OSSIR

Réunion du 10 Février 2015

Qui suis-je ?

- **Régis Senet** – Consultant sécurité chez XMCO depuis juin 2014
  Activités : Tests d'intrusion, audits, forensics, R&D

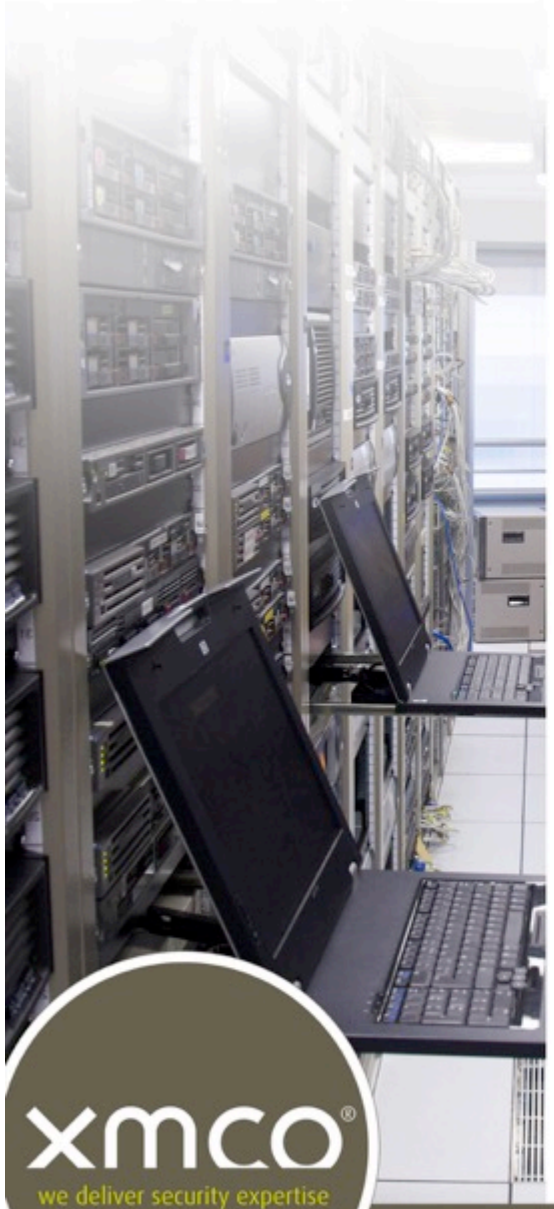
ActuSecu
Article complet disponible

xmco
we deliver security expertise

A TOR et à travers

Etude du réseau d'anonymisation en 2015, utilisation et faiblesses

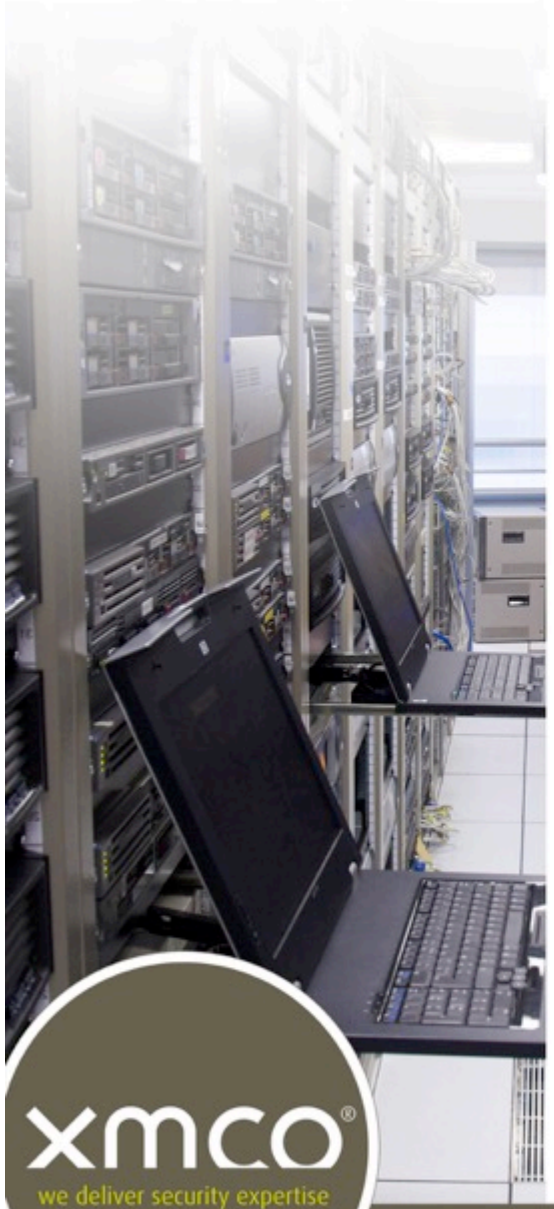
Sommaire



1. **Présentation du réseau TOR**
2. **dissecTor ou l'étude des nœuds de sortie**
3. **generaTor ou la détection des nœuds de sortie en écoute**
4. **Conclusion**
5. **Questions**

