SOPHOS
Cybersecurity delivered.

# Les bonnes pratiques de protection Endpoint pour bloquer les ransomwares

## Des conseils pratiques pour configurer votre solution Endpoint de manière optimale

*Un livre blanc Sophos. Septembre 2022*

Le nombre d'attaques de ransomware a explosé l'année dernière, avec des conséquences souvent désastreuses pour les organisations touchées.

66 % des personnes interrogées dans le cadre de notre enquête 'L'état des ransomwares 2022' ont déclaré que leur organisation avait été victime d'un ransomware l'an dernier, soit une augmentation de 78 % en un an. Des données ont été chiffrées par les attaquants dans près des deux tiers de ces incidents (65 %).

Le coût moyen de remédiation d'une attaque de ransomware s'élève globalement à 1,4 million de dollars. En outre, 90 % des victimes ont déclaré que l'attaque avait eu un impact sur leur capacité à fonctionner, tandis que 86 % des entreprises du secteur privé ont déclaré qu'elle avait entraîné une perte de clientèle ou de chiffre d'affaires.[1]

La hausse de ces attaques s'inscrit dans un phénomène de prolifération des menaces plus large : 72 % des participants ont constaté une intensification du volume, de la complexité et de l'impact des cyberattaques au cours de l'année dernière.

L'un des moyens les plus efficaces pour se défendre contre les ransomwares est de configurer correctement sa solution de protection Endpoint. Ce livre blanc analyse le mode opératoire des attaques de ransomware et les moyens nécessaires pour les bloquer. Il passe également en revue les bonnes pratiques à mettre en œuvre pour bien configurer votre protection Endpoint.

## Méthodes de déploiement des attaques de ransomware

Il existe autant d'auteurs de ransomware que de types d'attaques de ransomware différents. Certaines attaques sont très ciblées, tandis que d'autres sont plus opportunistes. Souvent, les attaquants scannent les réseaux à la recherche de vulnérabilités qui leur fourniront un accès à ces réseaux. Après avoir attaqué un centre éducatif canadien, un gang de ransomware a d'ailleurs rapporté :

*« Vous aviez une ancienne vulnérabilité critique Log4j non corrigée sur Horizon, c'est ainsi que nous avons pu pénétrer initialement. Il s'agissait d'un scan effectué en masse ; on ne vous visait pas spécialement. »*

Cet aveu met clairement en évidence l'exploitation par les attaquants des vulnérabilités non corrigées. C'est d'ailleurs la principale méthode de pénétration utilisée dans les cyberattaques (pas uniquement les ransomwares) sur lesquelles sont intervenus les experts en réponse de Sophos l'an dernier.

