]HackingTeam[

REMOTE CONTROL SYSTEM

GALILEO

Proof Of Concept

Revision	Author (s)	Release Date
1.0	FAE Team	2014, May 12th

Table of Contents

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 Scenario

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 and BBM, which is considered encrypted and secure, are used to communicate between all levels and with clients.

Also, they use their laptops both for personal activities, such as emailing and social networks, and for communicating some information with other members.

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
    - BBM messages, which include the most secret information exchanged between members of the organization
    - Location information to find dealing points and main drug storing place
    - Track SIM changes that suspects may do to avoid phone tapping
    - Sensitive files, such as pictures, on the suspects' phones
    - Information from social networks used by the suspects
    - Important files, such as PDF and DOC from suspects' laptops
    - Passwords stored on suspects' laptops

RCS Agent Deployment

REMOTE

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

- **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. This is true for both mobile and desktop platforms.
- **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

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

- **Silent Installer:** connecting the Blackberry to the computer, infection can be performed in few seconds
- **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.
- Visiting a **linked previously setup**, infection of the smartphone is fast and flawless.

]HackingTeam[