Remote Control System DEMO kit

The Remote Control System DEMO kit is a bootable CD-ROM that can install the RCS backdoor on any Microsoft Windows computer using an offline infection vector.

All the captured informations are sent to the demo server, and you need to use RCSConsole in order to access and view collected data.

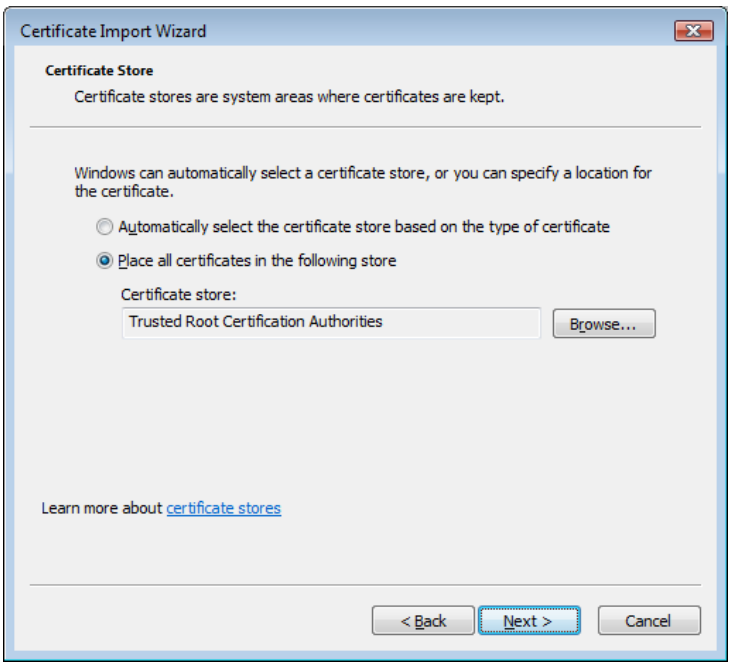
You should use a computer as target for infection, and another one for RCSConsole.

RCSConsole installation

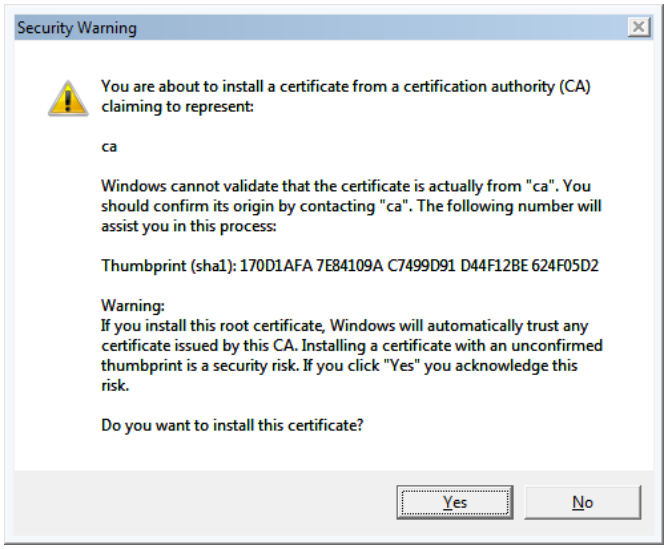
In order to use RCSConsole you need a computer with a graphical resolution of 1280x1024 pixels. Windows Vista is suggested as the optimal system to use RCSConsole.

(the following instructions are for Microsoft Windows Vista, but you can use other operating systems)

- Install Adobe AIR (you can download the latest version from *http://www.adobe.com/*)
- Install the TrueType font file (right-click on *font.ttf* and select “Install”)
- Install the CA certificate (right-click on *ca.crt* and select “Install Certificate”)
  - Click “Next >”
  - Select “Place all certificates in the following store” and click “Browse...”
  - Select “Trusted Root Certification Authorities” and click “OK”



  - Click on “Next >”
  - Click “Finish”

