Devolutions

État des menaces 2024 pour les gestionnaires de mots de passe

Auteur: William Matos
Date: 16 octobre 2024
Version: 1.0
TLP: Blanc

Table des matières

Introduction

Qu'est-ce qu'un rapport sur l'état des menaces?

Il s'agit d'un rapport détaillé qui décrit les menaces actuelles et émergentes en matière de cybersécurité impactant les organisations, les industries ou des régions spécifiques. Dans ce rapport, nous nous concentrerons sur les menaces liées aux gestionnaires de mots de passe et les incidents de sécurité affectant les entreprises spécialisées dans ce domaine.

Objectifs du rapport

Cependant, malgré leurs avantages, les gestionnaires de mots de passe ne sont pas à l'abri des menaces. L'évolution du paysage des menaces présente des risques significatifs pour ces outils, les cybercriminels élaborant sans cesse de nouvelles méthodes pour compromettre leur sécurité. Ce document vise à définir le paysage mondial des menaces liées aux gestionnaires de mots de passe, en offrant un aperçu complet des défis et des risques auxquels les utilisateurs et les développeurs sont confrontés.

Importance des gestionnaires de mots de passe

Dans le paysage numérique actuel, les gestionnaires de mots de passe sont devenus des outils indispensables pour les particuliers et les organisations souhaitant sécuriser leurs mots de passe. À mesure que la dépendance aux services numériques augmente, les menaces se multiplient également. Les gestionnaires de mots de passe offrent un moyen pratique et sécurisé d'emmagasiner, gérer et récupérer des mots de passe complexes, réduisant ainsi le risque de vol d'identifiants et renforçant la posture globale de cybersécurité.

Paysage actuel des menaces

Aperçu des cybermenaces

À mesure que les gestionnaires de mots de passe deviennent essentiels, ils attirent de plus en plus l'attention des cybercriminels. Le paysage des menaces comprend diverses méthodes d'attaque, notamment les voleurs d'informations, la publicité malveillante et les campagnes de logiciels malveillants avancés, toutes conçues pour compromettre des données sensibles telles que les mots de passe et les informations personnelles. Les principales menaces incluent :

1. Voleurs d'informations et logiciels malveillants
2. Publicité malveillante
3. Attaques sophistiquées et campagnes

Voleurs d'informations

Un **voleur d'informations** est un logiciel malveillant conçu pour dérober des informations sensibles telles que les mots de passe, les coordonnées bancaires et les données personnelles depuis un appareil infecté. Il se propage généralement via le hameçonnage, les téléchargements malveillants ou les vulnérabilités logicielles, collectant discrètement les données volées pour les envoyer aux attaquants en vue d'une utilisation abusive.

Selon l'équipe X-Force d'IBM, les vecteurs d'attaque initiaux courants lors des violations de sécurité impliquent souvent l'utilisation d'identifiants valides et de logiciels malveillants tels que les voleurs d'informations.

En résumé, l'augmentation de l'activité des voleurs d'informations et l'utilisation d'identifiants valides pour accéder aux systèmes illustrent une tendance croissante des cybercriminels à privilégier des approches furtives et indirectes pour infiltrer les réseaux et voler des informations précieuses. Ces méthodes leur permettent souvent d'éviter la détection pendant de plus longues périodes, augmentant ainsi les dommages qu'ils peuvent causer.

Accès initial à partir d'identifiants valides

Augmentation de 71 % de 2022 à 2023

L'utilisation de voleurs d'informations par les cybercriminels

Augmentation de 266 % de 2022 à 2023

Menaces émergentes liées aux voleurs d'informations

Dans cette section, nous examinerons des campagnes de voleurs d'informations, notamment Meduza Stealer, Stealc et Luca Stealer Trojan. Ces campagnes malveillantes ciblent au moins 13 gestionnaires de mots de passe, cherchant à compromettre des comptes en exploitant des dépôts de données, des plateformes de messagerie instantanée et des services automatisés de dépôts opérés par des bots pour récolter des identifiants.

Ces attaques aboutissent au vol de données hautement sensibles, telles que des identifiants de connexion, qui sont ensuite vendues sur le marché clandestin. Les cybercriminels impliqués sont motivés financièrement et se concentrent sur la monétisation des comptes compromis.

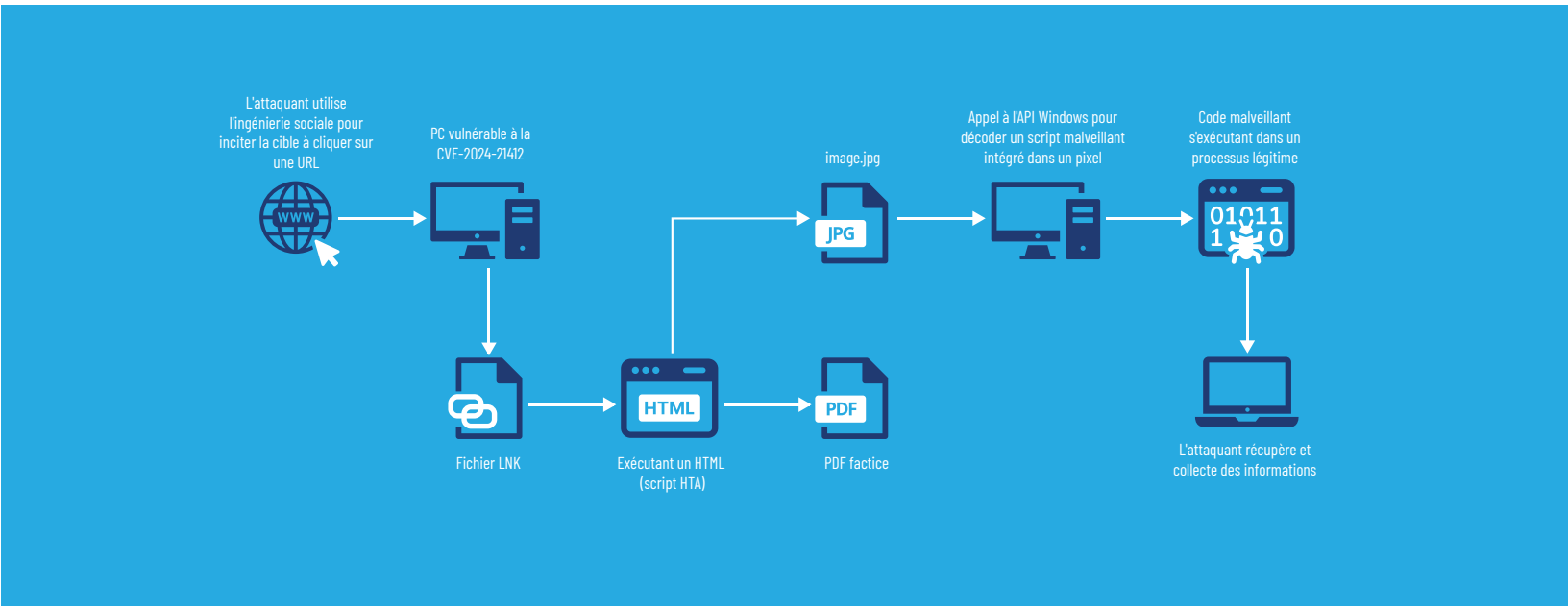
Les groupes de rançongiciels cherchent à réduire le temps nécessaire pour exploiter une cible, et l'utilisation de comptes compromis peut leur permettre de gagner du temps tout en rendant plus difficile pour les défenseurs de détecter des comportements suspects provenant d'un compte valide. Cela explique pourquoi les voleurs d'informations ont gagné en popularité au cours des dernières années.

