WAVESTONE

Rapport technique

Analyse des échanges de données réalisés par les « expériences connectées »
à l'ouverture d'un document dans Microsoft 365 Apps for enterprise

21 mars 2024 | Diffusion : Public

V1.0

Contexte et objectif du document

Lors d'analyses techniques, Wavestone a constaté que **les versions Microsoft 365 Apps for enterprise de PowerPoint et Word transféraient le contenu textuel des documents vers un point de terminaison appartenant à Microsoft, et ce dès l'ouverture du document, sans action utilisateur.**

Ce transfert de contenu est réalisé par les fonctionnalités « expériences connectées » de Microsoft PowerPoint et Word, activées par défaut et utilisant des services hébergés par Microsoft (traduction, prédiction de texte…). Des informations sur les expériences connectées sont disponibles ici : https://learn.microsoft.com/en-us/deployoffice/privacy/connected-experiences.

Ce fonctionnement est actif même lorsque le document n'est pas stocké dans le cloud de Microsoft, incluant donc les fichiers locaux (sur le poste de travail ou un serveur de fichier).

Le comportement est observé sur les clients lourds Office utilisés dans le cadre de l'abonnement Microsoft 365 Apps for Enterprise. Les autres versions de ces logiciels (LTSC en particulier) n'ont pas été testées. Les tests ont été réalisés sur les versions Windows de ces logiciels. Les autres supports (MacOS et OS mobiles notamment) n'ont pas été testés.

Ce document décrit :

- Le comportement observé
- Les éléments permettant d'identifier si un périmètre est concerné
- Les actions pour analyser ce comportement et le désactiver si nécessaire
- Les étapes nécessaires pour reproduire ce comportement

Sommaire

1 Comportement observé

1.1 Microsoft PowerPoint M365 Apps for enterprise

À l'ouverture d'un document Microsoft PowerPoint depuis Windows (version Microsoft 365 Apps for enterprise), il a été remarqué qu'une connexion *websocket* chiffrée (TLS) était réalisée par l'application avec le point de terminaison **augloop.office.com** :

