Qu'est-ce qu'un rançongiciel?

Un rançongiciel est un type de maliciel. Il s'agit d'un cybercrime qui permet de retenir des données en échange d'une rançon. L'accès aux données contenues sur des réseaux informatiques, des appareils mobiles et des serveurs est verrouillé jusqu'à ce que la victime paie la rançon.

Les rançongiciels ciblent principalement des entreprises, des individus ou des organisations comme des maisons d'enseignement, des gouvernements ou des hôpitaux. Les rançongiciels peuvent être de type chiffreur ou bloqueur.

Un rançongiciel peut prendre plusieurs formes. Une des méthodes les plus communes d'attaque par rançongiciel consiste à utiliser le hameçonnage. Le destinataire reçoit un courriel rédigé avec soin qui l'incite à ouvrir une pièce jointe ou à télécharger un fichier. Cette action installe un rançongiciel vecteur qui prend le contrôle de l'ordinateur et peut infiltrer le réseau informatique pour bloquer son accès à l'ensemble des utilisateurs.

L'objectif d'un rançongiciel est de convaincre la victime de payer une rançon pour déverrouiller l'accès à ses données. En général, les criminels exigent que le paiement se fasse sous forme de bitcoins – une cryptomonnaie qui ne peut pas être retracée. Une fois le paiement sécurisé, la victime reçoit un code de déverrouillage ou un fichier de décryptage qui libère les données sur le réseau informatique, l'appareil mobile ou les serveurs.

Le rançongiciel est une forme d'ingénierie sociale utillisé par les criminels pour infecter les ordinateurs, infiltrer les réseaux des entreprises et voler des données.

Quels sont les principaux types de rançongiciels ?

Rançongiciel chiffreur

Les rançongiciels de type chiffreur bloquent l'accès aux fichiers et aux données personnelles. Ils sont suffisamment intelligents pour trouver les données importantes sur les ordinateurs ou les appareils mobiles, les crypter et en bloquer l'accès aux victimes.

Les rançongiciels chiffreurs parcourent les ordinateurs et les appareils mobiles à la recherche de défauts et de faiblesses permettant d'accéder à des données qui n'ont pas été sauvegardées. On cible tous les types de données d'importance : informations financières, projets de travail d'envergure, numéros de téléphone, photos, rapports d'impôt et vidéos.

Ce type de maliciel est très ingénieux. Il permet de crypter toutes les données de valeur avant de se dévoiler à la victime. Les données sont tenues en otage jusqu'à ce que la victime accepte de payer la rançon.

En général, les rançongiciels chiffreurs ne bloquent pas l'ordinateur ou l'appareil mobile complet. Les victimes conservent l'accès aux zones qui ne sont pas cryptés ou retenus par le rançongiciel.

Le courriel est composé de façon à faire naître un sentiment d'urgence. Le destinataire doit agir pour se protéger d'un crime. Il semble provenir d'une source légitime comme le service à la clientèle d'Apple, d'une banque, de Microsoft, PayPal ou d'une autre entreprise connu.

Les rançongiciels chiffreurs sont également appelés bloqueurs de données.

Rançongiciel bloqueur

Les rançongiciels de type bloqueur verrouillent et ferment l'ordinateur ou l'appareil mobile au complet. On demande aux victimes de payer une rançon avant de libérer l'ordinateur ou l'appareil mobile.

En général, le système verrouillé donne un accès limité aux victimes, ce qui les oblige à interagir exclusivement avec le cybercriminel. Certaines sections du clavier peuvent être verrouillées ou la souris gelée de façon à ce que la victime puisse répondre uniquement aux demandes du rançongiciel.

Les rançongiciels bloqueurs n'infiltrent normalement pas le réseau informatique au complet ou n'attaquent pas des fichiers qui se trouvent sur l'ordinateur. Il est donc plus facile de trouver le maliciel et de l'éliminer sans payer la rançon.

Puisque les rançongiciels bloqueurs peuvent être supprimés de l'ordinateur, les criminels utilisent souvent des tactiques d'ingénierie sociale pour convaincre les victimes de payer. Par exemple, le rançongiciel se fait passer pour un organisme de l'administration fiscale ou d'application de la loi qui menace d'imposer des amendes ou d'autres pénalités suite à de supposées activités illégales en ligne. La victime panique et n'hésite pas à payer, quel que soit le prix.

Le rançongiciel chiffreur est également surnommé bloqueur d'ordinateur.

