Weaponizing the worm

RWH

November 4, 2019

Abstract

Your task is to take the self-replicating program and turn it into a virus. Specifically, the virus should only wrap the rc4 executable. It should log the key and file information.

The steps

Follow these steps and it will be straightforward.

first program

This program does the infection.

1. The program should check and see if a copy of rc4 is present
2. The program should read the copy of rc4 and see whether or not it is infected.
3. If (and only if) the rc4 program hasn't been infected, it should write a c-program with a reserved static area for the rc4 executable (it should figure out how much static storage is needed.) It should then compile and execute this second program.

   Alternatively you could use a hex encoding of the rc4 executable and insert it in the c language code.

   A "fully weaponized" version of this program would insert its own code into the second program so that it could keep propagating. You can do this if you want, in which case this program would have a pass similar to the original self-replicating program to insert its code into itself.

second program

This is the actual wrapped code.

1. As in the worm, check for the presence of the rc4 executable. If it is *not* present then do the same thing as the worm and generate a new executable with the rc4 code within in it. Replace the existing rc4 executable with your new one.
2. If the executable is present inside the code, write a copy to \tmp, use chmod or whatever is needed to make it executable, and then run it with the appropriate redirections of stdin, stdout and stderr (there are posix calls for this). Log the command line to some file. When it is finished delete the copy of rc4 from the \tmp directory.

   You will probably need to rewrite the way the program is called (i.e. if it was ".\rc4 key < a > b" you will likely need to do "\tmp key < a > b")