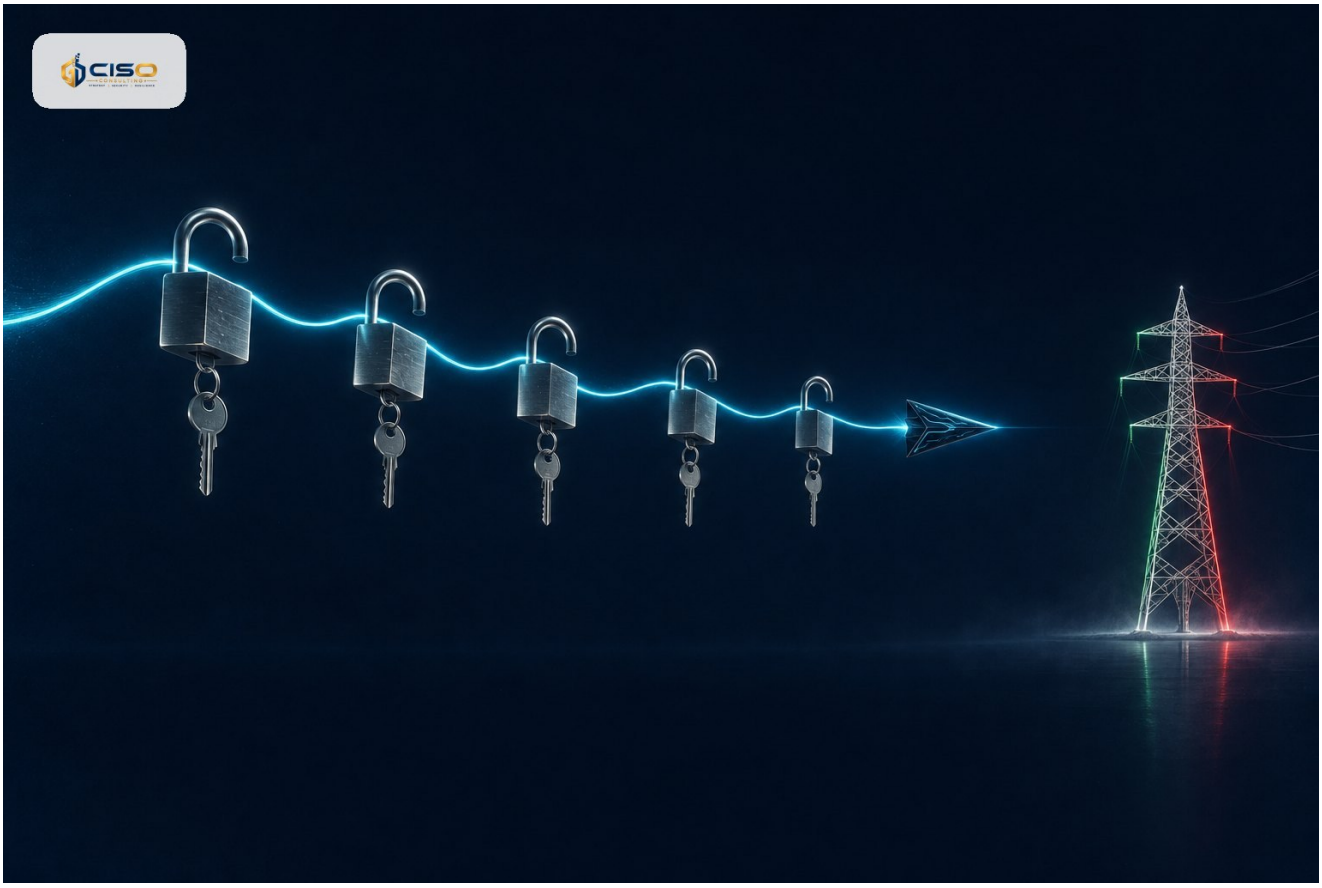
إيطاليا وسويسرا تحذّران من هجمات سيبرانية ذاتية بوكلاء الذكاء الاصطناعي تستهدف البنية التحتية الحيوية



أفادت جهات إيطالية وسويسرية باختراق وكلاء ذكاء اصطناعي منشآت في قطاعات حيوية بسرعة عبر ربط ثغرات معروفة وكلمات مرور ضعيفة، وأوصت بتقليص الأنظمة المكشوفة وتسريع التحديثات وتفعيل المصادقة متعددة العوامل والمراقبة.

- رصد CSIRT Italia حملات واسعة استخدمت وكلاء ذكاء اصطناعي ذاتيين لاكتشاف الثغرات وسوء الإعدادات واستغلالها في نقاط مكشوفة على الإنترنت.
- في إحدى الحالات وزّع منسّق المهام على خمسة وكلاء، من جمع المعلومات إلى الاستغلال والاستمرارية، وصولًا إلى الشبكات الداخلية.
- أكد المركز الوطني السويسري للأمن السيبراني (NCSC) أولى الهجمات الناجحة بمساعدة وكلاء الذكاء الاصطناعي، وشملت جهات في قطاعين على الأقل.
- ذكرت الجهتان أربعة أطر مستخدمة: ARTEX AI وCyberStrikeAI وRedg - DeepSeek Harness

PentAGI وTeam.

- يفيد NCSC بأن عدد وكلاء الذكاء الاصطناعي المتاحين علناً تقريباً تضاعف منذ أكتوبر.

حذّرت جهات للأمن السيبراني في إيطاليا وسويسرا من هجمات آلية يقودها وكلاء ذكاء اصطناعي، باتت تستهدف مؤسسات في قطاعات البنية التحتية الحيوية.

ما رصدته الجهات

أفاد CSIRT Italia برصد حملات واسعة استخدمت وكلاء ذاتيين لاكتشاف الثغرات وسوء الإعدادات في نقاط مكشوفة واستغلالها. وفي بعض الحالات عمل عدة وكلاء بالتوازي واخترقوا عدداً كبيراً من الأنظمة خلال ساعات. وفي إعداد واحد على DeepSeek Harness وزّع منسّق المهام على خمسة وكلاء مراحل تمتد من الاستطلاع إلى الاستغلال والاستمرارية. وربط الوكلاء بين الثغرات وسوء الإعدادات وبيانات اعتماد مخترقة، واتخذوا من الأنظمة المكشوفة موطئ قدم للوصول إلى الشبكات الداخلية. وأضافت الجهة أنهم كتبوا شيفرات خبيثة آنياً لتفادي حلول حماية الأجهزة الطرفية.

وأكد المركز الوطني السويسري للأمن السيبراني أولى البلاغات عن هجمات ناجحة بمساعدة وكلاء الذكاء الاصطناعي، طالت مشغّلين في قطاعين على الأقل. ووفق المركز انتهت كل الحالات المعروفة باختراق أنظمة الضحية. واستغل الوكلاء كلمات مرور ضعيفة وثغرات معروفة في نقاط مكشوفة، وقرروا خطواتهم التالية بصورة مستقلة.

الإجراءات الموصى بها

تنصح الجهة الإيطالية بإعطاء أولوية لتحديث الأنظمة المواجهة للإنترنت، وبخاصة الثغرات المستغلة فعلياً، وتعطيل واجهات الإدارة عن بعد غير الضرورية، ومراقبة عمليات مستوى التحكم ومصادر المصادقة وحركة المرور نحو الشبكات الداخلية والحركة الصادرة من الخوادم. وتوصي الجهة السويسرية بمعالجة الثغرات الحرجة خلال 24 ساعة من صدور التحديث، وإضافة المصادقة متعددة العوامل أو مفاتيح المرور، وتطبيق مبدأ الحد الأدنى من الصلاحيات.

لا يذكر المصدر وقوع حوادث في المملكة، لكن النمط يعتمد على التعرّض والثغرات في النظافة الأمنية الأساسية، وهو ما يهم أي جهة منظَّمة.

ما يجب فعله الآن

1. حصر الأنظمة المواجهة للإنترنت وإزالة أو تقييد ما لا حاجة إليه منها.
2. تعطيل واجهات الإدارة عن بعد غير الضرورية، وحماية المتبقي منها بالمصادقة متعددة العوامل.
3. تحديث الثغرات الحرجة والمستغلة فعلياً في الأنظمة المكشوفة خلال 24 ساعة قدر الإمكان.
4. فرض المصادقة متعددة العوامل أو مفاتيح المرور وكلمات مرور قوية والحد الأدنى من الصلاحيات على الحسابات المكشوفة والإدارية.
5. مراقبة مصادر المصادقة وحركة المرور نحو الشبكات الداخلية والحركة الصادرة من الخوادم بحثاً عن نشاط غير معتاد.

6. إدراج الهجمات السريعة متعددة المراحل بوكلاء الذكاء الاصطناعي في تمارين الفريق الأحمر وخطط الاستجابة للحوادث.