الخليج

اقتصاد, أسواق عالمية

29 مايو 2023 16:01 مساء

كاسبرسكي» تكشف عن عصابة سيبرانية تتجسس على الكيانات الدبلوماسية» في الشرق الأوسط وجنوب آسيا

دبي: «الخليج»

أعلنت «كاسبرسكي» عن اكتشاف عصابة جديدة من مجرمي الإنترنت تحمل اسم «غولدن جاكال»، تبيَّن أنها تنشط منذ عام 2019، لكنها لا تحمل ملفاً تعريفياً عاماً، بقيت تعمل خلف الكواليس. وبناءً على المعطيات التي خرج بها التحقيق، فقد تبين أن «هذه العصابة تستهدف عادة الكيانات الحكومية والدبلوماسية في الشرق الأوسط وجنوب آسيا».

وبدأت «كاسبرسكي» بمراقبة هذه العصابة في منتصف عام 2020، ولاحظت أنشطة بانتظام، بعد أن تبيّن لها وجود جهة فاعلة قادرة على التخفي بشكل دائم. ومن أهم هذه الميزات التي تتسم بها العصابة، استخدام مجموعة أدوات محددة تركز على التحكم في أجهزة ضحاياها، والانتشار عبر الأنظمة باستخدام محركات أقراص قابلة للإزالة، إضافة إلى تهريب ملفات معينة منهم، في إشارة قاطعة إلى أن التجسس هو المهمة الأساسية التي تقوم بها.

وأظهر تحقيق «كاسبرسكي» أن العصابة تستخدم أدوات تثبيت وهمية لبرنامج الاتصال «سكايب»، إضافة إلى وثائق خبيثة بنسق «وورد» كنواقل أولية لهجماتهم. وكانت أدوات تثبيت «سكايب» الزائفة عبارة عن ملف قابل للتنفيذ يبلغ

حجمه 400 ميغابايت تقريباً. أما الملف فهو عبارة عن برنامج مساعد صغير الحجم يحتوي على مصدرين، وهما: تروجان يحمل اسم «جاكال كونترول»، إضافة إلى مثبت سكايب مستقل للأعمال التجارية. وتم تتبع أول استخدام لهذه الأداة حتى عام 2020، بينما كان ناقل العدوى الآخر عبارة عن مستند خبيث يستخدم تقنية الحقن عن بُعد لتنزيل Follina خبيثة، ويستغل ثغرة تسمى «فولينا «HTML» صفحة».

الصفحة الأولى من المستند الضار

وأطلق على المستند اسم «مستند معرض الضباط الذين حصلوا على جوائز وطنية وأجنبية». ويظهر كنشرة معتمدة تطلب معلومات حول الضباط الذين تم تكريمهم من قبل الحكومة الباكستانية. وتم نشر أول وصف لثغرة «فولينا» في 29 مايو/أيار 2022، ويبدو أن هذا المستند قد تم تعديله في 1 يونيو/حزيران، أي بعد يومين من النشر، واكتشف لأول مرة في 2 يونيو/حزيران.

وتم إنشاء المستند لتحميل ملف خارجي من موقع إلكتروني شرعي ولكنه مخترق. وحال إتمام تحميل ذلك الملف القابل للتنفيذ، يتم تشغيله؛ حيث يحتوي على برنامج خبيث من تروجان «جاكال كونترول».

ويسمح تروجان الرئيسي «جاكال كونترول» للمهاجمين بالتحكم في الجهاز المستهدف عن بعد، ويوظفون في هذه العملية مجموعة من الأوامر المحددة والمدعومة مسبقاً. وقام المهاجمون على مر السنين بتوزيع أنواع مختلفة من هذه البرامج الخبيثة؛ إذ يتضمن بعضها رمزاً للحفاظ على الثبات، بينما تم إنشاء البعض الآخر لغرض التشغيل من دون إصابة النظام. وعادةً ما يصاب الجهاز بمكونات أخرى، مثل برنامج حزمة النص.

