Défense contre les attaques de type adversaire au milieu grâce à une authentification multifacteur résistante à l'hameçonnage

ITSM.30.031

Communications Security Establishment Canada
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité

Canada

Vue d'ensemble

Dans le paysage en constante évolution de la cybersécurité, la croissance des attaques de type adversaire au milieu (AitM pour *adversary-in-the-middle*) représente une menace importante pour les organisations. L'hameçonnage de type AitM est de plus en plus employé par les auteurs de menace depuis la migration des organisations vers le nuage, obligeant la ligne de défense principale à migrer de la protection traditionnelle des périmètres réseau vers la protection de l'identité comme priorité.

Les exigences de sécurité ont gagné en complexité, en particulier dans les environnements infonuagiques, et les auteurs de menace ont affiné leurs tactiques. Par conséquent, la mise en œuvre d'une authentification multifacteur (AMF) résistante à l'hameçonnage est essentielle pour maintenir une cybersécurité robuste.

La présente publication offre des détails sur des campagnes d'hameçonnage par AitM qui ont été observées, illustrant leur popularité, et expose les risques de ne pas protéger adéquatement les comptes infonuagiques. Tous les résultats rapportés dans cette publication se fondent sur l'analyse de plus de100 campagnes ayant été détectées par le Centre canadien pour la cybersécurité (Centre pour la cybersécurité), et ciblant les comptes Microsoft Entra ID entre 2023 et la première partie de l'année 2025. Bien qu'il ne s'agisse pas d'une présentation exhaustive de toutes les campagnes d'hameçonnage par AitM qui ont eu lieu partout dans le monde, cette publication offre néanmoins un instantané illustrant combien ces campagnes sont devenues répandues.

Cette publication vise les objectifs suivants :

- fournir une compréhension approfondie de l'origine des menaces;
- souligner l'importance, pour toutes les organisations, de renforcer les défenses par l'exploitation d'une AMF résistante par défaut à l'hameçonnage;
- offrir des recommandations pour améliorer la posture de sécurité des organisations contre ces campagnes sophistiquées.

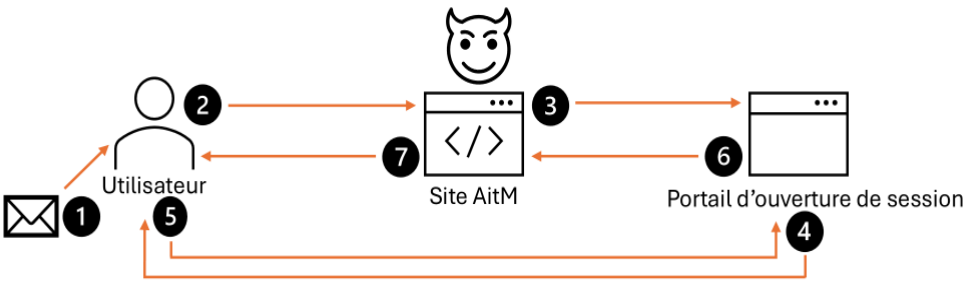
Table des matières

Liste des figures

Présentation de l'hameçonnage de type adversaire au milieu et de ses effets

L'hameçonnage AitM est une technique où l'auteur de menace intercepte la connexion entre une utilisatrice ou un utilisateur et un serveur d'identification. L'auteur de menace peut ensuite saisir tous les noms d'utilisateur, les mots de passe, les justificatifs et les jetons d'authentification multifacteur transmis au moyen de la connexion. Les personnes reçoivent typiquement un courriel d'hameçonnage contenant un lien vers un site malveillant déguisé en site Web légitime. Le stratagème déjoue l'utilisatrice ou l'utilisateur, qui fournit ses détails de connexion et qui complète le processus d'AMF. L'auteur de menace peut enregistrer ces informations pour usurper par la suite l'identité de l'utilisateur.

Figure 1 : Campagne d'hameçonnage d'un auteur de menace



Description longue – Figure 1 : Campagne d'hameçonnage d'un auteur de menace

Cette figure illustre comment un auteur de menace peut transmettre et acheminer un courriel d'hameçonnage contenant un lien vers un site d'hameçonnage AitM.

1. *L'utilisateur reçoit un courriel d'hameçonnage contenant un lien.*
2. *L'utilisateur se rend sur le site et est dirigé vers un portail d'ouverture de session qui semble légitime.*
3. *Le site d'hameçonnage AitM redirige vers un mandataire toutes les connexions au portail d'ouverture de session.*
4. *Le portail d'ouverture de session invite l'utilisateur à utiliser l'AMF.*
5. *L'utilisateur utilise une AMF non résistante à l'hameçonnage.*
6. *Cette action retourne un jeton validé et un témoin temporaire au site AitM.*
7. *Le site d'hameçonnage redirige l'utilisateur vers un autre site qui semble légitime.*

L'hameçonnage AitM n'est pas une nouveauté. Il a toutefois gagné en popularité auprès des auteurs de menace depuis la migration des organisations vers le nuage. Auparavant, les organisations engageaient des efforts soutenus pour renforcer leur première ligne de défense, c'est-à-dire le périmètre de leur réseau, au moyen de pare-feu et de réseaux privés virtuels (RPV). Elles doivent maintenant renforcer leur cybersécurité pour défendre leur nouvelle ligne de défense principale, soit le nuage. Pour ce faire, elles doivent protéger les couches d'identité du nuage au moyen d'un ensemble d'outils modernes, comme les stratégies d'accès conditionnel et l'authentification multifacteur (AMF).

