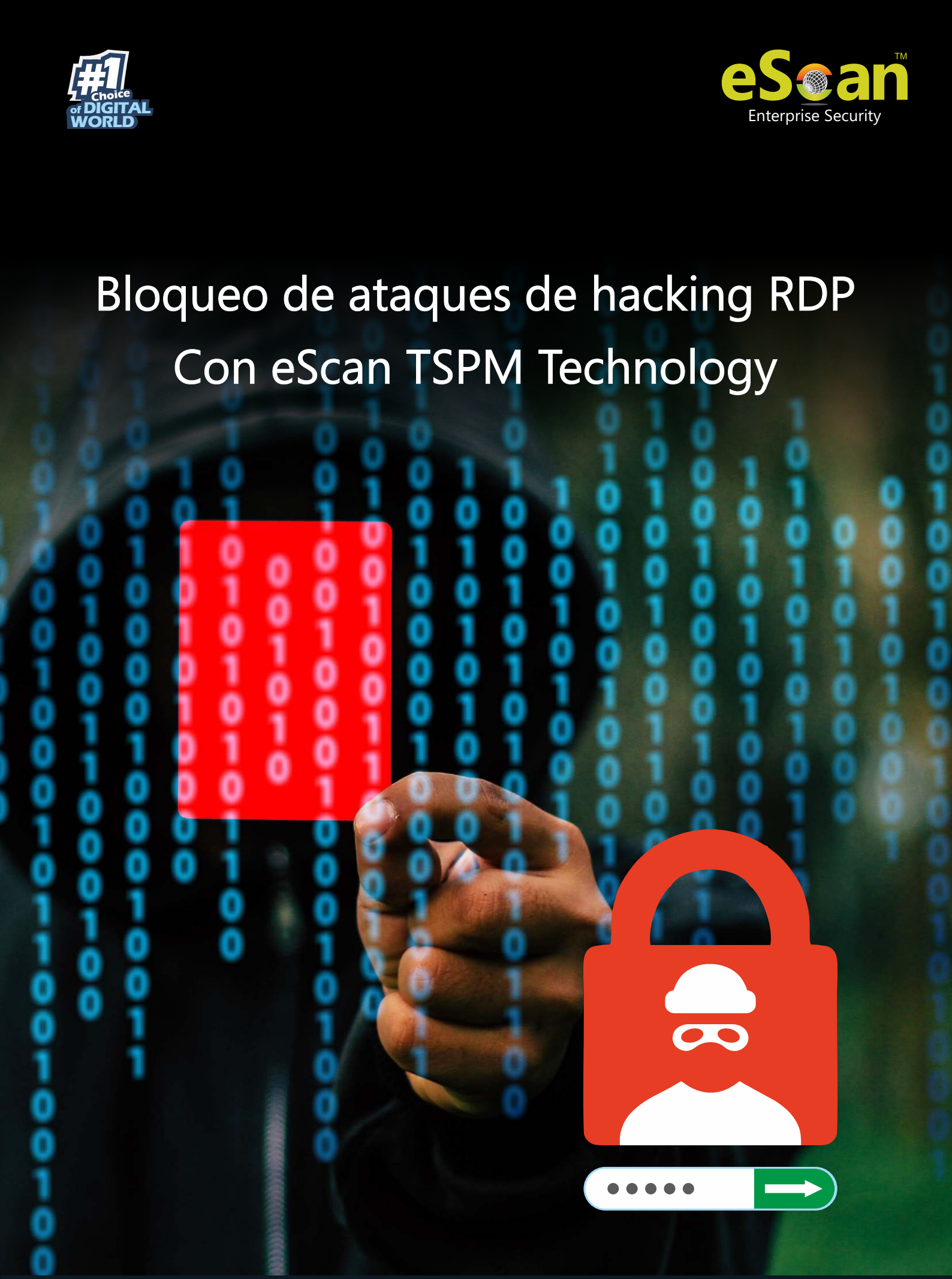
#1 Choice of DIGITAL WORLD

eScan™
Enterprise Security

# Bloqueo de ataques de hacking RDP Con eScan TSPM Technology



# eScan TSPM lanza una nueva tecnología para bloquear ataques de hacking RDP

Con la creciente complejidad de ciber-ataques, las empresas están gastando millones para evitar la ciber-delincuencia. Sin embargo, debido a las malas prácticas de seguridad, como el uso de las contraseñas de acceso al sistema elemental crea oportunidades más vulnerables para los delincuentes cibernéticos. En estos casos los delincuentes cibernéticos utilizan ataques de fuerza bruta para tomar el control de la red. Basado en el "Índice de exposición nacional" por un rápido informe7, el 73% de indios servidores RDP están expuestos a ataques de fuerza bruta, y ocupa el puesto 18 en el índice global.

