]HackingTeam[

REMOTE CONTROL SYSTEM

GALILEO

Proof Of Concept

Revision	Author (s)	Release Date
1.0	FAE Team	2014, February 28th

Table of Contents

1 Introduction 4
2 Proof of Concept Methodology 5
3 Scenarios 6

1 Introduction

Goal of the Proof Of Concept (POC) is to show main functionalities and possibilities of use for Remote Control System. The Proof Of Concept is lead by a product specialist, and is the perfect chance to ask any kind of questions and clarifications.

A POC can be done either at client's premises or at HackingTeam's offices. It consist in sample scenarios of investigations and demonstration of how RCS can be used in such situations.

2 Proof of Concept Methodology

All hardware necessary for a POC is provided by HackingTeam: server, targets, local network equipment.

The Client needs to provide:

- Meeting Room adequate to host HackingTeam's engineers and all other participants
- Wired connection to Internet, with a minimum bandwith of 4Mbit/s in download
- Projector or big TV screen (minimum resolution of 1280x800)

It is possible for the Client to provide its own target devices, but the following rules will always have to be agreed and respected:

- All devices to be used as targets have to belong to HackingTeam, the Client or the Partner
- All devices to be used as targets have to be in physical availability of the HackingTeam specialist leading the POC
- HackingTeam reserves the right to hold on to any device used as target during a POC if necessary
- HackingTeam reserves the right to completely wipe any data storage used during the POC (USB Thumbdrives, External Hard Drives, Hard Drives and other types of memory in the devices used)
- If the Client wishes to use its own devices for the POC, brand, model, Operating System version and installed software of each device has to be agreed in advance

3 Scenarios

Scenario 1: Money Laundering

Description:
A group of lawyers is laundering money from illegal business, and giving "clean" money back to their clients, in same or in other countries.
Suspects are based in home office and regular offices where they share computer network with family or with colleagues.
Targets use laptops and smartphones to communicate, and mainly rely on:

- **WhatsApp** for short explanations, meeting arrangements, etc.
- **Email** to share files and documents
- **Phone and Skype** calls for agreements and negotiations
- **Face to face** meetings

Available information:

- 1 Skype account
- 3 email accounts
- 2 suspects addresses (a home and an office)
- 2 mobile phone numbers
- 2 landline phone numbers

Actions:

1. Detect and infect target(s) using the available information.
2. Collect evidences for the court:
    a. Screenshots of the activity performed on mobiles by the targets
    b. Skype calls from the target's desktop
    c. WhatsApp and BBM conversations from the target's Blackberry
    d. List of contacts on the target's Android
    e. Gmail emails from the target's Android
    f. Position of at least one target's device
    g. Money balances sheets will be requested as evidence
    h. Contact information, which might be useful to open new investigations.
    i. Possible virtual currencies transfers.
    j. Managed bank accounts
    k. Anything else that can be collected as supporting evidence

RCS Agent Deployment

REMOTE

Different possibilities are available to remotely deploy the RCS Agent on a device:

- **Exploits:** Documents containing zero-day exploits can be shared using the contact information we have. Opening of such documents can result in a successful infection.
- **TNI:** using the Tactical Network Injector, it is possible to inject "infecting" traffic in the target's wifi connection; this will be doable either breaking into the target's home wifi with the TNI or waiting for the target to be on a public wifi (e.g. airport, Starbucks, etccetera).

- **Melted Application:** through the use of fake profiles, it is possible for the operator to gain enough trust from the target to have the chance to share documents and applications: this is when a melted application or social exploit can be used to infect the target.
- **NIA**: with ISP cooperation, we can inject traffic in the target's internet connection and infect his devices
- **Remote Message:** an Operating System upgrade or new application installation, sent through SMS or WAP Push Message, can be used as a vector to install the Agent on a mobile device.

PHYSICAL

With physical access to the target device, different vectors can be used. This condition can be achieved, for example, during a security check at the airport or breaking into the target's house. Physical infection vectors include:

- **Silent Installer:** with access to a running computer or mobile, few seconds will be enough to install the RCS Agent
- **Offline Installation:** when physical access to a computer which is turned off is available, this vector allows to you to install the RCS Agent without need to know any password, in few minutes.

Scenario 2: Drug Dealing

Description:
An organized group of drug dealers operates in a specific territory and has a pyramidal organization with managers, who purchase big quantities of drug, delivery guys, who distribute small quantities among local dealers, and pushers, who sell little quantities to final consumers.
Police arrested one of the drug pushers, and obtained the information needed to start investigations on the rest of the organization.

Targets use mobile phones to organize drug distribution and to manage money collection from pushers.

- Targets use Android and Blackberry phones
- WhatsApp messages are used to communicate between all levels and with clients.

Available information:

- One member of the organization has been arrested, and his mobile address book is now available
- Information about physical location of some of the members of the organization is known

Actions:

- Detect and infect targets(s) using the available information
- Collect evidence for the court:
    - Screenshots of the activity performed on mobiles by the targets
    - Contacts information to find other members of the organization
    - WhatsApp chats to figure out how organization works
    - Location information to find dealing points and main drug storing place
    - Track SIM changes that suspects may do to avoid phone tapping

RCS Agent Deployment

REMOTE

Applying social engineering techniques and taking advantage of familiarity between band members, an installer could be distributed in several ways:

- Sharing melted applications interesting for the members of the organization
- Sending an SMS or WAP push messages emulating service improvements by service provider

PHYSICAL

As police has an informer in target organization, it is possible to take advantage of different physical infection vectors:

- Local Installation: connecting the Blackberry to the computer, infection can be performed in few seconds
- Installation package: copying and running the RCS Agent on the target phone, infection can be performed quickly
- Visiting a linked previously setup, infection of the smartphone is fast and flawless.

]HackingTeam[