Dresden University of Technology

HAW HAMBURG

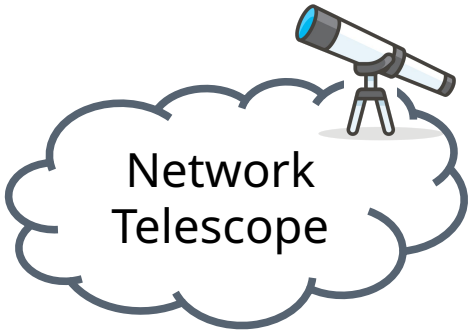
Isabell Egloff, Raphael Hiesgen, **Maynard Koch**, Thomas C. Schmidt, Matthias Wählisch

A Detailed Measurement View on IPv6 Scanners and Their Adaption to BGP Signals

ACM CoNEXT, Hong Kong // December 1-4, 2025

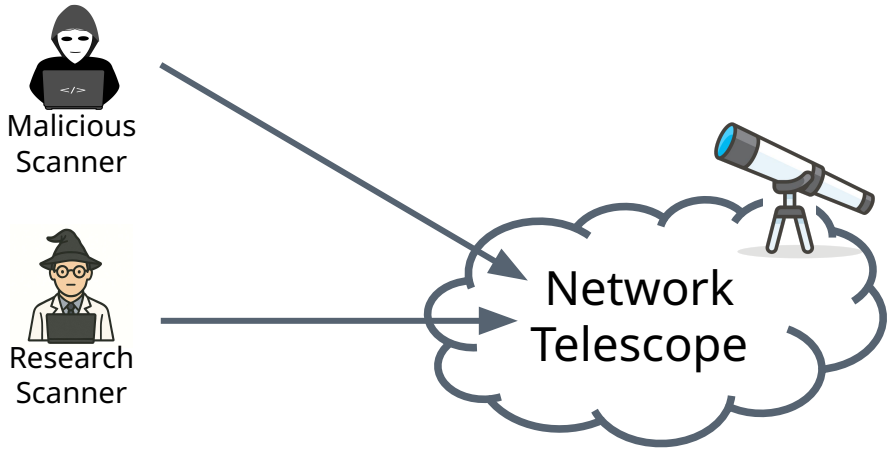
Understanding scanner behavior through passive observation

NTs are unused address space to capture unsolicited traffic



Understanding scanner behavior through passive observation

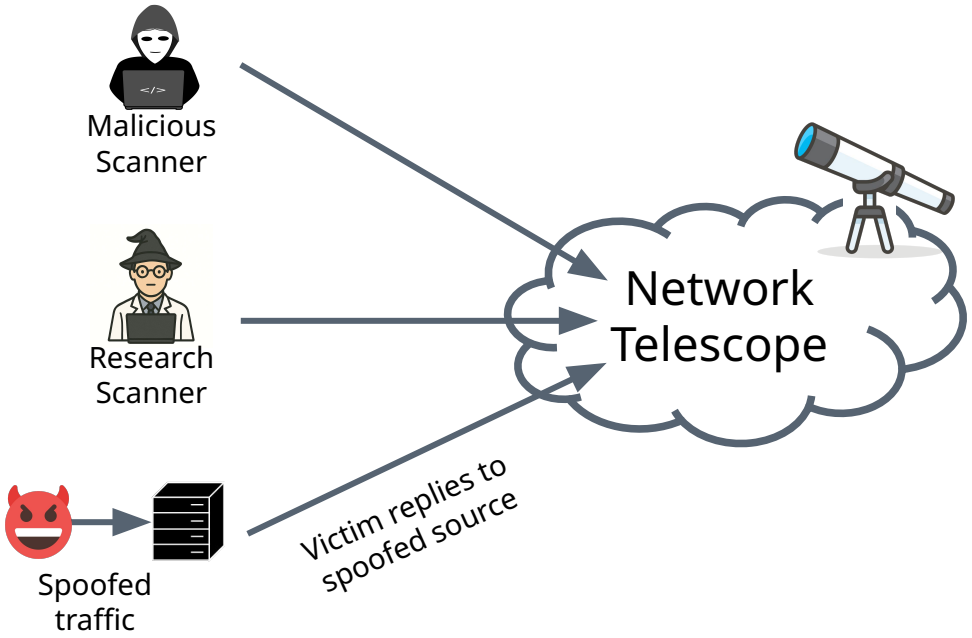
NTs are unused address space to capture unsolicited traffic



Stateless scans allow exploring the IPv4 address space in <1h.

Understanding scanner behavior through passive observation

NTs are unused address space to capture unsolicited traffic

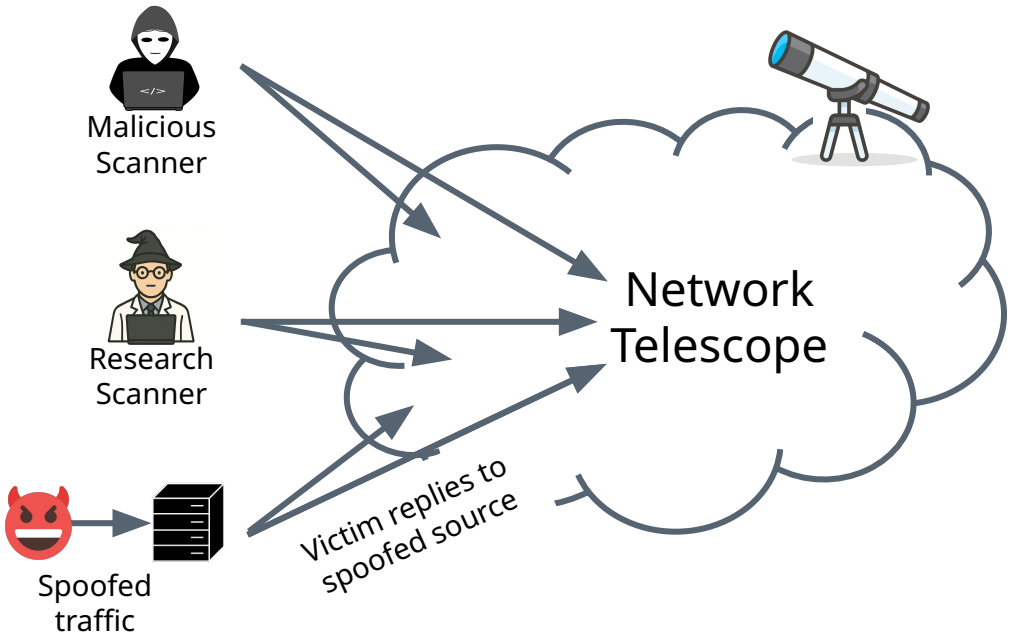


Stateless scans allow exploring the IPv4 address space in <1h.

Packets from hosts under attack reply to spoofed source IP addresses that belong to the telescope (backscatter).

Understanding scanner behavior through passive observation

NTs are unused address space to capture unsolicited traffic



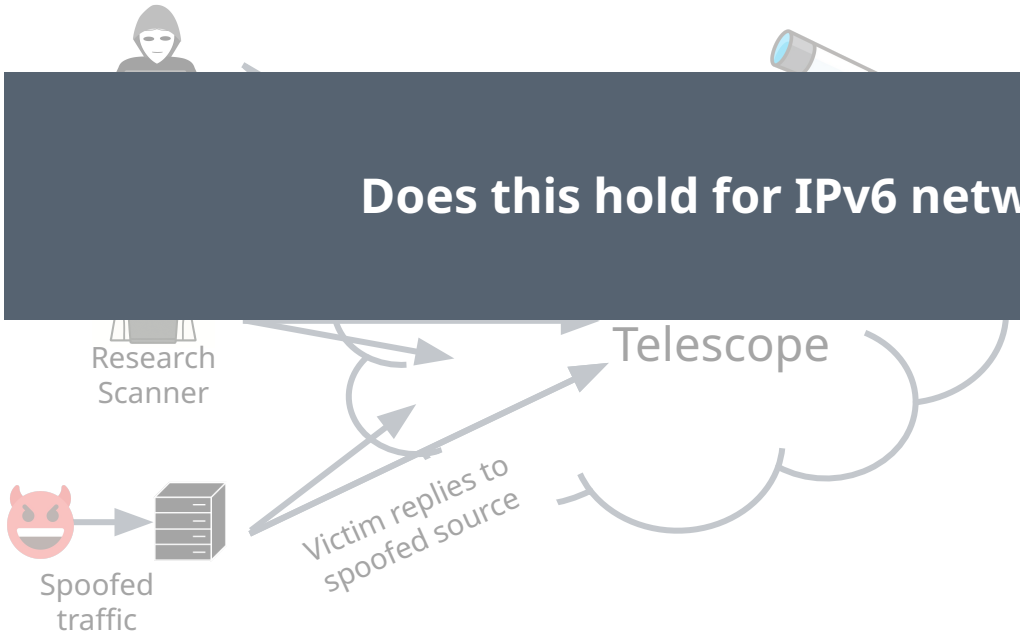
Stateless scans allow exploring the IPv4 address space in <1h.

Packets from hosts under attack reply to spoofed source IP addresses that belong to the telescope (backscatter).

The larger the telescope, the more scan traffic and backscatter can be observed.

Understanding scanner behavior through passive observation

NTs are unused address space to capture unsolicited traffic



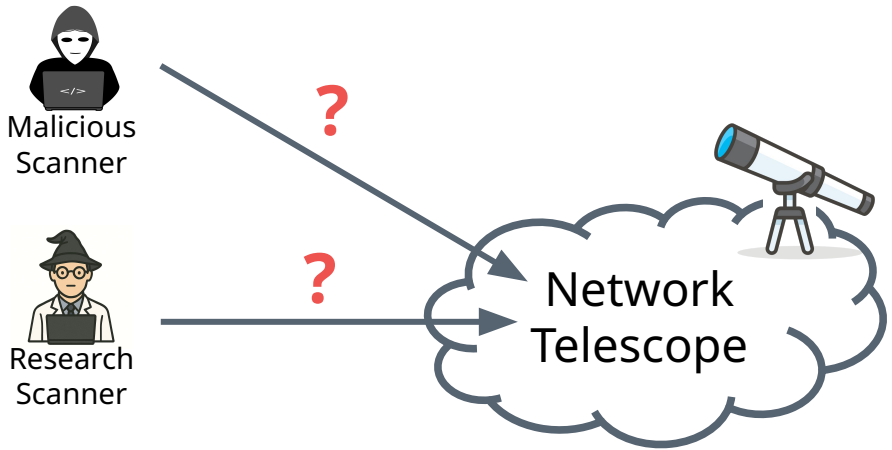
Does this hold for IPv6 network telescopes?

Stateless scans allow exploring the

(backscatter).

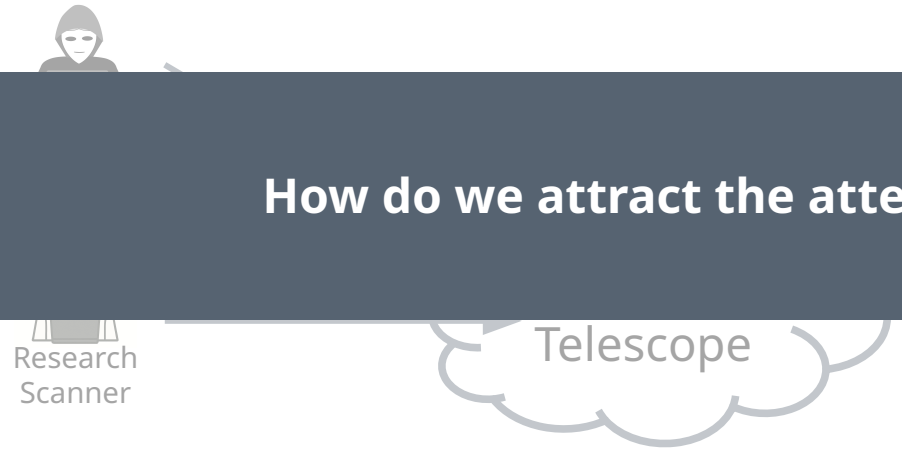
The larger the telescope, the more scan traffic and backscatter can be observed.

What do IPv6 network telescopes will observe?



