Carnivore

Le chien de garde du FBI sur Internet (1997–2005)

Stéphane Fosse
https://fosse.fr

27 février 2026

Carnivore, renommé DCS1000 en 2001, est un système d'interception réseau développé par le FBI et déployé chez les fournisseurs d'accès Internet américains à partir d'octobre 1997. C'est une boîte noire — littéralement un PC sous Windows NT sans écran ni clavier — que les agents fédéraux venaient installer dans les salles machines des ISP pour capturer les paquets IP d'un utilisateur ciblé par ordonnance judiciaire. Il a été abandonné discrètement dès 2001, et officiellement déclaré obsolète en janvier 2005.

1 Comment fonctionnait Carnivore techniquement ?

Carnivore est un *packet sniffer* — un analyseur de paquets réseau — fonctionnant sur un PC sous Windows NT, équipé d'un disque amovible Jaz de 2 Go sur lequel les données capturées étaient stockées. Le boîtier, dépourvu d'écran et de clavier sur site, était contrôlé à distance depuis un bureau du FBI via un lien téléphonique et le logiciel de prise en main à distance PCAnywhere. Un agent technique venait physiquement récupérer les disques Jaz à intervalles réguliers pour les rapporter au bureau.

L'architecture reposait sur deux couches logicielles distinctes. Un pilote noyau Windows — `TAPNDIS` et `TAPAPI` — capturait les paquets directement au niveau de l'interface réseau, avant même que le système d'exploitation ne les traite. Une bibliothèque applicative, `Carnivore.dll`, appliquait ensuite les filtres définis par l'ordonnance judiciaire : adresse IP de la cible, protocoles concernés (SMTP, POP, HTTP, FTP), plages de ports, identifiants DHCP ou RADIUS. L'interface graphique permettait aux agents de basculer entre deux modes : le mode *pen*, qui ne collecte que les métadonnées (adresses source et destination), et le mode *full content*, qui capture le contenu intégral des communications.

Le problème fondamental tenait à la nature du réseau IP. Sur un réseau commuté par paquets, la seule façon de cibler un utilisateur est d'inspecter d'abord tous les paquets qui transitent par le segment réseau auquel il est connecté, puis de filtrer ceux qui lui appartiennent. Carnivore ne faisait pas exception : selon le rapport d'évaluation indépendante commandé par le Département de Justice en décembre 2000 et réalisé par l'IIT Research Institute (IITRI) de Chicago, le système était « capable de balayages larges ». Mal configuré, il pouvait enregistrer l'intégralité du trafic de l'ISP. C'est exactement ce que l'EPIC (Electronic Privacy Information Center) démontra en novembre 2000, grâce à des documents internes du FBI obtenus par voie judiciaire via la loi FOIA : un test de Carnivore version 1.3.4 confirmait que le système pouvait « capturer et archiver de manière fiable tout le trafic non filtré » vers le disque dur interne [9].

2 Quelle était la base légale de Carnivore, et pourquoi était-elle contestée ?

Le FBI opérait Carnivore sous trois régimes juridiques distincts. Le plus courant était le *pen register* et le *trap and trace*, des ordonnances analogues à celles utilisées pour les écoutes téléphoniques traditionnelles, qui n'autorisent la collecte que des métadonnées — numéros composés, adresses de correspondants — et non du contenu. Le plus contraignant était le mandat *Title III*, issu de l'Omnibus Crime Control and Safe Streets Act de 1968, qui permettait l'interception du contenu intégral mais exigeait une démonstration de nécessité bien plus rigoureuse devant un tribunal fédéral. Un troisième cadre, le Foreign Intelligence Surveillance Act (FISA), s'appliquait aux enquêtes de contre-espionnage.

La critique principale formulée par l'Electronic Frontier Foundation (EFF) et l'ACLU était précisément ce problème de transposition. Les ordonnances *pen register* et *trap and trace* avaient été conçues pour le réseau téléphonique commuté, où les métadonnées (numéros de téléphone) et le contenu (voix) circulent sur des

canaux physiquement séparés. Sur Internet, ils sont mêlés dans chaque paquet IP. L'EFF démontrait devant le Sous-comité sur la Constitution de la Chambre des représentants, le 28 juillet 2000, que Carnivore récupérait structurellement plus d'informations que n'en autorisaient les ordonnances de type *pen* : les URLs visitées révèlent des intentions et des intérêts, les en-têtes d'e-mails exposent parfois des lignes d'objet qui sont du contenu à part entière [8]. Autoriser la police à utiliser ce type d'ordonnance faible pour surveiller Internet revenait, selon l'EFF, à abaisser le niveau de protection constitutionnelle garanti par le quatrième amendement.

