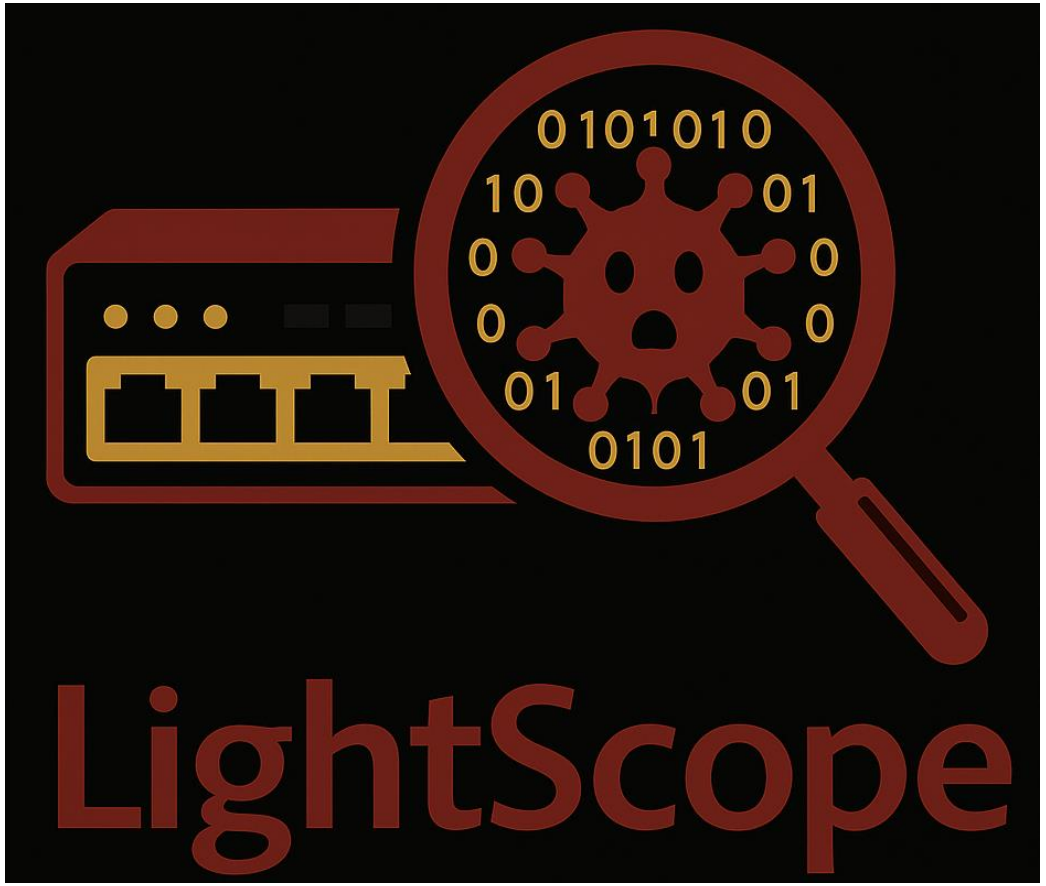
LightScope

LACNIC 45 -- 2026

Eric Kapitanski – kapitans@isi.edu

Advisor: Jelena Mirkovic



USC Viterbi
Information Sciences Institute

Why LightScope?

- Dark space for telescopes is shrinking
- LightScope provides new vantage points
  - LightScope leverages in-use IPs that attackers may know about
  - Full visibility L4 TCP scanning through L7 application interactions
- Complements dark space monitoring

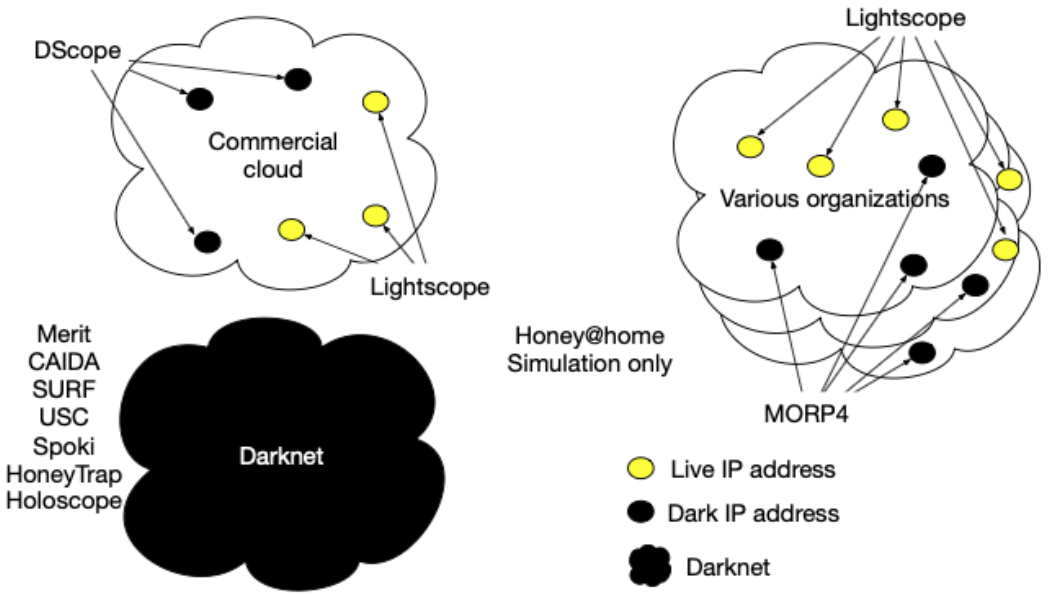
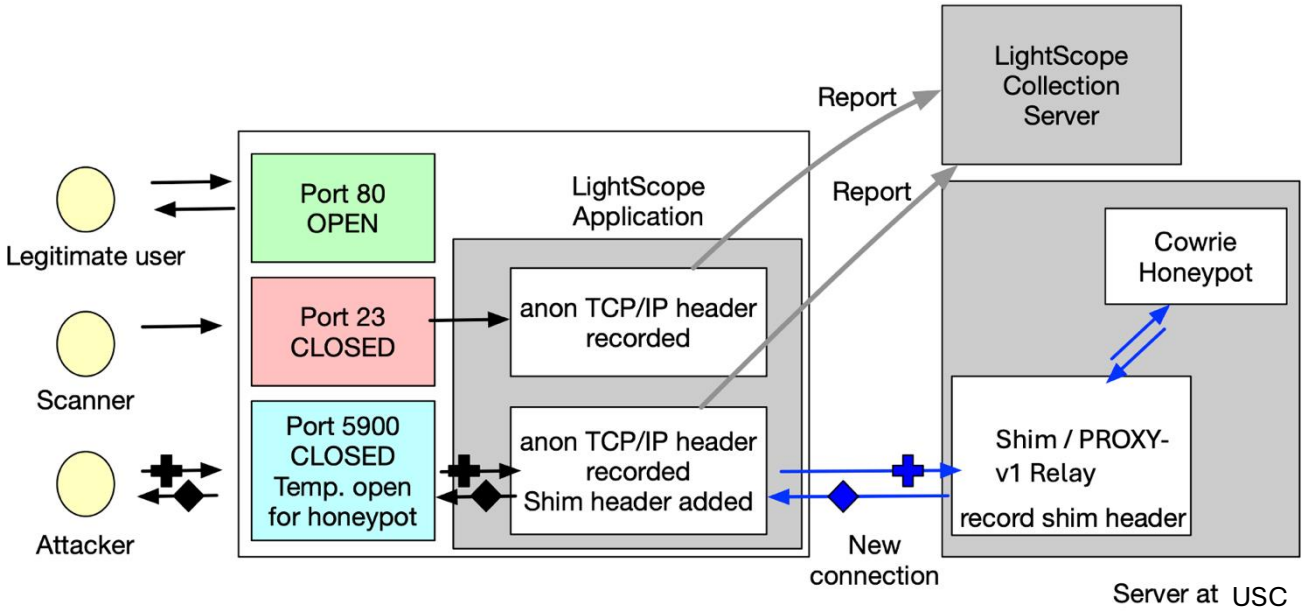


Figure 1: LightScope's deployment on live machines complements telescopes and honeynets located in dark spaces.