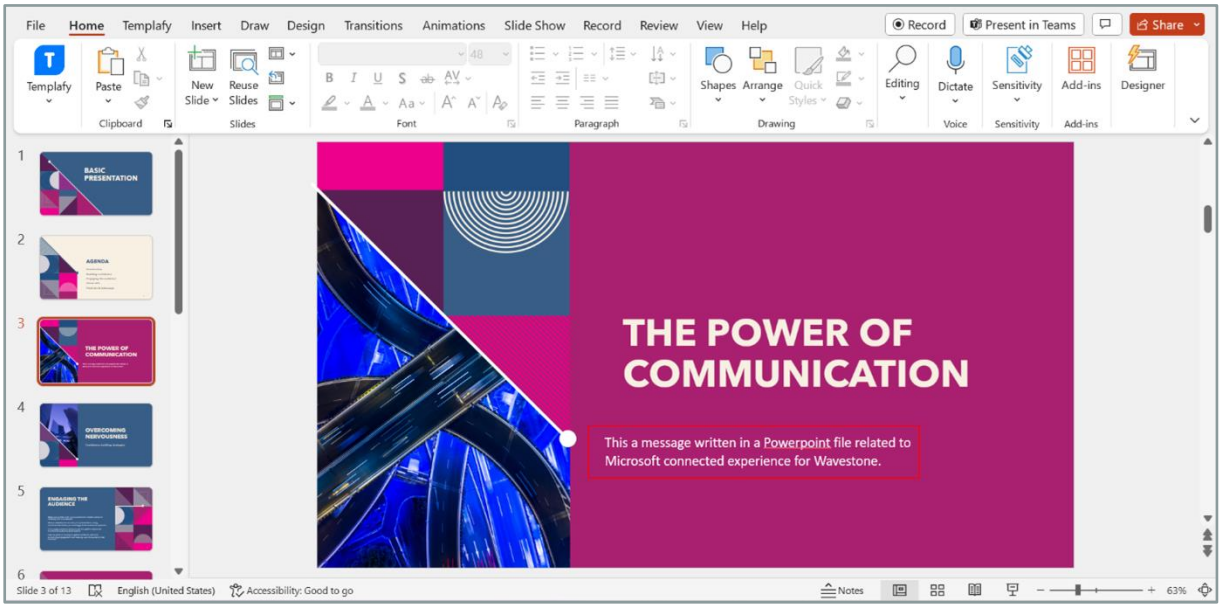

Figure 1 : Fichier Microsoft PowerPoint contenant du texte

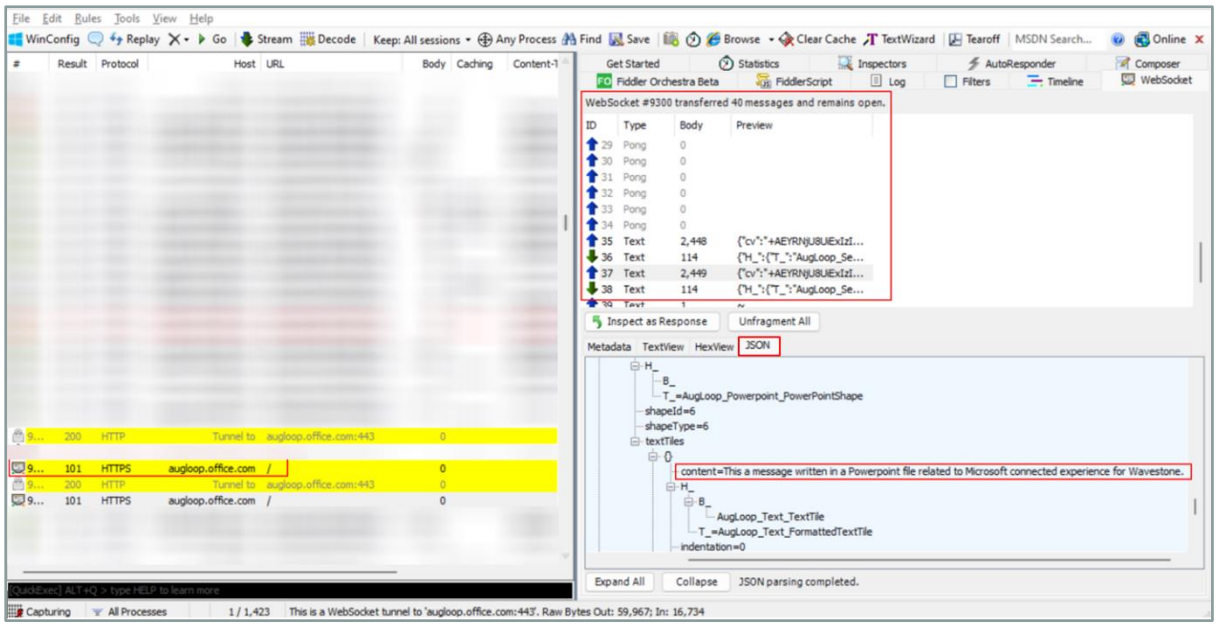

Figure 2: Websocket ouverte par l'application et message envoyé

Des messages sont alors échangés sur ce *websocket* chiffré, notamment l'envoi de messages JSON possédant le format suivant :


```
{"cv":"+AEYRNjU8UiExIzIBSksjA.216.1.1","seq":8,"ops":[{"parentPath":["session","
doc"],"items":[{"id":"258#707789176","contextId":"N9","body":{"shapes":[{"textTi
les":[{"indentation":0,"listType":6,"content":"The power of
communication","H_":{"T_":"AugLoop_Text_FormattedTextTile","B_":["AugLoop_Text_T
extTile"]}}],"shapeType":0,"shapeId":"2","creationId":"A29DE7F2-E890-4744-88DD-
A75F5E300513","bounds":{"left":4833938,"top":660400,"right":11428413,"bottom":61
97600},"H_":{"T_":"AugLoop_Powerpoint_PowerPointShape","B_":[]}},{"textTiles":[]
,"shapeType":5,"shapeId":"34","creationId":"9289CE93-EC50-55DB-CFE0-
1266AEC87B19","bounds":{"left":0,"top":762000,"right":4076700,"bottom":6858000},
"description":{"content":"Aerial view of a neon highway
intersection","H_":{"T_":"AugLoop_Text_TextTile","B_":[]}},"H_":{"T_":"AugLoop_P
owerpoint_PowerPointShape","B_":[]}},{"textTiles":[],"shapeType":9,"shapeId":"31
","creationId":"F466A906-2869-BB36-138E-
D45F62E92210","bounds":{"left":3903663,"top":4646613,"right":4178300,"bottom":49
21250},"isDecorative":true,"H_":{"T_":"AugLoop_Powerpoint_PowerPointShape","B_":
[]}},{"textTiles":[],"shapeType":9,"shapeId":"32","creationId":"06186C3A-548E-
AD87-3029-964123530768","bounds":{"left":-
98425,"top":660400,"right":4062413,"bottom":4810125},"isDecorative":true,"H_":{"
T_":"AugLoop_Powerpoint_PowerPointShape","B_":[]}},{"textTiles":[{"indentation":
0,"listType":6,"content":"This a message written in a Powerpoint file related to
Microsoft connected experience for
Wavestone.","H_":{"T_":"AugLoop_Text_FormattedTextTile","B_":["AugLoop_Text_Text
Tile"]}},{"indentation":0,"listType":6,"content":" ","H_":{"T_":"AugLoop_Text_Fo
rmattedTextTile","B_":["AugLoop_Text_TextTile"]}}],"shapeType":6,"shapeId":"6","
creationId":"3AD1E279-AE30-F930-05CA-
4B1F1C8F4898","bounds":{"left":4541838,"top":4646613,"right":9855200,"bottom":61
10288},"H_":{"T_":"AugLoop_Powerpoint_PowerPointShape","B_":[]}}],"isSlideHidden
":false,"themeId":"{4DA6DF5E-F5DF-461D-8863-
50E9C5721FD0}","sid":"258","cid":"707789176","bounds":{"left":0,"top":0,"right":
12192000,"bottom":6858000},"contentMasterMoniker":{"mainMasterMoniker":{"id":214
7483648,"cId":2464305198},"id":2147483704,"cId":1506966382},"H_":{"T_":"AugLoop_
Powerpoint_PowerPointSlide","B_":[]}}}],"H_":{"T_":"AugLoop_Core_UpdateOperation
","B_":["AugLoop_Core_Operation"]}}],"H_":{"T_":"AugLoop_Session_Protocol_SyncMe
ssage","B_":["AugLoop_Session_Protocol_Message"]},"messageId":"c13"}
```


