]HackingTeam[

Training of RCS

Installation of RCS Documentation of the installation process to ensure subsequent installations can be performed without assistance of HT
Activities
<u>Installation of RCSDB</u> - Documentation of Installation procedure - Documentation of required configuration for host OS including posts to be opened
<u>Installation of ASP server</u> - Documentation of Installation procedure - Documentation of required configuration for host OS including posts to be opened - Configuration of load balancing among multiple ASP servers. - Configuration of dummy web server and document options available
<u>Installation of HCM</u> - Documentation of Installation procedure - Documentation of required configuration for host OS including posts to be opened
<u>Installation of Viewer</u> - Documentation of Installation procedure - Documentation of required configuration for host OS including posts to be opened

Training by HT - Training for system administrator Learn best practices for administrative configuration of RCS
Activities
<u>Configuration of roles and permissions</u> Setup initial user accounts, user groups including appropriate permissions for each user group - Administrator - Technical Operator - Viewer
<u>Basic verification that RCS system works using simple FSA agent</u> - Creation - Infection - Trigger and reporting to ASP/RCSDB of captured information - Viewing of captured data - Shutdown of FSA
<u>Management of Activities and Targets</u> - Creation of activities and targets - Closure of activities and targets

Perform auditing Establish procedure for regular audit of access and actions performed by users accordingly to roles - Admin - Tech - User
Monitor system health Establish procedure to monitor health of critical system components and interventions to be performed when situations arise for - RCSDB - ASP - HCM Procedure for applying patches/upgrades
Performing disaster recovery Establish critical files required for disaster recovery in - RCSDB - ASP - HCM - Viewer Establish procedure for disaster recovery using backup files

Training by HT – Training for technical operator Learn best practices for operational configuration of RCS
Activities
Method of infection Explanation of exe melting procedure. - Practice melting with common executables Practice using USB and CD boot infection method Explanation and practice of injection proxy method Using PC/laptop
Creation of Backdoor Explanation of each trigger event - Executed Processes - Network Connection - Screensaver start/stop - Date/Time - Windows Event - Quota Explanation of each agent type (including limitations) - Key logger - URL monitoring - Userid/password monitoring - Screen Snapshot - Printing monitoring

- Clipboard monitoring - File Capture - Crisis - VoIP (cover Skype and Google Talk) - Microphone - Webcam - Instant Messaging Explanation of actions sent to backdoor - Synchronize - Start / Stop agent - Uninstallation - Command Execution
Controlling FSA agent Explanation of available actions to control backdoor.

Training by HT – Training for viewer Learn best practices for information collected by RCS
Activities
Viewing information Viewing of information collected by each individual agent - Key logger - URL monitoring - Userid/password monitoring - Screen Snapshot - Printing monitoring - Clipboard monitoring - File Capture - Crisis - VoIP (Skype and Google Talk) - Microphone - Webcam - Instant Messaging
Analysis of information Perform query within information collect by a single agent - Clarify what do the different query parameters mean Perform query within information collected across different agents on one target Perform query across targets Export options for collected information Export options for query results