Analyse de documents malveillants (partie 4) : mesures défensives, étapes suivantes et conclusion

Français

Jusqu'à présent, nous avons passé en revue une introduction à la modélisation des menaces, l'utilisation de machines virtuelles comme environnements pour analyser les logiciels malveillants et la façon d'analyser les documents PDF et Microsoft Office dans les parties précédentes. Tous ces sujets nous aideront à mieux soutenir les autres comme première ligne de défense contre les documents suspects.

Toutefois, même si nous soutenons les acteurs vulnérables (le public principal visé de cette série de messages), nous savons qu'il ne s'agit que de la moitié du travail. Nous devons également nous assurer de pouvoir fournir des conseils proactifs à nos bénéficiaires afin qu'ils soient bien protégés contre les documents malveillants avant que ceux-ci n'atteignent leurs disques durs. Avec tout le contenu que nous avons examiné, nous pouvons non seulement mieux comprendre les conseils classiques que nous donnons aux utilisateurs finaux, mais aussi proposer quelques mesures supplémentaires qui pourraient être utiles pour les acteurs vulnérables sujets à un risque accru.

La première idée que nous voulons renforcer est la suivante : dire aux militants, journalistes et médias qu'ils doivent éviter d'ouvrir les fichiers issus de sources inconnues n'est **pas** un conseil durable. Dans le cadre de leurs activités, ces personnes doivent ouvrir des fichiers qui leur sont envoyés et qui peuvent contenir des menaces, comme des invitations à une conférence de presse, des documents divulgués, des agendas d'événements, etc. Donc, le conseil le plus pertinent que nous puissions leur donner est de connaître les risques et de mettre en place des processus pour leur permettre d'ouvrir les fichiers de la manière la plus sûre possible.

Voici certaines mesures défensives qui peuvent être mises en œuvre contre les documents malveillants

En général

Solutions antivirus

De nombreux documents malveillants distribués font partie d'opérations massives qui sont documentées et intégrées avec succès dans des bases de données de détection antivirus. Gardez à l'esprit que cette recommandation ne garantit pas la détection des fichiers malveillants développés sur mesure pour des cibles spécifiques. Néanmoins, cela peut procurer une couche de sécurité qui vaut la peine d'être utilisée, surtout si vous travaillez avec de nombreux fichiers non fiables. Pensez à choisir un fournisseur réputé, activez la détection en temps réel si elle est disponible et maintenez la base de données à jour.

Maintenir les logiciels et les licences à jour

Chaque année, des centaines de nouvelles vulnérabilités sont découvertes et divulguées pour de nombreux programmes utilisés quotidiennement, y compris Microsoft Office et les lecteurs PDF, et ces vulnérabilités sont « corrigées » par des mises à jour logicielles. Ainsi, en maintenant tous les logiciels à jour, vous réduirez considérablement le risque qu'une personne mal intentionnée exploitant des vulnérabilités connues et documentées puisse réussir à attaquer une cible. Le piratage des logiciels a une incidence sur leur capacité à détecter et à appliquer les mises à jour logicielles, ce qui constitue un problème de sécurité. C'est pourquoi il est conseillé d'avoir un logiciel original du point de vue de la sécurité, avant même d'aborder les considérations juridiques.

Examiner les extensions de fichier des fichiers suspects

Certaines campagnes incitent les utilisateurs à ouvrir des fichiers dangereux d'un certain type déguisés en documents, comme les applications exécutables, les fichiers zip ou d'autres types de fichiers conteneurs comme les fichiers .iso, etc. Habituellement, ces fichiers incluent même des icônes personnalisées pour ressembler à des documents MS Word, PDF, etc. La vérification soigneuse des fichiers que nous téléchargeons et ouvrons nous apportera une couche supplémentaire de protection en détectant les fichiers dont le type n'est pas commun ou attendu.

