Babar et SNOWGLOBE
Quand la DGSE entre dans la cour des cyberespions

Stéphane FOSSE
fosse.fr

1er février 2026

Résumé

Babar est un logiciel espion développé par la Direction Générale de la Sécurité Extérieure (DGSE), l'agence de renseignement extérieur française. Découvert en novembre 2009 par le Centre de la sécurité des télécommunications du Canada (CSEC) et révélé au public en mars 2014 grâce aux documents d'Edward Snowden, ce malware constitue la première preuve documentée des capacités offensives de la France dans le domaine cyber. Le programme, nommé SNOWGLOBE par les Canadiens, ciblait principalement le programme nucléaire iranien, mais a aussi infecté des systèmes en Algérie, en Côte d'Ivoire, en Espagne, en Grèce, en Norvège et au Canada.

L'ironie de cette histoire mérite qu'on s'y arrête. Ce n'est pas la NSA qui a créé Babar, contrairement à ce qu'une lecture superficielle pourrait laisser croire. Les documents Snowden ont révélé que les services de renseignement canadiens, alliés des États-Unis au sein de l'alliance Five Eyes, avaient détecté et analysé un logiciel espion qu'ils attribuaient à un allié occidental : la France. L'arroseur arrosé, en somme. Les espions espionnaient les espions.

1 Comment le CSEC a découvert Babar

En novembre 2009, les analystes du CSEC repèrent une activité suspecte sur un réseau qu'ils surveillent déjà. Leur système WARRIORPRIDE, utilisé comme capteur, détecte une anomalie grâce au module REPLICANTFARM. Un fichier RAR protégé par mot de passe attire leur attention. Toujours le même mot de passe. Les analystes récupèrent les fichiers associés et identifient un malware inconnu par rétro-ingénierie.

Le logiciel collecte des emails depuis des comptes ciblés. Il « ressemble à un outil de collecte de renseignement étranger », note la présentation interne du CSEC datée de 2011. L'analyse révèle un implant sophistiqué baptisé SNOWBALL par les Canadiens, puis une version améliorée SNOWBALL 2, et enfin un implant plus avancé découvert mi-2010 qu'ils nomment SNOWMAN. L'ensemble de l'opération reçoit le nom de code SNOWGLOBE.

Les Canadiens exploitent une faiblesse de sécurité opérationnelle des opérateurs français. Grâce à leur accès passif au réseau mondial via le programme EONBLUE, ils observent un opérateur se connecter à l'un des serveurs de commande et contrôle. Authentification simple, hash faible. Cette erreur leur permet d'accéder eux-mêmes aux serveurs de contrôle du malware français.

2 L'architecture technique d'un espion numérique

Babar est une DLL Windows 32 bits écrite en C++. Une fois déployé sur une machine cible via un *dropper*, l'implant s'injecte dans les processus en cours d'exécution et applique des hooks Windows globaux pour intercepter les appels API. La sophistication technique n'atteint pas le niveau de Regin, le malware attribué au GCHQ britannique, mais le code remplit parfaitement sa mission d'espionnage.

Les capacités de Babar couvrent l'essentiel de ce qu'un service de renseignement peut souhaiter extraire d'un ordinateur infecté. L'implant enregistre les frappes clavier via l'API Windows RAWINPUT, capture le contenu du presse-papiers, prend des captures d'écran grâce à la bibliothèque GdiPlus, et intercepte les conversations audio des logiciels de téléphonie sur IP comme Skype, MSN Messenger, Yahoo ! Messenger, OoVoo, Nimbuzz, Google Talk ou X-Lite. Babar a de grandes oreilles.

La configuration chiffrée en AES contient la liste des applications surveillées. Les processus de bureautique comme Excel, Word, PowerPoint, Visio, Acrobat Reader, Notepad et WordPad sont ciblés pour identifier les documents manipulés. Les extensions surveillées incluent txt, rtf, xls, xlsx, ppt, ppts, doc, docx, pdf et vsd. Les données volées sont stockées localement dans le fichier `%COMMON_APPDATA%\MSI\update.msi` avant exfiltration vers les serveurs de commande.

