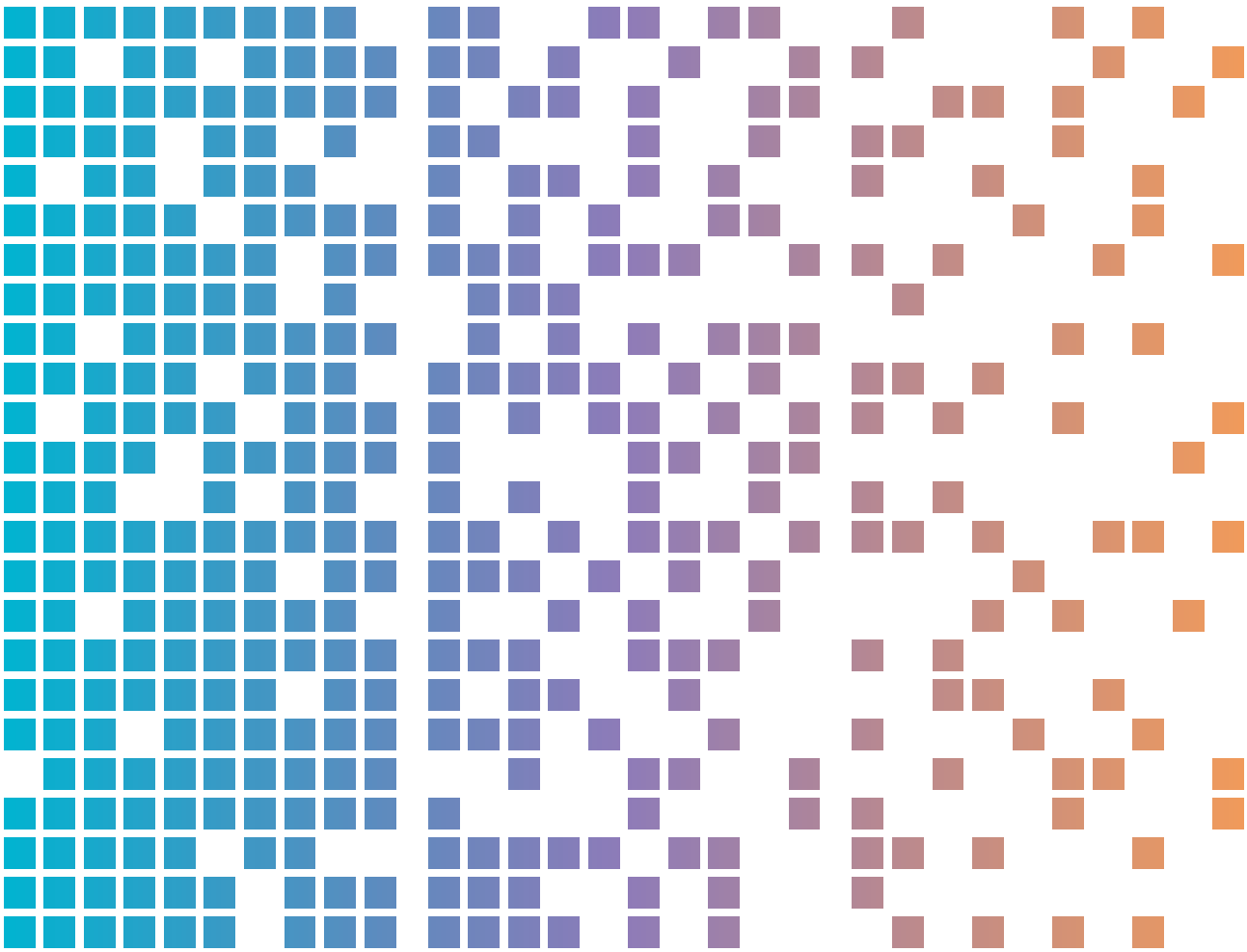
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Le braquage silencieux : les cybercriminels utilisent des logiciels malveillants voleurs d'informations pour compromettre les réseaux d'entreprise



Complexité du contenu
MODÉRÉE ● ● ○

Table des matières

Contexte

Les logiciels malveillants voleurs d'informations volent les identifiants des utilisateurs et les informations système que les cybercriminels exploitent, principalement à des fins lucratives. Des voleurs d'informations ont été observés lors d'attaques cybercriminelles contre de nombreuses organisations et secteurs à travers le monde, y compris en Australie. Cette publication fournit aux lecteurs des conseils de cybersécurité sur les logiciels malveillants voleurs d'informations, notamment sur les menaces et les mesures d'atténuation pour les organisations et leurs employés.

