Avis APT40

La tactique du ministère de la Sécurité d'État (Ministry of State Security - MSE) de la République populaire de Chine (RPC) en action

Australian Government

Australian Signals Directorate

National Cyber
Security Centre
a part of GCHQ

Communications
Security Establishment

**Canadian Centre
for Cyber Security**

Centre de la sécurité
des télécommunications

**Centre canadien
pour la cybersécurité**

Table des matières

Aperçu 5

Historique 5

Résumé des activités 5

Tactique notable 6

Outils 7

Études de cas 7

Étude de cas 1 8

Résumé exécutif 8

Conclusions de l'enquête 9

Détails 9

Chronologie visuelle 9

Chronologie détaillée 10

Tactiques et techniques des acteurs 11

Reconnaissance 11

Accès initial 11

Exécution 11

Accès aux identifiants 11

Mouvement latéral 11

Collecte 11

Exfiltration 11

Étude de cas 2 12

Résumé exécutif 12

Conclusions de l'enquête 13

Résumé de l'enquête 13

Hôtes internes 13

Chronologie de l'enquête 14

Tactiques et techniques des acteurs 15

Accès initial 15

Exécution 15

Persistance 15

Élévation des privilèges 15

Accès aux identifiants 15

Découverte 16

Collecte 16

Commande et contrôle 16

Recommandations en matière de détection et d'atténuation 17

Détection 17

Atténuations 20

MITRE ATT&CK – Historique des tactiques d'intérêt APT40 22

Présentation

Historique

Cet avis, rédigé par le Centre australien de cybersécurité de la Direction des signaux australiens (l'ACSC de l'ASD), l'Agence américaine pour la cybersécurité et la sécurité des infrastructures (CISA), l'Agence de sécurité nationale des États-Unis (NSA), le Federal Bureau of Investigation (FBI) des États-Unis, le Centre national de cybersécurité du Royaume-Uni (NCSC-UK), le Centre canadien pour la cybersécurité (CCCS), le Centre national de cybersécurité de Nouvelle-Zélande (NCSC-NZ), le Service fédéral de renseignement allemand (BND) et l'Office fédéral de la protection de la Constitution (BfV), le Service national de renseignement de la République de Corée (NIS) et le Centre national de cybersécurité du NIS, ainsi que le Centre national de préparation aux incidents et de stratégie pour la cybersécurité (NISC) et l'Agence nationale de police (NPA) du Japon – ci-après dénommés les « agences rédactrices » – décrit un groupe cybernétique soutenu par l'État de la République populaire de Chine (RPC) et sa menace actuelle envers les réseaux australiens. Cet avis s'appuie sur la compréhension commune de la menace par les agences rédactrices, ainsi que sur les enquêtes de l'ASD sur les incidents liés à l'ACSC.

Le groupe cybernétique soutenu par l'État chinois a déjà ciblé des organisations dans divers pays, dont l'Australie et les États-Unis, et les techniques décrites ci-dessous sont régulièrement utilisées par d'autres acteurs soutenus par l'État chinois à travers le monde. Par conséquent, les agences rédactrices estiment que ce groupe, et des techniques similaires, demeurent une menace également pour les réseaux de leurs pays.

Les agences rédactrices pensent que ce groupe mène des cyberopérations malveillantes pour le compte du ministère de la Sécurité d'État (MSE) de la République populaire de Chine (RPC). L'activité et les techniques utilisées recoupent celles des groupes identifiés comme Menace persistante avancée (Advanced Persistent Threat, APT) 40 (également connus sous les noms de Kryptonite Panda, GINGHAM TYPHOON, Leviathan et Bronze Mohawk dans les rapports sectoriels). Ce groupe a déjà été signalé comme étant basé à Haikou, dans la province de Hainan, en République populaire de Chine (RPC), et recevant des missions du MSE de la RPC, le ministère de la Sécurité d'État de Hainan. [2]
L'avis suivant fournit un échantillon d'études de cas significatives des techniques de cet adversaire en action contre deux réseaux victimes. Ces études de cas sont essentielles pour permettre aux professionnels de la cybersécurité d'identifier, de prévenir les intrusions d'APT40 sur leurs propres réseaux, et d'y remédier. Les études de cas sélectionnées sont celles pour lesquelles des mesures correctives appropriées ont été prises afin de réduire le risque de ré-exploitation par cet acteur malveillant ou d'autres. De ce fait, ces études de cas sont naturellement plus anciennes, afin de garantir que les organisations ont disposé du temps nécessaire pour remédier à la situation.

Résumé de l'activité

APT40 a ciblé à plusieurs reprises des réseaux australiens, ainsi que des réseaux gouvernementaux et privés de la région, et la menace qu'il représente pour nos réseaux est continue. Les techniques décrites dans cet avis sont régulièrement observées contre les réseaux australiens.

APT40 possède notamment la capacité de transformer et d'adapter rapidement les preuves de concept (proof-of-concept, POC) d'exploitation de nouvelles vulnérabilités et de les utiliser immédiatement contre les réseaux cibles possédant l'infrastructure de la vulnérabilité associée. APT40 effectue régulièrement des reconnaissances sur les réseaux d'intérêt, y compris ceux des pays des agences rédactrices, à la recherche d'opportunités de compromettre ses cibles. Ces reconnaissances régulières permettent au groupe d'identifier les appareils vulnérables, en fin de vie ou non maintenus sur les réseaux d'intérêt, et de déployer rapidement des exploits.
APT40 continue à exploiter des vulnérabilités avec succès depuis 2017.

APT40 exploite rapidement les vulnérabilités récemment rendues publiques dans des logiciels largement utilisés tels que Log4J (CVE 2021 44228), Atlassian Confluence (CVE-2021-31207, CVE-2021-26084) et Microsoft Exchange (CVE-2021-31207 ; CVE-2021-34523 ; CVE-2021-34473. L'ACSC de l'ASD et les agences rédactrices s'attendent à ce que le groupe continue d'utiliser des POC pour de nouvelles vulnérabilités de grande envergure dans les heures ou les jours suivant leur publication publique.

2 Département de la Justice des États-Unis. 2021. Quatre ressortissants chinois travaillant pour le ministère de la Sécurité d'État accusés d'une campagne mondiale d'intrusion informatique ciblant la propriété intellectuelle et des informations commerciales confidentielles, notamment des recherches sur les maladies infectieuses.

Figure 1. Organigramme TTP pour l'activité APT40

Ce groupe semble privilégier l'exploitation d'infrastructures vulnérables et accessibles au public plutôt que les techniques nécessitant une interaction avec l'utilisateur, telles que les campagnes d'hameçonnage, et accorde une grande importance à l'obtention d'identifiants valides pour permettre diverses activités de suivi. APT40 utilise régulièrement des shells Web (T1505.003) pour la persistance, en particulier au début du cycle de vie d'une intrusion. En général, après un accès initial réussi, APT40 se concentre sur l'établissement de la persistance pour maintenir l'accès à l'environnement de la victime. Cependant, comme la persistance intervient tôt dans une intrusion, elle est plus susceptible d'être observée dans toutes les intrusions, quelle que soit l'ampleur de la compromission ou des actions ultérieures entreprises.

Tactique notable

Bien qu'APT40 ait déjà utilisé des sites Web australiens compromis comme hôtes de commande et de contrôle (C2) pour ses opérations, le groupe a fait évoluer cette technique (T1594).

APT40 a adopté la tendance mondiale consistant à utiliser des appareils compromis, notamment des appareils destinés aux petites entreprises et aux bureaux à domicile (small-office/home-office, SOHO), comme infrastructure opérationnelle et redirecteurs « de dernier saut » (T1584.008) pour ses opérations en Australie. Cela a permis aux agences rédactrices de mieux caractériser et suivre les mouvements de ce groupe.

Nombre de ces appareils SOHO sont en fin de vie ou non corrigés et constituent une cible facile pour une exploitation de type N-Day. Une fois compromis, les appareils SOHO constituent un point de départ pour des attaques conçues pour se fondre dans le trafic légitime et défier les défenseurs de réseau (T1001.003).

Cette technique est également régulièrement utilisée par d'autres acteurs soutenus par l'État chinois dans le monde, et les agences rédactrices la considèrent comme une menace partagée. Pour plus d'informations, consultez les avis conjoints Des acteurs cybernétiques soutenus par l'État de la République populaire de Chine exploitent des fournisseurs de réseau et des appareils et Des acteurs soutenus par l'État de la République populaire de Chine (RPC) compromettent des infrastructures critiques américaines et maintiennent un accès persistant à ces infrastructures.

