Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Cybermenaces contre le secteur pétrolier et gazier du Canada

Canada

À propos du présent document

Auditoire

Le rapport fait partie d'une série d'évaluations des cybermenaces portant sur des recommandations relatives aux cybermenaces susceptibles de cibler les infrastructures essentielles du Canada. Il s'adresse aux dirigeantes et dirigeants du secteur pétrolier et gazier, aux professionnelles et professionnels de la cybersécurité devant protéger des actifs pétroliers et gaziers et aux lectrices et lecteurs non spécialisés qui s'intéressent à la cybersécurité des infrastructures essentielles. Pour des conseils sur des mesures techniques pour atténuer ces menaces, consultez la section *Ressources utiles* à la fin de cette présentation et/ou communiquez avec le Centre canadien pour la cybersécurité (Centre pour la cybersécurité).

Les sources peuvent utiliser l'appellation TLP:CLEAR lorsque les informations présentent un risque minimal ou nul de mauvaise utilisation, conformément aux règles et procédures applicables à la diffusion publique. Sous réserve des règles standard de copyright, les informations mentionnées en TLP:CLEAR peuvent être partagées sans restriction. Pour en savoir plus, consultez le lien suivant : Traffic Light Protocol.

Coordonnées

Prière de transmettre toute question ou tout enjeu relatif au présent document au Centre canadien pour la cybersécurité à contact@cyber.gc.ca.

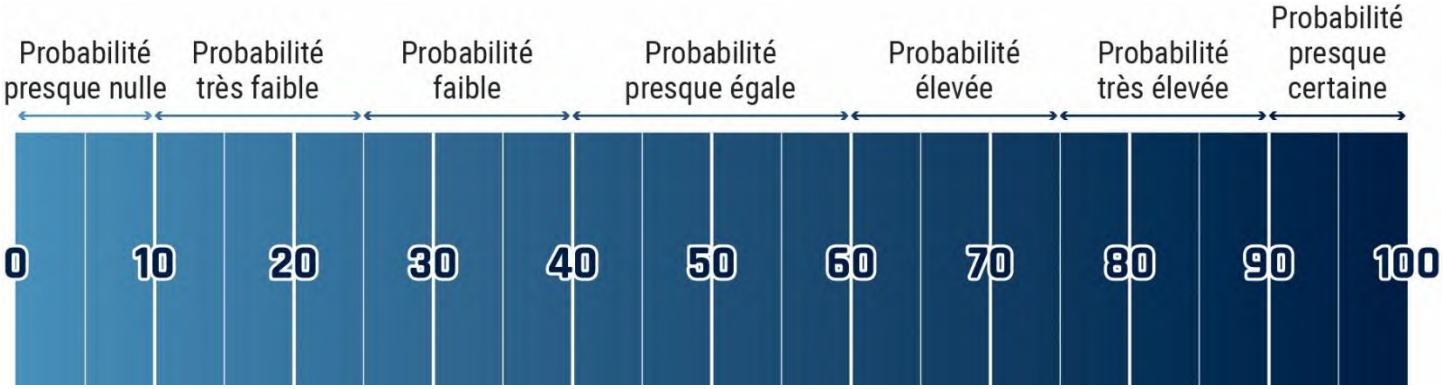
Méthodologie et fondement de l'évaluation

Les avis formulés dans la présente évaluation se basent sur de multiples sources classifiées et non classifiées. Ils sont fondés sur les connaissances et l'expertise en matière de cybersécurité du Centre pour la cybersécurité. Le rôle que joue le Centre pour la cybersécurité dans la protection des systèmes d'information du gouvernement du Canada lui confère une perspective unique des tendances observées dans un contexte de cybermenace, ce qui a contribué à la présente évaluation. Dans le cadre du volet du mandat du Centre de la sécurité des télécommunications touchant le renseignement étranger, le Centre pour la cybersécurité tire parti d'information précieuse sur les habitudes des adversaires dans le cyberespace. Bien que le Centre pour la cybersécurité soit toujours tenu de protéger les sources et méthodes classifiées, il fournira au lecteur, dans la mesure du possible, les justifications qui ont motivé ses avis.

Les avis du Centre pour la cybersécurité sont basés sur un processus d'analyse qui comprend l'évaluation de la qualité de l'information disponible, l'étude de différentes explications, l'atténuation des biais et l'usage d'un langage probabiliste. On emploiera des termes tels que « nous estimons que » ou « selon nos observations » pour communiquer les évaluations analytiques. On utilisera des qualificatifs comme « probabilité presque nulle », « probabilité faible » et « probabilité très élevée » pour exprimer les probabilités.

Les évaluations et analyses énoncées dans le présent document sont fondées sur des renseignements disponibles en date du 31 mars 2023.

Lexique des estimations



Cybermenaces contre le secteur pétrolier et gazier du Canada

Principaux avis

- Nous sommes d'avis que la probabilité est presque certaine que les activités de cybercriminalité motivées par le gain financier, plus particulièrement la compromission de courriel d'affaires et les rançongiciels, sont la principale cybermenace ciblant le secteur pétrolier et gazier. La probabilité est presque certaine que les rançongiciels sont la principale cybermenace pouvant affecter la fiabilité de l'approvisionnement en pétrole et en gaz pour les Canadiennes et Canadiens.
- Nous estimons que la probabilité est très élevée que le secteur pétrolier et gazier au Canada continue d'être ciblé par du cyberespionnage parrainé par des États à des fins commerciales ou économiques. Les secrets commerciaux exclusifs, la recherche, et les plans d'affaires et de production sont également à risque.
- Étant donné que le secteur pétrolier et gazier fait partie des infrastructures essentielles, nous estimons que la probabilité est très élevée que ce secteur constitue une cible stratégique pour les cyberactivités parrainées par des États pour faire acte de force étatique, surtout en période de tensions géopolitiques. Nous jugeons que la probabilité est très élevée que la principale cible des auteurs de cybermenace parrainés par des États soit les réseaux de technologie opérationnelle (TO) qui surveillent et contrôlent les plus importants actifs industriels du secteur. La probabilité est presque certaine que ces auteurs de menace parrainés par des États sont en train d'améliorer leurs capacités de sabotage des TO dans les infrastructures essentielles. Nous estimons que la probabilité est très faible que des auteurs de menace parrainés par des États veuillent intentionnellement perturber ou endommager l'infrastructure pétrolière et gazière au Canada en l'absence d'hostilités.
- Nous croyons également que les cibles les plus probables pour les auteurs de cybermenace cherchant à perturber l'approvisionnement en gaz et en pétrole au Canada sont les goulots d'étranglement pour ce qui est de la transmission du pétrole et des étapes de transformation. Parmi les cibles potentielles, nous notons les réseaux d'entreprises et de TO de pipelines de grand diamètre, les terminaux de transfert et les principales installations de raffinage.
- La Russie a manifesté à de nombreuses reprises son intention de démontrer sa puissance en lançant des cyberattaques destructrices contre les infrastructures essentielles stratégiques de ses adversaires à mesure que s'intensifient les crises géopolitiques. Le Centre pour la cybersécurité est au courant des efforts déployés par des auteurs de menace parrainés par la Russie pour compromettre les réseaux des fournisseurs d'infrastructures essentielles du Canada et des États-Unis et d'y établir une présence permanente (en vue de se prépositionner). Les organisations ciblées incluent des organisations du secteur pétrolier et gazier. Nous estimons que la probabilité est très élevée que l'espionnage russe, dont l'objectif est de se prépositionner dans les réseaux de TO, se poursuive.
- Nous croyons également que la probabilité est presque certaine que les auteurs de cybermenace parrainés par des États améliorent sans cesse leurs capacités leur permettant de mener des cyberactivités destructrices et débilitantes contre les infrastructures essentielles (IE). Ils collaborent également parfois avec des groupes d'auteurs de menace non étatiques afin d'accroître leur force de frappe, d'améliorer leurs capacités pour ainsi éviter une attribution directe. Le Centre pour la cybersécurité est conscient que la pratique bien établie de la Russie a été de collaborer avec des auteurs non étatiques pour mener des activités de cybermenace contre les infrastructures essentielles de l'Ukraine et de ses alliés.
- Nous estimons qu'il y a une probabilité presque égale que l'infrastructure pétrolière et gazière du Canada puisse être touchée par des cyberactivités contre des actifs américains, en raison de l'intégration transfrontalière.

Cybermenaces contre le secteur pétrolier et gazier du Canada

Introduction

Le secteur pétrolier et gazier apporte une contribution essentielle à l'économie canadienne et à la sécurité et au bien-être des Canadiennes et Canadiens. Ainsi, la cybersécurité de ce secteur est importante pour la sécurité nationale du Canada. Le secteur pétrolier et gazier emploie environ 600 000 Canadiennes et Canadiens et il ajoute 120 milliards de dollars à l'économie canadienne, soit 5 % du produit intérieur brut (PIB).[1] Au Canada, le pétrole et le gaz sont utilisés pour fournir l'énergie nécessaire pour chauffer des bâtiments, transporter des personnes et des marchandises, et ensemencer les champs et faire les récoltes. Ils servent également de matières premières pour de nombreux autres produits de fabrication.

Il est difficile d'exagérer l'importance du secteur pétrolier et gazier pour la sécurité nationale puisque la majorité de nos infrastructures essentielles dépendent des produits pétroliers et gaziers pour fonctionner. En même temps, les infrastructures essentielles, et plus particulièrement le secteur de l'énergie, sont de plus en plus à risque d'être visées par des activités de cybermenace.[2] Aux États-Unis, par exemple, Colonial Pipeline a attiré l'attention du monde entier en mai 2021 lorsque l'oléoduc a été forcé d'arrêter les opérations d'un des plus importants réseaux de pipelines (essence, diesel et carburéacteur) des États-Unis, à la suite d'une attaque par rançongiciel. Bien que les opérations ont pu être rétablies quelques jours plus tard, la perturbation de l'approvisionnement en carburant a quand même entraîné des pénuries causant le réacheminement de vols, une fièvre d'achat et une hausse des prix à court terme. Selon les estimations, au moment de la remise en service du pipeline, l'est des États-Unis n'était qu'à quelques jours de subir des pénuries alimentaires ainsi que d'autres pénuries en raison de la perturbation de l'approvisionnement en essence vers d'autres secteurs, comme celui du transport.[3]

Une introduction au secteur pétrolier et gazier

Les organisations qui participent directement au secteur pétrolier et gazier peuvent être divisées en trois catégories :

1. Secteur amont : les organisations participant à l'exploration, l'extraction et la production
2. Secteur intermédiaire : pipelines, transport et stockage
3. Secteur aval : raffinage, distribution et vente

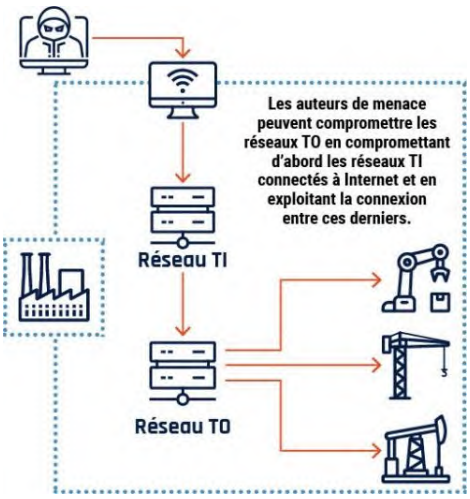
Les organisations du secteur pétrolier et gazier en amont participent à la découverte et à l'extraction de pétrole brut et de gaz naturel issus de dépôts naturels. Les activités commencent par une recherche et une planification environnementale et géographique; suivent ensuite les activités de forage et d'exploitation de puits de pétrole et de gaz, et l'exploitation des sables pétrolifères.

Les activités intermédiaires comprennent le stockage, le traitement et le transport des produits pétroliers et gaziers. Le transport du pétrole et du gaz se fait par pipeline, train, camion et navire pétrolier. Un pipeline est le principal moyen de distribution intermédiaire pour acheminer les produits pétroliers et gaziers des producteurs jusqu'aux consommateurs en Amérique du Nord. Le Canada s'étend d'est en ouest sur une distance d'environ 7 500 km. Dans cette étendue se trouvent environ 850 000 km de pipelines de collecte, d'alimentation, de transport et de distribution pour les produits pétroliers et gaziers. Cela comprend un peu moins de 120 000 km de pipelines de transport de grand diamètre utilisés pour distribuer d'importants volumes de pétrole et de gaz sur de longues distances, souvent entre les provinces ou dans d'autres pays.[4] De vastes installations de stockage sont reliées au réseau de pipelines pour faire face aux changements relatifs à l'offre et à la demande pour ainsi assurer une utilisation efficace des pipelines. En général, le gaz naturel est entreposé dans un grand réservoir souterrain. Des réservoirs hors sol sont utilisés pour le pétrole brut et le pétrole raffiné, les produits pétroliers finaux et le gaz naturel.

Les activités d'aval du secteur pétrolier et gazier sont responsables du raffinage du pétrole brut et du gaz naturel brut pour obtenir des produits finaux. Ce sont aussi les activités desquelles découlent la distribution et la vente de produits pétroliers et gaziers à la clientèle. Il est ici question de raffineries et d'usines de produits chimiques, ainsi que d'entreprises de distribution et de détail.

L'exposition aux cybermenaces

Les organisations pétrolières et gazières ont tendance à avoir une vaste zone d'attaque des systèmes numériques connectés. Ces systèmes pourraient inclure des systèmes de technologies de l'information (TI) organisationnels, des actifs de technologies opérationnelles (TO) industriels et un Web connecté de fournisseurs de produits et de services numériques. Comme nous l'avons mentionné dans l'Évaluation des cybermenaces nationales 2020, plus une organisation possède des actifs connectés à Internet, plus elle est à risque d'être visée par des cybermenaces.[5] En 2019, des données d'enquête de Statistiques Canada ont montré qu'environ 25 % de toutes les organisations canadiennes du secteur pétrolier et gazier ont signalé un cyberincident[6], ce qui représente le pourcentage le plus élevé parmi tous les secteurs des infrastructures essentielles.



Comme pratiquement toutes les industries à travers le monde, le secteur pétrolier et gazier a adopté la transformation numérique de ses TO dans la production, le transport et la distribution de ses produits. La transformation numérique des TO du secteur de l'énergie offre de nombreux avantages sur le plan de la gestion, du rendement et de la productivité. Par exemple, elle permet aux organisations de surveiller et de gérer de façon centralisée les dispositifs de TO qui pourraient être répartis sur de vastes territoires. Le Centre pour la cybersécurité estime qu'il y a une probabilité presque certaine que la transformation numérique des actifs de TO augmente la zone d'attaque des vulnérabilités qui se présente aux auteurs de cybermenace et qu'elle expose les actifs de TO du secteur pétrolier et gazier à des cybermenaces.[7]

Cybermenaces émanant de la chaîne d'approvisionnement numérique

Nous jugeons que la probabilité est élevée que les auteurs de cybermenace utilisant des méthodes moyennement ou grandement sophistiquées risquent de plus en plus de faire appel au ciblage indirect des organisations, en se tournant plutôt vers la chaîne d'approvisionnement.[8] Les auteurs de cybermenace ciblent la chaîne d'approvisionnement pour deux objectifs principaux : obtenir de la part des fournisseurs de la propriété intellectuelle et de l'information sur les TO ou les réseaux de l'organisation ciblée ayant une valeur de revente; et s'en servir comme moyen indirect pour obtenir l'accès à un des réseaux de l'organisation ciblée.[9] Les exploitants d'actifs industriels substantiels, y compris ceux du secteur pétrolier et gazier, dépendent d'une chaîne d'approvisionnement de produits et de services très variés, qui comprend des laboratoires, des fabricants, des fournisseurs, des intégrateurs et des entrepreneurs, de même que des fournisseurs de services gérés, Internet et infonuagiques, pour les opérations quotidiennes, la maintenance, la modernisation et le développement de nouvelles capacités. La dépendance des exploitants d'actifs de TO du secteur pétrolier et gazier à l'égard de la chaîne d'approvisionnement représente une vulnérabilité critique qui fournit aux auteurs de cybermenace de l'information privilégiée sur les systèmes de TI et de TO autrement protégés et des occasions de les infiltrer. Nous estimons que la probabilité est presque certaine que les auteurs utilisant des méthodes moyennement ou grandement sophistiquées continueront de cibler la chaîne d'approvisionnement à ces fins pendant au moins les 12 prochains mois.

La menace provenant d'une prolifération de cyberoutils

Le Centre pour la cybersécurité a remarqué que les cyberoutils préfabriqués et la formation pour utiliser ceux-ci sont de plus en plus répandus sur Internet. Selon nos observations, il existe une probabilité presque égale que les auteurs de menace disposant de moyens peu sophistiqués se tournent vers ces outils pour mener à bien une attaque de sabotage et perturber le secteur pétrolier et gazier.

À titre d'exemple, il existe également des modules d'exploitation des TO dans des cyberoutils offerts gratuitement, comme le cadre de source ouverte Metasploit qui a été développé et diffusé par des chercheuses et chercheurs et des professionnelles et professionnels dans le domaine de la sécurité pour tester la défense des réseaux de TO. Tous les auteurs malveillants, peu importe leur niveau de compétence technique, ont accès à ces outils ainsi qu'à des documents et tutoriels sur leur utilisation.[10] Le Centre pour la cybersécurité est aussi au courant de l'existence de logiciels criminels ayant un impact important, y compris Trickbot, Qakbot et Dridex, qui utilisent le cyberoutil répandu Cobalt Strike pour cibler de grandes organisations et les infrastructures essentielles du Canada. Metasploit et Cobalt Strike sont tous deux populaires auprès des États et des groupes criminels pour faciliter les activités de rançongiciel et de cyberespionnage.[11] Par ailleurs, la présence d'un vaste marché illégal offrant des cyberoutils et des services qui permettent aux cybercriminelles et cybercriminels (et potentiellement à d'autres auteurs de cybermenace) de réduire considérablement leur temps de préparation et de mener des campagnes plus complexes et sophistiquées. De nombreuses places de marché virtuelles permettent à des fournisseurs de vendre des cyberoutils et services spécialisés à des utilisateurs qui les emploient ensuite pour commettre des cybercrimes, dont de l'espionnage, des attaques par déni de service distribué (DDoS pour *Distributed Denial-of-Service*) et des attaques par rançongiciel.

De même, les auteurs malveillants peuvent se servir de l'une ou l'autre de ces cybercapacités pour commettre des actes de sabotage contre des systèmes TO.

Selon notre évaluation, la probabilité est élevée que la grande disponibilité de cybercapacités et de services criminels, commerciaux, volés et gratuits abaisse le degré de sophistication requis pour cibler et saboter les TO. Dans l'Évaluation des cybermenaces nationales 2020, le Centre pour la cybersécurité a observé que la croissance des marchés commerciaux pour les cyberoutils et les talents a permis de réduire le temps nécessaire aux auteurs de menace pour développer des cybercapacités. Certains fournisseurs conçoivent des capacités spécifiquement pour les TO et les vendent à des clientes et clients. Alors que de plus en plus d'auteurs de cybermenace accèdent à des cyberoutils commerciaux, les auteurs de menace qui souhaitent saboter des TO, mais qui ne disposaient pas des capacités nécessaires pour le faire auparavant, peuvent maintenant tenter plus facilement ce type de cybermenace. La prolifération d'outils commerciaux fait en sorte qu'il est de plus en plus difficile de détecter ces activités de cybermenace, de déterminer qui en sont les auteurs et de se défendre contre celles-ci. Nous estimons que **même si les menaces visant le secteur pétrolier et gazier et menées par d'autres auteurs de cybermenace sont actuellement faibles, la probabilité est élevée que le niveau inégal de cybersécurité de certains dispositifs de TO, l'accessibilité générale des dispositifs sur Internet par le biais de moteurs de recherche propres aux TO et la disponibilité de cyberoutils gratuits, contribueront probablement à faire augmenter, dans un avenir proche, la menace émanant d'auteurs de cybermenace disposant de moyens peu sophistiqués.**

La menace émanant de la cybercriminalité

Nous estimons que la probabilité est presque certaine que les cybercriminelles et cybercriminels, motivés par un gain financier, plus particulièrement ceux qui tentent la compromission de courriel d'affaires et le recours aux rançongiciels, soient la principale cybermenace ciblant le secteur pétrolier et gazier. Bien que la probabilité est presque certaine que la compromission de courriel d'affaires soit plus courante et plus onéreuse que le rançongiciel pour les victimes**, nous estimons que la probabilité est presque certaine que les rançongiciels soient la principale menace visant l'approvisionnement en pétrole et en gaz pour la clientèle.** L'écosystème de cybercriminalité clandestin évolue constamment afin de maximiser les profits et d'augmenter les paiements extorqués aux victimes.[12] Par exemple, l'adaptation de rançongiciel à un modèle de service (rançongiciel comme service, ou RaaS) et le recours répandu au vol et à la fuite de données sensibles pour accroître la pression à payer sont deux des principaux facteurs contribuant à la récente augmentation du taux de réussite des incidents.[13]

Le secteur pétrolier et gazier, tout comme d'autres parties du secteur de l'énergie, attire apparemment l'attention d'auteurs de cybermenace motivés par des gains financiers en raison de la valeur élevée des actifs de l'industrie et du niveau de dépendance de la clientèle aux produits de l'industrie.[14] Parmi les actifs de valeur du secteur pétrolier et gazier ciblés par des cybercriminelles et cybercriminels, nous notons la propriété intellectuelle et les plans d'affaires ainsi que les dépôts de renseignements sur la clientèle.

Étant donné que les organisations pétrolières et gazières font partie des infrastructures essentielles (IE) canadiennes, elles sont des cibles intéressantes pour l'extorsion en raison de l'importance de ces produits et services pour les Canadiennes et Canadiens. Les cyberactivités criminelles sont susceptibles de perturber les opérations et la prestation de produits et de services essentiels en limitant l'accès d'une entreprise à des données commerciales essentielles dans le réseau TI ou en empêchant le contrôle sûr des processus industriels dans le réseau de technologies opérationnelles (TO). L'interruption ou le sabotage des systèmes TO dans les infrastructures essentielles canadiennes représente une menace coûteuse pour les propriétaires et exploitants d'importants actifs TO, et pourrait compromettre la sécurité nationale, publique et environnementale, de même que l'économie.

Au début de mai 2021, par exemple, Colonial Pipeline a été victime d'un incident attribuable à DarkSide, groupe de cybercriminelles et cybercriminels basé en Russie qui est à l'origine des rançongiciels. Bien que l'activité n'aurait touché que les systèmes TI, l'entreprise a choisi d'interrompre ses activités, ce qui a engendré une hausse record des prix, des achats dictés par la panique et une pénurie d'essence. Par la suite, on a signalé que le Service fédéral de sécurité (ou FSB) de la Russie a mené des enquêtes sur des membres du groupe qui seraient responsables de l'incident Colonial et les a fait arrêter à la demande de représentantes et représentants américains.[15]

La probabilité est élevée que la haute visibilité de l'incident Colonial et les résultats mis en évidence par les organismes d'application de la loi aient incité certains groupes à faire des déclarations publiques précisant que les cibles avaient été modifiées pour ainsi épargner des infrastructures essentielles, et demandant dans des forums sur la criminalité d'interdire complètement les rançongiciels.[16] Toutefois, de telles déclarations concernant le secteur de la santé n'ont pas permis de diminuer l'ensemble du ciblage.[17] Nous estimons que la probabilité est élevée que ces déclarations ne sont qu'un prétexte et que cela ne permettra pas de diminuer de manière substantielle la menace qui pèse sur les organisations pétrolières et gazières à long terme.

Les cybercriminelles et cybercriminels sont opportunistes et ils n'hésiteront pas à exacerber des situations de crise à des fins lucratives. À la fin du mois de janvier 2022, par exemple, des incidents à deux filiales de l'entreprise allemande de transport de pétrole Marquard & Bahls ainsi qu'un incident non lié de rançongiciel aux ports de pétrole Amsterdam-Rotterdam-Antwerp (ARA) ont perturbé considérablement la livraison des produits pétroliers dans certains pays d'Europe continentale, aggravant ainsi potentiellement la crise énergétique causée

par l'invasion, alors imminente, de l'Ukraine par la Russie.[18] **Nous estimons que la probabilité est presque certaine que des cybercriminelles et cybercriminels continueront à cibler des organisations de grande valeur œuvrant dans le secteur pétrolier et gazier du Canada et partout dans le monde.**

Cybermenaces visant le secteur pétrolier et gazier parrainées par un État

Les activités de cybermenace parrainées par des États contre le secteur pétrolier et gazier sont devenues une réalité courante d'activités de cybermenace à l'échelle mondiale, plus particulièrement en période de tensions géopolitiques croissantes.[19] Des auteurs de cybermenace parrainés par des États et motivés par des enjeux politiques, dont la Russie, la Chine et l'Iran, ont ciblé le secteur de l'énergie mondial à des fins d'espionnage, de perturbation et de destruction. En général, les auteurs de menace parrainés par des États mènent des activités d'espionnage sur des cibles du secteur pétrolier et gazier pour obtenir du renseignement étranger (soutirer des données sur le secteur pétrolier et gazier ayant une valeur économique ou une valeur en tant que renseignement sur les relations étrangères) ou pour des raisons commerciales (obtenir des plans d'affaires ou une propriété intellectuelle de valeur à déployer pour acquérir un avantage concurrentiel national). Nous estimons que la probabilité est presque certaine que des auteurs de cybermenace parrainés par des États sont les auteurs de menace dotés des moyens les plus sophistiqués, et la probabilité est très élevée que certains d'entre eux aient les capacités nécessaires pour lancer des attaques coordonnées et cibler plus d'un composant des infrastructures essentielles à la fois. De plus, les auteurs de cybermenace parrainés par des États utilisent diverses tactiques pour travailler clandestinement; ce qui rend difficiles de détecter les activités et de déterminer qui est l'auteur de ces activités.

Espionnage industriel

Nous estimons que la probabilité est très élevée que le secteur pétrolier et gazier au Canada continue d'être ciblé par des États à des fins commerciales ou économiques. Cela peut comprendre des organisations à n'importe quel niveau de la chaîne de valeur du secteur pétrolier et gazier. Parmi les actifs numériques du secteur pétrolier et gazier qui ont de la valeur pour des États adversaires, nous notons les secrets commerciaux exclusifs, la recherche, les données sur la clientèle ainsi que les plans d'affaires et de production des organisations. Parmi ces actifs, nous notons également les plans de mise en valeur de champ pétrolier, ou la recherche et le développement d'équipements ou de techniques qui, s'ils sont volés, pourraient entraîner des désavantages concurrentiels en raison des pertes d'investissements, des pertes de revenus et des réputations entachées. Par exemple, en 2020, le service de contre-ingérence de la Norvège a indiqué que la Russie, la Chine et d'autres pays ont eu recours au cyberespionnage pour découvrir des secrets commerciaux de l'industrie pétrolière et des plans de production.[20]

Prépositionnement et développement des capacités

Le Centre pour la cybersécurité estime que les infrastructures essentielles, et surtout les TO connectées à un réseau dans les infrastructures essentielles, représentent des cibles stratégiques de perturbation ou de destruction pour les auteurs de cybermenace parrainés par des États en temps d'hostilités entre des pays.[21] Les gouvernements ainsi que les secteurs de l'énergie, de l'aqueduc, des télécommunications et des finances ont tous été ciblés en raison de tensions géopolitiques. Des cyberactivités offensives contre les TO du secteur pétrolier et gazier visant à empêcher l'approvisionnement en produits essentiels d'un pays ciblé pourraient servir à envoyer des messages intimidants sur la puissance et les capacités, à délégitimiser les gouvernements ciblés, à démoraliser les dirigeantes et dirigeants et le public, à éroder les défenses et à menacer la santé et la sécurité de la population. **Nous estimons que la probabilité est très faible que des auteurs de menace parrainés par des États veuillent intentionnellement perturber ou endommager l'infrastructure pétrolière et gazière au Canada en l'absence d'hostilités.**

Certains grands exploitants-propriétaires d'actifs de TO, comme les services publics, les pipelines et les raffineries du secteur pétrolier et gazier, sont des cibles peu probables pour l'espionnage commercial, puisque la plupart des adresses IP ayant une valeur commerciale en utilisation et en développement se trouvent dans la chaîne d'approvisionnement. Nous jugeons que la probabilité est élevée que les cyberactivités parrainées par des États contre les propriétaires d'actifs de TO œuvrant dans le secteur pétrolier et gazier avaient pour objectif de recueillir de l'information et de prépositionner des cyberoutils afin de pouvoir mener d'éventuelles activités de sabotage, ou encore de démontrer la cyberpuissance des États parrainant ces activités, en vue d'exercer une certaine intimidation en ligne. Les premiers stades de possibles cyberactivités de sabotage peuvent ressembler à de l'espionnage industriel.[22] Selon nos observations, la probabilité est très élevée que des auteurs de menace parrainés par des États utilisent l'information recueillie dans le cadre de leurs cyberactivités de reconnaissance et d'espionnage pour développer un accès et des capacités additionnelles pouvant leur permettre de saboter les TO utilisées dans les secteurs d'infrastructures essentielles du Canada, y compris le secteur pétrolier et gazier.

Le Centre pour la cybersécurité évalue que **la probabilité est presque certaine que les auteurs de cybermenace parrainés par des États améliorent continuellement leurs capacités de mener des cyberactivités destructrices et débilitantes contre les infrastructures**

essentielles. Ils arrivent à leurs fins en repérant et en accordant la priorité aux systèmes d'intérêt, en identifiant les vulnérabilités, en développant un accès et un prépositionnement dans ces systèmes, en menant des activités d'espionnage sur les TO utilisées et en développant des techniques et des outils pour perturber ou détruire les TO.[23] Au début de 2022, le maliciel Pipedream (aussi appelé Incontroller) a été découvert avec des modules servant à exploiter les postes de travail de surveillance des TO et à perturber l'automatisation des TO industrielles et des contrôleurs de sécurité que l'on trouve habituellement dans les installations de gaz naturel liquéfié et les centrales électriques.[24] Le niveau accru de sophistication technique du maliciel Pipedream comparativement à des maliciels antérieurs comme Triton met en évidence des auteurs parrainés par des États ainsi que les efforts que ceux-ci sont prêts à consacrer pour le développement de cybercapacités offensives visant des TO spécifiques.[25]

Nous estimons que la probabilité est élevée que les auteurs de cybermenace parrainés par des États cherchant à perturber l'approvisionnement en gaz et en pétrole au Canada ciblent les goulots d'étranglement pour ce qui est de la transmission du pétrole et des étapes de transformation, afin de maximiser les effets. Parmi les cibles potentielles de ces activités, nous notons les pipelines de grand diamètre, les terminaux portuaires et les grandes installations de raffinage.

Importantes cyberactivités parrainées par des États visant le secteur pétrolier et gazier

- À la fin de 2019 et au début de 2020, des auteurs de cybermenace parrainés par l'Iran ont lancé les maliciels effaceurs Zerocleare[26] et Dustman[27], des variants du maliciel Shamoon, dans les réseaux des cibles non identifiés du secteur de l'énergie saoudien et de Bapco, l'entreprise nationale de pétrole de Bahreïn, causant un nombre non signalé de perturbations des activités.[28]
- En 2018, un variant du maliciel iranien Shamoon a détruit près de 10 % du réseau de l'entreprise pétrolière et gazière italienne Saipem. Saipem est un important entrepreneur de l'entreprise saoudienne Saudi Aramco.[29]
- En 2017, des auteurs de cybermenace parrainés par la Russie ont mis à l'essai une capacité appelée Triton (ou Trisis) pour modifier le rendement d'un système instrumenté de sécurité (SIS) d'une installation pétrolière et gazière du Moyen-Orient. Un SIS est défini comme un dispositif TO spécialisé conçu pour détecter de façon indépendante les conditions de défaillance dans un procédé industriel et, au besoin, provoquer l'arrêt sûr de l'équipement. Les auteurs sont parvenus à accéder à l'installation à distance et à reprogrammer les dispositifs de commande du SIS, causant leur passage à l'état de défaillance, l'arrêt automatique du procédé industriel et l'enquête subséquente.[30] Plus tard, en 2018 et 2019, les mêmes auteurs ont accédé aux réseaux d'installations du secteur de l'énergie aux États et Unis.[31]
- De 2011 à 2018, des auteurs de cybermenace parrainés par la Russie ont mené une vaste campagne de cyberespionnage contre des entreprises américaines et européennes du secteur de l'énergie. Cette campagne a utilisé le maliciel Havex pour rechercher des composants de TO et extraire de l'information relative aux TO.[32]
- En 2012, des auteurs de cybermenace iraniens parrainés par des États déploient le maliciel effaceur Shamoon qui cible les réseaux de TI des entreprises Saudi Aramco et RasGas en Arabie saoudite et au Qatar. Les auteurs de cybermenaces ont pu ainsi supprimer des données de près de 30 000 ordinateurs, ce qui a forcé l'arrêt de nombreux réseaux internes.[33]
- Entre 2011 et 2013, des auteurs de cybermenace parrainés par la Chine ont mené une campagne de harponnage et d'ingérence contre des entreprises de pipelines pétrolières et gazières aux États-Unis.[34]

Contexte géopolitique actuel : L'invasion de l'Ukraine par la Russie

En avril 2022, le Centre pour la cybersécurité en collaboration avec ses organismes partenaires en cybersécurité de l'Australie, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis a émis des avertissements aux fournisseurs d'infrastructures essentielles par rapport à de possibles activités menées par des groupes criminalisés et des hacktivistes non étatiques prorusses et parrainés par la Russie, qui visaient à appuyer l'invasion de l'Ukraine par la Russie.[35] En juillet 2023, le Centre pour la cybersécurité a expliqué le rôle de ces auteurs en Ukraine et à l'extérieur de l'Ukraine dans son Bulletin sur les cybermenaces : Les activités de cybermenace liées à l'invasion de l'Ukraine par la Russie.[36]

La Russie a lancé à répétition des cyberattaques destructrices contre les infrastructures essentielles stratégiques afin de démontrer sa puissance lorsque les crises géopolitiques ont dégénéré en un conflit armé. En 2022, afin d'appuyer l'invasion de l'Ukraine, la Russie a mené une vaste cybercampagne visant les infrastructures essentielles de l'Ukraine, ce qui comprend le gouvernement et les secteurs de l'énergie, des télécommunications et des finances.[37] Cette campagne a utilisé des attaques par déni de service et diverses formes de maliciels destructeurs pour mener à une perturbation généralisée, souvent en coordination avec des attaques cinétiques. Par exemple, le 24 février 2022, des pirates informatiques parrainés par la Russie ont mené des activités de cybermenace destructrices contre le service d'Internet par satellite KA-SAT de Viasat en Ukraine pendant que les forces militaires russes envahissaient l'Ukraine, rendant ainsi les infrastructures essentielles pour Internet et les télécommunications inexploitables tout en perturbant l'accès Internet de la clientèle de Viasat à travers l'Europe.[38]

Menaces visant le Canada : Auteurs de menace parrainés par des États

Selon nos observations, la probabilité est presque certaine que des auteurs de cybermenace parrainés par la Russie mènent des activités de reconnaissance contre les infrastructures essentielles canadiennes, et la probabilité est très élevée que ces cyberactivités russes, dont l'objectif est de se prépositionner dans les réseaux de TO industriels, continuent. **Nous estimons que la probabilité est très faible que des auteurs de menace parrainés par la Russie lancent une attaque destructrice contre l'infrastructure pétrolière et gazière du Canada ou d'États alliés, tant qu'on ne perçoit pas d'hostilités imminentes entre le Canada et la Russie.**

Menaces visant le Canada : Auteurs de menace alliés à un État

La probabilité est très élevée que des cyberactivités menées par des groupes alliés à la Russie comme Killnet et Xaknet, afin d'appuyer l'invasion de l'Ukraine par la Russie, aient augmenté de manière considérable au cours des 12 derniers mois.[39] En général, ces groupes obtiennent l'accès à des réseaux pour déployer un rançongiciel et chiffrer des données, ce qui peut causer une importante perturbation des opérations, ou encore ils mènent des attaques par DDoS (souvent accompagnées de menaces d'extorsion) ou des activités de défiguration de site Web.[40] La probabilité est élevée que des cibles au sein d'un secteur sont choisies de manière opportuniste, en fonction de recherches de services exposés présentant des vulnérabilités connues, plutôt que de manière stratégique pour un maximum d'effet. Ces attaques sont souvent en réaction à des nouvelles faisant état que le pays ciblé manifeste son soutien pour l'Ukraine.[41]

Le Centre pour la cybersécurité est au courant des efforts déployés par des auteurs de menace alliés à la Russie pour compromettre les réseaux des fournisseurs d'infrastructures essentielles du Canada et des États-Unis et d'y établir une présence permanente. Les organisations ciblées incluent des organisations du secteur pétrolier et gazier. Nous estimons que la probabilité est très élevée que l'intention de ces activités soit de perturber les services essentiels pour produire un impact psychologique, et pour finalement affaiblir le soutien canadien à l'Ukraine. Nous estimons que la probabilité est presque certaine que ces activités se poursuivront pendant toute la durée de la guerre, et qu'elles vont même prendre de l'ampleur à mesure que les efforts d'invasion par la Russie déclineront ou que de nouvelles mesures de soutien à l'Ukraine seront annoncées. Même si les auteurs de menace non étatiques prorusses ont presque certainement des moyens ayant un plus faible niveau général de sophistication et des capacités techniques plus faibles que les auteurs parrainés par la Russie, nous estimons que la probabilité est presque égale que le secteur pétrolier et gazier du Canada subisse un incident perturbateur causé par des auteurs de menace prorusses, en raison de leur plus grande tolérance au risque, de l'augmentation de leur nombre et de leurs activités ainsi que du nombre de cibles vulnérables dans l'ensemble du secteur.

Nous estimons que la probabilité est très élevée que tant les auteurs de cybermenace parrainés par la Russie que les auteurs de menace prorusses considèrent l'Ukraine, les États-Unis et les principaux membres européens de l'OTAN comme des cibles plus prioritaires que le Canada. Cependant, **si les États-Unis sont ciblés, nous estimons qu'il y a une probabilité presque égale que le Canada soit aussi touché**, en raison de l'interconnectivité de l'infrastructure pétrolière et gazière des États-Unis et du Canada.

Importantes cyberactivités russes

- Les premières activités de sabotage parrainées par des États ciblant les infrastructures essentielles se sont produites en 2015 et en 2016 contre le réseau électrique de l'Ukraine et ont été causées par l'organisme de renseignement militaire de la Russie, c.-à-d. le service de la direction centrale du renseignement de l'état-major (GRU), que les chercheuses et chercheurs en cybersécurité appellent « l'équipe Sandworm ». En 2015, la Russie a été en mesure de mettre hors tension sept sous-stations de trois sociétés régionales ukrainiennes de distribution pendant trois heures, causant ainsi une panne d'électricité qui a touché 225 000 clientes et clients. Un an plus tard, un cyberincident survenu à Ukrenergo, société nationale d'électricité ukrainienne, a entraîné une panne d'électricité d'une heure dans le nord de Kiev. Ces incidents, qui se sont produits dans un contexte de tension entre la Russie et l'Ukraine, ont marqué un tournant dans l'histoire des cyberactivités visant le secteur de l'énergie. Ils montrent bien l'effet que peut avoir une cyberattaque perpétrée contre les infrastructures essentielles, particulièrement lors de conflits internationaux.[42]
- En juin 2017, le maliciel NotPetya a infecté des dizaines de milliers de dispositifs, dont ceux des réseaux d'infrastructures essentielles de l'Ukraine et du monde entier.[43] La probabilité est élevée qu'il s'agissait d'une attaque menée par la Russie visant à perturber les systèmes financiers ukrainiens.
- En 2018, le GRU a désactivé plus de 15 000 sites Web et organes de presse du gouvernement de la Géorgie dans le cadre d'efforts visant à déstabiliser le pays.[44]

Autres auteurs de menace

Nous estimons que des auteurs de menace dotés de moyens peu sophistiqués comme des terroristes, des hacktivistes, des adeptes de sensations fortes et des personnes mécontentes, motivés à attirer l'attention en embarrassant le secteur ou y porter préjudice au moyen d'incidents publics, sont actuellement plus susceptibles de prendre part à des activités qui ne passent pas inaperçues et qui sont nuisibles, comme la défiguration de sites Web, plutôt que de tenter une perturbation directe des TO. Depuis l'invasion massive de l'Ukraine par la Russie au début de février 2022, nous estimons que la probabilité est élevée que le rythme des opérations et la mobilisation de groupes

d'auteurs de menace non étatiques prorusses aient augmentés.[45] Le Centre pour la cybersécurité est conscient que la pratique bien établie de la Russie a été de collaborer avec des groupes d'auteurs non étatiques, comme des cybercriminelles et cybercriminels et des hacktivistes, pour mener des activités de cybermenace contre les infrastructures essentielles de l'Ukraine et de ses alliés. À titre d'exemple, Killnet, un groupe d'hacktivistes prorusses a mené des attaques par DDoS contre des sites Web d'exploitants d'infrastructures essentielles, y compris les sites de fournisseurs du secteur de l'énergie.[46]

Prévisions

La cybersécurité des infrastructures essentielles du Canada est aussi une question de sécurité nationale. Le secteur pétrolier et gazier au Canada joue un rôle important dans l'économie, à la fois comme contributeur au PIB, et comme fournisseur d'énergie à d'autres secteurs de l'économie canadienne, aux infrastructures essentielles et aux Canadiennes et Canadiens. L'importance et la haute visibilité du secteur pétrolier et gazier, ainsi que son exposition grandissante aux menaces découlant de la transformation numérique en fait une cible pour les auteurs de cybermenace qui prévoient d'importantes perturbations.

Le Centre pour la cybersécurité recommande à tous les propriétaires de réseau des infrastructures essentielles, y compris ceux du secteur pétrolier et gazier, de prendre les mesures nécessaires pour protéger leurs systèmes contre les cybermenaces décrites dans la présente évaluation, et, en particulier, par rapport aux événements géopolitiques entourant l'invasion de l'Ukraine par la Russie.[47] Le Centre pour la cybersécurité se joint à ses partenaires des États-Unis[48] et du Royaume-Uni[49] et recommande des mesures proactives de surveillance et d'atténuation sur les réseaux. Le document du Cybersecurity and Infrastructure Security Agency (CISA) des États-Unis intitulé : « Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure » met utilement en évidence les vulnérabilités connues pour avoir été exploitées par les auteurs de cybermenace russes, leurs tactiques, techniques et procédures, ainsi que les mesures de défense potentielles.

Ressources utiles

Détection et atténuation des menaces

- Introduction à l'environnement de cybermenaces
- Conseils en matière de cybersécurité en cas de niveaux de menace élevés (ITSAP.10.101)
- Ressources sur les rançongiciels
- Contrôles de cybersécurité de base pour les petites et moyennes organisations
- Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information
- Sécurité de l'Internet des objets pour les petites et moyennes organisations
- Conseils du Centre pour la cybersécurité sur la sécurité des dispositifs mobiles
- Contrats avec des fournisseurs de services gérés : facteurs relatifs à la cybersécurité à considérer
- Les 10 mesures de sécurité des TI : nº 2 – Appliquer des correctifs aux applications et aux systèmes d'exploitation (ITSM.10.096)
- Rapport conjoint sur les outils de piratage publiquement accessibles
- Cyberactivité malveillante ciblant les fournisseurs de services gérés

Évaluation des menaces

- Bulletin sur les cybermenaces : Les activités de cybermenace liées à l'invasion de l'Ukraine par la Russie
- Bulletin sur les cybermenaces : Cybermenaces visant les technologies opérationnelles
- La cybermenace provenant des chaînes d'approvisionnement
- Évaluation des cybermenaces nationales 2023-2024
- Bulletin sur les cybermenaces : Les cyberattaques visant le secteur canadien de l'électricité
- Bulletin sur les cybermenaces : La menace des rançongiciels en 2021

Services

- Fiche de renseignements sur le programme d'examen de la sécurité

Références

[1] Ressources naturelles Canada. Cahier d'information sur l'énergie 2021–2022. 23 décembre 2021.

[2] Centre canadien pour la cybersécurité. Évaluation des cybermenaces nationales 2023-2024. 28 octobre 2022.

[3]Halpern, S. The Colonial Pipeline Ransomware Attack and the Perils of Privately Owned Infrastructure. The New Yorker, 19 mai 2021.

[4] Ressources naturelles Canada. Le réseau de pipelines canadien. 14 septembre 2020.

[5] Centre canadien pour la cybersécurité. Évaluation des cybermenaces nationales 2020. 16 novembre 2020.

[6] Statistique Canada. Tableau : 22-10-0076-01,Types d'incidents de cybersécurité touchant les entreprises par industrie et taille de l'entreprise.

[7] Centre canadien pour la cybersécurité. Bulletin sur les cybermenaces : Les cybermenaces visant les technologies opérationnelles. 16 décembre 2021.

[8] Centre canadien pour la cybersécurité. La cybermenace provenant des chaînes d'approvisionnement. 8 février 2023.

[9] Centre canadien pour la cybersécurité. Bulletin sur les cybermenaces : Les cybermenaces visant les technologies opérationnelles. 16 décembre 2021.

[10] P. ex. : YouTube, https://github.com/miguelob/ICS-Hacking, https://scadahacker.com/resources/msf-scada.html, etc.

[11] Sheridan, K. Cobalt Strike & Metasploit Tools Were Attacker Favorites in 2020. DarkReading, 7 janvier 2021.

[12] Centre canadien pour la cybersécurité. Bulletin sur les cybermenaces : La menace des rançongiciels en 2021. 16 décembre 2021.

[13] Microsoft 365 Defender Threat Intelligence Team. Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself. Microsoft Threat Intelligence Center (MSTIC), 9 mai 2022.

[14]Trend Micro Inc. Cyber-Attacks on Industrial Assets Cost Firms Millions. Trend Micro News. 2 juin 2022.

[15] Tom Balmforth et Maria Tsvetkova. Russia takes down REvil hacking group at U.S. request – FSB. Reuters, 14 janvier 2022.

[16] Blogue ReliaQuest. Colonial Pipeline Attack Update: Cybercriminal forum XSS, Exploit and RaidForums ban all things ransomware. ReliaQuest. 14 mai 2021.

[17] Statista Research Department. Malware: most-targeted industries 2020-2021. Statista, 7 juillet 2022.

[18]Adam Janofsky. String of cyberattacks on European oil and chemical sectors likely not coordinated, officials say. Recorded Future. 3 février 2022., et Alexander Klimburg, Filipe Beato et Maciej Kolaczkowski. Why the energy sector's latest cyberattack in Europe matters. World Economic Forum, 4 février 2022.

[19] Centre canadien pour la cybersécurité. Évaluation des cybermenaces nationales 2020. 16 novembre 2020.

[20] Reuters. Russian, Chinese intelligence targeting Norwegian oil secrets: report, 3 décembre 2020.

[21] Centre canadien pour la cybersécurité. Bulletin sur les cybermenaces : Les cybermenaces visant les technologies opérationnelles. 16 décembre 2021.

[22] Assante, M.J. and R.M. Lee. The Industrial Control System Cyber Kill Chain. SANS Institute, 2015.

[23] Centre canadien pour la cybersécurité. « Bulletin sur les cybermenaces : Les cyberattaques visant le secteur canadien de l'électricité ». 30 novembre 2020.

[24] Cybersecurity and Infrastructure Security Agency. Alert AA22-103A, APT Cyber Tools Targeting ICS/SCADA Devices. 13 avril 2022.

[25] Dragos, Inc. CHERNOVITE's PIPEDREAM Malware Targeting Industrial Control Systems (ICS). 13 avril 2022 (en anglais seulement) Nathan Brubaker, Keith Lunden, Ken Proska, Muhammad Umair, Daniel Kapellmann Zafra, Corey Hildebrandt et Rob Caldwell. INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems. Mandiant, 13 avril 2022.

[26] Kessem, L. et l'équipe X-Force d'IBM Security. New Destructive Wiper 'ZeroCleare' Targets Energy Sector in the Middle East. IBM Security Intelligence Blog. 4 décembre 2019.

[27] Jenna McLaughlin. Saudis warn of new destructive cyberattack that experts tie to Iran. Yahoo News, 7 janvier 2020.

[28] Cimpanu, C., New Iranian data wiper malware hits Bapco, Bahrain's national oil company. ZDNet, 8 janvier 2020.

[29] Cimpanu, C., Shamoon malware destroys data at Italian oil and gas company. ZDNet, 13 décembre 2018.

[30] Johnson, B., D. Cuban, M. Krotofil., D. Scali, N. Brubaker et C. Glyer. Threat actors Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure. FireEye, 14 décembre 2017.

[31] Blogue Dragos. Threat Proliferation in ICS Cybersecurity: XENOTIME Now Targeting Electric Sector, in Addition to Oil and Gas. Dragos, Inc. 14 juin 2019.

[32] Nelson, N. The Impact of Dragonfly Malware on Industrial Control Systems. SANS Institute, 18 janvier 2016. Cybersecurity and Infrastructure Security Agency. Alert AA22-083A, Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector. 24 mars 2022.

[33] Finkle, J. Insiders suspected in Saudi cyber attack. Reuters, 7 septembre 2012.

[34] Cybersecurity and Infrastructure Security Agency. Alert AA21-201A, Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013. 21 juillet 2021.

[35] Cybersecurity and Infrastructure Security Agency. Alert AA22-110A, Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. Révisé le 9 mai 2022.

[36] Centre canadien pour la cybersécurité. Bulletin sur les cybermenaces : Les activités de cybermenace liées à l'invasion de l'Ukraine par la Russie. 14 juillet 2022.

[37] Centre canadien pour la cybersécurité. Bulletin sur les cybermenaces : Les activités de cybermenace liées à l'invasion de l'Ukraine par la Russie. 14 juillet 2022.

[38] Affaires mondiales Canada. Déclaration sur les cyberactivités malveillantes de la Russie qui touchent l'Europe et l'Ukraine. 10 mai 2022.

[39] Zdrok, N. Cyber War: Hackers' Transformation from Cyber Criminals to Hacktivists. Binary Defense Blog, 30 novembre 2022.

[40] Cybersecurity and Infrastructure Security Agency. Alert Code: AA22-110A, Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. Révisé le 9 mai 2022.

[41] M. Burgess. Russian "hacktivists" are causing trouble far beyond Ukraine. Ars Technica. 12 juillet 2022.

[42] Centre canadien pour la cybersécurité. « Bulletin sur les cybermenaces : Les cyberattaques visant le secteur canadien de l'électricité ». 30 novembre 2020.

[43] Centre canadien pour la cybersécurité. Évaluation des cybermenaces nationales 2018. 6 décembre 2018.

[44] Affaires mondiales Canada. Le Canada condamne la cyberactivité malveillante de la Russie envers la Géorgie. 20 février 2020.

[45] Zdrok, N. Cyber War: Hackers' Transformation from Cyber Criminals to Hacktivists. Binary Defense Blog, 30 novembre 2022.

[46] Cybersecurity and Infrastructure Security Agency. Alert AA22-110A, Cybersecurity Advisory: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. 9 mai 2022.
Forescout Vedere Labs. Killnet: Analysis of Attacks from a Prominent Pro-Russian Hacktivist Group. 2 juin 2022.

[47] Centre canadien pour la cybersécurité. Bulletin sur les cybermenaces : Le CCC rappelle aux exploitants des infrastructures essentielles du Canada de prendre conscience des activités de cybermenace connues qui sont parrainées par la Russie et de prendre des mesures d'atténuation contre celles-ci. 13 février 2022.

[48] Cybersecurity & Infrastructure Security Agency. CISA Urges Organizations to Implement Immediate Cybersecurity Measures to Protect Against Potential Threats. 18 janvier 2022.

[49] National Cyber Security Centre. NCSC joins US partners to promote understanding and mitigation of Russian state-sponsored cyber threats. 12 janvier 2022.

CAT. D96-101/2023F-PDF
ISBN 978-0-660-48766-3

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada