]HackingTeam[

RCS Network Injector

Datasheet

Important Notice

Document Approval

Revision	Author(s)	Release Date
1.1	Valeriano Bedeschi	6th December 2011

Table Of Contents

1 Overview

HackingTeam's *Network Injector* (NI) installs RCS Agents over the Target's Internet connection by using a patent-pending injection technique and a proprietary streaming melting technology.

Network Injector is capable of inserting an RCS Agent into any downloaded executable file and browsed web page, without visible changes in the content.

Deployment of the Network Injector can be done inside any network: from small home WiFi networks to geographically distributed Internet Service Providers.

Multiple users can be monitored and different types of injection are available, such as injection into web pages or downloaded applications.

1.1 Deployment scenarios

The Network Injector can operate in different network scenarios, either on a LAN or an intra-switch segment. Two network links are necessary for placing the device on the target network, one for monitoring and one for injection.

NOTE In case of failure of the appliance, there is no risk of connection shortage, since the IPA is not an inline device.

1.1.1 Monitoring

The first link is used for monitoring the traffic on the tapped LAN segment, either by using a mirror port of the switch (SPAN port), a network TAP interface (transparent inline connection) or a WiFi card in monitor mode.

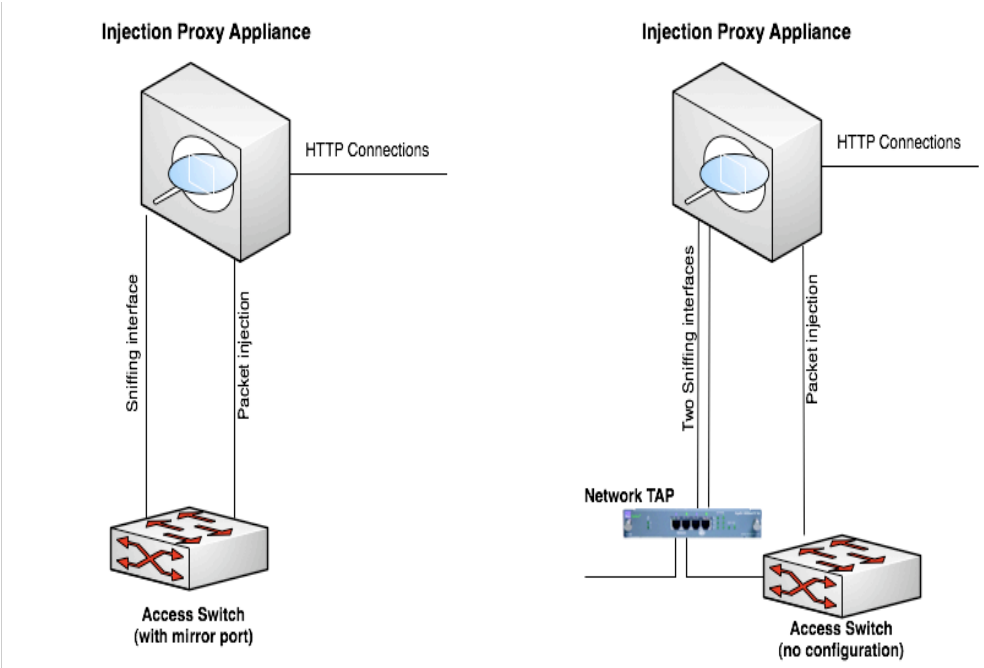

Figure 1 - Common IPA deployment scenarios

By using dedicated wire-speed network interfaces, IPA is compatible with many physical network links, and is capable of monitoring them even when running at full speed.
Connectors (GBIC) are provided for monitoring with Ethernet copper and Fiber Optic links.
NI can cope with up to 10Gbps traffic, and usually comes in two versions, with four 1Gbps ports or one 10Gbps port.

1.1.2 Packet injection

This second link is used for transparently proxying HTTP connections and crafting packets during the injection phase.

For the purpose of crafting packets, a valid IP address is required, better if on the same network under monitor.

> **NOTE** No disruptive packets are sent from the IPA.
> In the worst case, only connections related to the target under investigation may be in any way affected, dropper or modified.

