Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Rapport conjoint sur les outils de piratage publiquement accessibles

Canada

Contents

1 INTRODUCTION

Le présent rapport est le fruit de recherches menées en collaboration par les responsables de la cybersécurité des cinq États : l'Australie, le Canada, la Nouvelle-Zélande, le Royaume-Uni et les États-Unis.[1]

Dans ce rapport, nous faisons état de l'utilisation de cinq outils publiquement accessibles qui ont été employés à des fins malveillantes pour provoquer une série de cyberincidents survenus récemment en divers endroits du globe.

Nous formulons également, à l'intention des responsables de la défense des réseaux et des administrateurs de systèmes, des conseils permettant de réduire l'incidence de ces outils et de détecter les indices de leur utilisation dans les réseaux.

1.1 NATURE DES OUTILS

De fait, les outils faisant l'objet de la présente ne constituent que des exemples non exhaustifs des outils employés par les auteurs malveillants. Ainsi, lorsqu'il s'agit de préparer les mesures de défense d'un réseau, il faut savoir qu'il existe d'autres types de menaces.

Encore faut-il noter que les outils et les techniques d'exploitation des réseaux et des données que ceux-ci contiennent ne sont pas l'apanage des États ou des criminels du Web caché. De nos jours, des outils de piratage dotés de tout un éventail de fonctions sont largement accessibles et employés par une diversité d'entités, notamment par des informaticiens qui effectuent des tests de pénétration tout autant que par des auteurs de menace parrainés par un État ou par des membres du crime organisé, voire par des pirates amateurs.

En outre, ces outils ont été utilisés pour compromettre de l'information dans une diversité de secteurs, notamment la santé, les finances, les services et programmes gouvernementaux, et la défense. Leur disponibilité à grande échelle pose des difficultés à ceux et celles qui sont responsables de défendre les réseaux et de retracer les auteurs de menace.

L'expérience de nos cinq États indique clairement que, certes, il est important de développer de nouvelles capacités, mais qu'il importe tout autant de miser sur les outils et les techniques dont on dispose déjà. Même les groupes disposant des moyens les plus sophistiqués ont recours aux outils publiquement accessibles pour atteindre leurs objectifs.

Or, quels que soient les objectifs visés, il importe de savoir que la compromission des systèmes procède d'abord de l'exploitation de failles de sécurité couramment observées. En outre, l'exploitation des vulnérabilités présentées par les logiciels non corrigés ou par les systèmes inadéquatement configurés est le moyen privilégié par les auteurs malveillants qui tentent d'accéder à du contenu qui leur est interdit. Au reste, ce n'est que suivant une première compromission que les outils ici présentés entrent en jeu de façon à permettre aux attaquants de poursuivre leur exploitation des systèmes ciblés.

1.2 STRUCTURE DU RAPPORT

Les outils ici présentés se classent en cinq catégories : chevaux de Troie d'accès à distance (RAT pour *Remote Access Trojan*); scripts WebShell; voleurs d'identifiants; mouvements latéraux; et obfuscation de commande et contrôle (C2).

[1] L'Australian Cyber Security Centre (ACSC), le Centre canadien pour la cybersécurité (CCC), le New Zealand National Cyber Security Centre (NZ NCSC), la CERT New Zealand, le UK National Cyber Security Centre (UK NCSC) et le US National Cybersecurity and Communications Integration Center (NCCIC).

Pour chacun des outils, le rapport propose un aperçu des menaces possibles, puis indique le lieu et le moment où ces outils ont été employés par des auteurs malveillants. Sont également décrites les mesures favorisant la détection et réduisant l'incidence de chacun des outils.

En fin de rapport sont présentés tout un éventail de conseils généraux ayant pour objet d'améliorer les pratiques de défense des réseaux.

2 CHEVAL DE TROIE D'ACCÈS À DISTANCE : JBiFROST

Relevé pour la première fois en mai 2015, le cheval de Troie d'accès à distance (RAT) JBiFrost est un dérivé d'Adwind RAT, dont les racines remontent au Frutas RAT de 2012.

Un RAT est un programme qui, une fois installé dans un ordinateur ciblé, permet d'exécuter à distance des fonctions d'administration. Dans le contexte d'une intervention malveillante, ce programme peut servir, entre autres, à installer des portes dérobées et des enregistreurs de frappes, à faire des copies d'écran ou à exfiltrer des données.

Les RAT malveillants peuvent être difficiles à détecter puisqu'ils sont habituellement conçus pour ne pas paraître dans la liste des programmes en exécution et qu'ils peuvent imiter le comportement d'applications légitimes.

Pour contrer les analyses informatiques judiciaires, les RAT ont tendance à désactiver les mesures de sécurité des ordinateurs ciblés, notamment le gestionnaire de tâches et les outils d'analyse réseau comme Wireshark.

2.1 UTILISATION

JBiFrost est généralement employé par les cybercriminels et les auteurs peu spécialisés, mais ses capacités pourraient très bien être adaptées par des auteurs parrainés par un État.

Les autres RAT sont couramment utilisés par les groupes employant les menaces avancées persistantes (APT pour *Advanced Persistent Threat*), par exemple Adwind contre le secteur de l'aérospatial et de la défense, ou Quasar RAT, par APT10, contre une multiplicité de secteurs.

De plus, des auteurs malveillants ont été en mesure de compromettre certains serveurs dans le but d'introduire des RAT malveillants dans des ordinateurs ciblés. L'objectif était probablement d'établir un accès à distance aux fins d'exploitation ou bien de voler de l'information de valeur, notamment les identifiants bancaires, les renseignements sur la propriété intellectuelle et les renseignements nominatifs (PII pour *Personally Identifiable Information*).