Points clés

- Les logiciels malveillants voleurs d'informations, également appelés voleurs d'informations, sont conçus pour collecter des informations sur l'appareil d'une victime. Ces informations peuvent inclure les noms d'utilisateur et les mots de passe, les informations de carte bancaire, les portefeuilles de cryptomonnaies, les fichiers locaux et les données de navigation, y compris les cookies, l'historique utilisateur et les informations de formulaires de saisie automatique.
- Les cybercriminels peuvent chercher à acheter et à utiliser les identifiants volés associés aux comptes d'entreprise pour obtenir l'accès initial aux appareils de l'employeur de la victime, à ses clients et à d'autres systèmes de l'entreprise. Les conséquences ultérieures pour ces organisations peuvent inclure des logiciels de rançon, des extorsions, la compromission de la messagerie professionnelle et le vol de propriété intellectuelle.
- Le Centre australien de cybersécurité de la Direction des signaux australiens (l'ACSC de l'ASD) a identifié des failles de sécurité dans les réseaux d'entreprise, causées par l'accès d'employés à des ressources professionnelles depuis des appareils personnels compromis. Dans de nombreux cas, les cybercriminels ont obtenu l'accès initial aux réseaux d'entreprise en utilisant des identifiants d'utilisateur valides volés. Nos enquêtes ont montré que les compromissions importantes se produisaient généralement après que les cybercriminels ont réussi à accéder à des comptes d'utilisateurs privilégiés.
- déploient des voleurs d'informations sur les appareils de leurs victimes en utilisant un large éventail de techniques, notamment les courriels d'hameçonnage, les téléchargements de logiciels piratés, les techniques d'optimisation pour les moteurs de recherche (SEO), les publicités malveillantes ou les liens malveillants publiés sur les réseaux sociaux. En général, les appareils utilisés à la fois à des fins professionnelles et personnelles présentent un risque accru d'infection par ces techniques en raison du comportement des utilisateurs et de la faiblesse des contrôles de sécurité.
- Les voleurs d'informations offrent aux cybercriminels un modèle attractif pour monétiser leurs activités cybercriminelles, en particulier pour les cybercriminels débutants et, ceux dont les compétences techniques sont limitées. Certains cybercriminels commercialisent des produits de vol d'informations dans le cadre d'un programme de type Malware-as-a-Service (MaaS), en facturant un abonnement mensuel pour leur utilisation.

Historique

L'utilisation de voleurs d'informations par les cybercriminels représente une menace pour la sécurité et la sécurité des organisations australiennes. Les infections par voleurs d'informations sont souvent le signe avant-coureur d'incidents majeurs de cybersécurité, car les cybercriminels les utilisent pour collecter les identifiants des utilisateurs. Ces identifiants, notamment ceux donnant accès à des services distants accessibles en ligne ou à des comptes privilégiés, sont ensuite exploités pour permettre un accès initial aux systèmes et aux données de l'entreprise.

Remarque : Les courtiers en accès initial jouent un rôle spécialisé dans l'écosystème de la cybercriminalité en achetant et en validant les identifiants d'utilisateurs volés. Ils vendent ensuite aux enchères des identifiants d'utilisateur de haute qualité, destinés à des environnements d'entreprise recherchés, à des cybercriminels qui les utiliseront pour exploiter le réseau de l'entreprise.

Les identifiants d'utilisateur valides volés sont très précieux pour les cybercriminels, car ils accélèrent l'accès initial aux réseaux et aux systèmes d'entreprise. Avec des identifiants d'utilisateur valides volés, les cybercriminels peuvent contourner plusieurs tactiques et techniques courantes, notamment :

- l'identification et la recherche d'une cible ;
- l'identification des vulnérabilités du réseau de la cible ;
- le développement de vecteurs d'accès initial, tels que :
  - le matériel d'hameçonnage,
  - l'exploitation de vulnérabilités logicielles,
  - le ciblage de services distants, notamment le protocole RDP (Remote Desktop Protocol) ou les réseaux privés virtuels (virtual private network, VPN),
  - les attaques par force brute contre les identifiants d'utilisateur (deviner le mot de passe).

Ces étapes nécessitent un investissement en temps et un niveau d'aptitude technique qui constituent un obstacle pour certains cybercriminels. En particulier, les cybercriminels incapables de pénétrer les défenses des réseaux d'entreprise peuvent directement tirer profit des infections par vol d'informations, car ces infections permettent un accès rapide et facile aux identifiants des utilisateurs pour accéder aux réseaux d'entreprise souhaités.

En télétravail, certains employés utilisent leurs appareils personnels pour naviguer sur Internet, tant au travail que pour leur vie privée. Ce faisant, ils peuvent choisir de stocker leurs identifiants d'utilisateur dans les bases de données et extensions de mots de passe de leurs navigateurs Web, ou utiliser les fonctions de saisie automatique des navigateurs Web. Les voleurs d'informations ciblent ces bases de données de mots de passe, ainsi que les cookies d'authentification et autres données personnelles du navigateur Web.

