قال باحثون في الأمن الإلكتروني وعملاء سابقون، إن وكالة الأمن القومي الأميركية توصلت إلى كيفية إخفاء برمجيات تجسس في أعماق محركات الأقراص الصلبة التي تنتجها شركات وسترن ديجيتال وسيجيت وتوشيبا وغيرها من كبار المصنعين، مما وفر للوكالة الوسائل للتجسس على أغلبية أجهزة الكمبيوتر في العالم.

وكانت هذه المقدرة المنشودة منذ وقت طويل والتي تخضع لحراسة مشددة جزءا من مجموعة برامج تجسس اكتشفتها شركة كاسبرسكي لاب لأمن البرمجيات ومقرها موسكو، والتي كشفت سلسلة من عمليات التجسس الإلكتروني الغربية.

وقالت كاسبرسكي إنها اكتشفت أن أجهزة الكمبيوتر الشخصي في 30 دولة مصابة ببرنامج تجسس واحد على الأقل.

وحدثت أغلب الإصابات في إيران، تليها روسيا وباكستان وأفغانستان والصين ومالي وسوريا واليمن والجزائر.

وتشمل الأهداف منشآت حكومية وعسكرية وشركات اتصالات وبنوكا وشركات طاقة وباحثين نوويين ووسائل إعلام ونشطاء متشددين.

ورفضت الشركة الكشف عن اسم الدولة التي تقف وراء حملة التجسس، لكنها قالت إنها على صلة وثيقة مع السلاح الإلكتروني ستوكسنت الذي تتحكم فيه وكالة الأمن القومي الأميركية واستخدم في مهاجمة منشأة إيرانية لتخصيب اليورانيوم.

والوكالة مسؤولة عن جمع معلومات المخابرات الإلكترونية لحساب الولايات المتحدة.

وقال موظف سابق في الوكالة لرويترز إن تحليل كاسبرسكي صحيح، وإن الناس الذين مازالوا يعملون في وكالة التجسس يعطون قيمة كبيرة لهذه البرامج التجسسية على نفس قدر ستوكسنت.

وأكد ضابط مخابرات سابق آخر أن الوكالة طورت التقنية المرغوبة لإخفاء برمجيات التجسس في محركات الأقراص الصلبة، لكنه قال إنه لا يعرف جهود التجسس التي تعتمد عليها.

ورفضت المتحدثة باسم وكالة الأمن القومي الأميركية فاني فاينز التعليق.

"صقور الصحراء" العربية تخترق مؤسسات إعلامية وحكومية حساسة

تمكنت شركة تعمل في مجال أمن تقنية المعلومات من اكتشاف ما يعرف بحملة "صقور الصحراء"، وهي مجموعة تجسس إلكتروني تستهدف العديد من المؤسسات البارزة والأفراد المرموقين من دول الشرق الأوسط.

وتعتبر هذه أول مجموعة عربية معروفة تقوم بتطوير وتشغيل عمليات تجسس إلكتروني واسعة النطاق، وقد تم البدء بتطويرها وتجهيزها في العام 1102، إلا أن العملية الرئيسية والإصابات الحقيقية انطلقت فعلياً في العام 2013.

ووصلت هذه العملية إلى ذروة نشاطها في مطلع العام 5102،

وبحسب شركة "كاسبرسكي لاب"، فان الغالبية العظمى للأهداف تتركز في مصر وفلسطين وإسرائيل والأردن إلى جانب دول الشرق الأوسط.

وقد تمكنت المجموعة من مهاجمة أكثر من 3,000 ضحية في أكثر من 50 بلداً حول العالم، وسرقة أكثر من مليون ملف.

ويلجأ "صقور الصحراء" لتسليم عدوى البرمجية الخبيثة عن طريق التصيد الاحتيالي عبر رسائل البريد الإلكتروني والمشاركات على مواقع التواصل الاجتماعي ورسائل الدردشة.

كما أنهم يستخدمون العديد من التقنيات لحث الضحايا على تشغيل الملفات الخبيثة.

ومن أكثر تلك التقنيات انتشاراً على وجه التحديد تقنية تعرف بخدعة "التحكم بتغيير اتجاه امتداد الملف من اليمين الى اليسار".

كاتب المقالة :
تاريخ النشر : 18/02/2015
من موقع : موقع الشيخ محمد فرج الأصفر
رابط الموقع : www.mohammdfarag.com