الصين تصعد حربها الإلكترونية ضد الولايات المتحدة

الجمعة 22 يونيو 2018 03:06 م

وافقت الولايات المتحدة والصين في عام 2015 على هدنة رقمية حظرت على شركات القرصنة الخاصة سرقة الأسرار التجارية، وبالرغم من أن الاتفاق قد تم وصفه بأنه ناجح، إلا أنه لم يمنع المتطفلين الصينيين الذين ترعاهم الدولة من رفع حدة التصرفات غير المقبولة، وعلاوة على ذلك، فإنه من المؤكد أن الهدنة لم تبطئ من عمليات القرصنة التي تقع خارج نطاق الاتفاق، ويبدو في الآونة الأخيرة أن هذه التصرفات وصلت حد جمع المعلومات الدفاعية، وذلك مع قيام قراصنة الدولة في الصين بإعادة تنظيم أنفسهم خلال السنوات القليلة الماضية ليكونوا أكثر تخفيًا وفعالية في عمليات التجسس الرقمي

وتدل الهجمات الأخيرة على أنهم يقومون بتحسين خططهم للحصول على المعلومات الأكثر قيمة، حيث اخترق متسللون صينيون في الأسابيع الأخيرة مقاولاً تابعاً للبحرية الأمريكية يعمل لصالح مركز الحرب تحت سطح البحر، وسرقوا ما يصل إلى 614 جيجابايت من البيانات حول تكنولوجيا الأسلحة البحرية تحت سطح البحر، كما استهدفت الهجمات الصينية في الأشهر الأخيرة شركات التصوير بالأقمار الصناعية وشبكات الجغرافيا المكانية وشركات الاتصالات الأمريكية، وتسلط هذه الأحداث الضوء على حملات القرصنة السرية التي لا تتوقف والتي تتواصل بشكل مستمر بين الولايات المتحدة والصين

وقال ديفيد كينيدي David Kennedy، الرئيس التنفيذي لشركة تتبع التهديد Binary Defense Systems، والذي كان يعمل في السابق ضمن وكالة الأمن القومي NSA ومع وحدة استخبارات الإشارة التابعة لسلاح مشاة البحرية الأمريكية المارينز: "لقد تراجع النشاط الصيني بشكل كبير فيما يتعلق باختراق وسرقة معلومات وبيانات الملكية الفكرية، ولكن عندما يتعلق الأمر بالأسرار التجارية العسكرية والتأهب العسكري والاستعداد العسكري والاتصالات عبر الأقمار الصناعية وأي شيء ينطوي على قدرة الولايات المتحدة في الحفاظ على تفوقها التقني أو العسكري، فإن الصين تركز بشكل كبير على هذه الأهداف، كما أن الولايات المتحدة تفعل الشيء نفسه".

وتعكس عملية اختراق أجهزة الحواسيب الخاصة بمقاول تابع للبحرية الأمريكية U.S. Navy التركيز الصيني الكبير على سد أي فجوة تقنية أو عسكرية بينها وبين الولايات المتحدة، كما تم ضبط القراصنة الصينيين متورطين بهجمات خلال شهري يناير/كانون الثاني وفبراير/شباط لسرقة بيانات مهمة من شبكة غير سرية، حيث عند جمع البيانات معًا تمكنت الصين من الوصول إلى تصور كامل لأحدث تقنيات الولايات المتحدة في حربها تحت الماء، بالإضافة إلى تفاصيل حول عدد من الأنظمة الرقمية والميكانيكية ذات الصلة

وتتشابه الهجمات مع أنماط هجمات معروفة ومرتبطة بقراصنة صينيين، وكتب دانييل كوتس Daniel Coats، مدير المخابرات القومية الامريكية في تقرير تهديدات شهر فبراير/شباط "ستواصل الصين استخدام التجسس عبر الانترنت وتعزيز قدرات الهجمات الالكترونية لدعم أولوياتها في الامن القومي، ويستمر مجتمع المخابرات وخبراء الأمن ضمن القطاع الخاص في تحديد النشاط الإلكتروني المستمر من قبل الصين، حيث تركز معظم العمليات الإلكترونية الصينية على الصناعة الخاصة الأمريكية ومقاولي الدفاع أو شركات تكنولوجيا المعلومات والاتصالات".

ونشر محللون من شركة سيمانتيك Symantec هذا الأسبوع أبحاث حول سلسلة من الهجمات تعتمد نفس النمط تمت بين شهر نوفمبر/تشرين الثاني 2017 وشهر أبريل/نيسان 2018 من مجموعة قرصنة يطلق عليها اسم Thrip، وبالرغم من أن شركة سيمانتيك لا يمكنها إلى حد كبير تأكيد حصول هذه المجموعة على رعاية الدولة الصينية، لكنها تؤكد بثقة عالية أن هجمات Thrip تعود إلى أجهزة حاسب داخل الصين

وتطورت أساليب المجموعة، التي تتبعها سيمانتيك منذ عام 2013، عبر استخدام برمجيات خبيثة جاهزة للتسلل إلى الشبكات ومن ثم التحكم في الضوابط الإدارية وغيرها من أدوات الأنظمة للوصول إلى أماكن أعمق دون تعطيل أجهزة الإنذار، وساعدت هذه الأدوات والتقنيات الجاهزة في زيادة صعوبة تحديد وتتبع مجموعة Thrip، لكن سيمانتيك بدأت تلاحظ أنماطًا في أجهزة الكشف الخاصة بها قادت الباحثين إلى باب خلفي فريد من نوعه يثبت تورط Thrip.

ووجد الباحثون أدلة على وجود تدخلات في بعض شركات الاتصالات في جنوب شرق آسيا وشركة صور جغرافية مكانية أمريكية وشركتان من شركات الأقمار الصناعية الخاصة، بما في ذلك واحدة من الولايات المتحدة، ومتعهد دفاعي أمريكي، وكانت جميع الخروقات متعمدة وموجهة، إذ استخدم المخترقون في حالة شركات الأقمار الصناعية جميع الطرق الممكنة للوصول إلى أنظمة التحكم بالأقمار الصناعية المدارية الفعلية، بحيث كان من الممكن أن يؤثر هذا الاختراق على مسار القمر الصناعي أو تعطل تدفق البيانات

ويقول جون ديماجيو Jon DiMaggio، وهو كبير محللي استخبارات التهديد في شركة سيمانتيك، والذي قاد عمليات البحث خلف مجموعة Thrip: "إنه أمر مخيف، لقد ألقينا نظرة على الأنظمة التي كانوا مهتمين بها، وأين قضوا معظم الوقت، والأقمار الصناعية التي كانوا يحاولون التحكم بها والسيطرة عليها، كما أنهم كانوا يحاولون اختراق شركات الصور الجغرافية المكانية وشركات الاتصالات".

ويشير ديفيد كينيدي إلى أن عمليات الاختراق المتعلقة بجمع المعلومات قد تمثل أولوية لجميع الدول، ويمكن أحيانًا التساهل معها بشكل تبعًا لكونها متبادلة، إلا أنها قد تمثل بيانًا واضحًا عند وجود خلاف بين بلدين، ويوضح أنه ليس من المستغرب اكتشاف عمليات القرصنة الصينية المتصاعدة ضد الولايات المتحدة بسبب التوترات الجيوسياسية المتصاعدة بين البلدين حول التجارة وزيادة الرسوم الجمركية، حيث يمكن استخدام عمليات القرصنة كدليل على القوة في الكثير من الحالات