Contrairement aux appareils professionnels, les politiques de sécurité d'entreprise ne sont pas toujours appliquées aux appareils personnels, ce qui représente un risque accru pour les organisations. Par exemple, les employés peuvent se livrer à des activités telles que le téléchargement de logiciels piratés et la navigation en ligne à haut risque, augmentant ainsi leur exposition aux cybermenaces et aux infections par des logiciels malveillants.

Les voleurs d'informations, les distributeurs, les courtiers en accès initial et les affiliés aux logiciels de rançons constituent désormais un élément essentiel d'un écosystème de la cybercriminalité axé sur le profit. Cet écosystème gagne en efficacité lorsque les cybercriminels se spécialisent et développent des capacités ciblant des étapes spécifiques d'une attaque, puis vendent ces capacités sous forme de service à d'autres criminels affiliés.

Menaces

L'ACSC de l'ASD surveille l'augmentation des activités de vol d'informations à l'échelle mondiale, ce qui représente une menace croissante pour les réseaux australiens. Les rapports sectoriels indiquent que les voleurs d'informations ont été la variante de logiciel malveillant la plus répandue dans la cybercriminalité en 2023. L'augmentation du volume de données volées en vente sur les marchés du Dark Web et l'augmentation de l'activité des courtiers en accès initial exploitant ces données reflètent cette tendance à la hausse, qui s'est accélérée en 2024.

Écosystème des voleurs d'informations

Étape 1 : Acquérir le logiciel malveillant

Les voleurs d'informations sont généralement proposés, sur les marchés cybercriminels, sous forme de MaaS (Stealer-as-a-Service), ou vendus sous forme de code source. Le MaaS désigne un modèle commercial dans lequel un développeur de logiciels malveillants vend un abonnement à son logiciel malveillant à des particuliers via une plateforme Web, à l'instar des offres SaaS légitimes. Le modèle MaaS a abaissé les barrières à l'entrée pour les cybercriminels, car il permet à des individus sans compétences techniques approfondies de diffuser des logiciels malveillants et de collecter des informations volées pour les utiliser dans des cyberattaques.

Les voleurs d'informations proposés en MaaS le sont généralement à un tarif mensuel relativement abordable et permettent aux cybercriminels d'accéder à un tableau de bord dédié. Ce tableau de bord facilite la création de voleurs d'informations, organise les données volées et suit le nombre de systèmes compromis. Les opérateurs MaaS proposent des mises à jour de fonctionnalités, des outils et une assistance technique pour échapper à la détection des antivirus et attirer et fidéliser les abonnés. De nombreux voleurs d'informations peuvent s'auto-supprimer de l'appareil de la victime après avoir exfiltré les données.

Étape 2 : Diffusion

Les cybercriminels qui diffusent des voleurs d'informations et collectent des informations sur les appareils compromis sont appelés « ouvriers » (distributeurs de trafic). Les ouvriers dirigent les victimes vers des liens malveillants, facilitant ainsi la propagation des voleurs d'informations dans le cadre de campagnes de grande envergure. La plupart des campagnes sont aveugles et s'appuient sur des infections opportunistes. Cependant, certaines campagnes sont adaptées à des secteurs spécifiques et impliquent du hameçonnage ciblé contre des victimes spécifiques. Les ouvriers mènent ces campagnes plus ciblées en réponse à la demande des clients ; par exemple, lorsque les acheteurs cherchent à accéder à des organisations ou des secteurs spécifiques à forte valeur ajoutée.

Les ouvriers déploient des voleurs d'informations sur les appareils de leurs victimes en utilisant un large éventail de techniques, notamment :

- **les réseaux de zombies ou botnets** : réseaux de systèmes informatiques compromis contrôlés par des cybercriminels pour mener des actions malveillantes, telles que la diffusion de messages d'hameçonnage ou de logiciels malveillants;

- **l'hameçonnage** : tentatives d'obtenir des informations sensibles par tromperie, notamment courriel ou message direct sur les réseaux sociaux, les forums et les applications de messagerie. Ces méthodes de diffusion courantes ont abaissé la barrière d'entrée pour les cybercriminels :
  - ces messages contiennent généralement un lien malveillant, plutôt que des fichiers malveillants joints au courriel lui-même.
- **des résultats de recherche malveillants** : diffusés via des techniques d'optimisation pour les moteurs de recherche (SEO) qui redirigent les cibles vers des sites Web diffusant des logiciels malveillants déguisés en logiciels ou autres contenus légitimes ;
- **la publicité malveillante** : utilisation de code malveillant, injecté dans des publicités en ligne légitimes, pour diffuser des logiciels malveillants ;
- **les logiciels cassés ou piratés** : téléchargements, y compris de jeux vidéo, partagés via des vidéos YouTube, avec des liens malveillants dans la description ou les commentaires des vidéos, ou provenant de sites de téléchargement non fiables ;
- **les publicités et publications sur les réseaux sociaux** : redirigeant les cibles vers des fichiers malveillants déguisés ;
- **les mises à jour de logiciels malveillants** : généralement déguisées en mises à jour de navigateur Web.

