]HackingTeam[

RCS Network Injector Appliance

Datasheet

Important Notice

Document Approval

Revision	Author(s)	Release Date
1.2	Daniele Milan	3rd January 2012
1.3	FAE Team	February 2014

Table Of Contents

1 Overview

HackingTeam *Network Injector Appliance* (NIA) is a hardware appliance for monitoring target's Internet traffic and install RCS Agents over their Internet connection, using a patent-pending streaming injection technique and proprietary executable melting technology.

Injection may target executable files being downloaded or browsed web pages: no visible changes are presented to the Target.

1.1 Essential concepts

The NIA works on a set of assumptions and logics that must be understood before investigating where to place the NIA in the Internet Service Provider (ISP) network.

The basic piece of information needed by the NIA to perform an injection is a **rule**, that tells the NIA how to identify the target and an interesting HTTP connection, then how to modify that connection to install a RCS Agent on the Target's device.

1.1.1 Target identification

Target identification is usually done by matching the Target's **static IP address** with the address of all the HTTP connections seen by the NIA.

In case the ISP is using **Radius** as a way of identifying its subscribers upon connection, four different types of Radius attributes can be used to identify the target:

- Login
- Call ID
- Session ID
- Technical Key

By matching Radius packets the NIA discovers the IP address assigned to the Target, and uses it to match its HTTP connections.

1.1.2 Resource identification

Of all the HTTP connections issued by the Target, it's necessary to identify a subset of them that may be used to perform the injection.

HTTP connections refer to a Resource, a piece of information identified by an URL. Each rule must contain an URL that identifies one or more Resources to be injected.

For each rule, an URL must be provided to identify an HTTP Resource: the URL may contain wildcards as well, to permit identification of multiple Resources with a single rule.

NOTE Usage of wildcards to widen the matching of URLs must be used with great care, as it may dramatically increase the load on the NIA, especially when monitoring 10Gpbs links.

1.1.3 Injection

Once the Target and the Resource is identified, the injection takes place: the NIA sends some specially crafted packets to the target to redirect the interesting HTTP connection through itself, thus acting, for that specific HTTP connection only, as a transparent proxy.

This redirection process is heavily dependent on the speed at which packets can be sent to the Target, therefore making positioning of the NIA essential in being able to perform successful injections.

If the speed at which the NIA can send packets is not fast enough, the injection process may fail, thus preventing the injection from happening.

A key factor in positioning the NIA is proximity to the Target: being as near as possible to the Target dramatically raises the chances of performing successful injections.

Once the traffic passes through the NIA, the injection can be carried out introducing a minimal delay by using proprietary injection technology.

NOTE The process of “redirection” of the HTTP connection is patent-pending, so no further detail can be provided here.

1.2 ISP deployment and positioning

The NIA is designed to operate inside the network of an Internet Service Provider (ISP), monitoring the ISP subscribers: when a Target is identified, injection is performed selectively on specific HTTP connections.

The best positioning for the NIA is at the DSLAM, where it can monitor a fraction of the subscribers of the ISP, reducing the amount of aggregated traffic and thus making the deployment easier. Moreover, at the DSLAM there is all the information needed by the NIA, and injection of packets is simpler and have a much higher probability of being successful in performing the redirection process.

Even more important, **the DSLAM is the nearest we can get to the Target within the ISP network**, thus making the DSLAM the absolute best positioning for the NIA.

NOTE Currently, only IP-DSLAMs are supported by the NIA: old mixed analog/digital DSLAMs are not supported.

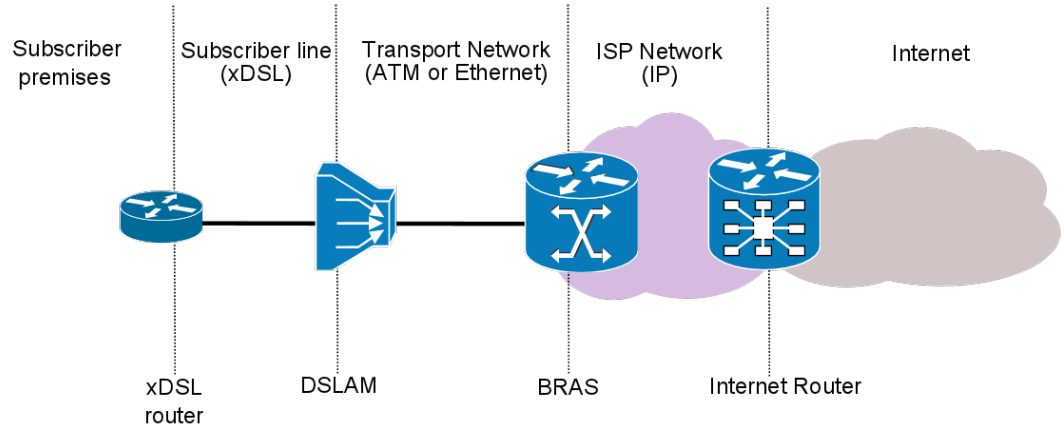

Figure 1 - ISP network diagram

In specific cases, that must be singularly studied, it may be possible to position the NIA at the BRAS level as well, tough undergoing some tradeoffs.

