Rançongiciels : comment les prévenir et s'en remettre

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Avril 2024 | ITSAP.00.099

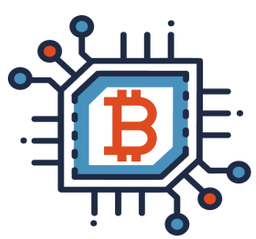
Un rançongiciel est un type de maliciel qui bloque l'accès aux fichiers ou aux systèmes jusqu'à ce que l'utilisatrice ou utilisateur verse une somme d'argent. Le rançongiciel peut se servir de votre réseau et infecter tous les dispositifs qui y sont connectés. Les auteures et auteurs de menace peuvent vous interdire l'accès aux fichiers de l'organisation en chiffrant vos données, en vous empêchant de vous connecter aux dispositifs de l'organisation et en ayant recours à des méthodes d'extorsion pour vous contraindre à payer une rançon pour empêcher la fuite de vos données.

Ils peuvent se procurer des rançongiciels sur le Web clandestin. Le code malveillant pour l'attaque est déjà écrit, ce qui fait que ces auteures et auteurs n'ont pas à savoir comment créer le script du code. C'est ce que l'on appelle le rançongiciel comme service (RaaS pour Ransomware-as-a-Service). De plus, les outils d'IA générative peuvent aider les auteures et auteurs de menace, avec peu ou pas d'expérience de codage, à concevoir un rançongiciel fonctionnel. La présente publication donne des conseils pour aider votre organisation à se préparer à faire face à une attaque par rançongiciel et à se rétablir après coup.

Manières dont un rançongiciel peut affecter des dispositifs

Les rançongiciels peuvent infecter les dispositifs par des liens malveillants ou des pièces jointes qui se trouvent sur des sites Web non sécurisés, dans des courriels d'hameçonnage et dans des applications de médias sociaux. Les auteures et auteurs de menace explorent vos réseaux pour trouver de l'information qu'ils pourraient exfiltrer et surveillent vos méthodes de communications avant de déployer un rançongiciel.

Si votre dispositif est infecté par un rançongiciel, vous recevrez un avis de rançon à votre écran vous indiquant que vos fichiers ont été chiffrés et qu'ils seront inaccessibles jusqu'à ce qu'une rançon ait été payée. Les auteures et auteurs de menace vont souvent menacer les victimes de détruire leurs données de façon permanente, ou de provoquer la fuite de celles-ci, si elles ne paient pas la rançon dans un délai précis. Ils exigent souvent de payer la rançon en monnaie numérique, comme des bitcoins étant donné que le transfert est difficile à retracer. Ils peuvent également demander que le paiement soit fait par cartes de crédit prépayées ou cartes-cadeaux.



Préparer son organisation

Passez en revue les étapes suivantes pour aider votre organisation à garder une longueur d'avance sur les attaques par rançongiciel.

Planifier

Élaborez un plan d'intervention en cas d'incident pour déterminer comment votre organisme surveillera et détectera les incidents et comment elle interviendra en cas d'incident. Votre plan doit aussi inclure des plans de sauvegarde, de reprise et de communications. Votre plan d'intervention en cas d'incident devrait déterminer les rôles que vos employées et employés doivent jouer et leur fournir des instructions détaillées en cas d'incident. Ce plan devrait être accessible hors ligne au cas où vos systèmes ne seraient pas disponibles.

- Élaborer un plan d'intervention en cas d'incident (ITSAP.40.003)
- Sauvegarder et récupérer vos données (ITSAP.40.002)
- Élaboration d'un plan de reprise informatique personnalisé (ITSAP.40.004)

Se préparer à une reprise

Votre organisation devrait mettre en place un plan de reprise. Parallèlement à votre plan d'intervention en cas d'incident, mettez votre plan de reprise à l'essai en effectuant des simulations et des exercices préparatoires. Les mises en situation devraient mettre à l'essai l'efficacité de votre intervention et mettre en lumière ce qui doit être amélioré.

