CIS2376 PRACTICAL

Week 17

Important Warning

Some of the techniques we have discussed in this weeks teaching materials should **not** be used or practiced on **any** University network. To do so could result in instant suspension from the University.

Questions

1. This question gets you to use the *Paimei* framework to locate key data structures within *winmine.exe*.

   - Launch *Paimei* by double clicking *paimei.bat* on your desktop.
   - Goto *Process Stalker* and click *Add Module*. Locate and select *winmine.exe.pida* and then load it into *Paimei* (this loads in a previous compiled database of facts about the *winmine.exe* binary).
   - Now create a target (named *winmine* say) and add three tags (one named *gui*, one *logic* and one named *ticking*) to the target.
   - Select the *gui* target and configure it as a process stalker.
   - Now use the *browse* button to locate the *C:\WINDOWS\system32\winmine.exe* executable.
   - Ensure that *basic blocks* is selected and all check boxes are unticked. Now press the *process stalking* button and allow *winmine.exe* to launch.
   - Interact with *winmine.exe* by selecting various GUI elements (such as pull down windows, help objects, etc.) and resizing the window. Once you've finished with your GUI based interactions, either kill the *winmine.exe* process or press the *stop stalking* button.
   - Now select the *ticking* tag and configure it as a process stalker.
   - Select the *ticking* tag and configure it as a filter.
   - Press the process stalker button and click **one** square within your playing grid. This square should **not** contain a mine - if this is the case: kill the *winmine.exe* process; clear the *ticking* tag; and then restart this step again.
   - Now select the *logic* tag and configure it as a process stalker.
   - Configure both the *gui* tag and *ticking* tag as filters.

- Press the *process stalking* button again. However, this time play the game until you hit a mine that explodes (you may find it useful here to be working here with a custom 9 by 9 grid with 64 mines!).
- Halt the process stalking (see above) and, after selecting the *logic* tag, synchronize with uDraw.
- Switching to the uDraw window allows you to examine the functions, from the control flow graph, that were hit on exploding the mine (well, minus those that resulted from those present within the *gui* and *ticking* tags!).

Using the above, can you locate code that helps to describe the possible values for each cell within *winmine.exe's* playing grid?

2. This question uses boron tagging to locate code of interest within the *sample1.zip* malware from the week 16 practicals.
   - First ensure that your virtual machine environment is setup as for the week 16 practicals.
   - Now use *Immunity Debugger* to launch a copy of *Windows Live Messenger.exe*.
   - Once the *Windows Live Messenger.exe* process has initialized itself, perform a search in memory for the strings:
     - Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7
     - Aa8Aa9Ab0
   - Now allow *Windows Live Messenger.exe* to carry on running and, at the GUI dialog window, enter the above strings as the email address and password respectively. Then click *SignUp* and allow the process to execute until it pauses (this pause is due to a programmer exception being generated!).
   - Search memory again looking for the above strings.

   Use the information you have gathered above to answer the following questions:

   a. Can you locate the first stack frame that contains pointers to the ASCII string Aa0Aa1?

   b. What potential functions can you identify that might manipulate the user credentials entered into the *Windows Live Messenger.exe* trojan?