

إشعار حول التهديدات الإلكترونية من الجهات المرتبطة بالحكومة الصينية



تستخدم الجهات المرتبطة بالحكومة الصينية مجموعة من الأدوات الآلية والتقنيات اليدوية لاختراق البيانات الحساسة في قطاعات مختلفة على مستوى العالم. يُنصح المؤسسات بتعزيز تدابير الأمن السيبراني للتخفيف من هذه التهديدات.

- تستخدم الجهات الفاعلة في الفضاء السيبراني أدوات مسح آلية وشبكات بوت.
- يستغلون الثغرات في أنظمة مثل Microsoft Exchange.
- يتم تحقيق الوصول المستمر من خلال برامج VPN.
- يُحث على المؤسسات تنفيذ المصادقة متعددة العوامل.
- تحديث الأنظمة في الوقت المناسب أمر حاسم لتقليل المخاطر.

نظرة عامة

تستخدم الجهات المرتبطة بالحكومة الصينية مجموعة من الأدوات الآلية والتقنيات اليدوية لاستهداف البيانات الحساسة. وقد تم ملاحظة هذه الأنشطة عبر مختلف القطاعات، بما في ذلك البنية التحتية الحيوية.

التقنيات المستخدمة

تستفيد الجهات الفاعلة من أدوات المسح الآلي والشبكات الكبيرة لتحديد الثغرات. يستغلون نقاط الضعف في الأنظمة، وخاصة من خلال هجمات البرمجة النصية عبر المواقع ورش الرمز السري على خوادم Microsoft Exchange. يتم الحفاظ على الاستمرارية عبر برامج VPN، مما يسمح باستخراج معلومات حساسة مثل رسائل البريد الإلكتروني والاعتمادات.

الإجراءات الموصى بها

للتخفيف من المخاطر المرتبطة بهذه التهديدات السيبرانية، يجب على المؤسسات اتخاذ تدابير استباقية. من الضروري تعطيل أي خدمات ومنافذ غير مستخدمة، وتعقيم مدخلات تطبيقات الويب لمنع هجمات الحقن، وتنفيذ المصادقة متعددة العوامل لجميع الخدمات. بالإضافة إلى ذلك، سيساعد تطبيق التحديثات في الوقت المناسب على تقليل احتمالية الاختراق.

ما يجب فعله الآن

1. تعطيل الخدمات والمنافذ غير المستخدمة.
2. تعقيم مدخلات تطبيقات الويب.
3. تنفيذ المصادقة متعددة العوامل لجميع الخدمات.
4. تطبيق التحديثات في الوقت المناسب على الأنظمة.