Il est difficile de protéger un environnement infonuagique contre les campagnes d'hameçonnage AitM. Le nuage est associé à des exigences de sécurité complexes qui évoluent constamment, au fur et à mesure que s'intensifient les campagnes menées par les auteurs de menace contre les couches d'identité du nuage. Cette évolution souligne l'importance du modèle de responsabilité partagée, où le client et les fournisseurs de services infonuagiques (FSI) doivent collaborer afin de favoriser une meilleure posture de sécurité. L'AMF résistante à l'hameçonnage est la nouvelle norme de l'industrie. Elle permet d'assurer une meilleure protection des identités et offre une plus grande résilience que les mots de passe ou les méthodes d'AMF traditionnelles à elles seules.

Les auteurs de menace peuvent facilement exploiter des techniques d'hameçonnage AitM grâce à des solutions sans codage, comme des fournisseurs AitM du Web clandestin ou encore des boîtes à outils AitM offrant une configuration automatisée. Il est possible de contrecarrer ces campagnes grâce aux moyens suivants :

- des facteurs d'AMF résistants à l'hameçonnage;
- des stratégies d'accès conditionnel précises qui exigent une connexion au moyen d'un dispositif enregistré;
- des stratégies d'accès conditionnel précises qui ne permettent de connexion qu'à partir d'une plage d'adresses IP ou d'adresses IP précises appartenant à l'organisation.

Passage à des attaques de type adversaire au milieu exploitant des mandataires

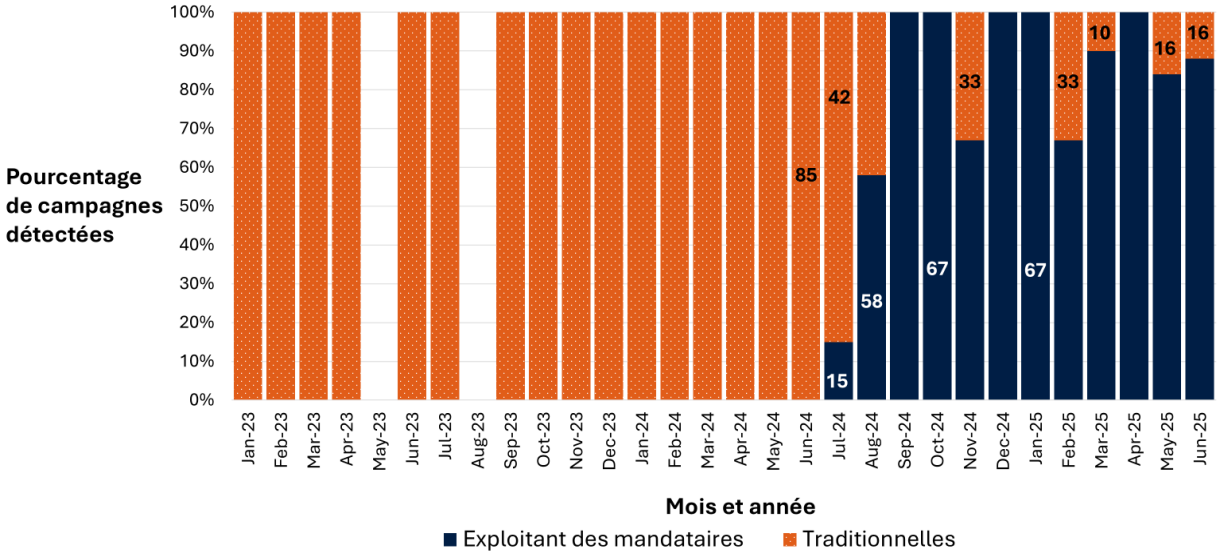
Les auteurs de menace qui mènent des campagnes d'hameçonnage AitM peuvent éviter d'être détectés en utilisant des trousses d'hameçonnage AitM exploitant des mandataires. Une trousse d'hameçonnage est un jeu préassemblé d'outils numériques permettant aux auteurs de menace de facilement créer de faux sites Web et recueillir des renseignements sensibles sur les utilisatrices et utilisateurs. Ces faux sites Web imitent souvent l'identité de marques de confiance pour ainsi tromper les utilisatrices et utilisateurs.

Avant le développement des trousses d'hameçonnage AitM exploitant des mandataires, les organisations pouvaient détecter les activités d'hameçonnage AitM en recherchant les connexions suspectes à leur environnement infonuagique et en comparant les adresses IP correspondantes à celles provenant de connexions à partir de leur réseau. Une ouverture de session à partir d'une connexion réseau ou d'une d'adresse IP suspecte vers un site Web douteux hébergé sur cette même adresse IP constituait un bon indicateur de campagne d'hameçonnage AitM.

Les trousses d'hameçonnage AitM exploitant des mandataires fonctionnent par l'ajout d'une série de serveurs mandataires entre l'utilisatrice ou l'utilisateur et le fournisseur d'identité. Cela fera en sorte que l'IP d'ouverture de session utilisée ne sera pas la même que celle qui semble correspondre au site Web d'hameçonnage. Il existe de nombreuses façons pour les auteurs de menace d'atteindre cet objectif, de sorte que les organisations ne peuvent plus se fier aux corrélations entre adresses IP pour la détection de toutes les campagnes d'hameçonnage AitM.

Au milieu de l'année 2024, le Centre pour la cybersécurité a ajouté de nouvelles capacités de détection internes pour l'hameçonnage AitM exploitant des mandataires et a commencé à détecter un nombre beaucoup plus élevé de campagnes. Cela a correspondu à un déclin des activités d'hameçonnage AitM traditionnelles décelées. On constate que les auteurs de menace ont pratiquement délaissé les campagnes d'hameçonnage AitM traditionnelles au profit des campagnes exploitant des mandataires.

