REMOTE CONTROL SYSTEM

GALILEO

THE HACKING SUITE FOR GOVERNMENTAL INTERCEPTION

Solution Description

]HackingTeam[

Table Of Contents

1 The Company

David Vincenzetti and Valeriano Bedeschi founded HackingTeam in 2003 to be exclusively focused on offensive security. In 2004, we were the first to propose an offensive solution for cyber investigations.

HackingTeam's technical staff consists of 50+ high-profile professionals, with many years of experience in every field of security and hacking; many of the developers of RCS are well known in IT security and the underground scene.

We develop effective, easy-to-use offensive technology for Law Enforcement and Intelligence Agencies.

Driven by passion and leaders in this field, we set the trend in offensive security solutions used daily to fight crime in all continents.

Fighting crime is easier with us.

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 monitoring and preventing crimes and threats to the Nation's security.

Remote Control System is the stealth, active interception solution for eligible "Governmental Agencies" (the "End User", hereinafter "End User" or "you"): a stealth investigative tool that hides itself inside the target devices and enables active data monitoring and process control. Remote Control System is designed to meet the higher expectations of the worldwide intelligence community.

Sensitive data is exchanged using encrypted channels or not exchanged at all, while sometimes it is exchanged using networks outside of your agency's reach. Remote Control System gives you the possibility to gather such information.

Remote Control System allows you to bypass encryption and gather information on your targets activities. The Agent is designed to be polymorphic and evade common antivirus software. Evidence collection is stealth and transmission of data to the RCS server is encrypted with strong encryption algorithms. The communication protocol is lightweight and designed to prevent fingerprinting. Identity and location of your premises is made anonymous.

All the components of Remote Control System are developed in Milan, Italy, by a team of over 50 professionals. We developed every line of our software: this make us able to timely fix bugs and customize the product according to your needs.

Remote Control System is deployed at your site to let you have total control on operations and security. Some of the key features of the solution are:

- High scalability and automatic load-balancing to easily manage thousands of concurrent targets.
- Separated front-end and back-end components with the possibility of geographically distributed installations
- Single point of control for all operations, with one-click upgrade and reconfiguration of deployed agents
- Highly granular user roles and privileges
- Integrated audit system, to safeguard against insider threats
- Custom reports in HTML for offline browsing
- Integration with 3rd party systems (e.g., monitoring centers or audio processing equipment)
- Integrated OCR function acquires text from images, documents and metadata
- Full text search on all evidence
- Integrated data mining for target profiling and entity correlation
- Automatic, "set and forget" backups
- Automatic evidence translation in foreign languages, for immediate understanding of the threat level
- Tag and annotate collected evidence

3 Architecture

The Remote Control System infrastructure is built of different components distributed in the End User's network, on the target devices and on the Internet.