xmco®
we deliver security expertise

Sommaire



1. **Présentation du réseau TOR**

2. dissecTor ou l'étude des nœuds de sortie

3. generaTor ou la détection des nœuds de sortie en écoute

4. Conclusion

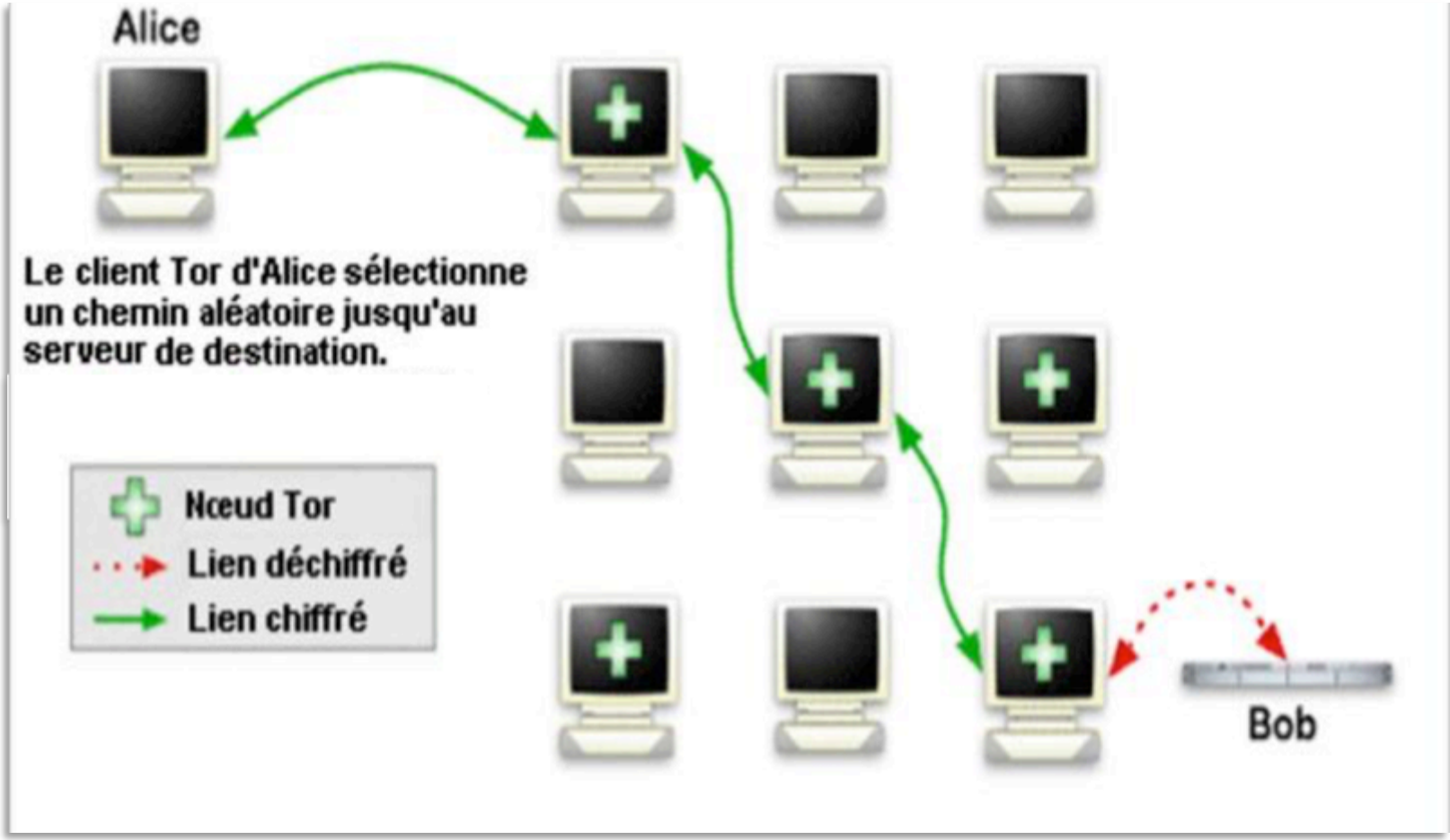
5. Questions

xmco®
we deliver security expertise

Présentation du réseau TOR

- **Réseau d'anonymat décentralisé et chiffré (en « oignon ») fondé en 2001**
- **Utilisation multipliée par deux depuis les révélations d'Edward Snowden**
- **A l'origine de nombreux projets largement utilisés**

Fonctionnement du réseau TOR



Fonctionnement du réseau TOR

Chiffrement des données

Qui utilise TOR ?

- Journalistes / Blogueurs
- Opposants politiques
- Professionnels de la SSI
- (cyber) terroristes
- Pirates / hacktivistes
- Pédophiles

1/3

2/3

Les attaques contre TOR

- **Attaques transitant via TOR**

  ShellShock, Drupal, spam, bruteforce sur interface d'administration, SQLi, etc.

- **Analyse passive du trafic**

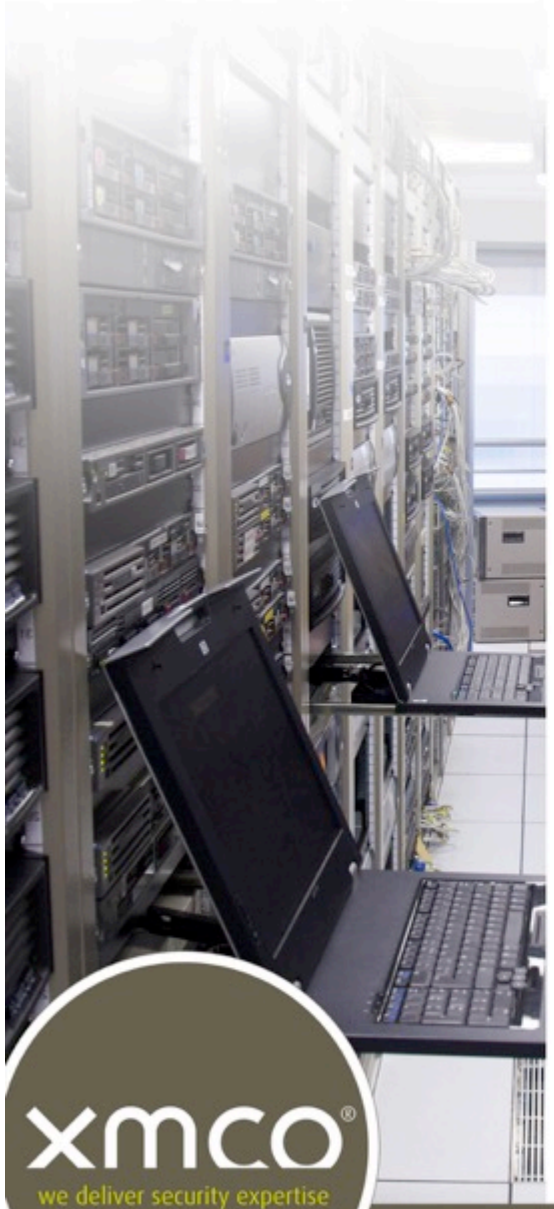
  Hack of The Year 2007, dissecTor, etc.

- **Injection de trafic dans les données relayées**

  ExitMap, article de Josh Pitts (en date du 23 octobre 2014), etc.

- **Attaques diverses et variées**
  - Opération Onymous visant à fermer plusieurs services cachés
  - Annulation d'une présentation de la BlackHat sur la désanonymisation de TOR
  - Rajout d'une clé USB dans l'un des principaux serveurs hébergeant des nœuds TOR
  - Etc.

