]HackingTeam[

Remote Control System “Galileo”

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
2.0	FAE Team	September 2013

Table Of Contents

1 The Company

Exclusively focused on offensive security, HackingTeam was founded in 2003 by David Vincenzetti and Valeriano Bedeschi. In 2004, it was the first to propose an offensive solution for cyber investigations.

HackingTeam technical team consists of innumerable high profile professionals, with years of experience in the field of security and hacking; many of the developers of RCS are well known in the security underground world.

Here in HackingTeam we believe that fighting crime should be easy: we provide effective, easy-to-use offensive technology to Law Enforcement and Intelligence Agencies. We believe that technology must empower, not hinder. The passion in what we do drives us as a leader in this field, setting the trend in offensive security solutions that is used daily to fight crime in six Continents.

2 Solution 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 the Lawful Interception Solution for governmental agencies. It is a stealth investigative tool dedicated to law enforcement and security agencies for digital investigations. It is a security 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. Using RCS gives you the possibility to gather such information.

RCS Agent, once installed on the target device, allows you to evade encryption and gather information of your target’s activity, without the constraint of physical boundary. The agent is designed to be polymorphic, to evade common Anti-Viruses and Anti-Rootkits. Evidence collection on monitored devices is stealth and transmission of collected data from the device to the RCS server is encrypted with military grade encryption algorithms. The communication protocol is specially designed to be lightweight and prevents fingerprinting. Identity and location of the Headquarter are hidden through the use of Anonymizers.

All the components of RCS are researched and developed in Milan, by a team of over 40 professionals focusing on all the aspects of offensive security. 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. It also means that your identity is not disclosed to any external parties.

All RCS installations are deployed at the Customer site, to guarantee total control on operations and security. Some of the key features of the RCS:

- 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, a safeguard to insider threat.
- 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
- Integrated OCR function converts screenshot images, documents and metadata to text
- Full text indexed search on all evidence
- Easily integrates with any third party Law Enforcement Monitoring Facilities (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
- Automatic, “set and forget” backups
- Automatically translates evidence from any language to any other language, breaking the language barrier in understanding the evidence collected
- Allow user to tag and include notes for every piece of evidence to enhance the value of the collected data
- Excellent reporting in HTML format, all evidence are embedded and can be reviewed just by using a browser

3 Architecture

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.