Étape 3 : Collecte de données

Une fois qu'un voleur d'informations s'exécute sur l'appareil de la victime, il commence à collecter des données sensibles sur la machine compromise. Outre le vol des identifiants utilisateur, lorsque les voleurs d'informations font partie d'un botnet, les cybercriminels peuvent contrôler à distance l'appareil compromis en envoyant des commandes de configuration pour activer des fonctionnalités supplémentaires ou diffuser d'autres logiciels malveillants. En général, les voleurs d'informations sont capables de voler :

- noms d'utilisateur et mots de passe, notamment ceux stockés dans les sessions/jetons d'authentification multifacteur (AMF) des navigateurs Web ;
- cookies d'authentification ;
- informations de formulaire de saisie automatique du navigateur Web ;
- identifiants, contenus et contacts de messagerie ;
- historique de navigation Web ;
- documents utilisateur
- informations de carte bancaire ;
- journaux de discussion des applications de messagerie ;
- informations système
- portefeuilles de cryptomonnaies ;
- identifiants VPN ou FTP (File Transfer Protocol).

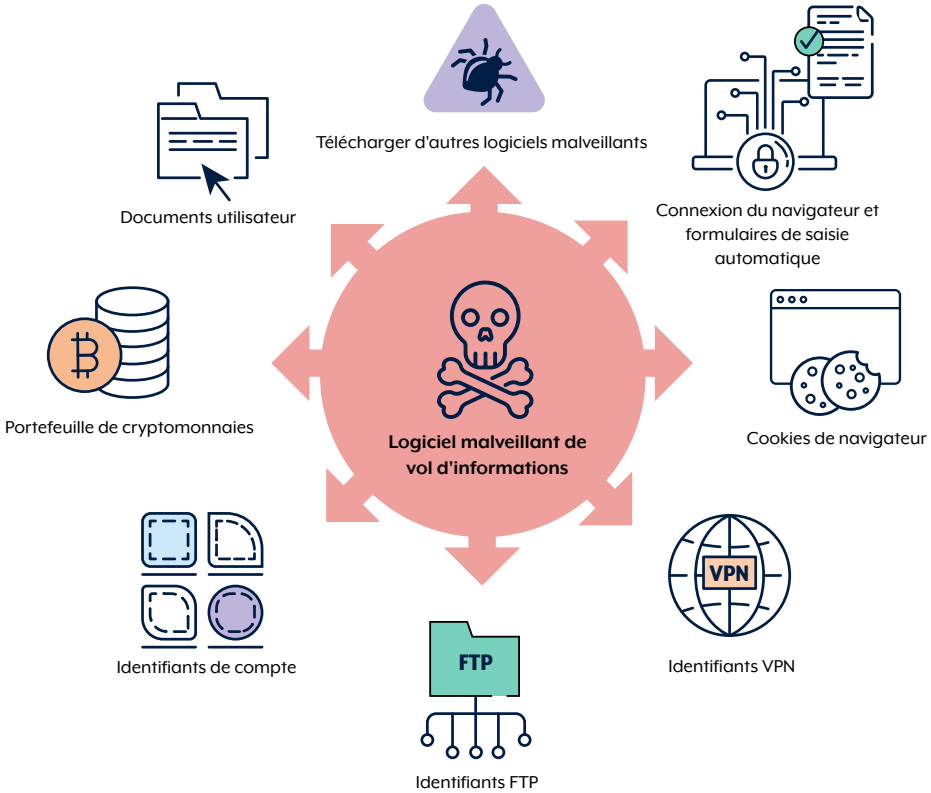


Figure 1. Fonctionnalité de vol d'informations

Certains cookies d'authentification de navigateur Web maintiennent la connexion d'un utilisateur à un compte ou à un service pendant plusieurs jours, évitant ainsi une réauthentification. En cas de vol, ces cookies d'authentification pourraient contourner efficacement les exigences de l'AMF et permettre aux cybercriminels d'accéder aux comptes des victimes, ainsi qu'aux réseaux et systèmes d'entreprise.

Étape 4 : Agrégation et monétisation des données

Les voleurs d'informations sont configurés pour exfiltrer les informations des victimes, appelées « journaux », vers des serveurs de commande et de contrôle malveillants. En général, les voleurs d'informations utilisent des applications de messagerie populaires, telles que Telegram et Discord, pour partager un flux de journaux avec les cybercriminels.

Des marchés spécialisés existent sur Telegram et sur le Dark Web pour la vente et le commerce de journaux. Les cybercriminels monétisent les journaux de diverses manières, notamment :

- en vendant les journaux sur des marchés criminels, notamment à des courtiers en accès initial ;
- en exploitant directement la victime, par le biais d'une usurpation d'identité et d'une extorsion ;
- en exploitant les informations pour un accès initial aux réseaux d'entreprise à des fins de logiciel de rançon.

