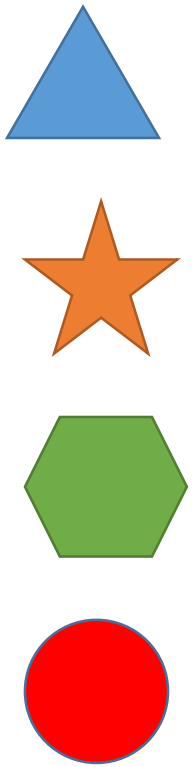
Principles of Analyzing Java RAT

RAT = Remote Access Tool = Remote Access Trojan

What is a RAT (Remote Access Tool/Trojan)?

RATs are malicious programs that run invisibly on host PCs and permit an intruder remote access and control

Features of a RAT



Often provide a wide-variety of functionality: key logger, screen capture, program execution, file modification, information stealing

Unlike ransomware, attempt to remain hidden

May be used as a pivot-point for infecting other systems

Need persistence, leave behind important clues

Lab Exercise Instructions

Download the file Java_RealWorld-CrossRAT.zip

Password to unzip the file is: crackinglessons.com

Use a virtual machine to analyze it

Thank you