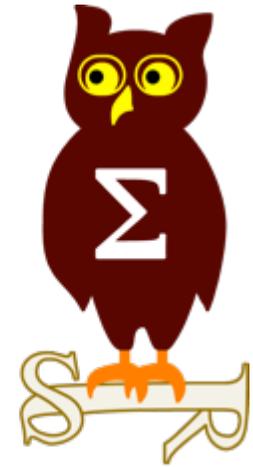




OSSIR



OSSIR

Réunion du 10 Février 2015

# Qui suis-je ?

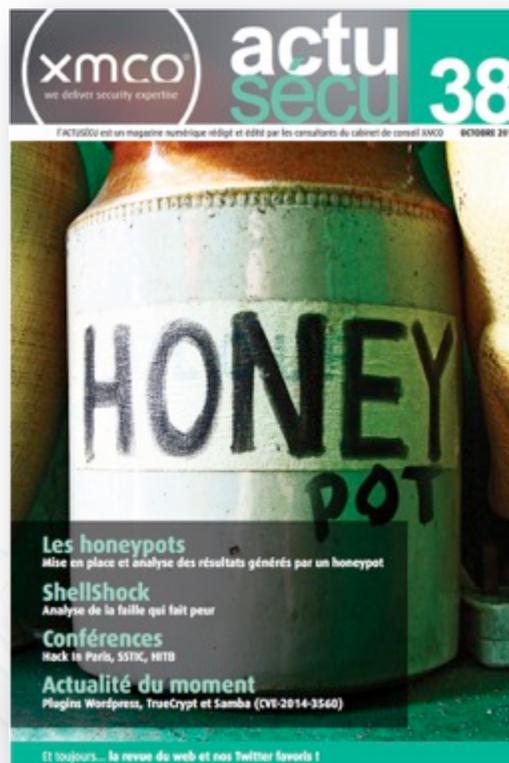
- **Régis Senet** – Consultant sécurité chez XMCO depuis juin 2014  
*Activités : Tests d'intrusion, audits, forensics, R&D*



Marc Behar  
marc.behar@xmco.fr  
11 bis, rue du Beauplais  
75001 Paris - France  
tel: +33 (0)1 47 34 66 61  
fax: +33 (0)1 45 66 29 55

