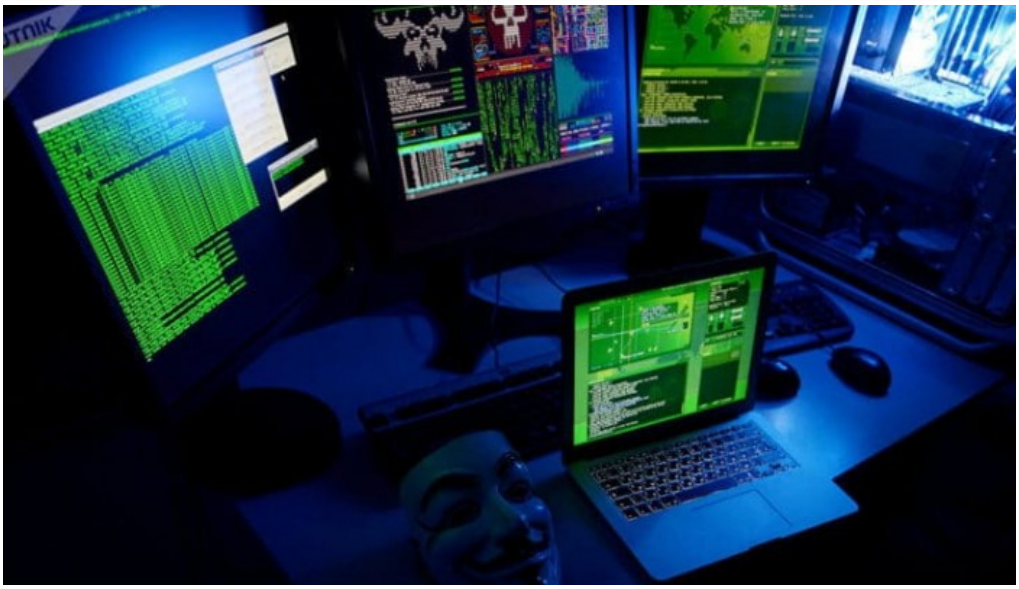
تحذيرات من اختراق الأقمار الصناعية واستخدامها كأسلحة



السبت 11 أغسطس 2018 10:08 م

تجمع آلاف المتسللين الأخلاقيين والباحثين الأمنيين في لاس فيغاس هذا الأسبوع لمعالجة بعض أكبر التهديدات المحتملة للأمن السيبراني، حيث كشف الباحثون خلال مؤتمر أمن المعلومات المسمى القبعات السوداء Black Hat عن كيفية استخدام المتسللين للاتصالات عبر الأقمار الصناعية من أجل شن هجمات سيبرانية وتحويل هوائيات تلك الأقمار الصناعية إلى أسلحة تعمل بشكل أساسي مثل أفران الميكروويف.

وأوضح الباحثون أن الاتصالات عبر الأقمار الصناعية المستخدمة من قبل الطائرات والسفن والجيش للاتصال بشبكة الإنترنت معرضة لخطر القرصنة، وأن التهديدات النظرية لم تعد كذلك، ووفقًا لبحث تم تقديمه في مؤتمر أمن المعلومات فإن عددًا من أنظمة الاتصالات عبر الأقمار الصناعية الشائعة عرضة للهجمات، والتي يمكنها أيضًا تسريب المعلومات واختراق الأجهزة المتصلة.

وتفيد الأبحاث أن الهجمات قادرة على تشكيل خطر حقيقي على سلامة المستخدمين العسكريين والبحريين والجويين، وحذر روبن سانتامارتا Ruben Santamarta، الباحث في شركة أمن المعلومات IOActive، في عرض قدمه يعتمد على أبحاث سابقة قدمها في عام 2014 من أن الاتصالات التي تستخدمها السفن والطائرات والجيش عرضة للقرصنة، وقال: "إن عواقب نقاط الضعف هذه صادمة، ولم تعد الحالات النظرية التي طورتها منذ أربع سنوات نظرية".

ويعمل الهجوم من خلال الاتصال بهوائيات تلك الأقمار الصناعية واستخدام نقاط ضعف أمنية في البرنامج الذي يشغل الهوائي، ويوفر الهجوم القدرة على تعطيل أو اعتراض أو تعديل جميع الاتصالات التي تمر عبر الهوائي، مما يسمح للمهاجمين بالتنصت على رسائل البريد الإلكتروني المرسلة من خلال الشبكة اللاسلكية على متن الطائرة أو شن هجمات قرصنة على الأجهزة المتصلة بشبكة القمر الصناعي.

كما يمكن قد تشكل هذه الهجمات خطرًا كبيرًا على السلامة في بعض الحالات المرتبطة بالجيش، حيث قد يكشف الهجوم عن موقع هوائي القمر الصناعي، وذلك نظرًا إلى أنه يحتاج إلى جهاز تحديد المواقع العالمي GPS مرفق للعمل، وأشار سانتامارتا أنه في حال تمكنت من تحديد موقع القاعدة العسكرية فإن هذا يشكل خطرًا على السلامة العامة، بخلاف الطائرة أو السفينة، والتي يكون موقعها الجغرافي محدد بشكل عام.

ويتعرض كل من المستخدمين العسكريين والبحريين لخطر ما وصفه سانتامارتا بالهجمات السيبرانية الجسدية، والتي تتجسد من خلال إعادة تحديد موضع الهوائي والتحكم به من أجل إطلاق هجمات الترددات الراديوية عالية الكثافة HIRF، وقال سانتامارتا: "نحن نحول أجهزة الاتصالات عبر الأقمار الصناعية إلى أسلحة ترددات لاسلكية، بحيث يتشابه هذا المبدأ مع مبدأ عمل أجهزة أفران الميكروويف، حيث يمكن لهجمات HIRF أن تسبب أضرارًا مادية للأنظمة الكهربائية.

وأوضح الخبير أن مخاطر السلامة ليست عالية بالنسبة لقطاع الطيران، لأنه يتم بناء الطائرات مع الأخذ بعين الاعتبار المعايير والتصاميم والاختبارات والتحصينات التي تحمي الطائرة وأنظمة الطيران التابعة لها باستخدام معدات الاتصالات عبر الأقمار الصناعية المحمولة جوًا من هجمات الترددات الراديوية عالية الكثافة HIRF، وعملت IOActive مع قطاع صناعة الطيران لضمان أن شركات الطيران المتضررة لا تعرض أساطيلها والركاب إلى مخاطر الإنترنت المفتوح.