Figure 3: *Le message envoyé transmet le contenu textuel des slides du fichier (en rouge)*

Le contenu des slides sous le format texte est donc transmis au point de terminaison augloop.office.com même si le document n'est pas stocké dans le cloud Microsoft, et ce sans action de l'utilisateur.

Lors de la modification du contenu d'un paragraphe de texte, l'envoi d'un message JSON contenant la modification est également réalisé**.**

Les versions testées de Microsoft PowerPoint possédant ce comportement sont les suivantes :

- **2402 - Build 17328.20162** Click-to-Run version Windows (Current channel – 4 mars 2024) ;
- **2308 - Build 16731.20550** Click-to-Run version Windows (Semi-Annual Enterprise channel – 13 février 2024) ;
- **2302 - Build 16130.20218** Click-to-Run version Windows (Current channel – 28 février 2023) ;
- **2202 - Build 14931.20132** Click-to-Run version Windows (Current channel – 8 mars 2022) ;
- **2108 - Build 14326.20404** Click-to-Run version Windows (Current channel – 14 septembre 2021) ;
- **1908 - Build 11929.20300** Click-to-Run version Windows (Current channel – 10 septembre 2019) (l'envoi de données ne s'effectue pas au moyen d'un websocket mais grâce à une requête POST au point de terminaison augloop.office.com).

Les versions antérieures et intermédiaires n'ont pas été testées. Les versions autres que Windows (MacOS, OS mobiles…) n'ont pas été testées.

1.2 Microsoft Word M365 Apps for enterprise

De manière similaire à Microsoft PowerPoint, il a également été remarqué qu'une connexion *websocket* chiffrée (TLS) était entreprise par l'application avec le point de terminaison **augloop.office.com** :

