

How Ransomware uses unprotected Remote Desktop Protocols

What is the scale of the problem?

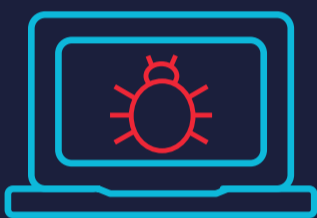


768%

RDP attacks increase between Q1 and Q4 2020¹

47%

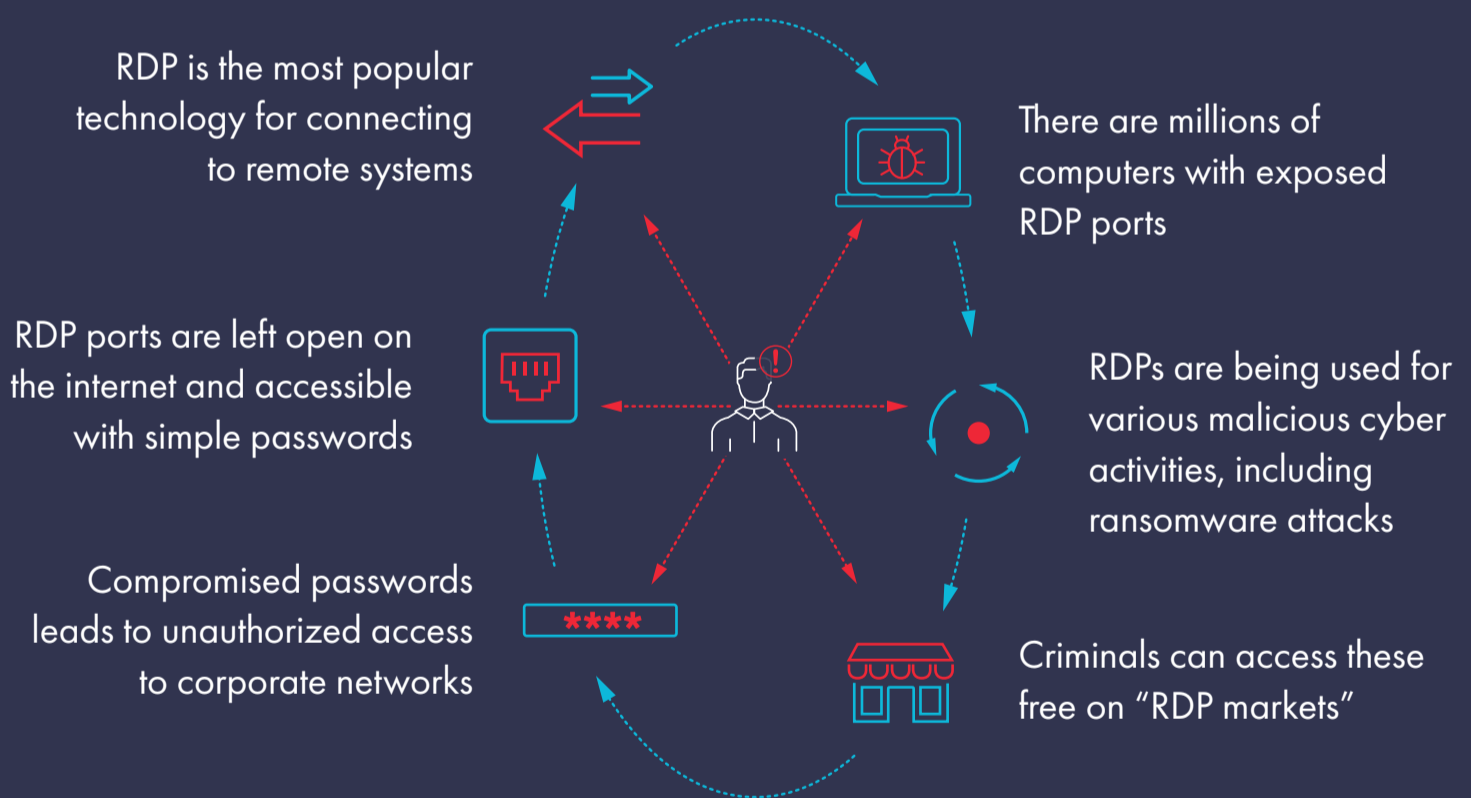
of ransomware involved threats actors leveraging the RDP in 2020²



4.7 million

misconfigured RDP machines open to the Internet according to Coveware³

What is the root cause of these attacks?



What can be done about it?



Avoid publishing unprotected remote desktops on the internet, protect the access point with MFA



Use RDP gateways - reverse proxy gateways obfuscate the port



Apply MFA to access the RDP gateway



Apply MFA to the network logon once inside the remote desktop as well

Follow us on:



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>