MANDIANT

RAPPORT

STRATÉGIES DE PROTECTION ET DE CONFINEMENT DES RANSOMWARES

Conseils pratiques pour la protection, le confinement et la sécurisation renforcée des terminaux

Sommaire

Présentation

Les ransomwares servent à prendre les données des victimes en otage et à les libérer contre le versement d'une rançon. Ce type d'attaque bloque instantanément l'accès aux fichiers, applications ou systèmes d'une victime jusqu'à ce que cette dernière verse une rançon aux cyberescrocs (en échange d'une clé de déchiffrement) ou restaure ses fichiers à partir de sauvegardes. Une fois infiltrés, la plupart des variants de ransomware exploitent des comptes utilisateurs dotés de privilèges élevés et les relations de confiance entre des systèmes pour se propager latéralement.

Il existe deux techniques courantes de propagation d'un ransomware à travers un environnement :

1. Propagation manuelle – Une fois infiltré, l'attaquant obtient des privilèges administrateur sur une grande partie de l'environnement :
   - Exécution manuelle de chiffreurs sur les systèmes ciblés
   - Déploiement de chiffreurs dans tout l'environnement à l'aide de fichiers de commandes Windows (montage de dossier partagé C$, copie du chiffreur, exécution avec Microsoft PsExec)
   - Déploiement de chiffreurs à l'aide d'objets de stratégie de groupe Microsoft (GPO)
   - Déploiement de chiffreurs à l'aide d'outils de déploiement de logiciels utilisés par l'entreprise victime
2. Propagation automatique :
   - Extraction d'identifiants ou de jetons Windows à partir du disque ou de la mémoire
   - Relations de confiance entre les systèmes – et exploitation d'outils comme Windows Management Instrumentation (WMI), SMB ou PsExec pour se connecter aux systèmes et exécuter des payloads
   - Méthodes d'exploitation de vulnérabilités non corrigées (par ex., EternalBlue – résolue dans le bulletin de sécurité Microsoft MS17-010)[1]

Ce livre blanc vous invite à découvrir des mesures pratiques de contrôle de la sécurité de vos terminaux de façon à limiter l'impact d'un ransomware ou d'autres variants de malwares sur vos systèmes. En cas d'attaque, et en fonction de la méthode de propagation utilisée par le variant, ces recommandations vous permettront de contrecarrer les plans de l'attaquant et d'endiguer l'incident.

Si ces dernières sont loin d'être exhaustives, elles constituent néanmoins les techniques les plus efficaces de confinement et de protection des terminaux contre une attaque par ransomware. Une implémentation proactive des contrôles listés dans ce document vous permettra quant à elle de protéger votre entreprise contre les ransomwares susceptibles de perturber ses opérations et de se propager à un grand nombre de ses systèmes.

1 Microsoft, Bulletin de sécurité Microsoft MS17-010 - Critique, 14 mars 2017.

Sécurisation renforcée des terminaux

Segmentation des terminaux

```
Tactique : propagation latérale à travers les systèmes à l'aide de protocoles standard du système
d'exploitation Windows
```

Pare-feu Windows

De nombreux variants de ransomware exploitent des comptes privilégiés pour accéder aux systèmes d'un environnement. Le protocole SMB (Server Message Block) est généralement utilisé comme canal de communication entre ces systèmes. Bien que ce protocole soit souvent nécessaire dans un environnement d'exploitation Windows (par ex., pour relier un poste de travail aux contrôleurs de domaine ou serveurs de fichiers), il est possible de limiter la portée des communications SMB directes autorisées entre les systèmes (par ex., entre les postes de travail).

En effet, vous pouvez configurer une politique de pare-feu Windows qui restreindra le champ des communications autorisées entre les terminaux courants de votre environnement. Vous pouvez appliquer cette politique au niveau local ou de façon centralisée via les stratégies de groupe. Au minimum, il est conseillé de bloquer les ports et protocoles suivants entre vos différents postes de travail, mais aussi de vos postes vers des serveurs autres que les contrôleurs de domaine et serveurs de fichiers :

- SMB (TCP/445, TCP/135, TCP/139)
- Remote Desktop Protocol (TCP/3389)
- Windows Remote Management / Remote PowerShell (TCP/80, TCP/5985, TCP/5986)
- WMI (plage de ports dynamique assignée via DCOM)

À l'aide des stratégies de groupe, vous pouvez configurer les paramètres de pare-feu Windows listés dans le tableau 1 afin de limiter les communications entrantes des terminaux de vos environnements.

Chemin des paramètres des stratégies de groupe :
Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Pare-feu Windows avec fonctions avancées de sécurité

TABLEAU 1. État de configuration recommandé du pare-feu Windows.

Paramètre de profil	État du pare-feu	Connexions entrantes	Enregistrer les paquets ignorés dans le journal	Enregistrer les connexions réussies dans le journal	Chemin d'accès du fichier journal	Taille maximale du fichier journal (Ko)
Domaine	Actif	Bloquer toutes les connexions ne correspondant pas à une règle préconfigurée	Oui	Oui	%systemroot%\system32\LogFiles\Firewall\pfirewall.log	4 096
Privé	Actif	Bloquer toutes les connexions	Oui	Oui	%systemroot%\system32\LogFiles\Firewall\pfirewall.log	4 096
Public	Actif	Bloquer toutes les connexions	Oui	Oui	%systemroot%\system32\LogFiles\Firewall\pfirewall.log	4 096

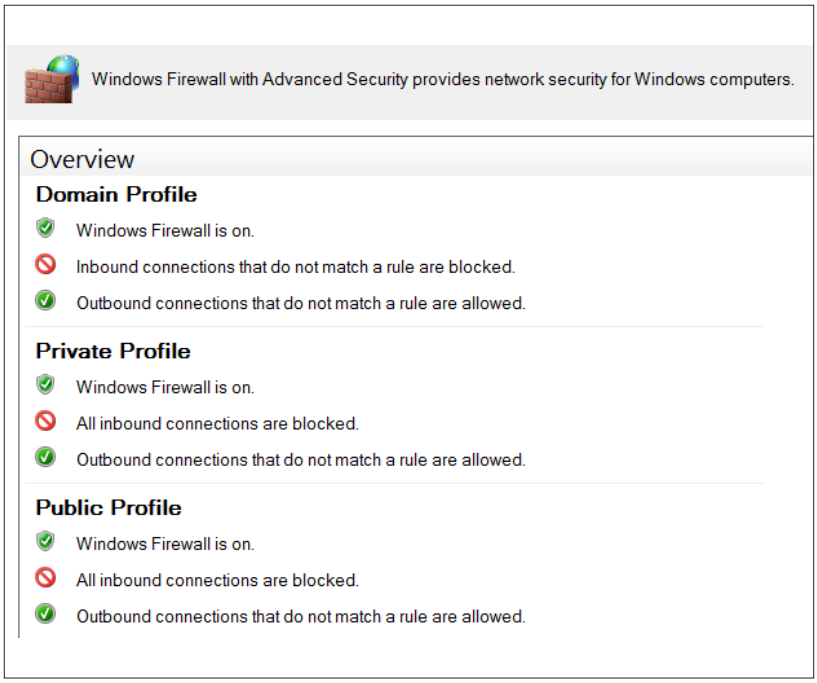

FIGURE 1. Configurations recommandées du pare-feu Windows.

En outre, afin que seules les règles de pare-feu gérées en central s'appliquent pendant le confinement (sans possibilité pour l'attaquant de les changer), vous pouvez sélectionner la valeur **« Non »** des paramètres **« Appliquer les règles de pare-feu locales »** et **« Appliquer les règles de sécurité de connexion locales »** pour tous les profils.

