Prenez l'avantage sur les cybercriminels

En savoir plus

60 % des DSI estiment perdre la bataille contre le cybercrime[1]. Alors comment développer une stratégie de sécurité gagnante ?

C'est souvent au moment où vous pensiez avoir sécurisé toutes les failles pouvant mettre votre réseau en péril qu'une nouvelle cyberattaque se présente. Plus sophistiquées et persistantes que par le passé, elles sont prêtes à impacter votre activité. Dans les faits, l'évolution de ces attaques ne semble connaître aucune interruption, raison pour laquelle 68 % des DSI pensent que les outils dédiés à la sécurité de leurs terminaux ne sont pas taillés pour affronter cette menace[1].

Ce phénomène est apparu plus clairement que jamais en 2018, à l'occasion d'une attaque qui avait pris pour cible le BIOS de plusieurs organisations majeures avec un maliciel désormais connu sous le nom de LoJax[2]. Les attaques contre le BIOS représentent une préoccupation depuis longtemps dans la mesure où il est pratiquement impossible de les détecter, il est extrêmement difficile de les éliminer, et les pirates disposent d'un contrôle presque total du PC infecté.

Et malgré l'éventualité de ce type d'attaque, les entreprises n'en avaient pas encore fait les frais – jusqu'à ce jour.

Si le maliciel LoJax nous a appris quelque chose, c'est bien que le système d'un PC est vulnérable aux attaques dès que vous le démarrez. Les antivirus et autres logiciels tiers ne suffisent pas à protéger votre réseau, notamment s'ils sont dans l'incapacité de surveiller les changements qui se produisent dans le BIOS. Ainsi, plutôt que de vous joindre aux 79 % d'entreprises qui s'en remettent uniquement à un logiciel antivirus[3], il serait dans votre intérêt de développer une stratégie de sécurité alternative. Comment ? La réponse se trouve dans les solutions de sécurité à plusieurs volets, directement intégrées au matériel.

Nous sommes convaincus que chaque décision relative à un PC est une décision de sécurité. C'est la raison pour laquelle nous avons conçu la gamme HP Elite, dotée d'une sécurité de pointe et comprenant des PC, postes de travail et terminaux destinés à la vente au détail. À titre d'exemple, le HP EliteBook x360 avec processeurs Intel® Core™ i7 8e génération en option possède des fonctionnalités de sécurité renforcées par le matériel lui-même. Vous bénéficiez ainsi d'une défense à plusieurs volets qui protège votre entreprise sous tous les angles.

Votre personnel est une cible mobile pour les pirates visuels

Nous proposons également des fonctionnalités de sécurité innovantes, comme HP Sure View Gen2[4], un filtre de confidentialité intégré en option qui vous protège instantanément contre toute tentative de piratage visuel. Découvrez également HP Sure Click[5], qui libère l'utilisateur final de la lourde tâche de distinguer les sites web sûrs des autres. Cet outil permet en effet au PC de créer lui-même une session de navigation isolée, et évite ainsi la propagation d'un éventuel maliciel d'un onglet infecté à un autre.

De même, si une attaque telle que LoJax frappe votre entreprise, vous pourrez continuer à travailler en toute sécurité et confidentialité grâce à la fonctionnalité de sécurité matérielle intégrée à votre PC. En tant que première et unique protection du BIOS capable de s'auto-réparer, HP Sure Start Gen4[6] détecte automatiquement toute attaque de maliciel, même si celui-ci lui est inconnu, et permet la restauration du BIOS.

Mais le renforcement de votre entreprise avec ces dispositifs de pointe peut parfois s'avérer fastidieux. C'est à ce moment que les solutions informatiques comme HP Device as a Service (DaaS)[7] entrent en jeu. HP DaaS simplifie la mise en place du matériel, des accessoires et des services de cycle de vie adéquats pour vos employés, le tout dans une approche flexible adaptée à vos besoins de sécurité.

Consultez notre Cyber-Security Field Manual (Manuel pratique de la cybersécurité) pour savoir comment renforcer la sécurité de votre entreprise et identifier les étapes nécessaires afin de vous protéger contre les cyberattaques.

Sources :

[1] https://www.bromium.com/company/press-releases/majority-cios-believe-they-are-losing-battle-against-cybercrime.html
[2] Recherches menées par ESET : « LoJax: First UEFI rootkit found in the wild, courtesy of the Sednit group », octobre 2018, https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group
[3] ID d'étude Statista 622857, « Small and medium sized enterprises in the U.S by Statista », octobre 2016
[4] L'écran de confidentialité intégré HP Sure View est une fonctionnalité facultative qui doit être configurée lors de l'achat.
[5] HP Sure Click est disponible sur la plupart des PC HP et est compatible avec Microsoft® Internet Explorer, Google Chrome et Chromium™. Parmi les pièces jointes compatibles se trouvent les documents Microsoft Office (Word, Excel, PowerPoint) et les fichiers PDF en lecture seule uniquement, lorsque Microsoft Office ou Adobe Acrobat sont installés.
[6] HP Sure Start Gen4 est disponible sur les produits HP Elite et HP Pro 600 équipés de processeurs AMD ou Intel® 8e génération.
[7] Les plans HP DaaS et/ou les composants inclus peuvent varier selon la région ou en fonction du partenaire de service HP DaaS agréé. Veuillez contacter votre représentant HP local ou votre partenaire DaaS agréé pour plus de détails dans votre région. Les services HP sont régis par les conditions générales d'utilisation HP applicables fournies ou indiquées au client lors de l'achat. Le client peut bénéficier de certains droits supplémentaires conformément aux lois locales applicables, et ces droits ne sont en aucun cas affectés par les conditions générales d'utilisation HP ou la garantie limitée HP fournie avec votre produit HP.

4AA7-5353FRE, avril 2019