Centre de la sécurité des télécommunications Canada
Communications Security Establishment Canada

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Les activités de cybermenace de la République populaire de Chine

Les auteurs de cybermenace de la RPC ciblent les entreprises de télécommunications dans le cadre d'une campagne mondiale de cyberespionnage

Cyberbulletin

1
D96-129/2025F-PDF
ISBN 978-0-660-77868-6

Canada

Introduction

Le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) et le Federal Bureau of Investigation (FBI) des États-Unis mettent en garde les Canadiennes et les Canadiens contre la menace que représente l'auteur de cybermenace parrainé par la République populaire de Chine (RPC) appelé Salt Typhoon dans les rapports de l'industrie. Le Centre pour la cybersécurité s'est précédemment joint à ses partenaires pour signaler que des auteurs de cybermenace de la RPC ont compromis les réseaux de grands fournisseurs mondiaux de services de télécommunications dans le but de mener une importante et vaste campagne de cyberespionnage. Le présent cyberbulletin vise à faire connaître la menace que font peser les activités de cybermenace de la RPC, particulièrement sur les organisations de télécommunications canadiennes, compte tenu des nouvelles compromissions d'entités au Canada en lien avec Salt Typhoon.

La menace visant les organisations canadiennes

Le Centre pour la cybersécurité est au courant des activités de cybermenace ciblant actuellement des entreprises de télécommunications canadiennes. Les responsables sont presque assurément des auteurs de menace parrainés par la RPC, plus précisément Salt Typhoon.

Trois dispositifs réseau enregistrés à une entreprise de télécommunications canadienne ont été compromis vraisemblablement par des auteurs de menace de Salt Typhoon à la mi-février 2025. Les auteurs ont exploité la vulnérabilité CVE-2023-20198 pour récupérer les fichiers de configuration en cours d'exécution des trois dispositifs et ont modifié au moins l'un des fichiers pour configurer un tunnel GRE, permettant ainsi la collecte de trafic à partir du réseau.

Dans des enquêtes distinctes, le Centre pour la cybersécurité a découvert des chevauchements entre des indicateurs malveillants associés à Salt Typhoon, qui avaient été signalés dans des rapports de partenaires et de l'industrie, **ce qui suggère que le secteur des télécommunications n'est pas le seul ciblé par cet auteur de menace.** En ciblant des dispositifs canadiens, les auteurs de menace pourraient recueillir de l'information sur le réseau interne d'une victime ou utiliser le dispositif d'une victime pour compromettre d'autres victimes. Dans certains cas, nous estimons que les activités des auteurs de menace se sont fort probablement limitées à la reconnaissance réseau.

Bien que notre compréhension de ces activités continue d'évoluer, nous évaluons qu'au cours des deux prochaines années, les auteurs de cybermenace de la RPC continueront presque certainement à cibler des organisations canadiennes dans le cadre de cette campagne d'espionnage, y compris des fournisseurs de services de télécommunications et leur clientèle. Pour surveiller et atténuer cette menace, nous encourageons les organisations canadiennes à consulter les ressources utiles à la fin de ce cyberbulletin, qui présentent notamment des conseils sur le renforcement de la sécurité des réseaux, les facteurs relatifs à la sécurité à considérer pour les dispositifs d'accès et de plus amples renseignements sur les cybermenaces liées à la RPC.

La menace visant les télécommunications

Les réseaux de télécommunications figurent presque certainement parmi les cibles d'espionnage les plus prioritaires des auteurs de cybermenace parrainés par des États. Les auteurs parrainés par des États hostiles comptent très probablement sur l'accès à des fournisseurs de services de télécommunications (FST) et à des réseaux de télécommunications partout dans le monde comme principales sources de collecte de renseignement étranger. Les FST détiennent du trafic de télécommunications, en plus de recueillir et de conserver de grands volumes de données sur la clientèle qui ont une valeur en matière de renseignement, y compris des données concernant les communications, l'emplacement et les dispositifs.

Les auteurs de cybermenace parrainés par des États compromettent constamment des FST à l'échelle mondiale, souvent dans le cadre de vastes programmes de renseignement de longue date, dans le but d'exfiltrer des données en masse sur la clientèle et de recueillir de l'information sur les cibles d'intérêt de grande valeur, comme des représentantes et représentants de gouvernement. Ces activités comprennent la géolocalisation et le suivi des personnes, la surveillance des appels téléphoniques et l'interception de messages texte. Les auteurs étatiques ont accédé à des réseaux de télécommunications et à des données en exploitant des vulnérabilités présentes dans les dispositifs réseau, tels que les routeurs, et en profitant de la conception mal sécurisée des systèmes qui acheminent, facturent et gèrent les communications.

En 2024, des enquêtes réalisées par des partenaires ont permis de découvrir que des auteurs de cybermenace parrainés par la RPC avaient compromis les réseaux de grands FST mondiaux, dont des entreprises américaines de services sans fil, très probablement dans le cadre d'une opération d'espionnage ciblée. D'après nos partenaires, ces auteurs ont été en mesure de voler, des FST compromis, des données sur les relevés d'appels de clientes et clients. Ils ont également recueilli des communications privées d'un nombre limité de personnes participant surtout à des activités politiques ou gouvernementales.

Nous nous préoccupons également des répercussions possibles sur les renseignements de nature délicate des organisations clientes qui travaillent directement avec les fournisseurs de services de télécommunications. Les auteurs de cybermenace de la RPC tentent fréquemment de compromettre les fournisseurs de services de confiance, notamment les fournisseurs de services infonuagiques, de services gérés et de services de télécommunications, pour accéder à de l'information sur les clientes et clients ou aux réseaux indirectement.

Les auteurs de cybermenace de la RPC exploitent les vulnérabilités dans les appareils périphériques connectés

Comme nous le soulignons dans l'Évaluation des cybermenaces nationales 2025-2026, les auteurs de cybermenace exploitent les vulnérabilités touchant les dispositifs de sécurité et de réseau situés en périphérie des réseaux, ce qui comprend les routeurs, les pare-feux et les solutions de réseau privé virtuel (RPV). En compromettant ces appareils périphériques connectés (également appelés « dispositifs d'accès »), un auteur de cybermenace peut s'introduire dans un réseau, surveiller, modifier et exfiltrer le trafic réseau circulant sur l'appareil ou possiblement pénétrer encore plus loin dans le réseau d'une victime.

Dans le cadre de la campagne actuelle, les auteurs de cybermenace de la RPC ciblent ces dispositifs réseau et exploitent les vulnérabilités existantes pour obtenir et maintenir un accès aux FST. Malgré des rapports publics faisant état de leurs activités, il est très probable que ces auteurs poursuivent leur ciblage.

Ressources utiles

Consultez les ressources en ligne suivantes pour obtenir de plus amples renseignements, ainsi que des avis et conseils utiles :

Rapports et bulletins

- Évaluations des menaces visant le Canada
  - Évaluation des cybermenaces nationales 2025-2026
- Bulletins et publications de partenaires
  - Enhanced Visibility and Hardening Guidance for Communications Infrastructure (en anglais seulement)
  - Bulletin sur les cybermenaces : Le Centre pour la cybersécurité invite les Canadiennes et Canadiens à s'informer et à se protéger contre les activités de cybermenace de la RPC

Avis et conseils

- Objectifs relatifs à l'état de préparation en matière de cybersécurité : Sécuriser les systèmes les plus essentiels
- Boîte à outils des objectifs relatifs à l'état de préparation en matière de cybersécurité intersectoriels

- Facteurs relatifs à la sécurité à considérer pour les dispositifs d'accès
- Conseils conjoints pour une meilleure visibilité et un renforcement accru de la sécurité pour l'infrastructure des communications
- Observations et stratégies d'atténuation liées aux activités menées par la République populaire de Chine ciblant les routeurs de périphérie