Quelles sont les techniques communément utilisées par les rançongiciels?

Cryptage de fichiers

Les rançongiciels chiffreurs utilisent soit le cryptage symétrique ou asymétrique des fichiers. Le cryptage symétrique permet le cryptage et le décryptage des données avec la même clé. Le cryptage asymétrique utilise une clé publique pour le cryptage des données et une clé privée pour le décryptage.

Le cryptage symétrique des données est une méthode beaucoup plus rapide. Toutefois, si la victime découvre la clé, le décryptage des données est également plus facile. En utilisant le cryptage asymétrique, le criminel n'a pas à se soucier de protéger la clé publique puisqu'elle ne peut pas être utilisée pour le décryptage des données.

Les rançongiciels chiffreurs les plus ingénieux utilisent une combinaison de cryptage symétrique et asymétrique. Les types communs de cryptage de fichiers comprennent une clé publique téléchargée, une clé publique intégrée et une clé symétrique intégrée.

Bloqueur d'écran

Les rançongiciels bloqueurs utilisent le verrouillage d'écran pour bloquer l'accès des victimes à leur ordinateur ou appareil mobile. Cela signifie que la victime n'a aucun accès à son ordinateur ou à son appareil mobile, y compris au système d'exploitation ou à d'autres services réseau.

Souvent, un message de demande de rançon est diffusé en continu sur l'écran. Parfois, un compte à rebours est affiché ou le montant de la rançon augmente avec le temps.

Les types communs de verrouillage d'écran comprennent les rançongiciels Android, les verrouilleurs de navigateur et les rançongiciels bloqueurs qui ciblent spécifiquement Windows.

Comment fonctionne un rançongiciel?

Téléchargeurs

Lorsqu'un téléchargeur infiltre un ordinateur, il en profite pour télécharger d'autres rançongiciels qui infectent l'ordinateur ou l'appareil mobile. De façon générale, ce type de rançongiciel permet aux cybercriminels de prendre le contrôle de l'ordinateur ou de l'appareil.

Publicité malveillante

De fausses publicités criminelles sont diffusées sur des sites Web légitimes et redirigent les victimes vers un site hébergeant une trousse d'exploitation.

Hameçonnage

Les courriels d'hameçonnage ou pourriels utilisent des techniques d'ingénierie sociale pour convaincre les victimes de télécharger ou d'ouvrir des pièces jointes.

Auto-propagation

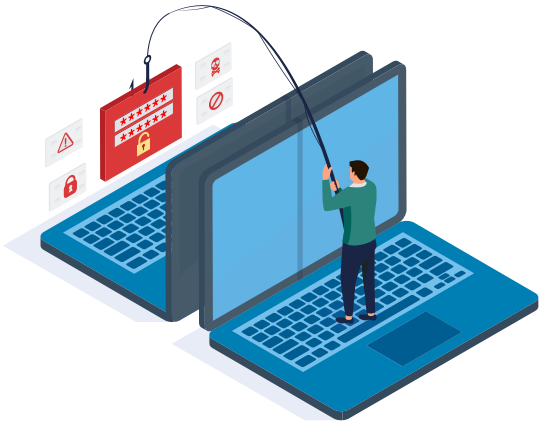
Le rançongiciel se propage dans le système affecté et attaque tout ordinateur ou appareil lié au réseau partagé.

Système de distribution du trafic

On utilise un système de distribution du trafic pour rediriger le trafic vers un site Web qui héberge une trousse d'exploitation. La trousse d'exploitation sert à identifier les points faibles de l'ordinateur et le rançongiciel est installé à l'aide d'un maliciel de téléchargement furtif.

Qui peut être la cible d'un rançongiciel?

N'importe quel gouvernement, entreprise, organisation ou personne peut être la cible d'un rançongiciel. Les cybercriminels ciblent toute personne prête à payer une rançon pour récupérer l'accès à ses réseaux informatiques, données, appareils mobiles ou serveurs.



Les cybercriminels ne se soucient pas de qui ils attaquent avec leurs rançongiciels. Pour cette raison, il est particulièrement important que vos employés et votre organisation soient en cybersécurité.

Les rançongiciels sont très faciles à utiliser par les cybercriminels. Il est donc très important que l'ensemble des employés de votre organisation soient conscients des menaces et des risques posés par les rançongiciels.

