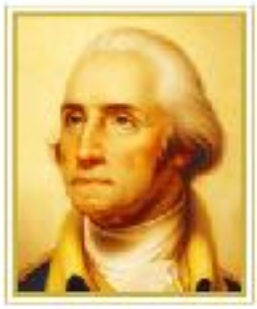

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON DC

Computer Science 6907-10
Computer Network Defense

Homework #6

Kevin Yasuda
Matthew Norris

Indicators of Compromise

For both of the examples below, please submit a brief writeup on the method that you used to identify the indicators (with screenshots as appropriate), the STIX/CybOX generation code that you wrote, and the actual STIX output. Any additional code that is required for the process to be repeatable (e.g. the Exit Node list generation script) should also be included in your submission.

1) Develop STIX to communicate the IOCs found via your prior analysis of the "plugin1 malware". Your IOCs must include at least the "best" (i.e. the most reliable) (1) host IOC and (1) network IOC. Explain your reasoning for why you picked these indicators as the "best".

2) Determine the current list of Tor Exit Nodes (i.e. pull an up to date list of Tor Exit Nodes for this assignment) and generate STIX output to document the Tor Exit Nodes as incident/ TTPs. (Try https://collector.torproject.org/recent/exit-lists/ OR Check Slides for notes on finding Tor Exit Nodes)

As usual for all of our homework assignments, state all assumptions made and why you made them.