Figure 2 : Comparaison des campagnes d'hameçonnage AitM traditionnelles et des campagnes exploitant des mandataires



Description longue – Figure 2 : Comparaison des campagnes d'hameçonnage AitM traditionnelles et des campagnes exploitant des mandataires

Ce diagramme à barres présente une comparaison entre les campagnes d'hameçonnage AitM traditionnelles et celles exploitant des mandataires d'après ce que le Centre pour la cybersécurité a été en mesure de catégoriser avec confiance entre 2023 et le milieu de 2025,

Janvier 2023 : AitM traditionnelle : 100 %; AitM exploitant des mandataires : 0 %

Février 2023 : AitM traditionnelle : 100 %; AitM exploitant des mandataires : 0 %

Mars 2023 : AitM traditionnelle : 100 %; AitM exploitant des mandataires : 0 %

Avril 2023 : AitM traditionnelle : 100 %; AitM exploitant des mandataires : 0 %

Mai 2023 : AitM traditionnelle : Néant; AitM exploitant des mandataires : Néant

Juin 2023 : AitM traditionnelle : 100 %; AitM exploitant des mandataires : 0 %

Juillet 2023 : AitM traditionnelle : 100 %; AitM exploitant des mandataires : 0 %

Août 2023 : AitM traditionnelle : Néant; AitM exploitant des mandataires : Néant

Septembre 2023 : AitM traditionnelle : 100 %; AitM exploitant des mandataires : 0 %

Novembre 2023 : AitM traditionnelle : 100 %; AitM exploitant des mandataires : 0 %

Décembre 2023 : AitM traditionnelle : 100 %; AitM exploitant des mandataires : 0 %

Janvier 2024 : AitM traditionnelle : 100 %; AitM exploitant des mandataires : 0 %

Février 2024 : AitM traditionnelle : 100 %; AitM exploitant des mandataires : 0 %

Mars 2024 : AitM traditionnelle : 100 %; AitM exploitant des mandataires : 0 %

Avril 2024 : AitM traditionnelle : 100 %; AitM exploitant des mandataires : 0 %

Mai 2024 : AitM traditionnelle : 100 %; AitM exploitant des mandataires : 0 %

Juin 2024 : AitM traditionnelle : 86 %; AitM exploitant des mandataires : 14 %

Juillet 2024 : AitM traditionnelle : 42 %; AitM exploitant des mandataires : 58 %

Août 2024 : AitM traditionnelle : 0 %; AitM exploitant des mandataires : 100 %

Septembre 2024 : AitM traditionnelle : 0 %; AitM exploitant des mandataires : 100 %

Octobre 2024 : AitM traditionnelle : 33 %; AitM exploitant des mandataires : 67 %

Novembre 2024 : AitM traditionnelle : 10 %; AitM exploitant des mandataires : 90 %

Décembre 2024 : AitM traditionnelle : 0 %; AitM exploitant des mandataires : 100 %

Janvier 2025 : AitM traditionnelle : 0 %; AitM exploitant des mandataires : 100 %

Février 2025 : AitM traditionnelle : 33 %; AitM exploitant des mandataires : 67 %

Mars 2025 : AitM traditionnelle : 10 %; AitM exploitant des mandataires : 90 %

Avril 2025 : AitM traditionnelle : 0 %; AitM exploitant des mandataires : 100 %

Mai 2025 : AitM traditionnelle : 16 %; AitM exploitant des mandataires : 84 %

Juin 2025 : AitM traditionnelle : 12 %; AitM exploitant des mandataires : 88 %

Un élément ayant contribué de manière importante à ce changement a été l'emploi par les auteurs de menace d'une trousse particulière d'hameçonnage AitM exploitant des mandataires. Pour de plus amples informations à propos de cette trousse, consultez l'article Field Effect discovers M365 adversary-in-the-middle campaign(en anglais seulement).

Les AMF résistantes à l'hameçonnage permettent encore de faire échec aux campagnes de type AitM, que celles-ci soient réalisées au moyen de trousses d'hameçonnage AitM traditionnelles ou exploitant des mandataires. Les AMF résistante à l'hameçonnage, comme les stratégies d'accès conditionnel de dispositifs enregistrés, interrompent le flux d'authentification lorsqu'une trousse d'hameçonnage AitM est repérée dans la connexion.

Tendances et techniques des attaques d'hameçonnage de type adversaire au milieu

Les trousses d'hameçonnage AitM sont de plus en plus sophistiquées et difficiles à détecter. Il peut sembler logique de se concentrer sur l'éradication de ces campagnes à la racine grâce à un meilleur filtrage des courriels d'hameçonnage. Toutefois, les auteurs de menace anticipent que les organisations amélioreront continuellement leurs programmes de protection contre l'hameçonnage et ajusteront leurs techniques en conséquence.