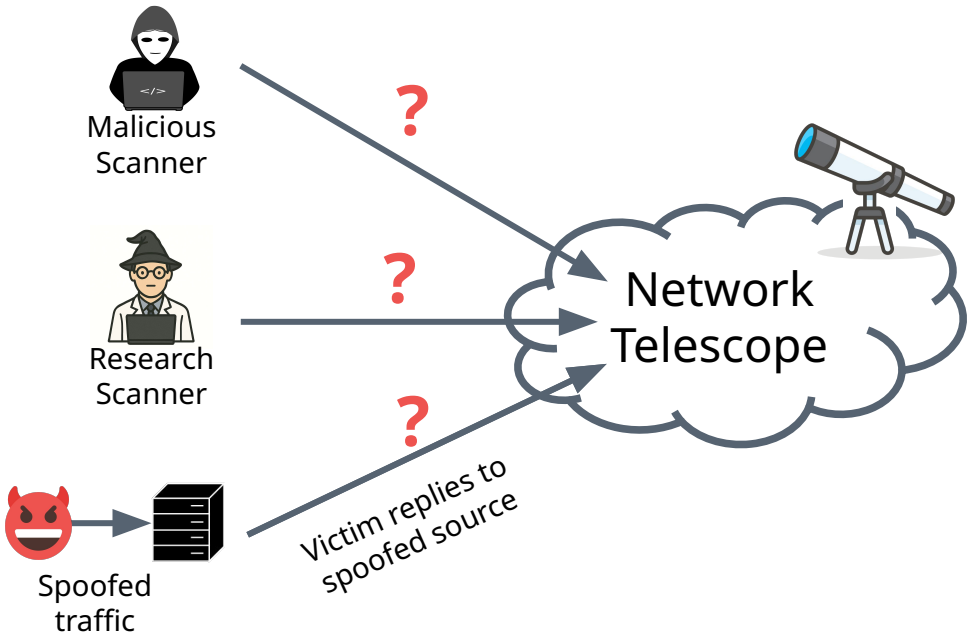
A full scan of the IPv6 address space is **infeasible**; scanners need efficient strategies for exploration.

What do IPv6 network telescopes will observe?



How do we attract the attention of scanners?

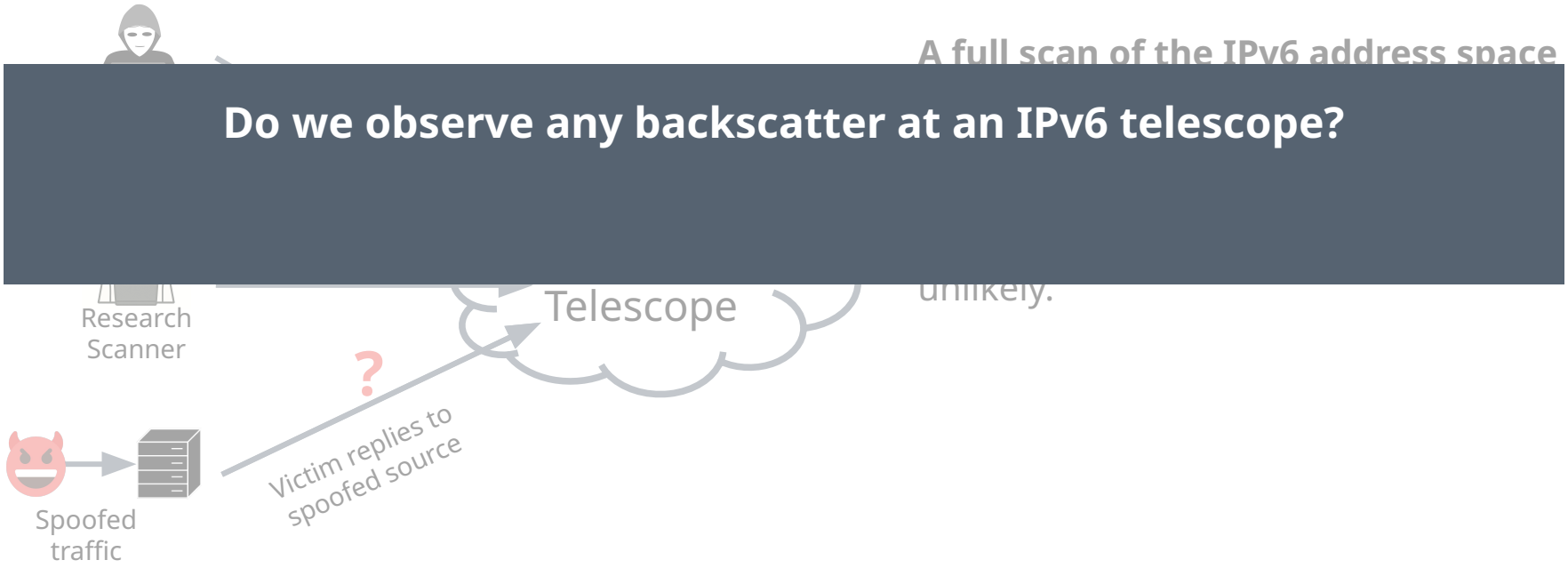
What do IPv6 network telescopes will observe?



A full scan of the IPv6 address space is **infeasible**; scanners need efficient strategies for exploration.

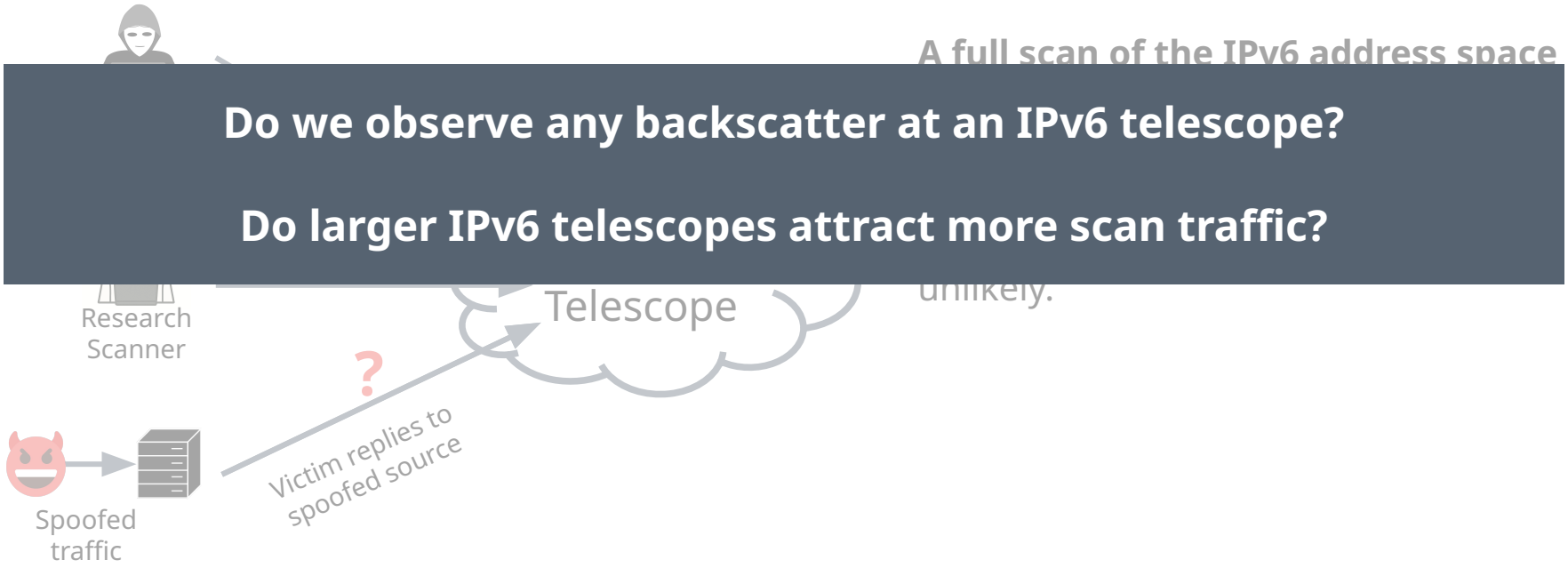
A randomly spoofed source IP address belonging to the telescope is unlikely.

What do IPv6 network telescopes will observe?



Do we observe any backscatter at an IPv6 telescope?

What do IPv6 network telescopes will observe?

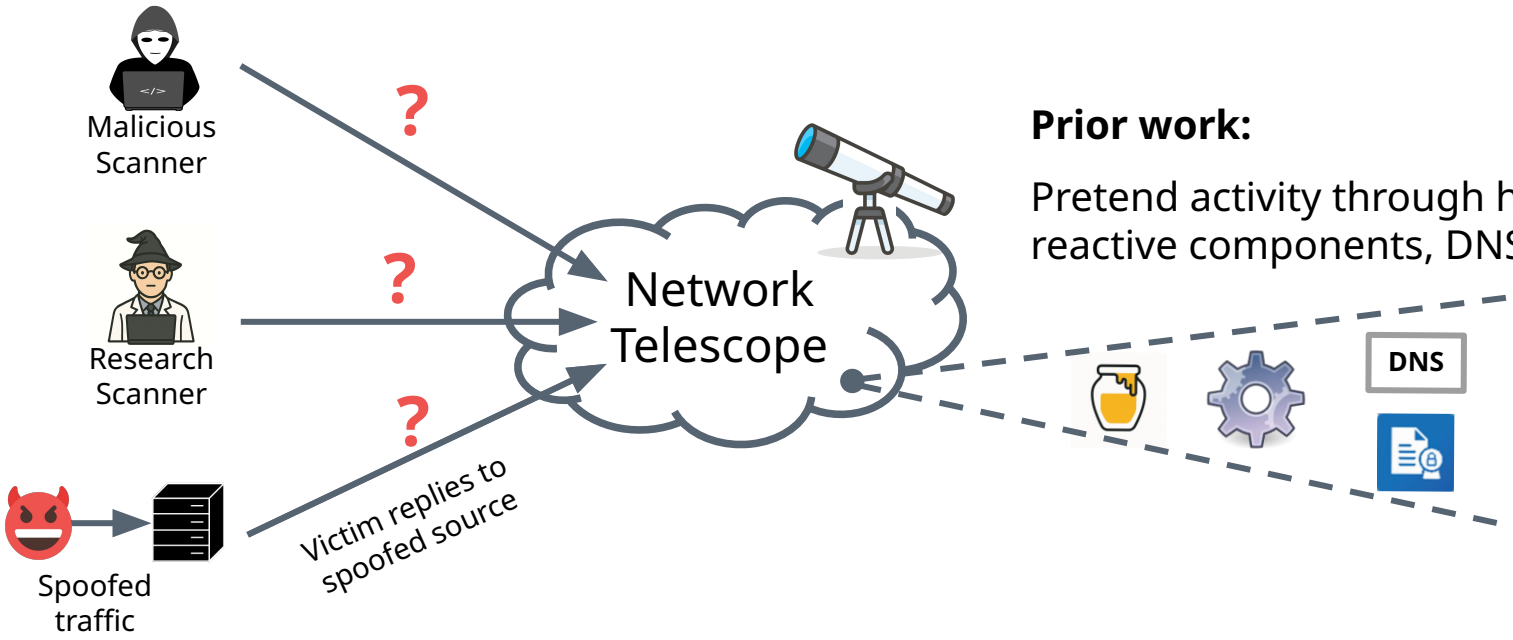


Do we observe any backscatter at an IPv6 telescope?

Do larger IPv6 telescopes attract more scan traffic?

Operating an IPv6 network telescopes is challenging

We need to deploy attractors to raise interest of scanners.

