Centre de la sécurité des télécommunications Canada
Communications Security Establishment Canada

D96-125/2024F-PDF
ISBN 978-0-660-75010-1

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Manipulation ciblée : campagnes de piratage psychologique et de harponnage de l'Iran

TLP:CLEAR

Canada

À propos de ce rapport

Le présent rapport concerne la menace que représentent les campagnes de pirate psychologique et de harponnage menées par des auteurs de menace parrainés par l'Iran. Il s'adresse aux spécialistes et aux gens qui œuvrent dans des domaines d'intérêt stratégique pour l'Iran, aux spécialistes de la cybersécurité et aux non-spécialistes qui s'intéressent à la cybersécurité. Pour obtenir des conseils sur des mesures d'atténuation techniques des menaces, consultez les conseils du Centre pour la cybersécurité ou communiquez avec le Centre pour la cybersécurité.

La mention TLP:CLEAR doit être utilisée conformément aux règles et aux procédures applicables à la diffusion publique lorsque le risque prévisible d'une utilisation abusive est faible ou négligeable. Tout en étant soumise aux règles standard de droit d'auteur, l'information TLP:CLEAR peut être distribuée sans aucune restriction. Pour obtenir de plus amples renseignements sur le protocole TLP (*Traffic Light Protocol*), prière de consulter le site Web du Forum of Incident Response and Security Teams (en anglais seulement).

Coordonnées

Prière de transmettre toute question ou problématique sur le présent document au Centre canadien pour la cybersécurité (CCC) à contact@cyber.gc.ca.

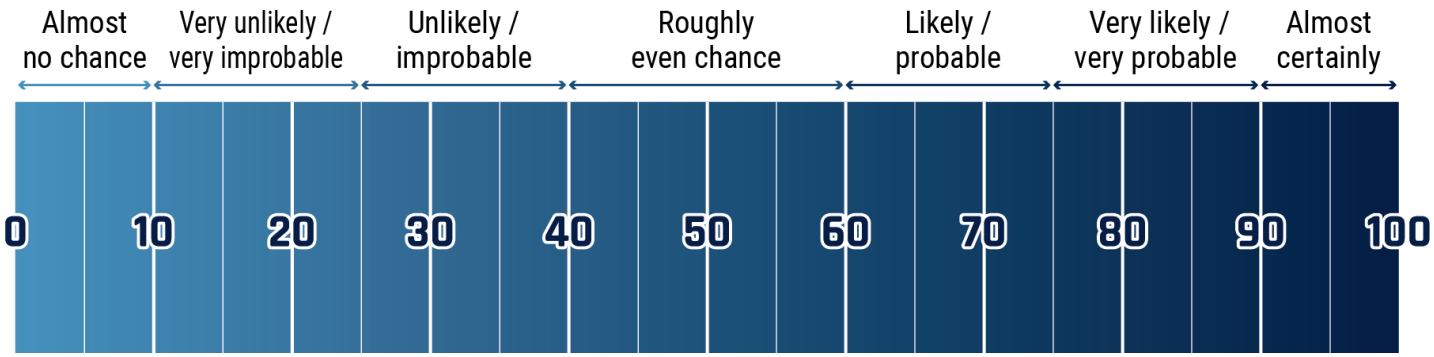
Méthodologie et fondement de l'évaluation

Les avis formulés dans la présente évaluation se basent sur de multiples sources classifiées et non classifiées. Ils sont fondés sur les connaissances et l'expertise en matière de cybersécurité du Centre pour la cybersécurité. Le rôle que joue le Centre pour la cybersécurité dans la protection des systèmes d'information du gouvernement du Canada lui confère une perspective unique des tendances observées dans un contexte de cybermenace, ce qui contribue à la présente évaluation. Le Centre pour la cybersécurité obtient, grâce au volet du mandat du Centre de la sécurité des télécommunications (CST) touchant le renseignement étranger, de l'information précieuse sur le comportement des adversaires dans le cyberespace. Bien qu'il soit toujours tenu de protéger les sources et méthodes classifiées, le Centre pour la cybersécurité fournit, dans la mesure du possible, les justifications qui ont motivé ses avis.

