INTRODUCTION

During a period it was requested to block anonymizer applications used by users to bypass traffic and surf the net or gain access to unauthorized sites.

It was noticed users were still able to access unauthorized sites using psiphon VPN application for Mobile (Andriod, iOS) and PC.

DESCRIPTION

Psiphon is an open-source Internet censorship circumvention tool that uses a combination of secure communication and obfuscation technologies (VPN, SSH, and HTTP Proxy).

It uses different evasion techniques to avoid detection including application signature regular update, cloud hosted (dynamic source IP), protocol and services used are not well understood.

How it Works

The application is available for Mobiles (Android, iOS) and PCs and when installed, the Psiphon client will automatically discover new Psiphon servers hosted in different location around the world and when the last server used is currently unavailable, another one can be used instead.

After a successful connection is established in VPN mode (Psiphon uses the L2TP/IPsec VPN protocol.), your entire device traffic will pass through the Psiphon network. When VPN mode is not enabled only applications that use the local HTTP and SOCKS proxies will be proxied. Psiphon uses SSH with the addition of an obfuscation layer on top of the SSH handshake to defend against protocol fingerprinting.

Protocols and Services uses by Psiphon

- http-proxy
- ike
- ipsec
- l2tp
- ssh
- ssh-tunnel (ssh+)
- unknown-tcp

Blocking Psiphon (Test conducted by Ricardo Andres Munoz of CheckMates)

a) Enable HTTP Inspection in all categories
b) Block categories: Anonymizers, Unknown traffic
c) Block SSH in Firewall Layer (I had to allow ssh to my specific destinations)

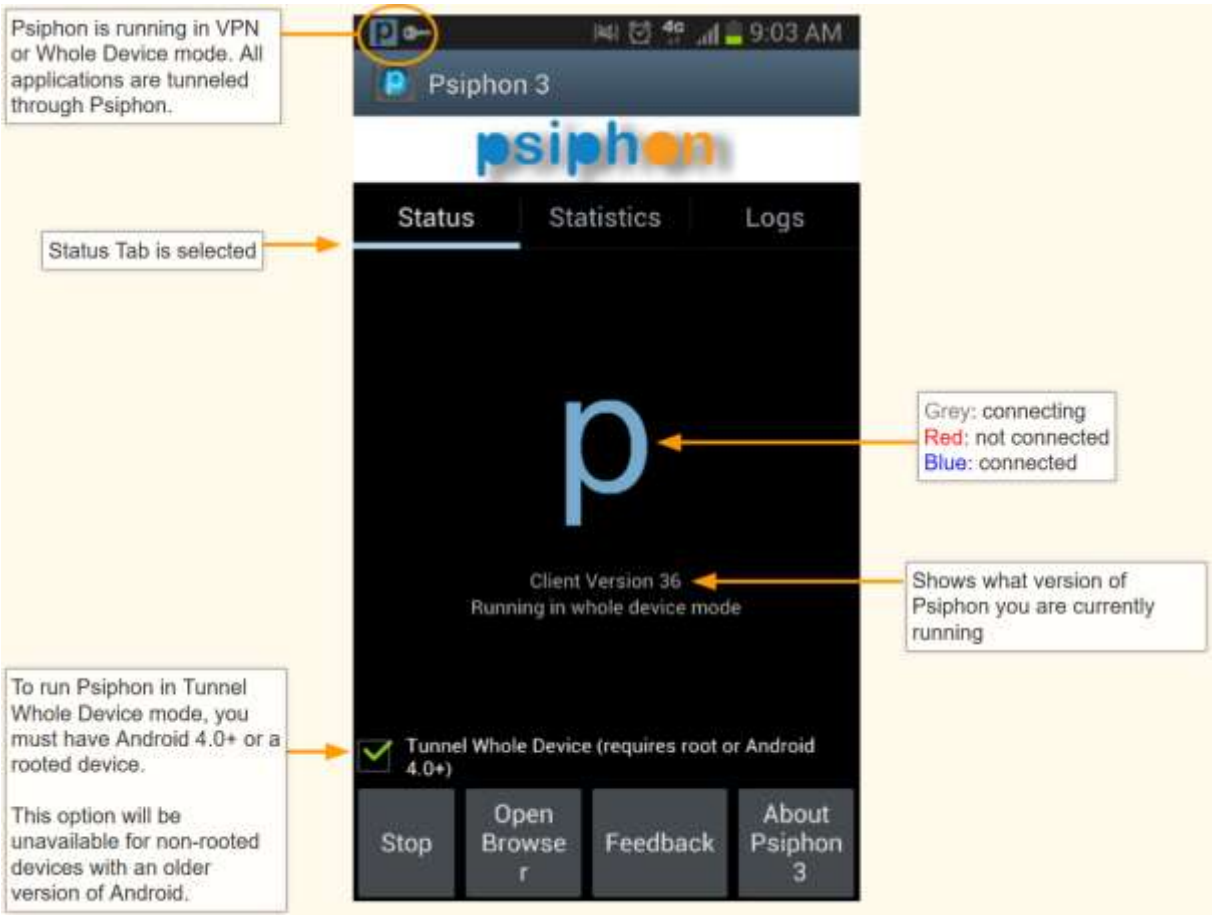
The problem is: A few applications are not identified by Check Point, so they are blocked because of the "unknown traffic" category drop

Issues regarding Blocking Psiphon

- Blocking unknown traffic is very crucial as it may result in blocking some legitimate traffic used by authorized applications.
- Enabling HTTPS Inspection requires certificate validation and it must be imported to all clients within the network and only clients with the certificate will be blocked.

How to use Psiphon (Android)

After installing, launching the App



When connected your source will be located from the server you connect to and all your traffic will be source from the IP provided.

For windows Psiphon automatically starts connecting when you run it. While it is connecting, a spinning icon is displayed. You may select one of the following tunnel modes: VPN (L2TP over IPsec), SSH, or SSH+ (SSH plus obfuscation, a randomized layer on top of SSH to avoid protocol fingerprinting).

Psiphon connection establishment process