Allo maman ?
J'ai 1500 jours d'uptime !

RESSI 2019 – Erquy

Public / TLP:WHITE

Sébastien Mériot – @smeriot – Responsable CSIRT-OVH

15 Mai 2019

28 Centres de données
18 Tbps de capacité réseau
AS16276 & AS35540
3M IPv4
1er fournisseur de Cloud en Europe

OVH

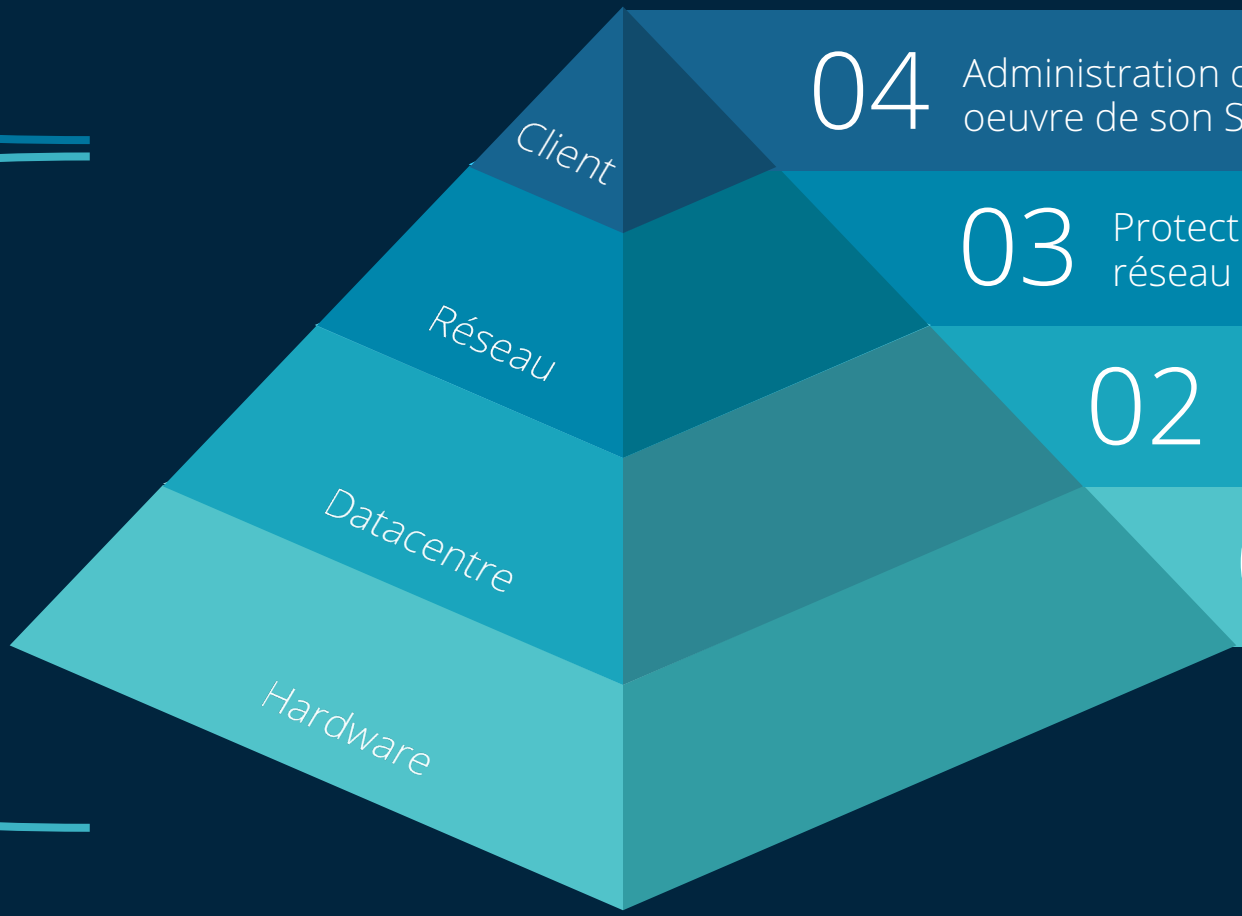
“OVH n’a pas accès aux données & services de ses clients.”

4 strates de sécurité

Vue macroscopique

Client

OVH



04 Administration de son service & mise en oeuvre de son SMSI.

03 Protection de notre coeur de réseau (DDoS, BGP Hijacking, ...)

02 Mise en oeuvre des SMSI OVH

01 Qualification du matériel utilisé.

Exemples des responsabilités

Attaques DDoS

Mise en place de mécanisme de protection contre les attaques par déni de service volumétrique.

