

]HackingTeam[

Remote Control System
[Delivery Acceptance Procedure](#)

| Revision | Author (s) | Release Date |
|-----------------|-------------------|------------------------------|
| 2.1 | FAE Group | 2015, 13 th April |

Contents

- 1 Objectives4**
 - 1.1 Functional Tests.....4
- 2 Frontend.....5**
 - 2.1 Procedure.....5
 - 2.2 Results5
- 3 User Creation.....6**
 - 3.1 Procedure.....6
 - 3.2 Results6
- 4 Group, Operation & Target creation.....7**
 - 4.1 Procedure.....7
 - 4.2 Results7
- 5 Factory Creation & Configuration8**
 - 5.1 Procedure.....8
 - 5.2 Results8
- 6 Remote Mobile Infector9**
 - 6.1 Procedure.....9
 - 6.2 Results9
- 7 Tactical Network Injector.....10**
 - 7.1 Procedure.....10
 - 7.2 Results10
- 8 Agent Creation & Lifecycle12**
 - 8.1 Procedure.....12
 - 8.2 Results12
- 9 Target Lifecycle.....13**
 - 9.1 Procedure.....13
 - 9.2 Results14
- 10 Backup15**
 - 10.1 Procedure.....15
 - 10.2 Results15
- 11 Connector16**
 - 11.1 Procedure.....16
 - 11.2 Results16

1 Objectives

This document details the Delivery Acceptance Procedure required for assessing the functional compliance of Remote Control System (RCS) installation.

The proposed test cases are to be performed during solution's delivery at Client's premises, carried out by Hacking Team Representatives and with the presence of Client Representatives.

All tests will be performed during or after Remote Control System (RCS) installation and - according to RCS license file acquired by the Client - some tests may be indicated as not applicable (N/A).

On completion of the Delivery Acceptance Procedure the Client shall sign the Delivery Certificate.

The signature date will be considered as the acceptance date for any future use or reference.

1.1 Functional Tests

The purpose of the proposed tests is to verify Remote Control System (RCS) functionalities within Client's specific installation, to ensure operational readiness.

Each test comes with an objective, a procedure and the expected results. Hacking Team and Client Representatives shall follow the procedure and accordingly report the results. Tests cases must be carried out in the presented order, to guarantee all pre-requisites are met.

The Client should consider these activities as a complete setup of Remote Control System (RCS) by Hacking Team Representatives, in accordance to the company best practices, to ensure that the system is operational and ready for use.

NOTE: Users, Groups, Operations, Targets and Agents created during the functional tests may be deleted after the Delivery Acceptance Procedure, leaving the Client with a clean RCS installation.

2 Frontend

This test case verifies that each Collector and Anonymizer is reachable from the Internet and responds correctly when interrogated.

2.1 Procedure

The activities required for this unit may be performed on any system connected to the Internet.

For each Collector and Anonymizer, please follow the steps listed below:

1. Open a web browser or open a new tab;
2. Connect the browser to the URL `http://<IP_Address>/`, where `<IP_Address>` is the IP address of the system to be tested;
3. Verify that the browser replies with the default web page (Error 404 Not Found).

2.2 Results

Please fill the table below indicating the result of the test with respect to the expected outcome.

| | Verified? |
|--|--|
| Each Anonymizer and Collector replies with default web page. | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |

3 User Creation

The scope of this test is to create and verify a complete set of Users, as required to use the system.

Upon completion of this test, the Client shall have one (1) User with *Administrator* role, one (1) with *System Administrator* role, one (1) with *Technician* role and one (1) with *Evidence Analyst* role.

3.1 Procedure

Steps for this test case are performed on the Console, as listed below:

1. Logon using the *Administrator* (admin) User created during installation.
2. Create a User with only *System Administrator* role.
3. Create a User with only *Technician* role.
4. Create a User with only *Evidence Analyst* role.
5. Verify that each User can login, using the Console.

3.2 Results

Please fill the table below indicating the result of the test with respect to the expected outcome.

| Login with <i>Administrator</i> User | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |
|---|--|
| Login with <i>System Administrator</i> User | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |
| Login with <i>Technician</i> User | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |
| Login with <i>Evidence Analyst</i> User | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |

4 Group, Operation & Target creation

The scope of this test is to create a Group, Operation and Target needed for the subsequent tests. Upon completion of this test the Client shall have one (1) Group, one (1) Operation and one (1) Target.

4.1 Procedure

Steps for this test case are performed on the Console, as listed below:

1. Logon using the *Administrator* User.
2. From the Operations panel, create a new Operation with name 'Test Operation'.
3. From the Accounting->Groups panel, create a new Group with name 'Test Group'.
4. Click on the Available Users (+) and add all the Users present.
5. Click on the Available Operations (+) and add 'Test Operation'.
6. From Operations->'Test Operation', create a new Target with name 'Test Target'.
7. Verify Operation, Group and Target creation using the Audit panel.

