



Les 40 principales techniques des ransomwares et l'art de les déjouer

Un guide de défense active et d'utilisation
de techniques de leurre

Introduction

Nombre de livres blancs, guides et rapports sur les ransomwares démarrent souvent de la même façon. Le premier paragraphe est truffé de statistiques sur le « coût des ransomwares », une place honorable est accordée aux variantes récentes et les secteurs d'activité les plus touchés sont brièvement évoqués avant de passer aux informations vraiment utiles.

Nul besoin de multiplier les commentaires alarmistes pour vous dire ce que vous savez déjà : personne n'aime les ransomwares, ils pèsent lourdement sur le business et les entreprises en sont victimes chaque année.

En tant que défenseur, il devient essentiel de mieux nous préparer à déjouer cette menace.

Sommaire

Introduction	4
De l'intérêt de ce guide ?	4
Pourquoi miser sur une défense active et des leurres ?	4
Conseils de mise en œuvre	4
Les 40 principales techniques utilisées par les ransomwares	5
Perspectives finales	14
Pour poursuivre la réflexion	14

De l'intérêt de ce guide

Vous consacrez déjà beaucoup d'efforts pour traiter les menaces qui pèsent sur votre sécurité. Mais comme en témoigneront les entreprises les mieux protégées au monde, aucune mesure de sécurité n'est totalement infaillible. Vous pouvez toutefois adopter dès maintenant des mesures simples, sans déployer d'outils complexes, ni investir des sommes considérables, afin de mieux vous protéger contre les ransomwares.

Ce guide a pour vocation de vous aider à agir en ce sens : prendre des mesures que vous maîtrisez pour vous protéger contre les ransomwares. Il vous aide à limiter la propagation des ransomwares et à en réduire l'impact.

Pourquoi miser sur une défense active et des leurres ?

La plupart des solutions aux problématiques de sécurité adoptent une approche cloisonnée. Vous voulez protéger les terminaux ? Protégez-les avec un EDR. Vous souhaitez améliorer votre visibilité ? Optez pour l'analyse du trafic réseau. Un comportement malveillant ? Faites appel à l'UEBA.

Les ransomwares interagissent avec toutes les entités de votre environnement informatique. Si vous concentrez vos efforts sur un seul périmètre, les résultats seront décevants. Pour faire face à un phénomène tel que les ransomwares, vous devez adopter une approche globale. Pour être efficace, votre stratégie doit couvrir les domaines critiques de votre environnement.

Une « défense active » y contribue. L'approche prend en compte différents cas d'utilisation pour garantir des résultats pertinents. Vous pouvez choisir le cas d'utilisation (en l'occurrence, le ransomware) et cibler les domaines dans lesquels vous souhaitez être le plus efficace (voir les conseils de mise en œuvre).

Comment une défense active contribue-t-elle à déjouer les ransomwares ?

- Créer une surface d'attaque factice à l'aide de leurres, dans le but de tromper l'adversaire.
- Réduire la surface d'attaque à l'aide de fonctions particulièrement efficaces pour éliminer les options à disposition de l'adversaire.
- Trouver des moyens astucieux et efficaces pour surveiller la surface d'attaque ouverte, afin de piéger les adversaires lorsqu'ils exécutent certaines phases inévitables de leur attaque.

Conseils de mise en œuvre

Nous vous recommandons de concentrer vos efforts sur les domaines suivants de votre environnement :

- DMZ
- Active Directory
- Segments hébergeant des serveurs critiques
- Comptes d'utilisateurs privilégiés
- Postes de travail privilégiés

Une fois ces domaines sécurisés, vous pouvez envisager une mise en œuvre plus large en fonction des capacités et des ressources disponibles.

Nous sommes conscients que certaines des techniques présentées dans ce guide exigent un certain investissement en temps et en énergie. Une défense efficace exige et exigera toujours un minimum d'efforts. C'est la raison pour laquelle nous n'avons abordé que les stratégies ayant un impact réellement positif sur vos actions de détection et de protection.

Vous n'êtes pas obligé de mettre en œuvre l'ensemble des préconisations de ce guide. Il ne s'agit que de recommandations. Mais le fait de mettre en œuvre ne serait-ce qu'une partie d'entre elles peut vous aider à contrôler et à réduire la surface d'attaque ciblée par les ransomwares. Ce qui représente déjà en soi une grande victoire.

À qui s'adresse le guide ?