2.2 CAPACITÉS

Le RAT JBiFrost est un programme Java; il est multiplateforme et multifonctionnel. Il constitue une menace pour divers systèmes d'exploitation, notamment Windows, Linux, MAC OS X, et Android.

JBiFrost permet à un pirate d'exécuter des pivots et des mouvements latéraux dans un réseau donné ou d'installer du logiciel malveillant additionnel. Il est principalement livré en tant que fichier joint à un courriel, généralement un avis de facturation, une demande de devis, un avis de versement, un avis d'expédition ou un avis de paiement; il est également accompagné d'un lien menant à un service d'hébergement de fichiers.

On a vu ce type d'infection à l'origine d'exfiltration de renseignements sur la propriété intellectuelle, d'identifiants bancaires et de PII. Les ordinateurs infectés par JBiFrost peuvent également faire partie de réseaux de zombies (*botnets*) et servir à des attaques par déni de service distribué (DDoS pour *Distributed Denial of Service*).

2.3 EXEMPLES

Depuis le début de 2018, on note un accroissement de l'utilisation de JBiFrost dans des attaques ciblant les responsables de l'infrastructure nationale essentielle ainsi que les intervenants de leur chaîne d'approvisionnement. On remarque également une augmentation de l'hébergement de RAT dans l'infrastructure de nos pays respectifs.

Au début de 2017, le RAT Adwin a été déployé par l'intermédiaire de courriels de mystification conçus pour laisser croire qu'ils provenaient des services réseau de SWIFT.

Bon nombre d'autres RAT publiquement accessibles, entre autres des dérivés de Gh0st RAT, ont été mis au jour alors qu'ils ciblaient une multiplicité de victimes au quatre coins du globe.

2.4 DÉTECTION ET PROTECTION

Voici quelques signes pouvant indiquer qu'une infection par le RAT JBiFrost aurait eu lieu :

- impossibilité de redémarrer l'ordinateur en mode sans échec (*Safe Mode*);
- impossibilité de démarrer ni l'éditeur de registre Windows ni le gestionnaire de tâches;
- accroissement important de l'activité du disque ou du trafic réseau;
- tentatives de connexion à des adresse IP malveillantes connues;
- création de nouveaux fichiers et répertoires, dont le nom est obscurci ou généré aléatoirement.

applications installées – reçoivent les mises à jour et les correctifs dès que ceux-ci sont disponibles. Le recours à un programme antivirus moderne disposant d'une fonction de mise à jour automatisée, et l'exécution régulière d'un balayage des systèmes contribuent également à contrer les plus récentes variantes du maliciel. Il serait utile de veiller à ce que l'organisation soit en mesure de journaliser les détections faites par l'antivirus, et ce, dans tous les secteurs du système concerné, et de procéder à une analyse approfondie des occurrences de RAT.

Le recours systématique à une liste blanche est recommandé pour prévenir les infections.

Les courriels-hameçons constituent les principaux mécanismes d'infection au moyen d'un RAT, y compris JBiFrost. On peut favoriser la lutte contre les infections JBiFrost en empêchant ces courriels d'hameçonnage d'atteindre les destinataires, notamment en apprenant aux utilisateurs comment reconnaître et signaler les courriels-hameçons, et en mettant en place des contrôles de sécurité qui entraveront les courriels malveillants avant qu'ils ne parviennent à compromettre les dispositifs. Pour obtenir de plus amples informations, consulter le plus récent guide du NCSC concernant les attaques par hameçonnage[2].

[2] https://www.ncsc.gov.uk/phishing

3 SCRIPT WEBSHELL : CHINA CHOPPER

China Chopper est un script WebShell publiquement accessible. Comme il est couramment utilisé depuis 2012, ce maliciel est abondamment documenté.

Les WebShell sont des scripts malveillants qui sont téléversés dans un hôte cible consécutivement à une compromission initiale; ils visent à fournir à l'auteur malveillant la possibilité d'exécuter à distance des fonctions d'administration.

Dès lors que l'accès est obtenu, les WebShell peuvent également servir de carrefours depuis lesquels d'autres hôtes du réseau sont ciblés à leur tour.

3.1 UTILISATION

Le script WebShell China Chopper est fréquemment utilisé par les auteurs malveillants pour accéder, à distance, à des serveurs Web compromis, depuis lesquels il permet de gérer les fichiers et les répertoires, et d'accéder à un terminal virtuel placé sur le dispositif compromis.

Comme China Chopper n'affiche qu'un faible volume, 4 ko, et qu'il dispose d'une charge utile aisément modifiable, il est difficile à détecter et à freiner.

3.2 CAPACITÉS

Le WebShell China Chopper se compose principalement de deux modules : le client China Chopper, qui est exploité par l'attaquant, et le serveur China Chopper, qui est installé dans le serveur Web du système ciblé et, lui aussi, exploité par l'attaquant.

Le client WebShell peut exécuter des commandes de terminal et gérer les fichiers conservés sur le serveur du système ciblé. Son hachage MD5 est accessible publiquement[3]

Web Shell Client	Hachage MD5
caidao.exe	5001ef50c7e869253a7c152a638eab8a

Le serveur du WebShell est téléversé en texte clair et peut être aisément modifié par l'auteur malveillant. Cette caractéristique rend difficile la définition d'un hachage qui soit en mesure de repérer l'activité de l'adversaire.

