

Exécution d'un programme

Éric BERTHOMIER
eric.berthomier@free.fr

17 octobre 2020



Comment se définit un exécutable ?

Exécutable

En informatique et en technologies de l'information, un fichier exécutable, parfois (par métonymie) un programme, ou simplement un exécutable est un fichier contenant un programme et identifié par le système d'exploitation en tant que tel.



Quels sont les types de programmes qui peuvent s'exécuter ?

- .EXE



Quels sont les types de programmes qui peuvent s'exécuter ?

- .EXE
- .BAT



Quels sont les types de programmes qui peuvent s'exécuter ?

- .EXE
- .BAT
- .COM



Quels sont les types de programmes qui peuvent s'exécuter ?

- .EXE
- .BAT
- .COM
- .CMD



Quels sont les types de programmes qui peuvent s'exécuter ?

- .EXE
- .BAT
- .COM
- .CMD
- .MSI



Quels sont les types de programmes qui peuvent s'exécuter ?

- .EXE
- .BAT
- .COM
- .CMD
- .MSI
- ...



Quels sont les types de programmes qui peuvent s'exécuter ?

- .EXE
- .BAT
- .COM
- .CMD
- .MSI
- ...



Quels sont les types de programmes qui peuvent s'exécuter ?

- .EXE
- .BAT
- .COM
- .CMD
- .MSI
- ...

Question

Quelles sont les caractéristiques de ces extensions de fichiers ?



Liaisons fatales ?

- HTML / JavaScript / HTA



Liaisons fatales ?

- HTML / JavaScript / HTA
- VBS / VBA



Liaisons fatales ?

- HTML / JavaScript / HTA
- VBS / VBA
- PowerShell



Liaisons fatales ?

- HTML / JavaScript / HTA
- VBS / VBA
- PowerShell
- ...



Liaisons fatales ?

- HTML / JavaScript / HTA
- VBS / VBA
- PowerShell
- ...



Liaisons fatales ?

- HTML / JavaScript / HTA
- VBS / VBA
- PowerShell
- ...

Question

Quelles sont les caractéristiques de ces extensions de fichiers ?



Liaisons douteuses ?

- Macros



Liaisons douteuses ?

- Macros
- .py Python



Liaisons douteuses ?

- Macros
- .py Python
- .reg



Liaisons douteuses ?

- Macros
- .py Python
- .reg
- PDF



Liaisons douteuses ?

- Macros
 - .py Python
 - .reg
 - PDF
- Flash Player



Liaisons douteuses ?

- Macros
 - .py Python
 - .reg
 - PDF
- Flash Player
 - Plugin Firefox



Liaisons douteuses ?

- Macros
- .py Python
- .reg
- PDF
- Flash Player
- Plugin Firefox
- Plugin IE



Liaisons douteuses - le cas de Adobe Reader

Indépendance de Flash Player

Vous devez disposer de Flash Player pour afficher du contenu Flash dans des fichiers PDF, des porte-documents PDF ...

Flash Player n'est plus fourni avec Adobe Reader et Acrobat.
Les fonctionnalités qui nécessitent Flash utilisent désormais la copie locale de Flash de l'ordinateur.



Surface d'attaque

Surface d'attaque

La surface d'attaque ou surface d'exposition est la somme des différents points faibles (les n vecteurs d'attaque z) par lesquels un utilisateur non autorisé (un n pirate z) pourrait potentiellement s'introduire dans un environnement logiciel et en soutirer des données.



Notre surface d'attaque

Quelques éléments en lien avec les extensions vues précédemment qu'ils nous faudrait bloquer.

- Ne pas laisser les fichier exécutables



Notre surface d'attaque

Quelques éléments en lien avec les extensions vues précédemment qu'ils nous faudrait bloquer.

- Ne pas laisser les fichier exécutables
- Ne pas laisser les fichiers avec Macros



Notre surface d'attaque

Quelques éléments en lien avec les extensions vues précédemment qu'ils nous faudrait bloquer.

- Ne pas laisser les fichier exécutables
- Ne pas laisser les fichiers avec Macros
- Ne pas laisser installer les extensions des navigateurs



Notre surface d'attaque

Quelques éléments en lien avec les extensions vues précédemment qu'ils nous faudrait bloquer.

- Ne pas laisser les fichier exécutables
- Ne pas laisser les fichiers avec Macros
- Ne pas laisser installer les extensions des navigateurs
- Ne pas pouvoir avoir des fichiers .reg



Notre surface d'attaque

Quelques éléments en lien avec les extensions vues précédemment qu'ils nous faudrait bloquer.

