كاسبرسكي تطرح أداة لاكتشاف هجمات التجسس التي تستهدف هواتف آيفون

الخميس 8 يونيو 2023 03:26 م

بعد إصدار تقريرها عن هجمات حملة (عملية المثلثات) Operation Triangulation التي تستهدف الأجهزة التي تعمل بنظام iOS، طرح باحثو كاسبرسكي أداة خاصة جديدة تحمل اسم (triangle_check) لتتولى عملية البحث التلقائي عن أي حالات إصابة بالبرامج الخبيثة. وتتوفر الأداة للمستخدمين في خدمة GitHub، لتكون متاحة للأجهزة التي تعمل بأنظمة macOS و Windows و Linux.

وفي مطلع شهر يونيو الجاري 2023، أصدرت كاسبرسكي تقريرًا عن وجود نوع جديد من التهديدات المتقدمة المستمرة التي تستهدف الأجهزة المحمولة التي تعمل بنظام iOS. وتقوم هذه الحملة على عمليات الاستغلال من خلال هجمات النقرة الصفرية zero-click (أي إنها لا تستدعي القيام بأي نقرة) عبر خدمة المراسلة الفورية iMessage لتشغيل البرامج الخبيثة. ومن ثم يمكنها السيطرة الكاملة على بيانات الجهاز والمستخدم، بهدف التجسس الخفيّ على المستخدمين.

وكان من بين الضحايا عدد من موظفي كاسبرسكي، ومع ذلك، يستبعد باحثو الشركة أن يكون نطاق الهجوم قد اتسع إلى ما هو أبعد من ذلك. ويهدف باحثو الشركة من وراء مواصلة التحقيق إلى توفير المزيد من المعلومات حول الانتشار العالمي لهذا النوع من برامج التجسس.

وتضمّن التقرير الأولي بالفعل وصفًا تفصيليًا للتحقق الذاتي من آليات تتبع الاختراق باستخدام أداة MVT للمساعدة في تشخيص اختراق الأجهزة. وأصدرت كاسبرسكي عبر خدمة GitHub لتطوير البرامج، أداة مساعدة خاصة تسمى (triangle_check).

وتتيح هذه الأداة المتاحة للأجهزة التي تعمل بأنظمة macOS، و Windows، و Linux في Python، للمستخدمين البحث تلقائيًا عن آثار الإصابة بالبرامج الخبيثة، ومن ثم التحقق من احتمال تعرض أجهزتهم للإصابة.

ويجب على المستخدم أولًا عمل نسخة احتياطية للجهاز قبل تثبيت الأداة المساعدة. وحال الانتهاء من ذلك، يمكنه تثبيت الأداة وتشغيلها. وإذا تم الكشف عن مؤشرات تدلّ على الاختراق، ستعرض الأداة "إشعارًا" يفيد بالكشف عنه، لتأكيد إصابة الجهاز.

وإذا ظهرت رسالة "مُريب"، فإنها تشير إلى اكتشاف مؤشرات أقل وضوحًا، وتدل على إصابة محتملة. وستظهر رسالة "لم يتم التعرف على أي أثر لاختراق محتمل" إذا لم تُكتشف أي مؤشرات تدل على الاختراق.

وقال (إيغور كوزنيتسوف) رئيس وحدة أوروبا الشرقية والشرق الأوسط وأفريقيا في فريق البحث والتحليل العالمي لدى كاسبرسكي: "نفخر اليوم بإصدار أداة عامة مجانية تتيح للمستخدمين التحقق من كون أجهزتهم قد تعرضت للإصابة بأي من التهديدات المعقدة التي ظهرت حديثًا. ومن خلال الإمكانات الموجودة في الأنظمة الأساسية، تساعد أداة "triangle_check" المستخدمين في فحص أجهزتهم تلقائيًا. وينبغي على مجتمع الأمن السيبراني توحيد جهوده للبحث عن التهديدات المتقدمة المستمرة الجديدة، ليسهم الجميع في بناء عالم رقمي أكثر أمانًا".