→ Frequent attacks in IPv4

type
— attacks
— interactions

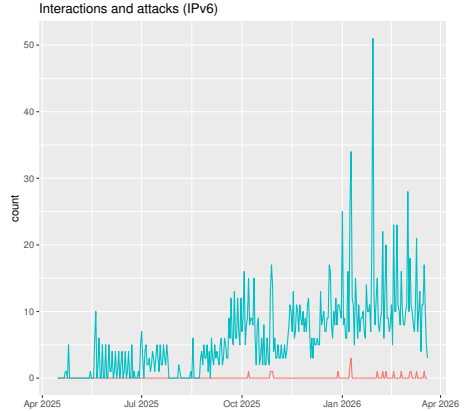


→ Frequent attacks in IPv4

type
— attacks
— interactions



→ Frequent attacks in IPv4



⇒ We see **no genuine attacks in IPv6**



But Why?

Possible Explanations



1. DDoS attackers **don't use the IPv6 Hitlist.**

1. DDoS attackers **don't use the IPv6 Hitlist.**
 - the Hitlist does attract scan traffic.

1. DDoS attackers **don't use the IPv6 Hitlist**.

- the Hitlist does attract scan traffic.
- do other exposure methods attract **genuine attacks**?

1. DDoS attackers **don't use the IPv6 Hitlist**.
 - the Hitlist does attract scan traffic.
→ do other exposure methods attract **genuine attacks**?
2. DDoS attackers **target other protocols in IPv6**.

1. DDoS attackers **don't use the IPv6 Hitlist**.
 - the Hitlist does attract scan traffic.
→ do other exposure methods attract **genuine attacks**?
2. DDoS attackers **target other protocols in IPv6**.
→ ...but which? (*we already support seven*)

1. DDoS attackers **don't use the IPv6 Hitlist**.
 - the Hitlist does attract scan traffic.
 - do other exposure methods attract **genuine attacks**?
2. DDoS attackers **target other protocols in IPv6**.
 - ...but which? (*we already support seven*)
3. Reflected DDoS attacks are **genuinely absent in IPv6** (or very rare).

1. DDoS attackers **don't use the IPv6 Hitlist**.
 - the Hitlist does attract scan traffic.
 - do other exposure methods attract **genuine attacks**?
2. DDoS attackers **target other protocols in IPv6**.
 - ...but which? (*we already support seven*)
3. Reflected DDoS attacks are **genuinely absent in IPv6** (or very rare).
 - more work is needed...

1. DDoS attackers **don't use the IPv6 Hitlist**.
 - the Hitlist does attract scan traffic.
 - do other exposure methods attract **genuine attacks**?
2. DDoS attackers **target other protocols in IPv6**.
 - ...but which? (*we already support seven*)
3. Reflected DDoS attacks are **genuinely absent in IPv6** (or very rare).
 - more work is needed...
 - can we **observe** reflected DoS attacks in IPv6 elsewhere? (e.g., at hosts, IXPs, CDNs, ...)

- We extended the **MP-H reflection honeypot** to support **IPv6**

- We extended the **MP-H reflection honeypot** to support **IPv6**
 - ...and **attracted scanners** through the **IPv6 Hitlist**.

- We extended the **MP-H reflection honeypot** to support **IPv6**
 - ...and **attracted scanners** through the **IPv6 Hitlist**.
- ... **we did not find reflected DDoS attacks in IPv6**, but. . .

- We extended the **MP-H reflection honeypot** to support **IPv6**
 - ...and **attracted scanners** through the **IPv6 Hitlist**.
 - ...we **did not find** reflected **DDoS attacks in IPv6**, but...
- ⇒ What **other methods and vantage points** could we use to study **DDoS attacks in IPv6**?