Utiliser des lecteurs « empruntés »

Une stratégie courante consiste à ouvrir les documents suspects dans un environnement éloigné de votre ordinateur qui est mieux équipé pour détecter et contenir toute menace potentielle. Un exemple classique consiste à ouvrir les fichiers en utilisant Google Drive (cela inclut les aperçus dans Gmail), car le fichier est effectivement ouvert sur les serveurs de Google avant d'être renvoyé vers nos ordinateurs, ce qui fait de Google (ou toute autre plateforme ayant des capacités similaires) l'acteur qui doit s'inquiéter des menaces spécifiques contenues dans les documents ouverts. L'un des inconvénients de cette approche est que nous perdons une certaine visibilité et réduisons notre capacité d'analyse, étant donné que nous ne téléchargeons pas les fichiers, mais cette option sera utile pour une utilisation quotidienne.

Utiliser des outils spécifiques conçus pour ce cas d'utilisation

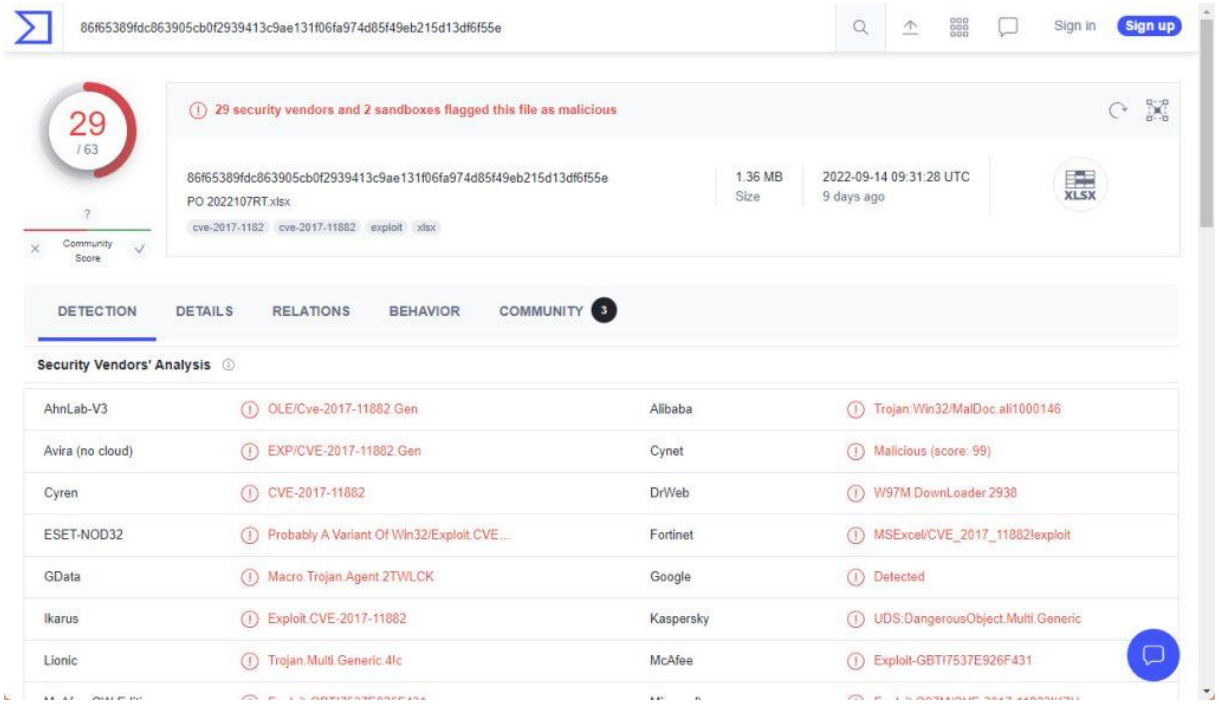
Il existe des outils qui suivent le même principe que celui consistant à utiliser un environnement sécuritaire pour ouvrir les fichiers, mais qui simplifient le processus pour l'utilisateur et qui génèrent ensuite des copies sécurisées contenant uniquement les éléments visibles (comme l'impression du document et la numérisation du résultat dans un fichier final). L'un de ces outils s'appelle Dangerzone. Il s'agit d'un programme qui reçoit un fichier suspect et génère une copie dont l'ouverture est sûre. Le seul inconvénient notable est que l'outil nécessite de télécharger des dépendances de quelques Go. Ainsi, si l'espace disque et/ou la vitesse et la stabilité du téléchargement constituent un problème, cet outil peut s'avérer plus difficile à configurer. Un autre outil pour atteindre cet objectif est le désinfecteur USB CIRCLean de Circ.lu, qui utilise un ordinateur séparé (ils proposent un Raspberry Pi) et deux clés USB. Sur la première clé, vous enregistrez les versions suspectes des fichiers, et le logiciel génère les copies de sauvegarde et les enregistre sur la deuxième

