

تحذير CISA بشأن برنامج الفدية SafePay: ما الذي ينبغي أن تراجعهُ المؤسسات المنظمة



نشرت CISA تحذيراً ضمن حملة #StopRansomware عن مجموعة SafePay النشطة منذ أغسطس 2024 ضد الشركات والبنى التحتية الحيوية. يوضح التحذير أساليب الدخول والانتشار والتشفير، ويحث المؤسسات على تطبيق الإجراءات الوقائية الموصى بها.

- تنشط SafePay بدرجة عالية منذ أغسطس 2024، وتستهدف شركات وبنى تحتية حيوية في أمريكا الشمالية والجنوبية وأوروبا وأستراليا.
- يتم الوصول الأولي عبر كلمات مرور مسروقة أو مخفنة، أو استغلال ثغرات في أنظمة الحماية، أو التصيد.
- ينشئ المهاجمون حسابات جديدة أو يستولون على حسابات قائمة، ويستخدمون أدوات النظام المشروعة للتنقل، ويعطلون وسائل الحماية.
- تُشفّر الملفات وتترك رسالة فدية تطلب الدفع بالعملات المشفرة.

أصدرت CISA تحذيراً ضمن حملة #StopRansomware يصف نشاطاً حديثاً لمجموعة برنامج الفدية SafePay. وبحسب التحذير، تنشط المجموعة بدرجة عالية منذ أغسطس 2024، واستهدفت شركات وبنى تحتية حيوية في أمريكا الشمالية والجنوبية وأوروبا وأستراليا. ولا يشير المصدر إلى استهداف داخل المملكة، غير أن الأساليب الموصوفة شائعة في بيئات كثيرة.

كيف تتم الهجمات

يدخل المهاجمون عادةً إلى الشبكة عبر سرقة كلمات المرور أو تخمينها، أو استغلال ثغرات في أنظمة الحماية، أو التصيد. وبعد الدخول يثبتون سيطرتهم بإنشاء حسابات جديدة أو الاستيلاء على حسابات قائمة، ثم يستخدمون أدوات النظام المشروعة للتنقل داخل الشبكة وتحديد الملفات ذات القيمة وتعطيل وسائل الحماية لتفادي الكشف. وفي المرحلة الأخيرة تُسَقَّر ملفات الضحية، وتُترك رسالة تطلب فدية بالعملة المشفرة.

الثغرات المشار إليها

يُدرج قسم المنتجات المتأثرة في التحذير الثغرة CVE-2020-3259 (كشف معلومات حساسة لجهة غير مصرح لها) والثغرة CVE-2023-20269، وغيرهما. والقائمة الكاملة في منشور CISA، وينبغي مطابقتها مع سجل أصولكم.

أهمية الأمر

لا تعتمد طرق الدخول على أساليب غريبة، بل على بيانات الدخول والمنتجات الأمنية غير المحدثة والتصيد. ويمكن للمؤسسات تقليل التعرض بمراجعة هذه الأساسيات، والتأكد من مراقبة إنشاء الحسابات وتغيير إعدادات أدوات الحماية. وتحث CISA المؤسسات على تطبيق إجراءات التخفيف الواردة في التحذير.

ما يجب فعله الآن

1. قارنوا الثغرات المذكورة في تحذير CISA بسجل الأصول والمنتجات لديكم، وأعطوا أولوية لمعالجة ما ينطبق منها.
2. راجعوا سياسات كلمات المرور وفعلوا المصادقة متعددة العوامل، خصوصاً للوصول عن بُعد والحسابات ذات الامتيازات.
3. فعّلوا التنبيه عند إنشاء حسابات جديدة أو تعديل الحسابات ذات الامتيازات.
4. راقبوا أي تعطيل أو تلاعب بأدوات الحماية، والاستخدام غير المعتاد لأدوات الإدارة المشروعة.
5. عزّزوا الوعي بالتصيد، واختبروا قابلية استعادة النسخ الاحتياطية غير المتصلة وخطة الاستجابة لبرامج الفدية.