

المهاجمون يواصلون استغلال ثغرات تغطية المصادقة متعددة العوامل في الوصول عبر VPN و RDP



تسلط حوادث الفدية الأخيرة الضوء على استغلال المهاجمين لثغرات المصادقة حيث تحمي المصادقة متعددة العوامل التطبيقات السحابية بينما يبقى الوصول عبر VPN و RDP وتسجيل دخول Windows محميًا بكلمة المرور فقط.

- شكلت بيانات الاعتماد المخترقة نقطة الوصول الأولي في 21% من حوادث الفدية المحققة في 2025، عادةً عبر RDP أو VPN
- استُخدم RDP مع حسابات مخترقة للتنقل الجانبي في حوالي 85% من تحقيقات الفدية
- تفرض المؤسسات غالبًا المصادقة متعددة العوامل للتطبيقات السحابية بينما تترك VPN و RDP وتسجيل دخول Windows محمية بكلمات المرور فقط
- تظل بيانات الاعتماد المسروقة فعالة عندما تقبل مسارات المصادقة كلمات المرور دون تحقق إضافي

- يمكن الذكاء الاصطناعي المهاجمين من تنفيذ هجمات قائمة على بيانات الاعتماد بسرعة ونطاق أكبر

مشكلة تغطية المصادقة

أظهرت حادثة فدية حديثة في أغسطس 2026 ثغرة مستمرة في استراتيجيات المصادقة المؤسسية. نجح مهاجم في الوصول إلى شبكة مؤسسية عبر حساب SonicWall SSL VPN يفتقر إلى **المصادقة متعددة العوامل**، رغم أن المؤسسة تفرض هذه المصادقة للتطبيقات السحابية. في غضون ساعتين تقريباً من الوصول الأولي، وصل المهاجم إلى وحدة التحكم بالنطاق عبر RDP وبدأ في تعداد Active Directory.

يعكس هذا النمط مشكلة أوسع حيث تطبق المؤسسات مصادقة قوية لمنصات SaaS المواجهة للإنترنت ومايكروسوفت 365 بينما تترك مسارات الوصول الحرجة مثل VPN و RDP وتسجيل دخول Windows محمية بكلمات المرور فقط. يخلق هذا النهج المجزأ ثغرات قابلة للاستغلال يستهدفها الجهات المهددة بشكل روتيني.

سرقة بيانات الاعتماد تبقى ناقل الهجوم الأساسي

تكشف التحقيقات في حوادث الفدية عن الفعالية المستمرة لبيانات الاعتماد المخترقة كوسيلة للوصول الأولي. وفقاً لأبحاث Mandiant، شكلت بيانات الاعتماد الشرعية المخترقة نقطة الدخول في 21 بالمائة من حالات الفدية في 2025 حيث أمكن تحديد الوصول الأولي، بشكل رئيسي عبر قنوات RDP أو VPN.

يمتد التهديد إلى ما بعد الوصول الأولي. ظهرت جلسات RDP باستخدام حسابات مخترقة أو منشأة حديثاً في أنشطة التنقل الجانبي في حوالي 85 بالمائة من حوادث الفدية المحققة. يضم الذكاء الاصطناعي هذا الخطر بتمكين المهاجمين من إجراء عمليات قائمة على بيانات الاعتماد بسرعة ونطاق متزايدين، رغم أن تكتيكات اختراق الهوية الأساسية تبقى دون تغيير إلى حد كبير.

معالجة الثغرة

يشير تقرير Verizon لتحقيقات اختراق البيانات إلى تورط بيانات الاعتماد المسروقة في 44.7 بالمائة من الاختراقات. بالنسبة للمؤسسات الخاضعة للتنظيم، السؤال الحاسم ليس ما إذا كانت المصادقة متعددة العوامل موجودة بل أين تستمر المصادقة بكلمة المرور فقط. يمثل تسجيل دخول Windows وجلسات RDP والوصول عبر VPN والخدمات القديمة المدعومة بـ Active Directory ثغرات تغطية شائعة تستدعي مراجعة منهجية.

يساعد توسيع حماية المصادقة متعددة العوامل لتشمل مسارات الوصول هذه في البيئات المحلية والهجينة، إلى جانب التدقيق المنتظم لكلمات المرور لتحديد الضعيفة أو المخترقة سابقاً، في تقليل فائدة كلمات المرور المسروقة قبل استغلالها.

ما يجب فعله الآن

1. إجراء تدقيق لتغطية المصادقة لتحديد جميع مسارات الوصول (VPN و RDP وتسجيل دخول Windows والخدمات القديمة) التي تقبل حالياً كلمات المرور دون المصادقة متعددة العوامل
2. توسيع فرض المصادقة متعددة العوامل لتشمل بوابات VPN وجلسات RDP ومصادقة Windows، وليس فقط التطبيقات السحابية ومنصات SaaS

3. تنفيذ تدقيق منتظم لكلمات مرور Active Directory لتحديد بيانات الاعتماد الضعيفة أو المعاد استخدامها أو المخترقة سابقاً
4. مراجعة ضوابط الوصول والتسجيل لـ RDP للكشف عن أنماط التنقل الجانبي باستخدام حسابات مخترقة
5. دمج أحداث المصادقة من نقاط الوصول المحلية والهجينة في منصات SIEM للمراقبة المركزية
6. وضع سياسة تتطلب المصادقة متعددة العوامل لجميع الحسابات المميزة وطرق الوصول عن بُعد، موثقة وفقاً لمتطلبات الضوابط الأساسية للأمن السيبراني من الهيئة الوطنية للأمن السيبراني وإطار الأمن السيبراني من مؤسسة النقد العربي السعودي