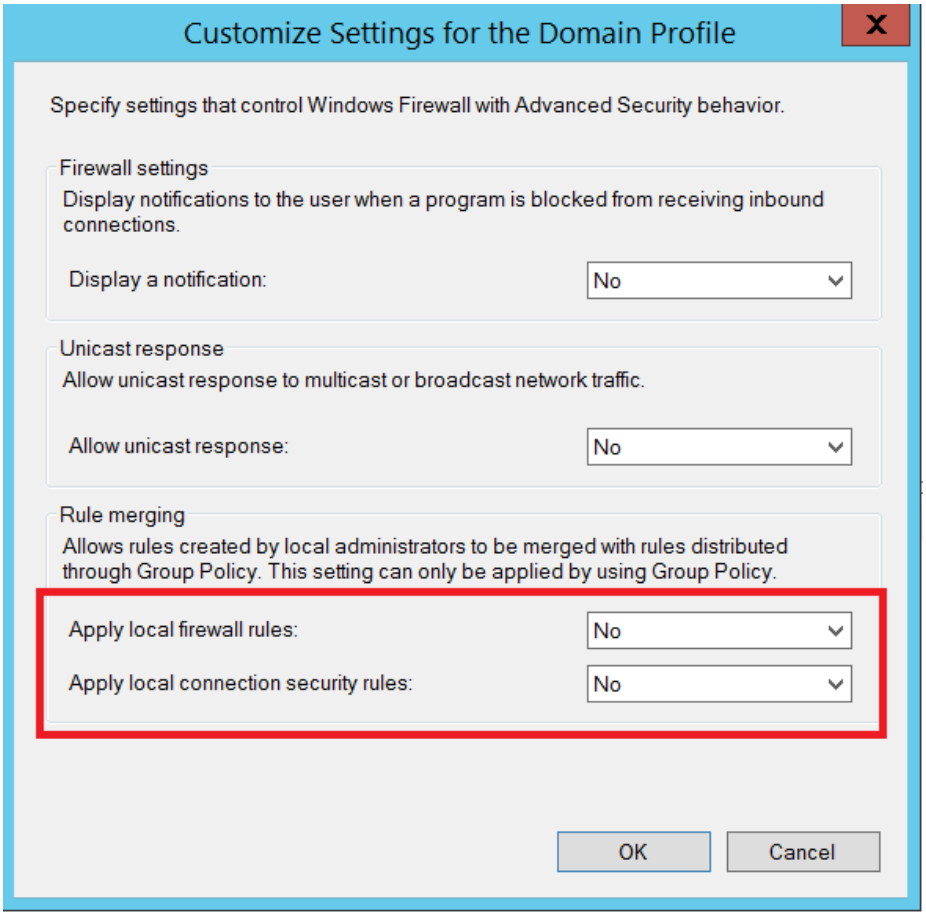

FIGURE 2. Paramètres personnalisés des profils de domaine du pare-feu Windows.

Pour confiner et isoler rapidement des systèmes, rien de tel que le paramètre centralisé du pare-feu Windows « Bloquer toutes les connexions » (cf. Figure 3) qui empêchera l'établissement de connexions entrantes vers un système. Vous pouvez l'appliquer tant aux postes fixes que portables. Toutefois, elle risque d'impacter vos opérations lorsque vous l'appliquez aux serveurs. En cas d'infection par ransomware, c'est tout de même un moindre mal pour endiguer la menace.

Remarque : une fois que le malware est confiné et que les communications entre vos systèmes ne représentent plus un danger pour votre environnement, vous pourrez de nouveau « autoriser » les « connexions entrantes » via les stratégies de groupe le cas échéant.

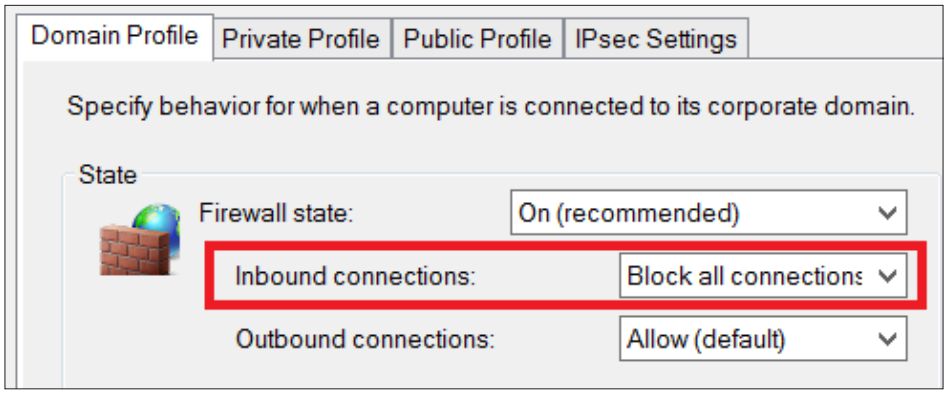

FIGURE 3. Pare-feu Windows – paramètre « Bloquer toutes les connexions.

La liste des ports et protocoles du tableau 2 recense les vecteurs de propagation et de mouvements latéraux les plus courants. Certes, il n'est pas envisageable de bloquer toutes les connexions entrantes des terminaux courants dans une optique de confinement. Toutefois, il est conseillé de bloquer au moins les ports et protocoles figurant dans ce tableau à l'aide du pare-feu Windows.

Pour les applications qui auraient besoin d'établir une connectivité entrante vers les terminaux utilisateurs, configurez la politique de pare-feu locale au moyen des adresses IP des systèmes autorisés à émettre des communications vers ces appareils (définition d'exceptions).

TABLEAU 2. Règles de blocage suggérées pour le pare-feu Windows.

Protocole / Port	Règle de pare-feu Windows	Ligne de commande à appliquer
SMB **TCP/445, TCP/139, TCP/135**	Règle prédéfinie : • Partage de fichier et d'impression	`netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=no`
protocole RDP **TCP/3389**	Règle prédéfinie : • Bureau à distance	`netsh advfirewall firewall set rule group="Remote Desktop" new enable=no`
WMI	Règle prédéfinie : • Windows Management Instrumentation (WMI)	`netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=no`
Windows Remote Management / Remote PowerShell **TCP/80, TCP/5985, TCP/5986**	Règle prédéfinie : • Windows Remote Management • Windows Remote Management (Compatibilité) Règle de port : • 5986	`netsh advfirewall firewall set rule group="Windows Remote Management" new enable=no` Via PowerShell : `Disable-PSRemoting -Force`

Name	Group	Profile	Enabled	Action
WinRm via HTTPs - Block Inbound		All	Yes	Block
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (SMB-In)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	All	Yes	Block
File and Printer Sharing (Spooler Service - RPC-EPM...	File and Printer Sharing	All	Yes	Block
Remote Desktop - Shadow (TCP-In)	Remote Desktop	All	Yes	Block
Remote Desktop - User Mode (TCP-In)	Remote Desktop	All	Yes	Block
Remote Desktop - User Mode (UDP-In)	Remote Desktop	All	Yes	Block
Windows Management Instrumentation (ASync-In)	Windows Managemen...	All	Yes	Block
Windows Management Instrumentation (DCOM-In)	Windows Managemen...	All	Yes	Block
Windows Management Instrumentation (WMI-In)	Windows Managemen...	All	Yes	Block
Windows Remote Management (HTTP-In)	Windows Remote Ma...	All	Yes	Block
Windows Remote Management (HTTP-In)	Windows Remote Ma...	All	Yes	Block

FIGURE 4. Suggestions de règles de pare-feu Windows à bloquer via les stratégies de groupe.

Par ailleurs, le pare-feu Windows peut être configuré de manière à empêcher certains fichiers binaires d'établir des connexions sortantes depuis les terminaux. En effet, au cours de ses missions de réponse aux attaques par ransomware, Mandiant a constaté le détournement de fichiers binaires Windows légitimes pour télécharger des backdoors et des chiffreurs à partir d'emplacements tant internes qu'externes.

Pour déjouer cette technique, les entreprises peuvent s'appuyer sur une série de règles de pare-feu Windows interdisant à des fichiers binaires spécifiques d'établir des connexions sortantes depuis un terminal.

À partir des exemples powershell.exe et bitsadmin.exe, découvrez dans la figure ci-dessous comment configurer les règles de pare-feu Windows à cet effet.

Outbound Rules

Name	Description
Bitsadmin - Outbound Blocking	
This rule might contain some elements that cannot be interpreted by the current version of GPMC reporting module	
Enabled	True
Program	%systemroot%\System32\bitsadmin.exe
Action	Block
Authorized computers	
Protocol	Any
Local port	Any
Remote port	Any
ICMP settings	Any
Local scope	Any
Remote scope	Any
Profile	All
Network interface type	All
Service	All programs and services
Group	
PowerShell - Outbound Blocking	
This rule might contain some elements that cannot be interpreted by the current version of GPMC reporting module	
Enabled	True
Program	%systemroot%\System32\WindowsPowerShell\v1.0\powershell.exe
Action	Block
Authorized computers	
Protocol	Any
Local port	Any
Remote port	Any
ICMP settings	Any
Local scope	Any
Remote scope	Any
Profile	All
Network interface type	All
Service	All programs and services
Group	
PowerShell - Outbound Blocking	
This rule might contain some elements that cannot be interpreted by the current version of GPMC reporting module	
Enabled	True
Program	%systemroot%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Action	Block
Authorized computers	
Protocol	Any
Local port	Any
Remote port	Any
ICMP settings	Any
Local scope	Any
Remote scope	Any
Profile	All
Network interface type	All
Service	All programs and services
Group	

FIGURE 5. Exemple de configuration de règle de pare-feu Windows pour empêcher certains fichiers binaires d'établir des connexions sortantes avec les terminaux.

Sécurisation renforcée des sessions RDP

Il n'est pas rare que les pirates utilisent le protocole RDP (Remote Desktop Protocol) pour accéder à des systèmes à distance, se propager latéralement au reste de l'environnement et déployer des malwares. À cet égard, les systèmes ouverts vers l'extérieur, connectés à Internet via le protocole RDP, encourent un risque non négligeable. Les attaquants pourront en effet exploiter RDP pour établir l'accès initial, se déplacer latéralement à travers son réseau, invoquer un ransomware et, éventuellement, exfiltrer des données.