Sommaire



1. Présentation du réseau TOR

2. **dissecTor ou l'étude des nœuds de sortie**

3. generaTor ou la détection des nœuds de sortie en écoute

4. Conclusion

5. Questions

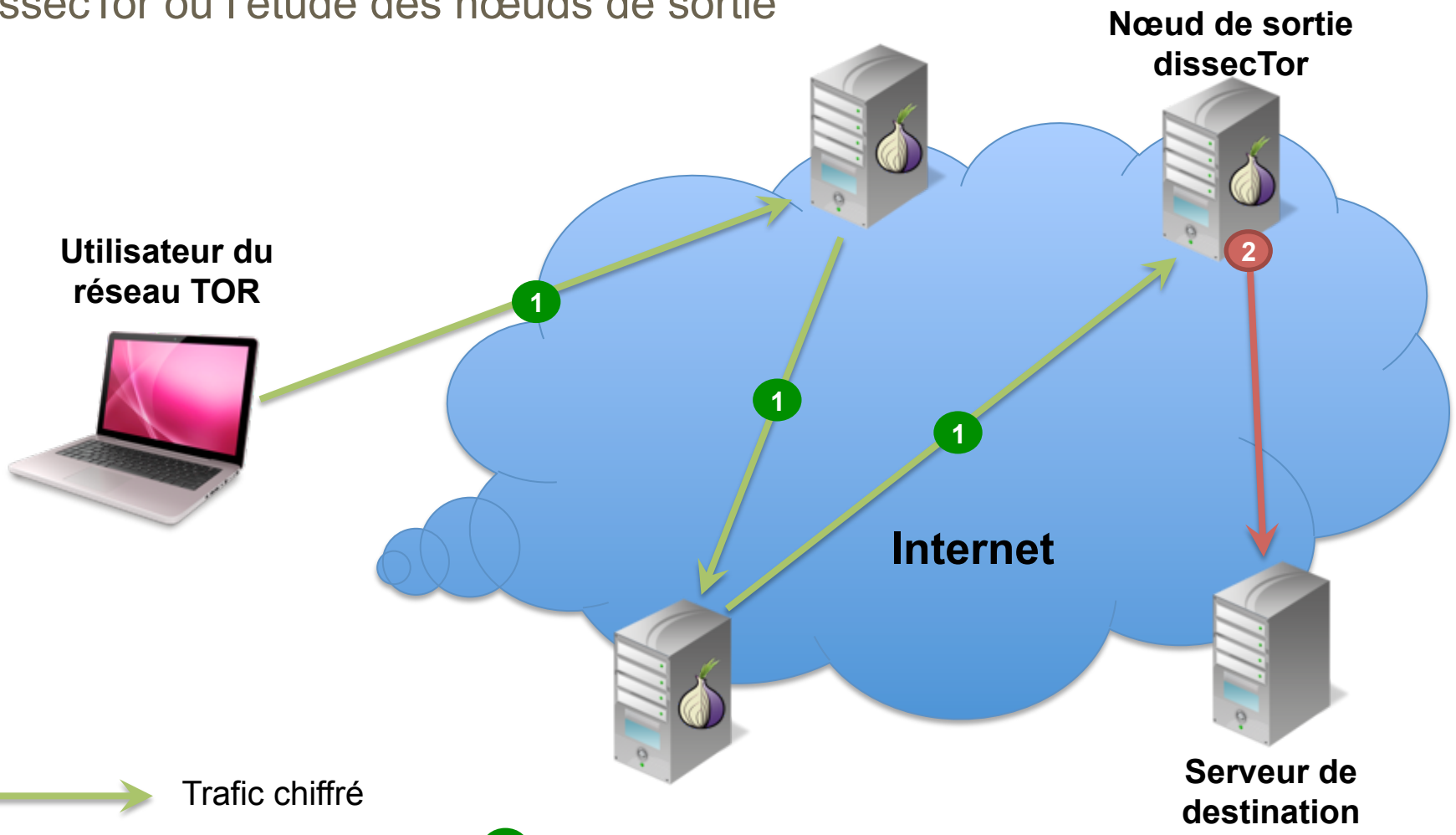
xmco®
we deliver security expertise

A TOR et à travers : Etude du réseau d'anonymisation en 2015, utilisation et faiblesses

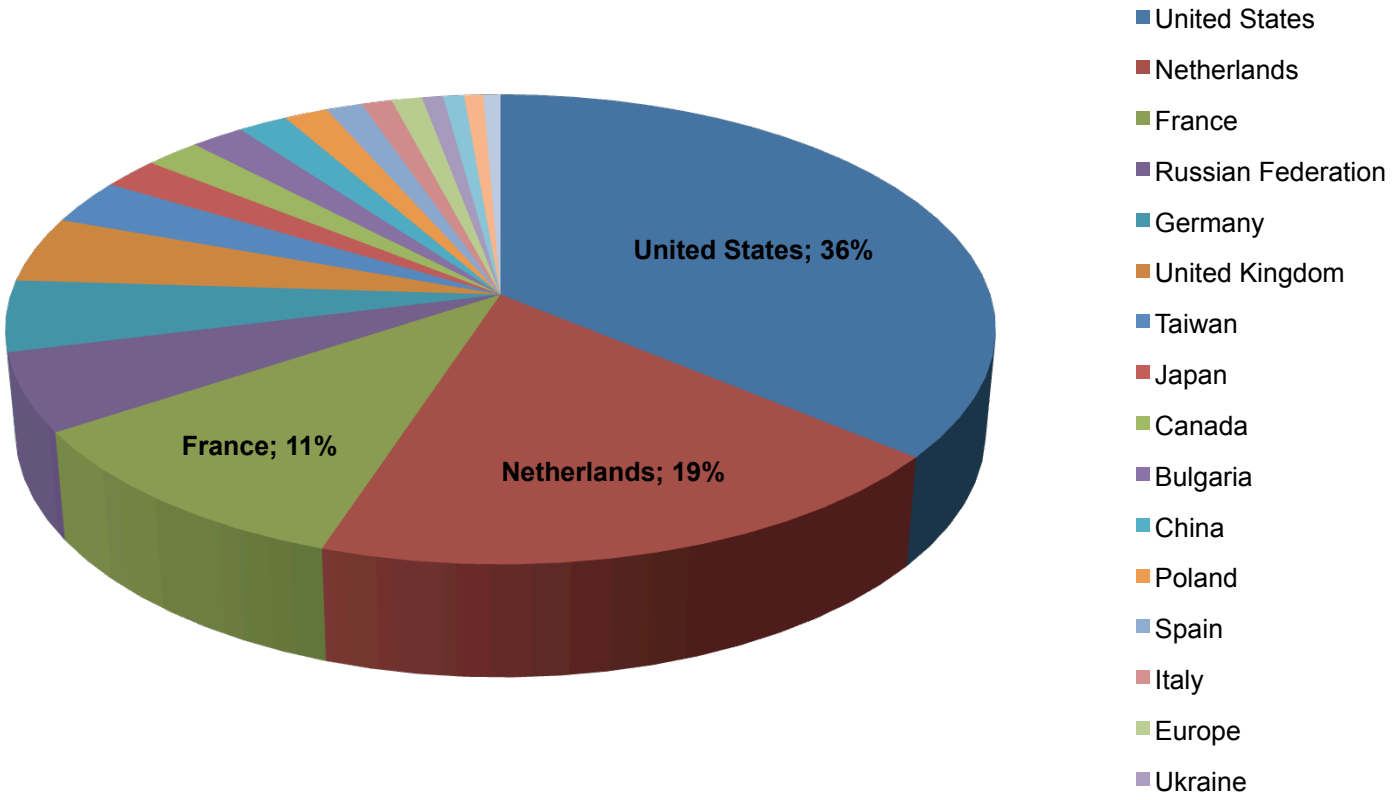
dissecTor ou l'étude des nœuds de sortie

