Project Raven : des ex-agents NSA au service de la surveillance émiratie

Stéphane FOSSE
fosse.fr

8 février 2026

Project Raven est un programme de cyberespionnage offensif opéré depuis Abu Dhabi entre 2009 et 2019 par d'anciens agents de la National Security Agency américaine, pour le compte du renseignement émirati. Révélé au grand public par les journalistes Christopher Bing et Joel Schectman de Reuters en janvier 2019, ce programme a ciblé des centaines de personnes à travers le monde — militants des droits humains, journalistes, opposants politiques, chefs d'État étrangers — au moyen d'exploits zero-click capables de compromettre des iPhone sans la moindre action de la victime.

Pour qui s'intéresse à l'architecture des systèmes de surveillance étatiques, Project Raven est un cas d'école. On y trouve tout : l'externalisation de compétences offensives à des mercenaires cyber, l'acquisition d'exploits zero-day sur un marché gris florissant, une chaîne de commandement volontairement opaque, et un cadre juridique suffisamment vague pour que des citoyens américains puissent espionner le monde entier pendant une décennie avant que quiconque ne soit inquiété. L'affaire illustre aussi, de façon brutale, ce qui arrive quand les outils de la contre-ingérence se retournent contre les personnes qu'ils étaient censés protéger.

De DREAD à DarkMatter : genèse d'un programme de surveillance

L'histoire commence en 2008-2009. Les Émirats arabes unis, fédération de sept émirats peuplée de neuf millions d'habitants, souhaitent se doter de capacités cyber offensives comparables à celles des grandes puissances. Le pays n'a pas le vivier technique pour le faire seul. Il se tourne vers CyberPoint, un petit sous-traitant de cybersécurité basé à Baltimore, fondé par Karl Gumtow en 2009, dont les clients comptent déjà le département de la Défense américain.

CyberPoint obtient du Département d'État américain, via la Directorate of Defense Trade Controls, une autorisation d'exportation de services de défense encadrée par l'ITAR (International Traffic in Arms Regulations). Le document autorise explicitement CyberPoint à travailler avec la NESA (National Electronic Security Authority, l'équivalent émirati de la NSA) pour la « protection de la souveraineté des EAU » à travers la « collecte d'informations issues de systèmes de communication à l'intérieur et à l'extérieur des EAU » et l'« analyse de surveillance ». Une clause interdit formellement de cibler des citoyens américains ou des entreprises américaines.

Le programme reçoit le nom de code DREAD (Development Research Exploitation Analysis Department) côté émirati. Côté américain, les opérateurs l'appellent Project Raven. L'équipe s'installe dans une villa convertie en centre opérationnel à Abu Dhabi — serveurs, salle d'opérations, salle de conférence, équipe de ciblage — et recrute progressivement plus d'une douzaine d'anciens agents de la NSA et du renseignement militaire américain. Les salaires sont attractifs : plus de 200 000 dollars par an pour les analystes, au-delà de 400 000 dollars pour certains managers.

Chaque nouvel arrivant passe par deux briefings successifs. Le « Purple Briefing » présente une mission défensive : déployer des pare-feu, des systèmes de détection d'intrusion. C'est une couverture. Immédiatement après, le « Black Briefing » révèle la réalité : Project DREAD est la « division opérationnelle offensive de la NESA » et « ne sera jamais reconnu publiquement ». Le schéma est classique dans le renseignement. Pour quelqu'un qui sort de la NSA, ces compartimentages n'ont rien de surprenant.

L'arsenal technique : Karma, exploits zero-click et compromission d'iPhone

Les premiers mois, Project Raven se concentre sur du renseignement anti-terroriste. Les cibles sont des cellules de l'État islamique actives dans la région. L'opération contribue, selon les anciens opérateurs, à évaluer les

menaces après l'attaque au couteau d'Abu Dhabi en 2014, où un militant affilié à Daech a poignardé mortellement une enseignante. Techniquement, les méthodes restent conventionnelles : reconnaissance de périmètre, exploitation de mots de passe par défaut sur des portails VPN gouvernementaux, mouvement latéral via Active Directory, exfiltration d'emails.

