"كانديرو" برنامج تجسس إسرائيلي استخدمته السعودية لإسكات المنتقدين

كشفت صحيفة "الجارديان" البريطانية، نقلا عن باحثين مقيمين في كندا عن وجود أدلة جديدة تشير إلى أن برنامج "كانديرو" الإسرائيلي يستخدم لاستهداف منتقدي الأنظمة الاستبدادية.

وقالت الصحيفة إن الباحثين وجدوا أدلة جديدة تشير إلى أن برامج التجسس التي صنعتها شركة إسرائيلية تم إدراجها مؤخرًا على القائمة السوداء في الولايات المتحدة، قد تم استخدامها لاستهداف منتقدي المملكة العربية السعودية والأنظمة الاستبدادية الأخرى. بما في ذلك بعض قراء موقع إخباري في لندن.

وأضافت الصحيفة أن التقرير الصادر عن الباحثين المقيمين في مونتريال من شركة Eset السلوفاكية، وهي شركة لأمن الإنترنت، كشف عن وجود روابط بين الهجمات ضد مواقع الويب البارزة في الشرق الأوسط والمملكة المتحدة، والشركة الإسرائيلية Candiru، التي أطلق عليها اسم "شركة الحرب الإلكترونية الأكثر غموضًا في إسرائيل" .

وتمت إضافة Candiru و Group NSO ، وهي شركة مراقبة إسرائيلية أكثر شهرة، إلى قائمة سوداء أمريكية هذا الشهر. بعد أن اتخذت إدارة بايدن خطوة نادرة باتهام الشركات بالعمل ضد مصالح الأمن القومي للولايات المتحدة.

هجمات حفر المياه:

وكشف تقرير شركة Eset عن معلومات جديدة حول ما يسمى "هجمات حفر المياه"، وهي إستراتيجية للهجوم على الكمبيوتر.

وفي مثل هذه الهجمات، يقوم مستخدمو برامج التجسس بإطلاق برامج ضارة ضد مواقع الويب العادية المعروفة بجذب القراء أو المستخدمين الذين يعتبرهم مستخدم البرامج الضارة "أهدافًا محل اهتمام".

وتسمح الهجمات المتطورة لمستخدم البرامج الضارة بتحديد خصائص الأفراد الذين زاروا الموقع . بما في ذلك نوع المتصفح ونظام التشغيل الذي يستخدمونه.

وفي بعض الحالات، يمكن لمستخدم البرامج الضارة إطلاق ثغرة تسمح لهم بالاستيلاء على كمبيوتر الهدف الفردي.

وعلى عكس برامج التجسس التي تحمل توقيع Group NSO، والتي تسمى بيغاسوس، والتي تصيب الهواتف المحمولة. يعتقد الباحثون أن برامج Candiru الضارة تصيب أجهزة الكمبيوتر.

ووجد الباحثون أن المواقع التي كانت "أهدافًا معروفة" لهذا النوع من الهجمات تشمل، موقع Middle East Eye ، وهو موقع إخباري في لندن.

إضافة إلى مواقع إلكترونية متعددة مرتبطة بوزارات حكومية في إيران واليمن.

وأدانت "ميدل إيست آي" الهجمات فيي بيان لها.

وقال رئيس تحرير الموقع، ديفيد هيرست ، إن المنفذ لم يكن غريباً عن محاولات القضاء على الموقع من قبل جهات حكومية وغير حكومية.

وأضاف: لقد تم إنفاق مبالغ طائلة من المال في محاولة لإخراجنا. هذا لم يمنعنا من الإبلاغ عما يجري في كل ركن من أركان المنطقة وأنا واثق من أنهم لن يوقفونا في المستقبل".

ويقول الباحثون في Eset إنه بمجرد اختراق مواقع الويب لا يكون كل فرد زار أحد مواقع الويب المخترقة معرضًا لخطر الاختراق.

ولكن يُعتقد أن مستخدمي البرامج الضارة قد استخدموا مواقع الويب كنقطة انطلاق للمساعدة في تحديد مجموعة أصغر بكثير من الأفراد الذين تعرضوا للاختراق ثم استهدفت.

استهداف موقع إلكتروني للسفارة الإيرانية في أبو ظبي:

من جانبه، قال ماتيو فو، الذي كشف الحملات، إن Eset طورت نظامًا داخليًا مخصصًا في عام 2018 للكشف عن "هجمات حفر المياه" على مواقع الويب البارزة.

وأوضح أنه في يوليو 2020 ، أبلغهم النظام أن موقعًا إلكترونيًا للسفارة الإيرانية في أبو ظبي ملوث بشفرة ضارة.

وقال "فاو": "أثار فضولنا الطبيعة البارزة للموقع المستهدف . وفي الأسابيع التالية لاحظنا أن المواقع الأخرى التي لها صلات بالشرق الأوسط قد تم استهدافها أيضًا".

أكدت شركة Eset على أن "جماعة التهديد" بعد ذلك "سكتت" حتى عادت إلى الظهور في يناير 2021. وظلت نشطة حتى أواخر صيف عام 2021. عندما تم "تنظيف" جميع المواقع التي لوحظ أنها كانت ضحية للهجمات.

وقالت الشركة إنها تعتقد أن أنشطة القرصنة انتهت في أواخر يوليو 2021. بعد تقرير صادر عن باحثين في Lab Citizen صدر بالاشتراك مع Microsoft . مفصلاً أنشطة المراقبة المزعومة لـ Candiru.

واتهم ذلك التقرير Candiru ببيع برامج تجسس لحكومات مرتبطة بمواقع الويب المزيفة لـ Lives Black الأهداف لاختراق استخدامها تم التي الدولية العفو منظمة ومواقع Matter.

وأشارت الصحيفة إلى أن هناك القليل من المعلومات العامة المتاحة حول Candiru، التي تأسست في عام 2014 وخضعت لعدة تغييرات في الأسماء.

زبائن في الخليج وأوروبا الغربية وآسيا :

ففي عام 2017 ، كانت الشركة تبيع برامجها الضارة لعملائها في الخليج وأوروبا الغربية وآسيا.

ووفقًا لدعوى قضائية نشرت في صحيفة إسرائيلية فإن كانديرو تعاملت مع أوزبكستان والمملكة العربية السعودية ودولة الإمارات العربية المتحدة .

وذكرت شركة مايكروسوفت أنها عثرت على ضحايا لبرامج التجسس في إسرائيل وإيران.

وتصدرت كانديرو عناوين الصحف هذا الشهر بعد أن أعلنت إدارة بايدن أنها أضافت الشركة إلى قائمة كيانات وزارة التجارة. وهي قائمة سوداء مخصصة عادة لأسوأ أعداء أمريكا . بما في ذلك المتسللين الصينيين والروس.

وقالت وزارة التجارة في بيانها الصحفي إن لديها أدلة على أن كانديرو طورت وقدمت برامج تجسس لحكومات أجنبية استخدمتها لاستهداف المسؤولين الحكوميين والصحفيين ورجال الأعمال والنشطاء والأكاديميين والعاملين بالسفارات.

وأكدت الوزارة على أن الأدوات ساعدت أيضًا في تمكين الحكومات الأجنبية من ممارسة "قمع عابر للحدود".