Comment les rançongiciels utilisent les protocoles RDP (Remote Desktop Protocol) non protégés

Quelle est l'étendue du problème ?

768%

d'attaques RDP en plus entre les trimestres 1 et 4 de 2020[1]

47%

des rançongiciels proviennent de pirates tirant parti du protocole RDP en 2020[2]

4.7 millions

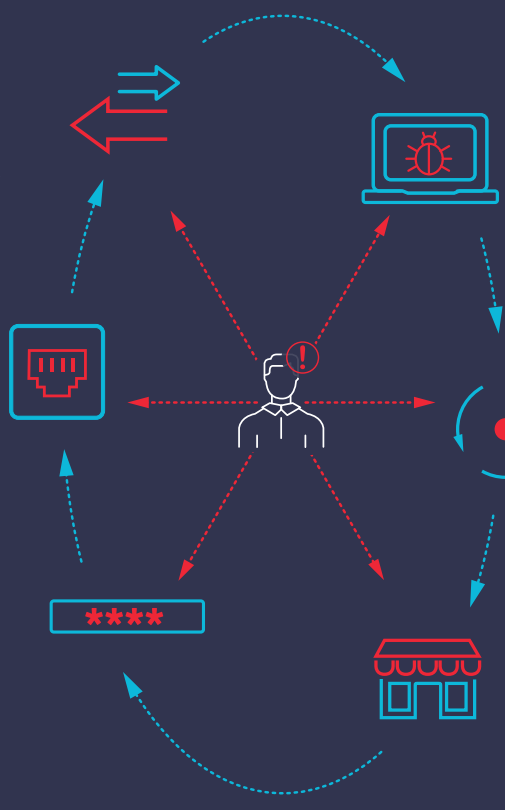
de machines avec RDP mal configurées sont ouvertes sur Internet, selon Coveware[3]

Quelle est la cause principale de ces attaques ?

Le protocole RDP est la technologie la plus populaire pour les connexions aux systèmes à distance

Les ports RDP restent ouverts sur Internet et accessibles à l'aide de mots de passe simples

Les mots de passe compromis aboutissent à des accès non autorisés aux ressources d'entreprise



Des millions d'ordinateurs sont équipés de ports RDP vulnérables

Les protocoles RDP sont utilisés pour différentes activités informatiques malveillantes, y compris les ransomwares

Les criminels peuvent y accéder gratuitement sur des « marchés spécialisés dans les RDP »

Que peut-on faire ?

Évitez de publier des bureaux à distance non protégés sur Internet, protégez le point d'accès grâce à l'authentification multi-facteurs

Utilisez des passerelles RDP : les passerelles de proxy inverse cachent le port

Mettez en place une authentification multi-facteurs pour accéder à la passerelle RDP

Mettez également en place une authentification multi-facteurs pour la connexion au réseau après avoir accédé au bureau à distance

Suivez-nous sur :

THALES
Building a future we can all trust

1 https://www.netsec.news/rdp-attacks-increased-by-768-in-2020-and-remain-a-key-attack-vector
2 https://www.lexology.com/library/detail.aspx?g=30323e3e-7660-4e5e-af70-5d2b8df2ec57
3 https://www.coveware.com/blog/2020/10/14/state-and-local-cybersecurity-defending-our-communities-from-cyber-threats-amid-covid-19