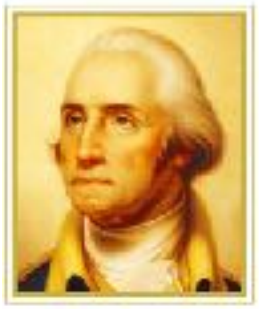

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON DC

Computer Science 6907-10
Computer Network Defense

Homework #3

Kevin Yasuda
Matthew Norris

Dynamic Malware Analysis

Analyze the "plugin1 malware" for IOCs (both host and network). Document the IOCs found via the requirements listed above. (check Blackboard for new URLs)

- The plugin1 malware can be obtained:
  - https://s3.amazonaws.com/gwucs.cnd.p2/Install+plugin1.exe
- The analysis tools can be obtained:
  - https://s3.amazonaws.com/gwucs.cnd.p2/MalwareAnalysisTools.zip
- An ISO containing both is available:
  - https://s3.amazonaws.com/gwucs.cnd.p2/MalwareAnalysisTools-Kit.iso

Submit a Malware Analysis report. The report must cover at least the following items and provide screenshots or details of your analysis to back up your findings.

1) How does the Install+plugin1.exe become persistent (i.e. restart after reboots of the system)?
2) What are the files or registry keys dropped by the install+plugin1.exe?
3) What does plugin1.exe do?
4) What files can be used to indicate if Install+plugin1.exe was run on a system?
5) What registry keys can be used to indicate if Install+plugin1.exe was run on a system?
6) What network indicators (e.g. DNS names, IP addresses, etc.) indicate if Install+plugin1.exe was run on a system?

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