DPIBON

“Dual use is megl che uan”

Chi sono

Massimo Bozza - Senior Security Engineer | Ethical Hacker

Ingegnere Elettronico, Security Engineer. Da sempre spinto dalla curiosità cerco di esplorare la tecnologia che mi circonda e convinto che l'informazione dei essere di tutti.

Mi occupo di Ethical Hacking e security testing, nel mio tempo libero i mie principali campi di ricerca sono sistemi embedded, sicurezza applicativa e mobile.

Twitter: @maxbozza
Linkedin: linkedin.com/in/maxbozza

Key findings

BAD TRAFFIC Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?

By Bill Marczak, Jakub Dalek, Sarah McKune, Adam Senft, John Scott-Railton, and Ron Deibert

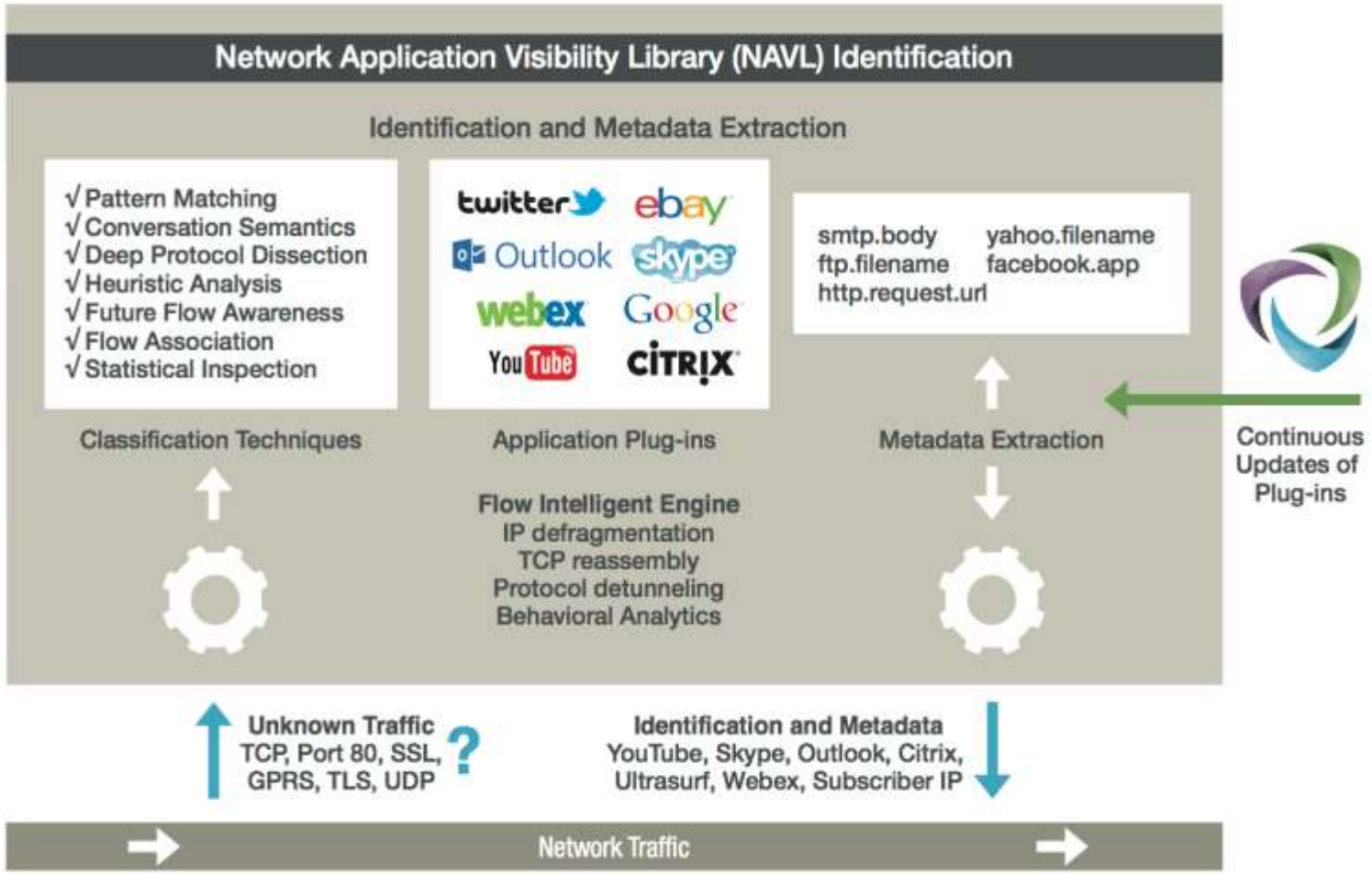
- Through Internet scanning, we found deep packet inspection (DPI) middleboxes on Türk Telekom's network. The middleboxes were being used to redirect hundreds of users in Turkey and Syria to nation-state spyware when those users attempted to download certain legitimate Windows applications.
- We found similar middleboxes at a Telecom Egypt demarcation point. On a number of occasions, the middleboxes were apparently being used to hijack Egyptian Internet users' unencrypted web connections en masse, and redirect the users to revenue-generating content such as affiliate ads and browser cryptocurrency mining scripts.After an extensive investigation, we matched characteristics of the network injection in Turkey and Egypt to Sandvine PacketLogic devices.
- We developed a fingerprint for the injection we found in Turkey, Syria, and Egypt and matched our fingerprint to a second-hand PacketLogic device that we procured and measured in a lab setting.
- The apparent use of Sandvine devices to surreptitiously inject malicious and dubious redirects for users in Turkey, Syria, and Egypt raises significant human rights concerns.

