How Ransomware uses unprotected Remote Desktop Protocols

What is the scale of the problem?





RDP attacks increase between Q1 and Q4 2020¹





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?

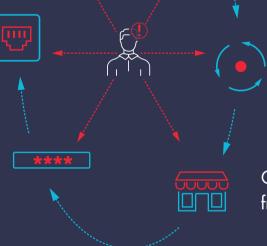
RDP is the most popular technology for connecting to remote systems



There are millions of computers with exposed RDP ports

RDP ports are left open on the internet and accessible with simple passwords

Compromised passwords leads to unauthorized access to corporate networks



RDPs are being used for various malicious cyber activities, including ransomware attacks

Criminals can access these free on "RDP markets"

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 B

Apply MFA to access the RDP gateway



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







 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