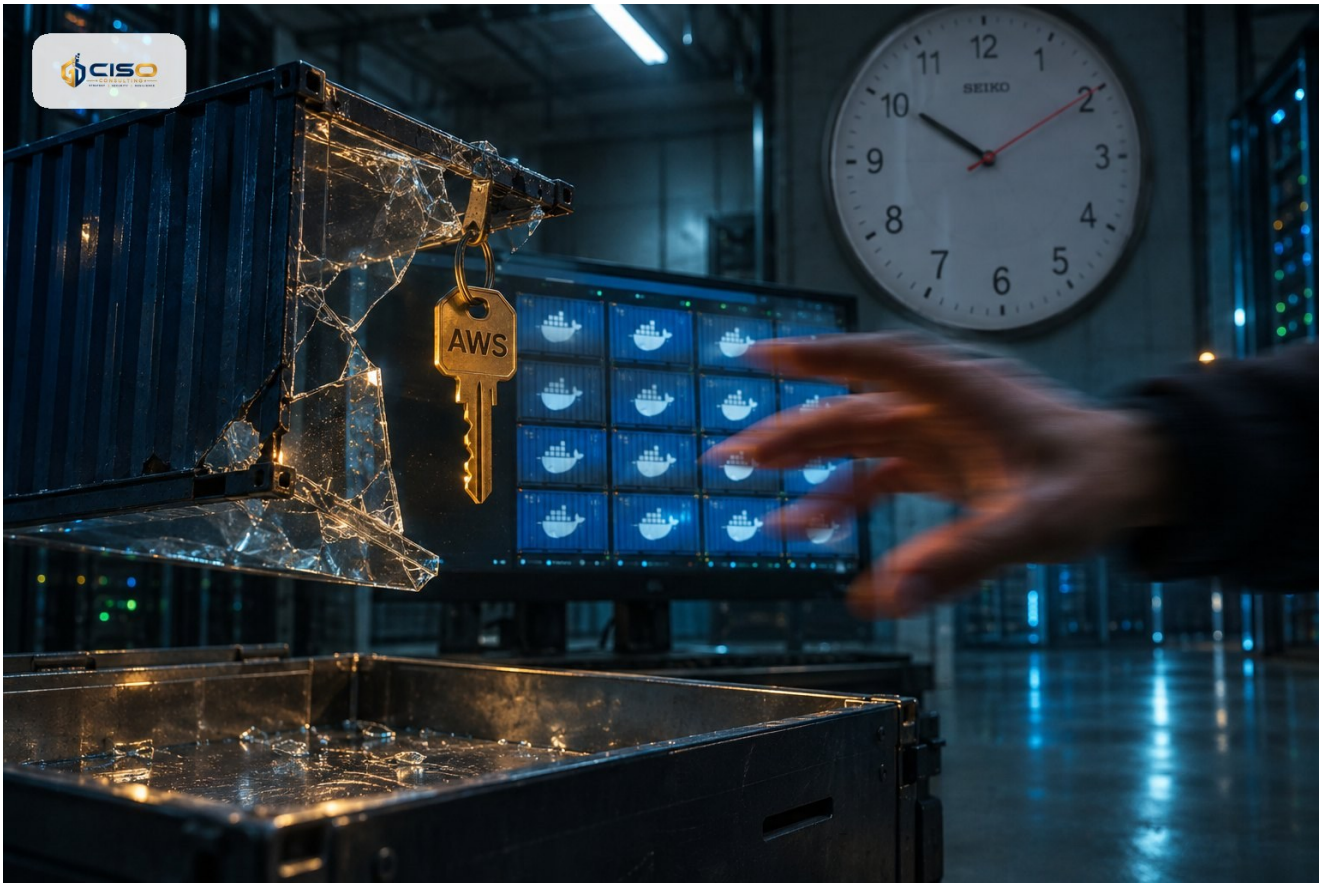
أبحاث: مفاتيح سحابية مسرّبة في صور Docker العامة استُغلّت خلال ثوانٍ



زرع باحثون من جامعة ستوني بروك بيانات اعتماد وهمية في 300 صورة Docker عامة، وقامت روبوتات باستخدام مفاتيح AWS خلال ثوانٍ؛ لذا يجب اعتبار أي مفتاح مسرّب مخترقًا لحظة نشره.

- وُضعت مفاتيح وهمية لـ AWS وOpenAI وAnthropic في 300 نسخة من صورة nginx على ثمانية سجلات خلال أربعة أشهر.
- تلقّت مفاتيح AWS أكثر من 140,000 استدعاء من أكثر من 5,000 عنوان IP، وجاء أسرع استدعاء بعد 7.86 ثانية من النشر.
- بلغ الوسيط الزمني لأول استخدام 51 ثانية، واستُخدمت جميع مفاتيح AWS خلال 15 دقيقة.
- استُنزفت أرصدة مفاتيح OpenAI وClaude بالكامل، بينما لم تُستخدم المفاتيح المقيّدة الصلاحيات لاستهلاك الرموز.
- الصور ذات الأسماء الموحية ببنية حساسة جذبت أكثر من ضعف عمليات السحب على Docker

.Hub

نشر الباحثان بيلي تسوفالاس ونيك نيكيفوراكيس من جامعة ستوني بروك 300 نسخة من صورة nginx الرسمية على ثمانية سجلات عامة، منها Docker Hub وAmazon ECR وRed Hat Quay. وضمّت كل نسخة مفاتيح وهمية لـ AWS وOpenAI وAnthropic. ورغم عدم الإعلان عن الصور، تلقّت مفاتيح AWS أكثر من 140,000 استدعاء من أكثر من 5,000 عنوان IP.

ما أظهرته التجربة

في الجولة الأولى على Docker Hub، استُخدمت أكثر من نصف مفاتيح AWS خلال دقيقة، وجميعها خلال 15 دقيقة، وبلغ الوسيط الزمني لأول استخدام 51 ثانية. أما مفاتيح OpenAI وClaude فقد استُنزفت أرصدتها، وفي بعض الحالات بعد انتظار أسابيع، وهو ما يرجّح الباحثون أنه يعكس إعادة بيع مفاتيح جرى التحقق منها.

ويبدو أن الروبوتات لا تشغّل الصور أصلاً؛ بل ترصد نقطة الفهرس في Docker Hub التي تسرد الصور الجديدة، وتقرأ ملف manifest لكل صورة، وتنزّل الطبقات المرجّح احتواؤها على بيانات اعتماد فقط، ثم تبحث فيها عن سلاسل تشبه المفاتيح. كما أن عدّاد السحب في Docker Hub يتأخر عن التنزيلات الفعلية بنحو 5 إلى 6 دقائق، فلا يستطيع مالك الصورة التفاعل في الوقت المناسب.

الدلالات

الدرس العملي أن النشر والاختراق يكادان يكونان حدثًا واحدًا. ولم تُستخدم المفاتيح محدودة الصلاحيات لاستهلاك الرموز، ما يدعم مبدأ الحد الأدنى من الصلاحيات. ويقترح الباحثون أن تفحص السجلات الصور عند رفعها بحثًا عن صيغ المفاتيح المعروفة، وأن تقيّد القائمة العامة لأحدث الصور. وكانت Docker قد أقرّت بالإفصاح وتراجع النتائج وقت كتابة الورقة.

وعلى الجهات التي تبني صور الحاويات وتنشرها أن تركّز على منع دخول الأسرار إلى الصور، وعلى سرعة الإلغاء إن حدث ذلك.

ما يجب فعله الآن

1. اعتبروا أي بيانات اعتماد وُجدت في صورة منشورة مخترقة وألغوها فورًا، ولا تعتمدوا على عدّاد السحب لتقدير الانكشاف.
2. أضيفوا فحص الأسرار إلى مسارات CI/CD للتحقق من خلو الصور من المفاتيح وبيانات الدخول قبل رفعها إلى أي سجل.
3. أصدروا مفاتيح السحابة وواجهات الذكاء الاصطناعي بصلاحيات مقيّدة وبأقل قدر لازم، وحدّدوا سقوف إنفاق وتنبيهات استخدام.
4. راجعوا صور الحاويات التي تنشرها فرقكم علنًا، وفضّلوا السجلات الخاصة لأحمال العمل الداخلية.
5. دوّروا مفاتيح السحابة والذكاء الاصطناعي دوريًا، وراقبوا سجلات نشاط AWS بحثًا عن فحوصات هوية أو استدعاءات من عناوين IP غير معروفة.