Tout change en 2016 avec l'acquisition de Karma, un outil de compromission d'iPhone dont le vendeur reste inconnu à ce jour. Karma exploite une vulnérabilité zero-day dans Apple iMessage pour transformer un simple numéro de téléphone ou une adresse email en point d'entrée total sur l'appareil de la cible. L'opérateur entre l'identifiant, Karma envoie un message invisible, et l'iPhone livre ses contacts, ses SMS, ses photos, sa géolocalisation — le tout sans aucun clic de la victime. C'est un exploit zero-click dans sa forme la plus pure. Il ne fonctionne que sur iOS et ne donne pas accès aux appels téléphoniques, mais pour le renseignement de signaux, c'est amplement suffisant.

En 2016 et 2017, Karma est utilisé contre des centaines de cibles à travers le Moyen-Orient et l'Europe : gouvernements du Qatar, du Yémen, d'Iran et de Turquie. Parmi les personnes compromises figurent l'émir du Qatar, Sheikh Tamim bin Hamad al-Thani, une ancienne vice-première ministre turque, Tawakkol Karman, lauréate du prix Nobel de la Paix yéménite, et — selon l'ouvrage de Nicole Perlroth, journaliste au New York Times — l'ancienne Première dame américaine Michelle Obama. Un correctif Apple diffusé en 2017 réduit l'efficacité de Karma, mais une seconde version, Karma 2, est développée par la suite.

En parallèle, les EAU utilisent d'autres outils commerciaux de surveillance. Le rapport du Citizen Lab de l'université de Toronto, publié en août 2016 par Bill Marczak et John Scott-Railton, documente l'usage du spyware Pegasus de la société israélienne NSO Group contre Ahmed Mansoor, militant émirati des droits humains. L'attaque repose sur une chaîne de trois exploits zero-day iOS baptisée « Trident », déclenchée par un simple clic sur un lien envoyé par SMS. Le coût estimé de cette chaîne d'exploits dépasse le million de dollars. Les EAU disposent donc d'un arsenal combinant des capacités internes (via Raven/DarkMatter) et des achats sur le marché commercial du spyware (NSO Group, et auparavant FinFisher et Hacking Team).

La dérive : des terroristes aux journalistes

La bascule se fait progressivement, sans rupture nette. Au bout de quatre à six mois, les missions de Project Raven s'éloignent du contre-terrorisme. La NESA demande de pénétrer les réseaux gouvernementaux d'un pays voisin — non pour traquer des financements terroristes, mais pour suivre les déplacements de la famille royale de ce pays, vérifier s'il y a eu corruption dans l'attribution d'un événement sportif, collecter du renseignement politique. « Nous sommes devenus le service de renseignement d'un pays étranger », confie « David », ancien opérateur de Raven, dans le podcast Darknet Diaries.

Après les Printemps arabes de 2011, les EAU considèrent les militants des droits humains et les journalistes critiques comme des menaces à la « stabilité nationale ». Project Raven reçoit l'ordre de cibler Rori Donaghy, un journaliste britannique de 25 ans qui anime le Emirates Center for Human Rights depuis Londres. Un blog WordPress, rien de plus. Mais Donaghy est interviewé par la BBC, ses articles paraissent dans le Financial Times et The Guardian. L'image internationale soignée des EAU commence à se fissurer. L'équipe de Raven le compromet par un email de phishing déguisé en invitation à un panel sur les droits humains, contenant un lien vers un faux site Al Jazeera. Trente et un tweets piégés lui sont aussi adressés, certains envoyés depuis les comptes de militants émiratis déjà emprisonnés — une tactique de compromission par usurpation d'identité de personnes détenues.

La crise diplomatique du Golfe, en juin 2017, amplifie les opérations. Les EAU, alliés à l'Arabie saoudite et à l'Égypte, imposent un blocus terrestre, aérien et maritime au Qatar, accusé de soutenir les Frères musulmans et de financer des médias d'opposition. Dans la semaine qui suit, Raven lance des attaques Karma contre au moins dix journalistes et dirigeants de médias. Parmi eux : Hamad bin Thamer bin Mohammed Al Thani, président du conseil d'administration d'Al Jazeera ; Faisal al-Qassem, présentateur de l'émission « The Opposite Direction » sur Al Jazeera ; Giselle Khoury, présentatrice de BBC Arabic ; Abdullah Al-Athba, rédacteur en chef du plus ancien journal qatari Al-Arab ; et des journalistes des chaînes londoniennes Al-Araby TV et Al-Hiwar. L'équipe Raven affectée au Qatar passe de deux à sept opérateurs à temps plein.

