AMNESTY INTERNATIONAL

COMMUNIQUÉ DE PRESSE

SOUS EMBARGO JUSQU'AU 7 OCTOBRE 2021 00:01 CET

Togo: un militant togolais ciblé par un logiciel espion fabriqué en Inde et lié à un groupe de hackers

- Un militant togolais pris pour cible au moyen d'un logiciel espion par le groupe de hackers Donot Team.
- Amnesty International dévoile les liens entre les attaques de Donot Team et Innefu Labs, une entreprise spécialisée dans la cybersécurité installée en Inde.
- C'est la première fois que Donot Team est publiquement reliée à des cyberattaques ciblant des militant·e·s en dehors de l'Asie du Sud.
- Des courriels infectés par des logiciels espions et de fausses applications Android peuvent accéder à la caméra et au microphone de l'appareil, voler des photos et des fichiers, et lire les messages WhatsApp.

Les militants au Togo peuvent risquer d'être pris pour cibles par des cybermercenaires de l'ombre, qui lancent des attaques numériques pour tenter de voler les données privées des victimes afin de les vendre à des clients privés, dévoile une nouvelle enquête menée par Amnesty International.

Dans son nouveau rapport publié aujourd'hui, Amnesty International révèle que le tristement célèbre groupe de hackers Donot Team a utilisé de fausses applications Android et des courriels infectés par des logiciels espions pour cibler un défenseur togolais des droits humains bien connu, dans le but de le placer illégalement sous surveillance. C'est la première fois que les spywares de Donot Team sont identifiés dans des attaques en dehors de l'Asie du Sud. Cette enquête a également permis de découvrir des liens entre le logiciel espion et l'infrastructure utilisée dans ces attaques, et Innefu Labs, une entreprise de cyber-sécurité basée en Inde.

Ce militant togolais, qui préfère garder l'anonymat pour des raisons de sécurité, travaille depuis longtemps avec des organisations de la société civile togolaise et est une voix essentielle qui défend les droits humains dans le pays. Ses appareils ont été ciblés entre décembre 2019 et janvier 2020, alors que le climat politique était tendu à l'approche de l'élection présidentielle de 2020 au Togo.

« À travers le monde, les cybermercenaires tirent sans scrupules profit de la surveillance illégale des défenseur·e·s des droits humains, » a déclaré Danna Ingleton, directrice adjointe d'Amnesty Tech.

« Tout le monde peut être une cible : des cybermercenaires vivant à des centaines de kilomètres peuvent pirater votre téléphone ou votre ordinateur, regarder où vous allez et à qui vous parlez, et vendre vos données privées à des gouvernements répressifs ou à des criminels.»

Des attaques persistantes via WhatsApp et par courriel ont tenté de piéger la victime pour qu'elle installe une application malveillante travestie en application de messagerie instantanée

sécurisée. Il s'agissait en fait d'un logiciel espion pour Android conçu pour extraire des informations parmi les plus sensibles et personnelles stockées sur le téléphone du militant.

Ce logiciel espion aurait permis aux auteurs de l'attaque d'avoir accès à la caméra et au microphone, de récupérer des photos et des fichiers stockés sur l'appareil, et même de lire les messages WhatsApp chiffrés< au moment de l'envoi et de la réception. Le caractère secret de ces attaques fait qu'il est extrêmement difficile pour les militant·e·s de détecter si leur téléphone est infecté.

« 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 ? », a déclaré à Amnesty International le défenseur des droits humains basé au Togo.

Cette enquête d'Amnesty International a mis à jour une suite de preuves techniques laissées par les auteurs de l'attaque qui prouve des liens entre l'infrastructure utilisée dans ces attaques et l'entreprise basée en Inde Innefu Labs. Cette entreprise annonce offrir des services autour de la sécurité numérique, l'analyse de données et la prévision policière à des agences de maintien de l'ordre et aux forces armées et affirme travailler avec le gouvernement Indien. Innefu Labs ne possède pas de politique de droits humains et ne semble pas mettre en œuvre une diligence raisonnable en matière de droits humains - malgré les énormes risques que ses produits représentent pour la société civile. Amnesty International a constaté que les attaques de Donot Team contre des organisations et des individus en Asie se concentraient pour la plupart dans le nord de l'Inde, au Pakistan et au Cachemire.