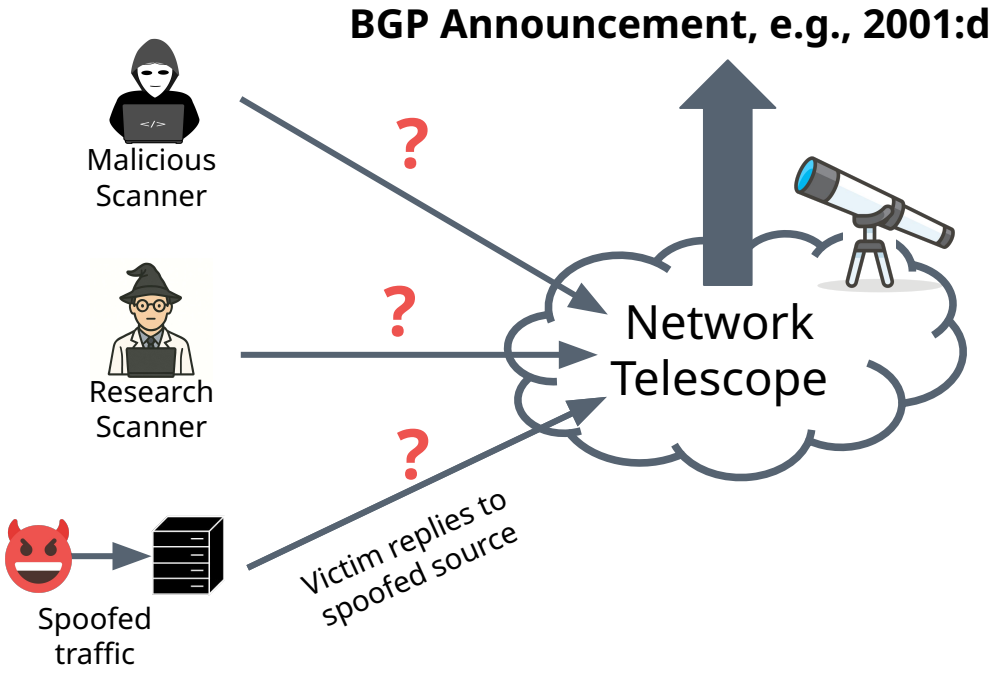


Prior work:

Pretend activity through honeypots, reactive components, DNS, or CT logs

Operating an IPv6 network telescopes is challenging

We need to deploy attractors to raise interest of scanners.



Prior work:

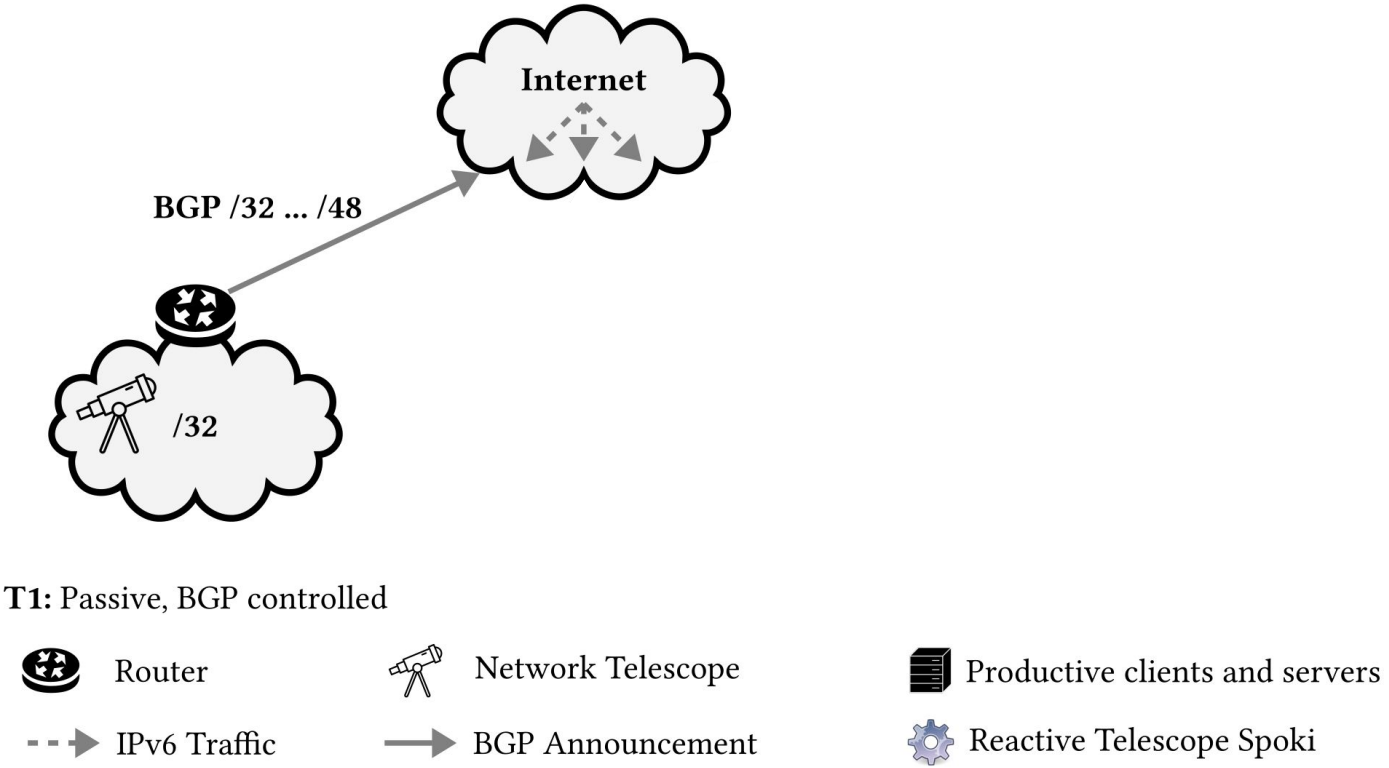
Pretend activity through honeypots, reactive components, DNS, or CT logs.

Our contribution, a new method to attract scanners:

Announce the telescope address space individually in BGP in a controlled experiment.

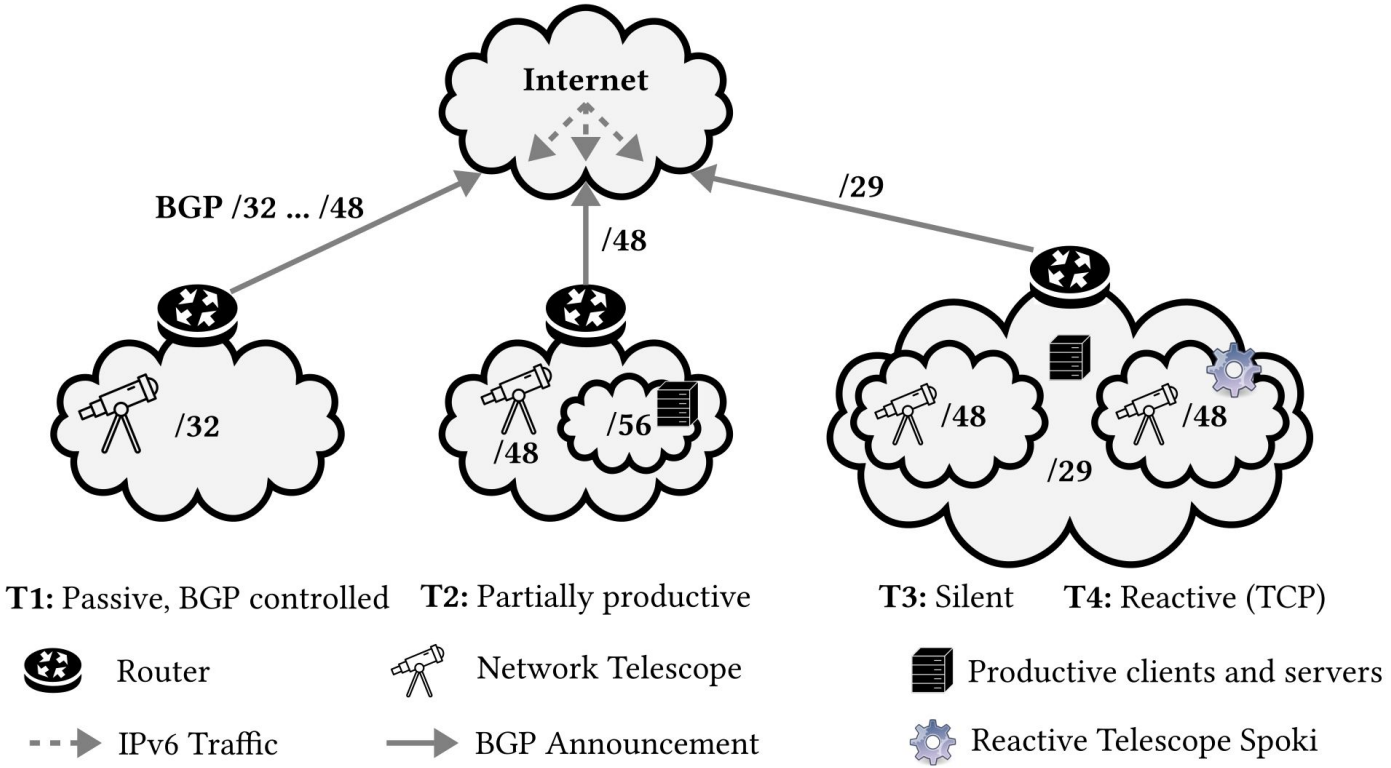
Measurement setup

We operate four IPv6 network telescopes under different conditions.



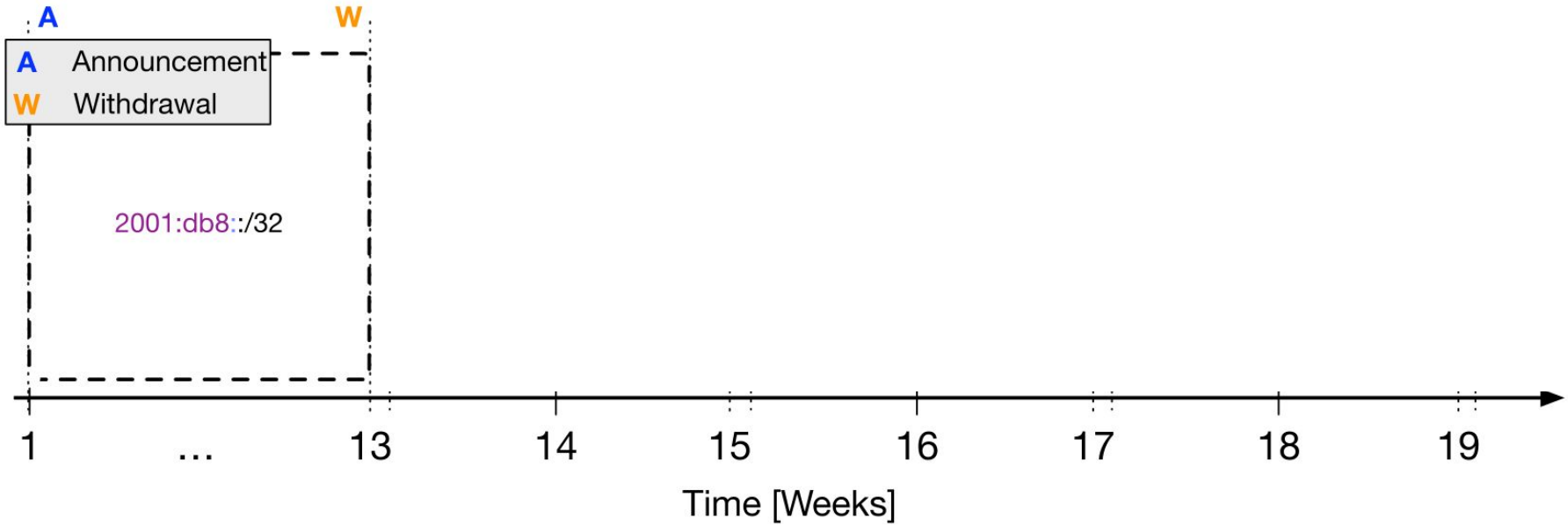
Measurement setup

We operate four IPv6 network telescopes under different conditions.



