RCS – Remote Control System
Datasheet

Table Of Contents

Overview

Remote Control System is the Ethical Hacking Solution for governmental agencies. It is a stealth investigative tool dedicated to law enforcement and security agencies for digital investigations. It is an eavesdropping software which hides itself inside the target devices and enables both active data monitoring and process control.

Sensitive data is often exchanged using encrypted channels or not exchanged at all; sometimes it is exchanged using networks outside of your agency's reach. Remote Control System, being totally invisible to the target and bypassing protection systems such as antivirus, antispyware and personal firewalls, gives you the possibility to gather such information.

Features

Following are the main characteristics of Remote Control System, including an overview of its Agent's capabilities and of the infection vectors available. Tools for controlling a target network are introduced, together with information about the architecture of the product, about the support channels and about the Team behind RCS.

Agent Desktop

- *Multiplatform*
  - Windows 8
  - Windows 7
  - Windows Vista
  - Windows XP
  - MacOSX Mountain Lion
  - MacOSX Lion
  - Linux
- *Stealth*
  - Is tested daily against 40 different Antiviruses and anti-rootkits
  - Process invisible to any process explorer
  - Its use of storage on the hard drive is randomly located, totally encrypted and invisible to the system
- *Secure, Invisible and Anonymous Communication*
  - Custom and dynamic communication protocol, extremely light and impossible to fingerprint
  - Bypasses Personal Firewalls and IDS: as long as the user can surf the web, the Agent can send data to Headquarters
  - All data connections are authenticated and encrypted with military grade encryption protocols
  - Identity and location of the Headquarters are hidden through the use of Anonymizers
- *Extraordinary data interception capabilities*
  - Contacts information
  - New and past appointments from different calendars
  - Monitoring and recording of VOIP Calls (Skype, LiveMessenger, and more)
  - Live pictures taken with the device webcam
  - Chat and messages from different Social Networks (Facebook, Twitter, and more)
  - Mail from different Mail Clients and Web Interfaces (Outlook, Windows Mail, GMail, and more)
  - Detailed information on hardware and software on the device
  - Automatic and on-the-fly interception and copy of any file opened, even when not available on the hard disk
  - Keylogger with the possibility to capture also on-screen keyboards
  - Live recording from the microphone of the device
  - Download of passwords stored on the device (Browsers, Mail clients, etcetera)
  - Position of the device, even when no GPS is available
  - Screenshots
  - List of visited websites
  - Download and Upload of files from the device
  - More…
- *Smart and autonomous*
  - All executables (Agents) created are totally different from each other

- Is able to determine the real IP address of target, even when TOR or other anonymizers are used
- Can be configured to execute actions according to many flexible events, giving it the possibility to act autonomously
- Lets the operator execute commands on the device
- Is able to protect itself against network sniffers or forensic tools
- Can automatically spread itself to other devices (even mobile)
- Easily upgradable with one click

Agent Mobile

- *Multiplatform*
  - Blackberry
  - iOS
  - Android
  - Symbian
  - Windows Mobile
- *Stealth*
  - Is tested daily against the main Antiviruses
  - Invisible to user
- *Secure, Invisible and Anonymous Communication*
  - Custom communication protocol, extremely light and impossible to fingerprint
  - Bypasses Personal Firewalls and IDS: as long as the user can surf the web, the Agent can send data to Headquarters
  - Can communicate with Headquarters through WiFi, LTE, 3G or GPRS connection
  - All data connections are authenticated and encrypted with military grade encryption protocols
  - Identity and location of the Headquarters are hidden through the use of Anonymizers
- *Extraordinary data interception capabilities*
  - Contacts information
  - New and past appointments from calendar
  - History of calls and calls recording
  - Possibility to listen to an ongoing conversation in real time
  - Sent and received e-mails and SMS
  - Chat from BBM, WhatsApp and other Messengers
  - Live pictures taken with the camera on the device
  - Detailed information on hardware and software on the device, including cell network information
  - Keylogger
  - Remote Audio Surveillance using the phone's microphone (no need to place a call)
  - Retrieve of passwords saved on the device
  - Position of the device, with and without use of GPS
  - Screenshots
  - List of visited websites
  - Download and Upload of files from the device
  - More…
- *Smart and autonomous*
  - All Agents created are totally different from each other
  - Can be configured to execute actions according to many flexible events, giving it the possibility to act autonomously
  - Can be controlled with covert SMS and send back information even when no data connection is available
  - Easily upgradable with one click

Infection Vectors

Desktop:

- *Through Website:* the target will be infected upon visiting a specified website; thanks to a proprietary zero-day exploit, no interaction is needed for the user visiting the infected website (such interaction is required without the use of a zero-day exploit).
    - All browsers are supported
    - No user interaction needed
    - The infecting website can be fully customizable
    - Can be integrated with any existing websites
    - Can target any user visiting the website, or a subset of them, according to needs
    - The link can be sent through email
    - Full support from HackingTeam for scenario analysis and website configuration
- *Through documents:* zero-day exploits are available, making it possible to infect a device:
    - Can be sent through email, including GMail
    - Microsoft Word Documents
    - Microsoft Excel Documents
    - PDF Documents
    - More…
- *Inside Application:* the Agent can be melted with any application; when run, only the original application will be visible to the user, while the Agent will be silently installed.
    - Agent can be disguised with any other Application
    - Perfect for social engineering attacks
    - Melted application can be remotely delivered
- *From the network:* TNI and NIA will let you infect any target on a LAN or connected to any ADSL; see the respective sections for details
- *Physical Access:* when physical access to the device is available, infection can be performed whether the computer is running or is turned off:
    - Without need of any user password
    - Infection performed in as little as few seconds
    - Computer can be unlocked if necessary
    - No limitations on hibernated systems
    - Easy to use: no training required
    - Documents, Images and other files can be retrieved from the target device, even without infecting it
- *USB Device:* the infection will be performed upon insertion into the target device, without user interaction:
    - Will perform infection in few seconds
    - Easy to use: no training required
    - Any USB Pendrive or other devices can be used
    - Can be used in covert operations

Mobile:

- *Physical Access:* when physical access to the device is possible, local installation can be performed.
- *Inside Application:* the Agent can be melted with any application; when run, only the original application will be visible to the user, while the Agent will be silently installed.
    - Agent can be disguised with any other Application
    - Perfect for social engineering attacks
    - Application can be remotely delivered
- *Through link:* a Web Link can be delivered to the person to be infected:
    - Can be sent through email. Including GMail
    - The link address can be hidden
    - Perfect for social engineering attacks

- *Through Message: a* Message containing an infecting link can be sent to the target. With this infection vector:
    - Agent can be configured to appear as any application (for example, as an Operating System update)
    - Through the use of a particular messaging protocol, the link will be automatically loaded and prompted to the user
    - Any text can be included in the message

Tactical Network Injector (TNI)

HackingTeam's *Tactical Network Injector* (TNI) is a portable solution to infect targets connected to a WiFi or wired network. It provides the operator with everything needed in order to crack a WiFi network, join it, identify the interested target and deploy the RCS agent. The TNI embeds a patented technology that permits it to operate without being inline.

WiFi Cracking Capabilities:

- *Wired Equivalent Privacy (WEP 64 and 128 bit):* exploiting protocol vulnerabilities, a WEP passphrase can be exposed in as little as 3 minutes;
- *WiFi Protected Access (WPA/WPA2):* using dictionary-based attacks, the TNI will automatically crack the WiFi password;
- *WiFi Protected Setup (WPS):* a special attack against the WPS protocol can be used to guarantee success in cracking a WiFi network.

Target Infection Capabilities:

The TNI supports the operator in the identification of the target on the field, discovering all hosts on the network and showing for each information that include:

- MAC Address
- IP Address
- Hostname
- Operating System
- Browser in use
- List of all visited website

The TNI supports different infection techniques:

- Injection takes place when the target visit any website on the Internet, without requiring any user interaction;
- Injection takes place when the target downloads any executable file (.exe) from the Internet;
- Injection takes place when user's applications try to update themselves;
- Injection takes place when the target user, prevented from viewing a video online, will perform the operations needed to see the video;
- Injection takes place when the TNI replaces any file with a different file provided by the operator.

Additional Features

- Emulate Rogue Wireless Access-Point providing free Internet Access for any computer, which will then be infectable;
- Unlock any computer when Locked
- Unlock Password-Protected Screensaver

- User password is not changed permanently
- Works with FireWire/1394, PCMCIA and Express Card
- Can retrieve Usernames and Passwords even for SSL/TLS-encrypted Sessions like Gmail
- Is delivered with additional batteries that can guarantee up to 35 hours of continuous operation, extra network cards and antennas: ready to be used on the field

Network Injector Appliance (NIA)

HackingTeam's *Network Injector Appliance* (NIA) is a solution designed to infect any target connected to the Internet. It includes the tools needed to identify and infect the desired target. The NIA embeds a patented technology that permits it to operate without being inline. The key features include:

- Is installed at Internet Service Provider's premises
- Doesn't need to be installed inline, thanks to a patented technology
- Different target identification possibilities:
    - IP Address or IP Range
    - MAC Address
    - DHCP Parameters
    - Radius Parameters
    - Content of packets through DPI
- Different infection techniques:
    - Injection takes place when the target visit any website on the Internet, without requiring any user interaction;
    - Injection takes place when the target downloads any executable file (.exe) from the Internet;
    - Injection takes place when user's applications try to update themselves;
    - Injection takes place when the target user, prevented from viewing a video online, will perform the operations needed to see the video;
    - Injection takes place when the TNI replaces any file with a different file provided by the operator.
- Available for 1GB and 10GB lines
- Easy management even when multiple NIA's are deployed
- Full support from HackingTeam in the implementation of any NIA Project.

Architecture

RCS Backend is totally internally developed and maintained. The main features include:

- High scalability and auto load-balancing, with the possibility to easily upgrade the system to *manage thousands of concurrent* targets
- Clearly divides front-end and back-end components and makes it possible to have geographically distributed systems
- Offers a single point of control for all operations, including one-click upgrade and configuration change for deployed agents
- Possibility to define highly granular user roles and privileges
- Read-only and integrated audit system
- Easy and intuitive Anonymizers configurations, which makes it easy to deploy, configure and dispose of anonymous proxies
- Easily creates custom reports on investigations and collected evidence

- Possibility to view and download all evidence from a single point, media evidence included
- Full text indexed search on all evidence, including images thanks to the integrated OCR
- Easily integrates with any third party Law Enforcement Monitoring Functionality (LEMF)
- Shows location of the device on Google Maps, giving the possibility to reconstruct the target's movements
- Integrated data mining engine for target profiling and evidence correlation: get real and useful information from the available evidence
- Evidence Protection (Court-proof Evidence according to European Standards)
- Automatic, "set and forget" backups

Thanks to an optional module, RCS is able to automatically translate evidence from any language to any other language, making it easy and immediate to understand the data freshly collected.

Training

HackingTeam will provide extended training, personalized according to Client's needs. Training possibilities include:

- Use of RCS
  - System Management
  - User Access Control
  - Agent Configuration
  - Agent Building and Deployment
  - Troubleshooting
- Ethical Hacking
  - Information Gathering
  - Network Scanning and Enumeration
  - Vulnerability Assessment
  - Vulnerability Exploitation
  - Privilege Escalation
  - Covering Tracks
  - Practical Software Exploitation
  - Wireless Intrusion
  - Password Cracking
- Operation Methodology
  - Scenario Analysis
  - In-house tests
  - Information Gathering
  - Email/SMS Spoofing
  - Email header analysis and tracking
  - Being anonymous on the Internet
  - Useful tools
- Social Engineering
  - The Social Engineering Cycle
  - Preparation
  - Person and website profiing
  - Social Attack
  - Persuasion techniques
  - Understanding the interlocutor

Support & Ticketing

Support to the client is guaranteed through the online Support Portal:

- Fast and competent answers
- Possibility to quickly review any ticket history
- Secure connection and information exchange
- Useful for news communication
- Immediate download of new releases and updates

Moreover, HackingTeam offers a *Custom Scenario Analysis* service. Taking advantage of this service, the Client will be able to share specific requirements with HT's experts and get custom solutions for maximum effectiveness. A solution can include development of custom code or engineering of ad-hoc devices, or anything that can help the Client reach her goal. The *Custom Scenario Analysis* service will be charged according to the complexity of the requirements and solutions involved.

The Team

Every single line of RCS is developed by HackingTeam: this means being able to quickly fix any bug and effectively customize the product according to Clients' needs.

HackingTeam can count innumerable high profile persons, with years of experience in the fields of security and hacking; many of the developers of RCS are well known in the security underground world.

RCS has a very fast and effective development cycle, with improvements and new features coming out often. The Client can expect:

- *Minor updates* every month: include bug fixes and security enhancements, keeping RCS bug free and invisible to updated and improved antiviruses and anti-rootkits
- *Updates* every 4 months: include improvements, such as new collection capabilities for the agents, support for new platforms or new versions of platforms or new features for an easier and more effective use of RCS
- *Major updates* every 15 months: include major new features, that both enhance the power of RCS and improve its architecture; major release can include change such as new data analysis capabilities or software architecture redesign.

New updates can be immediately downloaded from the secure Support Portal and autonomously deployed by the Client. The update installation process is easy and intuitive, and is able to automatically recognize the components that need to be updated on each part of the distributed RCS installation.