]HackingTeam[

Remote Control System “Da Vinci”

Whitepaper

Important Notice

HT s.r.l. shall bear no responsibility or liability to a client or to any person or entity with respect to liability, loss or damage caused or alleged to be caused directly or indirectly by any HT s.r.l. product. This includes, but is not limited to, any interruption of service, loss of business or anticipatory profits or consequential damage resulting from the use or operation of any HT products. Information in this document is subject to change without notice and does not represent a commitment on the part of HT s.r.l. The systems described in this document are furnished under a license agreement or non-disclosure agreement.

All information included in this document, such as text, graphics, photos, logos and images, is the exclusive property of HT s.r.l. and protected by international copyright laws. Permission is granted to view and photocopy (or print) materials from this document for personal, non-commercial use only. Any other copying, distribution, retransmission or modification of the information in this document, whether in electronic or hard copy form, without the express prior written permission of HT s.r.l., is strictly prohibited. In the event of any permitted copying, redistribution or publication of copyrighted material, no changes in, or deletion of, author attribution, trademark legend or copyright notice shall be made.

Document Approval

Revision	Author(s)	Release Date
1.5	Daniele Milan	18/05/2012

Table Of Contents

1 Overview

In modern digital communications, encryption is widely employed to protect users from eavesdropping.
Unfortunately, encryption also prevents law enforcement and intelligence agencies from being able to monitor and prevent crimes and threats to the nation’s security.

Remote Control System (RCS) is a solution designed to evade encryption by means of a software agent installed on the device to monitor. Evidence collection on monitored devices is stealth and transmission of collected data from the device to the RCS server is encrypted and untraceable.

All RCS installations are totally deployed at the Customer site, to guarantee total control on operations and security.

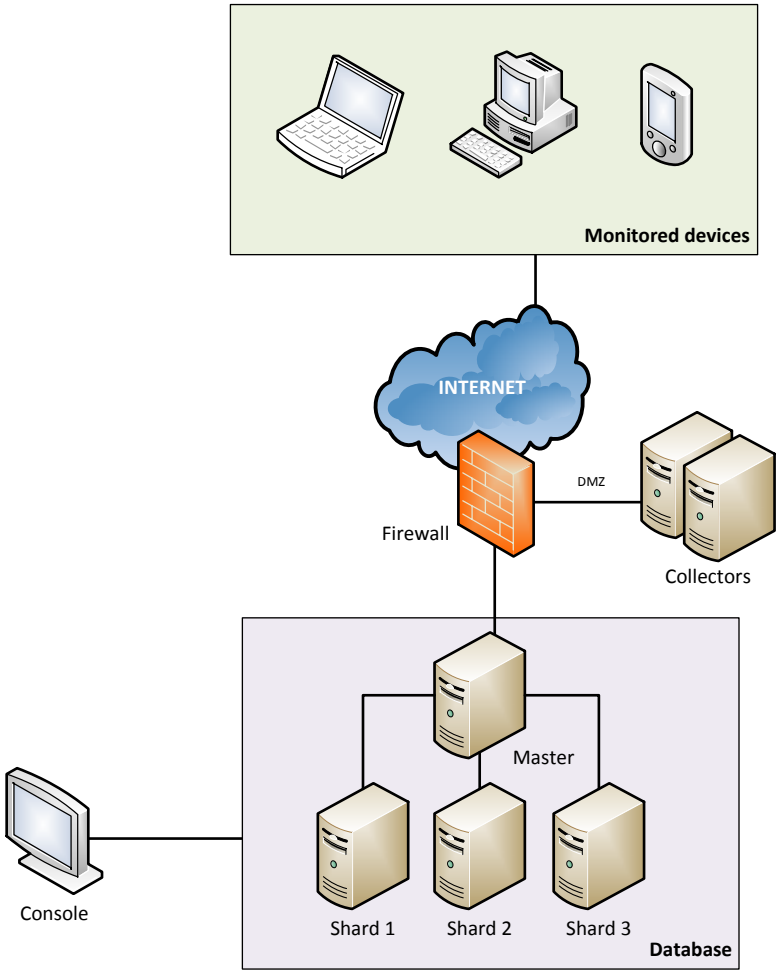

Figure 1 - Schema of RCS Installation

The RCS infrastructure is made up of different components: part of the components resides within the Customer’s network, part is to be installed on the devices to be monitored, and part can be placed anywhere on the internet, to prevent traceability and hide the connections coming from the monitored devices.

2 Customer Side Components

2.1 Collector

Collectors are the point of presence of RCS on the Internet, and the only way in for the Agents to contact the RCS Backend.

The main function of Collectors is receiving the Evidence from the Agents, and forwarding it to the Database for further processing. Collectors are also in charge of updating the Agents’ components, including their configuration, and sending them commands to perform special operations, like uninstallation.

Agents communicate with the Collectors using an encrypted and authenticated channel: no other component is capable of communicating with the Agents, and security is guaranteed by using strong double-layer encryption.

Agents need to reach the Collector anywhere they are, to maximize communication capabilities and give you control over the devices even when they’re on the other side of the world.

At least one Collector is needed in order to receive data from the Agents.

System requirements: Microsoft Windows 2008 R2 Standard (64bit)

2.2 Database

The Database is the core of the whole infrastructure: it stores all the Evidence collected from the targets and performs all the business logic.

RCS 8 *“Da Vinci”* introduces a new architecture that provides unmatched scaling capabilities: instead of scaling by switching to a more powerful, expensive server, scalability is obtained by adding more, less powerful servers, called Shards, and making them work in parallel.

By adding Shards, you will be able to monitor more Targets and dramatically increase the speed and storage capacity of your system: browsing the Evidence will be much faster, and you will be able to collect more information and retain it, always available, for longer times.

Every time you add a Shard, the database automatically balances itself, distributing the data according to the new resources made available: there is no need to perform complicated maintenance, it comes with autopilot.

A new “Set & Forget” backup system is integrated into the Database: choose what you want to backup, at what time and where to store it, and the system does the rest. You can backup the full database, make selective backups of a single Operation, Target or Agent, or even backup only the essential data for restoring, in less than 5 minutes, a perfectly operating copy of the system.

Server sizing depends mainly on the number of concurrent Devices monitored and the amount of Evidence stored.

System requirements: Microsoft Windows 2008 R2 Enterprise (64bit)

2.3 Console

RCS 8 *“Da Vinci”* introduces a brand new Console, vastly improved over the previous one: common flows of operations have been streamlined and simplified, a powerful **Search** feature is available to quickly access the desired information, and the whole Console have been re-designed to cope with the huge number of Targets, and the deriving amount of data, that the new Database is able to handle.

Configuring an Agent is now easier, and you can choose among two ways of doing it:

- **Basic:** allows for a quick and comprehensive configuration, taking you from zero to done in a few seconds: just a few clicks and the backdoor is ready.
- **Advanced:** gives finer control over the configuration, exposing all the options to let you come up with the most carefully studied, scenario fitting configuration you ever imagined. Even tough is more complex than the Basic, its drag & drop graphical representation makes it fast enough, even when you’re short on time.

The new **Search** capability, available almost everywhere with the Console, permits you to filter out the information you don’t care about at the time, and leave only the interesting bits. Perform searches with any criteria: by the name of the Agent you are looking for, or just a word in the description you’ve filled in when you created it. As soon as you start using it, you’ll realize that you can do without.

Role base access has been extended, introducing a new profile, the System Administrator, to the three already existing profiles:

- **Administrator**: manages users and groups, grant privileges, creates investigations, and audit the system to prevent abuses.
- **Technician**: prepares the vectors for Devices infection and configures the Agents’ behavior.
- **Analyst**: browses Evidence coming from the targets, tags and exports it for archival or further analysis.
- **System Administrator**: manages the components of the system at the hardware and software level.

Using the Alert feature, you can setup custom alerts and be warned in real time when Evidence of interest arrived: if desired, you can automatically set the Evidence relevance, to ease future searches.

All the Evidence collected is usable within the Console: you can visualize screenshots, listen to audio files, visualize their waveform and navigate maps of the collected locations. If further processing is required, each Evidence can be exported, in common file format, and imported in any third party software.

Within the Console you can monitor the health status of all the components of the system, with an integrated alerting module, that will promptly alert you in case of failure.

The Console can be installed on any computer.

Software requirements: Microsoft Windows 7 or Apple OS X

3 Target Side Components

3.1 RCS Agent

The Agent is the software that once installed on the target PC or smartphone to be monitored, collects all the desired Evidence.

Once collected, the Evidence is sent to the Collector by stealthily using the Internet connection of the monitored device: beware though that even if an Internet connection is not always available, the Agent will continue to collect the Evidence, waiting for better times to transfer it.

The Agent can be configured to collect all kinds of data from the target device: once collected, Evidence is stored encrypted and hidden on the device itself, until the Agent senses the opportunity to transfer it to the Collector.

The Agent behavior can be reconfigured at any time through the Console: a powerful event/action paradigm allows to define the Agents behavior, making them react differently according to the state of the Device and the external environment. For example, you may want to collect the Microphone audio only when the Device is within 50 meters of a meeting location, or you may want the Agent to go silent if any analysis that may spot its presence is performed on the Device.

Once configured, Agents are autonomous on their operation, even when they’re isolated from the Internet: no intervention by human operators is required.

All connections between Agents and Collectors are encrypted with strong algorithms and mutually authenticated, so there’s no risk of eavesdropping or data leakage. Moreover, the Agent is built to be non-attributable to the Customer that created it, to guarantee the safety of the Operation and the Customer, even in case of Agent disclosure and analysis.

The Agent is hidden from the user perspective, and resistant, during its whole lifetime, to most endpoint security suites available on the market, such as antivirus, personal firewalls and analysis tools. Furthermore, the Agent is capable of making itself permanent even if restoration technologies like DeepFreeze are active during its installation.

Agents can be uniformly controlled and configured through the Console, where all the peculiarities of the monitored Devices are transparent and automatically handled.

Specific functionalities may vary on different Platforms mainly due to hardware limitations: please refer to the Compatibility Grid to check for the available functionalities for the Platforms of interest to you.

3.1.1 Agent Deployment

Agents must be installed on target Devices in order to monitor them. A wide array of installation vectors is available to perform local or remote installations.

3.1.1.1 Local installation

When physical access to the Device is granted, local installation is usually very effective. Listed below are some examples of the Local installation vectors available:

- Booting/Running from USB/CD-ROM device (only for Desktops)
- Hard Disk physical connection (only for Desktops)
- SD/MMC Card infection (only for Mobiles)

3.1.1.2 Remote installation

Starting from the information available about your Target (email address, phone number, etc.) you should be able to identify the most effective installation vector. RCS provides all the possibilities to perform an installation on the Platforms that can be targeted. Some examples of the Remote Installation vectors available are listed here:

- Conceal the Agent within a native application, that once executed infects the Device;
- Use an exploit to embed the Agent within a PDF, a Word document or inside a Web page;
- Use the Network Injector to exploit the Internet connection of the Target and infect his PC or Mac while he browses the Web or downloads an application;
- Send an SMS to the Target’s smartphone, making it appear as an upgrade for the phone software: once accepted, the Agent will be on the Device.

3.1.1.3 Remote uninstallation

The Agent can be uninstalled from remote with a simple click. Once removed, the Agent and all its data is permanently deleted from the Device.

3.1.2 Evidence transmission

Evidence is transmitted from the Agent to its Collector using the communication channels available on the device. Agent’s configuration may instruct for a specific usage of these channels (e.g. use only WiFi and avoid 3G connections).

For Desktop Agents (Windows, OS X) transmission may be done using any wired or wireless Internet connection available. Within enterprise environments, where proxies or firewalls may be in place, credentials to authenticate against those devices are stolen from the target system and used to gain access to the Internet.

For Mobile Agents (BlackBerry, Android, iOS, Symbian) transmission happens by GPRS/UMTS/3G/4G data connections or WiFi. Even if those channels may be switched off by the user to save battery, the Agent is able to silently switch them on and use them for transmission, then shut them off again once done.

To avoid extra billing for the data connections used to send evidence, it’s possible to instruct Mobile Agents to use a different APN for evidence transfer connections.

Evidence transmission may be customized for each Agent by changing its configuration.

3.1.3 Offline evidence collection

Target devices may be unable to connect to the Internet for long periods of time. In that case, evidence shall be manually collected to prevent any loss of new evidence due to exhaustion of available space on the target device.

Two means of offline evidence collection are actually available:

- Bootable CD: a CD media from where to boot the target system. Allows evidence collection by saving it onto an external USB drive. Available for Windows and OS X.

- Bootable USB: a USB thumb drive from where to boot the target system. Evidence can be exported on an external USB drive. Available for Windows.

Once collected, evidence can be easily imported using the Console.

3.1.4 Collectable Evidence

Agents can collect different type of evidence depending on the type of Device they are running onto, either Desktop or Mobile, and the specific Platform targeted: please check the Compatibility Grid to verify what kind of Evidence can be collected from a specific Platform.

3.1.4.1 Desktop

On Desktops, an Agent can collect the following Evidence:

- **Facebook** chats and contacts
- **Gmail** emails
- Opened files (documents, images, data, etc.)
- Screenshots
- Visited web sites
- Mouse clicks
- Application passwords (Outlook, MSN, Internet Explorer, Firefox, etc.)
- Keystrokes (in any language)
- Copied and pasted text
- Printed documents
- Email
- **Location**
- Microphone audio
- Device information
- Camera Snapshots
- Calls made using **Skype**, MSN, Yahoo
- Instant Messaging (Skype, MSN, Yahoo, ICQ, etc.)
- Execute commands
- Upload and download files

3.1.4.2 Mobile

On Mobiles, an Agent can collect the following Evidence:

- Phone calls
- Address Book
- SMS and MMS
- Email
- Screenshots
- Location (Cell signal, Wi-Fi and GPS)
- Microphone audio
- Camera Snapshots
- SIM Information

3.1.5 Event/Action logic

Using an embedded event/action logic, the Agent can detect specific events and react with appropriate actions, giving it the chances to successfully face different scenarios and survive in the environment.

To give you an example of the capabilities of this event/action logic, here’s a list of events you can configure the Agent to react to, and the relative action that will be triggered:

Event	Action
The screen saver starts	Send the collected Evidence to the Collector
A given GPS position is reached	Start collecting the Microphone audio
Battery is running low	Stop collecting the Microphone audio, since it drains battery power
When a phone call is received	Take a snaphot with the front Camera, since probably our Target is looking at who’s calling, and he’s right in front of the Camera
After 30 days	Uninstall the Agent, since our Operation is over

Any event can be linked with any action, so that each time you can configure your Agent to fit your needs.

3.1.6 Communication

Agents for Desktop use standard Internet connectivity, wired and wireless, to communicate with the Collector, both in home and enterprise environments: the Agent is normally able to bypass network firewalls and proxies.

Agents for Mobile can be configured to use different ways of communication, where each connection type can be triggered by different events:

GPRS/UTMS/3G+: the Agent uses an existing data connection or forces the creation of a new one. A custom APN can be configured to avoid having the traffic generated by the Agent billed to the Target.

Wi-Fi: the Agent automatically recognizes open and preconfigured wireless Access Point (e.g.: airport, hotel, home) and connects with them in order to communicate with the Collector.

SMS: the Agent sends an invisible SMS containing valuable information such as SIM details or GPS position, especially useful when you’re on the field and you quickly need to find out where the Device is located.

USB: the Agent uses the PC Internet connection if the Device is connected via USB to synchronize its data or charge the battery.

3.1.7 OS compatibility

Agents for Desktop can be installed on following operating systems:

- Microsoft Windows XP, Vista and 7 (32/64 bit, all editions)
- Apple OS X 10.6 (Snow Leopard), 10.7 (Lion)

Agents for Mobile support the following platforms:

- Apple iOS 4.0, 4.1, 4.2, 4.3.3
- Nokia Symbian S60 3rd and 5th edition
- RIM BlackBerry 4.5, 4.6, 5.0, 6.0
- Google Android 2.2, 2.3

4 Internet Components

4.1 Anonymizers

Anonymizers are used to hide the real identity of the Customer to a Target that’s trying to track back to them, once the presence of the Agent have been discovered.

To avoid exposing the real IP address of the Collector, and therefore information that may lead to the identity of the Customer, Anonymizing nodes can be spread anywhere on the internet (see Annex) to route connections from the Agents through each of those nodes, before reaching the Collector.

Anonymizers can be safely placed in untrusted networks, even in foreign countries, since each connection is fully encrypted from the target to the frontend, and decryption is not possibile but on the Collector.

Anonymizers can be linked into one or more chains that can be fully controlled and monitored within the Console.