Veille technologique : Cybersécurité en entreprise

Jules RIQUIER

Dernièrement, l'entreprise sud-coréenne Genian a découvert que les fichiers MSC pouvaient être utilisés à des fins malveillantes. De nouvelles recherches menées par l'équipe d'Elastic ont permis de découvrir une nouvelle technique basée sur l'utilisation de ces fameux fichiers MSC : la technique "GrimResource". L'attaque GrimResource repose sur l'utilisation d'un fichier MSC malveillant qui sert à exploiter une faille de sécurité XSS basée sur le modèle DOM de la bibliothèque nommée "apds.dll". Il s'agit d'une vulnérabilité connue, qui a déjà été reportée à Adobe et Microsoft en 2018, mais qui n'a pas été corrigée. Ainsi, dans Windows 11, avec les dernières mises à jour de sécurité, la faille de sécurité peut être exploitée. Ceci est également vrai pour les autres versions de Windows.

En ajoutant une référence à la ressource APDS vulnérable dans la section StringTable appropriée d'un fichier MSC élaboré, les attaquants peuvent exécuter du JavaScript arbitraire dans le contexte de mmc.exe.", peut-on lire. Grâce à cette technique et à l'exploitation de cette faille de sécurité, les cybercriminels sont parvenus à récupérer et à exécuter un payload Cobalt Strike, afin d'infecter la machine et de la compromettre.

En général, il est conseillé aux administrateurs système de surveiller les points suivants :

-Opérations de fichiers impliquant apds.dll invoqué par mmc.exe.

- Exécutions suspectes via MCC, en particulier les processus lancés par mmc.exe avec des arguments de fichiers .msc.

-Allocations de mémoire RWX par mmc.exe provenant de moteurs de script ou de composants .NET.

-Création inhabituelle d'objets COM .NET au sein d'interprètes de scripts non standard comme JScript ou VBScript.

-Fichiers HTML temporaires créés dans le dossier INetCache à la suite d'une redirection XSS par APDS.

Elastic Security a également publié une liste complète des indicateurs GrimResource sur GitHub et fourni des règles YARA dans le rapport pour aider les défenseurs à détecter les fichiers MSC suspects.

Sources :

https://www.it-connect.fr/grimresource-fichiers-msc-et-faille-xss-non-corrigee-dans-windows/

https://www.bleepingcomputer.com/news/security/new-grimresource-attack-uses-msc-files-and-windows-xss-flaw-to-breach-networks/

https://github.com/elastic/labs-releases/tree/main/indicators/grimresource