La loi CALEA (Communications Assistance for Law Enforcement Act) de 1994, adoptée sous l'administration Clinton, constituait le socle de cette doctrine. Elle obligeait les opérateurs de télécommunications à concevoir leurs équipements de façon à faciliter les écoutes légales. Carnivore était, en pratique, la réponse technique du FBI à CALEA appliquée à l'Internet — mais CALEA elle-même avait expressément exclu les données circulant sur Internet de son champ d'application initial [3].

3 Qui a découvert Carnivore, et comment l'affaire a-t-elle éclaté ?

L'existence de Carnivore est devenue publique non pas à la suite d'une fuite, mais d'une procédure judiciaire. En avril 2000, lors d'une audition du Sous-comité sur la Constitution de la Chambre des représentants, l'avocat Robert Corn-Revere révéla que son client, un fournisseur d'accès Internet dont l'identité ne fut pas divulguée mais qui était EarthLink, avait été contraint par le FBI d'installer le système sur son réseau pour exécuter une ordonnance de surveillance. EarthLink avait résisté : l'installation avait provoqué des plantages de ses serveurs d'accès distant, coupant le service à environ 10 000 de ses clients. Le Wall Street Journal publia une enquête détaillée le 11 juillet 2000, et l'affaire devint nationale en quelques jours.

Dès le 12 juillet 2000, l'EPIC (Electronic Privacy Information Center), organisation de défense des droits numériques fondée à Washington en 1994, déposait une demande d'accès aux documents administratifs (FOIA) auprès du FBI [10]. Face au refus de répondre dans les délais légaux, l'EPIC porta l'affaire devant le tribunal fédéral du district de Columbia. Le juge James Robertson ordonna au FBI de produire ses documents tous les 45 jours. Au terme de la procédure, le Bureau affirma disposer de 3 000 pages de documents. Il en communiqua 1 502 partiellement caviardées et en retint 254 en totalité. Le code source de Carnivore ne fut jamais divulgué.

L'Attorney General Janet Reno ordonna une évaluation indépendante. Le Département de Justice sélectionna en septembre 2000 l'IIT Research Institute (IITRI) — après que le MIT, Purdue, Dartmouth et l'université de Californie à San Diego avaient refusé de participer, jugeant les conditions imposées par le DoJ trop restrictives pour garantir une évaluation véritablement indépendante [11]. L'IITRI remit son rapport final le 8 décembre 2000, pour un montant de 175 000 dollars.

4 Que révélait l'audit technique indépendant sur Carnivore ?

Le rapport IITRI est l'une des rares évaluations techniques sérieuses d'un outil de surveillance gouvernementale rendue partiellement publique de son vivant. Il est instructif, et pas seulement pour ce qu'il dit de favorable au FBI.

Sur le fond, l'IITRI conclut que Carnivore fonctionnait globalement dans les limites fixées par les ordonnances judiciaires lorsqu'il était correctement configuré. Mais le rapport identifiait plusieurs défaillances structurelles. La plus grave : l'absence totale de traçabilité des actions. Tous les opérateurs se connectaient au système sous le même compte Windows « administrator », sans qu'aucun journal d'audit ne permette de déterminer qui avait fait quoi. Si des données hors-cible étaient collectées, il était impossible d'identifier l'agent responsable. L'IITRI notait sobrement qu'il « n'avait pas trouvé de dispositions adéquates pour établir la responsabilité individuelle des actions effectuées pendant l'utilisation de Carnivore » [9].

Autre défaillance : le recours à PCAnywhere pour le contrôle à distance du boîtier installé chez l'ISP. Ce logiciel de prise en main accordait un accès complet à tous les fichiers du système, y compris les journaux, sans aucun mécanisme d'audit des accès distants. Un groupe de cinq chercheurs indépendants — Steven Bellovin et Matt Blaze d'AT&T Labs Research, David Farber de l'université de Pennsylvanie, Peter Neumann de SRI International, et Eugene Spafford de l'université Purdue — publia en décembre 2000 une critique circonstanciée du rapport IITRI, relevant notamment l'absence de recherche systématique de débordements de tampon (*buffer overflows*), la non-évaluation du comportement de Carnivore en mode RADIUS (protocole d'authentification des connexions dial-up), et le fait que le logiciel de second niveau `Packeteer`, chargé du traitement post-collecte, contenait des bugs que le FBI aurait dû détecter en interne bien avant l'audit externe [2].

