أخطر أدوات التجسس للبيع: كيف تم اختراق وكالة الأمن القومي الأمريكية؟

كتبه فريق التحرير | 17 أغسطس ,2016

ادعى قراصنة معلوماتية "هاكرز" إمكانية بيعهم لأنظمة اختراق وقرصنة إلكترونية متطورة أنشأتها وكالة الأمن القومي الأمريكية "NSA" بعد تسريب كيان مجهول لرمز حاسوب يستخدم في اختراق حواسب أخرى للعامة، مع خاصية تحميله لاستخدامهم الشخصي.

هذا وقد أكد العديد من الخبراء في مجال الأمن المعلوماتي وعلى رأسهم مؤسس شركة "Comae Technologies" لحماية الإنترنت مات سويتش أن رمز الحاسوب المسرب يشير أنه من أدوات "NSA".

كما زعمت المجموعة المسربة انتساب الحاسوب برمزه المسرب لكيان تجسس تابع لوكالة الأمن القومي الأمريكية، وجهات تجسس من أربع دول مختلفة، وهم أستراليا وكندا ونيوزيلندا وبريطانيا يسمون أنفسهم "Five Eyes".

أثارت العمليات التجسسية التي يتحدث عنها المسربون لغطًا كثيرًا، فيما دافع خبراء عن قانونية استخدام وكالة الأمن القومي الأمريكي لهذه الأدوات، مدعين أنها قد صممت للاستحواذ على أجهزة الراوتر وجدران الحماية الإلكترونية "firewall" بشكل قانوني، وأن الاستنتاج المنطقي الوحيد لنجاح هذه عملية التسريب بهذه الصورة، هو أن الرمز قد سرق من وكالة الأمن ذاتها أو أحد أعضاء حلف "Five Eyes" المصرح له باستخدام الرمز.

بينما وعدت المجموعة المسربة بإنشاء مزاد لبيع الأسلحة الإلكترونية، وهي ما تضاهي بيع صواريخ عسكرية للمدنيين.

قلق داخل الإدارة الأمريكية

ذكرت صحيفة نيويورك تايمز الأمريكية، أن الجماعة التي تطلق على نفسها "The Shadow Brokers" نشرت ما يبدو أنه رمز حاسوب يستخدم من قبل وكالة الأمن القومي لاختراق شبكات الحكومات الأجنبية، مما تسبب في قلق عميق بشأن احتمال تعرض تكتيكات الحرب الإلكترونية الأمريكية للقرصنة، بعد تأكيد معظم الخبراء الذين فحصوا المعلومات المنشورة المسربة، أنها تضم عينات حقيقة من أدوات الرمز المقصود، على الرغم من أن بعضها قديمة، وهي تستخدم في إنتاج

البرمجيات الخبيثة التي بنتها خصيصًا وكالة الأمن القومي الأمريكي.

حيث تم تصميم هذا الرمز لاختراق جدران حماية الشبكات والتسلل إلى أنظمة كمبيوتر الدول المنافسة مثل روسيا والصين وإيران، وهذا بدوره يسمح لوكالة الأمن القومي الأمريكي بزرع برنامج في أنظمة الشبكة المستهدفة، ويظل كامن لسنوات ويستخدم لمراقبة حركة المرور على الشبكة أو يمكن من خلاله شن هجوم إلكتروني عليها.

هل تقف روسيا خلف هذا الاختراق؟

وفقًا لخبراء فإن الترميز المسرب يحمل سلسلة من المنتجات عالية السرية التي طورتها وكالة الأمن القومي الأمريكي، وبعضها تم وصفه بعبارات عامة في الوثائق التي سربها قبل ثلاث سنوات إدوارد سنودن الموظف السابق بوكالة الأمن القومي، والذي يعيش حاليًا في روسيا.

ومع ذلك فإن رمز المعلومات التي نشرتها مجموعة القرصنة الأخيرة، لا تبدو أنها من أرشيف سنودن، إذ إن المعلومات التي سربها سنودن لا تحتوي على أي مصدر شفرة تستخدم لاقتحام شبكات القوى الأجنبية.

ومن جانبه لم يستبعد سنودن، الموظف السابق في وكالة الأمن القومي الأمريكية، إمكانية وقوف "أجهزة خاصة روسية" وراء المجموعة التي زعمت اختراقها لموقع الوكالة الأمريكية.

