SOPHOS

LES BONNES PRATIQUES ENDPOINT POUR BLOQUER LES RANSOMWARES

Livre blanc Sophos Juillet 2020

Les bonnes pratiques Endpoint pour bloquer les ransomwares

Dans notre enquête menée auprès de 5 000 responsables informatiques dans 26 pays, 51 % des répondants ont révélé avoir été touchés par un ransomware en 2019. Dans 73 % des cas, les attaquants sont parvenus à chiffrer les données. En outre, le coût moyen global de remédiation d'une attaque était d'environ 680 000 € (761 106 $).

Une des méthodes les plus efficaces pour se protéger contre les ransomwares est de bien configurer sa protection Endpoint. Dans ce livre blanc, nous analysons le mode opératoire des attaques de ransomware et les moyens nécessaires pour les bloquer, et nous passons en revue les bonnes pratiques à mettre en œuvre pour configurer votre protection Endpoint.

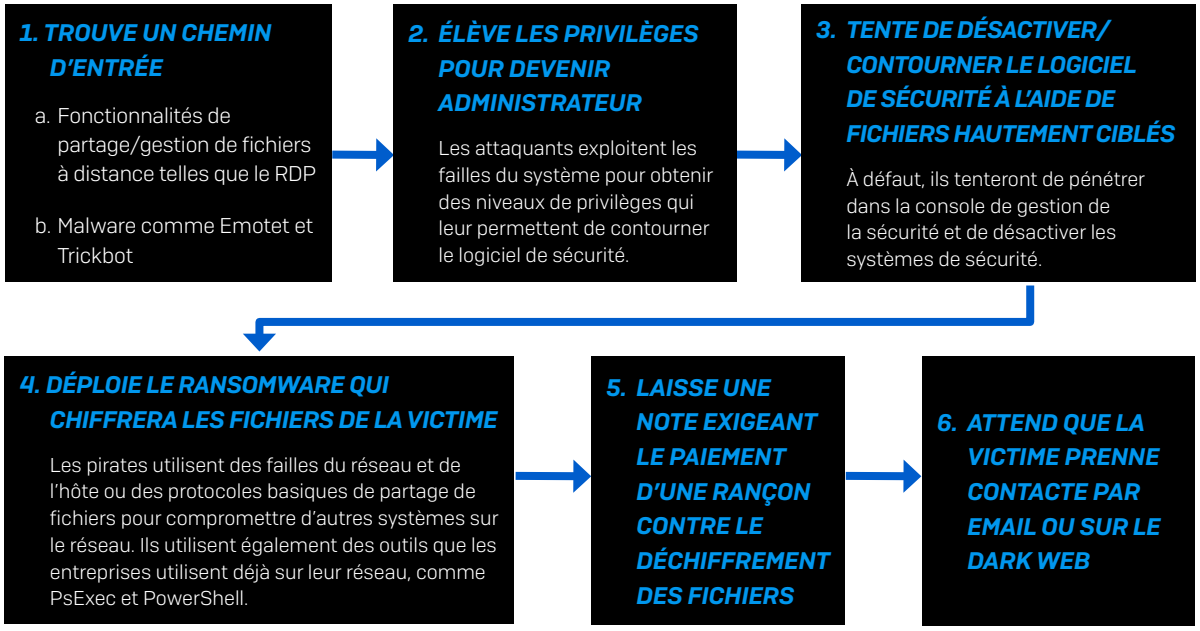
Méthodes de déploiement des attaques de ransomware

Ces dernières années, les attaques de ransomware ont peu à peu délaissé les attaques massives par force brute pour se concentrer sur des attaques ciblées, planifiées et exécutées manuellement, qui sont beaucoup plus difficiles à détecter et à bloquer. Analysons ensemble le fonctionnement de différentes formes de ransomware et les mesures que devrait prendre votre organisation pour s'en prémunir.

Les attaques de ransomware ciblées

Les attaques ciblées de ransomware demandent un fort investissement manuel, se concentrent sur une seule victime à la fois et réclament souvent des rançons exorbitantes. Les attaquants trouvent un chemin d'entrée sur le réseau et se déplacent latéralement, identifiant au passage les ressources de grande valeur. Pour toucher simultanément le plus de systèmes possible, ces attaques sont souvent lancées aux moments les plus inopportuns pour les victimes : la nuit, les week-ends ou pendant les vacances. Elles exploitent également plusieurs techniques afin de contourner les différentes couches de protection, ce qui les rend particulièrement efficaces.

