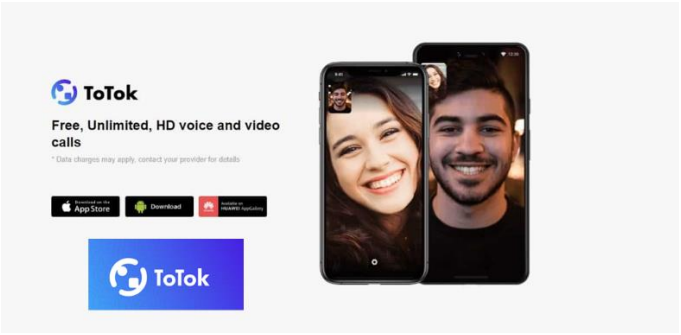
Le polémique sur l'application chiffrée TOTOK accusée de construire un narratif trompeur pour commercialiser un logiciel espion

par MSIE 41 de l'EGE

Crédit Deutsches Spionagemuseum Berlin



Crédit ToToK.ai

L'application de communication ToToK : la création d'un besoin par l'élimination de la concurrence, une promotion massive et un succès fulgurant

Lancée le 04 aout 2019 à Abu Dhabi, l'application de messagerie instantanée ToToK permet d'effectuer des appels voix et vidéo, le partage de données et des appels de groupe jusqu'à 20 participants en haute définition. La messagerie serait sécurisée dans la mesure où elle met en œuvre des protocoles de chiffrement réputés robustes (AES256, TLS/SSL, RSA2048 and SHA256).

Elle se présente comme une alternative gratuite aux célèbres messageries WhatsApp, Telegram, FaceTime, Facebook Messenger ou encore Signal, et cible en premier lieu les travailleurs expatriés aux émirats arabes unis (EAU) qui souhaitent communiquer avec leurs amis, leur famille et finalement entre eux au sein d'une grande communauté ToToK.

Si son succès est fulgurant, c'est surtout que les autorités émiraties ont créé ce besoin. En effet, en raison de l'approche très stricte de la vie privée et de l'application de la censure aux Emirats, les applications de communication classiques sont interdites ou soumises aux restrictions de fonctionnalités imposées par le gouvernement local. C'est ainsi que les utilisateurs réguliers de Skype, de FaceTime et WhatsApp (…) sont bloqués et doivent passer par un VPN[1], lorsque celui-ci n'est pas lui-même entravé, s'ils veulent utiliser leur application chiffrée.

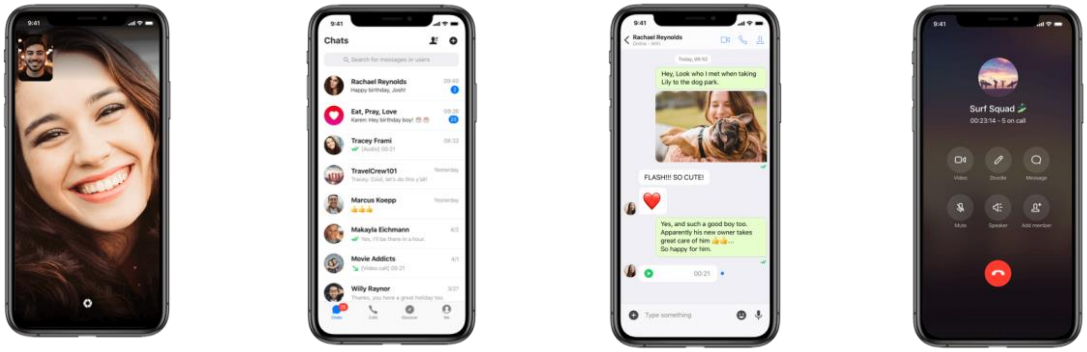

«تو توك»
منصة مكالمات متكاملة بجودة عالية

La promotion de l'application ToToK توتوك dans le média en langue arabe Al-Ittihad, média détenu par le gouvernement des EAU, est faite à deux reprises en aout 2019.

L'article insiste sur la gratuité de l'application, l'absence de publicité, l'utilisation d'Intelligence artificielle pour améliorer la qualité de communication et surtout, le fait que cette application n'est pas bloquée aux Emirats.

Source : https://alittihad.pressreader.com/al-ittihad/20190829

Dans ce contexte, ToToK arrive subitement à l'été 2019 sur un marché sans concurrence aux émirats, c'est « la seule application VoIP + Vidéo -chiffrée- qui fonctionne ici » disent les expatriés. Elle est alors disponible sur les magasins d'application App Store d'Apple et Play Store de Google. Entre août et septembre 2019, elle va enregistrer près de 8 millions de téléchargements cumulés sur les deux magasins d'application IOS et Android. Il est vrai que les développeurs ont eu la bonne idée de donner à leur messagerie un nom très proche du phénomène Chinois des réseaux sociaux **TikTok**, avec laquelle elle ne doit pas être confondue, ce qui leur offre une visibilité remarquable dans le monde entier.



