

## كاسبرسكي: ارتفاع هجمات برامج التجسس في الشرق الأوسط 11.8% في بداية 2023



دبي: «الخليج»

أشار تقرير جديد صادر عن «كاسبرسكي»، إلى أن «نسبة المستخدمين الذين تمت مهاجمتهم ببرامج التجسس في الشرق الأوسط، ارتفعت بنسبة 11.8% في بداية 2023، من الربع الأخير 2022 إلى الربع الأول 2023. وأبلغت قطر عن زيادة في هجمات برامج التجسس بنسبة 23.8%، ومصر 22.7%، والإمارات العربية المتحدة 10.1%، والكويت 7.8% والسعودية 4.5%.

وبحسب التقرير، لا تزال برامج التجسس تشكل تهديداً لمستخدمي أنواع مختلفة من الأجهزة، بما في ذلك أجهزة العمل منخفضة الأداء. ويتم استخدام هذه الفئة من الأجهزة في شبكات الشركات حول العالم، لإعداد مساحات عمل بكلفة أقل بكثير مما هي عليه عند استخدام أجهزة الكمبيوتر المحمولة أو أجهزة سطح المكتب التقليدية (أجهزة العمل كثيفة الأداء). ويمكن أن يكون جهاز العمل منخفض الأداء والمثبت على نظام تشغيل تقليدي، مثل «لينوكس» أو «ويندوز»، مستهدفاً بأنواع مختلفة من الهجمات، بما في ذلك برامج التجسس. وإذا تعرض للاختراق، يتم استخدامه نقطة دخول

إلى شبكة الشركة بأكملها، أو للحصول على البيانات السرية، والتحكم في الأجهزة الأخرى على الشبكة، وتشغيل البرامج الخبيثة.

نقاط الضعف

وبناءً على بيانات «كاسبرسكي»، يوجد هناك ما يزيد على 60 نقطة ضعف في هذه الأجهزة، ويمكن إساءة استغلالها من قبل مجرمي الإنترنت. واستجابة للتهديدات الإلكترونية المتقدمة، تروج كاسبرسكي لنهج المناعة السيبرانية.

بنية تحتية لأجهزة العميل منخفضة الأداء، بطريقة يمكن «Kaspersky Secure Remote Workspace» ويوفر حل إدارتها ووفق عملية تم إنشاؤها بالاعتماد على مبدأ التصميم الآمن، ونهج المناعة السيبرانية الذي يجعلها أكثر صموداً في مواجهة الهجمات الإلكترونية، مقارنة بأجهزة العميل التقليدية.

وإلى جانب «سينتيرم»، الشركة العالمية المنتجة لأجهزة العميل منخفضة الأداء، تنتج «كاسبرسكي» أول جهاز عميل من هذا النوع في العالم معزز بالمناعة السيبرانية، ولا يتطلب أدوات حماية إضافية من الفيروسات. ويكمن جوهر الحل المملوك للجهة المطورة. وتستبعد «microkernel» في نظام التشغيل «كاسبرسكي أو إس» من نوع «مايكروكرنل» أجهزة العميل منخفضة الأداء من كاسبرسكي إمكانية استغلال مجموعة واسعة من نقاط الضعف الشائعة في الأجهزة التقليدية الأخرى. وهناك مكون آخر من هذا الحل، وهو وحدة تحكم الإدارة الموحدة التي تحل مشكلة إدارة ومراقبة البنية التحتية لجهاز العميل منخفض الأداء.

المناعة السيبرانية

وقال فيكتور إيفانوفسكي، رئيس تطوير الأعمال في نظام التشغيل «كاسبرسكي أو إس»: «لقد اكتسبت أجهزة العميل منخفضة الأداء إقبالاً عالياً خلال السنوات الماضية، خاصة بعد الجائحة، حيث كانت الشركات تبحث عن طرق فعالة من حيث التكلفة لإنشاء أماكن عمل عن بعد، ويعتقد الكثيرون أيضاً أنها آمنة للاستخدام، وأقل عرضة للبرامج الخبيثة من الأجهزة التقليدية».

وتابع: «ومع ذلك، فإن هذا الاعتقاد ليس أكثر من خرافة، فأجهزة العميل منخفضة الأداء التي تقوم بتشغيل أنظمة تقليدية تكون عرضة للخطر، ويظهر بحثنا الداخلي أنه يمكن اختراقها بأداة بسيطة في أقل من 10 دقائق، واستخدامها للتجسس على المستخدمين، والحصول على البيانات السرية».

وأضاف: «نعتقد أن مستقبل تطوير أجهزة العميل منخفضة الأداء يجب أن تحدده المناعة السيبرانية، وتكون الهجمات التي تستهدف نظاماً معززاً بالمناعة السيبرانية غير فعالة، لأنها قادرة على مواصلة العمل حتى في البيئة العدوانية، ويمكنها منع هجمات المهاجمين المحتملين».