Blue Coat Systems
Surveillance web et censure de 2011 à 2013

Stéphane FOSSE
fosse.fr

2 février 2026

En octobre 2011, le collectif hacktiviste Telecomix publie 54 gigaoctets de logs extraits d'équipements de filtrage actifs en Syrie. Ces fichiers portent la signature d'une entreprise californienne jusqu'alors peu connue du grand public : Blue Coat Systems. L'affaire déclenche une enquête internationale qui révèle la présence de ces technologies de surveillance dans 83 pays, dont trois soumis à embargo américain.

Blue Coat Systems, basée à Sunnyvale en Californie, fabrique des *appliances* réseau destinées officiellement à l'optimisation et à la sécurité des infrastructures. Ses produits phares, ProxySG et PacketShaper, permettent de filtrer le trafic web, d'inspecter les connexions chiffrées SSL et de surveiller en temps réel plus de 600 applications. L'entreprise revendique plus de 15 000 clients dans le monde et dispose de bureaux en Amérique latine, au Moyen-Orient et en Asie-Pacifique. Ce qui fait la force commerciale de ces équipements fait aussi leur danger : les mêmes fonctionnalités qui protègent un réseau d'entreprise peuvent servir à censurer l'opposition politique et traquer les dissidents.

1 La découverte de 2011 : des proxies américains au service de la répression syrienne

L'histoire commence en août 2011, quelques mois après le début du soulèvement syrien contre le régime de Bachar el-Assad. Le site français Reflets.info, en collaboration avec Telecomix et Fhimt.com, publie une série d'articles documentant la présence d'équipements Blue Coat sur le réseau de Syrian Telecommunications Establishment. Les tests sont réalisés depuis l'intérieur du pays. Le 4 octobre 2011, Telecomix diffuse les logs de sept proxies SG-9000 couvrant neuf jours d'activité jusqu'au 4 août. Ces fichiers contiennent les traces de navigation de millions d'utilisateurs syriens.

Blue Coat nie d'abord toute implication. Le porte-parole Steve Schick déclare au Washington Post que l'entreprise ne vend pas à la Syrie et respecte les lois américaines sur l'exportation. Mais le 29 octobre 2011, face aux preuves accumulées, Blue Coat change de discours. Dans un article du Wall Street Journal, le vice-président Steve Daheb reconnaît que 13 appareils initialement expédiés via un distributeur de Dubaï vers le ministère irakien des Communications ont atterri en Syrie. L'entreprise admet que ces équipements communiquaient avec ses serveurs, mais affirme ne pas surveiller leur localisation géographique.

Le Citizen Lab, laboratoire de recherche de l'Université de Toronto spécialisé dans les technologies de surveillance, mène sa propre investigation. Ses chercheurs identifient des appareils Blue Coat sur quatre adresses IP supplémentaires appartenant à Syrian Telecommunications Establishment, portant le total bien au-delà des 13 reconnus officiellement. Les certificats de sécurité de ces machines les identifient comme des Blue Coat SG8100 Series. Les en-têtes HTTP confirment la présence d'appliances « BlueCoat-Security-Appliance » et de « NetCache appliance », une gamme rachetée par Blue Coat à Network Appliance en 2006.

2 Une tentative d'effacement des traces

Ce qui frappe les chercheurs du Citizen Lab, c'est la réaction des opérateurs syriens après la publication des logs par Telecomix. Un système de monitoring réseau accessible publiquement sur une adresse IP de la Syrian Computer Society affichait jusqu'alors les statistiques de trafic d'appareils clairement identifiés appelés BlueCoat ou NetApp (je passe la divulgation des adresses IP qui n'apportera rien à l'histoire). Entre le 14 et le 18 octobre 2011, quelqu'un renomme ces équipements. « BlueCoat » devient « Blue » ou « Bue ». « NetApp » devient « Net ». L'historique du trafic, qui remontait parfois à février 2011, est purgé : toutes les courbes recommencent au 17 octobre.

Cette tentative d'obfuscation, aussi maladroite soit-elle, suggère une volonté délibérée de masquer l'origine des équipements. Elle pose aussi une question troublante : qui a procédé à ces modifications ? Les administrateurs syriens, Blue Coat elle-même via un accès distant, ou un intermédiaire ?

3 La Birmanie : même technologie, même usage

Le Citizen Lab ne se limite pas à la Syrie. Ses chercheurs découvrent des indices convergents de la présence d'équipements Blue Coat en Birmanie, pays alors sous dictature militaire et également soumis à sanctions américaines. Trois éléments étayent cette conclusion.