Les avis du Centre pour la cybersécurité sont basés sur un processus d'analyse qui comprend l'évaluation de la qualité de l'information disponible, l'étude de différentes explications, l'atténuation des biais et l'usage d'un langage probabiliste. Le personnel du Centre pour la cybersécurité utilise des formulations telles que « nous évaluons que » ou « nous jugeons que » pour présenter une évaluation analytique. Les qualificatifs tels que « possiblement », « probable » et « très probable » servent à évoquer une probabilité.

Les évaluations et analyses énoncées dans le présent document sont fondées sur les renseignements disponibles en date du **2 février 2024**.

Échelle du lexique des estimations



Principaux avis

Nous estimons que les techniques de piratage psychologique des auteurs de cybermenace iraniens continuent d'être particulièrement sophistiquées et que ces derniers les utilisent pour améliorer leurs capacités de harponnage.

Nous estimons que les auteurs de cybermenace iraniens personnalisent leurs campagnes de piratage psychologique pour en améliorer l'efficacité en créant des personnages convaincants, en établissant des relations avec les personnes ciblées sur une période prolongée et en utilisant du contenu attrayant et fortement émotionnel lié à des questions géopolitiques d'actualité ou à des événements traumatisants.

Nous considérons que les auteurs de cybermenace iraniens déploient des efforts particuliers pour mener leurs campagnes de piratage psychologique et de harponnage afin de cibler les spécialistes qui ont de l'information que l'Iran juge utile sur les plans politiques, économiques ou du renseignement militaire.

Introduction

Selon nos observations, les auteurs de cybermenace iraniens s'appuient sur des techniques de piratage psychologique particulièrement sophistiquées qu'ils utilisent pour améliorer leurs capacités de harponnage. Pour appuyer leurs opérations de harponnage, ces auteurs utilisent des techniques, comme la création de personnages attrayants, se servent de leurres affectifs ou intéressants et établissent une relation à long terme avec les personnes qu'ils ciblent. L'Iran axe ses efforts de piratage psychologique sur les relations professionnelles dans les plateformes de médias sociaux afin d'obtenir de l'information sur les organisations qui servent ses intérêts politiques, économiques et militaires, notamment dans les secteurs de l'aérospatiale, de l'énergie, de la défense, de la sécurité et des télécommunications[1]. Les auteurs de menace iraniens mènent des opérations de piratage psychologique et de harponnage contre des cibles plus faciles, comme les comptes de courriel personnel ou de réseaux sociaux, afin de recueillir de l'information sur les réseaux renforcés du gouvernement ou d'organismes afin d'y avoir accès ultérieurement.

Qu'est-ce que le piratage psychologique?

Le piratage psychologique vise à manipuler une personne afin de la mener à faire quelque chose qui n'est pas dans son intérêt supérieur, comme divulguer des renseignements (données de connexion, informations sensibles, etc.).

Pour réussir une tentative de piratage psychologique, il faut cinq caractéristiques :

- Réciprocité : les gens sentent qu'ils ont l'obligation de régler une dette apparente
- Autorité : les gens répondent aux figures d'autorité
- Rareté : les gens accordent de la valeur aux choses qu'ils perçoivent comme étant rares
- Constance : les gens agissent afin de maintenir leur image sociale
- Preuve sociale : les gens tendent à faire confiance aux personnes qu'ils perçoivent comme étant semblables à eux

Les auteurs de cybermenace exploitent les sites de médias sociaux pour simuler leur légitimité et tromper leurs victimes afin de lancer ultérieurement leurs opérations de harponnage.

Procédé relatif aux campagnes de piratage psychologique sophistiquées de l'Iran

Nous estimons que les auteurs de cybermenace iraniens personnalisent leurs campagnes de piratage psychologique pour en améliorer l'efficacité en créant des personnages convaincants, en établissant des relations avec les personnes ciblées sur une période prolongée et en utilisant du contenu attrayant et fortement émotionnel lié à des questions géopolitiques d'actualité ou à des événements traumatisants.