Pour s'en prémunir, les entreprises doivent analyser leurs plages d'adresses IP publiques afin d'identifier leurs systèmes connectés à Internet via RDP (TCP/3389) et d'autres protocoles (SMB : TCP/445). Au minimum, il est préférable de ne pas autoriser les entrées et sorties de et vers Internet directement via RDP et SMB. Si les deux protocoles s'avèrent nécessaires sur le plan opérationnel, il est important d'implémenter des contrôles explicites afin de limiter les adresses IP sources autorisées à communiquer avec vos systèmes par leur intermédiaire.

Authentification multifacteur

Si vos opérations nécessitent l'utilisation de connexions RDP publiques, vous devriez implémenter l'authentification multifacteur. Pour cela, vous pouvez intégrer la technologie d'un autre fournisseur ou utiliser une passerelle des services Bureau à distance et le serveur d'authentification multifacteur Azure via RADIUS[2].

Authentification au niveau du réseau

Sur vos serveurs RDP publics, l'authentification au niveau du réseau (NLA) vous permet d'ajouter une étape de pré-authentification avant tout établissement d'une connexion. NLA vous protège également contre les attaques par force brute, qui ciblent souvent les serveurs RDP connectés à Internet.

Vous pouvez la configurer à partir de l'interface utilisateur (cf. Figure 6) ou via les stratégies de groupe (cf. Figure 7).

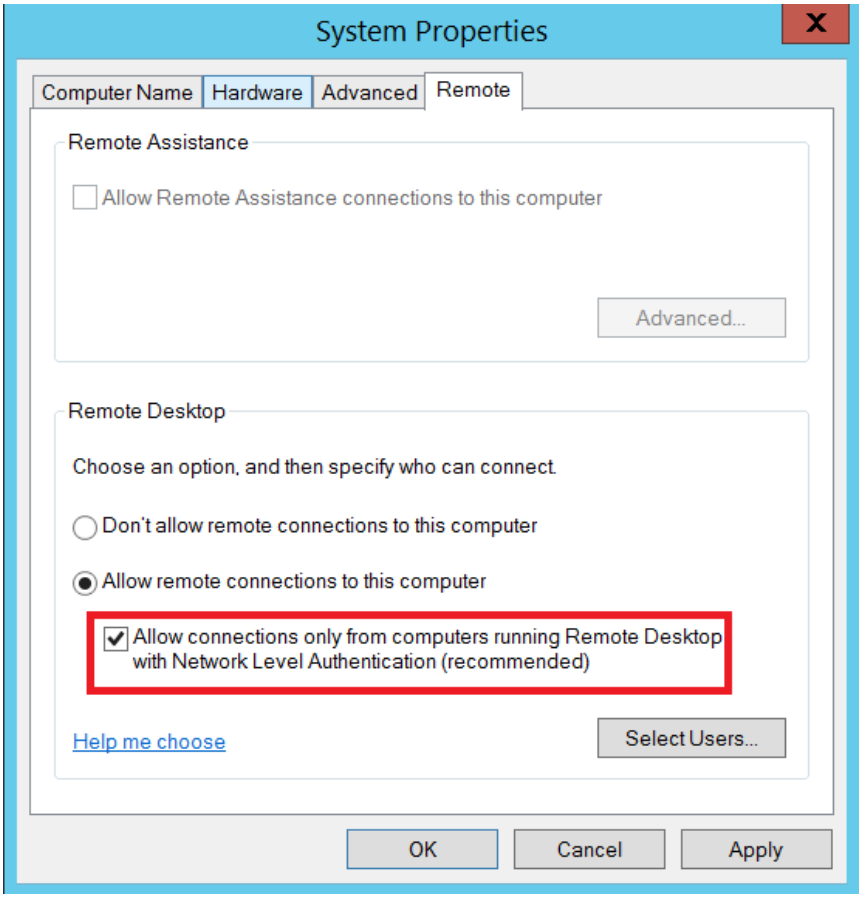

FIGURE 6. Activation de NLA via l'interface utilisateur.

2 Microsoft, Passerelle des services Bureau à distance et serveur Azure Multi-Factor Authentication avec RADIUS, 10 juillet 2018.

Pour activer l'authentification au niveau du réseau à l'aide des stratégies de groupe :

- Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de session Bureau à distance > Sécurité > Requérir l'authentification utilisateur pour les connexions à distance à l'aide de l'authentification au niveau du réseau

Setting	State	Comment
Server authentication certificate template	Not configured	No
Set client connection encryption level	Not configured	No
Always prompt for password upon connection	Not configured	No
Require secure RPC communication	Not configured	No
Require use of specific security layer for remote (RDP) connections	Not configured	No
Do not allow local administrators to customize permissions	Not configured	No
Require user authentication for remote connections by using Network Level Authentication	Enabled	No

FIGURE 7. Activation de NLA via les stratégies de groupe.

Mais attention :

- L'authentification au niveau du réseau pour vos sessions RDP nécessite le client du bureau à distance 7.0 (ou supérieur).
- NLA s'appuie sur CredSSP pour transmettre les requêtes d'authentification du système demandeur. Or, CredSSP stocke les identifiants dans la mémoire LSA de ce système. Ils pourront y rester même après la déconnexion de l'utilisateur. Son utilisation génère donc un risque d'exposition des identifiants en mémoire sur le système source.
- Sur le serveur RDP, les utilisateurs autorisés à se connecter à distance via le protocole RDP doivent pouvoir « Accéder à cet ordinateur à partir du réseau » lorsque NLA est activée. Il s'agit d'un privilège souvent refusé aux comptes utilisateurs afin de prévenir les mouvements latéraux.

Priver les comptes administrateurs de protocole RDP sur les systèmes connectés à Internet

Les comptes d'administrateurs locaux et de domaines dotés de privilèges élevés ne doivent pas pouvoir communiquer avec les serveurs publics via le protocole RDP (cf. Figure 8).

Pour leur interdire un tel accès via les stratégies de groupe :

- Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur > Interdire l'ouverture de session

Local Policies/User Rights Assignment

Policy	Setting
Deny access to this computer from the network	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on as a batch job	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on as a service	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on locally	MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on through Terminal Services	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts

FIGURE 8. Configuration de la stratégie de groupe pour empêcher les comptes d'administrateurs locaux et de domaines dotés de privilèges élevés d'utiliser RDP.

Désactivation des partages administratifs / cachés

```
Tactique : Propagation latérale à travers les systèmes via l'établissement de liaisons avec des partages
administratifs pour le déploiement d'outils ou de malwares
```

Certains variants de ransomware tenteront d'identifier les partages administratifs ou les dossiers partagés cachés, notamment ceux non explicitement associés à une lettre de lecteur. Ils s'en serviront pour établir une liaison avec les terminaux de tout un environnement. Pour confiner la menace, une entreprise devra parfois désactiver rapidement l'accès par défaut aux partages administratifs ou cachés depuis les terminaux. Pour cela, elle pourra modifier le registre, stopper un service ou utiliser le modèle de stratégie de groupe « Guide de sécurité Microsoft » du kit de ressources de conformité de la sécurité Microsoft[3].

Parmi les partages administratifs et cachés courants sur les terminaux :

- ADMIN$
- C$
- D$
- IPC$

Remarque : la désactivation des partages administratifs et cachés sur les serveurs, en particulier les contrôleurs de domaine, risque de nuire sérieusement au bon fonctionnement des systèmes d'un environnement basé sur les domaines.

En outre, dans les environnements qui utilisent PsExec, la désactivation du dossier d'administrateur partagé (ADMIN$) pourra vous empêcher d'utiliser cet outil pour vous interfacer à distance avec des terminaux.

Méthode du registre :

Il est possible de désactiver les partages administratifs et cachés sur les terminaux à l'aide du registre (cf. Figures 9 et 10).

Postes de travail :

```
HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
DWORD Name = "AutoShareWks"
Value = "0"
```

FIGURE 9. Valeur du registre pour la désactivation des partages administratifs sur des postes de travail.

Serveurs :

```
HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
DWORD Name = "AutoShareServer"
Value = "0"
```

FIGURE 10. Valeur du registre pour la désactivation des partages administratifs sur des serveurs.

3 Voir https://www.microsoft.com/en-us/download/details.aspx?id=55319

Méthode du service :

En stoppant le service « Serveur » sur un terminal, vous désactivez l'accès aux dossiers partagés hébergés sur celui-ci (cf. Figure 11).

