El Protocolo de Escritorio Remoto, objetivo de los ataques de fuerza bruta

La pandemia de COVID-19 obligó a realizar gran parte del trabajo de forma remota. Conscientes del cambio de escenario, los ciberdelincuentes -sobre todo los operadores de ransomware- intentan explotar las nuevas condiciones para aumentar sus ganancias. Los datos que aporta la telemetría de ESET, compañía líder en detección proactiva de amenazas, confirman el aumento del número de usuarios que sufrieron intentos de ataque de fuerza bruta, los mismos fueron detectados y bloqueados mediante la tecnología para la identificación de ataques de red de ESET.

Hoy en día, un porcentaje importante del trabajo se realiza a través de dispositivos hogareños para acceder a sistemas confidenciales de las empresas, por ejemplo, a través del Protocolo de Escritorio Remoto (RDP, por sus siglas en inglés) de Windows, que permite la conexión a la red corporativa desde computadoras remotas. Pese a la creciente importancia de los servicios de acceso remoto, las organizaciones suelen descuidar su correcta configuración y protección, los colaboradores usan contraseñas fáciles de adivinar y no hacen uso de capas adicionales de autenticación o protección.

Los cibercriminales suelen llevar a cabo ataques de fuerza bruta dirigidos a redes con protección deficiente, elevar sus permisos a nivel de administrador, y luego deshabilitar o desinstalar soluciones de seguridad para finalmente ejecutar programas maliciosos, tal es el caso del ransomware, que cifra y secuestra datos son cruciales para las víctimas.

Según datos de la telemetría de ESET, hay un notorio incremento en el número de intentos de ataques vía RDP.

Para tratar los riesgos asociados al aumento en el uso de RDP, los investigadores de ESET idearon una nueva capa de detección, llamada ESET Brute-Force Attack Protection, que está oculta dentro del motor de ESET Network Attack Protection y detecta grupos de intentos fallidos de inicio de sesión desde entornos externos, que sugieren un ataque de fuerza bruta entrante, y luego bloquea más intentos. Posteriormente, las direcciones IP correspondientes a los intentos de ataque se agregan a una lista que protege a millones de otros dispositivos de futuros ataques.

Con base en la telemetría de ESET, la mayoría de las IP bloqueadas entre enero y mayo de 2020 se detectaron en Estados Unidos, China, Rusia, Alemania y Francia.

Incluso con medidas de protección como ESET Brute-Force Attack Protection, las organizaciones deben mantener su acceso remoto configurado correctamente. Para ello, los especialistas de ESET comparten las siguientes recomendaciones:

 Deshabilitar los servicios RDP expuestos a Internet; si esto no es posible, minimizar la cantidad de usuarios que pueden conectarse directamente a los servidores de la organización a través de Internet.

 Establecer como requisito contraseñas complejas y extensas para todas las cuentas que pueden iniciar sesión a través de RDP.

 Usar una capa adicional de autenticación (MFA/2FA).

 Instalar una puerta de enlace de red privada virtual (VPN) como intermediaria para todas las conexiones RDP desde fuera de la red local.

 En el firewall perimetral, deshabilitar conexiones externas a máquinas locales en el puerto 3389 (TCP/UDP) o cualquier otro puerto utilizado por el protocolo RDP.

 Proteger mediante contraseñas el software de seguridad contra posibles alteraciones en su configuración o desinstalación.

 Aislar cualquier computadora insegura u obsoleta a la que se deba acceder desde Internet utilizando RDP y reemplazarla en caso de que sea innecesario su uso de forma remota.