REMOTE CONTROL SYSTEM

**A bugging device for computer crime investigations
and intelligence collection**

]Hacking**Team**[

REMOTE CONTROL SYSTEM

A bugging device for computer crime investigations and intelligence collection

Offensive security technology

The **Remote Control System** is a **stealth** investigative tool that can be used by law enforcement agencies for computer investigations. It enables all data and processes to be **passively** monitored and **actively** controlled on selected target computers, regardless of whether or not they are connected to the Internet.

Features

The **Remote Control System** enables the detection, monitoring and logging of a variety of information on target computers:
- Connections to Websites
- Received/sent e-mails
- Documents created, stored and deleted on a computer
- Any key typed on the keyboard, such as passwords, access keys, names, etc.
- Any document printed from the computer
- Any voice conversation originated or received from/on the computer, such as Skype conversations
- Remote audio spy
- Chat and instant messaging

The **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.

The **Remote Control System** hides itself deep inside the computer without:
- Modifying files during the installation phase
- Creating new files on the computer's hard disk
- Running new processes
- Establishing new network connections (if the computer is part of a network)

The **Remote Control System** is more than an eavesdropping device. It can:
- Access any user's information
- Execute any command on the target computer
- Detect specific events and act accordingly (If/ Then logic)

In addition, it can be installed:
- Without physically accessing the remote computer
- Using supported media like CD and USB drives ("on-site" installation)

Life cycle

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

Unique solution for maximum customer protection

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

Like an eavesdropping bug
Remote Control System: its most valuable feature is **stealthness**. The Remote Control System mimics the user's behavior in order to make it very difficult to identify, even for the most sophisticated user, a non user-generated "activity" on the target computer. It is in fact virtually impossible for any monitoring program running on the computer to detect the Remote Control System using network or system activities. The Remote Control System is invisible to most commercial protection systems such as anti-virus and anti-spyware software, personal firewalls, networks, process monitors and network analyzers.

Physical and online installation

The **Remote Control System** can be installed on the remote computer using physical and logical techniques:
- Physically, the bug can be installed by materially accessing the computer, which can be running or off. Example: the infection module is installed by opening the CD tray, inserting a specially-crafted CD bug-infection module, closing the tray and switching the computer on (if needed).
- Logically, the bug can be installed on the remote computer by means of one of the many **automatic hacking** technologies included in the Remote Control System package.

Remote Control System by Hacking Team

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

]Hacking Team[