Depending on the security policies present on the injection network, it may be necessary to allow some traffic on switches and routers for the IPA to work properly.

1.1.3 Management

Multiple Network Injectors can be separately managed trough the RCS Console: a different set of rules, unique to each NI, can be configured.

1.2 Deploying at the ISP

The most common scenario of deployment at the ISP is to monitor the ADSL line of subscribers under investigation.

When the Network Injector (NI) is placed on a network segment between the DSLAM concentrator and the ISP core network, any subscriber connected to the DSLAM can be monitored.

Identification of the specific subscriber can be done using one or more of the following criteria:

- RADIUS parameters
- Subscriber username
- Calling station ID
- Session ID
- NAS IP Address and NAS Physical Port
- Static IP Address
- String matching (e.g., email address, social network login)
- DHCP information

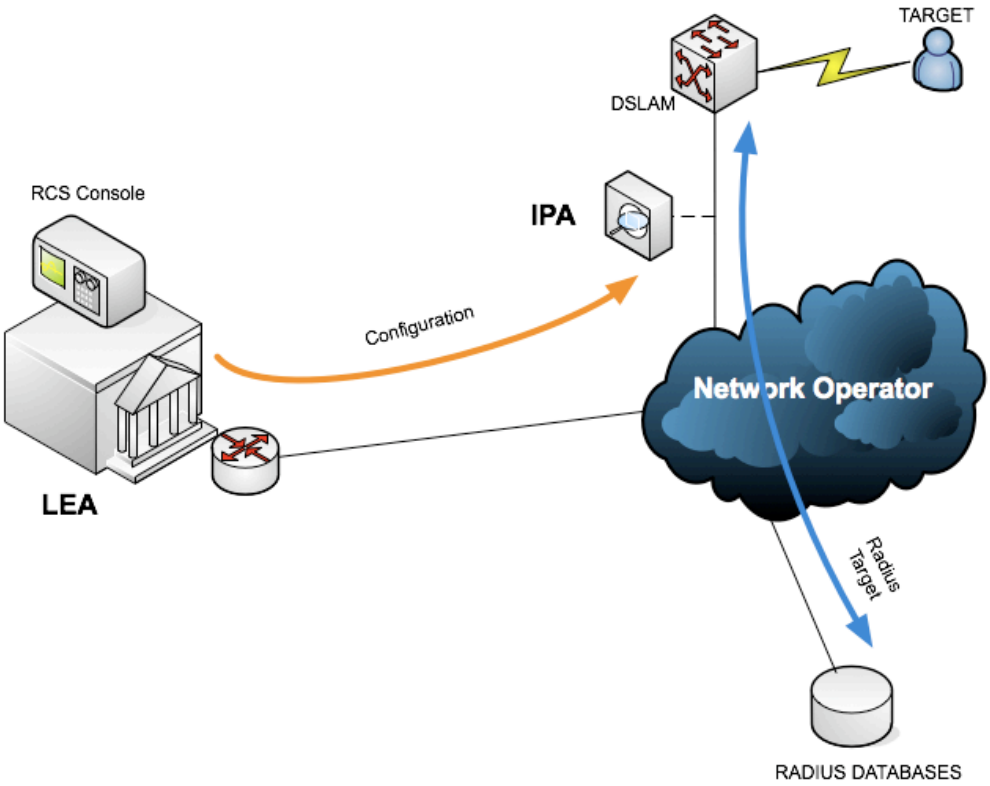

Figure 2 - ISP deployment

NOTE Installation and deployment of Network Injector on a ISP network is subject to validation by HackingTeam Engineers.

1.3 Usage in WiFi networks

If the target user is joined to a WiFi network, Network Injector must be equipped with two WiFi cards. One card is joined to the same network of the target, while the other card monitors the traffic of the same network.

2 Agent Deployment

Network Injector (NI) can embed RCS agents into different resources available on the web.

Resource	Description
Executable file	An RCS agent is embedded into any downloaded executable (e.g., setup packages, automatic software updates)
Web page	NI is able to inject special HTML code into any web page, triggering the installation of RCS agent during web browsing.
Any resource	Any resource download by the user can be replaced with an exploiting document generated by the Exploit Portal