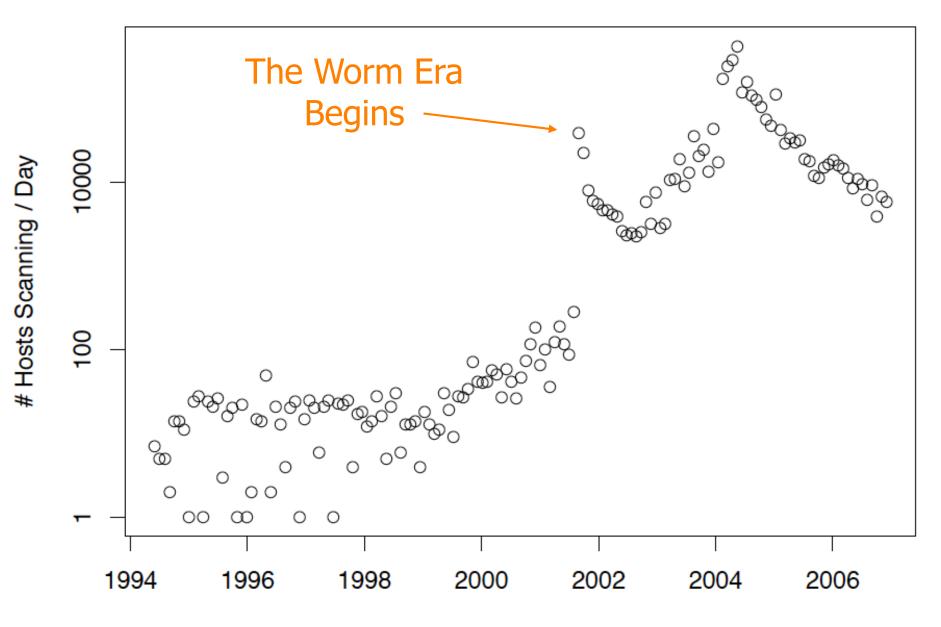
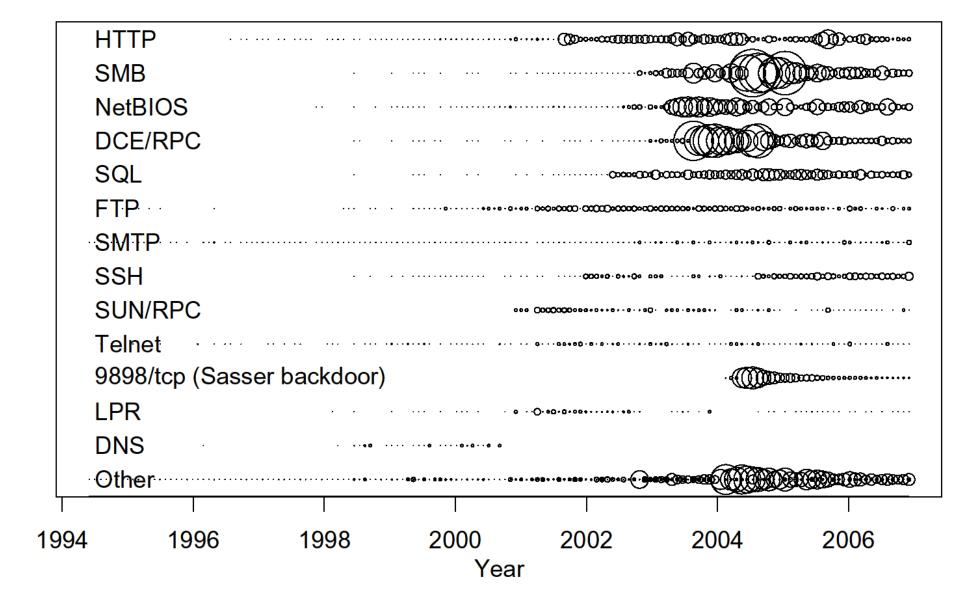
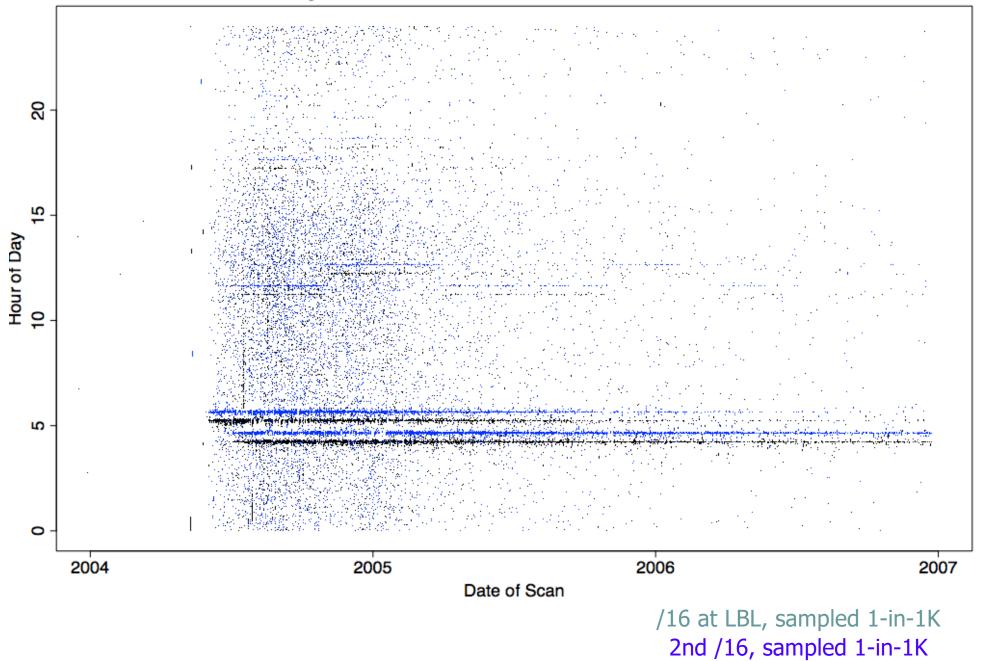
#### Scan Activity Seen At LBL