Des attaques contre les militants

L'espace d'action des défenseurs des droits humains au Togo s'est rétréci : en 2019, l'année précédant l'élection présidentielle, Amnesty International a noté l'adoption de lois restreignant les droits à la liberté d'expression et de réunion pacifique, et recensé des cas de violations commises par les autorités, notamment contre des militant·e·s pour la démocratie.

Plusieurs dignitaires religieux et figures de l'opposition politique au Togo auraient été la cible d'outils de surveillance numérique. En août 2020, The 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 cibles au moyen d'une faille de WhatsApp exploitée par NSO Group.

Le Projet Pegasus, coordonné par Forbidden Stories avec l'appui technique du Security Lab d'Amnesty International, a révélé cette année que les numéros de centaines de Togolaises et Togolais avaient été inscrits sur une liste de cibles potentielles du logiciel espion Pegasus de NSO Group. Parmi eux figuraient des journalistes indépendants et des membres des mouvements de l'opposition politique.

La menace de la surveillance ciblée, qu'elle soit réelle ou non, peut avoir de lourdes conséquences psychologiques sur les militant·e·s et un effet plus que délétère sur leur travail en faveur des droits humains. Malgré les multiples demandes d'Amnesty International et d'organisations de la société civile pour plus de transparence, on ne sait pas grand-chose sur

l'industrie de la cybersurveillance, qui évoque un véritable Far West, et on en sait encore moins sur le secteur florissant dans lequel évoluent les cybermercenaires.

« Le secteur de la surveillance échappe à tout contrôle avec des entreprises et des cybermercenaires agissant totalement dans l'ombre.

« Les entreprises de surveillance doivent cesser de donner la priorité aux profits, au détriment des personnes, et veiller à ce que les régimes répressifs ne se servent pas de leur technologie pour étouffer la société civile », a déclaré Danna Ingleton.

Amnesty International demande :

- à Innefu Labs de publier dans leur intégralité les conclusions d'un audit externe commissionné par l'entreprise sur les liens entre Innefu Labs et l'infrastructure et les outils d'espionnage utilisés dans l'attaque ciblant le militant au Togo et de mettre en œuvre une politique en matière de droits humains ; Innefu Labs doit également mettre en place une politique de droits humains.
- au gouvernement indien d'enquêter sur les cyberattaques liées à Innefu Labs et de prendre d'urgence des mesures visant à garantir que les entreprises de surveillance basées en Inde ne soient pas impliquées dans le ciblage de militant·e·s – ce que le droit international relatif aux droits humains interdit sans ambiguïté ;
- au gouvernement togolais de veiller à ce que tous les citoyen·ne·s, notamment les militant·e·s, soient protégés contre les atteintes aux droits humains, d'enquêter sur les préjudices causés par les cyberattaques menées par des acteurs du secteur privé et d'y apporter des réparations.

Dans une réponse écrite à Amnesty International, Innefu Labs a nié « l'existence de quelque lien que ce soit entre Innefu Labs et les logiciels espions attribués à 'Donot Team' » ou avec les attaques contre le défenseur des droits humains au Togo. Innefu Labs a également déclaré qu'ils n'ont pas connaissance d'aucune utilisation de leur adresse IP dans ces activités supposées.

Aucune preuve ne suggère une implication ou connaissance directe d'Innefu Labs dans les attaques contre le défenseur des droits humains au Togo utilisant les logiciels espions de Donot Team. Les activités attribuées à Donot Team peuvent impliquer plusieurs acteurs ou organisations distinctes ayant accès aux mêmes logiciels espions ou à une infrastructure partagée.

Notes pour les rédacteurs :

Pour plus d'information, y compris pour demander une copie sous embargo du rapport, veuillez contacter

tom.mackey@amnesty.org ou press@amnesty.org