Les chercheurs d’ESET confirment une augmentation significative du nombre de clients uniques qui ont signalé des tentatives d'attaque par force brute bloquées par la protection d’ESET contre les attaques réseau, et la nouvelle couche de protection d’ESET contre les attaques par force brute. Cette tendance a été observée depuis le début de la pandémie. La situation liée au COVID-19 a radicalement changé la nature du travail quotidien, obligeant les collaborateurs à effectuer une grande partie de leur travail via un accès à distance. Les cybercriminels, en particulier les opérateurs de ransomwares, sont conscients de ce changement et tentent d'exploiter de nouvelles opportunités d'augmenter leurs revenus illicites. Entre janvier et mai 2020, les États-Unis, la Chine, la Russie, l'Allemagne et la France étaient en tête de la liste des pays ayant le plus grand nombre d’adresses IP utilisées dans le cadre d’attaques par force brute.

« Avant le confinement, la plupart des collaborateurs travaillaient dans des bureaux et utilisaient des infrastructures supervisées par leur service informatique. Mais la pandémie de coronavirus a entraîné un changement majeur dans le statu quo. Aujourd'hui, une grande partie du travail de bureau se fait via des appareils personnels, et les collaborateurs accèdent aux systèmes sensibles de l'entreprise via le protocole RDP (accès à distance) de Windows, une solution propriétaire créée par Microsoft pour permettre la connexion au réseau de l'entreprise à partir d'ordinateurs distants, » explique Ondrej Kubovi?, Security Research & Awareness Specialist d’ESET.

« Malgré l'importance croissante de RDP, ainsi que d'autres services d'accès à distance, les entreprises négligent souvent de contrôler ses paramètres et sa protection. Les collaborateurs utilisent des mots de passe faciles à deviner, et sans couches supplémentaires

d'authentification ou de protection, rien n’empêche les cybercriminels de compromettre les systèmes d'une entreprise, » poursuit M. Kubovi?.

Figure 1. Tendance des tentatives d'attaques RDP contre des clients uniques (par jour) détectées par les technologies ESET

Selon la télémétrie d’ESET, la plupart des adresses IP bloquées entre janvier et mai 2020 étaient situées aux États-Unis, en Chine, en Russie, en Allemagne et en France. Les pays ayant la plus grande proportion d’adresses IP ciblées sont la Russie, l'Allemagne, le Japon, le Brésil et la Hongrie.

Figure 2. Pays ayant le plus grand nombre d'adresses IP bloquées (entre le 1er janvier et le 31 mai 2020)

RDP est devenu un vecteur d'attaque populaire durant ces dernières années, en particulier parmi les opérateurs de ransomwares. Ces cybercriminels s'introduisent souvent de force dans un réseau mal sécurisé, élèvent leurs privilèges au niveau administrateur, désactivent ou désinstallent les solutions de sécurité, puis installent des ransomwares pour chiffrer les données cruciales de l'entreprise.

D'autres pirates tentent également d'exploiter des connexions RDP mal sécurisées pour installer des malwares d’extraction de cryptomonnaie ou de création de portes dérobées, qui

peuvent être utilisés au cas où leur accès non autorisé via RDP aurait été identifié et fermé. Pour faire face aux risques croissants que pose l'utilisation de RDP, les chercheurs d’ESET ont conçu une nouvelle couche de détection intégrée à la protection d’ESET contre les attaques réseau, qui est conçue pour bloquer les attaques entrantes par force brute provenant d'adresses IP externes. Elle s’applique aussi bien au protocole RDP qu’au protocole SMB (partage de ressources). Cette nouvelle fonctionnalité a été baptisée ESET Brute-Force Attack Protection.
Pour plus d’informations et de données sur les attaques par force brute, ESET Brute-Force Attack Protection et la configuration adéquate de l’accès à distance, consultez le rapport complet « Remote access at risk: Pandemic pulls more cyber-crooks into the brute-forcing game sur WeLiveSecurity et l’article « More remote access, more brute-force attacks. Is this a new cyberpandemic? » Suivez l’actualité d’ESET Research sur Twitter.