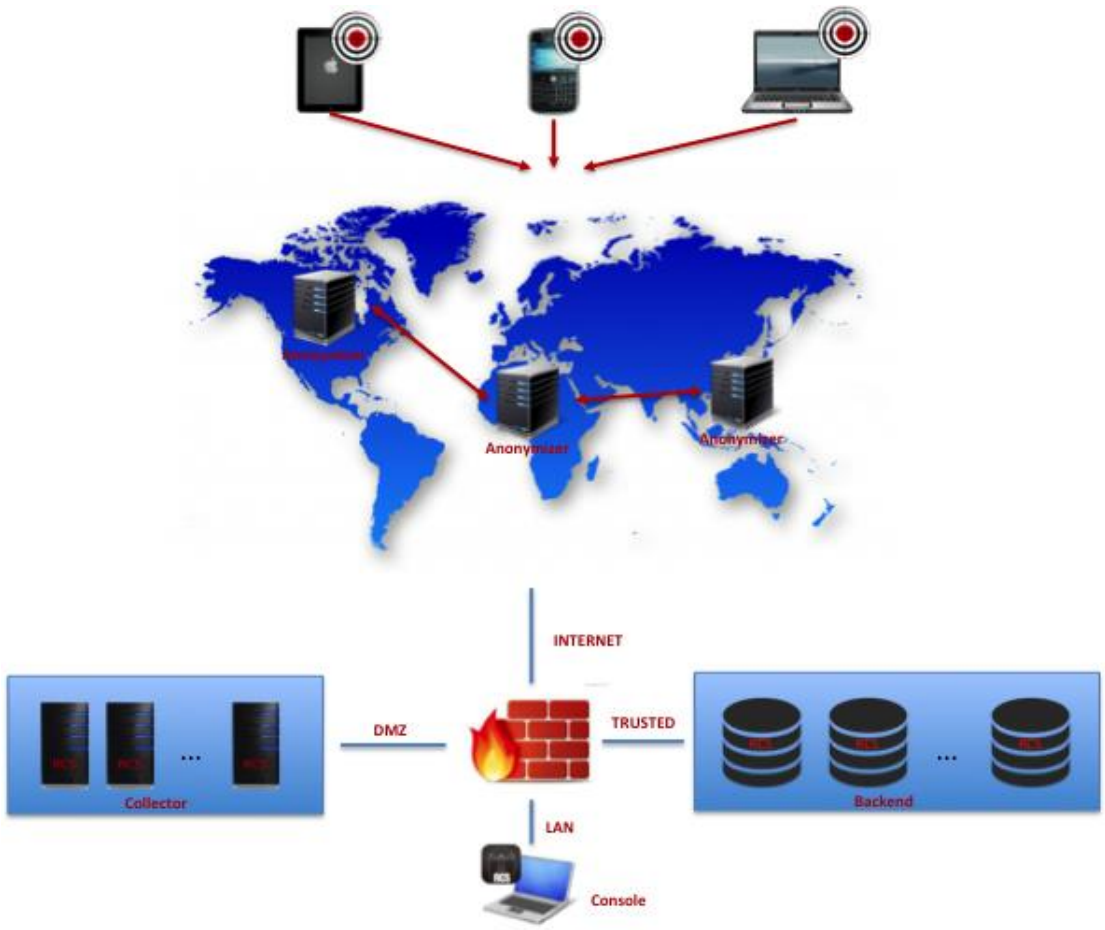

Figure 1 - Schema of RCS Architecture

3.1 Frontend

3.1.1 Collector

Collectors are the point of presence of RCS on the Internet. Agents running on target devices connect to Collectors to transmit data and receive commands.

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

Agents use Internet to contact the Collector; hence you control your targets regardless of where they are located.

3.1.2 Anonymizers

Anonymizers protect the Collector, avoiding the exposure of the actual IP address of the Collector and, with it, any information on your identity.

Anonymizers route the collected evidence and are freely deployed on the Internet. Safety of communication is granted by strong encryption of the communication channel.

3.2 Backend

3.2.1 Master Node

The Master Node is the core of the infrastructure: together with Shards, it stores all the targets' data and performs all the business logic.

Remote Control System provides unmatched scaling capabilities, obtained by adding servers and making them work in parallel. It features also automatic load balancing and the possibility to upgrade to manage thousands of concurrent targets.

The Master Node stores the collected data, manages the configuration of the Agents and the build of the Infection Vectors. Further it coordinates the whole infrastructure, balancing storage and computing needs among all the available nodes.

Set & Forget backup is integrated: choose what and when you want to backup and the system does it for you. You can backup the full database, make selective backups of a single Operation, Target or Agent, or backup the essential data for quickly restoring a working copy of your system.

3.2.2 Shards

Shards are used to increase the capacity of the system; they are easy to install and automatically integrate with the infrastructure.

By adding Shards you monitor more Targets and dramatically increase the response times and storage capacity of your system: browsing the Evidence is quicker and you retain the information, always available, for longer time.

When a Shard is added the database automatically balances itself, distributing the data according to the new resources available. There is no need to perform complicated maintenance.

3.3 Console

3.3.1 Single Point of Control

The Console is the single point of control for the whole system and allows performing all the operations according to the current user privileges.

Using the Console, you configure an Agent in two ways:

- **Basic**: a quick and comprehensive configuration based on ON-OFF switches, takes you from zero to done with a few clicks; your Agent is ready to be deployed in a matter of minutes.

- **Advanced**: gives finer control over the configuration, showing all the options to let you fine tune the configuration to suit your scenario at best. Its drag & drop GUI is very efficient and lets you specify articulated behaviors.

Role based access control (RBAC) enforces the appropriate access level of each user:

- **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.

Further privileges can be specified for each role, for finer control on the user's capabilities.

3.3.2 Support the Analyst

Search is available throughout the Console and lets you to filter the information and get to the interesting bits. Perform searches with any criteria, such as name or keyword in the description. Furthermore, Search features free text search on the collected data.

