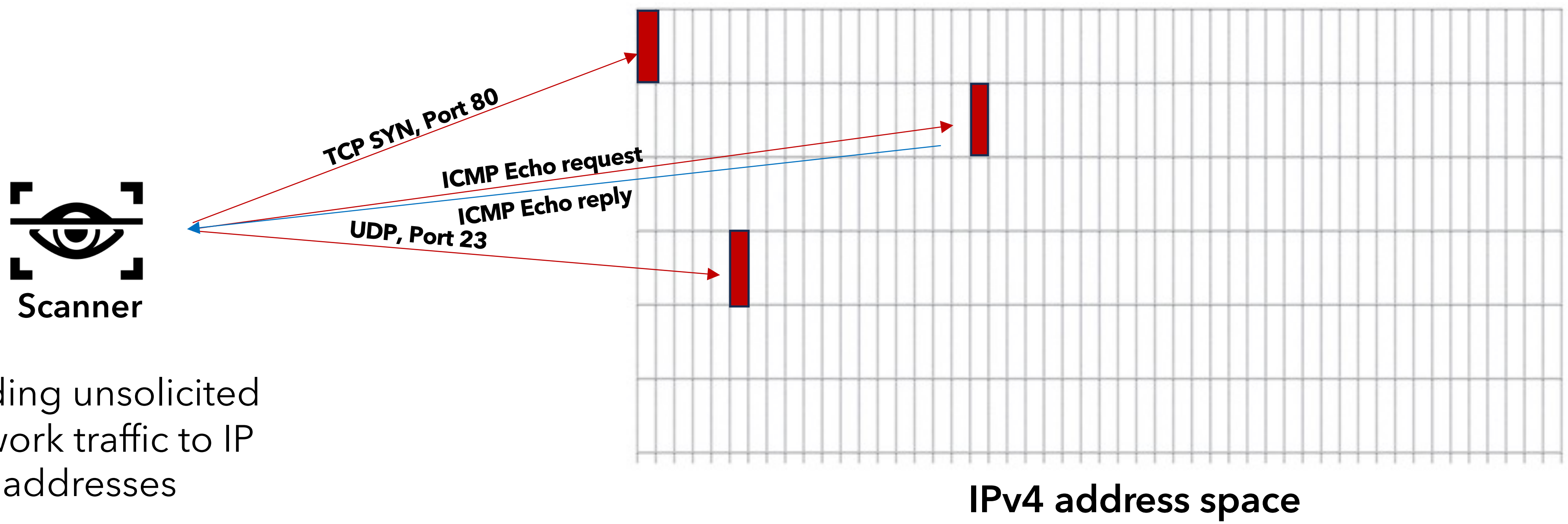
Glowing in the Dark

Uncovering IPv6 Address Discovery and Scanning Strategies in the Wild

Hammas Bin Tanveer, Rachee Singh, Paul Pearce, Rishab Nithyanand

32ND USENIX SECURITY SYMPOSIUM

What is internet scanning?

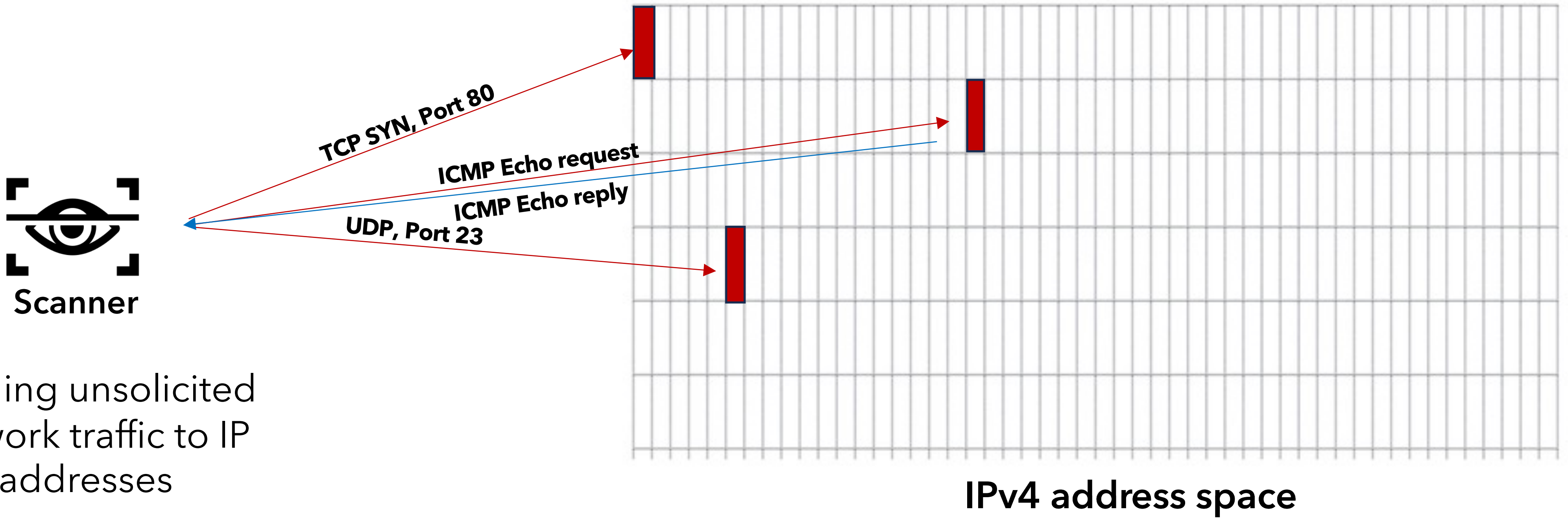


Sending unsolicited network traffic to IP addresses

Previous work

Internet scanning has been studied extensively for the past two decades

Led to the development of fast scanning tools e.g., ZMap



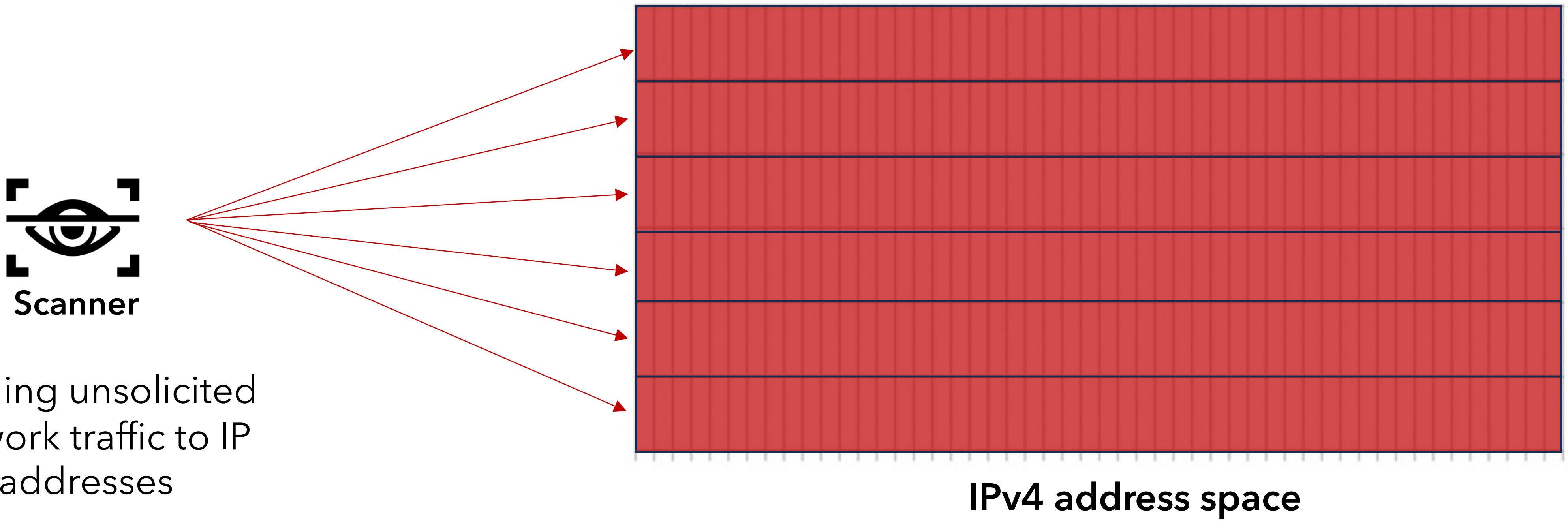
Sending unsolicited network traffic to IP addresses

Previous work

Internet scanning has been studied extensively for the past two decades

Led to the development of fast scanning tools e.g., ZMap

Fast scanning tool + good internet can scan the whole IPv4 address space in minutes



Sending unsolicited network traffic to IP addresses

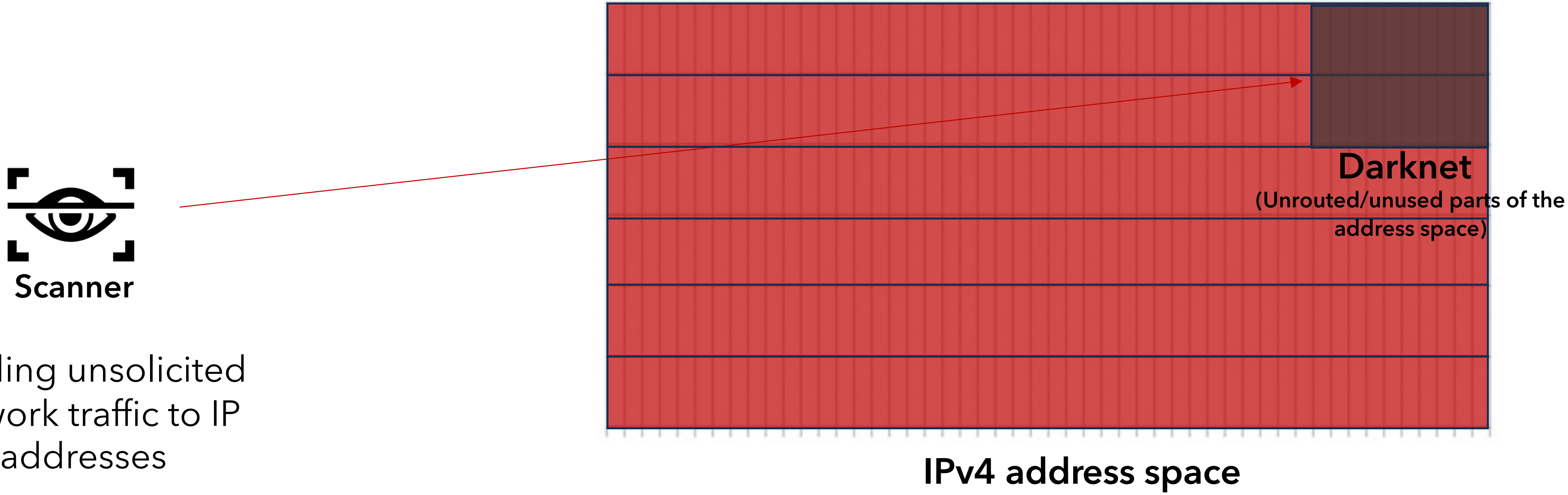
Previous work

Internet scanning has been studied extensively for the past two decades

Led to the development of fast scanning tools e.g., ZMap

Fast scanning tool + good internet can scan the whole IPv4 address space in minutes

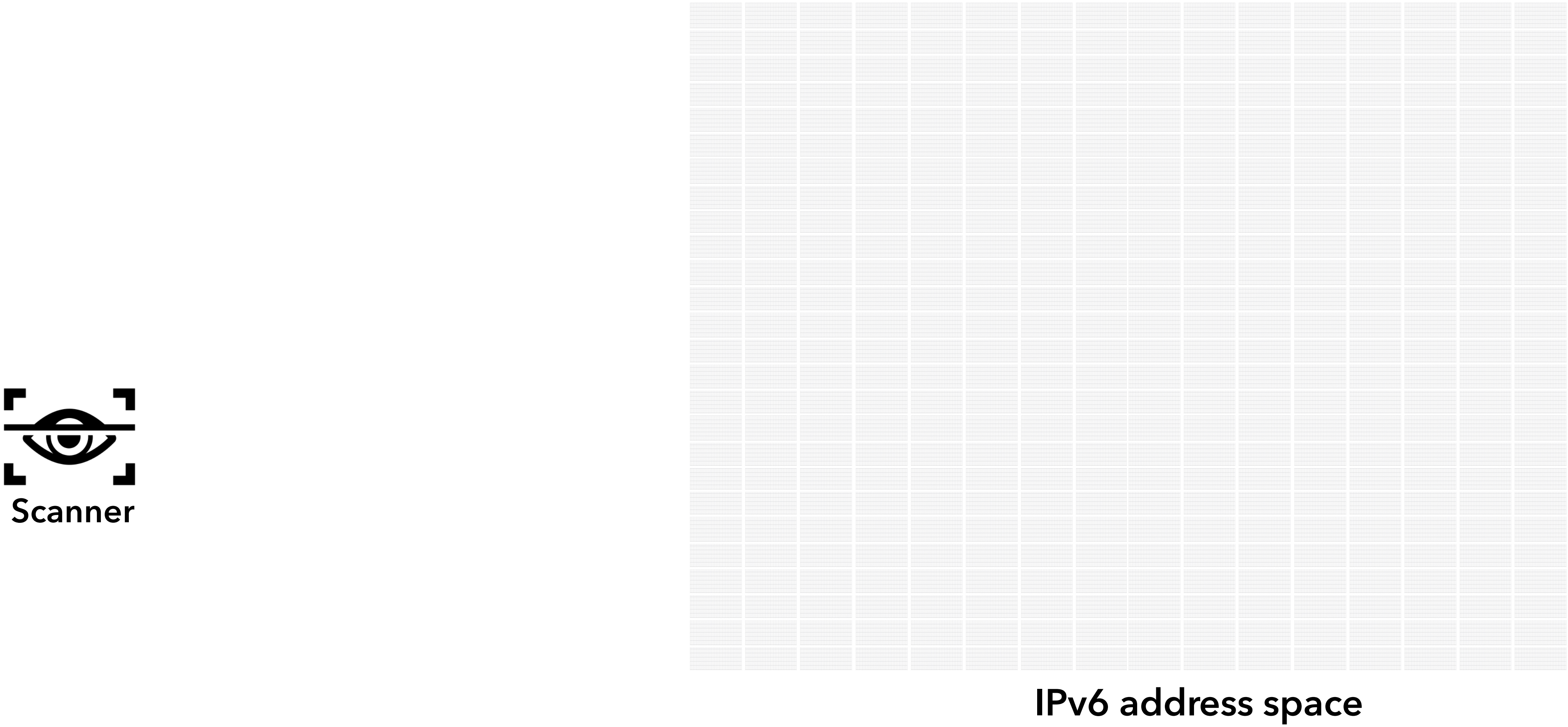
Darknets can be used to understand scanning prevalence and behavior



Sending unsolicited network traffic to IP addresses

Previous work

Tools + techniques developed to understand scanning do not translate to IPv6



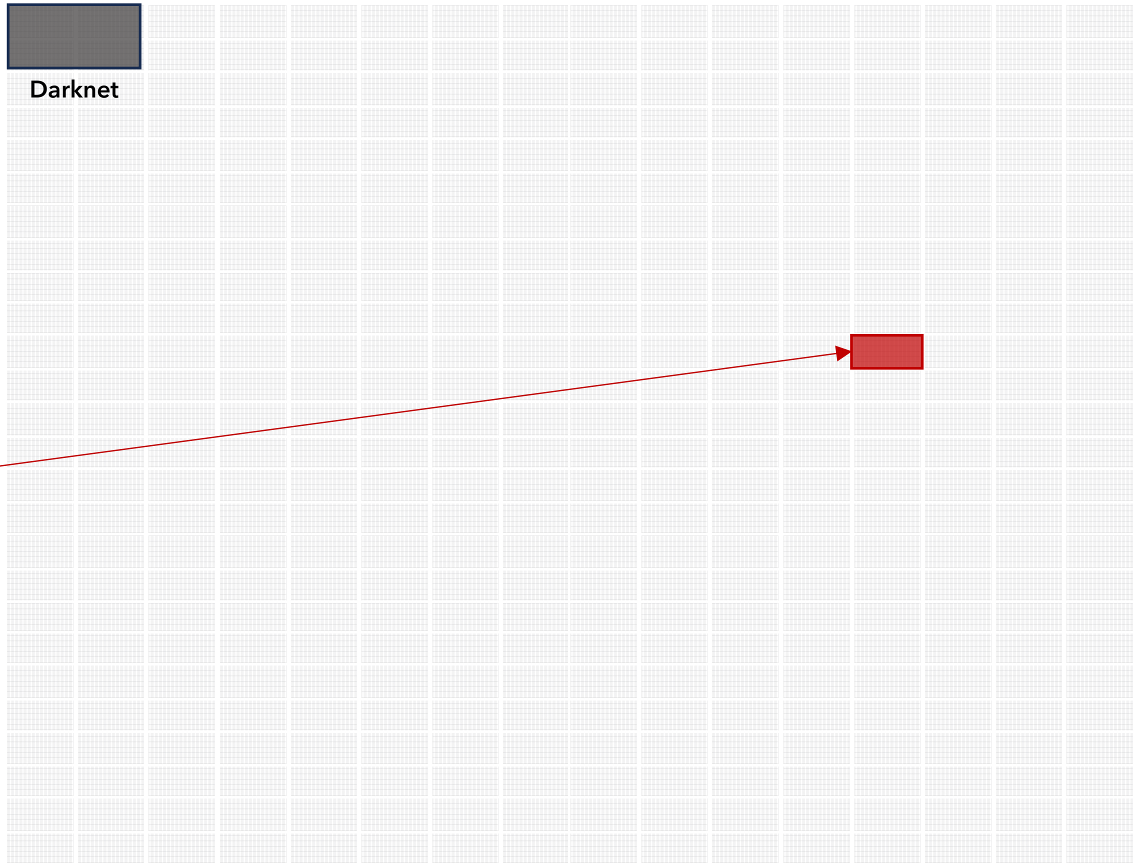
* Address space not drawn to scale

Previous work

Tools + techniques developed to understand scanning do not translate to IPv6

Impossible to brute-force scan the entire IPv6 address space

IPv6 darknets capture insignificant amount of scanning traffic compared to IPv4 darknets



* Address space not drawn to scale

Motivation

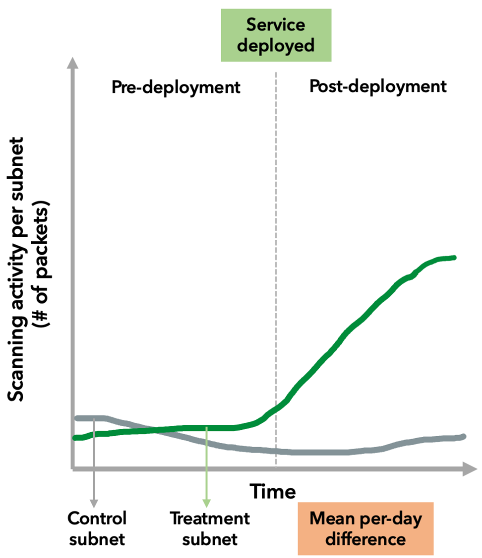
How to capture a more representative amount of IPv6 scanning traffic?

