الخليج

منوعات, محطات

17 أبريل 2025 19:54 مساء

نشاط «الروبوتات الخبيثة» يتزايد على الإنترنت

أصدرت شركة «تاليس»، المزود العالمي للتكنولوجيا والأمن، تقرير «إمبيرفا» عن الروبوتات السيئة لعام 2025، وهو تحليل عالمي لحركة الروبوتات الآلية عبر الإنترنت.

يكشف تقرير هذا العام، وهو الدراسة البحثية السنوية الثانية عشرة، أن الذكاء الاصطناعي التوليدي يُحدث ثورة في تطوير الروبوتات، مما يسمح للجهات الفاعلة الأقل تطوراً بشن حجم أكبر من هجمات الروبوتات مع زيادة التردد.

ويستفيد المهاجمون اليوم أيضاً من الذكاء الاصطناعي للتدقيق في محاولاتهم الفاشلة وتحسين التقنيات للتهرب من التدابير الأمنية بكفاءة عالية، وسط نظام بيئي متنامٍ للروبوتات كخدمة (BaaS) لخدمات الروبوت التجارية.

أضاف التقرير: تجاوزت حركة المرور الآلية حركة المرور التي يولدها الإنسان لأول مرة منذ عقد من الزمان، لتشكل 51% من إجمالي حركة المرور على «الويب» في عام 2024، ويرجع هذا التحول إلى حد كبير إلى صعود الذكاء الاصطناعي ونماذج اللغة الكبيرة، والتي عملت على تبسيط عملية إنشاء وتوسيع نطاق الروبوتات لأغراض خبيثة.

ومع تزايد إمكانية الوصول إلى أدوات الذكاء الاصطناعي، يستغل مجرمو الإنترنت بشكل متزايد هذه التقنيات لإنشاء ونشر برامج روبوتية ضارة تمثل الآن 37% من إجمالي حركة الإنترنت ـ وهي زيادة كبيرة من 32% في عام 2023.

هذا هو العام السادس على التوالي من النمو في نشاط الروبوتات الخبيثة، مما يفرض تحديات أمنية على المؤسسات التي تسعى جاهدة لحماية أصولها الرقمية.

السفر والتجزئة

يواجه قطاعا السفر والتجزئة مشكلة الروبوتات المتقدمة، حيث تشكل الروبوتات السيئة 41% و59% من حركة المرور على التوالي. في عام 2024، سيصبح قطاع السفر الأكثر تعرضاً للهجمات، حيث يمثل 27% من جميع هجمات الروبوتات، مقارنة بـ 21% في عام 2023. وكان التحول الأبرز في عام 2024 الانخفاض في هجمات الروبوتات المتقدمة التي تستهدف قطاع السفر (41%، انخفاضاً من 61% في عام 2023) والزيادة الحادة في هجمات الروبوتات البسيطة (52%، ارتفاعاً من 34%).

يشير هذا التحول إلى أن أدوات الأتمتة المدعومة بالذكاء الاصطناعي قد خفضت حواجز الدخول أمام المهاجمين، مما يسمح للجهات الفاعلة الأقل تطوراً ببدء هجمات روبوتية أكثر أساسية. بدلاً من الاعتماد حصرياً على التقنيات المتطورة، يستخدم مجرمو الإنترنت بشكل متزايد كميات كبيرة من الروبوتات البسيطة لإغراق مواقع السفر، مما يؤدي إلى هجمات أكثر تكراراً وانتشاراً.

صعود الروبوتات القائمة على الذكاء الاصطناعي: عصر جديد من تحديات الأمن السيبراني.

