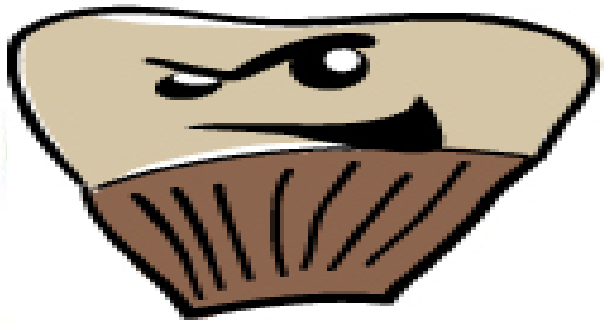
THALES



MUFF'in

Microsoft Unsecured Function Fingerprinter

Aider à la recherche de vulnérabilités via le recherche de propriétés d'exploitations

- Qu'est ce qu'une propriété d'exploitation ?...

- Restriction du champs de recherche.

Les composants de MUFF'in

Grace au Header PE

- Détection du DEP
- Détection de l'ASLR
- Détection du SafeSEH

Par fingerprinting

- Détection du cookie GS
- Detection des Exceptions

Par dataflow (basic)

- Suivis d'arguments

Mais que fait-il d'utile ?

- Recherche de propriétés d'exploitation
- Corrélation des éléments de recherche
- Mise en avant des fonctions présentant des caractéristiques de vulnérabilité

=> Diminution de l'espace de recherche d'une vulnérabilité.

⇒ Diminution du temps de recherche de vulnérabilités.

Demonstration

Vulnérabilité MS08-021 : GDI32.dll

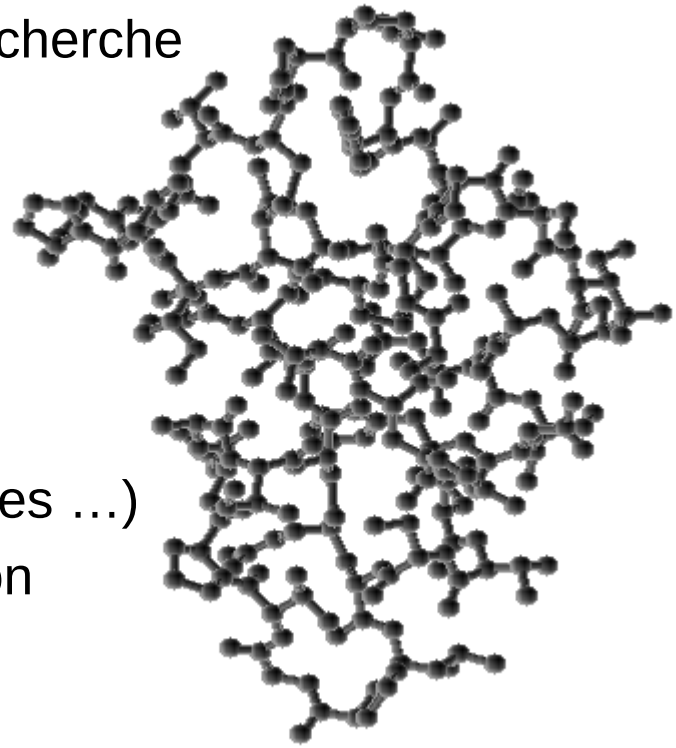
Conclusion

Aujourd'hui MUFF'in …

- … permet de restreindre le champs de recherche
- … aide à l'exploitation

Demain MUFF'in aura…

- … un dataflow plus poussé
- … d'autres éléments de recherche (boucles …)
- … plus de détection de voies d'exploitation



THALES

Des questions ?