Comment Windows 10 Anniversary Update a détourné deux attaques zero day

Les attaques zero day ont la particularité d'exploiter des vulnérabilités non corrigées des éditeurs. Dans ces conditions, les utilisateurs et entreprises ciblées par ce type d'attaques doivent multiplier les couches de protection pour s'en prémunir au mieux. Microsoft y répond notamment avec les solutions Windows Defender Application Guard (une couche de navigation virtualisée pour Edge) et Windows Defender Advanced Threat Protection (ATP, un service Cloud de détection des brèches de sécurité). Mais c'est loin d'être suffisant pour dormir sur ses deux oreilles.

Si les risques d'intrusion et d'exploitation systèmes sont les cauchemars des responsables en sécurité, les attaques zero-day présent également l'occasion pour l'éditeur de Redmond de vérifier la résilience de ses OS et s'assurer de l'efficacité des techniques d'atténuation pour maintenir les cyber-attaquants à distance le temps de corriger les vulnérabilités et déployer les correctifs. Dans ce cadre, les vulnérabilités CVE-2016-7255 et CVE-2016-7256 ont été l'occasion pour Microsoft de mesurer la qualité des couches préventives introduites avec Windows 10 Anniversary Update en août dernier. Corrigées seulement en novembre 2016 (bulletins MS16-135 et MS16-132), ces failles zero day affectant le noyau permettaient une élévation de privilège.

Vérification et sandbox

Notamment exploitée par le groupe de cyber-attaquants Strontium via une campagne de phishing ciblée et combiné à la faille CVE-2016-7855 affectant Adobe Flash, la CVE-2016-7255 vise à acquérir des droits de lecture-écriture en corrompant la structure tagWND.strName du kernel et en utilisant SetWindowTextW pour écrire du contenu dans la mémoire système. Pour limiter l'usage abusif de tagWND.strName, les développeurs OSR (Offensive Security Research) de Windows ont ajouté des vérifications supplémentaires pour des champs de base et de longueur indique l'éditeur dans un blog de Technet. *« Dans nos tests sur Anniversary Update, les exploits utilisant cette méthode pour créer une primitive RW (lecture-écriture, NDLR) dans le noyau sont inefficaces »*, assurent les auteurs du billet. Au pire, les tentatives de prise de contrôle provoquent *« des exceptions et des erreurs d'écran bleu »*. Un moindre mal.

La vulnérabilité CVE-2016-7256 a, pour sa part, été exploitée par un groupe dénommé Hankray qui s'appuyait sur une faille de la bibliothèque de police de Windows pour tenter d'installer une backdoor sur des versions antérieures de Windows, notamment Windows 8. Schématiquement, les polices étaient manipulées avec des adresses et données codées en dur pour refléter les configurations réelles de la mémoire. *« Ceci indique la probabilité qu'un outil secondaire génère dynamiquement le code d'exploitation au moment de l'infiltration »*, note les experts de Microsoft. Un code d'exploitation désormais contenu dans Windows 10 puisque l'analyse des polices ne se déroule plus dans le noyau mais dans AppContainer, un bac à sable (sandbox) isolé qui prévient l'obtention de privilèges et réduit donc les surfaces d'attaques depuis les polices système et autres vecteurs d'exploitation. Selon les tests opérés par les experts de l'équipe de sécurité de Microsoft, en cas de tentative d'attaque, le lecteur Font Viewer renvoie un message d'erreur signifiant que le

fichier analysé n’est pas une police valide.

Des vérifications étendues dans Creators Update

L’équipe d’experts soulignent qu’il s’agit ici de deux exemples précis sur la façon dont Windows 10 peut prévenir les attaques zero day. Et nombre d’autres techniques préventives viennent renforcer l’intégrité de Anniversary Update. Surtout si l’entreprise décide de souscrire au service Windows Defender ATP. Ce qui n’empêchera pas qu’il faudra continuer à scrupuleusement appliquer les correctifs de sécurité même si ces méthodes de vérification depuis Windows Defender ATP seront étendues dans Creators Update, la prochaine évolution notable de Windows 10 attendue en avril prochain.

Lire également
Collecte de données : Windows 10 va réduire la voilure sur la télémétrie
Microsoft résout les soucis réseau de Windows 10
Windows 10 Anniversary Update bon pour le service en entreprise