APT40 utilise occasionnellement des infrastructures acquises ou louées comme infrastructures C2 pour ses victimes dans le cadre de ses opérations ; cependant, cette pratique semble être en déclin relatif.

Outils

L'ACSC de l'ASD partage certains des fichiers malveillants identifiés lors des enquêtes décrites ci-dessous. Ces fichiers ont été téléchargés sur VirusTotal afin de permettre aux communautés plus larges de défense des réseaux et de cybersécurité de mieux comprendre les menaces contre lesquelles elles doivent se prémunir.

Études de cas

L'ACSC de l'ASD communique deux rapports d'enquête anonymisés afin de mieux faire comprendre comment les acteurs utilisent leurs outils et leur savoir-faire.

MD5	Nom du fichier	Informations supplémentaires
26a5a7e71a601be991073c78d513dee3	horizon.jsp	1 Ko | Source Java
87c88f06a7464db2534bc78ec2b915de	Index_jsp$ProxyEndpoint$Attach.class	597 O | Bytecode Java
6a9bc68c9bc5cefaf1880ae6ffb1d0ca	Index_jsp.class	5 Ko | Bytecode Java
64454645a9a21510226ab29e01e76d39	Index_jsp.java	5 Ko | Source Java
e2175f91ce3da2e8d46b0639e941e13f	Index_jsp$ProxyEndpoint.class	4 Ko | Bytecode Java
9f89f069466b8b5c9bf25c9374a4daf8	Index_jsp$ProxyEndpoint$1.class	3 Ko | Bytecode Java
187d6f2ed2c80f805461d9119a5878ac	Index_jsp$ProxyEndpoint$2.class	1 Ko | Bytecode Java
ed7178cec90ed21644e669378b3a97ec	Nova_jsp.class	7 Ko | Bytecode Java
5bf7560d0a638e34035f85cd3788e258	Nova_jsp$TomcatListenerMemShellFromThread.class	7 Ko | Bytecode Java
e02be0dc614523ddd7a28c9e9d500cff	Nova_jsp.java	15 Ko | Source Java

Étude de cas 1

Ce rapport a été anonymisé afin de permettre une diffusion plus large. L'organisation affectée est ci-après dénommée « l'organisation ». Certains détails spécifiques ont été supprimés afin de protéger l'identité de la victime et les méthodes de réponse aux incidents de l'ACSC de l'ASD.

Résumé exécutif

Ce rapport détaille les conclusions de l'enquête ACSC de l'ASD sur la compromission réussie du réseau de l'organisation entre juillet et septembre 2022. Ce rapport d'enquête a été fourni à l'organisation afin de résumer les activités malveillantes observées et de formuler des recommandations de correction. Les conclusions indiquent que la compromission a été entreprise par APT40.

Mi-août, l'ACSC de l'ASD a informé l'organisation d'interactions malveillantes avec son réseau provenant d'un appareil probablement compromis utilisé par le groupe fin août et, avec le consentement de l'organisation, l'ACSC de l'ASD a déployé des capteurs sur les hôtes du réseau de l'organisation vraisemblablement affectés. Ces capteurs ont permis aux analystes de la réponse aux incidents de l'ACSC de l'ASD de mener une enquête numérique approfondie. À l'aide des données de capteurs disponibles, les analystes de l'ACSC de l'ASD ont réussi à cartographier l'activité du groupe et à créer une chronologie détaillée des événements observés.

De juillet à août, parmi les principales activités des acteurs observées par l'ACSC de l'ASD, on peut citer :

- l'énumération des hôtes, qui permet à un acteur de construire sa propre cartographie du réseau ;
- l'utilisation d'un Web shell, offrant à l'acteur un premier point d'entrée sur le réseau et la capacité d'exécuter des commandes ; et
- le déploiement d'autres outils utilisés par l'acteur à des fins malveillantes.

L'enquête a révélé des preuves d'accès à de grandes quantités de données sensibles et des déplacements latéraux des acteurs sur le réseau (T1021.002). Une grande partie de la compromission a été facilitée par la mise en place par le groupe de multiples vecteurs d'accès au réseau, la structure horizontale du réseau et l'utilisation de logiciels non sécurisés développés en interne permettant de télécharger arbitrairement des fichiers. Les données exfiltrées comprenaient des identifiants d'authentification privilégiés permettant au groupe de se connecter, ainsi que des informations réseau permettant aux acteurs de récupérer un accès non autorisé si le vecteur d'accès initial était bloqué. Aucun autre outil malveillant n'a été découvert en dehors de ceux présents sur la machine exploitée initialement ; cependant, l'accès d'un groupe à des identifiants légitimes et privilégiés rendrait superflu tout outil supplémentaire. Les conclusions de l'enquête indiquent que l'organisation a probablement été délibérément ciblée par APT40, et non la victime opportune d'une vulnérabilité connue du public.

Conclusions de l'enquête

Mi-août 2022, l'ACSC de l'ASD a informé l'organisation qu'une adresse IP malveillante confirmée, présumée être affiliée à un cybergroupe soutenu par un État, avait interagi avec les réseaux informatiques de l'organisation entre juillet et août au moins. L'appareil compromis appartenait probablement à une petite entreprise ou à un particulier.

Vers la fin août, l'ACSC de l'ASD a déployé un agent basé sur l'hôte sur les hôtes du réseau de l'organisation, qui ont montré des signes d'impact de la compromission.

Certains éléments qui auraient pu étayé les efforts d'enquête n'étaient pas disponibles en raison de la configuration de la journalisation ou de la conception du réseau. Malgré cela, la volonté de l'organisation de fournir toutes les données disponibles a permis aux équipes d'intervention de l'ACSC de l'ASD de mener une analyse complète et de comprendre l'activité probable d'APT40 sur le réseau.

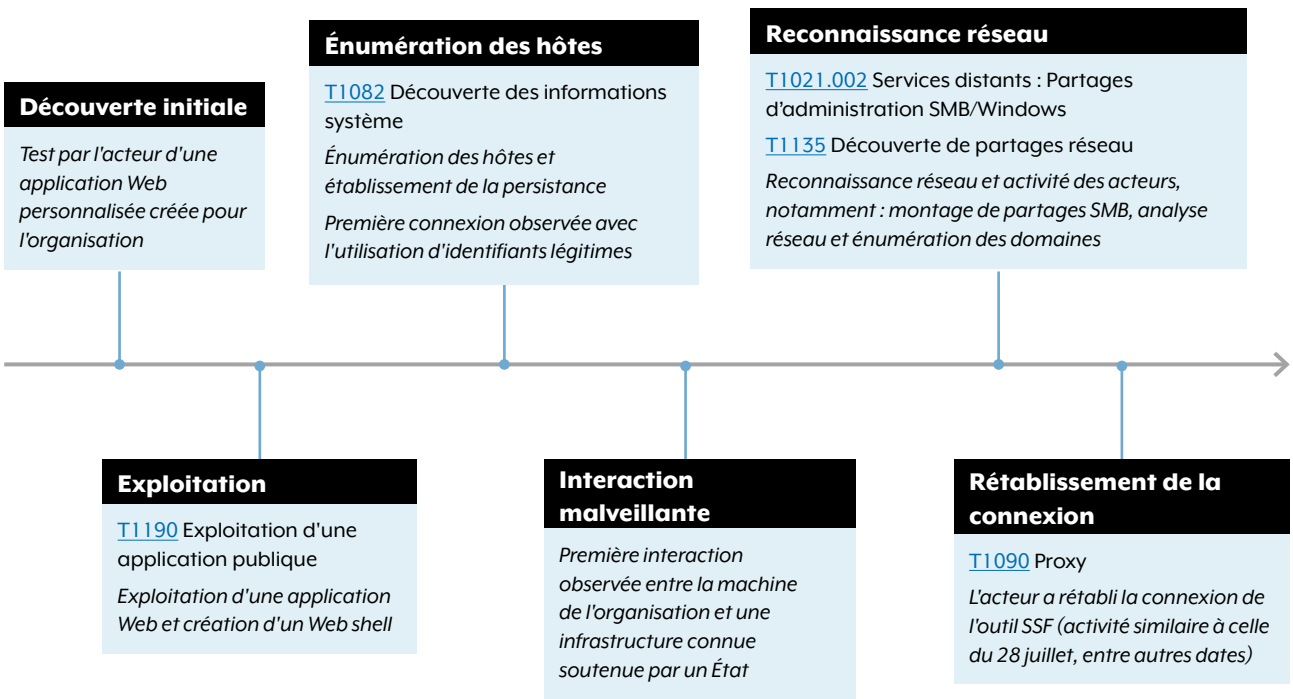
En septembre, après consultation de l'ACSC de l'ASD, l'organisation a décidé de bloquer l'adresse IP identifiée dans la notification initiale. En octobre, l'organisation a commencé la remédiation.

