

Mars

ISP interception



Solution description

Table of Contents

Overview.....	3
Solution Components	3
Operational Flow	4
ISP Responsibilities	4
Physical Integration Suggestion	5

Overview

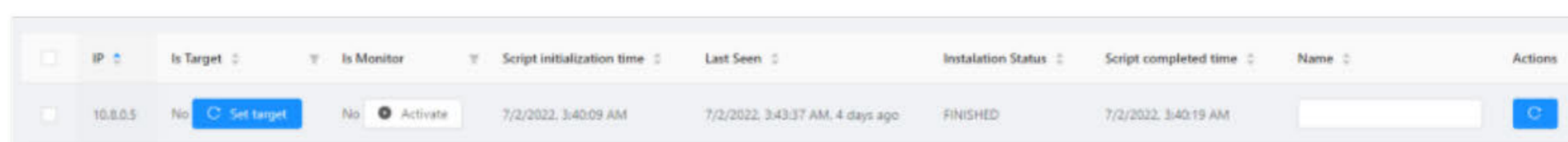
The Mars solution is a server integrated inside a mobile operator ISP (Internet Service Provider), to enable interception for zero-click infection for predefined targets over HTTP sessions. The Mars solution is implementing a MiTM (Man in the Middle) for intercepting targets at the ISP level. It is designed for law enforcement & intelligence agencies and requires full cooperation from the ISP for integration and operation.

The customer will create a list for the ISP to apply static IPs. The ISP will apply static IPs and forward traffic of these static IPs into the Mars server. The Mars server will be required to intercept the traffic of desired targets and manipulate it before forwarding to the desired destination. For non-target traffic the solution will forward the traffic to the next node in the ISP and will not interfering with the traffic.

Once an IP is set as target, the Mars server will decide how to act. In case the IP is marked as target, the Mars will intercept the traffic (MiTM) and wait for HTTP traffic. Once the Mars identifies the http request, it performs a 0-click infection ending with the target browsing in the requested website. In case of non-target IP traffic, all traffic, HTTP and other, are forwarded to the next ISP node, resulting by the device browsing to the requested website, without any interference.

Solution Components

1. **MARS server** – the MARS server is the physical component of the MARS system. The MARS server tasks are to check whether specific IPs traffic should be infected or forwarded seamlessly to the requested website. Meaning, once a target IP performs an HTTP request, before forwarding the traffic to the requested website, the MARS will infect the traffic and send the user to the requested website. If the request comes from a non-target IP, it will be transparently forwarded to the requested website.
2. **MARS admin** – the MARS admin is a web interface allowing the system operator to monitor and control the MARS server. The MARS admin includes the following main abilities:
 - a. **MSISDN Management** –
 - i. Review all the IPs that are forwarded into the MARS server.
 - ii. Manually add and exclude IPs that are expected to be forwarded.
 - iii. Choose relevant IPs to set as targets or deactivate existing targets that are no longer required.
 - iv. Choose relevant IPs to set or deactivate for monitoring (tracking domains the targets browse to)
 - v. Review information about the IPs such as: last seen time, actions status etc.



IP	Is Target	Is Monitor	Script initialization time	Last Seen	Installation Status	Script completed time	Name	Actions
10.8.0.5	No Set target	No <input checked="" type="radio"/> Activate	7/2/2022, 3:40:09 AM	7/2/2022, 3:43:37 AM, 4 days ago	FINISHED	7/2/2022, 3:40:19 AM		C

Figure 1 IP Management

- b. **Monitoring** –

- i. Review general traffic that is forwarded to the MARS server.
 - ii. Review specific IPs traffic to better understand the targets browsing preferences
- c. **Script Handling –**
- i. Select from predefined scripts
 - ii. Customize scripts

Operational Flow

The system operator accesses the MARS admin. The MARS admin presents an IP management section, which includes a list of all the IPs that are forwarded to the MARS server. From those IPs the operator can choose which to set as target. Additionally, he can manually add as targets IPs that haven't been forwarded to the MARS server yet, but are expected to. The admin updates the rules in the MARS server, this way the MARS server knows what to do when it receives specific IP traffic. A typical operational flow scenario description is:



Figure 2 Operational Flow

ISP Responsibilities

For the solution to work, there are some responsibilities that are required from the ISP.