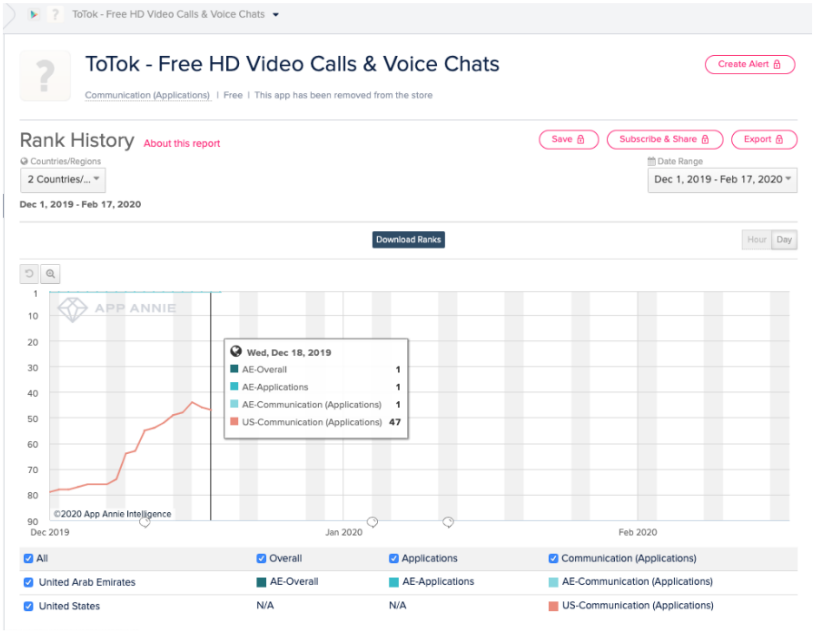
Photos tirées du site https://totok.ai le 16 octobre 2019 (via Waybackmachine sur Web.archive.org).

Courant 2019, des publicités semi-officielles font la promotion de ToToK comme étant l'application gratuite, longtemps recherchée par les émiratis. En décembre, les usagers de la messagerie payante BOTIM recevront même une alerte sur leur téléphone, leur demandant de basculer vers la nouvelle application gratuite, qualifiée de rapide, gratuite et sécurisée. Pour les y aider, un lien pour l'installation de ToToK est inclus dans le message. Le géant chinois des télécommunication Huawei fait aussi la promotion de ToToK[2], en proposant sur ses sites Internet de télécharger l'application qu'il décrit aussi comme gratuite, rapide et sécurisé, selon la formule consacrée par les émiratis.
Rapidement l'application gagne en popularité non seulement au moyen orient (EAU, Arabie Saoudite), mais aussi en Europe (Royaume Uni, Suède), en Asie et en Afrique, ce qui se comprend aisément lorsque l'on considère aux EAU une population composée à plus de 90% d'émigrés avec un besoin permanent d'échanges avec leurs proches restés à l'étranger. Si certains expatriés trouvent suspecte l'apparition d'une application gratuite, sans publicité et sans achat intégré, d'ailleurs la seule à toujours être non bloquée par les autorités, il demeure que la majorité des usagers n'est pas sensibilisée à la Cyber défense ou à la protection des données personnelles : circulez, il n'y a là, pas de sujet !

Un succès, aussi aux Etats-Unis…

Quant aux Etats-Unis, ToToK devient l'une des applications sociales parmi les plus téléchargées sur son territoire, la semaine du 09 décembre 2019. A ce moment, l'AppStore

d'Apple la classe 4ème application de la catégorie « réseaux sociaux », juste derrière WhatsApp, numéro 3.



Le succès prendra fin les 19 et 20 décembre 2019, à la suite des retraits de ToTok des magasins d'applications Google Play et App Store.

Source :
App Annie[3], société d'analyse des données mobiles (voir data.ai).

… puis la suppression des magasins d'application App Store et Google Play

Quelques temps avant la publication d'un article sur ToTok, trois journalistes du New York Times contactent les géants Google et Apple. Ils évoquent avec eux un article à paraître fin décembre, des soupçons d'espionnage étatique et leur demandent s'ils ont connaissance d'éléments sur les liens entre le gouvernement des EAU et ToTok. Les représentant des deux entreprises américaines répondent qu'ils vont investiguer.