- **Insertion d'un nœud de sortie dans le réseau TOR**
- **Analyse du trafic via des outils publics (dsniff, PCredz)**
- **Traitement des données**
  - Suppression des attaques de type bruteforce
- **Plus d'informations : ActuSecu #18**

dissecTor ou l'étude des nœuds de sortie



dissecTor ou l'étude des nœuds de sortie



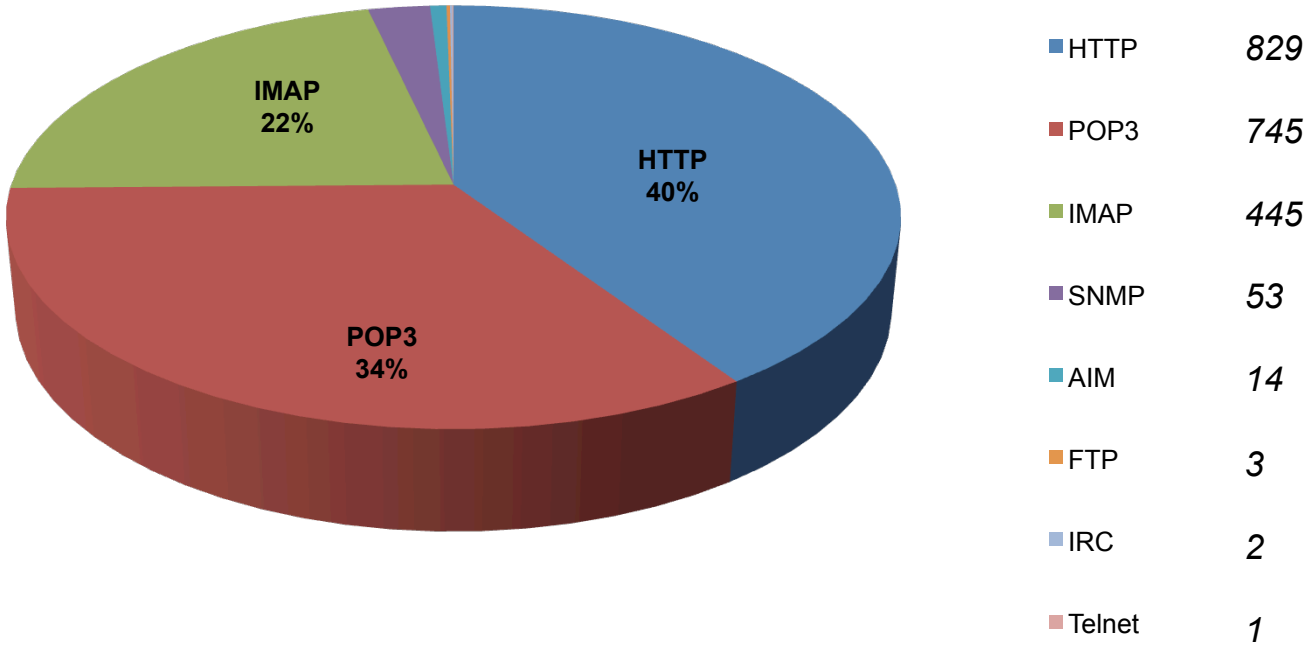
Répartition des adresses de destination

dissecTor : les résultats

- **Les statistiques**
  - Mots de passe divers captés : ~30 000
  - Mots de passe conservés : ~2 200

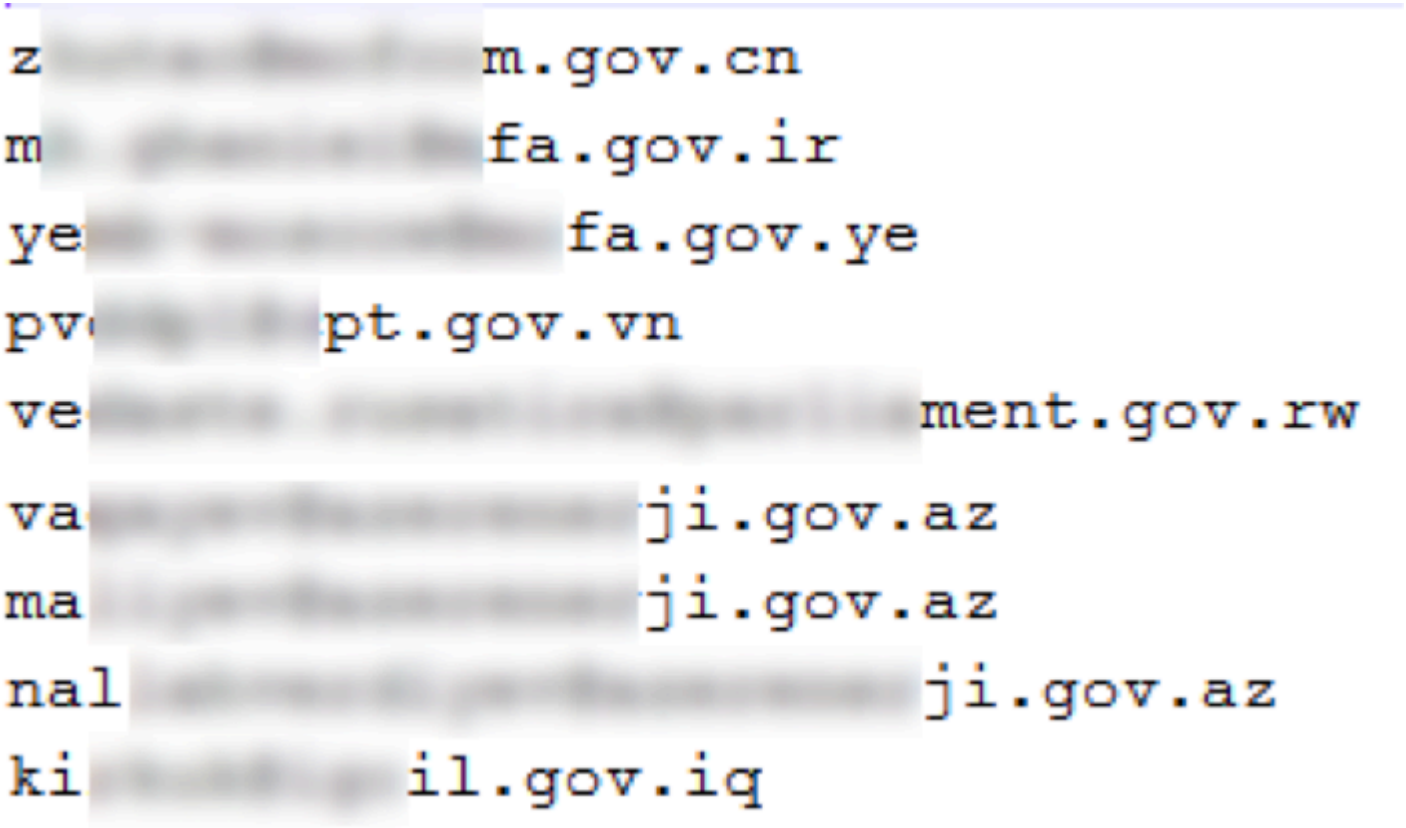
- **Pourquoi une telle différence ?**
  - Très nombreuses attaques de bruteforce (à destination de la Russie notamment)
  - Capture de certains hash par les outils utilisés

dissecTor : les résultats



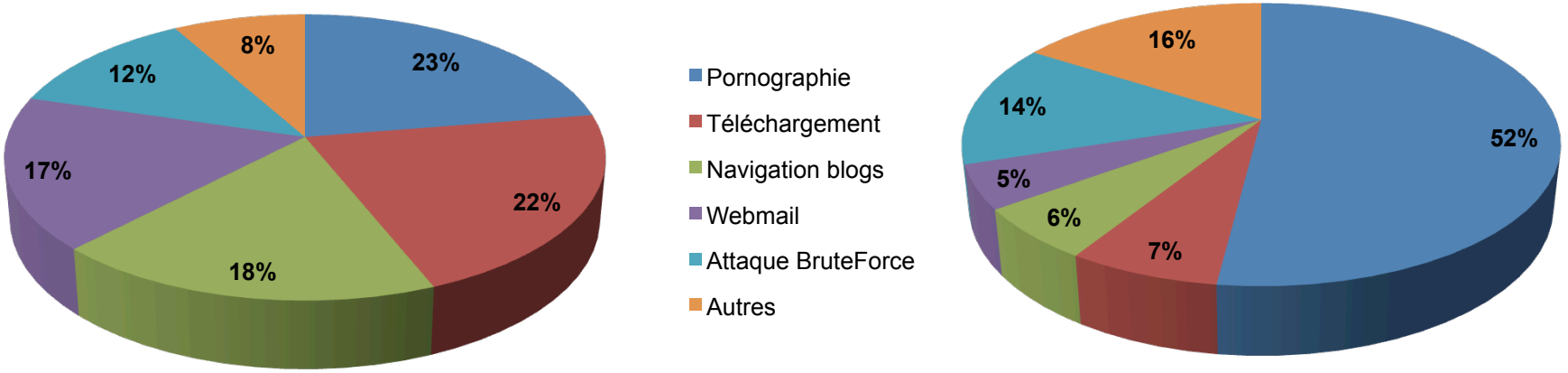
Répartition des mots de passe par protocole