Figure 1 : Processus de pirate psychologique et de harponnage

Création de personnages attrayants

Les auteurs de cybermenace iraniens créent et exploitent de faux personnages pour établir une relation avec les personnes ciblées et instaurer la confiance. Les relations sont typiquement établies à partir d'intérêts professionnels ou personnels de la victime. Les personnages permettent une approche organisée et interactive pour établir la confiance et l'apparence de légitimité auprès des victimes, et c'est d'autant plus facile aujourd'hui que les « personnalités professionnelles et sociales » d'un plus grand nombre de personnes sont en ligne et impossibles à distinguer de la « personnalité hors ligne ». Nous estimons que les auteurs de cybermenace iraniens ont probablement recours à des personnages de femmes séduisantes pour manipuler leurs cibles[2]. Nous croyons aussi que les auteurs de cybermenace iraniens se servent probablement de comptes de courriel déjà compromis et mystifiés pour donner une impression légitimité à leurs personnages et pour duper ultérieurement leurs victimes.

Les auteurs de cybermenace iraniens ont utilisé de faux personnages pour cibler des personnes qui œuvraient dans divers domaines, notamment :

- Entrepreneurs dans le domaine de la défense
- Personnel de l'industrie de l'aérospatiale
- Personnel du secteur de l'énergie
- Journalistes
- Universitaires
- Communauté de la recherche
- Activistes
- Figures politiques
- Diplomates
- Groupes de la société civile[3]

Étude de cas 1 : Instructrice d'aérobie de Liverpool ou pirate psychologique de l'Iran?

Une autrice ou un auteur de cybermenace iranien a utilisé le faux personnage de Marcella Flores, prétendument instructrice d'aérobie et entraîneuse professionnelle. Le personnage a établi une relation de plusieurs mois avec une personne qui travaillait pour un entrepreneur du secteur de l'aérospatiale.

Le faux personnage a nourri la relation à partir de plusieurs plateformes de communications, tant professionnelles que personnelles. Le personnage a ensuite transmis un maliciel à l'appareil de la victime à partir d'une feuille de calcul Excel déguisée en document de sondage sur l'alimentation[4].

Étude de cas 2 : Mia Ash

Mia Ash était un faux personnage utilisé entre 2016 et 2017 par les auteurs de cybermenace iraniens afin de cibler des organisations au Moyen-Orient. Mia Ash prétendait être une photographe professionnelle britannique de 30 ans. Son profil a été créé au moyen d'images volées, probablement d'un compte Instagram d'un photographe légitime. Elle était présente sur plusieurs médias sociaux, dont Facebook, Blogger et LinkedIn.

Le personnage utilisait LinkedIn pour communiquer avec une personne qui travaillait pour une organisation ciblée et il échangeait des messages avec la victime à propos de la profession, de la photographie et des voyages. Par la suite, le personnage a encouragé la victime à devenir ami Facebook. La correspondance pouvait se poursuivre sur WhatsApp par courriel ou sur Facebook. Après quelques semaines, Mia Ash envoyait un document Excel malveillant à propos d'un sondage sur la photographie en encourageant la personne ciblée à ouvrir le document au travail et à utiliser son adresse de courriel d'entreprise. Après une première campagne d'hameçonnage non fructueuse, les auteurs de menace ont probablement eu recours à des personnages pour accéder à des actifs d'organisations ciblées.

Utilisation répétée de personnages

Les auteurs de cybermenace iraniens réutilisent les personnages à plusieurs reprises, ce qui démontre probablement un effort soutenu pour la création et l'élaboration des personnages et de leur réseautage[5]. Les exemples suivants illustrent comment les auteurs de menace iraniens réutilisent les personnages pour atteindre leurs objectifs.

