article amsfonts, amsmath, amsthm, amssymb [urlcolor=blue,linkcolor=black,colorlinks=true]hyperref pdftitle = COMP 4200 (Winter 2009) Course Notes, pdfkeywords = pdf, hyperref, bookmarks, pdfauthor = Michael Himbeault [headsep=1cm,headheight=50pt]geometry [dvips]graphicx subfigure

thmTheorem[section] cor[thm]Corollary lem[thm]Lemma

*hypHypothesis

remark remark[thm]Remark

definition definition[thm]Definition

definition exampleExample[section]

definition algorithmAlgorithm[section]

document amsplain Merlin SRP - Project Update Michael Himbeault

Where We Came From Literature Review itemize

S everal papers on network payload signature based analysis. This is problematic for several reasons, the least of which is that it has difficulty handling encrypted payloads. It often requires the reverse engineering of network and communication protocols used by the specific malware in question necessitating that a copy of the program be on hand for analysis. This isn't particularly reasonable for Merlin's situation as the neither the expertise nor the time are available to devote to this method.

Additional problems include lack of scalability (For large networks with multiple different 'strains' of infection, this process must isolate each strain individually), portability (It doesn't port well from location to location) and adaptability.

For these reasons, this approach has been largely discarded.

A s was mentioned last time, the concept of "social interaction" of network hosts is an approach that is agnostic to payload schemes (But may care about payload size). This approach is not unknown to literature in this area and such graphs are known as Traffic Dispersion Graphs (TDGs). The originating paper appears to be TDG and discusses possible analysis of the resulting graphs. These graphs were captured by monitoring a network backbone and considering the resulting data.

A paper exists(TDG2) that looks at using TDGs for the purpose that was suggested in October; detecting malware based on the social characteristics of its network activity. This paper indicates that if the malware in question implements some simple peer-to-peer algorithms it is possible for it to reduces its footprint in a TDG-based analysis to such a level as to almost disappear into the background noise of normal activity. The scenario that this paper considers is significantly different form the scenario in the Merlin project for several reasons and so these results, while instructive, are not considered completely valid to this project.