Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Cyberactivité malveillante ciblant les fournisseurs de services gérés en technologie de l'information

POUR LES FOURNISSEURS DE SERVICES GÉRÉS ET LEURS CLIENTS

TLP:WHITE

Canada

1 CONTEXTE

Le Centre canadien pour la cybersécurité (le CCC) sait que des cyberactivités malveillantes continuent de cibler des fournisseurs de services gérés (FSG) en technologie de l'information (TI), et il fournit des avis et conseils aux FSG situés au Canada et aux entreprises canadiennes qui utilisent leurs services.

Depuis au moins le mois de mai 2016, l'auteur de menace responsable a utilisé diverses tactiques, techniques et procédures (TTP) afin de compromettre les réseaux d'un certain nombre de grands fournisseurs de services gérés (FSG) à l'échelle internationale, ce qui lui a permis de mettre la main sur les renseignements sensibles de clients. Ces activités ont touché des FSG et leurs clients partout dans le monde.

Le CCC fait remarquer que cet auteur de menace particulier n'est pas le seul à exploiter des relations de confiance afin de compromettre l'information des victimes, et que les mesures d'atténuation recommandées pour réduire les risques peuvent s'appliquer à d'autres situations.

1.1 QU'EST-CE QU'UN FOURNISSEUR DE SERVICES GÉRÉS (FSG) EN TECHNOLOGIE DE L'INFORMATION (TI)?

Les FSG[1] sont des entreprises qui offrent une gamme de services liés à la gestion de l'information et aux technologies de l'information. Cela comprend l'infrastructure physique, virtuelle ou infonuagique, ainsi que les fournisseurs qui gèrent des données stockées principalement dans un environnement virtuel.

Les organisations font de plus en plus appel aux FSG pour fournir une gamme de services d'infrastructure de TI et de soutien. La décision opérationnelle d'impartir le réseau de soutien informatique et la gestion informatique d'une entreprise peut être une solution de rechange à l'embauche de spécialistes en TI à l'interne ou une façon de permettre à une organisation de se concentrer sur ses opérations commerciales. Du point de vue de la sécurité, les FSG ont le potentiel de réduire les risques qui peuvent résulter du développement de la TI à l'interne dans les entreprises qui ne possèdent pas les ressources ou l'expérience nécessaires pour élaborer des solutions ponctuelles sécurisées.

1.2 POURQUOI LES FSG SONT-ILS CIBLÉS?

Les FSG constituent une proie de choix et de grande valeur aux yeux des auteurs de menace. En effet, les FSG nécessitent généralement un accès étendu à de multiples réseaux de clients afin d'effectuer leur travail de spécialiste en TI. La compromission d'un FSG peut toucher plusieurs clients à l'échelle mondiale et permettre à un auteur de menace d'accéder à plusieurs systèmes clients et à une quantité inestimable de données sensibles, ce qui risque d'entraîner la perte d'information exclusive, de perturber des activités opérationnelles, de causer des pertes financières et de nuire à la réputation de l'organisme touché.

Un auteur de menace réussit à compromettre un FSG en l'infiltrant grâce à divers moyens, comme le déploiement de logiciels malveillants (maliciels) perfectionnés pour un accès à distance. Dans certains cas, le maliciel déployé par un auteur de menace peut lui permettre d'éviter la détection et d'assurer sa persistance sur un réseau touché. Une fois que l'auteur de menace a pris pied dans le réseau du FSG, des outils sont utilisés pour voler des justificatifs d'identité légitimes, y compris ceux de l'administrateur de système. À la suite de l'obtention des justificatifs d'identité de l'administrateur du FSG, il est possible que les maliciels ne soient plus nécessaires, car les outils de gestion de réseau courants auxquels se fient les systèmes clients permettent de mieux dissimuler la

[1] Les fournisseurs de services gérés (FSG) comprennent également les fournisseurs de services infonuagiques (FSI) dans le contexte du présent document.

cyberintrusion. L'auteur de menace pourra alors accéder aux clients qui présentent un intérêt par l'intermédiaire des comptes et des interfaces réseau du FSG. Les données peuvent ensuite être comprimées, mises en lots pour être retirées, et exfiltrées depuis l'infrastructure du FSG ou du client jusqu'à celle de l'auteur de menace. Les clients du FSG dont la posture de sécurité est élevée sont moins susceptibles de remarquer les données acheminées vers un FSG que si elles étaient transmises directement vers Internet. Les clients du FSG dont la posture de sécurité est faible peuvent, quant à eux, être utilisés comme points d'exfiltration.

2 ATTÉNUATION DES MENACES ET CONSEILS

Comme aucune mesure ne saurait protéger et défendre à elle seule un réseau, le CCC recommande d'appliquer des mécanismes et solutions de défense multicouches afin de protéger les réseaux le mieux possible.

Certaines mesures de cybersécurité conventionnelles, comme les coupe-feux, risquent de ne pas être efficaces advenant la compromission d'un FSG. Toutefois, comme des mesures d'atténuation peuvent permettre de contrer les menaces internes ou les risques liés à la compromission des justificatifs d'identité, il convient de les présenter ici.

1. Google a annoncé qu'après la mise en œuvre de l'authentification à deux facteurs pour tous les comptes d'employés, aucune activité d'hameçonnage n'a réussi à toucher ses serveurs d'entreprise[2]. Cela prouve que l'authentification multifactorielle aide à limiter les attaques par hameçonnage, qui sont un vecteur communément utilisé pour installer le maliciel aux fins d'infiltration du réseau. L'authentification multifactorielle empêche également les auteurs de cybermenace d'accéder librement à l'information une fois qu'ils ont accédé aux réseaux, car les justificatifs d'identité stockés qu'un auteur de menace pourrait trouver dans un réseau sécurisé sont inutiles s'ils ne sont pas accompagnés d'au moins un deuxième facteur physique.

    - Bien que l'authentification multifactorielle soit conseillée pour tous les utilisateurs du système, elle l'est particulièrement aux points de connexion du système qui sont accessibles aux FSG et aux employés en télétravail. Les journaux associés à ces serveurs utilisés comme points de connexion doivent être séparés, centralisés et passés en revue régulièrement.

2. Les outils automatisés d'analyse comportementale peuvent établir le profil des habitudes et des besoins relatifs à la TI des employés sur le réseau d'entreprise, détecter les écarts par rapport aux modèles normaux et générer les alertes appropriées. Un logiciel d'analyse comportementale pourrait ainsi identifier les auteurs de menace qui se font passer pour des employés ayant des justificatifs d'identité valides, car leur activité s'écarterait des habitudes d'utilisation des TI de l'employé.
3. Le CCC recommande l'utilisation de solutions de gestion des accès privilégiés qui permettent de contrôler le moment où l'accès aux systèmes clients est accordé et retiré. Il convient de régulièrement passer en revue les journaux afin de valider l'accès aux réseaux des clients par rapport aux tâches autorisées.
4. Veuillez signaler toutes les compromissions soupçonnées dès que possible au CCC à contact@cyber.gc.ca pour obtenir une orientation et des conseils confidentiels.

ORIENTATION ET CONSEILS PRÉCIS VISANT À ATTÉNUER LES RISQUES LIÉS AUX FSG

[2] L'utilisation par Google de l'authentification à deux facteurs reposant sur une clé matérielle a permis de neutraliser l'hameçonnage des employés.
https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing

Voici les mesures que les FSG et leurs clients peuvent prendre de concert afin d'accroître la probabilité de détection et de réduire la probabilité d'une compromission réussie. Le CCC recommande aux FSG et à leurs clients de passer en revue les conseils d'atténuation suivants et d'envisager leur mise en œuvre dans le contexte de leur environnement de réseau.

2.1 POUR LES FOURNISSEURS DE SERVICES GÉRÉS (FSG) EN TI

Les moyens employés par l'auteur de menace – c'est-à-dire l'obtention d'accès à des justificatifs d'identité légitimes dans un réseau pour accéder à des données dans un autre – posent un problème unique pour les fournisseurs de services de confiance. Le CCC recommande à tous les FSG de renforcer leur posture de sécurité dans les domaines ci-dessous afin de réduire les chances de succès de l'auteur de menace en question. On s'attend à ce que la présente annonce génère beaucoup de publicité, ce qui amènera des clients à demander conseil à leurs FSG, qui pourront s'appuyer sur les avis ci-dessous pour orienter ces discussions.

2.1.1 CONTRÔLE DES COMPTES

- Il conviendra de limiter la capacité d'un compte d'administrateur local de se connecter à partir d'une session interactive locale (p. ex., la fonction « Refuser l'accès à cet ordinateur à partir d'un réseau »), et d'interdire l'accès depuis une session prenant en charge le protocole RDP (Remote Desktop Protocol).
- Les employés des FSG qui exercent des fonctions administratives auprès des clients doivent utiliser des mots de passe robustes et uniques pour accéder aux réseaux de chaque client qui relève de leur responsabilité. Les mots de passe doivent être réinitialisés si une compromission est soupçonnée ou avérée et, dans la mesure du possible, être complétés par une authentification multifactorielle.
- Des mécanismes comme les solutions de gestion des accès privilégiés doivent être déployés pour faire en sorte que l'accès aux comptes d'administrateurs et aux comptes des clients soit limité dans le temps, consigné et validé par rapport aux demandes approuvées.

2.1.2 SÉCURITÉ DU RÉSEAU

- Séparer les zones de gestion des clients du FSG pour limiter les mouvements latéraux entre elles.
  - Les paramètres du coupe-feu doivent être révisés et ajustés de façon à contrôler la gestion des connexions figurant sur la liste blanche entre le FSG et le client, entre le client et le FSG, et entre les consoles de gestion du FSG.
- Si un RPV est utilisé pour l'accès au réseau du client, scruter à la loupe ces interfaces afin de déceler toute activité inhabituelle et instaurer une journalisation détaillée.
- Mettre en œuvre la journalisation des serveurs DNS et surveiller les journaux pour déceler les comportements DNS anormaux, particulièrement les domaines des services DNS dynamiques.
- Interdire la gestion à distance sur Internet et l'utilisation de plages d'adresses IP par défaut.
- Fermer automatiquement la session après avoir configuré les routeurs.

2.1.3 GESTION DES POSTES DE TRAVAIL

- Les hôtes dont les compromissions sont confirmées doivent être retirés du réseau aux fins d'analyse judiciaire.
- Le nombre de justificatifs d'identité mis en cache devrait être réduit à un seul dans le cas d'un ordinateur portatif, ou à zéro dans le cas d'un ordinateur de bureau ou d'une immobilisation.
- Les résultats des analyses antivirus doivent être examinés sur une base régulière et continue.
- Des postes de travail de gestion doivent être dédiés à chaque client, que ce soit par la séparation du

matériel ou la virtualisation.

- Dans le cas des postes de travail qui détiennent les justificatifs d'identité de l'administrateur du FSG ou du client, le nombre d'applications Internet devrait être réduit au minimum ou supprimé entièrement, puisque chacune de ces applications représente un vecteur de compromission potentiel.

2.1.4 GESTION DES SERVEURS

- Ne pas utiliser de justificatifs d'identité mis en cache.
- Ne pas utiliser les postes de travail servant à l'administration des serveurs ou des dispositifs d'infrastructure pour un accès général à Internet.

2.2 POUR LES CLIENTS DES FSG

Les clients des FSG doivent s'assurer que des mécanismes de sécurité appropriés ont été choisis pour contrôler l'accès à leurs systèmes, que ce soit pour un employé, un administrateur ou un administrateur du FSG. L'accès à distance doit être accordé avec vigilance, au même titre que l'accès physique aux systèmes et à leurs renseignements sensibles. Le CCC recommande que tous les clients des FSG cherchent à renforcer leur posture de sécurité.

2.2.1 PASSATION D'UN CONTRAT AVEC UN FSG

- Veiller à ce que la solution du FSG satisfasse *par écrit* aux exigences de l'organisation en matière de respect de la loi, de sécurité et de protection des renseignements personnels.
- Demander comment les données sont séparées de celles du FSG et d'autres organisations clientes.
- Demander comment le FSG protège les comptes des administrateurs de réseau qui ont accès à des données exclusives contre l'usurpation d'identité par un auteur de menace.
- Déterminer pendant combien de temps le FSG conserve les journaux des activités, le niveau de détail de ces journaux, la façon dont ils sont protégés et s'ils sont centralisés.
- Demander quelles notifications le FSG fournira en cas de compromission de ses systèmes et, en particulier, des justificatifs d'identité administratifs.
- Demander quelles pratiques de gestion des correctifs le FSG adoptera afin de réduire au minimum les vulnérabilités.
- Établir des voies de communication distinctes des réseaux d'entreprise, qui seront utilisées en cas de compromission des réseaux de l'organisation ou du FSG.

2.2.2 CONTRÔLE DE L'ACCÈS DU FSG

- Éviter de fournir au FSG les justificatifs d'identité des comptes et l'accès aux systèmes sensibles qui ne relèvent pas de leurs responsabilités.
- Envisager la mise en œuvre d'une authentification multifactorielle (p. ex., jetons de sécurité pour l'accès à distance à tout dépôt de données sensibles) et d'une politique de mots de passe sûrs à l'échelle de l'organisation, en commençant par les comptes d'administrateurs et privilégiés.
- Envisager d'atténuer l'exploitation potentielle en surveillant les résultats de l'analyse des vulnérabilités et en suivant un cycle de correctifs prioritaire et réactif pour appliquer les plus récents correctifs à l'ensemble des systèmes d'exploitation, des applications, des logiciels et des logiciels tiers.
- Envisager de réduire et de surveiller le nombre de comptes d'administrateurs de domaine et d'entreprise.

- Surveiller régulièrement les résultats d'analyse antivirus et d'autres journaux réseau en vue d'y relever toute activité suspecte.
- Utiliser un plan de sauvegarde et de récupération des données pour tous les renseignements essentiels.

2.3 AUTRES CONSIDÉRATIONS

Avant de faire affaire avec un FSG, il convient de prendre en considération d'autres éléments qui ne se rattachent pas directement à la compromission dont traite le présent document :

- Tenir compte de facteurs comme le propriétaire des données, l'endroit où les données sont stockées, la méthode de sauvegarde ainsi que les mesures de sécurité en place.
- Envisager de demander à tout fournisseur de services dans quelle mesure il adhère à un cadre de gestion de la sécurité des TI. Se reporter au document du CCC intitulé *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (ITSG-33).
- Utiliser des contrôles cryptographiques pour protéger les données en transit entre l'organisation cliente et le fournisseur.

3 RESSOURCES

Pour obtenir une liste plus détaillée de conseils et de pratiques exemplaires, et pour obtenir de plus amples renseignements, veuillez consulter les documents suivants publiés par le CCC (sous la responsabilité du CCRIC) et nos partenaires internationaux.

Pratiques exemplaires en matière de cybersécurité : Passation de marché avec des fournisseurs de services gérés (IN-17-003)

https://cyber.gc.ca/fr/orientation/pratiques-exemplaires-en-matiere-de-cybersecurite-passation-de-marche-avec-des

Cyberactivité malveillante ciblant les fournisseurs de services gérés (AL17-004)

https://cyber.gc.ca/fr/avis/cyberactivite-malveillante-ciblant-les-fournisseurs-de-services-geres

Utiliser les mots de passe

https://www.pensezcybersecurite.gc.ca/cnt/prtct-yrslf/prtctn-dntty/usng-psswrds-fr.aspx

Guide Pensez cybersécurité pour les petites et moyennes entreprises

https://www.pensezcybersecurite.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-fr.aspx

La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie (ITSG-33) du CCC

https://cyber.gc.ca/fr/orientation/la-gestion-des-risques-lies-la-securite-des-ti-une-methode-axee-sur-le-cycle-de-vie

NCCIC – Advanced Persistent Threat Activity Exploiting Managed Service Providers (TA18-276B)

https://www.us-cert.gov/ncas/alerts/TA18-276B