Sécurité : des chercheurs demandent à Microsoft de ne pas abandonner EMET

Début novembre, Microsoft annonçait le retrait de son outil de sécurité EMET à la fin de son cycle actuel de vie, soit en juillet 2018. Un outil apprécié dont certains craignent déjà le départ. Des chercheurs demandent ainsi à l'éditeur de renoncer à cette retraite. La sécurité de Windows est probablement l'un des sujets les plus débattus et les plus riches. Avec une part de marché écrasante, le poids pesant sur les épaules de Microsoft est difficilement comparable à celui des autres systèmes. Non qu'il faille plaindre l'entreprise : elle a œuvré dans ce sens. Mais en 2004 et 2005, quand son Windows XP a commencé à crouler sous les attaques, elle a dû changer son fusil d'épaule.

La marche continue (et forcée) de la sécurité sous Windows

L'explosion d'Internet au début des années 2000 a largement simplifié l'exploitation des failles. Il n'était plus vraiment question de circulation de CD ou de DVD, mais d'une activation distante. Ce fut notamment la grande époque des vers Baster et Sasser, qui pouvaient attaquer en quelques minutes n'importe quel Windows XP connecté et qui n'avait pas la mise à jour idoine. À tel point que Microsoft avait pratiquement stoppé le développement de Vista pour se concentrer sur le Service Pack 2 de XP. Depuis, chaque Windows a intégré un nombre croissant de protections. Le SP2 avait par exemple implémenté une version maison du « NX bit », la DEP (Data Execution Prevention). Vista est allé plus loin avec l'un des principaux apports dans ce domaine, l'ASLR (Address space layout randomization), qui permet d'affecter des zones mémoire aléatoires à des composants clés afin que les malwares ne puissent plus les chercher sur cette seule information.

EMET, l'outil d'atténuation des risques

Cependant, et c'est ici qu'EMET (Enhanced Mitigation Experience Toolkit) intervient, il existe une limite à ce que peut faire un système d'exploitation – dans l'état actuel des choses – sans rendre l'utilisation du produit plus « pénible » pour l'utilisateur. C'est la difficile thématique du curseur se déplaçant entre la sécurité et la facilité d'utilisation. EMET est donc un outil proposé depuis longtemps par Microsoft pour

ceux qui veulent renforcer la sécurité, au détriment parfois de la simplicité. Il permet de forcer différents niveaux de protection sur les composants et logiciels, en forçant par exemple ces derniers à utiliser des techniques comme le DEP et l'ASLR, même quand ils n'ont pas été prévus pour. Avec parfois bien sûr un risque de mauvais fonctionnement, mais une barrière plus ou moins forte en cas de faille 0-day contre un élément n'ayant encore aucun correctif.

Microsoft veut arrêter EMET, l'université Carnegie Mellon pointe le danger

Or, Microsoft veut se débarrasser d'EMET. Pourquoi ? Parce que Windows 10 est arrivé entre temps. Dans son billet du 3 novembre, l'éditeur fait la liste des protections intégrées au système et qui n'étaient pas présentes avant, notamment dans Windows 7 qui sert souvent pour les comparaisons. Conscient toutefois de la grogne des utilisateurs d'EMET, la firme avait indiqué que la date initiale d'arrêt, le 27 janvier prochain, avait été repoussée au 31 juillet 2018. Pour les chercheurs de l'université de Carnegie Mellon, ce n'est pas suffisant. Leur CERT (Computer emergency réponse teams) a publié récemment un véritable plaidoyer pour que Microsoft revienne sur sa décision. Pourquoi ? Parce que Windows, même dans sa version 10, sera toujours beaucoup mieux protégé avec EMET que sans. D'ailleurs, dans un tableau qui fait l'inventaire des fonctionnalités, on voit clairement que Windows 7 avec EMET reste bien mieux protégé qu'un Windows 10 classique (mais moins qu'un Windows 10 avec EMET). Les chercheurs accusent Microsoft de mentir quand elle explique que Windows 10 n'a plus besoin d'EMET et que toutes les protections ont été intégrées. Ce qui est vrai pour le « tronc principal », mais l'entreprise omet un point important : la possibilité de forcer ces sécurités pour chaque application. Windows 10 n'offre effectivement par cette capacité, à moins justement qu'on ne lui adjoigne EMET justement.

	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

Le problème des sécurités forcées

Le CERT de l'université tient à faire le distinguo sur l'importance de l'outil. Les chercheurs reconnaissent que Windows 10intègre effectivement de très bons outils de sécurité et autres mesures d'atténuation des risques, mais les logiciels doivent avoir été spécifiquement compilés pour en tirer parti. EMET, à l'inverse, force automatiquement les mesures, au risque de créer parfois une incompatibilité. En prévoyant l'arrêt du support d'EMET pour juillet 2018, Microsoft laisse certes 18 mois supplémentaires aux entreprises pour s'y adapter. Mais les chercheurs pointent le danger inhérent à ce recul : quand le support s'arrêtera, d'autres logiciels de Microsoft, notamment Office 2007, ne seront plus supportés non plus. D'où l'intérêt de continuer à proposer l'outil, qui atténue sérieusement le risque de voir des failles 0-day exploitées.

Certaines mesures peuvent être manuellement appliquées

L'université précise cependant plusieurs points. D'abord, que l'arrêt du support d'EMET ne signifie pas qu'il arrêtera de fonctionner. Il ne sera cependant plus mis à jour, Microsoft ne fournira plus d'aide, et il sera sans doute plus difficile à télécharger. Ensuite, que d'un simple point de vue atténuation des risques, migrer vers Windows 10 est une bonne idée, de même qu'installer EMET tant que c'est possible (et si le besoin s'en faire sentir). Enfin, que certaines actions accomplies par EMET peuvent être réalisées manuellement. C'est notamment le cas de l'activation du DEP et de l'ASLR à l'échelle du système entier. Les chercheurs fournissent la marche à suivre, qui passe par une commande et l'édition du registre. Mais attention, certains logiciels peuvent ne pas être compatibles, auxquels cas ils ne fonctionneront plus. Il n'y aura alors pas de solution miracle : désactiver la protection « fautive » ou se passer du logiciel.

Publiée le 24/11/2016