À l'été de 2018, on a repéré des auteurs malveillants en train de cibler des serveurs Web, sur Internet, qui étaient vulnérables à CVE-2017-3066. L'activité était liée à une vulnérabilité d'Adobe Cold Fusion, la plateforme de développement d'applications Web, découlant de l'activation de la fonction d'exécution de code à distance. China Chopper constituait la charge utile de deuxième phase qui, une fois les serveurs compromis, était placée dans le système de façon à donner à l'auteur malveillant un accès distant à l'hôte ciblé.

Suivant l'exploitation d'une vulnérabilité informatique, le China Chopper en mode texte est placé sur le serveur Web du système ciblé. Une fois téléversé, le serveur WebShell devient accessible en tout temps par l'auteur malveillant qui dispose de l'application client. Une fois que la connexion est établie, cet auteur malveillant procède au traitement des fichiers et des données sur le serveur Web.

[3] Affiché initialement sur hxxp://www.maicaidao.com

Il peut notamment téléverser des fichiers sur le serveur infecté ou télécharger des fichiers depuis ce même serveur. Par exemple, au moyen de l'outil d'extraction de fichiers « *wget* », il peut télécharger des fichiers d'Internet et les téléverser sur le serveur infecté pour ensuite modifier, supprimer, copier ou renommer des fichiers ou encore en modifier l'horodatage.

3.3 DÉTECTION ET PROTECTION

La plus efficace des défenses contre un WebShell consiste d'abord à prévenir toute possibilité de compromission du serveur Web. Il faut donc veiller à ce que les logiciels tournant sur les serveurs Web du côté public soient toujours à jour et à ce que les correctifs soient installés sans délai. Applications de vérification personnalisées pour les vulnérabilités Web courantes[4].

L'une des caractéristiques de China Chopper est que chacune de ses activités génère un élément HTTP POST. Ce type d'occurrence est évident, ce qui le rend facilement détectable pour ceux qui ont recours à un outil de défense réseau.
Certes, le serveur WebShell de China Chopper est téléversé en texte clair, mais les commandes sont, quant à elles, exécutées par le client et codées en Base64, ce qui les rend aisément décodables.

L'adoption du protocole TLS (*Transport Layer Security*) par les serveurs Web entraîne le chiffrement du trafic passant par le serveur Web, ce qui complique la détection des activités de China Chopper pour les outils de détection réseau.

Le moyen le plus efficace de détecter et de contrer China Chopper est d'intervenir directement sur l'hôte (plus précisément sur le côté Internet des serveurs Web). Il existe des moyens simples de détecter la présence de WebShell, notamment au moyen de lignes de commandes dans les systèmes d'exploitation Linux ou Windows[5].

Pour repérer les WebShell à grande échelle, les responsables de la défense des réseaux devraient se concentrer sur la détection de deux éléments : l'exécution de processus suspects sur les serveurs Web (p. ex. l'exécution de virus compagnons sur les fichiers binaires PHP), et les connexions externes inhabituelles de la part des serveurs Web. Généralement, les connexions des serveurs Web vers un réseau interne sont prévisibles. Par conséquent, toute modification des habitudes de connexion pourrait annoncer la présence d'un WebShell. On peut administrer les autorisations d'accès réseau de façon à empêcher les processus du serveur Web de modifier les fichiers existants ou d'apporter des modifications aux répertoires où les PHP peuvent s'exécuter.

On recommande également que le contenu des journaux d'accès Web soient surveillés, en procédant, par exemple, à l'analyse du trafic. De cette façon, toute occurrence inattendue (sur le plan des pages ou des tendances du trafic) pourrait constituer un avertissement.

[4] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
[5] Un éventail de commandes et de signatures pouvant servir à contrer China Chopper se trouvent ici : www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-ii.html

4 VOLEUR D'IDENTIFIANTS : MIMIKATZ

Conçu en 2007, Mimikatz s'utilise principalement pour permettre à un auteur malveillant de collecter les identifiants d'autres utilisateurs qui ont ouvert une session sur un ordinateur Windows. En l'occurrence, les identifiants sont collectés directement dans la mémoire, plus précisément dans un processus Windows, à savoir le service LSASS (*Local Security Authority Subsystem Service*).

Les identifiants, qu'ils soient en texte clair ou sous forme de hachage, peuvent être réutilisés pour accéder à d'autres ordinateurs du même réseau.

Initialement, cet outil n'avait pas pour vocation de pirater des systèmes, mais depuis quelques années, Mimikatz refait surface en tant qu'outil couramment utilisé par des auteurs malveillants. Le fait qu'il ait donné lieu à nombre de compromissions en plusieurs lieux du globe a forcé les organisations de divers secteurs à revoir leurs mécanismes de défense réseau.

Généralement, Mimikatz est utilisé une fois que l'accès à un hôte a été obtenu et que l'auteur malveillant souhaite se déplacer dans l'ensemble du réseau interne. L'utilisation de cet outil peut causer de sérieux préjudices aux réseaux dont la sécurité comporte de profondes lacunes.

4.1 UTILISATION

Le code source de Mimikatz est publiquement accessible, ce qui permet aux auteurs malveillants de compiler leurs propres versions de l'outil et de développer de nouveaux modules d'extension ainsi que des fonctionnalités complémentaires.

Nos responsables de la cybersécurité ont remarqué une intensification de l'utilisation de Mimikatz de la part des auteurs malveillants, notamment dans le crime organisé et parmi les groupes parrainés par un État.

Dès lors qu'il a obtenu les accès d'administrateur local sur un hôte, un auteur malveillant peut, grâce à Mimikatz, se saisir des identifiants (hachage ou texte clair) d'autres utilisateurs, ce qui lui permet d'accroître le niveau de ses privilèges au sein d'un domaine et d'exécuter une multitude de tâches postexploitation et de mouvements latéraux.