Le rapport IITRI soulignait par ailleurs qu'en mode *pen*, Carnivore collectait les longueurs des messages et de leurs champs — ce qui permettait une analyse de trafic permettant d'identifier, par exemple, quelle page d'un site web un utilisateur avait visitée, à partir de la taille des objets retournés par le serveur. Ce type de collecte dépassait ce qu'autorisait une ordonnance *pen register* standard.

5 L'incident Ben Laden : quand Carnivore sabote une enquête antiterroriste

Le document le plus embarrassant pour le FBI fut rendu public par l'EPIC en mai 2002. Un mémo interne daté du 5 avril 2000, adressé à M. E. « Spike » Bowman, conseiller juridique associé chargé des affaires de sécurité nationale, décrit un incident survenu en mars 2000 lors d'une opération antiterroriste conduite par l'International Terrorism Operations Section (ITOS) et son « UBL Unit » — désignation officielle de l'unité chargée d'Oussama ben Laden.

Carnivore « a été activé et n'a pas fonctionné correctement ». Le système a capturé non seulement les communications de la cible autorisée par le tribunal, « mais aussi des e-mails de personnes non couvertes » — une violation directe du Wiretap Act fédéral. L'agent technique du FBI, « apparemment tellement perturbé, a détruit l'ensemble des e-mails collectés, y compris ceux concernant [la cible autorisée] ». En d'autres termes, une collecte illégale avait conduit à la destruction des preuves légalement autorisées [5].

Le mémo concluait : « Quand vous ajoutez cette histoire aux erreurs FISA couvertes dans [un autre document non divulgué], vous avez un schéma d'occurrences qui indique à l'OIPR une incapacité du FBI à gérer ses FISA. » L'OIPR est l'Office of Intelligence Policy and Review, l'organisme du Département de Justice chargé de superviser les opérations de surveillance au titre du Foreign Intelligence Surveillance Act. L'incident ne fut jamais rendu public par le FBI de son propre chef.

6 Pourquoi le FBI a-t-il finalement abandonné Carnivore ?

En janvier 2005, l'Associated Press révélait que le FBI n'avait pas utilisé Carnivore depuis 2001 [1]. Les rapports officiels soumis aux commissions judiciaires du Sénat et de la Chambre confirmaient que le Bureau avait réalisé cinq écoutes Internet en 2002 et huit en 2003, toutes via des logiciels commerciaux non identifiés publiquement. Aucune n'avait impliqué Carnivore.

La transition s'explique par plusieurs facteurs convergents. Les logiciels commerciaux — au premier rang desquels NarusInsight, développé par la société californienne Narus et capable d'analyser des dizaines de gigabits par seconde en temps réel — avaient rattrapé puis dépassé les capacités du système maison. Ils étaient moins onéreux à maintenir : le FBI n'a jamais divulgué le coût total de développement de Carnivore, mais des experts externes l'estimaient entre 6 et 15 millions de dollars, pour une durée de vie de quatre ans à peine.

Surtout, la relation avec les ISP avait évolué. Le FBI remboursait désormais les fournisseurs d'accès qui exécutaient eux-mêmes les écoutes ordonnées par les tribunaux. Cette délégation présentait un avantage considérable : l'ISP connaissait sa propre infrastructure bien mieux qu'un agent technique du FBI. Elle éliminait aussi la friction politique autour d'une boîte noire installée dans les locaux d'une entreprise privée sans que ses techniciens puissent en vérifier le fonctionnement. EarthLink avait maintenu sa résistance tout au long — après le 11 septembre 2001, elle continuait à exécuter les ordonnances elle-même, refusant l'installation de Carnivore sur ses réseaux.

Ce glissement vers l'externalisation aux ISP n'était pas une victoire pour la vie privée. C'était une mutation architecturale. La surveillance ne disparaissait pas : elle se fragmentait, se normalisait, devenait invisible. En 2007, un rapport basé sur des documents obtenus par l'EFF via la FOIA révélait que le successeur de Carnivore, le réseau DCSNet (Digital Collection System Network), était déployé « à l'intérieur du réseau d'un fournisseur d'accès, à la jonction d'un routeur ou d'un commutateur réseau », capable de stocker indistinctement tout le trafic transitant par ce nœud. L'architecture avait changé, pas l'ambition.

