4/2/11

Rootkit Detection

The system seems to be perfectly fine at the initial startup; nothing was abnormal. Once starting up the anti-malware software called, "Gmer." It shows up lots of file were infected and several rootkits might have been planted. In addition, used the anti-malware called, "Malwarebytes" to help out if Gmer missed anything and the comparison of the two softwares. It was confirmed there were two easily detected, hxdef100r and vanquish. Vanquish did not seems to be started up by the detection of anti-malware software. It only detected the execution and not infected files.

Hxdef100r seems more hidden than compare to vanquish and that rootkit does seem to be started up. Gmer software found the location in the disk where the hidden folder was. There was a readme file that was quite useful in explaining how the hxdef100r rootkit works and setup. It also told which API rootkit it hooked to; to confirm, I checked with the Gmer and it does seems to be hooked to those API. The reason was because it showed the address space which is another offset. This seems like "man-in-the-middle" attacked by hooking to the API to control the import address tables.

After exploring about hxdef100r, the two anti-malware softwares detected two specific files in the c:\system32\drivers folder. The files were msdirectx.sys and mmpc.sys. I started up the PEview software to see import and export address tables. I did discover in the PEview under the .rdata - image_debug_type_codeview, it is listed "c:\futo_enchanced\futo\exe\i386\msdirectx.pdb" which indicates there was FUto rootkit is present. The next file I look under the PEview was the mmpc.sys and did the same exact steps in the previous file. I did see it was shadowwalker rootkit was also present. It was label as "c:\shadowwalker_corey\BIN\i386\mmpc.sys."

When I finished inspecting the two files, Gmer listed couple other files that were in the same folder. I checked the folder and did discover a file called "FU.exe" which might seem to be the first generation of FU rootkit then became FUto. Another file that seems to be abnormal was the "ctr12cap.sys" because there was another file right below with the similar name "ctrl2cap.sys." In PEview, under image_debug_type_codeview shows the value of c:\bhf|objfre_wxp_86\i386\ctr12cap.pdb. I tried looking up in the internet seeing if there was a rootkit goes by the name "bhf," but there was no luck in it. I still do think it might be a rootkit because it acts the same as the futo and shadowwalker.

Most of the rootkit that I found was removed by malwarebytes. I also went into safe mode and rescanned it using the same software and removed the malware service that was not running under safe mode at startup. Also I remove couple files manually, but after a reboot, it seem there are some rootkit left that I have not been able to detect or remove.