4.2 Results

Please fill the table below indicating the result of the test with respect to the expected outcome.

| Test Operation created | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |
|---|--|
| Test Group created | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |
| Operation and Users associated to Group | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |
| Target created | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |
| Audit log entries are present | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |

5 Factory Creation & Configuration

The scope of this test is to create and verify Factories and configurations needed for subsequent tests. Upon completion of this test the Client shall have one (1) Desktop Factory and one (1) Mobile Factory.

5.1 Procedure

Steps for this test case are performed on the Console, as listed below:

1. Logon using the *Technician User*.
2. Move to *Operations-> Test Operation -> Test Target*;
3. Create a new factory of type DESKTOP with name *Test Desktop*.
4. Create a new factory of type MOBILE with name *Test Mobile*.
5. Open the *Test Desktop* factory, switch to Advanced Configuration, then press the Template button and load *DAP Desktop*.
6. Check Synchronization interval (every 60 seconds) and Host address (Frontend), then press the Save button.
7. Open the *Test Mobile* factory Advanced Configuration panel, press the Template button and load *DAP Mobile*.
8. Check Synchronization interval (every 60 seconds) and Host address (Frontend), then press the Save button.

5.2 Results

Please fill the table below indicating the result of the test with respect to the expected outcome.

| Desktop Factory created and configured | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |
|--|--|
| Mobile Factory created and configured | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |

6 Remote Mobile Infector

The scope of this test is to ensure that the Remote Mobile Infector (RMI) is able to craft and send an SMS with the link to an infection package.

6.1 Procedure

Steps for this test case are performed on the Backend server and on the Console, as listed below:

1. Ensure that a valid SIM card is inserted in the RMI modem and the modem is connected to a USB port of the RCS DB.
2. On the Backend server, run the AirCard Watcher application and ensure that the SIM card is correctly connected to a local mobile provider with at least 2 bars of signal strength.
3. Logon on the Console using the *Technician User*.
4. Open the *Test Mobile* factory Advanced Configuration panel and press the Build button.
5. Choose *Wap Push Message* and select *Multiplatform*.
6. Enter information in the following fields and click on create.
 - a. **Phone Number:** A valid mobile phone number including international area code (e.g. **+39 02 29060603**).
 - b. **Service Type:** SMS
 - c. **Text:** DAP test
7. The mobile phone number (6a) should receive the text message (6c) with a URL to the infection package.

6.2 Results

Please fill the table below indicating the result of the test with respect to the expected outcome.

| | |
|--|--|
| AirCard Watcher shows that the SIM card is connected to a local mobile provider | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |
| The Console indicates that the SMS has been successfully delivered. | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |
| The mobile phone number received the SMS with text and link to the infection package | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |

7 Tactical Network Injector

The scope of this test is to ensure that the Tactical Network Injector (TNI) is able to sniff and change the Target's network traffic, applying the infection.

7.1 Procedure

Steps for this test case are performed on the Tactical Network Injector (TNI) laptop and on the Console, as listed below:

1. On the Tactical Network Injector (TNI) laptop, ensure that the Backend server and the Target computer are on the same network (wired or wireless) and reachable.
2. On the Tactical Network Injector (TNI) laptop, ensure that the Target's network traffic is visible.
3. Logon on the Console using the *System Administrator User*.
4. From the *System -> Network Injectors* panel, create a new injector with name *Test Injector* and specify the right IP address.
5. Logoff the *System Administrator User* from the Console.
6. Logon again on the Console using the *Technician User*.
7. From the *System -> Network Injectors* panel, select the *Test Injector* injector and press the *Add a new rule* button.
 - a. **Target:** Test Target
 - b. **Ident:** TACTICAL
 - c. **Resource pattern:** *.exe
 - d. **Action:** INJECT-EXE
 - e. **Factory:** Test Desktop
8. Start the Tactical Network Injector (TNI), run the Tactical Control Center application and click on *Config*.
9. On the Console, press the *Apply rules* button and ensure that the new configuration is correctly received by the Tactical Network Injector (TNI) laptop and successfully applied.
10. On the Tactical Control Center application, click on *Start* and then on *Reauth all* button to get the IP address of the Target. Ensure the *Last website* column of the Target is shown. Select the Target and click on *Infect*.
11. Using a Target Windows Desktop, download Skype application from <http://www.skype.com>.
12. Run the downloaded Skype.
13. On the Console, verify that a new Agent is created for the Target computer.

7.2 Results

Please fill the table below indicating the result of the test with respect to the expected outcome.

| | |
|-------------------------------|--|
| New Injector created | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |
| New rule created and deployed | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |

| Injector correctly displayed Target's IP address | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |
|--|--|
| Injector correctly displayed Target's last website | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |
| Target successfully infected by the Injector | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |

8 Agent Creation & Lifecycle

The scope of this test is to create and verify Agents.

Upon completion of this test the Client shall have one (1) Desktop Agent and one (1) Mobile Agent.

NOTE: The result of this test case is a pre-requisite to subsequent test cases. Do not delete the output files until all the test cases are completed.
Modify the name of each output file to avoid accidental overwriting.

NOTE: Agents should be built only for platforms included in the Client's license.