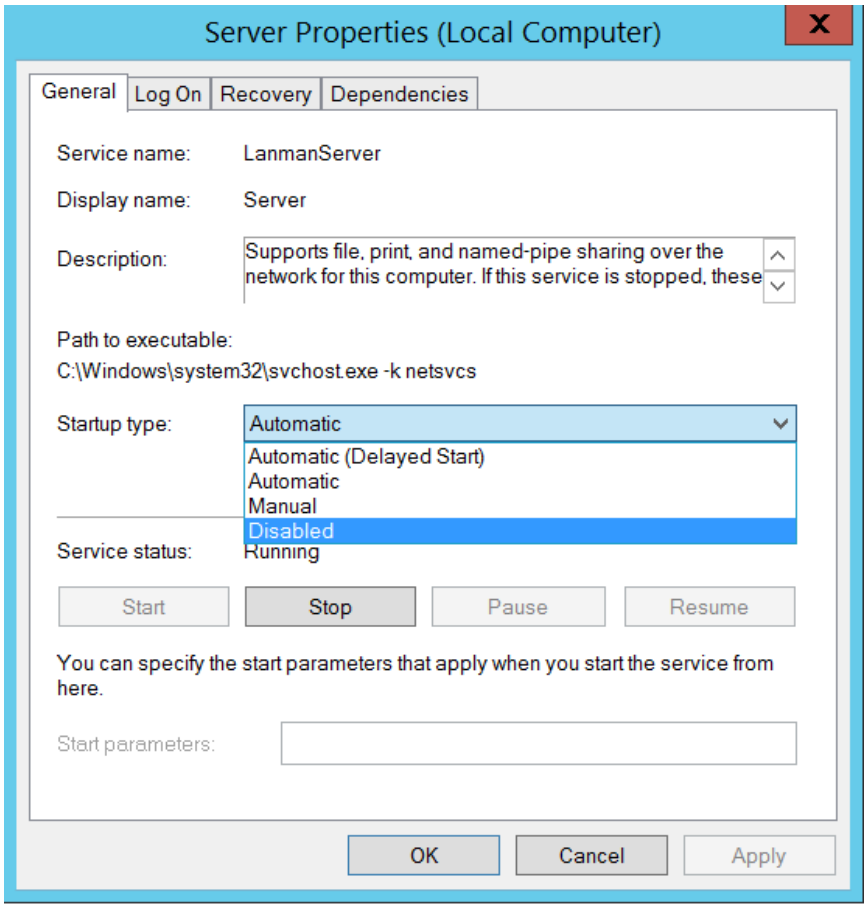

FIGURE 11. Propriétés du service « Serveur ».

Méthode de la stratégie de groupe :

À l'aide du modèle « MSS (Legacy) », il est possible de désactiver les partages administratifs et cachés sur un serveur ou un poste de travail via les paramètres de stratégie de groupe (cf. Figure 12).

- Configuration ordinateur > Stratégies > Modèles d'administration > MSS (Legacy) > MSS (AutoShareServer)
- Configuration ordinateur > Stratégies > Modèles d'administration > MSS (Legacy) > MSS (AutoShareWks)

Setting	State	Comment
MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)	Not configured	No
MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended e...	Not configured	No
MSS: (AutoShareServer) Enable Administrative Shares (recommended except for highly secure envi...	Disabled	No
MSS: (AutoShareWks) Enable Administrative Shares (recommended except for highly secure enviro...	Disabled	No

FIGURE 12. Désactivation des partages administratifs et cachés via le modèle de stratégie de groupe « MSS (Legacy) ».

Désactivation de SMB v1

```
Tactique : Propagation latérale à travers les systèmes via l'exploitation de vulnérabilités ou le
détournement de protocoles existants
```

En plus de corriger les vulnérabilités connues des protocoles courants (par ex., SMB)[4], il est conseillé de désactiver SMB v1 sur les terminaux afin de contrecarrer les méthodes de propagation de masse utilisées par certains variants de ransomware.

Vous pouvez désactiver SMB v1 sur Windows 7 et Windows Server 2008 R2 (et supérieures) à l'aide de PowerShell (cf. Figure 13), d'une modification du registre ou du modèle de stratégie de groupe « Guide de sécurité Microsoft » du kit de ressources de conformité de la sécurité Microsoft[5].

Avec PowerShell :

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

FIGURE 13. Ligne de commande PowerShell pour désactiver SMB v1.

Méthode du registre :

Il est possible de désactiver SMB v1 sur les terminaux à l'aide du registre (cf. Figures 13 et 14).

Désactivation du serveur SMB v1 :

```
HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
Entrée de registre : SMB1
REG_DWORD = "0" (Désactivé)
```

FIGURE 14. Clé de registre et valeur pour la désactivation d'un serveur SMB v1 (écouteur).

Désactivation du client SMB v1 :

```
HKLM\SYSTEM\CurrentControlSet\services\mrxsmb10
Entrée de registre : Start
REG_DWORD = "4" (Désactivé)

HKLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstation
Entrée de registre : DependOnService
REG_MULTI_SZ: "Bowser","MRxSmb20","NSI"
```

FIGURE 15. Clé de registre et valeur pour la désactivation d'un client SMB v1.

4 Microsoft, Bulletin de sécurité Microsoft MS17-010 - Critique, 10 octobre 2017.
5 Voir https://www.microsoft.com/en-us/download/details.aspx?id=55319

Méthode de la stratégie de groupe :

Il est possible de désactiver SMB v1 à l'aide des paramètres ci-dessous du modèle de stratégie de groupe « Guide de sécurité Microsoft ».

Setting	State	Comment
Configure SMB v1 server	Disabled	No
Configure SMB v1 client driver	Enabled	No
Configure SMB v1 client (extra setting needed for pre-Win8.1/2012R2)	Enabled	No

FIGURE 16. Désactivation d'un serveur SMB v1 via le modèle de stratégie de groupe « Guide de sécurité MS.

- Configuration ordinateur > Stratégies > Modèles d'administration > Guide de sécurité MS > Configurer le serveur SMB v1
- Configuration ordinateur > Stratégies > Modèles d'administration > Guide de sécurité MS > Configurer le pilote de client SMB v1
  - Activée
    - Configurer le pilote MrxSMB10
      - Désactiver le pilote

Setting	State	Comment
Configure SMB v1 server	Disabled	No
Configure SMB v1 client driver	Enabled	No
Configure SMB v1 client (extra setting needed for pre-Win8.1/2012R2)	Enabled	No

FIGURE 17. Désactivation d'un pilote de client SMB v1 via le modèle de stratégie de groupe « Guide de sécurité MS.

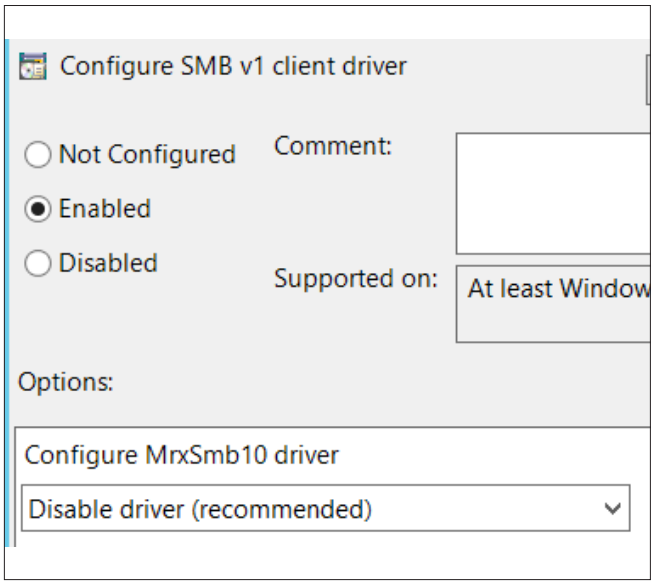

FIGURE 18. Désactivation d'un pilote de client SMB v1 via le modèle de stratégie de groupe « Guide de sécurité MS » – paramètre supplémentaire.

- Configuration ordinateur > Stratégies > Modèles d'administration > Guide de sécurité MS > Configurer le client SMB v1 (paramètre supplémentaire pour les systèmes antérieurs à Win8.1/2012R2)
  - Activée
    - Configurer les dépendances LanmanWorkstation
      - Bowser
      - MrxSMB20
      - NSI

Setting	State	Comment
Configure SMB v1 server	Disabled	No
Configure SMB v1 client driver	Enabled	No
Configure SMB v1 client (extra setting needed for pre-Win8.1/2012R2)	Enabled	No

FIGURE 19. Désactivation des paramètres supplémentaires d'un client SMB v1 via le modèle de stratégie de groupe « Guide de sécurité MS.

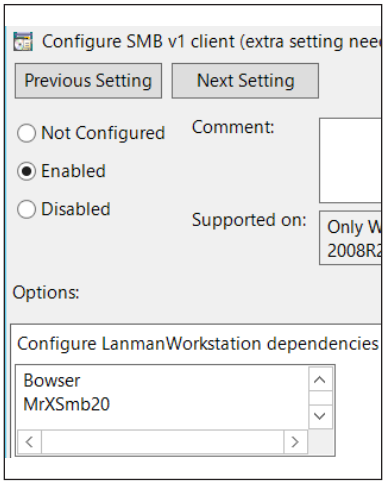

FIGURE 20. Désactivation d'un pilote de client SMB v1 via le modèle de stratégie de groupe « Guide de sécurité MS » – paramètres supplémentaires pour garantir l'absence de l'option « MRxSmb.

Renforcement de la sécurité de Windows Remote Management (WinRM)

```
Tactique : Propagation latérale à travers les systèmes via Windows Remote Management (WinRM) et
PowerShell Remoting
```

Certains attaquants utilisent Windows Remote Management (WinRM) pour propager manuellement leur ransomware dans l'environnement infiltré. Par défaut, WinRM est activé sur tous les systèmes d'exploitation Windows Server (depuis la version 2012), mais désactivé sur tous les systèmes d'exploitation client (Windows 7 et 10) et les plateformes serveur plus anciennes (Windows Server 2008 R2).

