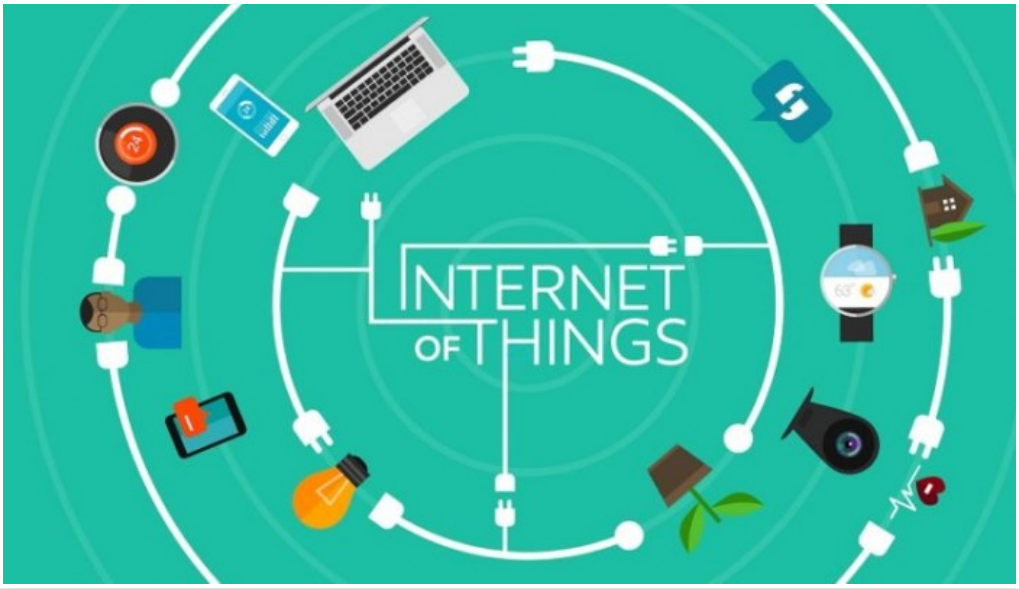
كاسبرسكي: عدد البرمجيات الخبيثة المستهدفة للأجهزة الذكية يقفز إلى أكثر من الضعف في 2017



الثلاثاء 4 يوليو 2017 11:07 م

خلصت دراسة قام بها باحثون في كاسبرسكي لاب إلى أن العدد الكلي لعينات البرمجيات الخبيثة المستهدفة للأجهزة الذكية قد ارتفع إلى أكثر من 7,000، وبأن أكثر من نصف هذا العدد قد سجل في عام 2017.

وبالنظر إلى أن عدد الأجهزة الذكية المستخدمة حول العالم حاليًا يتخطى حاجز الستة مليارات جهاز، يرى الباحثون أن هذا يعرض المزيد من الناس لمخاطر متنامية تتمثل في هجمات البرمجيات الخبيثة التي تستهدف أجهزتهم المتصلة بالإنترنت وحياتهم الرقمية ككل.

ويقول باحثو كاسبرسكي لاب لعله لم يعد خافيًا على أحد بأن جميع الأجهزة الذكية، كالساعات والتلفزيونات الذكية وأجهزة تنظيم حركة المرور بين الشبكات والكاميرات، متصلة ببعضها وتشكل مجتمعة ما يعرف بظاهرة إنترنت الأشياء IoT المتنامية، والتي هي عبارة عن شبكة من الأجهزة المزودة بتقنية داخلية تسمح لها بالتفاعل مع بعضها أو مع البيئة الخارجية المحيطة بها.

ونظرًا لوجود عدد هائل ومتنوع من الأجهزة، يرى الباحثون أن ظاهرة إنترنت الأشياء أصبحت هدفًا مغريًا لمجرمي الإنترنت. ومن خلال نجاحهم في اختراق أجهزة إنترنت الأشياء، يتمكن القراصنة من التجسس على الناس وابتزازهم، بل وجعلهم أيضًا شركاء لهم في الجريمة. والأسوأ من ذلك، وفقًا للباحثين، أن وجود شبكات Botnets التي تنطلق منها برمجيات خبيثة مثل Mirai وHajime ينذر بتفاقم تلك التهديدات الخطيرة.

وقد أجرى خبراء كاسبرسكي لاب دراسة بشأن البرمجيات الخبيثة المستهدفة لأجهزة إنترنت الأشياء لمعرفة مدى جدية تلك المخاطر. وفي هذا الإطار، قام الباحثون بنصب أفخاخ للقراصنة Honeypots، أي شبكات اصطناعية تحاكي الشبكات المشغلة لمختلف أجهزة إنترنت الأشياء (مثل أجهزة التوجيه الشبكي والكاميرات المتصلة وغيرها)، وذلك لمراقبة البرمجيات الخبيثة أثناء محاولة شن هجوم على الأجهزة الافتراضية. ولم يستدع الأمر منهم الانتظار طويلًا، إذ سرعان ما بدأت الهجمات التي تتم باستخدام عينات خبيثة معروفة وغير معروفة مسبقًا مباشرة بعد نصب تلك الأفخاخ.

