REMOTE CONTROL SYSTEM

GALILEO

THE HACKING SUITE FOR GOVERNMENTAL INTERCEPTION

Whitepaper

]HackingTeam[

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.

Document Approval

Revision	Author(s)	Release Date
2.1	FAE Team	September 2013

Table Of Contents

1 The Company

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

HackingTeam's technical staff consists of high-profile professionals, with years of experience in the 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 crimes and threats to the Nation's security.

Remote Control System (RCS) is a stealth, active interception solution for governmental agencies. It is a stealth investigative tool designed to meet the higher expectations of the worldwide intelligence community. RCS is a intrusive software which hides itself inside the target devices and enables 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. Also in this case, Remote Control System gives you the possibility to gather such information.

Remote Control System Agents, once installed on target devices, allows you to evade encryption and gather information of your target's activity. The agent is designed to be polymorphic and to evade common antivirus software. Evidence collection is stealth and transmission of data to the RCS server is encrypted with the strongest encryption algorithms. The communication protocol is designed to be lightweight and to prevent fingerprinting. Identity and location of your premises is made anonymous.

All the components of Remote Control System are developed in Milan by a team of over 40 professionals focusing on all the aspects of offensive security. We developed every line of our software: this make us able to fix any bug in the shortest time and customize the product according to your needs. It also means that we control all the process, thus protecting identity from being disclosed to any external party.

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

- High scalability and automatic load-balancing to easily manage thousands of concurrent targets.
- Clearly divided front-end and back-end components to have geographically distributed systems
- Single point of control for all operations, including one-click upgrade and configuration change for deployed agents
- Highly granular user roles and privileges, to let you organize operations on a need-to-know basis
- Integrated audit system, to safeguard against insider threats
- Easy and intuitive network configuration
- Custom reports in HTML for offline reviewal
- Export of evidence to 3rd party systems
- Integrated OCR function to make images, documents and metadata searchable
- Full text search on all evidence
- Integrated data mining for target profiling and entity correlation
- Automatic, "set and forget" backups
- Automatic translation of text in foreign languages, for immediate understanding of the threat level
- Severity-level tagging of evidence and notes for personal comments

3 Architecture

The Remote Control System infrastructure is made up of different components: part of the them resides within the Customer's network, part are 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 protect you from third parties: in the remote event that an Agent is discovered, your RCS infrastructure and your identity stay protected.

To avoid exposing the real IP address of the Collector and, with it, any information on your identity,, Anonymizers randomly route the collected evidence. They can be deployed anywhere on the Internet to route connections from the Agents through each of those nodes, before reaching the Collector.

Anonymizers are safely placed in untrusted networks, even in foreign countries. Each connection is fully encrypted from the target to the Collectors, thus preventing eavesdropping.

Anonymizers are linked into one or more chains and 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 infrastructure: it stores the Evidence collected from the targets and performs all the business logic.

Remote Control System 9 *Galileo* provides unmatched scaling capabilities: instead of switching to a more powerful, expensive server, scalability is obtained by adding more, less powerful servers. These servers work in parallel, auto load-balancing the workload. In this way, the system is easily upgraded to manage thousands of concurrent targets.

The Master Node also 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 nodes.

A Set & Forget backup system is integrated: choose what you want to backup and when 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 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 speed and storage capacity of your system: browsing the Evidence is much faster, you can collect more information and retain it, always available, for longer time.

When you add a Shard, 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

Our Console provides clean and simple navigation for improved ease of use. It is the single point of control for the whole system. The Console is able to cope with the large number of Targets that scalability allows,, and is designed to display big 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

Search is available throughout the Console, to let you to filter the information and find only the interesting bits. You can perform searches with any criteria: by the name of the Agent you are looking for or just a word in the description. The powerful Search algorithm allows you to search on the collected evidence, as if they were free text. As soon as you start using it, you'll realize that you can**'t** do without.

An integrated OCR parses all the collected evidence and makes pictures and documents searchable.

Using the Alert feature, you setup custom alerts to warn you in real time, either via email or console notification, when interesting evidence arrives: if desired, you can automatically set its relevance, to ease future searches.

