DROPOUTJEEP : l'implant NSA dans l'iPhone

Stéphane FOSSE
fosse.fr

15 février 2026

DROPOUTJEEP est un implant logiciel développé en 2008 par l'unité ANT de la National Security Agency américaine pour surveiller à distance les iPhone de première génération. Révélé fin décembre 2013 par le chercheur en sécurité Jacob Appelbaum, ce programme permettait d'accéder aux SMS, contacts, messagerie vocale, géolocalisation, et d'activer le microphone et la caméra sans que l'utilisateur ne s'en aperçoive.

Le 30 décembre 2013, lors de la 30ème édition du Chaos Communication Congress à Hamburg en Allemagne, Jacob Appelbaum présente une découverte qui fait l'effet d'une bombe dans la communauté de la sécurité informatique. Parmi un catalogue de 50 pages d'outils d'espionnage de la NSA, un document classifié « Top Secret » daté du 1er octobre 2008 décrit DROPOUTJEEP, un programme spécifiquement conçu pour compromettre l'iPhone d'Apple.

L'iPhone venait tout juste de sortir en juin 2007. Quatorze mois plus tard, la NSA disposait déjà d'un outil permettant un contrôle quasi-total de l'appareil. Le document technique est sans équivoque sur les capacités de l'implant : récupération des SMS, extraction de la liste de contacts, accès aux messages vocaux, géolocalisation via les antennes cellulaires, activation du microphone à distance pour capter les conversations environnantes, capture d'images via la caméra, et même la possibilité de transférer des fichiers dans les deux sens entre l'appareil compromis et les serveurs de la NSA.

L'ANT : l'arsenal secret de la NSA

DROPOUTJEEP n'est qu'une pièce d'un puzzle bien plus vaste. L'outil provient de l'unité ANT (Advanced Network Technology) de la NSA, une division spécialisée dans le développement d'implants matériels et logiciels destinés à l'espionnage. Cette unité travaille en soutien du TAO (Tailored Access Operations), le groupe d'élite de la NSA chargé de pénétrer les réseaux informatiques les plus protégés et d'accéder aux cibles les plus difficiles.

Le catalogue ANT révélé par Der Spiegel et Jacob Appelbaum présente un inventaire complet des outils disponibles pour les opérateurs de la NSA. On y trouve des câbles USB modifiés capables d'émettre et de recevoir des données par radiofréquence, des implants BIOS qui survivent au formatage complet d'un disque dur, des modifications de firmware pour disques durs Western Digital, Seagate et Samsung, ou encore des fausses antennes-relais GSM vendues 40 000 dollars l'unité.

L'ampleur des capacités techniques impressionne. Le TAO opère depuis un ancien site de fabrication de puces Sony à San Antonio au Texas. Ses équipes interceptent des colis contenant du matériel informatique en cours de livraison, installent discrètement des implants matériels ou logiciels, puis réexpédient les appareils modifiés à leurs destinataires sans que personne ne s'en aperçoive. Cette technique, appelée « interdiction » dans le jargon NSA, permet de compromettre des équipements avant même qu'ils n'arrivent chez leur propriétaire légitime.

Un taux de réussite troublant

Lors de sa présentation au 30C3, Jacob Appelbaum soulève une question qui dérange : « Pensez-vous qu'Apple les a aidés à construire ça ? Je ne sais pas. J'espère qu'Apple clarifiera. Je ne crois pas vraiment qu'Apple ne les ait pas aidés. Je ne peux pas encore le prouver, mais ils affirment littéralement que chaque fois qu'ils ciblent un appareil iOS, l'implantation réussira. » Cette affirmation, extraite du document NSA, laisse planer le doute sur une éventuelle collaboration ou, à tout le moins, sur l'existence de vulnérabilités majeures dans iOS que la NSA exploiterait sans les avoir signalées à Apple.

Le document classifié précise que l'installation initiale de DROPOUTJEEP nécessite des « méthodes d'accès rapproché » (*close access methods*). Autrement dit, l'implant ne peut pas être installé à distance en 2008. Un agent doit avoir un accès physique temporaire à l'iPhone ciblé. Mais le document ajoute qu'une « capacité

d'installation à distance sera poursuivie pour une version future ». On ignore si cette capacité a effectivement été développée dans les années suivantes.

Le statut du programme en octobre 2008 est indiqué comme « en développement », avec un coût unitaire de zéro dollar, ce qui suggère qu'il s'agit d'un outil purement logiciel ne nécessitant pas de composant matériel spécifique. Les communications entre l'implant et les serveurs NSA transitent de manière chiffrée et discrète, soit par SMS, soit par connexion de données GPRS, rendant leur détection particulièrement difficile.

