تطبيقات الحمايــة من البرمجيات الخبيثة في «أندرويد» سهلة الاختراق

استهدفت دراسة لجامعة «نورث ويسترن» الأميركية الكشف عن مدى فاعلية بعض من أشهر تطبيقات الحماية ومكافحة البرمجيات الخبيثة المستخدمة في نظام تشغيل «أندرويد»، وتوصلت إلى عجزها جميعاً عن مقاومة أنواع عدة من الهجمات عقب إجراء تحولات بسيطة في بنية الفيروسات المعروفة.

ووصف الباحث المشارك في الدراسة، يان شين، النتائج بأنها «مذهلة للغاية».

وقال: «لم يتمكن كثير من هذه البرامج من التعرف إلى هجمات مُتحوّلة عادية لا تنطوي على تغييرات في التعليمات البرمجية، وهو ما يمكن أن يقوم به مراهقون».

واعتمد الباحثون، المنتمون لجامعتيّ «نورث ويسترن» و«نورث كارولينا» في الولايات المتحدة، في اختبار تطبيقات مكافحة الفيروسات على تطوير أداة باسم «درويد شاميليون» لإجراء بعض التغييرات في مجموعة من البرمجيات الخبيثة المعروفة، منها «جينيمي» و«درويد دريم» و«فيك بلاير».

وتضمن التغيير تبديلات بسيطة في التعليمات البرمجية، أو تغيير اسم الملف، أو تغييرا بسيطا في مظهر الفيروسات مع احتفاظها بالقدر نفسه من الضرر.

واختبر الباحثون أثر البرمجيات الخبيثة المحولة على إصدارات كاملة لـ10 من أشهر برامج مكافحة الفيروسات لنظام تشغيل «أندرويد»، التي يعتمد عليها الملايين من المستخدمين، ومنها «نورتون»، و«كاسبر سكي»، و«لوك آوت»، و«ترند ميكرو»، و«إيه في جي»، و«إي إس إي

تي»، و«إيه إس تي سوفت آلياك»، و«دكتور ويب»، ولم تُفلح هذه البرامج في مقاومة الفيروسات الشائعة بعد إدخال تعديلات بسيطة في بنيتها، وهو ما يعني إمكانية اختراقها بسهولة مع تطبيق تحولات طفيفة على البرمجيات الخبيثة المعروفة، وذلك بحسب نتائج الدراسة، التي حملت عنوان «تقييم تطبيقات مكافحة البرمجيات الخبيثة لنظام (أندرويد) تجاه الهجمات المتحولة».

وأرجع الباحثون أوجه القصور في تطبيقات الحماية إلى اعتماد أغلبها على البحث عن توقيعات بالغة البساطة للبرمجيات الخبيثة وأنماط معينة من التعليمات البرمجية، يُمكن تغييرها بسهولة من حيث الشكل مع أدائها الدور نفسه.

وتقترح الدراسة تطوير هذه التطبيقات، بحيث تعتمد على تقنيات التحليل الساكن، لتتمكن من البحث الدلالي عن البرمجيات الضارة، ورصد الهجمات المتحولة بقدر أكبر من الدقة.

وامتدت الدراسة عاماً كاملاً ما بين فبراير 2012 والشهر نفسه من العام الجاري. وأشارت النتائج إلى تحسن برامج الحماية من الفيروسات خلال هذه الفترة؛ فبينما نجح 45٪ من توقيعات البرمجيات الضارة المُحوّلة في اختراقها سابقاً، تراجعت النسبة إلى 16٪ العام الجاري.

وقال الأستاذ المساعد في كلية «ماكورميك» للهندسة والعلوم التطبيقية، يان شين: «تُشير النتائج التي توصلنا لها من دون شك إلى حدوث تحسن، فلم تستسلم أدوات مكافحة البرمجيات الخبيثة كثيراً لهذه التحولات الطفيفة»، لكنه أشار إلى حاجة برامج الحماية من الفيروسات إلى مزيد من التطوير.

وأضاف: «إلى الآن، هذه المنتجات ليست قوية وفعالة بالدرجة المطلوبة لوقف البرمجيات الخبيثة».

وأشارت الدراسة إلى أنها لم تهدف إلى اختيار البرنامج الأفضل للحماية من البرمجيات الضارة، كما لم تقدم تقييماً شاملاً لمختلف خصائصها، إذ لم تتطرق إلى وظائف أخرى، مثل حماية الأجهزة في حال فقدانها، أو تصفية الرسائل القصيرة المزعجة، أو استهداف الهواتف من خلال رسائل البريد الإلكتروني.

وأرجعت سبب اختيار نظام «أندرويد» لاختباره إلى كونه النظام الأكثر انتشاراً بين مستخدمي الهواتف الذكية في مختلف أنحاء العالم، لكن هذا لا يعني في الوقت نفسه أن أنظمة التشغيل الأخرى بمنأى عن هجمات البرمجيات الضارة أو أنها تتمتع بحماية أفضل.

ويأمل الباحثون أن تُسهم نتائج الدراسة في تطوير الجيل التالي من تطبيقات مكافحة البرمجيات الضارة لـ«أندرويد».

وكانت تقارير لشركات متخصصة في إنتاج برامج مكافحة الفيروسات أشارت إلى تنامي عدد

البرمجيات الضارة التي تستهدف الهواتف الذكية، وذكر تقرير لشركة «إن كيو»، المتخصصة في إنتاج برامج الحماية للهواتف المحمولة، أن عدد البرمجيات الضارة وصل إلى ما يزيد على 65 ألف نوع خلال العام الماضي، وأشارت إلى أن نسبة 95٪ منها استهدفت نظام تشغيل «أندرويد»، وتأثر بها نحو 32.8 مليوححن جهاز.