3 Les indices qui pointent vers la France

L'attribution d'un malware à un État reste un exercice délicat. Les analystes du CSEC accumulent pourtant des indices convergents. Le nom interne du projet, « Babar », fait référence à l'éléphant de la série de livres pour enfants créée par Jean de Brunhoff en 1931. Le pseudonyme du développeur, « titi », est un diminutif français du prénom Thierry ou un terme argotique désignant une personne de petite taille.

Les détails techniques trahissent également l'origine francophone. L'interface de commande utilise l'anglais, mais les formulations ne sont pas idiomatiques. La *locale* des documents de phishing est configurée sur « fr_FR ». Plus révélateur encore : les tailles de fichiers sont exprimées en « ko » (kilo-octets) plutôt qu'en « kB » (kilobytes), une convention propre à la communauté technique française.

Une faute de frappe dans le code constitue une signature involontaire. La chaîne User-Agent contient « MSI 6.0 » au lieu de « MSIE 6.0 » (Microsoft Internet Explorer). Cette même erreur se retrouve dans EvilBunny, un autre malware de la même famille découvert par la chercheuse autrichienne Marion Marschalek. Les deux programmes partagent la même technique de détection des antivirus via WMI, la même méthode d'obfuscation des API, et communiquent avec des serveurs hébergeant des sites francophones.

4 Les cibles de l'opération SNOWGLOBE

L'Iran concentre l'essentiel des infections identifiées par le CSEC. Le ministère iranien des Affaires étrangères, l'Organisation de l'énergie atomique d'Iran, l'Université des sciences et technologies d'Iran, l'université Imam Hussein, l'université Malek-E-Ashtar et l'Organisation iranienne de recherche pour la science et la technologie figurent parmi les victimes documentées. Le ciblage du programme nucléaire iranien correspond aux priorités de renseignement françaises de l'époque.

Hors d'Iran, les infections touchent des pays aux profils variés. En Europe, la Grèce, l'Espagne, la Norvège et la France elle-même apparaissent dans la liste des victimes, possiblement via l'Association financière européenne. En Afrique, l'Algérie et la Côte d'Ivoire, anciennes colonies françaises, sont ciblées. Au Canada, une organisation médiatique francophone fait partie des cibles potentielles.

L'infrastructure de commande et contrôle utilise des serveurs répartis mondialement, principalement dans les pays de l'alliance Five Eyes : États-Unis, Canada, Royaume-Uni, mais aussi République tchèque, Pologne et Norvège. Les opérateurs français exploitent soit des services d'hébergement gratuit, soit des sites légitimes compromis, souvent francophones. Les scripts PHP `outbase.php` et `register.php` gèrent la communication avec les implants.

5 La famille Animal Farm révélée par Kaspersky

En mars 2015, les chercheurs de Kaspersky Lab publient une analyse qui replace Babar dans un contexte plus large. Ils identifient un groupe qu'ils nomment « Animal Farm », responsable de six familles de malwares liées : Babar, Bunny, Casper, Dino, NBot et Tafacalou. L'activité du groupe remonte au moins à 2007, comme le confirme un échantillon de Babar découvert par Palo Alto Networks en septembre 2017.

Casper, analysé par ESET, utilise deux exploits zero-day (CVE-2014-0515) dans une attaque de type « watering hole » ciblant des visiteurs d'un site syrien. Les techniques de code partagées entre Casper, Babar et Bunny confirment leur origine commune. Le niveau de sophistication et les cibles (gouvernements, médias, contractants militaires) correspondent au profil d'une agence de renseignement étatique disposant de ressources importantes.

6 La confirmation officieuse de Bernard Barbier

Pendant des années, la DGSE n'a jamais commenté officiellement les révélations sur Babar. La situation change en juin 2016 lors d'un symposium à CentraleSupélec. Bernard Barbier, ancien directeur technique de la DGSE de 2006 à 2014, prend la parole devant un public d'étudiants et de professionnels. Il confirme que Babar a bien été développé par la DGSE.

Cette déclaration, bien qu'officieuse puisque Barbier n'occupait plus de fonction officielle, constitue la première reconnaissance française de l'existence du programme. Elle valide l'analyse du CSEC qui concluait avec « une certitude modérée » à l'attribution française.