clé USB. Les défis les plus notables de cette approche sont l'utilisation d'un matériel dédié pour faire fonctionner les fichiers et l'ajout d'étapes physiques supplémentaires pour déplacer des fichiers vers et depuis des clés USB.

Vérifier les hachages des fichiers sur des plateformes de détection

Une autre stratégie courante en cas de confrontation avec des fichiers suspects consiste à vérifier dans des plateformes telles que VirusTotal si le fichier est reconnu comme étant malveillant. Cela nous aidera à gagner du temps si le fichier constitue une menace connue et nous donnera même des informations plus précieuses, telles que le type de logiciel malveillant qu'il tente d'exécuter et les messages des membres de la communauté relatifs au fichier. Il est très important de souligner que le téléchargement du fichier sur des outils tels que VirusTotal le mettra à la disposition de la communauté, en divulguant le contenu du document (qui pourrait contenir des informations sensibles), et potentiellement alerter les créateurs du document s'ils surveillent le fichier spécifique. Il est possible de contourner ce problème en évitant d'importer le fichier et en vérifiant simplement son hachage. Dans la première partie de cette série, des conseils sont fournis sur la façon de vérifier les hachages.

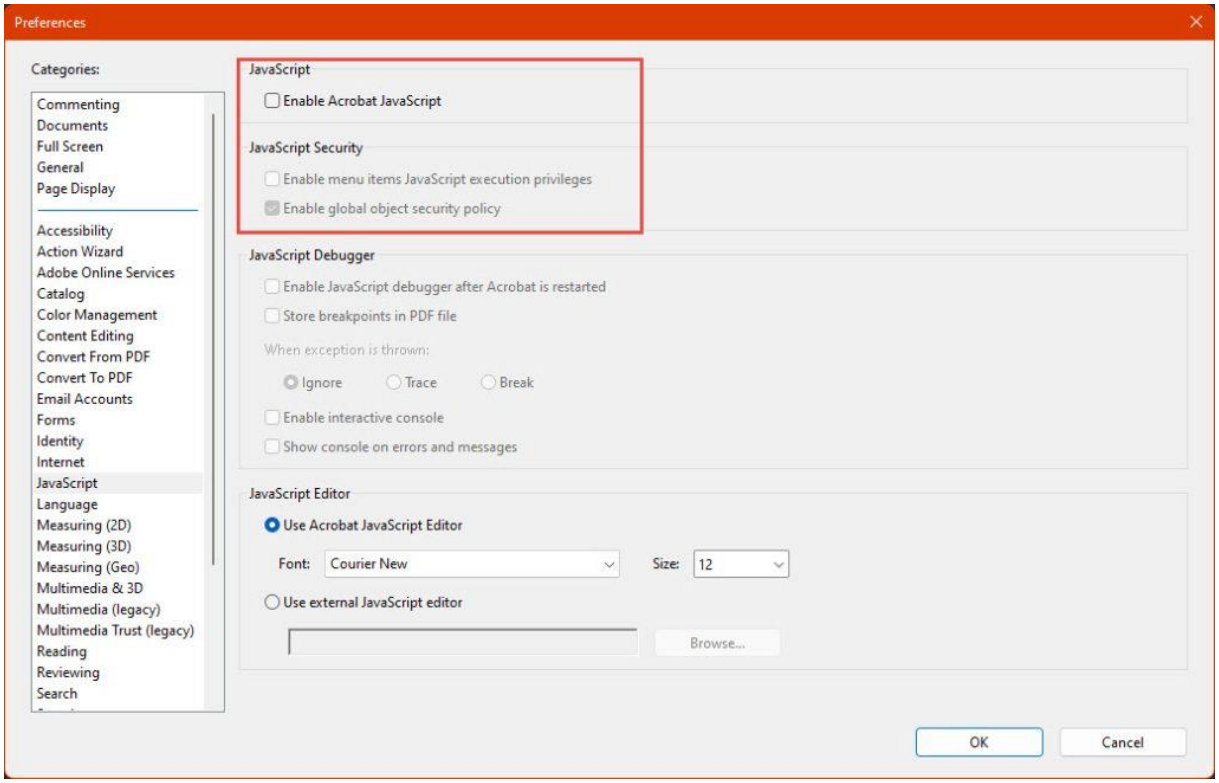
Exemple de recherche du hachage d'un fichier, août 2022