- Les professionnels désireux de déjouer les ransomwares à l'aide de pièges et leurres
- Les analystes du SOC
- Les responsables du SOC
- Toute personne concernée par les ransomwares

C'est parti !

Nous avons essayé de simplifier les choses autant que possible. Vous trouverez ci-dessous une liste de techniques utilisées par les ransomwares et les moyens de défense active correspondants, pour détecter le ransomware à un stade précoce ou freiner sa propagation. Nous avons également fourni des recommandations de mise en œuvre pour chaque tactique de défense active, avec un mapping aux techniques du référentiel MITRE Shield.

TACTIQUES / TECHNIQUES DES RANSOMWARES	DÉFENSE ACTIVE	POURQUOI ?	CONSEILS, ASTUCES & RECOMMANDATIONS	MAPPING À MITRE SHIELD
1 INFECTION INITIALE Infecte des ressources ouvertes comportant des vulnérabilités connues (telles que Wordpress/CMS, etc.).	Créer des applications de leurre sur Internet qui interceptent les ransomwares ciblant des ressources ouvertes présentant des vulnérabilités connues.	Une surface d'attaque factice est ainsi créée pour duper l'assaillant et perturber ses opérations.	Créer des leurres imitant les CMS Joomla ou Wordpress qui constituent des cibles privilégiées pour les assaillants.	Decoy Diversity > Application Diversity >
2 INFECTION INITIALE Utilisation de mots de passe communs (password spraying) sur des applications connues.	Créer des applications factices avec des mots de passe par défaut connus. Elles intercepteront les ransomwares qui tentent d'utiliser des mots de passe communs.	Une surface d'attaque factice est ainsi créée pour duper l'assaillant et perturber ses opérations.	Créer des leurres pour les applications comme Apache Tomcat et PhpMyAdmin.	Decoy Diversity > Application Diversity >

TACTIQUES / TECHNIQUES DES RANSOMWARES	DÉFENSE ACTIVE	POURQUOI ?	CONSEILS, ASTUCES & RECOMMANDATIONS	MAPPING À MITRE SHIELD
<p>3 INFECTION INITIALE</p> <p>Exploiter les vulnérabilités récemment divulguées (p. ex. une vulnérabilité de Microsoft Exchange).</p>	<p>Les hackers ciblent souvent des applications dont les vulnérabilités ont été récemment divulguées. Créez des leurres de ces applications pour attirer l'opérateur du ransomware.</p>	<p>Une surface d'attaque factice est ainsi créée pour duper l'assaillant et perturber ses opérations.</p>	<p>Créer des leurres d'applications telles que Microsoft Exchange et F5, dont les vulnérabilités ont été divulguées dans la presse.</p>	<p>Decoy Diversity > Application Diversity ></p>
<p>4 INFECTION INITIALE</p> <p>Attaque par force brute des serveurs RDP accessibles au public.</p>	<p>Bloquer les accès entrants sur le port RDP 3389 à partir du pare-feu de l'hôte/du réseau.</p> <p>Restreindre l'utilisation de RDP à des adresses IP connues (en particulier les serveurs cloud).</p>	<p>Réduit la surface d'attaque à disposition de l'assaillant en rendant les serveurs RDP inaccessibles. La propagation des ransomwares est limitée.</p>	<p>Utilisez le pare-feu Windows ou la console cloud pour bloquer tout accès à RDP.</p>	<p>Security Controls > Network Manipulation > Isolation ></p>
<p>5 INFECTION INITIALE</p> <p>Cibler des applications exécutées avec des privilèges d'administrateur.</p>	<p>Exécuter les applications DMZ avec un niveau minimal de privilèges.</p>	<p>Exécute les applications DMZ avec un niveau minimal de privilèges.</p>	<p>Exécuter les applications avec un niveau minimal de privilèges.</p>	<p>Admin Access ></p>
<p>6 INFECTION INITIALE</p> <p>Utilisation de PowerShell.</p>	<p>Bloquer PowerShell à l'aide de stratégies de groupe (GPO) ou d'un contrôle applicatif lorsque son utilisation n'est pas requise.</p> <p>Surveiller les connexions sortantes de PowerShell à l'aide du pare-feu Windows.</p> <p>Utiliser la fonction Script-block Logging.</p>	<p>Empêche l'exécution des ransomwares courants.</p> <p>Donne une visibilité sur les connexions Internet effectuées par PowerShell au sein d'un segment critique.</p> <p>Donne une visibilité sur les scripts PowerShell qui ont été exécutés.</p>	<p>Utiliser des stratégies GPO pour neutraliser PowerShell, activer l'audit et contrôler l'accès au pare-feu.</p>	<p>Security Controls > Baseline > Standard Operating Procedure ></p>
<p>7 INFECTION INITIALE</p> <p>Se connecte aux serveurs C2 à partir d'un segment DMZ infecté.</p>	<p>Limiter l'accès sortant à Internet au sein de la DMZ, à partir d'une liste blanche.</p>	<p>Bien que l'infection soit possible, le call back C2 à partir du segment sera mis en échec et perturbera le fonctionnement du ransomware.</p>	<p>Utiliser conjointement un firewall egress et un proxy d'entreprise pour bloquer l'accès à Internet.</p>	<p>Security Controls > Baseline > Standard Operating Procedure ></p>