As we get near the Internet Router, it becomes more and more difficult to figure out a possible positioning for the NIA: the amount of bandwidth becomes unmanageable, proper information needed by the NIA may be lacking, and we are as far as possible from the Target.

1.2.1 Monitoring

Monitoring happens by providing the NIA with a copy of the traffic, either by using a mirror port of the switch (SPAN port) or a network TAP interface (transparent inline connection).

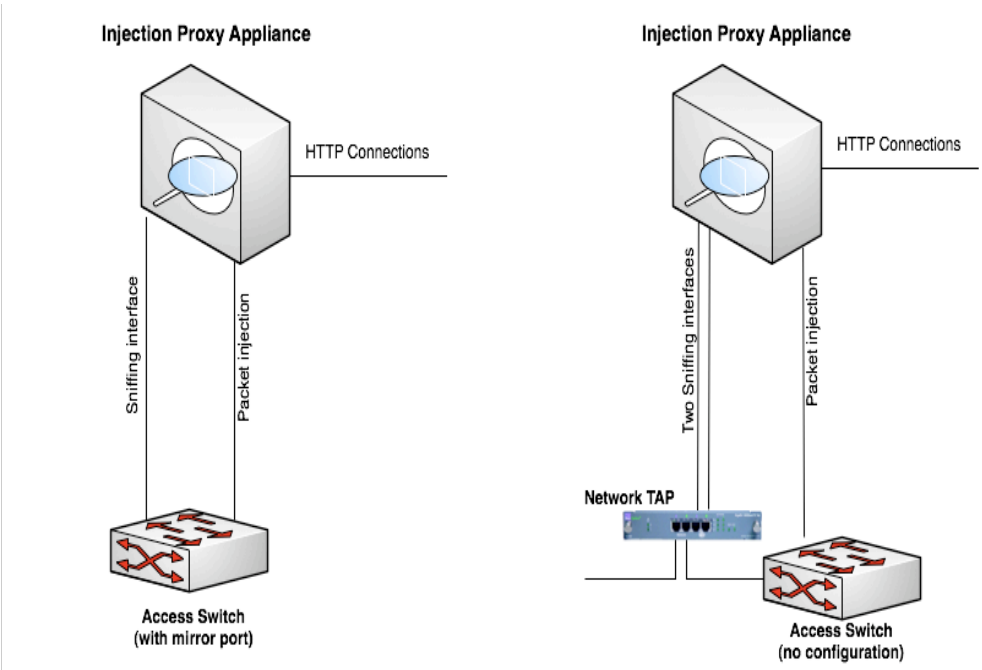

Figure 2 - Common NIA deployment scenarios

By using dedicated wire-speed network interfaces, the NIA is compatible with many physical network links, and is capable of monitoring them even when running at full speed.

1.2.2 Injection

A 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. Moreover the link must be on the same network under monitor, to be able to reach the Target with its own IP address, since the **packets will be injected with the same IP address of the Target as identified on the monitor link**.

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: this eventuality must be addressed case by case.

1.2.3 Specification

Monitoring

Connector Types: RJ45, LC 850nm, LC 1310nm

Max Speed: 10GB

Injection

Connector Types: RJ45

Note: Must be on the same network under monitor, with an IP Address reachable by the target.

Assumption

The sections above are based on the assumption that sniffing equipment (SPAN or TAP) is already deployed at the ISP. If there is none, additional equipment has to be deployed depending on the implementation scenario.

1.2.4 Agent Deployment

During injection, the NIA can embed RCS Agents into different types of HTTP resources.

Resource	Description
Executable file	When an executable application is downloaded, it appends the RCS Agent to the file. When the application is executed, the Agent is installed on the device
Web Pages	When the target visit any website on the Internet, it injects additional code to into the webpage.
YouTube	Forces the target to upgrade the Adobe Flash by blocking the video. Once upgraded, RCS Agent is installed on the computer.
Resource Replacement	You can replace any file on the web with a different file. I.e. it is possible to replace any .doc file downloaded by the target user with a .doc previously built and containing a zero-day exploit

2 Questionnaire

Following is a quick questionnaire, in two parts, to kickstart the technical review needed to prepare a plan of installation.

Please try to answer with as much detail as possible.

2.1 Questions for the Customer

Are you interested in making a permanent installation of the NIA within the ISP network?

If yes, is the installation aimed at deploying RCS Agents on a selected few targets or on entire networks?

How many ISPs are you willing to instrument with NIAs?

2.2 Questions for the ISP

How many DSLAMs do you have in your network?

What's the average aggregated bandwidth of the DSLAM?

What link type the DSLAM uses (copper, fiber)?

Please provide the protocol stack, up to the IP protocol, for traffic going from the DSLAM to the BRAS.

Is it possibile to mirror the traffic going from the DSLAM to the BRAS? Are there SPAN ports available or copper/optical TAPs in place?

Have you any statistic about the average amount (percentage) of DNS and HTTP traffic found in DSLAMs?

How are Subscribers identified within your network (eg. Static IP, Radius)?