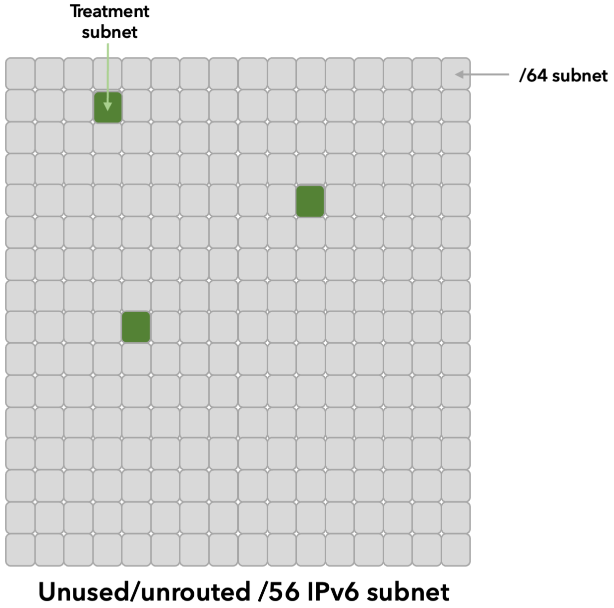
What strategies do IPv6 scanners use in the wild?

How can we make our IPv6 address spaces more secure against scanning?

Talk overview

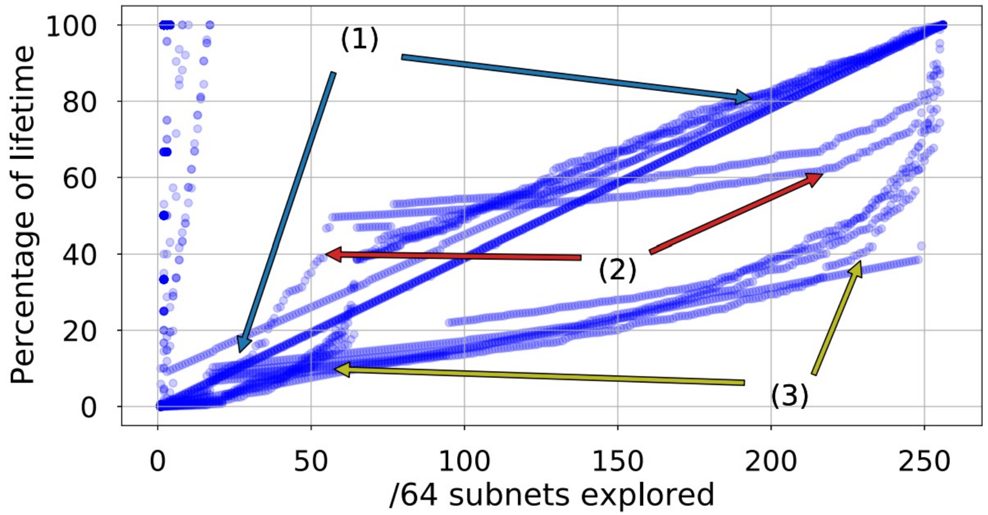
We introduce a **novel methodology** better suited for **capturing scanning traffic** in **IPv6 networks.**

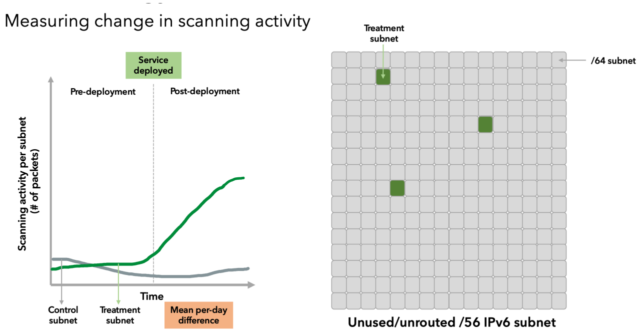




Talk overview

Using our methodology, we collect scanning traffic and present an **overview of scanning prevalence and strategies.**

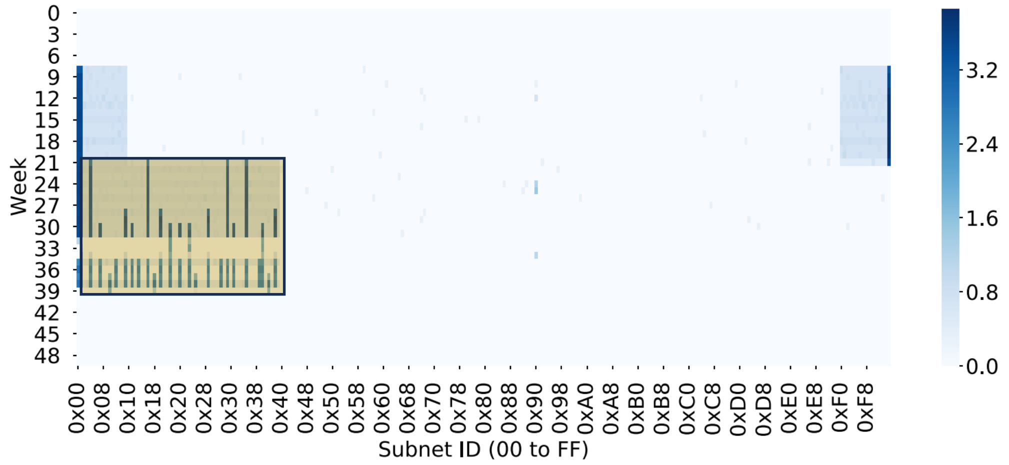


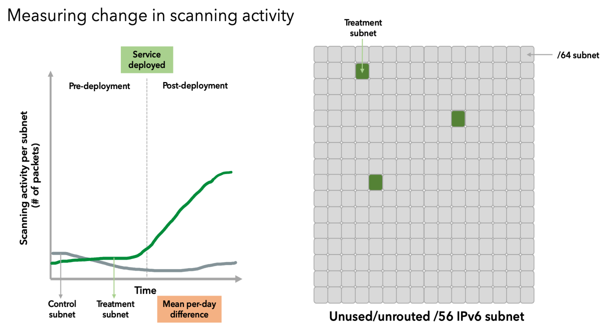


Develop methodology

Talk overview

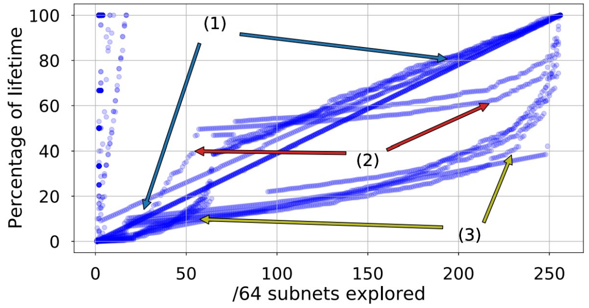
We present **security implications for network operators** by analyzing scanning strategies





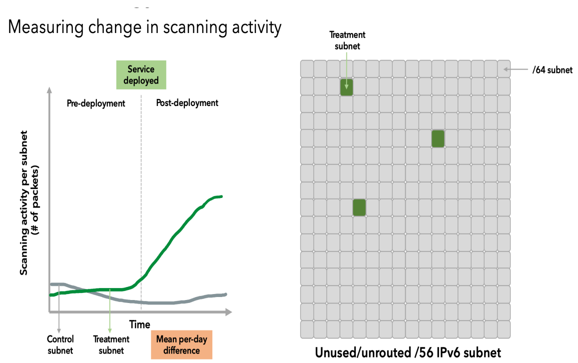
Develop methodology

Capture Traffic



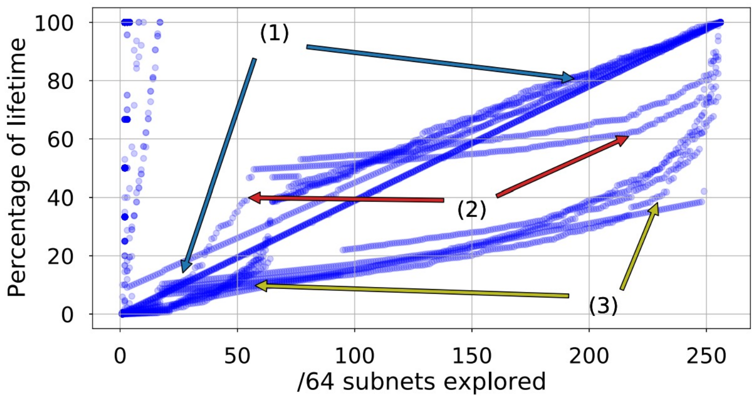
Overview of scanning prevalence and strategies

Talk overview



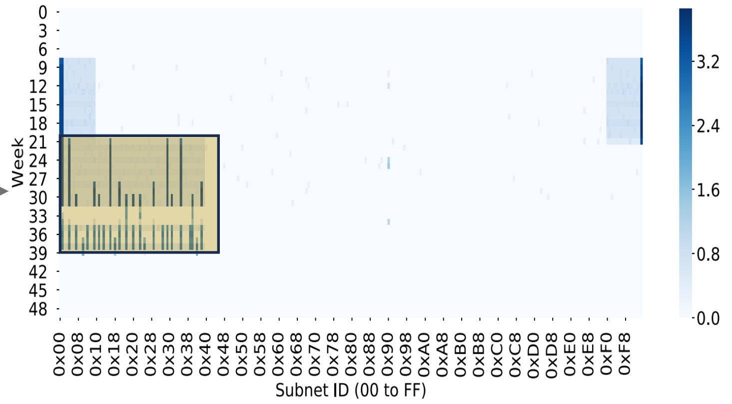
Develop methodology

Capture Traffic



Overview of scanning prevalence and strategies

Analyze scanners



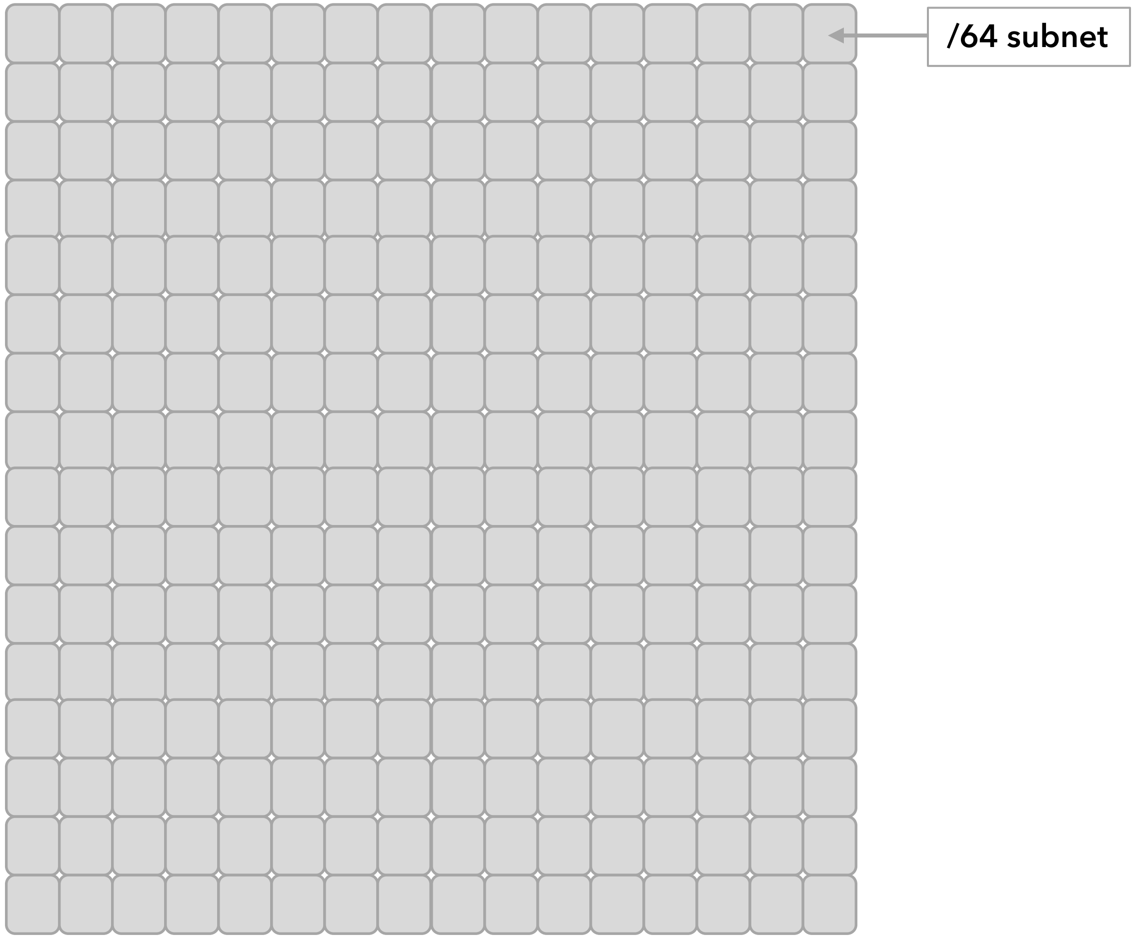
Present security implications

Methodology

Intuition: Due to the vastness of IPv6, scanners target regions of the address space with "live" IP addresses

Methodology

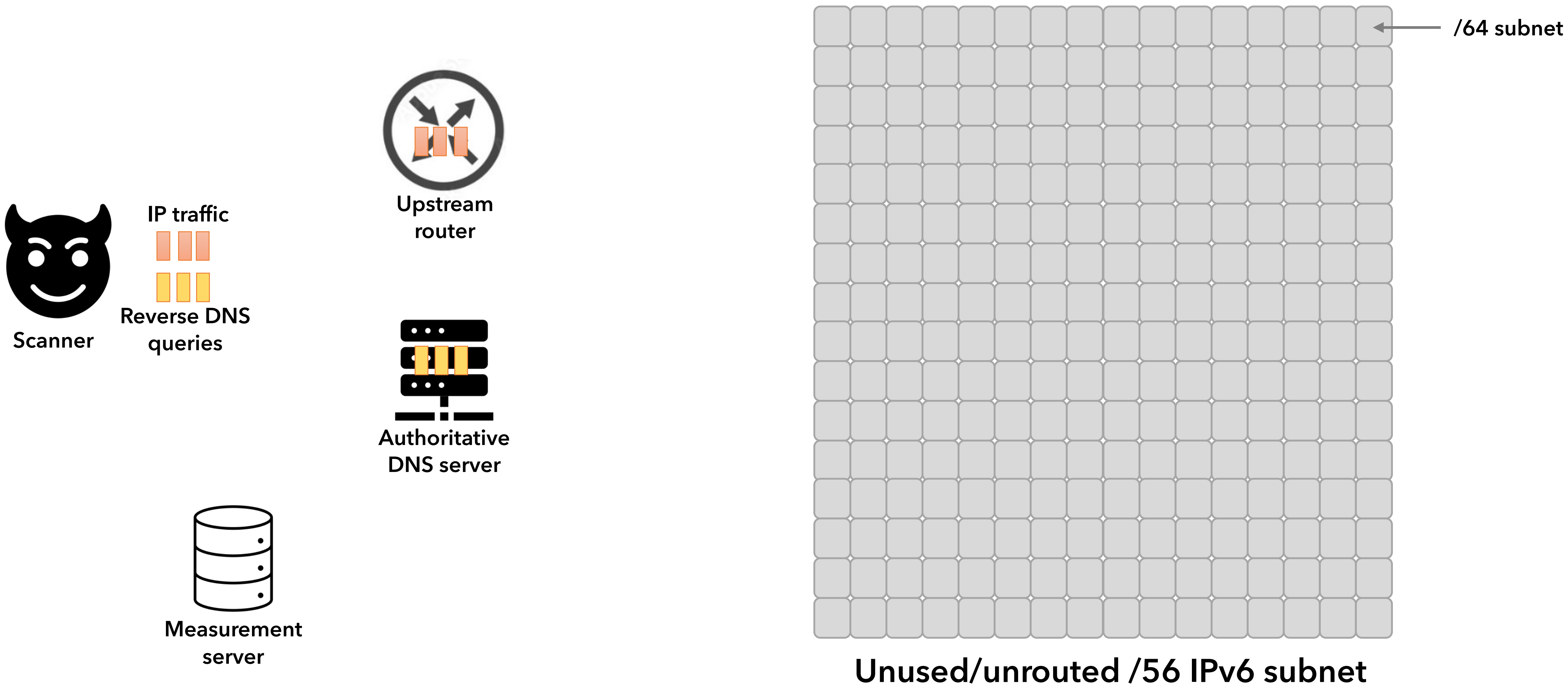
Intuition: Due to the vastness of IPv6, scanners target regions of the address space with "live" IP addresses



