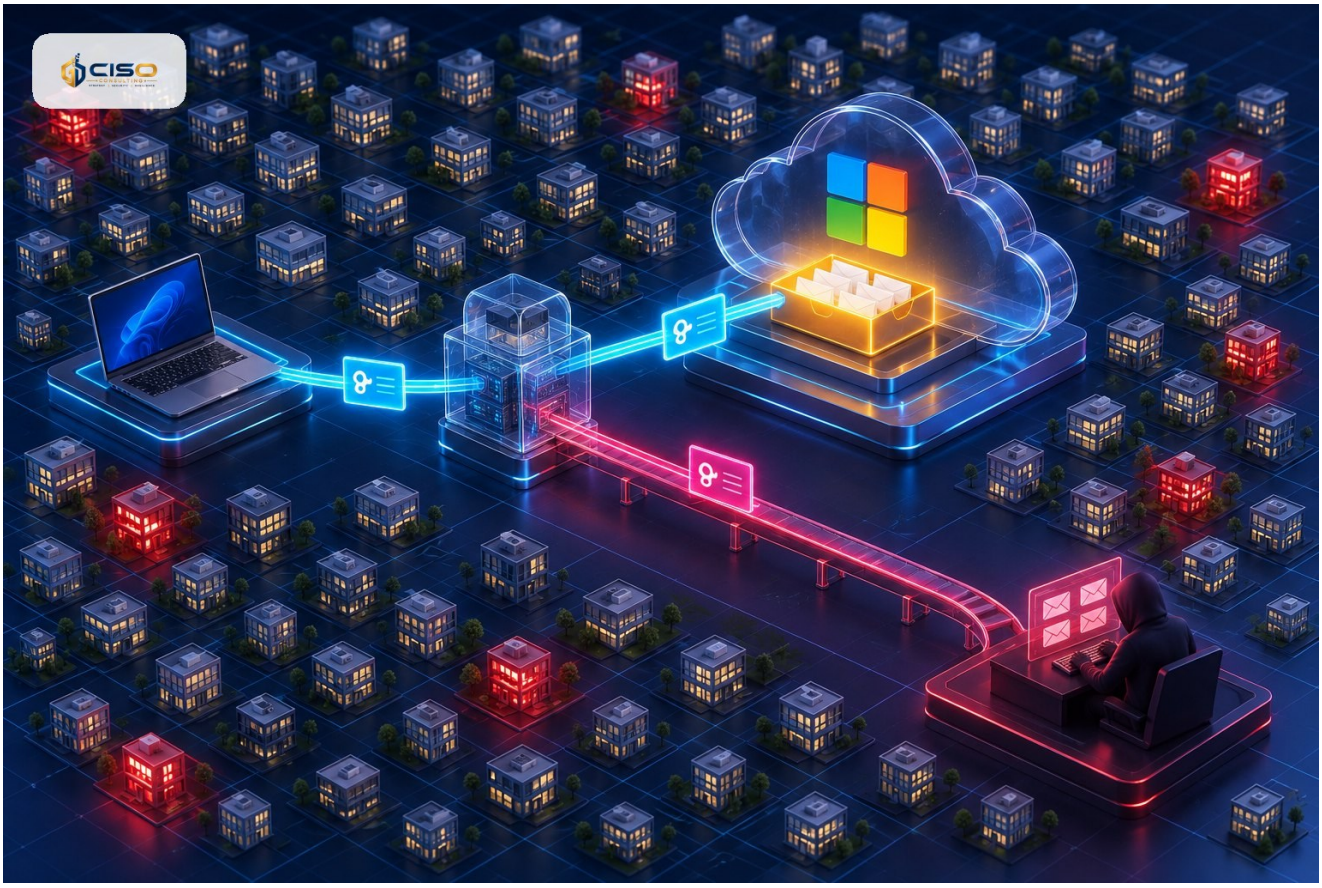
حملة إعادة استخدام الرموز تخترق 97 حساب Microsoft 365 في 79 جهة



رصدت Huntress حملة وسيط وسطي التقطت جلسات Microsoft 365 وأعادت استخدام الرموز المسروقة للوصول إلى البريد في 79 جهة بين 14 يوليو و22 سبتمبر 2026.

- تعتمد الحملة على وسيط وسطي (AitM) لالتقاط جلسات تسجيل الدخول.
- تُعاد بعد ذلك الرموز المسروقة لاختراق حسابات البريد.
- رصدت Huntress النشاط بين 14 يوليو و22 سبتمبر 2026.
- الأرقام المعلنة: 97 حسابًا مخترقًا في 79 جهة.
- سجلت Huntress 497 عملية دخول ناجحة إلى Microsoft 365، ولا يورد المقتطف تفاصيل إضافية.

ما الذي أُعلن

كشف باحثون عن حملة تستهدف Microsoft 365، يضع فيها المهاجمون وسيطًا وسطيًا (AitM) بين المستخدم وخدمة تسجيل الدخول. يلتقط هذا الوسيط جلسة الدخول، ثم يعيد المهاجمون استخدام الرموز المسروقة للوصول إلى حسابات البريد الإلكتروني.

رصدت Huntress النشاط بين 14 يوليو و22 سبتمبر 2026. ووفق التقرير، اختُرق 97 حسابًا في 79 جهة، وسجلت Huntress 497 عملية دخول ناجحة إلى Microsoft 365.

لماذا يهم ذلك

تعتمد إعادة استخدام الرموز على جلسة سبق توثيقها، لذلك لا تقتصر المسألة على كلمة المرور، وقد يبدو الدخول سليمًا في السجلات وهو في الواقع نشاط للمهاجم. ولا يتضمن المقتطف المتاح لنا وسائل الاستدراج ولا القطاعات المستهدفة ولا إجراءات تخفيف محددة، ولذلك لا نتجاوز ما ورد في التقرير.

الخطوات المقترحة

على الجهات التي تستخدم Microsoft 365 مراجعة طريقة حماية الجلسات والرموز وآلية اكتشاف عمليات الدخول الناجحة غير المعتادة. والإجراءات أدناه ممارسات عامة جيدة، وليست مأخوذة من التقرير نفسه.

ما يجب فعله الآن

1. مراجعة سجلات الدخول في Microsoft 365 بحثًا عن عمليات دخول ناجحة من مواقع أو أجهزة أو أوقات غير معتادة خلال الفترة من يوليو إلى سبتمبر 2026.
2. فحص صناديق البريد للحسابات المشبوهة بحثًا عن قواعد توجيه أو قواعد صندوق وارد جديدة.
3. إلغاء الجلسات والرموز النشطة وإعادة تعيين بيانات الاعتماد للحسابات التي تظهر عليها أنشطة مشبوهة.
4. تقييم مدى مقاومة أساليب المصادقة متعددة العوامل لتمرير الجلسات، وإعطاء الأولوية لأساليب أقوى للمستخدمين ذوي الصلاحيات العالية والمالية.
5. توعية الموظفين ومركز العمليات الأمنية بتصيد AitM وإضافة سيناريوهات إعادة استخدام الرموز إلى خطط الاستجابة للحوادث.