Offensive security technology

Remote Control System

Offensive security technology

Remote Control System is a **stealth** investigative tool for law enforcement agencies for the computer's investigations. It permits *passive* monitoring and *active* control of all data and processes on a selected target computers. Such computers might or might not be connected to the Internet.

Capabilities

Remote Control System permits the interception, monitoring and logging a variety of the information on the target computer:

- Connections to the web sites
- Received/Sent emails
- Documents which are created/stored/edited on a computer
- Any key typed on the keyboard, such as passwords, access keys, names, etc.
- Any document which is printed by computer
- Any voice conversation originated or received by computer, such as **Skype** conversations

Remote Control System is an electronic eavesdropping device. After it is installed on the target computer, it "listens to" what is "happening" inside the computer.

Remote Control System hides itself deeply inside the computer:
- No files get modified at installation phase
- No new files are created on the computer's hard disk
- No new processes are in execution
- No new connections done from/to the network (if the computer's network is connected)

Remote Control System is more than an eavesdroping device. In fact, it can:
- Access any user's information
- Execute any command on the target computer
- Detect particular events and act accordingly (if then logic)

Also, it can be installed:
- Without physical access to the remote computer (online installation)
- By means of supported media such as CD and USB drive ("in-loco" installation)

Life cycle

Remote Control System can be configured before the installation, in order to fulfill a specific requirements from the different investigative scenarios. After the configuration, the Remote Control System's **infection module** is installed into the **target** computer, by means of physical or logical techniques. After this process, the Remote Control System is controlled by using the Remote Control System's **control station**, which is, an encompassing **dashboard** used by investigators. Using the control station, the investigators can **re-program** Remote Control System remotely for a maximum efficiency.

HackingTeam

Uniqueness solution for the customer isolation

Each **Remote Control System** bug is virtually **unique** for each customer. What means that, the bugs generated by each Remote Control System systems are crafted differently, both in terms of the logical-binaries and the operating features. The different encryption keys configuration files and parameters guarantee that the "collision" between two Remote Control System products is technically infeasible.

Like an eavesdropping bug

Remote Control System, its most valuable feature is the **stealthness**. Remote Control System mimics user's behavior in order to make very difficult to tell, even for the most sophisticated user, that a not user-generated "activity" is going inside to the target computer. In fact, it is virtually impossible, for any monitoring program running on the computer itself, to detect the Remote Control System in function, either in terms of the network or system activities. Remote Control System is invisible to the most commercial protection systems such as anti-virus and anti-spyware software, personal firewalls, networks, process monitors and network's analyzers.

Physical and *online* installation

Remote Control System can be installed to the remote computer by means of both physical and logical ways:

- Physically, the bug can be installed by physically accessing to the computer. The computer might or might not being turned on. It is necessary to open the CD tray, insert a specially-crafted CD bug-infection, close the tray and turn on the computer (if needed). Alternatively, the job can be done by merely inserting a specially-crafted USB infection-pen in one of the computer's USB ports.

- Logically, the bug can be installed to the remote computer by means of a variety of *automatic hacking* technologies, included in the Remote Control System package.

Remote Control System the Hacking Team's Product

Remote Control System has been designed by Hacking Team, a leading provider of the computer's security solutions. Hacking Team's engineers have matured a very significant experience in the sector of hacking into the systems, and they are widely recognized among the best "*ethical hacking*" experts by the scientific community.

]HackingTeam[

Contacts: Mr. David Vincenzetti - info@hackingteam.it
HT Srl - Via Moscova, 13 - 20121 Milano - Italy
tel. +39 022 9060 603 - www.hackingteam.it

]HackingTeam[