Reaction to "ExecScent: Mining for New C&C Domains in Live Networks with Adaptive Control Protocol Templates"

1) Technical details (approach/technique) that you found novel/ Something specific you learned that you didn't know before

I think this paper is a pretty good example about classification of a large data set. They consider the difference in different networks and try to capture the difference by enabling their monitoring framework automatically adapt to that environment. This idea is novel.

2) Could I have done this work if I had the idea why or why not?

The author mentioned that their work is partially based on the malware data provided by a malware research facility. This is a necessary part to train the classifier. Whether we can do the same work depends on whether we can find the chance to cooperate with such kind of data providers.

3)Is there anything I could do to repeat or validate?

If we can apply a similar filter to Clarkson network and check the result against the malware database, I think we can find something interesting. The authors also mentioned that a limitation of this method is: to build a CPT, a malware sample should be captured in advance. A research of automatically building of CPT may also be an interesting aspect of research.

4) What is my best idea for follow on work that I could personally do?

I want to gather traffic data from a realistic environment and do analysis to see whether we can find anything interesting. I think Clarkson University will be a good environment to conduct such a test. As the only thing we need is HTTP access logs, I am pretty sure this would not cause big problem to the network gateway. We can do it in an asynchronous way and do the data processing using Amazon Hadoop Cluster, which makes data analysis trivial.

5)What is my best idea for follow on work that I'd like to see the authors do?

I want the author to explain more about their mathematical proof of the model they build. It gives me a feeling that they don't want to quantify their result. They just put everything in, and "try" different parameters then "expect" it to give a better result. I am expecting to see more formal proof of their classification method.

6)Any logistical experimental lessons I learned?

Python is slow... If I were the authors, I will capture the data and send it to some remote machines for further processing, rather than doing all the work in a real time fashion.

7)How does this compare to the other papers we read? Most similar? How different? Other comparisons?

This paper is targeting different areas from the papers we have read before. Thus no comparison is available.

8)What is your biggest criticism of the paper?

I have some concern about the method the authors used to measure the performance of their method in Section 5.3. To evaluate whether the new C&C domains they had classified are true positive, they claim to manually compare the list with CCBL list. However, they claim that they have found new domains that are not covered in CCBL. I think there's no way for them to verify whether the new domain they have found are actual fraudulent. More evidence must be provided to make it convincing.