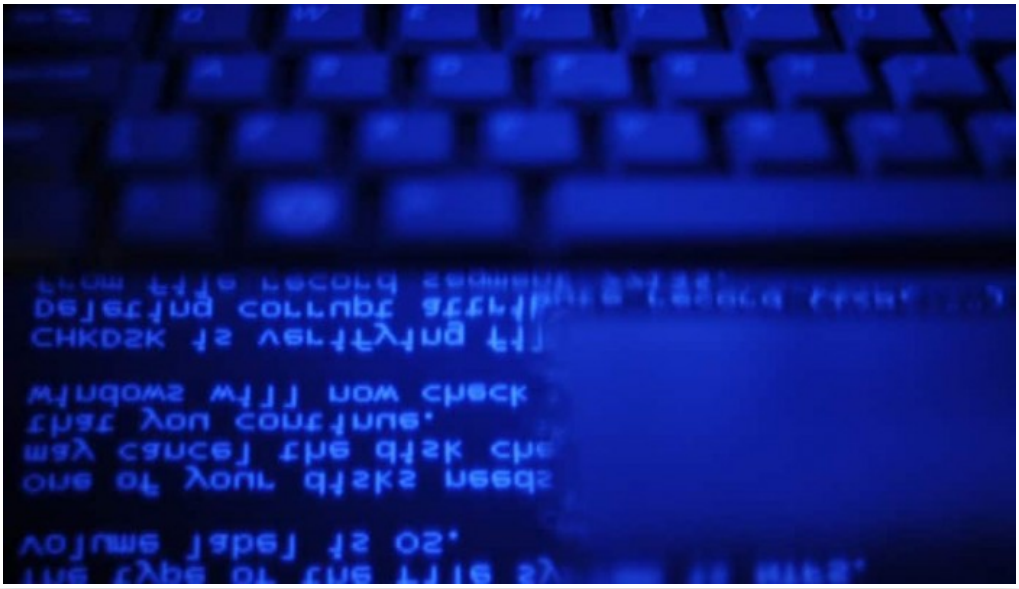
كاسبرسكي: قرصان بارع يستخدم شبكة بوتات على ويندوز لنشر برمجية ميراي الخبيثة



الخميس 23 فبراير 2017 07:02 م

يجري خبراء كاسبرسكي لاب حاليًا تحقيقات وتحليلات بشأن أول أداة من نوعها لنشر برمجية "ميراي" Mirai الخبيثة القائمة على نظام ويندوز وذلك في إطار جهودهم المكثفة للقضاء على شبكات التي تنطلق منها برمجية ميراي الخبيثة.

وتوصل الباحثون إلى أن عنصر الـ"بوت" بنظام ويندوز المنبثق عن تلك الشبكة يبدو وكأنه قد صمم من قبل مهاجم إلكتروني يمتلك مهارات أكثر تطورًا من نظرائه الذين كانوا يقفون وراء شن هجمات DDoS واسعة النطاق والمشغلة عن طريق برمجية ميراي الخبيثة في أواخر العام 2016. الأمر الذي نتج عنه مخاوف مثيرة للقلق من احتمال استخدام هجمات برمجية ميراي الخبيثة وصعوبة توقع أهدافها مستقبلًا.

ويُرجّح الباحثون أن يكون مصمم هذه البرمجية من الناطقين باللغة الصينية. وقد دلت بيانات كاسبرسكي لاب على ظهور تلك الهجمات على نحو 500 نظامًا مختلفًا في العام 2017، وأظهرت أن الأسواق الناشئة التي تستثمر بشكل واسع في التكنولوجيات المتصلة قد تكون هي تحديدًا معرضة لمخاطر الإصابة بتلك الهجمات.

وأوضح الباحثون أن أداة نشر البرمجية الخبيثة القائمة على نظام ويندوز تعد أغنى وأقوى من الكود المصدري لبرمجية ميراي الأصلية، ولكن معظم مكونات وتقنيات ومهام أداة نشر البرمجية الجديدة قديمة وتعود إلى بضع سنين. وبالتالي فإن قدرتها على نشر البرمجية الخبيثة ميراي محدودة: إذ تقتصر قدرتها على توصيل المكونات المصابة ببرمجية ميراي من مضيف ويندوز المصاب إلى جهاز إنترنت "لينكس" المعرض للإصابة، وذلك في حال تمكنها من اختراق جدار الحماية المنيع للوصول إلى بروتوكول تسجيل الدخول Telnet المؤدي إلى الجهاز القابل للتحكم عن بعد.