Le jeudi 19 et le vendredi 20 décembre 2019, l'application mobile ToTok est supprimée des deux magasins d'application (voir illustration App Annie ci-dessus). Google évoque la violation de règles d'utilisation non spécifiées, Apple continue son investigation d'après son service de communication.

L'application reste utilisable pour tous les usagers qui l'ont installée, et pour ceux qui se rendent directement sur le site de ToTok ou de Huawei.

Depuis les Etats-Unis, le NYT accuse ToTok d'espionnage de masse et livre une enquête approfondie

Le 22 décembre 2019, le NYT publie l'enquête des journalistes, Mark Mazzetti, Nicole Perlroth et Ronen Bergman, intitulée **It Seemed Like a Popular Chat App. It's Secretly a Spy Tool**[4]. Ils y accusent les services de renseignement émiratis d'avoir un accès direct aux messages et aux conversations vidéo échangées sur l'application ToTok.

Le rapport accuse le gouvernement des EAU de suivre les conversations, les déplacements en temps réel, les relations, les rendez-vous, d'enregistrer les sons et les images des usagers de l'application. Effectivement, pour utiliser l'application, les utilisateurs autorisent l'accès à leur microphone, leur calendrier, leur localisation, leur caméra et leur Wi-Fi, de telle sorte qu'il livre lui-même tous ses contenus en toute légalité.

Patrick Wardle est un expert cyber privé, spécialisé en vulnérabilités informatiques, avec une expérience de 2 ans comme auditeur à la NSA. Il a effectué des analyses forensiques[5] au profit du NYT, qui permettent de compléter ces recherches. D'après lui, ToTok serait une copie de la messagerie chinoise YeeCall, légèrement reprise et customisée pour des publics arabophone et anglophone. Il traquerait les positions et les contacts des usagers, au prétexte de leur donner une météo précise et de leur proposer une mise en relation avec leurs amis.

Un ancien de la NSA : « de la beauté dans cette approche d'espionnage »

Les clauses de confidentialité[6] mentionnent bien que les données personnelles peuvent être partagées avec les entreprises du groupe ("We may share your personal data with group companies"), les Services de l'Etat, les agences, les officiels, les usagers, toute organisation, etc. Elles comportent même onze fois la mention share your personal data.

L'analyste conclut qu'il y a « de la beauté dans cette approche » de renseignement, et qu'au lieu de dépenser 2.5 millions de dollars, selon sa grille de tarifs pour développer un exploit permettant d'accéder au téléphone Android d'une cible, il suffisait de l'inciter à télécharger cette application. Ainsi, volontairement mais sans le savoir, la cible communique elle même toutes les informations recherchées.

Son expérience d'analyste à la NSA lui permet de proposer un scénario-type d'une opération de collecte de renseignement dont ToToK serait la première étape. L'étape suivante consisterait à stocker puis à traiter les données avec des capacités de stockage remarquables, des compétences en Big Data, en analyse de données et en Intelligence artificielle. Et c'est justement ce que propose la société PAX AI[7]. Cet ancien département émancipé de DarkMatter en 2019 a pris beaucoup d'importance dans les domaines de l'Intelligence artificielle, du traitement massif des données, des technologies mobiles ainsi que du stockage (cloud and high performance Computing). Il peut tout à fait gérer les énormes stocks de données générés par ce type d'opération de collecte de renseignement.

Derrière ToToK, un écosystème complexe d'entreprises, mêlant cyberdéfense, renseignement et intelligence artificielle

L'enquête se prolonge le 02 janvier 2020 par une publication des recherches en OSINT[8] de Bill Marczak[9], un chercheur de Citizen Lab[10] à Toronto, spécialiste en cyber sécurité avec un tropisme vers les droits humains et la sécurité. Il révèle et nomme les liens entre les officiels émiratis et l'écosystème d'entreprises qui alimente leurs Services de renseignement : DarkMatter[11], Group 42, PEGASUS LLC[12] réorganisée et renommée PAX AI. Ayant eu recourt à un même certificat TLS, Il révèle la reprise du logiciel chinois YeeCall[13] par ToToK, via les entreprises émiraties Breej Holding, G42, l'entreprise chinoise YiKuaiHuDong Beijing Technology Co Ltd, et une phase transitoire où l'application ToToK s'appelle G42 IM avant de devenir ToToK en juillet 2019.

L'enquête du NYT sera ensuite mise à jour le 14 aout 2020 avec des éléments complémentaires sur l'enquête du FBI sur DarkMatter, sur PAX AI et leur réorganisation dans un conglomérat autour de la cyberdéfense.