Les simulations de rançongiciel vous permettent d'identifier les employés les plus vulnérables et de sensibiliser votre équipe sur la facilité de tomber dans le piège de l'ingénierie sociale.

Comment prévenir les rançongiciels

1 Investissez dans vos employés. Mettez l'emphase sur la sensibilisation au hameçonnage et à la sécurité pour réduire le risque humain. Servez-vous des outils gratuits de simulation d'hameçonnage pour informer vos collègues et identifier les risques.

2 Donnez à vos employés les outils et connaissances nécessaires pour reconnaître les risques de rançongiciel. Informez votre équipe sur la façon et la raison d'ouvrir des pièces jointes provenant d'expéditeurs inconnus.

3 À l'interne, formez des héros de la cybersécurité dédiés à garder votre organisation en sécurité. Cela augmentera la motivation de vos employés à changer leurs comportements.

4 Utilisez des plateformes de formation sur la sensibilisation à la sécurité et de simulation de rançongiciels qui permettent d'offrir un enseignement motivant et efficace.

5 Encouragez la création d'un environnement de soutien propice au changement de comportement. L'environnement de travail doit favoriser l'apprentissage et le développement d'une culture de sécurité.

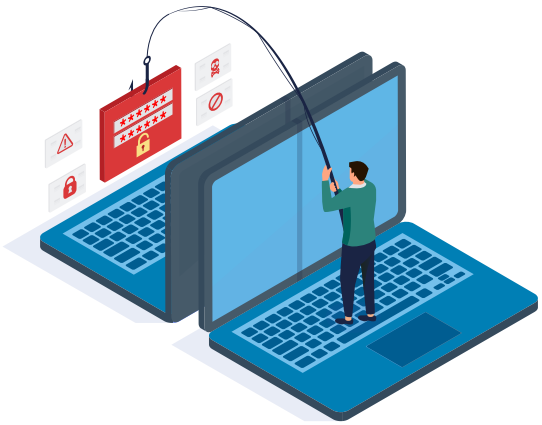
6 Profitez des formations automatisées et simples à utiliser pour maintenir un milieu d'apprentissage motivant, éducatif et facilement administrable. Consultez The Human Fix to Human Risk pour connaître les étapes à suivre afin d'élaborer un programme de sensibilisation à la sécurité efficace qui favorise les comportements sécuritaires.

7 Effectuez des communications et des campagnes en continu sur la cybersécurité, les rançongiciels et les risques que représentent les URL, les courriels et les pièces jointes.

8 Utilisez un modèle de livraison flexible qui comprend des vidéos animées, de la formation en ligne interactive, des services de sécurités gérés, des modules de microapprentissage et des simulations d'hameçonnage afin d'offrir un soutien en continu.

9 Profitez d'une séance de coaching CISO gratuite pour apprendre comment améliorer la sensibilisation actuelle par rapport aux rançongiciels ou créer un nouveau programme de sensibilisation à la sécurité.

Qu’est-ce qu’une simulation de rançongiciel?



Une simulation de rançongiciel est la meilleure façon de sensibiliser les utilisateurs sur les risques et d’identifier les employés les plus susceptibles de se faire prendre au piège des rançongiciels.

La simulation de rançongiciel vous permet d’intégrer la sensibilisation à la cybersécurité dans votre organisation de façon motivante et informative.

Les simulations de rançongiciel en temps réel constituent une façon rapide et pratique d’éduquer les gens et d’accroître la vigilance face aux attaques. Les participants constatent d’eux-mêmes comment il est facile de tomber dans le piège de se faire installer un rançongiciel sur son ordinateur ou son appareil mobile.

Quels sont les 10 principaux avantages des simulations de rançongiciel?

1. Agissez en prévention plutôt qu’en réaction aux risques de cybersécurité
2. Mesurer le degré de vulnérabilité de l’entreprise et des employés
3. Éliminer les risques que représentent les cybermenaces
4. Accroître la vigilance des utilisateurs face aux risques de rançongiciels et d’ingénierie social
5. Former des héros de la cybersécurité et instiller une culture de cybersécurité
6. Changer les comportements pour éliminer les réflexes de confiance automatique
7. Déployer des solutions anti-rançongiciels et anti-hameçonnage ciblées
8. Protéger vos précieuses données corporatives et personnelles
9. Évaluer les impacts de la formation en sensibilisation à la cybersécurité
10. Répondre aux exigences de l’industrie en matière de conformité