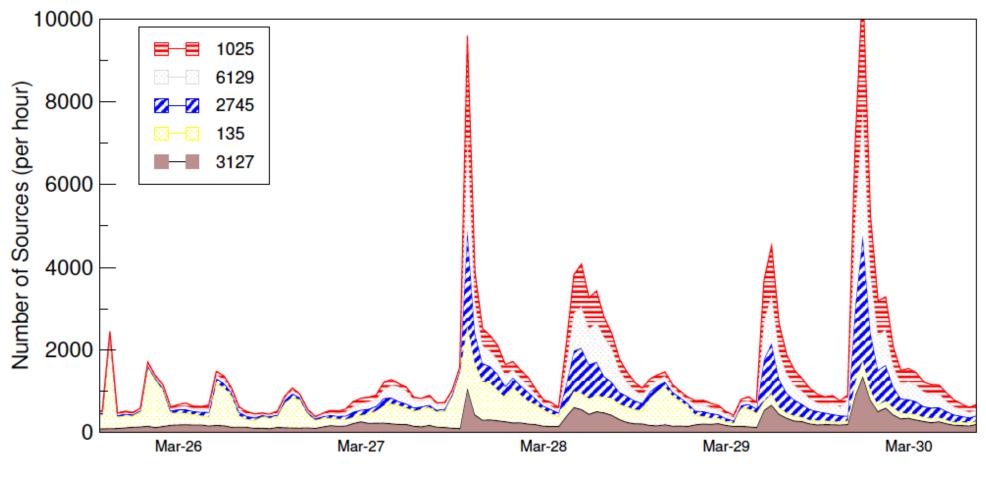


# **Services Scanned Over Time**



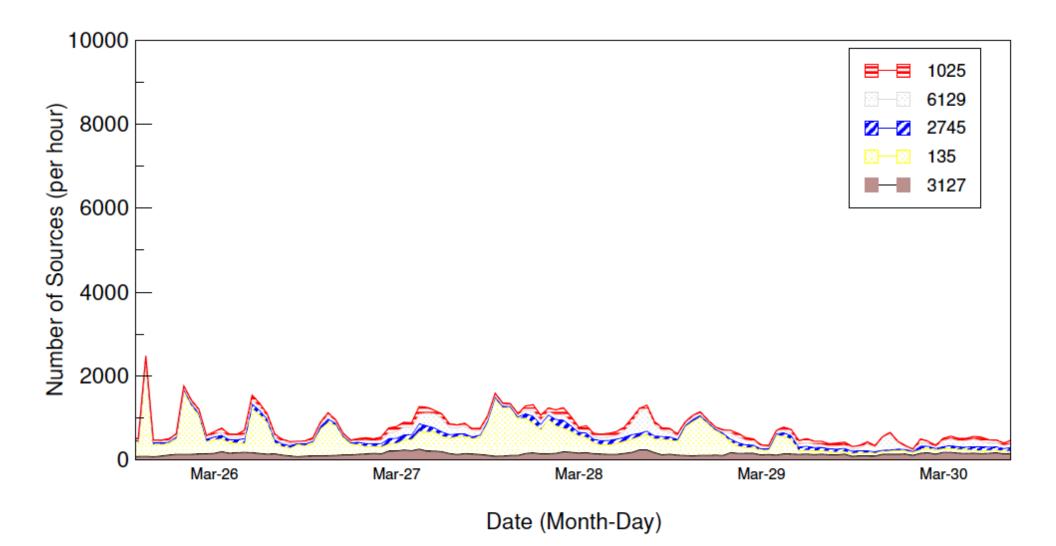
#### Daily Patterns Seen in 1023/TCP Scans





Date (Month-Day)

