>> Alexandre CAILLOT
>> Alexis ROBERT
>> Florian HEBERT
>> Léandre PERROT

« VOUS PRESENTE »

POWERING
DIGITAL
RESISTANCE

>> PLAN

/ TOR C'EST QUOI ?

/ L' HISTOIRE DE TOR

/ LE ROUTAGE EN OIGNONS

/ DEROULEMENT D'UNE CONNEXION

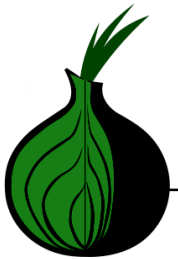
/ SES FAILLES

/ OUTILS

/ TOR C'EST QUOI ?

>> Protection contre la surveillance (analyse de trafic)
>> Contourner la censure
>> Eviter toute forme d'autorité et de contrôle

/ L' HISTOIRE DE TOR

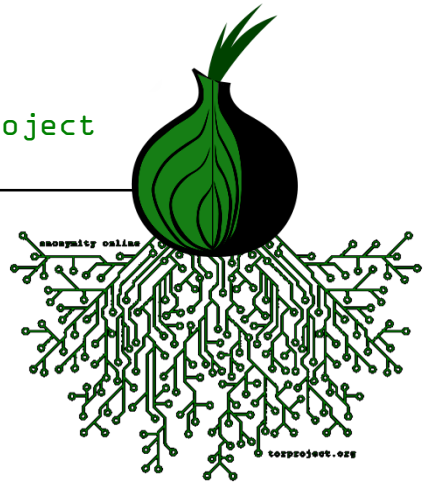


1995
>> Principe du routage en oignon

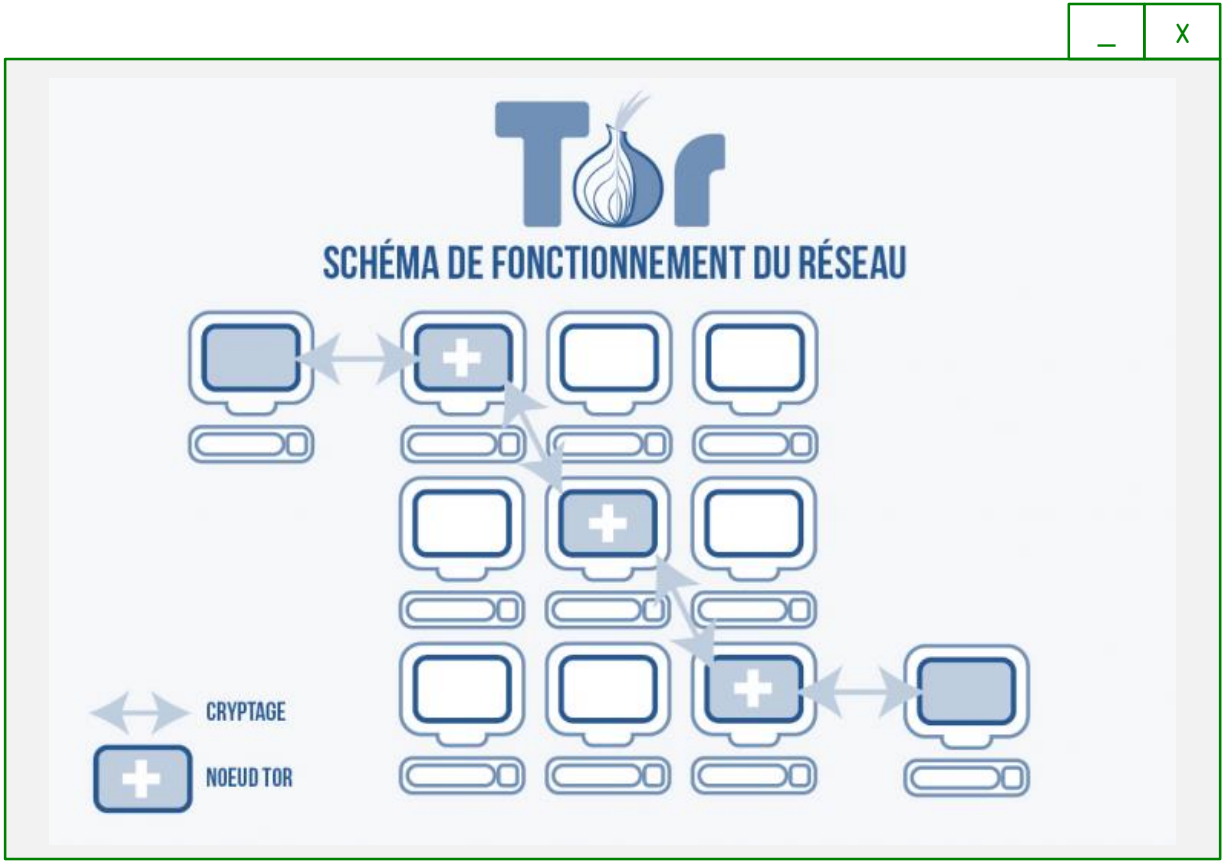
1997
>> Amélioration du routage en oignon

20 SEPTEMBRE 2002
>> Version alpha de TOR

DECEMBRE 2006
>> The Tor Project



/ LE ROUTAGE EN OIGNONS



>> Connexions passent par plusieurs proxys

>> Chaque proxy chiffre les paquets chacun leur tour

>> Seul le dernier proxy connait le message

/ LE ROUTAGE EN OIGNONS

>> Permet d'échapper aux autorités de certification

>> L'identité du propriétaire du site reste donc anonyme

>> En passant par des proxys grâce à TOR, la censure peut être contournée. Cependant le pays peut interdire l'accès aux relais TOR présents dans la liste publique

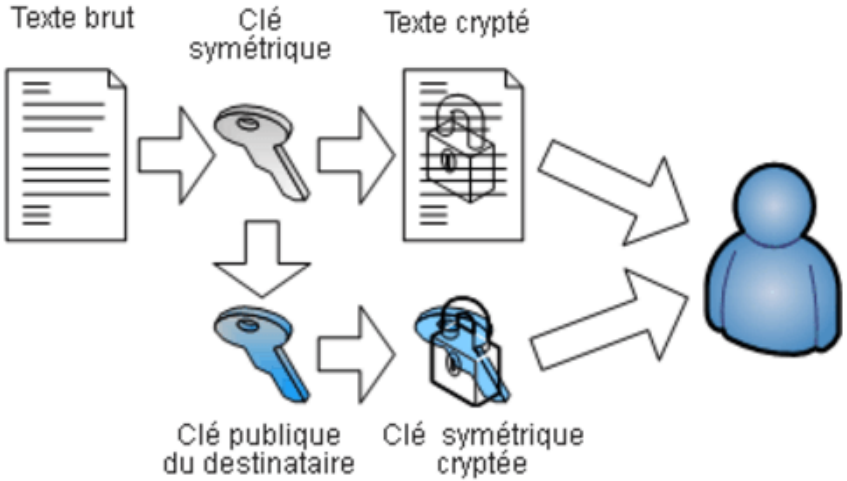
>> Les relais fournis pour TOR sont gratuits

/ DEROULEMENT D'UNE CONNEXION

Cryptographie hybrides

>> Tor transmet de manière anonyme des flux TCP grâce à une cryptologie hybride.
>> Associe la cryptographie asymétrique à la cryptographie symétrique
→ On chiffre le message avec une clé aléatoire par chiffrement symétrique
→ on effectue un chiffrement asymétrique sur la clé aléatoire avec clé publique / clé privée

Chaque nœud du circuit dispose d'une clef secrète qui lui est propre et ne connaît que son prédécesseur et son successeur au sein du circuit.

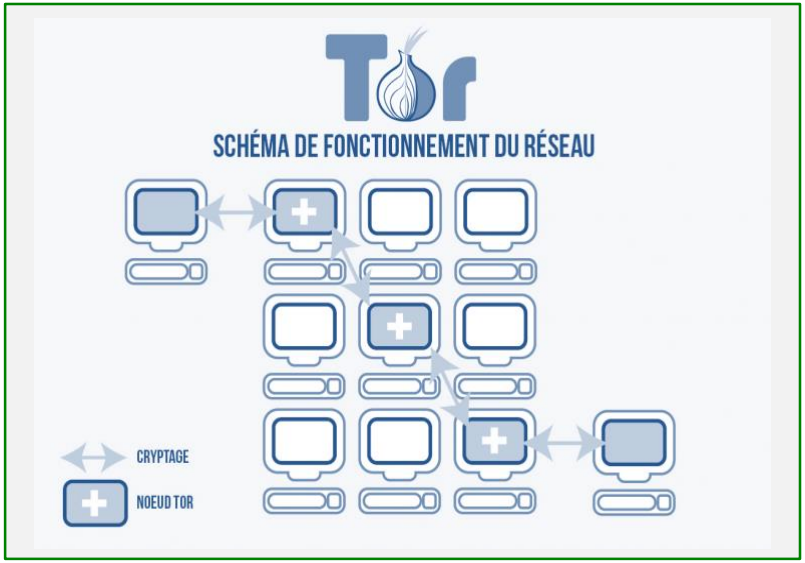


/ DEROULEMENT D'UNE CONNEXION

>> Pour acheminer un paquet au serveur, le client doit chiffrer son paquet de nombreuses fois :

1 Client chiffre son paquet TCP avec clef publique du dernier nœud n

2 Paquet TCP chiffré avec clef publique de l'avant-dernier nœud n-1



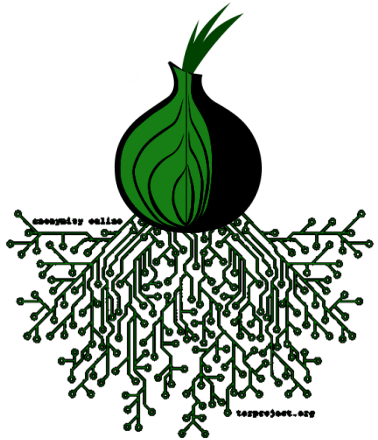
3 Client chiffre son paquet TCP avec clef publique du dernier nœud n-2

X La dernière fois paquet TCP chiffré avec la clef publique du premier nœud

/ DEROULEMENT D'UNE CONNEXION

>> Les relais déchiffrent le paquet lors de la réception:

1	Le premier relai déchiffre le paquet avec sa clé numérotée 1
2	le deuxième relai du circuit déchiffre le paquet avec la clef *2*
3	le deuxième relai du circuit déchiffre le paquet avec la clef *3*
X	Dernier serveur déchiffre ce paquet avec sa propre clé privée n et obtient l'original



/ SES FAILLES

GCHQ

/ SES FAILLES

>> ATTAQUE DE TIME PATTERN

>> Ecouter les nœuds d'entrée et de sortie

>> Chances d'écoute peut être augmentées si le pirate donne lui-même un motif temporel au flux, en inondant un nœud et en ralentissant donc le temps de traitement de la machine.

>> Une signature temporelle sera donc associée aux paquets qui traversent le nœud

/ OUTILS

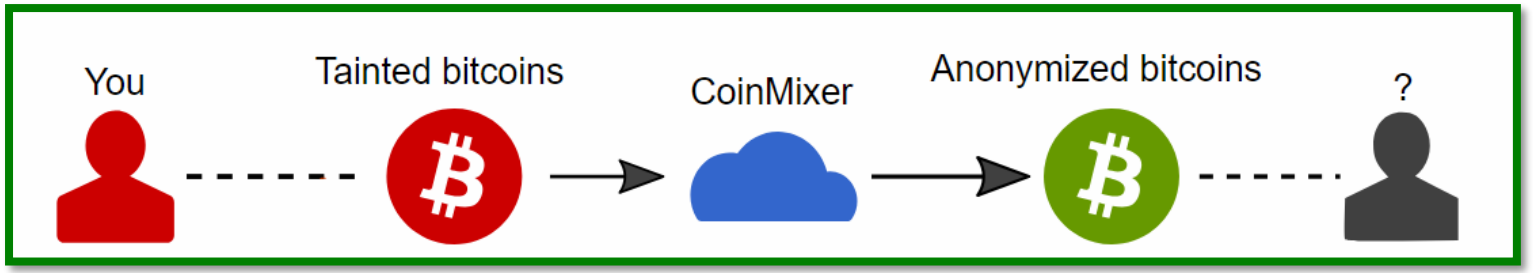
/ NAVIGUATEUR

/ OS

/ MESSAGERIE

RICOCHET

/ OUTILS >> utiliser Bitcoin anonymement



>> Flux classique d'un service de mixage Bitcoin

>> ACQUERIR DE MANIERE ANONYME DES BITCOINS

LocalBitcoins.com
Bringing Bitcoin Everywhere

>>

ELECTRUM

>> MERCI DE VOTRE ECOUTE