الخليج

اقتصاد, تقنية وسيارات

2 يونيو 2023 15:37 مساء

«برامج خبيثة تستهدف أجهزة «آي أو إس» لموظفي «كاسبرسكي

دبي: «الخليج»

كشف باحثو «كاسبرسكي» عن حملة جديدة من التهديدات المتقدمة المستمرة تستهدف الأجهزة المحمولة تعمل بنظام وتحتوي على برامج خبيثة غير معروفة سابقاً. وتقوم الحملة التي يطلق عليها اسم «عملية طريقة «iOS «آي أو إس المثلثاث»، بتوزيع عمليات الاستغلال من خلال هجمات النقرة الصفرية (التي لا تستدعي القيام بأي نقرة) عبر خدمة المراسلة الفورية «آي مسج»، لتشغيل البرامج الخبيثة التي يمكنها السيطرة الكاملة على الجهاز وبيانات المستخدم، بهدف التجسس الخفي على المستخدمين.

وتمكن خبراء «كاسبرسكي» من الكشف عن الحملة الجديدة الموجهة للهواتف المحمولة في أثناء مراقبة حركة المرور .(KUMA) على شبكتها الخاصة «واي فاي»، باستخدام منصتها للمراقبة والتحليل الموحد المعروفة اختصاراً باسم «iOS وبعد إجراء المزيد من التحليل، اكتشف باحثو الشركة أن عامل التهديد كان يستهدف أجهزة «آي أو إس للعشرات من موظفي الشركة.

ولا يزال التحقيق في أسلوب الهجوم مستمراً، ولكن تمكن باحثو «كاسبرسكي» حتى الآن من تحديد التسلسل العام للعدوى. وتستقبل الضحية رسالة عبر خدمة «آي مسج»، مع ملف مرفق يحتوي على النقرة الصفرية. ومع أنه لم يتم أي

تفاعل إضافي، فقد تسببت الرسالة بحدوث ثغرة أمنية أدت إلى تنفيذ التعليمات البرمجية للحصول على المزيد من الامتيازات، كما أتاحت السيطرة الكاملة على الجهاز المصاب. وحال نجاح المهاجم في إثبات وجوده داخل الجهاز، يتم حذف تلك الرسالة بصورة تلقائية.

وعلاوة على ذلك، تمكنت برامج التجسس من نقل المعلومات الخاصة بهدوء إلى الخوادم البعيدة، بما في ذلك التسجيلات الصوتية والصور من برامج المراسلة الفورية، وتحديد الموقع الجغرافي، والبيانات المتعلقة بعدد الأنشطة الأخرى لمالك الجهاز المصاب.

لا تأثير في منتجات الشركة

وتم التأكد أثناء التحليل من عدم وجود أي تأثير في منتجات الشركة وتقنياتها وخدماتها، ولم تتأثر بيانات مستخدمي عملاء «كاسبرسكي»، أو العمليات المهمة للشركة. ويمكن للمهاجمين الوصول إلى البيانات المخزنة على الأجهزة المصابة فقط. ورغم عدم التأكد من ذلك، يُعتقد أن الهجوم لم يكن موجهاً على وجه التحديد إلى «كاسبرسكي»، علماً بأنها الشركة الأولى التي نجحت في اكتشاف هذا النوع من التهديدات. ومن المرجح أن تتوصل الشركة في الأيام التالية إلى المزيد من المعلومات حول مدى الانتشار العالمي لهذا الهجوم الإلكتروني.

وقال إيغور كوزنتسوف، رئيس وحدة أوروبا الشرقية والشرق الأوسط وإفريقيا في فريق البحث والتحليل العالمي لدى «كاسبرسكي»: «عندما يتعلق الأمر بالأمن السيبراني، يمكن اختراق أكثر أنظمة التشغيل أماناً، وبما أن العصابات السيبرانية التي تشن هجمات التهديدات المتقدمة المستمرة لا تتوقف عن تطوير طرقها وأساليبها والبحث عن المزيد من نقاط الضعف الجديدة لاستغلالها، سيكون من الضروري على الشركات إعطاء الأولوية لأمن أنظمتها. ويشمل هذا التركيز على تعليم الموظفين وتوعيتهم، وتزويدهم بأحدث معلومات التهديدات وأدواتها، للتعرف بشكل فعال إلى التهديدات المحتملة والحماية منها. وفي الوقت الذي نواصل فيه تحقيقنا في «عملية طريقة المثلثات»، نتوقع الكشف عن المزيد من التفاصيل حول هذه التهديدات قريباً، حيث يمكن أن تكون هناك أهداف أخرى لعملية التجسس هذه خارج نطاق كاسبرسكي».