

## عصابة إنترنت تستهدف مؤسسات قانونية ومالية ووكالات سفر ببرمجية خبيثة جديدة



دبي: «الخليج»

التي تستخدمها عصابة Janicab استطاع خبراء كاسبرسكي تحديد نسخة ذات وظائف جديدة من البرمجية الخبيثة المختصة بالتهديدات المتقدمة المستمرة، للتسلل إلى مؤسسات معينة في عدة قطاعات. ورُصدت DeathStalker النسخة الجديدة في مناطق في أوروبا والشرق الأوسط، ووجد أنها تستغل بعض خدمات الويب الرسمية، مثل يوتيوب، ضمن سلسلة الإصابات.

مثلاً، إلى تحديات لوجستية وقانونية مستهدفة، وتحسين مكانة Janicab ويمكن أن تؤدي الإصابات بالبرمجية المنافسين، وعمليات تدقيق مفاجئة قد تكشف عن تحيزات وإساءات في استخدام الملكية الفكرية، ما يجعل أضرارها تختلف عن الأضرار التقليدية الناجمة عن هجمات من قبيل الابتزاز الرقمي أو الفدية.

برمجية خبيثة معيارية مكتوبة بلغة مفسرة، ما يعني أن الجهة التخريبية قادرة على إضافة Janicab يمكن اعتبار Janicab الوظائف أو تضمين الملفات، أو إزالتها، بجهد ضئيل. وتبين من قراءات كاسبرسكي الواردة عن بُعد أن نسخ

الأحدث قد شهدت تغيّرات ملموسة في بنيتها الهيكلية، مع وجود نسخ أرشيفية تحتوي على العديد من الملفات المكتوبة وغيرها من القطع المستخدمة لاحقاً في عملية الاختراق؛ وذلك على الرغم من أن آلية التوصيل لا تزال Python بلغة قائمة على التصيّد. بمجرد أن يتمّ خداع الضحية وفتح الملف الخبيث، يجري بالتتابع تحميل سلسلة من الملفات الخبيثة على النظام.

أو خدمات الويب، لاستضافة DDR في استخدامها لخدمات DeathStalker وتتمثل إحدى السمات المميّزة لبرمجية سلسلة مشفرة يُفكّ تشفيرها لاحقاً بغرسة من البرمجيات الخبيثة. ووفقاً لتقرير جديد، استطاعت كاسبرسكي تحديد استخدام روابط يوتيوب قديمة كانت موجودة في عمليات اقتحام تمّت في عام 2021. وكانت العصابة قادرة على العمل بسرية وتكرار استخدام بنيتها الخاصة بالقيادة والسيطرة، نظراً لصعوبة العثور على روابط الويب غير المدرجة

#### • غير مدرجة استُخدمت في عمليات اختراق حديثة YouTube عيّنة

في الأساس، على DeathStalker واشتملت المؤسسات المتأثرة التي وقعت ضمن المجال التقليدي للعصابة مؤسسات قانونية ومالية واستثمارية. لكن كاسبرسكي سجلت أيضاً نشاطاً استهدف وكالات السفر. واعتُبرت أوروبا والشرق الأوسط من مناطق العمل المثالية للعصابة، ولكن بدرجات متفاوتة بين دول المنطقتين. وقال الدكتور أمين حاسبيني رئيس مركز الأبحاث لمنطقة الشرق الأوسط وتركيا وإفريقيا في فريق البحث والتحليل تتمثل في سرقة DeathStalker العالمي لدى كاسبرسكي، إن بالإمكان الافتراض بأمان، بأن الأهداف الرئيسية لعصابة المعلومات السرية الخاصة بالنزاعات القانونية المتعلقة بكبار الشخصيات وبالأصول المالية الكبيرة، فضلاً عن المعلومات التجارية التي تمسّ التنافسية، والمعلومات حول عمليات الدمج والاستحواذ؛ وذلك بالنظر إلى أن المؤسسات القانونية والمالية «هدف مشترك لهذه العصابة». وأضاف: «يجب على المؤسسات العاملة في هذه القطاعات الاستعداد لمثل حالات الاختراق هذه، وتحديث نماذجها الخاصة بالتهديدات، لضمان بقاء البيانات آمنة». وينبغي للمؤسسات المتأثرة أن تعتمد على القوائم البيضاء للتطبيقات، وتدعيم أنظمة التشغيل، باعتبارها أساليب فعّالة لمنع محاولات الاقتحام؛ وذلك نظراً لاستمرار العصابة في استخدام برمجيات خبيثة مستندة إلى لغة مفسّرة، مثل في محاولات الاختراق الحديثة. كذلك على جهات الحماية أن تبحث أيضاً عن إجراءات VBS و VBE و Python يستخدم Janicab التي تعمل من دون واجهة مستخدم، نظراً لأن Internet Explorer المتصفح إنترنت إكسبلورر المتصفح في الوضع المخفي للتواصل مع البنية الأساسية للقيادة والسيطرة