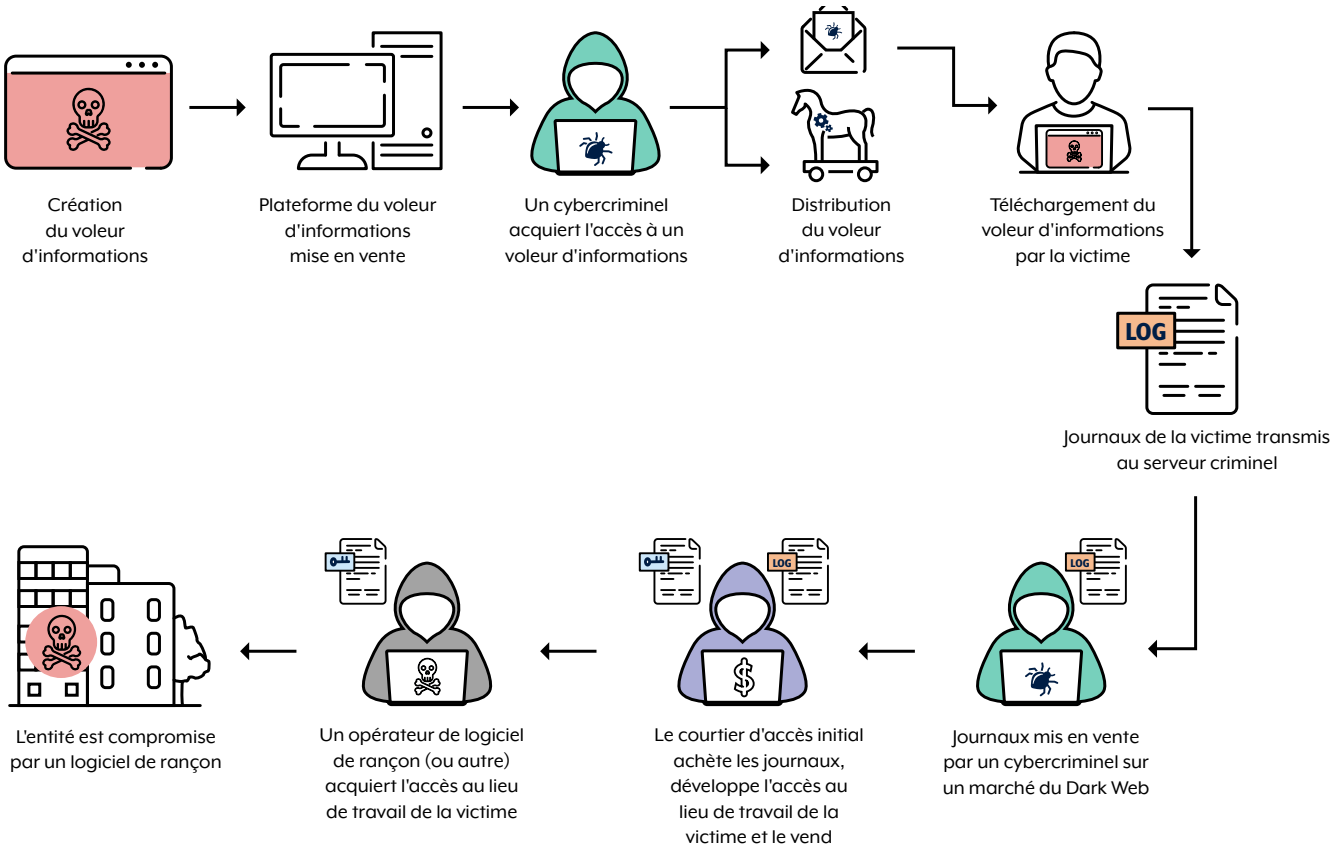


Figure 2. Écosystème du voleur d'informations et impact potentiel sur une organisation

