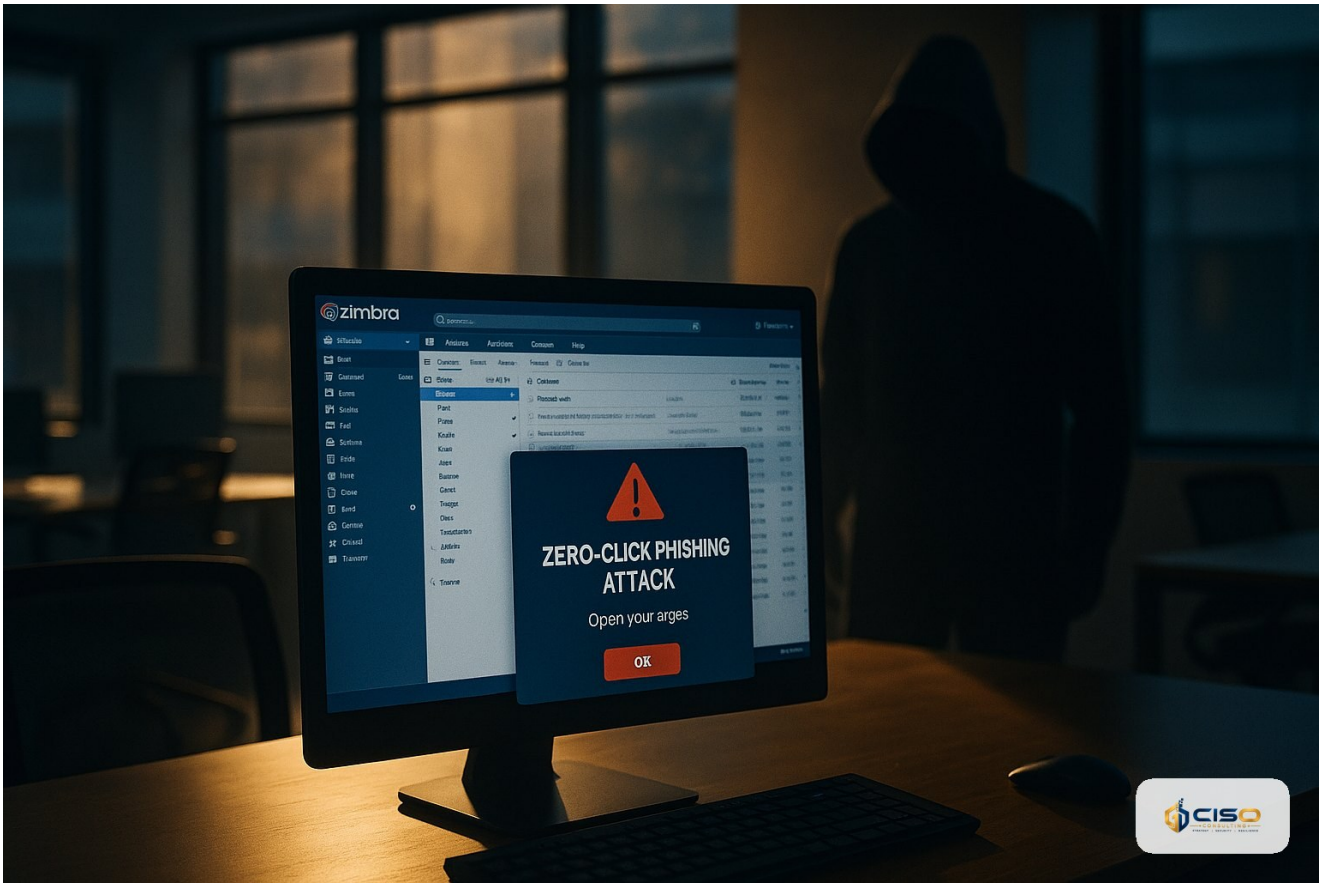
تحذير بشأن حملة تصيد جديدة بدون نقر تستهدف المنظمات الغربية



حددت المركز الوطني للأمن السيبراني وشركاؤه حملة تصيد جديدة بدون نقر من قبل فاعلين مدعومين من الدولة الروسية تستهدف المنظمات الغربية، وخاصة تلك التي تستخدم مجموعة زيمبرا للتعاون. يُنصح المنظمات بتعزيز تدابيرها للأمن السيبراني.

- يستخدم الفاعلون المدعومون من الدولة الروسية استغلالاً بدون نقر يسمى 'خلايا النحل' لاختراق أنظمة البريد الإلكتروني.
- تستهدف الحملة بشكل أساسي المنظمات التي تستخدم مجموعة زيمبرا للتعاون.
- يوصى بتصحيح الثغرات على الفور وتعزيز مراقبة الشبكة.
- يمكن تكييف التقنيات المستخدمة لاستغلال أنظمة البريد الإلكتروني الأخرى في المستقبل.
- يتم تشجيع المنظمات على التسجيل في خدمات التحذير المبكر للبقاء على اطلاع.

نظرة عامة

أصدر المركز الوطني للأمن السيبراني (NCSC) وشركاؤه الدوليون تحذيرًا بشأن حملة تصيد جديدة تنظمها فاعلون مدعومون من الدولة الروسية. تستخدم هذه الحملة استغلالاً بدون نقر يُعرف باسم 'خلايا النحل' للحصول على وصول غير مصرح به إلى أنظمة البريد الإلكتروني، مستهدفة بشكل خاص المنظمات التي تستخدم مجموعة زيمبرا للتعاون.

الآثار

على عكس أساليب التصيد التقليدية التي تتطلب تفاعل المستخدم، تسمح تقنية 'خلايا النحل' للمهاجمين باختراق الأنظمة بمجرد أن يقوم المستلم بعرض بريد إلكتروني ضار. يشكل هذا خطرًا كبيرًا على البيانات الحساسة وسلامة العمليات. المنظمات في قطاعات مثل الدفاع والحكومة والتكنولوجيا معرضة بشكل خاص.

الإجراءات الموصى بها

لتقليل المخاطر المرتبطة بهذه الحملة، يُنصح المنظمات باتخاذ الخطوات التالية:

- تصحيح أي ثغرات في مجموعة زيمبرا للتعاون على الفور.
- تعزيز قدرات مراقبة الشبكة لاكتشاف الأنشطة غير العادية.
- البقاء على اطلاع حول التهديدات المحتملة من خلال التسجيل في خدمات التحذير المبكر.
- توعية الموظفين بمخاطر التصيد وأهمية النظافة السيبرانية.
- مراجعة وتحديث خطط الاستجابة للحوادث بانتظام لمعالجة الانتهاكات المحتملة بشكل فعال.

ما يجب فعله الآن

1. تصحيح الثغرات في مجموعة زيمبرا للتعاون على الفور.
2. تعزيز قدرات مراقبة الشبكة لاكتشاف الأنشطة غير العادية.
3. التسجيل في خدمات التحذير المبكر للبقاء على اطلاع حول التهديدات.
4. توعية الموظفين بمخاطر التصيد وأهمية النظافة السيبرانية.
5. مراجعة وتحديث خطط الاستجابة للحوادث بانتظام.