Failles Meltdown – Spectre : premières attaques massives en vue ?

Du code JavaScript permet de mener des attaques à grande échelle exploitant les failles Meltdown et Spectre des processeurs. Les navigateurs Internet assurent qu'ils sont protégés contre cette menace. Vraiment ?

Selon **AV-TEST**, le nombre de malware exploitant les failles Spectre et Meltdown (touchant de nombreux processeurs) serait en progression rapide : 77 le 17 janvier, 119 le 23 janvier et 139 le 31 janvier.

La plupart de ces exploits sont créés par les spécialistes en sécurité eux-mêmes, afin de mettre machines et systèmes d'exploitation sur le grill. Avec comme objectif de vérifier qu'ils sont bien protégés contre les failles Meltdown et Spectre.

L'apparition d'un démonstrateur en JavaScript fait toutefois craindre l'imminence d'attaques via le Web, alertent certains experts.

Une pagaille monstre, qui profite aux pirates

AV-TEST confirme que tous les grands OS sont touchés : Windows, mais aussi macOS et Linux.

Les concepteurs de processeurs et les éditeurs de système d'exploitation travaillent à des parades, mais dans un désordre général, certains correctifs ayant pu avoir un impact sur la stabilité et les performances des machines.

La présence de code JavaScript adapté aux navigateurs Web les plus courants a également été confirmée par AV-TEST.

Mais les éditeurs se sont montrés plus rapides : Chrome, Edge et Firefox proposent tous aujourd'hui des contre-mesures bloquant les effets de Spectre/Meltdown. Reste le problème de l'application sans délai de ces mises à jour par les DSI en entreprise.

Dans l'intervalle, certains pirates ont profité de cette pagaille pour mener des attaques par phishing. Sous le prétexte de protéger les utilisateurs contre ces failles, ils ont diffusé le malware SmokeLoader.

(Photo credit: kjhosein on VisualHunt / CC BY-NC-SA)

(Rédaction APM)