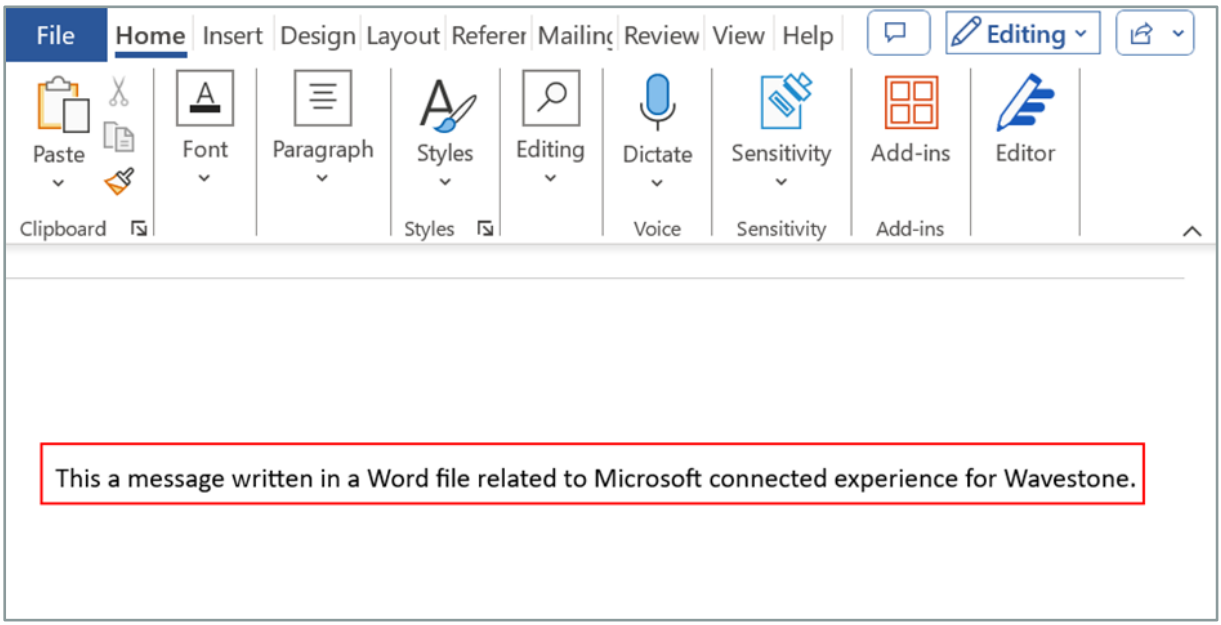

Figure 4: Fichier Microsoft Word contenant du texte

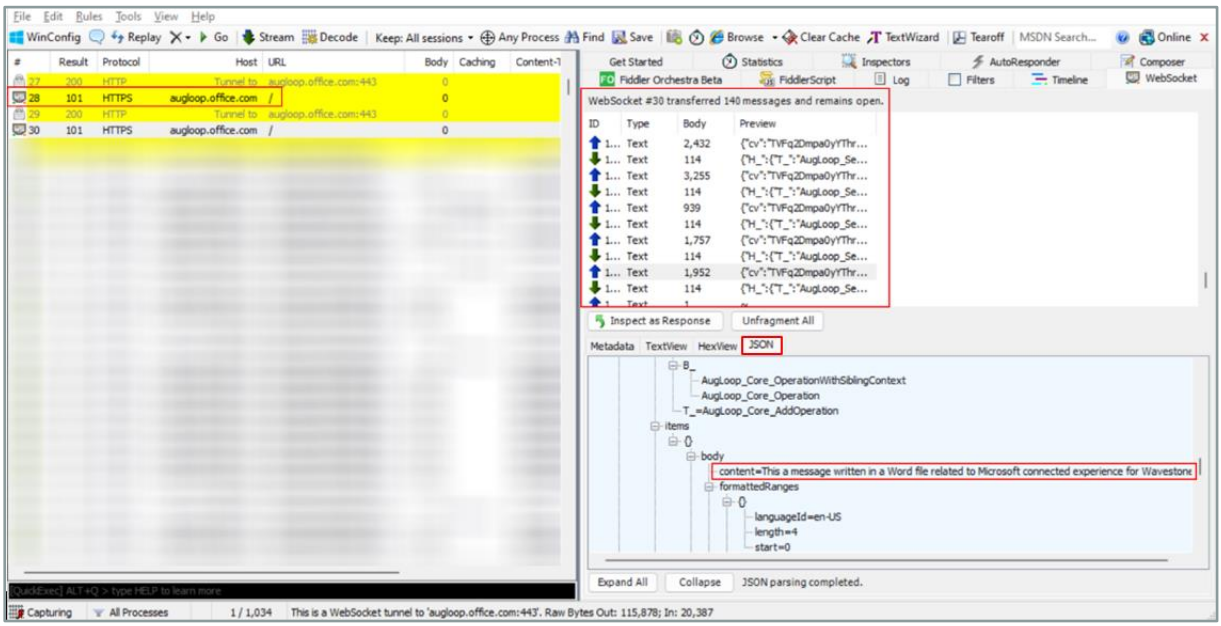

Figure 5: Websocket ouverte par l'application et message envoyé

Similairement à Microsoft PowerPoint, des messages sont alors échangés sur ce *websocket* chiffré, notamment l'envoi de messages JSON possédant le format suivant :


```
{"cv":"TVFq2Dmpa0yYThrAKi/o0Q.340.13","seq":40,"ops":[{"parentPath":["session","
doc","main"],"items":[{"id":"2BE76413-A9E6-4110-8F1E-
D7A359AD927B","sourceTimestamp":1710519873912,"revId":"1489729331","contextId":"
","body":{"content":"","H_":{"T_":"AugLoop_Text_FormattedTextTile","B_":["AugLoo
p_Text_TextTile"]}}}],"H_":{"T_":"AugLoop_Core_DeleteOperation","B_":["AugLoop_C
ore_Operation"]}},{"prevId":"B72D2646-F914-447B-B828-
03E75ED47E87","nextId":"DC908C9A-CC73-4725-AB1C-
EEA2AAA9AE97","parentPath":["session","doc","main"],"items":[{"id":"C37E25A4-
9172-4311-94AC-
BF00EB198334","sourceTimestamp":1710519874420,"revId":"2004318071","contextId":"
.N192","body":{"formattedRanges":[{"languageId":"en-
US","start":0,"length":1}],"content":"\r","H_":{"T_":"AugLoop_Text_FormattedText
Tile","B_":["AugLoop_Text_TextTile"]}}}],"H_":{"T_":"AugLoop_Core_AddOperation",
"B_":["AugLoop_Core_OperationWithSiblingContext","AugLoop_Core_Operation"]}},{"n
extId":"C37E25A4-9172-4311-94AC-
BF00EB198334","parentPath":["session","doc","main"],"items":[{"id":"B72D2646-
F914-447B-B828-
03E75ED47E87","sourceTimestamp":1710519874420,"revId":"2004318071","contextId":"
.N193","body":{"formattedRanges":[{"languageId":"en-
US","start":0,"length":4},{"languageId":"en-
US","start":4,"length":13},{"languageId":"en-
US","start":17,"length":4},{"languageId":"en-
US","start":21,"length":1},{"languageId":"en-
US","start":22,"length":25},{"languageId":"en-
US","start":47,"length":39},{"languageId":"en-
US","start":86,"length":8},{"languageId":"en-
US","start":94,"length":0}],"content":"This a message written in a Word file
related to Microsoft connected experience for
Wavestone.","H_":{"T_":"AugLoop_Text_FormattedTextTile","B_":["AugLoop_Text_Text
Tile"]}}}],"H_":{"T_":"AugLoop_Core_AddOperation","B_":["AugLoop_Core_OperationW
ithSiblingContext","AugLoop_Core_Operation"]}}],"H_":{"T_":"AugLoop_Session_Prot
ocol_SyncMessage","B_":["AugLoop_Session_Protocol_Message"]},"messageId":"c43"}
```


Figure 6: *Le message envoyé transmet le contenu textuel du fichier (en rouge)*

Le contenu du document Word sous le format texte est donc transmis au point de terminaison augloop.office.com même si le document n'est pas synchronisé avec le cloud Microsoft, et ce sans action de l'utilisateur.