An integrated OCR parses images, documents and file's meta-tags to **extract searchable text**.

With the **Alert** feature you are warned in real time, via email or console notification, when interesting evidence arrives: if desired, you can automatically set the evidence's relevance, to ease future searches.

With the Console you browse screenshots, listen to audio files, visualize their waveform and navigate maps of the locations.

The integrated **Report Generator** creates custom reports to share the collected data with third parties, whom can consult it from any browser.

Finally, you **monitor the health status** of all the components of the system and are promptly alerted in case of failure.

3.4 Optional Modules

3.4.1 Connector

The Connector integrates Remote Control System with 3rd party software, such as monitoring centers and audio processing equipment.

Connector exports evidence in JSON format, and HackingTeam supports the End User during the integration process.

3.4.2 Translation

The Translation module translates any textual evidence. The source language is automatically identified and you can choose the destination language among a wide selection. Translation is real time, and with one click you switch from the original version to the translation.

4 The Agent

The Agent is the software that extracts information from the device and monitors the user's activity. It is capable of collecting many kinds of information, ranging from social applications to classic key logging.

Agent normally sends the collected data to the Collector, but when Internet connection is not available collection continues while the Agent waits for the next opportunity to send.

Collected data is stored encrypted and hidden on the device. Decryption is possible only on the Backend, thus enforcing confidentiality of the collected data.

The Agent can be reconfigured at any time: a powerful event/action paradigm allows you to define the behavior, to make it 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 analysis of the device is undergoing.

Each Agent is autonomous in its operation, even when it is isolated from the Internet: no intervention by the operators is required for daily activities. All connections are mutually authenticated and encrypted with strong algorithms, thus avoiding the risk of eavesdropping or data leakage. Moreover, the Agent is built to be non-attributable to its creator, thus protecting the safety of your operations in case of Agent disclosure and analysis.

Agent is hidden from the user, and resistant to most antivirus and security suites available on the market..

Platform Compatibility

Agents can be installed on the following Operating Systems:

- Windows
- OS X
- Linux

For smartphones, RCS supports the following platforms:

- iOS
- Android
- BlackBerryWindows Phone

We constantly research the new platforms before or as soon as they are released, to provide support as soon as possible.

Refer to Appendix A for specific version support.

4.1 Agent Deployment

Depending on the scenario, target and needs that you have, a wide selection of installation vectors is available to assist you in deploying your Agents.

4.1.1 Infecting desktops and laptops

- **Remote Attack Service**: a dedicated team and service is dedicated to help deploying your Agents from remote. We provide consulting on scenario to determine the best attack approach and dedicated service to implement it effectively and safely.
- **Melted Application**: combine the Agent with most common applications. When run, the original application is presented to the user while the Agent is silently installed. This approach presents many advantages:
  - Agent is disguised as a common application
  - Melted application can be remotely delivered
  - Perfect for social engineering attacks
- **From the network**: Tactical Network Injector (TNI) and Network Injector Appliance (NIA) lets you infect targets via their WiFi and ADSL connections; see the respective sections for details;
- **Physical Access**: when physical access to the device is available, infection is performed whether the computer is running or is turned off:
  - User password is not required
  - Usually takes few seconds
  - Unlock computer if necessary
  - Support for hibernated systems
  - Easy to use
  - Retrieve documents, images and files without infecting

4.1.2 Infecting smartphones

- **Remote Attack Service**: a dedicated team and service is dedicated to help deploying your Agents from remote. We provide consulting on scenario to determine the best attack approach and dedicated service to implement it effectively and safely.
- **Deliver a web link:**
  - Send by email
  - Perfect for social engineering attacks
  - Deliverable from remote
- **Send a text message with a link**:
  - Appears as any application (e.g., an operating system update)
  - Link is loaded and, depending on the phone configuration, prompted to the user
  - Customize text to make it appealing to your target
- **Melted Application**: combine the Agent with most common applications. When run, the original application is presented to the user while the Agent is silently installed. This approach presents many advantages:
  - Agent is disguised as a common application
  - Perfect for social engineering attacks
  - Melted application can be remotely delivered
- **Physical Access**: when physical access to the device is available, local installation is performed:
  - …

4.1.3 Infecting in WiFi networks

HackingTeam's Tactical Network Injector (TNI) is a portable solution to infect targets via WiFi and LAN connections. The TNI embeds a patented technology that permits to operate without being in-line and features WiFi cracking, target identification and infection capabilities.