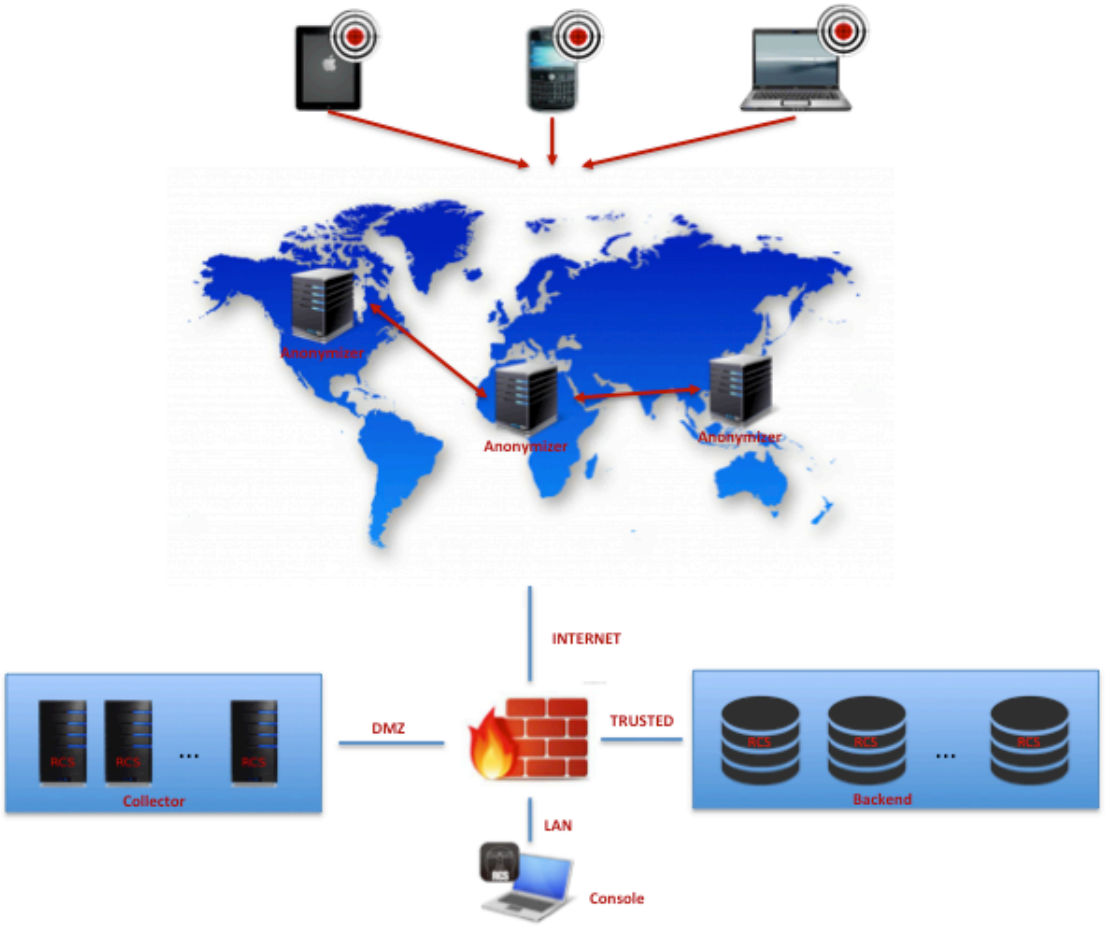


Figure 1 - Schema of RCS Architecture

3.1 Frontend

3.1.1 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 communicating with the Agent, making it possible to change their configuration, sending commands to perform special operations, etcetera.

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 strong double-layered encryption.

Agents need to reach the Collector anywhere they are, to maximize communication capabilities and give you control over the devices anywhere in the world.

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

3.1.2 Anonymizers

Anonymizers are used to hide the real identity of the Customer to anyone trying to figure out where the Agent is connecting to, in the remote event that its presence is discovered.

To avoid exposing the real IP address of the Collector and the possibility to link this information to the identity of the Customer, Anonymizers are used to send the collected evidence in seemingly random routes. They can be deployed anywhere on the Internet 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 possible if not in the Backend.

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

3.2 Backend

3.2.1 Master Node

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

RCS 8 *“Galileo”* architecture 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. It is capable of auto load-balancing, with the possibility to easily upgrade the system to manage thousands of concurrent targets.

The Master Node takes care of storing the evidence, using MongoDB as underlying Database, manages the configuration of the Agents and the build of the Infection Vectors, and coordinates the rest of the infrastructure balancing storage and computing needs between all the available Shards.

A “Set & Forget” backup system is integrated into the Database: choose what you want to backup, at what time, and the system will do the rest automatically. 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.

3.2.2 Shards

Shards, part of the Backend, are used to increase the number of concurrent Agents that can be supported; hot-plug, easy to install, automatically integrate with the rest of the Backend infrastructure, making it immediate to increase the overall capacity.

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 as it runs autonomously.

3.3 Console

3.3.1 Single Point of Control

RCS 8 *“Galileo”* Console provides a clean and simple feel with clear navigation for ease of use. It is the single point of control for the whole system, and allows performing any operation, according to user privileges. The Console is able to cope with the large number of Targets, and displaying huge amount of data.

Using the Console, it is possible to configure an Agent in two ways:

- **Basic:** allows for a quick and comprehensive configuration, taking you from zero to done in a few seconds: just a few clicks and the Agent is configured.

- **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. Its drag & drop graphical representation hides the complex logic from the user, is very efficient to use and lets you specify very articulated behaviors.

Role based access asserts the appropriate rights to the user in accessing the right information:

- **Administrator**: manages users and groups, grant privileges, creates investigations, and audits 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.

The finest privileges can be specified for each role, defining each activity on the system that a user is allowed to do.

3.3.2 Support for the Analyst

The **Search** capability, available almost everywhere with the Console, lets you to filter the information out 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. The powerful Search capability also allows you to perform free text search on the collected evidence. As soon as you start using it, you’ll realize that you can’t do without.

An integrated **OCR** will parse all collected evidence and extract searchable data for pictures, documents and any file with metatag.

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

All the Evidence collected is viewable 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 its original file format and can be imported by any third party software.