# ActuSecu

## Article complet disponible



# A TOR et à travers

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



## 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**

# 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

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

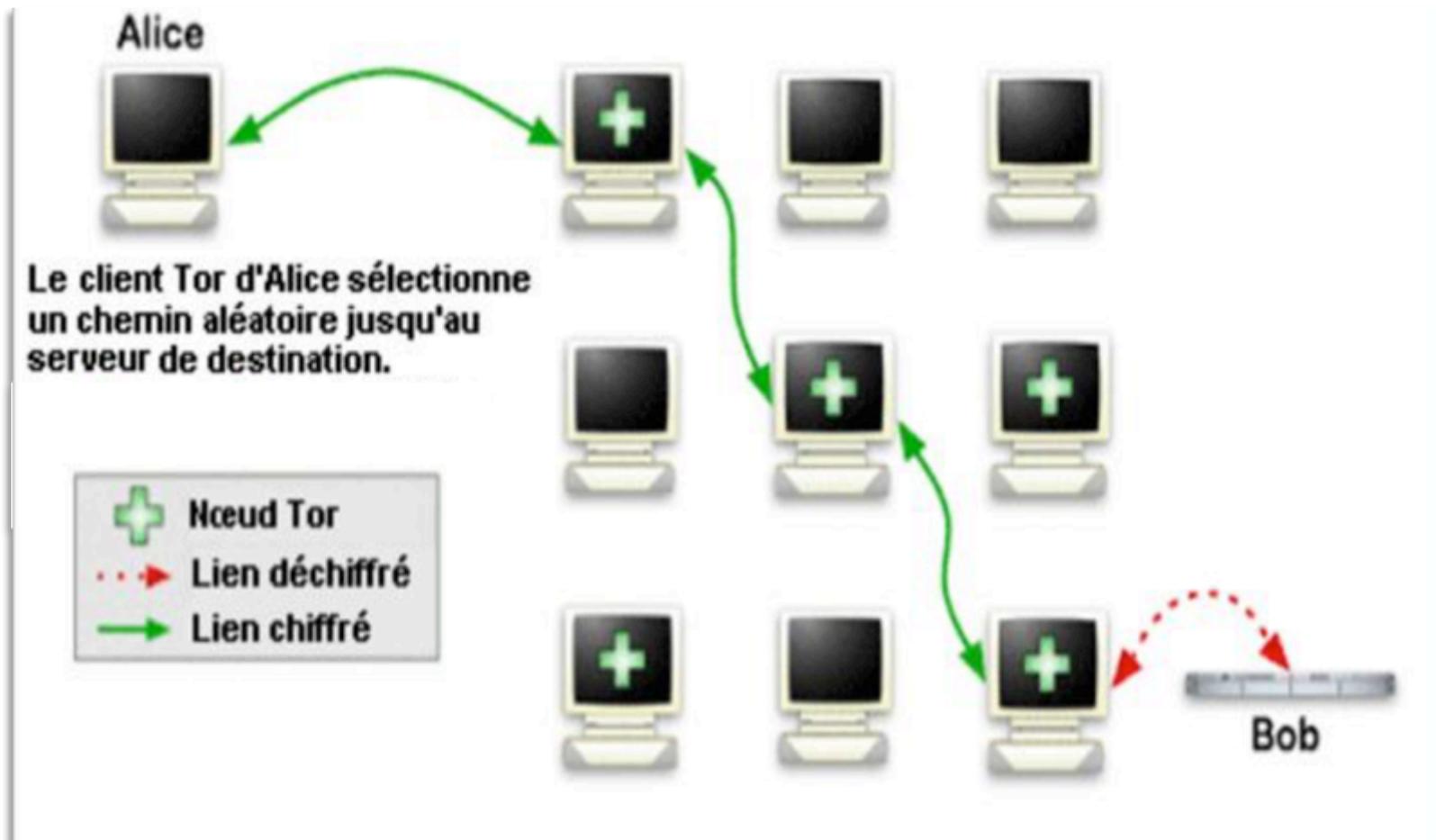
### Présentation du réseau TOR

- 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



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

### Fonctionnement du réseau TOR



*Fonctionnement du réseau TOR*

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

## Chiffrement des données



Déchiffrement des données



Chiffrement des données

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

Qui utilise TOR ?