C'est pourquoi Mimikatz a été amalgamé à d'autres trousses servant aux tests de pénétration et d'exploitation, notamment PowerShell Empire et Metasploit.

4.2 CAPACITÉS

Mimikatz est reconnu particulièrement pour sa capacité à extraire de la mémoire les identifiants en texte clair et en hachage, mais il est également en mesure d'exécuter une foule d'autres fonctions.

Entre autres, l'outil peut obtenir le hachage, les certificats et les clés à long terme de LAN Manager, de NTLM, pour les versions de Windows allant de XP (2003) à 8.1 (2012 R2). Il est également en mesure d'exécuter des tâches « pass-the-hash » et « pass-the-ticket » et de produire des tickets Kerberos (golden tickets).

Plusieurs des fonctionnalités de Mimikatz peuvent être automatisées au moyen de scripts, notamment PowerShell, ce qui permet à un auteur malveillant d'accélérer l'exploitation et de traverser un réseau compromis. Qui plus est, lorsqu'il s'exécute dans la mémoire sous la forme du script PowerShell « Invoke-Mimikatz » (version facilement accessible, mais très puissante), Mimikatz est particulièrement difficile à isoler et à identifier.

4.3 EXEMPLES

Depuis plusieurs années, Mimikatz est impliqué dans de nombreux incidents perpétrés par divers types d'auteurs malveillants. En 2011, il était principalement utilisé par des pirates impossibles à identifier qui cherchaient à tirer des identifiants d'administrateur de DigiNotar, l'autorité de certification néerlandaise. La perte de confiance en DigiNotar a d'ailleurs forcé l'entreprise à la faillite seulement un mois après la compromission.

Plus récemment, en 2017, Mimikatz a été utilisé conjointement avec d'autres outils de piratage dans les attaques par rançongiciel NotPetya et BadRabbit, qui avaient pour but d'extraire les identifiants se trouvant dans des milliers d'ordinateurs. Ces identifiants ont été utilisés pour faciliter le mouvement latéral et la propagation du rançongiciel dans les réseaux, chiffrant au passage les disques durs de nombreux systèmes dont les identifiants avaient été subtilisés.

De plus, une équipe de recherche de Microsoft a constaté l'utilisation de l'outil à l'occasion d'une cyberattaque sophistiquée qui avait ciblé bon nombre d'organisations réputées du domaine de la finance et des technologies. En raison de son association à de nombreux autres outils et de sa capacité à exploiter les vulnérabilités, Mimikatz a été utilisé pour copier et possiblement réutiliser l'image mémoire (dump) de quantités de hachages système.

4.4 DÉTECTION ET PROTECTION

La mise à jour de Windows contribue à réduire la quantité d'information pouvant être accessible à un auteur malveillant qui utilise l'outil Mimikatz, puisque Microsoft s'est donné comme objectif de renforcer la protection offerte par Windows chaque fois qu'une nouvelle version est mise en marché.

Pour prévenir l'extraction d'identifiants par le recours à Mimikatz, les responsables de la sécurité devraient désactiver les fonctions de stockage de mots de passe en texte clair dans la mémoire LSASS. Cette mesure est appliquée par défaut dans la version Windows 8.1/Server 2012 R2 et dans les versions subséquentes, mais peut être configurée dans les version antérieures qui ont reçu les correctifs de sécurité pertinents[6]. Les systèmes Windows 10 et Windows Server 2016 peuvent être protégés moyennant l'utilisation d'une plus récente fonctionnalité de sécurité appelée Credential Guard.
Credential Guard est activé par défaut dans les conditions suivantes :

- les composantes matérielles répondent aux spécifications de Microsoft Windows en matière de compatibilité matérielle ainsi qu'aux stratégies pour Windows Server 2016 et Windows Server Semi-Annual Branch;
- le serveur ne constitue pas le contrôleur du domaine.

Il conviendra de vérifier si les serveurs physiques et virtuels répondent aux exigences minimales de Microsoft pour chacune des versions de Windows 10 et de Windows Server[7].
La réutilisation des mots de passe, plus particulièrement ceux des comptes d'administrateur, simplifie considérablement les attaques pass-the-hash. Les organisations devraient configurer des stratégies d'utilisateur de façon à dissuader la réutilisation des mots de passe, et ce, même pour les comptes de niveau courant dans l'ensemble du réseau.

L'outil LAPS (*Local Admin Password Solution*) de Microsoft peut faciliter la gestion des mots de passe d'administrateur local, éliminant le besoin de définir et de stocker manuellement les mots de passe.

[6] https://support.microsoft.com/en-us/help/2871997/microsoft-security-advisory-update-to-improve-credentials-protection-a
[7] https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-requirements

Les administrateurs de réseau devraient assurer une surveillance et réagir en cas de création ou d'authentification de compte suspecte, de façon à prévenir l'exploitation des Golden Tickets ainsi que la persistance et les mouvements latéraux dans les réseaux. Dans le cas de Windows, des outils comme Microsoft ATA et Azure ATP peuvent s'avérer utiles.

Les administrateurs de réseau devraient s'assurer que les systèmes sont à jour et ont reçu les plus récents correctifs. Les effets de bon nombre de fonctionnalités de Mimikatz sont atténués ou considérablement réduits par les plus récentes versions et mises à jour de système. Toutefois, les responsables de la défense des réseaux devraient savoir qu'aucun correctif n'est parfait, que Mimikatz est en constante mutation et que des tiers développent régulièrement de nouveaux modules.