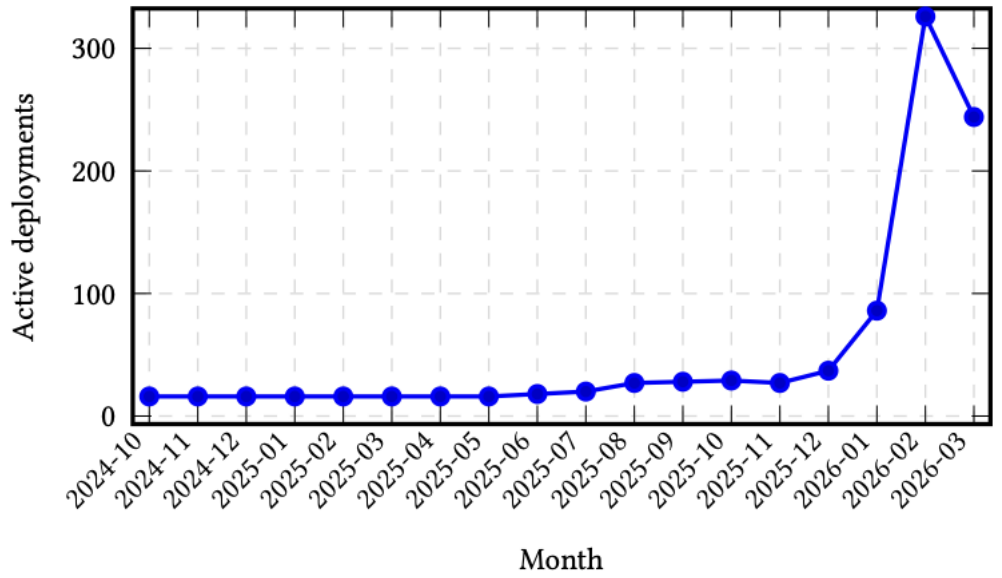
What is LightScope?

- LightScope leverages in-use IPs
  - Unused ports become telescopes/honeypots
    - Forwards to ISI honeypot
  - Anonymized adopter IP
    - Passed IRB
- Extremely lightweight
  - Over 295 NRP.Ai nodes, median 7.5% of a single core / 191 MB
- Limitations
  - TCP syn only
    - Keep resource utilization low
    - No UDP or backscatter



Current Deployment

- 27 domains
- 243 endpoints not behind a firewall or NAT

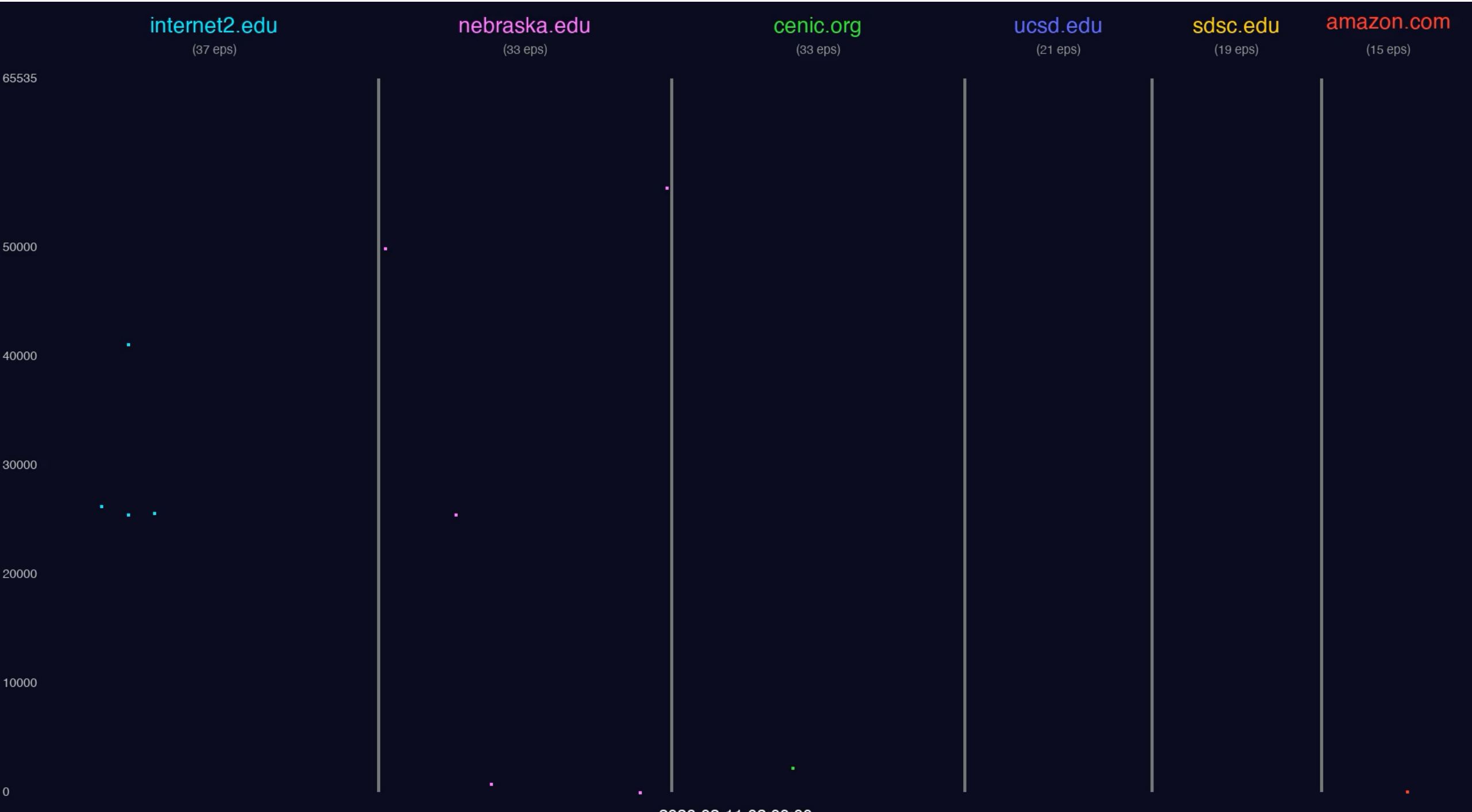


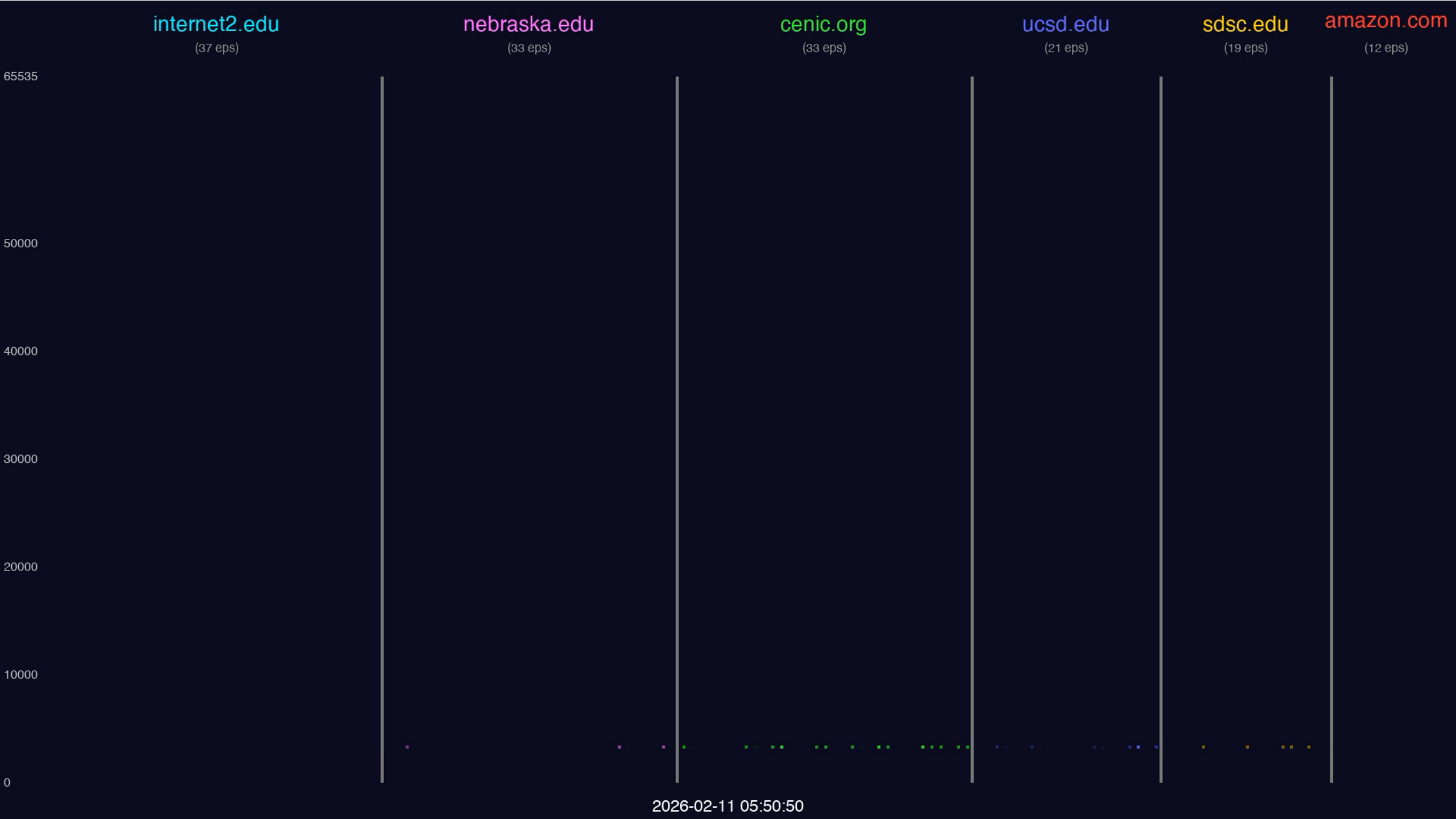
Domain	Endpoints	Domain	Endpoints
ucsd.edu	57	garr.it	1
internet2.edu	46	ionos.com	1
sdsc.edu	35	metronet.cz	1
nebraska.edu	28	ministryofcompute.com	1
amazon.com	15	nd.edu	1
Private	8	purevoltage.com	1
dfn.de	3	rg.net	1
fiu.edu	2	servarica.com	1
linode.com	2	solcon.nl	1
surf.nl	2	telekom.de	1
belnet.be	1	tpgtelecom.com.au	1
cesnet.cz	1	verizonbusiness.com	1
constant.com	1	No data	29
csc.fi	1		