Détails

Dès juillet, des acteurs ont pu tester et exploiter une application Web personnalisée (T1190) exécutée sur `<webapp>2-ext`, permettant au groupe de s'implanter dans la zone démilitarisée (DMZ) du réseau. Cette application a permis d'énumérer le réseau et tous les domaines visibles. Des identifiants compromis (T1078.002) ont été utilisés pour interroger Active Directory (T1018) et exfiltrer des données en montant des partages de fichiers (T1039) depuis plusieurs machines de la DMZ. L'acteur a mené une attaque Kerberoasting afin d'obtenir des identifiants réseau valides auprès d'un serveur (T1558.003). Selon les observations, le groupe n'a pas acquis de points de présence supplémentaires, ni dans la DMZ ni sur le réseau interne.

Chronologie visuelle

La chronologie ci-dessous offre un aperçu général des principales phases de l'activité des acteurs malveillants observées sur le réseau de l'organisation.



Chronologie détaillée

Juillet : Les acteurs ont établi une connexion initiale à la page d'accueil d'une application Web personnalisée (T1190) créée pour l'organisation (ci-après dénommée « application Web » ou « *webapp* ») via une connexion TLS (Transport Layer Security) (T1102). Aucune autre activité notable n'a été observée.

Juillet : Les acteurs commencent à énumérer le site Web de l'application à la recherche de terminaisons [2] pour approfondir leurs recherches.

Juillet : Les acteurs se concentrent sur les tentatives d'exploitation d'une terminaison spécifique.

Juillet : Les acteurs parviennent à envoyer un `POST` au serveur Web, probablement via un Web shell placé sur une autre page. Une deuxième adresse IP, probablement utilisée par les mêmes acteurs, commence également à publier sur la même URL. Les acteurs ont créé et testé plusieurs Web shells probables.

La méthode d'exploitation exacte est inconnue, mais il est clair que la terminaison spécifique était ciblée pour créer des fichiers sur `<webapp>2-ext`.

L'ACSC de l'ASD estime que les deux connexions d'adresses IP faisaient partie de la même intrusion, en raison de leur intérêt commun et de connexions initiales survenues à quelques minutes d'intervalle.

Juillet : Le groupe continue d'effectuer l'énumération des hôtes, à la recherche d'opportunités d'élévation de privilèges et en déployant un autre Web shell. Les acteurs se connectent à l'application Web en utilisant les identifiants compromis pour `<prénom.nom>@<domaine de l'organisation>`.

L'activité des acteurs ne semble pas avoir permis l'élévation de privilèges sur `<webapp>2-ext`. Les acteurs se sont alors tournés vers une activité réseau.

Juillet : L'acteur teste les identifiants compromis pour un compte de service[3], probablement codés en dur dans des binaires accessibles en interne.

Juillet : Les acteurs déploient l'outil open source Secure Socket Funnelling, utilisé pour se connecter à l'infrastructure malveillante. Cette connexion permet de canaliser le trafic des machines d'attaque des acteurs vers les réseaux internes de l'organisation, dont les noms sont exposés dans les journaux d'événements lorsqu'ils tentent d'utiliser les identifiants du compte de service.

Août : D'après les observations, les acteurs mènent une activité limitée, notamment en ne parvenant pas à établir de connexions impliquant le compte de service.

Août : Les acteurs effectuent une énumération importante du réseau et d'Active Directory. Un autre compte compromis est ensuite utilisé pour monter des partages[4] sur des machines Windows dans la DMZ, permettant ainsi une exfiltration de données réussie.

Il semble s'agir d'une utilisation opportuniste d'identifiants volés sur des machines montables dans la DMZ. Les pare-feu ont empêché l'acteur de cibler le réseau interne avec une activité similaire.

Août – septembre : L'outil SSF a rétabli une connexion à une adresse IP malveillante. Aucune autre activité du groupe n'est observée jusqu'à ce que son accès soit bloqué.

Septembre : L'organisation bloque l'adresse IP malveillante en la mettant sur la liste noire de ses pare-feu.

2 Dans ce contexte, une terminaison est une fonction de l'application Web.

3 Les comptes de service ne sont pas liés à des utilisateurs individuels, mais à des services. Dans un domaine d'entreprise Microsoft, il y a différents types de comptes.

4 Le montage de partages consiste à rendre les fichiers d'un système de fichiers accessibles à un utilisateur ou à un groupe d'utilisateurs.

Tactiques et techniques des acteurs

Le cadre MITRE ATT&CK est un recueil documenté de tactiques et de techniques employées par les acteurs malveillants dans le cyberespace. Ce cadre a été créé par l'organisation américaine à but non lucratif MITRE Corporation et fonctionne comme un langage commun mondial pour le comportement des acteurs malveillants.

L'ACSC de l'ASD évalue que les techniques et tactiques suivantes correspondent à l'activité malveillante de l'acteur :

Reconnaissance

T1594 – Recherche de sites Web appartenant à la victime

L'auteur a répertorié le site de l'application Web personnalisée afin d'identifier les possibilités d'accès au réseau.

Accès initial

T1190 – Exploitation d'une application publique (exploitation de l'application Web personnalisée)

T1078.002 – Comptes valides : Comptes de domaine (connexion avec des identifiants compromis)

L'exploitation d'applications Web personnalisées exposées à Internet a fourni un premier point d'accès à l'acteur. L'acteur a ensuite pu utiliser les identifiants compromis pour accéder au réseau.

Exécution

T1059 – Interpréteur de commandes et de scripts (exécution de commandes via le Web shell)

T1072 – Outils de déploiement logiciel (acteur utilisant l'outil open source Secure Socket Funneling (SSF) pour se connecter à une adresse IP)

Persistance

T1505.003 – Composant logiciel serveur : Web Shell (utilisation d'un Web Shell et de SSF pour établir l'accès)

Accès aux identifiants

T1552.001 – Identifiants provenant de bases de données de mots de passe (fichiers de mots de passe relatifs au système de gestion technique de bâtiment (GTB))

T1558.003 – Vol ou falsification de tickets Kerberos : Kerberoasting (attaque visant à obtenir des identifiants réseau)

Déplacement latéral

T1021.002 – Services distants : Partages SMB (montage de partages SMB par l'utilisateur depuis plusieurs appareils)

Collecte

T1213 – Données provenant de référentiels d'informations (manuels/documentation trouvés sur le serveur BMS)

Exfiltration

T1041 – Exfiltration via le canal C2 (exfiltration de données de l'acteur depuis Active Directory et le montage de partages)

Étude de cas 2

Ce rapport a été anonymisé pour permettre une diffusion plus large. L'organisation affectée est ci-après dénommée « l'organisation ». Certains détails spécifiques ont été supprimés afin de protéger l'identité de la victime et les méthodes de réponse aux incidents de l'ACSC de l'ASD.

Résumé exécutif

Ce rapport détaille les conclusions de l'enquête de l'ACSC de l'ASD sur la compromission réussie du réseau de l'organisation en avril 2022. Ce rapport d'enquête a été fourni à l'organisation afin de résumer les activités malveillantes observées et de formuler des recommandations de correction. Les conclusions indiquent que la compromission a été entreprise par APT40.

En mai 2022, l'ACSC de l'ASD a signalé à une organisation une activité malveillante suspectée affectant son réseau depuis avril 2022. Par la suite, l'organisation a informé l'ACSC de l'ASD de la découverte d'un logiciel malveillant sur un serveur connecté à Internet servant de portail de connexion à sa solution d'accès à distance. Ce serveur utilisait un produit de gestion des identifiants et des connexions à distance. Il sera désigné dans le présent rapport comme « l'appareil compromis ». Ce rapport détaille les conclusions de l'enquête et les recommandations de correction élaborées pour l'organisation suite à l'enquête menée par l'ACSC de l'ASD.

Des éléments de preuve indiquaient qu'une partie du réseau de l'organisation avait été compromise par un ou plusieurs cybercriminels via le portail d'accès à distance de l'organisation depuis au moins avril 2022. Ce serveur a pu être compromis par plusieurs acteurs et était probablement affecté par une vulnérabilité d'exécution de code à distance (RCE) largement médiatisée au moment de la compromission.

Parmi les principales activités des acteurs observées par l'ACSC de l'ASD, on peut citer :

- l'énumération des hôtes, qui permet à un acteur de construire sa propre carte du réseau ;
- l'exploitation d'applications connectées à Internet et l'utilisation de Web shells, donnant à l'acteur un premier point d'entrée sur le réseau et la capacité d'exécuter des commandes ;
- l'exploitation de vulnérabilités logicielles pour élever ses privilèges ; et
- la collecte d'identifiants pour permettre un déplacement latéral.