La communication à distance PowerShell (PowerShell Remoting) est une fonctionnalité Windows native d'exécution de lignes de commande à distance, basée sur le protocole WinRM.

Lorsque WinRM est activé sur un système d'exploitation client (autre que serveur), les configurations ci-dessous sont présentes sur ce terminal et la ligne de commande PowerShell de la figure 21 ne suffit pas pour y remédier.

- Écouteur WinRM configuré
- Exception de pare-feu Windows configurée

Ces éléments doivent être désactivés manuellement à l'aide des lignes de commande des figures 24 et 25.

PowerShell :

```
Disable-PSRemoting -Force
```

FIGURE 21. Ligne de commande PowerShell pour désactiver WinRM / PowerShell Remoting sur un terminal.

Remarque : la désactivation des communications à distance PowerShell n'empêche pas des utilisateurs locaux de créer des sessions PowerShell sur leur machine – ou des sessions destinées à des ordinateurs distants.

Une fois la commande exécutée, le message illustré à la figure 22 s'affiche.

```
PS C:\WINDOWS\system32> Disable-PSRemoting -Force
WARNING: Disabling the session configurations does not undo all the changes made by the Enable-PSRemoting or
Enable-PSSessionConfiguration cmdlet. You might have to manually undo the changes by following these steps:
    1. Stop and disable the WinRM service.
    2. Delete the listener that accepts requests on any IP address.
    3. Disable the firewall exceptions for WS-Management communications.
    4. Restore the value of the LocalAccountTokenFilterPolicy to 0, which restricts remote access to members of the
Administrators group on the computer.
```

FIGURE 22. Message d'avertissement après désactivation de PS Remoting.

Quant aux figures 23 à 26, elles détaillent les étapes supplémentaires nécessaires pour désactiver WinRM via PowerShell.

Stopper et désactiver le service WinRM.

```
Stop-Service WinRM -PassThruSet-Service WinRM -StartupType Disabled
```

FIGURE 23. Ligne de commande PowerShell pour stopper et désactiver le service WinRM.

Désactiver l'écouteur qui accepte les requêtes de n'importe quelle adresse IP.

```
dir wsman:\localhost\listener
Remove-Item -Path WSMan:\Localhost\listener\<Listener name>
```

FIGURE 24. Lignes de commande PowerShell pour la suppression d'un écouteur WSMAN.

Désactiver les exceptions de pare-feu pour les communications WS-Management.

```
Set-NetFirewallRule -DisplayName 'Windows Remote Management (HTTP-In)' -Enabled False
```

FIGURE 25. Ligne de commande PowerShell pour désactiver les exceptions de pare-feu pour WinRM.

Remettre la valeur de LocalAccountTokenFilterPolicy à zéro afin d'appliquer le filtrage de jetons UAC (mode d'approbation Administrateur) au compte administrateur intégré (RID 500).

```
Set-ItemProperty -Path
HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system -Name LocalAccountTokenFilterPolicy -Value 0
```

FIGURE 26. Ligne de commande PowerShell pour configurer la clé de registre de LocalAccountTokenFilterPolicy

Méthode de la stratégie de groupe :

- Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Windows Remote Management (WinRM) > Service WinRM > Autoriser la gestion de serveurs à distance via WinRM

Si le paramètre de la stratégie de groupe ci-dessus est « désactivé », le service WinRM ne répondra pas aux requêtes d'un ordinateur distant, même en cas de configuration d'écouteurs WinRM.

- Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Environnement distant Windows > Autoriser l'accès aux environnements distants

Ce paramètre de stratégie de groupe permet de configurer les accès distants pour l'exécution de scripts et de lignes de commande sur tous les shell pris en charge.

Exposition des identifiants et contrôle renforcé de leur utilisation

Utilisation de comptes locaux à distance

```
Tactique : Propagation et mouvements latéraux à l'aide du compte d'administrateur local intégré sur les terminaux
```

Les comptes locaux de terminaux sont souvent exploités par les attaquants pour leurs mouvements latéraux à travers un environnement. Cette tactique s'avère d'autant plus efficace lorsque plusieurs terminaux utilisent le même mot de passe de compte d'administrateur local intégré.

Afin de contrecarrer cette tactique, la mise à jour de sécurité Microsoft KB2871997[6] a introduit deux (2) SID bien connus qui permettent de limiter l'utilisation malveillante des comptes locaux à l'aide des paramètres de stratégie de groupe.

- S-1-5-113 : AUTORITÉ NT\Compte local
- S-1-5-114 : AUTORITÉ NT\Compte local et membre du groupe Administrateurs

En particulier, le SID « S-1-5-114 : AUTORITÉ NT\Compte local et membre du groupe Administrateurs » est ajouté à un jeton d'accès à un compte local si ce dernier est membre du groupe BUILTIN\Administrateurs. **Ce SID est le plus efficace pour bloquer un attaquant (ou un variant de ransomware) qui exploite les identifiants de comptes d'administrateurs locaux.**

Remarque : dans le cas du SID « S-1-5-114 : AUTORITÉ NT\Compte local et membre du groupe Administrateurs », si vous utilisez le clustering de basculement, cette fonctionnalité devra reposer sur un compte local non-administrateur (CLIUSR) pour la gestion des nœuds de cluster. Si ce compte fait partie du groupe Administrateurs local d'un terminal de votre cluster, le blocage des autorisations de connexion réseau pourra en effet paralyser les services de cluster. Veillez donc à bien tester cette configuration sur vos serveurs concernés par le clustering de basculement.

Étape 1 – Option 1 : SID S-1-5-114

Afin d'empêcher l'utilisation de comptes d'administrateurs locaux pour la propagation latérale, utilisez le SID « S-1-5-114 : AUTORITÉ NT\Compte local et membre du groupe Administrateurs » dans les paramètres suivants :

- Configuration ordinateur > Stratégies > Paramètres Windows> Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur
  - Interdire l'accès à cet ordinateur à partir du réseau (SeDenyNetworkLogonRight)
  - Interdire l'ouverture de session en tant que tâche (SeDenyBatchLogonRight)
  - Interdire l'ouverture de session en tant que service (SeDenyServiceLogonRight)
  - Interdire l'ouverture de session par les services Terminal Server (SeDenyRemoteInteractiveLogonRight)
  - Déboguer les programmes (SeDebugPrivilege) – droit d'accès utilisé lors des tentatives d'élévation de privilèges et d'injection de processus

Étape 1 – Option 2 : Filtrage de jetons UAC

Les paramètres de stratégie de groupe permettent également de contrôler l'utilisation de comptes locaux pour l'administration et les connexions à distance dans le cadre d'une ouverture de session réseau. Si tous les droits d'accès (mentionnés à l'option 1 ci-dessus) ne peuvent être restreints dans un court laps de temps, envisagez d'appliquer le filtrage de jetons UAC à vos connexions réseau via des comptes locaux.

Pour cela, vous pouvez utiliser le modèle de stratégie de groupe « Guide de sécurité Microsoft » du kit de ressources de conformité de la sécurité Microsoft évoqué plus haut[7].

Paramètre de stratégie de groupe :

- Configuration ordinateur > Stratégies > Modèles d'administration > Guide de sécurité MS > Appliquer des restrictions UAC aux accès réseau de comptes locaux

6 Microsoft, Avis de sécurité Microsoft : mise à jour permettant d'améliorer la gestion et la protection des informations d'identification, datée du 13 mai 2014.
7 Voir https://www.microsoft.com/en-us/download/details.aspx?id=55319

Une fois le paramètre activé, la valeur du registre (cf. Figure 27) sera configurée sur chaque terminal :

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy
REG_DWORD = “0” (Activé)
```

FIGURE 27. Clé de registre et valeur pour l’application des restrictions UAC aux comptes locaux.

Lorsqu’elle est fixée à “0”, les connexions à distance avec des jetons d’accès à haut niveau d’intégrité ne seront admises qu’à l’aide de l’identifiant en texte clair ou du hachage du mot de passe de l’administrateur local RID 500, en fonction de la valeur du paramètre « FilterAdministratorToken ».

Ce paramètre « FilterAdministratorToken » permet d’activer (1) ou de désactiver (0, valeur par défaut) le mode d’approbation pour l’administrateur local RID 500. En cas d’activation de ce mode, le jeton d’accès du compte d’administrateur local RID 500 est filtré. En d’autres termes, ce compte est soumis au contrôle de compte UAC (qui aide à prévenir son utilisation lors de tentatives de déplacements latéraux).

Paramètre de stratégie de groupe :
- Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Contrôle de compte d’utilisateur : mode Approbation administrateur pour le compte Administrateur intégré

Une fois le paramètre activé, la valeur du registre (cf. Figure 28) sera configurée sur chaque terminal.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\FilterAdministratorToken
REG_DWORD = “1” (Activé)
```

FIGURE 28. Clé de registre et valeur pour activer le mode d’approbation Administrateur pour les comptes d’administrateurs locaux.

