La manera como el ransomware utiliza los protocolos de escritorio remoto (RDP) desprotegidos

¿Cuál es la magnitud del problema?

El 768%

de los ataques a los protocolos de escritorio remoto desprotegidos (RDP, por sus siglas en inglés) aumentan entre el primer y el cuarto trimestre de 2020[1]

El 47%

del ransomware involucró actores de amenazas aprovechándose de los protocolos de escritorio remoto desprotegidos (RDP) en 2020[2]

4.7 millones

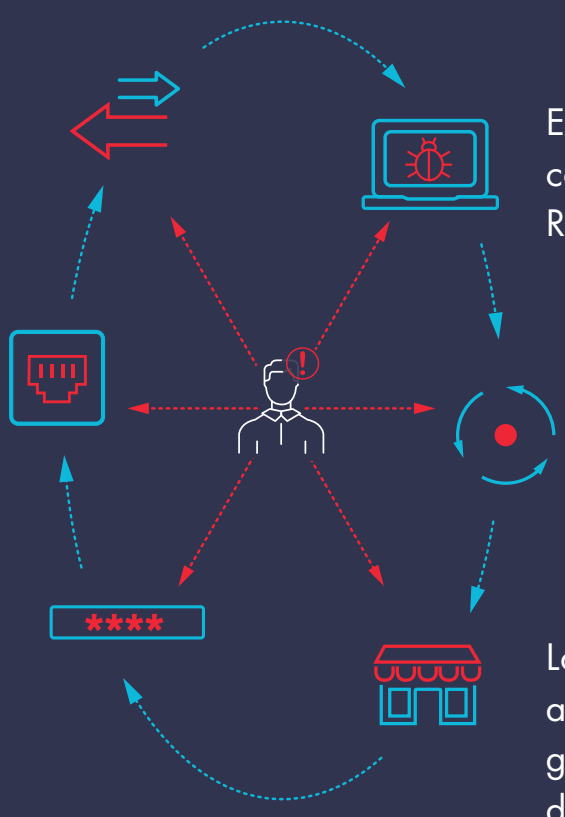
de máquinas con los protocolos de escritorio remoto desprotegidos (RDP) mal configuradas abiertas al Internet de acuerdo con Coveware[3]

¿Cuál es la causa principal de estos ataques?

RDP es la tecnología más popular para conectarse a sistemas remotos

Los puertos RDP se dejan abiertos en el Internet y se puede acceder a ellos con contraseñas simples

Las contraseñas vulneradas llevan al acceso no autorizado en las redes corporativas



Existen millones de computadoras con puertos RDP expuestos

Los RDP se utilizan para diversas actividades cibernéticas maliciosas, que incluyen los ataques de ransomware

Los delincuentes pueden acceder a estos de forma gratuita en los "mercados de RDP"

¿Qué se puede hacer al respecto?

Evite publicar escritorios remotos desprotegidos en Internet, proteja el punto de acceso con MFA

Utilice puertas de enlace RDP - Las puertas de enlace de proxy inverso ofuscan el puerto

Aplique el MFA al acceder a la puerta de enlace RDP

De igual manera, aplique el MFA al inicio de sesión de red una vez dentro del escritorio remoto

Síganos en:

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