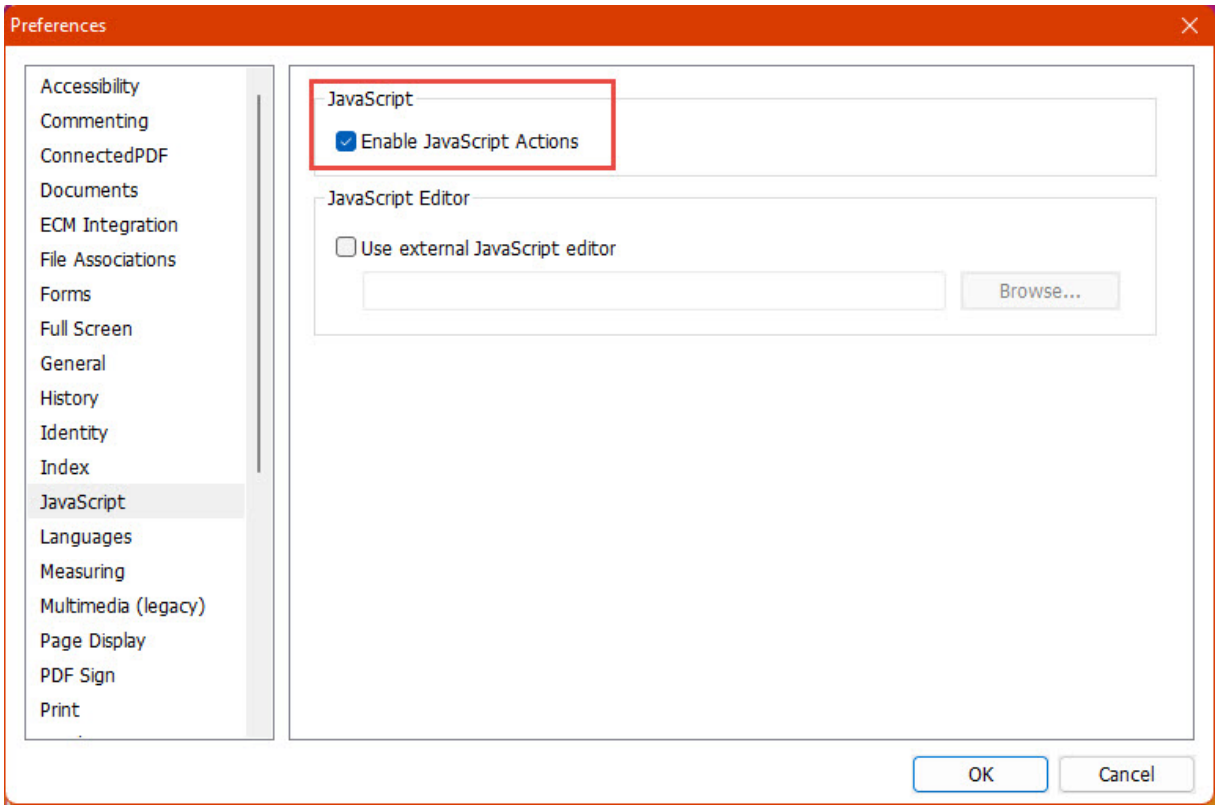
Exemple de résultats dans VirusTotal, août 2022

Spécifique aux fichiers PDF : désactivez l'exécution de Javascript dans le lecteur (et autres paramètres de sécurité)

Selon votre logiciel de lecture PDF, l'exécution du code JavaScript peut déjà être désactivée, mais il est conseillé de le vérifier si vous comptez ouvrir des fichiers suspects. En outre, selon le lecteur utilisé, vous pouvez disposer d'autres fonctionnalités de sécurité qui peuvent être configurées.