WiFi Cracking

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

Target Infection

The TNI operator identified the intended target by means of the following information:

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

Once the target is identified, the operator infects the target by taking advantage of the following events, common during Internet usage:

- downloads an executable file (.exe);
- visits a website;
- watches a YouTube video;
- visits a Web resource (e.g., pdf, docs).

Additional features are available to ease the infection process, such as:

- emulating a Rogue Access-Point, to provide free Internet Access to any computer;
- replace a legitimate web page with a custom one, for example to obtain login credentials or personal information;

Finally, the TNI is provided with additional batteries to extend its autonomy to up to 35 hours of continuous operation. Extra network cards and antennas are provided as well to extend its operational range.

4.1.4 Infecting on ADSL lines

HackingTeam's Network Injector Appliance (NIA) is a solution designed to infect targets connected to ADSL Internet lines. The key features are:

- deployed at the Internet Service Provider
- no need for inline installation, thanks to HackingTeam's patented technology
- target is identified by means of different criteria:
  - IP Address or IP Range
  - MAC Address
  - DHCP Parameters
  - Radius Parameters
  - Content of packets through DPI
- different infection techniques apply to different target activities:
  - downloads any executable file (.exe) from the Internet;
  - browses the web;
  - watches YouTube videos;
  - accesses Web resources (e.g., pdf or doc files).
- Available for 1GB and 10GB links, with fiber and copper connectors (SFP+)
- Easy management of multiple NIAs
- Dedicated support for project implementation at the ISP.

4.1.5 Remote uninstallation

The Agent is uninstalled from remote with a simple click. Once removed, the Agent and all its data are permanently deleted from the target device. You can configure the Agent to securely wipe all files, to resist to forensic analysis.

4.2 Collectable **Evidence**

Agents collect different type of evidence depending on the specific device and target platform. Different types of data are collected from desktops and smartphones.

4.2.1 Desktop

On Desktops, the Agent collects:

- Recording of Skype and voice applications calls
- Chat and messages from social networks (e.g., Facebook, Twitter, etc)
- Mail from clients and web interfaces (e.g., Outlook, Windows Mail, GMail, etc)
- Open files, even if encrypted and resident on external or network volumes
- Screenshots
- Visited web sites
- Passwords from browsers, mail clients, etc.
- Key logging, also from on-screen keyboards
- Clipboard text (copy&paste)
- Position, even if GPS is not present
- Microphone recording
- Information on hardware and software
- Webcam photos
- Contacts
- And much more

4.2.2 Mobile

On Mobiles, the Agent collects the following Evidence:

- BBM, WhatsApp and other Chat applications
- Information on hardware and software,
- Cell network information
- Call history
- Contacts
- Calendar appointments
- Emails and SMS
- Screenshots
- Key logging
- Stored passwords

- Position from cell signal, Wi-Fi or GPS
- Microphone recording
- Webcam photos
- Visited websites
- Download and upload of files
- And much more

4.2.3 Offline

Some target devices are not connected to the Internet for long periods. In that case, you can still collect evidence to prevent losses due to exhaustion of disk space.

You can choose between two ways to collect the evidence offline:

- **Bootable CD**: boot from a CD and operate by an easy GUI. Save the evidence onto an external USB drive. Available for Windows and OS X.
- **Bootable USB**: boot from an USB thumb drive. Same easy GUI to an external USB drive. Available for Windows.

Evidence collected offline can be imported in RCS using the Console. After importing, tou can manage them like any other evidence received through the Collectors.

4.3 Evidence transmission

Evidence is transmitted using the best communication channel available at each synchronization opportunity. Differently, by changing the Agent's configuration you can **instruct a specific usage of the available channels** (e.g. use only WiFi vs. use only 3G).

On Windows, OS X and Linux Agents, the Agent uses any wired or wireless Internet connection available, and in case of WiFi networks the Agent automatically uses open or preconfigured Access Points.

In enterprise environments the Agent bypasses proxies and firewalls to get access to the Internet.

On BlackBerry, Android, iOS, and Windows Phone, transmission uses either GPRS/UMTS/3G/4G or WiFi. If needed, the Agent can silently switch them on and then off once transmission is complete.

A custom Access Point Name (APN) can be used to avoid the target incurring in extra billing for the Agent's data connections; this proves useful when the target doesn't have a flat rate plan for his smartphone's data connections.