All collected evidence can be exported for conservation or further review, and the integrated **Automatic Report Generator** will make it easy to create reports to share the collected knowledge.

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.

3.4 Optional Modules

3.4.1 Connectors

Through the use of the Connectors Module, it is possible to integrate evidence collected with RCS into any existing Tool already in use. This makes it easy to import evidence from RCS to a Monitoring Center already in use, for maximum efficiency in the data mining process.

The Connectors Module exports evidence in JSON format, and HackingTeam will support the client for the necessary integration.

3.4.2 Translation

RCS integrates a Translation Module that, through the use of a third party server, can translate all collected evidence from any language to any other language. The translation happens in real time, and the analyst can switch from the original version to the translated version with one-click.

4 RCS Agent

The Agent is the software that has to be installed on the target PC or smartphone to be monitored; it extracts information already present on the device and keeps real-time user’s activity under surveillance.

Once collected, the Evidence is sent to the Collector: if an Internet connection is not always available, the Agent will continue to collect the Evidence, waiting for the next opportunity 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 you to define the Agents’ behavior, making them react 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 military grade 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.

Agents can be uniformly controlled and configured using the Console, the only application you need to access all the collected evidence and configure the Agent on your monitored device.

4.1 Platform Compatibility

Agents for Desktop can be installed on the most common Operating Systems:

- Windows
- MacOS X
- Linux

Agents for Mobile support the following platforms:

- Apple iOS
- Nokia Symbian
- BlackBerry
- Google Android
- Windows Phone 8

Refer to Attachment A for details on versions supported for each Operating System.

4.2 Agent Deployment

Agents must be installed on target Devices. Wide array of installation vectors are available to assist you in the deployment.

4.2.1 Desktop

- **Zero-Day Exploits**: zero-day exploits researched and developed in house to provide easy delivery through common applications are available.

- **Melted 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**: Tactical Network Injector (TNI) and Network Injector Appliance (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

4.2.2 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

- **Zero-Day Exploits:** zero day exploits researched and developed by HackingTeam’s reverse engineers are available to distribute the Agent through common applications on Mobile devices.

4.2.3 Tactical Network injector (TNI)

HackingTeam *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 in-line.

- **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 by displaying the following information:

  - *MAC Address*
  - *IP Address*
  - *Hostname*
  - *Operating System*
  - *Browser in use*
  - *List of all visited website*
  - *Attacks performed on the Target*

  The TNI supports different infection techniques:

  - Injection takes place when the target downloads any executable file (.exe) from the Internet;
  - Injection takes place when the target visits any website;
  - Injection takes place when the target user, prevented from viewing a video online, performs 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 targeted for infection;
  - Replace a legitimate web page with another customized by the operator for the purpose of obtaining user login credentials or critical information.
  - Comes 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

4.2.4 Network Injector Appliance (NIA)

HackingTeam *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 downloads any executable file (.exe) from the Internet;
  - Injection takes place when the target visits any website;
  - Injection takes place when user’s applications try to update;
  - 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
- Supports Fiber and Copper channels
- Easy management even when multiple NIA’s are deployed
- Full support from HackingTeam in the implementation of any NIA Project.

4.2.5 Remote uninstallation

The Agent can be uninstalled from remote with a simple click. Once removed, the Agent and all its data are permanently deleted from the Device. It is possible to configure the Agent to securely wipe all files from the device, in order to be resistant to any forensic analysis.

4.3 Collectable Evidence

Agents can collect different type of evidence depending on the type of Device, either Desktop or Mobile, and the specific target platform.

4.3.1 Desktop

On Desktops, an Agent can collect the following Evidence:

- 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)
- Automatic and on-the-fly interception and copy of any file opened, even when its encrypted and does not reside on the hard disk
- Screenshots
- List of visited web sites
- Download of passwords stored on the device (Browsers, Mail clients, etcetera)
- Keylogger with the possibility to capture also on-screen keyboards
- Copied and pasted text
- Position of the device, even when no GPS is available
- Recording from the microphone of the device
- Detailed information on hardware and software on the device
- Photos taken with the device webcam
- Monitoring and recording of VOIP Calls (Skype, LiveMessenger, and more)
- Download and Upload of files to and from the device
- Contacts information
- New and past appointments from different calendars
- More …