D'abord, les noms d'hôtes du fournisseur d'accès Yatanarpon Teleport correspondent exactement aux produits Blue Coat. Ces appellations reprennent les noms des modules complémentaires de la gamme ProxySG. Ensuite, les messages d'erreur affichés lors de tentatives d'accès à des sites bloqués en Birmanie sont identiques, mot pour mot, à ceux observés en Syrie et documentés dans les forums de support Blue Coat comme texte par défaut des appliances ProxySG. Enfin, et c'est l'élément le plus accablant, la corrélation entre les catégories de filtrage Blue Coat et les URL bloquées en Birmanie atteint 98,8%. Les chercheurs ont testé 1 669 URL depuis le pays. Sur les 330 appartenant aux dix catégories suspectées d'être entièrement bloquées (pornographie, LGBT, éducation sexuelle, contenu adulte, nudité, botnets, email, hacking, contournement de proxy), 326 étaient inaccessibles. Une telle correspondance est-ell fortuite ?

4 83 pays, trois rapports, une cartographie mondiale

Entre 2011 et 2013, le Citizen Lab publie trois rapports majeurs sur Blue Coat. Le premier, « Behind Blue Coat » de novembre 2011, documente la Syrie et la Birmanie. Le second, « Planet Blue Coat » de janvier 2013, identifie 61 appareils ProxySG et 316 PacketShaper à travers le monde en utilisant le moteur de recherche Shodan et des scans réseau. Le troisième, « Some Devices Wander by Mistake : Planet Blue Coat Redux » de juillet 2013, affine la méthodologie et confirme la présence d'équipements Blue Coat sur les réseaux publics de 83 pays.

Parmi ces pays figurent l'Iran, la Syrie et le Soudan, tous trois sous embargo américain. On trouve également les six États du Conseil de coopération du Golfe (sauf Oman), l'Égypte post-révolution, la Russie, la Chine, le Venezuela, la Turquie, la Thaïlande, la Malaisie, l'Indonésie, Singapour, la Corée du Sud, l'Afghanistan et l'Irak en reconstruction. Dans chacun de ces pays, les équipements ont été détectés sur des réseaux de fournisseurs d'accès ou d'organismes gouvernementaux, pas sur des infrastructures privées d'entreprises.

Le cas saoudien illustre parfaitement l'ambiguïté de ces déploiements. Blue Coat affiche sur ses supports marketing le King Abdulaziz City for Science and Technology (KACST) comme « success story » client. Or le KACST gère précisément le filtrage national de l'Internet saoudien, bloquant contenus politiques, religieux et relatifs aux droits humains sur ordre du ministère de l'Intérieur.

5 Les conséquences juridiques et l'amende de 2013

Dès novembre 2011, les sénateurs américains Mark Kirk et Bob Casey demandent au département du Commerce d'enquêter sur Blue Coat et NetApp, une autre entreprise dont le matériel de stockage équipait le système de surveillance syrien Asfador développé par l'italien Area SpA. En décembre 2011, le Bureau of Industry and Security (BIS) ajoute à sa « Entity List » un individu et une société des Émirats arabes unis pour avoir acheté des équipements Blue Coat et les avoir réexportés vers la Syrie en violation de l'Executive Order 13582 du 17 août 2011.

En avril 2013, le couperet tombe : Computerlinks FZCO, le distributeur émirati par lequel sont passés les appareils, écope d'une amende de 2,8 millions de dollars. Blue Coat elle-même n'est pas sanctionnée. L'entreprise a coupé les mises à jour et l'accès au service cloud WebPulse pour les appareils syriens, les laissant « fonctionner de manière autonome » selon ses propres termes. Elle affirme ne pas disposer de « kill switch » pour désactiver ses équipements à distance.

Une expérience menée par le Citizen Lab en juillet 2012 tend à confirmer que les appareils syriens ne « téléphonaient plus à la maison ». Les chercheurs ont créé des sites web de contournement, les ont soumis au service de catégorisation Blue Coat, puis ont vérifié leur accessibilité depuis la Syrie. Les sites catégorisés comme « Proxy Avoidance » restaient accessibles, suggérant que les appareils ne recevaient plus les mises à jour de la base de données. En parallèle, les domaines liés à Blue Coat (bluecoat.com, cfauth.com) étaient eux-mêmes bloqués depuis la Syrie.