Remarque : mieux vaut également veiller à ce que le paramètre « Contrôle de compte d’utilisateur : exécuter les comptes d’administrateurs en mode d’approbation d’administrateur » (option « EnableLUA ») reste activé (valeur par défaut). Dans le cas contraire, toutes les politiques UAC sont elles aussi désactivées. Il est alors possible de s’authentifier à distance en mode privilégié à l’aide des identifiants en texte clair ou des hachages de mot de passe de n’importe quel compte local du groupe Administrateurs local.

Paramètre de stratégie de groupe :
- Configuration ordinateur > Stratégies > Modèles d’administration > Guide de sécurité MS > Contrôle de compte d’utilisateur : exécuter les comptes d’administrateurs en mode d’approbation d’administrateur

Une fois le paramètre activé, la valeur du registre (cf. Figure 29) sera configurée sur chaque terminal. Il s’agit de la valeur par défaut du paramètre.

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA
REG_DWORD = “1” (Activé)
```

FIGURE 29. Clé de registre et valeur pour l’application des restrictions UAC aux comptes locaux.

Le filtrage de jetons d’accès UAC ne concernera aucun compte de domaine du groupe Administrateurs local sur un terminal.

Étape 2 : LAPS

Une fois ses comptes locaux privés d’authentification et d’accès aux terminaux à distance, une entreprise doit encore adopter une stratégie de randomisation des mots de passe pour son compte d’administrateur local intégré. Dans de nombreuses entreprises, le moyen le plus simple d’y parvenir consiste à déployer et utiliser Microsoft Local Administrator Password Solution (LAPS)[8].

8 Voir https://www.microsoft.com/en-us/download/details.aspx?id=46899

Réduction de l'exposition des comptes privilégiés et de service

Tactique : Propagation et mouvements latéraux à l'aide de comptes de domaine

Restriction d'accès des comptes avec privilèges

Pour propager un ransomware dans tout un environnement, les attaquants utilisent généralement des comptes privilégiés et de service pour leurs déplacements latéraux. Sans les résultats d'une investigation poussée, il est parfois difficile de connaître les identifiants exploités par un variant de ransomware pour se connecter à de nombreux systèmes d'un environnement.

Les comptes dotés de privilèges élevés dans un environnement ne devraient pas pouvoir se connecter sur des postes fixes et portables standard. Leur utilisation devrait se limiter à des systèmes dédiés (par ex., les postes de travail à accès privilégié, ou PAWS) sur des VLAN et niveaux protégés dont l'accès est limité. En clair, des comptes aux privilèges explicites devraient être définis pour chaque niveau et utilisés uniquement sur cette portion du réseau.

Nos recommandations visant à limiter les droits d'accès des comptes privilégiés s'appuient sur celles de Microsoft sur le sujet[9].

Afin de pouvoir endiguer rapidement une menace, envisagez d'interdire aux comptes dotés de privilèges élevés la connexion (locale ou à distance) aux postes fixes et portables standard et aux serveurs d'accès courants (par ex., l'infrastructure de postes de travail virtuels).

Vous pouvez configurer les paramètres ci-dessous via le chemin de stratégie de groupe suivant :

- Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur

Refusez explicitement l'accès des comptes privilégiés locaux et de domaine aux postes fixes et portables standard à l'aide des paramètres suivants (que vous pouvez configurer dans le cadre des stratégies de groupe comme à la figure 30) :

- Interdire l'accès à cet ordinateur à partir du réseau (ajoutez également S-1-5-114 : AUTORITÉ NT\Compte local et membre du groupe Administrateurs)
- Interdire l'ouverture de session en tant que tâche
- Interdire l'ouverture de session en tant que service
- Interdire l'ouverture d'une session locale
- Interdire l'ouverture de session par les services Terminal Server

Local Policies/User Rights Assignment

Policy	Setting
Deny access to this computer from the network	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on as a batch job	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on as a service	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on locally	MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts
Deny log on through Terminal Services	Local account and member of Administrators group, MCWHIRT\Domain Admins, MCWHIRT\Enterprise Admins, MCWHIRT\Schema Admins, MCWHIRT\Tier0-DomainAdmins, MCWHIRT\Tier0-ExchangeAdmins, MCWHIRT\Tier1-ServerAdmins, MCWHIRT\Tier1-ServiceAccounts

FIGURE 30. Exemple de restriction des droits d'accès d'un compte avec privilèges sur un poste de travail standard à l'aide des paramètres de stratégie de groupe.

9 Microsoft, Modèle de niveau administratif Active Directory, 13 février 2019.

Restriction d'accès des comptes de service

Il est également conseillé de renforcer la sécurité des comptes de service de domaine, ce afin de limiter leur utilisation sur les postes de travail distants interactifs et, le cas échéant, pour l'accès au réseau.

Sur les terminaux qui n'ont pas besoin de compte de service pour ouvrir des sessions distantes ou interactives, vous pouvez utiliser les paramètres de stratégie de groupe afin de limiter l'accès et ainsi l'exposition de ces comptes de service conformément aux recommandations.

- Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur
  - Interdire l'ouverture d'une session locale (SeDenyInteractiveLogonRight)
  - Interdire l'ouverture de session par les services Terminal Server (SeDenyRemoteInteractiveLogonRight)

Autre configuration recommandée pour renforcer la sécurité de vos comptes de service (sur les terminaux qui n'ont pas besoin de ces comptes pour accéder au réseau) :

- Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur
  - Interdire l'accès à cet ordinateur à partir du réseau (SeDenyNetworkLogonRight)

S'il vous faut un compte de service sur un seul terminal pour exécuter un service particulier, vous pouvez limiter encore davantage son utilisation à une liste prédéfinie de terminaux.

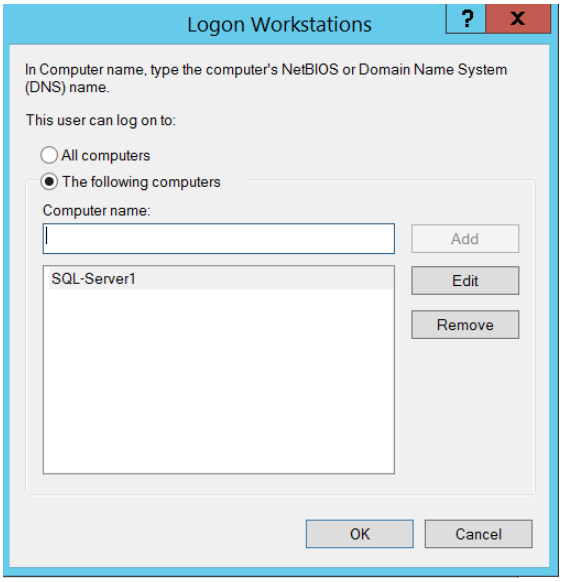

FIGURE 31. Option de restriction des terminaux auxquels un compte peut se connecter.

- Utilisateurs et ordinateurs Active Directory > Sélectionnez l'onglet Compte
  - Bouton « Se connecter à... » > Sélectionnez le bon ensemble d'ordinateurs autorisés (cf. Figure 31)

Groupe de sécurité « Utilisateurs protégés »

En utilisant le groupe de sécurité « Utilisateurs protégés » pour ses comptes privilégiés, une entreprise peut minimiser un certain nombre de facteurs de risque et contrecarrer les méthodes d'exploitation courantes de ces comptes sur les terminaux.

Introduit depuis les versions Microsoft Windows 8.1 et Microsoft Windows Server 2012 R2, le groupe de sécurité « Utilisateurs protégés » sert à gérer l'exposition des identifiants dans un environnement. En effet, les comptes de ce groupe bénéficient automatiquement de mesures de sécurité spécifiques :

- Le ticket TGT (Ticket Granting Ticket) Kerberos expire au bout de 4 heures, au lieu des 10 heures habituelles par défaut.
- Aucun hachage NTLM de compte n'est stocké dans LSASS puisque seule l'authentification Kerberos est utilisée (authentification NTLM désactivée).
- La mise en cache d'identifiants est bloquée. Un contrôleur de domaine doit pouvoir identifier le compte.
- L'authentification de compte WDigest est désactivée, quels que soient les paramètres de stratégie appliqués sur un terminal.
- Impossible d'utiliser DES et RC4 pour la pré-authentification Kerberos (Server 2012 R2 et version ultérieure). Le chiffrement AES s'applique.
- Impossible d'utiliser les comptes pour la délégation contrainte ou non (cela équivaut à activer le paramètre « Le compte est sensible et ne peut pas être délégué » pour les utilisateurs et ordinateurs Active Directory).

Pour que les comptes du groupe de sécurité « Utilisateurs protégés » bénéficient de ces mesures sur les contrôleurs de domaine, le niveau fonctionnel du domaine doit correspondre à Windows Server 2012 R2 (ou version ultérieure). Quant à la mise à jour de sécurité Microsoft KB2871997[10], elle étend la prise en charge de ces mesures de protection des comptes du groupe de sécurité « Utilisateurs protégés » aux systèmes Windows 7, Windows Server 2008 R2 et Windows Server 2012.

Remarque : les comptes de service (y compris les comptes de service administrés) ne doivent EN AUCUN CAS être ajoutés au groupe de sécurité « Utilisateurs protégés » – sans quoi l'authentification échouera.

10 Microsoft, Avis de sécurité Microsoft : mise à jour permettant d'améliorer la gestion et la protection des informations d'identification, datée du 13 mai 2014.

Protection des mots de passe en texte clair

Tactique : Collecte des identifiants en texte clair en mémoire

Outre la restriction des droits d'accès des comptes privilégiés, il convient d'implémenter des contrôles qui permettront de réduire l'exposition des jetons et identifiants en mémoire sur les terminaux.

Sur les systèmes d'exploitation Windows plus anciens, les mots de passe en texte clair sont effectivement stockés en mémoire (LSASS), principalement pour supporter l'authentification WDigest. Vous devez désactiver explicitement WDigest sur tous les terminaux Windows sur lesquels elle est activée par défaut.

Par défaut, l'authentification WDigest est désactivée sur les systèmes Windows 8.1+ et Windows Server 2012 R2+.

Depuis Windows 7 et Windows Server 2008 R2, après l'installation de la mise à jour de sécurité KB2871997[11], vous pouvez configurer l'authentification WDigest en modifiant le registre ou en utilisant le modèle de stratégie de groupe « Guide de sécurité Microsoft » du kit de ressources de conformité de la sécurité Microsoft[12].