La plupart des antivirus mis à jour sont en mesure de détecter et d'isoler la version non personnalisée de Mimikatz, et devraient donc être utilisés pour en relever les occurrences. Cependant, les auteurs malveillants peuvent souvent tenter de contourner les systèmes antivirus en exécutant l'outil en mémoire ou en modifiant légèrement le code original de ce même outil. Dès lors que Mimikatz est détecté, il conviendra de mener un examen approfondi, car cet indice indique presqu'invariablement qu'un auteur malveillant a réussi à pénétrer le réseau alors qu'on pourrait croire à l'exécution d'un simple processus automatisé.

Plusieurs fonctionnalités de Mimikatz misent sur l'exploitation des comptes d'administrateur. Par conséquent, il conviendra de veiller à ce que ces comptes soient attribués seulement lorsque c'est nécessaire. Lorsqu'un accès d'administrateur est requis, il est recommandé d'appliquer les principes de gestion des accès privilégiés.

Étant donné que Mimikatz ne peux tirer les identifiants que des comptes d'utilisateurs qui ont ouvert une session depuis un ordinateur compromis, les utilisateurs privilégiés (notamment les administrateurs de domaines) devraient éviter d'ouvrir des sessions sur des ordinateurs au moyen de leurs identifiants privilégiés. Microsoft est en mesure de fournir de plus amples détails sur la sécurisation de Active Directory[8].

Les responsables de la défense des réseaux devraient procéder à la vérification de l'utilisation des scripts, plus particulièrement de PowerShell, et analyser les journaux pour tenter de déceler d'éventuelles anomalies. Ainsi, le repérage de Mimikatz ou des attaques pass-the-hash s'en trouvera facilité, ce qui permettra de contrer les tentatives de contournement des logiciels de détection.

[8] https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

5 MOUVEMENTS LATÉRAUX : POWERSHELL EMPIRE

PowerShell Empire est un exemple d'outil de postexploitation ou de mouvement latéral. Il est conçu pour permettre à un auteur malveillant (ou à un technicien procédant à des tests de pénétration) de se déplacer dans un réseau après avoir réussi à obtenir l'accès. Au reste, Cobalt Strike et Metasploit constituent d'autres exemples de ce type d'outil. Empire peut également servir à générer des documents infectés ainsi que des exécutables qui ont pour objet de créer des accès réseau par l'ingénierie sociale.

Le cadre de PowerShell Empire (Empire) a été légitimement conçu en 2015 en tant qu'outil permettant de procéder à des tests de pénétration. Empire fait office de cadre pour une exploitation continue, à partir du moment où un auteur malveillant a réussi à obtenir l'accès à un système.

L'outil fournit à cet auteur la capacité d'accroitre le degré des privilèges, d'extraire des identifiants, d'exfiltrer de l'information et d'effectuer des mouvements latéraux dans un réseau. Grâce à ces capacités, Empire constitue un puissant outil. Comme il est conçu à partir d'une application légitime courante (PowerShell) et qu'il peut s'exécuter presqu'entièrement dans la mémoire, Empire peut s'avérer difficile à détecter dans un réseau qui a recours à des antivirus traditionnels.

5.1 UTILISATION

Le PowerShell Empire est de plus en plus utilisé par les auteurs malveillants œuvrant pour un État hostile ou pour le crime organisé. Au cours des dernières années, nous avons relevé son utilisation dans des cyberincidents qui ont eu lieu en plusieurs endroits du monde et qui ont touché plusieurs secteurs d'activité.

Les méthodes d'exploitation initiales peuvent varier d'une compromission à une autre, et les auteurs peuvent configurer le cadre Empire en fonction des scénarios d'attaque et des cibles visées.

Dès lors que cette caractéristique est combinée au large éventail des compétences et des visées que l'on retrouve au sein de la collectivité des utilisateurs d'Empire, il y a lieu de conclure que les possibilités de détection varieront grandement selon les contextes. Néanmoins, une compréhension approfondie de l'outil ainsi qu'une sensibilisation aux façons de l'employer constituent une étape importante dans la défense contre les attaques d'auteurs malveillants.

5.2 CAPACITÉS

Empire permet à un auteur malveillant de mener divers types d'attaques contre des ordinateurs et d'exécuter des scripts PowerShell, même lorsque le fichier « powershell.exe » n'est pas présent dans le système visé. Empire dispose d'une architecture souple, et ses communications sont chiffrées.

Il a recours à des modules pour exécuter des fonctions malveillantes plus précises. Ces modules mettent à la disposition des auteurs malveillants un éventail d'options qui favorisent la réussite des attaques menées sur les systèmes ciblés. Au nombre de ces options, notons l'accroissement des privilèges, la collecte d'identifiants, le recensement des hôtes, l'enregistrement des frappes, et le mouvement latéral au sein des réseaux.

En saison de sa convivialité, de sa configuration adaptable et de son aptitude à esquiver les mesures de détection, Empire est un outil de choix pour les auteurs malveillants de tous les niveaux.

5.3 EXEMPLES

Lors d'un incident qui a eu lieu en février 2018, le secteur de l'énergie du Royaume-Uni a été compromis par un auteur inconnu. Cette compromission a été détectée suivant des activités de balisage d'Empire configurées depuis les paramètres du profil par défaut d'Empire. En l'occurrence, il appert que les faibles privilèges d'accès associés au compte ciblé, celui de l'administrateur local, auraient fourni à l'auteur malveillant les accès dont il avait besoin pour commettre son forfait.

Au début de 2018, un auteur inconnu s'est servi de courriels et de fichiers joints malveillants aux couleurs des Jeux olympiques d'hiver dans une campagne d'hameçonnage ciblant des organisations de la Corée du Sud. Cette attaque affichait un degré supplémentaire de sophistication, en raison du recours à Invoke-PSImage, un outil qui encode les scripts PowerShell sous forme d'image.

