هل يمكن التنصت عبر كابلات الألياف الضوئية "الفايبر"؟

الجمعة 1 مايو 2026 06:00 م

كابلات الألياف الضوئية- أو الفايبر هي تقنية ثورية لنقل البيانات تعتمد على النبضات الضوئية بدلاً من الإشارات الكهربائية، مما يجعلها أسرع بكثير من الكابلات النحاسية التقليدية.

وتستخدم كابلات الألياف الضوئية خيوطًا زجاجية فائقة الرقة لنقل البيانات، وقد تبيّن أن هذه الخيوط الزجاجية حساسة للغاية للاهتزازات لدرجة أنها تُغيّر خصائص الإشارة الضوئية بشكل طفيف.

ومن الناحية النظرية، يسمح هذا بتحويل كابل الألياف الضوئية إلى ميكروفون والتنصت على المحادثات من على بُعد كيلومترات من مصدر الصوت، كما قالت شركة كاسبرسكي (Kaspersky)، الرائدة في مجال الأمن السيبراني.

عقبات التنصت البصري

ونشر باحثون من ثلاث جامعات في هونج كونج ورقة بحثية تُظهر طريقةً للتنصت عبر كابلات الألياف الضوئية، وذلك بعد أن درس باحثون روس الخصائص الفريدة لكابلات الألياف الضوئية لأول مرة عام 2012، وأقروا بإمكانية حدوث التجسس نظريًا. فيما درس الباحثون من هونج كونج إثبات إمكانية تطبيق التنصت عمليًا ولو جزئيًا.

وكان ذلك بشكل عملي من خلال شرح طريقة عمل الألياف الضوئية وطريقة توصيلها، حيث يتولى مزود خدمة الإنترنت إدارة ما يُسمى بشبكة التوزيع الضوئية (ODN)، التي يتصل بها المستخدمون. ويُطلق على الجهاز الموجود لدى المستخدم اسم وحدة الشبكة الضوئية (ONU).

ويُعدّ تنفيذ هجوم باستخدام هذه المعدات أمرًا بالغ الصعوبة. إذ يحتاج المهاجم المحتمل للتنصت على نقطة نهاية محددة في وحدة الشبكة الضوئية، إلى الوصول إلى بنية مزود الخدمة والتحكم في معدات شبكة التوزيع الضوئية (ODN).

ما هذا الجهاز؟ إنه موجّه شبكة أو محوّل ضوئي إلى إيثرنت - صندوق صغير يُوضع عادةً في خزانة المرافق المكتبية. وداخل المبنى، يتم توفير الاتصال إما عبر شبكة واي فاي أو شبكة محلية باستخدام كابلات إيثرنت. والأهم من ذلك، أنه من غير المرجح أن يمتد كابل الألياف الضوئية مباشرةً إلى منطقة حساسة.

وتتمثل معدات المهاجم في استخدام تقنية خاصة، إذ يرسل نبضات ضوئية عبر كابل الألياف الضوئية ويقيس خصائص إرسالها. وتُحدث الاهتزازات الطفيفة الناتجة عن خطوات الأقدام في غرفة قريبة من الكابل، بالإضافة إلى المحادثات المجاورة، ظاهرة تُعرف باسم "تشتت رايلي". وهذه الظاهرة بدورها تُسبب انحرافات دقيقة في خصائص الإشارة المنعكسة، والتي يلتقطها المهاجم باستخدام مستشعر ضوئي.

وقبل الانتقال إلى تسجيل الصوت، قرر الباحثون اختبار سيناريو أبسط. ولتبسيط المهمة، قاموا بتمديد كابل الألياف الضوئية حول محيط الغرفة وسجلوا خطوات الأقدام- التي تُحدث اهتزازات ملحوظة- بدلاً من المحادثات الهادئة.

وحققت هذه التجربة نجاحًا كبيرًا، إذ كانت خطوات الأقدام مسموعة بوضوح. مع ذلك، أثبت تسجيل الكلام البشري صعوبة بالغة. واتضح أنه حتى في ظروف المختبر، كان اعتراض محادثة بين شخصين أمرًا مستحيلاً.

ولتمكين المراحل اللاحقة من الهجوم، افترض الباحثون وجود جهاز تنصت عند نقطة دخول الألياف إلى الغرفة. وهذا الجهاز عبارة عن ميكروفون يحول الإشارات الصوتية إلى اهتزازات على كابل الألياف الضوئية، مما يُضخّم الإشارة ويُمكّن المهاجم من اعتراضها.

مزايا غير واضحة

لكن لماذا كل هذا العناء باستخدام الألياف الضوئية، إذا كان بإمكان الجهاز نقل المحادثة بنفسه عبر بيانات الهاتف المحمول أو خط الهاتف الأرضي للمبنى، بخاصةً أنه موجود بالفعل فوقها مباشرةً؟، لأن هناك ميزة واضحة لسيناريو الهجوم الذي اقترحه الباحثون.

يسهل اكتشاف جهاز تنصت عادي ينقل الصوت عبر شبكة الهاتف المحمول أو الإنترنت، بينما يمكن لجهاز نقل البيانات عبر اهتزازات كابلات الألياف الضوئية أن يعمل في سرية أكبر. ويسهل زرع مثل هذا الجهاز أثناء تركيب معدات الشبكة، ويصعب اكتشافه باستخدام أدوات الكشف التقليدية عن أجهزة التنصت.

ومن أهم مزايا هذا الهجوم الافتراضي إمكانية إجراء التنصت على بُعد كيلومترات من الغرفة المستهدفة، ما يُجنّب المهاجم تعريض نفسه لمخاطر إضافية بالتواجد بالقرب من الهدف. نظريًا، يُمكن أيضًا تخيّل سيناريو يتم فيه مدّ كابل ألياف ضوئية منفصل إلى غرفة مخصصة للمراقبة فقط، دون إثارة شكوك تُذكر لدى من تتم مراقبتهم.

في النهاية: هل يستطيع المهاجمون التجسس عن بُعد على أي مكان مزود بكابلات ألياف ضوئية؟، الإجابة: لا؛ إذ لا يزال ذلك مستحيلاً. مع ذلك، يُظهر البحث الذي أجراه باحثون من هونج كونج، والذي يُسلط الضوء على خصائص وسيط نقل البيانات الشائع، سيناريو ممكنًا تقنيًا- وإن كان غير مرجح ومكلفًا للغاية للتنفيذ- لهجوم مُستهدف.