Lors de la modification du contenu d'un paragraphe de texte, l'envoi d'un message JSON contenant la modification est également réalisé**.**

Les versions testées de Microsoft Word possédant ce comportement sont les suivantes :

- **2402 - Build 17328.20184** Click-to-Run version Windows (Current Channel – 12 mars 2024) ;
- **2402 - Build 17328.20162** Click-to-Run version Windows (Current Channel – 4 mars 2024) ;
- **2401 - Build 17231.20290** Click-to-Run version Windows (Monthly Enterprise Channel – 12 mars 2024) ;
- **2312 - Build 17126.20190** Click-to-Run version Windows (Monthly Enterprise Channel – 13 février 2024)**.**

La version 2308 - Build 16731.20550 Click-to-Run version Windows (Semi-Annual Enterprise channel – 13 février 2024) et d'autres versions antérieures ont été testées et ne semblent pas présenter ce comportement. Les versions intermédiaires aux versions énoncées n'ont pas été testées. Les versions autres que Windows (MacOS et OS mobiles…) n'ont pas été testées.

1.3 Autres logiciels de la suite Office

Les mêmes tests ont été réalisés sur les mêmes versions de Microsoft Excel et OneNote. **Ceux-ci ne semblent pas présenter le comportement d'envoi du contenu des fichiers à leur ouverture.**

2 Sécurité des données traitées par Microsoft lors de l'appel à augloop.office.com

La page suivante de Microsoft précise les conditions et les règles s'appliquant au service : https://learn.microsoft.com/en-us/deployoffice/privacy/connected-experiences

Cette page indique les modalités de traitement et protection des données transmises au service : https://learn.microsoft.com/en-us/deployoffice/privacy/connected-experiences-content

Les traitements réalisés par les expériences connectées bénéficient des engagements de confidentialité associés au contrat avec Microsoft et au service M365, en particulier le respect des limites de données de l'Union Européenne depuis janvier 2023 : https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn

3 Identification de la configuration actuelle et modalités de modification

Les éléments officiels de Microsoft sur la configuration et la désactivation des expériences connectées peuvent être trouvés sur les deux liens ci-dessous et doivent être suivis. Les éléments de ce chapitre sont fournis à titre informatif.

https://learn.microsoft.com/en-us/deployoffice/privacy/connected-experiences

https://learn.microsoft.com/en-us/deployoffice/privacy/manage-privacy-controls#policy-settings-for-connected-experiences