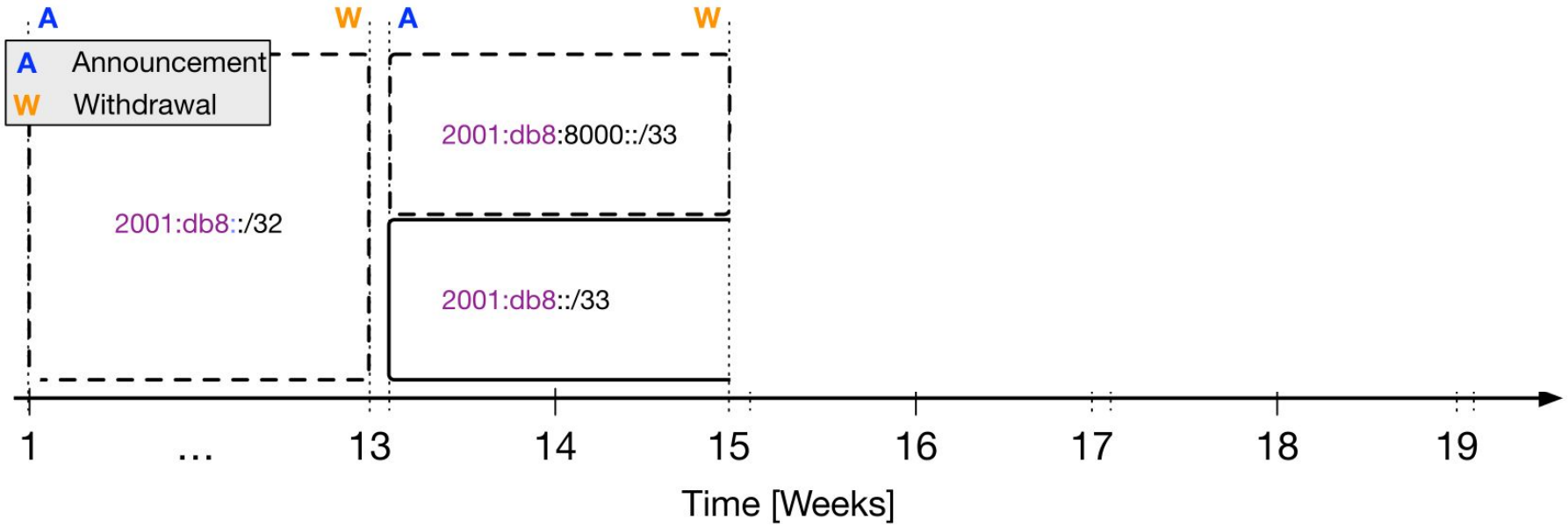
Initial observation period of 12 weeks

The address space of our telescope is visible as a single /32 announcement.



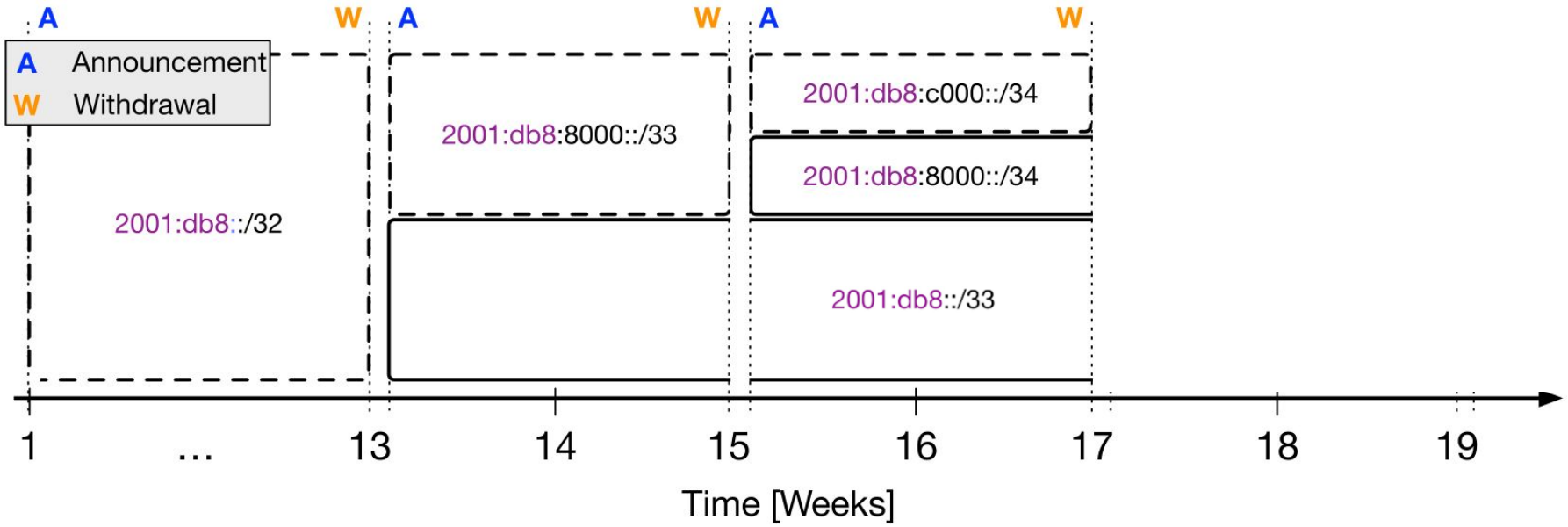
Splitting the telescope in BGP into more specific announcements

We withdraw the prefix for one day, then divide the prefix into two equally sized, more specific /33 announcements.

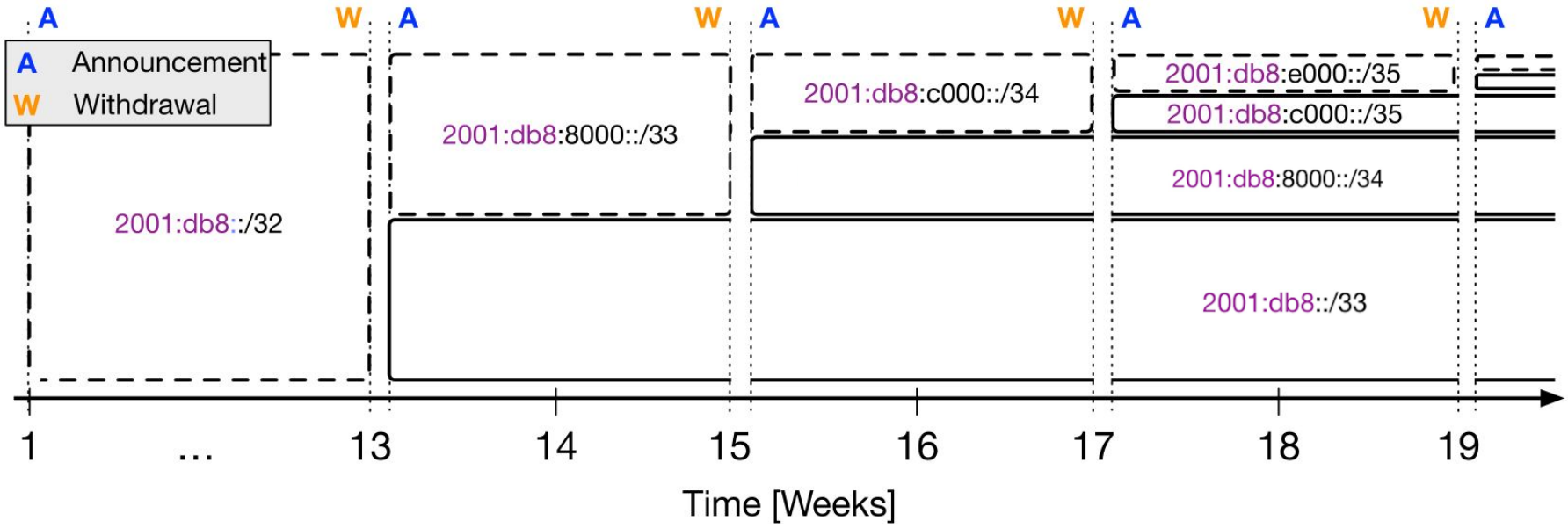


We repeat this process every two weeks

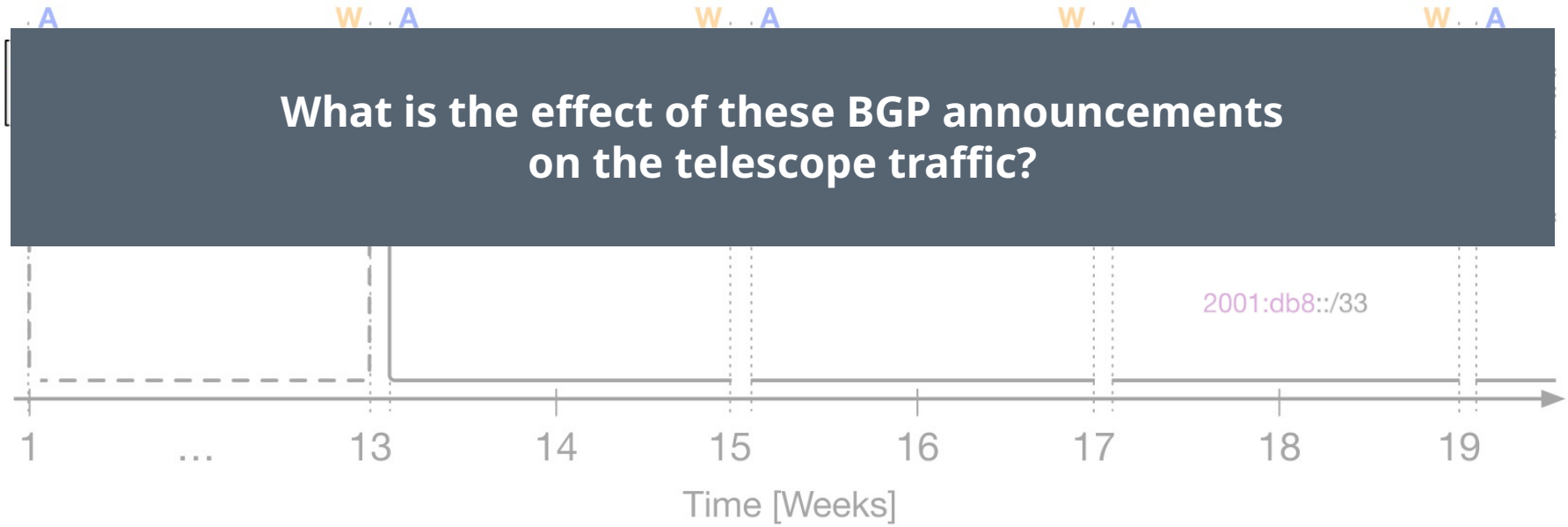
We split one of the two most specific prefixes into two more specific announcements.



We announce all (previously) created prefixes except the covering ones
We continue this process until we announce 17 prefixes, our most-specific prefix is /48.

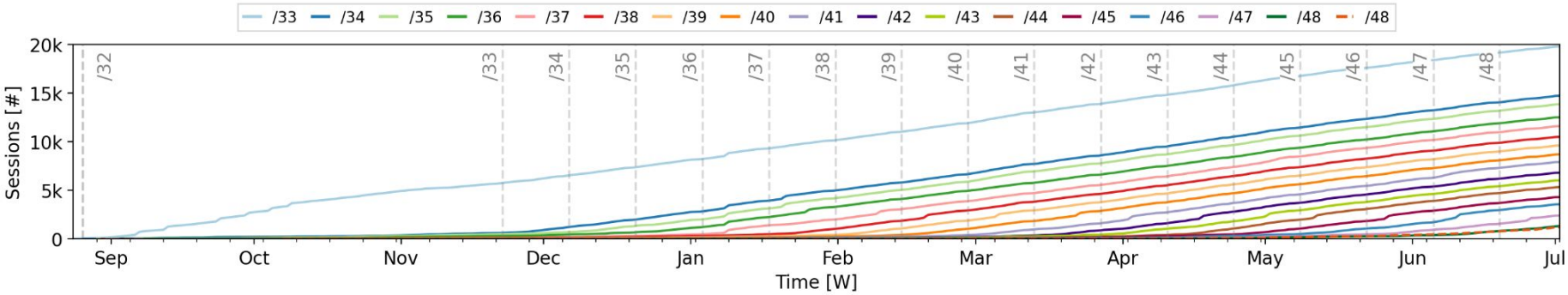


We announce all (previously) created prefixes except the covering ones
We continue this process until we announce 17 prefixes, our most-specific prefix is /48.



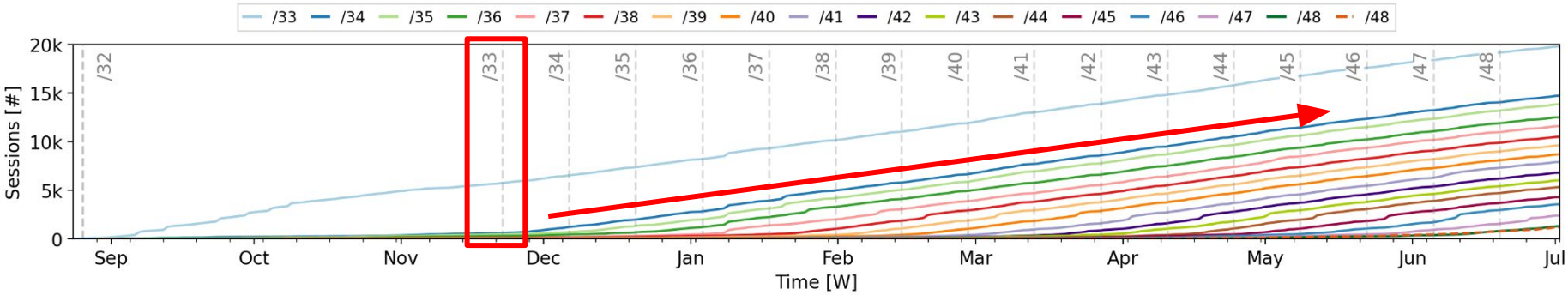
Clear trend towards BGP-aware scanning

New prefix announcements immediately attract the attention of scanners.



