ORHUS

État de l’art sur les macrovirus

Macro, de la brise à la tramontane

GUENARD Antoine
LAFARGUE Anaëlle
DINAR BAKIOUI Ismaël
ROIG Raphaël
POON Stéphane
14/12/2021

Table des matières

Qu’est-ce qu’un macrovirus ?

Une macro (ou macro-instruction) est une liste d'ordres préalablement enregistrés et correspondants à des tâches qui doivent être régulièrement effectuées par l'ordinateur. L’ordinateur peut alors les réaliser de façon automatique. Basiquement, ce sont des programmes préenregistrés sur un fichier qui peuvent se lancer automatiquement sur celui-ci (actions répétitives et complexes notamment).

Les logiciels de la suite Office utilisent **VBA** (*Visual Basic for Application*) comme langage de programmation pour l’écriture de macros.

Un macrovirus est une macro attachée à un fichier ou logiciels bureautique, qui est capable d’altérer ou d’exécuter des actions non désirées par l’utilisateur. Un macrovirus est alors en mesure de modifier des fichiers, télécharger des fichiers, récupérer des informations sur le système hôte, etc.

Un macrovirus est centré sur le côté logiciel et ne dépend donc pas du système d’exploitation sous-jacent permettant ainsi d’infecter n’importe quelle cible.

Un macrovirus est plus transmis via Phishing (hameçonnage), une technique utilisée par des fraudeurs pour obtenir des informations/données d’un utilisateur en se faisant passer pour quelqu’un de confiance. Un hackeur peut ainsi se faire passer pour une entreprise/une personne de confiance et envoyer un mail contenant un fichier avec des macros malveillantes pour réussir à soutirer des informations, modifier ou supprimer des fichiers.

Depuis la sortie de Microsoft Office 2000, Microsoft a désactivé l’exécution par défaut des macros au lancement du document. Néanmoins, tant que les macros sont disponibles pour l’utilisateur, le risque est toujours présent.

Types de macros :

On sépare les macrovirus en 4 types différents, chacun ayant des agissements différents sur la machine :

- **Standard :** Un processus basique qui peut être inséré dans le document et utilisé comme outil.
- **Batch :** Une macro Batch s'exécute plusieurs fois dans l'environnement de travail et crée un résultat après chaque analyse. La macro s'exécute une fois pour chaque enregistrement (ou un groupe sélectionné d'enregistrements) dans les données. Les entrées peuvent être configurées pour être utilisées dans chaque exécution du fichier ou uniquement dans des exécutions spécifiques.
- **Itérative :** Des macros qui se mettent en route pour un certain nombre (défini à l'avance) de fois ou jusqu'à ce qu'une certaine action soit faite.
- **Location Optimisateur :** Ce sont des macros itératives qui sont utilisées dans l'analyse du réseau pour identifier un ou des emplacements optimaux.

Types de macrovirus :

Les macros peuvent faire un grand nombre d'actions sur un ordinateur, de ce fait, beaucoup de macrovirus différents ont été créés, voici les plus connus :

- Concept :
    - Découvert en juillet 1995 et ciblant Microsoft Word
    - Le virus affichait une boîte de dialogue avec le nombre 1 et un bouton OK.
    - À ses débuts environ 20% des infections des virus sur les ordinateurs étaient des infections Concept, puis à partir de 1997 environ 50% des infections par virus étaient des infections Concept

- Melissa :
    - Découvert le 26 mars 1999
    - A infecté des milliers d'utilisateurs en quelques heures, une des propagations les plus rapides d'Internet
    - Le montant estimé des dégâts est de 385 millions de dollars (source : International Computer Security Association)
    - Melissa arrivait dans un email avec l'objet : "Important Message From <adresse email du compte infecté>" avec comme message "Here is that document you asked for … don't show anyone else 😉".
    - L'infection se répandait via les utilisateurs ayant Word (version 97 ou 2000) ou ceux ayant Outlook (version 97 ou 98)

- Wazzu :
    - Découvert en 1996.
    - Lorsque le document infecté était ouvert, le virus infectait le template NORMAL.DOT, ainsi les prochains documents créés étaient eux aussi infectés.
    - Le virus plaçait le mot wazzu à un moment au hasard dans le document.

D'autre macrovirus, on fait leurs apparitions en reprenant des principes similaires :

- Nuclear :
    - Apparu rapidement après Concept
    - À l'inverse de Concept n'annonce pas son infection
    - Lorsque l'on fax ou imprime un document, insertion de deux lignes de textes à la fin du document : "STOP ALL FRENCH NUCLEAR TESTING IN THE PACIFIC"

- Sharefun :
    - Basé partiellement sur Wazzu
    - Découvert le 18 février 1997
    - Est le premier virus à se propager via mail.
    - Ironiquement, a raté à se propager mondialement alors que c'était le premier virus à se propager via mail.