- Ne pas laisser les fichier exécutables
- Ne pas laisser les fichiers avec Macros
- Ne pas laisser installer les extensions des navigateurs
- Ne pas pouvoir avoir des fichiers .reg
- Mettre à jour IE / Firefox / Chrome / Opera ...



Notre surface d'attaque

Quelques éléments en lien avec les extensions vues précédemment qu'ils nous faudrait bloquer.

- Ne pas laisser les fichier exécutables
- Ne pas laisser les fichiers avec Macros
- Ne pas laisser installer les extensions des navigateurs
- Ne pas pouvoir avoir des fichiers .reg
- Mettre à jour IE / Firefox / Chrome / Opera ...
- Ne pas mettre Python



Notre surface d'attaque

Quelques éléments en lien avec les extensions vues précédemment qu'ils nous faudrait bloquer.

- Ne pas laisser les fichier exécutables
- Ne pas laisser les fichiers avec Macros
- Ne pas laisser installer les extensions des navigateurs
- Ne pas pouvoir avoir des fichiers .reg
- Mettre à jour IE / Firefox / Chrome / Opera ...
- Ne pas mettre Python
- Ne pas pouvoir exécuter le PowerShell



Notre surface d'attaque

Quelques éléments en lien avec les extensions vues précédemment qu'ils nous faudrait bloquer.

- Ne pas laisser les fichier exécutables
- Ne pas laisser les fichiers avec Macros
- Ne pas laisser installer les extensions des navigateurs
- Ne pas pouvoir avoir des fichiers .reg
- Mettre à jour IE / Firefox / Chrome / Opera ...
- Ne pas mettre Python
- Ne pas pouvoir exécuter le PowerShell
- ...



Exemples de Windows Defender (1/2)

- Bloquer le contenu exécutable à partir d'un client de messagerie et d'une messagerie Web



Exemples de Windows Defender (1/2)

- Bloquer le contenu exécutable à partir d'un client de messagerie et d'une messagerie Web
- Bloquer toutes les applications Office de créer des processus enfants



Exemples de Windows Defender (1/2)

- Bloquer le contenu exécutable à partir d'un client de messagerie et d'une messagerie Web
- Bloquer toutes les applications Office de créer des processus enfants
- Empêcher les applications Office de créer du contenu exécutable



Exemples de Windows Defender (1/2)

- Bloquer le contenu exécutable à partir d'un client de messagerie et d'une messagerie Web
- Bloquer toutes les applications Office de créer des processus enfants
- Empêcher les applications Office de créer du contenu exécutable
- Empêcher les applications Office d'injecter du code

dans d'autres processus



Exemples de Windows Defender (1/2)

- Bloquer le contenu exécutable à partir d'un client de messagerie et d'une messagerie Web
- Bloquer toutes les applications Office de créer des processus enfants
- Empêcher les applications Office de créer du contenu exécutable
- Empêcher les applications Office d'injecter du code dans d'autres processus
- Empêcher JavaScript ou VBScript de lancer du contenu exécutable téléchargé



Exemples de Windows Defender (1/2)

- Bloquer le contenu exécutable à partir d'un client de messagerie et d'une messagerie Web
- Bloquer toutes les applications Office de créer des processus enfants
- Empêcher les applications Office de créer du contenu exécutable
- Empêcher les applications Office d'injecter du code dans d'autres processus
- Empêcher JavaScript ou VBScript de lancer du contenu exécutable téléchargé
- Empêcher l'exécution de scripts potentiellement camouflés



Exemples de Windows Defender (1/2)

- Bloquer le contenu exécutable à partir d'un client de messagerie et d'une messagerie Web
- Bloquer toutes les applications Office de créer des processus enfants
- Empêcher les applications Office de créer du contenu exécutable
- Empêcher les applications Office d'injecter du code dans d'autres processus
- Empêcher JavaScript ou VBScript de lancer du contenu exécutable téléchargé
- Empêcher l'exécution de scripts potentiellement camouflés
- Bloquer les appels d'API Win32 à partir d'une macro Office



Exemples de Windows Defender (2/2)

- Bloquer les fichiers exécutables de s'exécuter, sauf si elles répondent une prévalence, d'âge ou liste approuvée critère



Exemples de Windows Defender (2/2)

- Bloquer les fichiers exécutables de s'exécuter, sauf si elles répondent une prévalence, d'âge ou liste approuvée critère
- Utiliser la protection avancée contre les ransomware



Exemples de Windows Defender (2/2)