La réponse rassurante de ToToK à sa communauté : une difficulté technique en cours de résolution

Le 23 décembre 2019, soit le lendemain suivant l'article du NYT et 3 jours après le retrait des deux principaux stores, l'éditeur de l'application effectue une première communication :

Sur son site, il s'adresse à la communauté ToToK, qu'il remercie et évalue – d'ailleurs très avantageusement- à plusieurs dizaines de millions de personnes dans plus de 100 pays. Il rapporte des témoignages incarné et émus : Tanveer qui, grâce à ToToK, arrive à parler à sa famille à l'étranger, Lutheramani qui recommande cette application « si pratique et agréable ». Ensuite, l'éditeur évoque les hauts standards de sécurité qu'il implémente tels que AES256, TLS/SSL, RSA and SHA256. Il rappelle que la protection de toute la communauté est au centre des préoccupations de ToToK, comme le respect de la vie privée conformément aux lois locales et internationales. Enfin, puisqu'il faut taire la rumeur, il est dit que l'application est temporairement inaccessible, simplement en raison d'une difficulté technique, que Google, Apple et ToTok sont d'ailleurs déjà bien engagés à résoudre.

Cette communication de crise délivre aux utilisateurs un narratif qui se veut rassurant, obfusquant les accusations portées par le NYT derrière la promesse de nouvelles

fonctionnalités, et une coopération enthousiaste et prometteuse avec les deux géants américains. Le rédacteur, à ce stade anonyme, rappelle que les téléchargements restent possibles sur leur propre site et sur les sites des constructeurs Coréen Samsung et chinois Huawei et Oppo. Surtout, les communicants de ToToK ont intégré l'idée que la perception de l'information est une question de liens et de communauté et, à partir de cette date, ils adresseront les prochains épisodes de leur narratif dans des « note(s) to the ToToK community »[14].

Giac et Long, les co-fondateurs honnêtes et loyaux de ToToK, et l'ex-analyste de la NSA

Le 24 décembre, les communicants de l'application émiratie se nomment enfin. Il s'agit de Giac et de Long qui, sans se présenter, signent leur article avec l'attache « co-fondateurs de ToToK ». Ce binôme, altruiste et soucieux, met en avant son ouverture d'esprit, son honnêteté et sa loyauté envers la communauté. Leur travail à son profit, au centre de toutes leurs attentions, leur procure bien-être et même bonheur. Ils n'ont pas voulu donner de l'importance à ceux qui ont construit les mensonges d'espionnage organisé, ceux qui ont tenté de vilipender leur travail, mis en péril l'entreprise puis insulté les utilisateurs en se moquant de leur enthousiasme pour ToToK. Mais il faut maintenant répondre par des faits, les voici donc :

- La sécurité et le respect de la vie privée des utilisateurs ToToK est leur priorité,
- Un ancien analyste de la NSA a effectué une étude technique qui conclut que « ToToK fait ce qu'il dit faire, rien de plus, donc pas d'exploit informatique, de backdoor ou autre malware ».

Le discours[15] de GIAC et Long oppose leurs propres valeurs d'ouverture et de transparence à l'agressivité de leurs détracteurs, ces derniers faisant la promotion de la peur, de la haine et souhaitant empêcher les gens de communiquer entre eux. Giac et Long cherchent à disqualifier l'étude technique du NYT en présentant les conclusions de leur propre ancien expert de la NSA, mais sans le nommer et sans aucun argument technique. Ils suggèrent avec ironie que ces résultats sont connus de l'agence d'espions américains (la NSA), à l'origine des diffamations.

Ce communiqué de ToToK, plus construit et agressif que le premier, est repris in extenso dès le 25 décembre par le média émirati en langue anglaise Gulf News.

Le contre discours dans les médias émiratis : le rôle et le positionnement de Gulf News

Gulf News est le premier quotidien anglophone des Emirats arabes unis. Il est toutefois fréquemment épinglé pour son manque de transparence, sa censure, le relai de la propagande émiratie, les informations non sourcées ou aux sources douteuses et les fausses informations. Sa proximité avec les personnages important du pouvoir est aussi relevée, notamment le Ministre d'Etat des Finances Obaid Humaid Al Tayer, qui se trouve aussi être le président d'Etisalat (principale firme de télécommunications et de services Internet, détenue majoritairement par l'Etat).

