***Brute Ratel C4 : L'outil prÃ©fÃ©rÃ© des hackers.***
**Internet**
PostÃ© par : JulieM
PubliÃ©e le : 11/7/2022 13:00:00

Selon un rÃ©cent rapport menÃ© par Unit42, des cybercriminels spÃ©cialisÃ©s dans les menaces persistantes avancÃ©es ont adoptÃ© Brute Ratel C4, un outil lÃ©gitime de test d'intrusion. Dirk Schrader, Resident CISO (EMEA) and VP of Security Research chez Netwrix, a fait le commentaire suivant :

Â« Le rÃ©cent rapport d'Unit42 sur un nouvel outil de commande et contrÃ´le (C2) appelÃ© Brute Ratel C4, dÃ©sormais prÃ©fÃ©rÃ© des attaquants Ã  son ennemi connu Cobalt Strike, devrait sonner l'alarme pour les cyber-dÃ©fenseurs.

Et voici pourquoi : cet outil semble Ã©chapper Ã  la dÃ©tection des outils EDR et des antivirus en gÃ©nÃ©ral, car il possÃ¨de des capacitÃ©s intÃ©grÃ©es pour garder les traces, en particulier celles en mÃ©moire cachÃ©es. Ce fait oblige les organisations Ã  vÃ©rifier leur architecture de cybersÃ©curitÃ©.

Comme les capacitÃ©s de dÃ©tection installÃ©es sur les solutions endpoints (EDR et antivirus prÃ©cÃ©demment nommÃ©s) ne sont pas suffisantes pour dÃ©tecter les activitÃ©s de commande et contrÃ´le utilisant le Brute Ratel C4, les Ã©quipes informatiques doivent assurer la sÃ©curitÃ© de l'organisation en concentrant leurs efforts sur les trois principales surfaces d'attaque : les donnÃ©es, les identitÃ©s et l'infrastructure.

Des outils comme Brute Ratel C4 ou Cobalt Strike sont exploitÃ©s par les attaquants pour Ã©tablir un canal de retour vers le centre de contrÃ´le, un canal qui doit Ãªtre pratiquement indÃ©tectable. C'est l'Ã©lÃ©ment clÃ© de leur chaÃ®ne d'attaque.

L'approche de la cyber-dÃ©fense de l'organisation doit viser Ã  briser cette chaÃ®ne tout en restant rÃ©siliente. L'Ã©quipe IT peut amÃ©liorer cette cyber-rÃ©silience en identifiant le type de donnÃ©es prÃ©cieuses stockÃ©es et leur emplacement exact. Cela permettra de concentrer les efforts de sÃ©curitÃ© sur ce qui est rÃ©ellement critique.

Par exemple, si des donnÃ©es sensibles se trouvent ouvertes Ã  un groupe d'utilisateurs jugÃ© trop important, elles devraient Ãªtre mises en quarantaine et portÃ©es Ã  l'attention des responsables IT et sÃ©curitÃ©. Une telle mesure est en revanche excessive pour des donnÃ©es non sensibles et ne fait que dÃ©tourner leur l'attention.

Une autre couche Ã  surveiller est celle des identitÃ©s. Le contrÃ´le des comptes d'utilisateurs et des comptes de services, ainsi que la mise en place d'un gouvernement d'accÃ¨s sont la pierre angulaire de la sÃ©curitÃ© des identitÃ©s.

Les privilÃ¨ges doivent Ãªtre gÃ©rÃ©s avec encore plus de soin : accordÃ©s pour une session spÃ©cifique, ils doivent Ãªtre rÃ©voquÃ©s lorsque cette session prend fin. Une telle approche Ã©limine les privilÃ¨ges permanents en place et rÃ©duit donc la surface d'attaque de l'organisation.

La derniÃ¨re piÃ¨ce de ce puzzle est le maintien de l'intÃ©gritÃ© des systÃ¨mes organisationnels, la dÃ©tection de tout changement survenant dans les actifs et l'infrastructure, de tout fichier abandonnÃ©, d'une bibliothÃ¨que de liens dynamiques (DLL) modifiÃ©e ou d'un changement de

configuration diminuant la  posture de sÃ©curitÃ©. Une dÃ©tection prÃ©coce augmente les chances de prÃ©venir une  compromission rÃ©elle des donnÃ©es. Â»