Dispenser une formation sur la sensibilisation à la sécurité au personnel

Fournissez à vos employées et employés de la formation personnalisée sur la cybersécurité et la gestion des dispositifs afin de vous assurer qu'ils ne soient pas victimes d'activités malveillantes comme des courriels d'hameçonnage et des téléchargements infectés.

- Offrir aux employés une formation sur mesure en cybersécurité (ITSAP.10.093)

Penser à une cyberassurance

Faites des recherches sur les fournisseurs de cyberassurance et sur les détails des polices d'assurance pour déterminer si votre organisme pourrait en tirer des avantages.

Centre de la sécurité des télécommunications Canada | Communications Security Establishment Canada

No de cat. D97-1/00-099-2024F-PDF ISBN 978-0-660-70608-5

Canada

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Protéger son organisation contre les attaques par rançongiciel

Utilisez les conseils ci-dessous pour protéger votre organisation contre les attaques par rançongiciel.

Appliquer des méthodes d'authentification robustes

Activez l'authentification multifacteur résistante à l'hameçonnage et utilisez des phrases de passe ou des mots de passe uniques et robustes sur tous les dispositifs et pour tous les comptes. Envisagez d'utiliser un gestionnaire de mots de passe pour créer et stocker les phrases de passe et mots de passe.

- Étapes à suivre pour déployer efficacement l'authentification multifacteur (AMF) ITSAP.00.105)
- Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)
- Conseils de sécurité sur les gestionnaires de mots de passe (ITSAP.30.025)

Sauvegarder les données

Mettez en œuvre un plan de sauvegarde pour votre organisation. Une copie de sauvegarde de vos données et de vos systèmes permet de récupérer vos données et de vous donner accès à vos systèmes essentiels dans l'éventualité d'un incident. Vous devez faire des copies de sauvegarde régulièrement pour vous assurer que vos sauvegardes ont les données les plus à jour en comparaison à celles en temps réel. Créez le plus de barrières de sécurité que possible entre vos systèmes de production et vos copies de sauvegarde afin de vous assurer que ces dernières sont chiffrées et stockées hors ligne sans connexion à Internet ou à des réseaux locaux. Les auteures et auteurs de menace peuvent infecter vos copies de sauvegarde avec des rançongiciels si ces dernières sont connectées à vos réseaux, ce qui minerait vos efforts de récupération. Mettre à l'essai votre processus de sauvegarde et de récupération est également essentiel pour vous assurer que votre reprise est rapide et efficace.

- Sauvegarder et récupérer vos données (ITSAP.40.002)
- Utiliser le chiffrement pour assurer la sécurité des données sensibles (ITSAP.40.016)

Adopter le principe de droit d'accès minimal

Gérez et surveillez les comptes et les accès des usagers en appliquant le principe de droit d'accès minimal. Donnez au personnel uniquement accès aux fonctions et aux privilèges dont il a besoin pour réaliser son travail.

Mettre en œuvre un modèle de sécurité à vérification systémique

Utilisez un modèle de sécurité à vérification systématique (ZT pour Zero Trust) pour protéger les données et les infrastructures contre les accès non autorisés. Les modèles de sécurité ZT se basent sur le principe de l'application à vérification systématique pour toutes les utilisatrices et tous les utilisateurs, toutes les applications et tous les dispositifs, à moins qu'ils aient obtenu une authentification une autorisation. L'authentification et l'autorisation font continuellement l'objet de réévaluations, et elles sont vérifiées chaque fois qu'un accès est demandé pour une nouvelle ressource.

- Modèle à vérification systématique (ou architecture zéro confiance) – (ITSAP.10.008)

Restreindre les privilèges administratifs

Mettez en place une confirmation pour chaque action qui nécessite des droits d'accès et des autorisations de niveau élevé, et limitez le nombre d'utilisatrices et utilisateurs ayant des comptes administratifs et des privilèges. Veillez à ce que les fonctions administratives se fassent à partir d'un poste de travail administratif. Envisagez le recours à une intégrité par deux personnes (TPI pour Two-Person Integrity) ou la double authentification pour valider et vérifier les tâches administratives sensibles.

- Gestion et contrôle des privilèges administratifs (ITSAP.10.094)

Mettre à jour et corriger les systèmes et les dispositifs

Obtenez les mises à jour et les correctifs qui corrigeront les vulnérabilités et les bogues connus de vos logiciels, matériels et systèmes d'exploitation. Les auteures et auteurs de menace peuvent facilement exploiter les systèmes et les dispositifs non corrigés ou qui ne sont pas pris en charge.

- Application des mises à jour sur les dispositifs (ITSAP.10.096)

Désactiver les macros

Assurez-vous de désactiver les macros par défaut afin de réduire les risques de propagation des rançongiciels dans les pièces jointes de Microsoft Office. Les versions plus récentes de Microsoft désactiveront par défaut les macros provenant d'Internet.

Segmenter les réseaux

Divisez votre réseau en plusieurs plus petites sections. Ainsi, il sera plus difficile pour un rançongiciel d'infecter l'ensemble du réseau.

- Les 10 mesures de sécurité des TI : No 5, Segmenter et séparer l'information (ITSM.10.092)

Mettre en place des outils de sécurité

Installez un antimaliciel et un antivirus sur vos systèmes afin de détecter les activités malveillantes et de sécuriser votre réseau avec un pare-feu pour protéger les dispositifs connectés. Pensez à installer un filtre de système d'adressage par domaines sur vos dispositifs mobiles pour bloquer les sites Web malveillants et filtrer le contenu dommageable. Vous pouvez également mettre en place un protocole DMARC, un système d'authentification et de signalement qui aide à protéger les domaines de votre organisme contre l'usurpation, l'hameçonnage et d'autres activités malveillantes. Assurez-vous que vos utilisatrices et utilisateurs se servent de votre réseau privé virtuel (RPV) pour accéder à votre réseau.

- Système d'adressage par domaine de protection (ITSAP.40.019)
- Directive de mise en œuvre : protection du domaine de courrier (ITSP.40.065 v1.1)
- Les réseaux privés virtuels (ITSAP.80.101)

Faire appel à des professionnelles et professionnels de la cybersécurité

Dans le cas d'un cyberincident, communiquer tout de suite avec une professionnelle ou un professionnel de la cybersécurité peut vous permettre de récupérer vos systèmes et vos données plus rapidement qu'avec votre personnel de TI en interne.

Centre de la sécurité des télécommunications Canada
Communications Security Establishment Canada

Canada

No de cat. D97-1/00-099-2024F-PDF ISBN 978-0-660-70608-5

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Se remettre d'une attaque par raçongiciel

Les étapes suivantes peuvent vous aider à éliminer ou à réduire la propagation d'un rançongiciel.

1. **Isolez immédiatement l'appareil :** Déconnectez vos dispositifs pour arrêter la propagation du rançongiciel à d'autres dispositifs connectés. Certaines souches de rançongiciels sont conçues pour rester en dormance sur un dispositif et se propager discrètement à d'autres dispositifs connectés aux réseaux avant de chiffrer les fichiers. Dans ces cas, il est possible que vous ne puissiez pas arrêter la propagation du rançongiciel.
2. **Signalez l'incident :** Signalez toute attaque par rançongiciel au service de police local, au Centre antifraude du Canada et au Centre canadien pour la cybersécurité. Parlez de l'incident aux employées et employés qui figurent dans votre plan d'intervention en cas d'incident et donnez-leur des directives claires quant à leurs rôles et responsabilités pour aider à gérer l'incident.
3. **Changez vos mots de passe :** Réinitialisez vos justificatifs d'identité, y compris les mots de passe de tous vos systèmes, dispositifs et comptes. Les auteures et auteurs de menace sauvegardent habituellement ces informations pour des attaques futures. Pensez à utiliser des phrases de passe pour vos dispositifs puisque celles-ci sont plus robustes et plus faciles à retenir.