TACTIQUES / TECHNIQUES DES RANSOMWARES	DÉFENSE ACTIVE	POURQUOI ?	CONSEILS, ASTUCES & RECOMMANDATIONS	MAPPING À MITRE SHIELD
<p>8 INFECTION INITIALE</p> <p>S'intègre dans une macro.</p> <p>Utilise la fonction DDE pour exécuter le code.</p>	<p>Nettoyer les macros à l'aide d'une stratégie GPO.</p> <p>Désactiver DDE via un GPO.</p> <p>Activer la fonction d'affichage protégé via un GPO.</p> <p>Déployer stratégiquement la stratégie GPO auprès des utilisateurs privilégiés et des utilisateurs qui n'ont pas besoin de la fonctionnalité.</p>	<p>Ralentit le fonctionnement du ransomware.</p> <p>Prive les adversaires de la possibilité d'utiliser des techniques courantes pour intégrer le code malveillant utilisé lors des infections initiales.</p>	<p>Utiliser des modèles de GPO pour contrôler les fonctionnalités de MS Office.</p> <p>Utiliser des fonctionnalités de sécurité de l'e-mai.</p>	<p>Email Manipulation ></p> <p>Standard Operating Procedure ></p>
<p>9 PERSISTANCE</p> <p>Rendre l'infection persistante via le registre.</p>	<p>Auditer les clés de registre Run.</p>	<p>Visibilité sur les tactiques de persistance utilisées par les ransomwares.</p>	<p>Auditer la création et la modification des cibles classiques comme les clés Run et les clés Startup.</p>	<p>Baseline ></p> <p>Hunting ></p>
<p>10 PERSISTANCE</p> <p>Assure la persistance via le module ScheduledTasks.</p>	<p>Auditer la création des tâches planifiées.</p>	<p>Visibilité sur les tactiques de persistance utilisées par les ransomwares.</p>	<p>Surveiller la présence d'un évènement ID 4698 de Windows généré à la création d'une tâche planifiée.</p>	<p>Baseline ></p> <p>Hunting ></p>
<p>11 PERSISTANCE</p> <p>Assure la persistance grâce au service WMI.</p>	<p>Auditer tout abonnement à un évènement WMI.</p>	<p>Visibilité sur les tactiques de persistance utilisées par les ransomwares.</p>	<p>Utiliser Sysmon pour détecter toute manipulation des événements WMI.</p> <p>En général, la plupart des systèmes disposent par défaut de deux abonnements pré-configurés aux événements WMI .</p>	<p>Baseline ></p> <p>Hunting ></p>
<p>12 CONTOURNEMENT DES DÉFENSES</p> <p>Met à l'arrêt les processus de sécurité.</p>	<p>Créer des processus factices de sécurité pour identifier les ransomwares qui tentent de mettre les processus de sécurité à l'arrêt.</p>	<p>Détecter tout ransomware qui tente de mettre à l'arrêt un processus de sécurité connu.</p>	<p>Créer des processus factices liés à des antivirus courants pour leurrer les ransomwares les ciblent.</p>	<p>Decoy Process ></p>
<p>13 CONTOURNEMENT DES DÉFENSES</p> <p>Arrête les services.</p>	<p>Surveiller le registre pour détecter les services de sécurité mis à l'arrêt.</p> <p>Services factices de sauvegarde et de base de données.</p> <p>Surveiller l'arrêt des services de sauvegarde et de base de données.</p>	<p>Alerte les défenseurs de la présence d'un assaillant qui tente de désactiver des services essentiels.</p>	<p>Lorsque les services sont arrêtés, la valeur de démarrage de la clé de registre du service passe à 4.</p> <p>Utiliser des services leurre pour Veeam, MSSQL et Oracle, qui sont régulièrement ciblés.</p>	<p>Decoy Process ></p> <p>Behavioral Analytics ></p>