3.1 Identification de la configuration actuelle

La configuration de ce comportement est gérée par la valeur de la clé de registre de type DWORD suivante :

```
Ordinateur\HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\office\16.0\common
\privacy\usercontentdisabled
```

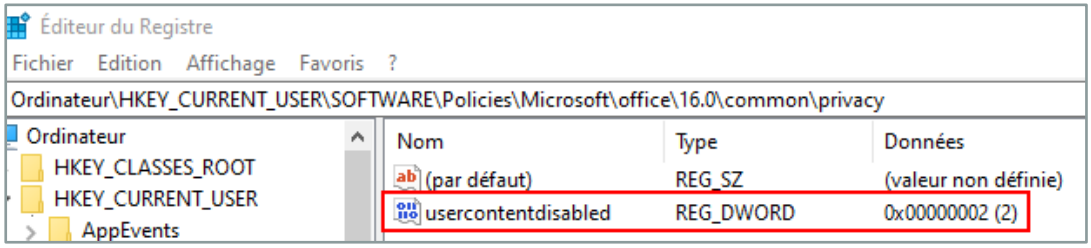

Figure 7 : Clé de registre

Les différentes valeurs de données possibles pour cette clé de registre sont les suivantes :

- **Clé ou dossier de registre absent** : aucune politique n'est définie, la politique par défaut s'applique et les données sont envoyées depuis Microsoft Word et Microsoft Powerpoint ;
- **1** : la politique autorise l'envoi de données et les données sont envoyées depuis Microsoft Word et Microsoft Powerpoint ;
- **2** : la politique désactive l'envoi de données.

3.2 Modalités et évaluation des impacts de la désactivation des expériences connectées analysant le contenu sur les éventuels périmètres le requérant

- En utilisant le service Cloud Policy pour Microsoft 365, la configuration peut être modifiée pour désactiver les expériences connectées envoyant du contenu, avec une granularité permettant de cibler les périmètres le requérant : https://learn.microsoft.com/en-us/deployoffice/admincenter/overview-cloud-policy

La configuration en question est nommée : `Allow the use of connected experiences in Office that analyze content`.

Cette configuration peut être modifiée depuis Intune (nom similaire au paramètre Cloud Policy pour Microsoft 365) ou les outils de modification de clés de registre.

Les expériences connectées analysant le contenu, regroupent de nombreuses fonctionnalités (traduction, prédiction de texte, lecture à haute voix…) listées ici : https://learn.microsoft.com/en-us/deployoffice/privacy/connected-experiences

Leur désactivation entraîne une perte de fonctionnalités pour les utilisateurs. Ainsi, il est recommandé d'identifier les éventuels périmètres concernés, notamment en tenant compte :

- De la politique de sécurité des données en vigueur : sensibilité des données manipulées, recours ou non à des stockages locaux, chiffrement des données, politique d'utilisation du cloud de Microsoft pour certaines données… ;
- Des impacts de la perte de ces fonctionnalités pour les utilisateurs concernés ;
- Des solutions alternatives de sécurisation possibles (version spécifique de PowerPoint et Word - LTSC sans expériences connectées, postes sans accès internet, VDI…).

4 Méthode de reproduction de l'analyse

Afin d'analyser les flux sortant des applications Microsoft Word et Microsoft Powerpoint, il est possible d'utiliser un logiciel proxy local en interception TLS support les *websockets* (par exemple Burp ou Fiddler Classic).

Il suffit ensuite **d'ouvrir un fichier Word ou Powerpoint** tout en capturant les messages transitant avec le proxy, de **modifier le contenu du document** et de rechercher des **connexions à augloop.office.com.** L'analyse du contenu des échanges permet de statuer sur l'envoi ou non d'informations.

Annexe : outillage pour observer ce comportement

Fiddler est un logiciel permettant **l'interception de données transitant sur l'hôte vers le réseau**. Afin de pouvoir mener l'analyse, il est nécessaire de remplir les prérequis suivants :

- Être administrateur local du poste ;
- Désactiver l'éventuel proxy effectuant de la capture de flux ;
- Avoir une connexion à Internet.