Détails d'une campagne de voleurs d'informations

Les voleurs d'informations ont exploité la vulnérabilité CVE-2024-21412, une faille dans Microsoft Defender SmartScreen qui permet aux attaquants de contourner les contrôles de sécurité en utilisant des raccourcis Internet malveillants. Des menaces telles que Lumma Stealer, Water Hydra, DarkGate, Meduza et ACR tirent parti de cette vulnérabilité de SmartScreen pour cibler leurs victimes.

La méthode d'attaque commence par attirer les victimes à cliquer sur une URL qui déclenche le téléchargement d'un fichier raccourci (LNK). Ce fichier télécharge à son tour un exécutable contenant un script HTML Application (HTA) avec du code PowerShell conçu pour récupérer des fichiers PDF factices et des injecteurs malveillants. Un injecteur notable décode du code malveillant caché dans un fichier image JPG en utilisant l'API Windows.

Une fois à l'intérieur, les voleurs s'implantent dans des processus Windows légitimes, permettant ainsi le début de l'exfiltration des données. Ces voleurs ciblent un large éventail d'informations sensibles, y compris les données provenant de navigateurs Web (comme Chrome et Firefox), de portefeuilles de crypto-monnaies (Binance, Ledger Live), d'applications de messagerie (Telegram, WhatsApp), de gestionnaires de mots de passe (Bitwarden, 1Password), d'applications VPN, de clients de messagerie et de clients FTP.

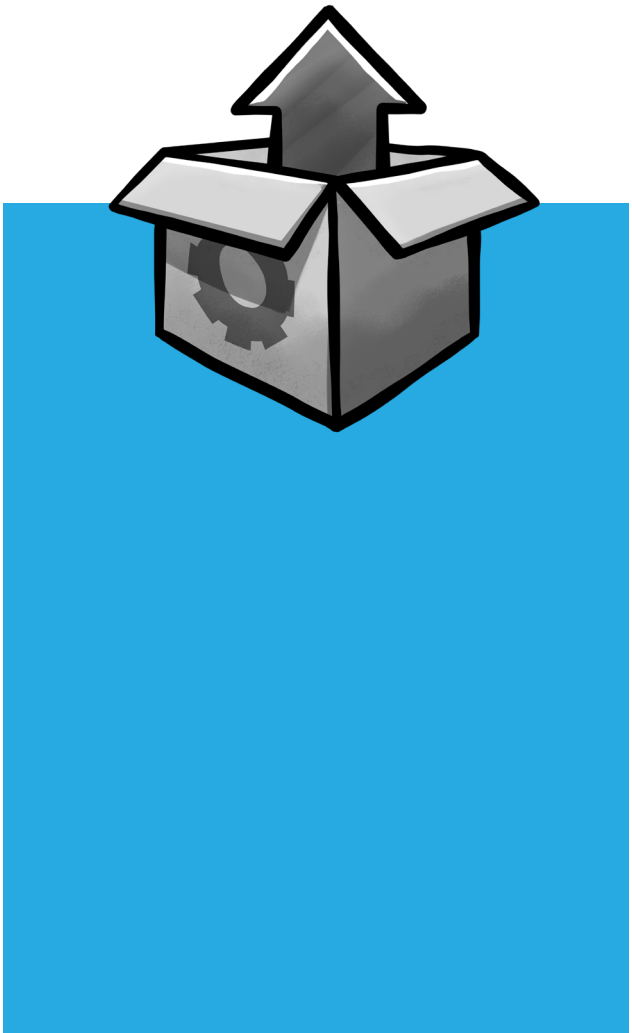


Publicité malveillante

Une seconde menace que nous avons découverte est la publicité malveillante, ou "malvertising". Ce terme désigne la pratique consistant à injecter du code ou des publicités malveillantes dans des réseaux de publicité en ligne légitimes. Ces publicités apparaissent sur des sites Web bien connus afin d'atteindre un large public et d'infecter un grand nombre de personnes.

Nous avons identifié plusieurs publicités pour de faux gestionnaires de mots de passe et un faux installateur de gestionnaire de bureau à distance sur un site d'échange pair-à-pair.

Cette technique exploite le fait que de nombreux nouveaux utilisateurs ne comprennent pas pleinement le produit ou ne connaissent pas son apparence habituelle. Les attaquants profitent de ce manque de connaissances pour tromper les utilisateurs et les inciter à cliquer ou à télécharger ces logiciels malveillants qui semblent légitimes au premier abord.



Malware ZenRat

En 2023, le malware ZenRat a émergé comme une menace majeure, diffusé via un faux package d'installation du gestionnaire de mots de passe Bitwarden.