8.1 Procedure

Steps for this test case are performed on the Console, as listed below:

1. Logon using the *Technician User*.
2. Open the *Test Desktop* factory Advanced Configuration panel and press the Build button.
3. Choose the Silent Installer Agent and select a client's available platform to infect.
4. Open the *Test Mobile* factory Advanced Configuration panel and press the Build button.
5. Choose the Installation Package Agent and select a client's available platform to infect.

8.2 Results

Please fill the table below indicating the result of the test with respect to the expected outcome.

| Silent Installer Agent created | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |
|------------------------------------|--|
| Installation Package Agent created | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |

9 Target Lifecycle

The scope of this test is to ensure that:

1. An Agent is installed on desktop and/or mobile target platform(s).
2. The Agent is able to collect evidences and synchronize with the Collector.
3. Evidence collected by the Agent is visible on the Console.
4. When requested, the Agent is removed from the target system.

The tests included in this section will be performed on the following platforms:

Desktop

| Platform | Vendor | Model | OS Version |
|----------|--------|-------|------------|
| | | | |
| | | | |

Mobile

| Platform | Vendor | Model | OS Version |
|----------|--------|-------|------------|
| | | | |
| | | | |

9.1 Procedure

Steps for this test case are mainly performed on the Console, as listed below:

1. Logon using the *Evidence Analyst* User.
2. Install the Agent using a vector suitable to the target platform.

NOTE: On Android platform, enable the option *Unknown sources* in *Settings -> Application* menu before the installation. Reboot the device once the Agent is installed.

NOTE: On mobile, after the Agent installation, wait for the device to go in standby mode to allow the synchronization.

3. From the *Operations -> Test Operation -> Test Target* panel, verify that a new icon is created for each infected device, select it and click *Add to Dashboard*.

NOTE: On desktop Windows, synchronization may take as long as 5 minutes. Some interaction with the keyboard or mouse may be required.

NOTE: On desktop Windows, once the Scout icon is present upgrade the Agent.

4. From the Dashboard panel, verify that evidences are correctly displayed.
5. From the *Operations -> Test Operation -> Test Target* panel, for each newly infected device click *Close*.
6. Wait for the next synchronization and check that the *Uninstall* flag is set.

9.2 Results

Please fill the table below indicating the result of the test with respect to the expected outcome.

Desktop

| Synchronization performed | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |
|--------------------------------------|--|
| Agent update to Elite (Windows only) | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |
| Data received and displayed | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |
| Agent closed | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |

Mobile

| Synchronization performed | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |
|-----------------------------|--|
| Data received and displayed | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |
| Agent closed | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |

10 Backup

The scope of this test is to ensure that the Backup feature is operating correctly.

10.1 Procedure

Steps for this test case are mainly performed on the Console, as listed below:

1. Logon using the *System Administrator User*.
2. From the *System -> Backup* panel, create a *New Backup Job*.
 - a. **Enabled:** *CHECKED*
 - b. **What:** metadata
 - c. **When:** Time 0:0 UTC Every 1 of the month
 - d. **Name:** Test Backup
3. Select the newly created backup job and click *Run Now*.
4. Verify that the backup job is completed successfully and that files are found in the designated location (C:\RCS\DB\backup).

10.2 Results

Please fill the table below indicating the result of the test with respect to the expected outcome.

| New backup job created | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |
|------------------------------------|--|
| Backup job successfully executed | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |
| Backup files are correctly created | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |

11 Connector

The scope of this test is to ensure that the Connector feature is operating correctly.

11.1 Procedure

Steps for this test case are listed below:

1. Logon using the *System Administrator User*.
2. From the *System -> Connectors* panel, create a *New Connector*.
 - a. **Enabled:** *CHECKED*
 - b. **Name:** Test Connector
 - c. **Path:** Test Desktop
 - d. **Type:** JSON
 - e. **Keep the evidence:** *CHECKED*
 - f. **Destination:** C:\
3. Wait for new evidences to be synchronized and verify that the Connector outputs JSON and accessory files to the designated location.

11.2 Results

Please fill the table below indicating the result of the test with respect to the expected outcome.

| New Connector created | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |
|---|--|
| Connector exported evidences successfully | <input type="checkbox"/> N/A <input type="checkbox"/> OK <input type="checkbox"/> Error: |

Delivery Certificate

Issued by the Client to Hacking Team

The following items (being either the Licensed Software or part of the Licensed Software) have been accepted for the purpose of this Agreement.

| Item | Value | Item | Value |
|-------------------------|-------|-------------------|-------|
| Users | | Agents | |
| Desktop platforms | | Mobile platforms | |
| Backend servers | | Frontend servers | |
| Anonymizers | | Network Injectors | |
| Remote Mobile Installer | | Alerting | |
| Intelligence | | Connectors | |
| OCR | | Translation | |

LNx = LINUX, OSx = OS X, WIN = WINDOWS, AND = ANDROID, BKB = BLACKBERRY, IOS = IOS, WPH = WIN PHONE

Other conditions attached to the Delivery Certificate.
(specify here if there are any conditions attached to the Certificate of Acceptance)

Client

Full name

Title

Signature

Hacking Team

Full name

Title

Signature

Date