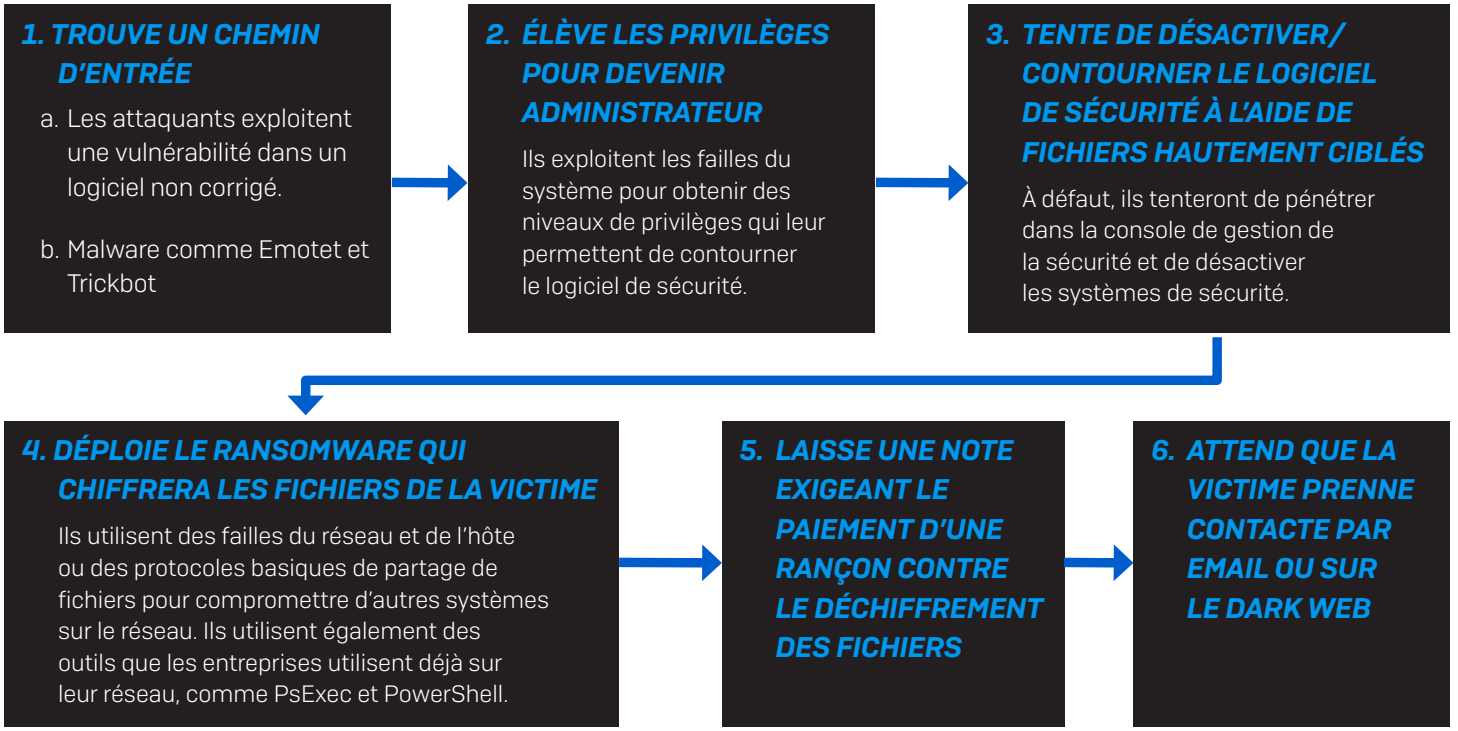
La hausse récente du volume d'attaques de ransomware peut être attribuée en grande partie à l'essor du modèle RaaS ou Ransomware-as-a-service. Les acteurs malveillants qui développent les ransomwares utilisent aujourd'hui ce modèle pour s'attaquer aux organisations.

Avec le modèle RaaS, un groupe de cybercriminels peut créer un ransomware et le louer à d'autres attaquants. Cela rend les ransomwares accessibles à un plus grand nombre d'attaquants que jamais auparavant.

Dès lors que ces derniers accèdent à l'environnement de leurs victimes, ils passent alors plusieurs jours, plusieurs semaines, voire plusieurs mois à explorer le réseau, à élever leurs privilèges, à exfiltrer des données ou à installer des malwares. En 2021, le temps de présence des ransomwares était en moyenne de 11 jours.[2] Cela offre aux défenseurs une fenêtre pour identifier et bloquer les intrus avant l'attaque.

1 L'état des ransomwares 2022 - Sophos
2 The Active Adversary Playbook 2022 - Sophos

Mode opératoire classique d'une attaque ciblée de ransomware :




## Protocole RDP ou Protocole de Déploiement de Ransomware ?

Le protocole RDP (Remote Desktop Protocol) a joué un rôle dans au moins 83 % des cyberattaques prises en charge par l'équipe de réponse aux incidents de Sophos en 2021, contre 73 % l'année précédente.[3]

Le RDP et les outils de partage de bureau comme Virtual Network Computing (VCN) sont des fonctionnalités légitimes et très utiles aux administrateurs qui leur permettent d'accéder aux systèmes et de les gérer à distance. Malheureusement, en l'absence de mesures de protection appropriées, ces outils sont couramment exploités par les auteurs de ransomware.

Notons toutefois l'apparition d'un changement dans la façon dont les attaquants utilisent le RDP. Dans 70 % des incidents analysés par Sophos, le RDP a été utilisé uniquement pour l'accès interne et les mouvements latéraux. Pour l'accès externe, il n'a été utilisé *que dans 1 % des cas*, et 12 % des attaques ont montré que les adversaires ont utilisé le RDP pour l'accès externe et le mouvement interne.[4]

3 The Active Adversary Playbook 2022 - Sophos
4 The Active Adversary Playbook 2022 - Sophos

Il est donc essentiel d'empêcher les attaquants d'utiliser le RDP pour les accès externes, les accès internes et les mouvements latéraux.