4.3.2 Mobile

On Mobiles, an Agent can collect the following Evidence:

- Detailed information on hardware and software on the device, including cell network information
- History of calls and calls recording
- Contacts information
- New and past appointments from calendar
- Sent and received e-mails and SMS
- Chat from BBM, WhatsApp and other Messengers
- Screenshots
- Keylogger
- Retrieve of passwords saved on the device
- Position of the device (Cell signal, Wi-Fi and GPS)
- Remote Audio Surveillance using the phone’s microphone (no need to place a call)
- Photos taken with the device camera
- List of visited websites
- Download and Upload of files from the device
- More …

4.3.3 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 in RCS using the Console and managed like all the rest of the evidence collected through Internet.

4.4 Evidence transmission

Evidence is transmitted from the Agent to the RCS 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 data connections (2G/3G/4G).

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 retrieved from the target system and used to gain access to the Internet.

For Mobile Agents (BlackBerry, Android, iOS, Symbian, Windows Mobile, Windows Phone) transmission happens by GPRS/UMTS/3G/4G data connections or WiFi. Even when such channels are switched off by the user, the Agent can be configured 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 Access Point Name (APN) for evidence transfer connections.

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

4.4.1 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/4G: 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.

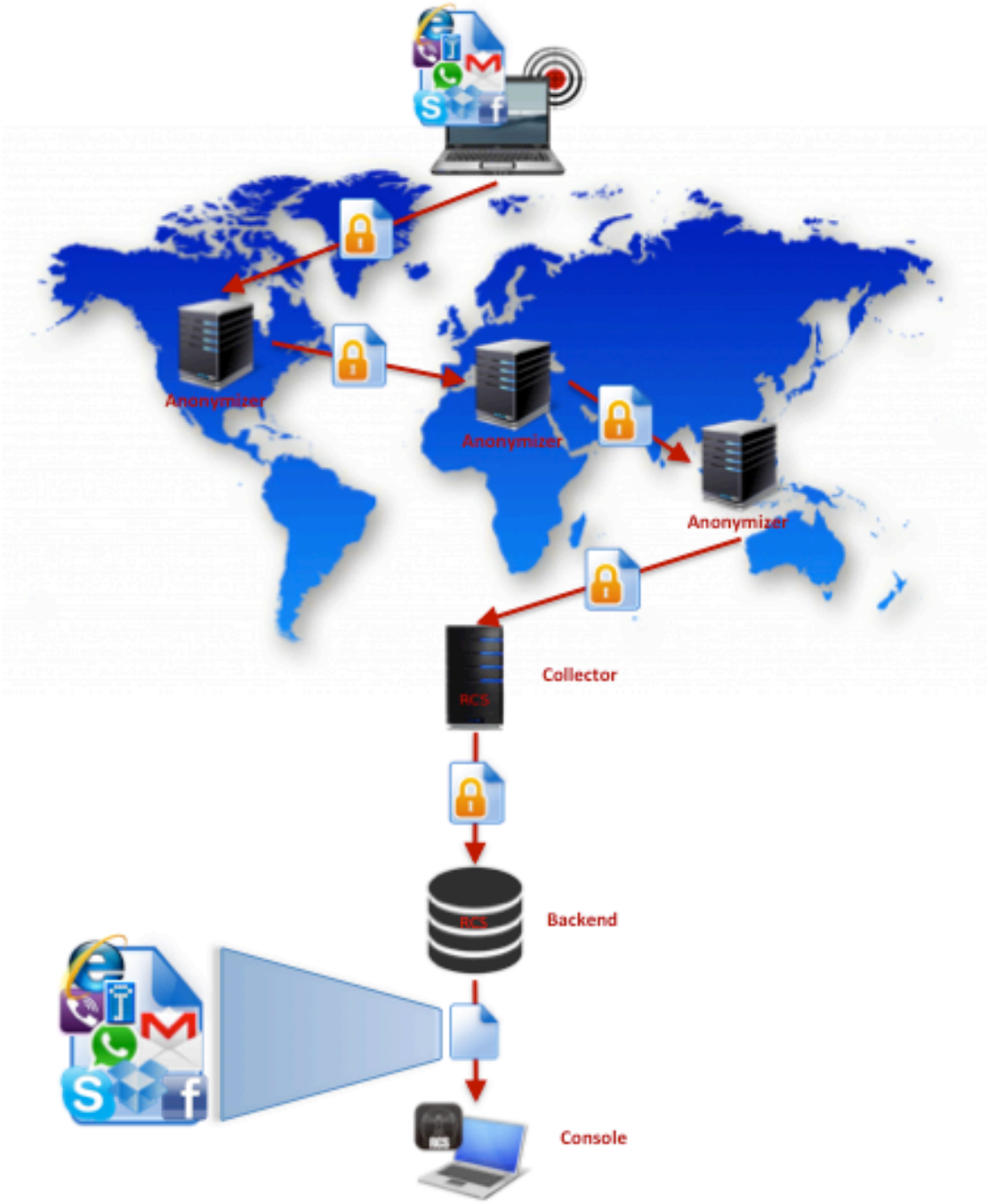


Figure 2 – Evidence flow of RCS

4.5 Event/Action Paradigm

Using embedded event/action logic, the Agent can detect specific events and react with appropriate actions, allowing it to collect relevant evidence without arousing suspicion.

Below is just an example of the capabilities of this event/action logic, some possible events and the relative actions 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

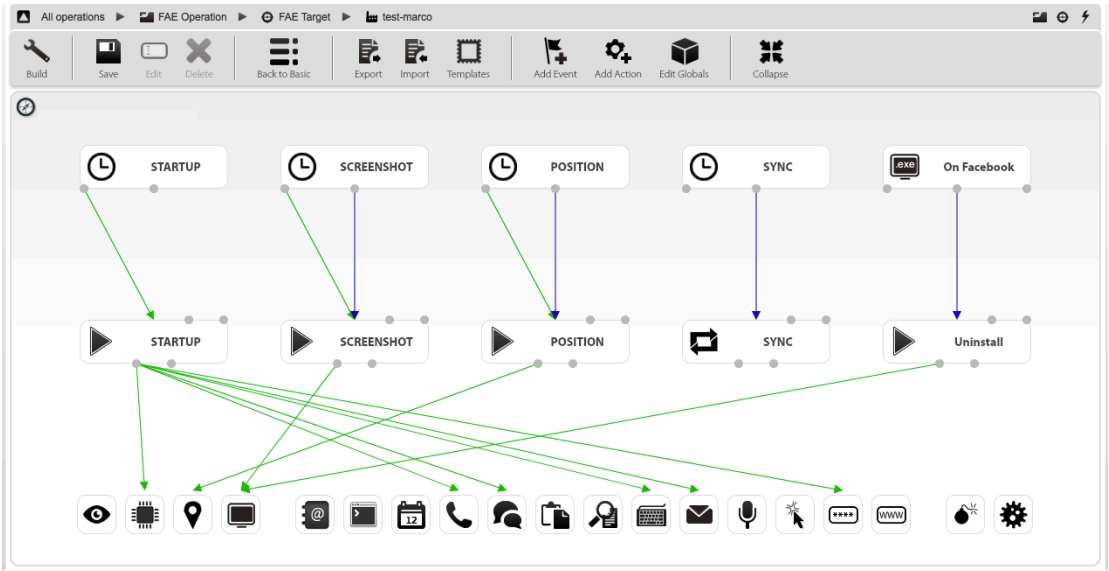


Figure 3 – Advanced Configuration Example 1

Any event can be linked with any action, so that each time you can configure your Agent to fit your needs. This allows very detailed configurations, easily adaptable to any specific scenario.