Mode opératoire classique d'une attaque ciblée de ransomware :



Les conséquences pour la victime peuvent être désastreuses. En effet, les cyberpirates sont de plus en plus audacieux et vont jusqu'à exiger des rançons à 6 chiffres. En outre, notre enquête a révélé que le paiement de la rançon doublait le coût de remédiation d'une attaque – plus de 1,4 million de dollars en moyenne à l'échelle mondiale.

Protocole RDP ou Protocole de Déploiement de Ransomware ?

Le RDP (Remote Desktop Protocol) ainsi que d'autres outils de partage de bureau, comme Virtual Network Computing (VNC), sont des fonctions légitimes et très pratiques, qui permettent aux administrateurs d'accéder et de gérer des systèmes à distance. Malheureusement, en l'absence de mesures de protection adéquates, ces outils sont une voie royale pour les attaquants qui les utilisent pour déployer leur ransomware.

Ne pas sécuriser correctement le RDP et d'autres protocoles de gestion à distance similaires derrière un réseau privé virtuel (VPN), ou au moins restreindre les adresses IP pouvant se connecter via le RDP, peut vous exposer à ces attaques. En effet, les attaquants utilisent souvent des outils de piratage par force brute qui vont essayer des centaines de milliers de noms d'utilisateurs et de mots de passe jusqu'à trouver la bonne combinaison et compromettre votre réseau.

Bonnes pratiques pour se protéger contre les ransomwares

Se protéger contre les ransomwares ne consiste pas uniquement à installer les dernières solutions de cybersécurité. Il est également essentiel de mettre en œuvre de bonnes pratiques de sécurité informatique, dont des formations régulières du personnel, dans le cadre de la stratégie de sécurité globale de l'organisation. Pour cela, assurez-vous de suivre ces 10 bonnes pratiques :

1. Patchez au plus tôt et fréquemment

Les malwares recherchent souvent des failles dans les applications courantes. Plus vous patcherez tôt vos postes, serveurs, appareils mobiles et applications, moins vous aurez de vulnérabilités pouvant être exploitées.

2. Sauvegardez régulièrement et conservez une copie récente hors ligne et hors site

Dans notre enquête, 56 % des responsables IT dont les données ont été chiffrées ont pu les restaurer grâce à des sauvegardes. Pour ne pas avoir à vous soucier des sauvegardes dans le Cloud ou des périphériques de stockage qui pourraient tomber entre de mauvaises mains, chiffrez vos sauvegardes et conservez-les hors-ligne et hors-site. En outre, élaborez un plan de reprise d'activité qui couvre la restauration des données.

3. Activez la visualisation des extensions de fichier

Windows cache par défaut l'extension des fichiers, vous obligeant à vous fier aux icônes pour les identifier. Afficher les extensions permet de détecter plus facilement les types de fichiers que vous et vos utilisateurs n'avez pas l'habitude de recevoir, tels que les fichiers JavaScript.

4. Ouvrez les fichiers JavaScript (.JS) dans Notepad

Ouvrir un fichier JavaScript dans Notepad l'empêche d'exécuter un script malveillant et vous permet d'examiner son contenu.

5. Désactivez les macros des documents MS dans les pièces jointes

Par mesure de sécurité, Microsoft a délibérément désactivé par défaut l'auto-exécution des macros il y a plusieurs années. Un grand nombre d'infections ont besoin que vous activiez vous-mêmes les macros pour réussir leurs attaques, alors ne le faites pas !

6. Soyez prudent avec les pièces jointes non sollicitées

Les cybercriminels se basent souvent sur un vieux dilemme : savoir qu'il ne faut pas ouvrir un document avant d'être sûr qu'il est légitime, mais ne pas pouvoir dire s'il est malveillant ou non avant de l'avoir ouvert. En cas de doute, abstenez-vous.

7. Contrôlez les droits administrateur

Réexaminez constamment qui dans votre organisation a des droits d'administrateur local et domaine. Identifiez les personnes et retirez les droits de celles qui n'en ont pas besoin. Ne restez pas connecté en tant qu'administrateur plus longtemps que ce dont vous avez besoin, et évitez de naviguer sur Internet, d'ouvrir des documents ou de réaliser d'autres activités usuelles en tant qu'admin.

8. Maintenez vos applications professionnelles à jour et restez informé des dernières fonctions de sécurité

Par exemple, Office 2016 est doté de la commande « Bloquer l'exécution des macros dans les fichiers Office provenant d'Internet » qui vous protège contre les contenus malveillants externes tout en vous permettant d'utiliser des macros en interne.

9. Contrôlez les accès réseau externes

Ne laissez pas de ports exposés au monde extérieur. Verrouillez l'accès RDP et tous les autres protocoles de gestion à distance de votre organisation. De plus, utilisez l'authentification multi-facteur et assurez-vous que vos utilisateurs s'authentifient via un VPN.

