SOPHOS

Les ransomwares distants

Le chiffrement malveillant à distance est une technique populaire utilisée dans environ 60 % des attaques de ransomware pilotées manuellement[1]. La plupart des solutions de sécurité Endpoint ont des difficultés à faire face à cette approche et si vous n'utilisez pas Sophos Endpoint, il y a de fortes chances que vous soyez exposé. Dans ce guide, vous en apprendrez plus sur les ransomwares distants et sur la protection anti-ransomware de pointe de Sophos, conçue pour les bloquer.

Un livre blanc Sophos. Décembre 2023

Qu'est-ce qu'un ransomware distant ?

Un ransomware distant, également appelé chiffrement à distance malveillant, survient lorsqu'un système endpoint compromis est utilisé pour chiffrer des données sur d'autres appareils du même réseau.

Dans le cas d'attaques manuelles, les attaquants tentent en général de déployer le ransomware directement sur les machines qu'ils veulent chiffrer. Ils abandonnent rarement lorsque leur première tentative est bloquée (par exemple, par des technologies de sécurité sur les appareils cibles) et choisissent plutôt de recourir à une autre approche puis de réessayer, encore et encore.

Une fois que les auteurs de l'attaque parviennent à compromettre un appareil, ils peuvent exploiter l'architecture de domaine de l'organisation pour chiffrer les données sur les machines reliées à un domaine administré. Toute l'activité malveillante (intrusion, exécution de la charge utile et chiffrement) se produit sur la machine compromise, ce qui permet de contourner les piles de sécurité modernes. Seul le transfert de documents vers et depuis d'autres machines indique que le système a été compromis.

80 % des cas de chiffrement malveillant à distance proviennent d'appareils non administrés sur le réseau[2], bien que certaines partent de machines qui ne disposent pas des défenses nécessaires pour empêcher l'intrusion des attaquants.

Pourquoi les ransomwares distants sont-ils si répandus ?

Le recours massif à cette stratégie s'explique en grande partie par son caractère évolutif : une seule machine non administrée ou insuffisamment protégée suffit à exposer l'ensemble du parc informatique d'une entreprise à un chiffrement malveillant, même si tous les autres appareils sont équipés d'une solution de sécurité Endpoint de dernière génération.

Pour ne rien arranger, les attaquants disposent d'un large arsenal de variantes de ransomware pour mener à bien leurs attaques. Nombre de familles de ransomware bien connues prennent en charge le chiffrement à distance malveillant, notamment Akira, BitPaymer, BlackCat, BlackMatter, Conti, Crytox, DarkSide, Dharma, LockBit, MedusaLocker, Phobos, Royal, Ryuk et WannaCry.

Une autre raison importante de la prévalence des ransomwares distants est que la plupart des produits de sécurité Endpoint s'avèrent inefficaces dans ce scénario, car ils se concentrent sur la détection des fichiers et processus malveillants des ransomwares sur le dispositif protégé. Mais dans le cas des attaques par chiffrement à distance, les processus s'exécutent sur la machine compromise, si bien que l'activité malveillante passe au travers des systèmes de protection Endpoint.

Sophos Endpoint, en revanche, est doté d'une défense robuste contre le chiffrement malveillant à distance, grâce à notre protection CryptoGuard, leader sur le marché.

Sophos CryptoGuard : protection anti-ransomware universelle, à la pointe de l'industrie

Sophos Endpoint intègre plusieurs couches de protection pour défendre les entreprises contre les ransomwares, notamment CryptoGuard, notre technologie anti-ransomware unique, incluse dans toutes les licences Sophos Endpoint.

Là où les solutions de sécurité Endpoint classiques recherchent uniquement les fichiers et processus malveillants, CryptoGuard analyse les fichiers de données pour rechercher tout signe de chiffrement malveillant, quel que soit l'emplacement d'exécution des processus. Cette approche le rend très efficace contre toutes les formes de ransomware, y compris le chiffrement malveillant à distance. S'il détecte un chiffrement malveillant, CryptoGuard bloque automatiquement l'activité et restaure les fichiers touchés vers leur état d'origine sain.

CryptoGuard exécute un puissant algorithme d'analyse des contenus lors des opérations de lecture et d'écriture des fichiers, afin de rechercher activement le chiffrement malveillant. Cette approche universelle est unique dans l'industrie et permet à Sophos Endpoint de bloquer les attaques de ransomware qui passent sous les radars des solutions classiques, y compris les attaques à distance et les variantes de ransomware inédites.

Figurant au nombre des fonctionnalités exclusives de Sophos Endpoint, CryptoGuard est inclus dans tous les abonnements Sophos Intercept X Advanced, Sophos XDR et Sophos MDR. Précisons que cette fonctionnalité est activée par défaut, ce qui garantit aux entreprises une protection complète contre les attaques de ransomware locales et à distance, sans qu'aucun réglage ou configuration ne soit nécessaire.

- **Détecte le chiffrement malveillant en analysant le contenu des fichiers**

  À la différence des autres solutions qui abordent les ransomwares dans une perspective anti-malware en se concentrant sur la détection de codes malveillants, CryptoGuard analyse les contenus à l'aide d'algorithmes mathématiques afin de repérer les chiffrements massifs et rapides de fichiers.

- **Bloque les attaques de ransomware locales et distantes**

  Comme CryptoGuard se concentre sur le contenu des fichiers, les tentatives de chiffrement par ransomware peuvent être détectées même lorsque le processus malveillant n'est pas en cours d'exécution sur l'appareil de la victime.

- **Annule automatiquement tout chiffrement malveillant**

  Lorsqu'il détecte un chiffrement de masse, CryptoGuard crée des sauvegardes temporaires des fichiers modifiés et annule automatiquement les modifications indésirées en restaurant les fichiers vers leur état d'origine sain. Sophos fait appel à une approche propriétaire, contrairement à d'autres solutions qui reposent sur l'utilisation de Windows Volume Shadow Copy, que les attaquants savent aisément contourner. Cette solution n'impose aucune limite quant à la taille et au type de fichier pouvant être récupéré, ce qui minimise l'impact sur la productivité de l'entreprise.

- **Bloque automatiquement les appareils distants**

  En cas d'attaque de ransomware distant, CryptoGuard bloque automatiquement l'adresse IP de l'appareil distant qui tente de chiffrer des fichiers sur la machine de la victime.

- **Protège l'enregistrement de démarrage principal (MBR)**

  CryptoGuard permet aussi de protéger l'appareil contre les ransomwares qui chiffrent l'enregistrement de démarrage principal (et empêchent donc le démarrage) et contre les attaques qui formatent le disque dur.

Découvrez les appareils non protégés

Un seul poste non protégé suffit à exposer votre organisation à une attaque de chiffrement à distance. Le déploiement de Sophos Endpoint procure une protection universelle robuste contre les ransomwares et le chiffrement malveillant. Mais comment pouvez-vous savoir si des appareils non protégés sont connectés à votre réseau ?

C'est là que Sophos Network Detection and Response (NDR) entre en jeu. Sophos NDR surveille le trafic réseau pour détecter les flux suspects et, ce faisant, identifie les appareils non protégés et les actifs malveillants dans l'environnement.

Pour une protection optimale contre les attaques de ransomware distant, installez Sophos Endpoint sur toutes les machines dans l'environnement et déployez Sophos NDR pour détecter les appareils non protégés sur votre réseau.

Renforcez dès aujourd'hui votre protection contre les ransomwares distants

Le chiffrement malveillant à distance est une technique de ransomware populaire que la plupart des solutions de sécurité Endpoint leaders peinent à bloquer. Si vous n'utilisez pas Sophos Endpoint, il y a de fortes chances que vous soyez exposé.

Pour en savoir plus sur Sophos Endpoint et comment la solution peut aider votre organisation à mieux se défendre contre les attaques avancées actuelles, dont les ransomwares distants, contactez un expert Sophos ou votre partenaire dès aujourd'hui. Vous pouvez également tester la solution dans votre propre environnement avec à un essai gratuit et sans engagement de 30 jours.

1 Rapport de défense numérique Microsoft. https://www.microsoft.com/fr-fr/security/security-insider/microsoft-digital-defense-report-2023

2 Burt, T. (5 octobre 2023). L'espionnage alimente les cyberattaques mondiales. Microsoft. https://blogs.microsoft.com/on-the-issues/2023/10/05/microsoft-digital-defense-report-2023-global-cyberattacks/

Sophos fournit des solutions de cybersécurité de pointe aux entreprises de toutes tailles, les protégeant en temps réel contre les menaces avancées telles que les malwares, les ransomwares et le phishing. Grâce à des fonctionnalités Next-Gen éprouvées, les données de votre entreprise sont sécurisées efficacement par des produits alimentés par l'intelligence artificielle et le Machine Learning.

2023-12-06 (WP-DD)

SOPHOS