Implications

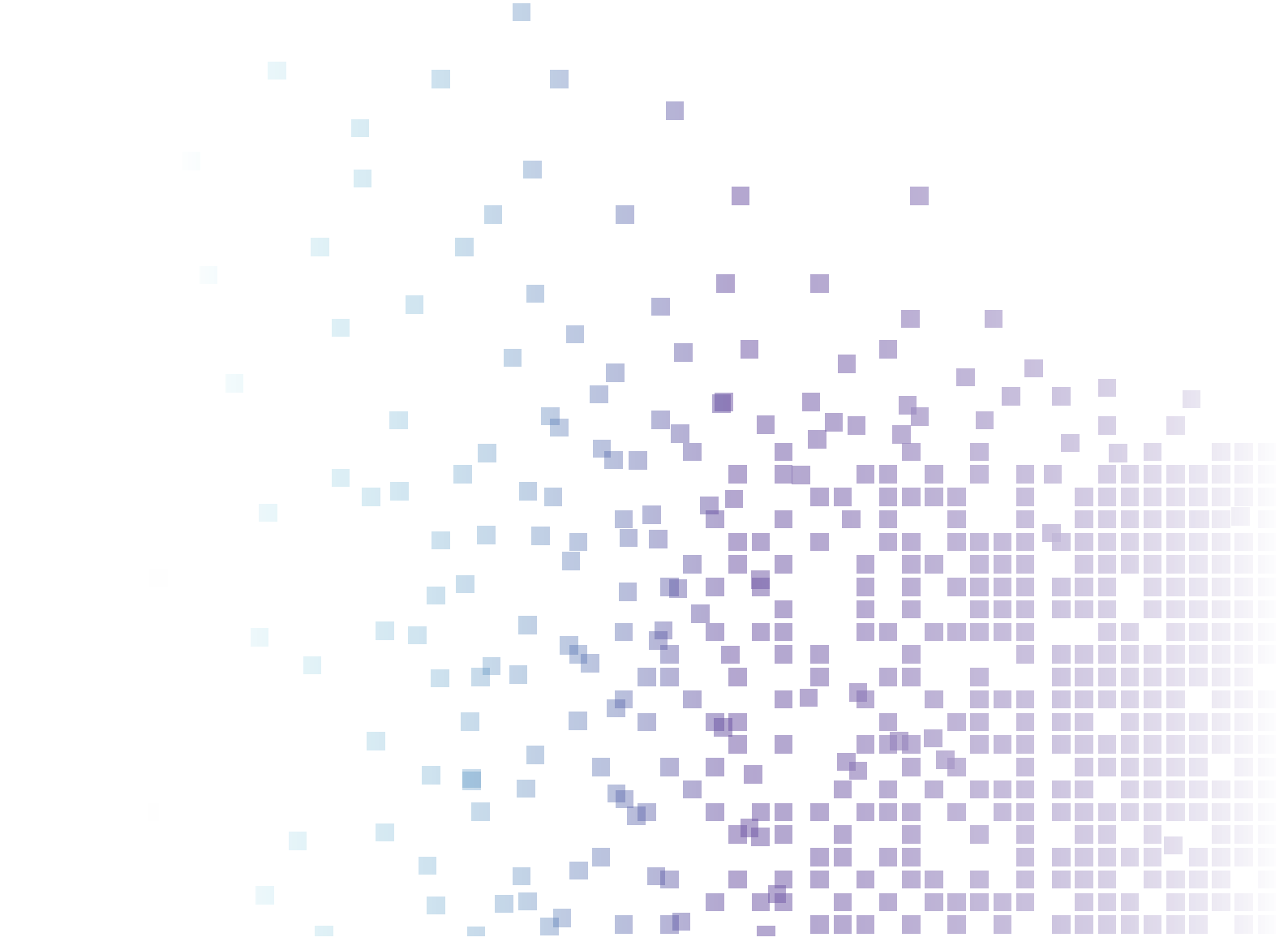
Les voleurs d'informations peuvent avoir de graves conséquences, tant pour les particuliers que pour les organisations. Lorsque les voleurs d'informations collectent les identifiants des utilisateurs, les cybercriminels peuvent les utiliser pour accéder aux réseaux ou aux systèmes d'entreprise avec des comptes utilisateurs valides, retardant souvent la détection par les propriétaires des systèmes.

Pour les **organisations** victimes de voleurs d'informations, les conséquences peuvent inclure :

- logiciel de rançon ;
- violation de données ;
- compromission de messagerie professionnelle;
- vol de propriété intellectuelle ;
- vol d'informations sensibles.

Pour une **personne** victime de voleurs d'informations, les conséquences peuvent inclure :

- accès non autorisé à sa messagerie personnelle ou à ses comptes de réseaux sociaux ;
- risque accru d'usurpation d'identité ;
- risque accru d'attaques par hameçonnage ;
- perte financière ou accès non autorisé à ses comptes financiers ;
- atteinte à la vie privée.



Étude de cas :

Cette étude de cas a été anonymisée pour permettre sa diffusion publique. Elle s'appuie sur plusieurs incidents de cybersécurité ayant affecté des entités australiennes qui ont signalé ces incidents à l'ACSC de l'ASD. L'entité concernée est ci-après dénommée « l'organisation ». Les noms des personnes mentionnées dans cette étude de cas sont fictifs et les informations ont été supprimées afin de protéger l'identité des victimes.

L'organisation est une entreprise australienne qui permet à ses employés d'accéder aux systèmes de l'entreprise depuis leurs appareils personnels. Alice est une employée de l'organisation qui travaille à distance.

Lorsqu'elle travaille à domicile, Alice accède à distance au réseau de son organisation via son ordinateur portable personnel. Alice a **téléchargé**, sur son **ordinateur portable personnel**, une version de Notepad++ (un type de logiciel de prise de notes) à partir d'un site Web qu'elle croyait légitime. Un **voleur d'informations** s'est fait passer pour l'installateur du logiciel Notepad++.