Exemple pour Acrobat Reader (août 2022, Menu Édition -> Préférences -> Javascript)



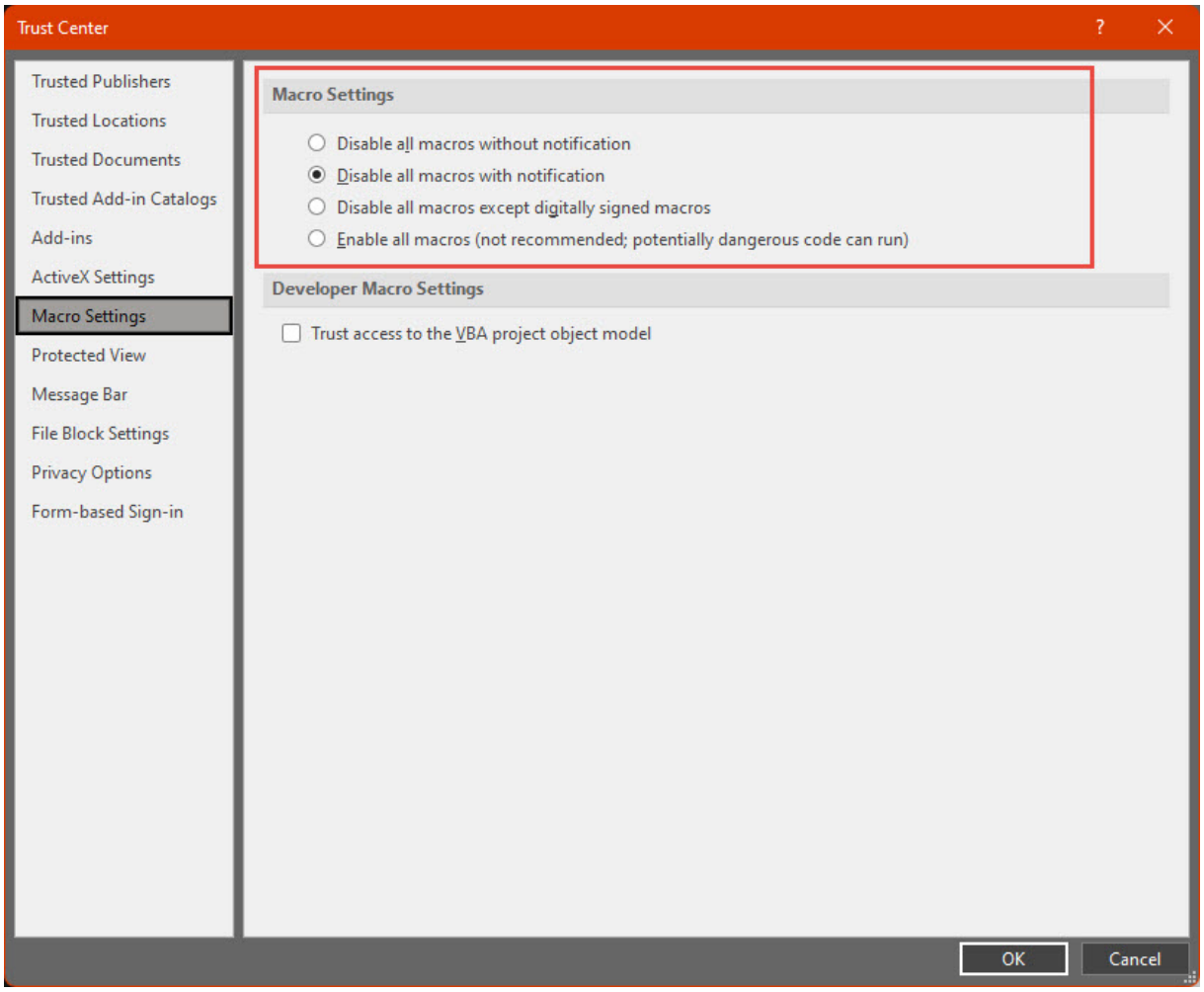
Exemple pour Foxit Reader (août 2022, Menu Fichier -> Préférences -> Javascript)

