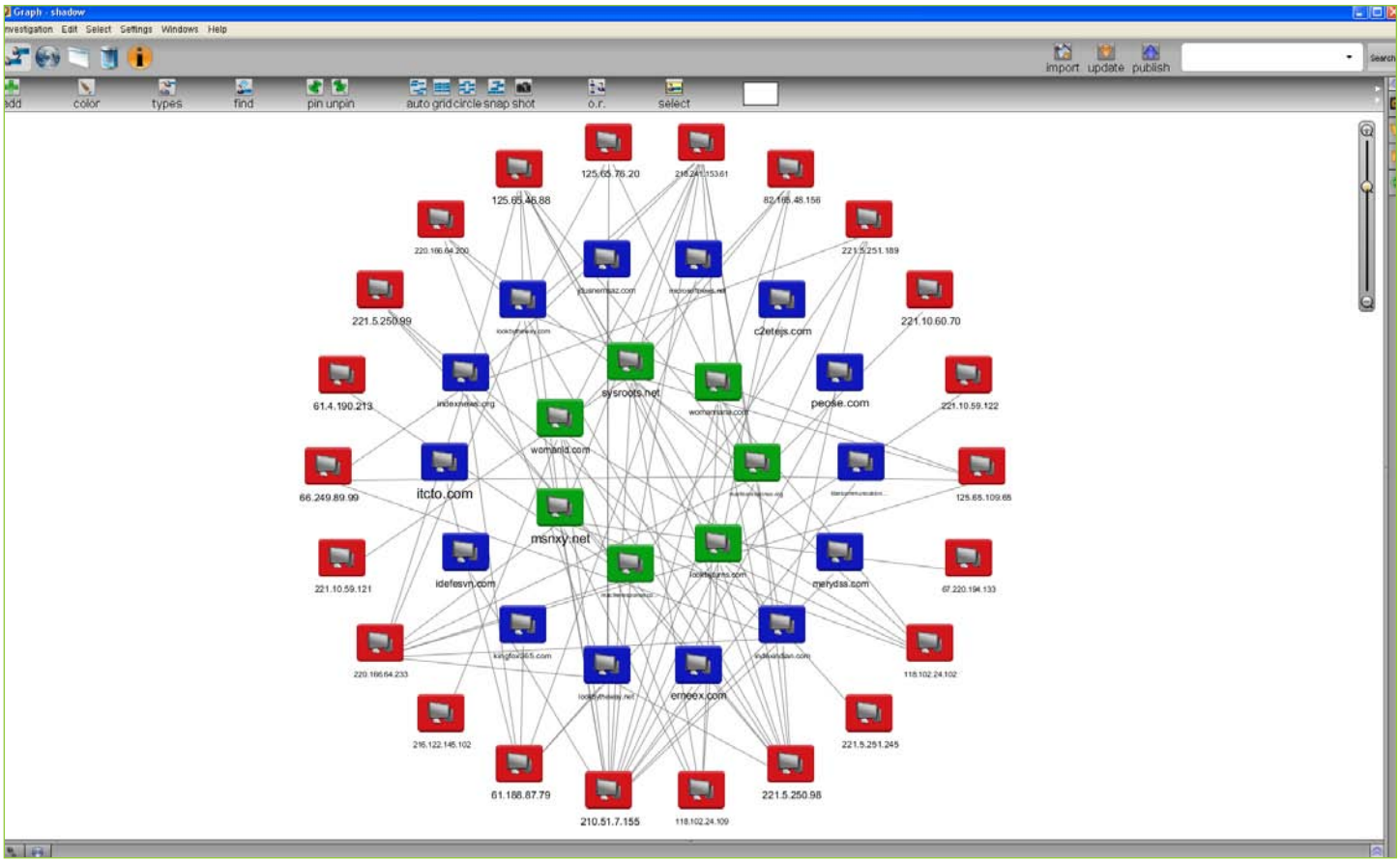
and victim systems. We were able to register and monitor four of the domain names mentioned in *Tracking GhostNet*. In addition, we were able to register several others which we linked to the *Shadow* network along with one, www.assam2008.net, which we believe to be yet another separate, but possibly affiliated, network.

- www.assam2008.net
- www.msnxy.net
- www.sysroots.net
- www.womanld.com
- www.womannana.com
- www.lookbyturns.com
- www.macfeeresponse.com
- www.macfeeresponse.org

We were able to observe the file paths associated with malware that were requested by compromised computers. In total, we found that during this period 6,902 unique IPs requested paths associated with the malware that used these hosts as command and control servers. However, counting the number of infected hosts purely by IP addresses is problematic. In fact, botnets are generally much smaller than the total sum of unique IP addresses would suggest (Stone-Gross et al. 2009; Rajab et al. 2007). This network, which is focused on stealing documents from specific targets, is expected to be small in size.

Figure 5:

Relationship between the DNS Sinkhole and Live Command and Control Servers



This Palantir screen shot captures the relationship between the domain names in our sinkhole (green), the web servers they were formerly hosted on (red) and the *Shadow* network's active domain names (blue).