Indicator of Compromise:

For execution:

1. Download this file ZenDeskrar
2. Rename ZenDesk.rar
3. Unzip ZenDesk.rar
4. Open the command line argument : cd to the directory ZenDesk

IOC 90.156.201.27,027.ru,99017f6eebbac24f351415dd410d522d,http://www.google.com

IOC is the executable

Four Parameters: 90.156.201.27,027.ru,99017f6eebbac24f351415dd410d522d,http://www.google.com

Some constraints for this program

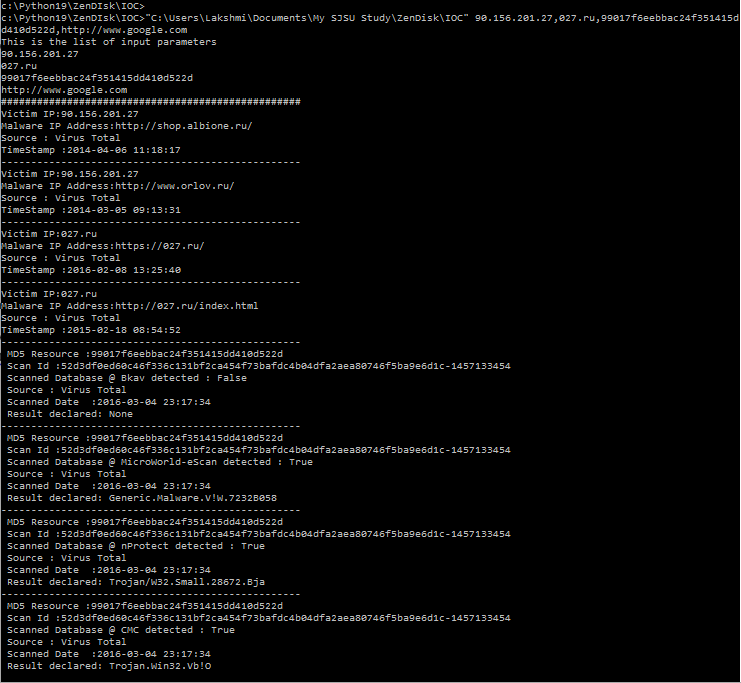
* All the parameters are strictly comma separated
* A max of four similar or different kind of indicators are passed to retrieve the details
* For the each IOC a max of three sections is displayed for ease of readability
* Virus Total is the other source used apart from HoneyPot to show multiple source co-relation

Two Sets of attachments one executable name ZenDeskrar and SourceCode in ZenDeskSourceFilesrar

Sample Execution shown below:

This program basically achieves the following output:

c:\Python19\ZenDIsk\IOC> C:\Users\Lakshmi\dist\IOC.exe 90.156.201.27,027.ru,99017f6eebbac24f351415dd410d522d,http://www.google.com



c:\Python19\ZenDIsk\IOC>"C:\Users\Lakshmi\Documents\My SJSU Study\ZenDisk\IOC" 90.156.201.27,172.31.13.124