TACTIQUES / TECHNIQUES DES RANSOMWARES	DÉFENSE ACTIVE	POURQUOI ?	CONSEILS, ASTUCES & RECOMMANDATIONS	MAPPING À MITRE SHIELD
<p>14 CONTOURNEMENT DES DÉFENSES</p> <p>Installe une VM headless légère.</p>	<p>Auditer les démarrages en mode headless des VM courantes telles que VirtualBox, VMware et Hyper-V sur des systèmes où elles ne devraient pas être installées</p>	<p>Permet de détecter les techniques qui contournent l'inspection par des solutions de détection et de réponse aux menaces sur les endpoints (EDR).</p>	<p>Rédiger des règles pour faire correspondre le hachage de fichiers à des exécutables qui autorisent les démarrages headless. Surveiller le démarrage de processus à la recherche d'arguments de ligne de commande.</p>	<p>Baseline > Hunting ></p>
<p>15 ÉLÉVATION DES PRIVILÈGES</p> <p>Mot de passe de l'administrateur local utilisé par force brute ou réutilisé.</p>	<p>Utiliser LAPS pour sécuriser les comptes des administrateurs locaux.</p> <p>Désactiver les connexions aux comptes de l'administrateur local sur le réseau.</p> <p>Créer des leurres d'informations d'identification liés à des comptes d'administrateurs locaux dans des fichiers non surveillés.</p>	<p>Maîtriser l'impact d'une réutilisation de mots de passe d'administrateurs locaux.</p>	<p>Insérer les mots de passe dans unattend.xml dans C:\Windows\Panther et surveiller qui accède à ce fichier.</p>	<p>Decoy Content > Security Controls > Standard Operating Procedure ></p>
<p>16 ÉLÉVATION DES PRIVILÈGES</p> <p>Mot de passe de l'administrateur de domaine utilisé par force brute (s'applique également à d'autres comptes privilégiés).</p>	<p>Créer un compte factice d'administrateur de domaine.</p> <p>Verrouiller les comptes d'administrateur de domaine pour qu'ils ne soient utilisés que sur le contrôleur de domaine.</p> <p>Auditer les tentatives d'ouverture de session de l'administrateur de domaine à partir d'emplacements non autorisés.</p>	<p>Protéger, détecter et déjouer les ransomwares qui ciblent un compte privilégié.</p>	<p>Créer un compte leurre et l'ajouter aux groupes AD privilégiés.</p> <p>Utiliser l'attribut logonworkstation pour contrôler les modalités de connexion des administrateurs.</p> <p>Surveiller les événements de connexion 4624, 4625, 4768, 4771, 4776.</p>	<p>Decoy Content > Standard Operating Procedure > Baseline > Hunting ></p>
<p>17 ÉLÉVATION DES PRIVILÈGES</p> <p>Vol de données d'identification à partir de navigateurs et de logiciels.</p>	<p>Déployer des informations d'identification factices pointant vers des systèmes leurres.</p>	<p>Redirige le ransomware vers une surface d'attaque factice, ce qui perturbe son fonctionnement et ralentit sa propagation.</p>	<p>Ajouter des identifiants leurres à Chrome, Edge, IE, Putty, et utiliser des systèmes et applications factices comme cible vers laquelle pointent les leurres.</p> <p>En option, ces informations d'identification peuvent être liées à des comptes factices d'Active Directory.</p>	<p>Decoy Account > Decoy Credentials > Decoy System ></p>

