Windows 7 avec EMET est plus sécurisé que Windows 10

Microsoft a programmé la fin de vie d'un outil dédié à la sécurité, EMET (Enhanced Mitigation Toolkit), au 31 juillet 2018 (un sursis de 18 mois a été accordé par l'éditeur, la retraite d'EMET était actée pour le 27 janvier 2017). Cette trousse est aujourd'hui présente sur Windows 7 et Windows 8. EMET peut appliquer une douzaine de mesures d'atténuation d'une attaque sur des programmes exécutés sur un PC. Ces mesures sont conçues pour bloquer des techniques souvent utilisées par les malwares comme le ROP (Return Oriented Programmation).

Or sur Windows 10, Microsoft a fait un autre pari sur l'atténuation des attaques, en reprenant des fonctionnalités d'EMET, mais pas la totalité. Les spécialistes de la sécurité et en particulier le CERT de l'Université Carnegie Mellon considèrent comme une erreur la mise au placard d'EMET et que la force de cet outil est son intégration forte avec le système d'exploitation. Pour le CERT académique, Windows 7 avec EMET est parfois plus sécurisé que Windows 10 sans EMET.

Une combinaison gagnante Windows 10 et EMET

A l'appui de ses dires, le CERT américain a dressé un tableau de comparaison (reproduit ci-dessous). Windows 7 tout seul est effectivement bien démuni à protéger des applications sans des mesures d'atténuation. Le niveau se relève en couplant l'OS avec EMET. Le constat est similaire avec Windows 10 qui se défend bien seul, mais ne protège pas complètement contre certaines menaces. Il devient par contre un bouclier plus efficace en l'associant avec EMET. La seule faiblesse est le CFG (Control Flow Guard) une plateforme de sécurité chargée de combattre les corruptions mémoires.

	Win7	Win7 + EMET	Win10	Win10 + EMET
Force System Mitigation				
DEP	Y	Y	Y	Y
SEHOP	Y	Y	Y	Y
ASLR	Y	Y	Y	Y
Pinning	N	Y	N	Y
Fonts	N	N	N	Y
Force Application Mitigation				
DEP	N	Y	Y	Y
SEHOP	N	Y*	Y	Y*
NullPage	N	Y	N	Y
HeapSpray	N	Y	N	Y
EAF	N	Y	N	Y
EAF+	N	Y	N	Y
ASLR	N	Y	Y	Y
BottupASLR	N	Y	Y	Y
LoadLib	N	Y	N	Y
MemProt	N	Y	N	Y
Caller	N	Y*	N	Y*
SimExecFlow	N	Y*	N	Y*
StackPivot	N	Y	N	Y
ASR	N	Y	N	Y
Fonts	N	N	N	Y
CFG	N	N	N	N

* 32-bit processes only

Conséquence de ce comparatif, les spécialistes soulignent « *la combinaison de Windows 10 et EMET est le meilleur compromis* ». Un message martelé par le CERT de Carnegie Mellon qui entend bien voir Microsoft faire machine arrière sur sa volonté d'enterrer EMET. La firme de Redmond pourrait étendre encore la fin du support de la trousse à outils, en sachant que la fin de Windows 7 est attendue en 2020.

A lire aussi :

Windows 10 : Microsoft remplace cmd.exe par PowerShell

Microsoft rouspète face à la faille de Windows 10 dévoilée par Google

Crédit Photo : Olivier le Moal-Shutterstock