- Personnage A féminin
    - Hiver 2020 : les auteurs de menace iraniens ont utilisé le Personnage A pour mener une opération de piratage psychologique contre une personne aux États-Unis.
    - Été 2020 : les auteurs de menace ont utilisé le Personnage A à nouveau pour mener des opérations de harponnage et de piratage psychologique contre plusieurs personnes. Ils ont exploité du contenu savant et des courriels sur le thème des actualités, où les victimes étaient redirigées vers des documents malveillants au moyen de liens ou de pièces jointes.
- Personnage B féminin
    - Printemps 2020 : les auteurs de cybermenace iraniens ont utilisé le Personnage B pour se lier d'amitié avec un ressortissant étranger sur LinkedIn. Les auteurs de cybermenace ont par la suite compromis un appareil ciblé et exfiltré des renseignements personnels sensibles et du contenu se trouvant sur l'appareil.
    - Été 2020 : les auteurs de cybermenace iraniens ont exploité le Personnage B à titre de recruteur pour cibler une personne qui travaillait pour un entrepreneur habilité du secteur de la défense des États-Unis. Ils ont ainsi obtenu le curriculum vitæ de la victime. Le personnage était également actif sur LinkedIn et a établi de nombreuses relations avec du personnel de différentes entreprises.
- Personnage C féminin
    - De l'été 2022 à l'été 2023 : les auteurs de menace iraniens ont exploité le Personnage C sur Facebook pour mener une campagne de piratage psychologique contre une personne qui travaille au Defense Industrial Base Sector des États-Unis. Le Personnage C a partagé un site Web avec la personne en question à propos d'un passe-temps commun.
    - Printemps 2023 : les auteurs de menace iraniens ont utilisé le Personnage C pour cibler différents employés de la Defense Industrial Base en fonction de leur affiliation d'entreprise sur Facebook. Le Personnage C alléguait mener une recherche et envoyait un questionnaire aux personnes ciblées.
- Personnage D féminin
    - De l'hiver 2021 à l'automne 2022 : les auteurs de menace iraniens ont ciblé une employée ou un employé du secteur de la défense en Europe au moyen du Personnage D sur un site de réseautage social orienté carrière. Après avoir établi la confiance, les communications ont été transférées vers le courriel, où le personnage a envoyé un document malveillant et a encouragé la cible à fournir des renseignements.
    - Printemps 2023 : les auteurs de cybermenace iraniens ont fort probablement utilisé le Personnage D pour cibler des comptes de courriel personnels. Dans un courriel de harponnage, ils encourageaient leurs victimes à suivre des liens malveillants qui demandaient l'entrée d'un mot de passe.
- Personnage E féminin
    - De l'automne 2022 à l'automne 2023 : les auteurs de menace iraniens ont utilisé le Personnage E, utilisé sur plusieurs plateformes de réseaux sociaux, se présentant à titre de journaliste posant des questions à propos des droits de la personne en Iran. L'intention probable du personnage était d'envoyer des fichiers malveillants à la cible.

- De l'été à l'automne 2023 : les auteurs de cybermenace iraniens ont exploité de multiples personnages (y compris le Personnage E) dans des opérations de harponnage et de piratage psychologique pour cibler des personnes qui œuvrent dans le secteur nucléaire.

Vulnérabilités émotionnelles et instauration de confiance : exploitation d'événements traumatisants

Les auteurs de cybermenace iraniens ont utilisé des personnages afin d'établir la confiance avec une personne ciblée en partageant des préoccupations concernant des événements traumatisants et des tragédies. Par exemple, il a été établi que des auteurs de cybermenace iraniens ont mené une campagne sur le thème de la guerre entre Israël et le Hamas et ont créé un faux site Web associé au mouvement « Bring Them Home Now ». Le site demandait le retour des otages israéliens détenus par le Hamas, et le site Web menait éventuellement au téléchargement d'une charge de virus.

En octobre 2022, suite au décès de Mahsa Amini et aux manifestations qui ont suivi en Iran, les auteurs de cybermenace iraniens ont créé de faux comptes Twitter (désormais X) pour le personnage Sara Shokouhi afin de mener une campagne de harponnage ciblant particulièrement les femmes associées à des activités de protestation, d'activisme politique et de recherche en droits de la personne, et ce, à l'intérieur comme à l'extérieur de l'Iran. Le personnage approchait ses victimes, prétendument au nom du groupe de réflexion U.S. Atlantic Council, afin d'instaurer la confiance et d'établir une relation pendant plusieurs semaines. Par la suite, le personnage tentait de voler des données d'identification ou de déployer des maliciels sur l'ordinateur ou l'appareil mobile de la victime[6].

Ciblage d'anciens combattants et combattantes souffrant d'un trouble de stress post-traumatique

En 2020, des auteurs de cybermenace iraniens ont mené une campagne de piratage psychologique sur le thème des troubles de stress post-traumatique (TSPT) pour cibler des fonctionnaires et des entrepreneurs du secteur de la défense au moyen d'un personnage fictif, qui est un psychologue doté d'un compte LinkedIn. Le personnage menait des enquêtes auprès de membres du service militaire qui souffraient de TSPT à la suite d'une expérience de combat. Le personnage a incité ses victimes à suivre des liens probablement malveillants et à fournir des coordonnées professionnelles.