L'ACSC de l'ASD a découvert qu'un acteur malveillant avait exfiltré plusieurs centaines de paires nom d'utilisateur/mot de passe uniques sur l'appareil compromis en avril 2022, ainsi qu'un certain nombre de codes d'authentification multifacteur et d'artefacts techniques liés aux sessions d'accès à distance. Après examen par l'organisation, les mots de passe se sont avérés légitimes. L'ACSC de l'ASD estime que l'acteur a pu collecter ces artefacts techniques pour détourner ou créer une session de connexion à distance en tant qu'utilisateur légitime, et accéder au réseau interne de l'organisation via un compte d'utilisateur légitime.

Résultats de l'enquête

Résumé de l'enquête

L'ACSC de l'ASD a déterminé que l'auteur de l'attaque avait compromis des appareils fournissant des sessions de connexion à distance au personnel de l'organisation et utilisé cette compromission pour tenter de mener d'autres activités. Ces appareils se composent de trois hôtes à équilibrage de charge sur lesquels les premiers signes de compromission ont été détectés. L'organisation a arrêté deux des trois hôtes à équilibrage de charge peu après la compromission initiale. Par conséquent, toutes les activités ultérieures se sont déroulées sur un seul hôte. Les autres serveurs associés à l'appareil compromis étaient également dotés d'un équilibrage de charge similaire. Par souci de lisibilité, tous les appareils compromis sont désignés dans la majeure partie de ce rapport par le terme « appareil unique ».

L'acteur aurait exploité des vulnérabilités connues du public pour déployer des Web shells sur l'appareil compromis à partir d'avril 2022. On estime que les acteurs malveillants du groupe ont obtenu des privilèges élevés sur l'appareil. L'ACSC de l'ASD n'a pas pu déterminer l'étendue complète de l'activité en raison du manque de disponibilité des journaux. Cependant, les preuves présentes sur l'appareil indiquent qu'un acteur a réalisé les opérations suivantes :

- la collecte de plusieurs centaines de paires nom d'utilisateur/mot de passe authentiques ; et
- la collecte d'artefacts techniques qui auraient pu permettre à un acteur malveillant d'accéder à une session d'infrastructure de bureau virtuel (VDI) en tant qu'utilisateur légitime.

L'ACSC de l'ASD estime que l'acteur aurait cherché à développer la compromission du réseau de l'organisation. Les artefacts exfiltrés par l'acteur lui ont peut-être permis de détourner ou d'initier des sessions de bureau virtuel en tant qu'utilisateur légitime, un utilisateur qu'il aurait choisi, y compris en tant qu'administrateur. L'acteur a peut-être utilisé ce vecteur d'accès pour compromettre encore davantage les services de l'organisation afin d'atteindre des objectifs de persistance et autres.

Les autres appareils de l'organisation au sein de l'environnement géré par l'hébergeur n'ont montré aucune preuve de compromission.

Accès

L'hôte hébergeant l'appareil compromis assurait l'authentification via Active Directory et un serveur Web pour les utilisateurs se connectant aux sessions VDI (T1021.001).

Emplacement	Noms d'hôtes des appareils compromis (à équilibrage de charge)
Centre de données 1	HÔTE1, HÔTE2, HÔTE3 (HOST1, HOST2, HOST3)

L'infrastructure de l'appareil comprenait également des hôtes de passerelle d'accès qui fournissent un tunnel vers l'infrastructure VDI à l'utilisateur, une fois qu'il possède un jeton d'authentification généré et téléchargé depuis l'appareil.

Il n'y a eu aucune preuve de compromission de ces hôtes. Cependant, les journaux des hôtes de passerelle d'accès ont montré des interactions significatives avec des adresses IP malveillantes connues. Il est probable que cela reflète une activité survenue sur cet hôte, ou des connexions réseau avec l'infrastructure d'un acteur malveillant ayant atteint cet hôte. La nature de cette activité n'a pas pu être déterminée à l'aide des preuves disponibles, mais indique que le groupe a cherché à se déplacer latéralement dans le réseau de l'organisation (TA0008).

Hôtes internes

L'ACSC de l'ASD a examiné des données limitées provenant du segment réseau interne de l'organisation. Les activités malveillantes tentées ou réussies connues pour avoir affecté le segment de réseau interne de l'organisation comprennent l'accès des acteurs aux artefacts liés au VDI, l'extraction d'un serveur SQL interne (T1505.001) et le trafic inexpliqué observé provenant d'adresses IP malveillantes connues via les dispositifs de passerelle d'accès (TA0011).

Grâce à son accès à l'appareil compromis, le groupe a collecté d'authentiques noms d'utilisateur, mots de passe (T1003) et valeurs de jetons MFA (T1111). Le groupe a également collecté des jetons Web JSON (JWT) (T1528), un artefact d'authentification utilisé pour créer des sessions de connexion à des postes de travail virtuels. L'acteur a peut-être pu les utiliser pour créer ou détourner des sessions de postes de travail

virtuels (T1563.002) et accéder au segment de réseau interne de l'organisation en tant qu'utilisateur légitime (T1078).

L'acteur a également utilisé l'accès à l'appareil compromis pour extraire un serveur SQL (T1505.001) résidant sur le réseau interne de l'organisation. Il est probable que l'acteur a eu accès à ces données.

Les preuves disponibles auprès de la passerelle d'accès ont révélé que le trafic réseau transitait par cet appareil ou vers celui-ci à partir d'adresses IP malveillantes connues. Comme décrit ci-dessus, cela pourrait indiquer que des cybercriminels ont affecté ou utilisé cet appareil, potentiellement pour s'infiltrer dans le réseau interne.

Chronologie de l'enquête

La liste ci-dessous présente une chronologie des principales activités découvertes lors de l'enquête.

Heure	Événement
Avril 2022	Des adresses IP malveillantes connues interagissent avec l'hôte de la passerelle d'accès HOST7. La nature des interactions n'a pas pu être déterminée.
Avril 2022	Tous les hôtes, HOST1, HOST2 et HOST3, ont été compromis par un ou plusieurs acteurs malveillants, et des Web shells ont été placés sur ces hôtes. Un fichier journal a été créé ou modifié sur HOST2. Ce fichier contient des informations d'identification probablement récupérées par un acteur malveillant. Les fichiers /etc/security/opasswd et /etc/shadow ont été modifiés sur HOST1 et HOST3, indiquant que les mots de passe ont été modifiés. Les preuves disponibles sur HOST1 suggèrent que le mot de passe de l'utilisateur « sshuser » a été modifié.
Avril 2022	HOST2 a été fermé par l'organisation. Des Web shells supplémentaires (T1505.003) ont été créés sur HOST1 et HOST3. HOST1 a subi des tentatives d'attaque SSH par force brute depuis HOST3. Un fichier journal a été modifié (T1070) sur HOST3. Ce fichier contient des informations d'identification (T1078) probablement capturées par un acteur malveillant. Les JWT ont été capturés (T1528) et exportés vers un fichier sur HOST3. HOST3 a été fermé par l'organisation. Toute activité ultérieure se déroule sur HOST1.
Avril 2022	Des Web shells supplémentaires ont été créés sur HOST1 (T1505.003). Les JWT ont été récupérés et exportés vers un fichier sur HOST1.
Avril 2022	Des Web shells supplémentaires sont créés sur HOST1 (T1505.003), et une adresse IP malveillante connue interagit avec l'hôte (TA0011). Une adresse IP malveillante connue interagit avec l'hôte de passerelle d'accès HOST7.
Mai 2022	Une adresse IP malveillante connue a interagi avec l'hôte de passerelle d'accès HOST7 (TA0011). Un événement d'authentification d'un utilisateur est lié à une adresse IP malveillante connue dans les journaux sur HOST1. Un Web shell supplémentaire est créé sur cet hôte (T1505.003).
Mai 2022	Un script sur HOST1 a été modifié par un acteur (T1543). Ce script contient une fonctionnalité qui aurait extrait des données d'un serveur SQL interne.
Mai 2022	Un fichier journal supplémentaire a été modifié pour la dernière fois sur HOST1 (T1070). Ce fichier contient les paires nom d'utilisateur et mot de passe du réseau de l'organisation, supposés légitimes (T1078).
Mai 2022	Un fichier journal supplémentaire a été modifié pour la dernière fois (T1070). Ce fichier contient les JWT collectés sur HOST1.
Mai 2022	Des Web shells supplémentaires ont été créés sur HOST1 (T1505.003). À cette date, l'organisation a signalé la découverte d'un Web shell datant d'avril 2022 à l'ACSC de l'ASD.
Mai 2022	Plusieurs scripts ont été créés sur HOST1, dont un nommé Log4jHotPatch.jar.
Mai 2022	La commande iptables-save a été utilisée pour ajouter deux ports ouverts à l'hôte de la passerelle d'accès. Les ports étaient 9998 et 9999 (T1572).