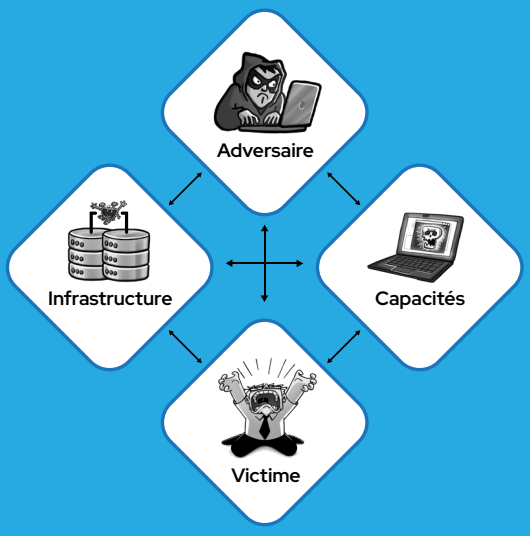
Les cybercriminels ont utilisé la **publicité malveillante** sur Google Ads, exploitant le classement des annonces pour diriger les utilisateurs vers une version clonée du site légitime de Bitwarden. Ce faux site se faisait même passer pour **Opensource.com**, en copiant un article de Scott Nesbitt pour paraître crédible. Le malware incite les utilisateurs à saisir leurs identifiants — nom d'utilisateur, mot de passe et clé secrète — permettant ainsi aux attaquants de voler des informations sensibles.

ZenRat est également diffusé via **l'empoisonnement SEO**, des bundles de logiciels publicitaires et des campagnes de phishing par e-mail. Il opère à la fois en interne et en externe, avec des adresses IP malveillantes retracées dans divers endroits. Ces attaques sont principalement motivées par des gains financiers, cherchant à monétiser les données volées ou à vendre des accès compromis.

ZenRAT est une variante de malware apparue en tant que Trojan d'accès à distance (RAT), souvent associée à des activités cybercriminelles. Il est conçu pour offrir aux attaquants un accès non autorisé à un système infecté, leur permettant de mener une large gamme d'actions malveillantes.

Motivation : exfiltrer des informations précieuses afin de les vendre sur le dark web.

Serveur C2 (Command and Control).



Dans notre cas, ZenRAT a été diffusé via un faux package d'installation du gestionnaire de mots de passe Bitwarden.

Contrôle à distance : le malware offre à l'attaquant un accès complet à la machine de la victime.

Il enregistre les frappes au clavier, prend des captures d'écran et récupère des fichiers sensibles.

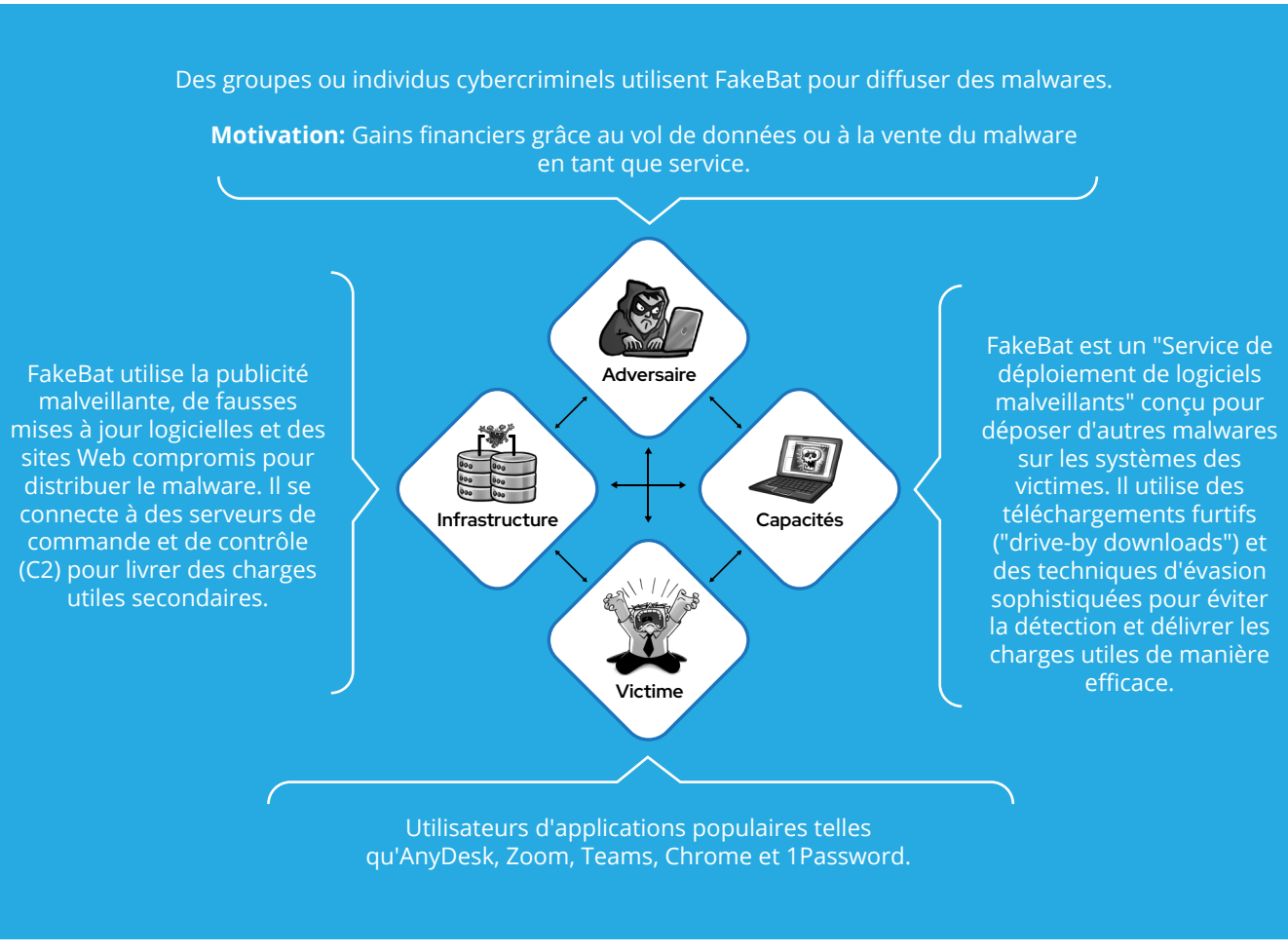
Opportunistes, ils chercheront à piéger quiconque avec la campagne frauduleuse de Bitwarden.