All the collected data is viewable within the Console: view screenshots, listen to audio files, visualize their waveform and navigate maps of the locations. If further processing is required, evidence can be exported in its original file format; you can then import it into any third party software. The integrated Automatic Report Generator will make it easy to create reports to share the collected knowledge.

From the Console you can also monitor the health status of all the components of the system, and be promptly alerted in case of failure.

3.4 Optional Modules

3.4.1 Connectors

Through the use of the Connectors Module, you can export the collected data into any 3rd party software. This makes it easy to use RCS as a source of data for your Monitoring Center.

The Connectors Module exports evidence in JSON format, and HackingTeam supports the client during the necessary integration.

3.4.2 Translation

HackingTeam offers a Translation Module that can translate all collected evidence. The source language is automatically identified and you can select a set of destination languages. 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 is installed on target's PC or smartphone; it extracts information present on the device and keeps user's activity under control.

Once collected, the Evidence is sent to the Collector: when Internet connection is not available, the Agent continues to collect, waiting for the next opportunity to transfer it.

Collected data is stored encrypted and hidden on the device. Decryption is possible only on the Backend.

The Agent can be reconfigured at any time: a powerful event/action paradigm allows you to define the behavior, making 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.

Agents are autonomous in their operations, even when they're isolated from the Internet: no intervention by the operators is required for day to day activities.

Agent's connections are encrypted with strong algorithms and mutually authenticated, thus there js no risk of eavesdropping or data leakage. Moreover, the Agent is built to be non-attributable to you, to guarantee the safety of your operations, even in case of Agent disclosure and analysis.

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

You uniformly control and configure your Agents through the Console, from where you access all your Remote Control System infrastructure.

4.1 Platform Compatibility

Agents can be installed on the following Operating Systems:

- Windows
- OS X
- Linux

For smartphones, RCS supports the following platforms:

- iOS
- Android
- BlackBerry
- Windows Phone

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

4.2 Agent Deployment

A wide selection of installation vectors are available to assist you in the deployment of your Agents during your field operations.

4.2.1 Deploying to desktops and laptops

- Zero-Day Exploits: we have an internal team for research and development of zero-day exploits. We focus on providing exploits targeting the most common applications (e.g., Microsoft Office, Internet Explorer, etc.).
- Melted Application: you can combine the Agent with any application. When run, the original application is presented to the user; meanwhile, 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
- From the network: Tactical Network Injector (TNI) and Network Injector Appliance (NIA) lets you infect targets connected to Wifi networks or through their 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:
  - No need to know the user password
  - Infection performed in as little as few seconds
  - Computer can be unlocked if necessary
  - No limitations on hibernated systems
  - Easy to use
  - Documents, images and files in general can be retrieved from the target device, even without infection

4.2.2 Deploying to smartphones

- Physical Access: when physical access to the device is available, local installation is performed:
  - Melted application: the Agent is combined with any application; when run, the original application is presented to the user, while the Agent is silently installed.
  - Agent pretends to be a common application
  - Perfect for social engineering attacks
  - Application can be remotely delivered
- Through a web link: a Web Link is delivered to your target.
  - By sending an email
  - Accompanying the link with appealing text
  - Perfect for social engineering attacks
- Through messages: a message containing an URL is sent to the target. With this infection vector:
  - Agent appears as a common application
  - the link can be automatically loaded and prompted to the user

- you can include text in the message

- Zero-Day Exploits: we research and develop zero day exploits also for mobile devices, targeting the most common platforms (e.g., Android) and native applications, for maximum efficacy.

4.2.3 Deploying in WiFi networks

HackingTeam's Tactical Network Injector (TNI) is a portable solution to infect targets connected to WiFi and LAN networks. The operator bypasses the WiFi network protection, joins it, identifies the target of interest and deploys the RCS agent. The TNI embeds a patented technology that permits to operate without being in-line.

WiFi Cracking Capabilities

- Wired Equivalent Privacy (WEP 64 and 128 bit): exploiting protocol vulnerabilities, the WEP passphrase is found in less than 3 minutes;
- WiFi Protected Access (WPA/WPA2): using dictionary-based attacks, the TNI automatically cracks the WiFi password;
- WiFi Protected Setup (WPS): a special attack against the WPS protocol is used to crack the WiFi network.