https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/

Come funziona

Differenti tipi di packet inspection

- PI (Packet Inspection) controllo solo intestazione dei pacchetti
- DPI (Deep Packet Inspetcion) controllo intestazione e contenuto del pacchetto
- ADPI (Advanced Deep Packet Inspection) in grado di applicare la Cross Packet Inspection (XPI) in modo che vengano rilevate firme che partono su un determinato pacchetto e continuano su pacchetti successiv; al fine di procedere con analisi così sofisticate è necessaria un'elevata capacità di caching e di calcolo per poter garantire alti throughput

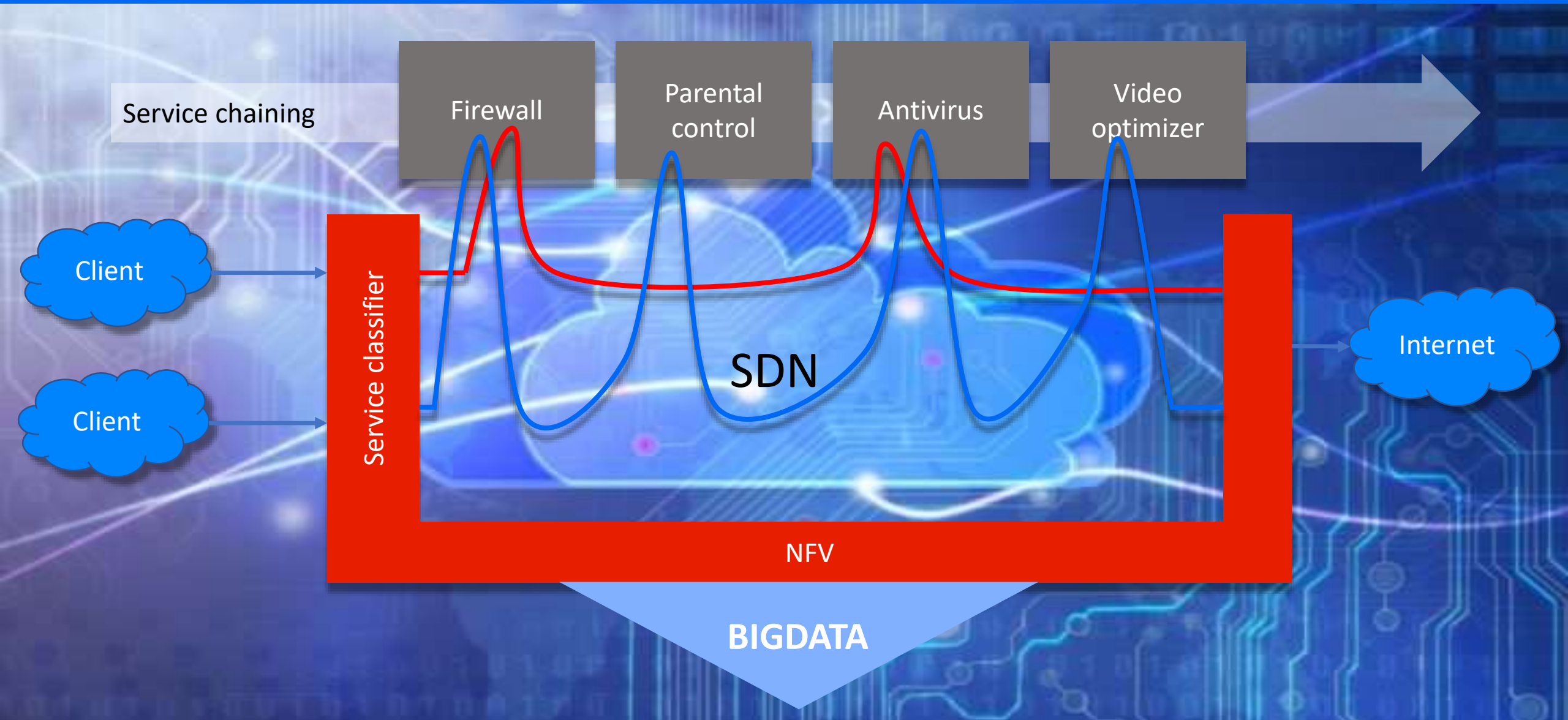


Esempio degli apparati procera networks analizzati da citizen lab

Come funziona

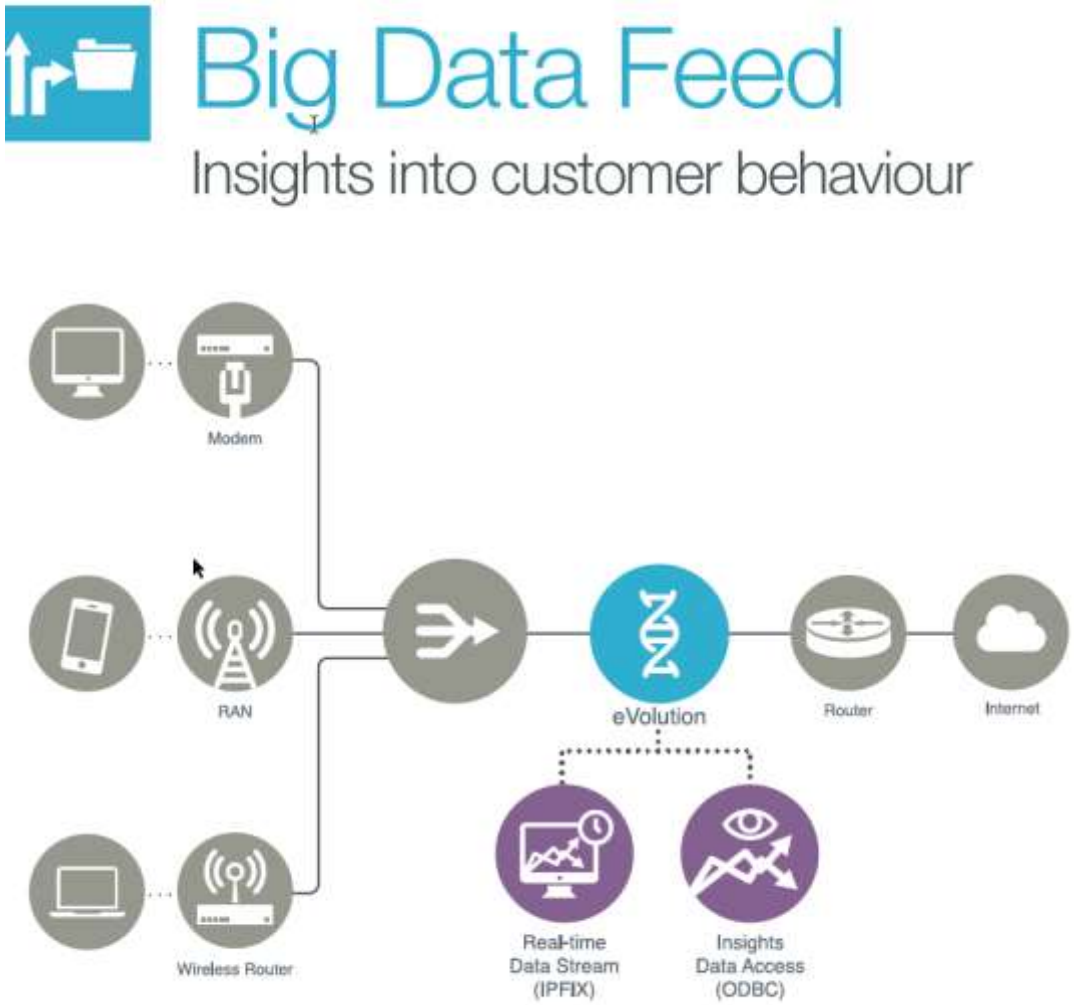
- **Quali funzioni svolge il DPI?**
- **Chi sono i player del mercato DPI?**