وتوجد هناك أداة مهمة ثانية تستخدمها عصابة «غولدن جاكال»، وهي «جاكال ستيل» التي يمكن استخدامها لمراقبة محركات الأقراص «يو إس بي» القابلة للإزالة والمشاركة عن بُعد، إضافة إلى جميع محركات الأقراص المنطقية في النظام المستهدف. ويمكن أن تعمل البرامج الخبيثة كعملية قياسية أو كخدمة، وبما أنها لا تتمكن من الحفاظ على الثبات، يستدعى الأمر الاستعانة بمكون آخر من أجل تثبيتها.

أدوات إضافية

وتستخدم «غولدن جاكل» أيضاً عدداً من الأدوات الإضافية، ومنها «جاكل ورم» و«جاكل بيرانفو» و«جاكل سكرين واتشر»؛ حيث تقوم بنشرها في حالات محددة تمكّن باحثو «كاسبرسكي» من رصدها، وتهدف تحديداً إلى التحكم في أجهزة الضحايا، وسرقة بيانات اعتمادهم، وتصوير لقطات لسطح المكتب وما إلى ذلك، بينما يبقى التجسس الهدف النهائي لهذه العصابة.

ويقول جيامباولو ديدولا، باحث أمني أول في فريق البحث والتحليل العالمي لدى كاسبرسكي: «تعد عصابة غولدن جاكال، مثيرة للاهتمام في مجال التهديدات المتقدمة المستمرة، ومحاولاتها الابتعاد عن الأنظار. وعلى الرغم من اكتشاف أول عملية لها في يونيو/حزيران 2019، فإنها نجحت في التخفي. ونظراً لامتلاكها مجموعة أدوات برامج خبيثة متقدمة، تمكنت من شن هجمات على الكيانات الحكومية والدبلوماسية في الشرق الأوسط وجنوب آسيا. ولا تزال بعض عمليات زرع البرامج الخبيثة في مراحل التطوير، الأمر الذي يحتّم على فرق الأمن السيبراني البقاء على يقظة تامة من أي هجمات محتملة قد تقوم بها هذه العصابة، ونأمل أن يساعد تحليلنا على منع نشاطها».

إجراءات حماية

ولتفادي مخاطر الهجمات المستهدفة التي تشنها جهات تهديد معروفة أو غير معروفة، يوصي باحثو «كاسبرسكي» باتباع الإجراءات التالية:

تزويد فريق مركز العمليات الأمنية بإمكانية الوصول إلى أحدث معلومات التهديدات. وتعد بوابة استخبارات التهديدات من كاسبرسكي إحدى المواقع المناسبة للحصول على هذه المعلومات؛ حيث توفر البيانات المتعلقة بالهجمات الإلكترونية والأفكار التي جمعتها كاسبرسكي على مدار 20 عاماً.

الارتقاء بمهارات فريق الأمن السيبراني للتعامل مع أحدث التهديدات المستهدفة، من خلال الأنشطة التدريبية التي توفرها «كاسبرسكي» عبر الإنترنت والتي تم تطويرها من قبل خبراء فريق البحث والتحليل العالمي.
تطبيق حلول اكتشاف نقاط النهاية والاستجابة لها، مثل برنامج كاسبرسكي إندبوينت ديتكشين والاستجابة للمساعدة على اكتشاف مستوى نقطة النهاية، والتحقيق في الحوادث في الوقت المناسب ومعالجتها. إلى جانب اعتماد حلول حماية نقاط النهاية الأساسية، وينصح بتطبيق حل آمن على مستوى الشركات للكشف عن التهديدات المتقدمة على مستوى الشبكة في مرحلة مبكرة، مثل منصة كاسبرسكي المضادة للهجوم المستهدف.
وبما أن العديد من الهجمات المستهدفة، تبدأ بالتصيد الاحتيالي أو تقنيات الهندسة الاجتماعية الأخرى، يُنصح بتوفير تدريبات التوعية الأمنية وعلم المهارات العملية لفريقك، ومنها على سبيل المثال، منصة كاسبرسكي للتوعية الأمنية التلقائية.