Tests on Windows 7

Infection methods

The following infection methods will be shown, complete with an explanation of the typical operating scenario they apply to:

- Physical infection (CD, USB Thumb drive)
- Infection by exploit
- Tactical Network Injector

Data collection

The following data is collected from the target device and shown to the Console operator, together with an example of their relevance toward a successful investigation:

- Skype Calls
- Microphone
- Gmail, Facebook and Skype contacts list
- Camera still pictures
- Chats from different applications (e.g., Skype, Facebook, Twitter)
- List of visited URL
- Files opened by the target
- Stored Passwords from Internet Explorer and Firefox
- General informations on the device (hardware specs, operating system, installed applications)
- Keylogs
- Location of the computer

Remote actions

The following examples of remote actions are shown to demonstrate the additional capabilities of the system:

- Making the computer temporarily unusable
- Uninstalling the Agent remotely from the Console

Tests on Android or Blackberry

Infection methods

The following infection methods will be shown, complete with an explanation of the typical operating scenario they apply to:

- Physical infection (installation package),
- QR Code
- WAP Push Message (if supported by local mobile operators)

Data collection

The following data is collected from the target device and shown to the Console operator, together with an example of their relevance toward a successful investigation:

- Chat (e.g., WhatsApp, Viber, WeChat)
- Microphone
- Call history
- Contacts list
- SMS
- Calendar
- Location of the smartphone
- General infromation on the device (hardware specs, operating system, installed applications)
- History of opened applications

Note: some of the above collection capabilities may require a rooted Android device.

Remote actions

The following examples of remote actions are shown to demonstrate the additional capabilities of the system:

- Making the smartphone temporarily unusable
- Uninstalling the Agent remotely from the Console