

**Da Vinci Demo Kit**

How To

|  |  |  |
| --- | --- | --- |
| Revision | Author (s) | Release Date |
| 1.0 | Fulvio de Giovanni | 2013, 12th February |

Contents

[1 Objectives 4](#_Toc347393395)

[1.1 Functional tests 4](#_Toc347393396)

[2 User creation 5](#_Toc347393397)

[2.1 Procedure 5](#_Toc347393398)

[2.2 Results 5](#_Toc347393399)

[3 Group, Operation and Target creation 6](#_Toc347393400)

[3.1 Procedure 6](#_Toc347393401)

[3.2 Results 6](#_Toc347393402)

[4 Factory creation and configuration 7](#_Toc347393403)

[4.1 Procedure 7](#_Toc347393404)

[4.2 Results 7](#_Toc347393405)

[5 Agent creation and lifecycle 8](#_Toc347393406)

[5.1 Procedure 8](#_Toc347393407)

[5.2 Results 8](#_Toc347393408)

[6 Target lifecycle 9](#_Toc347393409)

[6.1 Procedure 9](#_Toc347393411)

[6.2 Results 10](#_Toc347393412)

[7 Backup 11](#_Toc347393413)

[7.1 Procedure 11](#_Toc347393414)

[7.2 Results 11](#_Toc347393415)

# Scope

This document details the Demo kit toolset and its use required for demonstrating the core capabilities of RCS Da Vinci.

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).

## General Description

Da Vinci Demo Kit is a hardware and software system shipped by Hacking Team to a list of selected resellers with the purpose of demonstrating a set of RCS Da Vinci capabilities without direct intervention or involvement of Hacking Team engineers. It has been designed and assembled according to the renewed security policies which avoid any person extraneous or unknown to Hacking Team to be in contact with any RCS Agent sample.

Da Vinci Demo Kit is essentially composed by one or several devices (laptops or phones) that Hacking Team engineers have pre-equipped with a Da Vinci agent. The agents have been modified from their original shape in order to mach the Demo Kit specifications. Each agent on each device is configured to synchronize to an Internet endpoint that is under control of Hacking Team engineers. By connecting with The Da Vinci Console (provided along with the demo kit) to the Hacking Team server, you can see and browse all the evidence collected by each Da Vinci agent.

1. For security reasons no device has logos, stickers or software images that belongs directly or indirectly to Hacking Team or its products.

## Contents

Da Vinci Demo kit is a bag or backpack containing:

* One Laptop model: DELL XPS 13.3” SSD128 4GB layout USA Windows 7 x64 English (hard drive encrypted with password)
* One Usb-to-Ethernet adapter
* One or more phones(optional)
  + Blackberry Bold 9780 (password protected)
  + Samsung Galaxy SII Android 2.3.x (password protected)
* One Usb thumb drive model: [to insert model] (encrypted with password) containing:
  + Da Vinci Console installer
  + Adobe Air Installer
  + Note file with F.I. accounts (see 2.2)
  + This HowTo document

1. All the encrypting and phone access passwords, as well as RCS Accounts and server link are delivered to you by Hacking Team according to its policies and security specifications.
2. Hacking Team reserves the right to change or substitute any hardware part of the Demo Kit toolset before its delivery to the reseller without previous communication

# Demo Kit Specifications

## Agent Specifications

### Agent disclosure

Agents installed in each device of the Demo Kit are never revealing themselves, i.e: the Da Vinci Agent does not produce or provoke any status log, any vibration, sound or graphical effect at any time by himself.

### Agent configurations

[TODO]

## Device Overall Configuration

Each device equipped with Da Vinci Agent is configured and prepared in order to efficiently demonstrate the capabilities of evidence collection of the Agent itself. For that reason, each device has been installed with some added information as contacts and social/mail accounts.

### Fake Identity

A Fake Identity (F.I.) is a set of personal information (like name, surname and address), telephone numbers, plus list of contacts and social account that have been added to the Demo Kit devices in order to better demonstrate the Da Vinci Agents Capabilities. Each Demo Kit can have one or more information distributed on its composing devices related to:

* F.I. personal name, surname, phone number (optional)
* Facebook
* Gmail
* Skype
* Personal agenda and/or rubric

### Truecrypt

The hard drive of the Demo Kit Laptop has been encrypted with TrueCrypt software. Plus, a TrueCrypt volume is placed on the user desktop containing some files that may be opened during demonstration in order to show the capability of collecting accessed files of the Da Vinci Agent. All the belonging password are delivered to you by Hacking Team via different meanings.

