

# MARC BLANCHARD VIRUS DOCTEUR

## [Définition&Explications] Technologies embarquées dans les virus

Dans cette section pour tout public, je vais essayer d'aborder de manière la plus compréhensible un certain nombre de termes que nous utilisons dans notre métier, nos laboratoires et que, peut-être, vous rencontrerez dans les différents compte-rendus scientifiques sur ce site.

Dans ce post, voici une petite explication sur certaines variantes de technologie embarquées dans les codes des virus.

Les catégories que nous allons expliquer ci-dessous peuvent être imbriquées dans codes programmes des virus.

### **Virus multi-partite ou virus bi-valent**

C'est un virus qui capable d'infecter 2 ou plusieurs types de fichiers dans le même code.

Exemples :

- Un EXE peut infecter les fichiers EXE et le secteur de boot
- Un EXE peut infecter les fichiers EXE et le normal.dot

Les familles des virus Junky ou Tequila appartiennent au premier exemple.

### **Virus polymorphes ou polymorphiques**

Ce type de virus change son code à chaque infection

Le décodage est géré par le code du virus lui-même !

Il est très difficile de le voir dans un désassembleur parce que la plupart du temps ces virus contiennent une routine anti-debug.

Dans ce cas, il est impossible de voir le code du virus.

On peut juste utiliser un viewer hexadécimal ? mais bien souvent le virus est crypté.

La solution la plus facile consiste à travailler avec ?baits file? et d'analyser les différences.

Exemple : MTX

### **Virus furtifs**

Cette catégorie de virus peut se supprimer ou se camoufler quand un programme spécifique tourne sur la machine (par exemple un antivirus)

Généralement ils interceptent les interruptions int21h AH=11h,12h,4Eh,4Fh, int25h,int13h

Pour les voir, nous avons besoin de trouver le fichier infecté et de le regarder en hexadécimal depuis une machine saine.

Note: Un virus macro furtif est appelé ainsi si la fonction Outils/Macro disparaît.

### **Virus furtifs d'encryption/déryption à la volée**

Ce type de virus est rare !

Le concept est que le virus chiffre le disque dur et sa position est sur le MBR (MultiBootRecord) qui lui même contient l'algo de cryptage/Décryptage à la volée.

Quand le virus chiffre complètement le disque dur, il n'est plus possible d'accéder aux données.

Exemple : OneHalf

### **Virus métamorphes**

C'est une technologies très complexe qui utilise EPO (EntryPointObscuring).

Le virus insère/modifie lui-même un JMP dans l'EntryPoint sans aucune autre modification dans le header du fichier.

Il est très difficile pour un moteur de scan de voir la différence entre le code du programme et celui du virus. (ex:MTX).