## Bonnes pratiques pour se protéger contre les ransomwares

Pour se protéger contre les ransomwares, il ne suffit pas d'installer les solutions de cybersécurité les plus récentes. Il est indispensable d'adopter de bonnes pratiques de sécurité informatique, en particulier de bien former les employés de manière régulière. Assurez-vous de mettre en place ces neuf bonnes pratiques :

### 1. Patchez au plus tôt et fréquemment

L'exploitation de vulnérabilités non corrigées a été la cause première de près de la moitié (47 %) des incidents investigués par Sophos en 2021.[5] Les malwares exploitent souvent les failles de sécurité des applications les plus utilisées. Plus vous appliquez tôt les correctifs à vos endpoints, serveurs, mobiles et applications, moins de failles pourront être exploitées par les cybercriminels.

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

Dans notre enquête 'L'état des ransomwares 2022', 73 % des responsables informatiques dont les données avaient été chiffrées ont pu les restaurer à l'aide de sauvegardes. Chiffrez vos sauvegardes et conservez-les hors ligne et hors site. Vous éviterez ainsi les problèmes de sauvegarde dans le Cloud ou de périphériques de stockage tombant entre de mauvaises mains. En plus de cela, restaurez régulièrement vos données à partir des sauvegardes.

### 3. Activez la visualisation des extensions de fichier

Le paramètre par défaut de Windows est de masquer les extensions de fichiers, vous obligeant à utiliser leurs vignettes pour les identifier. Activez les extensions pour repérer plus facilement les fichiers JavaScript (JS) et les autres types de fichiers que vous et vos utilisateurs n'ont pas l'habitude de recevoir.

### 4. Ouvrez les fichiers JS dans Notepad

L'ouverture d'un fichier JS dans Notepad l'empêche d'exécuter des scripts malveillants et vous permet d'examiner son contenu.

### 5. N'activez pas les macros des pièces jointes reçues par email

Par mesure de sécurité, Microsoft a délibérément désactivé par défaut l'auto-exécution des macros il y a plusieurs années. De nombreux fichiers malveillants tenteront de vous persuader de réactiver les macros. Ne le faites pas !

### 6. Soyez prudent avec les pièces jointes non sollicitées

Les cybercriminels font souvent appel à un vieux dilemme : nous savons qu'il ne faut pas ouvrir un document avant d'être sûr qu'il est légitime, mais nous ne pouvons pas dire s'il est malveillant ou non avant de l'avoir ouvert. Dans le doute, ne l'ouvrez pas, tout simplement.

### 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 nécessaire. Et évitez de naviguer sur Internet, d'ouvrir des documents ou d'effectuer des tâches professionnelles régulières lorsque vous utilisez vos droits

5 The Active Adversary Playbook 2022 - Sophos

administrateur.

**8. Réglementez l'accès aux réseaux internes et externes**

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

**9. Utilisez des mots de passe complexes**

On ne saurait trop insister sur ce point. Un mot de passe faible et prévisible peut permettre aux hackers d'accéder à l'ensemble de votre réseau en quelques secondes. Nous recommandons de choisir des mots de passe uniques, composés d'au moins douze caractères, mêlant lettres majuscules et lettres minuscules, et d'ajouter une ponctuation aléatoire C0mM3*Ce1a!

## Bonnes pratiques pour votre protection Endpoint

Outre les solutions de sécurité réseau, l'utilisation d'une solution XDR (Extended Detection and Response) dotée de technologies avancées de prévention et des capacités de chasse aux menaces est l'une des méthodes les plus efficaces pour se protéger contre les attaques de ransomware.

Mais pour offrir une cyber protection maximale, ces technologies doivent être configurées correctement.