Hébergeur
80%

Client
20%

Vulnérabilité Wordpress

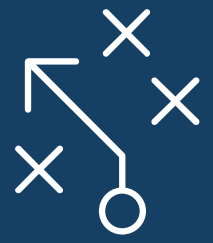
Mise à jour du CMS pour se prémunir d'une compromission éventuelle permettant d'armer le serveur.

Hébergeur
20%

Client
80%

> La sécurité se mesure en prenant le maillon le plus fragile de la chaîne.

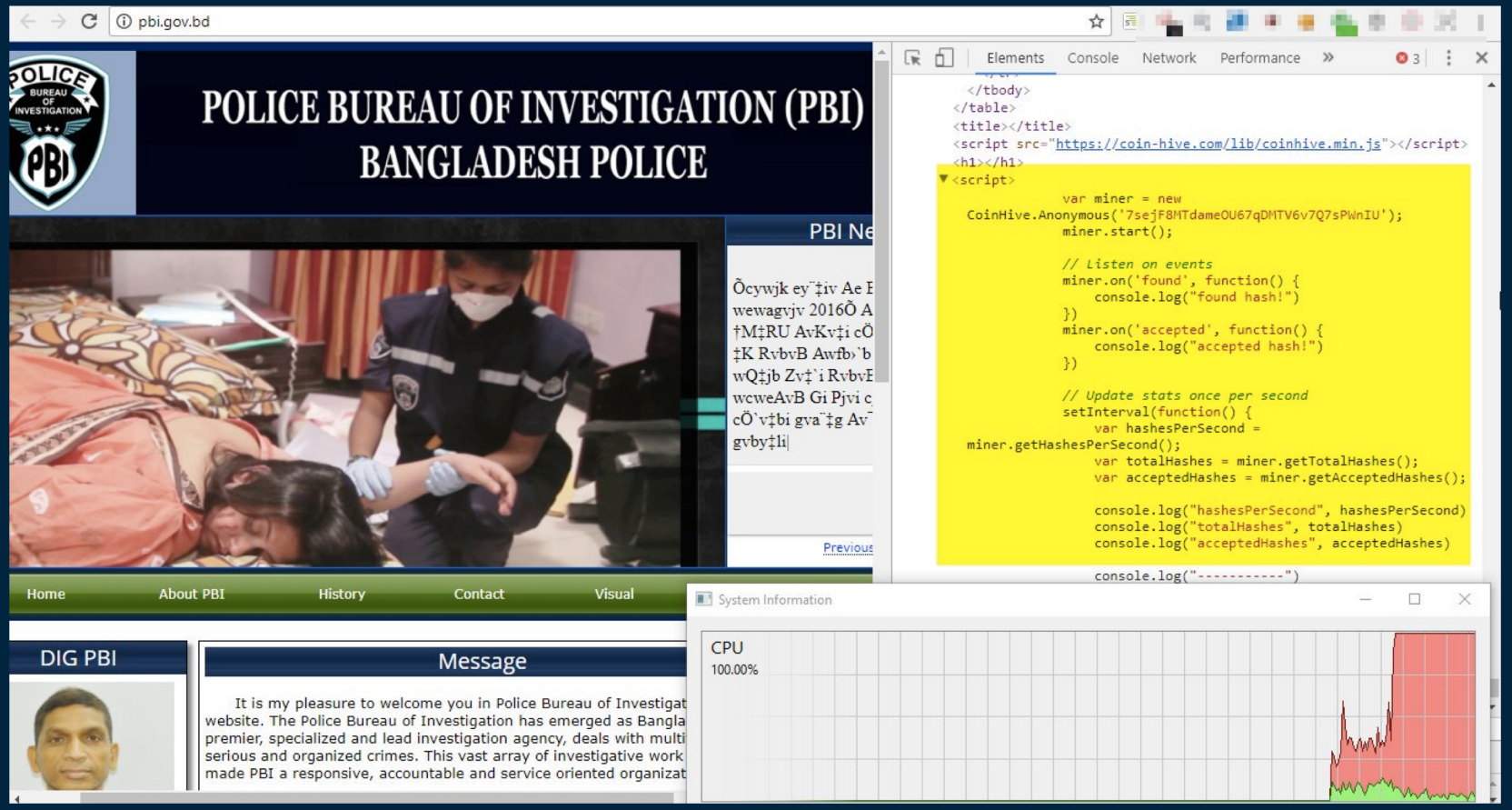
OVH



Abus de Service

Communément appelé « Abuse », l'abus de service constitue une infraction aux conditions de service et/ou à la législation en vigueur et nécessite une action corrective de la part du ou des clients incriminés.