4.4 Off-channel communication

Agents for smartphones can send invisible SMS containing valuable information such as SIM details or GPS position; this is especially useful when you're on the field and you need to find out where the Device is located.

Moreover, you can also send commands to the Agent via SMS; once received, the SMS is not shown and actions are performed as configured. For example, you can instruct to Agent to send you back his position.

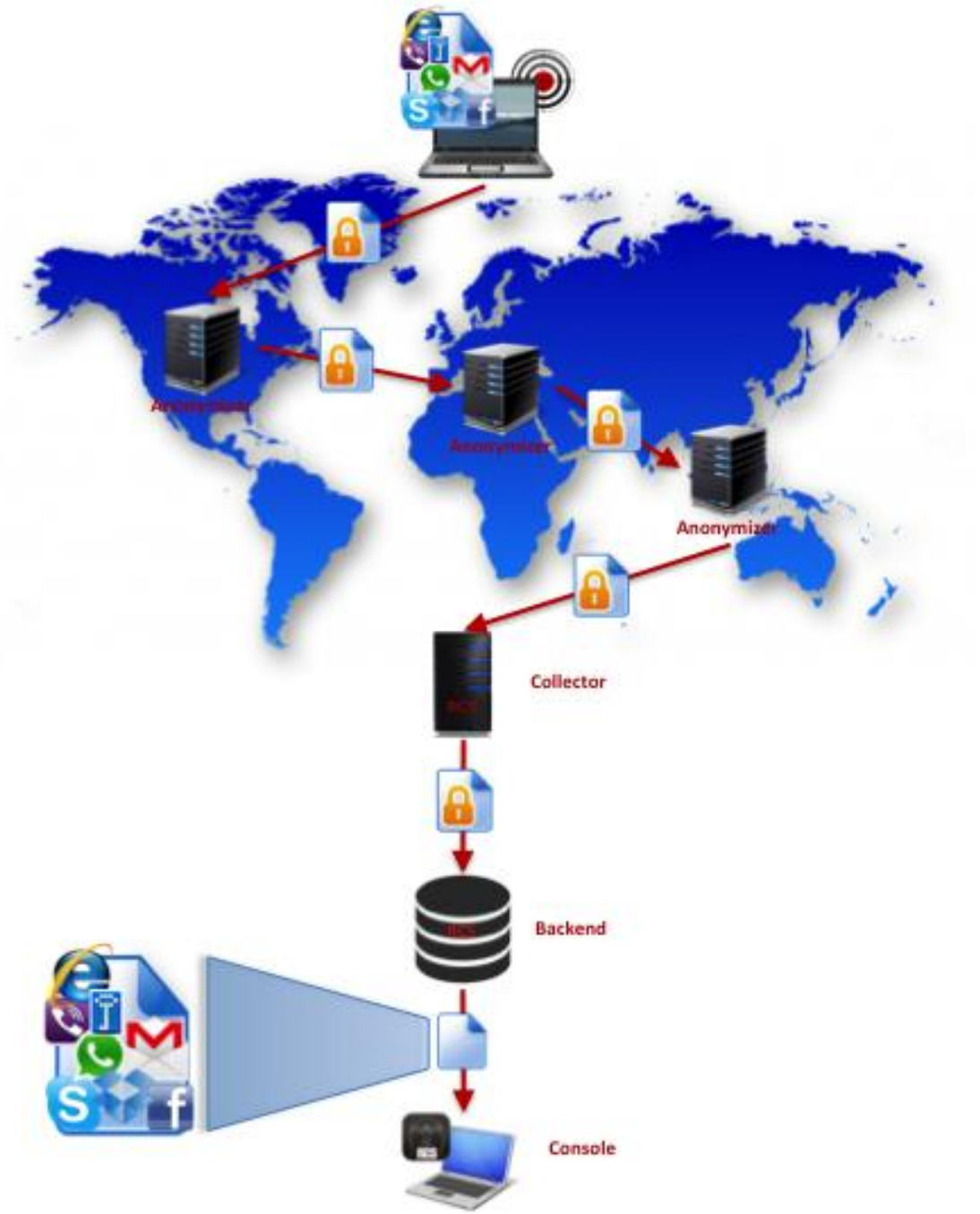

Figure 2 – Evidence flow of RCS

4.5 Event/Action Paradigm

You want to configure each Agent to operate according to criteria designed to suit the specific scenario. Using the embedded event/action logic you instruct the Agent to react to a set of events. At the same time, you tell the Agent which evidence to collect.