	TACTIQUES / TECHNIQUES DES RANSOMWARES	DÉFENSE ACTIVE	POURQUOI ?	CONSEILS, ASTUCES & RECOMMANDATIONS	MAPPING À MITRE SHIELD
18	ÉLÉVATION DES PRIVILÈGES Vol d'informations d'identification présentes en mémoire.	Déployer des identifiants factices dans CredMan et en mémoire. Créer un groupe d'utilisateurs protégés pour les comptes privilégiés. Verrouiller les autorisations pour les comptes privilégiés Protections LSASS.	Réduit la surface d'attaque permettant le détournement d'identifiants de comptes privilégiés présents en mémoire. La détection à l'aide d'identifiants factices perturbe le fonctionnement des ransomwares qui utilisent ces identifiants.	Le groupe "Protected User" permet d'em- pêcher le stockage d'informations d'iden- tification en mémoire. Cette solution présente néanmoins quelques inconvenients opéra- tionnels qu'il convient d'évaluer. S'applique à des comptes à privilégiés très élevés.	Standard Operating Procedure > Admin Access > Decoy Credentials > Security Controls >
19	ÉLÉVATION DES PRIVILÈGES Tente de compromettre des comptes disposant de droits pour créer des stratégies de groupe (GPO).	Créer des comptes factices avec des droits de GPO. Verrouiller les comptes disposant de droits de GPO pour qu'ils ne se connectent qu'au contrôleur de domaine. Traquer l'utilisation de comptes avec droits GPO à partir d'emplacements qui ne sont pas usuels.	Perturbe la recherche de droits GPO effectuée par le ransomware, lors d'une tentative d'identification ou d'utilisation du compte. Préviend la fuite d'informations d'identification des comptes GPO vers des systèmes autres que des contrôleurs de domaine.	Détecter la tentative d'identification des comptes leurres avec droits de GPO en auditant les attributs du compte. Utiliser l'attribut logonworkstation pour contrôler l'endroit où les administrateurs avec droits GPO peuvent se connecter.	Standard Operating Procedure > Admin Access > Decoy Credentials > Security Controls > Hunting >
20	ÉLÉVATION DES PRIVILÈGES Tente de compromettre les comptes d'administrateur SCCM.	Créer des comptes SCCM factices. Créer un système SCCM factice répertorié dans Active Directory. Restreindre l'utilisation des comptes SCCM à certains serveurs seulement. Traquer l'utilisation de comptes SCCM à partir d'emplacements peu communs.	Perturber la recherche de droits SCCM par le ransomware en détectant les tentatives d'identification et d'utilisation du compte ou l'identification des serveurs SCCM.		Standard Operating Procedure > Admin Access > Decoy Credentials > Security Controls > Hunting >
21	ÉLÉVATION DES PRIVILÈGES Attaques de l'Active Directory telles que Kerberoasting.	Créer des comptes leurres pouvant être exploités par Kerberoasting.	Perturber les attaques par mot de passe qui facilitent l'accès aux informations d'identification privilégiées.	Rendre tout compte leurre susceptible de faire l'objet d'une attaque Kerberoasting en définissant l'attribut SPN. Veiller à ce que le mot de passe comporte au moins 30 caractères afin de limiter les attaques par force brute.	Decoy Account >

	TACTIQUES / TECHNIQUES DES RANSOMWARES	DÉFENSE ACTIVE	POURQUOI ?	CONSEILS, ASTUCES & RECOMMANDATIONS	MAPPING À MITRE SHIELD
22	SÉLECTION DE LA CIBLE Scanne le segment DMZ local.	Ajouter des systèmes leurres dans la DMZ.	Si l'infection initiale réussit, cela permettra de détecter le ransomware dès sa phase amont de découverte.	Veiller à ce que les leurres avec partage fichiers soient placés dans la DMZ.	Decoy System >
23	SÉLECTION DE LA CIBLE Sélectionne les systèmes cibles parmi les ordinateurs présents dans Active Directory.	Créer des systèmes de leurres dans Active Directory et activer l'audit pour consigner les tentatives d'identification à leur encontre. Établir une base de référence et enquêter sur tous les comptes et systèmes qui mènent une reconnaissance dans Active Directory.	Les leurres, associés à l'analyse de base, permettent de repérer plus facilement les tentatives de reconnaissance contre Active Directory et de prendre les mesures qui s'imposent.	Positionner des systèmes leurres dans différentes UO. Ajouter des noms d'hôtes qui incitent les ransomwares à cibler des listes spécifiques, tels que « srv » ou « server ». Ajouter des attributs tels que le système d'exploitation et sa version pour rendre le leurre encore plus crédible.	Decoy System > Baseline >
24	SÉLECTION DE LA CIBLE Identifie les lecteurs mappés et les partages de fichiers sur l'hôte infecté.	Introduire des informations factices d'identification. Créer des systèmes leurres annonçant des partages de fichiers.	Trompe le ransomware et l'incite à analyser des fichiers partagés fictifs.	CredMan constitue un emplacement classique pour stocker des informations sur les espaces de partage. Des lecteurs cachés peuvent être créés dans le registre.	Decoy Credential > Decoy System >
25	SÉLECTION DE LA CIBLE Identifie les partages de fichiers à partir d'Active Directory.	Créer des comptes leurres dans Active Directory avec des indicateurs de partage de fichiers dans leurs attributs.	Détourne le ransomware vers les partages de fichiers fictifs si la tactique d'identification du malware cible Active Directory.	Les attributs tels que profilepath, homedirectory et scriptpath sont analysés pour identifier les partages de fichiers.	Decoy Account > Decoy Credential >
26	SÉLECTION DE LA CIBLE Identifie les sous- réseaux à partir des sites et sous-réseaux Active Directory.	Créer des sous- réseaux factices avec des systèmes de leurre.	Perturbe l'activité du ransomware en l'orientant vers des réseaux de leurre.	Ajouter une description au sous- réseau pour en faire une cible de choix, par exemple Segment de serveurs critiques.	Decoy System > Decoy Network >