Malware FakeBat

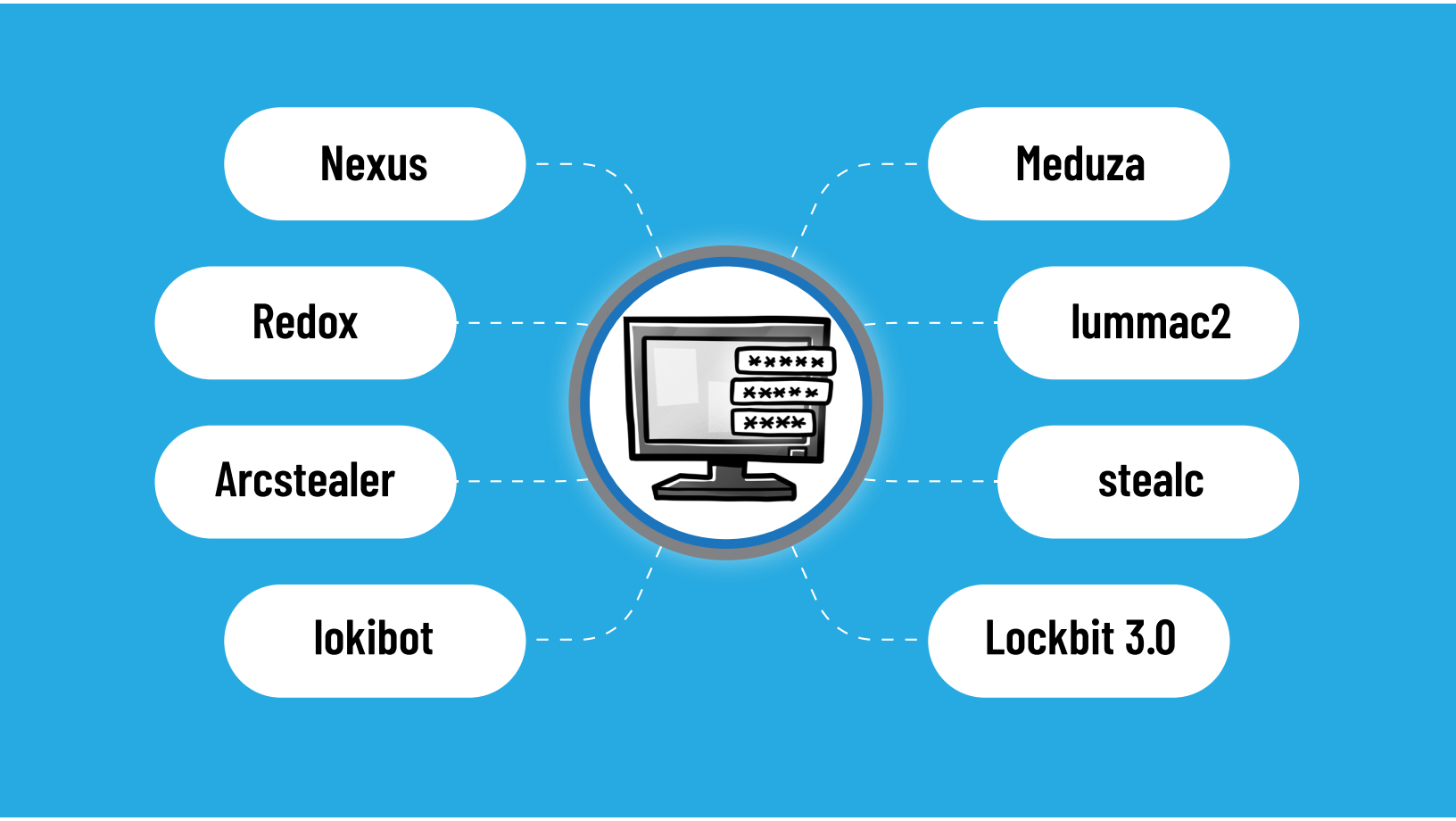
Un autre malware utilisant une technique similaire est FakeBat. Ce malware constitue une menace hautement sophistiquée, distribuée via la publicité malveillante, des tactiques d'ingénierie sociale, des sites Web compromis et de fausses mises à jour de navigateurs. Il utilise une technique appelée téléchargement furtif ("drive-by download"), qui consiste à télécharger automatiquement un malware sur le système de l'utilisateur en exploitant des vulnérabilités du navigateur ou en l'intégrant à des logiciels légitimes tels que les gestionnaires de mots de passe, AnyDesk ou Teams.

FakeBat est un "Service de déploiement de logiciels malveillants" (LaaS), un service où le malware est vendu ou loué à d'autres cybercriminels. La principale fonction d'un loader est de déployer des charges utiles malveillantes supplémentaires sur un ordinateur compromis. Les cybercriminels utilisent les plateformes LaaS pour distribuer facilement leurs malwares sans avoir à développer leurs propres loaders, en faisant un élément clé d'un autre service : le "Malware-as-a-Service" (MaaS).

Les prix des services FakeBat varient de 1000 à 5000 dollars américains par semaine ou par mois, selon le forfait.

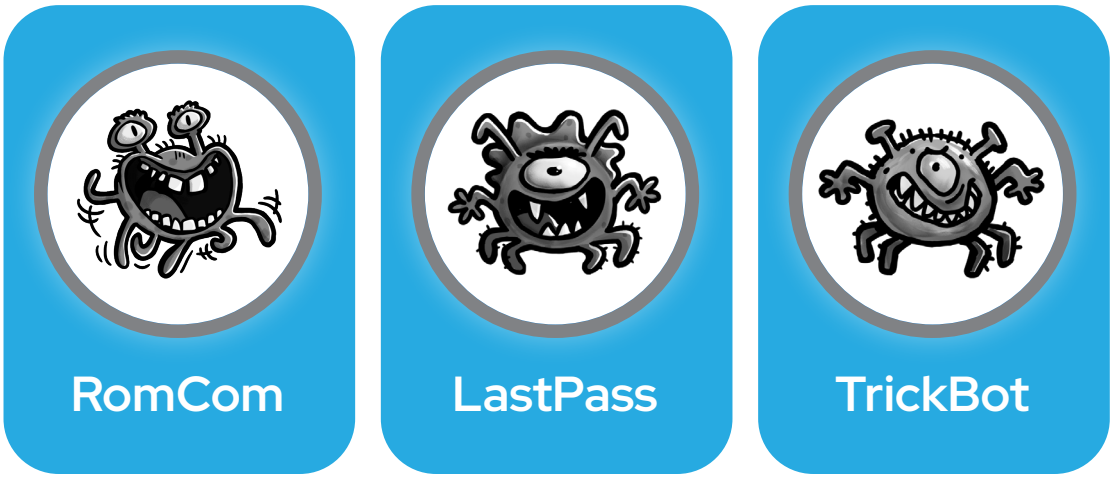


Principaux malwares connus pour cibler les gestionnaires de mots de passe



(https://securitysenses.com/posts/malware-targeting-password-managers)

Attaques sophistiquées



Cette section explore plusieurs cybermenaces de grande envergure qui illustrent la sophistication croissante des campagnes de malwares modernes, en se concentrant sur RomCom, LastPass et TrickBot.