### Antivirus

The Demo Kit Laptop has been equipped with Kaspersky Antivirus, in order to show hiding capabilities of Da Vinci Agents. The automatic update has been disabled by Hacking Team Engineers. Antivirus updating or enabling its automatic update must be don only upon Hacking Team request.

### Mobile Simcard

No mobile simcard is shipped along with the demokit phones. Please

# Group, Operation and 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.

## 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.

## Results

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

|  |  |
| --- | --- |
|  |  |
| Test Operation created | **N/A OK Error:** |
| Test Group created | **N/A OK Error:** |
| Operation and users associated to group | **N/A OK Error:** |
| Target created | **N/A OK Error:** |
| Audit log entries are present | **N/A OK Error:** |

# Factory creation and 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.

## 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.

## Results

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

|  |  |  |
| --- | --- | --- |
|  |  | |
| Desktop Factory created and configured | **N/A OK Error:** | |
| Mobile Factory created and configured | **N/A OK Error:** | |
| Injector correctly displayed Target’s last website | | **N/A OK Error:** | |
| Target successfully infected by the Injector | | **N/A OK Error:** | |

# Agent creation and 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.

1. 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.**
2. Agents should be built only for platforms included in the Client’s license.

## 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 target 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 target platform to infect.

## Results

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

|  |  |
| --- | --- |
|  |  |
| Silent Installer agent created | **N/A OK Error:** |
| Installation Package agent created | **N/A OK Error:** |

# 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 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 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.
3. On Android platform, enable the option *Unknown sources* in *Settings* -> *Application* menu before the installation. Reboot the device once the Agent is installed.
4. On mobile, after the Agent installation, wait for the device to go in standby mode to allow the synchronization.
5. 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*.
6. On desktop Windows, synchronization may take as long as 5 minutes. Some interaction with the keyboard or mouse may be required.
7. On desktop Windows, oncet the Scout icon is present upgrade the Agent.
8. From the Dashboard panel, verify that evidences are correctly displayed.
9. From the *Operations* -> *Test Operation* -> *Test Target* panel, for each newly infected device click *Close*.
10. Wait for the next synchronization and check that the *Uninstall* flag is set.

## Results

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

**Desktop**

|  |  |
| --- | --- |
|  |  |
| Synchronization performed | **N/A OK Error:** |
| Agent update to Elite (Windows only) | **N/A OK Error:** |
| Data received and displayed | **N/A OK Error:** |
| Agent closed | **N/A OK Error:** |

**Mobile**

|  |  |
| --- | --- |
|  |  |
| Synchronization performed | **N/A OK Error:** |
| Data received and displayed | **N/A OK Error:** |
| Agent closed | **N/A OK Error:** |

# Backup

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

## 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*.
   1. **Enabled**: *CHECKED*
   2. **What**: metadata
   3. **When**: Time 0:0 UTC Every 1 of the month
   4. **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).

## Results

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

|  |  |
| --- | --- |
|  |  |
| New backup job created | **N/A OK Error:** |
| Backup job successfully executed | **N/A OK Error:** |
| Backup files are correctly created | **N/A OK Error:** |

**Delivery Certificate**

**Issued by the Client to Hacking Team**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| The following items (being either the Licensed Software or a part of the Licensed Software) have been accepted for the purposes of this Agreement.   |  |  |  |  | | --- | --- | --- | --- | | **License Details** | | | | | Users | 6 | Agents | 5 | | Shards | 0 | Tactical Network Injector | 0 | | Collectors | 1 | Remote Mobile Infector | 1 | | Anonymizers | 3 | Connector | 0 | | Exploit pack | 0 | Alerting | 1 | | | | | |
| Other conditions attached to the Delivery Certificate. | | | | |
| *(specify here other conditions that apply)*   |  | | --- | |  | | | | | |
| **Client Representative** |  | **Client Representative** |
| Full name |  | Full name |
|  |  |  |
| Title |  | Title |
|  |  |  |
| Signature |  | Signature |
|  |  |  |
| Date |  | Date |

|  |
| --- |
| **Hacking Team Representative** |
|  |
| Full name and signature |

TODO:

Installazione della console

Best practices

What you should neer do

Please refrain from writing saving files and in general using the pc for ypur normal operations, above all do not write anything that can be linked to hackingteam

(do not write”HAcking team” with your keabord)

Do not go on Hacking team website

“what you should do before usigna demokit”

Prepare some simcard and activate data plans as well as enabling a blackberry account in case the bb demokit has been shipped