AS Type ($n = 6$)	
education	206
hosting	22
isp	5
private deployment	8
government	1
unknown	1

Ext. Dst. IP Country ($n = 20$)					
US	213	AE	1	IE	1
DE	6	AU	1	IN	1
NL	3	BE	1	IT	1
CA	2	BH	1	JP	1
CZ	2	FI	1	NZ	1
GB	2	FR	1	SG	1
RO	2	HK	1		

Table 2: Breakdown of LightScope endpoints by network type (left) and geolocation (right)


internet2.edu
(37 eps)
nebraska.edu
(33 eps)
cenic.org
(33 eps)
ucsd.edu
(21 eps)
sdsc.edu
(19 eps)
amazon.com
(15 eps)
65535
50000
40000
30000
20000
10000
0

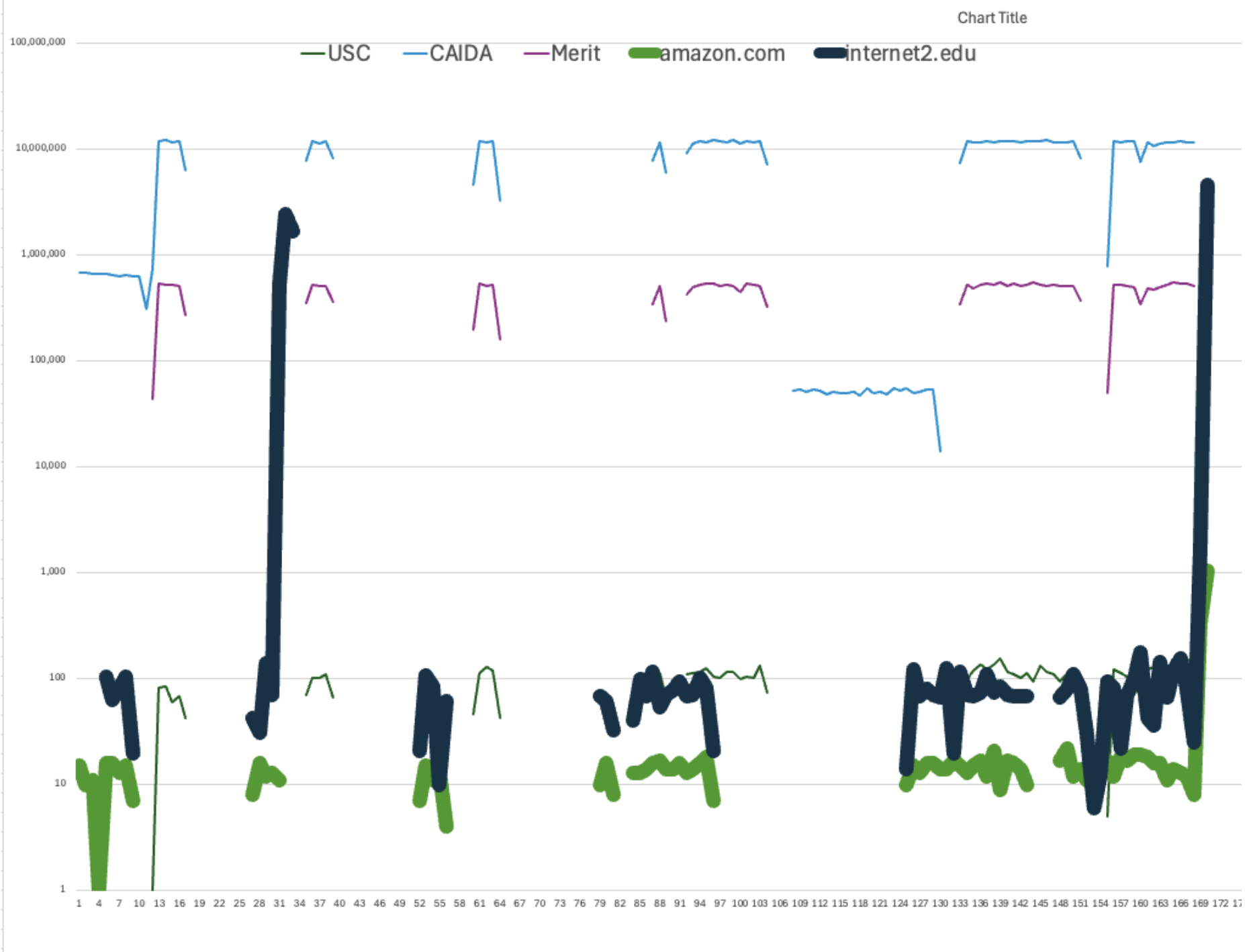

internet2.edu
(37 eps)
nebraska.edu
(33 eps)
cenic.org
(33 eps)
ucsd.edu
(21 eps)
sdsc.edu
(19 eps)
amazon.com
(12 eps)
65535
50000
40000
30000
20000
10000
0
2026-02-11 05:50:50

