غوغل: المهاجمون ينتقلون من توجيه الذكاء الاصطناعي يدويًا إلى أطر وكلاء مستقلة متعددة



أفادت غوغل بأن المهاجمين باتوا يستخدمون أطر وكلاء ذكاء اصطناعي مستقلة ومتعددة بدل التوجيه اليدوي، لتنفيذ اختراقات متعددة المراحل بسرعة أكبر، ومنها ARTEX وCAIRN وCyberStrikeAI وPentAGI.

- تقول غوغل إن استخدام المهاجمين للذكاء الاصطناعي تجاوز التوجيه اليدوي.
- يجري الآن نشر أطر هجومية مستقلة متعددة الوكلاء.
- من الأطر المذكورة: ARTEX وCAIRN وCyberStrikeAI وPentAGI.
- تُستخدم هذه الأطر لتنفيذ اختراقات متعددة المراحل بسرعة تشغيلية أعلى.
- كما يستفيد المهاجمون من قدرات النماذج اللغوية الكبيرة.

ما الذي أعلنته غوغل

كشفت غوغل أن استخدام الجهات المهاجمة للذكاء الاصطناعي تجاوز مرحلة التوجيه اليدوي. فهي تنشر اليوم أطرًا هجومية مستقلة متعددة الوكلاء لتنفيذ اختراقات متعددة المراحل بسرعة تشغيلية أعلى.

ومن الأطر التي ورد ذكرها **ARTEX** و**CAIRN** و**CyberStrikeAI** و**PentAGI**. كما أشارت إلى أن المهاجمين يستفيدون في الوقت نفسه من قدرات النماذج اللغوية الكبيرة (LLMs).

الدلالات لفرق الأمن

لا يتضمن المقتطف المتاح تفاصيل تقنية أو معلومات عن ضحايا أو ثغرات محددة، لذا ينبغي أن تبقى الاستنتاجات متزنة. الخلاصة الرئيسة تتعلق بالسرعة: يمكن تنفيذ هجمات متسلسلة المراحل بجهد بشري أقل ووقت أقصر. ومن المرجح أن تضيق الفجوة بين ظهور الضعف ومحاولة استغلاله.

وبالنسبة للجهات المنظمة، يعزز ذلك أهمية الأساسيات: سرعة المعالجة، وضبط الصلاحيات والهويات، ومراقبة قادرة على اكتشاف النشاط متعدد المراحل لا الأحداث المنفردة.

خطوات مقترحة

يُنصح بمراجعة تقرير غوغل الكامل عند توفره وربط نتائجه بنموذج التهديدات لديكم، واعتماده مدخلاً في تقييمات المخاطر القائمة دون تغييرات عاجلة غير مخططة.

ما يجب فعله الآن

1. الاطلاع على تقرير غوغل الكامل وربط نتائجه بنموذج التهديدات لديكم.
2. مراجعة مدد المعالجة وإدارة الثغرات وتقصيرها حيثما أمكن.
3. تشديد ضوابط الصلاحيات المميزة والهويات للحد من الحركة الجانبية.
4. التأكد من قدرة قواعد المراقبة والكشف على ربط أنشطة الاختراق متعددة المراحل.
5. إطلاع مجلس الإدارة ولجنة المخاطر على تسارع الهجمات بدعم الذكاء الاصطناعي.