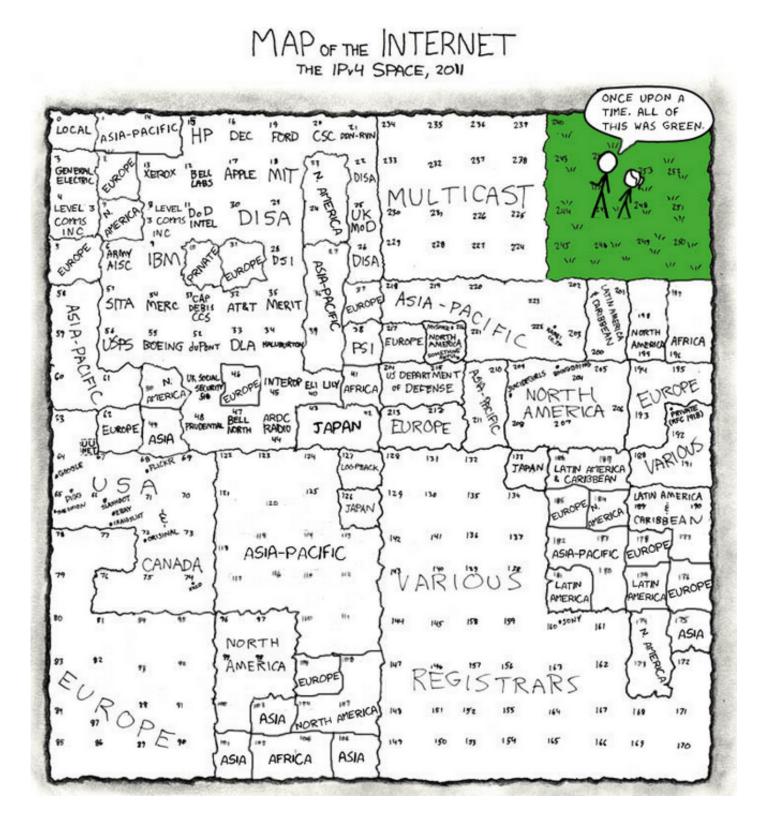
#### (a) Agobot Sources: UW I



#### (b) Agobot Sources: UW II

		LBL	ICSI
1	Total inbound connections	15,614,500	161,122
2	Size of local address space	131,836	512
3	Active hosts	5,906	217
4	Total unique remote hosts	190,928	29,528
5	Scanners detected by Bro	122	7
6	HTTP worms	37	69
7	other_bad	74,383	15
8	remainder	116,386	29,437

### Table 1. Summary of datasets



#### IPv4:

You are looking at the entire network. Each number on the map represents the n/8 subnet under it.

Zoom on the left to see a higher or lower subnet. Change the color coding mode on the right (currently colors represent organizations in the rows below). Click on a point or enter an IP address or hostname in the box to get information about that IP and its networks. Leave it blank to see where you are.

	0	1	14	15-	16	19	20	21	234	235	236	239	240	241	254	255	
	3	2	13	-12	17	18	23	22	233	232	237	238	243	242	253	252	
	4	7	8	11	30	29	24	25	230	231	226	225	244	247	248	251	
	5	6	9	10	31	28	27	26	229	228	227	224	245	246	249	250	
	58	57	54	53	32	35	36	37	218	219	220	223	202	201	198	197	Mode:
	59	56	55	52	33	34	39	38	217	216	221	222	203	200	199	196	de:
+	60	61	50	51	46	45	40	41	214	215	210	209	204	205	194	195	•
	63	62	49	48	47	44	43	42	213	212	211	208	207	206	193	192	normal
:u	64	67	68	69	122	123	124	127	128	131	132	133	186	187	188	191	mal
Zoom:	65	66	.71	70	121	120	125	126	129	130	135	134	185	184	189	190	0
	78	77	728	73	118	119	114	113	142	141	136	137	182	183	178	177	country
	79	76	75	474 <sub>0</sub>	117	116	115	112	143	140	139	138	181	180	179	176	ntry
	80	81	94	95	96	97	110	111	144	145	158	159	160	161	174	175	
	83	82	93	92	. 99	98	109	108	147	146	157	156	163	162	173	172	
	84	87	88	91	100	103	104	107	148	151	152	155	164	167	168	171	
	85	86	89	90	101	102	105	106	149	150	153	154	165	166	169	170	

#### IPv4:192.

You are looking at the 192/8 network. Each number on the map represents the 192.n/16 subnet under it.

Zoom on the left to see a higher or lower subnet. Change the color coding mode on the right (currently colors represent organizations in the rows below). Click on a point or enter an IP address or hostname in the box to get information about that IP and its networks. Leave it blank to see where you are.



## GQ: Building a Large-Scale Honeyfarm

- Honeyfarm: use a network telescope to route scan traffic to a set of honeypots
- Goal: scale to 100,000s of monitored addresses …

Physical Honeyfarm Servers

• ... at high fidelity