Spécifique aux fichier Office : minimisez l'utilisation des macros dans les activités légitimes

Même s'il existe de nombreux cas d'utilisation acceptables et inoffensifs pour les macros, leur utilisation fréquente dans les documents et l'habitude de les autoriser pourraient ouvrir exposer l'utilisateur au risque de recevoir des documents malveillants et d'autoriser accidentellement ses macros. Les organisations en particulier devraient être conscientes de cette situation et planifier en conséquence ou supprimer l'utilisation des macros, ou préparer des processus pour assurer leur gestion, en considérant comment gérer les fichiers non fiables.

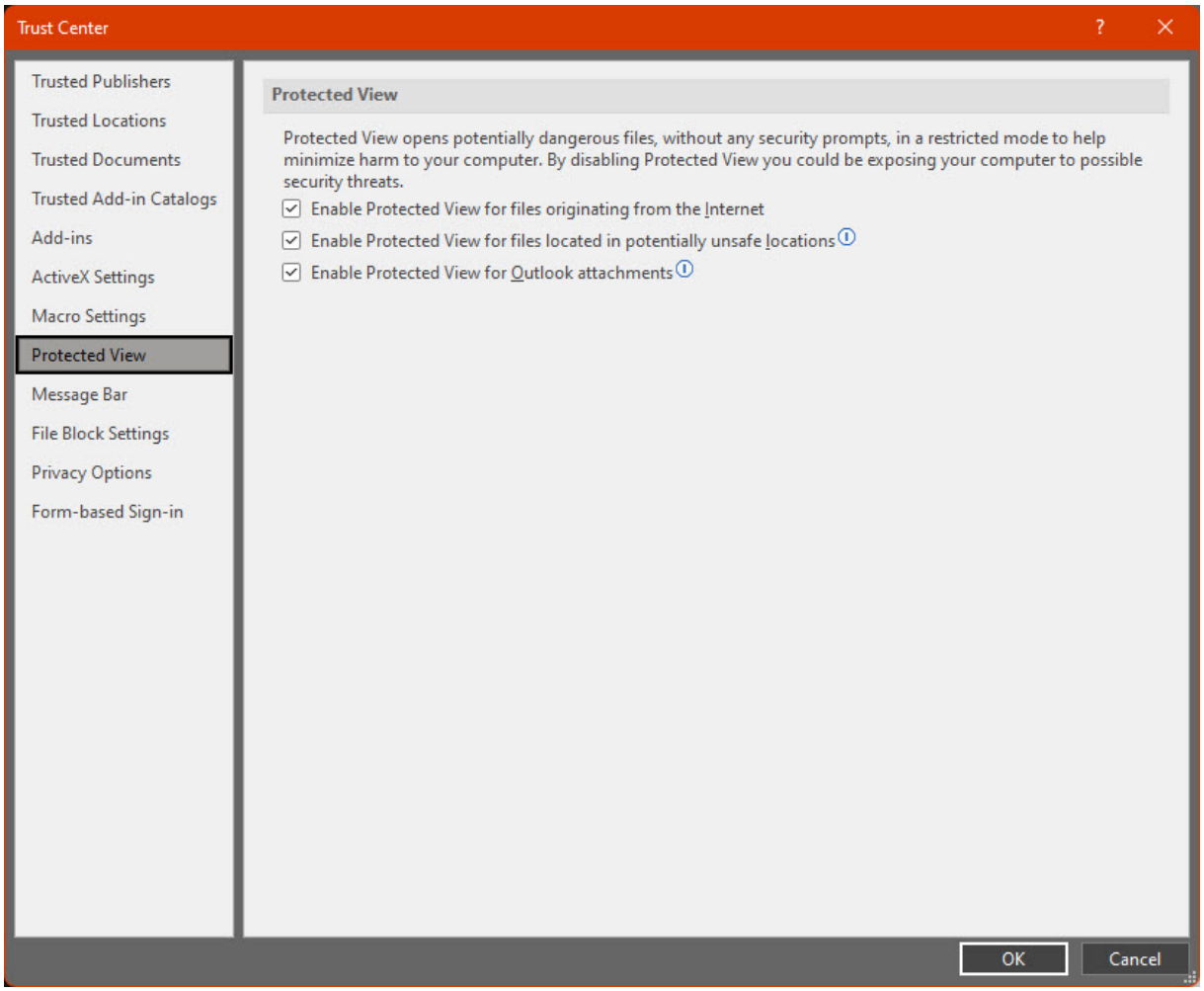
Spécifique aux fichiers Office : désactivez les macros et consultez le Centre de gestion de la confidentialité