En décembre 2017, l'auteur malveillant APT 19 a ciblé un cabinet d'avocats multinational au moyen de d'une campagne d'hameçonnage. En l'occurrence, APT 19 s'est servi d'une macros PowerShell obscurcie et incorporée dans un document MS Word généré par Empire.

Nos responsables de la cybersécurité sont également au fait qu'Empire est utilisé pour cibler les établissements d'enseignement. Selon une occurrence qui a été signalée, un auteur a utilisé Empire pour tenter d'obtenir un accès permanent au moyen du consommateur d'événement de l'Infrastructure de gestion Windows (WMI pour *Windows Management Instrumentation*). Dans ce cas, toutefois, l'agent Empire n'est pas parvenu à établir une connexion réseau, car la connexion HTTP était bloquée par une appliance de sécurité locale.

5.4 DÉTECTION ET PROTECTION

L'identification des occurrences malveillantes de PowerShell peut être difficile en raison de l'omniprésence des occurrences légitimes de PowerShell sur les hôtes et de leur utilisation accrue dans la maintenance des environnements organisationnels.

Pour parvenir à identifier les scripts potentiellement malveillants, il faudrait que les activités de PowerShell soient intégralement journalisées. En l'occurrence, il est recommandé de recourir aux blocs de scripts ainsi qu'aux transcriptions PowerShell.

Les plus anciennes versions de PowerShell devraient être supprimées de tout environnement pour veiller à ce qu'elles ne soient pas éventuellement utilisées pour contourner la journalisation et les contrôles, des fonctions ajoutées dans les plus récentes versions de PowerShell. Le blogue de Digital Shadows[9] propose un excellent résumé des pratiques de sécurité liées à PowerShell.
Le composant d'intégrité du code faisant partie des plus récentes versions de Windows peut servir à limiter les fonctionnalités de PowerShell, ce qui permet d'entraver, voire d'empêcher l'exécution des scripts PowerShell en cas d'intrusion.

Une approche multisolution préconisant la signature de code, l'application d'une liste blanche ainsi que le recours au mode de restriction du langage sert à réduire, voire à prévenir l'effet des scripts PowerShell malveillants en cas d'intrusion. Par ailleurs, comme ils ont une incidence sur les scripts légitimes, ces contrôles devraient être l'objet de tests approfondis avant d'être déployés.

Lorsqu'elles mettent en perspective leur usage de PowerShell, les organisations constatent souvent que l'outil n'est utilisé légitimement que par un faible nombre d'employés techniques. Dès lors que l'on peut dresser un portrait de ces activités légitimes, il peut être relativement aisé de surveiller et d'analyser les utilisations malveillantes ou fortuites de PowerShell.

[9] https://www.digitalshadows.com/blog-and-research/powershell-security-best-practices/

6 OUTILS D'OBFUSCATION DE C2 : HTRAN

Il arrive que les auteurs malveillants tentent de cacher le lieu depuis lequel ils tentent de compromettre une cible. Pour ce faire, ils peuvent notamment utiliser des outils génériques de protection des renseignements personnels, TOR entre autres, ou encore des outils spécialisés d'obfuscation du lieu où ils se trouvent.

Le transmetteur de paquets HUC (HTran pour *HUC Packet Transmitter*) est l'un de ces outils de procuration utilisé pour intercepter et rediriger les connexions TCP (*Transmission Control Protocol*) depuis l'hôte local vers un hôte distant. De cette façon, il est possible de dissimuler les communications entre un adversaire et les réseaux ciblés. Cet outil est en libre accès dans l'Internet depuis 2009, au moins.

Ainsi, HTran facilite la connexion TCP entre le système ciblé et un mandataire contrôlé par un auteur malveillant. Les auteurs malveillants peuvent recourir cette technique pour détourner leurs paquets à travers nombre d'hôtes compromis en exécutant HTran de façon à accroître leur accès aux hôtes d'un réseau.

6.1 UTILISATION

On a régulièrement remarqué le recours à HTran dans les réseaux du gouvernement et de l'industrie.

On constate que divers types d'auteurs malveillants utilisent HTran ainsi que d'autres passerelles de connexion dans le but de :

- contourner les systèmes de détection des intrusions installés dans les réseaux;
- se fondre au trafic courant ou tirer parti des relations d'approbation du domaine pour contourner les contrôles de sécurité;
- obscurcir ou cacher l'infrastructure C2 ou les communications;
- créer des infrastructures C2 pair-à-pair ou en maillage pour éviter les mécanismes de détection et fournir des connexions persistantes à l'infrastructure.

6.2 CAPACITÉS

HTran peut s'exécuter dans divers modes, lesquels sont en mesure de réacheminer le trafic au sein d'un réseau en amalgamant deux prises TCP. Ces modes diffèrent les uns des autres selon le lieu d'initiation des prises TCP, à savoir localement ou à distance. Voici les trois modes en question :

- **serveur (écoute)** – les deux prises TCP sont initiées à distance;
- **client (esclave)** – les deux prises TCP sont initiées localement;
- **proxy (tran)** – l'une des prises TCP est initiée à distance et l'autre, localement, dès lors que du trafic provenant de la première connexion a été reçu.

HTran peut s'autoinjecter dans des processus en exécution, puis installer un dissimulateur d'activité (*rootkit*) de façon à cacher les connexions provenant du système d'exploitation hôte. Le recours à ces fonctionnalités provoque également la création de nouvelles entrées dans le registre Windows, permettant ainsi à HTran de garantir un accès permanent au réseau ciblé.

