Cisco Ransomware Defense : tenir les ransomwares éloignés

Vous souhaitez mieux vous protéger des ransomwares, quelle que soit leur méthode d'infiltration ? Nous sommes les seuls à proposer des produits et une architecture de sécurité pour y parvenir.

Vue d'ensemble

Les fichiers et les données sont d'une importance vitale pour l'entreprise. Il est impératif de pouvoir les protéger et préserver la productivité de votre entreprise.

Malheureusement, vous n'êtes par à l'abri d'un ransomware. Il s'agit d'un logiciel malveillant, ou malware, qui bloque les données présentes sur l'ordinateur d'une entreprise ou d'un utilisateur, comme des documents, des photos ou de la musique. L'utilisateur ne peut débloquer ou récupérer ses fichiers que contre le paiement d'une rançon. Sans défenses appropriées, le ransomware peut infliger de tels dégâts que l'entreprise peut être réduite à ressortir des stylos et du papier.

Les ransomwares se propagent généralement via des kits d'exploit, des publicités malveillantes (des annonces infectées qui diffusent le malware sur un site web), l'hameçonnage (des e-mails frauduleux qui semblent fiables à première vue) ou des campagnes de spam. L'attaque se déclenche lorsqu'un utilisateur clique sur un lien ou sur une pièce jointe d'un e-mail d'hameçonnage. L'infection peut également survenir lorsque les utilisateurs visitent des sites qui contiennent des publicités malveillantes, conçues pour attaquer automatiquement leurs ordinateurs.

Découvrez Cisco® Ransomware Defense. Notre solution réduit les risques d'attaques par ransomware grâce à une approche multicouche qui protège l'ensemble de votre infrastructure, de la couche DNS aux terminaux en passant par le réseau, la messagerie et le web. Les défenses intégrées suivent une approche architecturale et permettent une visibilité et une réactivité sans précédent pour combattre les ransomwares.

Les bénéfices

- **Réduisez les risques liés aux ransomwares** pour mieux vous concentrer sur votre cœur de métier.
- **Bénéficiez d'une protection immédiate** grâce à une solution de sécurité qui bloque les menaces avant qu'elles affectent votre système.
- **Profitez d'une visibilité et d'une réactivité sans équivalent** grâce à une approche architecturale, depuis la couche DNS jusqu'au réseau en passant par le terminal.
- **Empêchez les programmes malveillants de se propager latéralement** par le biais d'une stricte segmentation du réseau.
- **Tirez parti des recherches et données sur les ransomwares** du centre Cisco Talos

Des menaces puissantes qui gagnent du terrain

C'est l'année des ransomwares. Et elle s'avère considérablement rentable. Le ransomware est rapidement devenu le type de malware le plus lucratif.

Selon le FBI, il représente un marché annuel approchant le milliard de dollars. Le groupe de recherche Cisco Talos démontre qu'une seule campagne de ransomware peut générer jusqu'à 60 millions de dollars chaque année. Les ransomwares gagnent tellement de terrain qu'ils deviennent même le thème de prédilection de certaines émissions de télévision.

Les hackers, qui disposent de suffisamment de fonds pour cela, vont continuer à innover en créant des ransomwares toujours plus virulents. Nous pensons que les ransomwares pourront de plus en plus se propager automatiquement, dans le but de bloquer de vastes pans de réseaux. Les infrastructures IT des entreprises pourraient se retrouver reléguées à leur niveau des années 1970.

De nos jours, ce sont surtout des produits isolés qui luttent contre les ransomwares. Nous devons envisager une approche plus architecturale, capable de prendre en charge les divers vecteurs d'infections.

Cette présentation s'intéresse aux divers vecteurs et aux méthodes utilisées par les hackers. Les acteurs de la protection doivent sécuriser la messagerie et le web, bloquer l'accès aux infrastructures malveillantes sur Internet, stopper les fichiers de ransomwares qui parviennent à atteindre un terminal, bloquer les instructions de type contrôle-commande (C&C) et empêcher facilement les déplacements latéraux des ransomwares en cas d'infection.

Que contient la solution ?