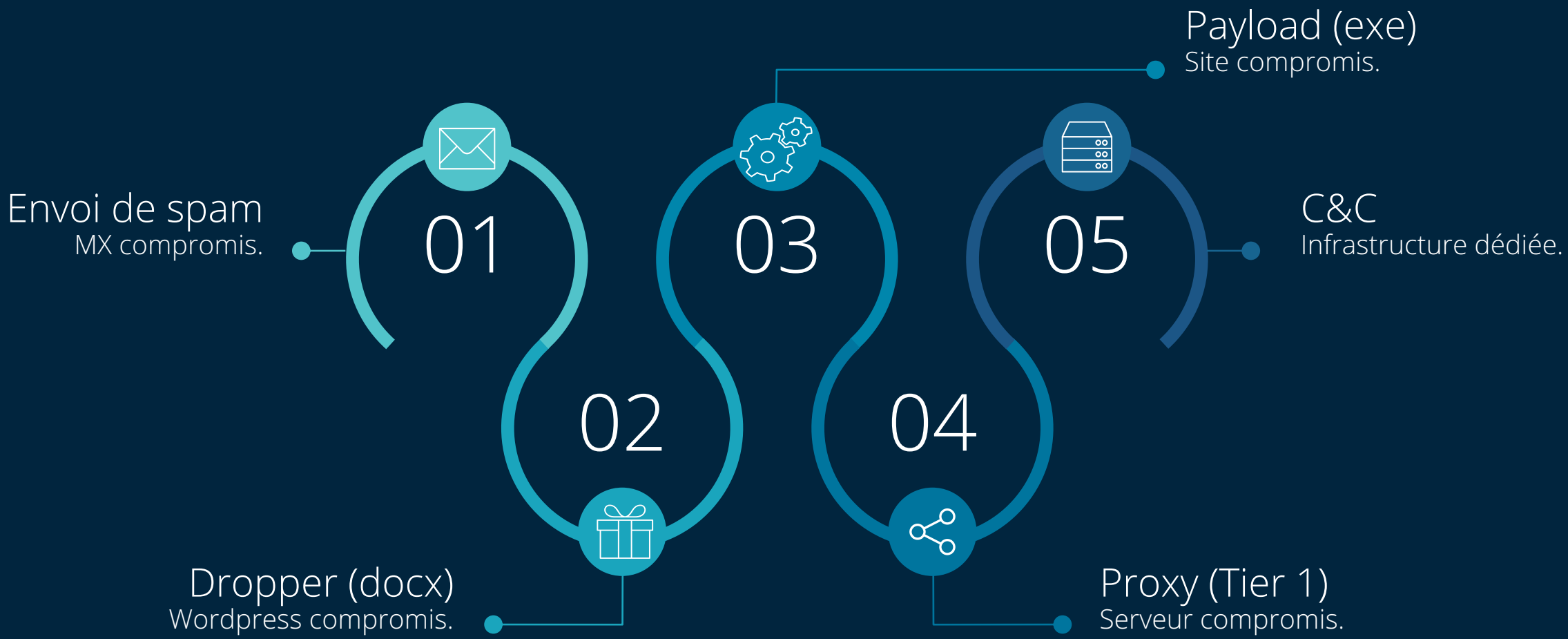
abuse@ovh.net
https://www.ovh.com/fr/abuse