Clear trend towards BGP-aware scanning

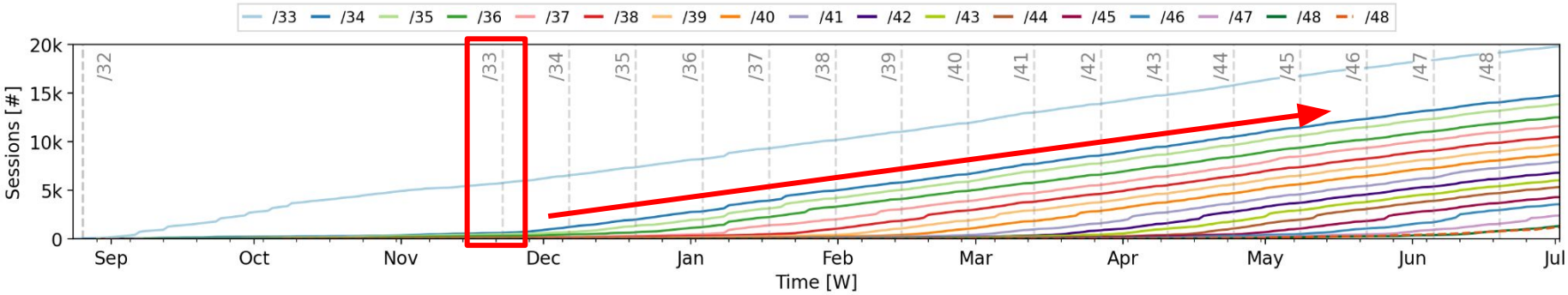
New prefix announcements immediately attract the attention of scanners.



Subnets of our telescope **receive a significant amount of traffic** only when they are **individually announced in BGP.**

Clear trend towards BGP-aware scanning

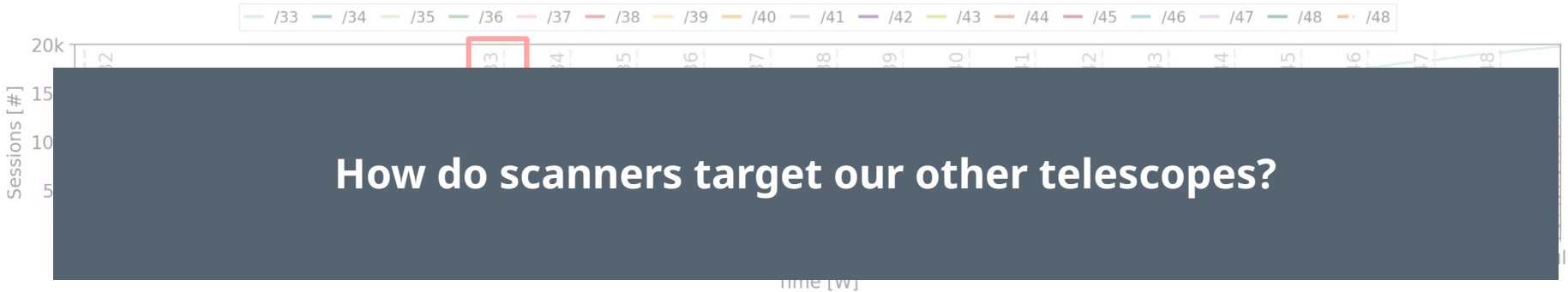
New prefix announcements immediately attract the attention of scanners.



Subnets of our telescope **receive a significant amount of traffic** only when they are **individually announced in BGP.**
90% of all scan sources probe the respective **low-byte address** (e.g., 2001:db8::1) of the announced (more specific) prefixes.

Clear trend towards BGP-aware scanning

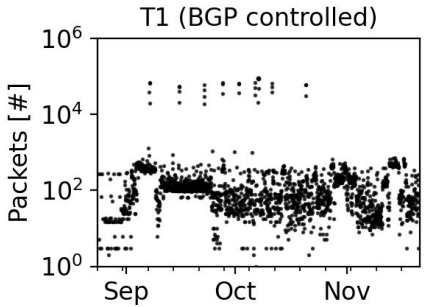
New prefix announcements immediately attract the attention of scanners.



Subnets of our telescope **receive a significant amount of traffic** only when they are **individually announced in BGP.**
90% of all scan sources probe the respective **low-byte address** (e.g., 2001:db8::1) of the announced (more specific) prefixes.

Telescope traffic during the initial 12 weeks

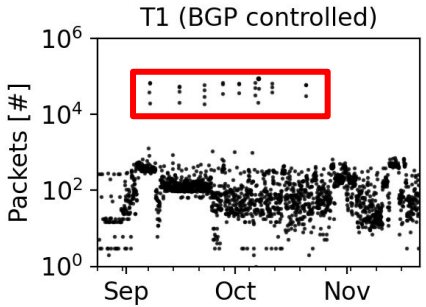
Individual BGP announcements attract significantly more attention.



We capture 2.2M packets at our BGP controlled telescope T1.

Telescope traffic during the initial 12 weeks

Individual BGP announcements attract significantly more attention.

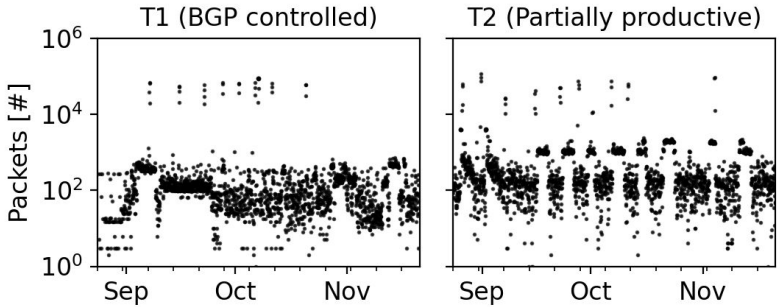


We capture 2.2M packets at our BGP controlled telescope T1.

Two scan campaigns contribute 87% of all packets at telescope T1.

Telescope traffic during the initial 12 weeks

Individual BGP announcements attract significantly more attention.



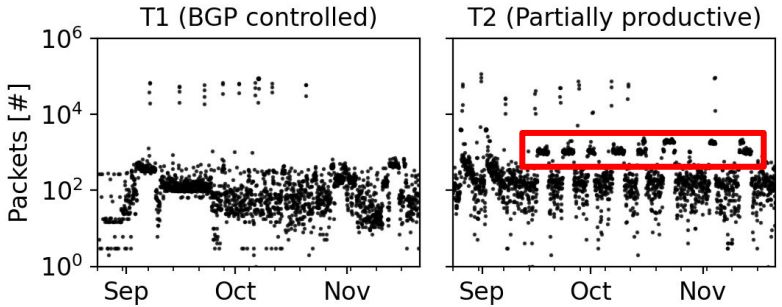
We capture 2.2M packets at our BGP controlled telescope T1.

Two scan campaigns contribute 87% of all packets at telescope T1.

We observe 2.5M packets at telescope T2

Telescope traffic during the initial 12 weeks

Individual BGP announcements attract significantly more attention.



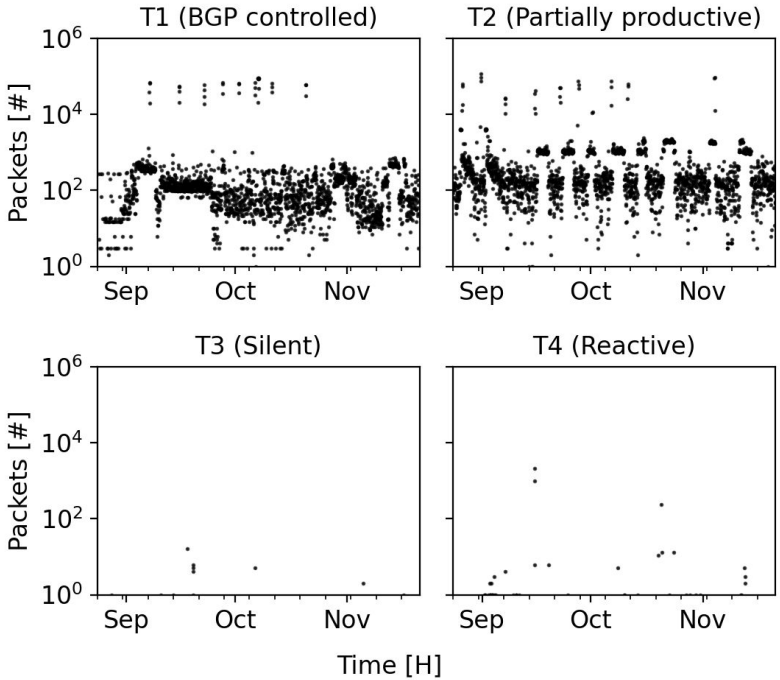
We capture 2.2M packets at our BGP controlled telescope T1.

Two scan campaigns contribute 87% of all packets at telescope T1.

We observe 2.5M packets at telescope T2, with a traffic pattern caused by a single telescope address that is present in DNS.

Telescope traffic during the initial 12 weeks

Individual BGP announcements attract significantly more attention.



We capture 2.2M packets at our BGP controlled telescope T1.

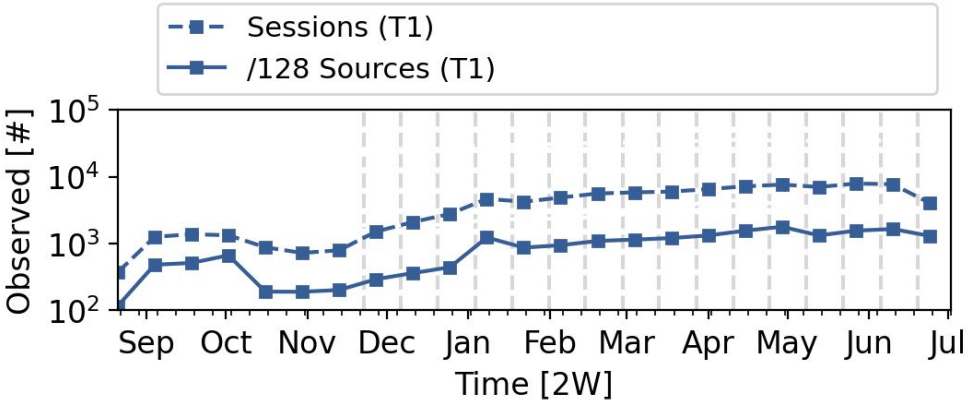
Two scan campaigns contribute 87% of all packets at telescope T1.

We observe 2.5M packets at telescope T2, with a traffic pattern caused by a single telescope address that is present in DNS.

Telescopes T1 and T2 receive 4-6 orders of magnitude more traffic than the telescopes T3 and T4.

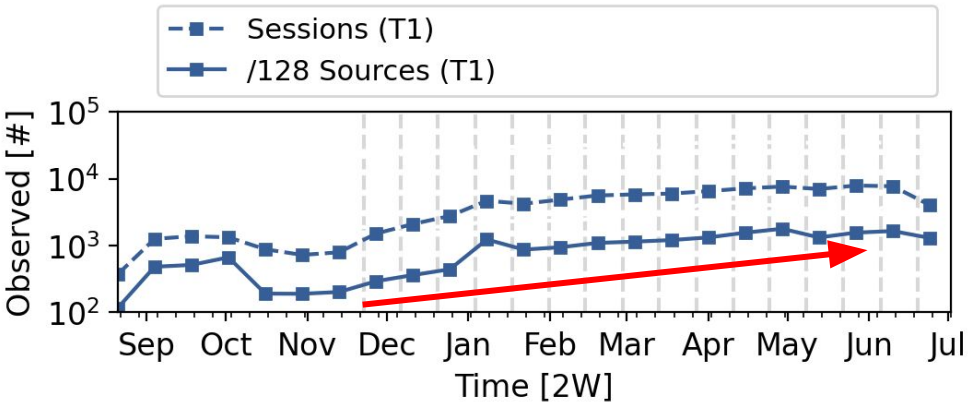
Number of bi-weekly sessions and sources during experiment time

Announcing more prefixes increases attention of scanners.