وبالرغم من هذه القيود، يعتقد الباحثون أن هذا الرمز التشفيري ناتج عن تصميم مطوّر متمرّس يمتلك مستوى أعلى من الخبرة والمهارة، مع أنه قد يكون شخص حديث العهد بلعبة ميراي.

وتدل المؤشرات التي جمعها المحللون في البرمجية الخبيثة مثل الرموز والدلائل اللغوية على أنه قد تم بناء وتجميع هذا الرمز على نظام صيني، ولكن سيرفرات المضيف محتفظ بها في تايوان. وتظهر حالات إساءة استخدام الشهادات ذات رموز الدخول المسروقة من شركات صينية بأن المطور يتحدث على الأرجح اللغة الصينية.

وقال كيرت بومجارتنر، الباحث الأمني الرئيسي في كاسبرسكي لاب: "إن ظاهرة انتقال برمجية ميراي الخبيثة بين منصة لينكس ومنصة ويندوز هو مصدر قلق حقيقي، كونه يشير إلى ظهور المزيد من المطورين ذوي الخبرة على الساحة. وقد تسبب طرح كود المصدر لبرمجية Zeus المنبثقة عن برمجية حصان طروادة الخبيثة المستهدفة للقنوات المصرفية في العام 2011 في إحداث مشكلات كبيرة استمرت لسنوات وعانى منها مجتمع الإنترنت، كما أن طرح كود المصدر لجهاز إنترنت الأشياء الملغم ببرمجية ميراي في العام 2016 سوف يتسبب في عمل الشيء ذاته بالنسبة لمجتمع الإنترنت".

وأضاف بومجارتنر أن هناك المزيد من المهاجمين ذوي الخبرة والذين يمتلكون الكثير من المهارات المتطورة والتقنيات الحديثة قد بدأوا بالفعل الاستفادة من رموز تشفير برمجية ميراي الخبيثة المتوفرة مجانًا. إن شبكات الروبوت القائمة على نظام ويندوز التي تقوم بنشر أجهزة إنترنت الأشياء الملغمة ببرمجية ميراي الخبيثة تحدث تحولًا حاسمًا في عالم القرصنة، ويتسبب في انتشار برمجية ميراي الخبيثة لتصل إلى الأجهزة والشبكات المتوفرة حديثا والتي لم تكن متاحة سابقًا لعصابة ميراي. وهذه ليست سوى البداية.

ووفقًا لبيانات القياس عن بعد المقدمة من قبل كاسبرسكي لاب، جرت مهاجمة ما يقارب 500 نظامًا مختلفًا في العام 2017 من قبل هذا المكون الخبيث الـ"بوت" بنظام ويندوز مع محاولات تم الكشف عنها ومنعها على حد سواء

واستنادًا إلى وسائل تحديد الموقع الجغرافي من خلال عناوين بروتوكول الإنترنت المستخدمة في المرحلة الثانية من الهجوم، كانت الدول الأكثر عرضة لتلك الهجمات هي الأسواق الناشئة التي استثمرت بشكل واسع في مجال التكنولوجيا المتصلة مثل الهند وفيتنام والمملكة العربية السعودية والصين وإيران والبرازيل والمغرب وتركيا وملاوي ودولة الإمارات العربية المتحدة وباكستان وتونس وروسيا ومولدافيا وفنزويلا والفلبين وكولومبيا ورومانيا وبيرو ومصر وبنغلاديش

وتتعاون شركة كاسبرسكي لاب مع فرق الاستجابة لطوارئ الكمبيوتر وموردي خدمات الاستضافة ومشغلي الشبكات لمواجهة هذا التهديد المتنامي للبنية التحتية للإنترنت، وذلك من خلال إخراج عدد كبير من سيرفرات التحكم والسيطرة من الخدمة

وأوضحت الشركة الروسية المتخصصة في أمن المعلومات أن من شأن إخراج هذه السيرفرات من الخدمة بشكل سريع وناجح أن يقلل من حجم المخاطر والتعطيل التي تسببها الشبكات الروبوت الخبيثة القائمة على أجهزة إنترنت الأشياء سريعة التطور والنمو ونظرًا لأنه بإمكان كاسبرسكي لاب الاستفادة من خبرتها وعلاقاتها مع فرق الاستجابة لطوارئ الكمبيوتر والموردين حول العالم، تمكنت الشركة من تقديم العون لتسريع وتيرة وأداء هذه الجهود