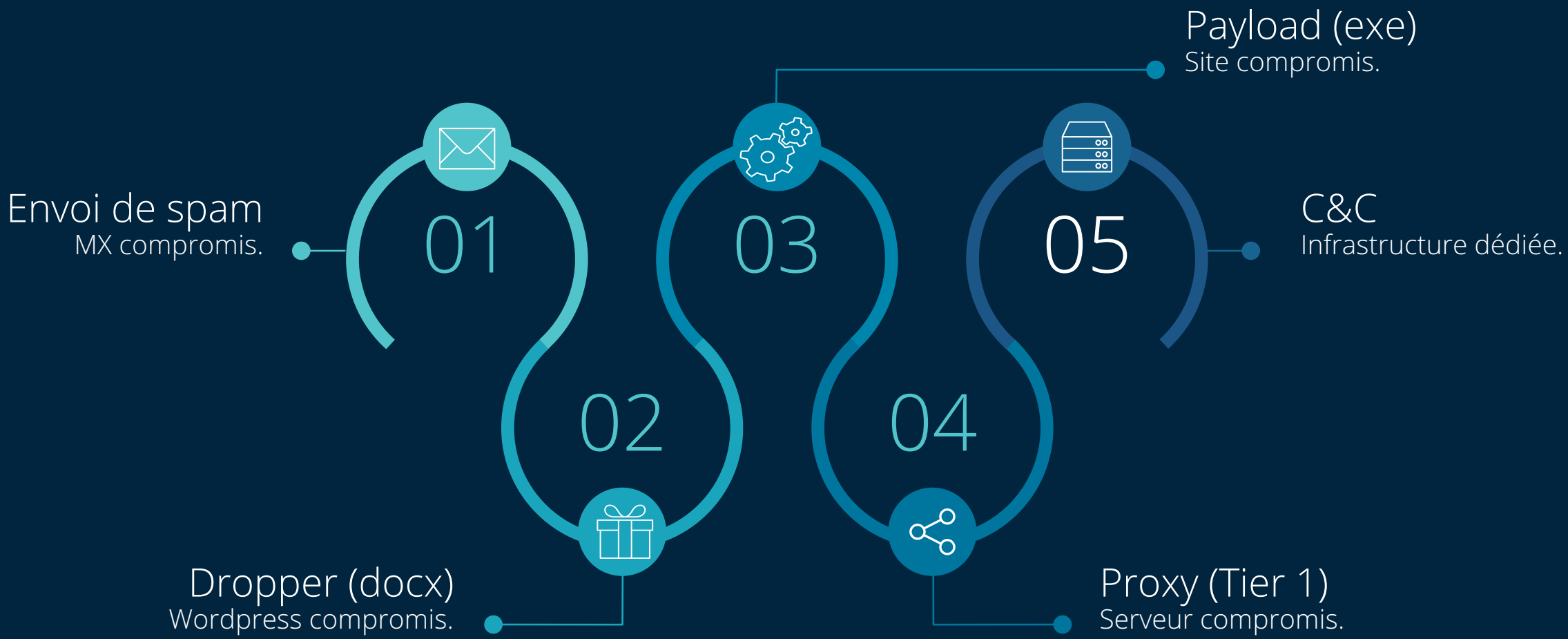
Police du Banglasdesh

Le site officiel a hébergé pendant de nombreuses semaines un crypto-mineur sur son site web suite à une compromission.