Number of bi-weekly sessions and sources during experiment time

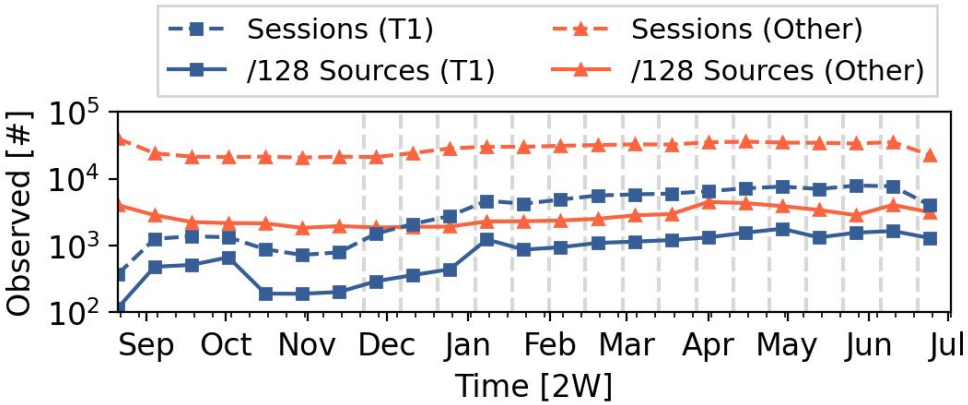
Announcing more prefixes increases attention of scanners.



The more prefixes we announce in BGP, the more sessions and individual sources can be observed at the **BGP-controlled telescope**.

Number of bi-weekly sessions and sources during experiment time

Announcing more prefixes increases attention of scanners.



The more prefixes we announce in BGP, the more sessions and individual sources can be observed at the **BGP-controlled telescope**.

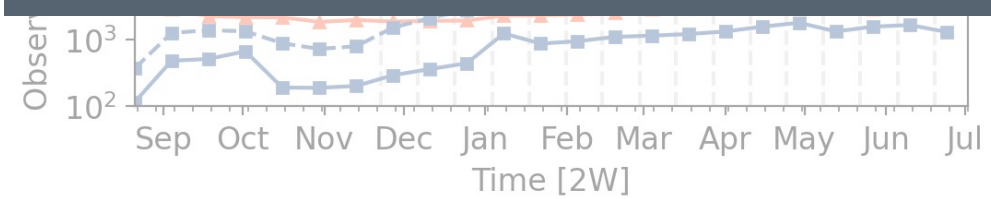
In contrast, the number of **sessions** and **sources** at the other telescopes **remains at the same level.**

Number of bi-weekly sessions and sources during experiment time

Announcing more prefixes increases attention of scanners.

Do we observe any backscatter?

From 51M packets, **six packets** show backscatter characteristics.



The more prefixes we announce in

and **sources** at the other telescopes **remains at the same level.**

IPv6 scanners explore the address space **BGP aware.**

IPv6 scanners explore the address space **BGP aware.**

The more prefixes an IPv6 network telescope announces, **the more attention** it receives.

IPv6 scanners explore the address space **BGP aware.**

The more prefixes an IPv6 network telescope announces, **the more attention** it receives.

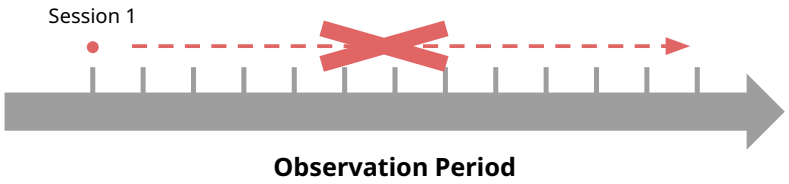
We developed a taxonomy to analyze the behavior of scanners.

A taxonomy to classify scanners

1. **Temporal behavior**
2. Target network selection
3. Target address selection

Temporal behavior of scanners

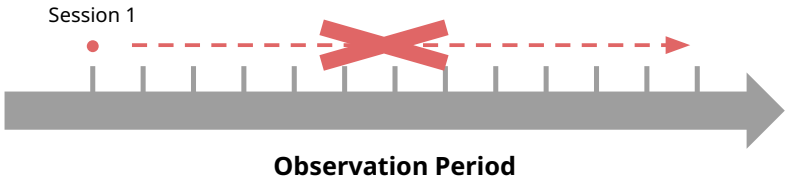
One-off:



One-off: Observed once, for a single session

Temporal behavior of scanners

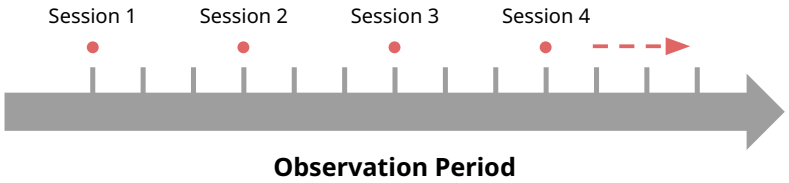
One-off:



One-off: Observed once, for a single session

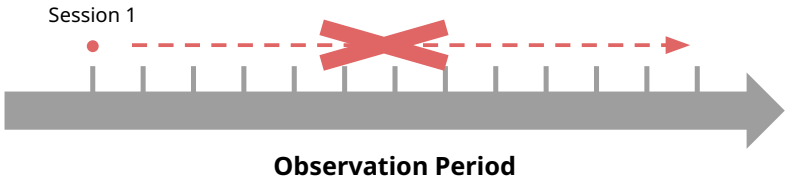
Periodic: Regular revisits, showing periodicity

Periodic:



Temporal behavior of scanners

One-off:

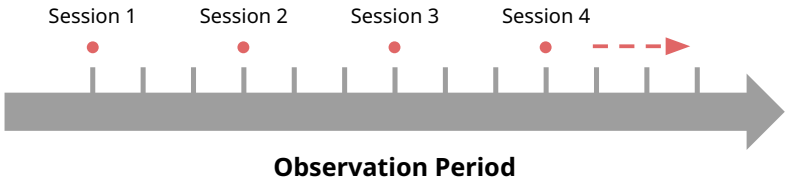


One-off: Observed once, for a single session

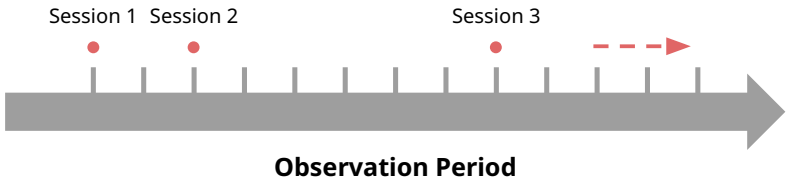
Periodic: Regular revisits, showing periodicity

Intermittent: Irregular revisits, no periodicity

Periodic:



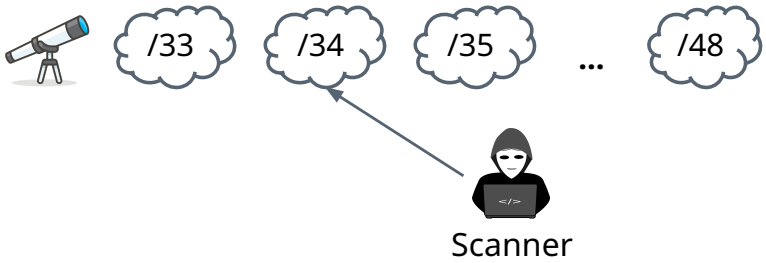
Intermittent:



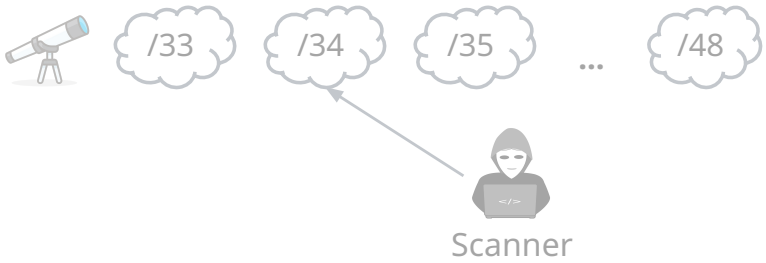
A taxonomy to classify scanners

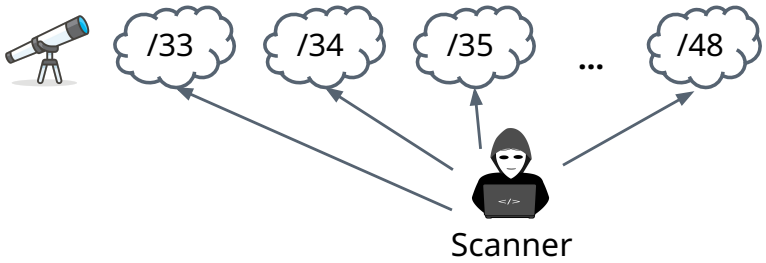
1. Temporal behavior
2. **Target network selection**
3. Target address selection

Single-prefix scanner targets addresses within a single prefix but ignores other announcements.

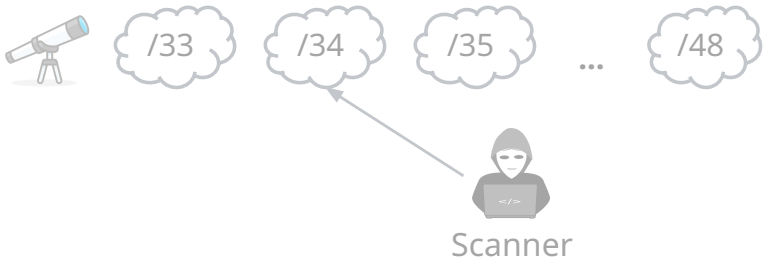


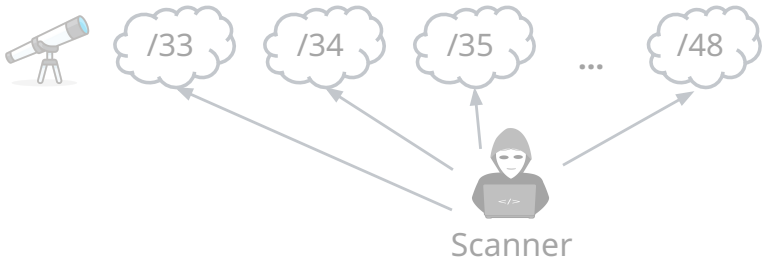
Network-size independent scanner probes evenly distributed across all announced prefixes.