La réaction d'Apple et le doute persistant

Le 31 décembre 2013, Apple publie un communiqué ferme : « Apple n'a jamais travaillé avec la NSA pour créer une porte dérobée dans aucun de nos produits, y compris l'iPhone. De plus, nous n'avons pas eu connaissance de ce programme NSA présumé ciblant nos produits. » La société ajoute qu'elle prend au sérieux la sécurité et la vie privée de ses utilisateurs, et qu'elle enquête systématiquement sur toute tentative de compromettre ses systèmes, « peu importe qui en est à l'origine ».

Cette déclaration pose autant de questions qu'elle n'en résout. Comme le note un analyste dans les discussions techniques qui suivent, donner le code source d'iOS à la NSA sans participer directement au développement de l'implant pourrait techniquement permettre à Apple de prétendre n'avoir « jamais travaillé avec la NSA ». La formulation soigneuse du communiqué laisse ce type d'interprétation ouverte.

Bruce Schneier, cryptographe reconnu internationalement, publie une analyse technique détaillée de DROPOUTJEEP en février 2014. Il souligne que le document date de 2008 et ne concerne que les premiers iPhone. La sécurité d'iOS a considérablement évolué depuis, notamment avec l'iPhone 3GS qui apporte des améliorations majeures. Schneier rappelle cependant que l'existence même de ce programme témoigne de l'intention et de la capacité de la NSA à compromettre les iPhone. Rien ne permet d'affirmer que ces travaux se sont arrêtés en 2008.

Les limites du chiffrement de bout en bout

L'équipe de 1Password, éditeur d'un gestionnaire de mots de passe réputé, publie une analyse pragmatique des implications de DROPOUTJEEP pour la sécurité des données. Leur conclusion est sans appel : une fois le système d'exploitation compromis, aucune application ne peut garantir la sécurité des informations qu'elle traite. DROPOUTJEEP pouvait extraire les fichiers chiffrés de 1Password depuis l'iPhone, même si l'implant ne permettait probablement pas de capturer directement le mot de passe maître en mémoire.

Cette limitation technique illustre un principe fondamental de la sécurité informatique : le chiffrement de bout en bout protège les données en transit et au repos, mais devient inopérant si l'une des deux « extrémités » est sous le contrôle d'un attaquant. DROPOUTJEEP représente exactement ce type de menace. L'implant s'exécute au niveau du système d'exploitation, en amont de toutes les protections logicielles mises en place par les applications.

Un second lanceur d'alerte

Une question demeure : d'où provient le catalogue ANT ? Contrairement à ce qu'on pourrait croire, il ne fait probablement pas partie des documents divulgués par Edward Snowden. Bruce Schneier affirme sur son blog ne pas avoir trouvé de référence au catalogue ANT dans l'archive Snowden à laquelle il a eu accès. James Bamford, journaliste spécialisé dans les agences de renseignement américaines, arrive à la même conclusion après avoir consulté l'intégralité des documents fournis par Snowden.

L'hypothèse d'une seconde source s'impose. Un autre employé ou contractant de la NSA aurait transmis ces documents à Jacob Appelbaum ou directement à Der Spiegel. Cette multiplicité des fuites témoigne d'un malaise profond au sein même de l'agence, où certains agents considèrent que les programmes de surveillance dépassent les limites acceptables.

Que sait-on des victimes ?

Contrairement aux programmes de surveillance de masse comme PRISM qui aspirent des données sur des centaines de millions de personnes, DROPOUTJEEP relève de la surveillance ciblée. L'installation nécessitant un accès physique à l'appareil en 2008, le nombre de cibles reste forcément limité. Les documents publiés ne révèlent ni le nombre de personnes infectées, ni leur identité, ni leur localisation géographique.

On peut néanmoins établir un profil des cibles potentielles. Le TAO est décrit dans les documents internes comme l'unité qui « obtient l'inaccessible ». Elle intervient sur les cibles jugées prioritaires et difficiles d'accès

par les moyens conventionnels. Il s'agit vraisemblablement de personnalités politiques étrangères, de dirigeants d'entreprises stratégiques, de diplomates, de journalistes, ou de militants que la NSA ne peut surveiller par les canaux habituels.

Aucune donnée personnelle volée via DROPOUTJEEP n'a fait surface sur le dark web. La NSA n'est pas une organisation criminelle qui commercialise les informations qu'elle collecte. Elle les exploite pour ses propres besoins de renseignement et les partage éventuellement avec ses partenaires des Five Eyes (Royaume-Uni, Canada, Australie, Nouvelle-Zélande). Les données restent classifiées et ne circulent que dans des canaux contrôlés.

Le programme est-il toujours actif ?