Ahmed Mansoor : le dissident à un million de dollars

Le cas d'Ahmed Mansoor concentre toute la violence du système. Cet Émirati, récipiendaire du prix Martin Ennals (parfois surnommé le « Nobel des droits humains »), est la cible la plus surveillée de Project Raven. Son nom de code interne est « Egret ». Il est ciblé sans interruption de 2012 à 2017 par un arsenal qui évolue au fil des ans : spyware FinFisher en 2011 (déguisé en PDF d'une pétition pro-démocratie), spyware Hacking Team en 2012 (via un document Word piégé exploitant la vulnérabilité CVE-2010-3333), tentatives de compromission par

Java en 2013, puis divers RAT (XTremeRAT, SpyNet, njRAT) en 2013-2014, et enfin Pegasus de NSO Group en 2016 via la chaîne d'exploits Trident.

Mansoor a le réflexe de ne pas cliquer sur le lien Pegasus et de le transmettre au Citizen Lab. Cette décision conduit Apple à publier en urgence le correctif iOS 9.3.5 en dix jours. Mais la vigilance technique ne protège pas contre la répression physique. En mars 2017, Mansoor est arrêté par les autorités émiraties. Il est condamné en procès secret à dix ans de prison pour « atteinte à l'unité du pays » — un délit qui n'existe dans aucune démocratie. Selon Human Rights Watch et le Gulf Centre for Human Rights, il est depuis détenu à l'isolement dans la prison d'Al-Sadr, près d'Abu Dhabi, dans des conditions qui relèvent de la torture. Sa femme, Nadia, dont le téléphone a également été compromis par Raven (nom de code : « Purple Egret »), vit en isolement social à Abu Dhabi, ses voisins l'évitant par peur d'être à leur tour surveillés.

Trois fournisseurs de spyware différents, basés dans trois démocraties différentes (Allemagne/Royaume-Uni pour FinFisher, Italie pour Hacking Team, Israël pour NSO Group), ont vendu leurs produits aux EAU en toute connaissance du profil de ce client. Comme le note le Citizen Lab : le fait que ces entreprises soient toutes issues de démocraties en dit long sur l'absence de régulation effective du commerce transfrontalier de spyware.

Le transfert vers DarkMatter et la ligne rouge américaine

Fin 2015, la dynamique de pouvoir bascule. Les EAU ne veulent plus que leur programme national de renseignement soit contrôlé par des étrangers. Le contrat avec CyberPoint prend fin. Project Raven passe sous la coupe de DarkMatter, une entreprise émiratie fondée en 2014 par Faisal Al Bannai, également fondateur d'Axiom, l'un des plus gros distributeurs de téléphones mobiles de la région. DarkMatter emploie plus de 650 personnes et se présente publiquement comme un développeur de cybersécurité défensive.

Les opérateurs américains ont le choix : rejoindre DarkMatter ou rentrer au pays. Environ un quart d'entre eux partent. Les autres restent, dont Lori Stroud, l'ancienne analyste NSA qui deviendra plus tard la lanceuse d'alerte. Les conditions de travail se durcissent. Les officiers émiratis de la NESA prennent le contrôle des opérations quotidiennes. Une catégorie « Emirate-eyes only » apparaît pour certaines cibles, excluant les Américains de la boucle.

Au printemps 2017, Stroud découvre dans le système de ciblage un passeport américain. En fouillant une file d'attente normalement réservée au personnel émirati, elle tombe sur des noms américains dans une catégorie inédite : la « white category » — pour les citoyens des États-Unis. La profession indiquée : journaliste. Stroud alerte son supérieur, Marc Baier. Il lui demande de laisser tomber. Elle insiste. DarkMatter la met en congé forcé, lui confisque ses téléphones et son passeport, et la fait escorter hors du bâtiment. Elle passe deux mois bloquée aux EAU avant d'être autorisée à rentrer aux États-Unis, où le FBI l'attend à l'aéroport.