Lorsqu'Alice a tenté d'installer le logiciel, le voleur d'informations s'est activé et a commencé à **récupérer les identifiants de l'utilisatrice** sur son ordinateur portable. Il s'agissait notamment de son nom d'utilisateur et de son mot de passe professionnels, enregistrés dans la fonction d'enregistrement des identifiants de son navigateur Web. Le voleur d'informations a ensuite envoyé ces identifiants à un serveur de commande et de contrôle distant contrôlé par un groupe de cybercriminels.

Les journaux volés ont été regroupés avec d'autres, puis **vendus à des cybercriminels** via un marché du Dark Web.

Un cybercriminel nommé Bob a acheté les identifiants d'Alice et découvert les identifiants d'accès aux services du réseau de son organisation. L'organisation d'Alice n'avait **pas configuré l'authentification AMF** pour ces services. Ainsi, il suffisait que Bob utilise les identifiants volés pour **s'authentifier et accéder** au réseau d'entreprise.

Bob a accédé au réseau d'entreprise d'Alice sans se faire repérer grâce aux **identifiants valides volés**. Bob a pu s'infiltrer latéralement dans le réseau d'entreprise, identifiant des données sensibles appartenant à l'organisation et les exfiltrant afin de l'extorquer.

Après avoir volé les données sensibles, Bob a **crypté** les **bases de données et les systèmes de fichiers** de l'organisation pour les rendre inaccessibles.

Mesures d'atténuation

Les organisations peuvent ne pas être en mesure d'appliquer des contrôles sur les appareils connectés à leur réseau d'entreprise, en particulier sur les appareils personnels utilisés par les employés en télétravail. L'ACSC d'ASD recommande aux organisations de se concentrer sur la mise en œuvre de contrôles pour se protéger contre le risque de vol d'informations ciblant les identifiants des utilisateurs. Les mesures d'atténuation sont les suivantes :

Formez le personnel à la cybersécurité

- Prévenir les tentatives d'ingénierie sociale ciblée et les téléchargements de fichiers malveillants en dispensant une formation efficace au personnel.
- Sensibilisez votre organisation aux voleurs d'informations, à leurs méthodes de diffusion et aux menaces d'hameçonnage (phishing).

Sécurisez les comptes d'entreprise

- Mettez en œuvre l'AMF :
- Mettez en œuvre l'AMF sur les services externes et internes, les systèmes et les référentiels de données sensibles, en particulier pour la messagerie Web, les VPN et les comptes utilisateurs privilégiés qui accèdent aux systèmes critiques. La meilleure pratique consiste à mettre en œuvre une AMF résistante à l'hameçonnage sur tous les comptes.
- Désactivez les comptes utilisateurs lorsqu'ils ne sont plus nécessaires.
- Restreindre les privilèges d'administrateur :
- Effectuez l'administration réseau et les autres tâches à privilèges uniquement sur un poste de travail dédié et verrouillé (c'est-à-dire un poste d'administrateur sécurisé).
- Appliquez les meilleures pratiques de moindre privilège en exigeant des administrateurs qu'ils utilisent des comptes utilisateurs à privilèges pour la gestion des systèmes et des comptes utilisateurs standard pour les tâches non administratives.
- Empêchez les comptes utilisateurs à privilèges (à l'exception de ceux explicitement autorisés à accéder aux services en ligne) d'accéder à Internet, à la messagerie électronique et aux services Web.
- Envisagez de mettre en œuvre une administration juste-à-temps pour les systèmes et les applications.
- Imposez la gestion et l'audit des comptes utilisateurs à privilèges.
- Mettez à jour régulièrement les mots de passe, en particulier ceux des comptes d'accès distant externes.
- Appliquez des délais d'expiration et des politiques de suppression pour les jetons de session et les cookies.

Renforcez la mobilité de l'entreprise.

- Effectuez une évaluation des risques liés à la mobilité d'entreprise et mettez en œuvre des directives de renforcement de la mobilité d'entreprise.
- Mettez en œuvre une politique BYOD (Bring Your Own Device) si vous autorisez vos employés à utiliser leurs appareils personnels pour le travail, car les appareils gérés par l'entreprise sont plus sécurisés que les appareils personnels non gérés.

Examinez et évaluez les risques liés à la chaîne d'approvisionnement liés à l'accès des fournisseurs à vos réseaux, notamment les fournisseurs de logiciels en tant que service (SaaS) et les fournisseurs de services gérés. Comment gérer votre sécurité lorsque vous faites appel à un fournisseur de services gérés.