Cisco Ransomware Defense rassemble tous les composants nécessaires pour mettre en place une architecture de sécurité capable de faire face aux ransomwares. Vous pouvez choisir la solution complète ou sélectionner les composants qui répondent à un besoin de sécurité immédiat.

La solution Ransomware Defense comprend :

- Cisco Umbrella, qui bloque les menaces au niveau de la couche DNS, loin de votre réseau
- Cisco Advanced Malware Protection (AMP) for Endpoints, qui empêche l'exécution des ransomwares sur les terminaux

- Cisco Email Security, qui intercepte les messages d'hameçonnage et les spams contenant des ransomwares à la fois dans le cloud et sur site
- Cisco AMP, qui peut être instantanément ajouté aux produits de sécurité de la messagerie à l'aide d'une licence facile à activer, pour analyser de manière statique et dynamique (sandboxing) les pièces jointes inconnues transitant par la passerelle Cisco de sécurité de la messagerie
- Le pare-feu de nouvelle génération Cisco Firepower™, qui bloque le trafic de type contrôle-commande et les fichiers malveillants sur le réseau
- Cisco ISE via le réseau Cisco pour segmenter votre réseau de façon dynamique et éviter que le ransomware se propage latéralement

Avec Ransomware Defense, le réseau de l'entreprise devient exécuteur pour endiguer la diffusion des ransomwares. Ils ne pourront pas se propager aussi facilement en cas d'infection.

Les services de sécurité Cisco supervisent instantanément le processus de riposte en cas d'attaque. Ils rationalisent les déploiements de la solution AMP, des pare-feu de nouvelle génération et d'autres produits.

Les principales caractéristiques

- Empêcher les ransomwares d'infiltrer le réseau ou de se télécharger sur des ordinateurs portables
- Isoler les ransomwares si jamais ils parviennent à pénétrer dans le réseau

Nos services de sécurité aident à lutter contre les ransomwares

L'équipe des services de sécurité Cisco dédiée à la gestion des incidents peut vous aider à vous préparer, mais aussi à riposter en cas d'attaques par ransomware.

De plus, nos services d'intégration de la sécurité s'attaquent aux problèmes architecturaux relatifs à la solution. Ils rationalisent le déploiement des technologies comme AMP for Endpoints et les pare-feu de nouvelle génération Cisco FirePower. Notre équipe dispose d'un savoir-faire approfondi dans le domaine des solutions de sécurité intégrée pour accélérer l'adoption des technologies nécessaires avec un minimum de perturbation.

Plus globalement, les entreprises doivent également s'assurer qu'elles disposent des technologies et des politiques appropriées en matière de sauvegarde des données afin de se protéger contre les ransomwares.

« Nous avons fortement réduit notre surface d'exposition aux ransomwares issus du web et avons pu améliorer l'expérience de nos utilisateurs en matière de connectivité Internet. »

– Octapharma

Cisco Capital

Un financement pour vous aider à atteindre vos objectifs

L'offre de financement Cisco Capital® peut vous aider à acquérir la technologie dont vous avez besoin pour atteindre vos objectifs et rester compétitif. Nous pouvons vous aider à réduire vos CapEx, à accélérer votre croissance et à optimiser vos investissements et votre ROI. L'offre de financement Cisco Capital permet une certaine flexibilité pour l'achat de matériel, de logiciels, de services et d'équipements tiers complémentaires. Le montant du paiement est connu à l'avance. Les solutions de financement Cisco Capital sont disponibles dans plus de 100 pays. En savoir plus.

L'avantage Cisco

Les ransomwares trouveront tôt ou tard le moyen d'infiltrer votre entreprise. Les e-mails d'hameçonnage, les bannières web compromises et les spams sont autant de vecteurs d'attaques qui doivent être protégés. Nous sommes les seuls à proposer une architecture de sécurité capable de relever ce défi. Les produits isolés ne suffisent pas. Notre solution s'appuie sur les recherches du centre Cisco Talos, qui a effectué des enquêtes approfondies sur les ransomwares, pour nous permettre de vous offrir une protection multicouche efficace. Nous bloquons les ransomwares et les combattons s'ils parviennent à s'infiltrer sur votre réseau, ce qui peut malheureusement se produire.

C22-737492-01 08/16