Unused/unrouted /56 IPv6 subnet

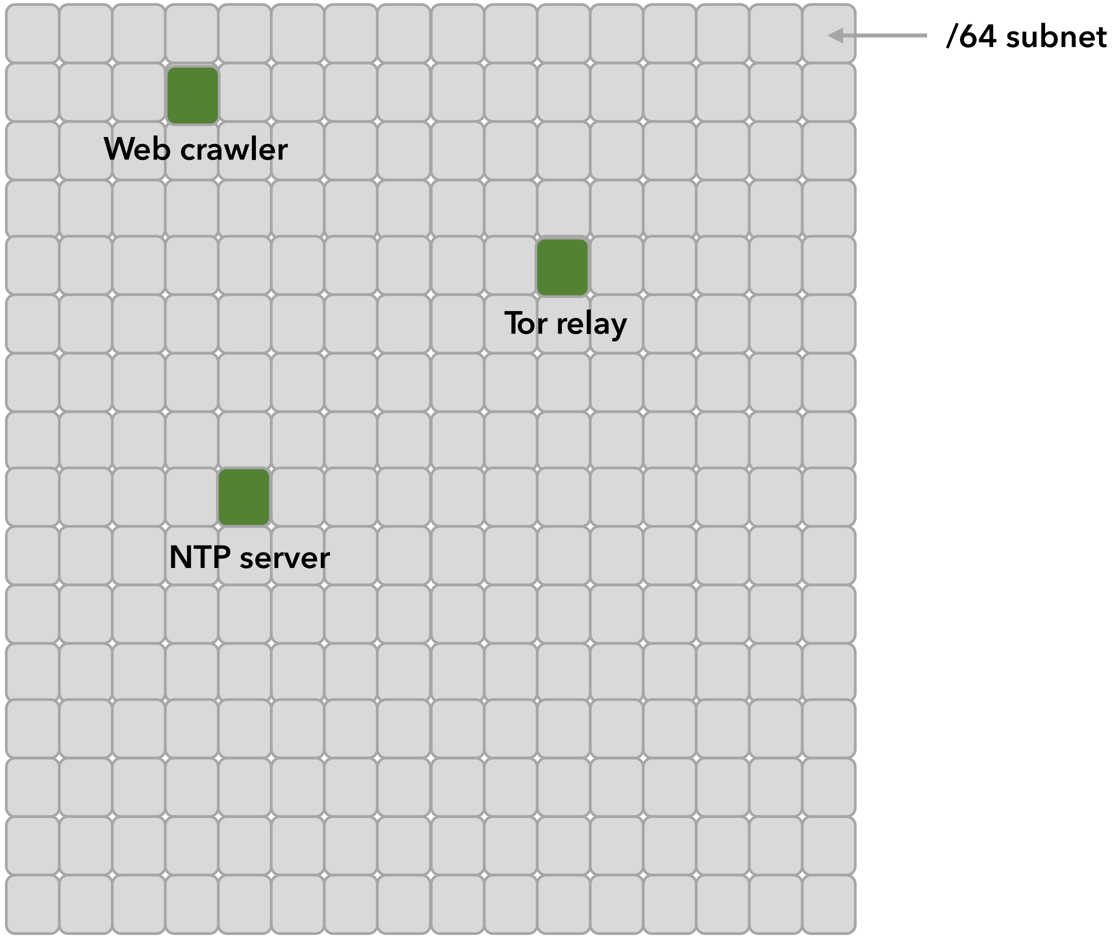
Methodology

Capture network traffic + reverse DNS queries towards our /56 subnet



Methodology

Simulating a "live" address space

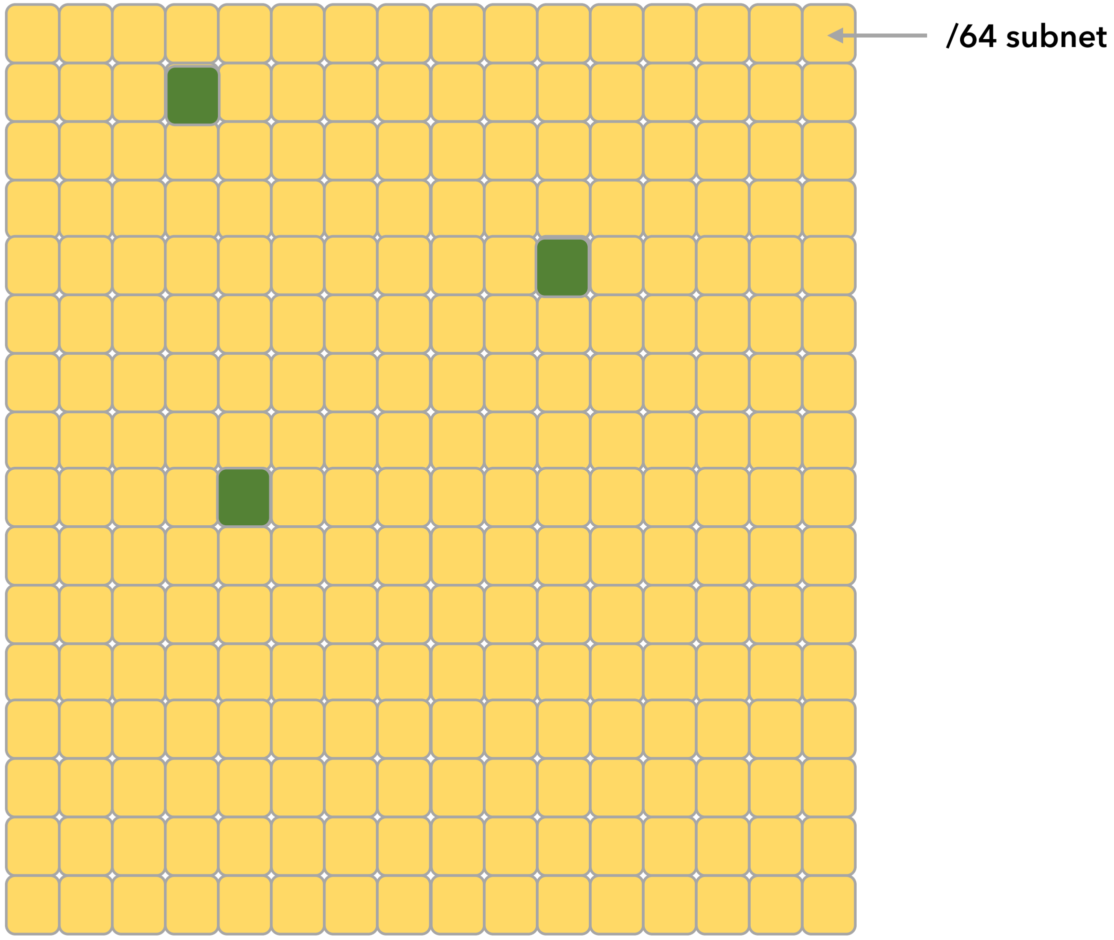


Unused/unrouted /56 IPv6 subnet

Methodology

Our definition of a scanner

An IP address that sends unsolicited network traffic to a /128 IPv6 address on which none of our services were run.



Unused/unrouted /56 IPv6 subnet

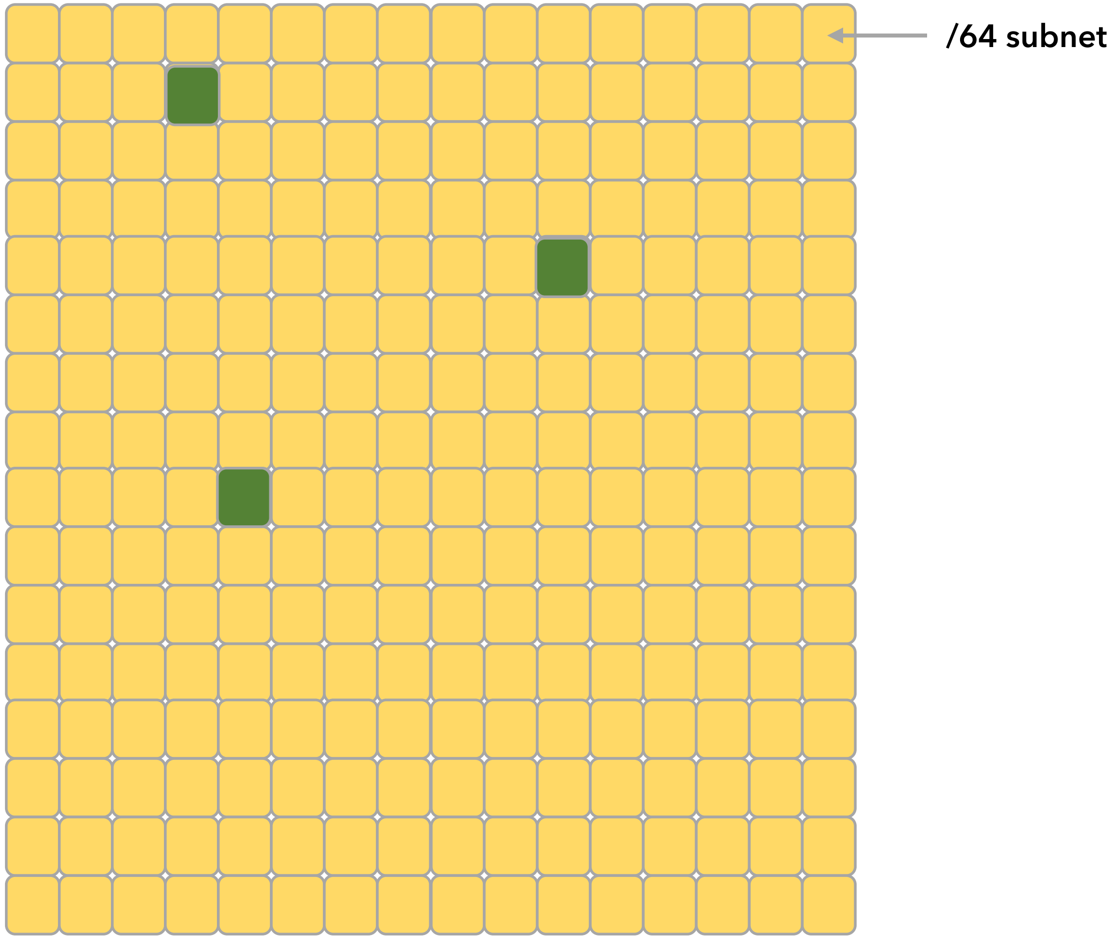
Methodology

Our definition of a scanner

An IP address that sends unsolicited network traffic to a /128 IPv6 address on which none of our services were run.

IP scanner: IP traffic e.g., ICMP, TCP, UDP etc.

DNS scanner: Reverse DNS queries



Unused/unrouted /56 IPv6 subnet

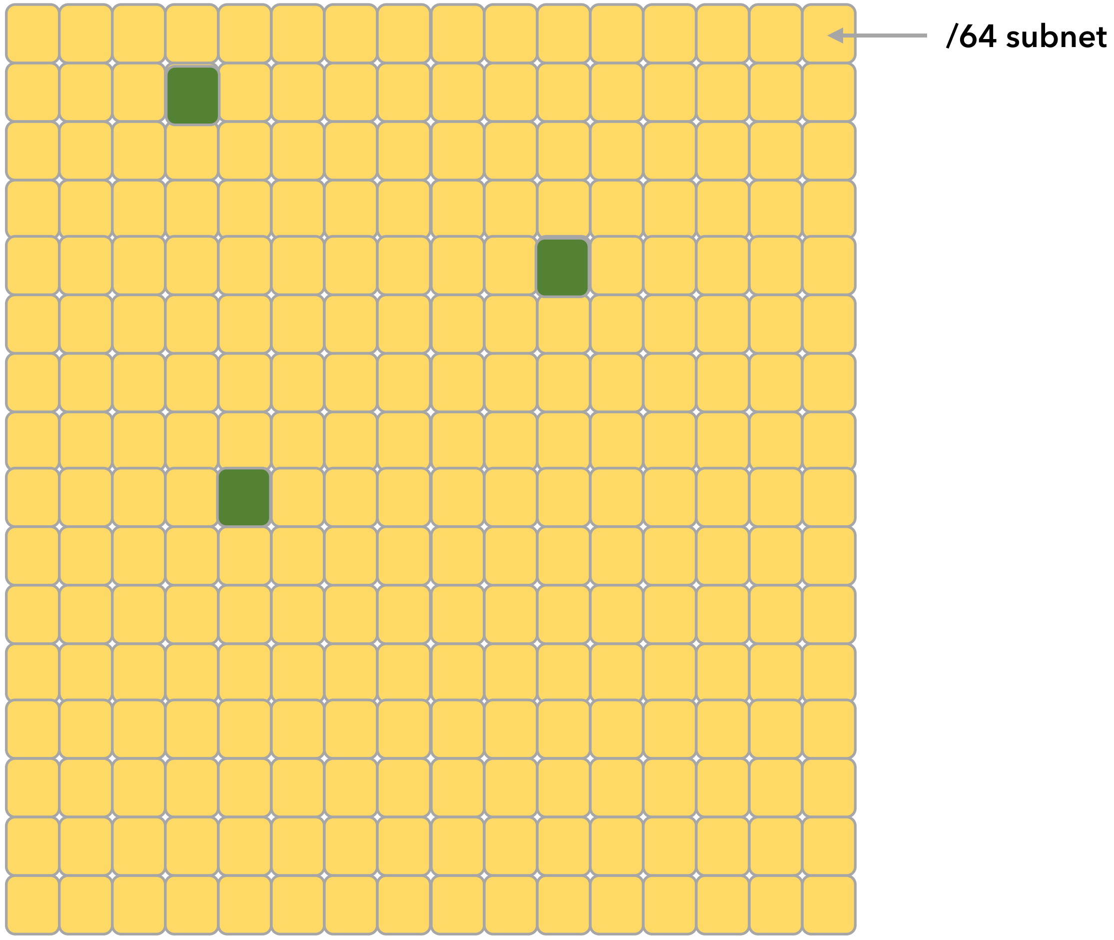
Methodology

Our definition of a scanner

An IP address that sends unsolicited network traffic to a /128 IPv6 address on which none of our services were run.

IP scanner: IP traffic e.g., ICMP, TCP, UDP etc.

