الساعة الذكية تكشف المستحيل: اختراق "غير مرئي" لأشد الحواسيب تحصيناً

كشف فريق من الباحثين عن وسيلة اختراق غير تقليدية تستهدف أنظمة الحواسيب المعزولة عن الشبكات air-gapped، عبر الساعات الذكية التي تلتقط بيانات حساسة تُرسل عبر إشارات فوق صوتية لا يمكن سماعها.

والثغرة الجديدة التي تحمل اسم SmartAttack تمثل تهديداً أمنياً لواحدة من أكثر وسائل الحماية الرقمية اعتماداً في المؤسسات الحساسة وهي الحواسيب المعزولة بشكل كامل عن شبكة الإنترنت.

وفي دراسة قُبلت للنشر في مؤتمر IEEE COMPSAC 2025، أوضح الباحثون بقيادة موردخاي جوري، أن:"هذه الطريقة تستغل الميكروفونات المدمجة في الساعات الذكية لاستقبال إشارات فوق صوتية يتم بثها من مكبرات الصوت الخاصة بالحواسيب المعزولة، وذلك بعد تثبيت برمجية خبيثة على متنها".

وتعمل البرمجية الخبيثة المثبتة مسبقاً على هذه الحواسيب، على إرسال البيانات بشكل مشفّر عبر هذه الإشارات فوق الصوتية باستخدام تقنية تُعرف باسم "تبديل التردد الثنائي" (Binary Frequency Shift

كيلوهرتز 19.5 تردد يمثل حين في ،"0" القيمة كيلوهرتز 18.5 تردد يمثل حيث ،(Keying - B-FSK القيمة "1".

وتُرسل هذه الإشارات لاسلكياً على هيئة موجات فوق صوتية غير مسموعة، وتلتقطها ميكروفونات الساعات الذكية القريبة، سواء كانت هذه الأجهزة مزروعة عمداً من قبل جهة معادية أو تم اختراقها مسبقاً.

وتقوم تطبيقات خاصة على الساعة بتحليل هذه الترددات وتحويلها إلى بيانات رقمية مفهومة، والتي يمكن لاحقاً إرسالها إلى الخارج باستخدام الاتصال اللاسلكي مثل الواي فاي، البلوتوث أو الشبكة الخلوية، بعد مغادرة مرتدي الساعة للمنشأة الحساسة.

ويشير الباحثون إلى أن:"نقطة البداية لهذا الهجوم تعتمد غالباً على تهديد داخلي، مثل موظف ناقم، أو حاسوب تم اختراقه ضمن سلسلة التوريد، مما يسهل زرع البرمجية الخبيثة على الجهاز المستهدف".

وبعد تثبيت البرمجية، لا تعتمد على الشبكات التقليدية، بل توظف المكونات الفيزيائية للجهاز – وتحديداً مكبر الصوت – كقناة لنقل البيانات.

ورغم براعة التقنية، إلا أن لها حدوداً عملية، أبرزها أن ميكروفونات الساعات الذكية أصغر حجماً وأقل حساسية من تلك الموجودة في الهواتف الذكية، ما يجعل استقبال الإشارات أضعف وأكثر عرضة للتشويش، خصوصاً في حالات الترددات العالية أو انخفاض شدة الإشارة، كما أن فعالية الاستقبال تعتمد بشكل كبير على موضع الساعة واتجاهها بالنسبة لمصدر الصوت، حيث تكون النتائج أفضل عند وجود خط رؤية مباشر بين الساعة ومكبر الصوت.

وأما فيما يتعلق بمدى الإرسال، فقد حُدّد بين 6 إلى 9 أمتار، بينما تتراوح سرعة نقل البيانات بين 5 إلى 50 بت في الثانية، وهي سرعة بطيئة للغاية تجعل من عملية تسريب كميات كبيرة من البيانات مهمة طويلة ومجهدة.

ومع ذلك، فإن خطورة هذه التقنية تكمن في إثبات أن الحواسيب المعزولة ليست منيعة كما يُعتقد، وأن التهديدات قد تأتي من قنوات غير تقليدية.

وقد سبق لجوري أن قدم دراسات مشابهة أظهرت إمكانية تسريب البيانات من الأجهزة المعزولة عبر وسائل

متعددة مثل إشارات الضوء من شاشات LCD، وتقلبات البيانات داخل الذاكرة العشوائية RAM، ومؤشرات إضاءة بطاقات الشبكة، والإشعاع الكهرومغناطيسي من كابلات USB وSATA، بل وحتى من خلال وحدات تزويد الطاقة.

ويرى الباحثون، أن:"هذا النوع من الهجمات، رغم صعوبته النظرية والعملية، يمثل إنذاراً مبكراً لصناع القرار والخبراء في أمن المعلومات. كما أوصوا باتخاذ عدد من الإجراءات الوقائية، أبرزها حظر دخول الساعات الذكية إلى المرافق الحساسة، أو إزالة مكبرات الصوت من الحواسيب المعزولة، حيث تمثل المصدر الرئيسي للإشارات".

وفي حال عدم إمكانية تنفيذ تلك الإجراءات، يمكن استخدام تقنيات أكثر تعقيداً، مثل التشويش فوق الصوتي، والذي يعتمد على إصدار ضوضاء شاملة تُربك الإشارة الأصلية، إلى جانب تطوير جدران حماية برمجية قادرة على رصد أي نشاط غير معتاد لمكبرات الصوت، وكذلك فرض حواجز مادية تمنع انتقال الصوت.