TACTIQUES / TECHNIQUES DES RANSOMWARES	DÉFENSE ACTIVE	POURQUOI ?	CONSEILS, ASTUCES & RECOMMANDATIONS	MAPPING À MITRE SHIELD
--	----------------	------------	-------------------------------------	------------------------

27 PROPAGATION EN INTERNE

Scannez le réseau à la recherche de ports utilisés par le malware pour se déplacer en interne, le plus souvent, les ports 135, 445, 3389 et 5985/5986.

Positionner des systèmes leurres sur la DMZ et les segments hébergeant des serveurs critiques.
Assurer une isolation pour empêcher l'identification d'un segment à partir d'un autre, vers la DMZ et les segments de serveurs clés.
Appliquer une authentification 2FA pour les serveurs critiques d'entreprise.
Rechercher les connexions à ces ports, avec le segment DMZ comme source.

Empêche la propagation en interne des ransomwares, pour éviter d'impacter les activités métiers.
Permet également de détecter les ransomwares qui tentent de pirater des cibles critiques.

Utiliser des systèmes de leurre pour détecter et isoler les ransomwares et réduire la surface d'attaque qui leur est accessible.
Analyser le trafic sur les principaux ports utilisés pour le déplacement en interne à partir de la DMZ permet de déceler rapidement les anomalies.

[Decoy Account >](#)
[Isolation >](#)
[Network Manipulation >](#)
[Hunting >](#)

28 PROPAGATION EN INTERNE

Scanne le réseau à la recherche de bases de données.

Ajouter des bases de données factices au sein de la DMZ et des segments de serveurs clés
Assurer une isolation pour empêcher l'identification d'un segment à partir d'un autre, vers la DMZ et les segments de serveurs clés.
Définir le profil type des connexions à partir du segment DMZ.
Rechercher les connexions vers les serveurs de base de données communs.

Empêche la propagation en interne des ransomwares, pour éviter d'impacter les activités métiers.
Permet également de détecter les ransomwares qui tentent de pirater des cibles critiques.

Utiliser des systèmes de leurre pour détecter et isoler les ransomwares et réduire la surface d'attaque qui leur est accessible.
L'analyse du trafic sur les principaux ports de déplacement en interne à partir de la DMZ permet de rapidement déceler les anomalies.
Rechercher les connexions vers les ports 1433, 3306 et 1521.

[Decoy System >](#)
[Decoy Diversity >](#)
[Isolation >](#)
[Baseline >](#)
[Hunting >](#)

29 PROPAGATION EN INTERNE

Distribue la charge de chiffrement sur SMB, avec par exemple PsExec.

Neutraliser le protocole SMB sur une base Best efforts.
Ajouter des systèmes leurres pour encourager des interactions via SMB.
Désactiver le partage admin\$ pour empêcher l'exécution d'outils tels que PsExec.

La neutralisation du protocole SMB en mode Best effort permet de déjouer les ransomwares qui utilisent ce protocole pour se propager. D'où un impact maîtrisé des ransomwares.
Les leurres permettent de détecter les menaces.

Neutraliser les flux SMB entrants entre les postes de travail pour réduire la surface d'attaque accessible aux ransomwares.