Scanner:
78.128.114.126

Mainly port
3389 RDP

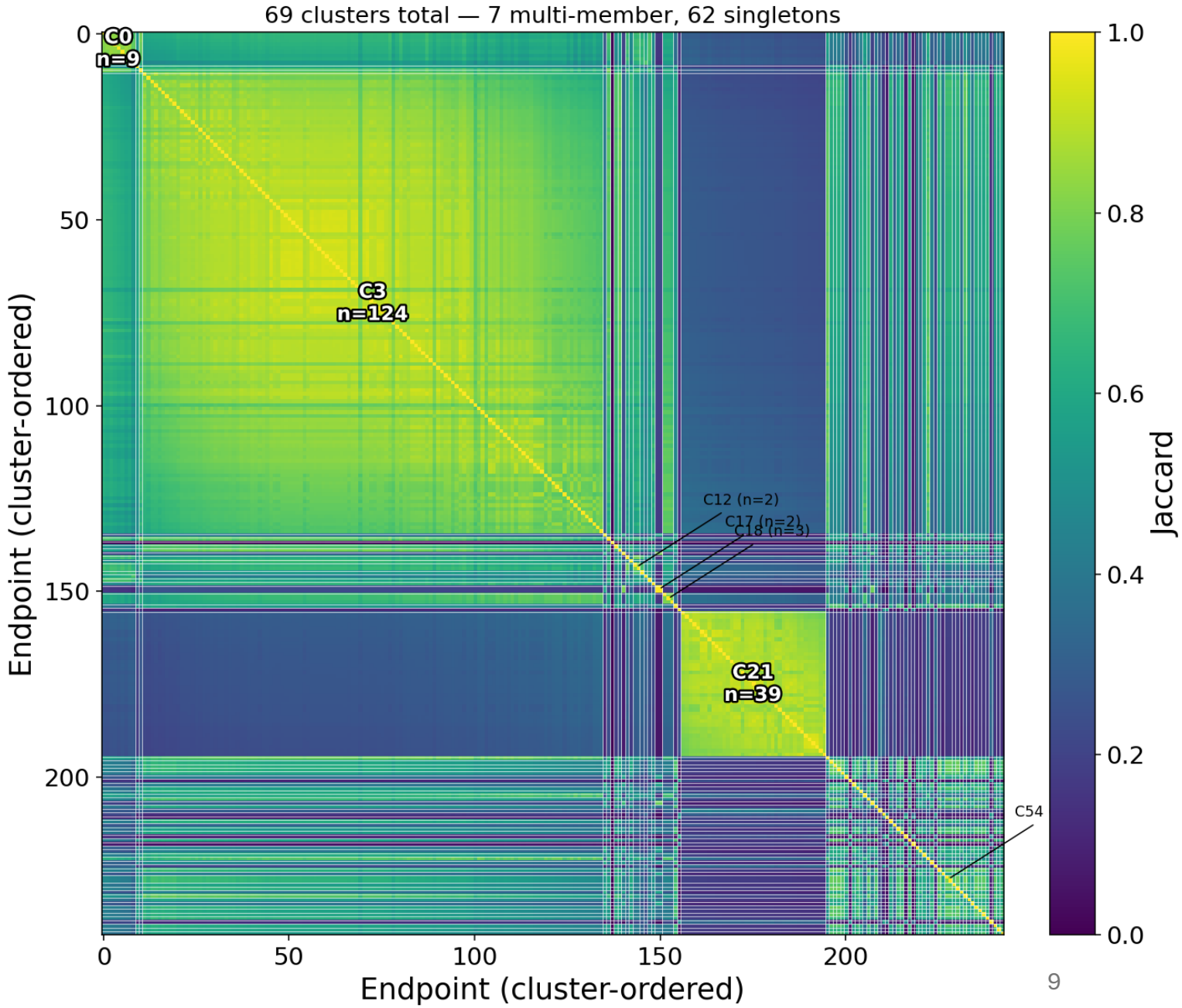
Never
Completes
3-way
handshake




Chart Title
USC
CAIDA
Merit
amazon.com
internet2.edu
100,000,000
10,000,000
1,000,000
100,000
10,000
1,000
100
10
1
1 4 7 10 13 16 19 22 25 28 31 34 37 40 43 46 49 52 55 58 61 64 67 70 73 76 79 82 85 88 91 94 97 100 103 106 109 112 115 118 121 124 127 130 133 136 139 142 145 148 151 154 157 160 163 166 169 172

Endpoint Port Scan Similarity

- Some endpoints on different domains are scanned similarly
- Jaccard similarity
  - J=1: same ports, J=0: totally different
- Overlap of sets of TCP ports scanned
  - Clusters J> 0.8
- **Cluster 3**
  - 20 different domains
  - Broad scanners
- **Cluster 21**
  - 1 domain, UCSD.edu
  - Targeted scanning



LightScope, Telescopes, and Honeynets

Table 5: Port-based Jaccard index between vantage points, restricted to the source IPs that probed LS (LightScope) and each of the six comparison sources.

	LS	Merit	SURF	USC	Spoki	HoneyTrap	Columbia
LS	—	0.07	0.07	0.08	0.05	0.00	0.09
Merit	0.07	—	**1.00**	**0.98**	0.09	0.05	0.24
SURF	0.07	**1.00**	—	**0.98**	0.10	0.05	0.25
USC	0.08	**0.98**	**0.98**	—	0.10	0.05	0.26
Spoki	0.05	0.09	0.10	0.10	—	0.04	0.11
HoneyTrap	0.00	0.05	0.05	0.05	0.04	—	0.07
Columbia	0.09	0.24	0.25	0.26	0.11	0.07	—

Passive telescopes

reactive

honeypot

residential

LightScope sees unique port scan combinations

Exclusive IPs

LightScope sees exclusive scanner IPs

Table 6: Scanner-IP exclusivity across seven vantage points and LightScope. *Exclusive* IPs were observed by only this source during our observation period

	Source	Endpoints	Exclusive	% Excl.	Excl./EP
	LightScope	243	70,371	8.9 %	189.7
passive telescopes	CAIDA	16,777,216	13,907,690	68.4 %	0.83
	Merit	475,904	4,246,069	45.7 %	8.9
	SURF	768	12,854	1.5 %	16.7
	USC	17,408	66,765	3.2 %	3.8
reactive	Spoki	256	1,277,833	37.9 %	4,991.5
honeynet	HoneyTrap	98	44,248	7.5 %	451.5
residential	Columbia	1,810	211,725	18.6 %	117.0

Commercial Threat Intelligence Platforms

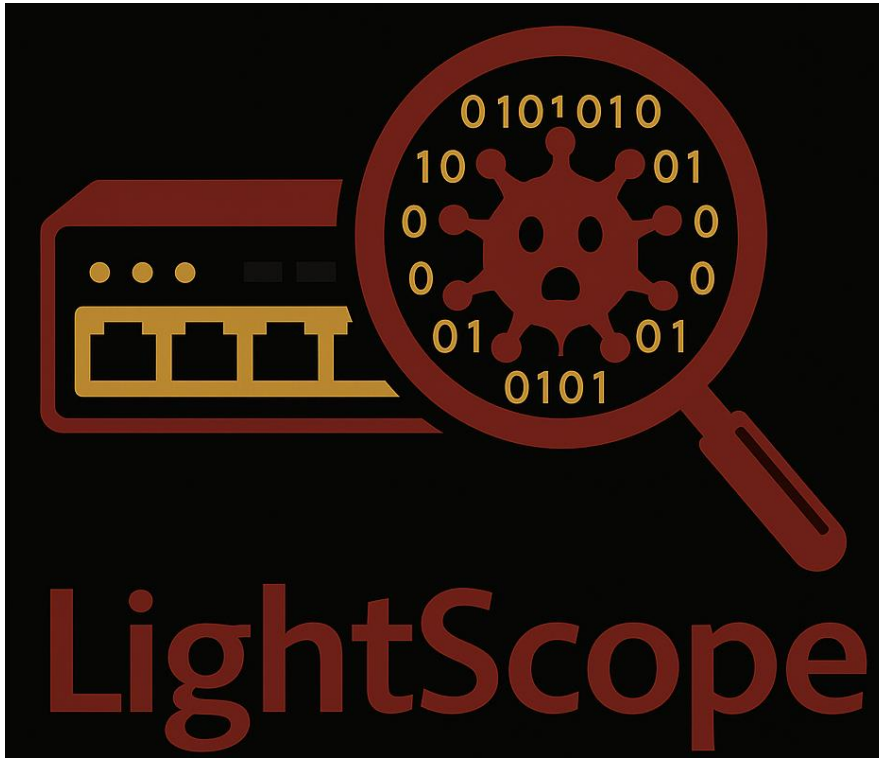
- LightScope observed 13,667 IPs logging into honeypot ports and running commands
- GreyNoise classified 74% as malicious
- AbuseIPDB recommended blocking 58%

Source	Category	IPs	% of total
GreyNoise coverage and classifications			
GreyNoise	Observed	13,609	99.6%
GreyNoise	No record	58	0.4%
GreyNoise	Malicious	10,175	74.4%
GreyNoise	Suspicious	3,067	22.4%
GreyNoise	Unknown	361	2.6%
GreyNoise	Benign	6	< 0.1%
GreyNoise	Not classified as malicious	3,492	25.6%
AbuseIPDB coverage and abuse confidence scores			
AbuseIPDB	Returned score	13,667	100.0%
AbuseIPDB	Reported malicious activity, score > 0	13,400	98.0%
AbuseIPDB	No reported malicious activity, score = 0	267	2.0%
AbuseIPDB	Score 1–24	977	7.1%
AbuseIPDB	Score 25–74	4,458	32.6%
AbuseIPDB	Score ≥ 75	7,965	58.3%
AbuseIPDB	Score 100, subset of score ≥ 75	7,030	51.4%
AbuseIPDB	Score < 75, below recommended block threshold	5,702	41.7%

Conclusion

- Closed ports on live production hosts are a useful new measurement vantage point