Microsoft Office a récemment modifié sa politique concernant les macros plusieurs fois. À l'heure où vous lisez ce contenu, Office peut donc avoir des macros activées ou désactivées par défaut, et des règles peuvent être en place en fonction de l'origine des fichiers, etc. Pour avoir plus de visibilité et de contrôle, il est possible de consulter le Centre de gestion de la confidentialité pour voir et configurer directement le comportement lié aux macros.

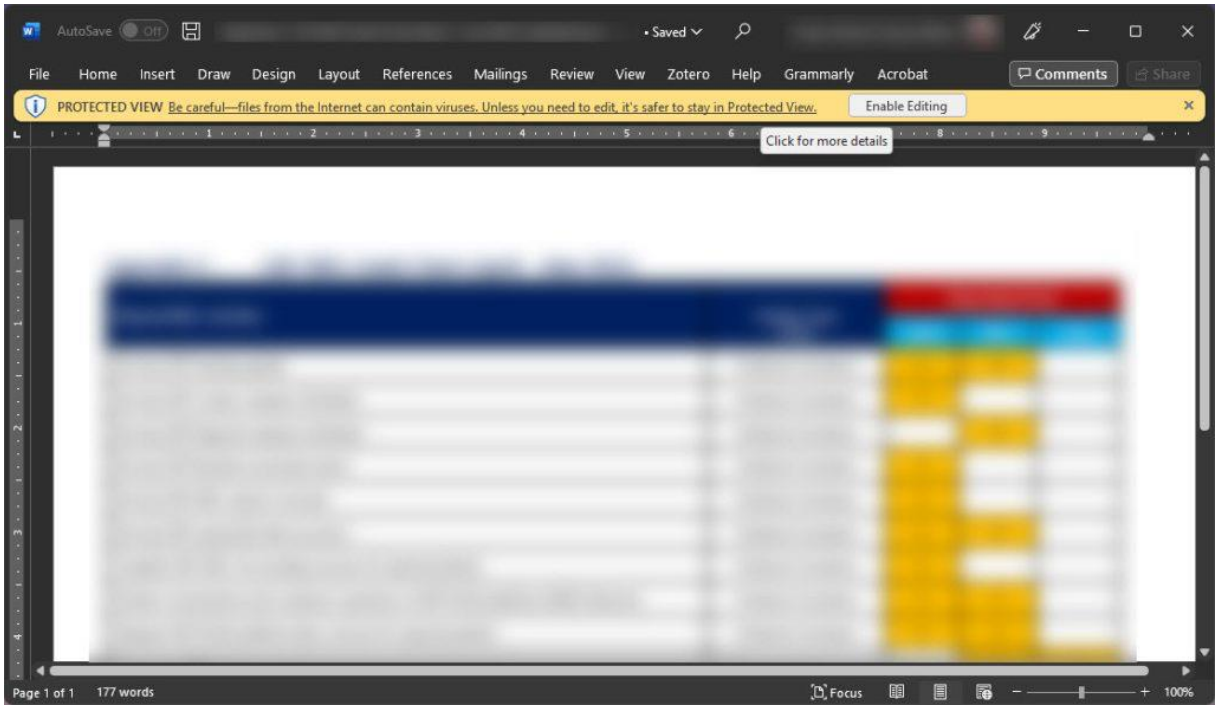


Centre de gestion de la confidentialité pour MS Office (août 2022, Menu Fichier -> Options -> Centre de gestion de la confidentialité -> Paramètres du Centre de gestion de la confidentialité -> Paramètres des macros)