```
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential
REG_DWORD = “0”
```

FIGURE 32. Clé de registre et valeur pour la désactivation de l'authentification WDigest.

Méthode du registre :

Vous devez également configurer explicitement le paramètre de registre "TokenLeakDetectDelaySecs" (cf. Figure 33) afin de supprimer de la mémoire les identifiants des utilisateurs déconnectés au bout de 30 secondes, comme sous Windows 8.1 et supérieures.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\TokenLeakDetectDelaySecs
REG_DWORD = “30”
```

FIGURE 33. Clé de registre et valeur pour le paramètre « TokenLeakDetect DelaySecs.

Méthode de la stratégie de groupe :

Il est possible de désactiver l'authentification WDigest à l'aide d'un paramètre du modèle de stratégie de groupe « Guide de sécurité Microsoft » (cf. Figure 34).

- Configuration ordinateur > Stratégies > Modèles d'administration > Guide de sécurité MS > Authentification WDigest

Setting	State	Comment
Configure SMB v1 server	Not configured	No
Configure SMB v1 client driver	Not configured	No
Configure SMB v1 client (extra setting needed for pre-Win8.1/2012R2)	Not configured	No
Extended Protection for LDAP Authentication (Domain Controllers only)	Not configured	No
Turn on Windows Defender protection against Potentially Unwanted Applications (DEPRECATED)	Not configured	No
Enable Structured Exception Handling Overwrite Protection (SEHOP)	Not configured	No
Apply UAC restrictions to local accounts on network logons	Not configured	No
WDigest Authentication (disabling may require KB2871997)	Disabled	No
Lsass.exe audit mode	Not configured	No
LSA Protection	Not configured	No
Remove "Run As Different User" from context menus	Not configured	No
Block Flash activation in Office documents	Not configured	No

FIGURE 34. Désactivation de l'authentification WDigest via le modèle de stratégie de groupe « Guide de sécurité MS.

11 Microsoft, Avis de sécurité Microsoft : mise à jour permettant d'améliorer la gestion et la protection des informations d'identification, datée du 13 mai 2014.
12 Voir https://www.microsoft.com/en-us/download/details.aspx?id=55319

Par ailleurs, nous recommandons de vérifier si les clés « Autoriser » englobent certaines applications (cf. Figure 35), car cela permettrait aux fournisseurs CredSSP / tspkgs de stocker des mots de passe en clair en mémoire.

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Credssp\PolicyDefaults
```

FIGURE 35. Clé de registre supplémentaire pour renforcer la sécurité des mots de passe en texte clair en mémoire.

Puisque la mise à jour de sécurité Microsoft KB2871997[13] ne s'applique pas à Windows XP, Windows Server 2003 et Windows Server 2008, pour désactiver l'authentification WDigest sur ces plateformes, vous devez supprimer WDigest de la liste des packages de sécurité LSA du registre, et ce avant un redémarrage du système (cf. Figures 36 et 37).

```
HKLM\System\CurrentControlSet\Control\Lsa\Security Packages
```

FIGURE 36. Clé de registre pour modifier les packages de sécurité LSA.

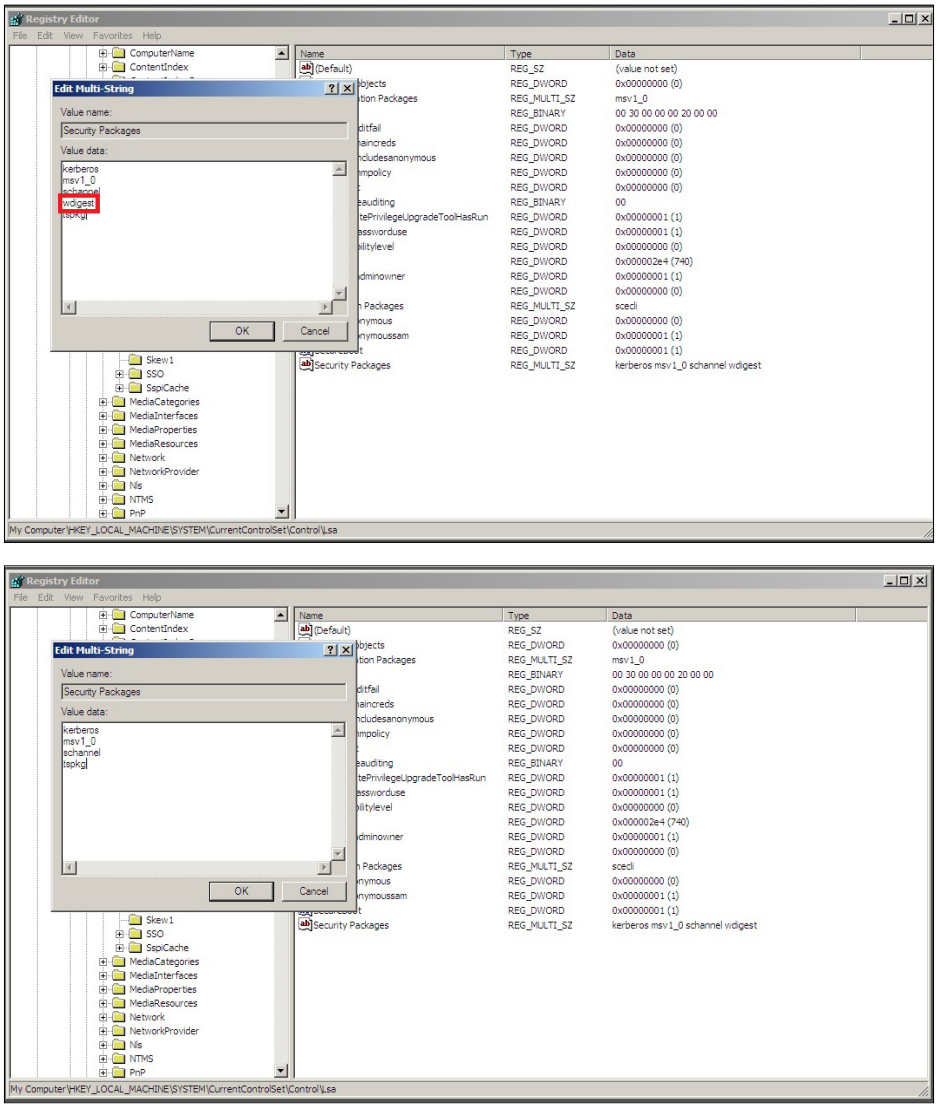

FIGURE 37. Clé de registre des packages de sécurité LSA avant et après la suppression de l'authentification WDigest de la liste des fournisseurs.

13 Microsoft (May 13, 2014). Microsoft Security Advisory: Update to improve credentials protection and management; May 13, 2014.

Par défaut, les paramètres de stratégie de groupe ne sont de nouveau traités et appliqués que si ladite stratégie a été modifiée avant l'intervalle d'actualisation par défaut.

De nombreux attaquants « activent » l'authentification WDigest manuellement sur les terminaux en modifiant directement le registre (ils fixent la valeur de UseLogonCredential à "1"). Même sur les terminaux où WDigest est désactivée automatiquement par défaut, il est donc préférable d'appliquer les paramètres de stratégie de groupe illustrés à la figure 33 – et de prévoir le retraitement automatique des stratégies pour les paramètres configurés.

- Configuration ordinateur > Stratégies > Modèles d'administration > Système > Stratégie de groupe > Configurer le traitement de la stratégie de sécurité
  - Activé – Traitement même en cas de GPO inchangés
- Configuration ordinateur > Stratégies > Modèles d'administration > Système > Stratégie de groupe > Configurer le traitement de la stratégie du registre
  - Activé – Traitement même en cas de GPO inchangés

Isolation du contrôleur de domaine (DC) et élaboration du plan de reprise

En cas d'attaque par ransomware, les entreprises doivent pouvoir compter sur un plan bien rodé qui leur permettra d'isoler rapidement les systèmes critiques. Il leur faut s'assurer qu'au moins un contrôleur de domaine peut être mis hors ligne/déconnecté et isolé en toute sécurité pour chaque domaine au sein de forêts gérées de confiance. Tout chiffrement de la partition du disque qui héberge la base de données Active Directory (%SYSTEMROOT%\ntds\ntds.dit) et SYSVOL (%SYSTEMROOT%\SYSVOL) sur tous les contrôleurs de domaine perturberait fortement l'accès aux services et fonctionnalités de domaine pour l'ensemble des applications et services basés sur des domaines (authentification, résolution de nom, traitement des GPO, etc.). Si les sauvegardes de contrôleur de domaine ne sont pas à jour ou se retrouvent chiffrées, les entreprises devront alors reconstruire entièrement la forêt Active Directory, au risque de paralyser davantage leur activité.

Quand les équipes Mandiant sont appelées à intervenir sur un déploiement actif de ransomware, les premières mesures qu'elles recommandent à l'entreprise victime sont les suivantes. D'une part, isoler au moins un contrôleur de domaine (de préférence un contrôleur doté de rôles FSMO - Flexible Single Master Operation). D'autre part, s'assurer que ses sauvegardes hors ligne de SYSVOL (%SYSTEMROOT%\SYSVOL*) et des GPO sont à jour et accessibles. Par mesure de précaution, en cas de nécessité d'une récupération – faisant autorité ou non – du contrôleur de domaine, les entreprises doivent veiller à attribuer une valeur connue au mot de passe du mode restauration des services d'annuaire (DSRM), et ce pour tous les contrôleurs de domaine. La figure 40 ci-dessous détaille le processus pour attribuer une valeur connue au mot de passe pour les entreprises dépourvues de mot de passe DRSM. Les étapes sont à suivre pour chaque contrôleur de domaine.