Exemple : Emotet

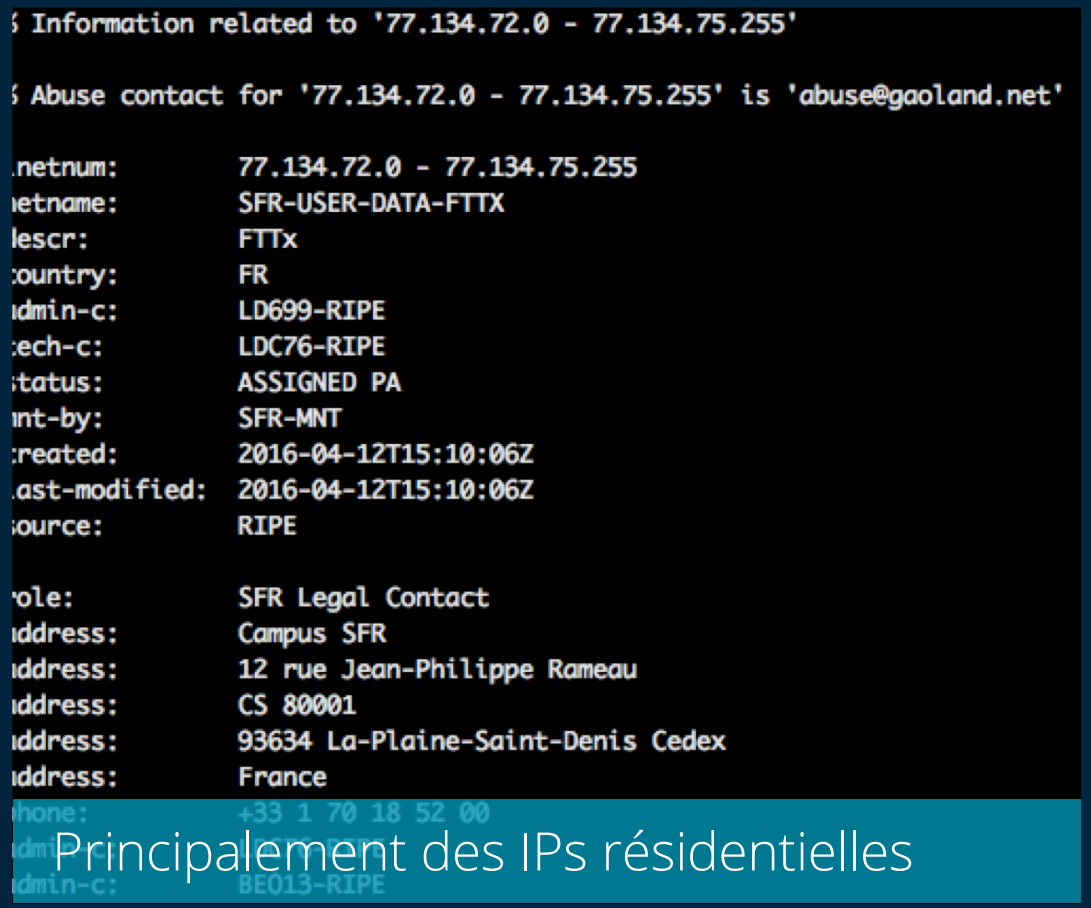


Exemple : Emotet



Un cercle vicieux

Service en ligne de location de proxy

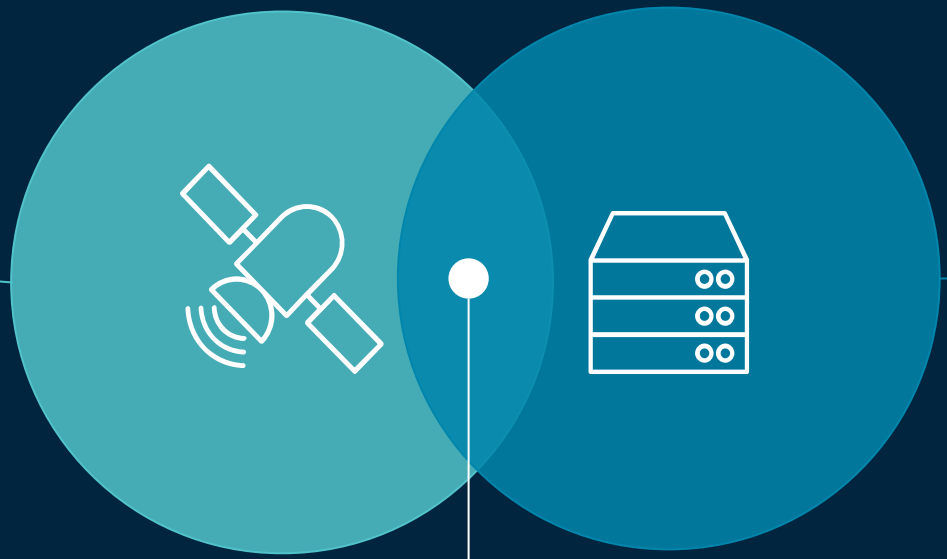


Principalement des IPs résidentielles

Réseau ou Equipement terminal ?

Réseau

Mécanismes complexes généralement mis en œuvre par les opérateurs et/ou les transitaires permettant de garantir une QoS acceptable.
L'équipement terminal n'est pas considéré comme de confiance par défaut.



Equipement terminal

L'administrateur a le devoir d'appliquer une hygiène stricte en matière de sécurité avec un inventaire et un suivi.
Le réseau ne doit pas être considéré comme un lieu de confiance. Le chiffrement doit être réalisé de point à point au plus proche des interlocuteurs.

Conditions nécessaires pour une sécurité optimale.

La clef :
Eduquer & Sensibiliser

Il n'est pas possible de sécuriser durablement un périphérique sans l'implication de l'utilisateur (et du constructeur).

01 Eveiller

02 Impliquer

03 Outiller

04 Contrôler

Merci pour votre attention

Sébastien Mériot
@smeriot
Responsable CSIRT-OVH

RESSI – Erquy | 15/05/2019

csirt@ovh.com

0x43F7 C95E 4EB5 7EF1

2 Rue Kellermann – 59100 Roubaix

09.72.62.30.01

OVH