- Bloquer les fichiers exécutables de s'exécuter, sauf si elles répondent une prévalence, d'âge ou liste approuvée critère
- Utiliser la protection avancée contre les ransomware
- Bloquer les informations d'identification vol à partir du sous-système d'autorité de sécurité locale (lsass.exe) Windows



Exemples de Windows Defender (2/2)

- Bloquer les fichiers exécutables de sexécuter, sauf si elles répondent une prévalence, dâge ou liste approuvée critère
- Utiliser la protection avancée contre les ransomware
- Bloquer les informations didentification vol à partir du sous-système dautorité de sécurité locale (lsass.exe) Windows
- Bloquer les créations de processus issus de commandes PSEXec et WMI



Exemples de Windows Defender (2/2)

- Bloquer les fichiers exécutables de sexécuter, sauf si elles répondent une prévalence, dâge ou liste approuvée critère
- Utiliser la protection avancée contre les ransomware
- Bloquer les informations didentification vol à partir du sous-système dautorité de sécurité locale (lsass.exe) Windows
- Bloquer les créations de processus issus de commandes PSEXEC et WMI
- Bloquer les processus non approuvés et non signés qui sexécutent de USB



Exemples de Windows Defender (2/2)

- Bloquer les fichiers exécutables de sexécuter, sauf si elles répondent une prévalence, dâge ou liste approuvée critère
- Utiliser la protection avancée contre les ransomware
- Bloquer les informations didentification vol à partir du sous-système dautorité de sécurité locale (lsass.exe) Windows
- Bloquer les créations de processus issus de commandes PSEXEC et WMI
- Bloquer les processus non approuvés et non signés qui sexécutent de USB
- Empêcher les applications de communication Office de créer des processus enfants



Exemples de Windows Defender (2/2)

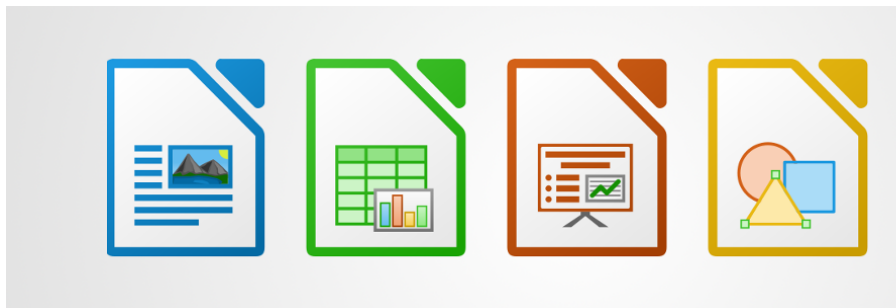
- Bloquer les fichiers exécutables de sexécuter, sauf si elles répondent une prévalence, dâge ou liste approuvée critère
- Utiliser la protection avancée contre les ransomware
- Bloquer les informations didentification vol à partir du sous-système dautorité de sécurité locale (lsass.exe) Windows
- Bloquer les créations de processus issus de commandes PSEXEC et WMI
- Bloquer les processus non approuvés et non signés qui sexécutent de USB
- Empêcher les applications de communication Office de créer des processus enfants
- Empêcher Adobe Reader de créer des processus enfants



Un exemple de problématique



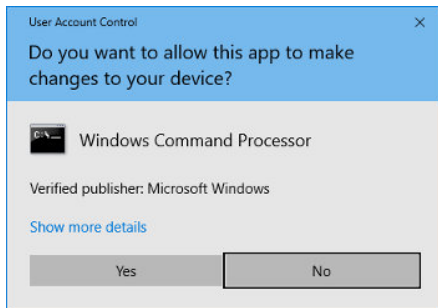
Un exemple de problématique



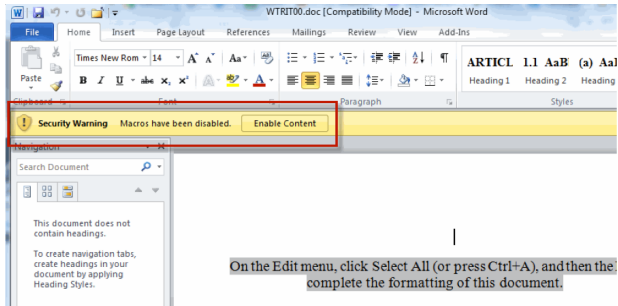
Libre Office intègre en natif Python pour pouvoir réaliser des macros notamment ...



UAC : User Account Control



Macros



On the Edit menu, click Select All (or press Ctrl+A), and then the complete the formatting of this document.



Code

REPRENDRE LE SCHEMA

