الكشف عن اختراق أهداف حكومية وسياسية عراقية عبر شبكة تجسس ايرانية

كشفت شركة "مانديانت" التي تعود إلى شركة "غوغل" ،اليوم الجمعة، معلومات عن وحدة تجسس واختراق إيرانية، وأوضحت أنها رصدت مؤشرات حديثة عن هذه الشبكة عملت على أهداف حكومية وسياسية داخل العراق، مبينة أنها لها قدرة في الهندسة العكسية وقدرات التهرب من الكشف.

وقالت الشركة في تقرير تابعته وكالة "المطلع"، أن:"UNC1860 هي جهة تهديد دائمة ترعاها إيران ومن المرجح أنها تابعة لوزارة الاستخبارات والأمن الإيرانية".

وأضافت أن:"لهذه الشبكة مجموعة الأدوات المتخصصة والأبواب الخلفية السلبية التي تدعم العديد من الأهداف، بما في ذلك دورها كمزود وصول أولي محتمل وقدرتها على وصول مستمر إلى الشبكات ذات الأولوية العالية، مثل تلك الموجودة في مجال الحكومة والاتصالات في جميع أنحاء الشرق الأوسط".

ووصلت هذه المجموعة لعمليات تدميرية استهدفت إسرائيل في أواخر أكتوبر 2023 وألبانيا في عام 2022، فيما تحتفظ بترسانة من الأدوات المساعدة ومجموعة من الأبواب الخلفية السلبية المصممة للحصول على

موطئ قدم قوي في شبكات الضحايا وإنشاء وصول مستمر وطويل الأمد.

وأشارت إلى أن:"الشبكة لها قدرة في الهندسة العكسية وقدرات التهرب من الكشف، مايعني انها جهة تهديد هائلة من المرجح أن تدعم أهدافًا مختلفة تتراوح من التجسس إلى عمليات الهجوم على الشبكة، في عام 2020، شنت هجوما لإجراء عمليات مسح واستغلال إضافية ضد كيانات وقد لوحظ أن الفاعل يقوم بمسح عناوين IP تقع بشكل أساسي في السعودية في محاولة لتحديد الثغرات المكشوفة".

وبينت الشركة أنها:"استجابت للعديد من الاشتباكات في عامي 2019 و2020 حيث تعرضت المنظمات التي تعرضت للاختراق من قبل جهات يشتبه في أنها تابعة لـ APT34 للاختراق، وعلى نحو مماثل".

وحددت الشركة أيضًا مؤشرات حديثة على التحول العملياتي نحو أهداف مقرها العراق من قبل كل من المجموعات المرتبطة بـ APT34 و UNC1860

ويأتي هذا التقرير، بعد أشهر من تقرير مماثل تحدث عن شبكة باسم "APT42" ، وهي شبكة إيرانية أيضا قامت بانتحال صفة صحفيين واعلاميين للتواصل مع ضحاياها من كبار الشخصيات في الشرق الأوسط.