In the table below there are some examples of the capabilities of the event/action logic:

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

In Figure 3 and 4 you can experience the look&feel of the advanced configuration. Events are freely linked to actions, and Actions are themselves linked to collection modules. With this paradigm you can easily design the behavior of each of your Agents.

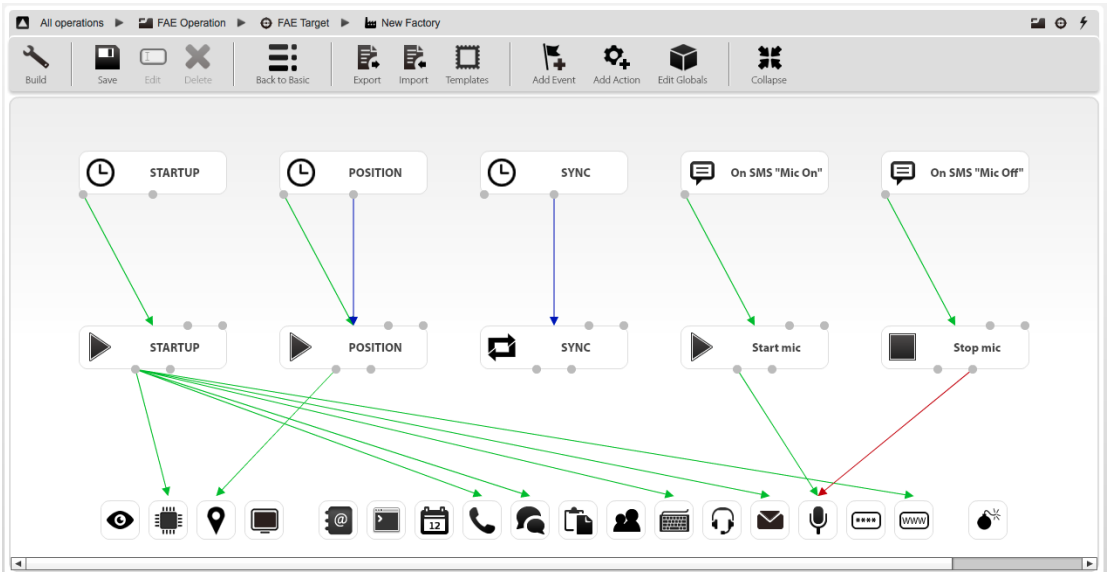

Figure 3 – Advanced Configuration Example

5 Intelligence

Accessing high-level, essential information in a timely manner is critical and often makes the difference to a successful investigation.

Remote Control System provides a correlation engine that highlights all the relevant high-level information about your targets and operations. With the Intelligence module, you dramatically speed up you investigation and immediately discover relations among targets, places and communications.

The Intelligence module is divided in two major functionalities:

- **Profiling** builds the target's profile, combining digital and real identity;
- **Correlation** synthesizes information on interactions (e.g., communications, meetings, etc) among different targets and operations.

Furthermore, you can manually load additional information (e.g., target's photos, phone numbers, accounts, etc.) to make correlation even more comprehensive and powerful.

5.1 Profiling

Profiling concentrates useful information about each target, such as a list of all of his' digital accounts (eg. Facebook, Twitter, Gmail, Skype, etc..), his most contacted people (through e-mail, messages or phone calls), his most visited web sites and his last known position.

Profile information is filtered by date to see how the profile evolves in time.