Protégez votre réseau d'entreprise

- Maintenez les applications et les systèmes d'exploitation à jour.
- Appliquez des politiques de sécurité locales pour renforcer le contrôle des applications grâce à une liste d'autorisations stricte.
- Mettez en œuvre une segmentation du réseau pour séparer les segments en fonction du rôle et des fonctionnalités.
- Auditez et surveillez les activités des utilisateurs, en particulier pour les employés distants.
- La surveillance des comptes privilégiés peut révéler des accès non autorisés à des données sensibles ou des activités de transfert de données inhabituelles, telles que le téléchargement de volumes importants de données vers un réseau externe.
- Mettez en œuvre des politiques et des outils de prévention des pertes de données pour empêcher les transferts non autorisés.

Devenez partenaire du réseau de cybersécurité de l'ASD et rejoignez le service de partage de renseignements sur les cybermenaces (Cyber Threat Intelligence Sharing, CTIS) de l'ASD.

- Le CTIS est une plateforme de partage bidirectionnelle qui permet aux partenaires gouvernementaux et industriels de recevoir et de partager des informations sur la cyberactivité malveillante.
- L'ACSC de l'ASD surveille l'activité des voleurs d'informations et partage les détails de l'infrastructure de commandement et de contrôle active via la plateforme CTIS.
- Inscrivez-vous pour devenir partenaire et protéger les données de votre organisation et de vos clients contre les menaces cybercriminelles.

Préparez-vous à une compromission

- Élaborez un plan de réponse aux incidents de cybersécurité à utiliser en cas de compromission par un voleur d'informations. Assurez-vous que les employés savent quoi faire et qui contacter s'ils soupçonnent avoir téléchargé un fichier suspect.

Mettez en œuvre les huit mesures essentielles de l'ACSC de l'ASD

- Outre les mesures d'atténuation mentionnées ci-dessus, l'ACSC de l'ASD recommande vivement de mettre en œuvre les huit mesures essentielles de l'ACSC de l'ASD.

Conseils pour vos employés en télétravail

- Protégez vos informations sur vos appareils personnels
  - Développez une bonne hygiène informatique : ne cliquez pas sur des fenêtres contextuelles ou liens suspects, et ne téléchargez pas de fichiers ou de logiciels provenant de sources inconnues ou non fiables.
  - Utilisez des mots de passe distincts pour vos comptes professionnels et personnels. Utilisez l'AMF pour vos comptes personnels lorsque cela est possible.
  - Ne stockez pas vos identifiants professionnels dans un gestionnaire de mots de passe personnel, sauf autorisation expresse de votre employeur. Cela inclut le gestionnaire de mots de passe de votre navigateur Web. **En cas de doute, demandez à votre employeur de vous fournir un gestionnaire de mots de passe d'entreprise.**
  - Ne vous connectez pas à vos comptes professionnels depuis des postes de travail partagés ou collectifs.
  - Soyez attentif aux données stockées dans la fonction de saisie automatique de votre navigateur Web. Les voleurs d'informations ciblent les données enregistrées par les navigateurs dans les formulaires de saisie automatique. Lorsque vous remplissez des formulaires Web, pensez à saisir manuellement les données sensibles, telles que les numéros de carte bancaire, plutôt que de les enregistrer dans la fonction de saisie automatique de votre navigateur.
  - Déconnectez-vous de tous les services en ligne et effacez les cookies de votre navigateur après une session de navigation afin de réduire la quantité d'informations accessibles aux voleurs d'informations.
  - Assurez-vous que l'antivirus intégré à votre système d'exploitation est activé. Si vous utilisez un antivirus tiers, assurez-vous qu'il est à jour et qu'il provient d'un fournisseur fiable.

Assistance

Les organisations australiennes affectées ou ayant besoin d'aide concernant une compromission par un voleur d'informations peuvent contacter l'ACSC de l'ASD au **1300 CYBER1 (1300 292371)** ou en soumettant un rapport sur cyber.gov.au/report.

L'ACSC de l'ASD encourage les entités à signaler toute activité réseau suspecte et les indicateurs de compromission associés aux voleurs d'informations, même si un incident est considéré comme contenu. Nous utilisons les informations que vous fournissez pour améliorer notre compréhension des tactiques, techniques et procédures des acteurs de cybermenace, ce qui nous aide à avertir d'autres organisations australiennes qui ont été ciblées de la même manière.

Avis de non-responsabilité

Les éléments figurant dans ce guide sont de caractère général et ne doivent pas être considérés comme des conseils juridiques ou une forme d'aide dans des circonstances particulières ou dans une situation d'urgence. Pour toute question importante, vous devriez obtenir les conseils d'un professionnel indépendant relativement à vos circonstances spécifiques.

Le Commonwealth n'endosse aucune responsabilité en cas de dommages, de perte ou de dépenses découlant de l'utilisation des informations contenues dans ce guide.

Pour en savoir plus ou pour signaler un incident de cybersécurité, contactez-nous :

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Vous ne pouvez appeler ce numéro que depuis l'Australie.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre