Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ | ÉVALUATION DES CYBERMENACES NATIONALES 2018

ESPIONNAGE PARRAINÉ PAR DES ÉTATS ET MENACES CONTRE LES INFRASTRUCTURES ESSENTIELLES

Les infrastructures essentielles comprennent les réseaux et les systèmes dont les Canadiens dépendent chaque jour pour leurs ressources et services essentiels, notamment les systèmes énergétiques, les réseaux d'approvisionnement en eau, les services publics, les systèmes de transport, les chaînes agroalimentaires et les réseaux financiers.

Les auteurs de menaces parrainés par des États mènent des activités de cyberespionnage contre les infrastructures essentielles du Canada et d'autres pays alliés. De telles activités incluent la reconnaissance et la collecte de renseignement dans les secteurs de l'énergie, de l'aérospatiale et de la défense. Les institutions publiques sont une cible alléchante, puisqu'elles détiennent des renseignements personnels, de précieuses données de recherche et de l'information sensible. On s'attend à ce que les auteurs de menaces parrainés par des États continuent de mener des tentatives de cyberespionnage contre les entreprises et les infrastructures essentielles du Canada afin de réaliser leurs objectifs stratégiques nationaux.

Secteurs des infrastructures essentielles du Canada

Les activités de cybermenace qui ciblent les infrastructures essentielles du Canada peuvent avoir des conséquences graves et considérables. Les auteurs de cybermenaces moins sophistiqués peuvent tirer avantage de la prolifération des cyberoutils malveillants et de la nature interconnectée de l'équipement et des systèmes industriels pour perturber, même par inadvertance, les infrastructures essentielles du Canada.

QUE FAIT LE GOUVERNEMENT DU CANADA?

L'un des principaux objectifs du nouveau Centre canadien pour la cybersécurité est de s'attaquer à ces cybermenaces en constante évolution en collaboration avec les propriétaires et exploitants des infrastructures essentielles du Canada, ainsi que tous les ordres de gouvernement, le secteur privé et le milieu universitaire. Ces partenariats stratégiques permettront de faciliter la communication d'information, d'intégrer les technologies de cyberdéfense et de renforcer la cyberrésilience du Canada.

Pour appuyer ces objectifs, le CST a diffusé l'an dernier un de ses outils d'analyse et de détection de maliciels, connu sous le nom de Chaîne de montage (Assemblyline). Cet outil a été employé à l'échelle nationale et internationale pour automatiser la détection des maliciels et soutenir le travail des analystes en cybersécurité dans plusieurs secteurs.

Le projet de loi C-59, la *Loi concernant des questions de sécurité nationale*, permettrait au CST et au Centre canadien pour la cybersécurité de communiquer plus d'informations concernant les cybermenaces aux propriétaires et exploitants des infrastructures essentielles du Canada, et de leur fournir sur demande une assistance opérationnelle et technique qui les aidera à protéger ces réseaux.

En 2017, le Centre de la sécurité des télécommunications (CST) a informé ses partenaires des États-Unis d'une cybercompromission visant le secteur de l'énergie. Lors de cet incident, des auteurs de cybermenaces parrainés par un État étranger avaient réussi à accéder aux systèmes sécurisés et isolés à un point tel qu'ils auraient pu interrompre le transit d'énergie.

CONSEILS PRATIQUES POUR LES PROPRIÉTAIRES ET EXPLOITANTS DES INFRASTRUCTURES ESSENTIELLES

- Mettre en œuvre une liste blanche des applications
- Isoler les applications Web
- Assurer la protection au niveau de l'hôte
- Protéger l'information au niveau organisationnel
- Intégrer, surveiller et défendre les passerelles Internet
- Appliquer des correctifs aux applications et aux systèmes d'exploitation
- Pour en savoir plus, prière de visiter cyber.gc.ca

Canada