dissecTor : les résultats



Mots de passe d'adresses email gouvernementales

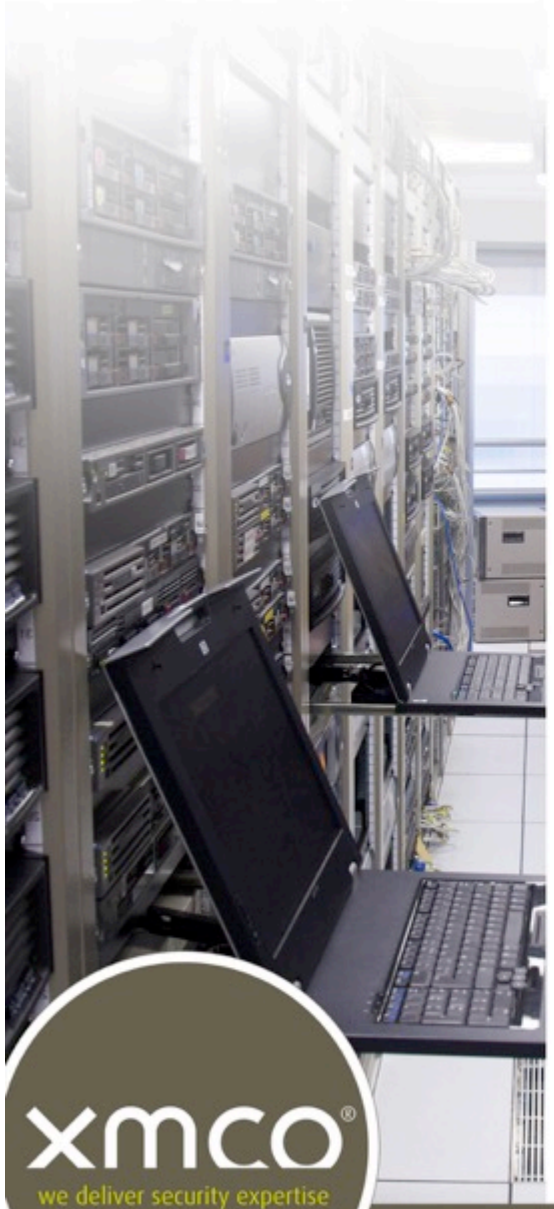
dissecTor : les résultats



2008

2014

Sommaire



1. Présentation du réseau TOR

2. dissecTor ou l'étude des nœuds de sortie

3. **generaTor ou comment détecter des nœuds de sortie en écoute**

4. Conclusion

5. Questions

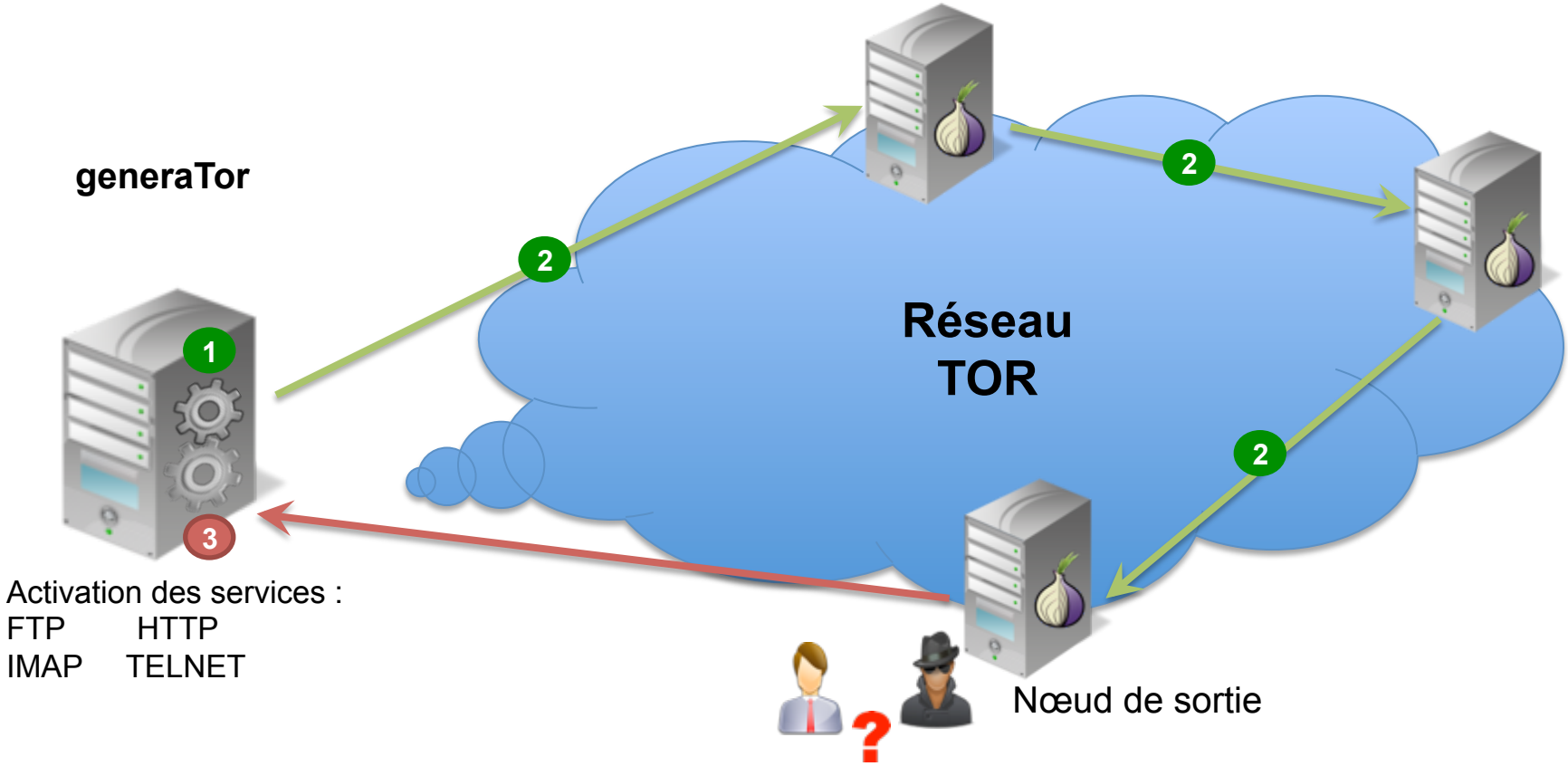
xmco®
we deliver security expertise

Présentation de generaTor

- **Framework développé en python**
- **Automatise des connexions non sécurisées via le réseau TOR**
  - FTP
  - HTTP
  - IMAP
  - TELNET
- **Analyse les connexions reçues sur notre serveur**
- **Détecte d'éventuels rejeux d'identifiants**
  - Se base sur un quadruplet unique :

    identifiant / mot de passe / protocole / nœud de sortie

generaTor ou comment détecter des nœuds de sortie en écoute



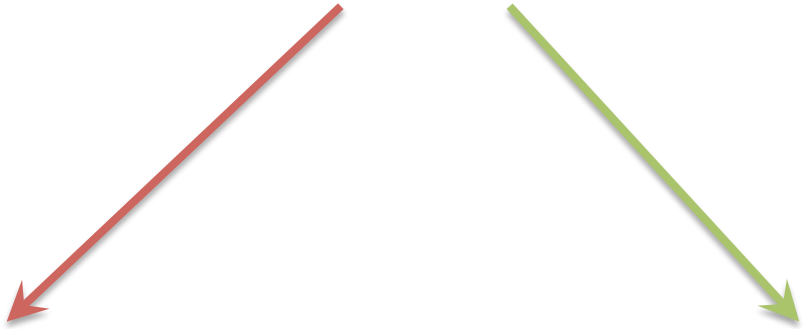
Trafic chiffré

Trafic non chiffré

1. Génération d'un couple identifiant / mot de passe unique en fonction du nœud de sortie et du protocole
2. Envoi des requêtes d'authentification vers notre serveur via le réseau TOR
3. Ecoute des connexions entrantes sur notre serveur pour identifier d'éventuels rejeux d'authentification

generaTor ou comment détecter des nœuds de sortie en écoute

Le nœud de sortie est-il en écoute ?