7 Conclusion : Carnivore comme révélateur d'une tension permanente

Carnivore n'a directement espionné que quelques dizaines de personnes entre 1998 et 2001 — le FBI évoque lui-même environ 25 déploiements sur cette période, principalement dans des affaires de contre-espionnage et de contre-terrorisme. Ce n'est pas un programme de surveillance de masse au sens de PRISM ou d'XKeyscore. Mais il a posé pour la première fois, de façon concrète et publiquement documentée, les questions que chaque système de surveillance légitime doit résoudre : comment cibler sans collecter en masse, comment auditer sans laisser de traces falsifiables, comment confier un outil aussi puissant à une institution sans mécanisme de contrôle externe effectif ?

Les réponses du FBI à ces questions étaient, en 2000, insatisfaisantes. Tous les opérateurs connectés comme « administrator ». Aucune piste d'audit fiable. Un système capable de capturer le trafic non filtré de l'ensemble des clients d'un ISP. Un incident antiterroriste classifié impliquant une collecte illégale suivi de la destruction des preuves légales. Et une évaluation indépendante dont les universités les plus réputées refusèrent de se charger faute de garanties suffisantes d'indépendance.

Vingt-cinq ans plus tard, la tension entre surveillance légale et collecte de masse ne s'est pas résolue : elle s'est simplement déplacée vers des architectures moins visibles. Les ISP intègrent désormais des capacités d'écoute légale dès la conception de leurs équipements, conformément aux exigences de la CALEA étendue aux réseaux IP en 2005. Les systèmes d'analyse de trafic profond (*deep packet inspection*) opèrent en permanence au cœur des infrastructures. Et la question que posait l'EPIC en 2000 — « Carnivore donne accès aux communications privées de tous les abonnés d'un fournisseur d'accès » — reste, sous une forme ou une autre, ouverte.

Ce qui a changé, c'est la visibilité. Carnivore était une boîte qu'on voyait arriver dans la salle machine. Ce qui lui a succédé, on ne le voit plus.

Références

[1] Associated Press. FBI Ditches Carnivore Surveillance System. Anglais. Annonce officielle de l'abandon de Carnivore, publiée par Fox News via AP. Jan. 2005.

[2] Steven M. Bellovin et al. Comments on the Carnivore System Technical Review. Anglais. AT&T Labs Research, Université de Pennsylvanie, SRI International, Purdue University CERIAS. Déc. 2000.

[3] Andrew Crocker et Nate Cardozo. CALEA. Anglais. Electronic Frontier Foundation. Historique du Communications Assistance for Law Enforcement Act de 1994 et de ses extensions successives. Août 2018.

[4] Electronic Privacy Information Center (EPIC). EPIC Carnivore Page. Anglais. Archive complète de la procédure FOIA contre le FBI, 2000–2005. 2000.

[5] Electronic Privacy Information Center (EPIC). FBI's Carnivore System Disrupted Anti-Terror Investigation. Anglais. Communiqué de presse révélant l'incident de mars 2000 lors d'une opération de l'unité Ben Laden du FBI. Mai 2002.

[6] Thomas C. Greene. How Carnivore Works. Anglais. The Register. Analyse technique de l'interface Carnivore d'après le rapport IITRI. Déc. 2000.

[7] Pew Internet & American Life Project. Carnivore and Internet Surveillance. Anglais. Étude d'opinion sur la perception de Carnivore par le public américain en 2001. Avr. 2001.

[8] Deborah S. Pierce. EFF Position on FBI "Carnivore" Snooping System. Anglais. EFFector vol. 13 n° 6. Témoignage de l'EFF devant le Sous-comité sur la Constitution, 28 juillet 2000. Août 2000.

[9] Stephen P. Smith et al. Independent Technical Review of the Carnivore System — Final Report. Anglais. Technical Report IITRI CR-030-216. Commandé par le Département de Justice américain. Contrat n° 00-C-0328. IIT Research Institute (IITRI), déc. 2000.

[10] David L. Sobel et Marc Rotenberg. Complaint for Injunctive Relief — EPIC v. Department of Justice. Anglais. Civil Action déposée devant l'United States District Court for the District of Columbia. Juill. 2000.

[11] United States House of Representatives, Subcommittee on the Constitution. Fourth Amendment Issues Raised by the FBI's "Carnivore" Program. Anglais. Audition du Sous-comité sur la Constitution, Committee on the Judiciary. Juill. 2000.