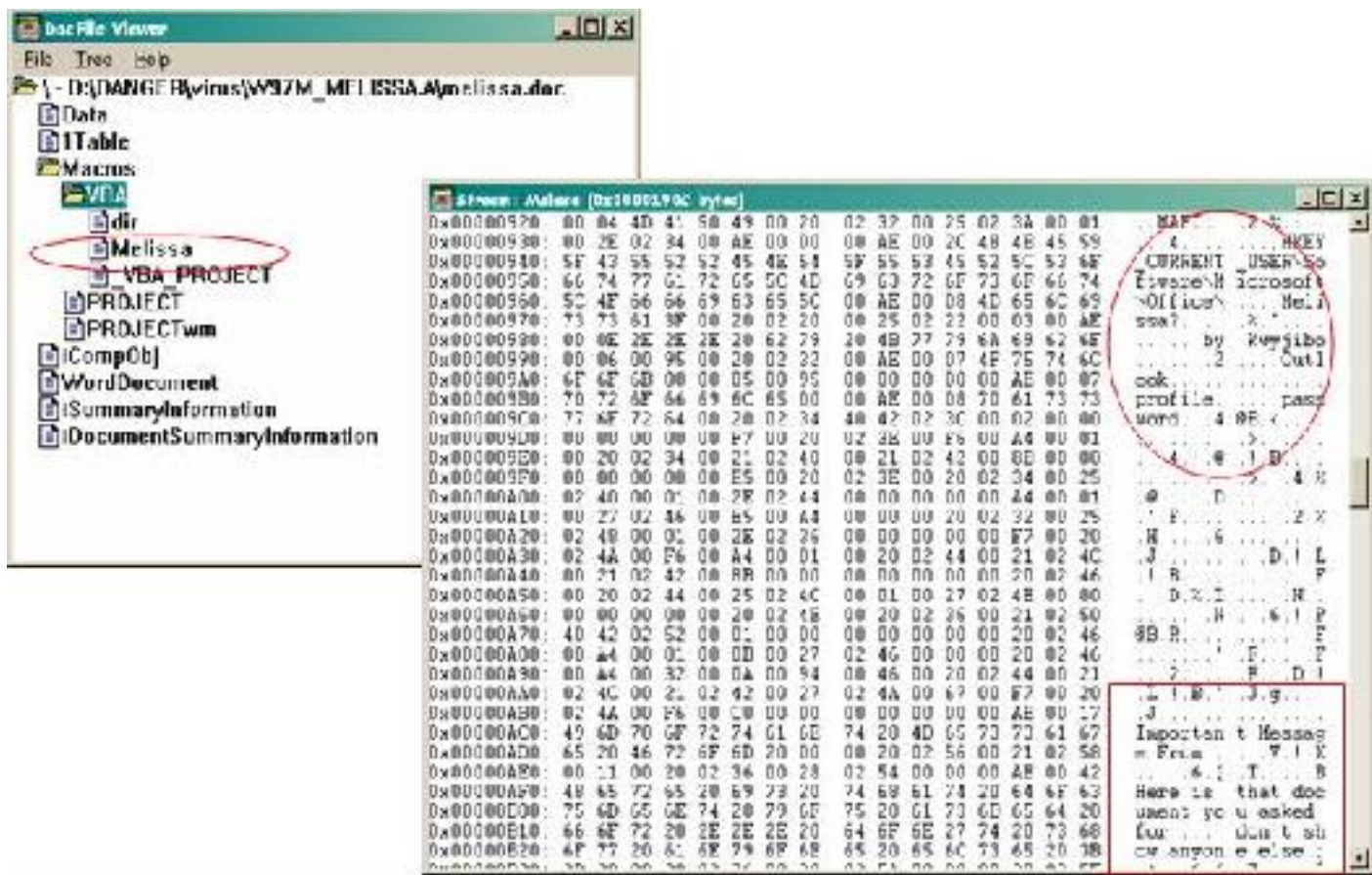
Les virus métamorphes peuvent utiliser les instructions du Co-Processeur & MMX (Multi-Media) (ex:THORIN).

Les virus métamorphes peuvent utiliser le calcul de checksum de fichiers quand les Kernel est infecté, simulant ainsi un update d'OS (ex:KRIZ)