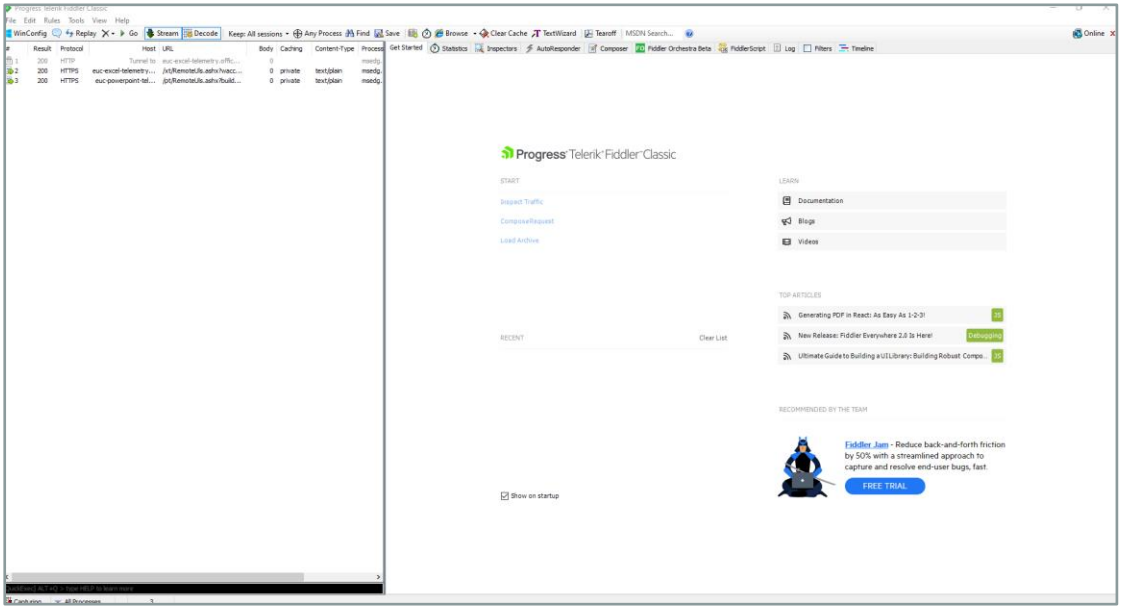

Figure 8 : Page d'accueil de Fiddler Classic

Afin de permettre à Fiddler de capturer et analyser les flux chiffrés en HTTPS, il est nécessaire d'activer le déchiffrement dans les options :

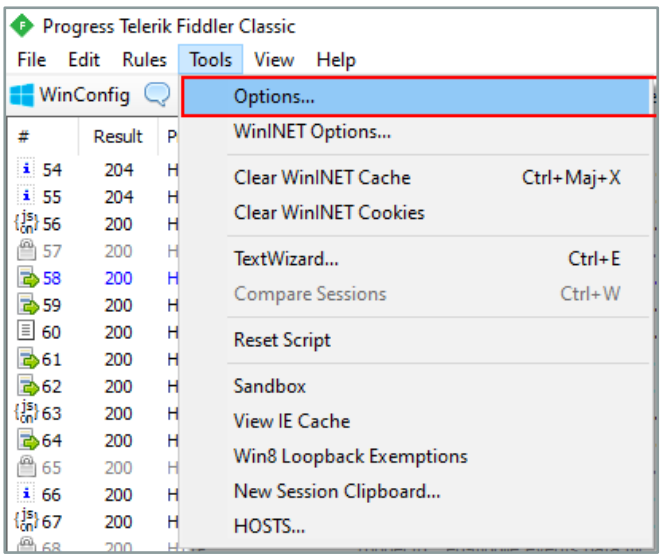

Figure 9 : Options de Fiddler

Dans l'onglet HTTPS, il est nécessaire de cocher l'option HTTPS :