10. Utilisez des mots de passe complexes

On ne saurait trop insister sur ce point. Un mot de passe faible et prévisible peut permettre aux pirates d'accéder à l'ensemble de votre réseau en quelques secondes. Nous recommandons de les rendre impersonnels, d'utiliser au moins 12 caractères mélangeant des majuscules, des minuscules et des signes de ponctuation Ju5te.CoMM3ça !

Bonnes pratiques pour votre protection Endpoint

En complément d'un pare-feu de nouvelle génération, l'une des méthodes les plus efficaces pour se protéger contre les attaques de ransomware consiste à utiliser une protection Endpoint. Toutefois, celle-ci doit être configurée correctement afin de fournir une protection optimale.

Suivez ces bonnes pratiques pour protéger vos systèmes Endpoint contre les ransomwares :

1. Activez toutes vos politiques et vérifiez que tous les paramètres désirés sont actifs

Cela peut sembler évident, mais c'est un moyen sûr d'obtenir la meilleure protection Endpoint possible. Les politiques de sécurité sont conçues pour bloquer des menaces spécifiques, et en vérifiant régulièrement qu'elles sont toutes activées, vous vous assurez que vos ordinateurs sont protégés, en particulier contre les nouvelles familles de ransomware.

De plus, il est essentiel d'activer les fonctionnalités qui détectent les techniques d'attaque sans fichier et les comportements des ransomwares pour empêcher les criminels d'infiltrer vos postes et de déployer un ransomware. Ces fonctionnalités vous permettent également de remédier plus facilement aux attaques si elles parviennent à s'infiltrer d'une manière ou d'une autre dans votre environnement.

2. Vérifiez régulièrement vos exclusions

Les exclusions (qui empêchent l'analyse de répertoires et de types de fichier de confiance à la recherche de logiciels malveillants) sont parfois utilisées pour satisfaire les demandes des utilisateurs qui estiment que la solution de protection ralentit leur système. Les exclusions peuvent également être utilisées pour réduire les risques de faux positifs potentiels.

Avec le temps, la liste de répertoires et de types de fichiers exclus peut finir par affecter un nombre croissant de personnes sur le réseau. Et les malwares qui parviennent à se frayer un chemin jusqu'aux répertoires exclus (qui peuvent avoir été déplacés accidentellement par un utilisateur) ont toutes les chances de réussir parce qu'ils seront d'emblée exclus de l'analyse.

Veillez à vérifier régulièrement votre liste d'exclusions dans vos paramètres de protection et à maintenir le nombre d'exclusions aussi proche de zéro que possible.

3. Activez l'authentification multi-facteur sur votre console

L'authentification multi-facteur, ou MFA pour Multi-Factor Authentication, fournit une couche de sécurité supplémentaire au premier facteur d'authentification - qui consiste généralement en un mot de passe. Il est conseillé d'activer la MFA dans toutes vos applications et de l'appliquer systématiquement pour tous les utilisateurs qui ont accès à votre console de sécurité.

Cela garantit que l'accès à votre protection Endpoint est sécurisé et qu'aucune modification accidentelle ou malveillante ne soit apportée à vos paramètres, ce qui pourrait affaiblir la protection de vos postes. Il est également essentiel d'activer la MFA pour sécuriser le RDP.

4. Assurez-vous que tous les systèmes Endpoint sont bien protégés

Un moyen rapide d'assurer une protection optimale est de vérifier régulièrement que vos ordinateurs sont protégés et à jour. Un appareil qui ne fonctionne pas correctement peut ne pas être protégé et être ainsi vulnérable à une attaque de ransomware. Les outils de sécurité Endpoint fournissent souvent ces informations, et il est utile de mettre en œuvre un programme de maintenance de la sécurité informatique pour surveiller régulièrement la présence de problèmes potentiels.

5. Assurez la maintenance régulière de la sécurité du système informatique

Maintenir une hygiène informatique régulière garantit que vos postes et les logiciels qui y sont installés fonctionnent avec un maximum d'efficacité. Non seulement cela atténue vos risques de cybersécurité, mais cela vous fera gagner un temps précieux en cas de futurs problèmes.

Il est particulièrement important de mettre en œuvre un programme de maintenance de la sécurité informatique pour se prémunir contre les attaques de ransomware et d'autres cybermenaces. Par exemple : s'assurer que le RDP ne fonctionne que là où vous en avez besoin, vérifier régulièrement les problèmes de configuration, surveiller les performances des appareils et supprimer les programmes indésirables ou inutiles. Le contrôle de l'hygiène informatique peut vous informer sur la nécessité de mettre à jour certaines applications logicielles, y compris votre logiciel de sécurité. C'est aussi un moyen sûr de garantir que vos données sont sauvegardées régulièrement.