Ces attaques exploitent des techniques avancées telles que l'hameçonnage, le typosquattage et les applications infectées par des malwares pour cibler des victimes dans divers secteurs. Par exemple, le trojan RomCom se fait passer pour un logiciel Devolutions afin de diffuser des malwares, ciblant particulièrement les organisations de santé en Ukraine et aux États-Unis.

La violation de sécurité de LastPass met en évidence les risques liés au vol d'identifiants parmi les employés privilégiés. Parallèlement, TrickBot continue d'évoluer avec des chaînes d'attaques complexes conçues pour voler des identifiants et infiltrer des réseaux.

À travers ces études de cas, nous obtenons un aperçu de la manière dont les menaces sophistiquées exploitent les vulnérabilités, révélant des schémas critiques dans l'évolution du paysage des menaces.

Le trojan RomCom

Le trojan RomCom consiste à ce que des attaquants se fassent passer pour des sites Web de logiciels légitimes ou fictifs afin de tromper les utilisateurs et les inciter à télécharger des malwares. Elle utilise des techniques telles que le hameçonnage, le typosquattage et les logiciels trojanisés, incluant des applications populaires comme Devolutions Remote Desktop Manager et KeePass.

Une fois installé, le malware offre un accès à distance permettant l'exfiltration de données. La campagne cible principalement des politiciens ukrainiens et des organisations de santé aux États-Unis, les attaquants étant suspectés d'appartenir au groupe Cuba Ransomware.

Active entre 2022 et 2023, cette campagne est motivée par des enjeux géopolitiques, avec pour objectif principal de recueillir des informations sensibles liées au conflit en Ukraine, en ciblant spécifiquement les organisations et individus impliqués dans cette crise.

Aperçu de la chaîne d'attaque

1.

Reconnaissance: Les attaquants identifient leurs cibles, principalement des politiciens ukrainiens et des organisations de santé américaines, en se concentrant sur ceux soutenant les efforts pro-Ukraine.

2.

Préparation offensive: Ils créent des versions trojanisées de logiciels populaires comme Devolutions Remote Desktop Manager et KeePass, en intégrant des charges utiles malveillantes dans des applications ayant une apparence légitime.

3.

Livraison: Le malware est distribué via des courriels de hameçonnage ciblé et des sites Web frauduleux imitant étroitement des pages de téléchargement de logiciels légitimes. Ces sites sont promus par des annonces Google pour attirer les victimes.

4.

Exploitation: Les victimes sont trompées pour télécharger et installer le logiciel trojanisé, accordant ainsi, à leur insu, aux attaquants un accès à leurs systèmes.

5.

Installation: Une fois l'application malveillante installée, le malware s'exécute et établit une porte dérobée ("backdoor") permettant un accès à distance.

6.

Commande et Contrôle (C2): Le malware communique avec des serveurs C2, utilisant souvent des certificats SSL auto-signés pour chiffrer le trafic et échapper à la détection.

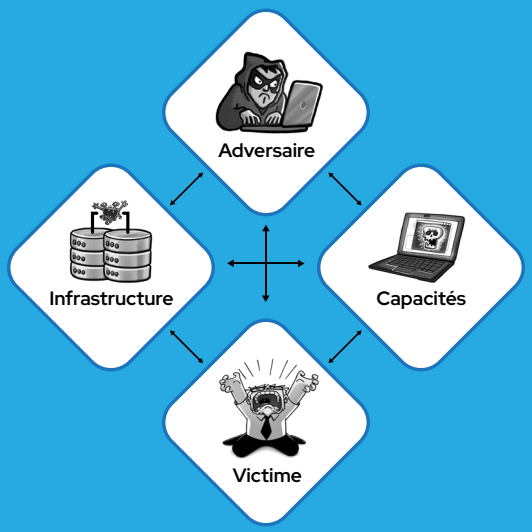
7.

Actions sur les objectifs: Les attaquants exfiltrent des données sensibles, y compris des informations liées au conflit en Ukraine, en utilisant la porte dérobée pour un accès à distance. Les objectifs de la campagne incluent à la fois des gains financiers et des avantages géopolitiques.

La campagne est suspectée d'être menée par le groupe Cuba Ransomware (également connu sous les noms Tropical Scorpius ou Void Rabisu), bien que l'attribution soit encore en cours de confirmation. Leurs motivations semblent être à la fois financières et géopolitiques, ciblant des organisations soutenant l'Ukraine.

Les attaquants s'appuient sur des sites Web frauduleux qui imitent des pages de téléchargement de logiciels légitimes (par exemple, Devolutions Remote Desktop Manager et KeePass). Ces sites clonés sont promus à l'aide d'annonces Google pour générer du trafic vers les téléchargements malveillants.

Les serveurs de commande et de contrôle (C2) utilisent des certificats SSL auto-signés pour chiffrer le trafic, rendant ainsi la détection et l'attribution plus difficiles.



Les attaquants utilisent plusieurs techniques sophistiquées:

Hameçonnage et typosquattage pour tromper les victimes et les inciter à visiter des sites malveillants.

Logiciels trojanisés intégrant des charges utiles DLL x64 pour infiltrer les systèmes des victimes.

Une fois installés, les malwares offrent un accès à distance et permettent l'exfiltration de données.

Les attaquants utilisent également des techniques anti-débogage et d'obfuscation pour échapper à la détection.

Les principales cibles sont les politiciens ukrainiens et les organisations de santé américaines. Ces victimes ont été choisies en raison de leur proximité avec des organisations pro-Ukraine, en particulier celles impliquées dans l'aide aux réfugiés pendant le conflit en cours.

Aperçu de l'incident LastPass

En 2022 et 2023, LastPass a subi des violations significatives, principalement motivées par des cybercriminels recherchant des gains financiers. Lors de la première attaque, des hackers ont compromis un ordinateur portable d'entreprise pour accéder à un environnement de développement cloud, volant du code source et des données sensibles. Cela leur a permis d'accéder aux systèmes de LastPass et de dérober des sauvegardes de coffres clients ainsi que des métadonnées associées.