7 Ce que Babar révèle des capacités françaises

Babar n'est pas Stuxnet. Le malware français ne sabote pas de centrifugeuses nucléaires. Il collecte du renseignement de manière classique : interception de communications, vol de documents, surveillance d'activité. Son niveau technique, qualifié de « sophistiqué mais pas exceptionnel » par les analystes, place la France dans le peloton des puissances cyber, derrière les États-Unis, la Russie et probablement la Chine, mais au niveau d'acteurs comme le Royaume-Uni ou Israël.

Les erreurs de sécurité opérationnelle ayant permis au CSEC de remonter jusqu'aux serveurs de contrôle suggèrent une organisation encore en phase d'apprentissage au moment de la découverte en 2009. L'utilisation de sites compromis francophones comme infrastructure trahit une certaine insouciance, ou peut-être un manque de ressources pour acquérir des serveurs plus discrets.

L'affaire Babar confirme surtout que la surveillance numérique n'est pas l'apanage des Anglo-Saxons. Les révélations Snowden ont souvent été interprétées comme une mise en accusation exclusive de la NSA et de ses partenaires Five Eyes. La découverte de SNOWGLOBE rappelle que tous les États disposant de moyens suffisants développent des capacités offensives dans le cyberespace. La France n'y fait pas exception.

8 Le programme est-il toujours actif ?

Les documents disponibles ne permettent pas de déterminer si l'opération SNOWGLOBE est toujours en cours. L'exposition médiatique de 2014-2015 a probablement conduit la DGSE à modifier ses outils et ses méthodes. Kaspersky indiquait en 2015 que le groupe Animal Farm restait actif. Aucune information publique n'a été publiée depuis sur l'évolution de ces programmes.

Le nombre exact de victimes reste inconnu. Les documents du CSEC mentionnent des infections dans une dizaine de pays, mais la présentation de 2011 ne donne pas de chiffres précis. L'infrastructure de commande et contrôle permettait de gérer plusieurs centaines d'implants simultanément, à en juger par les captures d'écran des interfaces d'administration. Rien n'indique que des données personnelles aient été revendues sur le dark web : Babar est un outil de renseignement étatique, pas un malware criminel.

Les échantillons analysés datent de 2007 à 2015. Huit années d'activité documentée pour un programme d'espionnage étatique, c'est à la fois beaucoup (signe de succès opérationnel) et peu (les programmes américains comme PRISM ont été révélés après plus d'une décennie d'existence). L'éléphant Babar a peut-être pris sa retraite, ou simplement changé de costume.

Références

[1] Pierre Alonso. Logiciel espion Babar : la France, suspect numéro 1. In : *Libération* (fév. 2015).

[2] CSEC. SNOWGLOBE: From Discovery to Attribution. document classifié TOP SECRET//COMINT, révélé par Edward Snowden. 2011.

[3] Jacques Follorou et Glenn Greenwald. Espionnage : la France soupçonnée par les services canadiens. In : *Le Monde* (mars 2014).

[4] Lorenzo Franceschi-Bicchierai. Meet Babar, a New Malware Almost Certainly Created by France. In : *Vice Motherboard* (fév. 2015).

[5] Kaspersky Lab GReAT. Animals in the APT Farm. Kaspersky SecureList. Mars 2015.

[6] Marion Marschalek. Babar: Suspected Nation State Spyware In The Spotlight. Cyphort Labs. Fév. 2015.

[7] Paul Rascagnères. Babar: espionage software finally found and put under the microscope. G DATA SecurityLabs. Fév. 2015.

[8] Der Spiegel. The Digital Arms Race: NSA Preps America for Future Battle. In : *Der Spiegel* (jan. 2015).

[9] Martin Untersinger. Le programme espion Babar a un "grand frère" : Evil Bunny. In : *Le Monde* (fév. 2015).

[10] Wikipedia. Babar (logiciel malveillant). Wikipédia français. 2015.

[11] ZDNet. Quand l'ancien directeur de la DGSE confirme le piratage de l'Élysée par les US. In : *ZDNet* (juin 2016).