Les conséquences judiciaires : un précédent ambigu

Le 14 septembre 2021, le département de la Justice américain annonce un accord de poursuites différées (*deferred prosecution agreement*) avec trois anciens opérateurs : Marc Baier (49 ans), Ryan Adams (34 ans) et Daniel Gericke (40 ans). Les charges portent sur deux chefs de conspiration : violation de l'Arms Export Control Act et de l'ITAR (pour avoir fourni des services de défense à un gouvernement étranger sans licence), et violation du Computer Fraud and Abuse Act (pour accès non autorisé à des systèmes informatiques). C'est la première fois que le piratage informatique est poursuivi en tant que violation de l'ITAR.

Les trois hommes acceptent de payer respectivement 750 000, 600 000 et 335 000 dollars d'amende — soit 1,685 million de dollars au total. Ils renoncent à toute habilitation de sécurité, acceptent une interdiction à vie d'en obtenir de nouvelles, et se voient imposer des restrictions d'emploi permanentes dans les domaines de l'exploitation de réseaux informatiques et de l'exportation de services de défense. Le département d'État prononce en 2022 un « debarment » de trois ans supplémentaires au titre de l'ITAR.

L'analyse juridique publiée par Lawfare en octobre 2021, signée Brandon L. Van Grack et Joseph Folio, deux anciens du département de la Justice, place les choses en perspective. En apparence, l'accord est clément : une violation ITAR de cette nature peut théoriquement entraîner vingt ans de prison. B. Stephanie Siegmann, ancienne procureure fédérale spécialisée en sécurité nationale, qualifie la conduite des trois accusés de « bien plus grave que celle de nombreuses personnes poursuivies par le DoJ au fil des ans pour violations ITAR ». La clémence s'explique probablement par la coopération des accusés avec le FBI et par le risque, pour l'accusation, de devoir produire des informations classifiées lors d'un procès public. Mais pour Lawfare, le message est ailleurs : le département de la Justice signale que fournir des capacités cyber offensives à un gouvernement étranger constitue désormais un acte criminel, même quand ce gouvernement est un allié des États-Unis.

DarkMatter, Mozilla, et l'infrastructure de confiance du web

L'affaire a des répercussions au-delà du renseignement. En 2017, DarkMatter avait déposé une demande auprès de Mozilla pour devenir autorité de certification SSL/TLS — ce rôle de « tiers de confiance » qui permet de garantir l'identité des sites web et la sécurité des connexions HTTPS. Toutes les autorités de certification approuvées par les navigateurs peuvent émettre des certificats pour n'importe quel site au monde. Si une organisation impliquée dans de la surveillance obtient ce statut, elle peut théoriquement créer de faux sites bancaires ou de messagerie et intercepter le trafic des utilisateurs.

Après les révélations de Reuters en janvier 2019, Mozilla examine la candidature de DarkMatter sous un jour nouveau. En juillet 2019, l'organisation la rejette — une décision sans précédent, puisque les refus reposaient jusque-là sur des critères techniques, pas sur des enquêtes journalistiques. Mozilla révoque également le statut provisoire que DarkMatter avait obtenu en 2017 et marque comme non sécurisés les 275 sites déjà certifiés par l'entreprise. En mai 2019, DarkMatter avait tenté de transférer son activité de certification vers une nouvelle entité appelée DigitalTrust, contrôlée par DM Investments, elle-même propriété du fondateur de DarkMatter, Faisal Al Bannai. Mozilla juge que cette structure ne garantit aucune indépendance réelle. Google Chrome et Apple Safari suivent la décision de Mozilla.

Du point de vue de l'architecture de confiance d'Internet, cette affaire est un rappel brutal. Le modèle PKI (Public Key Infrastructure) repose sur la confiance accordée aux autorités de certification. Si un acteur étatique offensif parvient à s'y insérer, c'est l'ensemble de la chaîne de confiance HTTPS qui est compromise. Project Raven a montré que la tentative était bien réelle.