4. **Déterminez quel est le type de rançongiciel auquel vous faites face :** Utilisez les informations de la note de rançon (p. ex., les URL listées) et les nouvelles extensions dont vos fichiers chiffrés ont hérité afin d'alimenter vos recherches sur de possibles attaques récurrentes et d'identifier le rançongiciel.
   - Si vous trouvez un outil de déchiffrement en ligne, ou si des organismes chargés de l'application de la loi peuvent être en mesure de vous fournir un, passez à l'étape suivante.
   - Si aucun outil de déchiffrement n'est disponible en ligne pour la souche de rançongiciel à laquelle vous faites face, effacez toutes les données de votre dispositif de façon sécuritaire et réinstallez le système d'exploitation.

5. **Mettez en place des mesures correctives au point d'entrée :** Avant de reconnecter vos systèmes et dispositifs au réseau ou à Internet, vous devez découvrir comment l'auteure ou auteur de menace a réussi à accéder à votre réseau, à vos systèmes et à vos dispositifs, puis appliquer des mesures de sécurité afin de prévenir une nouvelle attaque.
6. **Restaurez vos systèmes et vos données à partir de votre copie de sauvegarde :** Analysez vos copies de sauvegarde pour vous assurer qu'aucun rançongiciel ou autre logiciel malveillant ne s'y trouvent. Stockez vos copies de sauvegarde hors ligne pour atténuer les risques qu'un rançongiciel les infecte. Une fois que vous êtes confiant, restaurer vos systèmes et vos dispositifs à partir de vos copies de sauvegarde.
7. **Mettez à jour vos systèmes et appliquez les correctifs :** Mettez à jour tous vos dispositifs, matériels et logiciels et appliquez-leur les correctifs offerts. Appliquez les correctifs à votre système d'exploitation et assurez-vous que tous les antivirus, antimaliciels et pare-feu des logiciels sont à jour.
8. **Passez en revue l'incident et offrez une formation continue :** Passez en revue l'incident avec votre personnel et offrez-lui une formation continue portant sur les mesures préventives qui permettent de se protéger contre les attaques par rançongiciel, comme apprendre à identifier des pièces jointes et des courriels suspects. Servez-vous des menaces courantes et des incidents passés pour vous garder à jour et vous préparer pour le futur.

Les risques associés au paiement d'une rançon

La décision de payer une auteure ou un auteur de menace pour qu'il vous redonne vos fichiers et vos dispositifs est difficile et vous vous sentirez probablement pressé de répondre à ses demandes. Avant de payer, communiquez avec votre poste de police local et signalez le cybercrime. Payez la rançon n'est habituellement pas recommandé, pour les raisons suivantes :

- le paiement ne garantit pas l'accès à vos fichiers, car les auteures et auteurs de menace pourraient demander encore plus d'argent après que vous avez payé une première rançon;
- le paiement encourage les auteures et auteurs de menace à continuer d'infecter vos dispositifs et ceux d'autres organismes avec des rançongiciels puisqu'ils peuvent compter que vous continuerez de payer à chaque attaque;
- les auteures et auteurs de menace peuvent utiliser des maliciels effaceurs qui semblent en apparence être des rançongiciels pour altérer ou supprimer de façon permanente vos fichiers une fois la rançon payée, les rendant ainsi irrécupérables;
- vos données ont probablement été copiées et l'auteure ou auteur de menace peut les divulguer ou les utiliser dans le but de faire des gains;
- votre paiement pourrait être utilisé pour soutenir d'autres attaques par rançongiciel ou des organisations terroristes.

Pour en savoir plus

Reportez-vous aux conseils suivants pour en savoir plus sur les points importants que nous avons relevés :

- Guide sur les rançongiciels (ITSM.00.099)
- Facteurs à considérer par les clients de services gérés en matière de cybersécurité (ITSM.50.030)
- Êtes-vous victime de piratage? (ITSAP.00.015)
- Les outils de sécurité préventive (ITSAP.00.058)
- Reconnaître les courriels malveillants (ITSAP.00.100)

Centre de la sécurité des télécommunications Canada
Communications Security Establishment Canada

No de cat. D97-1/00-099-2024F-PDF ISBN 978-0-660-70608-5

Canada