

勒索軟體如何利用未受保護的遠端桌面協定 (RDP)

你知道問題的規模有多大嗎？

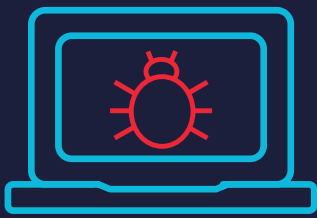


2020 年第一季到第四季，
RDP 攻擊增加了

768%

47%

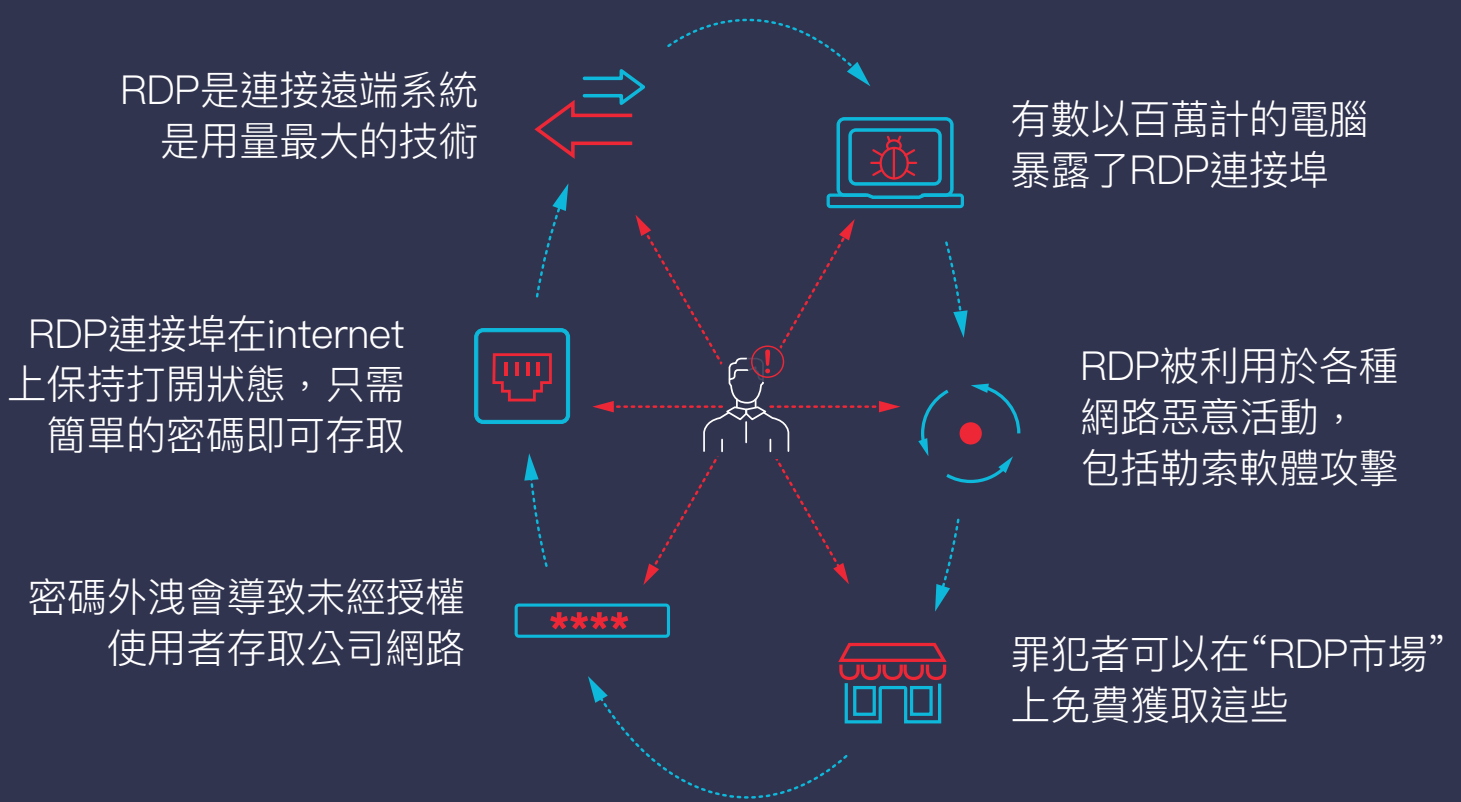
2020年有47%的勒索軟體跟利用
RDP 的威脅行為者有關



4.7 萬

根據 Coveware 的資料顯示，有470萬台配置
錯誤的 RDP 裝置正在移動到互聯網

導致這些攻擊的根本原因是什麼？



對此我們應該做些什麼防範？



避免在 internet 上
發佈未受保護的
遠端桌面，使用
MFA保護存取點



使用 RDP 閘道
– 反向代理閘道
混淆連接埠



採用 MFA 存取
RDP 閘道



使用遠程桌面
應用時也將 MFA
採用於網絡登錄

請關注我們的網站



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>