Le défi lancé à la démocratie indienne par l'application Tek Fog

written by Chinmayee Naik | 28 avril 2022

Outil au service du parti au pouvoir, une application mobile malveillante sert à manipuler les discours relayés par les principaux médias sociaux en Inde, automatisant une large diffusion de messages de haine et de harcèlements ciblés.

Le 6 janvier 2022, *The Wire*, un média indien qui défend l'intérêt public et les valeurs démocratiques, a révélé l'existence d'une application secrète très sophistiquée appelée Tek Fog[1]. Utilisée par les cybergroupes affiliés au parti hindouiste ultraconservateur du Premier ministre Narendra Modi – le Bharatiya Janata Party ou BJP –, cette application pour téléphone portable sert à manipuler les principaux médias sociaux en Inde, ainsi que les plateformes de messagerie cryptées. L'enquête, qui a duré vingt mois, montre comment Tek Fog automatise les discours de haine ou le harcèlement ciblé, en diffusant des messages de propagande, résultat d'une alliance diabolique entre la high-tech et la vile politique.

En raison de son usage à grande échelle et de son degré de sophistication inédit, explique *The Wire*, Tek Fog est un puissant instrument de propagande automatisée en ligne, qui joue un rôle dans la construction du discours public des acteurs de l'État, comme auprès des entrepreneurs en Inde. L'application elle-même semble être le pilier d'un vaste réseau, encore largement inexploré, de travailleurs rémunérés et de bénévoles qui déploient des stratégies de désinformation sur les plateformes de médias sociaux pour déformer, corrompre les conversations publiques au profit du parti au pouvoir en Inde. À cette fin, Tek Fog est notamment capable de créer une multitude de fausses adresses temporaires en déjouant les systèmes d'authentification des réseaux Telegram, Google, Facebook, Twitter.

Dans une série de tweets publiés en avril 2020, un compte Twitter anonyme, @Aarthisharma08, a allégué l'existence de l'application Tek Fog, prétendant être un employé mécontent de la cellule des technologies de l'information (IT Cell) du Bharatiya Janata Party. Ces tweets affirment que cette application est un instrument au service des agents politiques affiliés au parti au pouvoir pour gonfler artificiellement la popularité du parti, harceler ses détracteurs et manipuler à grande échelle la perception du public sur les principales plateformes de médias sociaux.

Au cours des vingt mois suivants, une correspondance s'est mise en place

avec l'équipe de *The Wire*, qui a méticuleusement fait le tri entre ce qui pouvait être vérifié et ce qui ne pouvait pas l'être parmi les allégations de l'informateur. Les principales conclusions de l'enquête mettent au jour des caractéristiques alarmantes de l'application Tek Fog.

Influencer le discours public *via* les tendances Twitter et Facebook

L'un des principaux objectifs de l'application est de prendre le contrôle de la section « Tendances » de Twitter et de Facebook. Tek Fog utilise dans ce but des outils d'automatisation intégrés pour « auto-retweeter » ou « autopartager » des tweets individuels ou collectifs, ainsi que pour « spammer » les hashtags existants avec des comptes contrôlés par les agents de l'application. Ainsi, sur l'écran d'accueil de Tek Fog, s'affiche une liste des « tendances du jour » que les agents de l'application ont pour mission d'amplifier sur Twitter et Facebook à l'aide de fonctionnalités d'automatisation.

Pour montrer l'efficacité de l'application sur le fonctionnement de Twitter, l'informateur anonyme, lanceur d'alerte, a fourni aux auteurs de *The Wire* deux captures d'écran de hashtags à promouvoir, une liste de hashtags déjà amplifiés avec Tek Fog et une liste de comptes Facebook ou Twitter gérés par des agents utilisant l'application. Deux heures plus tard, chacun des hashtags fournis a atteint la section *« Trending »* des plateformes après avoir été amplifié de manière truquée par une série de comptes suspects.

Cette fonctionnalité est principalement utilisée pour stimuler la propagande du parti de droite BJP sur ces réseaux sociaux, en l'exposant à un public plus large et faisant ainsi apparaître les récits et les campagnes politiques extrêmes plus populaires qu'ils ne le sont en réalité.

Piratage de comptes WhatsApp actifs ou inactifs afin de propager la désinformation

Le lanceur d'alerte a affirmé que Tek Fog permettait à des cybergroupes d'accéder aux comptes WhatsApp de citoyens – cette messagerie est extrêmement populaire en Inde, notamment pendant les campagnes électorales – grâce à une fonctionnalité intégrée. Les agents, qui se servent de Tek Fog, accèdent ainsi à distance aux comptes WhatsApp « actifs » et « inactifs » (« inactif » signifiant que la personne à laquelle appartient ce numéro de téléphone ne se sert pas de l'application, soit parce qu'elle l'a désinstallée, soit parce qu'elle a réinitialisé son téléphone) afin d'envoyer grâce à Tek Fog des messages ciblés aux « contacts habituels » ou encore à « tous les contacts » de ces numéros de téléphone piratés.

