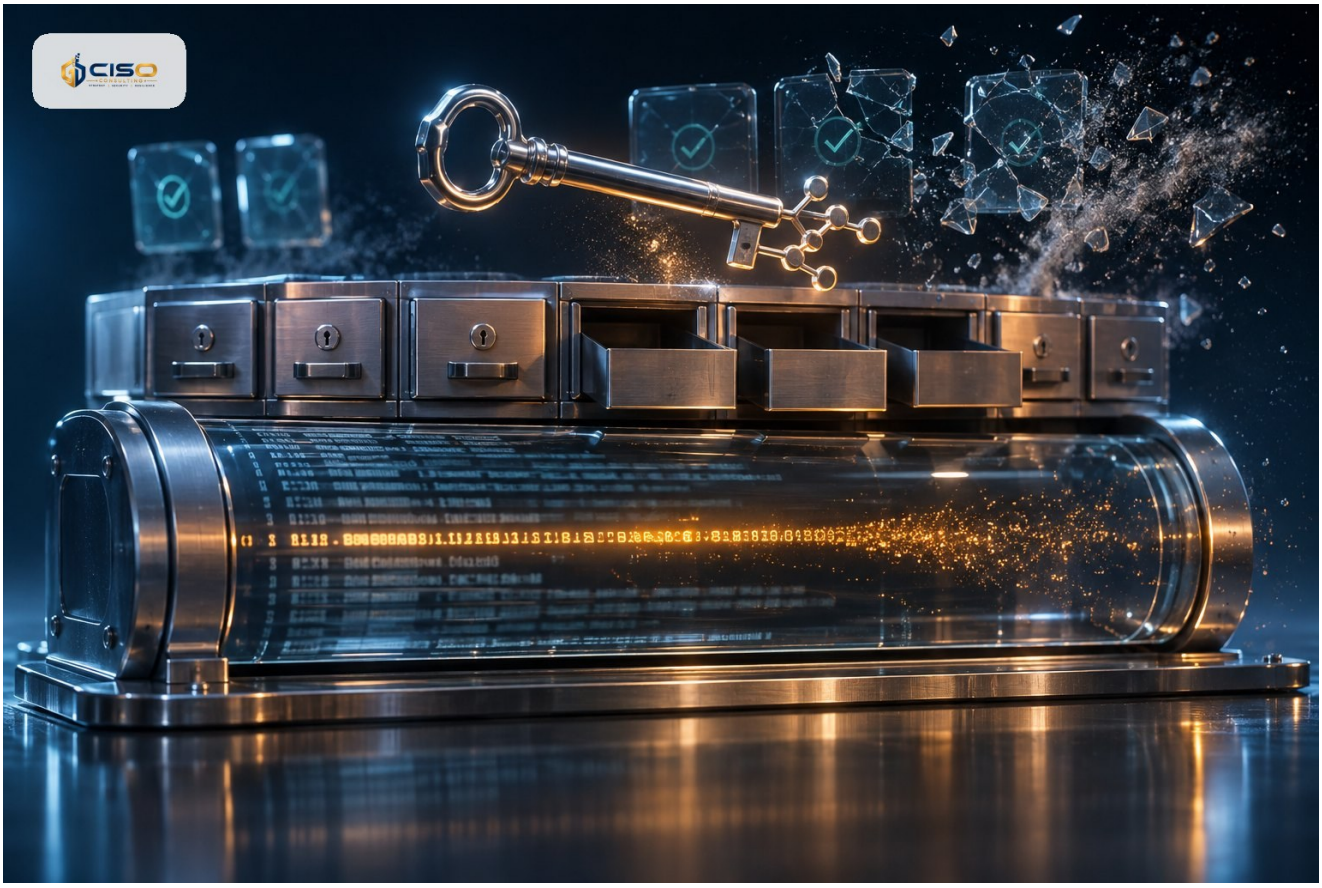
حملة Gheist تستخدم رموز GitHub المسروقة لاستخراج الأسرار من سجلات Actions



تصف Wiz حملة آلية تستخدم رموز GitHub مسروقة لإضافة مسارات عمل تطبع أسرار المستودع في سجلات Actions، ثم تنزّل السجلات وتحذف التشغيلات. طالت الهجمات مستودعات خاصة وبيئات GitHub Enterprise.

- الحملة المسماة Gheist آلية وتبدأ من رموز GitHub مسروقة.
- يزرع المهاجمون مسارات عمل تكتب أسرار المستودع في سجلات GitHub Actions.
- ينزّلون السجلات ثم يحذفون التشغيلات، مما يقلل الأثر الظاهر.
- تفيد Wiz بنجاح الهجمات ضد مستودعات خاصة وبيئات GitHub Enterprise.
- يشير المصدر إلى إجراء وقائي من GitHub لكن المقتطف لا يورد تفاصيله.

ما الذي ورد في التقرير

وفق تحليل لشركة أمن السحابة Wiz نقله موقع The Hacker News، تستغل حملة آلية تُدعى Gheist رموز GitHub المسروقة. وبرمز صالح يضيف المهاجمون مسار عمل (workflow) إلى المستودع، وعند تشغيله يطبع أسرار المستودع في سجلات GitHub Actions.

ثم ينزّل المهاجمون هذه السجلات ويحذفون تشغيلات مسار العمل. وتذكر Wiz أن الأسلوب نجح ضد مستودعات خاصة وبيئات GitHub Enterprise، فلا تكفي الاستضافة الخاصة أو المؤسسية وحدها للحماية.

أهمية الأمر

قد تنكشف الأسرار المخزنة لخطوط البناء والنشر، مثل بيانات الاعتماد ومفاتيح الأنظمة السحابية وأنظمة الإنتاج، دون أي تعديل في شيفرة التطبيق. ولأن التشغيلات تُحذف، قد لا يُظهر استعراض سجل التشغيلات المرئي هذا النشاط. ويشير المصدر كذلك إلى إجراء وقائي من GitHub يوقف أمرًا ما، لكن النص المتاح مقطوع، لذلك لا نصف آلية عمله ولا مدى فائدته.

التوجه العملي

يُنصح بالتعامل مع أي اشتباه في سرقة رمز على أنه احتمال انكشاف أسرار، لا مجرد وصول غير مصرح به إلى المستودع. وعلى الفرق مراجعة الرموز القائمة وما تصل إليه والأسرار الواقعة ضمن صلاحياتها.

ما يجب فعله الآن

1. حصر رموز GitHub المستخدمة، وإزالة غير المستخدم منها، وتقييد الباقي بأقل صلاحية لازمة.
2. تدوير الأسرار المخزنة في المستودعات وActions عند الاشتباه بسرقة رمز.
3. مراجعة تغييرات مسارات العمل الأخيرة وسجلات التدقيق بحثًا عن مسارات أو تشغيلات أو عمليات حذف غير متوقعة.
4. تقييد من يحق له إنشاء مسارات العمل أو تعديلها، واشتراط المراجعة على تغييرات ملفاتها.
5. إدراج اختراق الرموز وانكشاف أسرار خطوط النشر ضمن خطط الاستجابة للحوادث.