FinFisher
Anatomie d'un spyware commercial pour la surveillance d'État

Stéphane FOSSE
fosse.fr

1er février 2026

FinFisher est un logiciel espion commercial développé par la société allemande FinFisher GmbH, basée à Munich, et commercialisé exclusivement auprès des gouvernements et agences de renseignement par le groupe britannique Gamma International. Entre 2011 et 2022, ce spyware a été déployé dans au moins 32 pays, ciblant des opposants politiques, des journalistes et des militants des droits humains. L'affaire FinFisher illustre comment l'industrie de la surveillance légale peut dériver vers des outils de répression politique. </section>

Origines et architecture commerciale de Gamma International

Gamma International, société britannique fondée dans les années 1990, s'est positionnée sur le marché de l'interception légale de communications. Son produit phare, la suite FinFisher, a été développé par sa filiale allemande FinFisher GmbH à partir de 2008. Le marketing de l'entreprise présente ces outils comme des solutions d'interception légale destinées à surveiller criminels et terroristes. La réalité documentée par les chercheurs raconte une autre histoire.

Le modèle économique de Gamma repose sur trois piliers. D'abord, la vente de licences logicielles avec un système par nombre de cibles simultanées. Ensuite, des contrats de maintenance et mises à jour annuels. Enfin, des formations sur site dispensées aux équipes des clients. Une liste de prix divulguée en 2014 révèle qu'un système FinSpy pour dix cibles coûtait 120 000 euros, auquel s'ajoutait 2 340 euros par licence d'activation. Les contrats de support s'étalaient sur trois à cinq ans.

Gamma a tissé un réseau de revendeurs en Europe. La société suisse Elaman GmbH, partageant la même adresse que FinFisher à Munich, agissait comme distributeur régional. Dreamlab Technologies, autre entreprise suisse, assurait des prestations de formation. Ces intermédiaires permettaient d'atteindre des clients auxquels une vente directe aurait posé problème.

Comment fonctionne le spyware FinSpy ?

FinSpy, le composant central de la suite FinFisher, est un logiciel de prise de contrôle à distance fonctionnant sur Windows, macOS, Linux, Android, iOS, BlackBerry et Symbian. Une fois installé sur la machine cible, il capture les frappes clavier, intercepte les communications Skype, enregistre via la webcam et le microphone, extrait les fichiers du disque dur et géolocalise l'appareil. Sur mobile, il accède aux SMS, au carnet d'adresses, aux journaux d'appels et peut activer des appels espions silencieux.

L'architecture technique distingue trois composants. Le FinSpy Master est le serveur de commande et contrôle installé chez le client gouvernemental. Il stocke les données collectées et gère les opérateurs. Les FinSpy Relays sont des serveurs proxy hébergés dans des pays tiers pour masquer la localisation du Master. Enfin, le FinSpy Agent est l'interface graphique permettant aux opérateurs de configurer et analyser les cibles. Gamma vantait que ce système rendait « pratiquement impossible » de remonter jusqu'au quartier général.

L'infection des cibles passait par plusieurs vecteurs. Le document commercial de Gamma cite l'installation physique sur des ordinateurs de cybercafés dans des « zones critiques ». Des pièces jointes malveillantes dans des e-mails de phishing étaient courantes. Plus sophistiqué, le FinFly ISP permettait une injection réseau au niveau du fournisseur d'accès, redirigeant les mises à jour logicielles légitimes vers des versions piégées. ESET a documenté en 2017 cette technique dans deux pays non nommés, et le Citizen Lab a identifié des équipements d'injection réseau en Égypte.

Le chiffrement des communications entre les agents infectés et les serveurs de contrôle utilisait RSA 2048 et AES 256. Chaque échantillon contenait une configuration encodée au format TLV, incluant les adresses des

serveurs proxy, les intervalles de connexion et les modules activés. L'analyse par Amnesty International en 2020 a révélé des versions Linux et macOS jusque-là inconnues, utilisant l'obfuscateur LLVM pour compliquer l'analyse. Ces versions exploitaient des vulnérabilités comme CVE-2015-5889 pour l'escalade de privilèges.

Prolifération mondiale et victimes documentées

Les travaux du Citizen Lab de l'Université de Toronto ont cartographié la propagation de FinFisher. Leurs scans successifs entre 2012 et 2015 ont identifié des serveurs de commande et contrôle dans 25 pays en 2013, puis 32 en 2015. Ces pays incluent des démocraties comme l'Allemagne et la Belgique, mais aussi des régimes autoritaires comme le Turkménistan, l'Éthiopie et le Bahreïn.

Le cas du Bahreïn est le mieux documenté. En 2012, des activistes pro-démocratie ont reçu des e-mails piégés contenant FinSpy. L'analyse a révélé que les communications remontaient vers un serveur de l'opérateur Batelco dans le royaume. Bahrain Watch a identifié 77 ordinateurs ciblés appartenant à des avocats réputés, des journalistes et des figures de l'opposition. Gamma a d'abord nié, affirmant qu'il s'agissait d'une copie de démonstration volée. Les documents internes divulgués en 2014 ont démenti cette version en montrant des tickets de support technique échangés avec les autorités bahreïnies.

En Éthiopie, un échantillon FinSpy découvert utilisait comme appât des photos de membres de Ginbot 7, un groupe d'opposition désigné organisation terroriste par le gouvernement en 2011. Le serveur de contrôle, hébergé chez Ethio Telecom, l'opérateur d'État, est resté actif pendant plusieurs années. Des dissidents éthiopiens résidant au Royaume-Uni et aux États-Unis ont été infectés, ce qui a conduit l'Electronic Frontier Foundation à engager une action en justice.

