Opération Socialist : quand le GCHQ britannique espionne son allié belge

Stéphane FOSSE
fosse.fr

14 février 2026

Entre 2010 et 2013, le Government Communications Headquarters britannique, le GCHQ, a infiltré l'infrastructure de Belgacom, le principal opérateur de télécommunications belge, dans le cadre d'une opération baptisée « Socialist ». Cette intrusion, révélée en 2013 par Edward Snowden, constitue le premier cas documenté d'un pays de l'Union européenne lançant une cyberattaque contre l'infrastructure critique d'un autre État membre.

Belgacom n'était pas une cible ordinaire. L'entreprise, partiellement détenue par l'État belge, compte parmi ses clients la Commission européenne, le Conseil européen et le Parlement européen. Sa filiale Belgacom International Carrier Services, ou BICS, opère l'un des plus importants hubs d'itinérance mobile au monde. Quand un voyageur utilise son téléphone en Europe, il y a de fortes chances que sa communication transite par les réseaux de BICS.

L'été 2012, des employés de Belgacom remarquent des anomalies dans leurs systèmes. Les serveurs de messagerie ne répondent plus correctement. Il faut attendre juin 2013 pour que les équipes de sécurité identifient l'ampleur du problème. Les ordinateurs de l'entreprise sont infectés par un malware qui se fait passer pour un logiciel Microsoft légitime. Le virus vole des données et les transmet vers des serveurs distants.

Un malware d'État d'une sophistication inédite

Le 16 septembre 2013, Belgacom publie un communiqué rassurant. L'intrusion a été détectée, le nettoyage est en cours, aucune donnée client n'a été compromise. Quatre jours plus tard, le magazine allemand Der Spiegel publie des documents issus des archives d'Edward Snowden. Le coupable n'est pas la NSA américaine comme beaucoup le soupçonnaient, mais le GCHQ britannique.

Les présentations classifiées du GCHQ révèlent que l'opération Socialist visait à améliorer l'exploitation de Belgacom et à cartographier son infrastructure. Les documents montrent que l'agence britannique avait accès aux systèmes de Belgacom depuis 2010, via sa filiale BICS. Le chef du Network Analysis Centre du GCHQ qualifie l'opération de « succès ».

En novembre 2014, les chercheurs de Symantec publient un rapport technique sur un malware qu'ils baptisent Regin. Il s'agit de l'outil le plus sophistiqué qu'ils aient jamais analysé, comparable à Stuxnet, le virus développé conjointement par les États-Unis et Israël pour saboter le programme nucléaire iranien. Ronald Prins, fondateur de Fox-IT, la société néerlandaise chargée de nettoyer les systèmes de Belgacom, confirme que Regin est bien le malware utilisé lors de l'attaque. « C'est le malware le plus sophistiqué que j'ai jamais étudié », déclare-t-il à The Intercept.

Regin fonctionne par étapes. Cinq couches chiffrées s'empilent, chacune révélant peu d'informations sur l'ensemble. Pour comprendre le malware, il faut récupérer les cinq étapes. L'architecture modulaire permet d'adapter les capacités à chaque cible. Un module surveille le trafic des serveurs web Microsoft IIS, un autre collecte les données des stations de base GSM, un troisième extrait les emails des bases Exchange. Certaines traces du code remontent à 2003, mais Symantec identifie deux versions majeures. La première, active entre 2008 et 2011, disparaît brutalement. La seconde réapparaît en 2013.

Le malware ne stocke pas de fichiers multiples sur le système infecté. Il utilise son propre système de fichiers virtuel chiffrés, contenu dans un unique fichier au nom anodin. Les fichiers internes sont identifiés par des codes numériques, pas par des noms. Regin communique avec ses serveurs de commande via ICMP, des commandes dissimulées dans les cookies HTTP, ou des protocoles TCP et UDP personnalisés. Frank Groenewegen, chercheur chez Fox-IT, témoigne que le virus représente une avancée technique majeure.

Quantum Insert : l'ingénierie sociale portée à son paroxysme

Comment infecte-t-on des ingénieurs expérimentés qui travaillent pour un opérateur de télécommunications ? Le GCHQ a utilisé une technique baptisée Quantum Insert, développée en partenariat avec la NSA américaine.

Les espions britanniques commencent par identifier les employés de Belgacom qui travaillent dans la maintenance réseau et la sécurité. Ils repèrent lesquels utilisent LinkedIn ou Slashdot. Ensuite, ils préparent des copies exactes de ces sites web, auxquelles ils ajoutent un élément invisible : un petit morceau de malware qui transforme l'ordinateur de la victime en outil d'espionnage.

La méthode Quantum Insert repose sur une course de vitesse. Le GCHQ place des serveurs ultra-rapides à des points stratégiques du backbone Internet. Quand la cible demande à accéder à LinkedIn, ces serveurs interceptent la requête. Si le serveur du GCHQ répond plus vite que le véritable LinkedIn, même d'une milliseconde seulement, le navigateur de la victime affiche la page piégée. La page légitime arrive ensuite, mais le navigateur l'ignore. Le malware est déjà installé.

Dans le cas de Belgacom, trois ingénieurs ont été ciblés. Leurs machines leur donnaient un « bon accès » aux parties sensibles de l'infrastructure, selon les termes mêmes des documents du GCHQ. Une fois ces ordinateurs compromis, les espions britanniques ont pu progresser dans le réseau. L'attaque s'est déroulée par étapes entre 2010 et 2011, pénétrant toujours plus profondément dans les systèmes de Belgacom.

Les enquêteurs ont découvert que les routeurs centraux de Belgacom, fabriqués par Cisco, avaient également été infectés. Ces équipements constituent le cœur du réseau. Ils traitent d'énormes volumes de communications privées. Leur compromission permettait au GCHQ d'intercepter le trafic avant même qu'il soit chiffré, contournant ainsi la protection des VPN. L'agence britannique pouvait également localiser des téléphones mobiles via le protocole GPRS 2G et lancer des attaques de type « man-in-the-middle » contre les smartphones des cibles.

Objectifs stratégiques : bien au-delà du terrorisme

Le GCHQ voulait espionner les téléphones utilisés par des cibles lors de leurs déplacements en Europe. Mais l'agence avait un objectif plus large. Une fois infiltrée dans Belgacom, elle prévoyait de compromettre les liaisons de données reliant Belgacom à ses partenaires internationaux, surveillant ainsi les communications entre l'Europe et le reste du monde. Une carte classifiée, baptisée « Belgacom_connections », illustre la portée géographique de l'entreprise en Europe, au Moyen-Orient et en Afrique du Nord.

La véritable cible était BICS. Cette filiale gère le système GRX, ou GPRS Roaming Exchange, qui permet aux utilisateurs de téléphones mobiles de se connecter lorsqu'ils voyagent à l'étranger. Il n'existe qu'une vingtaine de fournisseurs GRX dans le monde. Compromettre BICS donnait accès à un volume considérable de trafic d'itinérance, notamment en provenance du Moyen-Orient et d'Afrique. À l'époque, la pénétration des smartphones dans ces régions était bien plus faible qu'aujourd'hui, mais le trafic GPRS transitant par les hubs GRX restait massif.

Philippe Langlois, expert en réseaux mobiles, explique qu'avec un accès aux routeurs GRX, un service de renseignement peut lire l'intégralité des communications Internet d'une cible, tracer sa localisation et installer des logiciels espions sur son appareil. Cette approche contourne la fragmentation des centaines d'opérateurs mobiles mondiaux en visant les quelques dizaines de points de passage obligés.

Le GCHQ ne s'est pas arrêté à Belgacom. Les documents Snowden révèlent que l'agence a également ciblé les centres de compensation de facturation mobile internationale. Ces entreprises, peu connues du grand public, traitent les paiements entre opérateurs mobiles et accèdent ainsi à d'énormes volumes de métadonnées de connexion. Comfone, basée à Berne en Suisse, et Mach, rachetée depuis par Syniverse et Starhome, figurent en tête de liste. Pour Mach, le GCHQ avait identifié trois ingénieurs réseau à cibler en Inde. La même technique Quantum Insert a été déployée.

Une enquête judiciaire qui aboutit nulle part

Belgacom a investi plusieurs millions de dollars pour nettoyer ses systèmes et renforcer sa sécurité. Mais des sources proches de l'investigation estiment que le nettoyage n'a été que partiel. Certaines parties du malware du GCHQ n'auraient jamais été complètement supprimées. L'entreprise s'est rebaptisée Proximus en septembre 2014.

Le procureur fédéral belge a ouvert une enquête criminelle. Pendant cinq ans, les enquêteurs ont cherché des preuves matérielles au-delà des documents Snowden. En 2018, le quotidien belge De Standaard révèle qu'ils ont trouvé des adresses IP britanniques dans les communications du malware. Trois de ces adresses appartenaient à une entreprise britannique, indiquant que le gestionnaire du logiciel espion se trouvait au Royaume-Uni. Un rapport confidentiel du parquet fédéral belge, présenté au Conseil national de sécurité, conclut que le GCHQ a probablement espionné Belgacom sur ordre de ministres britanniques.

Quand les autorités belges demandent au Home Office britannique de coopérer avec l'enquête, la réponse est un refus catégorique. Le Royaume-Uni invoque sa souveraineté, sa sécurité et son ordre public. Cette absence de coopération n'a rien de surprenant. Pour des raisons diplomatiques évidentes, Londres ne va pas reconnaître avoir piraté l'un de ses plus proches alliés, un pays qui héberge les institutions clés de l'Union européenne et de l'OTAN.

Les enquêteurs belges savaient dès le départ qui était responsable. Mais ils voulaient construire leur propre dossier, avec leurs propres sources. Ils ont même envisagé d'interroger Edward Snowden comme témoin, pour qu'il authentifie les documents et fournisse son propre témoignage. Le procureur Frederic Van Leeuw a écarté cette option, jugée trop dommageable diplomatiquement. Snowden était en Russie, où il avait demandé l'asile. L'interroger aurait pu contrarier les États-Unis, un allié puissant dont la Belgique avait besoin pour lutter contre la menace terroriste islamiste en Europe.

Malgré l'indignation politique initiale, l'enquête s'est terminée sans sanction, sans compensation, sans arrestation, sans interrogatoire, sans excuse et sans admission de culpabilité. Le dossier a été transmis au Parlement belge et discrètement classé.

Quelle ampleur, combien de victimes ?

Quantifier précisément le nombre de personnes espionnées via l'opération Socialist reste impossible. Les documents révélés ne fournissent pas ces chiffres. Ce que l'on sait, c'est que le GCHQ a infecté plus de 120 systèmes informatiques chez Belgacom, dont jusqu'à 70 ordinateurs personnels d'employés. Selon les aveux de l'entreprise, 5 000 machines ont finalement été compromises.

Le trafic d'itinérance transitant par BICS concerne des millions d'utilisateurs de téléphones mobiles voyageant en Europe, au Moyen-Orient et en Afrique. Les clients de Belgacom incluent les institutions européennes, ce qui signifie que les communications de fonctionnaires, de diplomates et de responsables politiques de l'Union européenne ont potentiellement été interceptées. Mais il n'existe aucune liste publique des cibles effectivement surveillées.

Le malware Regin a été identifié dans dix pays. Symantec rapporte que 28

Aucune donnée n'a été revendue sur le dark web. L'opération Socialist était une opération de renseignement étatique, pas une attaque cybercriminelle. Les données collectées servaient à la surveillance stratégique et tactique menée par le GCHQ dans le cadre de l'alliance Five Eyes, qui regroupe les États-Unis, le Royaume-Uni, l'Australie, la Nouvelle-Zélande et le Canada. Ces agences partagent leurs renseignements. Ce que le GCHQ collectait via Belgacom était probablement accessible à la NSA américaine.

Un programme terminé ?

L'opération Socialist, dans sa configuration initiale, s'est achevée en 2013 lorsque Belgacom a découvert l'intrusion. Les systèmes ont été nettoyés, du moins en partie. Mais le programme QUANTUM, dont Quantum Insert fait partie, n'a jamais cessé. La NSA et le GCHQ continuent d'utiliser ces techniques contre d'autres cibles dans le monde.

Les documents Snowden de 2014 décrivent une vision à long terme du GCHQ : « N'importe quel appareil mobile, n'importe où, n'importe quand ! » Une présentation datée de 2012 indique que l'agence voulait augmenter sa capacité opérationnelle à déployer des implants à distance en connaissant uniquement le numéro de téléphone mobile de la cible, ce qu'elle qualifie de « game changing ».

Bruce Schneier, expert en sécurité informatique, a analysé les documents Snowden et constate que les techniques QUANTUM représentent un danger permanent. Les serveurs ultra-rapides du GCHQ et de la NSA restent positionnés sur le backbone Internet. Ils peuvent intercepter et rediriger le trafic vers des serveurs FOXACID, qui hébergent des exploits personnalisés. Selon une présentation interne de la NSA, le taux de succès des missions utilisant Quantum Insert atteint 80

Les entreprises de sécurité informatique ont identifié Regin dès 2011, mais elles n'ont rien dit publiquement avant novembre 2014. Microsoft a ajouté une détection de variantes de Regin à sa base de données de malwares le 9 mars 2011. F-Secure a découvert une version ancienne en 2009 sur le serveur d'un client en Europe du Nord. Kaspersky Lab suivait activement Regin depuis trois ans avant la publication de son rapport. Mikko Hyppönen, directeur de la recherche chez F-Secure, explique sur Twitter que des clients leur avaient demandé de ne pas divulguer publiquement le malware trouvé sur leurs réseaux. Fox-IT, qui a nettoyé les systèmes de Belgacom, déclare qu'elle ne voulait pas interférer avec les opérations de la NSA et du GCHQ.

Cette omerta soulève une question dérangeante. Les entreprises de cybersécurité ont pour mission de protéger leurs clients contre les menaces. Mais quand la menace provient d'un État, surtout un État allié, elles semblent préférer le silence. Symantec affirme qu'il lui a fallu un an pour analyser Regin avant de publier son rapport. En réalité, toutes ces entreprises attendaient simplement qu'une autre brise le silence.

Ce que l'opération Socialist révèle du fonctionnement des services de renseignement

L'opération Socialist illustre plusieurs réalités de l'espionnage moderne. D'abord, les frontières géographiques et politiques ne limitent pas les services de renseignement. Le Royaume-Uni et la Belgique sont des alliés au sein de l'OTAN et de l'Union européenne. Cela n'a pas empêché le GCHQ de pirater l'infrastructure critique belge.

Ensuite, les télécommunications constituent des cibles prioritaires. Compromettre un opérateur donne accès à des milliers, voire des millions de communications. Les routeurs GRX, les centres de facturation mobile et les points d'échange Internet sont des portes d'entrée vers le trafic mondial. Il n'existe que quelques dizaines de ces infrastructures critiques. Leur sécurisation devrait être une priorité stratégique pour tous les pays.

Troisièmement, la sophistication technique des malwares étatiques dépasse de loin celle des outils cybercriminels ordinaires. Regin représente des années de développement et des ressources considérables. Les entreprises et même les États de taille moyenne ne peuvent pas lutter à armes égales contre ces capacités.

Enfin, l'absence de conséquences juridiques ou diplomatiques pour le GCHQ montre que le droit international n'a pas suivi l'évolution du cyberespace. Il n'existe pas de mécanisme efficace pour sanctionner un État qui pirate un autre État, même entre alliés. La Belgique a tenté de faire respecter le droit. Elle a échoué.

Quant aux citoyens ordinaires, ils sont pris au milieu. Leurs communications transitent par des infrastructures que des services de renseignement étrangers peuvent avoir compromises. Ils ne le sauront probablement jamais. Et même s'ils le savaient, ils ne pourraient rien y faire. Le chiffrement de bout en bout devient la seule protection fiable, mais il ne protège pas contre l'interception des métadonnées, qui révèlent déjà beaucoup sur nos vies.

En 2018, Belgacom devenue Proximus a investi plus de 55 millions de dollars pour réformer ses procédures de sécurité interne. L'entreprise a créé une unité de cyberdéfense et recruté des « hackers éthiques » qui tentent régulièrement de pénétrer ses réseaux pour identifier les vulnérabilités. Ces mesures arrivent après la bataille. Mais dans le domaine de la cybersécurité, la prochaine bataille n'est jamais très loin.

Références

[1] A Socio-Technical Framework to Improve cyber security. In : *CEUR Workshop Proceedings*. T. 2398. 2019.

[2] Gareth Corfield. Belgium: Oi, Brits, explain why Belgacom hack IPs pointed at you and your GCHQ. The Register, oct. 2018.

[3] Ryan Gallagher. How U.K. Spies Hacked a European Ally and Got Away With It. The Intercept, fév. 2018.

[4] Ryan Gallagher. Operation Socialist: The Inside Story of How British Spies Hacked Belgium's Largest Telco. The Intercept, déc. 2014.

[5] Ryan Gallagher. Secret Malware in European Union Attack Linked to U.S. and British Intelligence. The Intercept, nov. 2014.

[6] Kaspersky Lab. The Regin Platform: Nation-State Ownage of GSM Networks. Whitepaper. Kaspersky Lab, nov. 2014.

[7] Laura Poitras et Der Spiegel Staff. Britain's GCHQ Hacked Belgian Telecoms Firm. Der Spiegel, sept. 2013.

[8] Laura Poitras et Der Spiegel Staff. Quantum Spying: GCHQ Used Fake LinkedIn Pages to Target Engineers. Der Spiegel, nov. 2013.

[9] Jack Rhysider. Operation Socialist. Darknet Diaries Podcast #48. 2019.

[10] Bruce Schneier. Regin Malware. Schneier on Security, déc. 2014.

[11] Symantec Security Response. Regin: Top-tier espionage tool enables stealthy surveillance. Whitepaper. Symantec, nov. 2014.