1. **Physical integration** – a main component in the solution is integration of the MARS server, which should reside in the local network of the ISP. Specific elaboration about the physical integration will be presented in the section “Physical Integration”
2. **Predefining static IPs** - the MARS solution supports traffic of up to 100 clients at once. Therefore, the ISP can predefine the known targets IPs to be statically defined and forwarded to the MARS server. It is important that the targets IPs remain static for the whole time of the operation as this is how the server will recognize the target. Once the infection process is completed, they could be released from the MARS.
3. **Traffic forwarding (ISP Gateway)** – traffic from the relevant IPs should be forwarded to the MARS server. In the ISP gateway there will be a code (script, bash, IP tables configuration) that will redirect the traffic of a given IP addresses list to the MARS server. The data frame should not be changed, and addresses should stay the same.
4. **Internet connection** – the MARS solution requires that the MARS server will be provided with a secure internet connection in order to enable the infection process.

Physical Integration Suggestion

The physical integration details vary based on the internal architecture of the specific ISP. A suggestion for physical integration could be similar to the following. Intellexa welcomes a mutual discussion with local ISP to reach a compatible and acceptable solution.

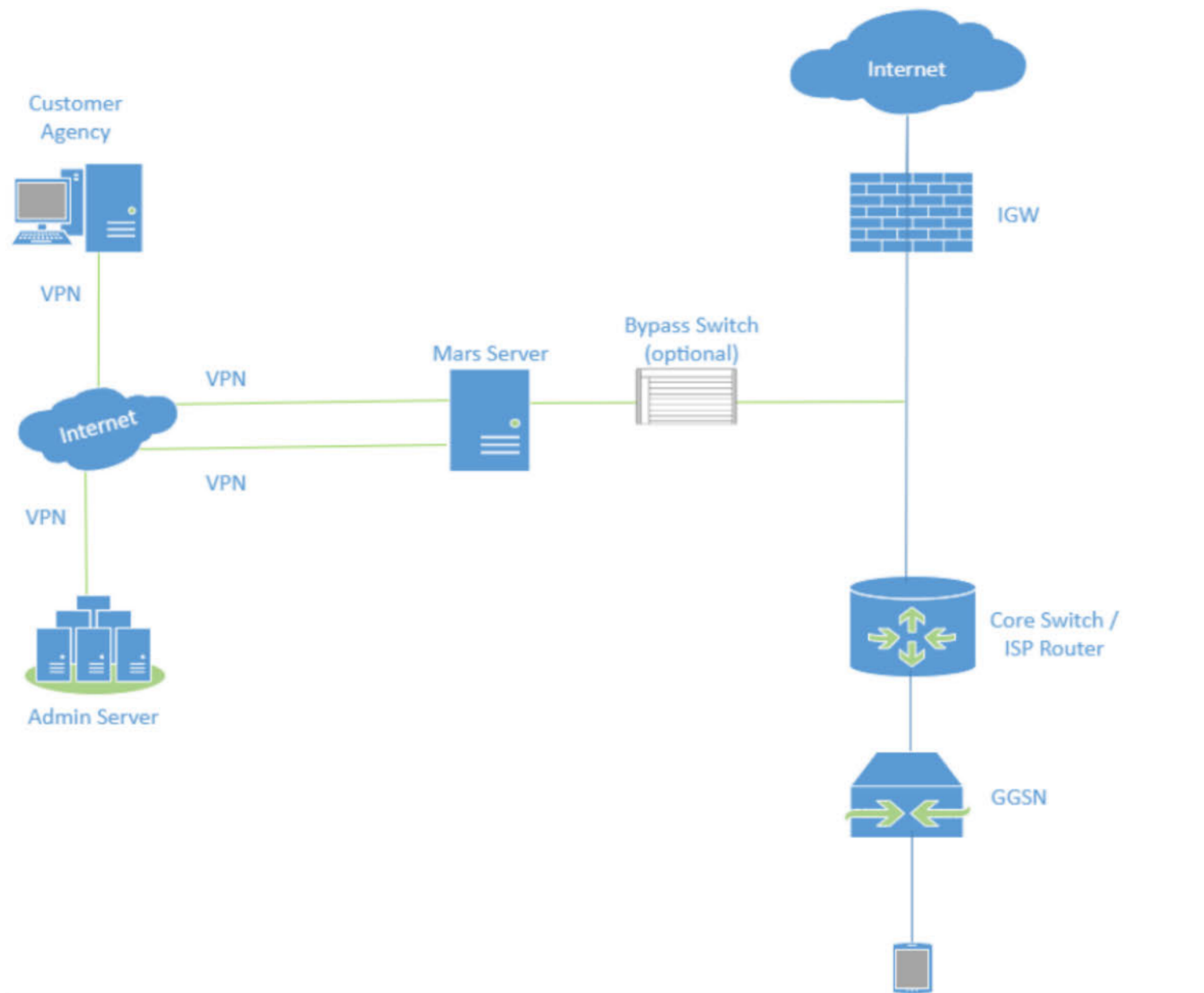


Figure 3 Suggested Architecture