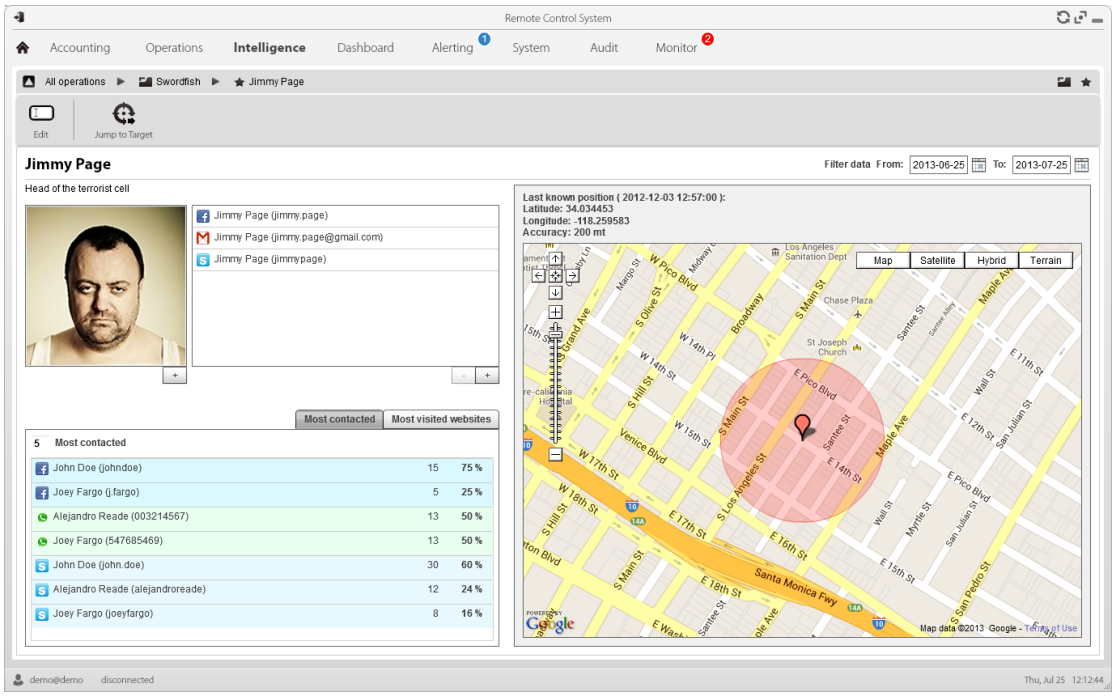

Figure 4 – Profiling of a target

5.2 Correlation

Correlation gives you insight on the relations and interactions between targets and operations. With it you get aggregated information about the movements of your targets and their habits of communicating.

Drill down and see the details that make up each relation. It is easy to identify the places where your target works, lives or meets his accomplices and to analyze the communication flux between them all.

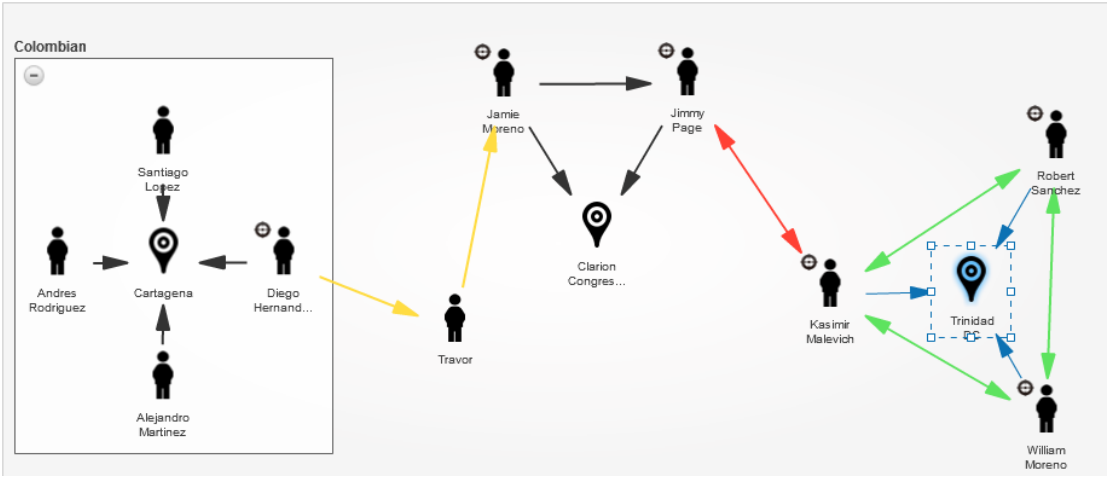

Figure 5 - example of complex relationships

Within the correlation view it is also possible to see where your target is moving during the day, by means of animations that make it immediate to identify when and where the suspects meet.