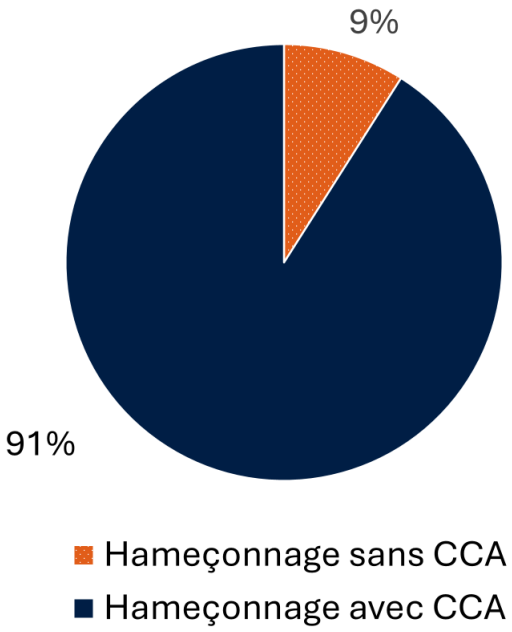
Le Centre pour la cybersécurité a analysé plus de 100 campagnes entre 2023 et le milieu de 2025 et a établi que les auteurs de menace ont utilisé une combinaison d'attaques par hameçonnage reposant sur la compromission de courriels de fournisseurs, qui est un type de compromission de courriels d'affaires, et d'attaques par exploitation de ressources externes (attaques de type « living off trusted sites »).

Campagnes d'hameçonnage par compromission de courriel d'affaires

Dans le cadre des campagnes d'hameçonnage par compromission de courriels d'affaires (CCA), les auteurs de menace réussissent à compromettre des organisations légitimes, à voler la liste des contacts de confiance et à envoyer des courriels d'hameçonnage AiTM contenant des liens vers des services licites comme SharePoint, Dropbox ou d'autres fournisseurs d'hébergement de confiance. Les fichiers hébergés chez ces fournisseurs de confiance contiennent un lien vers un site d'hameçonnage AitM, mais le lien est intégré à un fichier hébergé chez le fournisseur en question, et non dans le courriel d'hameçonnage en tant que tel. Cela complexifie davantage la détection et l'identification de la source d'une compromission AitM.

Du point de vue de l'utilisatrice ou de l'utilisateur, le courriel provient d'un contact de confiance et contient un lien vers un fichier partagé, une situation qui peut sembler typique pour le contact en question. De plus, les auteurs de menace peuvent adapter le service de partage de fichier en fonction des communications antérieures entre deux utilisateurs afin de dissimuler avec soin leurs campagnes d'hameçonnage AitM.

Figure 3 : Répartition de l'hameçonnage par CCA



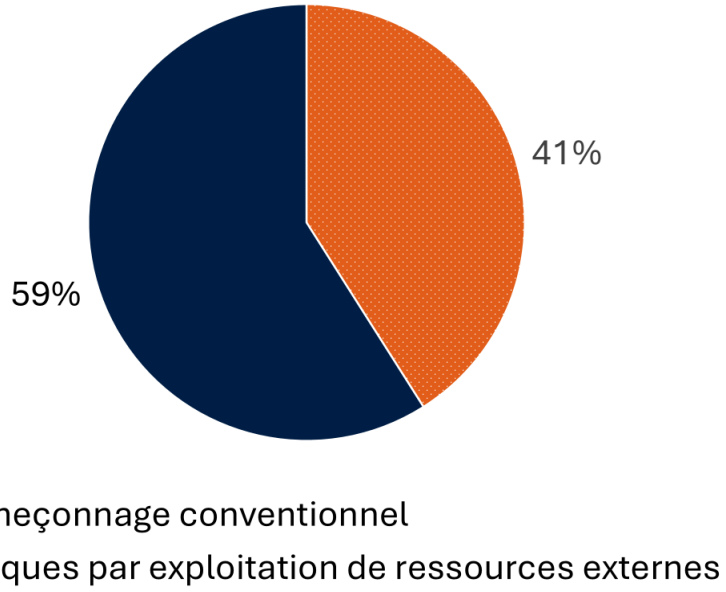
Description longue – Figure 3 : Répartition de l'hameçonnage par CCA

Ce diagramme à secteurs présente la répartition des campagnes d'hameçonnage par CCA comparativement aux autres types de campagnes, selon ce que le Centre pour la cybersécurité a été en mesure d'analyser et de catégoriser entre 2023 et le milieu de 2025. Les campagnes d'hameçonnage par CCA représentent 91 % des campagnes analysées.

Techniques d'attaque par exploitation de ressources externes

Les campagnes d'hameçonnage AitM basées sur des attaques par exploitation de ressources externes représentaient plus de la moitié des campagnes catégorisées par le Centre pour la cybersécurité. Les autres campagnes exploitaient des méthodes d'hameçonnage traditionnelles (comme des liens ou des fichiers joints malveillants compris directement dans le contenu des courriels). Les organisations doivent donc sensibiliser les utilisateurs à propos des risques associés aux campagnes d'hameçonnage AitM basées sur des attaques par exploitation de ressources externes, et offrir une formation permettant de mieux détecter ce type de campagne.

Figure 4 : Répartition des techniques d'hameçonnage



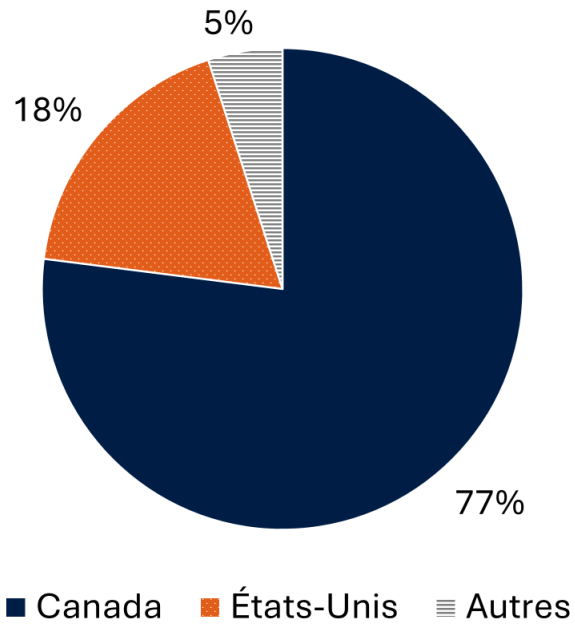
Description longue – Figure 4 : Répartition des techniques d'hameçonnage

