]HackingTeam[

RCS Injection Proxy Appliance

Whitepaper

Important Notice

HT s.r.l. shall bear no responsibility or liability to a client or to any person or entity with respect to liability, loss or damage caused or alleged to be caused directly or indirectly by any HT s.r.l. product. This includes, but is not limited to, any interruption of service, loss of business or anticipatory profits or consequential damage resulting from the use or operation of any HT products. Information in this document is subject to change without notice and does not represent a commitment on the part of HT s.r.l. The systems described in this document are furnished under a license agreement or non-disclosure agreement.

All information included in this document, such as text, graphics, photos, logos and images, is the exclusive property of HT s.r.l. and protected by international copyright laws. Permission is granted to view and photocopy (or print) materials from this document for personal, non-commercial use only. Any other copying, distribution, retransmission or modification of the information in this document, whether in electronic or hard copy form, without the express prior written permission of HT s.r.l., is strictly prohibited. In the event of any permitted copying, redistribution or publication of copyrighted material, no changes in, or deletion of, author attribution, trademark legend or copyright notice shall be made.

Document Approval

Revision	Author(s)	Release Date
1.0		

Table Of Contents

1 Overview

HackingTeam's *Injection Proxy Appliance* (IPA) is an offensive security device for performing remote installation of RCS agents, by using a patent-pending injection technique and a proprietary streaming melting technology.

IPA is capable of injecting an RCS installer into any downloaded executable file and browsed web page, without any visible change in the content.

Different physical links are supported for deployment inside any network: from small home WiFi networks to geographically distributed Internet Service Providers with thousands of subscribers.

Multiple users can be continuously monitored and injection of different resources (e.g., web pages, installers) can be performed concurrently.

1.1 Deployment scenarios

Injection Proxy 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.

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.

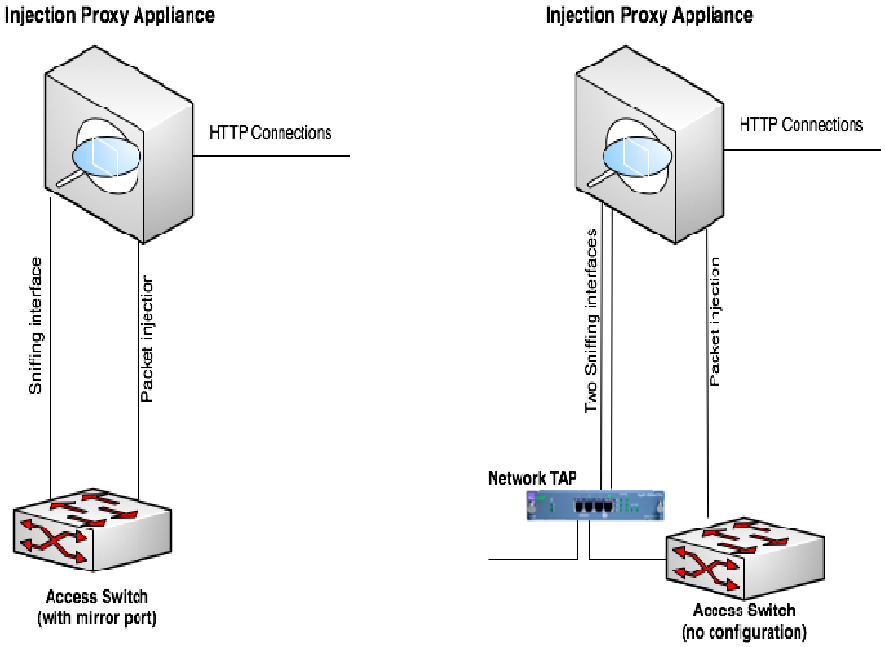

Figure 1 - Common IPA deployment scenarios

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.

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.

1.2 Deploying at the ISP

The most common scenario of deployment at the ISP is to monitor all the ADSL line subscribers connected to a particular DSLAM (**D**igital **S**ubscriber **L**ine **A**ccess **M**ultiplexer) concentrator.

When the IPA is placed on a network segment between the DSLAM concentrator and the ISP core network, any end-user connected to the DSLAM can be targeted.

Identification of the specific user to be targeted may be done using any 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

By specifying multiple rules, it’s possible to identify multiple targets, even if each one needs different criteria for identification.

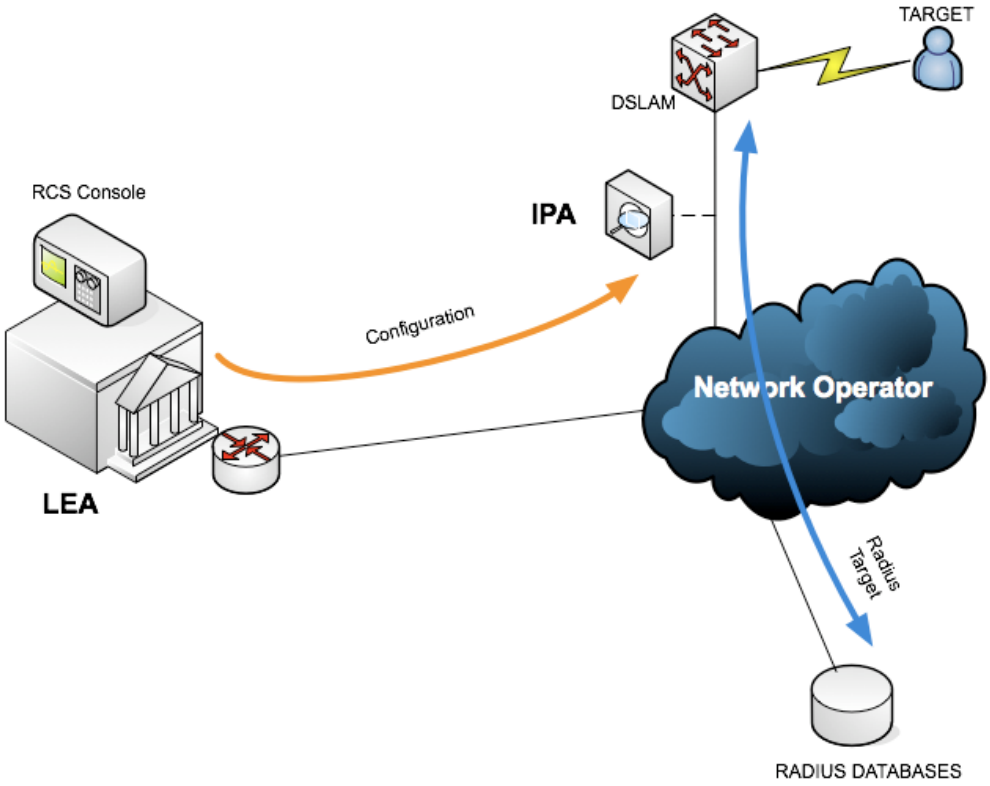

Figure 2 - ISP deployment

NOTE	Installation and deployment of IPA on a target ISP network is subject to validation by HT engineers.

1.3 Usage in WiFi networks

If the target user is joined to a WiFi network, the Injection Proxy must be equipped with two WiFi cards. One card must be joined to the same network, by knowing the access key if any; the other card must be able to monitor the WiFi traffic of the same network.

By using RCS console it’s possible to centrally manage multiple IPA installations.

2 Agent Deployment

IPA 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	IPA 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