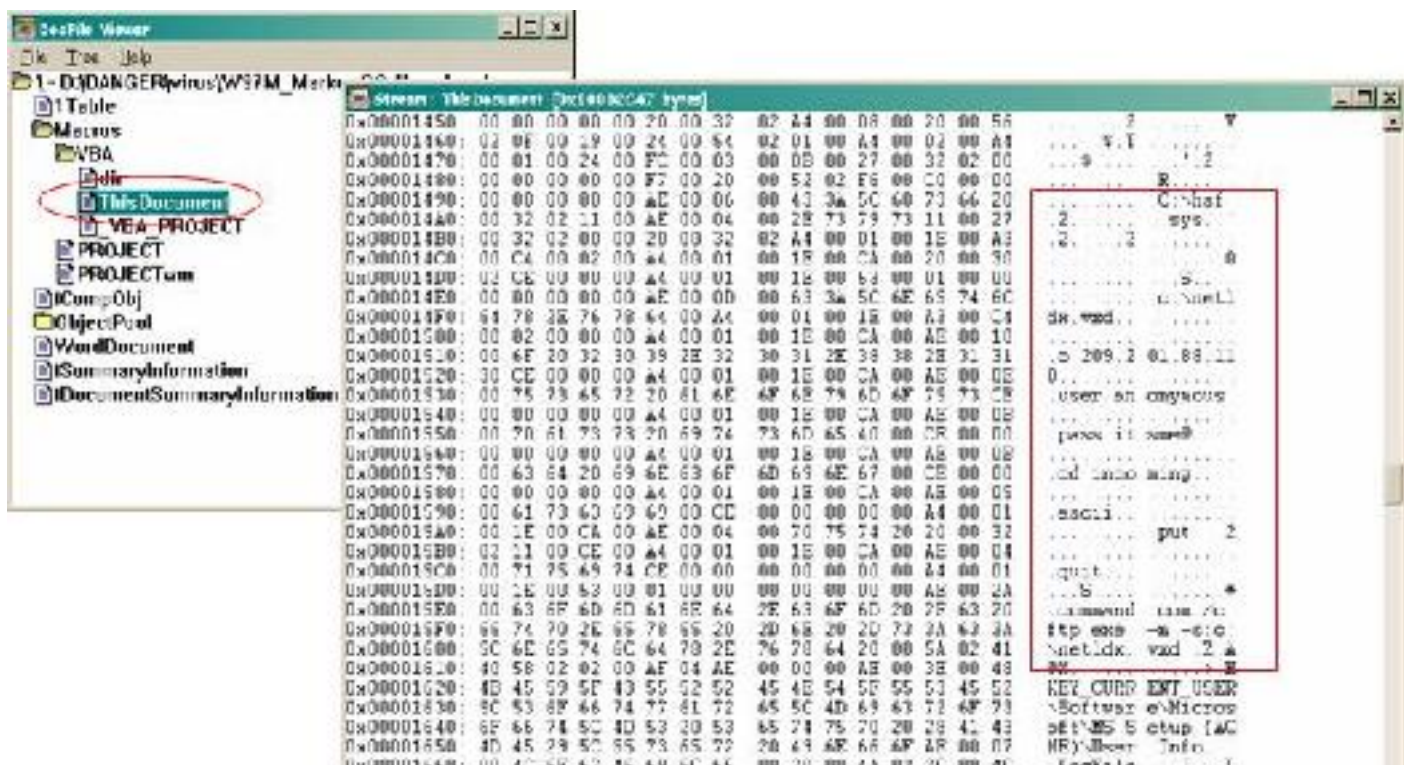
### **Virus macros**

Il lance un contrôle visual basic et lance une session MAPI invisible pour l'utilisateur.

Par exemple, pour Melissa Virus, il utilise le carnet d'adresses d'Outlook pour envoyer les messages et les attachements.



Des variantes macros permettent même au code macro du virus de se cacher via les classes des fichiers word, Excel, Powerpoint.