Plus de six mois après cette violation initiale, LastPass a lié l'attaque d'août à une campagne prolongée. Les hackers ont utilisé les données de la première brèche, une violation chez un tiers, et une vulnérabilité d'exécution de code à distance sur l'ordinateur personnel d'un ingénieur DevOps pour voler plusieurs ressources et sauvegardes. Ils ont capturé le mot de passe maître de l'ingénieur, accédant ainsi à des coffres chiffrés et à des sauvegardes critiques de bases de données. L'attaque a exploité un malware de keylogging via un module logiciel vulnérable.

L'attaquant a ciblé l'un des quatre ingénieurs DevOps ayant accès aux clés de déchiffrement, capturé leur mot de passe maître après l'authentification multifactorielle et accédé au coffre d'entreprise de l'ingénieur, permettant l'accès à des ressources sensibles et des sauvegardes.

Pour plus d'informations sur l'incident, consultez cet article:
https://www.cybersecuritydive.com/news/lastpass-cyberattack-timeline/643958/

En plus de ces violations, les utilisateurs de LastPass ont été ciblés par des cybercriminels se faisant passer pour des membres du personnel, utilisant le **kit d'hameçonnage Crypto Chameleon** pour renforcer leurs attaques. Bien que ces attaques d'hameçonnage aient affecté des employés et des utilisateurs, LastPass a rapporté que leurs systèmes centraux sont restés intacts.

Qu'est-ce que le kit d'hameçonnage Crypto Chameleon?

Le **kit d'hameçonnage Crypto Chameleon** est un outil utilisé par les cybercriminels pour créer des attaques d'hameçonnage imitant des services légitimes. Il fournit des modèles et des mécanismes pour tromper les utilisateurs et les inciter à divulguer des informations sensibles, telles que des identifiants de connexion, facilitant ainsi la mise en œuvre de campagnes d'hameçonnage ciblées et efficaces.

Résumé du déroulement de l'attaque:

1. **Accès initial:** Probablement obtenu par une attaque de hameçonnage ou une technique d'ingénierie sociale ciblant un employé disposant d'un accès privilégié.
2. **Élévation de privilèges:** Les attaquants ont élevé leurs privilèges, probablement en obtenant l'accès à des systèmes clés.
3. **Mouvement latéral:** Ils ont navigué à travers le réseau, atteignant finalement et exfiltrant les coffres clients chiffrés.
4. **Exfiltration de données:** Les données des coffres volés ont été transférées hors des systèmes de LastPass via des canaux chiffrés, probablement par petits lots afin d'éviter la détection.
5. **Évasion des défenses:** Tout au long de l'attaque, l'adversaire a utilisé des techniques pour échapper à la détection, en exploitant possiblement des outils légitimes présents dans l'environnement.

Chaîne d'attaque

Reconnaissance: Les attaquants ont probablement recueilli des informations sur les employés de LastPass disposant d'un accès privilégié.

Préparation offensive: Une campagne de hameçonnage ciblant un ingénieur DevOps senior a été lancée.

Livraison: Un courriel de hameçonnage a livré le maliciel d'enregistreur de frappe ("malware keylogger") sur l'appareil de l'ingénieur.

Exploitation: Les attaquants ont capturé le mot de passe maître et les identifiants de l'employé.

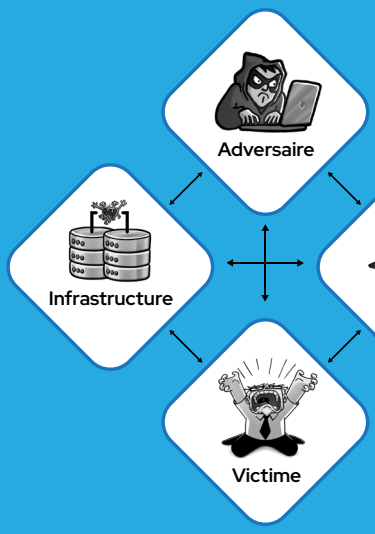
Installation: Le logiciel enregistreur de frappe a permis aux attaquants de maintenir une persistance.

Commande et Contrôle: Accès à distance au stockage infonuagique et aux coffres d'entreprise.

Actions sur les objectifs: Exfiltration des coffres chiffrés et des métadonnées sensibles.

Qui: Un groupe de cybercriminels sophistiqués visant des gains financiers, utilisant le hameçonnage et exploitant des vulnérabilités sur le système d'un ingénieur DevOps.

Comment: Les attaquants ont utilisé des courriels de hameçonnage, des logiciels malveillants d'enregistreur de frappe et des vulnérabilités d'exécution de code à distance, en exploitant des logiciels tiers pour maintenir l'accès.



Quoi: Ils ont capturé des mots de passe maîtres, obtenu l'accès aux clés de déchiffrement du stockage infonuagique, exfiltré des coffres chiffrés et des données de sauvegarde sensibles.

Qui: LastPass, son environnement de développement, ses ingénieurs DevOps, et les clients affectés dont les données de coffre et métadonnées ont été compromises.

Aperçu de TrickBot

Une attaque sophistiquée s'est produite, dans laquelle le malware TrickBot a facilité l'installation d'une fausse application 1Password, permettant une infiltration plus profonde et une meilleure évasion des défenses. Dans ce cas, le malware TrickBot a été délivré via un courriel de hameçonnage et déployé sur le système de la victime.

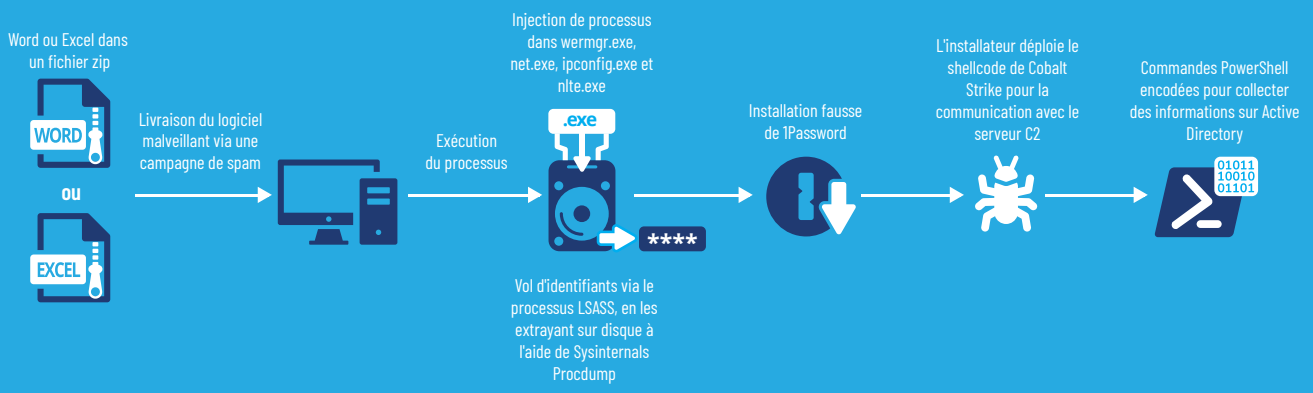
Il a utilisé des outils intégrés de Windows pour effectuer une reconnaissance, voler des identifiants et permettre un accès à distance via Cobalt Strike. Les attaquants ont installé un faux gestionnaire de mots de passe 1Password pour masquer leurs activités, qui servait secrètement à déployer d'autres malwares.