Fausses collaborations et occasions professionnelles

Les auteurs de cybermenace iraniens font intervenir des intérêts professionnels partagés, présentent une possibilité de collaboration avec la victime, établissent un niveau de confiance supplémentaire et tentent d'accéder à des renseignements à partir du procédé. Dans plusieurs secteurs, y compris les universités, le journalisme, la recherche, l'activisme et les organisations non gouvernementales, la collaboration en ligne est un acte de routine. Les personnes appartenant à ces professions sont précieuses non seulement pour leurs connaissances, mais également pour leur réseau de contacts, les personnes qu'elles côtoient et les endroits auxquels elles peuvent accéder.

Occasions d'emploi

Les auteurs de cybermenace iraniens ont mené plusieurs opérations où ils ont eu recours à des personnages qui prétendaient être recruteurs et travailler pour des entreprises provenant du pays des victimes afin d'offrir des occasions d'emploi. Ces opérations ciblent habituellement les entrepreneurs du domaine de la défense des États-Unis au Moyen-Orient et les sous-traitants associés aux grandes compagnies de défense[7].

Groupes de réflexion et instituts de recherche

Les auteurs de menace iraniens ont usurpé l'identité du président de la Middle East Institute aux États-Unis et ont communiqué avec des activistes iraniens et d'autres pays. Ils ont demandé à leurs victimes d'établir un partenariat et de collaborer sur leur sujet d'expertise. Une fois la confiance établie avec la victime après plusieurs messages, les auteurs de menace invitaient la personne à participer à une réunion virtuelle. Ils ont par la suite envoyé un lien malveillant afin de voler les données d'identification de la victime[8].

Conférences

Dans une opération menée en 2021 pour recueillir des informations stratégiques à propos des relations avec Téhéran, les auteurs de cybermenace iraniens se sont fait passer pour des universitaires de la School of Oriental and African Studies (SOAS) de l'Université de Londres souhaitant organiser une conférence. Des personnages ont ciblé des spécialistes en politique étrangère, des journalistes et des universitaires spécialistes de la politique au Moyen-Orient. Ils ont établi des relations avec leurs cibles et communiqué avec elles afin de pouvoir ultérieurement leur envoyer un lien vers un site compromis pour s'inscrire à une conférence[9].

Il a été établi que des auteurs de cybermenace iraniens ont ciblé des membres du personnel de Human Rights Watch des journalistes et des activistes des droits de la personne au moyen de WhatsApp. Ces auteurs prétendaient faire partie d'un groupe de réflexion au Liban et invitaient les personnes à une conférence. Les auteurs se faisaient passer pour une personne ayant déjà travaillé pour le groupe de réflexion et ont utilisé un format similaire aux invitations précédentes du groupe[10].

Médias et expertise

Les auteurs de cybermenace iraniens ont eu recours à des personnages journalistiques à de multiples occasions afin de mener des opérations d'ingérence ou d'influence auprès de leurs victimes. Un rapport de 2020 indiquait que les auteurs de cybermenace iraniens ont mis au point de faux personnages pour usurper l'identité de réels journalistes de grands journaux, dont le New York Times, CNN et The Wall Street Journal. Les auteurs de menace pouvaient ensuite mener leurs victimes vers des plateformes de clavardage chiffrées, comme WhatsApp, et éventuellement les renvoyer vers des conférences vidéo truquées où la victime présumément continuerait d'être compromise[11].

Perspective

Dans la foulée de la pandémie de COVID-19, les entreprises ont eu tendance à réaliser de plus en plus d'activités en ligne (conférences, recrutement, formation, discussions publiques). Cette tendance offre probablement et continuera d'offrir aux auteurs de cybermenace iraniens et à d'autres groupes davantage d'occasions pour mener des opérations de piratage psychologique.

Les percées des technologies d'IA, comme les images et la voix synthétisées, permettront aux auteurs de cybermenace de créer des personnages en ligne qui seront encore plus crédibles. Au début du mois de février 2024, les auteurs de menace iraniens ont interrompu une télédiffusion aux Émirats arabes unis et ont exploité un hypertrucage de lecteur de nouvelles pour présenter un rapport sur la guerre de Gaza[12].