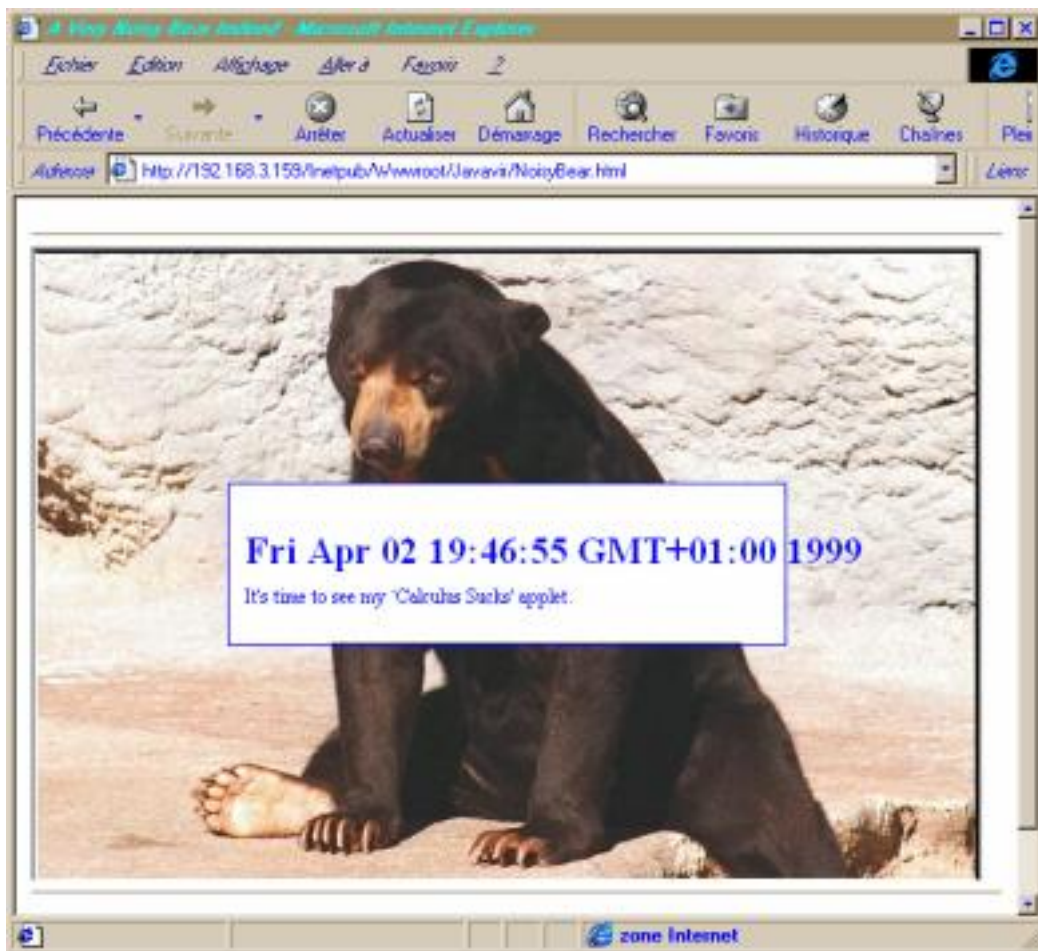


Ils se glissent dans cette zone, qui, théoriquement, est réservée pour les wiziwig, les imprimantes. Pour cette catégories de virus, les éditeurs d'antivirus ont été obligés de modifier leurs moteurs de scan.

### **Virus JAVA**

Les virus JAVA ont été développés pour tester les fonctionnalités.

Nous appelons cela Proof of the Concept. Ce POC a été modifiée pour créer un ver JavaScript.



### **Virus de script**

Les virus de script sont généralement des codes malicieux compagnons.

Deux types de comportement peuvent être constatés:

- S'inclure dans la signature de mail
- Spam ou utilisation d'IRC, MSN, ICQ, Yahoo messenger pour se propager

Leurs langages peuvent être :

- HTML Script
- VBS Script
- JavaScript
- PHP coté serveur
- Virus de Script

Les scripts malicieux VBS&JS utilisant les technologies d'encryption et de polymorphisme (ex:VBS\_KALAMAR).

Ils peuvent être « embedded » (insérés) dans des fichiers html/xml (ex:VBS\_KAKWORM)

Les instructions du script peuvent être très dangereuses pour le système d'exploitation, les applications et les données (ex:VBS\_LOVELETTER)

Les droits du script sont ceux des droits de l'utilisateur (en local ou en réseau)

### **Virus plaisantins dits JOKE**

Les Jokes sont développés dans le but de perturber les compagnies

Ils n'ont pas d'effet destructeur, mais font perdre du temps aux administrateurs

On a tous bien connu le socle coca-cola qui lorsque l'utilisateur exécutait ce code avec un icône coca-cola, cela ouvrait le CDROM, faisant penser à un porte gobelet !!!

Mais des jokes plus pernitéux se sont vus entraînés de grave conséquences, comme une simulation d'un formatage du disque dur...alors qu'en fait, il suffisait de cliquer sur CANCEL !!!



Leurs arrivées : mail, ftp, http, cdrom, clefs usb, etc?



Copyright : Blanchard [Virus Docteur] Marc - 2007-10-08 18:16:45  
Creative Commons Deed

Paternité - Pas d'Utilisation Commerciale - Pas de Modification 2.5

Vous êtes libres :

- \* de reproduire, distribuer et communiquer cette création au public

Selon les conditions suivantes :

Paternité. Vous devez citer le nom de l'auteur original.

Pas d'Utilisation Commerciale. Vous n'avez pas le droit d'utiliser cette création à des fins commerciales.

Pas de Modification. Vous n'avez pas le droit de modifier, de transformer ou d'adapter cette création.

\* A chaque réutilisation ou distribution, vous devez faire apparaître clairement aux autres les conditions contractuelles de mise à disposition de cette création.

\* Chacune de ces conditions peut être levée si vous obtenez l'autorisation du titulaire des droits.

Ce qui précède n'affecte en rien vos droits en tant qu'utilisateur (exceptions au droit d'auteur : copies réservées à l'usage privé du copiste, courtes citations, parodie...)

Ceci est le Résumé Explicatif du Code Juridique (la version intégrale du contrat).

<http://creativecommons.org/licenses/by-nc-nd/2.5/>