Evoluzione


Service chaining
Firewall
Parental control
Antivirus
Video optimizer
Client
Client
Service classifier
SDN
Internet
NFV
BIGDATA

Usi e dualuse

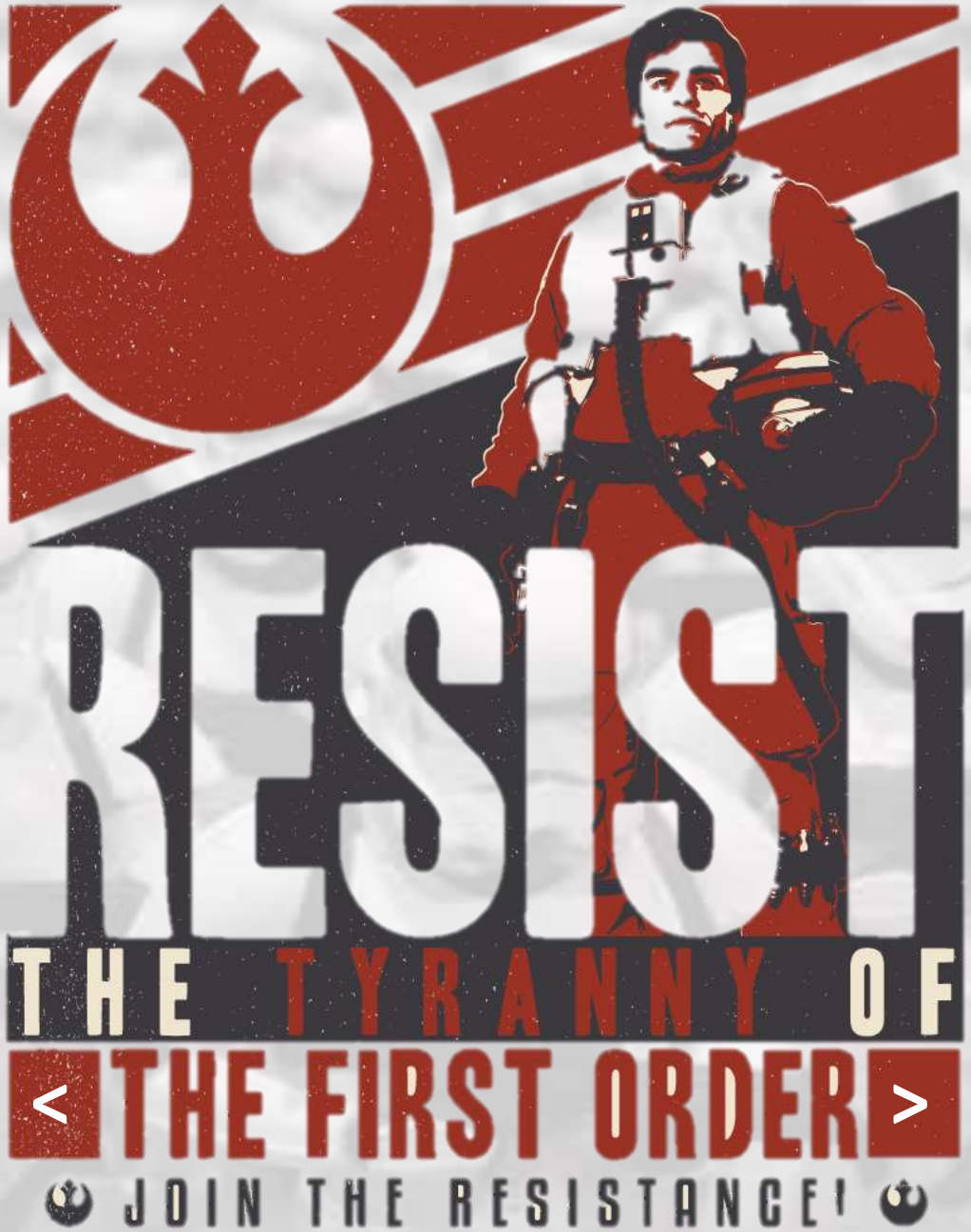
Usi e dualuse



BACKGROUND

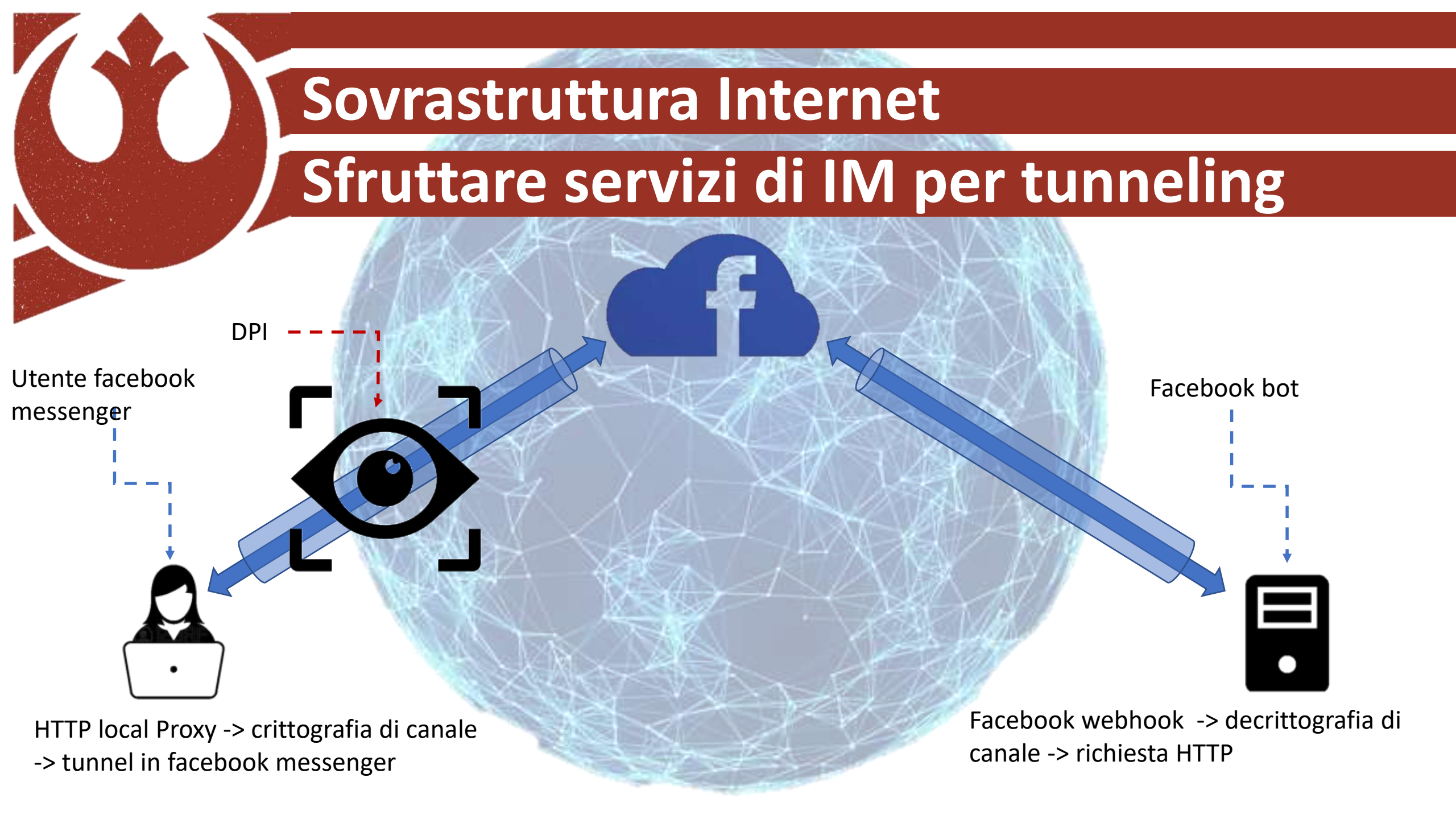
Network operators worldwide are looking to gain insights into the experience that they are delivering to their subscribers. Many operators are turning to Big Data solutions to gather more intelligence on what is happening on their networks. They are looking to increase revenue, reduce OPEX, increase customer loyalty through targeted offerings, enhance the overall customer experience, simplify business operations, reduce churn, reduce time to market for new services, and accelerate the creation of personalized services.

Usi e dualuse


RESIST
THE TYRANNY OF
THE FIRST ORDER
JOIN THE RESISTANCE!

Sovrastruttura Internet

Sfruttare servizi di IM per tunneling



Sovrastruttura Internet

Sfruttare servizi di IM per tunneling