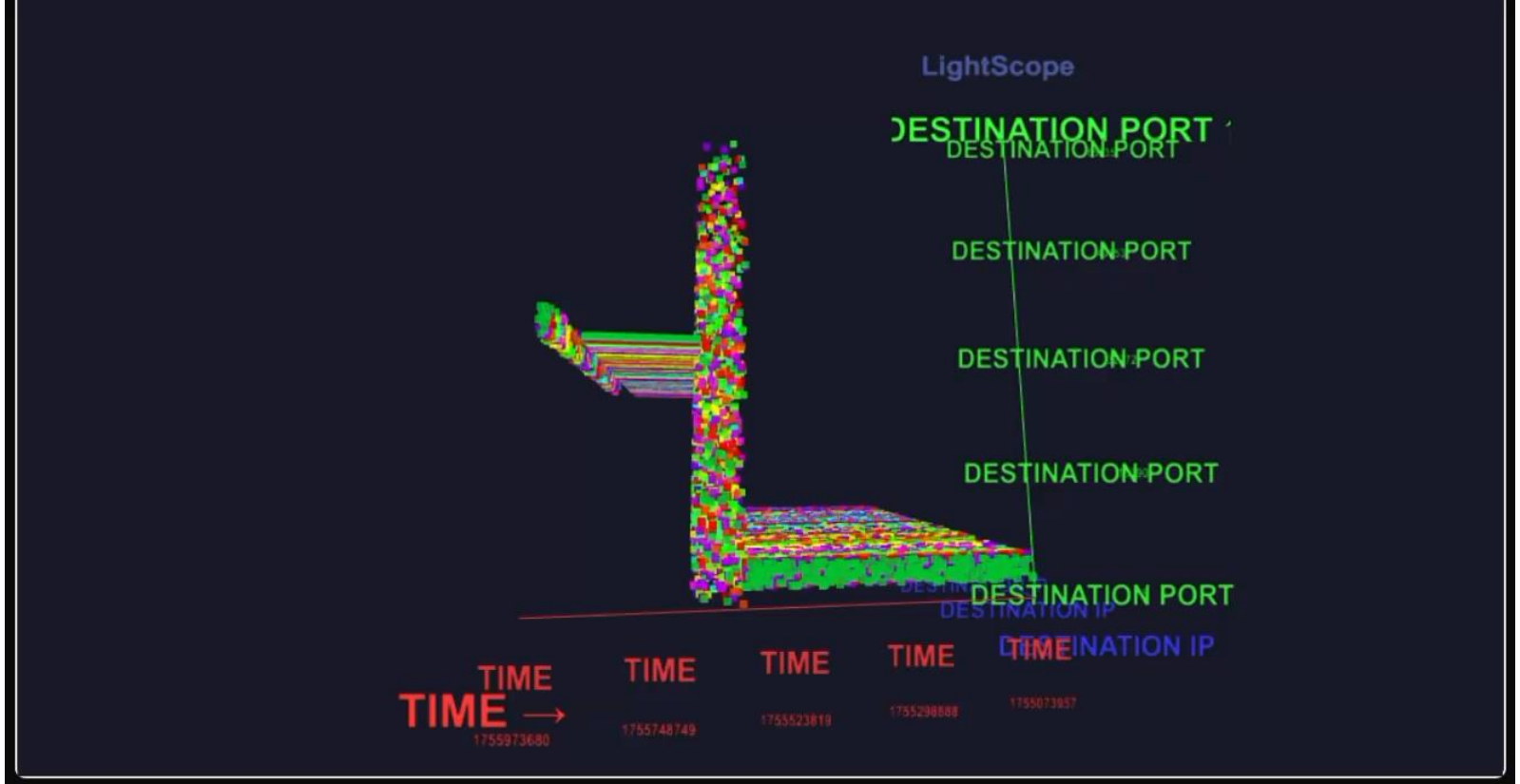
- www.lightscope.isi.edu
- Email: kapitans@isi.edu