Google وClaudeBot وByteSpider Bot وChatGPT وظهور أدوات الذكاء الاصطناعي المتقدمة، بما في ذلك Cohere AI وPerplexity AI وGemini لا يؤدي فقط إلى تحويل تفاعلات المستخدم ولكن أيضاً إلى الأساليب التي ينفذ بها المهاجمون التهديدات السيبرانية. وفقاً لفريق أبحاث التهديدات في إمبيرفا، يتم الاستفادة من أدوات الذكاء الاصطناعي المستخدمة على نطاق واسع في الهجمات الإلكترونية، حيث كان برنامج ByteSpider Bot وحده مسؤولاً عن 54% من جميع الهجمات المدعومة بالذكاء الاصطناعي. ومن بين المساهمين المهمين الآخرين AppleBot بنسبة 13%، و ClaudeBot26%، و ChatGPT User Bot 6 بنسبة 6%.

آثار خطيرة

قال تيم شانج، المدير العام لأمن التطبيقات في شركة تاليس: «إن الارتفاع الكبير في إنشاء الروبوتات المعتمدة على الذكاء الاصطناعي له آثار خطيرة في الشركات في جميع أنحاء العالم». «نظراً لأن حركة المرور الآلية تمثل أكثر من نصف إجمالي نشاط الويب، فإن المؤسسات تواجه مخاطر متزايدة من الروبوتات السيئة، والتي أصبحت أكثر انتشاراً كل يوم».

ومع تزايد مهارة المهاجمين في استخدام الذكاء الاصطناعي، يمكنهم تنفيذ مجموعة متنوعة من التهديدات السيبرانية ـ بدءاً من هجمات الحرمان من الخدمة الموزعة واستغلال القواعد المخصصة وانتهاكات واجهة برمجة التطبيقات. ورغم أن الهجمات التي تعتمد على الروبوتات أصبحت أكثر تعقيداً على نحو متزايد، فإنها تشكل تحديات كبيرة لجهود الكشف عنها.

وأضاف شانج: «يلقي تقرير هذا العام الضوء على التكتيكات والتقنيات المتطورة التي يستخدمها مهاجمو الروبوتات». إن ما كان يُعتبر في السابق أساليب تهرب متقدمة أصبح الآن ممارسة قياسية للعديد من الروبوتات الخبيثة. في هذه البيئة سريعة التغير، يجب على الشركات تطوير استراتيجياتها. من الضروري اعتماد نهج متكيف واستباقي، والاستفادة

من أدوات الكشف عن الروبوتات المتطورة وحلول إدارة الأمن السيبراني الشاملة لبناء دفاع مرن ضد المشهد المتغير باستمرار للتهديدات المتعلقة بالروبوتات».

تشكل الروبوتات الضارة التي تستهدف منطق أعمال واجهة برمجة التطبيقات تهديداً متزايداً للمؤسسات الحديثة وتكشف النتائج الأخيرة التي توصل إليها فريق أبحاث التهديدات في إمبيرفا عن ارتفاع كبير في الهجمات الموجهة إلى واجهات برمجة التطبيقات، حيث يستهدف 44% من حركة الروبوتات المتقدمة واجهات برمجة التطبيقات. لا تقتصر هذه الهجمات على نقاط نهاية واجهة برمجة التطبيقات فحسب؛ بل إنها تستهدف منطق الأعمال المعقد الذي يحدد كيفية عمل واجهات برمجة التطبيقات. يقوم المهاجمون بنشر روبوتات مصممة خصيصاً لاستغلال الثغرات الأمنية في سير عمل واجهة برمجة التطبيقات، والمشاركة في عمليات الاحتيال الآلية في الدفع، واختطاف الحسابات، واستخراج البيانات.

البيانات الحساسة

يكشف التحليل الوارد في التقرير عن استراتيجية متعمدة من جانب المهاجمين السيبرانيين لاستغلال نقاط نهاية واجهة برمجة التطبيقات التي تدير البيانات الحساسة وعالية القيمة. وتُعد آثار هذا الاتجاه شديدة التأثير بشكل خاص في الصناعات التي تعتمد على واجهات برمجة التطبيقات في عملياتها ومعاملاتها المهمة. وتتحمل قطاعات الخدمات المالية والرعاية الصحية والتجارة الإلكترونية العبء الأكبر من هذه الهجمات الروبوتية المتطورة، مما يجعلها أهدافاً رئيسية للجهات الخبيثة التي تسعى إلى اختراق المعلومات الحساسة.