Une autre fonctionnalité intéressante de MS Office est la vue protégée, qui permet, en considérant l'origine d'un fichier, de l'ouvrir dans un environnement de bac à sable avec peu de privilèges ou d'accès pour interférer avec l'ordinateur, en assurant ainsi une couche supplémentaire de protection. L'un des problèmes liés à ce mode est que, comme pour le blocage des macros, un bouton est présent dans le ruban situé au-dessus du document via lequel l'utilisateur peut désactiver la fonctionnalité de vue protégée et permettre ainsi les attaques lorsque le créateur du document trompe l'utilisateur en l'incitant à désactiver cette protection.



Paramètres de la vue protégée (août 2022, Menu Fichier -> Options -> Centre de gestion des comptes -> Paramètres du centre de gestion des comptes -> Vue protégée)



Vue protégée pour un document MS Word (août 2022)

Et ensuite ?

Tout d'abord, lorsque vous recevez un fichier suspect, vous avez les compétences nécessaires pour effectuer une première analyse afin de détecter tout problème de sécurité évident. Les scénarios possibles peuvent être résumés comme suit :

1. Si le fichier ne semble pas contenir d'éléments dangereux, nous pouvons réduire le niveau de suspicion du fichier.
   - Si, par hasard, la cible présente un niveau de risque élevé, nous pouvons consulter des collègues ou des groupes plus spécialisés.
2. Si le fichier semble malveillant, nous pouvons tenter de rechercher son hachage sur des plateformes telles que VirusTotal. Ainsi, s'il s'agit d'un échantillon connu de logiciel malveillant, nous pourrons trouver des informations plus détaillées qui nous seront utiles pour comprendre la nature de la menace, l'ampleur de la campagne, etc.
3. Si les menaces contenues dans le fichier sont faciles à détecter et à comprendre, mais inconnues auprès de la communauté, nous devrions fournir un aperçu des détails lors des recherches supplémentaires ou lorsque nous sollicitons de l'aide.
4. Si les éléments contenus dans le fichier semblent avancés, difficiles à comprendre ou même difficiles à classer en tant que menaces, et que le hachage du fichier est inconnu des plateformes publiques, il peut être utile de contacter des organismes plus spécialisés qui pourront examiner le fichier à la recherche de menaces moins évidentes.

Nous conseillons également en général :

- Évitez d'exécuter le moindre code suspect (sauf si vous comprenez les risques et prenez les précautions respectives, qui ne sont pas abordées dans ce contenu)
- Faites des recherches plus approfondies sur les éléments que vous constatez et que vous ne connaissez pas. Il existe de nombreuses commandes et façons différentes d'accomplir des choses avec le code, et il est impossible de les connaître toutes. Il est donc normal et attendu de consulter la documentation à la recherche d'instructions ou de fonctionnalités spécifiques pour mieux comprendre les fonctionnalités d'une macro ou d'autres éléments inconnus.

Gardez à l'esprit que l'analyse de documents malveillants (et de logiciels malveillants en général) est une carrière complète qui nécessite généralement des années d'expérience pour traiter les cas plus avancés. Nous insistons sur le fait que ce document est une introduction à une partie spécifique de l'analyse des logiciels malveillants, qui, espérons-le, encouragera le lecteur à en apprendre davantage et à acquérir plus de compétences dans ce domaine. Toutefois, étant donné le risque associé à l'utilisation d'artefacts malveillants sans processus et considérations de sécurité appropriés, nous déconseillons aux lecteurs d'ajouter des processus et des outils d'analyse supplémentaires aux flux de travail présentés sans connaître ces processus et ces outils, surtout s'ils impliquent l'exécution de logiciels malveillants (ou leur analyse dynamique).

Il s'agit d'un contenu en constante révision. Si vous avez des questions ou des commentaires, veuillez contacter cguerra@internews.org