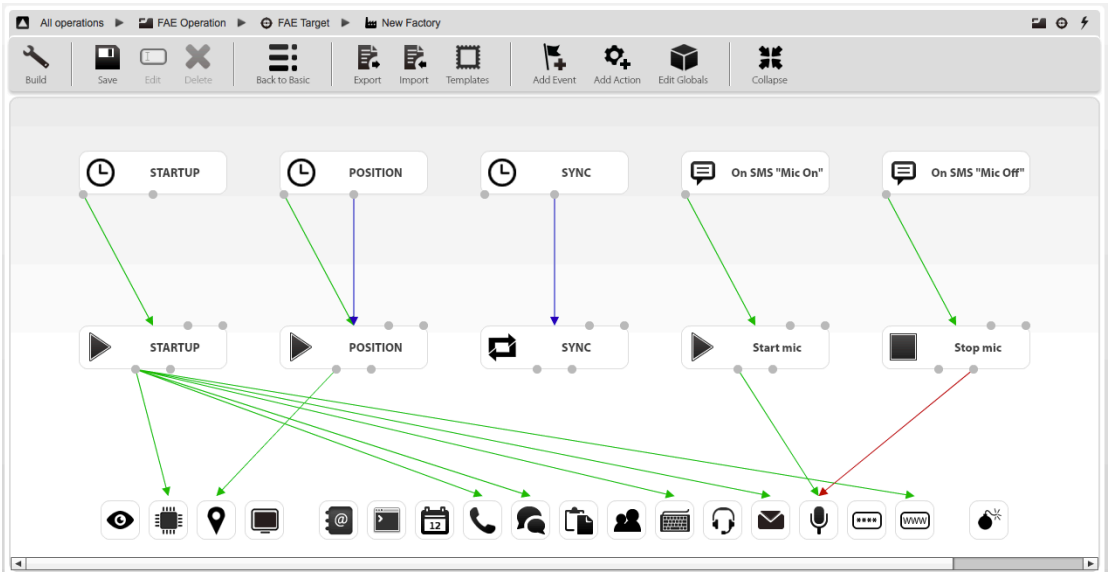


Figure 4 – Advanced Configuration Example 2

5 Intelligence

The data collected through different methods can grow indefinitely, making it hard to extract useful information from raw data.

As evidences are collected over time, displaying essential information in a timely manner becomes critical. The Intelligence module operates directly and automatically on all incoming data streams in order to provide "profiling cards" (or entities) for all targets under investigation.

The Intelligence module operates independently, analyzing incoming evidences on-the-fly and automatically creating relevant records for each entity.

Some information can also be loaded manually (eg. target’s photos, phone numbers, accounts, etc.) to enable correlation of previously collected data.

Intelligence is composed of two modules, profiling and correlation. Profiling automatically creates a profile for each target, showing the digital identity of your target; correlation gives information on interactions (communications, meetings, etc) between different targets.

5.1 Profiling

Each entity gives you access to useful information about the target, such as a list of all the digital accounts (eg. Facebook, Twitter, Gmail, Skype, etc..), a list of the most contacted people (through e-mail, messages or phone calls), the most visited web sites and his last known position.

Data shown can be filtered by date, giving you the possibility to see how things change during time.