ولوحظ أن معظم الهجمات المسجلة من قبل خبراء الشركة قد استهدفت مسجلات الفيديو الرقمية أو الكاميرات الرقمية المعتمدة على بروتوكول الإنترنت (63%) وكانت نسبة 20% من هذه الهجمات موجهة ضد أجهزة الشبكة، بما في ذلك أجهزة التوجيه والمودم DSL وغير ذلك. وشكلت الأجهزة الأكثر استخدامًا من قبل الأفراد، مثل الطابعات والأجهزة المنزلية الذكية، ما يقرب من نسبة 1% من الأهداف.

وبرزت الصين (17%) وفيتنام (15%) وروسيا (8%) من أكثر 3 دول تعرضت أجهزة إنترنت الأشياء فيها للهجمات، وتضم كلًا منها عددًا هائلًا من الأجهزة المصابة، تلتها البرازيل وتركيا وتايوان بنسبة كلية بلغت 7%.

وفي إطار هذه التجربة المستمرة، تمكن الباحثون حتى الآن من جمع معلومات حول أكثر من سبعة آلاف عينة لبرمجيات خبيثة مصممة خصيصا لاختراق الأجهزة المتصلة بالإنترنت.

ووفقًا لتحليلات الخبراء، فإن السبب الكامن وراء هذا الارتفاع يعود ببساطة إلى أن أجهزة إنترنت الأشياء غير محمية بالقدر الكافي وبإمكان مجرمي الإنترنت الوصول إليها بسهولة. ومن الملاحظ أيضًا أن معظم الأجهزة الذكية تعمل عن طريق أنظمة تشغيل قائمة على لينكس، مما يجعل شن الهجمات عليها مهمة أكثر سهولة نظرًا لأنه بإمكان المجرمين كتابة رمز تشفير برمجي عام يستهدف عددًا كبيرًا من الأجهزة في آن معًا.

إن ما يفاقم من خطورة هذا الأمر يتمثل في احتمال انتشاره على نطاق واسع. فقد أشار خبراء متخصصون في هذا القطاع إلى أنه يوجد حاليًا أكثر من 6 مليارات جهاز ذكي قيد الاستخدام حول العالم. ومعظم هذه الأجهزة لا تحتوي على حل أمني لحمايتها، ثم إن مصنعي الأجهزة لا يطرحون أي تحديثات أمنية أو نظام تشغيل جديد لها. وبالتالي، فهذا يشير إلى أن هناك الملايين من أجهزة إنترنت الأشياء التي من المحتمل تعرضها للاختراق، أو أنها مخترقة بالفعل.

وقال فلاديمير كوسكوف، خبير الأمن في كاسبرسكي لاب: "إن أمن الأجهزة الذكية يعد مسألة جدية ولا يمكن التهاون فيها، وينبغي علينا جميعًا أن نكون مدركين لأبعادها وتداعياتها. أظهرت نتائج العام السابق بأنه إلى جانب كون الأجهزة المتصلة معرضة للاختراق، فهي تنطوي أيضًا على تهديدات حقيقية وخطيرة".

وأضاف كوسكوف: "لقد شهدنا زيادة كبيرة في عينات البرمجيات الخبيثة المستهدفة لأجهزة إنترنت الأشياء، ولكن التهديدات والمخاطر المحتملة تبقى أكبر بكثير وعلى ما يبدو أن المنافسة المحتدمة في سوق هجمات DDoS تدفع المهاجمين للبحث عن مصادر جديدة من شأنها أن تساعدهم على شن هجمات أقوى وأعنف".

وتابع: "وأظهرت برمجية Mirai التي تنطلق من شبكة Botnet الخبيثة أن الأجهزة الذكية قد تمنح مجرمي الإنترنت ما يحقق لهم مآربهم، لا سيما من خلال عدد الأجهزة التي يمكنهم استهدافها والتي يصل عددها إلى بضعة مليارات حاليًا ويتوقع محللون أن ينمو هذا العدد ليتراوح بين 20-50 مليار جهاز بحلول العام 2020".

ولغرض حماية الأجهزة، يوصي خبراء كاسبرسكي لاب بعدم استخدام الجهاز، في حال لم يكن ضروريًا، عن طريق الاتصال بإحدى الشبكات الخارجية، وبضرورة إيقاف تفعيل كافة خدمات الشبكة التي لا يُحتاج إليها لاستخدام الجهاز، بالإضافة إلى أنه في حال كان هناك كلمة مرور رئيسية أو عالمية لا يمكن تغييرها، أو تعذر إيقاف تفعيل الحساب المضبوط مسبقا، يجب إيقاف تفعيل خدمات الشبكة التي يتم استخدام الأجهزة من خلالها أو القيام بحجب الاتصال بالشبكات الخارجية

وقبل استخدام الجهاز، يوصي الخبراء بتغيير كلمة المرور الافتراضية وضبط كلمة مرور جديدة، بالإضافة إلى ضرورة إجراء تحديث دوري لنظام تشغيل الجهاز وفقًا لأحدث نسخة، في حال أمكن ذلك