**Malware Analysis – Windows Live Messenger**

**Student: Hong Zhang**

This malware is a malicious Trojan of Windows Live Messenger which is a fake instant messenger client. It has the capability to capture the victim’s logon credentials. I will use dynamic analysis to analyze its behaviors and see what capabilities are built into this malicious executable.

Because we need to execute malware in an isolated laboratory system, I will use RADISH, our VMware to set up my lab. Next thing is we need to install python in the operating system. Finally, it is the analysis part.

The first approach in this analysis is using RegShot to scan the Windows registry in full C: drive. I took two snapshots and compared them. The 1st shot captured the current state of the Windows registry. The 2nd shot was taken after I run the malware. In the following comparing report, there were three files added. These infected files are WINDOWS LIVE MESSENGER.EXE-5F1931EE.pf, msnsettings.dat and pas.txt. The file, pas.txt contains victim’s logon credentials, such as username and password. Its purpose is hackers use them to hack victim’s real Windows Live Messenger. The file, msnsettings.dat contains an exe file named msnmsgr.exe. We can compare this msnsettings file which I executed to that msnsettings file which is from the CFO's computer. The main differences are the second file change the header and add something. In the first line, the second file changed from "hello" to "test." After executing msnmsgr.exe, the msnsettings file from the CFO's computer added gsmtp185.google.com and [mastercleanex@gmail.com](mailto:mastercleanex@gmail.com).

Now, it is the turn for the second approach. The tool which I used is Process Monitor which can help us understand how the malicious program interacted with the file system and the registry. To use Process Monitor, run it while infecting the system. After using two filters, Process Name = Windows Live Messenger, Operation = WriteFile, we will only see a single event showing the malware is writing to the pas.txt file.

The third tool used to do the analysis is FackNet. After running it, FakeNet has various services listening to interact with the malware and make the malware think that it has access to the internet (even though it does not.) Then, execute this malware and through FakeNet, we will see the server, PracticalMalwareAnalysis.com which uses Port 25 for SMTP to send out some information, maybe emails. After I hit "Sign In" in the malware, the malware is trying to collect the user's email address and password. Then, the malware mail the information to [mastercleanex@gmail.com](mailto:mastercleanex@gmail.com).

Now, we can check out the malware in the OllyDbg debugger. Using this tool to analyze the malware’s source code, we will find the malware is looking for the string “test” in the email address field. That is a trigger for this malware. Then, when we run this Trojan and type “test” in the email address field, we will find a secret menu which allows you to configure the trojan’s operation.

In this malware, the hacker uses the Trojan to capture victim’s credentials when they use this fake version of Windows Liver Messenger. Then, the information of their username and password was saved to local C:\pas.txt. Next, the file was sent to the hacker’s computer through [mastercleanex@gmail.com](mailto:mastercleanex@gmail.com). At the same time, the attacker used msnsettings.dat to store its configuration. The attacker customized the configuration by typing “test” into the “E-mail address” field. The customized configuration came from the saved msnsettings file from the CFO's computer.