# غوغل تكشف أداة تجسس روسية متقدمة تُهدد حكومات وصحفيين

كشفت شركة غوغل عن أداة تجسس سيبرانية جديدة تُعرف باسم "LostKeys"، قالت إنها تُستخدم حاليًا من قبل مجموعة قرصنة روسية تُعرف باسم COLDRIVER.

ووفقًا لتقرير فريق استخبارات التهديدات التابع لـ "غوغل" (GTIG)، فقد تم رصد البرنامج لأول مرة في يناير الماضي، حيث جرى توظيفه في عمليات تجسس إلكترونية معقدة تستهدف حكومات غربية وصحفيين ومراكز أبحاث ومنظمات غير حكومية، بحسب تقرير نشره موقع "androidheadlines".

وتستخدم مجموعة COLDRIVER برنامج LostKeys ضمن هجمات رقمية تُعرف باسم "ClickFix"، تعتمد بشكل كبير على الهندسة الاجتماعية لخداع الضحايا وتشغيل نصوص PowerShell مشبوهة، مما يفتح المجال أمام تحميل برامج خبيثة إضافية.

ويُوصف "LostKeys" بأنه "مكنسة رقمية" تستخرج ملفات بعينها من أجهزة الضحايا، بما في ذلك مستندات وبيانات مكتوبة بلغة Script Basic Visual، ثم ترسلها إلى المهاجمين.

وكما أنه يجمع معلومات النظام وينفذ أوامر عن بُعد.

مجموعة COLDRIVER، المعروفة أيضًا باسم Blizzard Star وGroup Callisto، تنشط منذ عام 2017، وتُتهم بتنفيذ عمليات قرصنة تستهدف وزارات الدفاع ومراكز حكومية ومنظمات غير ربحية في الغرب.

وسبق أن أكدت أجهزة استخبارات غربية، من ضمنها المملكة المتحدة وأعضاء تحالف "العيون الخمس"، أن:"المجموعة تعمل بتوجيه مباشر من جهاز الأمن الفيدرالي الروسي (FSB)".