Remote Control System

POC

Table of Contents

1 Overview

The purpose of the demonstration is to give the client an overview of the most prominent functionalities of Remote Control System (RCS).

The demo is operated by a Field Application Engineer (Engineer from here on), simulating a hypothetical investigation, during which our Engineer will:

- Impersonate the target under investigation and perform selective actions, usually considered safe, on the target's device (laptop or smartphone). The actions will include browsing a trusted website, opening some encrypted documents and making a Skype call.

- Impersonate the LEA operator and review the collected evidence, then remotely control the agent.

1.1 Prerequisites

Our Engineer will bring all the necessary equipment for the demo, consisting of the following main components, and excluding accessories (e.g. power adapters, cables, etc):

- Windows 7 laptop protected by Kaspersky Internet Security 2012
- BlackBerry smartphone
- RCS Server
- Network Injector
- Network Router and Switch to replicate a simplified ISP network.

NOTE If required, a complete list of all the equipment is available, comprehensive of the serial numbers for identification of each piece.

To experience the demo, the following equipment must be available at the premises where the demo is to be given:

- A wall projector (best if capable of 1280x800 resolution).
- A wired Internet connection (min. 1mbps).

NOTE WiFi connection is not supported.

In case a firewall is present, the following ports must be open for outgoing connections:

- 53/UDP (dns)
- 80/TCP (http)
- 443/TCP (https)

NOTE The Internet connection is mandatory to showcase Skype calls collection, installation of the agent through ISP networks and infection of BlackBerry smartphones.

1.2 Demo Scenario

The demo will be performed as a hypothetical investigation: our Engineer will act both as the Target under investigation and as the LEA Officer in charge of reviewing the evidence collected and infer conclusions.

1.3 Demonstration setup

The demonstration is composed of the following elements:

RCS Agent: a software component to be installed on both Targets (laptop and smartphone). The Agent is invisible to security suites (i.e. antivirus and anti-rootkit) and able to autonomously collect evidence out of the device on which is installed, according to a preset configuration.

Desktop Target: an off-the-shelf laptop running Windows 7, with common applications and browsers installed (e.g. Firefox, Skype, TrueCrypt), used as a target for the infection.

NOTE To show invisibility to antivirus software, the Desktop Target is protected with **Kaspersky Internet Security 2012**, updated to the day of the demo.

BlackBerry Target: an off-the-shelf BlackBerry 9300 Curve smartphone, updated with the latest version available of the operating system.

RCS Server: a laptop running the server installation of Remote Control System. The laptop will act both as collector for the collected evidence and as the Console system to review the evidence. Both the Desktop Target and the BlackBerry Target send the collected evidence to this system, either through WiFi or Ethernet LAN connection.

Network Injector: a laptop equipped with two network cards and running the Network Injector software. This system is able to monitor the traffic of the Desktop Target, and by selectively modifying it, injects a Java applet into browsed web pages according to a set of configurable rules (i.e. inject the applet when the target identified by IP 1.2.3.4 browses to www.facebook.com).

Network Switch: an Ethernet switching device, intended to simulate the internal ISP network. The Switch has one port configured for mirroring the traffic of all the devices connected to it: this port is used by the Network Injector to monitor the traffic of the Desktop Target.

Network Router: provides Internet connection to the Switch and isolates the demo environment from the outside network.

RCS Console: our online demo system, which may be used to perform necessary operations during the demo, such as sending an SMS to infect the BlackBerry Target.

2 The Demo

Our engineer will perform a sequence of specific operations to perform the demo, starting as the Target, and then moving to the LEA Officer role.

Following are the details of both parts, together with summary tables.

2.1 As the Target using a Desktop system

2.1.1 Infection of the Target Desktop

Installation of the RCS Agent by injecting a Java applet into a webpage (e.g. login.live.com). The injection will be performed using the Network Injector in our demo environment, which conceptually imitates the network of an ISP:

- Switch imitates the Core network, onto which potential Targets are connected;
- Router isolates the ISP network and imitates its connection to the Internet.

NOTE After successful installation of RCS Agent on the Target Desktop, the desktop wallpaper is changed. This is only for the purpose of the demo and it's not going to happen during real usage of RCS.

2.1.2 Camera snapshots

A series of snapshots is collected using the webcam that sits on top of the laptop screen.