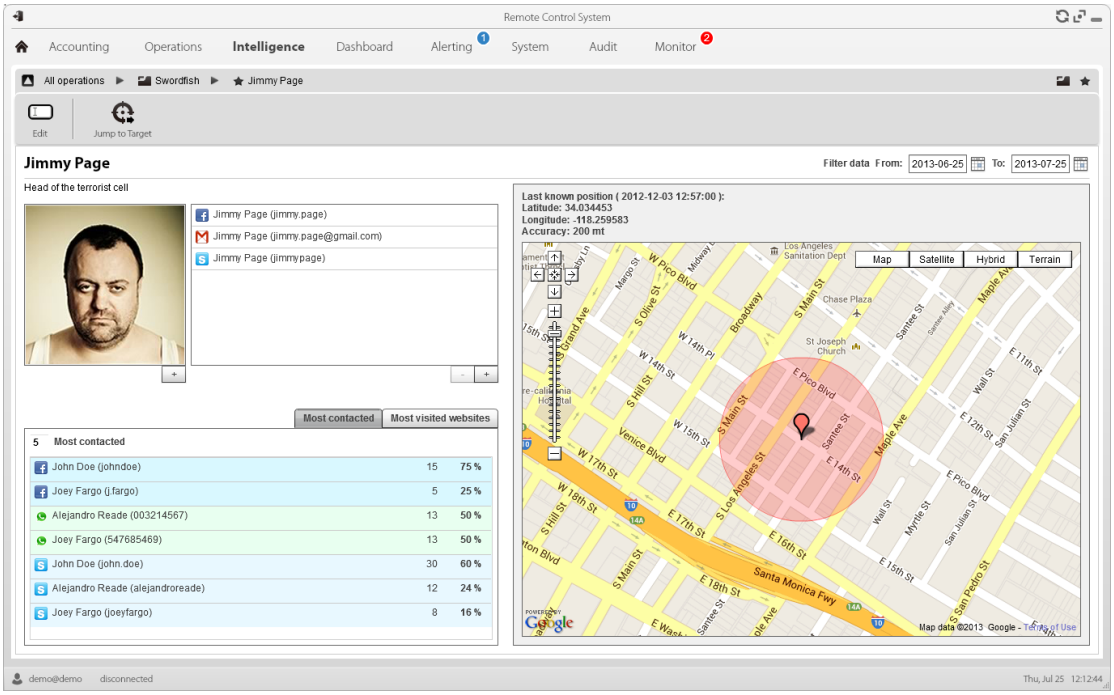
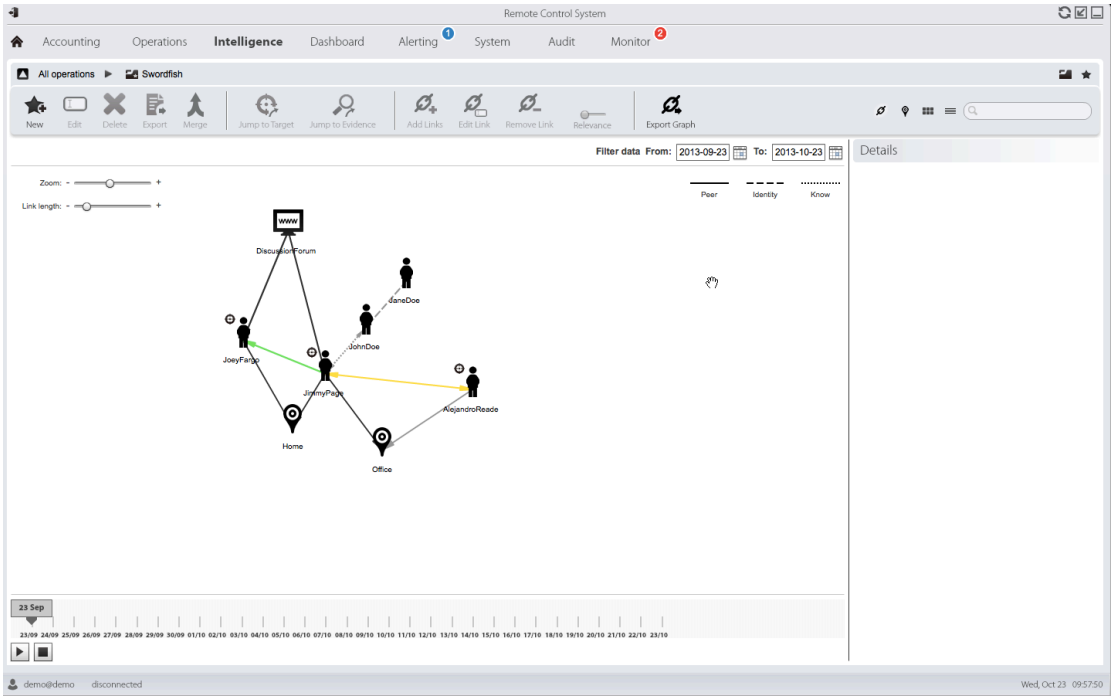


