إطار Cairn المفتوح المصدر لاختبار الاختراق بالذكاء الاصطناعي يظهر في هجمات وثّقتها أربع شركات أمنية



وثّقت أمازون وGambit وNorForge وUnit 42 استخدام مهاجمين لإطار Cairn المفتوح المصدر لتشغيل وكلاء ذكاء اصطناعي مستقلين ضد أهداف حقيقية، وتنصح بأتمتة الاستجابة وإثبات القدرة على الاستعادة.

- تصف Amazon Threat Intelligence جهة تهديد مرتبطة بالصين شغّلت وكلاء مبنيين على Cairn بعنوانين IP وهدف واحد فقط، واستهدفت جامعات في شرق آسيا ابتداءً من 8 سبتمبر 2026.
- بعد نحو يوم من المحاولات الفاشلة، استغل الوكلاء ثغرة غير معروفة سابقاً (path traversal) في تطبيق مفتوح المصدر للتصوير الطبي بالذكاء الاصطناعي، وحصلوا على reverse shell بصلاحيات root.
- أمازون هي رابع شركة أمنية خلال نحو شهرين توثّق استخدام Cairn ضد أهداف حقيقية، بعد

Unit 42 وNorForge وGambit Security.

- تستخدم جماعات إجرامية وتجسسية أطراً مفتوحة المصدر أخرى منها ARTEX وPentAGI وHexStrike AI وCyberStrikeAI.
- تتركز التوصيات على الاستجابة الآلية للإنذارات عالية الثقة، ونظافة الهوية، وتقليص سطح الهجوم، والترقيع، وإثبات استعادة الأنظمة الحيوية للإيراد.

أفادت عدة شركات أمنية برصد مهاجمين يستخدمون Cairn، وهو إطار مفتوح المصدر يصفه مطوّره بأنه محرك عام لحل المشكلات يبحث عن مسار من نقطة البداية إلى الهدف عبر فضاء حالات مجهول. لم يُصمَّم الإطار خصيصاً لاختبار الاختراق، لكنه أثبت فعاليته فيه.

ما رصدته أمازون

عثرت Amazon Threat Intelligence على نسخة Cairn مستضافة علناً وتعمل دون مصادقة، وقدّرت من الإعدادات والتعليمات والمخرجات أن المشغّل جهة مرتبطة بالصين. زوّد المشغّل الوكلاء بعناوين IP مستهدفة وبهدف الحصول على shell. وبدءاً من 8 سبتمبر 2026 عمل الوكلاء ضد جامعات في شرق آسيا، فقضوا نحو 16 ساعة على خادم Redis يسمح بالوصول دون مصادقة، ثم أكثر من ست ساعات في تجربة أكثر من 30,000 تركيبة بيانات اعتماد مبنية على نحو 80 اسم مستخدم جُمعت من مصادر عامة. ولم ينجح أي من ذلك.

جاء الاختراق عبر ثغرة path traversal غير معروفة سابقاً في نقطة رفع الملفات بتطبيق مفتوح المصدر للتصوير الطبي بالذكاء الاصطناعي. انتقل الوكلاء من استكشاف واجهة API إلى كتابة ملفات عشوائية على الخادم خلال نحو 11 دقيقة، ثم حصلوا لاحقاً على reverse shell بصلاحيات root. وتدخّل مشغّل بشري مرة واحدة ليمنح الوكلاء نفقاً إلى شبكة جامعة ثانية تعمل بالبرنامج نفسه.

نمط أوسع

وثّقت Gambit Security وNorForge وUnit 42 استخداماً مشابهاً من جهات ذات دوافع مالية ومن جهات يُشتبه بارتباطها بالصين، ضد متاجر إلكترونية وقطاعات أشباه الموصلات والدفاع والمجتمع المدني. وأشارت Unit 42 إلى أن الثغرات المستغلة كانت في معظمها كلمات مرور ضعيفة وتجاوزات مصادقة وثغرات CVE قديمة. وترى Gambit أن الترقيع السريع وحده لم يعد كافياً.

التوجه الدفاعي

توصي أمازون باعتماد إنذارات عالية الثقة تُطلق استجابة آلية، مع إشراف بشري على النتائج، لأن الوكلاء قد يتفوقون في السرعة على فرز مراكز العمليات. ويجب توقع هجمات متواصلة لا تتعب. وتنصح Gambit بتحديد الأنظمة التي تُبقي الإيراد جارياً وإثبات إمكانية استعادتها تحت الهجوم.

ما يجب فعله الآن

1. راجعوا إجراءات مركز العمليات بحيث تُطلق الإنذارات عالية الثقة احتواءً آلياً، مع إشراف المحللين على النتائج بدل مراجعة كل إجراء.
2. احصروا الخدمات المكشوفة للإنترنت مثل Redis وقواعد البيانات المتجهية ولوحات الإدارة وVPN،

وأزيلوا الوصول دون مصادقة أو التعرّض غير الضروري.

3. عزّزوا نظافة الهوية بفرض المصادقة متعددة العوامل وإزالة كلمات المرور الضعيفة والافتراضية ومراقبة هجمات تجريب كلمات المرور واسعة النطاق.
4. افحصوا تطبيقات الذكاء الاصطناعي والتصوير مفتوحة المصدر في بيئتكم بحثاً عن نقاط رفع ملفات مكشوفة، وطبّقوا تحديثات المورّد فوراً.
5. حدّدوا الأنظمة الحيوية للإيراد واختبروا استعادتها تحت هجوم محاكى، ووثّقوا النتائج لأغراض الضمان وفق ضوابط NCA ECC وإطار SAMA CSF.