

CISA وشركاؤها: برنامج الفدية SafePay اخترق أكثر من 600 جهة في قطاعات البنية التحتية الحيوية



أفادت CISA وجهات شريكة بأن SafePay أصاب 600 جهة على الأقل في قطاعات البنية التحتية الحيوية منذ أغسطس 2024، عبر بيانات اعتماد مكشوفة وهجمات تخمين وأجهزة حافة غير محدّثة.

- أصاب SafePay ما لا يقل عن 600 جهة في قطاعات حيوية متعددة منذ أغسطس 2024.
- يحصل المهاجمون على الوصول الأولي عبر بيانات اعتماد مكشوفة وتخمين كلمات المرور والوصول عبر VPN وحسابات مصيدة التصيد وثغرات أجهزة الحافة.
- قد يهدف المهاجمون النسخ الاحتياطية الظلية (shadow copies) ويعيدون ضبط أجهزة التخزين المتصلة بالشبكة التي تحوي النسخ الاحتياطية لتعطيل التعافي.
- تعتمد المجموعة الابتزاز المزدوج وتعمل بشكل خاص دون شركاء تابعين.
- تتضمن النشرة المشتركة مؤشرات اختراق (IOCs) وأساليب وتقنيات (TTPs)، وتحذّر من أن دفع الفدية لا يضمن استعادة الملفات.

نشرت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية (CISA)، بالتعاون مع مكتب التحقيقات الفيدرالي والخدمة السرية الأمريكية وشرطة ولاية راينلاند-بفالتس الألمانية (Landeskriminalamt Rheinland-Pfalz) وجهات إنفاذ القانون البريطانية، نشرة مشتركة عن مجموعة برامج الفدية **SafePay**. وتفيد النشرة بأن المجموعة أصابت ما لا يقل عن 600 جهة في قطاعات بنية تحتية حيوية متعددة منذ أغسطس 2024، مع ضحايا في أمريكا الشمالية والجنوبية وأوروبا وأستراليا.

كيف تتم الهجمات

تذكر النشرة عدة طرق للوصول الأولي: بيانات اعتماد مكشوفة، وهجمات تخمين كلمات المرور، والوصول عبر VPN، وحسابات استُدرج أصحابها بالتصيد، والاستغلال الآلي للثغرات معروفة في أجهزة الحافة والأنظمة المكشوفة على الإنترنت. وبعد الدخول قد يهدف المهاجمون النسخ الظلية (shadow copies) ويعيدون ضبط أجهزة التخزين المتصلة بالشبكة التي تحتوي النسخ الاحتياطية، مما يعقد التعافي. كما تسرق المجموعة وثائق حساسة قبل التشفير وتهدد بنشرها إن لم تُدفع الفدية.

ظهرت المجموعة في أغسطس 2024 وتعمل بشكل خاص دون شركاء تابعين. ولا يعرض موقع التسريب الخاص بها إلا الضحايا الذين لم يدفعوا، لذا فإن العدد الفعلي للضحايا أعلى من المعلن.

ما توصي به الجهات

تنصح الجهات بتقييد الأدوات والصلاحيات الإدارية للحد من الحركة الجانبية، وتطبيق المصادقة متعددة العوامل وسياسات إدارة الهوية وبيانات الاعتماد والوصول، وإعطاء أولوية لتحديث شبكات VPN وجدران الحماية وأجهزة الحافة الأخرى المدرجة في كتالوج CISA للثغرات المستغلة فعليًا. وتضيف أن دفع الفدية لا يضمن استعادة الملفات، وتشجع الضحايا على إبلاغ جهات إنفاذ القانون. وتتضمن النشرة مؤشرات اختراق وأساليب وتقنيات مستخلصة من تحقيقات في نشاط امتد من نوفمبر 2024 إلى أغسطس 2026.

ولا يذكر المصدر نشاطًا محددًا في المملكة أو الخليج، لكن أساليب الوصول الموصوفة تنطبق على أي جهة لديها وصول عن بُعد مكشوف.

ما يجب فعله الآن

1. مراجعة أجهزة VPN وجدران الحماية والأجهزة الأخرى المكشوفة على الإنترنت، وإعطاء أولوية لتحديث ما ورد منها في كتالوج CISA للثغرات المستغلة فعليًا.
2. فرض المصادقة متعددة العوامل على الوصول عن بُعد والحسابات ذات الصلاحيات العالية، وفحص سجلات VPN بحثًا عن بيانات اعتماد مكشوفة أو محاولات تخمين.
3. تقييد الأدوات والصلاحيات الإدارية للحد من الحركة الجانبية بعد أي اختراق.
4. حماية النسخ الاحتياطية بالاحتفاظ بنسخ غير متصلة أو غير قابلة للتعديل، وتقييد الوصول إلى أجهزة التخزين المتصلة بالشبكة، ومراقبة حذف النسخ الظلية.
5. إدخال مؤشرات الاختراق والأساليب الواردة في النشرة ضمن أدوات الكشف وإجراء عمليات بحث استباقي.
6. تحديث خطة الاستجابة لحوادث الفدية بما يشمل الإبلاغ للهيئة الوطنية للأمن السيبراني والجهات المختصة الأخرى.