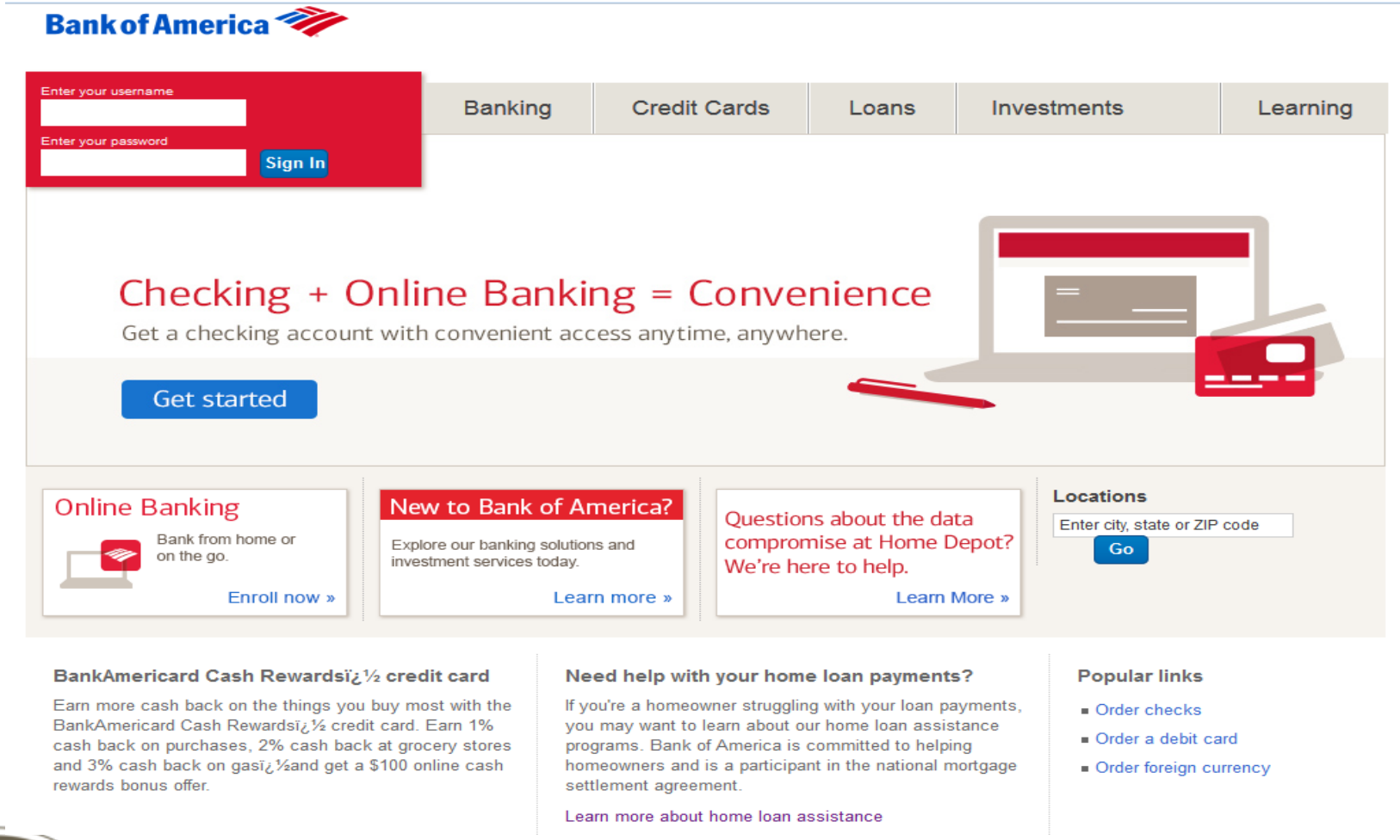
Plusieurs authentifications reçues par le serveur

OUI

Une seule authentification reçue par le serveur

NON

generaTor ou comment détecter des nœuds de sortie en écoute

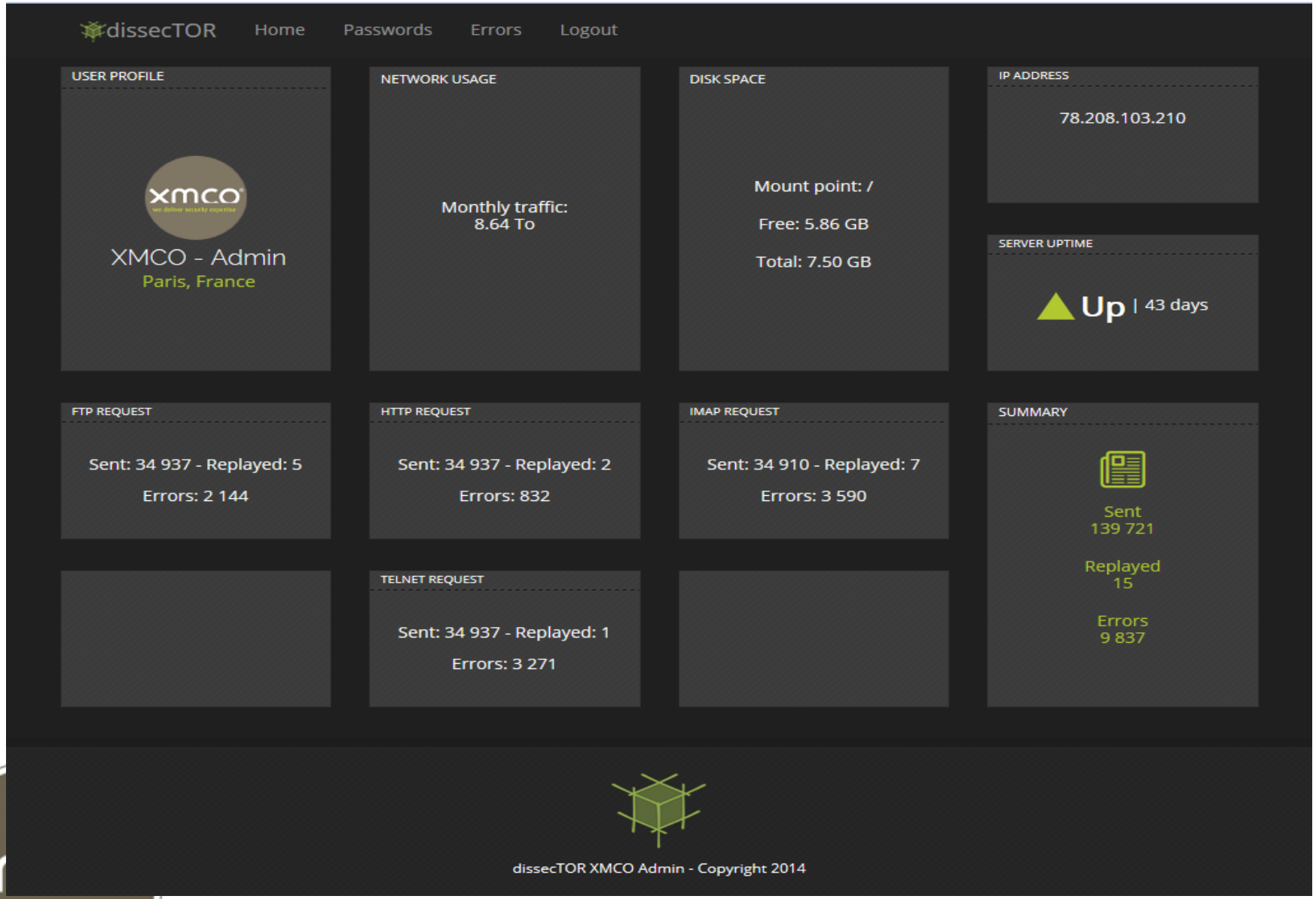


Interface Web incitant le rejeu d'authentification

generaTor : les résultats

- **~ 135 000 connexions effectuées sur un mois**
- **15 identifiants rejoués dans les deux mois :**
  - 5 pour le protocole FTP
  - 2 pour le protocole HTTP
  - 1 pour le protocole Telnet
  - 7 pour le protocole IMAP
- **~ 10 000 erreurs (7%)**
  - Protocole non accepté par le nœud de sortie
  - IP de destination rejetées par le nœud de sortie

generaTor ou comment détecter des nœuds de sortie en écoute



A TOR et à travers : Etude du réseau d'anonymisation en 2015, utilisation et faiblesses

