DÃ©tecter et attÃ©nuer les attaques impliquant Cobalt Strike
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 7/2/2022 13:00:00

Cobalt Strike est devenu un outil de sÃ©curitÃ© offensive omniprÃ©sent, largement exploitÃ© par les cybercriminels et les groupes APT.

Dirk Schrader, Resident CISO EMEA et VP of Security Research chez Netwrix, aborde la question de la dÃ©tection et de l'attÃ©nuation des attaques impliquant Cobalt Strike :

Â« Afin de se dÃ©fendre contre Cobalt Strike et d'en assurer la dÃ©tection, il faut avant tout savoir que les cybercriminels nâutilisent les fonctionnalitÃ©s de furtivitÃ© et les techniques dâÃ©vasion offertes par cet outil quâaprÃ¨s la premiÃ¨re infection. Cobalt Strike dÃ©crit lui-mÃªme son outil comme un âagent de post-exploitationâ.

La meilleure dÃ©fense, et la plus efficace, contre ce type dâagent consiste Ã rendre lâinfiltration dâune infrastructure aussi difficile que possible pour lâattaquant. Il sâagit dâappliquer les mesures de cyber-hygiÃ¨ne habituelles, de corriger les vulnÃ©rabilitÃ©s, de dÃ©sactiver les comptes inutilisÃ©s, de mettre en place une stratÃ©gie de mots de passe adÃ©quate, voire dâappliquer un modÃ¨le de type âZero-Trustâ.

Bien entendu, tout cela ne garantit pas quâun attaquant ne rÃ©ussira pas Ã pÃ©nÃ©trer dans le rÃ©seau. Dans ce scÃ©nario, il est impÃ©ratif de connaÃ®tre les TTP (tactiques, techniques et procÃ©dures) couramment utilisÃ©es lors des tentatives de dÃ©ploiement de Cobalt Strike.

Lâune des tendances Ã©mergentes consiste Ã adopter une stratÃ©gie dâexploitation des ressources, Ã se servir des outils fournis avec le systÃ¨me dâexploitation, comme lâutilisation de Powershell ou de Command dans les environnements Windows. Câest en surveillant lâexploitation de ces derniers que vous serez en mesure de dÃ©tecter le processus dâinstallation dâune balise Cobalt.

Parmi les autres indicateurs importants Ã surveiller, citons les Ã©vÃ©nements systÃ¨me, comme lâobservateur dâÃ©vÃ©nements de Windows, et les Ã©vÃ©nements tels que lâID 7045, qui signale lâinstallation dâun nouveau service. Les balises Cobalt Strike sâexÃ©cutent souvent sous la forme dâun service, camouflÃ© derriÃ¨re des noms anodins.

La mise en place dâune procÃ©dure de surveillance spÃ©ciale permettant de dÃ©tecter tout changement dans les services installÃ©s, lancÃ©s et en cours dâexÃ©cution sur une machine donnÃ©e contribuera Ã dÃ©tecter un implant Cobalt Strike.

Pour le reste, il convient d'accorder une attention particuliÃ¨re aux communications Commande et ContrÃ´le, câest-Ã -dire aux informations de commande et de contrÃ´le Ã©changÃ©es entre un dispositif infectÃ© et le serveur distant. Cobalt Strike propose de nombreuses fonctions destinÃ©es Ã dÃ©jouer la dÃ©tection, notamment dans cet aspect de sa fonctionnalitÃ©.

Cependant, pour Ã©tablir une communication, des paquets doivent circuler entre les terminaux. Une surveillance approfondie, combinÃ©e Ã des renseignements actualisÃ©s sur les serveurs Commande et ContrÃ´le connus, se rÃ©vÃ©lera Ã©galement utile Ã cet Ã©gard.

De maniÃ¨re gÃ©nÃ©rale, la cyberdÃ©fense consiste Ã compliquer et Ã rendre aussi difficile

que possible la tÃ¢che dâ□□un attaquant qui cherche Ã passer inaperÃ§u, et ce, tout au long du processus dâ□□attaque, et pas seulement au cours dâ□□une seule phase. Â»Â