Tactiques et techniques des acteurs

Vous trouverez ci-dessous plusieurs tactiques et techniques identifiées au cours de l'enquête

Accès initial

T1190 Exploitation d'une application publique

Le groupe a probablement exploité des vulnérabilités d'exécution de code à distance (RCE), d'élévation de privilèges et de contournement d'authentification dans le produit de gestion des identités et des connexions à distance pour obtenir un accès initial au réseau.

Cette méthode d'accès initiale est considérée comme la plus probable pour les raisons suivantes :

- Le serveur était alors vulnérable à ces CVE à ce moment ;
- Les tentatives d'exploitation de ces vulnérabilités provenaient d'une infrastructure d'acteurs connus ; et
- La première activité malveillante interne connue s'est produite peu après les tentatives d'exploitation.

Exécution

T1059.004 Interpréteur de commandes et de scripts : Shell Unix

Le groupe a exploité avec succès les vulnérabilités ci-dessus et a peut-être pu exécuter des commandes dans un shell Unix disponible sur l'appareil affecté. Les détails complets des commandes exécutées par les acteurs ne peuvent être fournis, car elles n'ont pas été enregistrées par l'appareil.

Persistance

T1505.003 Composant du logiciel serveur : Web shell

Les acteurs ont déployé plusieurs Web shells sur l'appareil affecté. Il est possible que plusieurs acteurs distincts aient déployé des Web shells, mais que seul un nombre restreint d'acteurs aient utilisé ces shells. Les Web shells auraient permis à l'acteur d'exécuter des commandes arbitraires sur les appareils compromis.

Élévation de privilèges

T1068 Exploitation pour élévation de privilèges

Les données disponibles ne décrivent pas le niveau de privilèges atteint par les acteurs. Cependant, en utilisant des Web shells, les acteurs auraient obtenu un niveau de privilèges comparable à celui du serveur Web de l'appareil compromis. Les vulnérabilités supposées présentes sur l'appareil compromis auraient permis aux acteurs d'obtenir les privilèges root.

Accès aux identifiants

T1056.003 Capture d'entrée : Capture du portail Web

Les preuves sur l'appareil compromis ont montré que l'acteur avait récupéré plusieurs centaines de paires, noms d'utilisateur/mot de passe, en texte clair, supposées légitimes. Il est probable que ces captures ont été réalisées grâce à une modification du processus d'authentification authentique, qui a généré les identifiants dans un fichier.

T1111 Interception d'authentification multifacteur

L'acteur a également récupéré la valeur des jetons MFA correspondant à des connexions légitimes. Ces valeurs ont probablement été récupérées en modifiant le processus d'authentification authentique pour générer ces valeurs dans un fichier. Il n'existe aucune preuve de compromission du « serveur secret » qui stocke les valeurs uniques assurant la sécurité des jetons MFA.

T1040 Reniflage de réseau

L'acteur aurait récupéré des JWT en récupérant le trafic HTTP sur l'appareil compromis. Il existe des preuves que l'utilitaire tcpdump a été exécuté sur l'appareil compromis, ce qui pourrait expliquer la capture de ces JWT par l'acteur.

T1539 Vol de cookie de session Web

Comme décrit ci-dessus, l'acteur a capturé des JWT, analogues à des cookies de session Web. Il aurait pu les réutiliser pour établir un accès ultérieur.

Découverte

T1046 Découverte de services réseau

Il existe des preuves que l'utilitaire d'analyse réseau nmap a été exécuté sur l'appareil compromis afin d'analyser d'autres appareils du même segment de réseau. L'acteur l'a probablement utilisé pour découvrir d'autres services réseau accessibles, susceptibles de présenter des opportunités de déplacement latéral.

Collecte

Les preuves disponibles ne révèlent pas comment les acteurs ont collecté les données, ni précisément ce qui a été collecté depuis l'appareil compromis ou d'autres systèmes. Cependant, il est probable que les acteurs ont eu accès à tous les fichiers de l'appareil compromis, y compris les identifiants capturés (T1003), les valeurs des jetons MFA (T1111) et les JWT décrits ci-dessus.

Commande et contrôle

T1071.001 Protocole de couche application : Protocoles Web

Les acteurs utilisaient des Web shells pour la commande et le contrôle. Les commandes Web shell étaient transmises via HTTPS via le serveur web existant sur l'appareil (T1572).

T1001.003 Obfuscation des données : Usurpation de protocole

Les acteurs utilisaient des appareils compromis comme point de départ pour des attaques conçues pour se fondre dans le trafic légitime.

Recommandations de détection et d'atténuation

L'ACSC de l'ASD recommande vivement la mise en œuvre des Huit contrôles essentiels de l'ASD et des stratégies associées pour atténuer les incidents de cybersécurité. Vous trouverez ci-dessous des recommandations sur les mesures de sécurité réseau à prendre pour détecter et prévenir les intrusions d'APT40, suivies de mesures d'atténuation spécifiques pour quatre TTP clés résumées dans le tableau 1.

Détection

Certains des fichiers identifiés ci-dessus ont été déposés dans des emplacements tels que C:\Users\Public* et C:\Windows\Temp*. Ces emplacements peuvent être pratiques pour l'écriture de données, car ils sont généralement accessibles en écriture à tous, c'est-à-dire que tous les comptes utilisateurs enregistrés dans Windows ont accès à ces répertoires et à leurs sous-répertoires. N'importe quel utilisateur peut ensuite accéder à ces fichiers, ce qui permet des déplacements latéraux, des contournements de défense, des exécutions avec de faibles privilèges et des préparations pour l'exfiltration.

Les règles Sigma suivantes recherchent une exécution à partir d'emplacements suspects comme indicateur d'activité anormale. Dans tous les cas, une enquête ultérieure est nécessaire pour confirmer l'activité malveillante et son attribution.

Titre : Exécution accessible en écriture à tous - Temp

ID : d2fa2d71-fbd0-4778-9449-e13ca7d7505c

Description : Détecter l'exécution d'un processus depuis C:\Windows\Temp.

Historique

Cette règle examine spécifiquement les exécutions à partir de C:\Windows\Temp*. Temp est plus largement utilisé par des applications bénignes et constitue donc un indicateur de malveillance moins fiable que les exécutions à partir d'autres sous-répertoires accessibles en écriture à tous dans C:\Windows.

La suppression des applications exécutées par les utilisateurs SYSTEM ou NETWORK SERVICE réduit considérablement la quantité d'activités bénignes sélectionnées par cette règle.

Cela signifie que la règle peut ignorer des exécutions malveillantes à un niveau de privilèges plus élevé, mais il est recommandé d'utiliser d'autres règles pour déterminer si un utilisateur tente d'élever ses privilèges à SYSTEM.

Investigation :

1. Examinez les informations directement associées à l'exécution de ce fichier, telles que le contexte utilisateur, le niveau d'intégrité de l'exécution, l'activité consécutive immédiate et les images chargées par le fichier.
2. Examinez le processus contextuel, le réseau, le fichier et les autres données connexes sur l'hôte afin de déterminer si l'activité est malveillante.
3. Si nécessaire, tentez de collecter une copie du fichier pour une rétro-ingénierie afin de déterminer sa légitimité.

Références :

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

Auteur : ACSC de l'ASD

Date : 19/06/2024

Statut : expérimental

Mots-clés :

- tlp.green
- classification.au.official
- attack.execution

Source du journal :

```
catégorie : process_creation
produit : windows
```

Détection :

```
temp :
    Image|startswith: 'C:\\Windows\\Temp\\'
common_temp_path:
    Image|re|ignorecase : 'C:\\Windows\\Temp\\\
    {[a-fA-F0-9]{8}-([a-fA-F0-9]{4}-){3}[a-fA-F0-9]
    {12}\}\\'
system_user :
    User :
    - 'SYSTEM'
    - 'NETWORK SERVICE'
```

dismhost :

Image|endswith : 'dismhost.exe'

known_parent :

ParentImage|endswith :

- '\\esif_uf.exe'
- '\\vmtoolsd.exe'
- '\\cwainstaller.exe'
- '\\trolleyexpress.exe'

condition : temp et non (common_temp_path ou system_user ou dismhost ou known_parent)

Faux positifs :

- Des applications d'audit de liste blanche ont été observées exécutant des exécutables depuis Temp.
- Temp contiendra légitimement un ensemble d'applications d'installation et de lanceurs. Il est donc judicieux d'évaluer la fréquence de ce comportement sur un réseau surveillé (et de déterminer s'il peut être ajouté à la liste blanche) avant de déployer cette règle.