generaTor ou comment détecter des nœuds de sortie en écoute

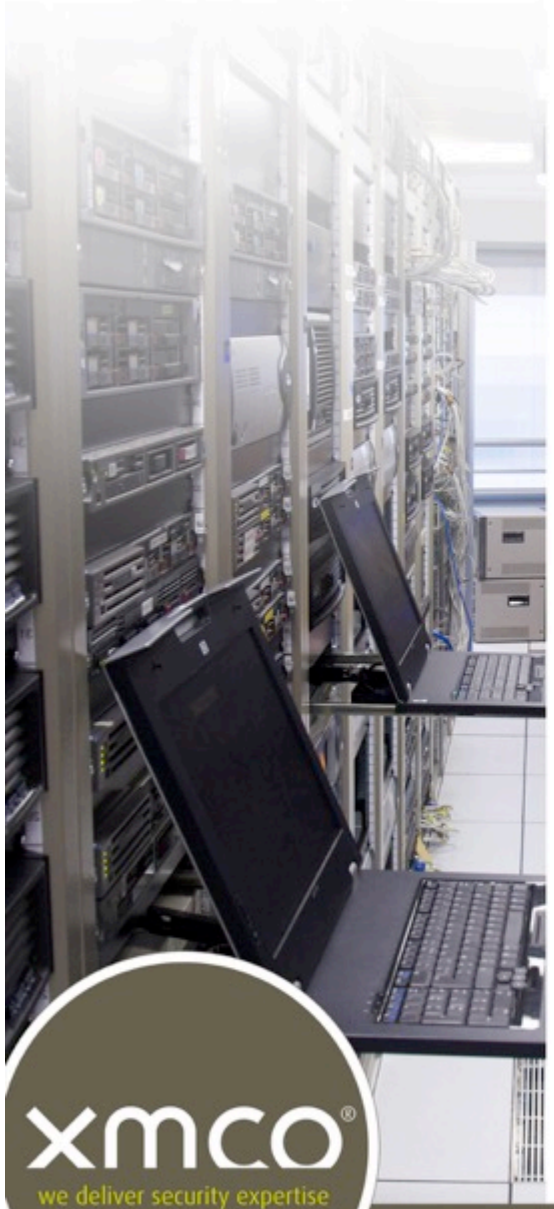
dissecTOR Home Passwords Errors Logout

Show 25 entries Search:

Protocol	Exit node	Login	Password
FTP	3 5.7	yb000000966	gvXuprf
FTP	5 27.83	ftp_usr_53zj53	l(?OLl)-$$
FTP	7 8.216	ftp_user_706ty706	NNgC!gT?ydO
FTP	1 221.211	ru000000964	qB&DxVm
FTP	8 .166	ftp_usr_86on86	HXyAuKiCh
HTTP	2 19.145	web_758dn758	$opehHodZRV
HTTP	1 .22	user_376rp376	tSXIeXlBrEJ
IMAP	3 .2	june_aragon@bank_account.eu	9UL.zK6BiNv4U
IMAP	3 4.92	lavander_le@bank_account.org	AU4B54QbOGsbk
IMAP	4 4.183	abigail_le@bank_account.com	FUMICypmAXZCk
IMAP	1 168.95	seth_gréco@bank_account.gov.gb	HU9RjKWZRlch6
IMAP	1 243.53	gerald_curin@bank_account.org	KUHTctiHjTwmw
IMAP	4 6.20	stephanie_fuentes@bank_account.org	MUbK2XtWiUpKA
IMAP	1 201.211	bryan_meier@bank_account.com	OUN90luWwZu5M
TELNET	8 2.48	telnet_648jm648	o$gZpAeyij!

Showing 1 to 15 of 15 entries Previous Next

Sommaire



1. Présentation du réseau TOR

2. dissecTor ou l'étude des nœuds de sortie

3. generaTor ou comment détecter des nœuds de sortie en écoute

4. **Conclusion**

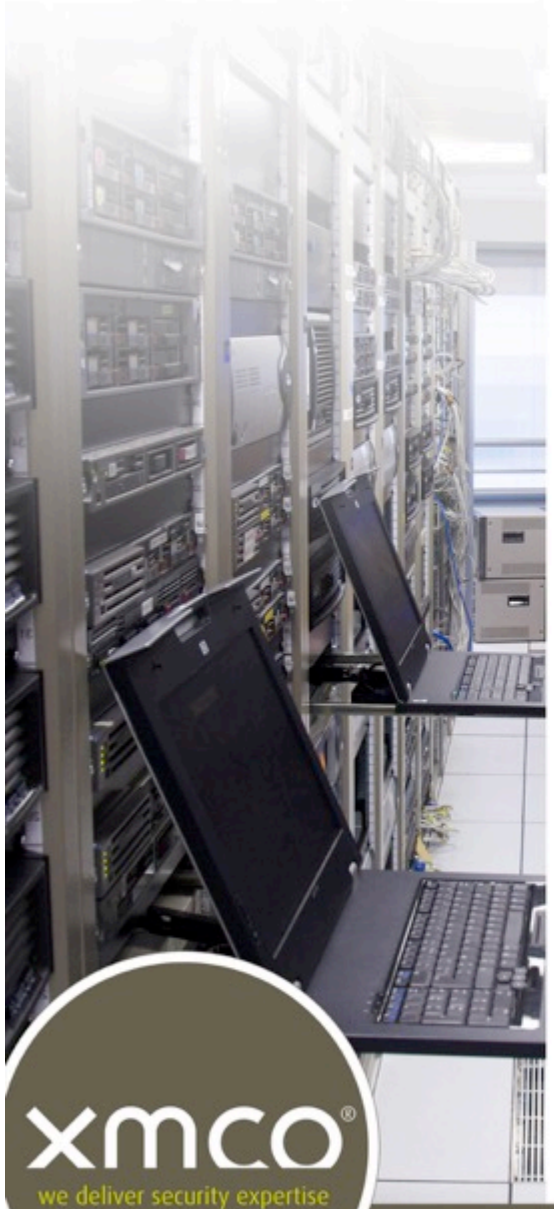
5. Questions

xmco®
we deliver security expertise

Conclusion

- **TOR n'assure pas la confidentialité des données transitant par le réseau**
- **TOR permet de palier les problèmes d'anonymat MAIS :**
  - Un chiffrement bout-à-bout doit être mis en place
  - La vigilance des utilisateurs reste primordiale
- **L'étau se resserre sur l'anonymat :**
  - Restez à l'écoute : https://blog.torproject.org/

Sommaire



1. Présentation du réseau TOR

2. dissecTor ou l'étude des nœuds de sortie

3. generaTor ou comment détecter des nœuds de sortie en écoute

4. Conclusion

5. **Questions**

xmco®
we deliver security expertise

Fin de la présentation

Questions

regis.senet@xmco.fr