6.3 EXEMPLES

Selon les enquêtes récentes de nos responsables de la cybersécurité, HTran aurait été utilisé pour maintenir et cacher des accès distants aux environnements ciblés.

Dans le cas d'un incident, l'auteur malveillant a réussi à compromettre, du côté de l'Internet, des serveurs Web sur lesquels tournaient des applications Web désuètes et vulnérables. Cet accès a permis le téléversement de scripts WebShell qui ont ensuite servi au déploiement d'outils, notamment HTran.

HTran a été installé dans le répertoire \ProgramData, alors que les autres outils étaient utilisés pour reconfigurer le serveur de façon à ce qu'il accepte les communications employant le protocole Remote Desktop Protocol (RDP).

L'auteur a ensuite lancé une commande visant à démarrer HTran en tant que client, ce qui a permis d'établir, par le port 80, une connexion avec un serveur de l'Internet, lequel réachemine le trafic RDP depuis une interface locale.

Dans ce cas, HTTP a été choisi pour que le trafic se fonde au trafic courant qui était censé provenir du serveur Web pour aller dans l'Internet. Voici d'autres ports couramment utilisés :

- Port 53 – DNS;
- Port 443 - HTTP sur TLS/SSL;
- Port 3306 - MySQL

En utilisant HTran de cette façon, l'auteur malveillant a été en mesure d'utiliser RDP pendant de nombreux mois sans être repéré.

6.4 DÉTECTION ET PROTECTION

Comme les attaquants doivent disposer d'un accès à un ordinateur pour être en mesure d'installer et d'exécuter HTran, les responsables de la défense des réseaux devraient donc installer les correctifs de sécurité et utiliser des mesures adéquates de contrôle des accès pour empêcher l'installation d'applications malveillantes.

La surveillance réseau[10] ainsi que les coupe-feu permettent de détecter et de prévenir les connections non autorisées tentées au moyen d'outils comme HTran.
Dans certains des échantillons analysés, le dissimulateur d'activité de HTran ne cache les renseignements sur les connexions que lorsque le mode « proxy » est utilisé. Lorsque le mode « client » est employé, les responsables de la défense des réseaux sont en mesure de voir les détails ayant trait aux connexions TCP qui sont tentées.

HTran comprend également un mode de débogage qui s'avère utile pour ces responsables. Dès lors qu'une destination ne répond plus, HTran génère un message d'erreur qui se présente comme suit :

```
sprint(buffer, “[SERVER]connection to %s:%d error\r\n”, host, port2);
```

Ce message d'erreur est envoyé en texte clair au client qui tente de se connecter. Les responsables de la protection réseau peuvent tenter de relever la présence de ce message d'erreur pour ainsi détecter, le cas échéant, les occurrences de HTran dans leur environnement.

[10] https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes

7 MESURES GÉNÉRALES DE DÉTECTION ET DE PRÉVENTION

Il existe une série de mesures permettant de renforcer la cybersécurité de l'organisation et de protéger celle-ci contre l'utilisation des outils cités dans le présent rapport. Nous conseillons aux responsables de la protection des réseaux de consulter attentivement l'information se trouvant aux adresses suivantes.

Les 10 mesures de sécurité des TI du CCC https://cyber.gc.ca/fr/top-10-it-security-actions

CCCS Cyber Hygiene https://cyber.gc.ca/fr/orientation/pratiques-exemplaires-en-cybersecurite

Facteurs de cybersécurité à considérer par la direction :
https://cyber.gc.ca/fr/orientation/facteurs-de-cybersecurite-considerer-par-la-direction-conseils-lintention-du

Utiliser une authentification multifactorielle (authentification à deux facteurs ou à deux étapes) pour réduire l'incidence des compromissions de mots de passe. Voir les conseils du CCC :
https://cyber.gc.ca/fr/orientation/guide-sur-lauthentification-des-utilisateurs-dans-les-systemes-de-technologie-de

Protéger les dispositifs et les réseaux en les tenant à jour et à niveau : utiliser les plus récentes versions prises en charge, appliquer les correctifs de sécurité dès qu'ils sont disponibles, utiliser un antivirus et effectuer des balayages régulièrement de façon à contrer les maliciels connus. Voir les conseils du CCC :
https://cyber.gc.ca/fr/orientation/correction-des-systemes-dexploitation-et-des-applications-bulletin-de-securite-des ti

Appliquer les contrôles d'architecture pour la séparation des réseaux. Voir les conseils du CCC :
https://www.cyber.gc.ca/fr/orientation/considerations-de-conception-relatives-au-positionnement-des-services-dans-les-zones

Protéger les interfaces de gestion des systèmes opérationnels essentiels. Plus particulièrement, recourir à l'architecture « Browse-down » pour empêcher les auteurs malveillants d'accéder facilement aux actifs essentiels.

Préparer une capacité de surveillance réseau qui soit apte à collecter les données requises pour analyser les intrusions dans les réseaux.

Mettre à jour/à niveau les systèmes et les logiciels. Veiller à ce que le système d'exploitation et les applications de productivité demeurent à jour/à niveau. Les utilisateurs disposant de licences Office 365 peuvent utiliser la fonction « Démarrer en un clic » pour maintenir leurs applications de bureautique à jour.

Utiliser les systèmes et les logiciels modernes. Ils disposent des meilleurs mécanismes intégrés de sécurité.