Nous vous recommandons donc de suivre ces sept bonnes pratiques pour bien protéger vos endpoints contre les ransomwares :

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

Cela peut paraître évident, mais c'est une condition sine qua non pour obtenir la meilleure protection Endpoint possible. Les politiques de sécurité sont conçues pour bloquer des menaces spécifiques. Le fait de vérifier régulièrement que toutes les options de protection sont activées permet de s'assurer que vos endpoints sont protégés contre les ransomwares actuels et émergents. Les deux mesures suivantes sont fortement conseillées :

**A) Activer la protection antialtération**

Cela empêche toute modification ou suppression non autorisée de logiciels de cybersécurité. L'une des premières actions visées par les attaquants et les malwares après avoir accédé au système est d'essayer de désactiver ou de supprimer localement tout logiciel de sécurité présent.

**B) Activer la journalisation analytique (idéalement dans le Cloud)**

Si vous êtes attaqué, vous voudrez savoir ce qui s'est passé. Très souvent, la plupart des données ne seront plus disponibles car les attaquants auront effacé les journaux du système pour dissimuler leurs traces. Ou alors vous pouvez perdre l'accès à votre appareil. Enregistrer ses activités dans le Cloud (par exemple dans le Sophos Data Lake) vous permet de conserver des informations importantes.

Enfin, activez les fonctions qui détectent les techniques d'attaque sans fichier et les comportements de ransomware afin d'empêcher

les criminels d'infiltrer vos endpoints et de déployer des souches de ransomwares néfastes.

Les clients Sophos qui gèrent leur sécurité Endpoint dans Sophos Central bénéficient de l'outil « Vérifier l'état du compte », qui évalue automatiquement la configuration de votre compte pour identifier les failles potentielles et vous aide à les modifier afin d'optimiser la protection. Cliquez ici pour accéder à notre outil.

### 2. Vérifiez régulièrement vos exclusions

Les exclusions empêchent la recherche de malwares dans les répertoires et les types de fichiers de confiance. Elles sont parfois utilisées pour réduire les délais du système et minimiser le risque de faux positifs dans les alertes de sécurité.

Au fil du temps, une liste grandissante de répertoires et de types de fichiers exclus peut avoir un impact sur de nombreuses personnes sur un réseau. Les logiciels malveillants qui parviennent à s'introduire dans des répertoires exclus (peut-être déplacés accidentellement par un utilisateur) ont toutes les chances de réussir.

Vérifiez régulièrement votre liste d'exclusions dans vos paramètres de protection et limitez leur nombre. Pour celles que vous ne pouvez pas supprimer, faites en sorte qu'elles soient aussi spécifiques que possible. Par exemple, plutôt que d'exclure un répertoire ou un lecteur d'une base de données, excluez uniquement des fichiers spécifiques avec leur chemin complet. Vous empêcherez ainsi le malware de contourner votre sécurité et de s'exécuter à partir du même dossier.

### 3. Activez l'authentification multi-facteur (MFA) sur votre console

La MFA fournit une couche de sécurité supplémentaire au premier facteur d'authentification — qui consiste généralement en un mot de passe. Il est essentiel d'activer la MFA sur l'ensemble de vos applications pour tous les utilisateurs ayant accès à votre console de sécurité. Cela garantit que l'accès à votre solution de sécurité Endpoint est sécurisé et reste protégé contre les tentatives accidentelles ou délibérées de modifier vos paramètres, ce qui pourrait rendre vos endpoints vulnérables aux attaques. Il est également essentiel d'activer la MFA pour sécuriser le RDP.

### 4. Assurez-vous que tous les endpoints sont bien protégés

Vérifiez régulièrement vos appareils pour savoir s'ils 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. Un programme de maintenance informatique s'avère également utile pour vérifier régulièrement les problèmes informatiques potentiels.

### 5. Maintenez une bonne hygiène informatique

Instaurer une maintenance informatique régulière garantit que vos systèmes, et les logiciels qui y sont installés, fonctionnent avec une efficacité maximale. Cette pratique limite vos risques de cybersécurité et peut vous faire gagner du temps lorsque vous devez remédier à des incidents futurs.

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 bon moyen de s'assurer que vos données sont sauvegardées régulièrement.

### 6. Chassez activement les adversaires actifs sur votre réseau

Dans le paysage actuel des menaces, les acteurs malveillants sont plus rusés que jamais. Ils déploient souvent des outils légitimes et utilisent des identifiants volés pour éviter la détection. Afin d'identifier et de bloquer ces attaques de type « living off-the-land », il est indispensable de chasser de manière proactive les menaces avancées et les adversaires actifs. Une fois découverts, vous devez également être capables de prendre les mesures nécessaires pour les bloquer rapidement.