Types d'infections :

Les macrovirus peuvent effectuer différents types d'infections, par exemple :

- Trojan :
    - Rovnix : La victime recevait un document ayant une fausse alerte Microsoft demandant à autoriser les macros. Une fois ceci fait, la macro implémentait 3 scripts cachés permettant de récupérer les mots de passe et d'enregistrer ce qui était tapé au clavier.
    - Dridex : Après activation des macros sur le document malveillant, celles-ci enregistraient le logiciel Dridex permettant de voler les données bancaires de la victime.

- Ransomware :
    - Locky : La macro une fois autorisée chiffrait les dossiers de la victime pour les tenir en otage, attendant une rémunération pour récupérer les fichiers.

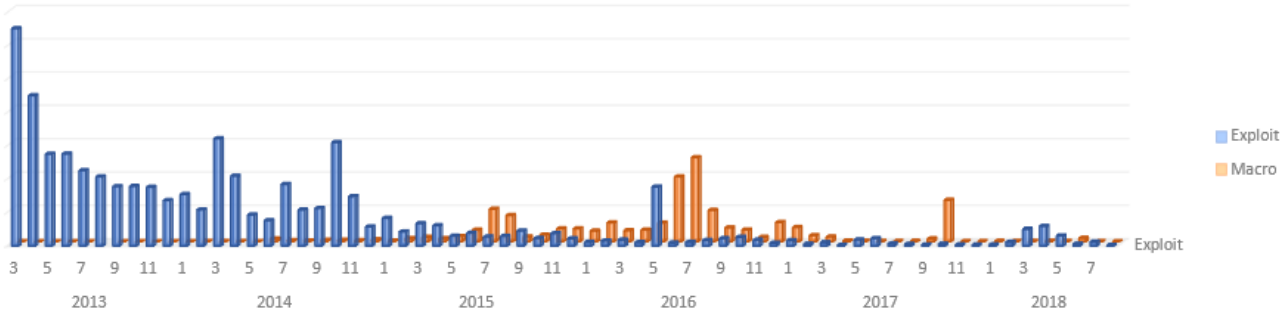
- Logiciels espions :
    - Gator : logiciel diffuseur de spyware qui enregistre les liens des sites web visités pour les stocker et cibler les pages web publicitaires diffusés chez l'internaute.
    - Cydoor: logiciel qui a pour but de télécharger des publicités des serveurs Cydoor, le logiciel se met à jour automatiquement et il ne peut pas être désinstaller avec Windows Uninstaller.

- Rootkits :
    - ZeroAccess : rootkit noyau qui a affecté plus de 2 millions d'utilisateurs dans le monde. Ce rootkit télécharge et installe un maliciel sur la machine infectée l'intégrant dans un botnet mondial utilisé par les pirates pour effectuer d'autres attaques.
    - Flame : Flame surveille le trafic du réseau, peut effectuer des captures d'écran et audio, enregistrer l'activité du clavier.

Éléments statistiques :

Voici des éléments statistiques concernant l'impact des macrovirus, et comment ceux-ci arrivent à être l'un des principaux vecteurs d'infection d'attaque par Phishing.

- 62% des appareils infectés par des logiciels malveillants étaient des appareils grand public tandis que 38% étaient des systèmes d'entreprise.
- 20% des Américains ont fait face à des attaques de ransomware.
- 38% des pièces jointes malveillantes étaient au format Microsoft Office.
- L'erreur humaine est à l'origine de plus de 85% des violations de cybersécurité.
- 94% des logiciels malveillants sont livrés par e-mail.
- 71% des attaques sont motivées financièrement, suivi par le vol de propriété intellectuelle puis l'espionnage
- On a constaté une résurgence des attaques par macros au cours des dernières années par rapport aux attaques exploitant des faiblesses des applications



Prévalence des attaques exploitant des faiblesses des applications contre des attaques macros observée via Windows Defender ATP

Modes de propagation :

Un macrovirus peut être propagé par plusieurs moyens différents :

- Pièce jointe d'un message électronique (mail)
- CD-ROM
- Clé USB
- Téléchargé par l'utilisateur suite à une action de Phishing

Que peut faire un macrovirus ?

Un macrovirus est capable d'effectuer plusieurs actions sur un ordinateur comme d'envoyer des emails, télécharger des documents/logiciels sur internet ou même d'éxécuter des logiciels, modifier des fichiers Office en s'y attachant, uploader des informations sur internet (ou les envoyés au créateur du virus), corrompre des données, formater des disques durs...

Évolution des mesures contre les macrovirus :

Initialement les macrovirus infectaient majoritairement les documents Word et Excel et ciblaient majoritairement le système d'exploitation Windows. Depuis, les macrovirus peuvent infecter d'autre systèmes d'exploitation.

Depuis la sortie de Microsoft Office 2000, les macros sont désactivées par défaut.

Depuis Microsoft 2007, les fichiers avec l'extension "x" (docx, xlsx, pptx) ne peuvent plus contenir des macros, seuls les fichiers avec l'extension "m" (docm, xlsm, pptm) peuvent contenir des macros.

