Tor, un vecteur privilégié pour la fraude bancaire ?

Au même titre que l'écrivain grec Esope considérait la langue comme la pire et la meilleure chose, le réseau Tor a lui aussi son double visage. Il a été créé pour éviter la censure et permet d'échanger dans un quasi anonymat. Tor est utilisé quotidiennement par environ **2,5 millions d'utilisateurs**. Le réseau comprend environ **6 000 relais présents dans 89 pays**. Le logiciel Tor Browser a été téléchargé 150 millions de fois au cours de la dernière année.

Mais c'est la face obscure de Tor ou plutôt son utilisation par les cybercriminels qui inquiète les autorités. Le dernier exemple en date est mis en évidence par **un rapport du FinCEN**, division du Département du Trésor en charge de collecter et d'analyser les données sur les transactions financières pour lutter contre le blanchiment d'argent. L'expert en sécurité Brian Krebs s'est procuré une copie de cette étude et montre l'examen de 6 048 cas d'activité suspecte déposés par les banques entre août 2001 et juillet 2014. Les experts financiers ont cherché des liens de correspondances avec un des 6 000 nœuds connus du réseau Tor. Ils ont déterminé **975 résultats concordants** qui totalisent **24 millions de dollars d'activités frauduleuses**.

Un difficile contrôle et un blocage inefficace

Le rapport indique que « *l'analyse des documents montre que certains déclarants (les banques) étaient au courant des connexions via Tor. Il révèle aussi que la majorité des dépôts sont liés à la cybercriminalité* ». Dans son analyse, FinCEN constate qu'une grande majorité des fraudes se déroulent par le biais **d'un vol d'identité ou de prise de contrôle du compte**.

L'équivalent de TracFin aux États-Unis n'exonère pas la responsabilité des banques, « *certaines activités suspectes auraient pu être évitées si l'institution de dépôt avait été au courant que son réseau était accessible via des adresses IP Tor* ». Tout en reconnaissant que la plupart des répondants ignoraient que les fraudes transitaient par le réseau d'anonymisation (cf tableau ci-dessous). Problème : cette pratique augmente très rapidement, constatent les enquêteurs. « *D'octobre 2007 à mars 2013, les dépôts ont augmenté de 50 %. Au cours de la période plus récente, 1er mars 2013 au 11 juillet 2014, les dépôts sont en hausse de 100 %* », écrivent-ils.

Diversity of Filers						
FILER	Money Services Businesses	Depository Institutions - Banks	Broker Dealers	MSB - Prepaid Card Providers	Depository Institutions- Credit Unions	MSB - Virtual Currency Exchangers
SARS	138	133	27	15	3	2
%	43%	42%	8%	5%	1%	1%

Filers Awareness of IP Association		
FILER	Knew IPs were Tor-related	Did NOT know IPs were Tor-related
# of SARS	10	308
% of Filers	3%	97%

Types of Suspicious Activity in Tor-related SARs		
SUSPICIOUS ACTIVITY	# of SARs	Percentage
Other[1]	164	52%
Identity Theft	140	44%
Money Laundering	110	35%
Unusual use of money transfer(s)	78	25%
Account Takeover	77	24%
Unauthorized electronic intrusion / Computer Intrusion	13	4%
Provided questionable or false documentation	12	4%
Suspicious concerning the source of funds	11	3%
Two or more individuals working together	9	3%
Forgeries	8	3%
Transaction with no apparent economic, business, or lawful purpose	8	3%
Suspicious use of multiple accounts	6	2%

[1] A review of Suspicious Activity referred to as "Other" determined that the majority of these activities were associated with Account Takeover and/or Identity Theft.

Est-ce que **le filtrage ou le blocage des adresses IP Tor** pourrait constituer une solution ? Pour Nicholas Weaver, chercheur au ICSI (International Computer Science Institute) de l'Université de Californie, interrogé par Brian Krebs, « *une telle approche n'aura pas d'impact significatif sur la fraude* ». Réagissant au rapport du FinCEN, il « *n'est pas très surpris car Tor est facile à utiliser par les cybercriminels pour masquer leur identité* ». Cependant, il souligne qu' « *il existe d'autres techniques pour cacher les adresses d'origine* ». Par ailleurs, le réseau Tor peut être utilisé par des personnes pour de bonnes raisons et elles seront alors directement impactées par une décision de blocage ou de filtrage.

A lire aussi :

Facebook investit Tor, pour lutter contre la censure

Tor : l'anonymat n'est pas toujours synonyme de sécurité

Crédit Photo : Lim ChewHow-Shutterstock