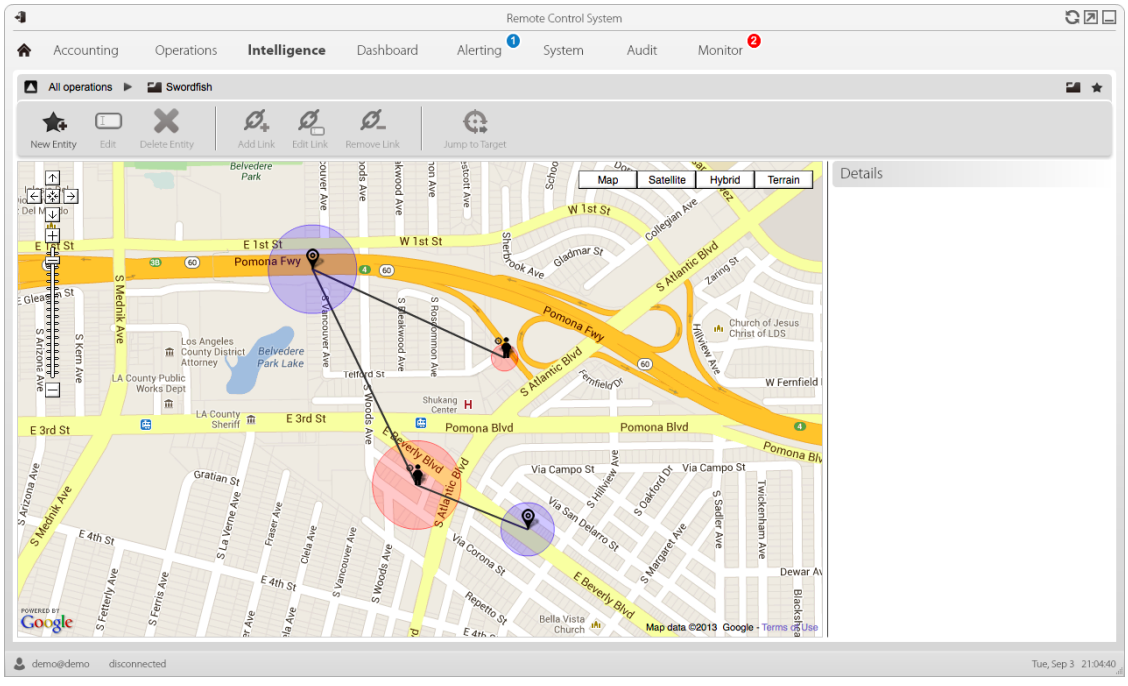

Figure 6 - example of multiple targets movement analysis

6 Compliance

RCS is designed to enforce 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 are 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; the RCS Collector accepts only evidence that maintains its integrity, so that only information generated on the suspect's device is considered good and stored.

7 Maintenance

7.1 Support

You access support for your Remote Control System by an online support portal, with the following benefits:

- Prompt and competent answers
- Quickly review all your case history
- Immediate download of new releases and updates
- Protected by secure authenticated connection

Furthermore, HackingTeam offers a **Custom Scenario Analysis service**. Taking advantage of this service, you can shares specific requirements with HT's experts and get custom solutions. The solution can include development of custom code or engineering of ad-hoc devices, or other means that help you in reaching your goal.

7.2 Maintenance & Quality Assurance

As part of the maintenance and quality assurance procedure of Remote Control System, HackingTeam developed an internal testing system, named RiTe, which simulates a set of real targets with various software configurations. Every night, more than 500 single test units are performed on those environments to assess a set of quality requirements:

- Invisibility against 50+ security suites and antivirus products;
- Collection of social applications data;
- Agent lifetime (i.e., installation, runn'ing, upgrade, uninstallation);
- Exploit lifetime (i.e., sending, exploitation, Agent installation and invisibility)

These tests allow us to improve our level of support in many areas:

- Shorter reaction time in case of anomalies or sudden changes in the environment;
- Timely communications to mitigate the impact on your operations;
- Enhanced support procedures.

Finally, as part of the Maintenance process, HT offers custom testing in case of particular scenarios or uncommon target environments (e.g., lesser or local antivirus software, odd versions of operating systems, etc).

8 Training

When you acquire Remote Control System, product training is included upon delivery: an experienced engineer is at your site to explain how to proficiently operate the system, train your staff and test their level of preparation. In case of further needs, for example to go in-depth into specific topics, we are available to provide tailored follow-up trainings. For more information about the product training, please refer to the attached "HT_Galileo_ProductTraining" document.

Moreover, HackingTeam offers a track of proven training courses that already helped many governmental agencies in strengthening their IT security skills. Please refer to the attached "HT_ITTraining" document.

In case you want to have a custom course or track, contact your sales representative.