En Égypte, le département de recherche technologique utilisait FinFisher en parallèle d'outils concurrents comme ceux de Hacking Team. Le Citizen Lab a établi des connexions entre l'infrastructure FinFisher égyptienne et le groupe d'attaquants NilePhish, actif contre la société civile depuis 2019. Cette même infrastructure servait à distribuer FinSpy via de faux sites de mise à jour Adobe Flash Player.

Les documents internes de Gamma divulgués en 2014 par un hacktiviste se faisant appeler Phineas Fisher ont révélé l'étendue de la clientèle. Parmi les entités identifiées figurent le DGFI au Bangladesh, la police fédérale belge, le BIA en Serbie, le NIS au Kenya, la Sûreté générale libanaise, le CSDN marocain et le SSSD mongol. Un contrat de 287 000 euros avec l'Indonésie mentionnait le Lembaga Sandi Negara, l'agence nationale de chiffrement.

Révélations et fin des opérations

Le 6 août 2014, 40 gigaoctets de données internes de Gamma ont été publiés sur Internet. Le pirate a documenté sa méthode d'intrusion dans un manifeste technique, détaillant l'exploitation d'une vulnérabilité zero-day dans l'appliance VPN de l'entreprise. Ces documents comprenaient le code source de FinSpy, des listes de clients, des correspondances commerciales et des tarifs. L'enquête italienne sur ce piratage a été classée sans suite en 2017.

Privacy International et le European Center for Constitutional and Human Rights ont déposé une plainte auprès de l'OCDE en 2013, accusant Gamma d'avoir violé les lignes directrices sur les entreprises multinationales en exportant vers le Bahreïn. En 2015, le point de contact national britannique de l'OCDE a conclu que Gamma avait effectivement manqué à ses obligations en matière de droits humains, une première pour une entreprise de surveillance.

Les autorités allemandes ont finalement agi. En 2019, le parquet de Munich a ouvert une enquête sur FinFisher GmbH pour exportation illégale de technologies de surveillance vers la Turquie sans licence. En mars 2022, des perquisitions ont été menées dans les locaux de l'entreprise. Quelques mois plus tard, FinFisher GmbH a déposé le bilan et cessé ses activités.

Le hack de Phineas Fisher a eu des répercussions au-delà de FinFisher. En 2015, le même individu a compromis Hacking Team, principal concurrent italien, divulguant 400 gigaoctets de données. Ces révélations successives ont alimenté le débat sur la régulation de l'industrie des logiciels espions. L'amendement Wassenaar de 2013, qui soumet les « logiciels d'intrusion » au contrôle des exportations d'armements, a été adopté en partie à cause des scandales FinFisher.

Ce que FinFisher révèle du marché de la surveillance

L'affaire FinFisher a mis en lumière un marché estimé à cinq milliards de dollars en 2011, avec une croissance de vingt pour cent par an. Les salons ISS World, surnommés « Wiretapper's Ball », se tiennent chaque année à Washington, Prague, Brasilia, Johannesburg, Dubaï et Kuala Lumpur. FinFisher était présent dans la plupart

d'entre eux, ainsi qu'au salon Security and Policing de Farnborough et au FBI Executives Training de San Antonio.

La clause contractuelle révélée dans les documents internes de Gamma interdit aux acheteurs d'utiliser FinFisher contre des cibles en Allemagne. Cette restriction suggère soit une exigence des autorités allemandes pour autoriser l'exportation, soit une précaution juridique de l'entreprise. Elle n'empêchait pas les clients de cibler leurs propres citoyens.

Le successeur commercial de FinFisher reste actif sous d'autres formes. Amnesty International a documenté en 2024 des ventes de produits FinFisher vers l'Indonésie entre 2017 et 2023, via des filiales et des sociétés écrans. Le marché des logiciels espions commerciaux s'est restructuré autour d'acteurs comme NSO Group et son produit Pegasus, Candiru, ou QuaDream, tous israéliens.

Pour les responsables de la sécurité des systèmes d'information, FinFisher illustre une réalité inconfortable. Les techniques d'intrusion développées pour la surveillance légale finissent entre les mains de régimes qui les retournent contre leurs citoyens. Les mêmes vulnérabilités zero-day vendues par VUPEN à Gamma pour son « Exploit Portal » pouvaient servir à infecter un journaliste bahreïni ou un opposant éthiopien. La frontière entre sécurité offensive et répression politique tient à la nature du client, pas à la technologie.

Références

[1] Bahrain Watch. UK spyware used to hack Bahrain lawyers, activists. Privacy International, août 2014.

[2] Bill Marczak et al. Mapping FinFisher's Continuing Proliferation. Citizen Lab, oct. 2015.

[3] Morgan Marquis-Boire et al. You Only Click Twice: FinFisher's Global Proliferation. Rapp. tech. Citizen Lab, mars 2013.

[4] P. Maynard et K. McLaughlin. Big Fish, Little Fish, Critical Infrastructure: An Analysis of Phineas Fisher. Avr. 2020. arXiv : 2004.14360.

[5] Privacy International. Six things we know from the latest FinFisher documents. 2014.

[6] Security Lab. German-made FinSpy spyware found in Egypt, and Mac and Linux versions revealed. Amnesty International, sept. 2020.

[7] WikiLeaks. SpyFiles. documents commerciaux Gamma International. Décembre 2011 et septembre 2014. 2011.