Les comptes WhatsApp « actifs » reçoivent un message sous la forme d'un

fichier multimédia (image ou vidéo) en provenance d'un contact inconnu. Ce fichier contiendrait un logiciel espion activé dès lors que le fichier multimédia a été téléchargé par la cible, rendant le téléphone vulnérable. L'activité de ce compte peut dès lors être suivie *via* Tek Fog. Les agents sont ainsi en mesure d'accéder à distance au compte WhatsApp ciblé, sans le consentement du propriétaire qui n'a pas connaissance de l'« exploit » et ils attendent que le compte devienne inactif pour l'utiliser. Le choix d'accéder uniquement aux comptes WhatsApp inactifs semble être une contrainte stratégique – et non technologique –, car l'envoi de faux messages depuis un compte actif pourrait susciter des échanges et éveiller des soupçons.

Souhaitant vérifier cette allégation, *The Wire* a demandé au lanceur d'alerte de faire une démonstration en direct de cet « exploit » en piratant un compte WhatsApp appartenant à un membre de son équipe et en envoyant un message personnalisé à ses contacts habituels. Peu après, la réception de ce message par les cinq utilisateurs « fréquemment contactés » – dont un collègue travaillant sur l'enquête – confirmait que cet usage intrusif de Tek Fog était parfaitement fonctionnel au moment de l'enquête. Six minutes plus tard, le lanceur d'alerte a de plus partagé un enregistrement d'écran de l'application qui les montrait en train d'exécuter la tâche.

Cette fonctionnalité vise à diffuser à la plus large audience possible des informations erronées en s'appuyant sur les réseaux personnels des utilisateurs inactifs. WhatsApp ayant acquis une grande popularité en tant qu'outil de campagne, le BJP a ainsi trouvé des moyens malveillants d'atteindre le public *via* cette messagerie.

Harcèlement ciblé *via* une base de données soigneusement constituée

L'adressage de messages, à la fois massif et ciblé grâce aux algorithmes, vers un vaste réseau de comptes d'opposants politiques et de citoyens ordinaires, est la caractéristique la plus importante – et la plus alarmante – de l'application.

Les captures et les vidéos d'écran de l'application Tek Fog prouvent l'existence d'une importante base de données de citoyens classée par profession, religion, langue, âge, sexe, affinités politiques et même caractéristiques physiques. Cette base de données permet aux agents de « répondre systématiquement » à des individus ou à des groupes en générant de manière automatique des mots-clés et des phrases, dont la grande majorité sont abusifs ou désobligeants.

Les agents utilisent ces informations pour cibler les destinataires en fonction de critères précis. Cette pratique peut aller du harcèlement sur de nombreux comptes à l'envoi de messages vulgaires dans leur boîte de réception Twitter. Selon une analyse des captures d'écran de

l'application Tek Fog fournies par le lanceur d'alerte, les femmes journalistes et les musulmans sont les personnes les plus souvent visées. C'est une nouvelle façon malveillante orchestrée par le BJP de disséminer un récit mensonger et de nourrir la haine entre les différentes communautés.

Le média indien a pu vérifier que, sur une période de quatre mois début 2021, 18 % des réponses reçues par les 280 femmes journalistes les plus suivies sur Twitter émanaient de comptes pilotés par Tek Fog. *« Le parti le plus puissant d'Inde dépense ses ressources pour abuser des femmes afin de les faire taire. C'est le prix que les femmes paient pour exister sur les médias sociaux… »*, écrit Sagarika Ghose, une des femmes journalistes concernées qui a 4,1 millions de followers.[2]

Elle a également tweeté *« #TekFog n'est pas une application anonyme : ses manipulateurs sont politiquement alignés. Il n'est pas étonnant que l'élite du pouvoir en Inde se taise. Leur silence a permis et a normalisé cet abus malveillant à l'encontre des femmes. Et demain, ce pourrait être vos filles »*.[3]

Modification de nouvelles existantes pour créer des *fake news*

Une autre fonctionnalité avancée de Tek Fog démontrée par le lanceur d'alerte anonyme consiste à modifier des mots-clés dans des articles d'actualité en ligne pour créer des *fake news* (par exemple, « BJP » remplacé par « Congrès » ou « gauche » par « droite »), ou encore de générer des *junk news* politiques avec un récit fictif en modifiant le lien d'un article publié.

Le lanceur d'alerte a fourni également à l'équipe de *The Wire* un lien internet qui pointait vers une version falsifiée d'un article rédigé pour le journal en ligne *The Print*, comme preuve de l'efficacité de cette fonction. La chaîne d'interrogation du lien truqué contenait un code intégré qui renvoyait à une page web ressemblant à une page de la publication originale, mais le titre et certaines parties du texte avaient été modifiés, détournant ainsi les propos de l'auteur (*The Wire* en propose des captures d'écran dans son article[4]). L'article généré est très réaliste, et il conserve le style et le ton de l'original. Si vous ignorez l'existence de Tek Fog, vous n'avez aucune raison de soupçonner que vous lisez un faux article.

Outre les fonctionnalités mentionnées ci-dessus, la nature sophistiquée de l'application permet à ses utilisateurs de détruire toutes les preuves compromettantes de leurs activités, de ne laisser aucune trace. Deux entreprises indiennes de technologies, Persistent Systems et Mohalla Tech Pvt. Ltd (propriétaire du très populaire réseau social ShareChat), ainsi que Devang Dave, l'ancien responsable national des médias sociaux et de l'informatique du BJYM (le parti des jeunes du BJP)

et actuel responsable des élections pour le BJP dans le Maharashtra, ont été accusés d'avoir développé l'application Tek Fog, mais ils nient tout rapport avec celle-ci. Devang Dave a également accusé *The Wire* d'*« utiliser un jargon technique pour tromper tout le monde »*[5].

Une session YouTube Live, organisée par *The Wire* avec des spécialistes des technologies numériques, a prolongé la publication de la série d'articles afin d'aller davantage au cœur du sujet[6]. À mesure que les plateformes de médias sociaux gagnent en popularité, la bataille politique se déplace sur internet, avec un impact de plus en plus fort du discours en ligne sur les croyances et les opinions individuelles.

La possibilité que des hommes politiques ou des acteurs privés sans scrupule détournent ces plateformes est une atteinte sans précédent à la liberté d'expression et d'affiliation politique qui doit être garantie à tous les citoyens. L'usage d'une telle application est une atteinte délibérée à la démocratie. Il constitue également une violation de l'Information Technology Act of India, institué en 2000 selon lequel l'utilisation d'applications comme Tek Fog contre des citoyens indiens est en contradiction avec la loi indienne, qui considère le piratage des ressources informatiques comme une infraction pénale.

Les logiciels tels que Tek Fog violent le droit à la vie privée et à la liberté d'expression politique, tout en manipulant le processus électoral au moyen des réseaux sociaux, dont les intérêts restent avant tout commerciaux. L'usage de cette application malveillante constitue une menace sérieuse pour tous les aspects de la vie des citoyens indiens, quant à leurs opinions politiques, religieuses, ou à leur genre. Le danger existe donc que de telles applications, même sous une forme moins sophistiquée, soient utilisées à des fins politiques dans d'autres pays, transgressant les normes démocratiques et brisant la garantie d'un discours public libre et indépendant, deux éléments intrinsèques aux principales démocraties de ce monde.

Bien qu'il n'y ait pas en Inde de législation spécifique sur les réseaux sociaux, le gouvernement de Narendra Modi a pris diverses mesures afin de réguler davantage internet. Ces dispositions visent à lutter contre les *« évolutions inquiétantes »*, notamment les fausses nouvelles, les images altérées des femmes et les propos injurieux, ainsi que contre la criminalité, le terrorisme et l'incitation à troubler l'ordre public. En conséquence, le gouvernement s'arroge le droit de notifier aux plateformes qu'un élément d'information est illégal ou encore de superviser le respect par les sites d'information de l'obligation qui leur est faite d'adhérer à un code de déontologie. En outre, lorsque cela s'avère nécessaire pour garantir la sécurité nationale ou lutter contre la criminalité, les plateformes de médias sociaux doivent permettre aux autorités d'identifier les auteurs de messages privés[7]. Le gouvernement a largement abusé de ces dispositions en invoquant la

sécurité intérieure, ce dont plusieurs incidents récents témoignent.

Sources :

1. « Tek Fog : An App with BJP footprints for cyber troops to automate hate, manipulate trends », Anshuman Kaul, Devesh Kumar, *The Wire*, thewire.in, January 6, 2022.
2. « Tek Fog in action : targeting women journalists, pushing communal narrative on COVID, Delhi violence », Anshuman Kaul, Devesh Kumar, *The Wire*, thewire.in January 14, 2022.
3. Tweet de Sagarika Ghose, twitter.com/sagarikaghose/status, January 9, 2022.
4. « Tek Fog: morphing URLs to make real news fake, “Hijacking” WhatsApp to drive BJP propaganda », Anshuman Kaul, Devesh Kumar, *The Wire*, thewire.in, January 10, 2022.
5. Tweet de Devang Dave, twitter.com/DevangVDave/status, January 6, 2022.
6. « Tek Fog — Dangerous new world | The Wire LIVE | The Wire Investigates | #TekFog », *The Wire*, youtube.com, January 17, 2022.
7. « India’s misguided war on social media », Kate Jones, *World Politics Review*, worldpoliticsreview.com, June 1er, 2021.