Short Paper Review

Extending Black Domain Name List by Using Co-occurrence Relation between DNS queries

NTT labs the ATT of Japan

Claims:
• They can identify unknown black domain names by the co-occurrence of these names with known black domains.
• They have a very high success rate at identifying unknown black domains.
• They make the assumption that if multiple hosts query for two domain names and one is black then the other one is assumed to be black.

Pros:
• I believe that the theory here is sound. It a botnet infected host is looking to find a rendezvous point then it will try lots of different domains to find the right one. Many of these may be blacklisted and not reachable. I would think that a bot would just keep trying until they find one. This would be a visible sign that would support this theory.

Cons:
• I can tell by the writing that English was not the authors’ primary language.
• Their diagrams were a little hard to understand. The picture should say only one thing and it should be very clear.
• They only collected data for one hour? This does not seem like a sufficient amount of data to write a paper on.
• I thought the way they resolved the issue with popular websites was a little weak. They just reduced the weighting on them so they would not taint the results. I think they could have done a better job. The only way to do this weighting is to know where the infected hosts are.

Further Research:
• I believe we could do a better job of this research and I would like to try.