Les technologies Endpoint telles que l'EDR (Endpoint Detection and Response) et le XDR (Extended Detection and Response) fournissent des fonctions de chasse aux menaces et de neutralisation. Les organisations disposant de ces technologies devraient en tirer pleinement parti.

Bon nombre d'entreprises peinent à maintenir une couverture 24 h/24 pour se protéger contre les attaques avancées de ransomware. C'est pourquoi les services gérés de détection et de réponse ou MDR (Managed Detection and Response) jouent un rôle essentiel. Les services MDR fournissent une chasse aux menaces 24 h/24 et 7 j/7, orchestrée par des experts spécialisés dans la détection et la réponse aux cyberattaques, que les solutions technologiques seules ne peuvent pas assurer. Ils offrent également le plus haut niveau de protection contre les attaques de ransomware avancées pilotées par des humains.

## Sophos protège contre les ransomwares

Nous offrons une technologie de protection multi-couche contre les menaces (Sophos Endpoint Protection)

Sophos Intercept X Endpoint détecte et bloque 99,98 % des attaques avant qu'elles ne puissent s'exécuter. Cette solution repose sur une protection multi-couche avancée, qui comprend :

- Une technologie comportementale anti-ransomware qui détecte les processus de chiffrement malveillants et restaure les fichiers vers leur état d'origine sain.
- Des fonctionnalités anti-exploit qui détectent les techniques d'attaque sans fichier.
- Des modèles de Deep Learning basés sur l'IA qui identifient et bloquent les ransomwares avant qu'ils ne puissent s'exécuter.

L'outil intégré « Vérifier l'état du compte » évalue automatiquement la configuration de votre compte pour repérer les failles de sécurité potentielles, comme les politiques ou les fonctionnalités qui ne seraient pas activées. Il fournit également des conseils pratiques pour remédier aux problèmes identifiés et optimiser votre protection.

De plus, la plateforme de gestion Sophos Central applique automatiquement la MFA pour toute demande d'accès, renforçant la sécurité de votre console.

### Outils proactifs pour la chasse aux menaces et l'hygiène informatique (Sophos XDR)

Sophos XDR fournit des outils sophistiqués qui vous permettent de chasser les menaces et de maintenir une bonne hygiène informatique sur l'ensemble de votre parc. Il permet à votre équipe de lancer des requêtes détaillées pour identifier les menaces avancées, les adversaires actifs, les appareils non protégés et les vulnérabilités informatiques potentielles, et pouvoir ainsi les bloquer rapidement.

Vous disposez d'un accès aux données de l'appareil en temps réel, de 90 jours de données sur disque, de 30 jours de données stockées dans le référentiel Cloud Sophos Data Lake et d'une liste d'éléments suspects générée automatiquement. Avec cela, vous avez toutes les informations dont vous avez besoin pour commencer votre investigation et chasser les ransomwares actifs.

## Service MDR 24 h/24, 7 j/7 (Sophos MDR)

Avec Sophos MDR, vous bénéficiez d'une équipe de chasseurs d'élite disponible 24 h/24 et 7 j/7 qui détecte les attaques et y remédie à votre place. Forts de leur expérience, qui se compte en milliers d'heures, nos experts ont déjà vu et traité tout ce qu'un attaquant est capable de faire avec un ransomware. Ils vous assurent une protection ultime contre ce type de menaces.

## Conclusion

Les ransomwares continuent d'évoluer. Nous ne parviendrons peut-être jamais à les éradiquer, mais nos bonnes pratiques de protection Endpoint permettront à votre entreprise d'être protégée de manière optimale contre ces 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 de sécurité.
4. Assurez-vous que chaque endpoint est bien protégé avec une solution à jour.
5. Maintenez une bonne hygiène informatique.
6. Chassez les adversaires actifs sur votre réseau.

Pour en savoir plus sur Sophos XDR, consultez la page www.sophos.com/xdr

Pour en savoir plus sur Sophos MTR, consultez la page www.sophos.fr/MDR

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.



2022-09-01 FR-WP (DD)

SOPHOS