Malware Analysis

Problem Statement: For this project, you will be given a live sample of malware to reverse-engineer and analyze to determine its capabilities. Specifically, your task will be to answer the following set of questions:

1. Is the malware protected / obfuscated? If so, what techniques are used to hide its functionality?
2. Does the malware try to disable any Personal Security Products (PSPs), such as Anti-Virus, IDS, etc.? If so, what techniques are used?
3. Can you discern anything about the developer or origin of the malware? Please describe.
4. Can you determine what language was used to write the malware? If yes, what? Please explain how you came to your conclusion.
5. What function(s) does the malware perform? Describe how you discovered its capabilities.
6. Does the malware have any self-propagation logic (e.g., worm)? If so, please describe.
7. How does the malware persist on the target host?
8. Does the malware communicate with any remote servers? Please list any IPs, etc. that you find.
9. Can the malware author remotely command and control the malware?
10. How might a system administrator notice a machine on the network is infected with this malware?
11. How can an infected user detect and remove the malware?
12. How would a user be infected with the malware?
13. What is the public name of this malware?
14. Please describe the tools and techniques you used to perform your analysis.

Challenge Problem: Now that you have a detailed understanding of the malware, your final goal is to modify the sample to perform some additional functionality of your choosing and/or change how it behaves on target. Can you repackage it such that no PSP product can detect or recognize it as the original sample? Please document your methods for adding/changing the sample and any tools used.