6 Un problème qui dépasse Blue Coat

L'affaire Blue Coat s'inscrit dans un marché de la surveillance numérique estimé à plus de 5 milliards de dollars en 2011. Reporters Sans Frontières a classé Blue Coat parmi les cinq « ennemis de l'Internet » dans son rapport spécial de mars 2013, aux côtés d'Amesys, Gamma International, Hacking Team et Trovicor. Ces entreprises partagent un modèle commun : des technologies « dual-use » développées dans des pays démocratiques, vendues à des régimes autoritaires via des intermédiaires parfois complaisants.

Le terme « dual-use », dans le jargon du contrôle des exportations, désigne traditionnellement les biens à usage civil et militaire. Appliqué aux technologies de l'information, il recouvre une réalité plus floue. Un proxy de filtrage web protège légitimement un réseau d'entreprise contre les malwares. Le même équipement, déployé à l'échelle nationale par un gouvernement autoritaire, devient un outil de censure politique et de surveillance de masse. La différence tient à l'acheteur et à l'usage, pas au produit.

Cette ambiguïté complique considérablement la régulation. L'arrangement de Wassenaar, qui coordonne les contrôles à l'exportation entre 42 pays, couvre les technologies de chiffrement et certains équipements d'interception. Mais les proxies de filtrage web échappent largement à son champ d'application. L'Electronic Frontier Foundation préconise une approche « Know Your Customer » : plutôt que de lister des technologies, obliger les vendeurs à enquêter sur leurs clients. Blue Coat elle-même n'a jamais répondu aux questions posées par le Citizen Lab sur ses procédures de due diligence en matière de droits humains.

7 Ce qui reste après la découverte

Blue Coat Systems a été rachetée par Bain Capital en 2015 pour 2,4 milliards de dollars, puis par Symantec en 2016 pour 4,65 milliards. La marque a progressivement disparu, absorbée dans la division Enterprise Security de Symantec, elle-même acquise par Broadcom en 2019. Les équipements ProxySG et PacketShaper existent toujours sous d'autres appellations.

Quant aux personnes surveillées, leur nombre reste impossible à établir précisément. Les 54 gigaoctets de logs syriens couvrent neuf jours de trafic sur sept proxies. L'analyse de ces fichiers par des chercheurs indépendants a révélé les habitudes de navigation de centaines de milliers d'utilisateurs : sites d'information consultés, réseaux sociaux fréquentés, tentatives de contournement de la censure. Amnesty International et Human Rights Watch ont documenté des cas d'activistes syriens torturés après avoir été identifiés grâce à leur activité en ligne. Le lien direct avec les équipements Blue Coat n'a jamais été formellement établi, mais la corrélation temporelle et technique laisse peu de place au doute.

L'affaire Blue Coat a au moins produit un effet durable : elle a mis en lumière l'existence d'une industrie de la surveillance commerciale longtemps restée dans l'ombre. Les recherches du Citizen Lab sur FinFisher, Hacking Team puis le groupe NSO s'inscrivent dans cette continuité. La question posée en 2011 reste ouverte : comment empêcher que des technologies développées dans des démocraties servent à réprimer ailleurs ?

Références

[1] Electronic Frontier Foundation. 'Know Your Customer' Standards for Sales of Surveillance Equipment. Oct. 2011.

[2] Sari Horwitz. Syria using American software to censor Internet, experts say. In : *Washington Post* (oct. 2011).

[3] Reflets.info. BlueCoat's role in Syrian censorship and nationwide monitoring system. Sept. 2011.

[4] Reporters Sans Frontières. The Enemies of the Internet Special Edition: Surveillance. Mars 2013.

[5] Telecomix. Syrian Blue Coat device logs. Oct. 2011.

[6] The Citizen Lab. Behind Blue Coat: Investigations of Commercial Filtering in Syria and Burma. Nov. 2011.

[7] The Citizen Lab. Planet Blue Coat: Mapping Global Censorship and Surveillance Tools. Jan. 2013.

[8] The Citizen Lab. Some Devices Wander by Mistake: Planet Blue Coat Redux. Juill. 2013.

[9] U.S. Department of Commerce Bureau of Industry and Security. BIS Adds Two Parties to Entity List for Sending Internet Filtering Equipment to Syria. Déc. 2011.

[10] Jennifer Valentino-Devries, Paul Sonne et Nour Malas. U.S. Firm Acknowledges Syria Uses Its Gear to Block Web. In : *Wall Street Journal* (oct. 2011).