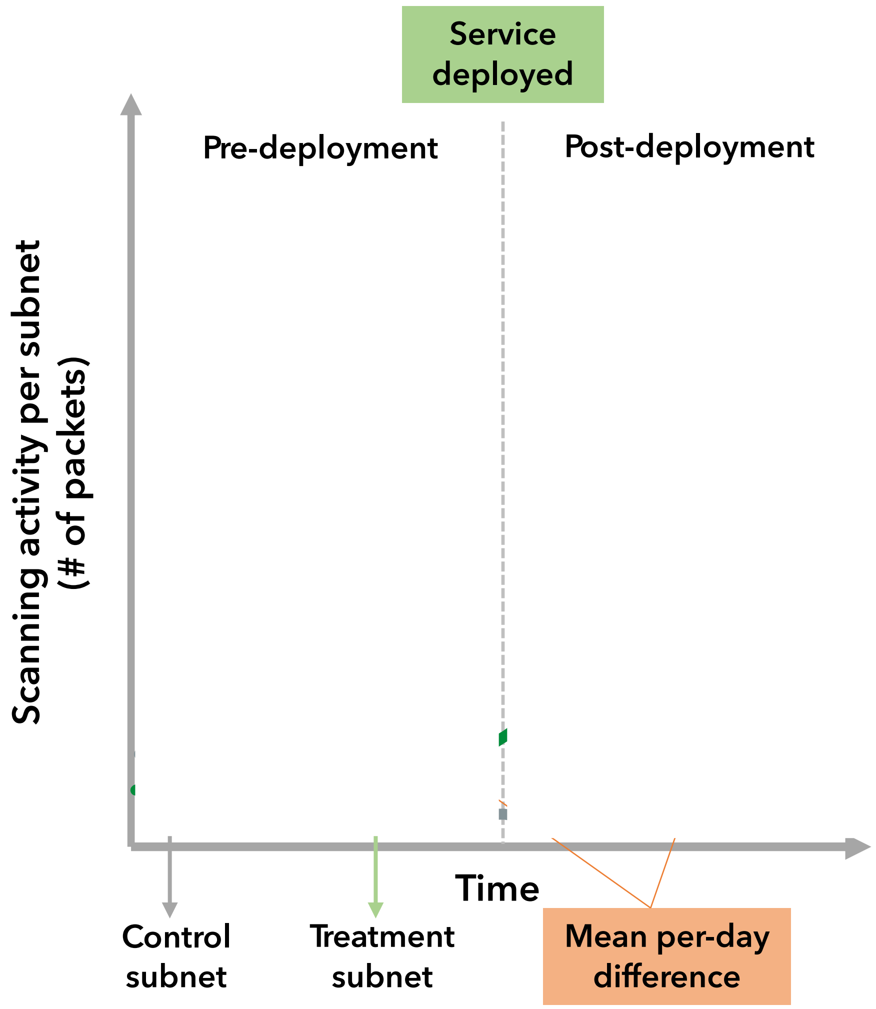
DNS scanner: Reverse DNS queries

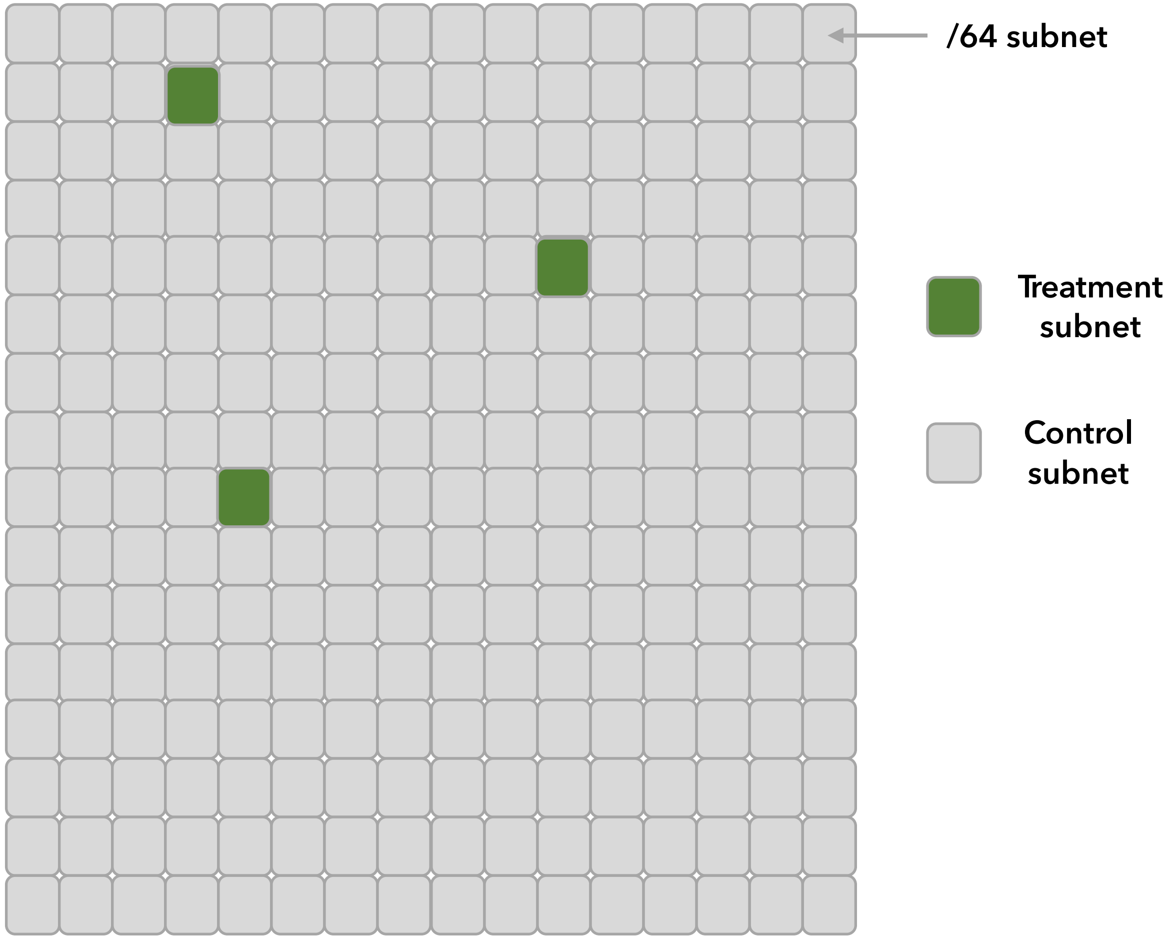


Unused/unrouted /56 IPv6 subnet

Methodology

Measuring change in scanning activity

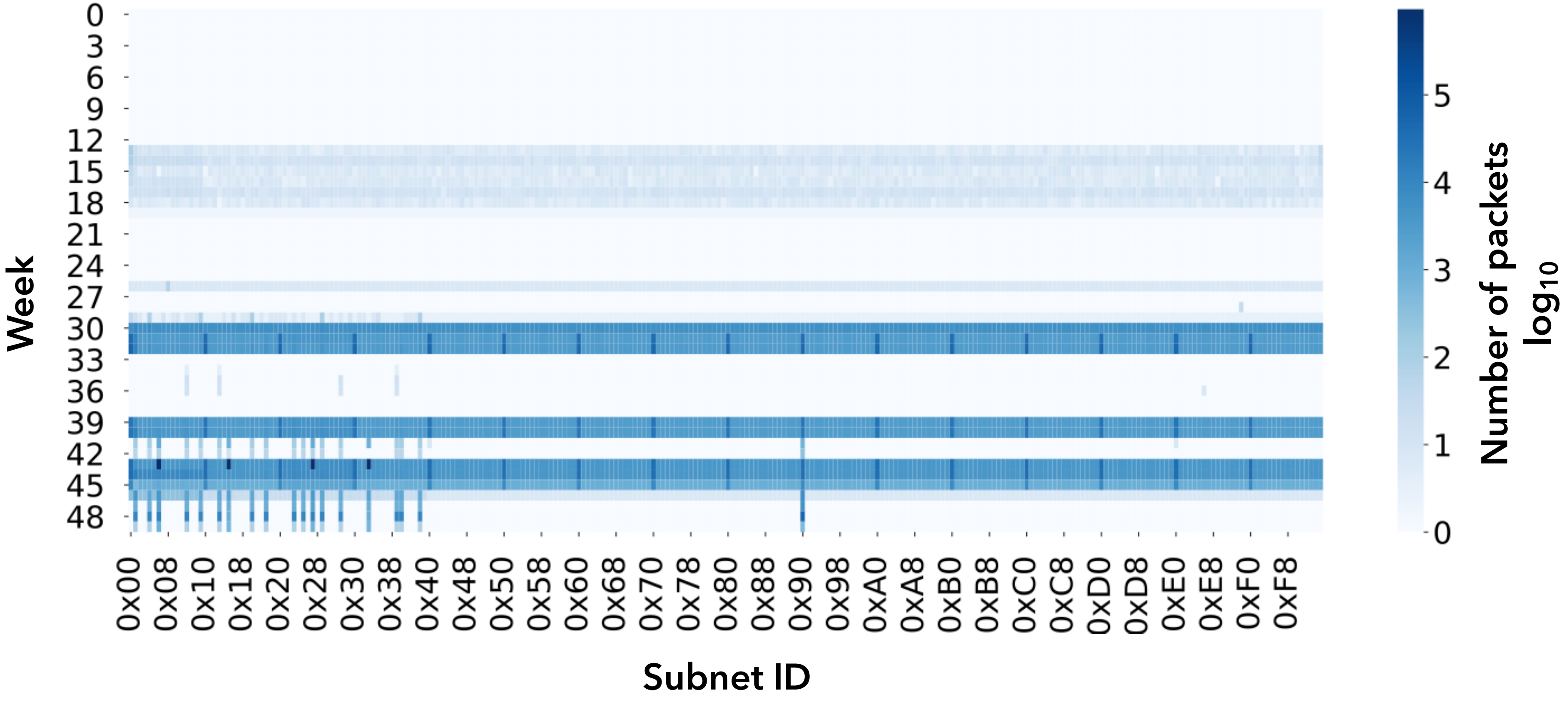




Unused/unrouted /56 IPv6 subnet

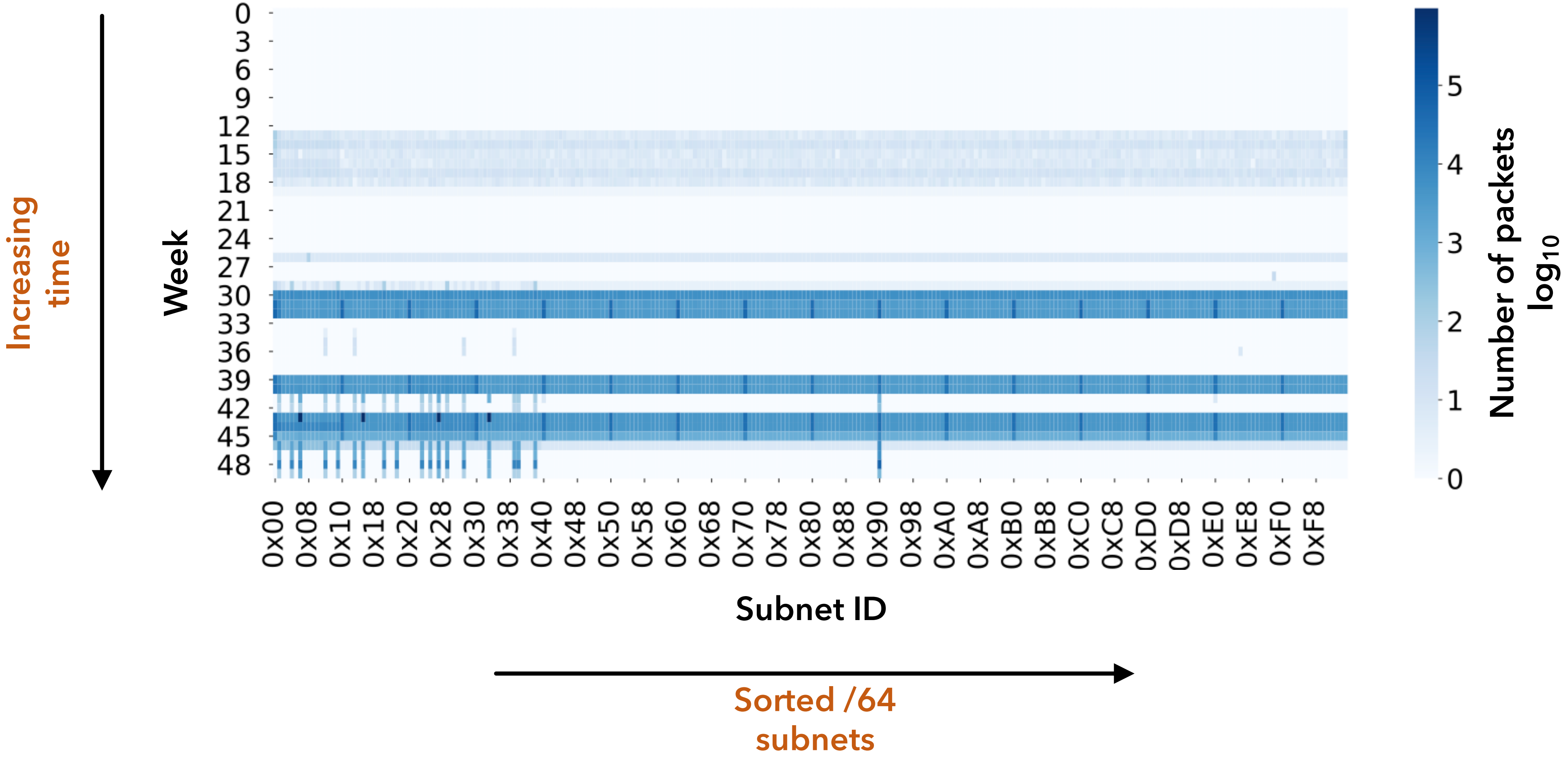
Results

Overview of scanning traffic received



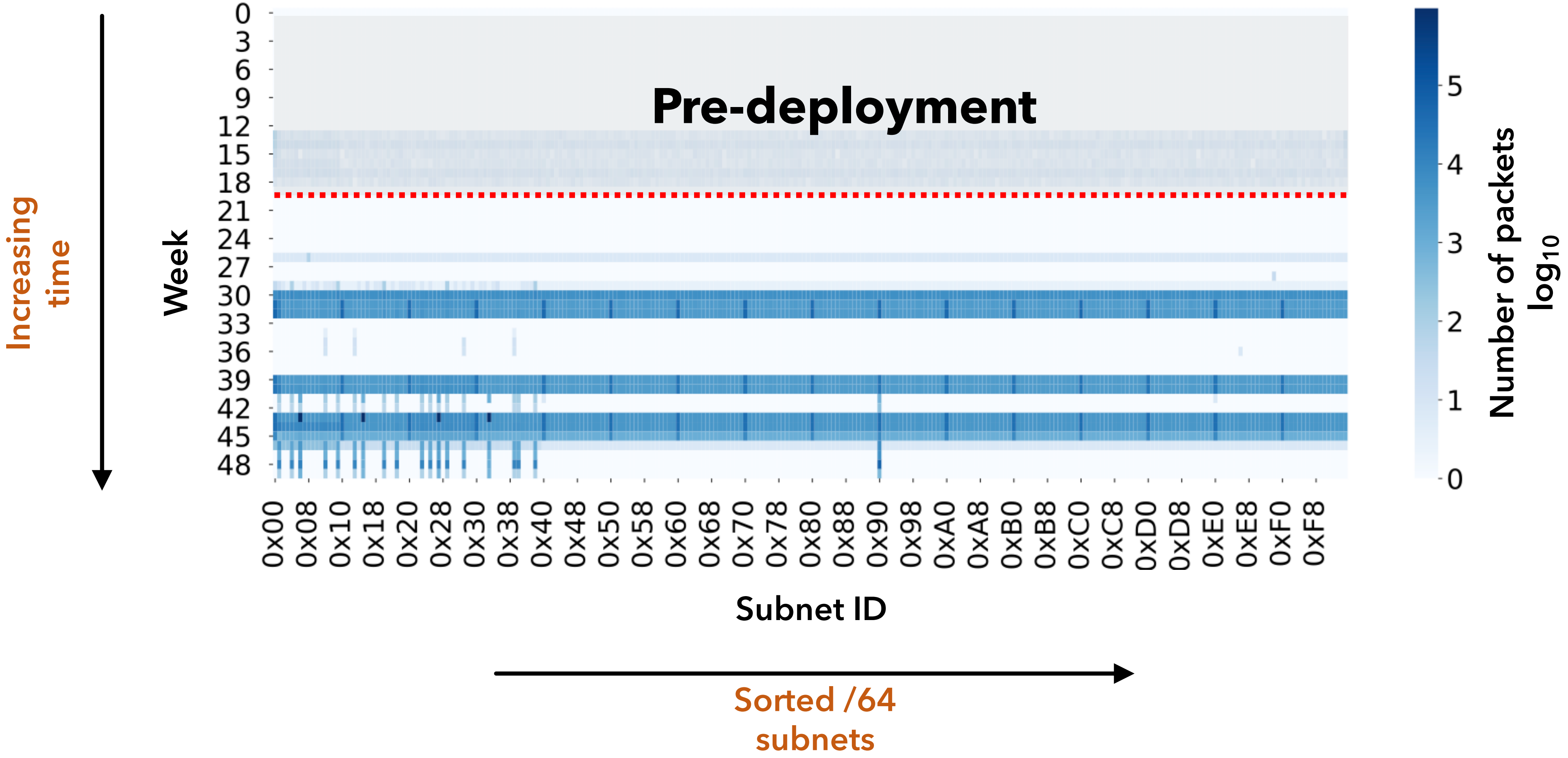
Results

Overview of scanning traffic received



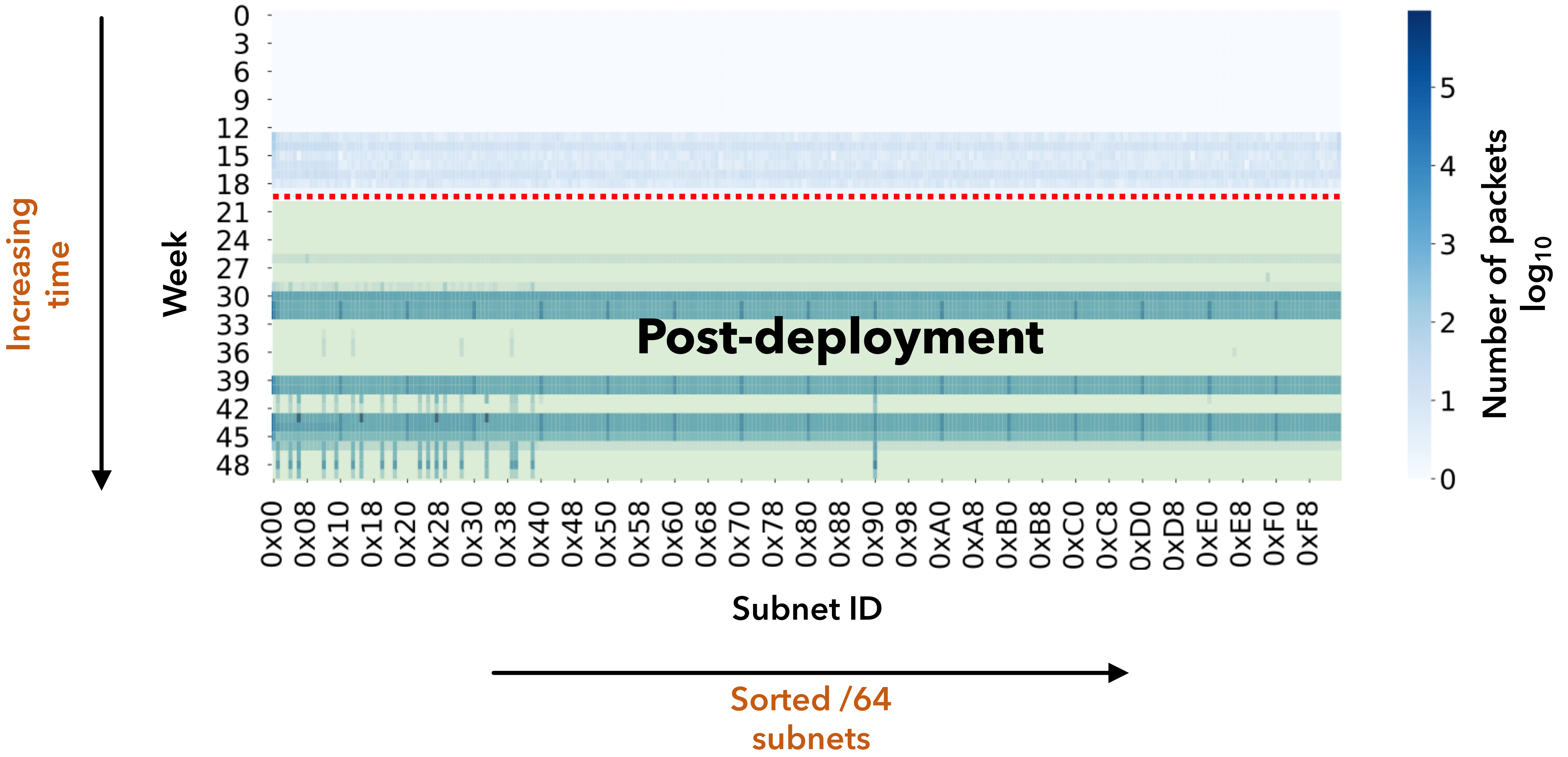
Results

Overview of scanning traffic received



Results

Overview of scanning traffic received

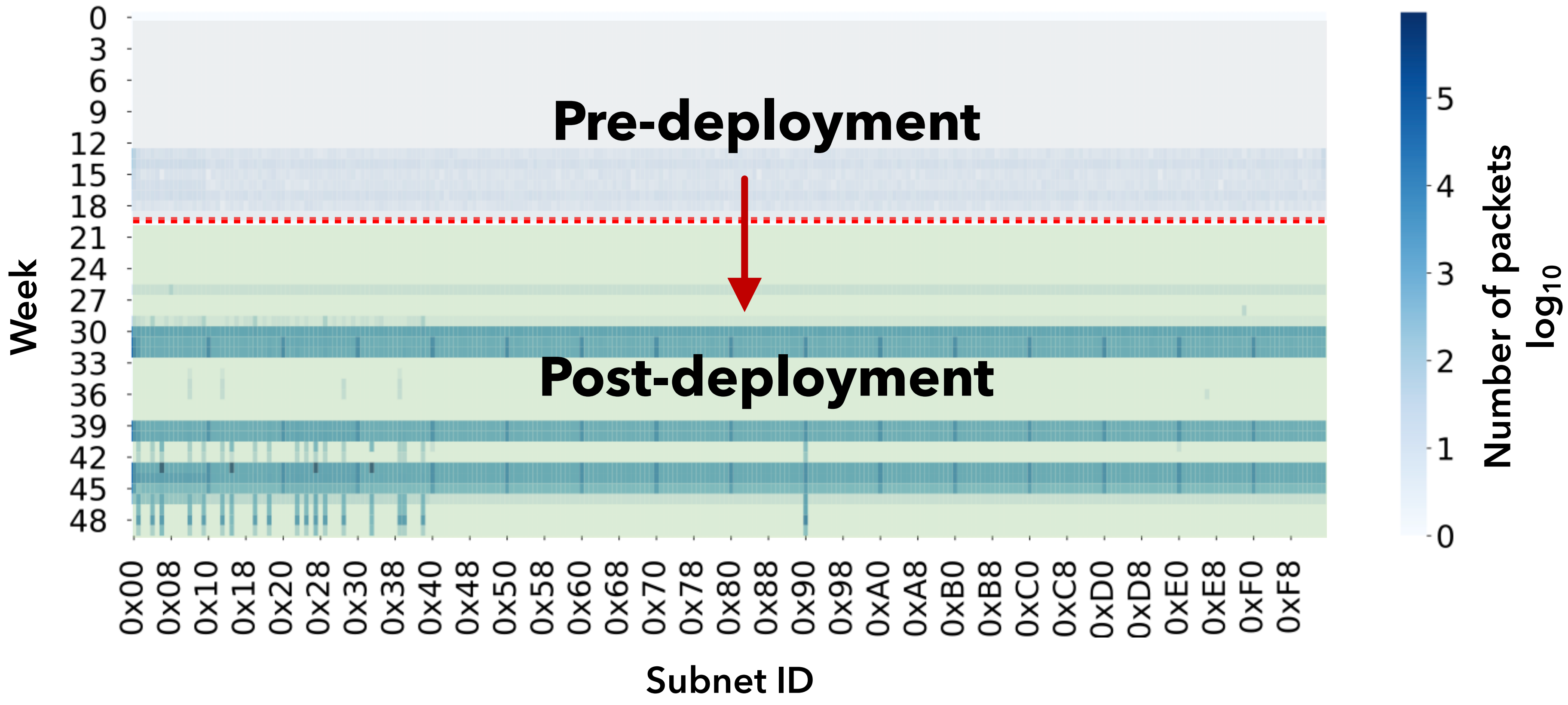


Results

Overview of scanning traffic received

200X increase in # of scanners

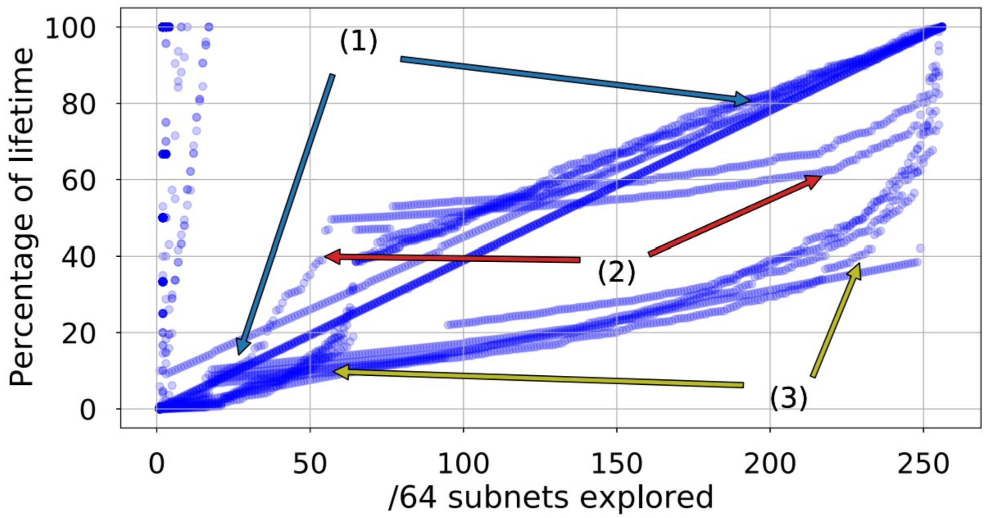
1000X increase in scanning traffic

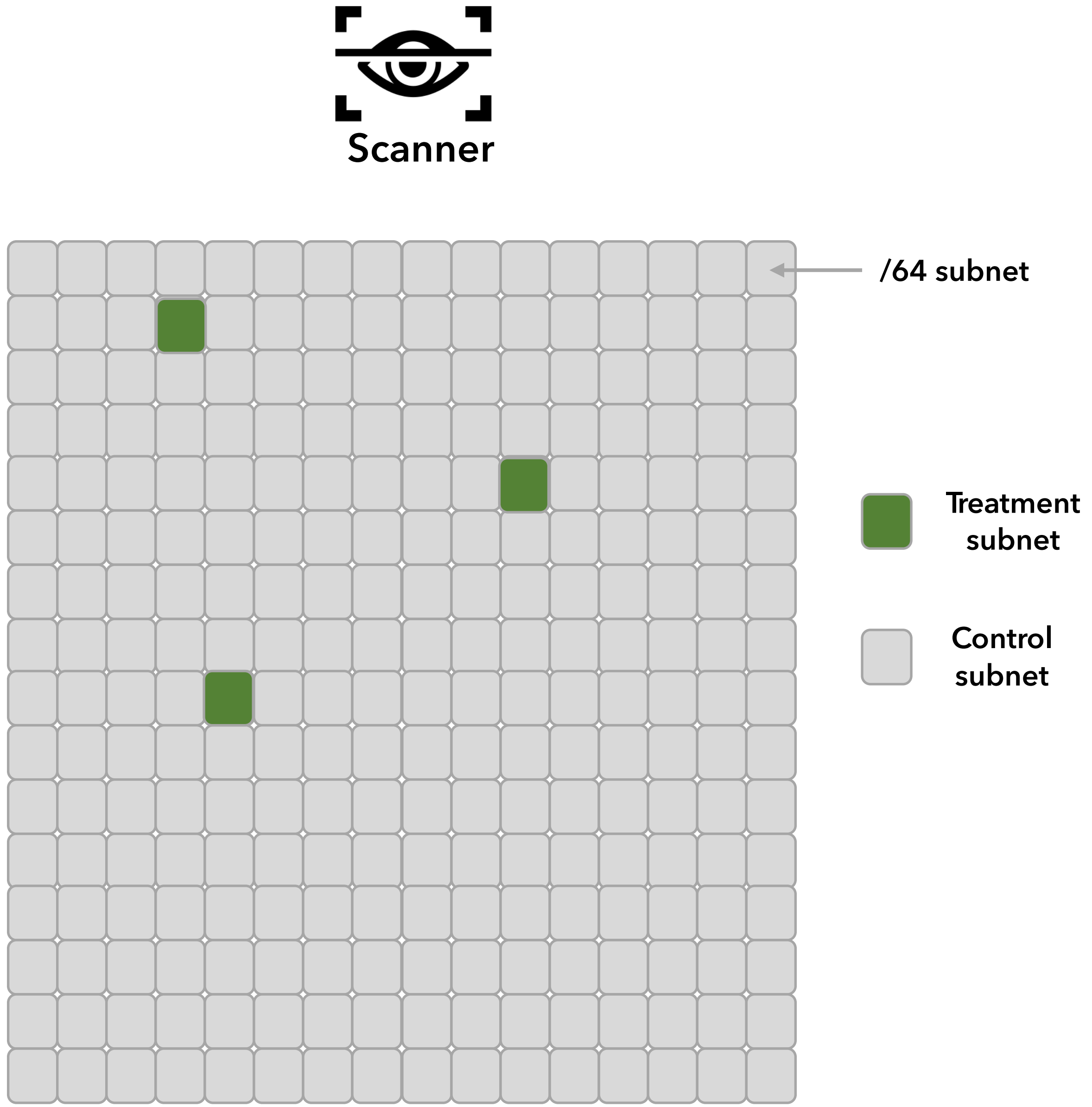


Results

Scanner strategies

Scanning strategies over time

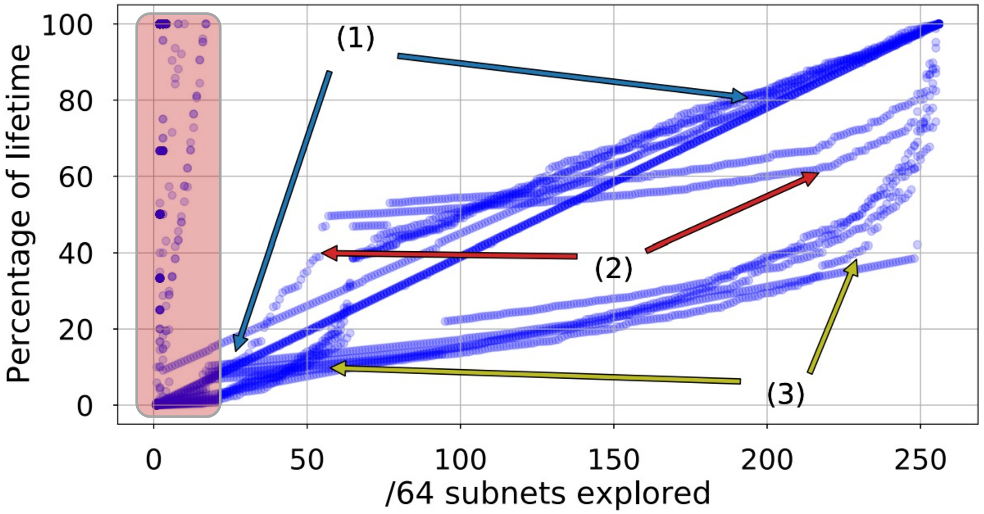


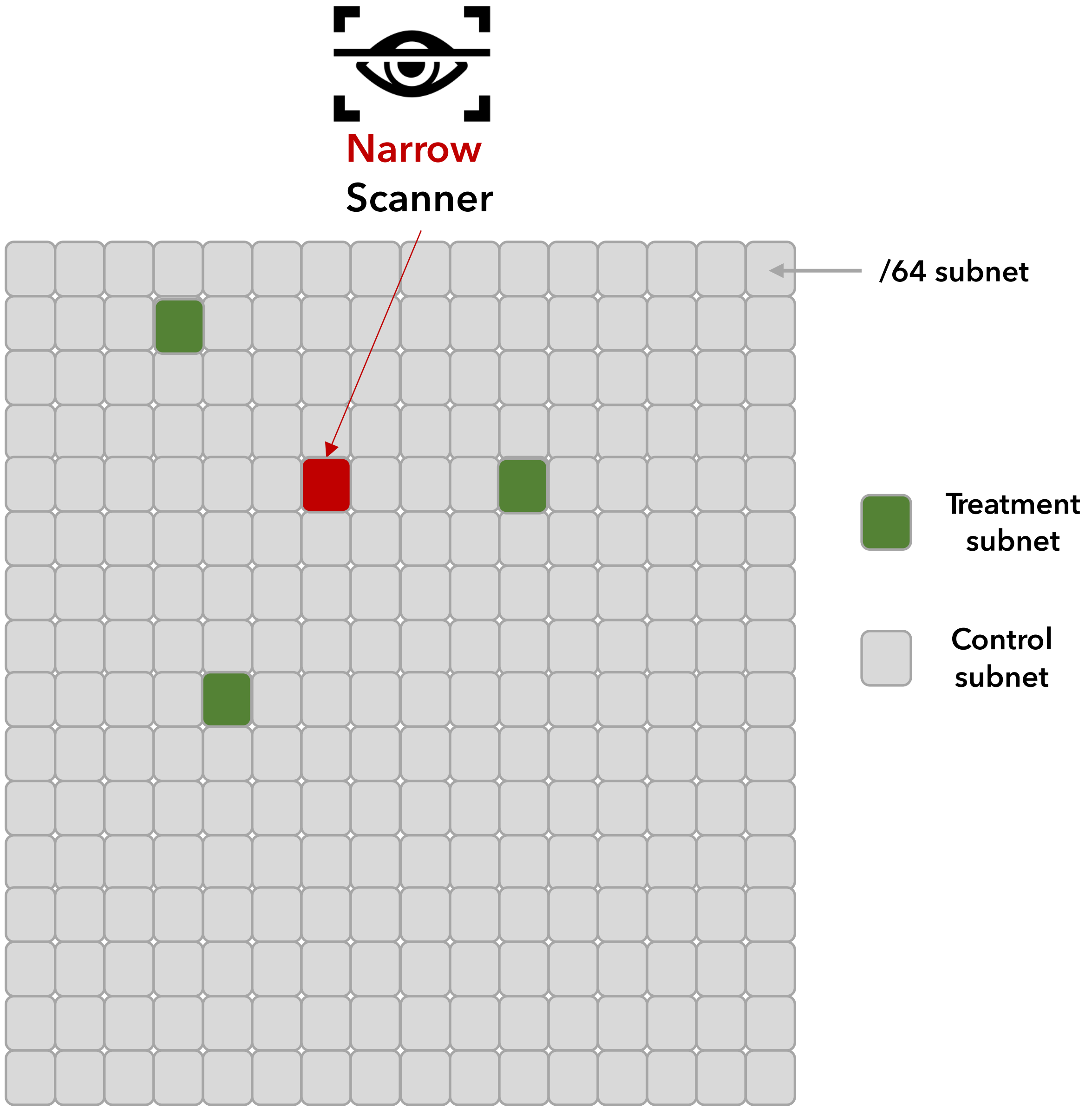


Results

Scanner strategies

