كاسبرسكي: القراصنة يستغلون "أوفيس" لجمع المعلومات عن ضحايا مستقبليين لهجمات موجهة

الاثنين 25 سبتمبر 2017 06:09 م

اكتشف الخبراء العاملون لدى شركة كاسبرسكي لاب خاصية استغلها القراصنة في البرنامج الشهير الخاص بإعداد المستندات من أجل شن هجمات موجهة على الضحايا.

وأوضح خبراء عملاق أمن المعلومات الروسية أنه معلومات الجهاز والبرامج المحملة عليه تُرسل إلى القراصنة مباشرة باستخدام تطبيق خبيث يُفعَل عند فتح مستند "أوفيس" عادي في البرنامج، من دون تفاعل من طرف الضحية. وتساعد هذه المعلومات القراصنة في تحديد طبيعة الهجمات المستقبلية التي ينبغي تنفيذها لخرق الجهاز المستهدف.

وأضاف الخبراء أن طريقة الهجوم هذه تعمل على إصداري الحاسوب والمحمول من برنامج معالجة النصوص الشهير. وراقبت كاسبرسكي لاب هذه الطريقة في تعريف الضحايا التي لجأ إليها جاسوس رقمي واحد على الأقل، ودعاها باحثو الشركة "فريكي شلي". وتم إعلام مطوري البرنامج بهذه المشكلة لكن لم يجرِ تصحيحها بالكامل.

ورصد خبراء كاسبرسكي لاب، أثناء التحقيق في هجمات "فريكي شلي"، رسائل إلكترونية تدعي الموثوقية تحتوي ملفات من نوع OLE2، المبنية على تقنية ربط المكونات وتضمينها، والتي تساعد التطبيقات في إنشاء ملفات تركيبية تحتوي على معلومات من مصادر متعددة، منها الإنترنت.

ووفقًا للخبراء، لم يكن إلقاء نظرة سريعة على هذه الملفات كافيًا لإثارة الشكوك، إذ إنها احتوت على نصائح مفيدة عن الاستعمال الصحيح لمحرك البحث جوجل، ولم تحتوِ على أي استغلاليات أو برامج خبيثة معروفة، لكن التمعن في تصرفات هذه الملفات كشف عن تقديمها طلب GET الخاص بجلب المعلومات وإحضارها إلى صفحة خارجية متى ما فُتح الملف. واحتوى طلب المعلومات هذا على معلوماتٍ عن متصفح الإنترنت المثبت، وإصدار نظام التشغيل، وبعض المعلومات عن البرامج الأخرى المحملة على جهاز الضحية. وقد تمثلت المشكلة بأن الصفحة الخارجية ليس من المفترض أن يرسل إليها "أوفيس" أية معلومات.

ووضحت أبحاث كاسبرسكي لاب التالية أن هذه الهجمة تعتمد على كيفية معالجة معلومات محتويات الملف وتخزينها. ويحتوي كل ملف رقمي على بيانات وصفية لتصميم الملف، ومصدره ومكان النص، ومصادر الصور إن كانت موجودة، ومعلومات أخرى. وفي الحالات الطبيعية، يقرأ البرنامج هذه البيانات ويركب الملف بناءً عليها بمجرد أن يتم فتحه، باعتبارها "خريطة دلالية".

وأشارت نتائج تحقيق باحثي كاسبرسكي لاب، إلى أن بوسع القراصنة تعديل المعامل المسؤول عن تحديد مصادر الصور من خلال العبث ببرمجة الملف، بهدف جعله يرسل المعلومات المذكورة مسبقًا إلى موقعٍ يتحكم به مصدر التهديد.

واعتبر ألكساندر لسكن، مدير مجموعة الكشف الإرشادي لدى كاسبرسكي لاب، هذه الخاصية خطيرة بالرغم من أنها لا تتسبب بهجمات بحد ذاتها، بسبب ما قال إنه "دعمها لعمليات خبيثة ممكنة الحصول"، كونها لا تحتاج إلى التفاعل من قبل المستخدم، فضلًا عن قابليتها للانتشار حول العالم، نظرًا إلى شعبية البرنامج المستخدم وانتشاره الواسع، وقال: "رأينا حتى الآن مثالًا واحدًا فقط لاستعمال هذه الخاصية، لكننا نتوقع أن يُقدم مزيد من القراصنة على استغلالها في المستقبل، نظرًا إلى صعوبة اكتشافها".

ويقترح خبراء كاسبرسكي لاب على المستخدمين أمورًا تُجنبهم الوقوع ضحايا لهذه الهجمات، أولها الامتناع عن فتح الرسائل المرسلة من عناوين غير معروفة، وعدم فتح أي مرفقات فيها، إضافة إلى الاعتماد على حلول أمنية مثبتة قادرة على إيقاف هذه الهجمات، مثل حلول الحماية من كاسبرسكي لاب.