Ce diagramme à secteurs présente la répartition des techniques d'hameçonnage selon ce que le Centre pour la cybersécurité a été en mesure d'analyser et de catégoriser entre 2023 et le milieu de 2025. Les attaques par exploitation de ressources externes représentaient 59 % des campagnes analysées, comparativement à 41 % pour les attaques conventionnelles (menées au moyen de liens ou de fichiers intégrés, par exemple).

Secteurs ciblés

Le Centre pour la cybersécurité a étudié les organisations et les secteurs ciblés par les campagnes d'hameçonnage AitM. La figure 5 ci-dessous présente la répartition des victimes de CCA par pays, illustrant que la plupart des organisations touchées et ayant transmis des courriels d'hameçonnage AitM au gouvernement du Canada ainsi qu'à des partenaires du secteur des infrastructures essentielles se trouvent au Canada. Ces résultats révèlent que les auteurs de menace ont recours à la compromission de courriels de fournisseurs (CCF), étant donné que les organisations canadiennes interagissent essentiellement avec d'autres organisations canadiennes dans leurs activités au quotidien.

Figure 5 : Répartition des victimes de CCA par pays



Description longue – Figure 5 : Répartition des victimes de CCA par pays

Ce diagramme à secteurs présente la répartition des victimes de CCA selon ce que le Centre pour la cybersécurité a été en mesure d'analyser et de catégoriser entre 2023 et le milieu de 2025. Le pourcentage pour le Canada est de 77 %, comparativement à 18 % pour les États-Unis. Les 5 % restants sont répartis parmi des pays non déterminés.

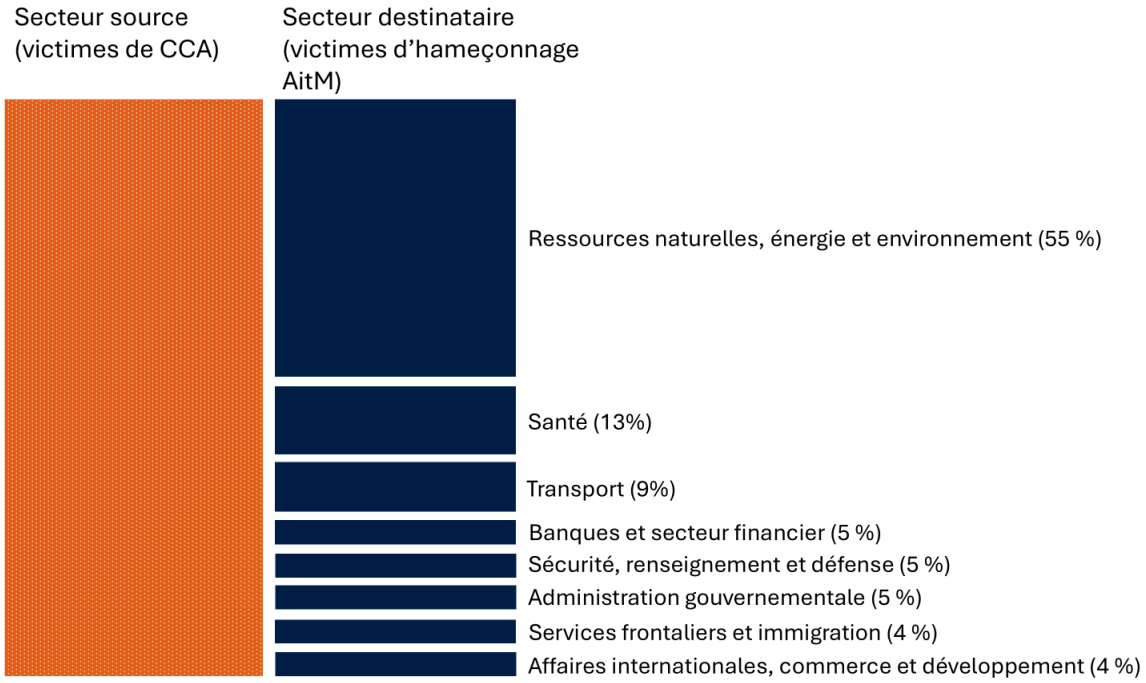
Le Centre pour la cybersécurité a établi que le tiers des victimes de CCA se trouvaient dans le secteur des ressources naturelles, de l'énergie et de l'environnement. Le secteur de l'industrie et du développement des entreprises suit de près, avec le secteur des services aux Autochtones Canada par la suite.

En examinant de plus près les victimes ayant reçu des courriels d'hameçonnage AitM, le Centre pour la cybersécurité a observé une répartition similaire. Le quart des victimes se trouvent dans le secteur des ressources naturelles, de l'énergie et de l'environnement, suivi par le secteur de la sécurité, du renseignement et de la défense, puis du secteur de la santé et du secteur de l'administration gouvernementale.