Scanning strategies over time

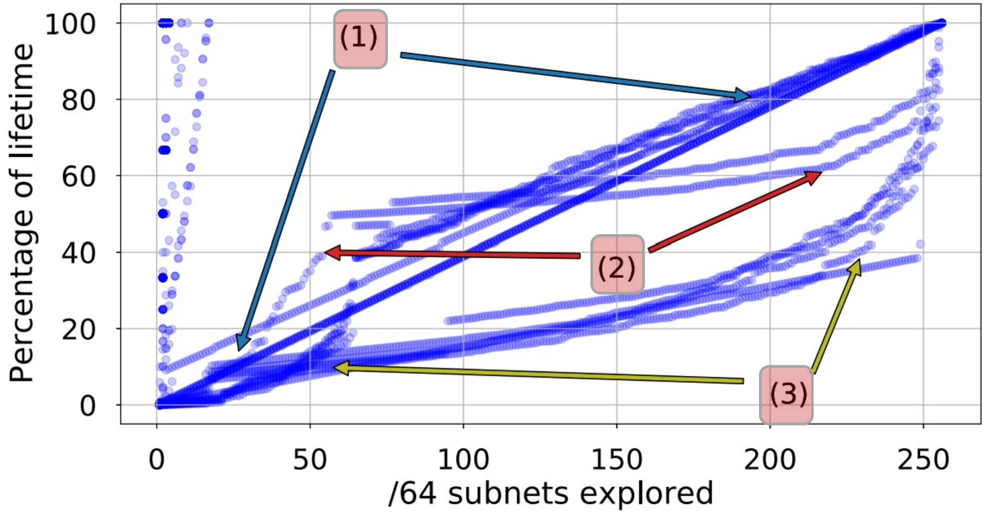


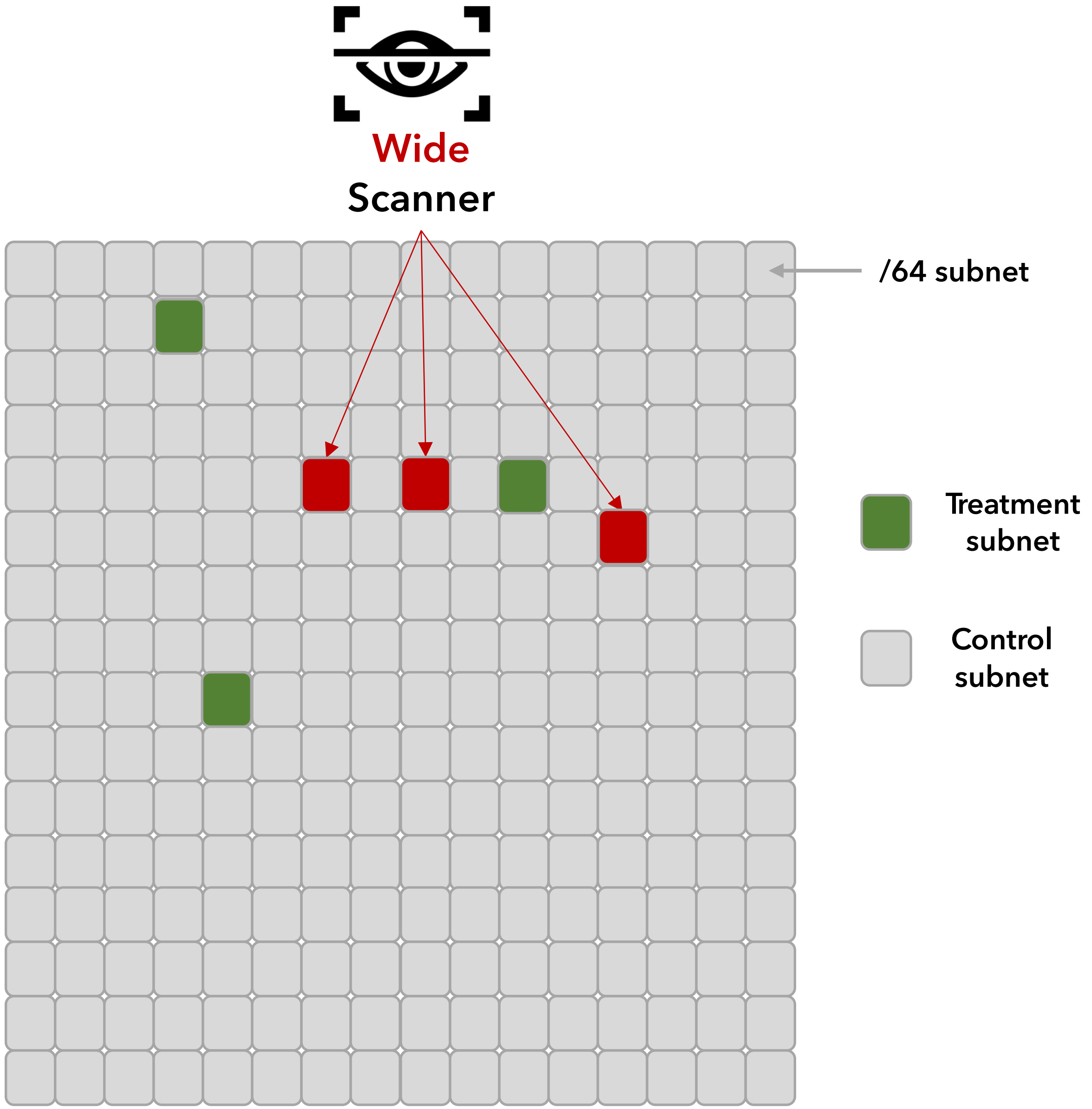


Results

Scanner strategies

Scanning strategies over time

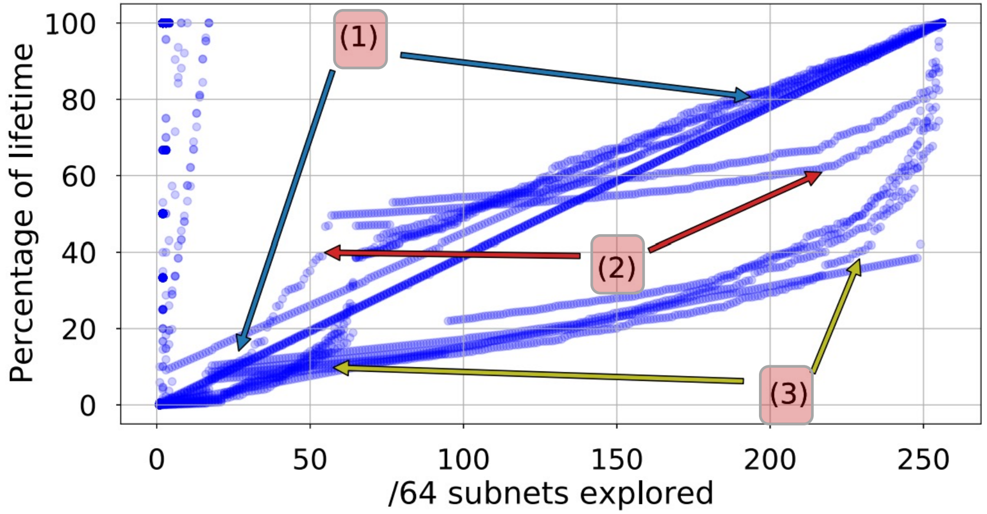


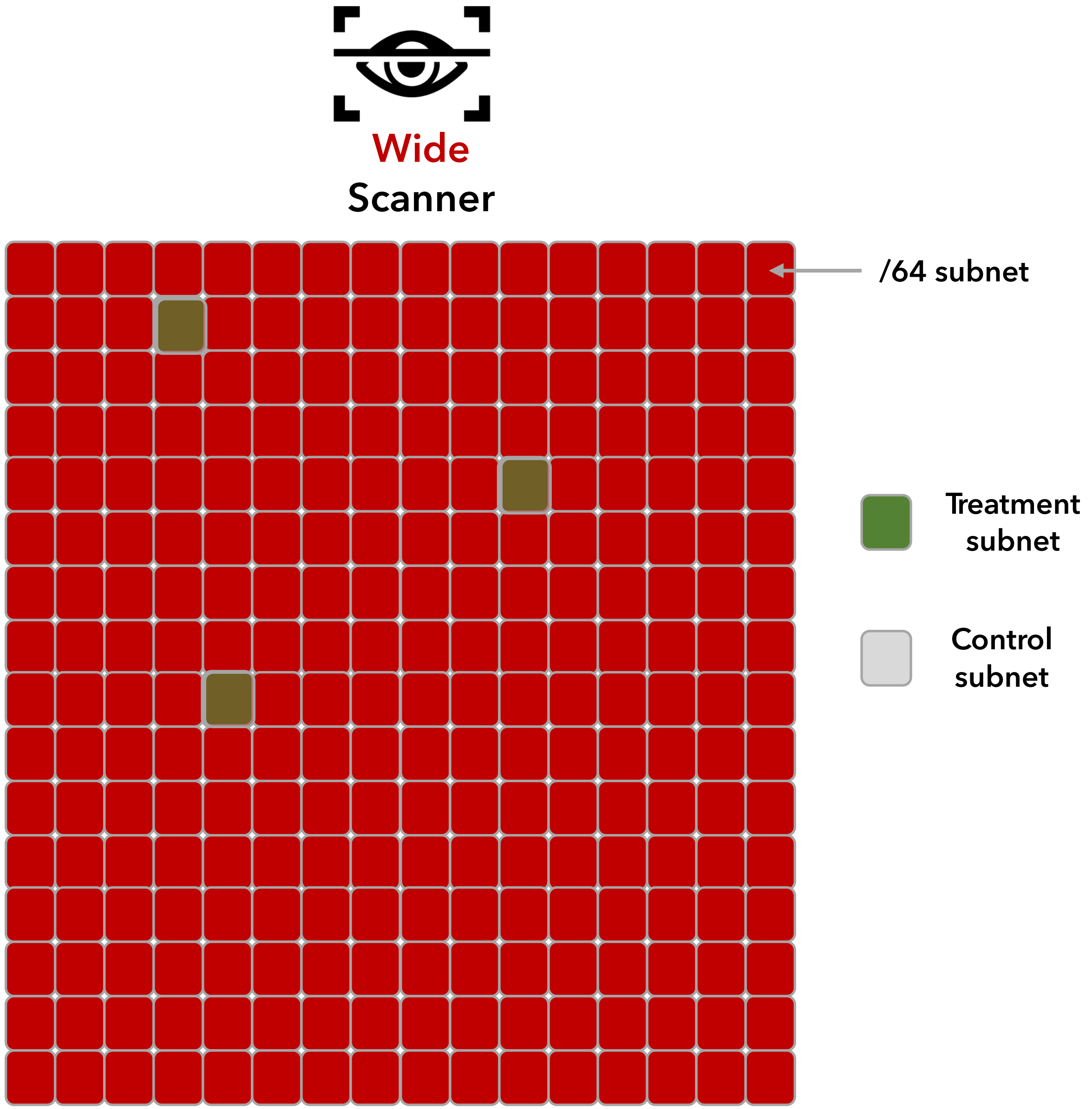


Results

Scanner strategies

Scanning strategies over time

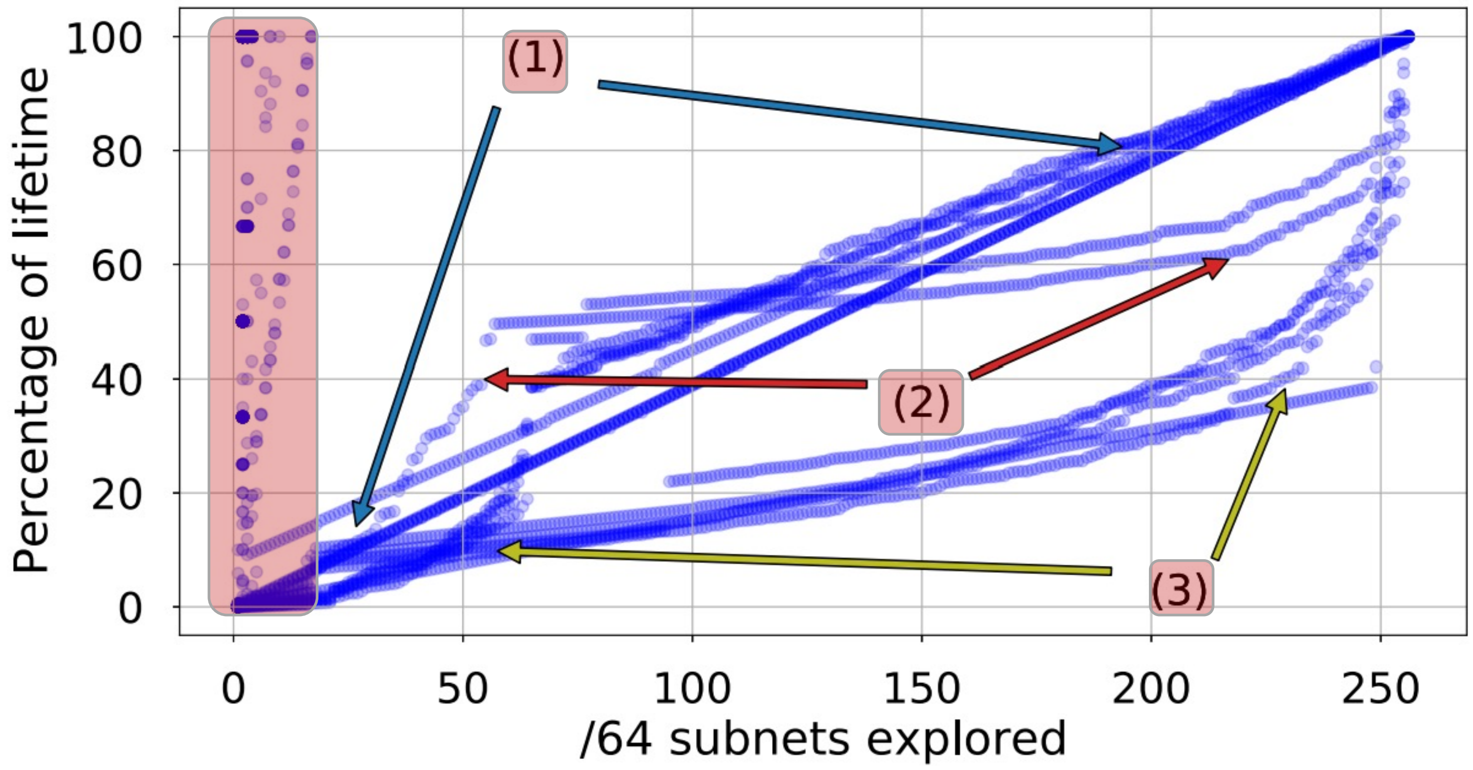




Results

Scanner strategies

Scanning strategies over time



We observe presence of both narrow and wide scanners

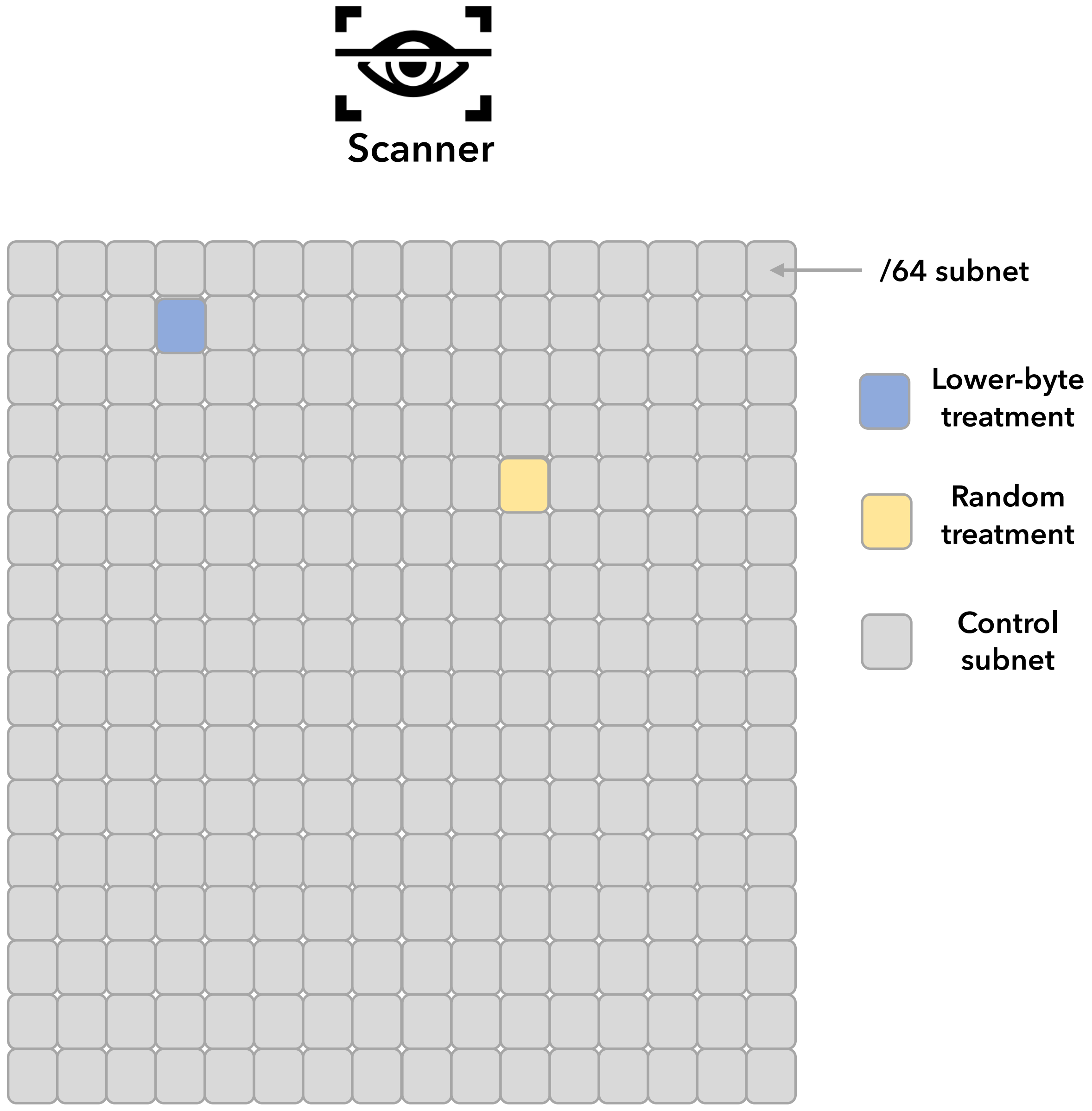
Results

Scanner strategies

Scanner preference by address type

2001:0DB8:AC10:FE01**:0000:0000:0000:0002**
Lower-byte address

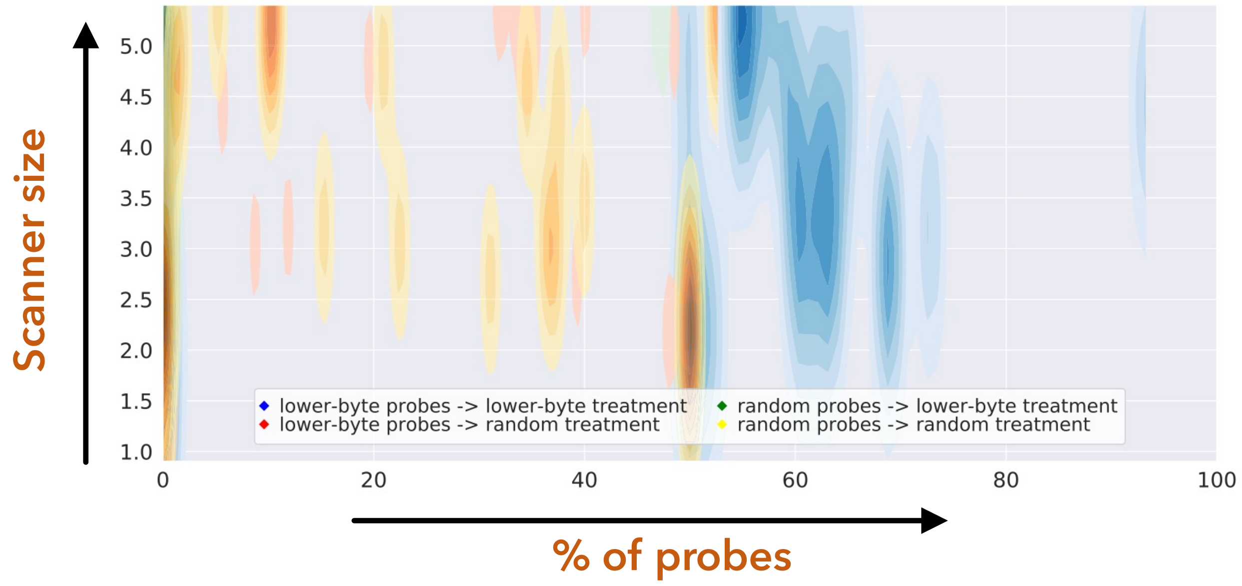
2001:0DB8:AC10:FE01**:3201:AC22:D654:98242**
Random-byte address

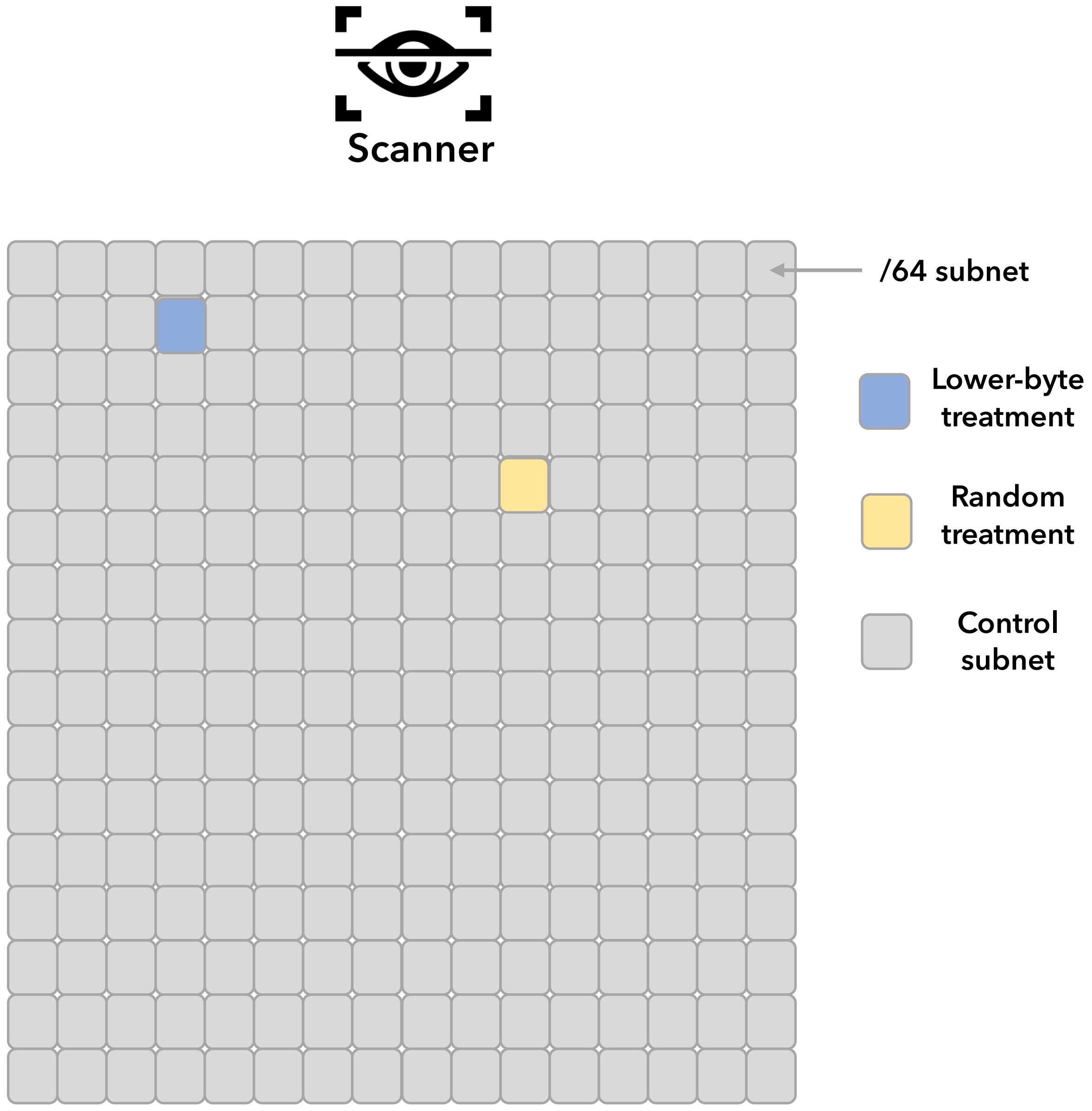


Results

Scanner strategies

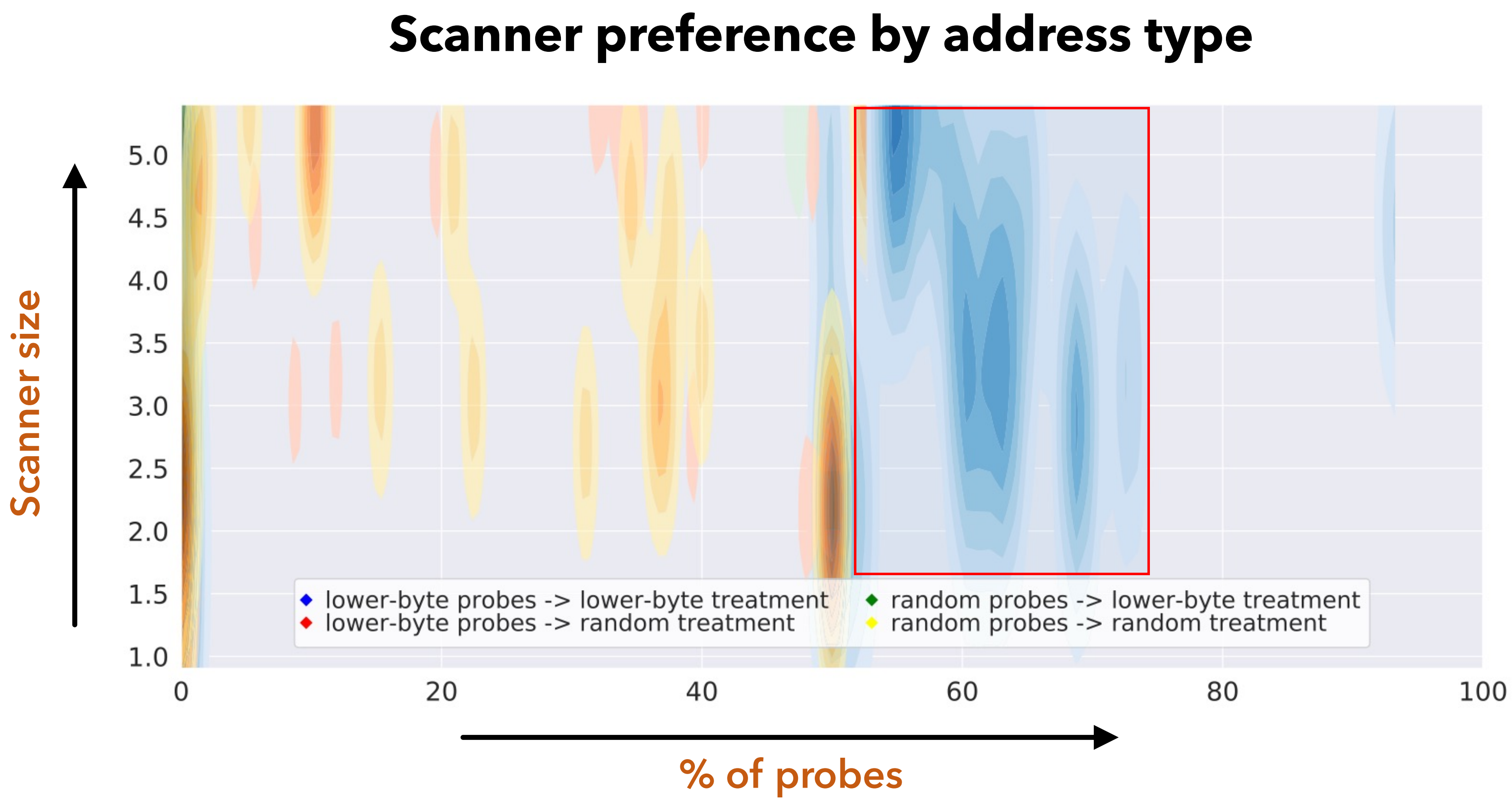
Scanner preference by address type





Results

Scanner strategies



Scanners of all sizes primarily target lower-byte treatment subnets