Atténuer la capacité des intrus à se déplacer au sein des systèmes et des réseaux. Porter une attention particulière aux éventuels points d'entrée (p. ex. les systèmes de tierces parties qui ont accès au réseau central. À l'occasion d'un incident, désactiver l'accès distant pour les systèmes de tierces-parties, et ce, jusqu'à l'on ait effectivement établi que ces systèmes sont sûrs. Voir les conseils du CCC:
https://cyber.gc.ca/fr/orientation/pratiques-exemplaires-en-matiere-de-cybersecurite-passation-de-marche-avec-des

Utilisation d'une liste blanche des applications. Si l'environnement opérationnel le permet, envisager d'utiliser une liste blanche des applications autorisées. Cette mesure aide à prévenir l'exécution des applications malveillantes. Voir les conseils du CCC : https://cyber.gc.ca/fr/orientation/utilisation-dune-liste-blanche-des-applications-bulletin-de-securite-des-ti-lintention

Gérer les macros avec précaution : Désactiver les macros d'Office, sauf celles d'applications particulières qui sont requises; n'activer que les macros dont les utilisateurs ont régulièrement besoin; et veiller à l'installation des plus récents correctifs pour Office et pour la plateforme sous-jacente.

Utiliser un antivirus. Tenir les logiciels antivirus à jour/à niveau et envisager de recourir à un antivirus infonuagique (cloud-backed) qui permet de faire des économies d'échelle. Veiller à ce que l'antivirus soit en mesure de balayer les macros de MS Office. Voir les conseils du CCC : https://cyber.gc.ca/fr/chaine-de-montage-assemblyline

Défense par couches contre l'hameçonnage. Détecter et mettre en quarantaine les fichiers joints malveillants et les pourriels avant qu'ils ne se rendent aux destinataires. Une défense multicouche réduit considérablement les risques de compromission.

Considérer les utilisateurs comme étant la première ligne de défense. Indiquer au personnel comment signaler les courriels suspects et veiller à ce qu'ils se sentent à l'aise de le faire. Donner suite à leurs signalements sans tarder. Ne jamais sanctionner un utilisateur pour avoir cliqué sur des liens d'hameçonnage ou avoir ouvert un fichiers joint suspect. Voir les conseils du CCC : https://cyber.gc.ca/fr/orientation/reconnaitre-les-courriels-malveillants-itsap00100

Déployer un système de détection d'intrusions au niveau de l'hôte. Divers produits gratuits ou payants sont disponibles pour répondre à divers besoins selon les moyens financiers.

Défendre les systèmes et les réseaux contre les attaques par déni de service. Voir les conseils du CCC : https://www.securitepublique.gc.ca/cnt/rsrcs/cybr-ctr/2012/tr12-001-fr.aspx

Défendre l'organisation contre les rançongiciels. Conserver des copies de sûreté des fichiers importants et les protéger contre les maliciels; ne jamais payer de rançon, puisqu'il n'est pas garanti que les données soient rendues de nouveau accessibles. Voir les conseils du CCC : https://www.securitepublique.gc.ca/cnt/rsrcs/cybr-ctr/2013/in13-004-fr.aspx

Traiter les renseignements personnels adéquatement et en toute sécurité. Voir les conseils du commissaire à la protection de la vie privée : https://www.priv.gc.ca/fr/sujets-lies-la-protection-de-la-vie-privee/loi-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/

Autres publications du CCC : https://cyber.gc.ca/fr/publications

7.1.1 VOIR ÉGALEMENT LES CONSEILS FORMULÉS PAR NOS PARTENAIRES INTERNATIONAUX :

- **ACSC Strategies** https://acsc.gov.au/infosec/mitigationstrategies.htm
- **ACSC Essential Eight** https://acsc.gov.au/publications/protect/essential-eight-explained.htm
- **CERT NZ's critical controls 2018** https://www.cert.govt.nz/it-specialists/critical-controls/
- **CERT NZ's Top 11 cyber security tips for your business** https://www.cert.govt.nz/businesses-and-individuals/guides/cyber-security-your-business/top-11-cyber-security-tips-for-your-business/
- **NCSC NZ Resources** https://www.ncsc.govt.nz/resources/
- **New Zealand Information Security Manual** https://www.gcsb.govt.nz/the-nz-information-security-manual/
- **NCSC-UK's Prevent and detect lateral movement in your organisation's networks** https://www.ncsc.gov.uk/guidance/preventing-lateral-movement
- **NCSC-UK's Protecting your organisation from malware (small business guide)** https://www.ncsc.gov.uk/guidance/protecting-your-organisation-malware

- **NCSC-UK's Preventing malware-based attacks across various scenarios** https://www.ncsc.gov.uk/guidance/mitigating-malware
- **NCSC-UK's Protecting Management Interfaces blog post** https://www.ncsc.gov.uk/blog-post/protect-your-management-interfaces
- **NCSC-UK's Review and refresh your incident management processes** https://www.ncsc.gov.uk/guidance/10-steps-incident-management
- **NCSC-UK's Obsolete Platforms Guidance** https://www.ncsc.gov.uk/guidance/obsolete-platforms-security
- **NCSC-UK's Manage bulk personal datasets** https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-introduction
- **NCCIC Tip: Handling Destructive Malware** https://www.us-cert.gov/ncas/tips/ST13-003
- **NCCIC Tip: Supplementing Passwords** https://www.us-cert.gov/ncas/tips/ST05-012
- **NCCIC Tip: Understanding Patches** https://www.us-cert.gov/ncas/tips/ST04-006
- **NCCIC Tip: Understanding Antivirus** https://www.us-cert.gov/ncas/tips/ST04-005
- **NCCIC Tip: Protecting Your Privacy** https://www.us-cert.gov/ncas/tips/ST04-013