هاكر ايرانى محترف يخترق حملة ترامب البرلمانية ...وايران تنفى

الجمعة 23 أغسطس 2024 10:14 م

نقلا عن مجلة "رويترز" ، قال باحثون وخبراء يتابعون مجموعة الاختراق الإلكتروني الإيرانية التي اخترقت حملة المرشح الرئاسي الجمهوري دونالد ترامب إنها معروفة بوضع برامج مراقبة على الهواتف المحمولة لضحاياها مما يمكنهم من تسجيل المكالمات وسرقة الرسائل النصية وتشغيل الكاميرات والميكروفونات بصمت

ويعتقد على نطاق واسع أن القراصنة الإيرانيين المتهمين، الذين يُعرفون باسم APT42 أو CharmingKitten لدى مجتمع أبحاث الأمن السيبراني، مرتبطون بقسم استخباراتي داخل الجيش الإيراني، والمعروف باسم منظمة استخبارات الحرس الثوري الإسلامي أو IRGC-

وقال مصدر لرويترز إن ظهورهم في الانتخابات الأمريكية جدير بالملاحظة، بسبب نهجهم التجسسي الغازي ضد أهداف عالية القيمة في واشنطن وإسرائيل

قال جون هولتكويست، كبير المحللين في شركة الأمن السيبراني الأمريكية مانديانت، الذي أشار إلى أبحاث سابقة: "ما يجعل (APT42) خطيرة بشكل لا يصدق هو فكرة أنها منظمة لها تاريخ في استهداف الأشخاص المعنيين جسديًا"., يفتح علامة تبويب جديدةوقد كشفت التحقيقات أن المجموعة كانت تراقب الهواتف المحمولة للناشطين والمحتجين الإيرانيين وقد تعرض بعضهم للسجن أو التهديد الجسدي في البلاد بعد وقت قصير من اختراق هواتفهم

قال متحدث باسم البعثة الإيرانية الدائمة لدى الأمم المتحدة في نيويورك في رسالة بالبريد الإلكتروني إن "الحكومة الإيرانية لا تملك ولا تضمر أي نية أو دافع للتدخل في الانتخابات الرئاسية الأميركية".

وقال المتحدثون باسم ترامب إن إيران تستهدف الرئيس السابق والمرشح الجمهوري الحالي لأنهما لا يؤيدان سياساته تجاه طهران مستهدفة للغاية

لم يتم ذكر اسم طاقم APT42 الذي استهدف ترامب رسميًا في لوائح اتهام إنفاذ القانون الأمريكية أو التهم الجنائية، مما يترك تساؤلات حول هيكلهم وهويتهم لكن الخبراء يعتقدون أنهم يمثلون تهديدًا كبيرًا

قال ليفي جوندرت، كبير مسؤولي الأمن في شركة الاستخبارات الإلكترونية الأمريكية Recorded Future وعميل خاص سابق في الخدمة السرية: "إن جهاز الاستخبارات التابع للحرس الثوري الإيراني مكلف بجمع المعلومات الاستخباراتية للدفاع عن مصالح الجمهورية الإسلامية وتعزيزها وإلى جانب فيلق القدس، فإنهم أقوى كيانات الأمن والاستخبارات داخل إيران".

في شهر مارس، اكتشف محللو Recorded Future محاولات اختراق من قبل APT42 ضد مجموعة إعلامية مقرها الولايات المتحدة تدعى Iran International، والتي قالت السلطات البريطانية سابقًا إنها, يفتح علامة تبويب جديدةكانوا هدفا للعنف الجسدي, يفتح علامة تبويب جديدةوالتهديدات الإرهابية التي تشنها عناصر مرتبطة بإيران

قال هولتكويست إن المتسللين يستخدمون عادة برامج ضارة للهواتف المحمولة تسمح لهم "بتسجيل المكالمات الهاتفية، وتسجيلات الصوت في الغرف، وسرقة رسائل SMS (النصية)، وأخذ الصور من الجهاز"، وجمع بيانات الموقع الجغرافي

في الأشهر الأخيرة، أرسل مسؤولو حملة ترامب رسالة إلى الموظفين تحذرهم من توخي الحذر بشأن أمن المعلومات، وفقًا لشخص مطلع على الرسالة وقال الشخص، الذي طلب عدم الكشف عن هويته لأنه غير مسموح له بالتحدث إلى وسائل الإعلام، إن الرسالة حذرت من أن الهواتف المحمولة ليست أكثر أمانًا من الأجهزة الأخرى وتمثل نقطة ضعف مهمة

ولم تستجب حملة ترامب لطلب التعليق كما رفض مكتب التحقيقات الفيدرالي ومكتب مدير الاستخبارات الوطنية التعليق

ولم تجب الخدمة السرية على أسئلة حول ما إذا كان نشاط القرصنة الإيراني قد يكون مقصودًا لدعم الهجمات المادية المخطط لها في المستقبل وفي بيان أرسل إلى رويترز، قال متحدث باسم الخدمة السرية إنهم يعملون بشكل وثيق مع شركاء مجتمع الاستخبارات لضمان "أعلى مستوى من السلامة والأمن" ولكن لا يمكنهم مناقشة الأمور "المتعلقة بالمعلومات الاستخباراتية الوقائية".

كما تقوم مجموعة APT42 بشكل شائع بانتحال شخصية الصحفيين ومراكز الأبحاث في واشنطن في عمليات هندسة اجتماعية معقدة تعتمد على البريد الإلكتروني والتي تهدف إلى إغراء المستهدفين بفتح رسائل مفخخة، مما يسمح لهم بالاستيلاء على الأنظمة

وقال جوش ميلر، محلل التهديدات في شركة بروف بوينت لأمن البريد الإلكتروني، إن "حملات التصيد الاحتيالي التي تقوم بها المجموعة تستهدف بشكل كبير وتستند إلى أبحاث جيدة؛ وتستهدف المجموعة عادة عددًا صغيرًا من الأفراد". وغالبًا ما تستهدف نشطاء مناهضين لإيران، ومراسلين لديهم إمكانية الوصول إلى مصادر داخل إيران، وأكاديميين من الشرق الأوسط ومستشارين في السياسة الخارجية وشمل ذلك اختراق مسؤولين حكوميين غربيين ومقاولين دفاعيين أمريكيين

على سبيل المثال، في عام 2018، استهدف المتسللون العاملين في المجال النووي ومسؤولي وزارة الخزانة الأميركية في الوقت الذي انسحبت فيه الولايات المتحدة رسميا من خطة العمل الشاملة المشتركة، وفقا لما قاله أليسون ويكوف، المحلل البارز للاستخبارات السيبرانية في شركة الخدمات المهنية برايس ووتر هاوس كوبرز

بدأ ظهور APT42 علنًا في السباق الرئاسي الجاري في وقت سابق من هذا الشهر بعد تقرير, يفتح علامة تبويب جديدةبواسطة مايكروسوفت (MSFT.O), يفتح علامة تبويب جديدةفي 9 أغسطس/آب، قالت وكالة الأمن القومي الأمريكية إن المجموعة كانت تحاول اختراق حسابات موظفين في حملة رئاسية لم يتم الكشف عن اسمها

لا تزال مجموعة APT42 تستهدف بشكل نشط مسؤولي الحملة الانتخابية وشخصيات إدارة ترامب السابقة التي تنتقد إيران، وفقًا لمنشور على مدونة, يفتح علامة تبويب جديدةمن قبل فريق أبحاث الأمن السيبراني في Google.