فيسبوك تكتشف ارتباط قراصنة مشهورين بشركة فيتنامية

السبت 12 ديسمبر 2020 09:12 م

وجد محققو الأمن السيبراني في شركة فيسبوك أن مجموعة للقرصنة يُشتبه منذ مدة طويلة في أنها تتجسس نيابة عن الحكومة الفيتنامية ترتبط بشركة لتقنية المعلومات في مدينة (هو تشي مينه).

ويعد إعلان فيسبوك يوم الجمعة هو الأول من الشركة عن عملية قرصنة هجومية، وإن أُكّدَتْ، فستكون حالة نادرة من الجواسيس السيبرانيين المدعومين حكوميًا، والذين يتبعون منظمة معينة.

ويُتَّهم القراصنة – المعروفون باسم OceanLotus، أو APT32 – لسنوات بالتجسس على المعارضين السياسيين، والشركات، والمسؤولين الأجانب. وكانت وكالة رويترز قد ذكرت في وقت سابق من العام الحالي أن المجموعة حاولت اختراق وزارة إدارة الطوارئ الصينية، وحكومة ووهان عندما بدأ فيروس (كوفيد-19) COVID-19 بالانتشار.

وقالت شركة فيسبوك: إنها وجدت روابط بين هجمات إلكترونية نُسبت سابقًا إلى OceanLotus وشركة فيتنامية تُدعى CyberOne Group في مدنية (هو تشي مينه). ونفت شركة CyberOne صلتها بالقراصنة.

وقال شخص يدير صفحة الشركة على فيسبوك التي عُلّقت الآن، لوكالة رويترز: "لا علاقة لنا بشركة OceanLotus". وأضاف: "أنتم مخطئون".

وقالت فيسبوك: إن القراصنة استخدموا منصاتها لتنفيذ مجموعة من الهجمات الإلكترونية، التي استخدم بعضها حسابات مزيفة لخداع أهداف من خلال التظاهر بأنهم ناشطون، وشركات، وأشخاص معجبون.

وقال (ناثانيال جلايشر) – رئيس سياسة الأمن السيبراني في فيسبوك: إن فريقه وجد أدلة فنية تربط صفحة CyberOne في فيسبوك بالحسابات المستخدمة في حملة القرصنة، بالإضافة إلى هجمات OceanLotus الأخرى.

ورفض الإفصاح عن الأدلة الدقيقة، قائلًا: إن فعل ذلك سيجعل تعقب المجموعة أصعب في المستقبل. ولكنه قال: إنها تشمل البنية التحتية على الإنترنت، والشفرات الخبيثة، وأدوات القرصنة الأخرى وتقنياتها.

وقال جليشر: "يستخدم الممثلون في هذا الفضاء بعض التقنيات المحددة للغاية، وإن نحن كشفنا عن كيفية ملاحظتنا لها، فإن ذلك سيضر حقًا بقدرتنا على اكتشاف المزيد من تلك التقنيات".

وكانت مجموعة OceanLotus شديدة النشاط في دول جنوب شرق آسيا، مع أنها لم تكن ذائعة الصيت في الغرب، على غرار بعض عمليات القرصنة الصينية، والروسية المشتبه بها والمدعومة حكوميًا.

وقالت فيسبوك: إنها لا تمتلك أدلة كافية تجعلها تنسب OceanLotus إلى غير شركة CyberOne، التي قالت: إنها استخدمت أيضًا أسماء أخرى، مثل: CyberOne Security، و CyberOne Technologies، و Hành Tinh Company Limited، و Planet، و Diacauso.

ولا تكشف شركة CyberOne إلا القليل من المعلومات عن نفسها على موقعها على الإنترنت، مكتفية بالقول: إن لديها نحو 200 موظف يقدمون مجموعة من "تقنيات الأمان الأساسية".