2.1.3 Encrypted documents

Documents protected with TrueCrypt are collected as soon as they are opened.

TrueCrypt works by creating a container file into which documents can be stored. The container itself is a single binary file, but if opened by providing the correct password, unlocks its content and makes it available as an additional drive.

Access to the stored documents is protected by **AES-256 encryption algorithm**.

2.1.4 Skype call and chat messages

A call made using Skype, either to a Skype account or to a mobile phone, is collected, together with all the contacts registered within Skype.

2.1.5 Location of the Target Desktop

Location of the Target Desktop is inferred by using WiFi information, where available.

NOTE If the Target System is unable to see any WiFi network in the surroundings, or Google have not mapped the surroundings, it may be impossibile to infer the location of the target.

2.1.6 Accessory evidence

Other kinds of evidence is collected during the normal operation of the RCS Agent, such as:

- Keylogging
- Address book (e.g. Skype contacts)
- Mouse clicks
- Browsed URLs
- Clipboard (Text copied and pasted)
- Stored passwords (e.g. Internet Explorer saved passwords)
- List of executed applications
- General information on the device

2.2 As the Target using a BlackBerry

2.2.1 Infection of the BlackBerry with a WAP-PUSH SMS or SMS containing a link

A WAP-Push SMS / SMS containing a link will be sent from a remote server to the BlackBerry Target, concealed as an update coming directly from Research In Motion (the manufacturers of BlackBerries) or a link coming from a local operatore. The Target (our Engineer), by accepting the message, involuntarily performs the installation of the RCS Agent.

2.2.2 Collection of screen snapshots

Upon infection and according to configuration, a number of snapshots of the Target BlackBerry screen will be taken.

2.2.3 Collection of contacts

Upon infection, the contacts already present on the phone are collected. Any new contact registered after that moment is collected as well.

2.2.4 Collection of emails & SMS

All the emails and SMS sent and received, and already present on the phone at the time of the infection, are collected. Any new email or SMS sent or received thereafter is collected as well.

2.2.5 Collection of BlackBerry Messenger

Messages sent using BlackBerry messenger are collected as they were normal SMS.

This is true for messages already present on the phone at the time of infection or messages sent or received thereafter.

2.2.6 Location of the BlackBerry

Location of the Target BlackBerry is inferred by using either GSM cell information or WiFi information (where available).

> **NOTE** If the Target BlackBerry is unable to see any WiFi network in the surroundings, or Google have not mapped the surroundings, the location of the target is inferred using only GSM cell information.

2.3 As the LEA Officer

2.3.1 Evidence review

The Engineer, acting as the LEA Officer, will show the Customer how it's possible to review, prioritize and export all of the collected evidence using the RCS Console

2.3.2 Alerting

The LEA Officer will show how the alerting feature can highlight specific evidence, according to pre-set rules. The feature is useful to be alerted upon reception of evidence containing a specific keyword (e.g. the word "explosive"), and to have a quick link that permits the Officer to jump directly to the evidence of interest, and automatically prioritize it.

2.3.3 Overview of other infection vectors (optional)

If time is available, or per Customer request, our Engineer will give an overview of all the infection vectors available, together with a brief description of possible scenarios in which they can be used.

2.3.4 Overview of the backdoor configuration (optional)

Each Agent works according to a configuration set upon creation: that configuration may be changed anytime to adapt the Agent to changes in the environment in which it's working, or due to changed investigation needs.

An overview of the Event-Action Logic that drives the Agent behavior is given, together with examples of common configurations and hints to address specific scenarios (e.g. maximize duration of battery on smartphones).

2.4 Conclusions

Once the demo is complete, the Customer shall be aware of the key features of Remote Control System, as to provide interception of encrypted communications and accessory evidence that is usually not transmitted over the network, and thus impossible to collect using traditional means that operate at the network level.

2.5 Summary table: Target Desktop

Action
Infection of the Target Desktop using the Network Injector
Camera snapshots.
Encrypted documents.
Skype call and contacts.
Location (WiFi).

2.6 Summary table: Target BlackBerry

Action
Infection of the BlackBerry with an SMS
Contacts.
Email and SMS.
BlackBerry Messenger.
Location (GSM/WiFi).

2.7 Summary table: LEA Officer

Action
Evidence review.
Alerting.
Overview of infection vectors.
Overview of backdoor configuration.