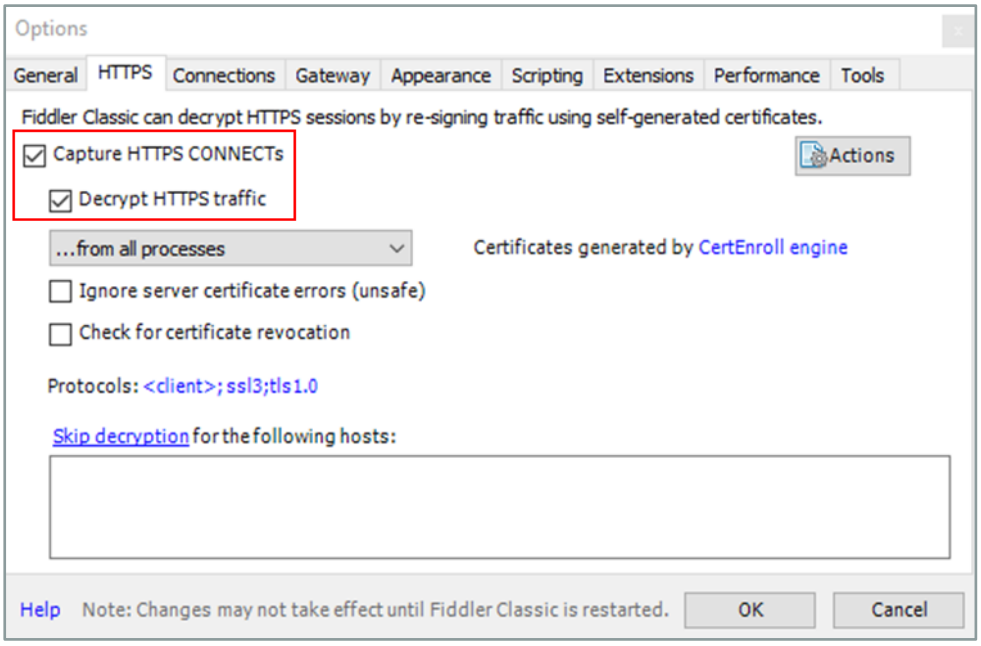

Figure 10 : Activation du déchiffrement HTTPS

S'il s'agit de la première fois que cette option est cochée, Fiddler demandera la **création d'un certificat auto-signée** lui permettant de chiffrer/déchiffrer les données qu'il intercepte. Cette action nécessite des droits administrateurs locaux. Il faut ensuite **ajouter le certificat comme étant de confiance en validant la fenêtre s'affichant**. Une fois validé, l'interception est prête et les flux peuvent être analysés :

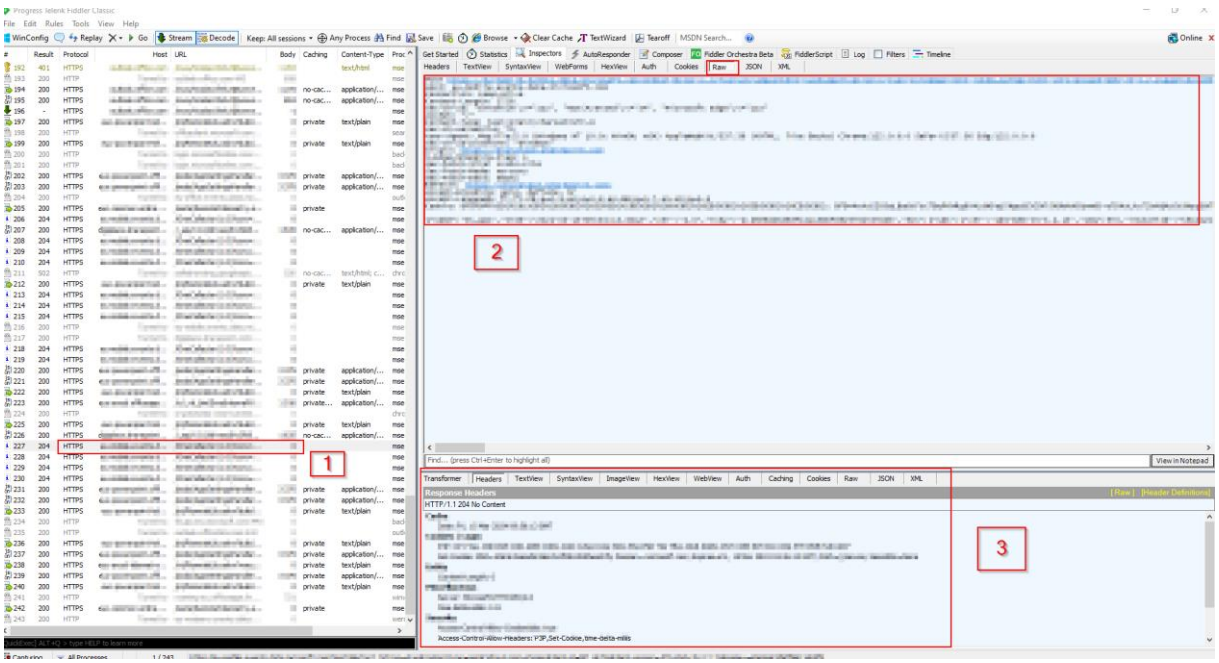

Figure 11 : Interface Fiddler en interception

L'interface est découpée de la façon suivante :

- Dans le cas d'un message HTTP :
  - 1 : message intercepté ;
  - 2 : détail du message intercepté (format de visualisation à sélectionner au-dessus, JSON dans le cadre de cette analyse) ;
  - 3 : réponse au message intercepté (format de visualisation à sélectionner au-dessus, JSON dans le cadre de cette analyse).
- Dans le cas d'un websocket (cf. affichage Fig. 2) :
  - 1 : websocket ;
  - 2 : liste des messages interceptés ;
  - 3 : message (entrant ou sortant) sélectionné (format de visualisation à sélectionner au-dessus, JSON dans le cadre de cette analyse).