Malgré l'infiltration de plusieurs systèmes, l'opération s'est arrêtée sans exfiltration de données, laissant la raison de cette interruption incertaine.

Qu'est-ce que le malware TrickBot?

TrickBot est un trojan bancaire modulaire apparu en 2016, conçu pour voler des informations financières et des identifiants de connexion. Il se propage via des courriels de hameçonnage ou d'autres malwares et peut se déplacer à travers les réseaux. TrickBot peut également déployer d'autres logiciels malvaillants, comme des rançongiciels, ce qui en fait une menace majeure.

Il communique avec des serveurs de commande et de contrôle pour recevoir des instructions et utilise des techniques d'évasion pour éviter la détection.



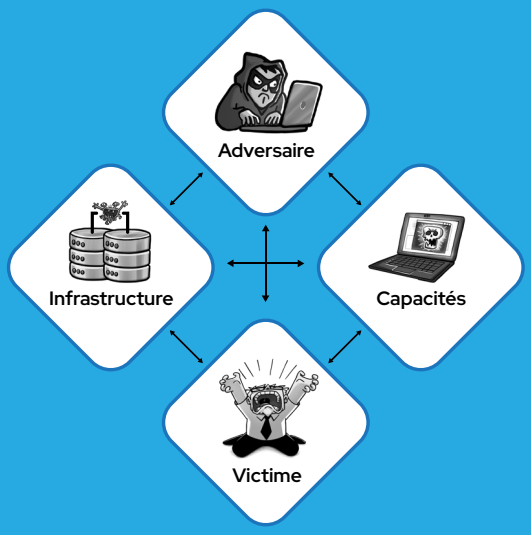
Qui: Probablement un groupe de cybercriminels motivés par des gains financiers ou des acteurs malveillants utilisant TrickBot comme outil pour mener des attaques de hameçonnage, voler des identifiants et déployer d'autres logiciels malveillants, tels que des rançongiciels.

Comment:

Pourriels malvaillants: Utilisé pour diffuser TrickBot via des e-mails de hameçonnage contenant des pièces jointes malveillantes (par ex., fichiers Word/Excel).

Serveurs de commande et contrôle (C2): TrickBot communique avec son infrastructure C2 pour recevoir des instructions, télécharger des modules supplémentaires et exfiltrer les données volées.

Outils: TrickBot exploite des outils système intégrés (par ex., PowerShell, WMIC) et des utilitaires tiers (comme Sysinternals ProcDump) pour effectuer des tâches de reconnaissance, de persistance et d'exfiltration de données.



Quoi:

Vol d'identifiants: TrickBot extrait le processus LSASS et modifie le registre pour dérober des données d'authentification.

Injection de processus: Injecte des charges utiles dans des processus légitimes (par ex., wermgr.exe) pour échapper à la détection.

Reconnaissance: Utilise des outils de découverte réseau comme net.exe et ipconfig.exe pour collecter des informations sur le réseau compromis.

Persistance: Crée des tâches planifiées et déploie un faux installateur 1Password pour maintenir sa présence et masquer d'autres activités malveillantes.

Qui: Les cibles peuvent être à la fois des utilisateurs individuels et des organisations.

Environnement: Vise généralement les systèmes Windows et les organisations avec des environnements en réseau, facilitant ainsi les déplacements latéraux de TrickBot et l'exfiltration des données.

Conclusion

Résumé des découvertes

Les gestionnaires de mots de passe sont des outils essentiels pour la sécurité, mais ils sont de plus en plus ciblés par les cybercriminels. Des voleurs d'informations, tels que Meduza Stealer et Stealc, cherchent à dérober des données sensibles provenant des gestionnaires de mots de passe et d'autres applications.

Les attaquants utilisent des tactiques telles que le hameçonnage, la publicité malveillante et l'ingénierie sociale pour accéder aux identifiants des utilisateurs et à des informations précieuses.

Menaces émergentes:

1. Voleurs d'informations: Des malwares tels que Meduza, Lumma et ACR exploitent des vulnérabilités comme CVE-2024-21412 dans Microsoft Defender SmartScreen pour contourner les contrôles de sécurité, infectant les appareils afin de voler des données provenant de navigateurs, de portefeuilles de crypto-monnaies, d'applications de messagerie et de gestionnaires de mots de passe tels que Bitwarden et 1Password.

2. Publicité malveillante: Cette technique consiste à placer des annonces malveillantes, trompant les utilisateurs pour qu'ils téléchargent de faux gestionnaires de mots de passe ou gestionnaires de bureaux à distance. ZenRat est un exemple notable, distribué via des sites Web clonés et des courriels de hameçonnage pour voler les identifiants des utilisateurs.

Campagnes sophistiquées:

3. Malware ZenRat: Distribué via de faux installateurs de Bitwarden, ZenRat détourne les identifiants des utilisateurs et des données sensibles en exploitant la publicité malveillante sur des plateformes comme Google Ads.

4. Malware FakeBat: Utilise des techniques de téléchargement furtif ("drive-by download") pour exploiter les vulnérabilités des navigateurs et déployer des charges malveillantes supplémentaires.

5. TrickBot: Une attaque sophistiquée impliquant le malware TrickBot, qui a installé une fausse application 1Password pour permettre une infiltration plus profonde et le déploiement de malwares supplémentaires via des outils comme Cobalt Strike.

Recommandations finales

Des logiciels malvaillants comme Citadel, Arkei et Racoon Stealer ciblent de plus en plus les gestionnaires de mots de passe tels que Bitwarden, LastPass et KeePassXC. Bien que ces voleurs d'informations puissent capturer des mots de passe actifs, ils ne récupèrent pas tous les mots de passe stockés en une seule fois. Nous avons observé une augmentation du nombre de voleurs d'informations, comme Meduza Stealer, apparaissant sur les plateformes du dark web, reflétant la tendance croissante de service de logiciel malveillants, qui permettent à des criminels moins expérimentés de lancer des cyberattaques plus facilement.