Rien dans les documents publiés ne permet d'affirmer que DROPOUTJEEP a été abandonné. Le document de 2008 mentionne explicitement que des versions futures poursuivront une « capacité d'installation à distance ». La NSA dispose de budgets considérables et emploie certains des meilleurs hackers du pays. Il serait naïf de penser qu'elle a renoncé à compromettre les iPhone alors que ces appareils sont devenus omniprésents chez les cibles qui l'intéressent.

La sécurité d'iOS a progressé. Le chiffrement matériel, l'Enclave sécurisée introduite avec l'iPhone 5S, les mises à jour régulières du système, et la politique restrictive d'Apple vis-à-vis des applications tierces ont considérablement rehaussé le niveau de protection. Mais dans le même temps, la NSA a continué à développer ses capacités offensives. Le jeu du chat et de la souris se poursuit.

Les révélations de 2013 ont au moins eu un effet bénéfique : elles ont poussé Apple et les autres fabricants à renforcer la sécurité de leurs systèmes d'exploitation. Apple a multiplié les fonctionnalités de protection, notamment le mode de verrouillage USB qui empêche l'accès aux données de l'iPhone via le port Lightning si l'appareil est resté verrouillé plus d'une heure. Ces évolutions techniques rendent l'implantation d'outils comme DROPOUTJEEP plus complexe, sans pour autant la rendre impossible.

Un gouvernement « black hat »

L'équipe de 1Password formule une accusation qui résume bien le problème éthique posé par DROPOUTJEEP : « Si le gouvernement américain a connaissance de vulnérabilités dans iOS ou dans tout autre système et qu'il ne les divulgue pas à Apple, nous n'avons absolument pas d'autre choix que de considérer le gouvernement américain comme un acteur malveillant. »

Cette position tranche avec la rhétorique habituelle de la NSA qui se présente comme le défenseur de la sécurité nationale. En accumulant des vulnérabilités zero-day sans les signaler aux éditeurs de logiciels, l'agence affaiblit la sécurité de tous les utilisateurs de ces systèmes. Les mêmes failles que la NSA exploite peuvent être découvertes indépendamment par des États hostiles ou des groupes criminels. Chaque vulnérabilité gardée secrète devient un risque pour l'ensemble de l'écosystème numérique.

Le débat dépasse largement le cadre technique. Il pose la question du rôle acceptable d'une agence de renseignement dans une démocratie. Jusqu'où peut-on aller au nom de la sécurité nationale ? La NSA a-t-elle le droit de saboter délibérément la sécurité des produits américains pour faciliter ses opérations d'espionnage, y compris contre des alliés ? Les révélations sur DROPOUTJEEP et le catalogue ANT ont alimenté une réflexion de fond sur ces questions, sans pour autant apporter de réponses définitives.

Treize ans après la création de DROPOUTJEEP, le programme reste un symbole de l'ambition démesurée de la NSA et de sa volonté de pénétrer tous les systèmes, y compris ceux fabriqués par les entreprises américaines. Les documents classifiés de 2008 ne nous disent rien de l'état actuel des capacités de l'agence contre iOS, mais ils rappellent que la surveillance de masse et la surveillance ciblée se complètent dans une architecture globale de collecte du renseignement où rien n'échappe vraiment au regard des agences.

Références

[1] Jacob Appelbaum. To Protect And Infect, Part 2 - The Militarization of the Internet. In : *30th Chaos Communication Congress*. Transcription disponible à https://www.nakedcapitalism.com/2014/01/jacob-appelbaum-30c3-protect-infect-militarization-internet-transcript.html. Hamburg, déc. 2013.

[2] Jacob Appelbaum et al. Inside TAO: Documents Reveal Top NSA Hacking Unit. In : *Der Spiegel* (déc. 2013).

[3] Jacob Appelbaum et al. NSA's Secret Toolbox: Unit Offers Spy Gadgets for Every Need. In : *Der Spiegel* (déc. 2013).

[4] Bill Chappell. Report Details NSA's Alleged High-Tech Tricks For Snaring Data. In : *NPR* (déc. 2013).

[5] Graham Cluley. DROPOUTJEEP. Can the NSA spy on every iPhone on the planet? Fév. 2014.

[6] DROPOUTJEEP ANT Product Data. Rapp. tech. Document classifié TOP SECRET. National Security Agency, oct. 2008.

[7] Jeffrey Goldberg. The NSA can do what to my iPhone? 1Password Blog, jan. 2014.

[8] David Lyon. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. In : *Big Data & Society* 1.2 (juill. 2014).

[9] Bruce Schneier. DROPOUTJEEP: NSA Exploit of the Day. Schneier on Security, fév. 2014.

[10] Joseph Verble. The NSA and Edward Snowden: surveillance in the 21st century. In : *ACM SIGCAS Computers and Society* 44.3 (2014).