Scanners primarily send lower-byte scans regardless of subnet type

Security implications

for network operators

Lower-byte addresses receive 350,000x more traffic than random-byte addresses.
Use semantically opaque interface identifiers.

2001:0DB8:AC10:FE01:0000:0000:0000:0002
Lower-byte address

2001:0DB8:AC10:FE01:3201:AC22:D654:98242
Random-byte address

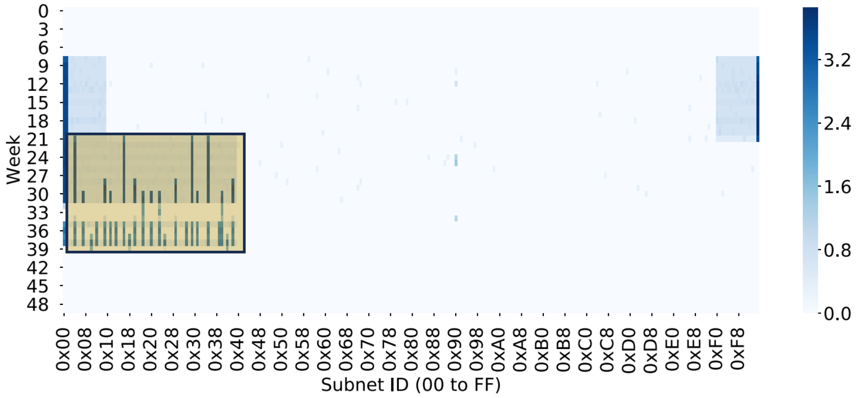
Security implications
for network operators

Lower-byte addresses receive 350,000x more traffic than random-byte addresses.
Use semantically opaque interface identifiers.

2001:0DB8:AC10:FE01:**0000:0000:0000:0002**
Lower-byte address

2001:0DB8:AC10:FE01:**3201:AC22:D654:98242**
Random-byte address

NXDOMAIN scanning can significantly reduce number of probes to identify an active address
Dynamically generate PTR records "on the fly"



Security implications

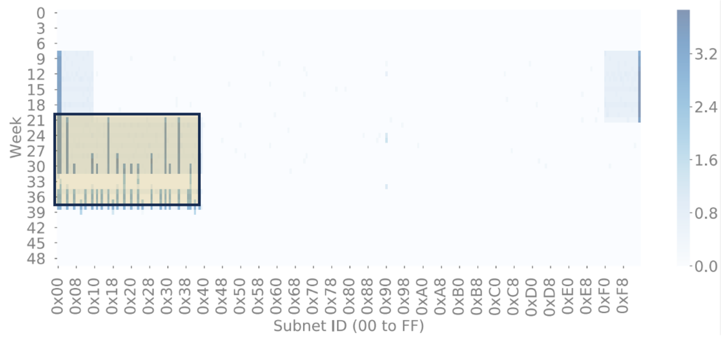
for network operators

Lower-byte addresses receive 350,000x more traffic than random-byte addresses.
Use semantically opaque interface identifiers.

2001:0DB8:AC10:FE01:**0000:0000:0000:0002**
Lower-byte address

2001:0DB8:AC10:FE01:**3201:AC22:D654:98242**
Random-byte address

NXDOMAIN scanning can significantly reduce number of probes to identify an active address
Dynamically generate PTR records "on the fly"



Most IPv6 scanners are reported on abuse databases
Using popular IP blocklists can preemptively stop network scanning

Conclusion

We develop a novel methodology to capture a more representative amount of scanning traffic in IPv6 networks

We uncover a set of diverse scanning strategies employed by IPv6 scanners

We present security recommendations for network operators to make IPv6 address spaces more secure against scanning

Conclusion

We develop a novel methodology to capture a more representative amount of scanning traffic in IPv6 networks

We uncover a set of diverse scanning strategies employed by IPv6 scanners

We present security recommendations for network operators to make IPv6 address spaces more secure against scanning

We also...