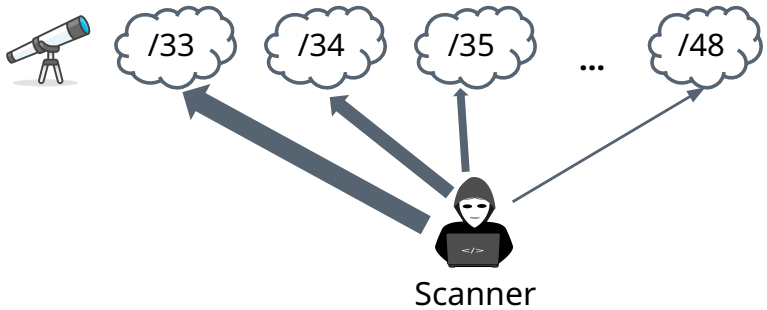




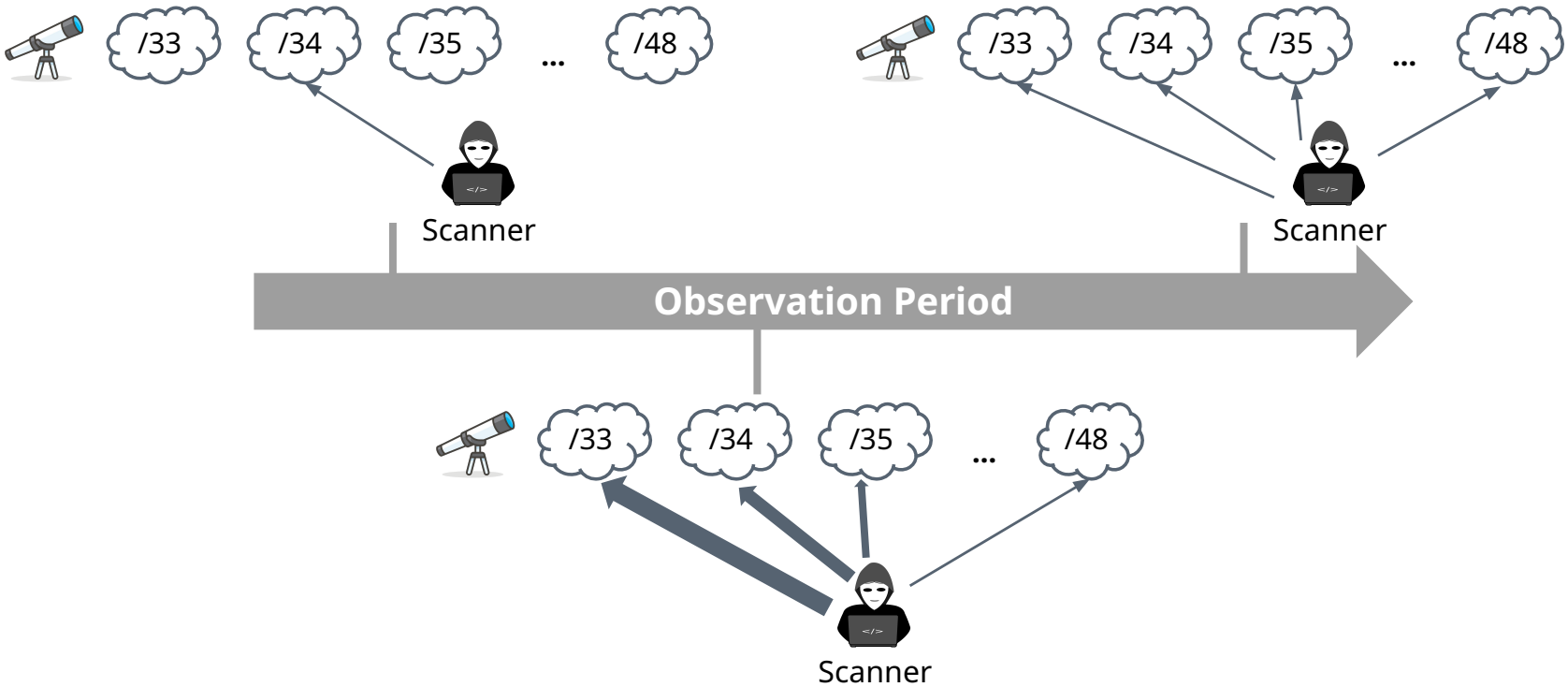
Network-size dependent scanner sends more probes to larger prefixes.







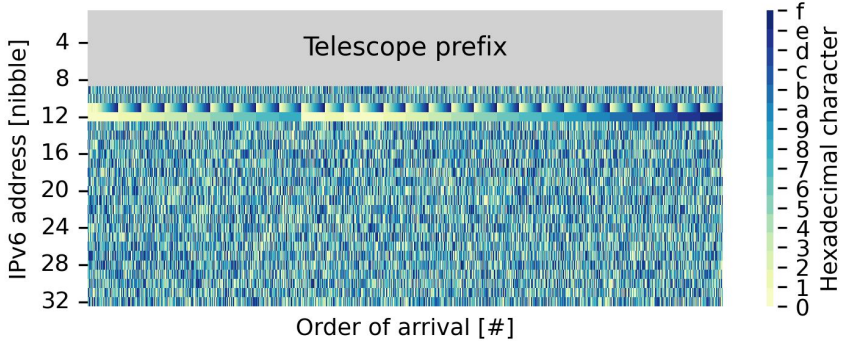
Inconsistent behavior scanners show different behavior at different points in time.

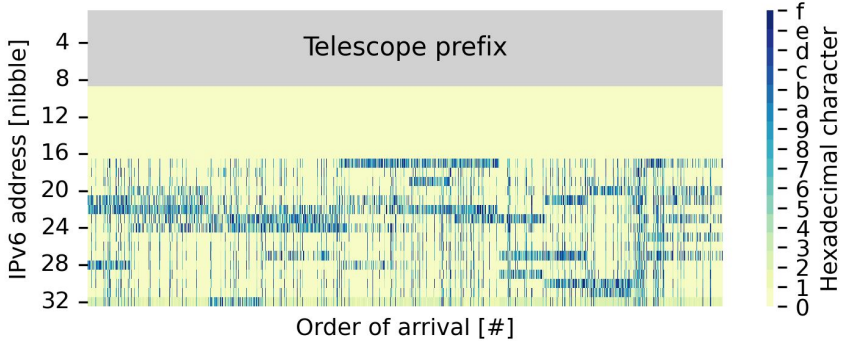


A taxonomy to classify scanners

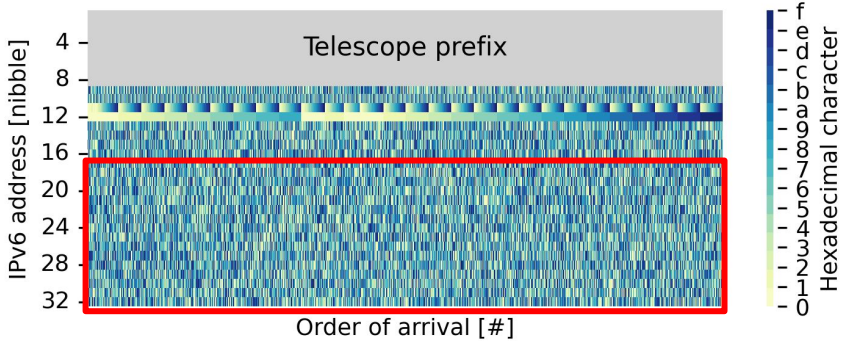
1. Temporal behavior
2. Target network selection
3. **Target address selection**

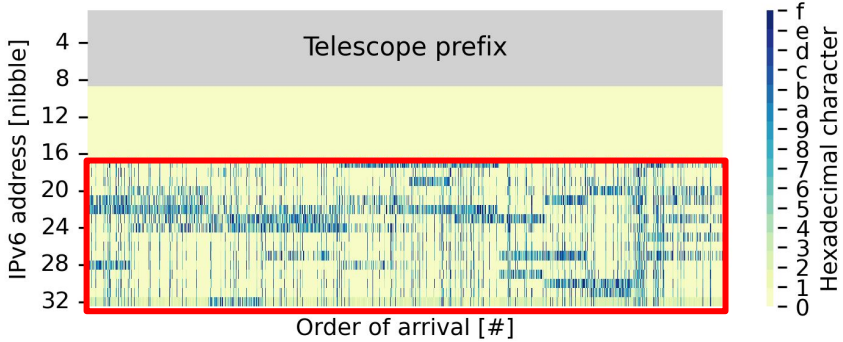
Target address selection
Random and structured scanning





Target address selection
Random and structured scanning

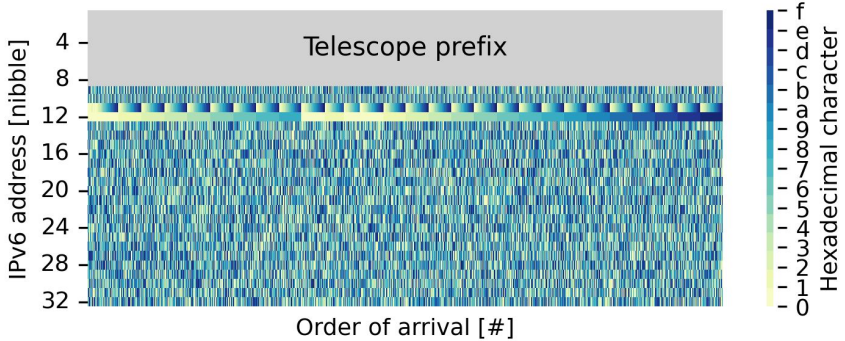




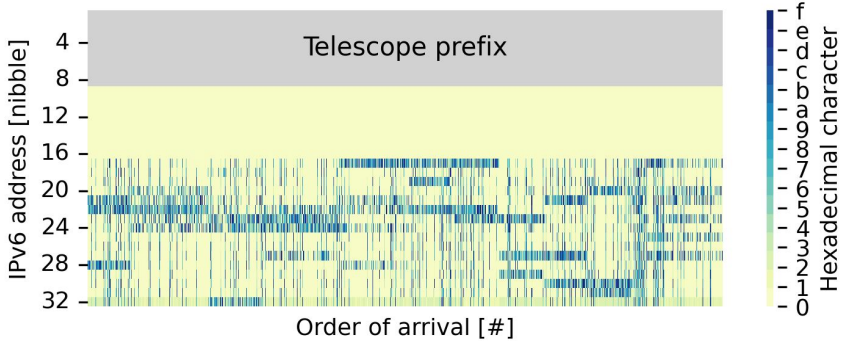
We use standardized tests for randomness by using, e.g., the 64 host bits **(nibble 17 to 32)** of every target address in a session to **assess if the target address selection follows a random or structured approach.**

Target address selection
Random and structured scanning

Example of random target selection:



Example of structured target selection:



We use standardized tests for randomness by using, e.g., the 64 host bits **(nibble 17 to 32)** of every target address in a session to **assess if the target address selection follows a random or structured approach.**

Target address selection
Random and structured scanning

Example of random target selection:

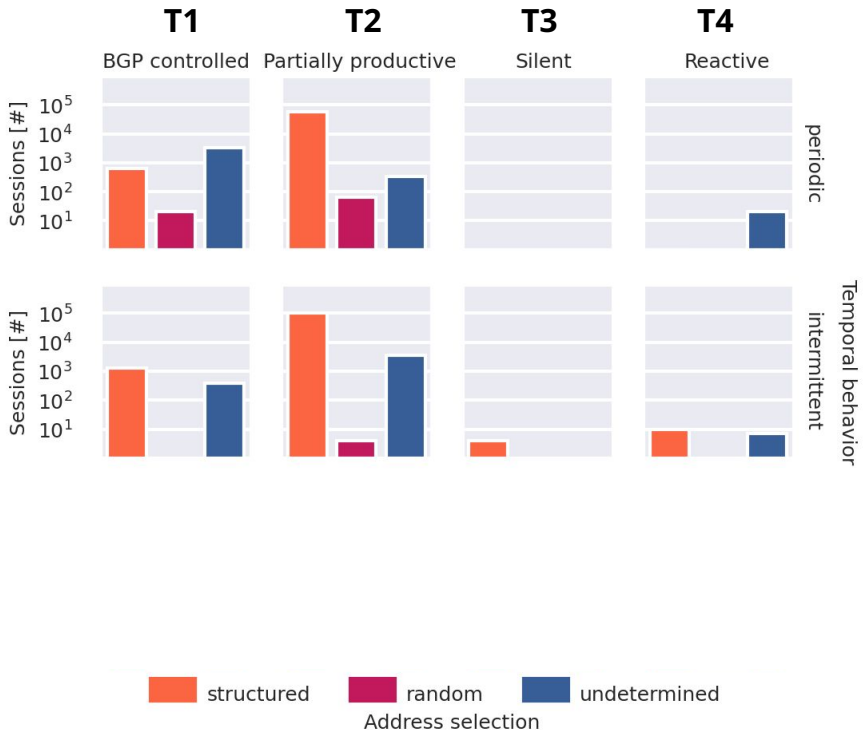
Example of structured target selection:

How do the different types of scanners behave?

We use standardized tests for randomness by using, e.g., the 64 host bits **(nibble 17 to 32)** of every target address in a session to **assess if the target address selection follows a random or structured approach.**

Behavior of scanners across all four telescopes

Initial observation period.