وحمل سنودن موظفي الوكالة الأمريكية مسؤولية ضياع ملفات معظمها عبارة عن أدوات اختراق، متهمًا إياهم بالتقاعس والإهمال.

تصريحات سنودن نقلتها وسائل إعلام روسية وعلى رأسها موقع سبوتنيك، الذي نقل تغريدات سنودن عبر موقع "تويتر"، والتي قال فيها إنها "دلائل غير مباشرة" تشير إلى إمكانية وقوف روسيا وراء الهجوم الإلكتروني على وكالة الأمن القومي الأمريكية، ورأى أن الهدف من الهجوم هو الحصول على ما يمكن المخترقين من إثبات مسؤولية الولايات المتحدة عن عدد من الهجمات الإلكترونية.

جدير بالذكر أن العملية تأتي بعد الإعلان عن تسريب رسائل بريد إلكتروني وملفات تعود لمسؤولين في الحزب الديمقراطي وكذلك الجمهوري، تم اختراقها بالفعل، فيما يعتقد متخصصون أمنيون أن الاختراق ربما تم لحساب روسيا تحديدًا.

أحدث برمجيات التجسس المتقدمة في العالم على المشاع

أشارت شركة كاسبرسكي لاب المتخصصة بالحماية والأمن إلى توفر معلومات عن استخدام مجموعة Equation السرية لبعض البرمجيات الخبيثة الأكثر تقدمًا، ومساعدتها في تطوير دودة الحواسيب الشهيرة "ستكسنت" Stuxnet.

وقالت المجموعة السرية في بيان نشرته على مدونتها بأنها ستقوم ببيع الأدوات والملفات لأعلى سعر ضمن مزاد، وأن هذه الملفات أفضل بكثير من دودة ستكسنت.

وتستهدف الأدوات كما شرح الخبراء، جدران الحماية التابعة لشركات مثل سيكسو Cisco وجونيبر

Juniper وفورتينت Fortinet والشركة الصينية Topsec بشكل محدد.

وأشارت إحدى شركات الحماية إلى احتواء إحدى عينات الملفات المعروضة للبيع على عنوان بروتوكول إنترنت IP مسجل من قِبل وزارة الدفاع الأمريكية.

ولا يعرف بعد الطريقة التي اتبعتها مجموعة Shadow Brokers للحصول على تلك الملفات والأدوات، ويشير أحد الاحتمالات إلى إمكانية قيامهم بعملية احتيال كبيرة، وهي طريقة شائعة جدًا في أوساط القرصنة.

وتطلب مجموعة Shadow Brokers من المشترين الدفع عن طريق العملة الرقمية "بيتكوين"، وعرضت الملفات والأدوات بشكل كامل مقابل مليون بيتكوين، أي ما يعادل 566 مليون دولار.

وتبدو معظم هذه الملفات حتى الآن عبارة عن أدوات اختراق، ورغم أنه من غير الواضح كمية المعلومات والملفات التي حصل عليها المخترقون، إلا أنه يبقى السؤال الأهم حول شرعية هذه البيانات، في ظل الطلب الكبير للأموال الذي قد يدل على زيف كثير من هذه المعلومات، وأنهم قاموا بنشر بعض الصور المثيرة للاهتمام ومن ثم عقد مزاد على Bitcoin لاستكمال المهمة دون أن يكون لديهم البيانات الدقيقة التي يتحدثون عنها.

وتعد وكالة الأمن القومي خيارًا منطقيًا للاستهداف نظرًا لأن هناك حد أدنى من المعلومات المعروفة حول Equation Group ولا تستطيع NSA أن تقوم بالتعليق بشكل علني على هذا الموضوع.

وفي حال ثبتت صحة هذه المعلومات فعملية الاختراق هذه ستكون واحدة من أهم عمليات الاختراق خلال سنوات، وهو ما جعل مجلة "فورين بوليسي" تصف عملية القرصنة الحالية بأنها قد تكون "تاريخية" مقارنة بخطورة الدور المكلفة الوكالة به، كما أضافت المجلة أن وكالة الأمن القومي لم ترد على استفسارها عن حقيقة الاختراق.