Gouvernement du Canada | Government of Canada

Bulletin sur les cybermenaces : Le CCC exhorte les exploitants des infrastructures essentielles du Canada à prendre conscience des activités de cybermenace connues qui sont parrainées par la Russie et à prendre des mesures d'atténuation contre celles-ci

De : Centre canadien pour la cybersécurité

Le Centre canadien pour la cybersécurité encourage la communauté canadienne de la cybersécurité, surtout les responsables de la défense des réseaux des IE, à prendre conscience des activités de cybermenace parrainées par l'État russe et à se protéger contre elles. Il se joint à ses partenaires des États Unis (en anglais seulement) et du Royaume Uni (en anglais seulement) et recommande des mesures proactives de surveillance et d'atténuation sur les réseaux.

Le Centre canadien pour la cybersécurité, qui fait partie du Centre de la sécurité des télécommunications, sait que des activités étrangères de cybermenace, notamment menées par des auteurs parrainés par la Russie, ciblent les opérateurs des réseaux des IE du Canada ainsi que

leur technologie opérationnelle (TO) et leur technologie de l'information (TI). L'avis publié par les partenaires américains attire l'attention sur les vulnérabilités que les auteurs de cybermenace russes ont déjà exploitées ainsi que sur les tactiques, techniques et procédures (TTP) qu'ils utilisent.

Le Centre canadien pour la cybersécurité exhorte les responsables de la défense des réseaux des IE du Canada :

- À se préparer à isoler des composants et des services d'IE d'Internet et des réseaux organisationnels et internes si un auteur de menace malveillant pouvait être tenté de les perturber. Lorsqu'ils utilisent des systèmes de contrôle industriels ou une technologie opérationnelle, tester les contrôles manuels pour veiller à ce que les fonctions essentielles soient toujours fonctionnelles advenant l'indisponibilité ou la compromission du réseau de l'organisation.
- À intensifier la vigilance organisationnelle. Surveiller leurs réseaux en accordant une attention particulière aux TTP figurant dans l'avis du CISA (en anglais seulement). Veiller à ce que le personnel chargé de la cybersécurité et des TI soit en mesure de repérer et d'évaluer rapidement tout comportement inattendu ou inhabituel sur le réseau. Activer la journalisation pour faciliter les enquêtes sur les problèmes et les événements.
- À améliorer leur posture de sécurité : Appliquer les correctifs aux systèmes, particulièrement ceux pour les vulnérabilités figurant dans l'avis du CISA (en anglais seulement), et permettre la journalisation et les sauvegardes. Activer la surveillance du réseau et des points terminaux (p. ex., logiciel antivirus) et recourir à l'authentification multifacteur, le cas échéant. Créer des sauvegardes hors ligne et les mettre à l'essai.
- À se doter d'un plan d'intervention en cas de cyberincident, d'un

plan de continuité des activités et d'un plan de communication, et se préparer à les appliquer.
- À informer le Centre canadien pour la cybersécurité de toute activité suspecte ou malveillante.

Consultez les ressources en ligne ci-dessous pour obtenir de l'information supplémentaire et des avis et conseils utiles :

Détection et atténuation de la menace :

- Destructive malware targeting Ukrainian organizations. Microsoft Threat Intelligence Center (MSTIC). 15 janvier 2022
- Bulletin de cybersécurité conjoint : Approches techniques à la détection et à l'atténuation des activités malveillantes
- Sécurisez vos comptes et vos dispositifs avec une authentification multifacteur (ITSAP.30.030)
- Facteurs à considérer en matière de cybersécurité pour votre site Web (ITSM.60.005)
- Facteurs relatifs à la sécurité à considérer pour les systèmes de contrôle industriels (ITSAP.00.050)
- Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information (ITSM.10.089)
- Correction des systèmes d'exploitation et des applications - Bulletin de sécurité des TI à l'intention du gouvernement du Canada (ITSB-96)

Évaluation des menaces :

- Évaluation des cybermenaces nationales 2020
- Bulletin sur les cybermenaces : Les cybermenaces visant les technologies opérationnelles
- Bulletin sur les cybermenaces : Les cyberattaques visant le secteur canadien de l'électricité

Planification :

- Guide de Sécurité publique Canada
- Guide sur les rançongiciels (ITSM.00.099)

Pour obtenir d'autres conseils et avis utiles, consultez la section Information et conseils de notre site Web ou abonnez-vous à nos comptes de réseaux sociaux.

Veuillez communiquer avec nous pour obtenir de plus amples avis et conseils ou pour signaler un incident.

Courriel : contact@cyber.gc.ca
Sans frais : 1-833-CYBER-88 (1-833-292-3788)

Date de modification :
2022-01-26