Target Infection Capabilities

The TNI supports the operator in identifying the target on the network by discovering the hosts. For each host found, the following information is reported:

- 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, for example when the target:

- downloads any executable file (.exe) from the Internet;
- visits any website;
- opens a YouTube video;
- visits any Web resource.

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 the target's 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.

4.2.4 Deploying at the Internet Service Provider

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

- installed in the Internet Service Provider's premises
- no need for inline installation, thanks to HackingTeam's patented technology
- target can be identified via different criteria, covering all the possibilities:
    - IP Address or IP Range
    - MAC Address
    - DHCP Parameters
    - Radius Parameters
    - Content of packets through DPI
- different infection techniques, to be used when the target:
    - downloads any executable file (.exe) from the Internet;
    - browses the web;
    - watches YouTube videos;
    - accesses any Web resource..
- Available with 1GB and 10GB ports, with fiber and copper connectors (SFP+)
- Easy management of multiple NIAs
- Project study, implementation and support for full ISP coverage.

4.2.5 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 from the device, to resist forensic analysis.

4.3 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.

4.3.1 Desktop

On Desktops, the Agent collects:

- Chat and messages from different social networks (Facebook, Twitter, etc)
- Mail from native clients and web interfaces (Outlook, Windows Mail, GMail, etc)
- Any file opened, even if encrypted and and resident on external drives
- Screenshots
- Visited web sites
- Stored passwords from browsers, mail clients, etc.
- Keylogging, also from on-screen keyboards
- Text in the clipboard (copy&paste)
- Position, even when no GPS is available
- Microphone recording
- Information on hardware and software
- Webcam photos
- Recording of Skype and voice applications calls
- Download and upload of files
- Contacts
- And much more

4.3.2 Mobile

On Mobiles, the Agent collects the following Evidence:

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

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

4.3.3 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 among 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.

4.4 Evidence transmission

Evidence is transmitted from the Agent to the RCS Collector using the best communication channel available on the device. Differently, you can instruct a specific usage of these channels (e.g. use only WiFi and avoid data connections (2G/3G/4G), by changing the Agent's configuration.

For Windows, OS X and Linux Agents, transmission is done using any wired or wireless Internet connection available. In case of WiFi networks, the Agent automatically recognizes open and preconfigured Access Points and connects to them.

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 obtain access to the Internet.

For BlackBerry, Android, iOS, and Windows Phone Agents, transmission is done via GPRS/UMTS/3G/4G or WiFi. If the device has transmission switched off, the Agent silently switches them on, to shut them off again once transmission is complete.

To avoid extra billing for the data connections used to send evidence, simply instruct the Agent to use a different Access Point Name (APN).

4.5 Off-channel 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.

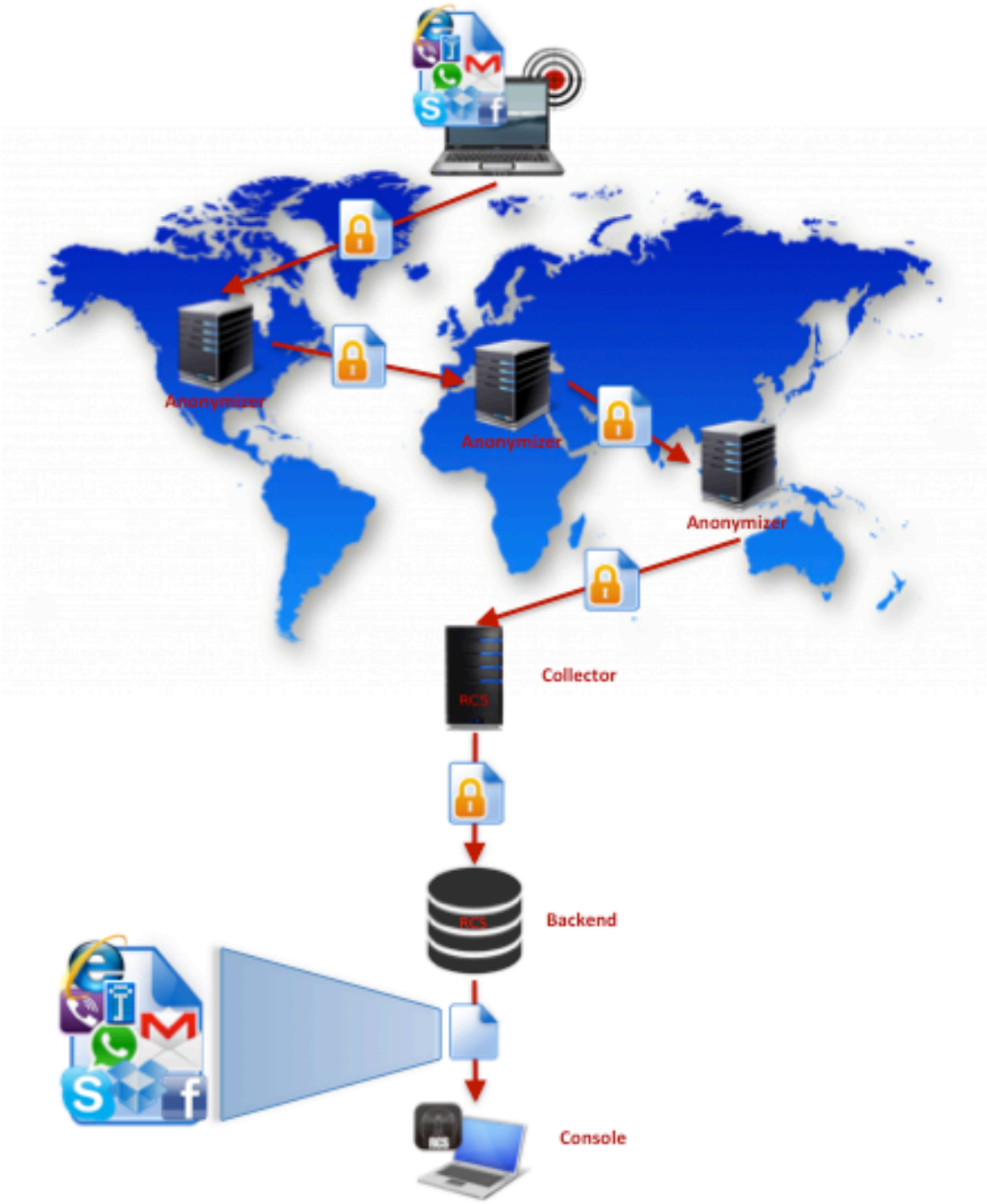


Figure 2 – Evidence flow of RCS

4.6 Event/Action Paradigm

You can configure each Agent to work according to criteria designed for the specific scenario. Using the embedded event/action logic and the drag&drop interface, you instruct the Agent to detect a set of events and react accordingly. Moreover, you collect only the relevant evidence, without arousing suspicion.

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 linked to actions, and Actions can be linked to collection modules. With this paradigm you can easily design the behavior of each of your Agents.

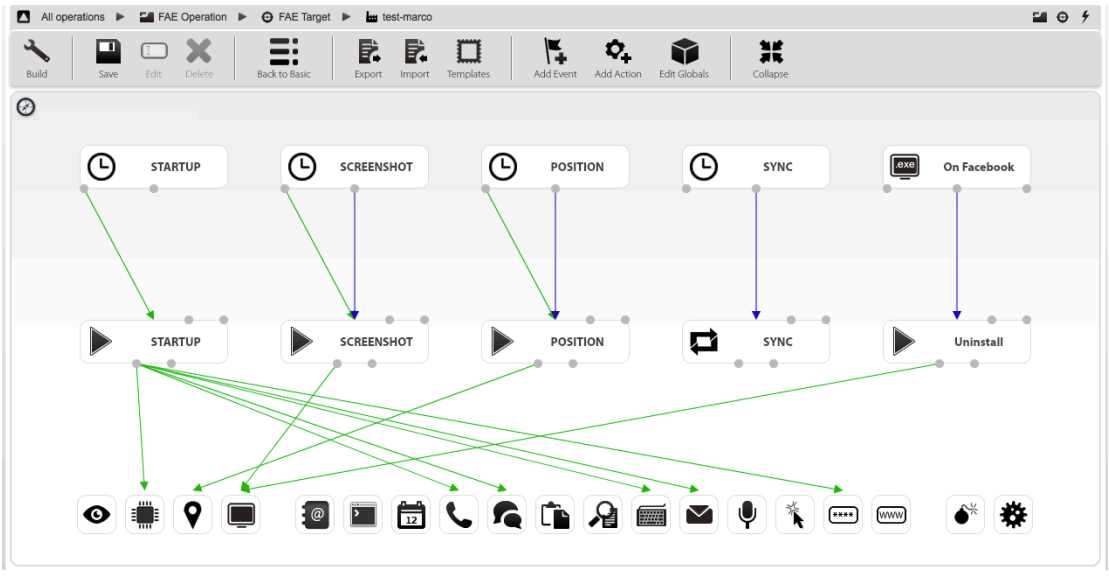


Figure 3 – Advanced Configuration Example 1

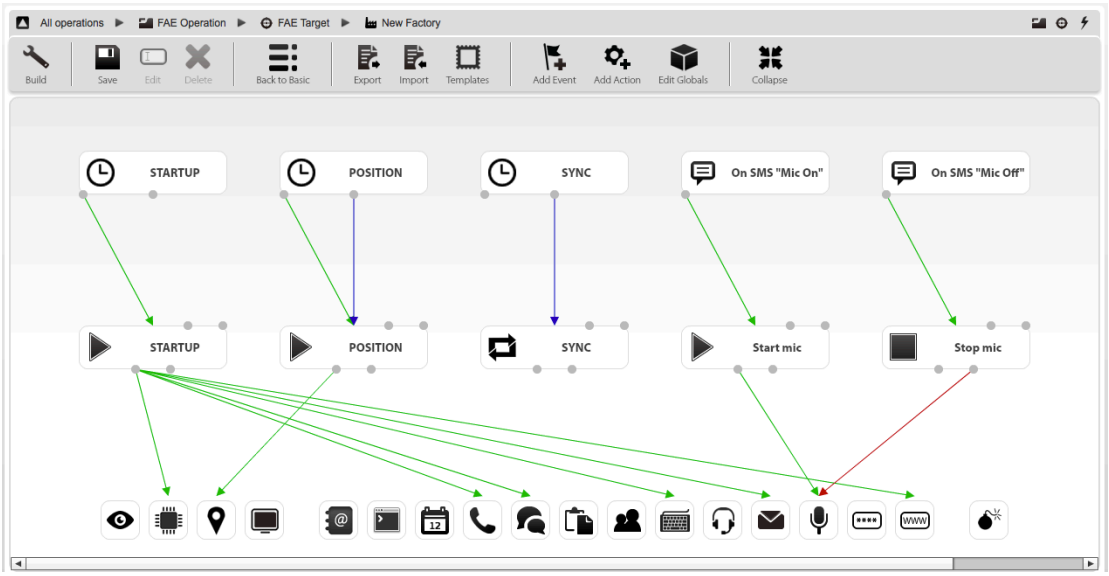


Figure 4 – Advanced Configuration Example 2

5 Intelligence

The better understand the data you collect, Remote Control System provides a correlation engine that highlights all the relevant features. With the Intelligence module, you can dramatically speed up you investigation, by immediately discovering relations among targets, places and communications.

The Intelligence module is divided in two major functionalities: profiling and correlation:

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

Profiling and correlation automatically process all incoming data, in realtime. Furthermore, you can manually load additional information (eg. target's photos, phone numbers, accounts, etc.) to make correlation even more comprehensive and powerful..

5.1 Profiling

Profiling gives you access to useful information about the 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.

Information can be filtered by date, giving you the possibility to see how things change in time.

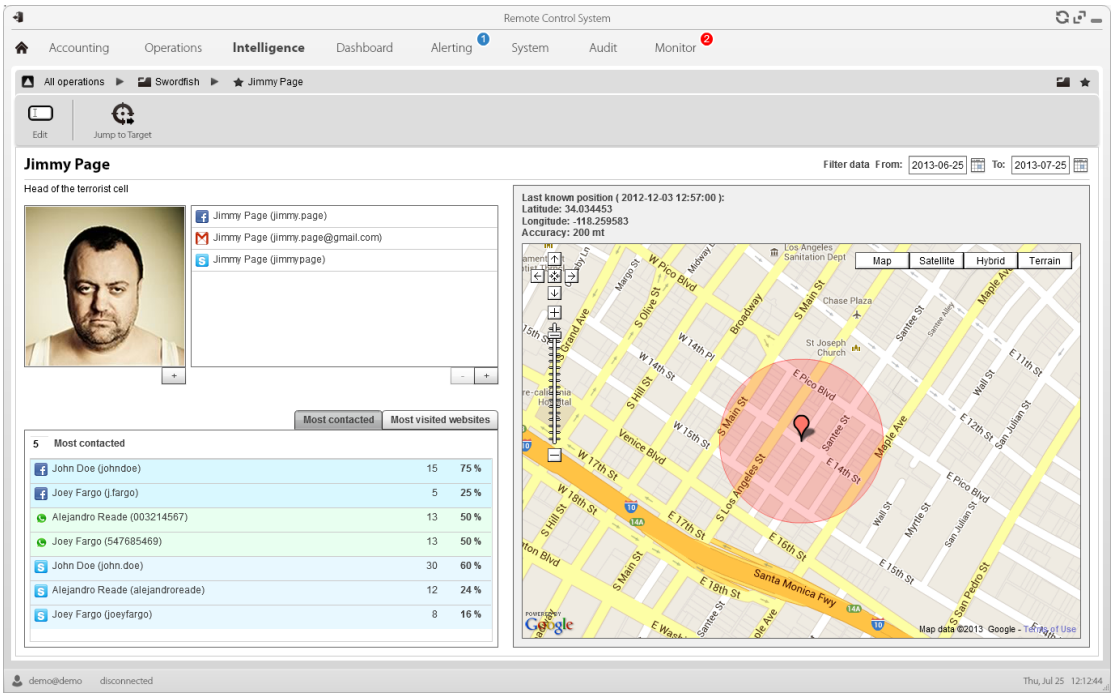
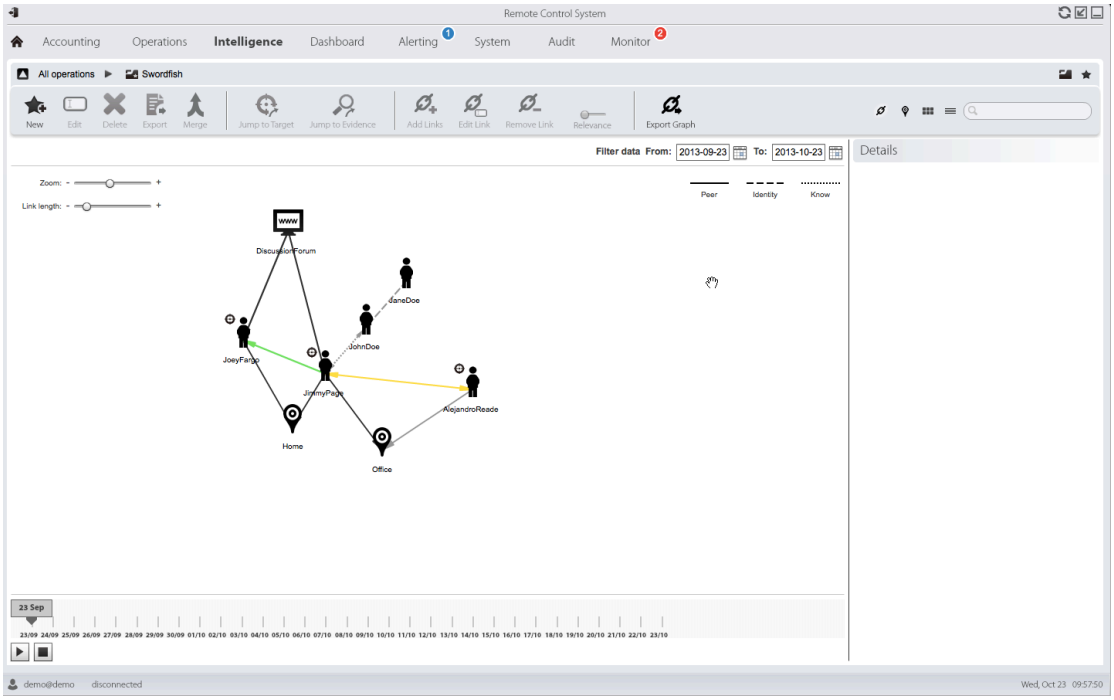


Figure 5 – Profiling of a target

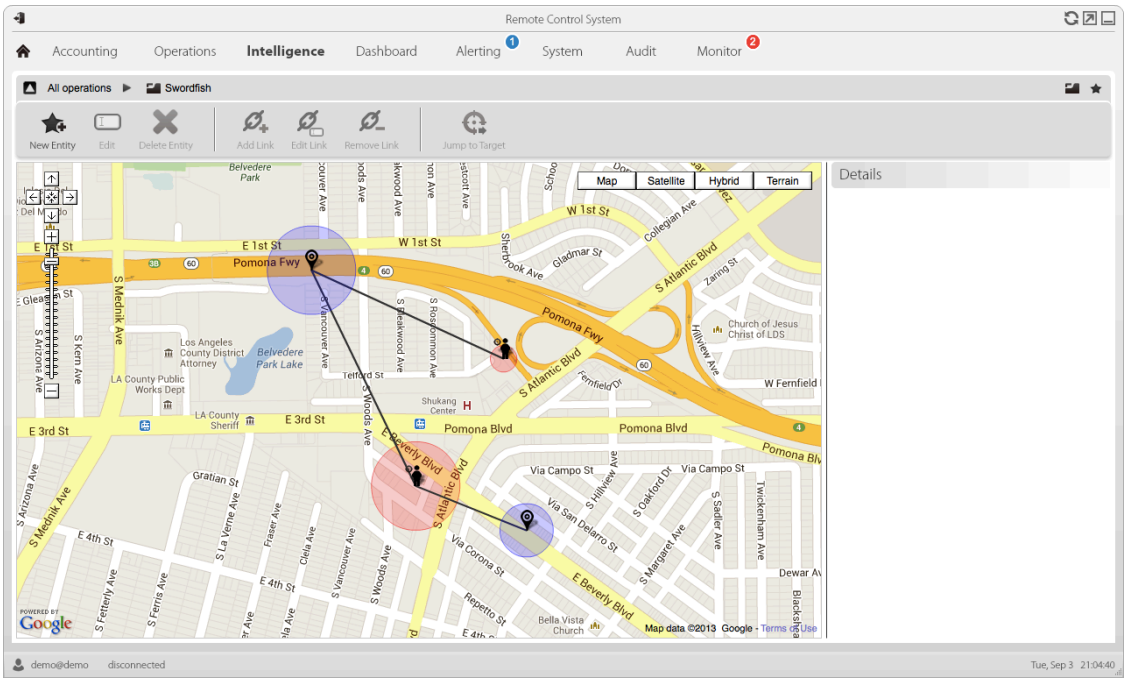
5.2 Correlation

Correlation allows you to have a deep insight on the relations between your targets, in an easy to understand view. You can add new entities, specify persons of interest or indicate a place that want to take into account in your investigations.

The Correlation module shows you the relations between entities, with the possibility to drill down and see the details that made up the relation itself. It is easy to identify the places where your target works, lives or meets his accomplices. Further, it is easy to analyze the communication flux between a target and everybody else, even if they are not being actively investigated.



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.


Remote Control System
Accounting
Operations
Intelligence
Dashboard
Alerting
System
Audit
Monitor
All operations
Swordfish
New Entity
Edit
Delete Entity
Add Link
Edit Link
Remove Link
Jump to Target
Details
Map
Satellite
Hybrid
Terrain
Pomona Fwy
E 1st St
W 1st St
S Atlantic Blvd
Pomona Blvd
E 3rd St
E Beverly Blvd
Via Campo St
Belvedere Park
Belvedere Park Lake
Los Angeles County District Attorney
LA County Public Works Dept
LA County Sheriff
Shukang Center
Church of Jesus Christ of LDS
Bella Vista Church
Map data ©2013 Google
demo@demo
disconnected
Tue, Sep 3 21:04:40

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:

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

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 always available 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. The 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.