Niveau : faible

Titre : Exécution accessible en écriture à tous - Sous-répertoire système non - temporaire

ID : 5b187157-e892-4fc9-84fc-aa48aff9f997

Description : Détecter l'exécution d'un processus depuis un emplacement accessible en écriture à tous dans un sous-répertoire de l'emplacement d'installation du système d'exploitation Windows.

Historique :

Cette règle recherche spécifiquement l'exécution depuis des répertoires accessibles en écriture à tous hors de l'emplacement C:\, et plus particulièrement C:\Windows*, à l'exception de C:\Windows\Temp (plus largement utilisé par des applications bénignes et donc un indicateur malveillant de faible fiabilité).

Les dossiers Données d'application (AppData) sont exclus si un fichier est exécuté en tant que SYSTEM ; il s'agit d'une méthode bénigne d'exécution de nombreux fichiers d'application temporaires.

Après avoir effectué une analyse réseau initiale et identifié les exécutions bénignes connues à ces emplacements, cette règle devrait rarement se déclencher.

Investigation :

1. Examinez les informations directement associées à l'exécution de ce fichier, telles que le contexte utilisateur, le niveau d'intégrité de l'exécution, l'activité consécutive immédiate et les images chargées par le fichier.
2. Examinez le processus contextuel, le réseau, le fichier et les autres données connexes sur l'hôte afin de déterminer si l'activité est malveillante.
3. Si nécessaire, tentez de collecter une copie du fichier pour effectuer une rétro-ingénierie afin de déterminer sa légitimité.

Références :

https://gist.github.com/mattifestation/5f9de750470c9e0e1f9c9c33f0ec3e56

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

Auteur : L'ACSC de l'ASD

Date : 19/06/2024

Statut : expérimental

Mots-clés :

- tlp.green
- classification.au.official
- attack.execution

Source du journal :

catégorie : process_creation

produit : Windows

Détection :

writable_path:

Image|contient :

- ':\\$Recycle.Bin\\'
- ':\\AMD\\Temp\\'
- ':\\Intel\\'
- ':\\PerfLogs\\'
- ':\\Windows\\addins\\'
- ':\\Windows\\appcompat\\'
- ':\\Windows\\apppatch\\'
- ':\\Windows\\AppReadiness\\'
- ':\\Windows\\bcastdvr\\'
- ':\\Windows\\Boot\\'
- ':\\Windows\\Branding\\'
- ':\\Windows\\CbsTemp\\'
- ':\\Windows\\Containers\\'
- ':\\Windows\\csc\\'
- ':\\Windows\\Cursors\\'
- ':\\Windows\\debug\\'
- ':\\Windows\\diagnostics\\'
- ':\\Windows\\DigitalLocker\\'
- ':\\Windows\\dot3svc\\'
- ':\\Windows\\en-US\\'
- ':\\Windows\\Fonts\\'
- ':\\Windows\\Globalization\\'
- ':\\Windows\\Help\\'
- ':\\Windows\\IdentityCRL\\'
- ':\\Windows\\IME\\'
- ':\\Windows\\ImmersiveControlPanel\\'
- ':\\Windows\\INF\\'
- ':\\Windows\\intel\\'

- ':\\Windows\\L2Schemas\\'
- ':\\Windows\\LiveKernelReports\\'
- ':\\Windows\\Logs\\'
- ':\\Windows\\media\\'
- ':\\Windows\\Migration\\'
- ':\\Windows\\ModemLogs\\'
- ':\\Windows\\ms\\'
- ':\\Windows\\OCR\\'
- ':\\Windows\\panther\\'
- ':\\Windows\\Performance\\'
- ':\\Windows\\PLA\\'
- ':\\Windows\\PolicyDefinitions\\'
- ':\\Windows\\Prefetch\\'
- ':\\Windows\\PrintDialog\\'
- ':\\Windows\\Provisioning\\'
- ':\\Windows\\Registration\\CRMLog\\'
- ':\\Windows\\RemotePackages\\'
- ':\\Windows\\rescache\\'
- ':\\Windows\\Resources\\'
- ':\\Windows\\SchCache\\'
- ':\\Windows\\schemas\\'
- ':\\Windows\\security\\'
- ':\\Windows\\ServiceState\\'
- ':\\Windows\\servicing\\'
- ':\\Windows\\Setup\\'
- ':\\Windows\\ShellComponents\\'
- ':\\Windows\\ShellExperiences\\'
- ':\\Windows\\SKB\\'
- ':\\Windows\\TAPI\\'
- ':\\Windows\\Tasks\\'
- ':\\Windows\\TextInput\\'
- ':\\Windows\\tracing\\'
- ':\\Windows\\Vss\\'
- ':\\Windows\\WaaS\\'
- ':\\Windows\\Web\\'
- ':\\Windows\\wlansvc\\'
- ':\\Windows\\System32\\Com\\dmp\\'
- ':\\Windows\\System32\\FxsTmp\\'
- ':\\Windows\\System32\\Microsoft\\Crypto\\RSA\\MachineKeys\\'
- ':\\Windows\\System32\\Speech\\'
- ':\\Windows\\System32\\spool\\drivers\\color\\'
- ':\\Windows\\System32\\spool\\PRINTERS\\'
- ':\\Windows\\System32\\spool\\SERVERS\\'
- ':\\Windows\\System32\\Tasks_Migrated\\Microsoft\\Windows\\PLA\\System\\'
- ':\\Windows\\System32\\Tasks\\'
- ':\\Windows\\SysWOW64\\Com\\dmp\\'
- ':\\Windows\\SysWOW64\\FxsTmp\\'
- ':\\Windows\\SysWOW64\\Tasks\\'

appdata:

Image|contient : '\\AppData\\'
Utilisateur : 'SYSTEM'

condition : writable_path et non appdata

Faux positifs :

Des applications d'audit de listes blanches ont été observées exécutant des exécutables depuis ces répertoires.

Il est vraisemblable que les scripts et les outils d'administration utilisés dans les environnements surveillés se trouvent dans l'un de ces répertoires et qu'il faille traiter ce problème au cas par cas.

Niveau : élevé

Titre : Exécution accessible en écriture à tous - Utilisateurs

ID : 6dda3843-182a-4214-9263-925a80b4c634

Description : Détecter l'exécution d'un processus depuis C:\Users\Public* et d'autres dossiers accessibles en écriture à tous dans Utilisateurs.

Historique :

Les dossiers AppData sont exclus si un fichier est exécuté en tant que SYSTEM ; il s'agit d'une méthode bénigne d'exécution de nombreux fichiers d'application temporaires.

Investigation :

1. Examiner les informations directement associées à l'exécution de ce fichier, telles que le contexte utilisateur, le niveau d'intégrité de l'exécution, l'activité consécutive immédiate et les images chargées par le fichier.
2. Analyser le processus contextuel, le réseau, le fichier et les autres données connexes sur l'hôte afin de déterminer si l'activité est malveillante.
3. Si nécessaire, tenter de collecter une copie du fichier pour une rétro-ingénierie afin de déterminer sa légitimité.

Références :

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

Auteur : l'ACSC de l'ASD

Date : 19/06/2024

Statut : expérimental

Mots-clés :

- tlp.green
- classification.au.official
- attack.execution

Source du journal :

catégorie : process_creation
produit : Windows

Détection :

utilisateurs :

Image|contient :

- ':\\Users\\All Users\\'
- ':\\Users\\Contacts\\'
- ':\\Users\\Default\\'
- ':\\Users\\Public\\'
- ':\\Users\\Searches\\'

appdata:

Image|contient : '\\Appdata\\'

Utilisateur : 'SYSTEM'

condition : utilisateurs et non appdata

Faux positifs :

- Il est vraisemblable que les scripts et les outils d'administration utilisés dans les environnements surveillés se trouvent dans le répertoire Public ou un sous-répertoire, et ce problème doit être traité au cas par cas.

Niveau : moyen

Atténuations

Journalisation

Lors des enquêtes de l'ACSC de l'ASD, un problème courant qui réduit l'efficacité et la rapidité des investigations est le manque d'informations de journalisation complètes et historiques dans plusieurs domaines, notamment les journaux de requêtes du serveur Web, les journaux d'événements Windows et les journaux de proxy Internet.

L'ACSC de l'ASD recommande de revoir et de mettre en œuvre ses directives sur la journalisation et le transfert des événements Windows, y compris les fichiers de configuration et les scripts du référentiel de journalisation des événements Windows et les directives du Manuel de sécurité de l'information pour la surveillance des systèmes, notamment la centralisation et la conservation des journaux pendant une période appropriée.