تشكل واجهات برمجة التطبيقات العمود الفقري للتطبيقات الحديثة، مما يتيح الاتصال عبر الخدمات، وبث العمليات، وتقديم تجارب عملاء مخصصة على نطاق واسع. وهي تدعم وظائف أساسية مثل معالجة المدفوعات وإدارة سلسلة التوريد والتحليلات المعتمدة على الذكاء الاصطناعي، مما يجعلها لا غنى عنها لتعزيز الكفاءة وتسريع تطوير المنتجات وفتح مصادر دخل جديدة.

وأضاف شانج أيضاً: «إن منطق الأعمال المتأصل في واجهات برمجة التطبيقات قوي، ولكنه يخلق أيضاً نقاط ضعف فريدة تسعى الجهات الخبيثة إلى استغلالها». «ومع تبني المؤسسات للخدمات المستندة إلى السحابة وهندسة الخدمات المصغرة، من الضروري أن نفهم أن الميزات التي تجعل واجهات برمجة التطبيقات ضرورية يمكن أن تجعلها أيضاً عرضة لخطر الاحتيال وانتهاكات البيانات».

تواجه الخدمات المالية والرعاية الصحية وصناعات التجارة الإلكترونية مخاطر متزايدة.

صناعات مهددة

يقدم تقرير «إمبيرفا» عن الروبوتات السيئة لعام 2025 تحليلاً متعمقاً يسلط الضوء على الصناعات الأكثر عرضة للخطر. تعد الخدمات المالية والرعاية الصحية والتجارة الإلكترونية القطاعات الأكثر تضرراً، وهي الصناعات التي تعتمد على واجهات برمجة التطبيقات للعمليات الحرجة والمعاملات الحساسة، مما يجعلها أهدافاً جذابة لهجمات الروبوتات المتطورة.

كان قطاع الخدمات المالية هو القطاع الأكثر استهدافاً لهجمات الاستيلاء على الحسابات، حيث شكل 22% من جميع الحوادث، يليه قطاع الاتصالات ومقدمي خدمات الإنترنت بنسبة 18%، ثم قطاع الحوسبة وتكنولوجيا المعلومات بنسبة

17%. لطالما كانت الخدمات المالية هدفاً رئيسياً لهجمات الاستيلاء على الحسابات بسبب القيمة العالية للحسابات والطبيعة الحساسة للبيانات المعرضة للخطر. تمتلك البنوك وشركات بطاقات الائتمان ومنصات التكنولوجيا المالية كميات هائلة من معلومات التعريف الشخصية، بما في ذلك تفاصيل بطاقة الائتمان والحساب المصرفي، والتي يمكن بيعها بشكل مربح على الويب المظلم. إضافة إلى ذلك، أدى الانتشار المتزايد لواجهات برمجة التطبيقات داخل الصناعة إلى توسيع سطح الهجوم، مما سمح لمجرمي الإنترنت باستغلال نقاط الضعف مثل ضعف أساليب المصادقة والترخيص، وبالتالي تسهيل عمليات الاستيلاء على الحسابات وسرقة البيانات.

ويعتمد تقرير«إمبيرفا» عن الروبوتات السيئة على رؤى من فرق خدمات محللي الأمن وبحوث التهديدات. يعتمد تحليلنا على البيانات التي تم جمعها من جميع أنحاء شبكة «إمبيرفا» العالمية في عام 2024، بما في ذلك حظر 13 تريليون طلب روبوت سيئ عبر آلاف المجالات والصناعات. توفر مجموعة البيانات هذه رؤى رئيسية حول نشاط الروبوت لمساعدة المؤسسات على فهم المخاطر المتزايدة للهجمات الآلية ومعالجتها.