En los últimos 2 meses, eScan observó que en la mayoría de los ataques podrían ser ransomware contribuyó a los ciberdelincuentes con rogue sesiones RDP para tomar el control de servidores & inyectando ransomware con el fin de extorsionar a los rescates de empresas desprevenidos. La metodología para ello está siendo ejecutado inteligentemente, tomando todas las medidas posibles para pro activamente deshabilitar el control en tiempo real de tecnología y/o desinstalar cualquiera productos antimalware instalado en dichos puntos finales.

La administración de TI y gestión de activos para cada organización es una tarea tediosa, y a fin de simplificar el proceso de resolución de problemas / mantenimiento, Los administradores hacer uso de varias tecnologías de acceso remoto: Remote Desktop Protocol (RDP), así como para acceder a la interfaz gráfica de otro ordenador a través de una conexión de red.

Cabe señalar que la seguridad de RDP se limita a contraseñas fuertes y una conexión segura por medio de la aplicación TLS para mitigar las diversas formas de fuerza bruta / adivinar la contraseña de ataques o ataques MITM.

Debido a diversas razones, no cada organización implementa las directivas de contraseña, y en muchos casos es el usuario quien tiene que elegir su propia contraseña. Además, la reutilización de contraseñas es otra área de preocupación que debe ser encarado.

## Uso de RDP

Para facilitar la gestión centralizada de los ordenadores, las organizaciones implementan la RDP y acceder a estos sistemas, ya sea a través de LAN o Internet. A fin de proteger los sistemas habilitado RDP de forasteros, VPN puede ser implementado, pero en la mayoría de los casos, los administradores pueden configurar el firewall para abrir RDP para los sistemas que desea administrar de manera remota.

## Ataques de RDP

Pen-testing plataformas tales como Kali ofrecen Bruteforce RDP y explotar las herramientas que se utilizan específicamente para sistemas de focalización con Internet hacia sistemas de RDP. Ataque de fuerza bruta podría generar un gran número de notificaciones de inicio de sesión fallido y se registran. Además, los usuarios ni siquiera son conscientes del continuo ataque de fuerza bruta, ya que no es imprescindible que el ataque podría tener lugar cuando el usuario debería estar conectado y funcionando en el sistema.

- Error autenticaciones RDP aunque sean sometidas a auditorías de registro, pero nunca se alertó a los usuarios siempre tienen éxito en la violación de la seguridad. Esto ha redundado en el aumento de la fuerza bruta de las sesiones RDP.
- Debido al hecho de que los usuarios nunca fueron conscientes de la RDP autenticaciones, los autores en todos los casos fueron capaces de obtener el control total del sistema.
- Los atacantes tras la exitosa explotación permitiría aplicar los backdoors o pivote a otros sistemas y, en algunos casos, infectar los sistemas con ransomware.

## TSPM - Módulo de protección de Servicios de Terminal Server

El módulo de protección de eScan de Servicios de Terminal Server (TSPM) no sólo detecta los intentos de fuerza bruta, pero también identifica heurísticamente Direcciones IP / Hosts sospechosos y bloquea los intentos de acceso desde ellos y para salvaguardar los sistemas de futuros ataques, las direcciones IP y hosts de futuros ataques tienen prohibido iniciar cualquier otras conexiones con el sistema.

Como se ha mencionado anteriormente, se ha sabido que los atacantes intenta desinstalar las aplicaciones de seguridad de sistemas comprometidos, a fin de encubrir sus pistas y dejar que los administradores obtengan alertó sobre la violación. EScan TSPM detecta y detiene estos intentos demasiado, además los administradores son también alertó acerca de las medidas preventivas iniciadas por TSPM.

En el panorama actual, donde los atacantes están intentando aprovechar cada debilidad reconocida sea sistemas sin parches o la incapacidad de los usuarios / administradores para mantener la higiene, la contraseña del eScan TSPM protegería los sistemas/organizaciones de tales ataques.