Pour éviter les trojan de vol de mots de passe, ne vous laissez pas tromper par des techniques d'ingénierie sociale, car la plupart de ces logiciels malveillants sont installés lorsque les utilisateurs exécutent involontairement un programme malveillant. Mettez régulièrement à jour vos logiciels, en particulier ceux figurant dans le catalogue des vulnérabilités exploitées connu de la CISA.

Malgré les menaces visant les gestionnaires de mots de passe, nous recommandons toujours d'en utiliser un pour éviter des risques plus importants, comme la réutilisation de mots de passe ou l'utilisation de mots de passe faibles. Bien qu'ils ne soient pas totalement infaillibles, les gestionnaires de mots de passe réduisent considérablement les risques de compromission en traitant ces vulnérabilités majeures, qui sont bien plus susceptibles d'être exploitées que le gestionnaire de mots de passe lui-même.

MITRE ATT&CK

ZenRat

Tactique	Technique (MITRE ATT&CK)	Description
Accès initial	Publicité malveillante (T1598)	Distribué via des annonces malveillantes et des sites Web clonés
Identifiant d'exécution	Hameçonnage d'identifiants (T1566)	Utilise des e-mails de hameçonnage pour attirer les victimes vers des sites frauduleux.
Défense contre l'accès	Vidage des identifiants (T1003)	Vole les identifiants des utilisateurs, y compris ceux des gestionnaires de mots de passe.
Évasion des défenses	Fichiers ou informations obfusqués (T1027)	Utilise l'obfuscation pour échapper à la détection.
Exfiltration	Exfiltration via un canal C2 (T1041)	Transmet les données volées aux serveurs de commande et de contrôle.

FakeBot

Tactique	Technique (MITRE ATT&CK)	Description
Accès initial	Téléchargement furtif (T1189)	Distribué via des sites Web compromis ou des mises à jour malveillantes de navigateurs.
Exécution	Injection de processus (T1055)	S'injecte dans des processus légitimes pour échapper à la détection.
Persistance	Persistance via des tâches ou travaux planifiés (T1053)	Établit une persistance en créant des tâches planifiées.
Accès aux identifiants	Vidage des identifiants (T1003)	Vole des identifiants en capturant les entrées de diverses applications.
Évasion des défenses	Interpréteur de commandes et de scripts (T1059)	Utilise des scripts malveillants pour l'exécution, tels que PowerShell.

RomCom

Tactique	Technique (MITRE ATT&CK)	Description
Accès initial	Hameçonnage (T1566)	Utilise des courriels de hameçonnage ciblé conduisant au téléchargement de logiciels trojanisés.
Persistance	Typosquattage (T1596.002)	Crée des domaines frauduleux ressemblant à des sites de logiciels légitimes.
Exécution	Logiciels trojanisés (T1072)	Utilise des versions modifiées de logiciels légitimes pour distribuer des logiciels malveillants.
Commande et Contrôle	Commande et Contrôle via un canal chiffré (T1573)	Communique avec des serveurs C2 en utilisant un trafic chiffré.
Exfiltration	Exfiltration via un service Web (T1567)	Transfère les données volées via des canaux sécurisés et chiffrés.

Incident LastPass

Tactique	Technique (MITRE ATT&CK)	Description
Reconnaissance	Collecte d'informations sur l'identité de la victime (T1589)	Les attaquants ont probablement recueilli des informations sur les employés de LastPass disposant d'un accès privilégié.
Accès initial	Hameçonnage (T1566)	Des courriels de hameçonnage ont été envoyés à un ingénieur DevOps senior pour obtenir un accès initial.
Exécution	Exploitation pour l'exécution côté client (T1203)	Un enregistreur de frappe a été installé après le courriel de hameçonnage, exploitant le système.
Persistance	Manipulation de compte (T1098)	Un enregistreur de frappe a été installé pour maintenir la persistance et surveiller l'activité de l'ingénieur.
Élévation de privilèges	Comptes valides (T1078)	Les attaquants ont utilisé les identifiants volés pour accéder à des systèmes privilégiés.
Évasion des défenses	Fichiers ou informations obfusqués (T1027)	Les attaquants ont utilisé des techniques pour échapper à la détection et se fondre dans le trafic réseau légitime.
Accès aux identifiants	Capture des entrées (T1056)	Le mot de passe maître a été capturé au moment de sa saisie lors de l'authentification.
Découverte	Collecte d'informations sur le système (T1082)	Les attaquants ont recueilli des informations sur l'environnement compromis.
Mouvement latéral	Services à distance (T1021)	Des identifiants compromis ont été utilisés pour se déplacer latéralement à travers le réseau.
Exfiltration	Exfiltration via un canal C2 (T1041)	Les coffres chiffrés volés et les métadonnées ont été transférés via des canaux chiffrés.

TrickBot

Tactique	Technique (MITRE ATT&CK)	Description
Accès initial	Hameçonnage (T1566)	Distribué via des courriels de hameçonnage contenant des pièces jointes ou des liens malveillants.
Exécution	Injection de processus (T1055)	Injecte du code malveillant dans des processus légitimes pour échapper à la détection.
Accès aux identifiants	Vidage des identifiants (T1003)	Vole des identifiants en extrayant la mémoire de processus comme LSASS.
Mouvement latéral	Services à distance (T1021)	Utilise des identifiants compromis pour se déplacer latéralement au sein d'un réseau.
Persistance	Tâches ou travaux planifiés (T1053)	Établit une persistance en créant des tâches ou travaux planifiés.
Évasion des défenses	Fichiers ou informations obfusqués (T1027)	Obfusque le code malveillant pour échapper à la détection par les outils de sécurité.

Devolutions

À PROPOS DE DEVOLUTIONS

Basée à Lavaltrie, Québec, Canada, Devolutions propose des solutions de productivité et de sécurité à plus de 800 000 professionnels de l'informatique et utilisateurs finaux d'entreprise dans plus de 140 pays à travers le monde. Veuillez adresser vos demandes et demandes d'essai gratuit via les moyens suivants :

Courriel: sales@devolutions.net

Téléphone: +1 844 463.0419

Chat en direct via notre site Web: https://devolutions.net/fr/