Les VPN commerciaux sont-ils vraiment sécurisés ?

Peut-on faire aveuglément confiance aux VPN pour sécuriser les communications Internet entre deux postes ? Apparemment non. Du moins, pas pour tous les réseaux privés virtuels si l'on en croit une étude de cinq universitaires britanniques et italiens. Les équipes de chercheurs des universités de Sapienza à Rome et Queen Mary à Londres se sont penchées sur 14 des plus populaires services commerciaux de VPN (ceux qui remontent parmi les vingt premiers sur Google) vantés pour leurs capacités à garantir l'anonymat, protéger la vie privée, contourner les censures, échapper à la surveillance, etc.

Leurs utilisateurs risquent d'être consternés en apprenant notamment que *« la majorité des services VPN souffrent de fuites de trafic IPv6 »* et sont notamment faillibles aux attaques par détournement de DNS *« qui autorisent la capture du trafic en toute transparence »*, notent les chercheurs dans leur compte-rendu. Sur les 14 VPN étudiés, seuls 4 n'ont pas révélé de fuites en IPv6 et **seul 1 est protégé contre les détournements de DNS** (serveurs de noms de domaines).

Provider	Countries	Servers	Technology	DNS	IPv6-leak	DNS hijacking
Hide My Ass	62	641	OpenVPN, PPTP	OpenDNS	Y	Y
IPVanish	51	135	OpenVPN	Private	Y	Y
Astrill	49	163	OpenVPN, L2TP, PPTP	Private	Y	N
ExpressVPN	45	71	OpenVPN, L2TP, PPTP	Google DNS, Choopa Geo DNS	Y	Y
StrongVPN	19	354	OpenVPN, PPTP	Private	Y	Y
PureVPN	18	131	OpenVPN, L2TP, PPTP	OpenDNS, Google DNS, Others	Y	Y
TorGuard	17	19	OpenVPN	Google DNS	N	Y
AirVPN	15	58	OpenVPN	Private	Y	Y
PrivateInternetAccess	10	18	OpenVPN, L2TP, PPTP	Choopa Geo DNS	N	Y
VyprVPN	8	42	OpenVPN, L2TP, PPTP	Private (VyprDNS)	N	Y
Tunnelbear	8	8	OpenVPN	Google DNS	Y	Y
proXPN	4	20	OpenVPN, PPTP	Google DNS	Y	Y
Mullvad	4	16	OpenVPN	Private	N	Y
Hotspot Shield Elite	3	10	OpenVPN	Google DNS	Y	Y

Table 1. VPN services subject of our study

L'IPv6 mal pris en charge

Concernant les problèmes avec l'IPv6, les chercheurs expliquent que, si les clients VPN prennent bien en compte les tables de routage en IPv4, ils tendent à ignorer celles du nouveau protocole IP. *« Aucune règle n'est ajoutée pour rediriger le trafic dans le tunnel IPv6*, expliquent les auteurs. *Cela peut entraîner le contournement de l'interface virtuelle du VPN pour l'ensemble du trafic IPv6. »* Une vulnérabilité critique à l'heure où les volumes de trafic en IPv6 s'accroissent au fil des mois. Pour s'en prémunir, il suffit de désactiver le trafic IPv6… quand l'OS le permet. Ce qui n'est pas le cas d'Android.

Si le trafic IPv4 est bien pris en charge par les clients VPN, il n'en reste pas moins sous la menace des risques de contournement de DNS. *« L'attaquant peut rediriger toutes les requêtes DNS vers ses propres proxy locaux, contournant ainsi le tunnel VPN, et prendre aussi bien le contrôle du trafic IPv4 que IPV6. »* Pour les chercheurs, ce problème est principalement imputable à Windows qui n'a pas de règles de paramétrage des DNS et permet à chaque interface d'indiquer son propre serveur de domaine. *« En raison de la façon dont Windows traite une résolution DNS, tout retard dans une réponse du tunnel VPN peut déclencher une autre requête DNS à partir d'une interface différente, ce qui entraîne une*

fuite », précise le rapport. Pour essayer de s'en prémunir, les auteurs conseillent aux utilisateurs d'adopter une approche proactive en vérifiant régulièrement (au moins une fois par minute) l'état de fonctionnement du DNS.

Peu de problème pour les VPN d'entreprise

Par ailleurs, les universitaires notent que la plupart des services de «tunnellisation» VPN s'appuient sur des technologies dépassées comme le PPTP qui, associé au protocole d'authentification MS-CHAPv2, *« est affecté de sérieuses vulnérabilités de sécurité bien connues au sein de la communauté depuis des années »*. Autant directement envoyer ses données aux attaquants. *« La situation la plus alarmante correspond à celle où les personnes utilisent les services de VPN pour se protéger de la surveillance dans les régimes oppressifs*, alertent les chercheurs. *Dans de tels cas, les utilisateurs qui croient être anonymes et sécurisés exposeront pleinement leurs données et leur activité en ligne. »*

Point rassurant pour les DSI, les VPN fournis par les entreprises à leurs employés ont plus de chance d'échapper à ces maux. *« Les fuites de trafic IPv6 ne sont pas possibles quand les connexions au réseau de l'entreprise à l'extérieur du tunnel VPN ne sont pas autorisées (en supposant que toutes les configurations soient effectuées correctement)*, estiment les auteurs du rapport. *En revanche, le détournement de DNS pourrait fournir les noms des ressources accessibles dans le réseau de l'entreprise privée. Toutefois, à moins que l'attaquant n'ait une connaissance détaillée du réseau d'entreprise, la résolution de nom échouera et l'utilisateur se verra notifier l'erreur et arrêtera éventuellement d'utiliser le VPN. »*

Lire également
La faille Heartbleed exploitée pour attaquer les VPN d'entreprise
TheGreenBow, premier VPN au monde certifié EAL3+
Hacking : pourquoi les États s'en prennent aux éditeurs de sécurité