Le Centre pour la cybersécurité a mis en corrélation les secteurs concernés par la CCA et ceux touchés par l'hameçonnage AitM afin d'établir des tendances à propos des secteurs qui envoient et des secteurs qui reçoivent ce type de courriel. Nous avons observé que 41 % des secteurs touchés

par la CCA ont également envoyé des courriels d'hameçonnage au sein du même secteur, ce qui est cohérent avec les résultats liés à la CCF mentionnés précédemment. Le graphique ci-dessous en offre un exemple. Les exceptions notables à cette tendance concernent le secteur de l'hébergement et le secteur juridique, probablement en raison du fait que les hôtels et les cabinets d'avocats desservent des clients dans des secteurs diversifiés.

Figure 6 : Victimes de CCA dans le secteur des ressources naturelles, de l'énergie et de l'environnement envoyant des courriels d'hameçonnage AitM à d'autres victimes



Description longue – Figure 6 : Victimes de CCA dans le secteur des ressources naturelles, de l'énergie et de l'environnement envoyant des courriels d'hameçonnage AitM à d'autres victimes

La figure présente les victimes de CCA dans le secteur des ressources naturelles, de l'énergie et de l'environnement qui envoient des courriels d'hameçonnage AitM à d'autres victimes. Les données sont basées sur les résultats analysés par le Centre pour la cybersécurité entre 2023 et le milieu de 2025. Le secteur des ressources naturelles, de l'énergie et de l'environnement a envoyé 55 % de ses courriels d'hameçonnage dans ce même secteur, 13 % au secteur de la santé, 9 % au secteur du transport, 5 % au secteur des banques et des finances, 5 % au secteur de la sécurité, du renseignement et de la défense, 5 % au secteur de l'administration gouvernementale, 4 % au secteur des services frontaliers et de l'immigration, et 4 % au secteur des affaires internationales, du commerce et du développement.

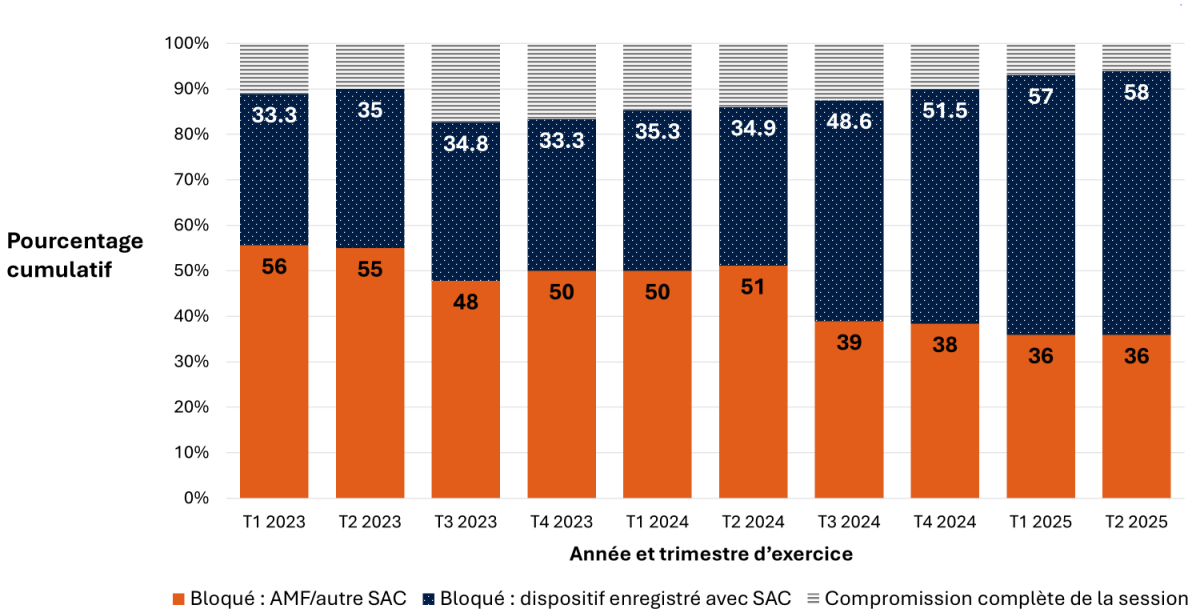
Importance de l'authentification multifacteur résistante à l'hameçonnage

Les campagnes d'hameçonnage AitM sont de plus en plus répandues. Toutefois, il existe déjà une solution permettant d'atténuer les risques, et ce, peu importe le type de campagne : l'AMF résistante à l'hameçonnage. Cette solution est en fait la seule façon d'enrayer complètement ce type de

campagne et d'intervenir avant que les auteurs de menace puissent prendre le contrôle d'une session vérifiée au moyen d'une AMF.

Selon les résultats du Centre pour la cybersécurité, les cas de compromission complète de session au sein du gouvernement du Canada et des partenaires des infrastructures essentielles ont connu une baisse au cours des dernières années. Cela s'explique principalement par le fait que ces organisations utilisent désormais des stratégies d'accès conditionnel (SAC) sur dispositifs enregistrés ou d'autres stratégies d'accès conditionnel exigeant une AMF résistante à l'hameçonnage, en plus d'appliquer des restrictions rigoureusement contrôlées sur les adresses IP lors des ouvertures de session. Les compromissions de session complète sont en baisse, leur valeur la plus élevée ayant atteint 20 % à la fin du troisième trimestre de 2023 pour s'établir à 10% au début de 2025.

Figure 7 : Pourcentage cumulatif des résultats d'hameçonnage AitM au fil du temps



***Description longue – Figure 7 :* Pourcentage cumulatif des résultats d'hameçonnage AitM au fil du temps**

Ce diagramme à barres compare le pourcentage cumulatif des résultats d'hameçonnage AitM analysés par le Centre pour la cybersécurité entre 2023 et le milieu de 2025.

