Michael Esposito
Network Defense 2

HW6

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”.

I used the python-stix and python-cybox libraries to assist in creating Stix output. The indicators of compromise I used consisted of host IOCs and network IOCs. These IOCs were:

- Install+plugin1.exe file with hash value
- Plugin1.exe file with hash value and default install location
- A Windows registry key
- Network traffic to IP address 192.168.52.2

These indicators are reliable and offer objective results on whether a host is infected with plugin1.exe. I had hoped to have more specific network indicators. Unfortunately, I could not successfully define the network observable definitions in cybox to indicate source IP, destination IP and protocol. Two Stix examples and the python-stix and python-cybox Github repos were helpful in figuring out the required Python boilerplate code and the proper way of defining observables.

http://stixproject.github.io/documentation/idioms/malware-hash/
http://stixproject.github.io/documentation/idioms/block-network-traffic/
https://github.com/STIXProject/python-stix
https://github.com/CybOXProject/python-cybox

I used StixViz to visualize the entities I had created and confirm that the links between entities were suitable. My XML file is `ioc_plugin1.xml`.

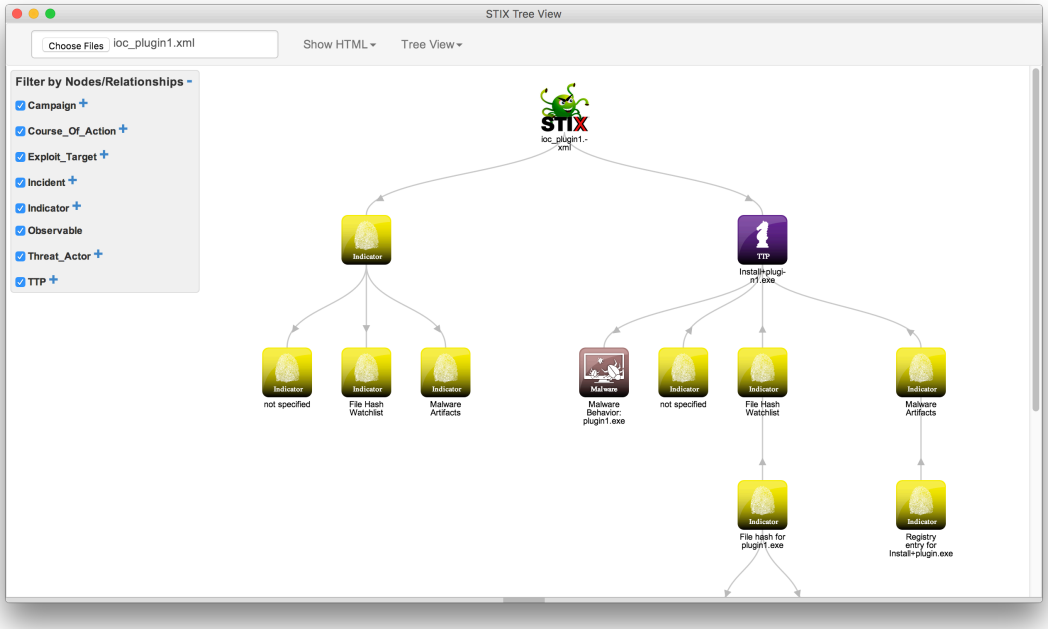

Figure 1: Using StixViz to visualize my XML files

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.

I used the following list of Tor exit nodes. Each entry contained a node's ID and associated IP address.

https://collector.torproject.org/recent/exit-lists/2018-05-04-19-02-00

The important piece of information for CTI is the IP address, so I used Python's regex module to output each exit node's IP address. I created a Course Of Action, and this course of action contains every node's IP address as an observable. A potential course of action may involve blocking each of these IP addresses on a firewall, which my XML file helps convey. My XML file is `coa_tor.xml`