Come gli attacchi ransomware sfruttano i Remote Desktop Protocol non protetti

Qual è la portata del problema?

768%

Aumento percentuale degli attacchi RDP tra il T1 e il T4 del 2020[1]

47%

Percentuale di attacchi ransomware in cui gli autori delle minacce hanno sfruttato gli RDP nel 2020[2]

4.7 milioni

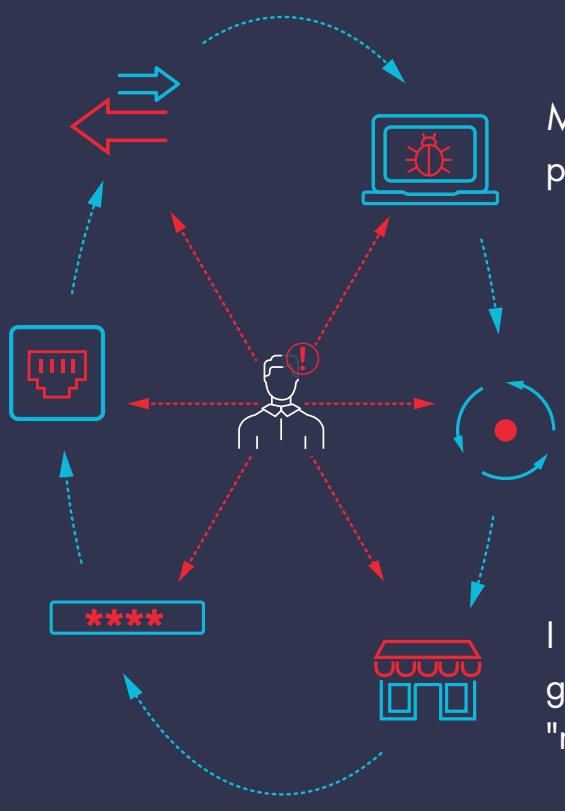
Numero di macchine RDP configurate non correttamente con accesso a Internet secondo Coveware[3]

Qual è la causa alla base di questi attacchi?

Il protocollo RDP è la tecnologia più diffusa per la connessione ai sistemi remoti

Le porte RDP vengono lasciate aperte su Internet e sono accessibili con password semplici

Le password compromesse causano accessi non autorizzati alle reti aziendali



Milioni di computer hanno porte RDP esposte

I protocolli RDP vengono usati per attività informatiche illecite, tra cui gli attacchi ransomware

I criminali possono trovarli gratuitamente nei cosiddetti "mercati RDP"

Cosa si può fare?

Evita di pubblicare desktop remoti non protetti su Internet e proteggi l'access point con la MFA

Usa gateway RDP: i gateway con proxy inverso offuscano la porta

Applica la MFA all'accesso al gateway RDP

Applica la MFA anche all'accesso alla rete una volta all'interno del desktop remoto

Seguici su::

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