T1 2023 : Bloqué : AMF/autres SAC : 55,6 %; bloqué : SAC sur dispositif enregistré : 33,3 %; compromission complète de la session : 11,1 %

T2 2023 : Bloqué : AMF/autres SAC : 55 %; bloqué : SAC sur dispositif enregistré : 35 %; compromission complète de la session : 10 %

T3 2023 : Bloqué : AMF/autres SAC : 47,8 %; bloqué : SAC sur dispositif enregistré : 34,8 %; compromission complète de la session : 17,4 %

T4 2023 : Bloqué : AMF/autres SAC : 50 %; bloqué : SAC sur dispositif enregistré : 33,3 %; compromission complète de la session : 16,7 %

T1 2024 : Bloqué : AMF/autres SAC : 50 %; bloqué : SAC sur dispositif enregistré : 35,3 %; compromission complète de la session : 14,7 %

T2 2024 : Bloqué : AMF/autres SAC : 51,2 %; bloqué : SAC sur dispositif enregistré : 34,9 %; compromission complète de la session : 14 %

T3 2024 : Bloqué : AMF/autres SAC : 38,9 %; bloqué : SAC sur dispositif enregistré : 48,6 %; compromission complète de la session : 12,5 %

T4 2024 : Bloqué : AMF/autres SAC : 38,4 %; bloqué : SAC sur dispositif enregistré : 51,5 %; compromission complète de la session : 10,1 %

T1 2025 : Bloqué : AMF/autres SAC : 35,9 %; bloqué : SAC sur dispositif enregistré : 57 %; compromission complète de la session : 7 %

T2 2025 : Bloqué : AMF/autres SAC : 35,9 %; bloqué : SAC sur dispositif enregistré : 58 %; compromission complète de la session : 6,1 %

Le Centre pour la cybersécurité continue d'observer un flux constant de campagnes d'hameçonnage AitM à partir de CCA. Cela indique que les auteurs de menace estiment qu'il y a suffisamment de comptes non protégés par une AMF résistante à l'hameçonnage et que les campagnes d'hameçonnage AitM restent une technique de compromission de compte intéressante de leur point de vue.

Amélioration des mécanismes de défense contre les attaques par interception et leur évolution

Une AMF résistante à l'hameçonnage peut prévenir les campagnes AitM, mais peut se révéler difficile à mettre en œuvre pour les organisations. La configuration de l'environnement infonuagique peut également représenter un défi, et la plupart des méthodes d'AMF résistante à l'hameçonnage sont payantes.

Les organisations doivent peser le pour et le contre des risques et des répercussions potentielles des cyberincidents en fonction des coûts de mise en œuvre d'une AMF résistante à l'hameçonnage. Pour faire un choix éclairé, les organisations doivent prendre en considération les facteurs suivants :

- Comparativement aux coûts de correction et de reprise à la suite d'une violation de données, fournir des méthodes d'AMF résistante à l'hameçonnage (clés de sécurité FIDO2, clés d'accès, Windows Hello Entreprise) aux utilisatrices et utilisateurs représente certainement un investissement rentable.
- Les données et l'information peuvent être cruciales pour les activités d'une entreprise ou contenir des renseignements personnels très sensibles, et toute compromission peut avoir des répercussions considérables et engendrer des coûts importants pour l'organisation.

- Une compromission d'identité peut miner de manière importante la réputation d'une organisation.

Certaines organisations migrent vers des appareils qui sont enregistrés auprès de leurs services des TI et optent pour une AMF résistante à l'hameçonnage. Toutefois, les auteurs de menace ont souvent une longueur d'avance et peuvent lancer des campagnes d'hameçonnage AitM avant même que les organisations aient l'occasion d'adopter des options qui résistent à l'hameçonnage.

Traitement des lacunes et des vulnérabilités à haut risque

Les organisations devraient déployer une AMF résistante à l'hameçonnage pour toutes les utilisatrices et tous les utilisateurs, sans exception. Elles devraient également évaluer leur posture en matière de protection de l'identité et identifier les lacunes et les vulnérabilités à haut risque. Nous présentons ci-dessous des exemples de lacunes ou de vulnérabilités à haut risque que les organisations devraient traiter immédiatement afin de prévenir les compromissions par AitM.

Administrateurs utilisant des méthodes d'AMF faibles

Les organisations devraient prévoir une AMF résistante à l'hameçonnage pour tous les comptes d'administrateur, sans exception, et ce, dans toutes les stratégies d'accès conditionnel. De plus, elles devraient éliminer toutes les méthodes de sauvegarde non protégées contre l'hameçonnage de ces comptes, car les campagnes d'hameçonnage AitM pourraient y opérer une brèche.

Appareils personnels sans AMF résistante à l'hameçonnage ou restrictions relatives à l'emplacement

Les cibles principales des auteurs de menace sont les utilisatrices et utilisateurs qui peuvent se connecter au système au moyen de leurs propres appareils à l'extérieur de l'espace d'adressage IP contrôlé par l'organisation et sans AMF résistante à l'hameçonnage. Cela représente une lacune à très haut risque qu'une organisation devrait rectifier immédiatement.

Si les organisations demandent que les utilisatrices et utilisateurs utilisent leur propre appareil (une stratégie appelée « prenez vos appareils personnels » ou PAP), elles doivent déployer une AMF résistante à l'hameçonnage et s'assurer que les utilisateurs ne pourront pas avoir recours à des méthodes de rechange faibles. Comme autre option, les organisations pourraient exiger que toutes les connexions à partir d'un appareil personnel passent par le réseau privé virtuel de l'entreprise et s'accompagnent d'une stratégie d'accès conditionnel restreignant les connexions à cet espace d'adressage IP précis.