Present an in-depth analysis of DNS scanners and their strategies

Present an analysis of scanner characteristics, origins and payload analysis of scanning traffic

usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Glowing in the Dark: Uncovering IPv6 Address Discovery and Scanning Strategies in the Wild

Hammas Bin Tanveer, *The University of Iowa;* Rachee Singh, *Microsoft and Cornell University;* Paul Pearce, *Georgia Tech;* Rishab Nithyanand, *University of Iowa*

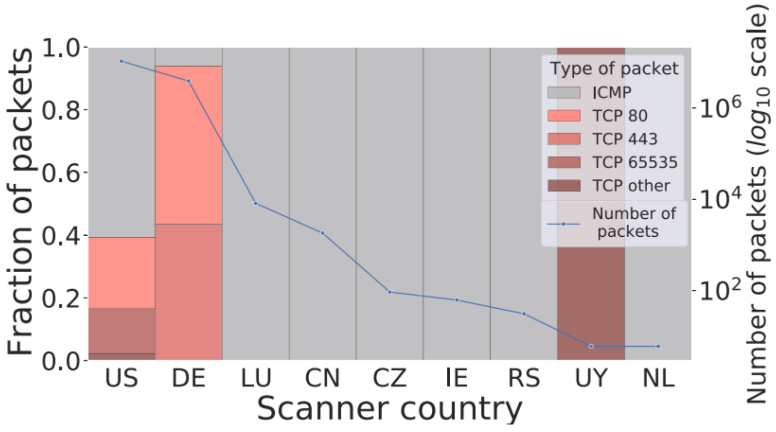
https://www.usenix.org/conference/usenixsecurity23/presentation/bin-tanveer

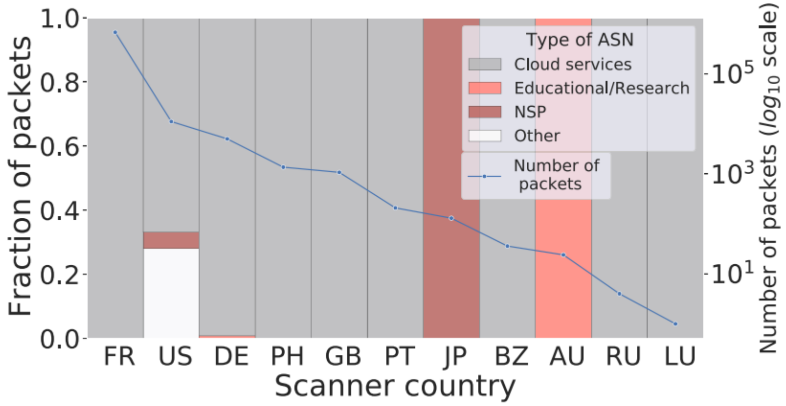
For all questions, comments and discussions
hammas-tanveer@uiowa.edu

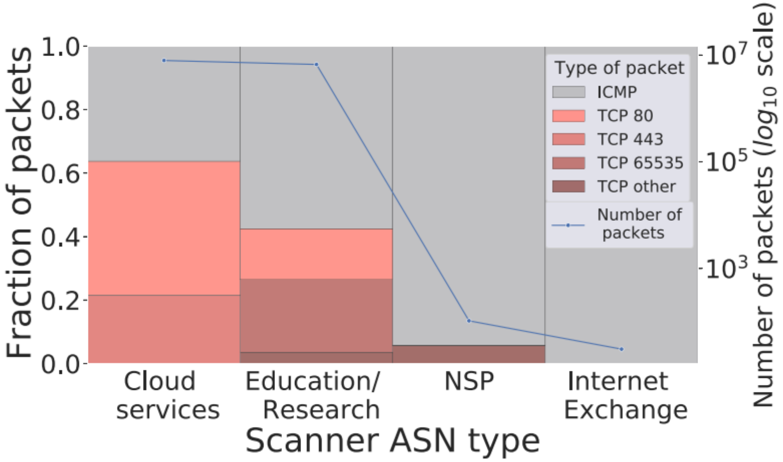
BACKUP SLIDES

Results
Scanner characteristics

Origins of scanning traffic are concentrated by geography and AS type



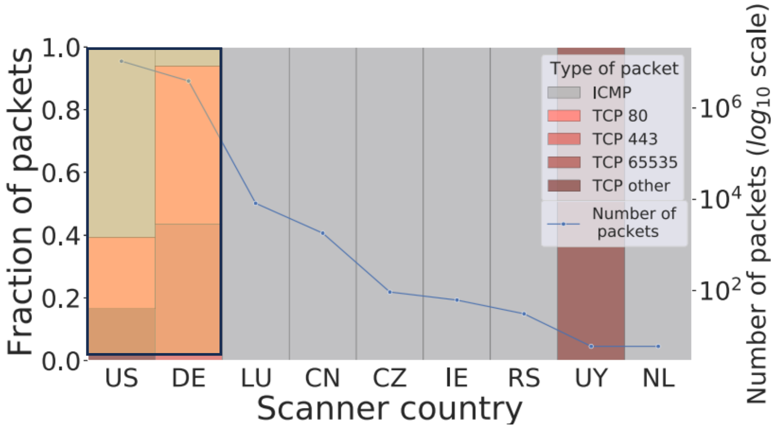


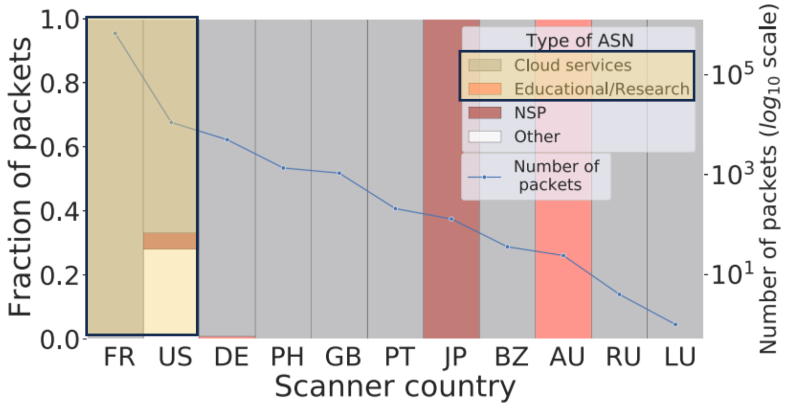


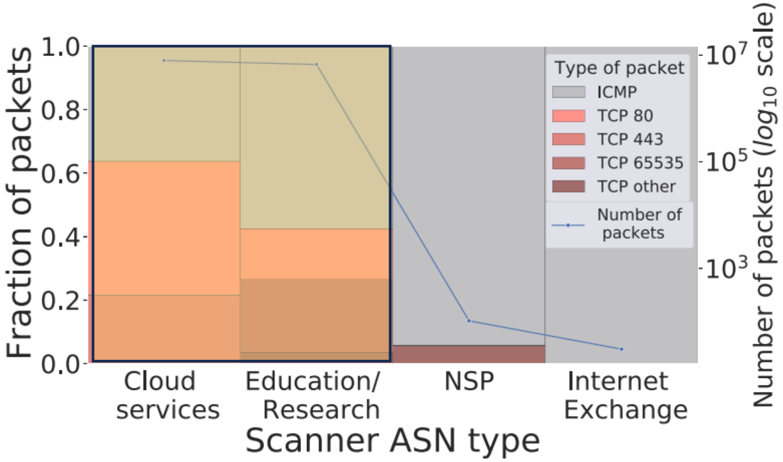
Results
Scanner characteristics

Origins of scanning traffic are concentrated by geography and AS type

99% of all traffic originates from 3 countries and 2 AS types.



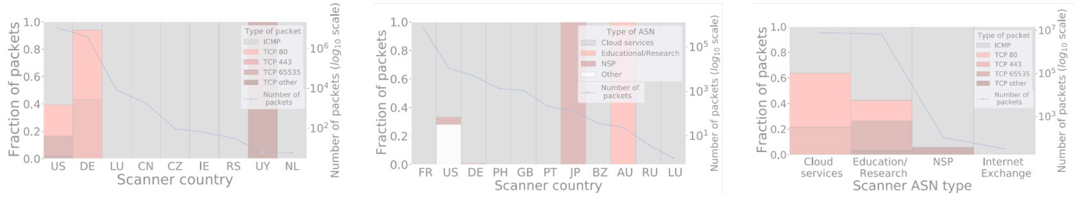




Results
Scanner characteristics

Origins of scanning traffic are concentrated by geography and AS type

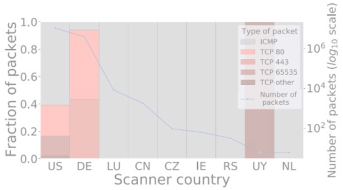
99% of all traffic originates from 3 countries and 2 AS types.

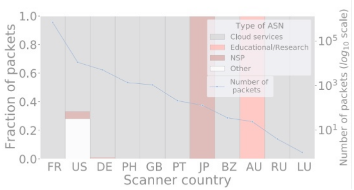


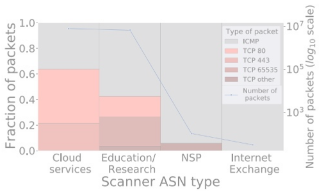
ICMPv6 is the most scanned protocol

2013	2018	2020	2022
ICMPv6	HTTP	HTTP	ICMPv6
TCP – 7	ICMPv6	ICMPv6	HTTP
HTTP	-	HTTPS	HTTPS
SSH	-	Redis	TCP – 65535
HTTPS	-	IRC	Telnet

Results
Scanner characteristics







Origins of scanning traffic are concentrated by geography and AS type

99% of all traffic originates from 3 countries and 2 AS types.

ICMPv6 is the most scanned protocol

54% of all scanning traffic consisted of ICMPv6 packets; temporal change in scanner's protocol preference

2013	2018	2020	2022
ICMPv6	HTTP	HTTP	ICMPv6
TCP - 7	ICMPv6	ICMPv6	HTTP
HTTP	-	HTTPS	HTTPS
SSH	-	Redis	TCP - 65535
HTTPS	-	IRC	Telnet

Results
Scanner characteristics

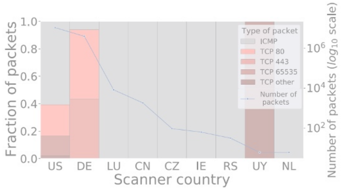
Origins of scanning traffic are concentrated by geography and AS type

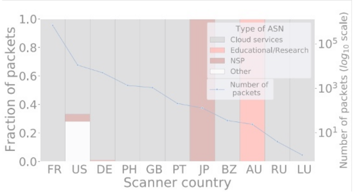
99% of all traffic originates from 3 countries and 2 AS types.

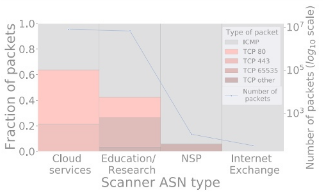
ICMPv6 is the most scanned protocol

54% of all scanning traffic consisted of ICMPv6 packets; temporal change in scanner's protocol preference

IPv6 scanners are reported on abuse databases







2013	2018	2020	2022
ICMPv6	HTTP	HTTP	ICMPv6
TCP – 7	ICMPv6	ICMPv6	HTTP
HTTP	-	HTTPS	HTTPS
SSH	-	Redis	TCP – 65535
HTTPS	-	IRC	Telnet

Results

Scanner characteristics

Origins of scanning traffic are concentrated by geography and AS type

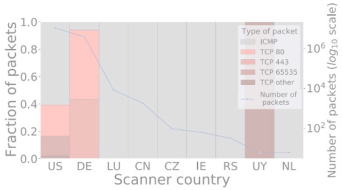
99% of all traffic originates from 3 countries and 2 AS types.

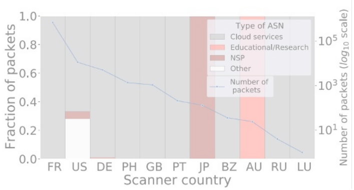
ICMPv6 is the most scanned protocol

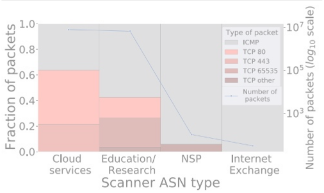
54% of all scanning traffic consisted of ICMPv6 packets; temporal change in scanner's protocol preference

IPv6 scanners are reported on abuse databases

Scanners responsible for 51% of scanning traffic were reported on AbuseIPDB.



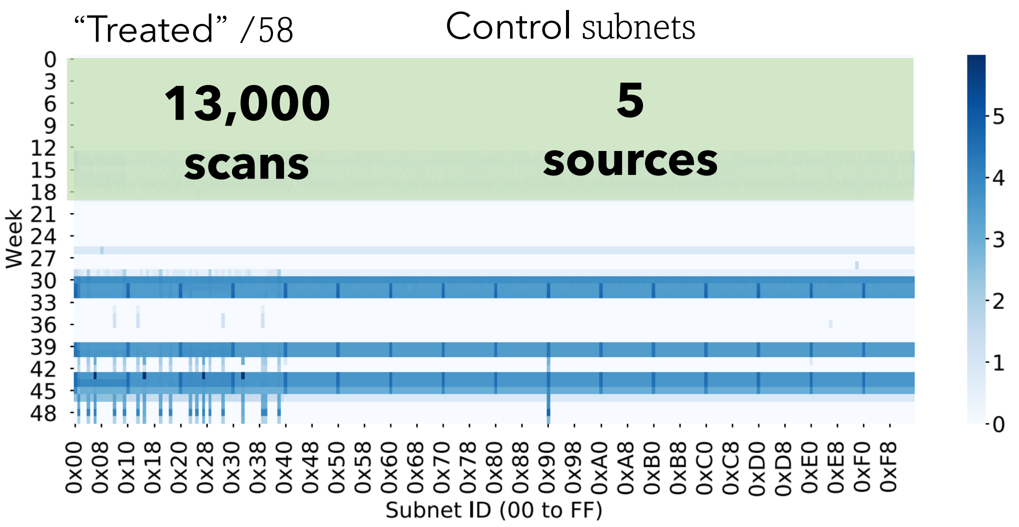




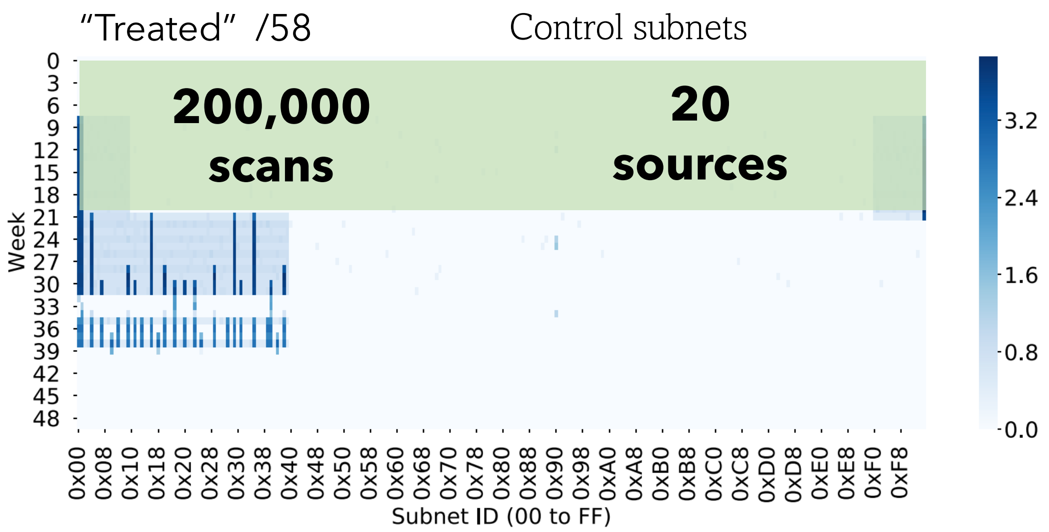
2013	2018	2020	2022
ICMPv6	HTTP	HTTP	ICMPv6
TCP – 7	ICMPv6	ICMPv6	HTTP
HTTP	-	HTTPS	HTTPS
SSH	-	Redis	TCP – 65535
HTTPS	-	IRC	Telnet

Results

Scanning activity **before** deployment of services



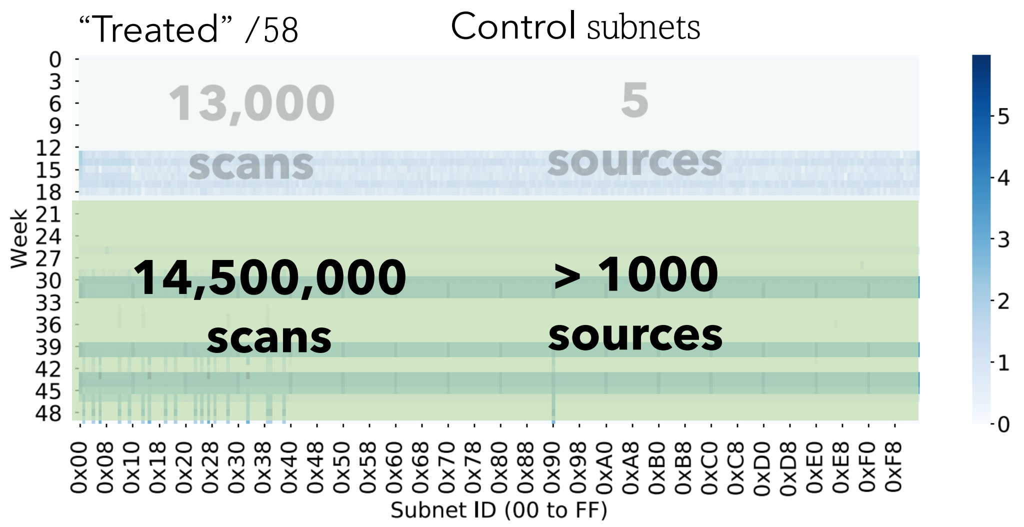
IP scanning



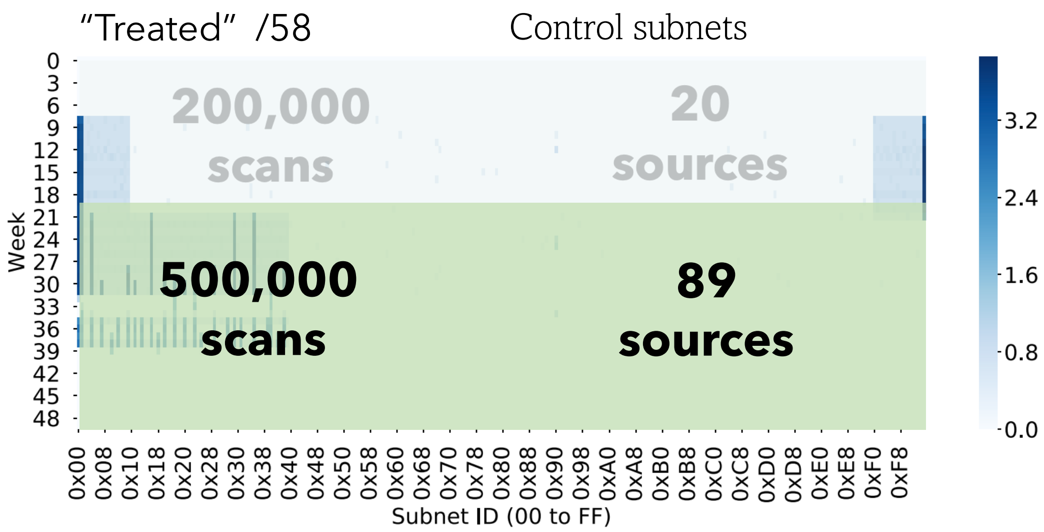
DNS scanning

Results

Scanning activity **after** deployment of services



IP scanning



DNS scanning