



**RCS Network Injector**

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.

All contents of this document are: Copyright © 2014 HT s.r.l. All rights reserved.

Document Approval

| Revision | Author(s) | Release Date |
| --- | --- | --- |
| 1.2 | Daniele Milan | 3rd January 2012 |
| 1.3 | FAE Team | 13th February 2014 |

**Table Of Contents**

1. Overview 5

1.1 Infection Scenarios 5

1.2 Network Injector Appliance Capabilities 5

2. ISP deployment and positioning 6

3.1 Monitoring 7

3.2 Injection 7

3.3 Agent Deployment 8

3. Essential concepts 9

2.1 Target identification 9

2.2 Resource identification 9

2.3 Injection 10

4. Questionnaire 11

4.1 Questions for the Customer 11

4.2 Questions for the ISP 11

# 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 an innovative patent technology that allows live streaming injection and executable melting without being inline.

With the Network Injector Appliance you can turn the Internet connection of your target into a powerful infection vector. The Network Injector Appliance allows you to inject an Agent while your target browses the Internet. Do it with a wide portfolio of attacks, ranging from simple content replacement to an advanced multi-stage, zero-day exploit based attacks. Install the Agent in your target device without get in touch with him and without him ever knowing.

The Network Injector Appliance is suitable for many attacks, including:

* Injecting into downloaded applications, also during independent updates;
* Forcing O.S. components upgrade (e.g., Flash);
* Injecting a zero-day exploit into any webpage;
* Replacing any web content.

## Infection Scenarios

The NIA is a solution designed to infect any target connected to the Internet. It includes all the tools needed to identify and infect the desired target. After identification the target’s device could be infected using one of the following approaches:

* Waiting or persuading the target to download any executable file (.exe) from the Internet;
* Waiting when target’s device applications try to update;
* Waiting or persuading the target to view a video hosted by youtube;
* Waiting or persuading the target surfing the web with IE;
* Replacing any file accessed via Internet by the target with a different file provided by the operator.

## Network Injector Appliance Capabilities

The Appliance is engineered to be easily integrated in most common network implementations, safeguarding the network from service interruption and guaranteeing full network flows visibility.

The key features include:

* Installation at Internet Service Provider’s premises;
* Supports Fiber and Copper channels;
* Compatible with redundant network paths;
* Supported throughput up to 10GB;
* Doesn’t need to be installed inline, thanks to a patented technology it provides:
	+ noninvasive and surgical attacks, excluding all side effects of inline appliances;
	+ no impact on the ISP in case of failures;
* Easy management even when multiple NIA’s are deployed.

# ISP deployment and positioning

The Network Injector Appliance (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 Network Injector Appliance (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.

1. 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.

## 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.

## 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**.

1. No disruptive packets are sent from the NIA.
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 NIA to work properly: this eventuality must be addressed case by case.

## Agent Deployment

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

|  |  |
| --- | --- |
| **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 provided by HT Support Team |

# Essential concepts

The Network Injector Appliance (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.

## 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.

## 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.

1. 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.

## 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.

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

# 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.

## 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?

## 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)?