6. Faites la chasse aux indices d'attaquants actifs dans votre réseau

Dans le paysage actuel des menaces, les acteurs malveillants sont plus rusés que jamais, déployant des techniques furtives pour mener des attaques de ransomware dévastatrices. Les organisations ont besoin d'outils qui leur permettent de poser des questions détaillées afin de pouvoir identifier les menaces avancées et les adversaires actifs. Une fois ces menaces trouvées, les organisations ont également besoin d'outils pour prendre rapidement les mesures appropriées afin de les bloquer.

Si votre solution Endpoint est dotée de fonctions EDR (Endpoint Detection and Response) assurez-vous qu'elles sont activées et que vous les utilisez.

7. Complétez par une couche d'expertise et d'action humaine – le ransomware n'est que la partie émergée de l'attaque

Le ransomware n'est que la phase finale pour les pirates. Pour déployer un ransomware, ils auront déjà pénétré votre réseau et éventuellement exfiltré des données à votre insu – parfois même des mois avant qu'une attaque n'ait lieu.

La technologie seule ne suffit souvent pas pour arrêter ces intrusions. Prenez l'exemple d'une caméra de sécurité : elle vous permet de voir comment les voleurs pénètrent dans votre propriété, mais ce n'est qu'avec des agents de sécurité que vous pouvez empêcher le vol. La même chose peut s'appliquer à la cybersécurité. La meilleure façon de se prémunir véritablement contre ce type d'intrusion est d'ajouter une couche d'expertise humaine dans la stratégie de sécurité informatique.

Les services MDR (Managed Service and Response) sont essentiels à cet égard. En associant vos équipes IT internes à une équipe externe d'experts de haut vol spécialisés dans la traque des menaces et leur remédiation vous bénéficiez de conseils pratiques pour remédier aux causes profondes des incidents récurrents.

Sophos Intercept X Advanced with EDR

Sophos Intercept X Advanced with EDR inclut toutes les fonctionnalités dont vous avez besoin pour protéger votre organisation contre les attaques de ransomware, telles que Ryuk, Sodinokibi, Maze et Ragnar Locker.

Intercept X est doté de la technologie anti-ransomware qui détecte les processus de chiffrement malveillants et les stoppe avant qu'ils ne puissent se propager sur votre réseau. La technologie anti-exploit stoppe la propagation et l'installation du ransomware, le Deep Learning bloque le ransomware avant qu'il ne s'exécute et CryptoGuard empêche le chiffrement malveillant des fichiers et les restaure vers leur état d'origine sain.

De plus, Sophos EDR vous aide à maintenir l'hygiène de vos opérations informatiques sur l'ensemble de votre parc informatique. Sophos EDR permet à votre équipe de poser des questions détaillées pour identifier les menaces avancées, les attaquants actifs et les failles informatiques potentielles, puis de prendre les mesures appropriées pour les bloquer. Il vous permet de détecter les attaquants passés entre les mailles du filet qui se cachent sur votre réseau et attendent de déployer un ransomware.

Sophos Managed Threat Response (MTR)

Le service Sophos MTR ajouter de l'expertise humaine à votre stratégie de sécurité multicouche. Une équipe de haut vol spécialisée dans la traque des menaces recherche les menaces pour vous de manière proactive. Si vous les autorisez, ces experts prennent des mesures pour intercepter, contenir et neutraliser les menaces, et vous fournissent des conseils pratiques pour remédier aux causes profondes des incidents récurrents.

Conclusion

Bien qu'ils soient déjà bien implantés dans le paysage actuel des cybermenaces, les ransomwares ne cesseront jamais d'évoluer. Nous ne parviendrons peut-être jamais à les éradiquer complètement, mais en suivant les bonnes pratiques de protection Endpoint décrites dans ce document, votre organisation aura les meilleures chances de se protéger contre les dernières menaces.

En résumé :

1. Activez toutes vos politiques et vérifiez que tous les paramètres désirés sont actifs
2. Vérifiez régulièrement vos exclusions
3. Activez l'authentification multi-facteur (MFA) sur votre console
4. Assurez-vous que tous les systèmes Endpoint sont bien protégés
5. Assurez la maintenance régulière de la sécurité du système informatique
6. Faites la chasse aux indices d'attaquants actifs dans votre réseau
7. Complétez par une couche d'expertise et d'action humaine – Le ransomware n'est que la partie émergée de l'attaque

Essayez Sophos Intercept X gratuitement à la page www.sophos.fr/endpoint

Pour en savoir plus sur Sophos MTR, aller sur www.sophos.fr/MTR

Équipe commerciale France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

200702 WPFR (NP)

SOPHOS