- **Overall, we rate Gulf News Questionable based on poor sourcing, a lack of transparency, the promotion of state propaganda, and a few failed fact checks.**

Detailed Report

Reasoning: **Poor Sourcing, Propaganda, Lack of Transparency, Censorship, Failed Fact Checks**
Bias Rating: **RIGHT**
Factual Reporting: **MIXED**
Country: **United Arab Emirates**
Press Freedom Rating: **LIMITED FREEDOM**
Media Type: **Newspaper**
Traffic/Popularity: **High Traffic**
MBFC Credibility Rating: **LOW CREDIBILITY**

Media Bias / Fact Check

Ci-contre, au 27 septembre 2022, l'évaluation de l'objectivité et de la crédibilité du média Gulf News par le site MBFC media bias fact check.

Citizen Lab retrouve Giac et Long dans le cache de Google… au sein de Group 42

A la suite de ce communiqué, Bill Marzack prolonge ses recherches OSINT et identifie Giac et Long à Giacomo Ziani et Long Ruan. Effectivement, le chercheur de CitizenLab a retrouvé dans le cache du moteur de recherche Google, les traces de leurs comptes LinkedIn et Twitter :
En décembre 2019, Giac était encore employé par Group 42, comme Marketing and Communications Manager, Long était chief operating officer de YeeCall depuis septembre 2017.
Entre les 21 et 27 décembre 2029, en début de crise, leurs profils Twitter et LinkedIn sont modifiés et antidaté à août 2019, de manière à les faire correspondre au narratif initié le 23 décembre : ils se présentent maintenant, respectivement et rétroactivement, comme ToToK : Co-Founder-Head of Business et ToToK : Co-Founder Head of technology.

Réaction de l'autorités de régulation des télécommunications émiraties (TRA)

Le 27 décembre 2019, l'autorité de régulation des télécommunications émiraties[16] réagi par une communication officielle relayée immédiatement dans un article du Gulf News, UAE law strictly prohibits espionage, TRA responds to ToTok.

Le logo du TRA, https://tdra.gov.ae/

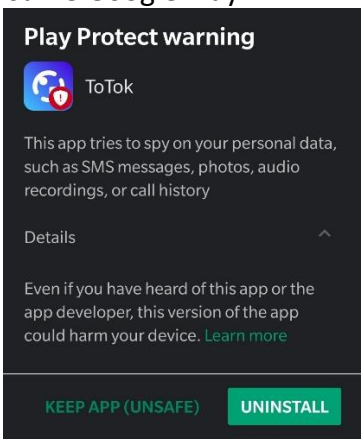
Le TRA annonce qu'il étudie les allégations concernant la politique de confidentialité des applications de communication voix et vidéo aux EAU, incluant ToToK. Cette communication de crise, habile, a pour effet de replacer ToToK parmi les autres applications de communication, puis de diluer cette affaire dans un discours encourageant l'entreprenariat aux EAU et le soutien aux nouvelles technologies[17]. Le TRA rappelle que toutes les applications sont évaluées de façon continue et non définitive, que l'espionnage est strictement interdit, et qu'elle veille bien évidemment à la protection de la vie privée des usagers.
Le rédacteur anonyme de la dépêche Gulf News évoque un débat animé autour du retrait de l'application de l'Apple store.

Giac s'adresse à Google et Apple : « ToToK adhère maintenant à toutes les exigences »

Le 27 décembre, GIAC aborde un nouvel épisode dans sa communication de crise. Dans un message d'1 minute 36 secondes, adressé à Apple et Google, il demande avec déférence aux deux entreprises américaines de soutenir la « startup » qui se trouve dans une situation très difficile. Il nie tout lien avec un gouvernement, comme les EAU, les Etats-Unis ou la Chine. Il ouvre le dialogue, les invite dans les bureaux de l'entreprise et annonce qu'il ont travaillé très dur avec leurs équipes et celles des américains, de telle sorte que Maintenant, ToToK adhère strictement à chacune de leurs exigences.
Giac demande la restauration de ToToK sur les magasins d'application. Reprenant son narratif initial, il ajoute que la communauté dépend d'eux, que des millions de personnes attendent pour communiquer avec leurs familles et leurs amis, particulièrement en cette période de vacances. Pourtant, à ce stade, quels que soient les discours de Giac, rien n'empêche les millions d'usager de ToToK de communiquer entre eux, seuls les nouveaux téléchargements depuis les stores américains étant supprimés, certes avec une mention de soupçons d'espionnage pour Google Store (voir play protect ci-dessous).

Le soutien des médias locaux et de l'autorité de régulation des télécommunications

Dès le lendemain, Gulf News reprend -à nouveau- le communiqué de l'entreprise émiratie. Le média en ligne indique que l'autorité de régulation des télécommunications émiraties (TRA) suit de près plusieurs applications de communication aux EAU. Dans la soirée, le TRA fera une déclaration officielle certifiant que les applications certifiées respectent strictement tous les standards, incluant ToToK. Le communiqué est diffusé largement par les médias locaux[18], sans autre commentaire, mais avec un lien alternatif pour télécharger l'application.
Si Apple ne reviendra pas sur sa décision, du côté de Google la manœuvre est payante. Ainsi, le 04 janvier 2020, avec le soutien des médias locaux et des autorités, ToToK fait son retour sur le Google Play.



Pourtant, ToToK ne retrouvera pas son succès initial, n'arrivant pas à entrer dans le top des 1700 meilleures applications référencées et sera à nouveau supprimée du magasin le 15 février, officiellement pour ces raisons d'échec commercial : l'application n'intéresse personne, elle disparait du magasin.
La nouveauté, c'est que le service anti-malware d'Android, Google Play Protect, affiche une mise en garde inquiétante à l'usager et lui demande de désinstaller l'application pour des raisons très explicites d'espionnage des données personnelles.

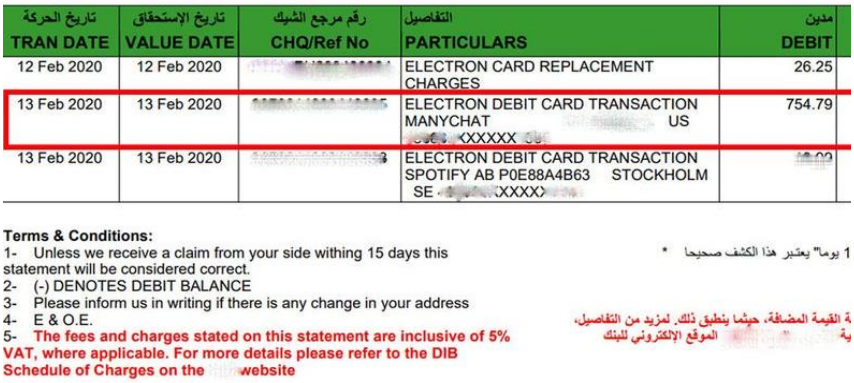
Un changement de stratégie vis-à-vis d'Apple : le danger des applications malveillantes de l'Apple Store

Le quotidien Gulf News, aux émirats arabes unis, tente l'exploration d'une nouvelle voie le 13 février 2020.

Yousra zaki est une jeune et sympathique égyptienne, spécialisée en journalisme et en relations publique, passée par des études de Média à Toronto et de Mass Communication à l'American University of Sharjah. En 2020, elle est chroniqueuse et écrit dans le média Gulf News, dans les colonnes hôtellerie, alimentation, culture et lifestyle. Elle écrit d'ailleurs "I can write about anything I want, as long as it's a great story to tell".

image credit GulfNews

Dans un article court et simple à comprendre, la chroniqueuse Yousra zaki explique comment, en toute bonne foi, elle s'est fait voler 199 US $ de son compte Apple parce que l'opérateur Apple avait autorisé sur son magasin d'applications, une application malveillante usurpant ToTok.

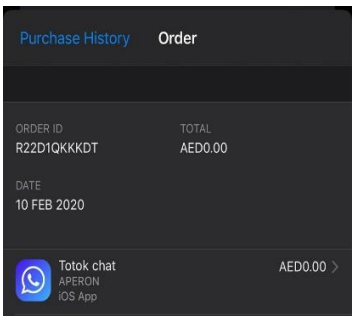


تاريخ الحركة TRAN DATE	تاريخ الإستحقاق VALUE DATE	رقم مرجع الشيك CHQ/Ref No	التفاصيل PARTICULARS	مدين DEBIT
12 Feb 2020	12 Feb 2020		ELECTRON CARD REPLACEMENT CHARGES	26.25
13 Feb 2020	13 Feb 2020		ELECTRON DEBIT CARD TRANSACTION MANYCHAT US XXXXX	754.79
13 Feb 2020	13 Feb 2020		ELECTRON DEBIT CARD TRANSACTION SPOTIFY AB P0E88A4B63 STOCKHOLM SE XXXX	

Terms & Conditions:
1- Unless we receive a claim from your side withing 15 days this statement will be considered correct.
2- (-) DENOTES DEBIT BALANCE
3- Please inform us in writing if there is any change in your address
4- E & O.E.
5- **The fees and charges stated on this statement are inclusive of 5% VAT, where applicable. For more details please refer to the DIB Schedule of Charges on the website**

1 يوما" يعتبر هذا الكشف صحيحا *

ة القيمة المضافة، حيثما ينطبق ذلك. لمزيد من التفاصيل، ية الموقع الإلكتروني للبنك



La jeune femme a pris soin de faire des copies d'écran de ses achats gratuits.

Produisant de nombreuses copies d'écrans des différentes étapes de son achat de l'application, et même son relevé bancaire, elle raconte ses déconvenues dans un narratif

plaisant, jamais agressif envers Apple. La chroniqueuse est soucieuse de ses données personnelles, elle a même pris le soin de flouter les informations critique.
Dans cette histoire simple et abordable par tous, les employés d'Apple -Meghan puis Jamie- sont très sympathiques, mais n'arriveront pas à aider la jeune et sympathique Dubaïote.
Le narratif est simple : puisque ToToK n'est plus sur Apple store, les jeunes dubaïotes branchés qui souhaitent échanger avec leur amis et leur famille ne le peuvent plus et sont exposés aux fausses applications usurpant ToToK, que l'on découvre malveillantes, qu'Apple a pourtant autorisé sur son site.

ToToK met en avant le rôle double d'opérateur et de concurrent d'Apple et de Google

En février 2020, ToToK tentera un ultime narratif avec de nouveaux arguments. Dans un communiqué du 20 sur leur site, la startup cherche à attribuer la suppression définitive et la mise en garde de Play Protect à ceux qui occupent la position dominante du marché des applications, Google et Apple. Bien qu'ils soient ultradominant, il s'agit de répandre l'idée qu'ils redoutent la concurrence de la startup aux 10 millions de téléchargements.
L'entreprise émiratie tente de leur mettre la pression en leur opposant les plateformes Samsung, Huawei, Xiaomi et Oppo, en plus de leur propre site totok.ai. Dans un contexte de découplage Sino-américain, c'est un argument pertinent mais qui ne changera pas les positions officielles d'Apple et Google.

L'erreur de ToToK : s'attaquer -involontairement- aux ressortissants américains alors que l'écosystème cyber émirati est déjà dans le viseur du FBI ?

Dès le 29 janvier 2019, l'agence REUTERS indique qu'une enquête du FBI est en cours depuis les Etats-Unis sur l'écosystème cyber émirati (Darkmatter et entreprises affiliées, PEGASUS, PAX AI, etc.). Sous couvert de lutte contre le terrorisme, ces entreprises auraient bénéficié des services d'anciens du renseignement américain et de membres des services de sécurité émiratis. En résumé, il s'agit d'activités « Hackers-for-Hire » des anciens espions ingénieurs cyber, experts en exploits et autres pénétrations de systèmes, en violation des lois ITAR[19]. Il est toutefois compliqué de discerner formellement si ces activités ont vraiment pu se faire sans l'approbation des services de renseignement américains.
Les reproches sont graves et concernent des crimes, de l'espionnage numérique de personnalités du Golfe (dont un Vice-Premier Ministre turc et l'Emir du Qatar), d'opposants politiques locaux ou étrangers, de dissidents, de journalistes étrangers ou encore de militants des droits humains.
Le 7 septembre 2021, au moment où ToToK débute sa « success story » sur les magasins d'applications américains, l'enquête du FBI débouche sur la condamnation des trois anciens employés de la communauté du renseignement américain et de l'Armée US. Ils concluent un accord avec le département de la justice américaine (DOJ) pour éviter la prison, mettre fin aux poursuites et à les concernant. Ils sont notamment condamnés au paiement d'1.685.000 US Dollars de pénalités, à la restriction de leurs activités futures et au bannissement à vie de toute habilitation de sécurité.
La concomitance de la judiciarisation de DarkMatter aux Etats-Unis (agence REUTERS concernant RAVEN) et des affaires relevées par le New York Times (ToToK) n'est donc pas surprenante. Elle a déclenché la suppression de l'application ToToK des magasins des géants américains Apple et Google.

En définitive, l'étude fine des narratifs ToToK a révélé la présence de nombreux acteurs :

Un écosystème de cyber-renseignement étatique complexe, utilisant des sociétés écran, une participation d'experts -anciens agents de la NSA, dénoncée par la justice américaine et que les Services américains auraient aidé à structurer, au nom de la lutte contre le terrorisme. Une application chinoise, une nouvelle application permettant la collecte et vraisemblablement

l’analyse de toutes les données personnelles, les échanges et les déplacements des usagers de ToToK. Un logiciel espion par consentement, car finalement, les usagers veulent bien y consentir, dans la mesure où il n’y a pas accès à une solution alternative.
ToTok a-t-elle été débordée par son succès aux Etats-Unis ? A-t-elle manqué de coordination avec son entreprise mère ? A-t-elle fait les frais des opérateurs et concurrents américains ? Les officiels émiratis ont-ils pêché par excès de confiance ou sentiment d’impunité ?

Liens et principaux sites consultés :

https://totok.ai/news-feb20-2020
https://totok.ai/download-android
https://alittihad.pressreader.com/al-ittihad/20190829
https://totok.ai/news-feb20-2020
https://totok.ai/download-android
https://totok.ai/privacy
https://gulfnews.com/uae/government/uae-law-strictly-prohibits-espionage-tra-responds-to-totok-allegations-1.1577469674071
https://gulfnews.com/uae/i-downloaded-a-fake-totok-app-and-they-stole-199-from-my-apple-pay-account-1.1581578051115
https://www.numerama.com/cyberguerre/607163-lapp-de-messagerie-accusee-despionnage-totok-a-completement-rate-son-comeback.html
L'application App Annie, devenue data.ai : https://www.data.ai/apps/all-stores
https://mediabiasfactcheck.com/gulf-news/
https://www.courrierinternational.com/notule-source/gulf-news
https://www.vice.com/en/article/dyg8qv/google-reinstates-reported-uae-surveillance-app-totok
https://appgallery.huawei.com/app/C101085053?appId=C101085053&source=appshare&subsource=C101085053
https://proteuscyber.com/fr/privacy-database/news/5156-us-fines-former-nsa-employees-who-provided-hacker-for-hire-services-to-uae-the-record-by-recorded-future
https://www.justice.gov/opa/pr/three-former-us-intelligence-community-and-military-personnel-agree-pay-more-168-million
https://www.liberation.fr/planete/2019/02/04/des-cybermercenaires-americains-a-abou-dhabi_1707198/
https://www.reuters.com/investigates/section/usa-raven/

---

[1] VPN : Un Virtual private Network permet de chiffrer les données échangées, dans un « tunnel » établi entre l'usager et des serveurs VPN afin de consulter des ressources ou de communiquer sur Internet. L'échange est rendu inintelligible (« noirci ») pour le fournisseur d'accès ou les Services gouvernementaux.
[2] Au 11/01/2023, l'application est toujours proposée sur le site de Huawei, avec 78 millions de téléchargements et une mise à jour en date du 04 janvier 2023.
[3] App Annie, spécialisé dans les données et l'analyse du marché des apps mobiles, est devenue data.ai en février 2022.
[4] Accessible en suivant le lien https://www.nytimes.com/2019/12/22/us/politics/totok-app-uae.html
[5] Dans ce contexte, l'analyse forensique est une étude fine qui permet de caractériser un logiciel en extrayant des données, analysant son comportement, le comparant, en mettant en corrélation des traces suspectes et des données de différents fichiers, etc.
[6] https://totok.ai/privacy/
[7] AI pour *artificial Intelligence*. PAX AI est le nouveau nom donné à l'entreprise PEGASUS en 2019.
[8] OSINT : Open Source Intelligence, recherches de renseignement (d'origine) en sources ouvertes aussi appelé ROSO en français.
[9] https://billmarczak.org/
[10] https://citizenlab.ca/
[11] Réorganisée en 2019-2020, DarkMatter était une firme de CyberIntelligence installée à Abu Dhabi, réputée pour des hackings. Elle a fait l'objet d'enquête du FBI et de poursuites par la justice américaine.
[12] PEGASUS LLC ne doit pas être confondue avec le logiciel homonyme de l'entreprise israélienne NSO
[13] En décembre 2019, YeeCall était présentée sur Google Play comme une application libre et non bloquée de vidéo and VoIP pour les usagers des EAU, Arabie saoudite, Oman, Qatar, Egypte, Inde, Pakistan, Bangladesh, Philippines, Etats-Unis (…). Ces pays fournissent la majorité des expatriés aux EAU. Consulté en 2023, l'application n'y est plus proposée, tout comme sur App Store IOS.
[14] Voir à cet effet le site de ToToK en suivant le lien https://totok.ai/news-dec23, à copier dans l'URL puisqu'il n'est pas accessible directement sur le site totok.ai
[15] https://totok.ai/news-dec24
[16] TRA: The UAE Telecommunications Regulatory Authority, à Abu Dhabi.
[17] Sont citées par le TRA, la 5G, Blockchain, IOT, les applications ayant recours à l'intelligence artificielle AI.
[18] https://www.khaleejtimes.com/tech/uaes-tra-issues-statement-on-totok-app-allegations ou
[19] ITAR: International Traffic in Arms Regulations