```
netdom query fsmo
```

FIGURE 38. Ligne de commande pour définir un contrôleur de domaine doté d'un rôle FSMO.

```
backup-gpo -domain "domain.local" -all -path "c:\temp\gpo-backups"
```

FIGURE 39. Ligne de commande PowerShell pour sauvegarder tous les objets de stratégie de groupe (GPO) d'un domaine.

```
PS C:\Windows\system32> ntdsutil
C:\Windows\System32\ntdsutil.exe : définition du mot de passe DRSM
Réinitialisation du mot de passe administrateur DRSM : réinitialisation invalide du mot de passe sur le
serveur
Veuillez saisir le mot de passe pour le compte administrateur DRSM : ****************
Veuillez confirmer le nouveau mot de passe : ****************
Votre mot de passe a bien été enregistré.

Réinitialisation du mot de passe administrateur DRSM : q
C:\Windows\System32\ntdsutil.exe:
```

FIGURE 40. Lignes de commande pour définir le mot de passe DSRM sur un contrôleur de domaine (DC).

Il arrive qu'une récupération des services de domaine soit uniquement possible en restaurant Active Directory à partir de sauvegardes DC antérieures. Dans ce cas, l'entreprise doit commencer par s'assurer qu'elle dispose d'un plan stratégique de sauvegarde testé et opérationnel, garantissant la disponibilité et l'intégrité du schéma et des services de domaine à reconstituer. Voici les bonnes pratiques à suivre en amont :

- **Sauvegardes hors ligne :** veiller à sécuriser et conserver les sauvegardes DC hors ligne à l'écart des sauvegardes en ligne
- **Chiffrement :** chiffrer les données de sauvegarde pendant le transfert (via le réseau), mais également quand elles sont au repos ou mises en miroir vers un lieu de stockage hors site.
- **Configuration des alertes pour les opérations de sauvegarde :** configurer les solutions et technologies de sauvegarde afin de détecter et de signaler toutes les opérations critiques à la disponibilité et à l'intégrité des données de sauvegarde (par ex., : suppression des données de sauvegarde, élimination des métadonnées de sauvegarde, restaurations, erreurs de support).
- **Conservation des données :** s'assurer que les produits et technologies de sauvegarde conservent les sauvegardes pour une durée prédéfinie avant d'écraser ou de purger les données.
- **Contrôle des accès basé sur les rôles :** recourir aux contrôles d'accès basé sur les rôles pour tout accès aux sauvegardes et aux applications régissant les sauvegardes de données. L'objectif est de limiter le nombre des comptes disposant de droits d'accès aux données conservées et aux paramètres de configuration.
- **Test et vérification :** vérifier régulièrement que les données peuvent être restaurées et reconstituées à partir de sources aussi bien en ligne que hors ligne. Les processus de restauration (faisant autorité ou non) des contrôleurs de domaine doivent être documentés et testés.

Autorisation et monitoring des objets de stratégie de groupe (GPO)

Couramment employé par les acteurs du ransomware, le déploiement de chiffreurs consiste à modifier la configuration d'un GPO existant ou à créer un nouveau GPO, et de relier cet objet à la racine du domaine ou à un vaste ensemble d'unités organisationnelles (UO) contenant des objets « ordinateurs ». En exploitant des tâches programmées, des scripts de démarrage/d'ouverture de session, ou des paramètres d'installation de packages logiciels, les cybercriminels peuvent profiter des fonctionnalités natives au sein d'Active Directory pour accomplir leur mission. Et ce, sans avoir besoin de s'interfacer avec chaque terminal de l'environnement pour appeler les chiffreurs.

Il est donc important que les entreprises prennent les devants et inspectent le périmètre d'action des GPO configurés, ainsi que la dernière modification horodatée. L'objectif : s'assurer que toutes les modifications correspondent bien aux activités autorisées et attendues.

```
get-gpo -all | export-csv -path "c:\temp\gpo-listing-all.csv" -NoTypeInformation
```

FIGURE 41. Ligne de commande PowerShell pour examiner la portée des GPO configurés – y compris la dernière modification horodatée.

Une autre recommandation porte sur l'examen des permissions accordées pour les GPO existants, et en particulier l'analyse du champ d'action des comptes et groupes habilités à modifier les GPO au sein d'un domaine. En effet, il est important de bien protéger et de classer dans la catégorie « à privilèges » l'ensemble des comptes ou groupes de sécurités capables de modifier un grand nombre de GPO, ou des objets de stratégie de groupe qui leur sont liés, et d'appliquer des paramètres de sécurité pour un grand nombre de terminaux (par ex., : Stratégie de domaine par défaut).

```
$GPOPermission = Foreach ($GPO in (Get-GPO -All | Where-Object {$_.DisplayName -like "*"})){
  {
    Foreach ($Perm in (Get-GPPermissions $GPO.DisplayName -All | Where-Object {$_.Permission -like "*"}))
{
    {
     New-Object PSObject -property @{GPO=$GPO.DisplayName;Trustee=$Perm.Trustee.Name;Permission=$Perm.
Permission}
    }
  }
$permissions | Select GPO,Trustee,Permission | Export-CSV c:\temp\GPO-Permissions.csv -NoTypeInformation
```

FIGURE 42. Lignes de commande PowerShell pour recenser les GPO existants et les autorisations attribuées.

Ainsi, il est possible de détecter les modifications apportées aux GPO en passant au crible les journaux d'événements de sécurité sur les contrôleurs de domaine pour l'ID d'événement 5136. Pour cela, l'auditing « Audit Directory Service Changes » doit être activé. La figure 43 illustre comment la modification d'un journal d'événement de sécurité pour le GPO Stratégie de domaine par défaut (au GUID bien connu de 31B2F340-016D-11D2-945F00C04FB984F9) et l'ajout d'une tâche planifiée (extension côté client de AADCED64-746C-4633-A97C-D61349046527) sont détectés.

FIGURE 43. Détection de l'ID d'événement 5136 pour les modifications de GPO.

Conclusion

À l'heure où les attaquants sont déterminés à monétiser leurs exploits, les ransomwares font courir de graves dangers aux entreprises. Nous espérons donc que ce livre blanc vous aura fourni les recommandations pratiques nécessaires pour vous prémunir contre ces attaques et endiguer la menace déjà infiltrée. Loin de se vouloir un guide complet des tactiques et moyens de contrôle à votre disposition, ce document représente toutefois une référence précieuse pour les entreprises confrontées aux ransomwares. Il se base sur notre vaste expérience de terrain à aider nos clients à se protéger et à récupérer de ce type d'attaque. Et nous espérons qu'il vous aidera à en faire autant.

Pour en savoir plus, rendez-vous sur **www.mandiant.fr**

Mandiant
11951 Freedom Dr, 6th Fl, Reston, VA 20190
+1(703)935-8012
833.3MANDIANT (362.6342)
info@mandiant.com

À propos de Mandiant
Depuis 2004, Mandiant® s'impose comme le partenaire de confiance des entreprises soucieuses de leur sécurité. Aujourd'hui, l'expertise et la Threat Intelligence leader de Mandiant sous-tendent des solutions dynamiques qui aident les organisations à développer des programmes plus efficaces et à instaurer une plus grande confiance dans leurs cyberdéfenses.

MANDIANT