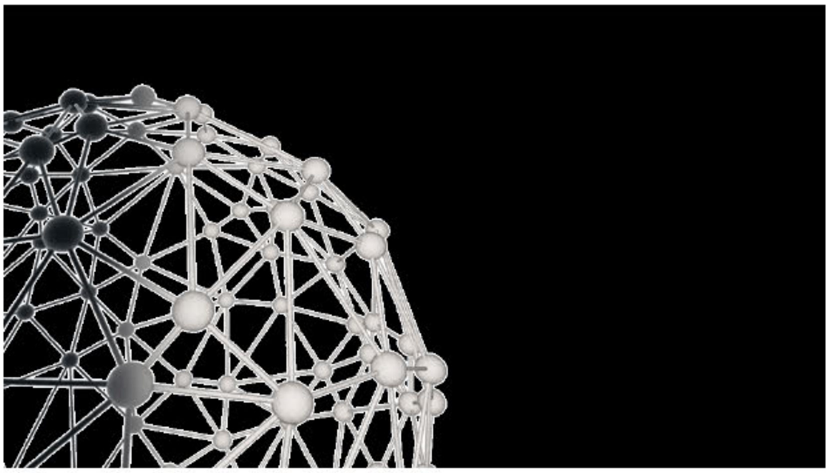
]HackingTeam[

REMOTE CONTROL SYSTEM GALILEO

Proof Of Concept



Revision	Author (s)	Release Date
1.1	FAE Team	2014, April 18th

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 1200x800)

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

Scenario: 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 Windows laptops and Android smartphones to communicate, and mainly rely on:

- **WhatsApp** for short explanations, meeting arrangements, etc.
- **Email** to share files and documents
- **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 (emulated environment).
- **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.

EVIDENCE COLLECTION:

On Desktop:

- Windows 7 SP1
- McAfee Antivirus
- Firefox used as browser

The following evidence are collected

	Verified?		
List of Facebook Friends	□ **N/A**	□ **OK**	□ **Error:**
List of contact in Gmail webmail	□ **N/A**	□ **OK**	□ **Error:**
Recording of Skype call	□ **N/A**	□ **OK**	□ **Error:**
Webcam Pictures	□ **N/A**	□ **OK**	□ **Error:**
Facebook Private Messages	□ **N/A**	□ **OK**	□ **Error:**
Device Information	□ **N/A**	□ **OK**	□ **Error:**
PDF opened by the user	□ **N/A**	□ **OK**	□ **Error:**
Mails from Outlook.com	□ **N/A**	□ **OK**	□ **Error:**
Mails from Gmail webmail	□ **N/A**	□ **OK**	□ **Error:**
Microphone recording	□ **N/A**	□ **OK**	□ **Error:**
Position	□ **N/A**	□ **OK**	□ **Error:**
Screenshots	□ **N/A**	□ **OK**	□ **Error:**

On Mobile:

- Samsung Galaxy SII
- Android 4.0.3
- Rooted device

The following evidence are collected

	Verified?		
List of contacts saved on the Phone	□ **N/A**	□ **OK**	□ **Error:**
Past and Future events on calendar	□ **N/A**	□ **OK**	□ **Error:**
List of calls after infection	□ **N/A**	□ **OK**	□ **Error:**
Device Information	□ **N/A**	□ **OK**	□ **Error:**
Whatsapp chats	□ **N/A**	□ **OK**	□ **Error:**
Viber chats	□ **N/A**	□ **OK**	□ **Error:**
Skype chats	□ **N/A**	□ **OK**	□ **Error:**
SMS after infection	□ **N/A**	□ **OK**	□ **Error:**
Microphone recording	□ **N/A**	□ **OK**	□ **Error:**
List of saved wifi passwords	□ **N/A**	□ **OK**	□ **Error:**
Position	□ **N/A**	□ **OK**	□ **Error:**
Screenshot	□ **N/A**	□ **OK**	□ **Error:**

INFECTIONS:

Windows 0-day Exploit	Verified?
On a vulnerable PC, infection is performed through exploitation of Microsoft Word, using a .docx document. The PC will have the following characteristics: • Windows 7 SP1 • Microsoft Office 2013 • Adobe Flash for Internet Explorer, latest version	□ **N/A** □ **OK** □ **Error:**

Tactical Network Injector	Verified?
On a Windows PC, infection is performed through injection of traffic in a Youtube stream. The PC will be configured as follows: • Windows 7 SP1 • Internet Explorer used for browsing	□ **N/A** □ **OK** □ **Error:**

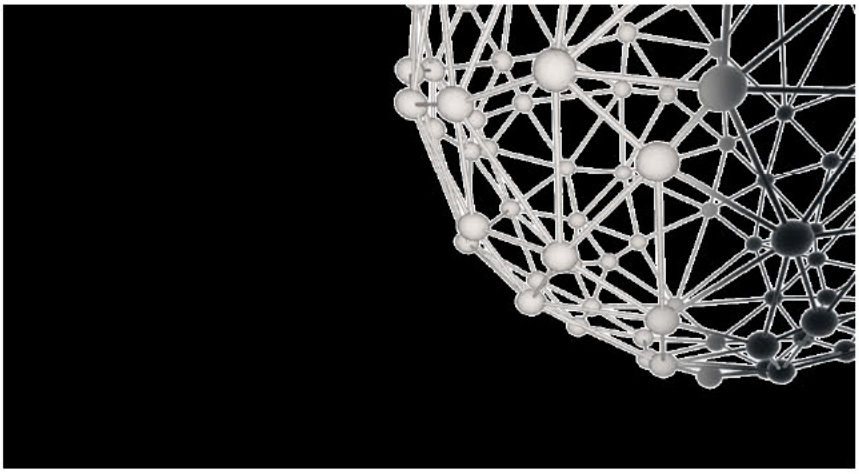
Windows Melted Application	Verified?
On a Windows PC, infection is performed through installation of a melted application. The PC will be configured as follows: • Windows 7 SP1 • VLC Media Player Installer used for melting	□ **N/A** □ **OK** □ **Error:**

SMS Message on Blackberry	Verified?
On a Blackberry, infection is performed sending an SMS message containing a link to the infecting Application. The following Blackberry will be used: • Blackberry Curve 9300 • Blackberry version 6.0.x	□ **N/A** □ **OK** □ **Error:**

QR Code link on Android	Verified?
On a Android phone, infection is performed visiting a weblink from a QR Code generated by RCS. The following Android will be used: • Samsung Galaxy SII • Android 4.0.3	□ **N/A** □ **OK** □ **Error:**

OS X Silent Installer	Verified?
On a MacBook Pro, infection is performed through installation of a Silent Installer. The Mac will be as follows: • MacBook Pro • OS X Mavericks	□ **N/A** □ **OK** □ **Error:**

Linux Silent Installer	Verified?
On a PC running Linux, infection is performed through installation of a Silent Installer. The PC will be as follows: • Ubuntu 12.04	□ **N/A** □ **OK** □ **Error:**



]HackingTeam[