Gestion des correctifs

Appliquez rapidement les correctifs à tous les appareils et services exposés à Internet, y compris les serveurs et applications Web et les passerelles d'accès à distance. Envisagez la mise en œuvre d'un système centralisé de gestion des correctifs pour automatiser et accélérer le processus. L'ACSC de l'ASD recommande la mise en œuvre des directives de gestion des systèmes de l'ISM, notamment les contrôles de mise à jour des correctifs système, le cas échéant.

La plupart des exploits utilisés par l'acteur étaient connus du public et des correctifs ou des mesures d'atténuation étaient disponibles. Les organisations doivent s'assurer que les correctifs de sécurité ou les mesures d'atténuation sont appliqués à l'infrastructure connectée à Internet dans les 48 heures et, si possible, utiliser les dernières versions des logiciels et des systèmes d'exploitation.

Segmentation du réseau

La segmentation du réseau peut rendre la localisation et l'accès aux données sensibles d'une organisation beaucoup plus difficiles pour les pirates. Segmentez les réseaux pour limiter ou bloquer les mouvements latéraux en refusant le trafic entre les ordinateurs, sauf si nécessaire. Les serveurs importants tels qu'Active Directory et autres serveurs d'authentification ne doivent être administrés que depuis un nombre limité de serveurs intermédiaires, ou « serveurs de saut ». Ces serveurs doivent être étroitement surveillés, bien sécurisés et limiter le nombre d'utilisateurs et d'appareils pouvant s'y connecter.

Indépendamment des cas identifiés où les mouvements latéraux sont empêchés, une segmentation supplémentaire du réseau aurait pu limiter davantage la quantité de données auxquelles les acteurs ont pu accéder et qu'ils ont pu extraire.

Mesures d'atténuation supplémentaires

Les agences rédactrices recommandent également les mesures d'atténuation suivantes pour lutter contre l'utilisation des TTP par APT40 et d'autres acteurs.

- Désactivez les services, ports et protocoles réseau inutilisés ou inutiles.
- Utilisez des pare-feu applicatifs Web (Web application firewalls, WAF) performants pour protéger vos serveurs et applications Web.
- Appliquez le principe du moindre privilège pour limiter l'accès aux serveurs, aux partages de fichiers et aux autres ressources.
- Utilisez l'authentification multifacteur (AMF) et les comptes de services gérés pour rendre les identifiants plus difficiles à pirater et à réutiliser. L'AMF doit être appliquée à tous les services d'accès à distance accessibles par Internet, notamment :
  - Messagerie électronique Web et cloud
  - Plateformes collaboratives
  - Connexions à des réseaux privés virtuels
  - Services de bureau à distance
- Remplacer les équipements en fin de vie.

Tableau 1. Stratégies/techniques d'atténuation

TTP	Huit stratégies essentielles d'atténuation	Contrôles ISM
Accès initial T1190 Exploitation des applications publiques	Correctifs pour les applications Correctifs pour les systèmes d'exploitation Authentification multifacteur Contrôle des applications	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
Exécution T1059 Interpréteur de commandes et de scripts	Contrôle des applications Restriction des macros Microsoft Office Restriction des privilèges d'administrateur	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
Persistance T1505.003 Composant logiciel serveur : Web Shell	Contrôle des applications Restrictions des privilèges d'administrateur	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
Accès initial/Élévation des privilèges/Persistance T1078 Comptes valides	Correctifs des systèmes d'exploitation Authentification multifacteur Restriction des privilèges d'administrateur Contrôle des applications Renforcement des applications utilisateur	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

Pour obtenir des conseils généraux supplémentaires en matière de détection et d'atténuation, veuillez consulter les sections Atténuations et détection sur la page Web de la technique MITRE ATT&CK pour chacune des techniques identifiées dans le résumé MITRE ATT&CK à la fin de cet avis.

Avis de non-responsabilité

Les informations contenues dans ce rapport sont fournies « en l'état » à titre informatif uniquement. Les agences rédactrices ne cautionnent aucune entité commerciale, aucun produit, aucune entreprise ni aucun service, y compris les entités, produits ou services liés dans ce document. Toute référence à des entités commerciales, produits, processus ou services spécifiques par une marque de service, une marque déposée, un fabricant ou autre ne constitue ni n'implique une approbation, une recommandation ou un favoritisme de la part des agences rédactrices.

Ce document est marqué TLP:CLEAR. La divulgation n'est pas limitée. Les sources peuvent utiliser TLP:CLEAR lorsque les informations présentent un risque minimal ou nul d'utilisation abusive, conformément aux règles et procédures applicables en matière de diffusion publique. Sous réserve des règles standard de droit d'auteur, les informations TLP:CLEAR peuvent être diffusées sans restriction. Pour en savoir plus sur le protocole Traffic Light, consultez cisa.gov/tlp

MITRE ATT&CK – Relevé des tactiques d'intérêt d'APT40

Reconnaissance (TA0043)	
Recherche de sites Web appartenant à des victimes (T1594)	Collecte d'informations sur l'identité des victimes : Identifiants (T1589.001)
Analyse active : Analyse des vulnérabilités (T1595.002)	Collecte d'informations sur l'hôte de la victime (T1592)
Recherche de sites Web/domaines ouverts : Moteurs de recherche (T1593.002)	Collecte d'informations sur le réseau de la victime : Propriétés du domaine (T1590.001)
Collecte d'informations sur l'identité de la victime : Adresses courriel (T1589.002)	

Développement des ressources (TA0042)	
Acquisition d'infrastructures : Domaines (T1583.001)	Acquisition d'infrastructures (T1583)
Acquisition d'infrastructures : Serveur DNS (T1583.002)	Comptes compromis (T1586)
Développer les capacités : Certificats de signature de code (T1587.002)	Infrastructure de compromission (T1584)
Développer les capacités : Certificats numériques (T1587.003)	Développer les capacités : Logiciels malveillants (T1587.001)
Obtention de capacités : Certificats de signature de code (T1588.003)	Création de comptes : Comptes Cloud (T1585.003)
Infrastructure compromise : Appareils réseau (T1584.008)	Obtention de capacités : Certificats numériques (T1588.004)

Accès initial (TA0001)	
Comptes valides (T1078)	Hameçonnage (T1566)
Comptes valides : Comptes par défaut (T1078.001)	Hameçonnage : Pièce jointe d'hameçonnage ciblé (T1566.001)
Comptes valides : Comptes de domaine (T1078.002)	Hameçonnage : Lien d'hameçonnage ciblé (T1566.002)
Services distants externes (T1133)	Exploitation d'une application publique (T1190)
Compromission « drive-by » (par visite de site) (T1189)	

Exécution (TA0002)	
Instrumentation de gestion Windows (T1047)	Interpréteur de commandes et de scripts : Python (T1059.006)
Tâche/Emploi planifié : À (T1053.002)	Interpréteur de commandes et de scripts : JavaScript (T1059.007)
Tâche/Emploi planifié : Tâche planifiée (T1053.005)	API native (T1106)
Interpréteur de commandes et de scripts (T1059)	Communication interprocessus (T1559)
Interpréteur de commandes et de scripts : Shell de commandes Windows (T1059.003)	Services système : Exécution de services (T1569.002)
Interpréteur de commandes et de scripts : PowerShell (T1059.001)	Exploitation pour l'exécution client (T1203)
Interpréteur de commandes et de scripts : Visual Basic (T1059.005)	Exécution par l'utilisateur : Fichier malveillant (T1204.002)
Interpréteur de commandes et de scripts : Shell Unix (T1059.004)	Interpréteur de commandes et de scripts : Apple Script (T1059.002)
Tâche/Emploi planifié : Cron (T1053.003)	Outils de déploiement logiciel (T1072)

Persistance (TA0003)	
Comptes valides (T1078)	Composant logiciel serveur : Web shell (T1505.003)
Démarrage d'applications Office : Macros de modèles Office (T1137.001)	Création ou modification d'un processus système : Service Windows (T1543.003)
Tâche/Emploi planifié : À (T1053.002)	Exécution automatique au démarrage ou à la connexion : Clés d'exécution du registre/Dossier de démarrage (T1547.001)
Tâche/Emploi planifié : Tâche planifiée (T1053.005)	Exécution automatique au démarrage ou à la connexion : Modification de raccourci (T1547.009)
Services distants externes (T1133)	Flux d'exécution du piratage : Piratage de l'ordre de recherche des DLL (T1574.001)
Tâche/Emploi planifié : Cron (T1053.003)	Flux d'exécution du piratage : Chargement latéral de DLL (T1574.002)
Manipulation de compte (T1098)	Comptes valides : Comptes cloud (T1078.004)
Comptes valides : Comptes de domaine (T1078.002)	