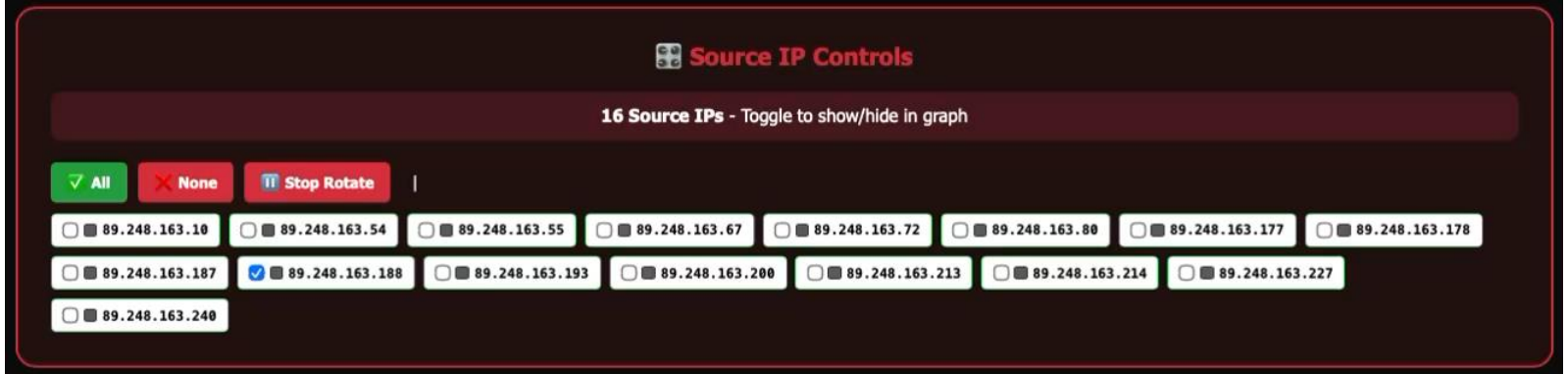


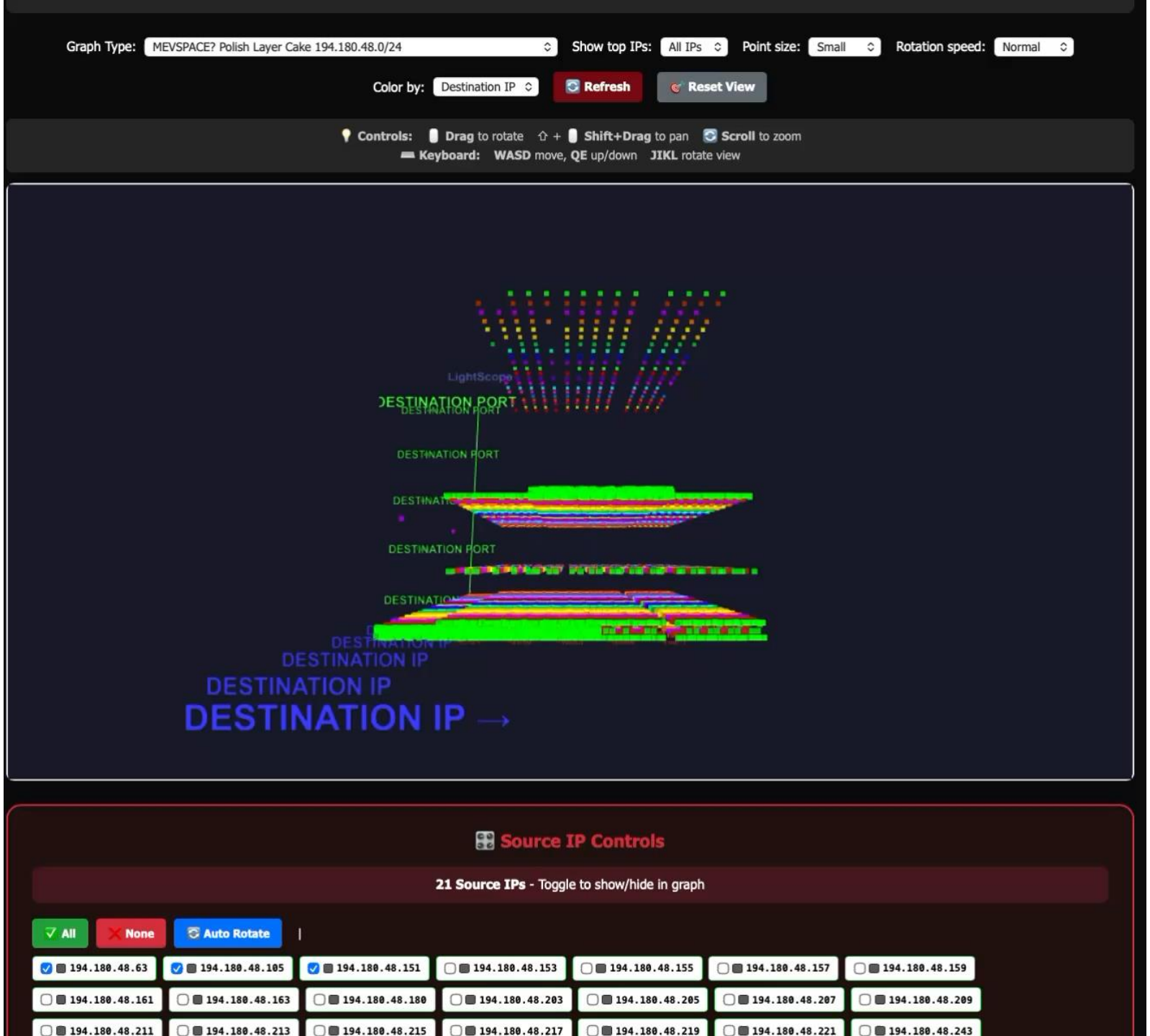
Backup Slides

Future Work

- De-sharding large-scale scanning campaigns based on behavior and temporal analysis

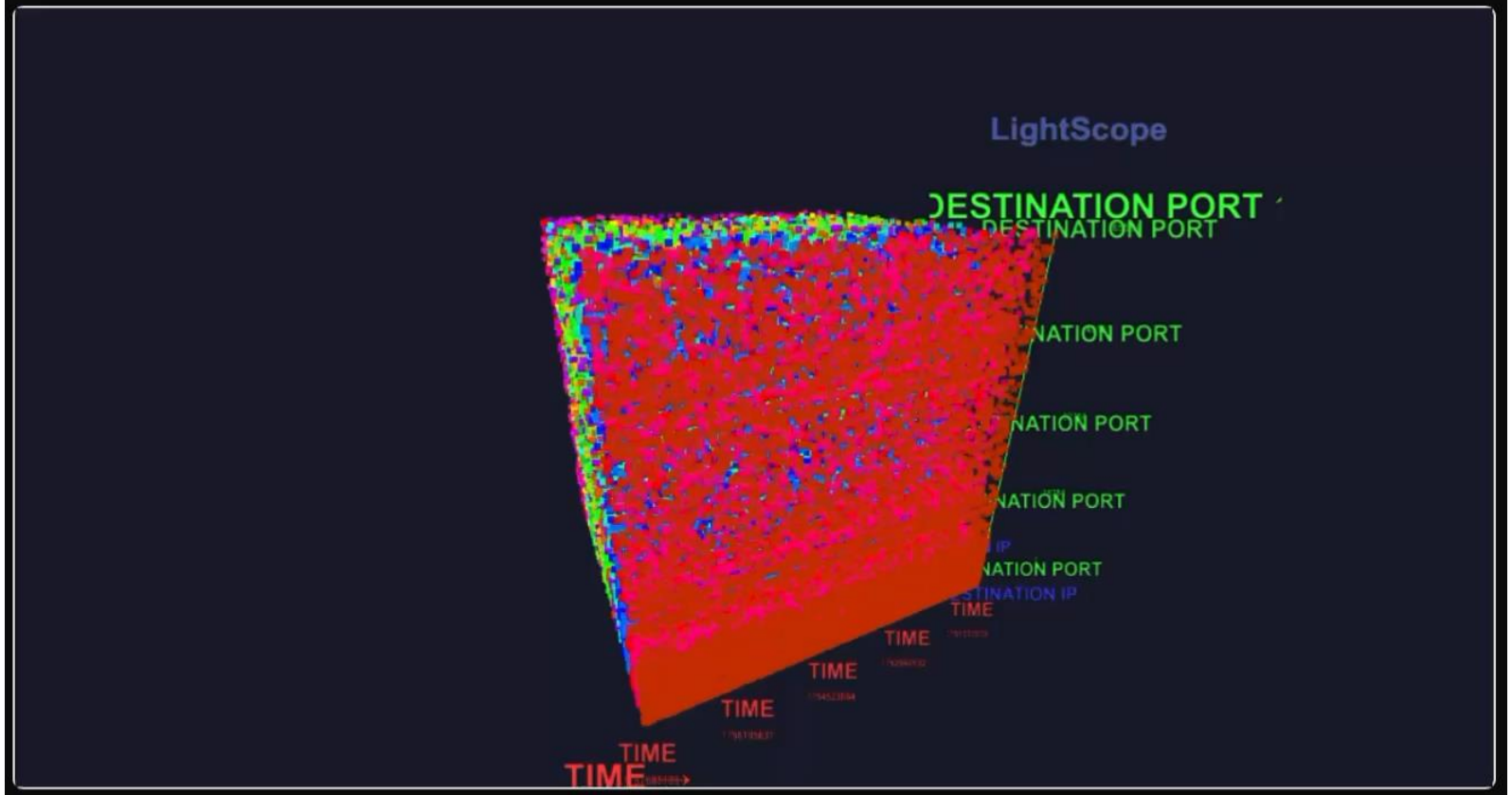

LightScope
DESTINATION PORT
DESTINATION PORT
DESTINATION PORT
DESTINATION PORT
DESTINATION PORT
DESTINATION IP
TIME
TIME
TIME
TIME
TIME
TIME
1755973680
1755748749
1755523819
1755298888
1755073957


Source IP Controls
16 Source IPs - Toggle to show/hide in graph
All
None
Stop Rotate
89.248.163.10
89.248.163.54
89.248.163.55
89.248.163.67
89.248.163.72
89.248.163.80
89.248.163.177
89.248.163.178
89.248.163.187
89.248.163.188
89.248.163.193
89.248.163.200
89.248.163.213
89.248.163.214
89.248.163.227
89.248.163.240


Graph Type: MEVSPACE? Polish Layer Cake 194.180.48.0/24
Show top IPs: All IPs
Point size: Small
Rotation speed: Normal
Color by: Destination IP
Refresh
Reset View
Controls: Drag to rotate + Shift+Drag to pan Scroll to zoom
Keyboard: WASD move, QE up/down JIKL rotate view
LightScope
DESTINATION PORT
DESTINATION PORT
DESTINATION PORT
DESTINATION PORT
DESTINATION IP
DESTINATION IP
DESTINATION IP
Source IP Controls
21 Source IPs - Toggle to show/hide in graph
All
None
Auto Rotate
194.180.48.63
194.180.48.105
194.180.48.151
194.180.48.153
194.180.48.155
194.180.48.157
194.180.48.159
194.180.48.161
194.180.48.163
194.180.48.180
194.180.48.203
194.180.48.205
194.180.48.207
194.180.48.209
194.180.48.211
194.180.48.213
194.180.48.215
194.180.48.217
194.180.48.219
194.180.48.221
194.180.48.243

Controls: Drag to rotate ⇧ + Shift+Drag to pan Scroll to zoom

Keyboard: WASD move, QE up/down JIKL rotate view

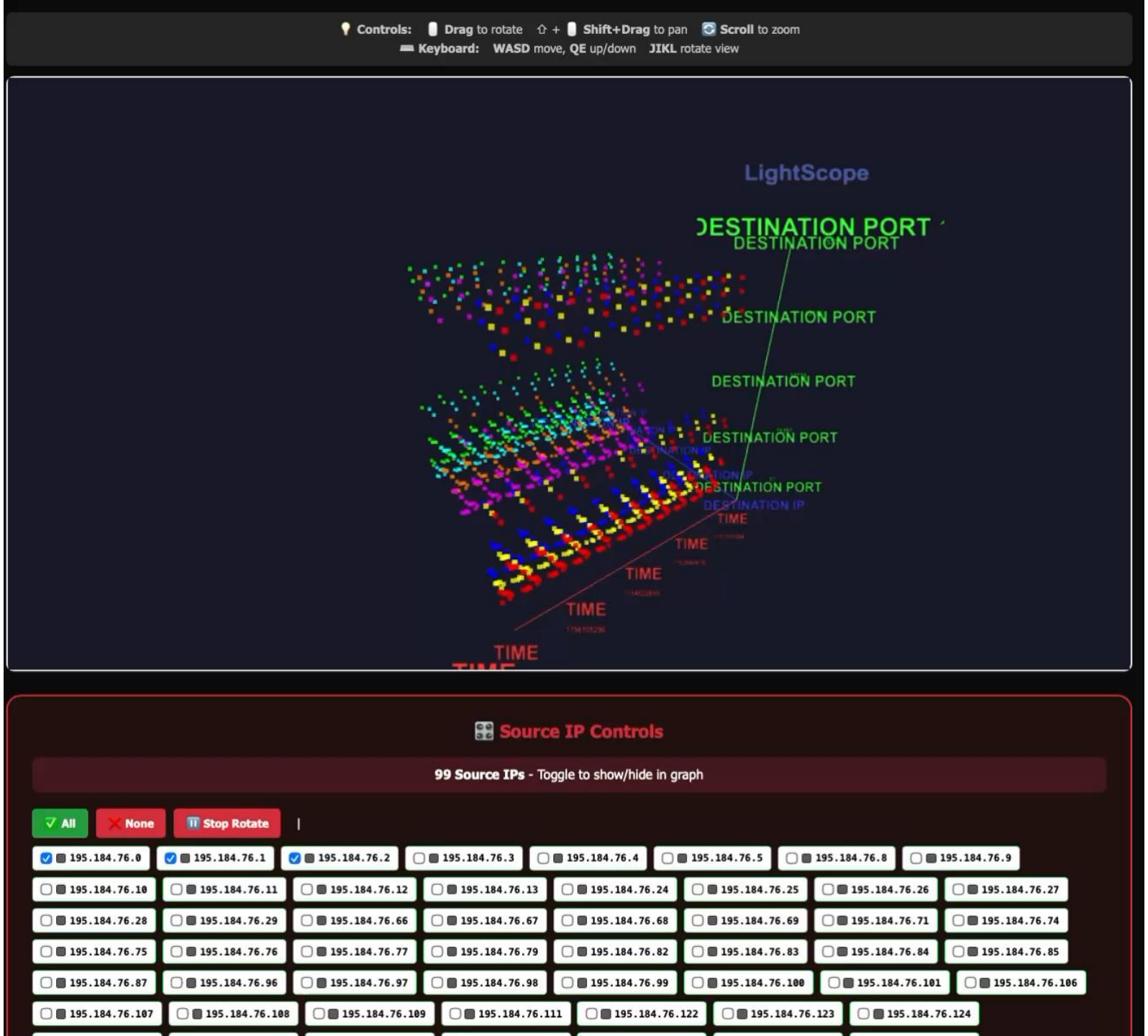


Source IP Controls

48 Source IPs - Toggle to show/hide in graph

All None Stop Rotate |

167.94.138.96	167.94.138.97	167.94.138.98	167.94.138.99	167.94.138.100	167.94.138.101	167.94.138.102	167.94.138.103
167.94.138.104	167.94.138.105	167.94.138.106	167.94.138.107	167.94.138.108	167.94.138.109	167.94.138.110	
167.94.138.111	167.94.138.128	167.94.138.129	167.94.138.130	167.94.138.131	167.94.138.132	167.94.138.133	
167.94.138.134	167.94.138.135	167.94.138.136	167.94.138.137	167.94.138.138	167.94.138.139	167.94.138.140	
167.94.138.141	167.94.138.142	167.94.138.143	167.94.138.144	167.94.138.145	167.94.138.146	167.94.138.147	
167.94.138.148	167.94.138.149	167.94.138.150	167.94.138.151	167.94.138.152	167.94.138.153	167.94.138.154	
167.94.138.155	167.94.138.156	167.94.138.157	167.94.138.158	167.94.138.159			


Controls: Drag to rotate ⇧ + Shift+Drag to pan Scroll to zoom
Keyboard: WASD move, QE up/down JIKL rotate view
LightScope
DESTINATION PORT
DESTINATION PORT
DESTINATION PORT
DESTINATION PORT
DESTINATION PORT
DESTINATION IP
TIME
TIME
TIME
TIME
TIME
Source IP Controls
99 Source IPs - Toggle to show/hide in graph
All
None
Stop Rotate
195.184.76.0
195.184.76.1
195.184.76.2
195.184.76.3
195.184.76.4
195.184.76.5
195.184.76.8
195.184.76.9
195.184.76.10
195.184.76.11
195.184.76.12
195.184.76.13
195.184.76.24
195.184.76.25
195.184.76.26
195.184.76.27
195.184.76.28
195.184.76.29
195.184.76.66
195.184.76.67
195.184.76.68
195.184.76.69
195.184.76.71
195.184.76.74
195.184.76.75
195.184.76.76
195.184.76.77
195.184.76.79
195.184.76.82
195.184.76.83
195.184.76.84
195.184.76.85
195.184.76.87
195.184.76.96
195.184.76.97
195.184.76.98
195.184.76.99
195.184.76.100
195.184.76.101
195.184.76.106
195.184.76.107
195.184.76.108
195.184.76.109
195.184.76.111
195.184.76.122
195.184.76.123
195.184.76.124

Multi-domain Attackers

Table 4: Telescope visibility for IPs reaching *at least* each depth.

≥ Depth	IPs	USC	Merit	SURF	Spoki	Columbia	HoneyTrap
TCP SYN only	749,965	70.6%	74.3%	60.7%	57.9%	53.3%	47.1%
Connect	147,710	70.5%	76.3%	65.4%	67.3%	62.4%	65.2%
Login attempt	52,737	55.8%	61.6%	48.9%	55.1%	54.0%	56.2%
Login success	19,317	20.1%	30.8%	14.7%	21.4%	36.7%	20.7%
Commands	13,667	13.6%	18.2%	9.0%	16.7%	40.2%	16.0%
File transfer	10,283	6.4%	11.1%	3.1%	5.2%	42.6%	4.1%

*Any telescope excluding CAIDA.

Scanners

Attackers

Exclusivity increases down the attack funnel

Metrics

- Measure how much our observations add to those from telescopes and honeynets
- Quantify visibility of different LightScope endpoints
- Leverage previously used metrics, such as:
  - Exclusivity: number/percentage of scanners seen in no other source
  - Jaccard-based similarity: how a given scanner scans ports on different vantage points (1 – identical ports, 0 – no overlapping ports)

Interdomain Endpoint Scanning Differences

- Endpoints, even on the same network, can be scanned differently

Domain	Endpoints	# pairs	min J	median J	max J
ucsd.edu	65	2,080	0.067	0.322	0.950
internet2.edu	47	1,081	0.181	0.603	0.922
nebraska.edu	39	741	0.148	0.883	0.944
sdsc.edu	38	703	0.038	0.834	0.936
amazon.com	14	91	0.616	0.746	0.942
private deployment	8	28	0.654	0.889	0.916
dfn.de	3	3	0.777	0.792	0.815
linode.com	2	1	0.418	0.418	0.418
fiu.edu	2	1	0.012	0.012	0.012
surf.nl	2	1	0.504	0.504	0.504

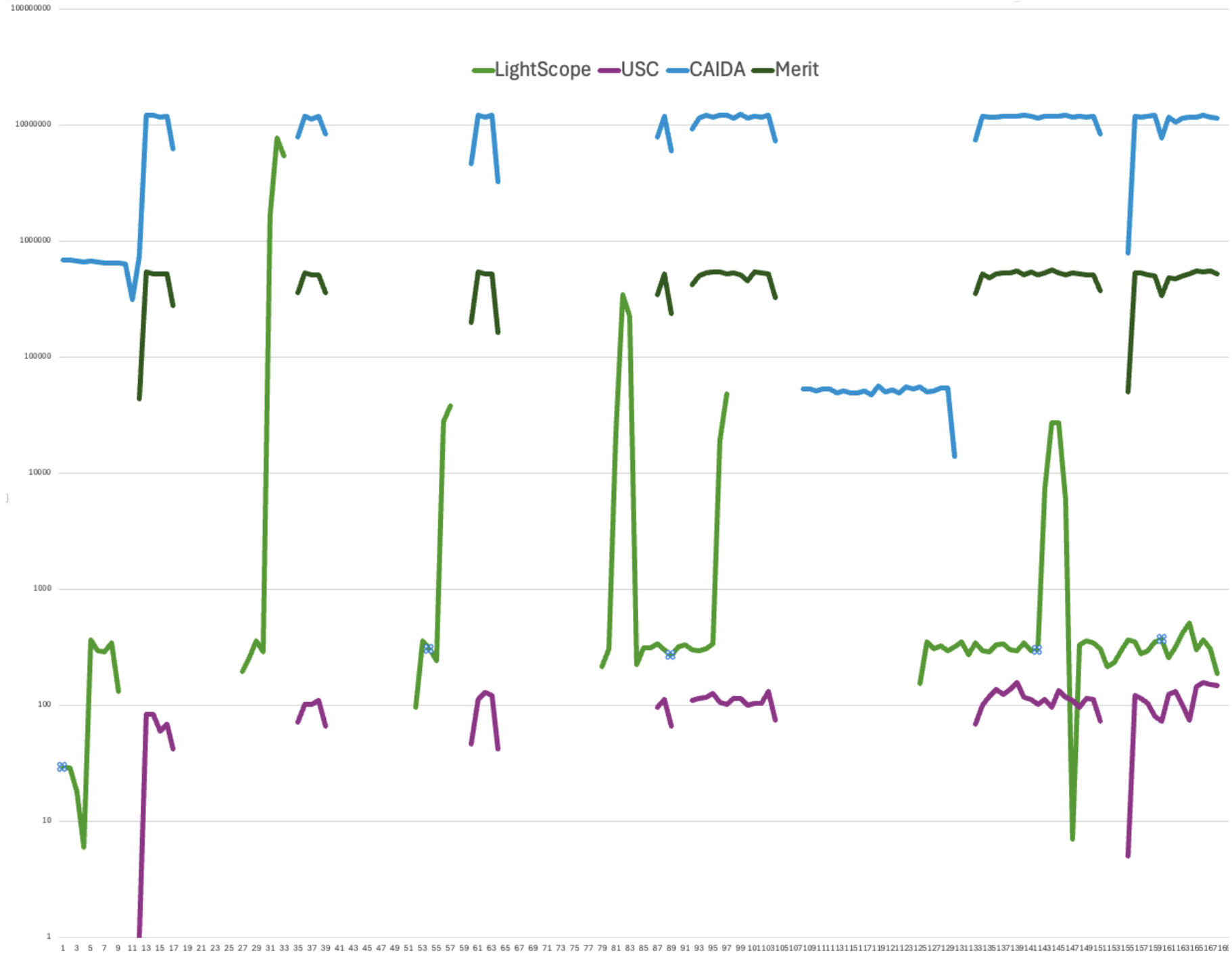
Table 9: Per-domain within-domain port-set Jaccard, restricted to domains with at least two endpoints in the 243-endpoint filter

Scanner Density

- Replicated from DScope (Pauley et al., USENIX Security 2023)
- $\overline{IP}$: mean number of unique scanners per endpoint per 10-min window
- σ_{IP} : standard deviation

Source	$\overline{IP}$	σ_{IP}
LightScope (overall)	**70.38**	**62.15**
USC /17	53.26	20.80
Merit	50.25	9.93
SURF	58.68	19.96
DScope (Pauley et al., 2023)		
DScope cloud (AWS)	69	27.1
Merit	40	13.9

LS domain	Endpoints	$\overline{IP}$	σ_{IP}
(unknown)	3	468.06	225.16
linode.com	2	133.22	26.26
ozarksgo.net	1	105.90	21.71
ionos.com	1	101.46	23.17
amazon.com	14	98.21	23.24
private deployment	8	92.69	21.06
gatech.edu	3	87.55	30.95
ministryofcompute.com	1	83.02	17.03
sdsc.edu	38	79.49	29.52
nd.edu	1	77.21	16.54
nebraska.edu	39	75.41	27.10
purevoltage.com	1	74.44	16.95
internet2.edu	45	73.49	20.72
rg.net	1	71.49	18.24
solcon.nl	1	66.89	27.13
servarica.com	1	66.85	16.12
csc.fi	1	66.70	11.24
telekom.de	1	63.88	25.06
metronet.cz	1	63.33	30.79
verizonbusiness.com	1	61.43	15.43
garr.it	1	60.92	29.38
belnet.be	1	60.67	19.53
surf.nl	2	58.27	24.33
constant.com	1	54.93	57.60
dfn.de	3	50.75	10.63
cesnet.cz	1	36.77	7.61
fiu.edu	2	36.44	36.68
ucsd.edu	64	33.31	31.74
unknown	2	26.78	28.03


LightScope
USC
CAIDA
Merit
10000000
1000000
100000
10000
1000
100
10
1

Related Work

	Infra	Live / Dark	Single / Distributed	Static / Dynamic Loc.	Passive Only	Honeypot	L4 Analysis
telescopes	CAIDA	dark	single	static	✓	×	✓
	Merit	dark	single	static	✓	×	✓
	SURF	dark	single	static	✓	×	✓
	USC	dark	single	static	✓	×	✓
	MORP4	dark	distributed	dynamic	✓	×	✓
low honey	DScope	dark	distributed	dynamic	×	low-int, all TCP ports	✓
	Spoki	dark	single	static	×	low-int, all TCP ports	✓
	HoneyTrap	dark	distributed	static	×	low-int, all TCP ports	✓
hybrid	Holoscope	dark	distributed	dynamic	✓	variable, containerized	✓ disjoint (L4/L7 on separate IPs)
	Honey@home	dark, live	distributed	dynamic	×	low & high-int, static ports	× discards incomplete handshakes
	LightScope	live	distributed	dynamic	✓	medium-int, dynamic ports	✓

closest related work (2005), honeypot only, not deployed anywhere, concept only

Deployed ASNs

ASN(s)	Organization / Owner	Count	ASN(s)	Organization / Owner	Count
AS26397	UC San Diego	66	AS156	Northeastern University	1
AS396955, AS396961	Internet2	49	AS1741	CSC / FUNET	1
AS195	San Diego Supercomputer Center	42	AS20473	The Constant Company (Vultr)	1
AS7896	University of Nebraska	39	AS213230	Hetzner Online GmbH	1
AS16509, AS14618	Amazon.com, Inc.	21	AS23859	University of New South Wales	1
private deployment		8	AS2611	BELNET	1
AS7018	AT&T Enterprises, LLC	5	AS26548	PureVoltage Hosting Inc.	1
AS2637	Georgia Institute of Technology	4	AS26832	Rica Web Services	1
[NULL]	Missing ASN value	4	AS2852	CESNET	1
AS680	DFN (German Research Network)	3	AS3209	Vodafone GmbH	1
AS701, AS22394	Verizon Business	3	AS3320	Deutsche Telekom AG	1
AS1103	SURF B.V.	2	AS33539	ISP-MANAGEMENT	1
AS1929	University of Massachusetts Amherst	2	AS35779	mCloud doo	1
AS20080	Florida International University	2	AS3927	RGnet OU	1
AS30600	Metronet	2	AS399214	Ministry of Compute Inc.	1
AS3303	Swisscom	2	AS4	University of Southern California	1
AS63949	Akamai Connected Cloud (Linode)	2	AS43708	DATAMAT CZ s.r.o. (metronet.cz)	1
AS7922	Comcast Cable Communications, LLC	2	AS5650	Frontier Communications	1
AS8075	Microsoft Corporation	2	AS693	University of Notre Dame	1
AS11078	Brown University	1	AS8560	IONOS SE	1
AS12414	Solcon Internetdiensten B.V.	1	AS9790	Two Degrees Networks Limited	1
AS137	Consortium GARR	1	unknown	unknown	1

Multi-domain Attackers

Table 4: Telescope visibility for IPs reaching *at least* each depth.

≥ Depth	IPs	USC	Merit	SURF	Spoki	Columbia	HoneyTrap	Any*	CAIDA	Excl.
TCP SYN only	749,965	70.6%	74.3%	60.7%	57.9%	53.3%	47.1%	81.0%	87.8%	8.7%
Connect	147,710	70.5%	76.3%	65.4%	67.3%	62.4%	65.2%	87.3%	87.3%	6.6%
Login attempt	52,737	55.8%	61.6%	48.9%	55.1%	54.0%	56.2%	79.0%	81.6%	10.0%
Login success	19,317	20.1%	30.8%	14.7%	21.4%	36.7%	20.7%	57.9%	74.4%	18.1%
Commands	13,667	13.6%	18.2%	9.0%	16.7%	40.2%	16.0%	53.8%	72.3%	19.2%
File transfer	10,283	6.4%	11.1%	3.1%	5.2%	42.6%	4.1%	48.8%	77.5%	19.3%

*Any telescope excluding CAIDA.

Scanners

Attackers

Not seen on any telescope

Exclusivity increases down the attack funnel