L'infrastructure du rÃ©seau malveillant Qakbot dÃ©mantelÃ©e

SÃ©curitÃ©

PostÃ© par : JerryG
PubliÃ©e le : 1/9/2023 13:00:00

Le 26 aoÃ»t 2023, une collaboration internationale entre les forces de police et les systÃ¨mes judiciaires des Ã□tats-Unis, de l'Allemagne, des Pays-Bas et de la France a entraÃ®nÃ© le dÃ©mantÃ¨lement de l'infrastructure du rÃ©seau malveillant Qakbot, accompagnÃ© de la saisie de 8,6 millions de dollars en crypto-monnaies.

Dans le cadre de cette opÃ©ration, le FBI a redirigÃ© le flux de trafic vers ses propres serveurs, libÃ©rant ainsi toutes les machines du botnet et neutralisant ses activitÃ©s. Cette action a entraÃ®nÃ© la dÃ©sactivation d'environ cinquante serveurs dans les pays partenaires, suivie de la mise hors service du reste de l'infrastructure.

Selon John Fokker, chef du renseignement sur les menaces du Centre de Recherche AvancÃ©e de Trellix

Â« AprÃ¨s Genesis Market en mai et l'infiltration du ransomware Hive en janvier, lâ□□annÃ©e 2023 est de nouveau marquÃ©e par le dÃ©mantÃ¨lement par le FBI d'un rÃ©seau dâ□□envergure mondiale.

Depuis la premiÃ¨re dÃ©tection de Qakbot en 2007, Ã©galement connu sous les noms de QBot, QuakBot et Pinkslipbot, ce botnet trÃ¨s rÃ©sistant est restÃ© actif, donnant souvent Ã nos chercheurs l'impression de jouer au jeu du chat et de la souris.

Il n'a cessÃ© d'Ã©voluer, d'ajouter de nouvelles fonctionnalitÃ©s et de trouver de nouveaux moyens d'Ã©chapper Ã la dÃ©tection, en contournant toujours la possibilitÃ© dâ□□un dÃ©mantÃ¨lement, jusqu'Ã aujourd'hui. C'est une excellente nouvelle que le FBI et ses partenaires aient pu immobiliser ce botnet jusquâ□□Ã lors trÃ¨s persistant et il est Ã espÃ©rer qu'il restera hors ligne pour de bon.

Le processus de dÃ©mantÃ¨lement n'est pas si simple, comme en tÃ©moigne notre rÃ©cente participation au dÃ©mantÃ¨lement de Genesis Market et aux arrestations de REvil.

La lutte contre la cybercriminalitÃ© exige une bonne dose de dÃ©vouement et une forte collaboration pour dÃ©manteler les infrastructures complexes des ransomwares.

L'augmentation du nombre de dÃ©mantÃ¨lements et d'arrestations montre que les cybercriminels doivent surveiller leurs arriÃ¨res. Les forces de l'ordre et l'industrie recherchent toutes les occasions de perturber les acteurs de la menace, et d'autres dÃ©mantÃ¨lements sont imminents. Â»Â