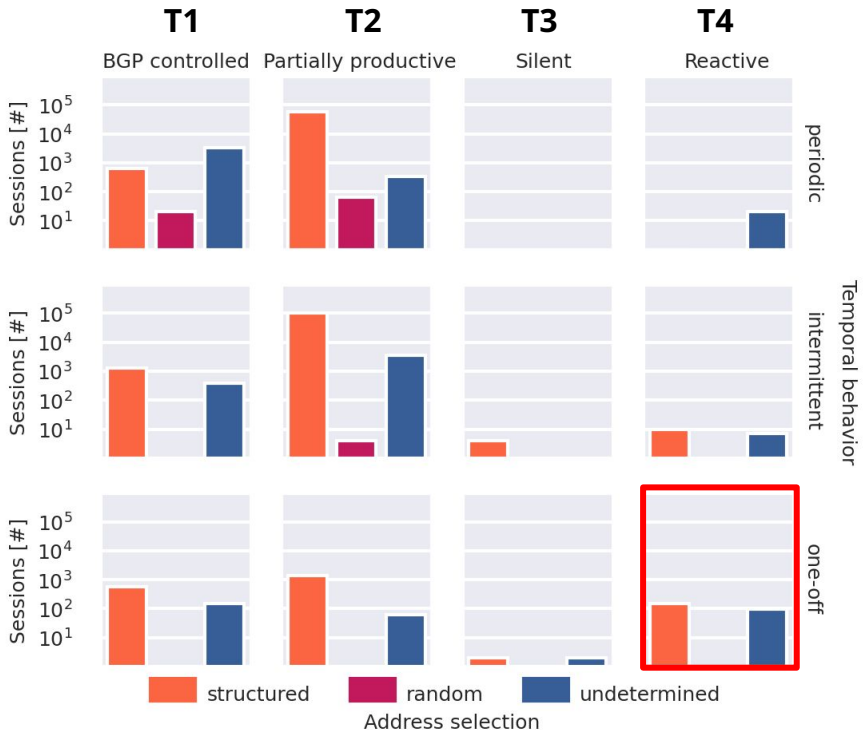
Behavior of scanners across all four telescopes

Initial observation period.

Most scanners return (intermittent: 41% or periodic: 29%) and follow a **structured scanning** strategy.

Behavior of scanners across all four telescopes

Initial observation period.

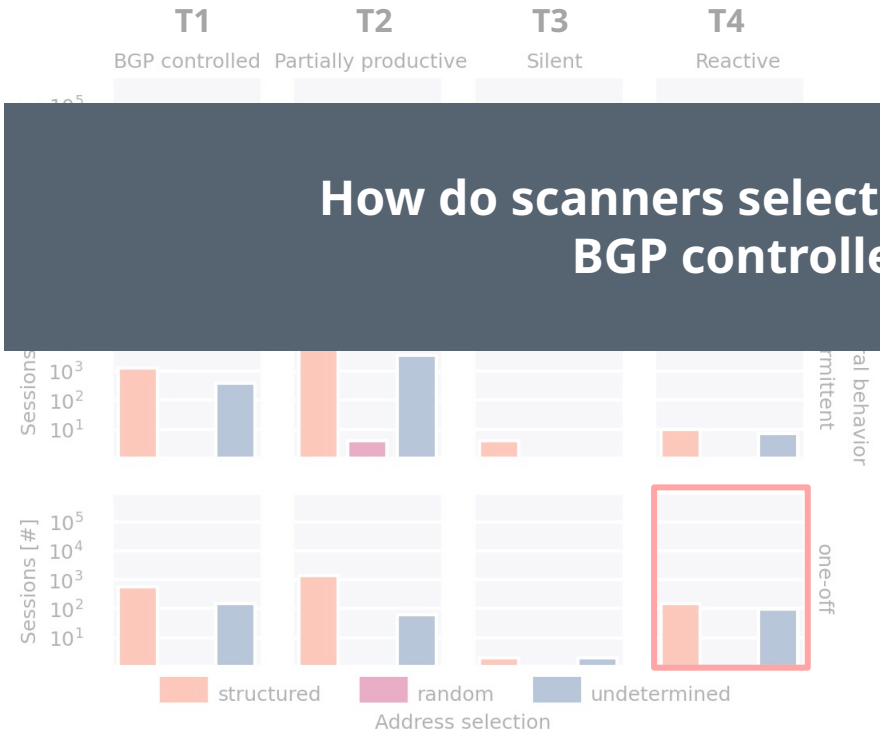


Most scanners return (intermittent: 41% or periodic: 29%) and follow a **structured scanning** strategy.

The relative share of one-off scanners is significantly higher for T4 compared to T1-T3.

Behavior of scanners across all four telescopes

Initial observation period.



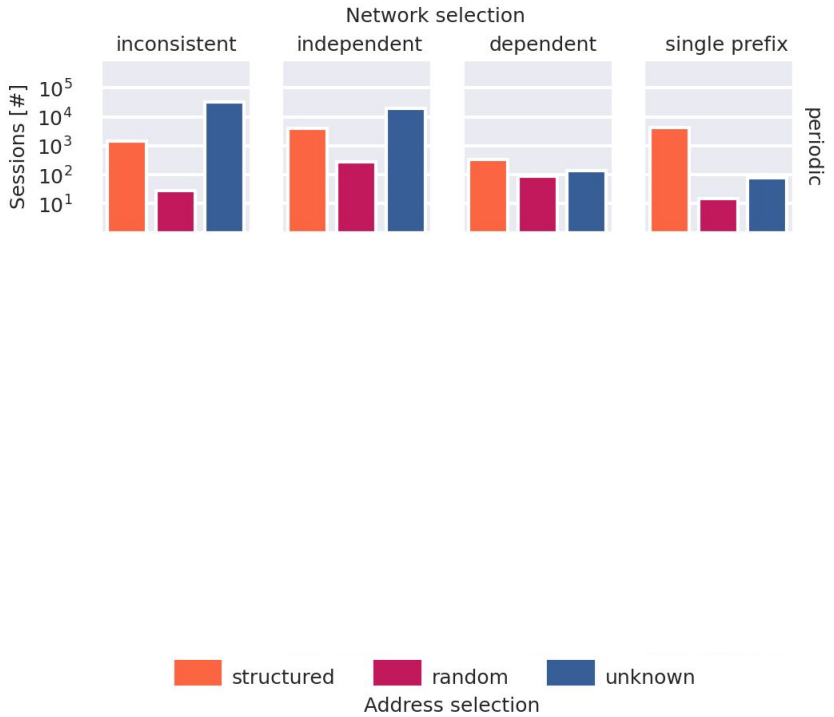
How do scanners select the target prefix at our BGP controlled telescope?

Most scanners return (intermittent:

T4 compared to T1-T3.

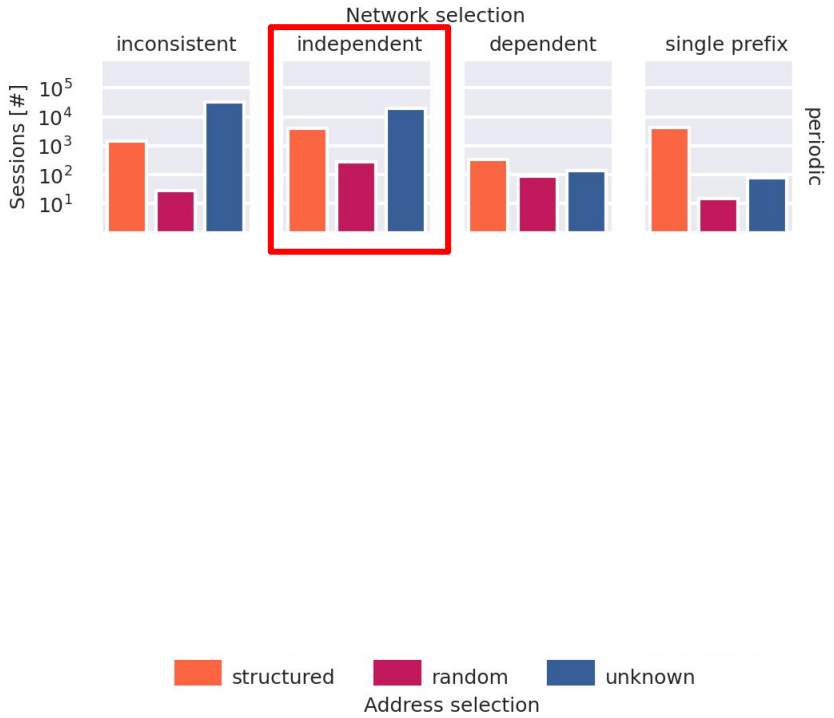
Behavior of scanners at the BGP controlled telescope (T1)

Full observation period.



Behavior of scanners at the BGP controlled telescope (T1)

Full observation period.



Periodic scanners select the target network mostly **independent** of their size.

Behavior of scanners at the BGP controlled telescope (T1)
Full observation period.

Periodic scanners select the target network mostly **independent** of their size.

The majority of intermittent scanners show inconsistent behavior.

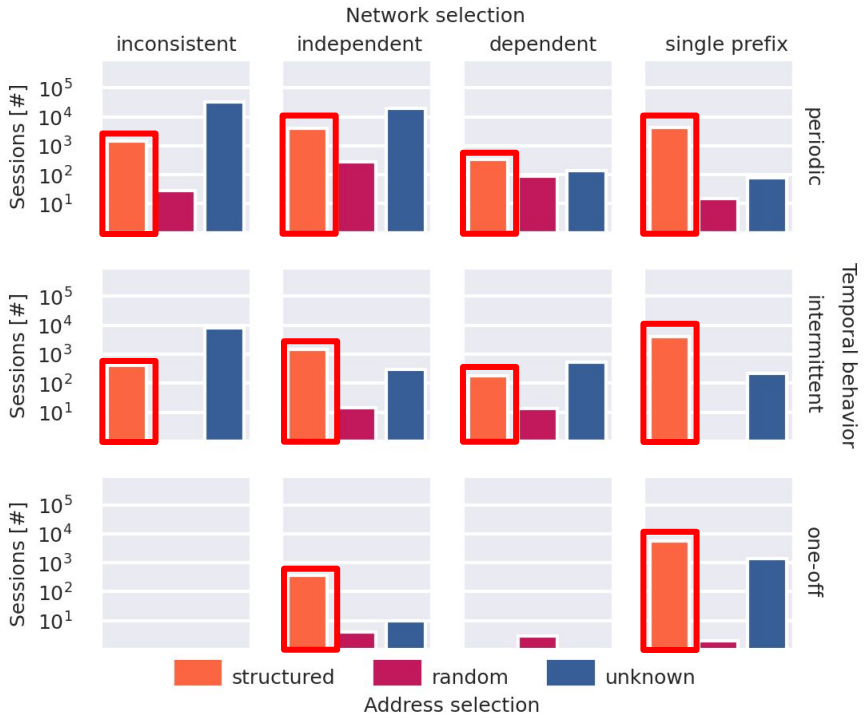
Behavior of scanners at the BGP controlled telescope (T1)
Full observation period.

Periodic scanners select the target network mostly **independent** of their size.

The majority of intermittent scanners show inconsistent behavior.

One-off scanner probe in most cases only a single prefix.

Behavior of scanners at the BGP controlled telescope (T1)
Full observation period.



Periodic scanners select the target network mostly **independent** of their size.

The majority of intermittent scanners show inconsistent behavior.

One-off scanner probe in most cases only a single prefix.

Structured target address selection dominates.

Conclusion

1. **IPv6 telescopes hardly receive any attack backscatter**

Conclusion

1. IPv6 telescopes hardly receive any attack backscatter
2. **Announcing the telescope address space individually in BGP increases visibility**

Conclusion

1. IPv6 telescopes hardly receive any attack backscatter
2. Announcing the telescope address space individually in BGP increases visibility
3. **The network telescope size is of lower relevance in IPv6 compared to IPv4**

Conclusion

1. IPv6 telescopes hardly receive any attack backscatter
2. Announcing the telescope address space individually in BGP increases visibility
3. The network telescope size is of lower relevance in IPv6 compared to IPv4
4. **Visibility of the telescope increases with more individual BGP announcements**

Conclusion

1. IPv6 telescopes hardly receive any attack backscatter
2. Announcing the telescope address space individually in BGP increases visibility
3. The network telescope size is of lower relevance in IPv6 compared to IPv4
4. Visibility of the telescope increases with more individual BGP announcements
5. **Structured target addresses (e.g., low-byte) are preferred by many scanners**

Conclusion

1. IPv6 telescopes hardly receive any attack backscatter
2. Announcing the telescope address space individually in BGP increases visibility
3. The network telescope size is of lower relevance in IPv6 compared to IPv4
4. Visibility of the telescope increases with more individual BGP announcements
5. Structured target addresses (e.g., low-byte) are preferred by many scanners

More details can be found in the paper!
All artifacts for this paper are available under
https://doi.org/10.5281/zenodo.16419095