Élévation des privilèges (TA0004)	
Tâche/Emploi planifié : À (T1053.002)	Création ou modification d'un processus système : Service Windows (T1543.003)
Tâche/Emploi planifié : Tâche planifiée (T1053.005) :	Exécution automatique au démarrage ou à la connexion : Clés d'exécution du registre/Dossier de démarrage (T1547.001)
Injection de processus : Piratage d'exécution de thread (T1055.003)	Exécution automatique au démarrage ou à la connexion : Modification de raccourci (T1547.009)
Injection de processus : Creux de processus (T1055.012)	Flux d'exécution du piratage : Piratage de l'ordre de recherche de DLL (T1574.001)

Élévation de privilèges (TA0004)	
Comptes valides : Comptes de domaine (T1078.002)	Exploitation pour élévation de privilèges (T1068)
Manipulation de jetons d'accès : Usurpation/Vol de jetons (T1134.001)	Exécution déclenchée par un événement : Modification de la configuration du shell Unix (T1546.004)
Injection de processus : Injection de bibliothèque de liens dynamiques (T1055.001)	Comptes valides : Comptes de domaine (T1078.002)
Comptes valides : Comptes locaux (T1078.003)	

Évasion de défense (TA0005)	
Rootkit (T1014)	Exécution de commandes indirectes (T1202)
Fichiers ou informations obfusqués (T1027)	Exécution du proxy binaire système : Mshta (T1218.005)
Fichiers ou informations obfusqués : Emballage logiciel (T1027.002)	Exécution du proxy binaire système : Regsvr32 (T1218.010)
Fichiers ou informations obfusqués : Stéganographie (T1027.003)	Contournement des contrôles de confiance : Signature de code (T1553.002)
Fichiers ou informations obfusqués : Compilation après livraison (T1027.004)	Modifications des autorisations de fichiers et de répertoires : Modification des autorisations de fichiers et de répertoires sous Linux et Mac (T1222.002)
Attaque par usurpation d'identité : Correspondance avec un nom ou un emplacement légitime (T1036.005)	Virtualisation/Évasion de la sandbox : Vérifications système (T1497.001)
Injection de processus : Détournement d'exécution de thread (T1055.003)	Attaque par usurpation d'identité (T1036)
Chargement de code réflectif (T1620)	Dégradation des défenses : Désactivation ou modification du pare-feu système (T1562.004)
Injection de processus : Évidement de processus (T1055.012)	Masquage d'artefacts : Fichiers et répertoires cachés (T1564.001)
Suppression d'indicateurs : Suppression de fichiers (T1070.004)	Masquage d'artefacts : Fenêtre cachée (T1564.003)
Suppression d'indicateurs : Horodatage (T1070.006)	Piratage de flux d'exécution : Piratage de l'ordre de recherche des DLL (T1574.001)
Suppression d'indicateurs : Effacement des journaux d'événements Windows (T1070.001)	Piratage de flux d'exécution : Chargement latéral des DLL (T1574.002)
Modification du registre (T1112)	Service Web (T1102)
Désobfuscation/Décodage de fichiers ou d'informations (T1140)	Attaque par usurpation d'identité : Attaque par usurpation d'identité d'une tâche ou d'un service (T1036.004)
Dégradation des défenses (T1562)	

Accès aux identifiants (TA0006)	
Vidage des identifiants du système d'exploitation : Mémoire LSASS (T1003.001)	Identifiants non sécurisés : Identifiants dans les fichiers (T1552.001)
Vidage des identifiants du système d'exploitation : NTDS (T1003.003)	Force brute : Devinette de mot de passe (T1110.001)
Reniflage de réseau (T1040)	Authentification forcée (T1187)

Accès aux identifiants (TA0006)	
Identifiants provenant de bases de données de mots de passe : Trousseau (T1555.001)	Vol ou falsification de tickets Kerberos : Kerberoasting (T1558.003)
Capture d'entrée : Enregistrement de frappe (T1056.001)	Interception d'authentification multifacteur (T1111)
Vol de cookie de session Web (T1539)	Vol de jeton d'accès d'application (T1528)
Exploitation pour accès aux identifiants (T1212)	Force brute : Cassage de mot de passe (T1110.002)
Capture d'entrée : Capture du portail Web (T1056.003)	Vidage des identifiants du système d'exploitation : DCSync (T1003.006)
Identifiants des bases de données de mots de passe (T1555)	Identifiants des bases de données de mots de passe : Identifiants des navigateurs Web (T1555.003)

Découverte (TA0007)	
Découverte des services système (T1007)	Découverte des informations système (T1082)
Découverte de fenêtres d'applications (T1010)	Découverte de compte : Compte local (T1087.001)
Interrogation du registre (T1012)	Découverte d'informations système, technique T1082 – Entreprise |MITRE ATT&CK®
Découverte de fichiers et de répertoires (T1083)	Découverte de l'heure système (T1124)
Découverte des services réseau (T1046)	Découverte du propriétaire/utilisateur du système (T1033)
Découverte du système distant (T1018)	Découverte de l'approbation du domaine (T1482)
Découverte de comptes : Compte de messagerie (T1087.003)	Découverte de comptes : Compte de domaine (T1087.002)
Découverte des connexions réseau du système (T1049)	Virtualisation/Évasion de la sandbox : Vérifications système (T1497.001)
Découverte de processus (T1057)	Découverte de logiciels (T1518)
Découverte des groupes d'autorisations : Groupes de domaines (T1069.002)	Découverte des partages réseau, technique T1135 - Entreprise | MITRE ATT&CK®
Découverte de la configuration réseau du système : Découverte de connexion Internet (T1016.001)	

Déplacement latéral (TA0008)	
Services distants : Protocole Bureau à distance (T1021.001)	Services distants (T1021)
Services distants : Partages d'administration SMB/ Windows (T1021.002)	Utilisation d'un autre moyen d'authentification : Transfert du ticket (T1550.003)
Services distants : Gestion à distance Windows (T1021.006)	Transfert d'outils latéral (T1570)

Collecte (TA0009)	
Données du système local (T1005)	Archivage des données collectées : Archivage via la bibliothèque (T1560.002)
Données du lecteur réseau partagé (T1039)	Collecte de courriels : Collecte de courriels à distance (T1114.002)

Collecte (TA0009)	
Capture d'entrée : Enregistrement de frappe (T1056.001)	Données du presse-papiers (T1115)
Collecte automatisée (T1119)	Données des référentiels d'informations (T1213)
Capture d'entrée : Capture depuis un portail Web (T1056.003)	Données mises en scène : Mise en scène des données à distance (T1074.002)
Données mises en scène : Mise en scène des données locales (T1074.001)	Données collectées archivées (T1560)
Collecte de courriels (T1114)	

Exfiltration (TA0010)	
Exfiltration via le canal C2 (T1041)	Exfiltration via un protocole alternatif : Exfiltration via un protocole non C2 chiffré asymétrique (T1048.002)
Exfiltration via un protocole alternatif (T148)	Exfiltration via un service Web : Exfiltration vers un stockage cloud (T1567.002)

Commande et contrôle (TA0011)	
Obfuscation des données : Usurpation d'identité de protocole (T1001.003)	Service Web : Résolution des interruptions de service (T1102.001)
Port fréquemment utilisé (T1043)	Service Web : Communication unidirectionnelle (T1102.003)
Protocole de couche applicative : Protocoles Web (T1071.001)	Transfert d'outils d'entrée (T1105)
Protocole de couche applicative : Protocoles de transfert de fichiers (T1071.002)	Proxy : Proxy interne (T1090.001)
Proxy : Proxy externe (T1090.002)	Port non-standard (T1571)
Proxy : Proxy multi-sauts (T1090.003)	Tunneling de protocole (T1572)
Service Web : Communication bidirectionnelle (T1102.002)	Canal crypté (T1573)
Canal crypté : Cryptographie asymétrique (T1573.002)	Transfert d'outils d'entrée (T1105)
Proxy, technique T1090 - Entreprise | MITRE ATT&CK®	

Impact (TA0040)	
Arrêt de service (T1489)	Effacement du disque (T1561)
Arrêt/Redémarrage du système (T1529)	Piratage de ressources (T1496)

Remarques

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.

Droits d'auteur

Utilisation du blason

Les conditions dans lesquelles le blason peut être utilisé sont détaillées sur le site Web du Département du Premier Ministre et du Cabinet Informations et directives sur le blason du Commonwealth | pmc.gov.au.

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