Figure 5 – Intelligence: suspect’s profile

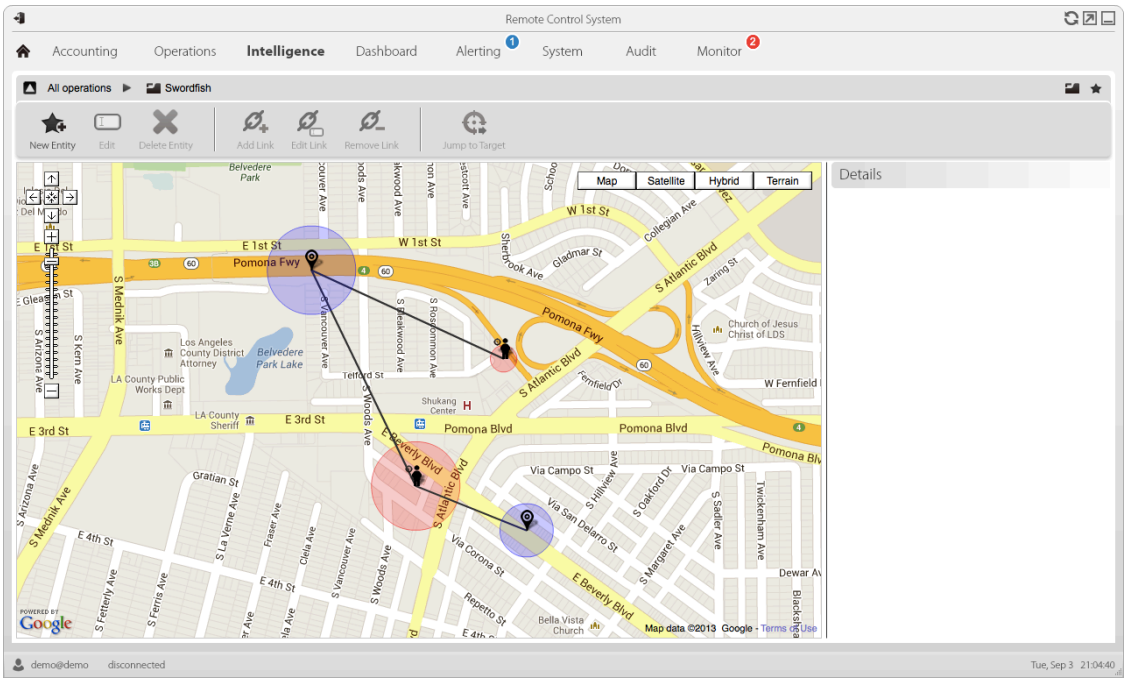
5.2 Correlation

Correlation will allow you to have a deep insight on the relations between your targets, in an easy to understand view. You will be able to add new entities, to specify another person of interest, a place relevant for your operation or a digital resource that you need to take into account in your investigations.

The correlation module will show you the links between all the different entities, with the possibility to drill down into details about communications and places of interest. It will be easy for you to identify the places where your target works, lives or meets his accomplices, and to analyze the flux of communications between the person you are investigating and everybody else, whether they are under investigation or not.



Within the correlation view it is also possible to see how your target is moving, with animations that will make it immediate for you to see when and where the suspects meet.



6 Compliance

RCS is designed to guarantee the legitimate use of the System and the integrity of the collected data. This is accomplished mainly through:

- **User and Privileges Management:** the definition of four different standard roles and the possibility to granularly assign privileges for each user, guarantees that each user can do only what is allowed to do.
- **Group Management:** the possibility to assign users to one or more Groups makes it possible to limit the evidence viewable by each user, making it natural to define different teams for different operations.
- **Audit:** the Audit section lists all operations executed by each user; this section cannot be modified or deleted, and it never expires: at any time, a user authorized to do so, will be able to review all operations performed on the system since day one.
- **Integrity of evidence:** evidence collected from monitored devices is immediately encrypted and a checksum is created; only evidence that maintains its integrity will be accepted by the RCS Collector, so that only information generated on the suspect’s device will become RCS Evidence.

7 RCS Software Cycle

RCS has a very fast and effective development cycle, with improvements and new features coming out often. Our 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 new major 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.

8 Training

HackingTeam provides extended and personalized training, according to Client’s needs. Possible training agenda includes:

- 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 profiling
  - Social Attack
  - Persuasion techniques
  - Understanding the interlocutor

9 Support and 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.

Attachment A – Platform Compatibility

Following, the details on the Platforms Supported by Remote Control System

Desktop

OSX	Linux	Windows
Mountain Lion	Ubuntu 13.04	8
Lion	Ubuntu 12.10	7
Snow Leopard	Ubuntu 12.04.2	Vista
	Ubuntu 12.04.01	XP SP3
	Ubuntu 12.04	
	Mint 15	
	Mint 14	
	Mint 13	
	Debian 7.1	
	Debian 7.0	

Mobile

Android	BlackBerry	iOS	Symbian	Win Phone
4.1	7.1	6.1.2	Symbian3	8
4.0	7.0	6.1.1	9.4 (5th ed.)	
3.x	6.0	6.0.x	9.3 (3rd ed. FP2)	
2.3	5.0	5.x	9.2 (3rd ed. FP1)	
	4.6	4.x	9.1 (3rd ed. MR)	
	4.5	3.x		