[Decoy System >](#)
[Isolation >](#)
[Admin Access >](#)
[Security Controls >](#)

	TACTIQUES / TECHNIQUES DES RANSOMWARES	DÉFENSE ACTIVE	POURQUOI ?	CONSEILS, ASTUCES & RECOMMANDATIONS	MAPPING À MITRE SHIELD
30	PROPAGATION EN INTERNE Distribue la charge de chiffrement via une stratégie GPO.	Surveiller la création de stratégies de groupe (GPO), en particulier celles qui distribuent les tâches planifiées et les clés de registre.	Recevoir une alerte lorsqu'un GPO est créé pour distribuer des tâches planifiées et des clés de registre.	Auditer toute création d'un GPO. En option, mener un audit sur le dossier Politiques dans C:\Windows\Sysvol\ et surveiller la création des fichiers ScheduledTask.xml et Registry.xml.	Baseline > System Activity Monitoring >
31	PROPAGATION EN INTERNE Distribue la charge de chiffrement via SCCM ou d'autres outils de déploiement de logiciels.	Surveiller la création de stratégies SCCM Déployer les stratégies SCCM selon un calendrier défini. Traquer l'utilisation des comptes SCCM.	Recevoir une alerte lorsqu'une stratégie SCCM est créée ou mise à disposition en dehors des horaires classiques.	Surveiller l'utilisation des comptes SCCM via les événements de sécurité 4768 et 4624. Faire attention à l'origine de la connexion.	Baseline > System Activity Monitoring > Hunting >
32	CHECKLIST AVANT CHIFFREMENT Met à l'arrêt les débogueurs.	Créer un processus de leurre pour les débogueurs.	Détecter les activités du ransomware lorsqu'un processus de leurre est mis à l'arrêt.	Créer un processus fictif pour windbg.exe et procmon.exe.	Decoy Process >
33	CHECKLIST AVANT CHIFFREMENT Vérifie les mutex (exclusions mutuelles) pour éviter une réinfection.	Abandonner les mutex pour les ransomwares récents.	Fait de l'hôte une cible inintéressante pour les ransomwares.	Utile si vous êtes sous la menace imminente d'une variante spécifique de ransomware.	Pocket Litter >
34	CHECKLIST AVANT CHIFFREMENT Vérifie si vous travaillez dans un environnement de machines virtuelles et évite toute infection.	Créer des clés de registre factices avec des références à des machines virtuelles. Créer des processus et services factices, cohérents avec les environnements de machines virtuelles.	Fait de l'hôte une cible inintéressante pour les ransomwares.	Utiliser des noms de processus tels que vmware-vmx.exe	Decoy Content > Pocket Litter > Decoy Process >
35	CHECKLIST AVANT CHIFFREMENT Met à l'arrêt les processus de la base de données et de MS Office pour éviter les verrouillages de fichiers.	Créer des processus de leurre pour les produits MS Office.	Détecte l'activité du ransomware lorsqu'il met fin au processus.	Utiliser des noms de processus tels que winword.exe et EXCEL.exe.	Decoy Process >

	TACTIQUES / TECHNIQUES DES RANSOMWARES	DÉFENSE ACTIVE	POURQUOI ?	CONSEILS, ASTUCES & RECOMMANDATIONS	MAPPING À MITRE SHIELD
36	<p>CHECKLIST AVANT CHIFFREMENT</p> <p>Exfiltre les fichiers importants comme preuve d'accès pour demander une rançon.</p>	Créer des fichiers de leurre pour détecter toute exfiltration des données.	<p>La détection d'une l'exfiltration de données peut constituer une ultime ligne de défense.</p> <p>Réduire l'impact d'une attaque sur l'entreprise.</p>	Ajoutez des noms de fichiers tels que motsdepasse.xls, ressources.xls, Donnees_financieres.docx, etc.	Decoy Content > Pocket Litter >
37	<p>CHECKLIST AVANT CHIFFREMENT</p> <p>Supprime les shadow copies (clichés instantanés) des volumes.</p> <p>Supprime les points de restauration Windows en supprimant toutes les sauvegardes à l'aide de wbadmin.</p> <p>Désactive le mode de récupération dans la configuration de démarrage à l'aide de bcdedit.</p>	Traquer les créations de processus et les arguments de ligne de commande suspects.	Alerte les défenseurs en cas d'infection imminente de l'hôte.	Traquer des démarrages de processus par vssadmin.exe, bcdedit.exe, et wbadmin.exe	Hunting > System Activity Monitoring >
38	<p>CHIFFREMENT</p> <p>Chiffre les fichiers avec des extensions courantes et importantes.</p>	Créer des fichiers de leurre pour piéger les ransomwares.	La détection d'une tentative malveillante de chiffrement des données est une méthode de défense pour protéger l'entreprise face à la menace.	Ajouter des extensions telles que .txt, .pdf, .pst, .bak, etc.	Decoy Content > Pocket Litter >
39	<p>CHIFFREMENT</p> <p>Renomme l'extension du fichier.</p>	Surveiller les fichiers renommés	La détection d'une tentative malveillante de chiffrement des données est une méthode pour protéger l'entreprise face à la menace.	Auditer un fichier de leurre et créer une règle de suivi lorsque les logs indiquent que le nom du fichier leurre présente une extension différente de celle définie initialement.	System Activity Monitoring >
40	<p>CHIFFREMENT</p> <p>Suit les symlinks (raccourcis), les lecteurs mappés et les espaces de partage de fichiers.</p>	Créer des leurres pour les symlinks, lecteurs mappés et espaces de partage factices.	Détourne les ransomwares vers la surface d'attaque factice, pour maîtriser l'impact sur l'activité métier.	Ajouter un symlink sur le bureau.	Decoy Content > Pocket Litter >