Étant donné que les auteurs de cybermenace souhaitent attirer des personnes intéressées par les événements actuels, ces techniques de piratage psychologique pourront être combinées aux cyberopérations d'information de l'Iran. Les auteurs de cybermenace iraniens ont exploité des opérations d'information durant la pandémie de la COVID-19[13]. Celles-ci ont d'ailleurs été intensifiées depuis le début de la guerre Israël-Hamas en octobre 2023. Ces opérations d'information ont ciblé davantage le public international, surtout en Occident[14]. Nous évaluons que l'Iran pourrait probablement combiner ces opérations à des campagnes de piratage psychologique afin de cibler des personnes ou des organisations concernées par le conflit.

L'Iran continue de renforcer ses capacités de piratage psychologique en acquérant l'infrastructure pour mener ses campagnes de piratage psychologique sophistiquées, en établissant de nouveaux vecteurs de communication avec ses cibles et en créant des réseaux de personnages et de la formation.

Lecture complémentaire

Le Centre pour la cybersécurité publie régulièrement des avis et des conseils pour aider la population canadienne et les organisations au Canada à se protéger contre les cybermenaces courantes, dont les menaces décrites dans la présente évaluation, comme le harponnage et le piratage psychologique.

Consultez les ressources en ligne ci-dessous pour obtenir de l'information supplémentaire ainsi que des avis et conseils utiles :

- Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101)
- Reconnaître les courriels malveillants (ITSAP.00.100)
- Piratage psychologique (ITSAP.00.166)
- Repérer les cas de mésinformation, désinformation et malinformation (ITSAP.00.300)
- Intelligence artificielle (ITSAP.00.040)
- Les outils de sécurité préventive (ITSAP.00.058)

[1] Emil Sayegh. Inside the Shadowy World of Iranian Cyber Espionage Group APT 33. Forbes. 28 mars 2023, Collin Anderson et Karim Sadjadpour. Iran's Cyber Threat: Espionage, Sabotage and Revenge. Carnegie Endowment for International Peace. 1er janvier 2018.

[2] INSIKT Group. Social Engineering Remains Key Tradecraft for Iranian APTs. Recorded Future. 30 mars 2022.

[3]Human Rights Watch. Iran: State-Backed Hacking of Activists, Journalists, Politicians. 5 décembre 2022; INSIKT Group. Social Engineering Remains Key Tradecraft for Iranian APTs. Recorded Future. 30 mars 2022; Emil Sayegh. Inside the Shadowy World of Iranian Cyber Espionage Group APT 33. Forbes. 28 mars 2023.

[4] Joshua Miller, Michael Raggi et Crista Giering. I Knew you were trouble: TA456 Targets Defence Contractor with Alluring Social Media Persona. Proofpoint. 28 juillet 2021.

[5] INSIKT Group Social Engineering Remains Key Tradecraft for Iranian APTs. Recorded Future. 30 mars 2022.

[6] Ravie Lakshmanan. Iranian Hackers Target Women Involved in Human Rights and Middle East Politics. The Hacker News. 9 mars 2023.

[7] INSIKT Group. Social Engineering Remains Key Tradecraft for Iranian APTs. Recorded Future. 30 mars 2022.

[8] CERTFA Lab. Charming Kitten: « Can we Have a Meeting? »: Important puzzle pieces of Charming Kitten's cyber espionage operations. 8 septembre 2022.

[9] INSIKT Group. Social Engineering Remains Key Tradecraft for Iranian APTs. Recorded Future. 30 mars 2022.

[10]Human Rights Watch. Iran: State-Backed Hacking of Activists, Journalists, Politicians. 5 décembre 2022; INSIKT Group. Social Engineering Remains Key Tradecraft for Iranian APTs. Recorded Future. 30 mars 2022.

[11]Human Rights Watch. Iran :State-Backed Hacking of Activists, Journalists, Politicians. 5 décembre 2022.

[12] Dan Milmo. Iran-backed Hackers Interrupt UAE TV Streaming Services with Deepfake news. The Guardian, 8 février 2024.

[13] Mark Dubowitz et Saeed Ghasseminejad. Iran's Covid-19 Disinformation Campaign. Combatting Terrorism Centre Sentinel. Volume 13, numéro 6. Juin 2020.

[14] Microsoft Threat Intelligence. Iran surges cyber-enabled influence operations in support of Hamas. 26 février 2024.