Outils pour automatiser la création de macros :

Pour automatiser la création d'une macro, il existe différents outils et méthodes :

1. Unicorn PowerShell based payload:
   - Ce payload utilise une version inférieure de Powershell.exe en ligne de commande pour installer un autre virus (on parle de 2nd stage)
   - Le problème de cette attaque est que le script n'utilise que Powershell.exe et qu'une boite de message est présentée à l'utilisateur lui demandant de fermer le fichier Word/Excel. Le payload ne s'exécute qu'à la fermeture du fichier.

2. regsvr32 based method
   - Cette méthode créée un outil intégré de Microsoft nommé regsvr32 qui est normalement utilisé pour enregistrer des objets (OLE Controls / ActiveX) même depuis des ressources à distance en utilisant un fichier scriptlet (.sct). L'attaque tire parti de cette fonctionnalité par le biais de fichiers scriptlet malveillants.
   - L'avantage de cette méthode est que regsvr32 est sur liste blanche par défaut et peut donc s'exécuter même dans un environnement contrôlé par des SRPs (Software Restriction Policies).

3. Metasploit generated payload vba-exe
   - L'outil msfvenom de Metasploit permet de générer un payload vba-exe en deux parties : une macro à coller dans l'éditeur macro d'un fichier office et qui utilise la fonction Auto_Open pour s'exécuter au démarrage de la machine hôte, et un fichier exe encodé contenant le payload qui doit être lui collé au sein même du document.

4. Metasploit generated payload vba-psh
   - En utilisant toujours l'outil msfvenom pour générer un payload vba-psh similaire au payload Unicorn car il invoque aussi Powershell.exe

5. Empire generated Windows/macro stager
   - L'outil PowerShell Empire peut créer une macro préparant un écouteur (listener).

6. Using Veil-Evasion generated powershell.exe command within Luckystrike generated macro
   - Cette méthode génère un fichier bat (commande PowerShell) avec Veil-Evasion qui sera exécuté par une macro préparer par Luckystrike.

7. wePWNise architecture-independent Macro dynamically bypassing SRPs+EMET
   - L'outil wePWNise de MWRLabs permet d'intégrer des payload x86 et x64 générés au préalable directement dans des scripts VBS capables d'énumérer eux-mêmes les politiques de sécurité SRPs et EMET pour trouver les failles et les utiliser pendant l'exécution de la macro. Cela en fait un outil très utile dans des environnements particulièrement surveillés.

8. Custom macro taking commands from Author property to feed them to StdIn of Powershell
    - En utilisant la commande VBA ActiveWorkbook.BuiltinDocumentProperties("Author") et CreateObject("WScript.Shell") on peut passer une commande PowerShell en la plaçant dans les propriétés de l'auteur du document pour éviter que cette commande soit enregistrée dans l'Event Logs de Windows.

9. ActiveX-based (InkPicture control, Painted event) autorun macro
    - Dans "Developer tab on ribbon -> Insert -> More Controls -> Microsoft InkPicture Control", on peut ajouter en double cliquant ce qui va faire apparaître une fenêtre de modification de macro où l'on peut coller une des macros ci-dessus.
    - Cette méthode permet de lancer automatiquement la macro sans utiliser AutoOpen() and Document_Open(), de plus au lieu d'avoir à l'ouverture du fichier "Macros have been disabled" on a "Some active content has been disabled" ce qui permet plus facilement de forcer la victime à cliquer sur "enable content".

10. Generate Base64-encoded HTA application to be decoded using certutil
    - Cette méthode consiste à générer un fichier (souvent une application HTA qui est permet de réduire la détection d'antivirus classique) puis le télécharger via un script powershell, puis le faire passer par cerutil pour le décoder (base64) et le lancer.

Comment se protéger des macrovirus :

Pour se protéger des macrovirus, l'utilisateur doit éviter de désactiver la sécurité intégrée contre les macros dans les options de la suite Office (Options -> Centre de gestion de la confidentialité)

L'utilisateur peut aussi verrouiller le document NORMAL.DOT avec un mot de passe, ce qui permet de diminuer le risque d'infection sur d'autres documents.

Bibliographie :

http://virus.wikidot.com/

https://web.archive.org/web/20110604162558/http:/support.microsoft.com/kb/187243/en

https://web.archive.org/web/20060612205443/http:/ciac.org/ciac/bulletins/i-023.shtml

https://www.howtogeek.com/171993/macros-explained-why-microsoft-office-files-can-be-dangerous/

https://www.techtarget.com/searchsecurity/definition/macro-virus

https://softwarelab.org/fr/rootkit/

https://www.kaspersky.fr/resource-center/threats/computer-viruses-and-malware-facts-and-faqs

https://gist.github.com/mgeeky/9dee0ac86c65cdd9cb5a2f64cef51991/