Réflexions finales

La sécurité face aux ransomwares.

Les ransomwares constituent un sujet fascinant. Tous les professionnels de la sécurité, des RSSI aux analystes, doivent essayer de comprendre leur fonctionnement, les stratégies et tactiques qui permettent d'en maîtriser l'impact, ainsi que les actions à mener si vous en êtes victime. Voici pourquoi :

1. Les ransomwares ciblent tous les secteurs d'activité.
2. Les ransomwares peuvent potentiellement cibler tous les pans de l'environnement informatique : périmètre réseau, cœur de réseau, terminaux, Active Directory, applications et cloud.
3. Il s'agit de la seule menace actuelle capable de perturber lourdement les opérations de l'entreprise, voire de les paralyser.

Le ransomware met à l'épreuve chaque composante de votre plan de sécurité : protection, détection, réponse, préparation aux incidents, gestion des vulnérabilités, conformité, gouvernance, reprise après sinistre, sensibilisation à la sécurité, compétences, expertises et communication.

Une défense active contre les ransomwares est un objectif essentiel. Déployez cette défense face à des ransomwares dont l'impact peut se propager jusqu'à vos dirigeants, vos actionnaires, vos clients, vos partenaires externes et vos collaborateurs.

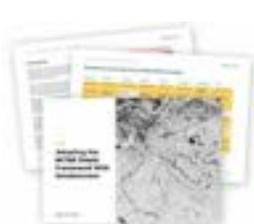
De plus, les tactiques des ransomwares se recoupent avec d'autres types de menaces : ainsi, si vous parvenez à maîtriser cette problématique, vous aborderez forcément des problématiques fondamentales et urgentes pour la sécurité pour votre entreprise.

Ressources complémentaires



Détection des menaces et défense active grâce à des leurres

[Télécharger le livre blanc >](#)



Adopter le cadre MITRE Shield avec Zscaler Deception

[Télécharger le document >](#)



Bâtir un plan de défense active suite à un rapport de test d'intrusion

[Télécharger le manuel >](#)



Défendre votre réseau, vos endpoints, votre cloud et AD à l'aide de leurres

[Bénéficier d'une démo >](#)



Experience your world, secured.™

À propos de Zscaler

Zscaler (NASDAQ : ZS) accélère la transformation digitale de ses clients pour qu'ils gagnent en agilité, efficacité, résilience et sécurité. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et les pertes des données, en connectant de manière sécurisée les utilisateurs, les appareils et les applications, quelle que soit leur localisation. Adossée à plus de 150 data centers dans le monde, Zero Trust Exchange est la plus grande plateforme cloud de sécurité SSE proposée en mode inline. Pour en savoir plus, rendez-vous sur [zscaler.fr](https://www.zscaler.fr) ou suivez-nous sur Twitter [@zscaler](https://twitter.com/zscaler).

©2023 Zscaler, Inc. Tous droits réservés. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, et ZPA™ sont des marques déposées ou des dénominations commerciales appartenant à Zscaler, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales appartiennent à leurs propriétaires respectifs. Données non contractuelles.