La plus grande difficulté consiste à éviter toute tentation de faire des exceptions pour des applications, des utilisatrices ou utilisateurs ou des groupes particuliers. À titre de base de référence, toutes les utilisatrices et tous les utilisateurs devraient recourir, par défaut et sans exception, à une AMF résistante à l'hameçonnage.

Sensibilisation des employés

Les organisations devraient également former les employés à la façon de détecter et de signaler des campagnes AitM. Bon nombre d'utilisatrices et d'utilisateurs ouvriront un courriel et cliqueront sur les liens qui l'accompagnent si le courriel semble provenir d'une source de confiance. Les organisations doivent penser à inclure les sujets ci-dessous dans les formations au sujet des campagnes d'hameçonnage.

Scénarios de compromission de courriel d'affaires

Plus les utilisatrices et utilisateurs seront sensibilisés à la popularité des campagnes par CCA, plus ils seront en mesure de les détecter. Avant de cliquer sur un lien dans un courriel, les utilisatrices et utilisateurs devraient avoir le réflexe de se poser quelques questions, comme ce qui suit :

- Est-ce que je reçois normalement des fichiers Dropbox non sollicités de cette personne?
- Est-ce que la personne m'envoie généralement des documents SharePoint?

Si une utilisatrice ou un utilisateur reçoit des fichiers non sollicités, la personne devrait communiquer avec l'expéditeur en utilisant une autre méthode (par exemple, par téléphone) afin de confirmer que le document a été partagé intentionnellement.

Vérification soigneuse des URL lors de l'ouverture d'une session au moyen d'un service de connexion

La vérification de la légitimité des URL peut poser des difficultés, car l'ouverture de session associée à certains sites, comme Microsoft Entra ID, présente des URL très longues. Par conséquent, les utilisatrices et utilisateurs risquent de ne pas remarquer la présence d'un domaine douteux dans le chemin d'accès. Leur apprendre à repérer le domaine de premier niveau dans une URL, ainsi que les domaines anticipés à cet emplacement, peut faire une grande différence pour bloquer ce type de campagne.

Évitement des connexions multiples

Les utilisatrices et utilisateurs doivent souvent se connecter à leurs comptes au moyen d'un service infonuagique de gestion des identités et de l'accès, comme Microsoft Entra ID. Cela leur permet d'accéder à des applications comme Microsoft SharePoint ou Teams au moyen d'une

authentification unique. Par conséquent, en sachant qu'elles ne devraient pas avoir besoin de s'identifier à nouveau pour accéder à des applications ou partager des fichiers, ces personnes y penseront à deux fois si le système leur demande une nouvelle fois d'entrer leurs justificatifs d'identité.

Une autre technique utile consiste à suggérer aux utilisatrices et utilisateurs d'ouvrir un nouvel onglet et de se connecter directement au service de partage de fichiers avant de cliquer sur un lien. Après une connexion directe au service, le système ne devrait pas demander aux utilisatrices et utilisateurs d'entrer leurs identifiants une nouvelle fois lorsqu'ils cliquent sur le lien dans le courriel. Si les personnes reçoivent un message d'invite, cela est un indice qu'il pourrait s'agir d'une campagne d'hameçonnage AitM.

Hygiène de mots de passe

Même si les utilisatrices et utilisateurs savent comment détecter les campagnes d'hameçonnage AitM, il restera tout de même des situations où des campagnes parviendront à berner certaines personnes et à les convaincre de fournir leur nom d'utilisateur et leur mot de passe avant que les attaques ne soient bloquées par les stratégies d'accès conditionnel. Cela signifie que les auteurs de menace peuvent obtenir les noms d'utilisateurs et mots de passe de personnes, même s'ils n'ont pas eu accès à une session vérifiée au moyen d'une AMF. Il s'agit d'une raison importante pour les organisations de rappeler à leurs utilisatrices et utilisateurs de ne pas réutiliser d'anciens mots de passe. Une fois que les auteurs de menace obtiennent des justificatifs d'identité, ils peuvent s'en servir sur d'autres portails de l'organisation non protégés au moyen de l'AMF (par exemple, des portails Web patrimoniaux, ou des dispositifs RPV moins bien protégés).

Résumé

Les campagnes d'hameçonnage AitM sont de plus en plus sophistiquées et se retrouvent dans tous les secteurs. Cette publication met en évidence qu'il existe plusieurs mesures que les organisations peuvent exploiter afin d'atténuer ce type de menace. Toutefois, la meilleure défense contre les campagnes d'hameçonnage AitM consiste à mettre en œuvre une AMF résistante à l'hameçonnage, et ce, par défaut et sans exception.

Pour obtenir des conseils supplémentaires sur la cybersécurité, veuillez consulter les documents suivants :

- Mesures de cybersécurité de base à l'intention des petites organisations (ITSAP.10.300)
- Offrir aux employés une formation sur mesure en cybersécurité (ITSAP.10.093)
- Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)

La présente publication est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour de plus amples renseignements, veuillez communiquer avec le Centre pour la cybersécurité :

- Courriel : contact@cyber.gc.ca
- Téléphone : 613-949-7048 ou 1-833-CYBER-88

Date d'entrée en vigueur

Le présent document entre en vigueur le

Historique des révisions

Révision	Modifications	Date
1	Première version.	30 octobre 2025

D97-4/30-031-2025F-PDF
ISBN 978-0-660-79386-3