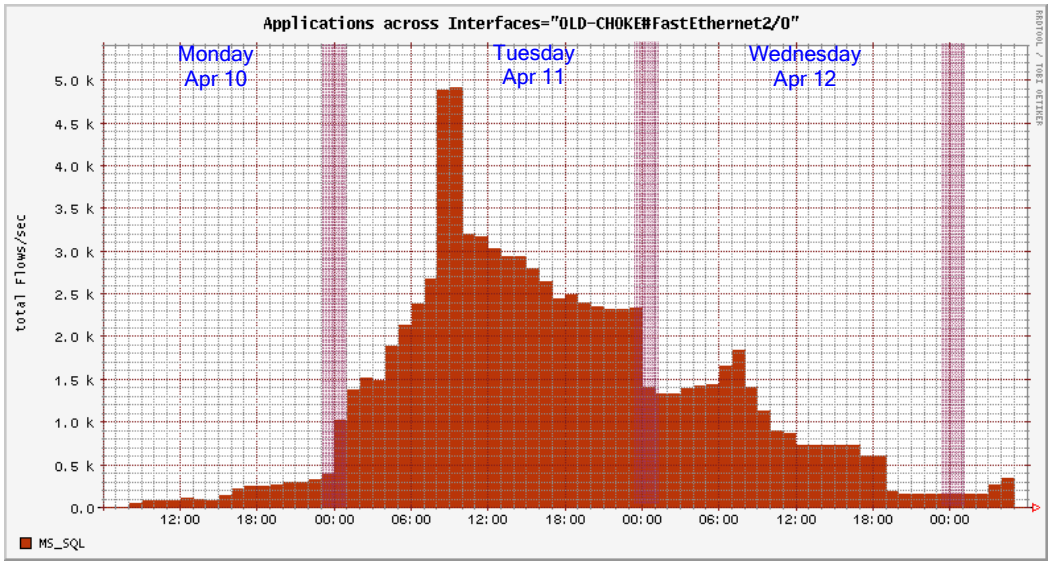
Worm Analysis

Worm propagation behavior:



Timeline

Date	Time	IP	Hostname	Description
10-Apr	7:30:00	10.76.8.95	lcnu508fmj2	Laptop connects to network and shows immediate signature of W32.Toxbot.B backdoor activity (tcp port 6556)
10-Apr	7:50:09	10.76.8.95	lcnu508fmj2	Initiates an HTTPS connection to 212.78.81.51 (vi-ads-1183.ads.vi.net)
10-Apr	7:50:13	10.76.8.95	lcnu508fmj2	Begins a TCP SYN scan on port 1433 of the 10.x.x.x space
10-Apr	9:52:07	10.65.5.39	adminresource	Infected by 10.76.8.95/lcnu508fmj2
10-Apr	12:42:01	10.66.102.95	10.66.102.95	Infected by 10.65.5.39/adminresource
10-Apr	15:08:35	10.64.85.87	nwn401a4000	Infected by 10.65.5.39/adminresource
10-Apr	15:54:51	10.50.4.42	vau_cnmsec	Infected by 10.65.5.39/adminresource
10-Apr	16:31:34	10.64.104.90	vau_det_soc1	Infected by 10.34.104.97/dsexpress1
10-Apr	19:27:04	10.66.104.92	nwn40111190	Infected by 10.65.5.39/adminresource
10-Apr	20:30:31	10.34.20.118	lcnu507g8z4	Infected by 10.66.102.95
10-Apr	22:00:06	10.64.101.91	CLS4003260	Infected by 10.66.104.92/nwn40111190
10-Apr	23:43:06	10.68.101.46	VWN404A5480	Infected by 10.34.20.118/lcnu507g8z4
10-Apr	23:47:49	10.65.4.196	sim	Infected by an unknown host
11-Apr	0:11:10	10.61.100.42	vwn434a7410	Infected by an unknown host
11-Apr	0:49:47	10.65.4.234	hpsim	Infected by an unknown host
11-Apr	1:02:23	10.64.85.86	pwn401a3990	Infected by an unknown host
11-Apr	1:59:25	10.162.101.47	CLS-40668504	Infected by 10.64.102.52/acme-b7rfyv0vr
11-Apr	2:19:00	10.64.102.52	acme-b7rfyv0vr	Infected by an unknown host