Microsoft está tomando medidas para prevenir los ataques de fuerza bruta del Protocolo de Escritorio Remoto (RDP) como parte de las últimas compilaciones del sistema operativo Windows 11, en un intento por elevar la línea de base de seguridad para enfrentar el panorama de amenazas en evolución.

Con ese fin, la política predeterminada para las compilaciones de Windows 11, particularmente, las compilaciones de Insider Preview 22528.1000 y posteriores, bloqueará de forma automática las cuentas durante 10 minutos después de 10 intentos de inicio de sesión no válidos.

> *«Las compilaciones de Win11 ahora tienen una política de bloqueo de cuenta POR DEFECTO para mitigar RDP y otros vectores de contraseñas de fuerza bruta. Esta técnica se utiliza muy comúnmente en ransomware operado por humanos y otros ataques. ¡Este control hará que la fuerza bruta sea mucho más difícil, lo cual es increíble!»,* dijo David Weston, vicepresidente de seguridad y empresa del sistema operativo de Microsoft.

Cabe mencionar que, aunque esta configuración de bloqueo de cuenta ya está incorporada en Windows 10, no está habilitada de forma predeterminada.

También se espera que la función, que sigue a la decisión de la compañía de reanudar el bloqueo de macros de la aplicación Visual Basic (VBA) para documentos de Office, se adapte a versiones anteriores de Windows y Windows Server.

Aparte de las macros maliciosas, el acceso RDP por fuerza bruta fue durante mucho tiempo uno de los métodos más populares utilizados por los atacantes para obtener acceso no autorizado a los sistemas Windows.

Se sabe que LockBit, que es uno de los grupos de ransomware más activos de 2022, por lo general confía en RDP para el punto de apoyo inicial y las actividades de seguimiento. Otras familias vistas usando el mismo mecanismo incluyen Conti, Hive, PYSA, Crysis, SamSam y

Dharma.

Al implementar este nuevo umbral, el objetivo es disminuir de forma significativa la efectividad del vector de ataque RDP y prevenir las intrusiones que se basan en la adivinación de contraseñas y las credenciales comprometidas.

> *«El RDP de fuerza bruta es el método más común usado por los atacantes que intentan acceder a los sistemas de Windows y ejecutar malware»,* dijo Zscaler el año pasado.

> *«Los actores de amenazas buscan puertos RDP abiertos públicamente para realizar ataques distribuidos de fuerza bruta. Los sistemas que usan credenciales débiles con objetivos fáciles y, una vez comprometidos, los atacantes venden el acceso a los sistemas pirateados en la web oscura a otros ciberdelincuentes».*

Microsoft, en su documentación, advierte sobre posibles ataques de denegación de servicio (DoS) que podrían orquestarse al abusar de la configuración de la política de umbral de bloqueo de la cuenta.

> *«Un usuario malintencionado podría intentar mediante programación una serie de ataques de contraseña contra todos los usuarios de la organización. Si el número de intentos es mayor que el valor del Umbral de bloqueo de la cuenta, el atacante podría potencialmente bloquear todas las cuentas»,* dijo la empresa.