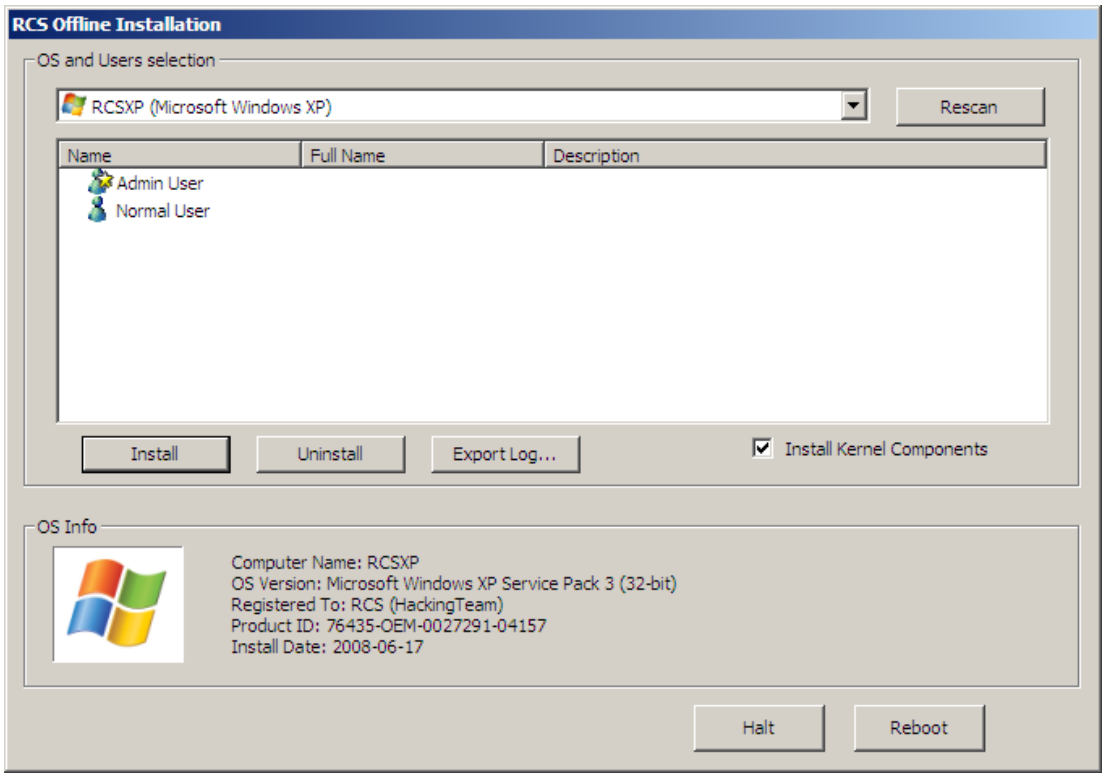


- Click “Yes”, then click “OK”

- Install RCSConsole (double-click on RCSConsole.air file and follow the wizard)

Backdoor installation

The offline infection vector must be booted from the CD-ROM drive (check your BIOS settings). After the startup screen, RCS Offline Installation will appear.



In the dropdown at the top, you can find all the systems that can be infected by the backdoor, either on internal or external hard drives: entries with colored logo are supported by RCS, while grayed ones are recognized by the system but you cannot infect them. When you select an operating system, some useful data are displayed at the bottom of the screen in the OS Info frame.

If you connect an external hard drive, you can click on “Rescan” to add new entries to the list.

Users are listed when you select an entry: only users with colored icons can be infected by RCS.

You can recognize user attributes looking at the different icons:

-  administrator
-  normal user
-  domain user with a local profile

To install the backdoor you have to select one or more users and then click on “Install”, then confirm and check that a green sign appears near the user. You can recognize the infection status for an user looking at the different icons:

-  backdoor is correctly installed
-  backdoor installation is broken/corrupted

To uninstall the backdoor you have to select one or more users and then click on “Uninstall”, then confirm and check that the green sign disappears near the user.

You can terminate the RCS Offline Installation process clicking on “Halt” or “Reboot”.

Backdoor configuration

The backdoor provided with the DEMO kit has a default configuration that shows all the main capabilities of the product. This configuration cannot be changed by the user.

The backdoor connects to the HackingTeam demo server in order to send collected data, that can be accessed using the RCSConsole. This connection is performed automatically every 3 minutes, but you can force an immediate synchronization running the *charmap.exe* utility.

The configuration collects the following data:

- Started/stopped applications
- Files (pdf, rtf, doc, docx, xls, xlsx) up to 500Kb and newer than 01/01/2010
- VoIP calls and chat sessions (Skype)
- Clipboard contents
- Device information
- Email messages newer than 01/01/2010
- Mouse clicks (for virtual keyboards and pin pads)
- Saved passwords
- Snapshots (every 3 minutes)
- Websites URLs

If needed, you can uninstall the backdoor online running *calc.exe*.