Ce qu'on sait du périmètre de la surveillance

Les documents et témoignages ne permettent pas de dresser un bilan chiffré définitif du nombre total de personnes espionnées. L'investigation Reuters mentionne « des centaines » de cibles compromises via Karma en 2016-2017 à travers le Moyen-Orient et l'Europe. Les catégories de cibles documentées couvrent des militants des droits humains aux EAU et à l'étranger, des journalistes (BBC Arabic, Al Jazeera, Al-Araby TV, Al-Hiwar, Al-Arab), des opposants politiques, des gouvernements étrangers (Qatar, Iran, Yémen, Turquie), des adolescents critiques sur Twitter, et des citoyens américains — y compris des journalistes. L'outil Karma vise exclusivement les iPhone. Les opérations de compromission classiques (phishing, exploitation de vulnérabilités web, mouvement latéral) ciblent aussi des postes de travail et des serveurs gouvernementaux.

Sur la question de la revente de données sur le dark web, aucune source parmi les documents disponibles n'en fait mention. Les données exfiltrées par Raven étaient transmises aux officiers émiratis de la NESA qui supervisaient les opérations. Leur exploitation restait dans le périmètre du renseignement d'État. Ce n'est pas un programme à finalité commerciale — c'est un appareil de surveillance souverain.

Project Raven en tant que programme opéré par des Américains sous contrat s'est déroulé de 2009 à 2019 environ. La transition de CyberPoint vers DarkMatter s'opère fin 2015-début 2016. Lori Stroud est évincée en 2017. Les poursuites judiciaires concernent des actes commis entre décembre 2015 et novembre 2019. DarkMatter a depuis évolué vers Digital14 (rebaptisé après 2021), mais les capacités cyber offensives des EAU n'ont pas disparu — elles se sont émancipées de la tutelle américaine. Le programme a atteint son objectif initial : former le renseignement émirati à l'autonomie technique.

En mars 2022, en réponse directe aux révélations sur Project Raven, le Congrès américain a adopté des restrictions imposant une période de carence de trente mois aux anciens agents du renseignement avant de pouvoir travailler pour un gouvernement étranger, avec obligation de déclaration annuelle ensuite. C'est un début. Mais la question structurelle demeure : quand un État achète des compétences offensives et des exploits sur étagère, les contrôles à l'exportation restent le seul verrou. Et ce verrou, pendant dix ans, n'a pas tenu.

Références

[1] Al Jazeera. US hackers helped UAE spy on Al Jazeera chairman: Reuters. 1er avr. 2019.

[2] Christopher Bing et Joel Schectman. Project Raven: Inside the UAE's Secret Hacking Team of American Mercenaries. Reuters, 30 jan. 2019.

[3] Catalin Cimpanu. US fines former NSA employees who provided hacker-for-hire services to UAE. The Record from Recorded Future News, 14 sept. 2021.

[4] Human Rights Watch et Gulf Centre for Human Rights. The Persecution of Ahmed Mansoor: How the United Arab Emirates Silenced its Most Famous Human Rights Activist. 27 jan. 2021.

[5] Bill Marczak et John Scott-Railton. The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender. Research Report 78. Citizen Lab, University of Toronto, 24 août 2016.

[6] Nicole Perlroth. This Is How They Tell Me the World Ends: The Cyberweapons Arms Race. Bloomsbury Publishing, fév. 2021. isbn : 978-1635576054.

[7] Jack Rhysider. Project Raven. 2019.

[8] Joel Schectman et Christopher Bing. Mozilla blocks UAE bid to become an internet security guardian after hacking reports. Euronews/Reuters, 9 juill. 2019.

[9] Suzanne Smalley. State Department debars ex-NSA cyber mercenaries who aided vast UAE surveillance operation. CyberScoop, août 2022.

[10] U.S. Department of Justice. Deferred Prosecution Agreement — United States v. Marc Baier, Ryan Adams, Daniel Gericke. Case. 14 sept. 2021.

[11] Brandon L. Van Grack et Joseph Folio. Prosecuting Project Raven: A New Frontier for Export Control Enforcement. Lawfare, 20 oct. 2021.