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



1/3



2/3

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

### 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.



## 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

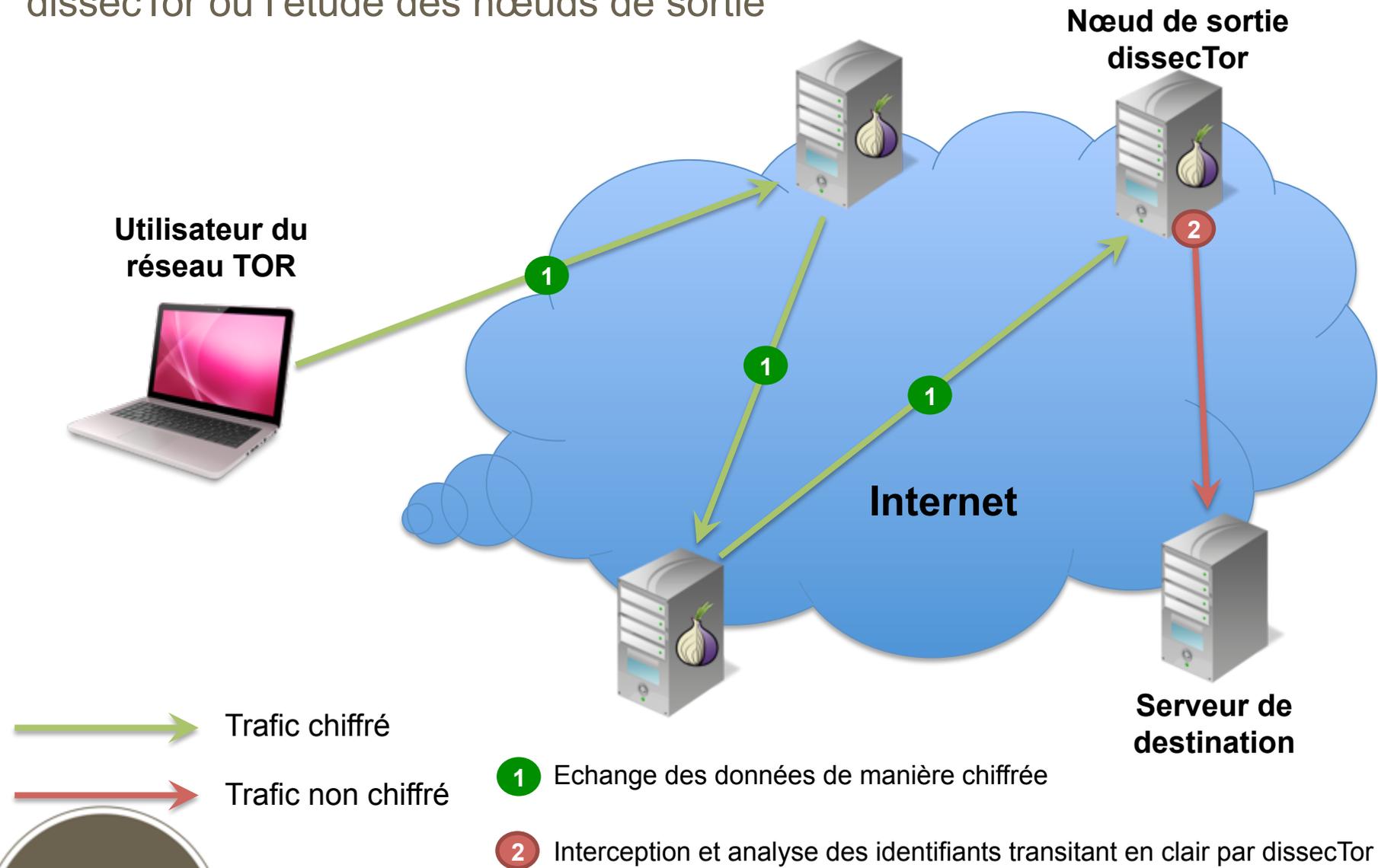
## A TOR et à travers : Etude du réseau d'anonymisation en 2015, utilisation et faiblesses dissecTor ou l'étude des nœuds de sortie

- 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



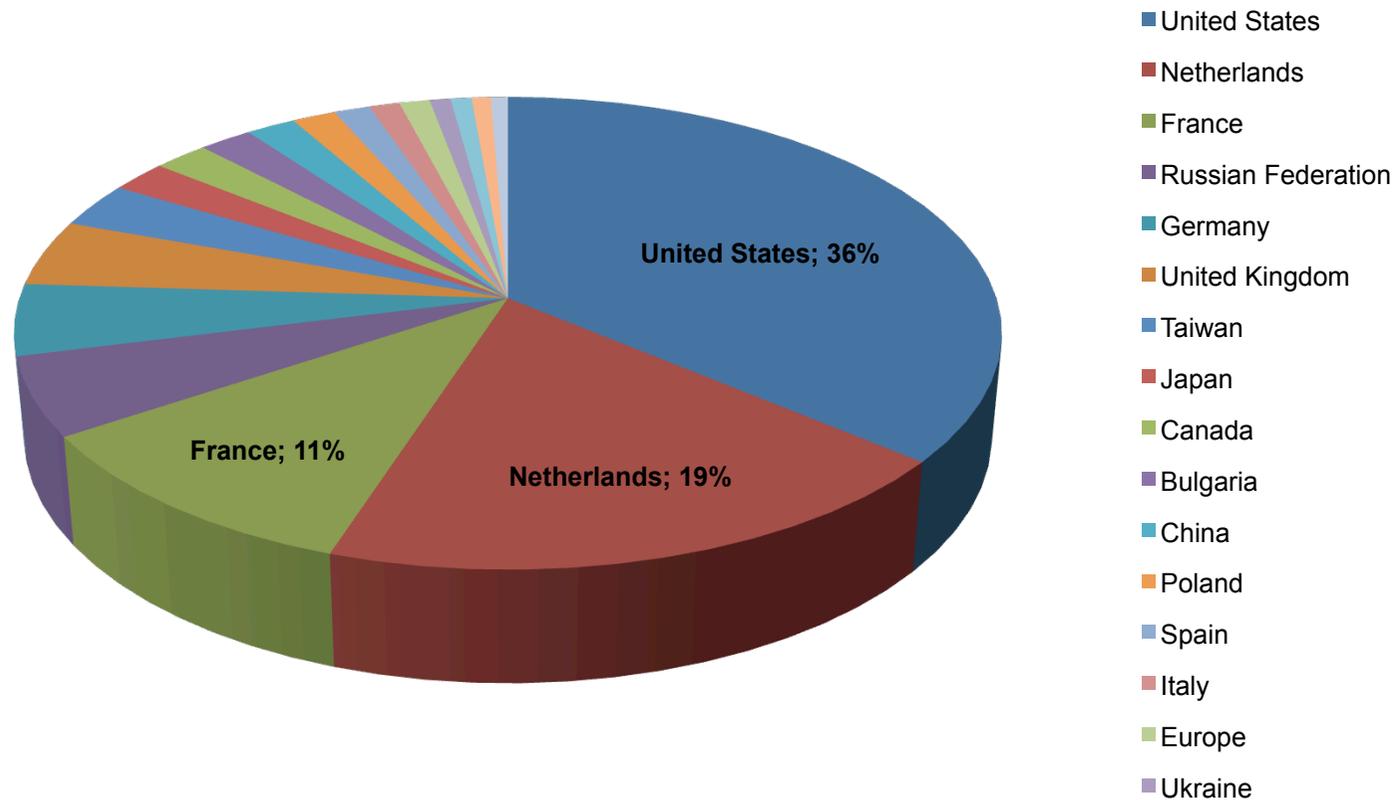
# A TOR et à travers : Etude du réseau d'anonymisation en 2015, utilisation et faiblesses

## dissecTor ou l'étude des nœuds de sortie



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

dissecTor ou l'étude des nœuds de sortie



Répartition des adresses de destination

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

### ■ Les statistiques

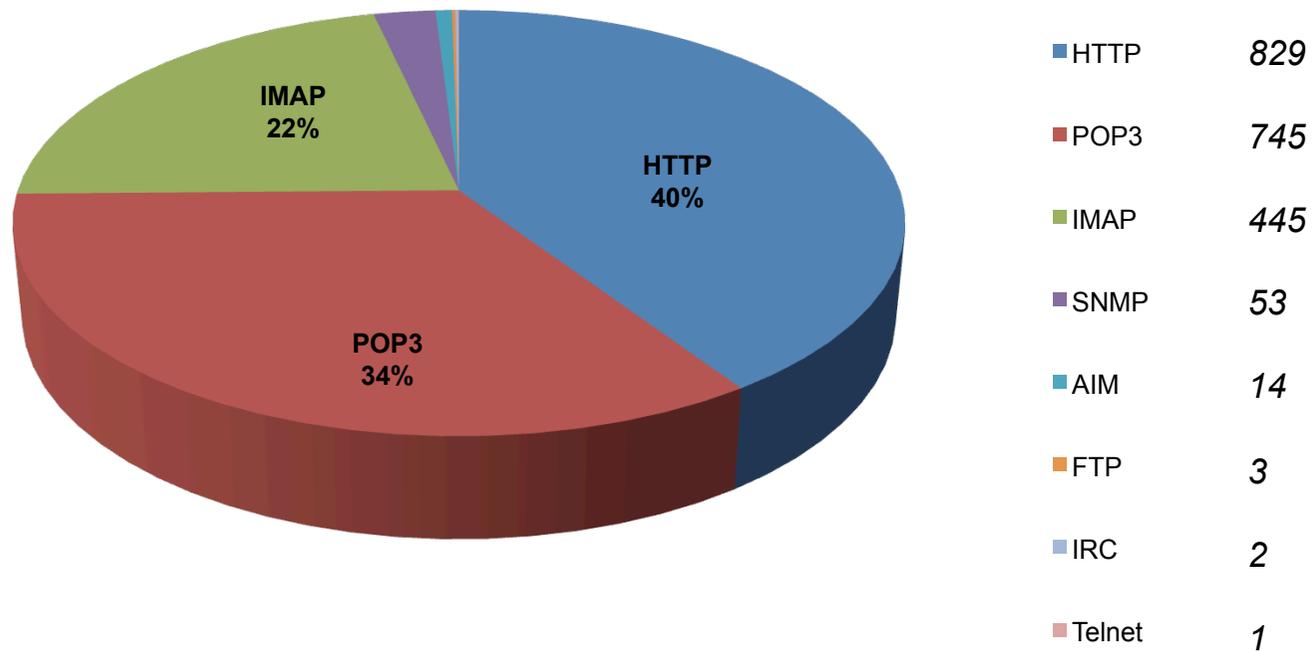
- Mots de passe divers captés : ~30 000
- Mots de passe conservés : ~2 200

### ■ Pourquoi une telle différence ?

- Très nombreuses attaques de bruteforce (à destination de la Russie notamment)
- Capture de certains hash par les outils utilisés



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



Répartition des mots de passe par protocole

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

### dissecTor : les résultats

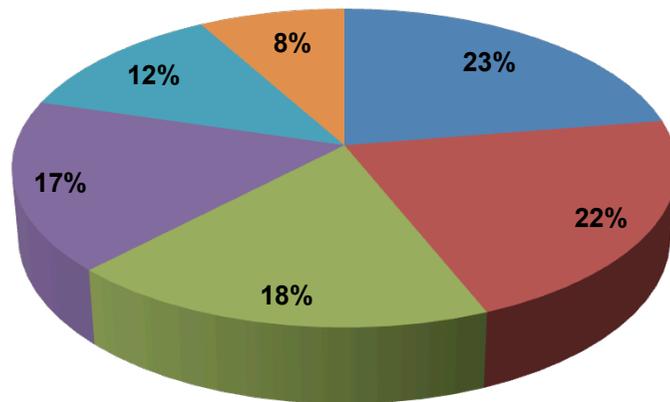
z [redacted] m.gov.cn  
m [redacted] fa.gov.ir  
ye [redacted] fa.gov.ye  
pvt [redacted] pt.gov.vn  
ve [redacted] ment.gov.rw  
va [redacted] ji.gov.az  
ma [redacted] ji.gov.az  
nal [redacted] ji.gov.az  
ki [redacted] il.gov.iq

Mots de passe d'adresses email gouvernementales



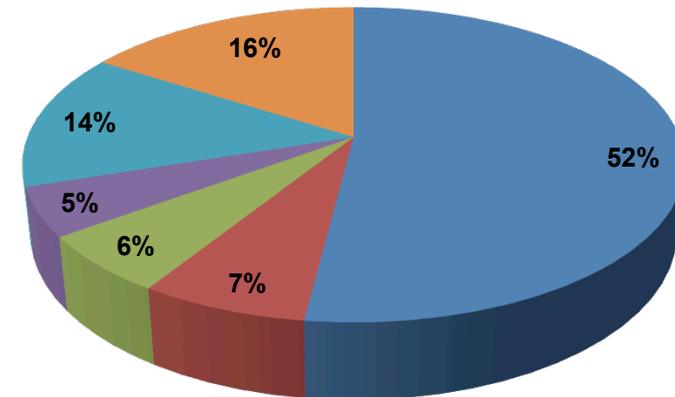
## A TOR et à travers : Etude du réseau d'anonymisation en 2015, utilisation et faiblesses

### dissecTor : les résultats



2008

- Pornographie
- Téléchargement
- Navigation blogs
- Webmail
- Attaque BruteForce
- Autres



2014

## 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 comment détecter des nœuds de sortie en écoute**
4. Conclusion
5. Questions

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

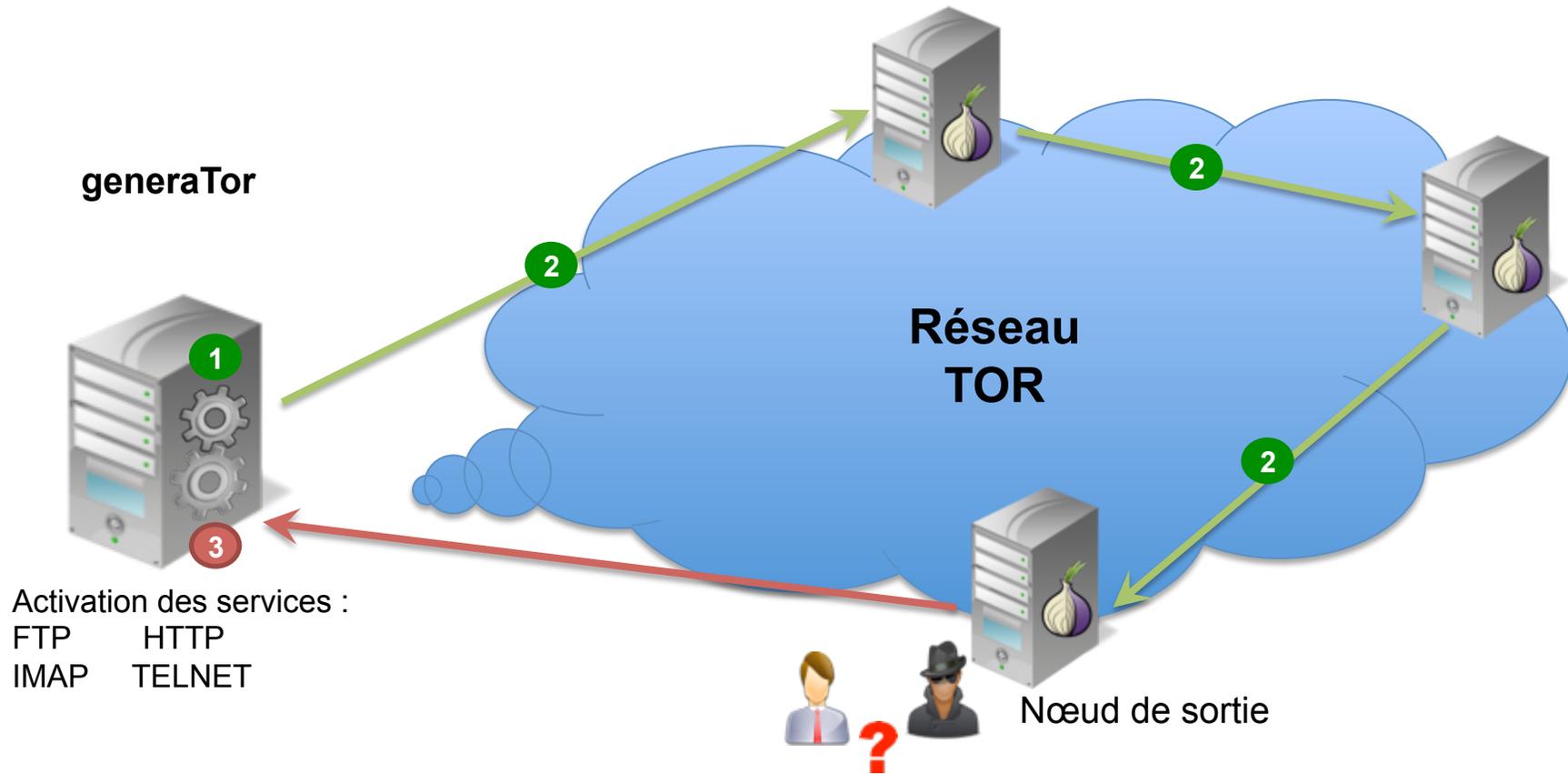
### Présentation de generaTor

- **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**



# 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



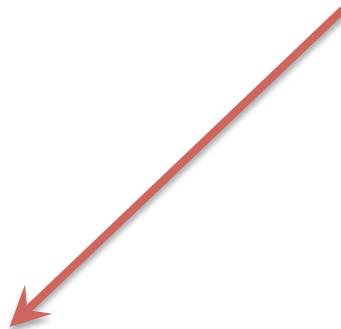
→ Trafic chiffré

→ 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 jeux d'authentification

**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

**Le nœud de sortie est-il en écoute ?**



Plusieurs authentifications  
reçues par le serveur

**OUI**

Une seule authentification  
reçue par le serveur

**NON**



# 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

The screenshot shows the Bank of America website interface. At the top left is the Bank of America logo. Below it is a red login box with two input fields: "Enter your username" and "Enter your password", followed by a "Sign In" button. To the right of the login box is a navigation menu with tabs for "Banking", "Credit Cards", "Loans", "Investments", and "Learning".

The main content area features a large banner with the text "Checking + Online Banking = Convenience" and "Get a checking account with convenient access anytime, anywhere." Below this is a blue "Get started" button. To the right of the text is an illustration of a laptop displaying a banking interface, a red pen, and a red credit card.

Below the banner are four promotional boxes:

- Online Banking**: "Bank from home or on the go." with an "Enroll now »" link.
- New to Bank of America?**: "Explore our banking solutions and investment services today." with a "Learn more »" link.
- Questions about the data compromise at Home Depot? We're here to help.** with a "Learn More »" link.
- Locations**: "Enter city, state or ZIP code" with a "Go" button.

At the bottom, there are three more sections:

- BankAmericard Cash Rewards 1/2 credit card**: "Earn more cash back on the things you buy most with the BankAmericard Cash Rewards 1/2 credit card. Earn 1% cash back on purchases, 2% cash back at grocery stores and 3% cash back on gas 1/2 and get a \$100 online cash rewards bonus offer."
- Need help with your home loan payments?**: "If you're a homeowner struggling with your loan payments, you may want to learn about our home loan assistance programs. Bank of America is committed to helping homeowners and is a participant in the national mortgage settlement agreement." with a "Learn more about home loan assistance" link.
- Popular links**:
  - Order checks
  - Order a debit card
  - Order foreign currency



## Interface Web incitant le rejeu d'authentification

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



## 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

The screenshot displays the dissecTOR XMCO Admin interface with the following sections:

- Navigation:** dissecTOR, Home, Passwords, Errors, Logout
- USER PROFILE:** xmco logo, XMCO - Admin, Paris, France
- NETWORK USAGE:** Monthly traffic: 8.64 To
- DISK SPACE:** Mount point: /, Free: 5.86 GB, Total: 7.50 GB
- IP ADDRESS:** 78.208.103.210
- SERVER UPTIME:** Up | 43 days
- FTP REQUEST:** Sent: 34 937 - Replayed: 5, Errors: 2 144
- HTTP REQUEST:** Sent: 34 937 - Replayed: 2, Errors: 832
- IMAP REQUEST:** Sent: 34 910 - Replayed: 7, Errors: 3 590
- TELNET REQUEST:** Sent: 34 937 - Replayed: 1, Errors: 3 271
- SUMMARY:** Sent 139 721, Replayed 15, Errors 9 837

dissecTOR XMCO Admin - Copyright 2014

## 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 [FR] 5.7	yb000000966	gvXuprf
FTP	5 [FR] 27.83	ftp_usr_53zj53	l(?OLI)-\$\$
FTP	7 [FR] 8.216	ftp_user_706ty706	NNgClgT?ydO
FTP	1 [FR] 221.211	ru000000964	qB&DxVm
FTP	8 [FR] .166	ftp_usr_86on86	HXyAuKiCh
HTTP	2 [SE] 19.145	web_758dn758	\$opehHodZRV
HTTP	1 [DE] .22	user_376rp376	tSXleXlBrEj
IMAP	3 [FR] .2	june_aragon@bank_account.eu	9UL.zK6BiNv4U
IMAP	3 [FR] 4.92	lavander_le@bank_account.org	AU4B54QbOGsbk
IMAP	4 [SE] 4.183	abigail_le@bank_account.com	FUMICypmAXZCk
IMAP	1 [FR] 168.95	seth_gréco@bank_account.gov.gb	HU9RjKWZRlch6
IMAP	1 [FR] 243.53	gerald_curin@bank_account.org	KUHTctiHjTwmw
IMAP	4 [FR] 6.20	stephanie_fuentes@bank_account.org	MUbK2XtWiUpKA
IMAP	1 [FR] 201.211	bryan_meier@bank_account.com	OUN90luWwZu5M
TELNET	8 [FR] 2.48	telnet_648jm648	o\$gZpAeyij!

Showing 1 to 15 of 15 entries Previous Next



## 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 comment détecter des nœuds de sortie en écoute
4. Conclusion
5. Questions

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

### 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'état se resserre sur l'anonymat :
  - Restez à l'écoute : <https://blog.torproject.org/>



# 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 comment détecter des nœuds de sortie en écoute
- 4.** Conclusion
- 5.** Questions

# Fin de la présentation

Questions



[regis.senet@xmco.fr](mailto:regis.senet@xmco.fr)

