بالو ألتو نتوركس: برمجيات إنترنت الأشياء الخبيثة تستغلّ الثغرات الأمنية الجديدة في أجهزة الراوتر الم

الأربعاء 24 يناير 2018 08:01 م

بحلول أوائل شهر ديسمبر من العام 2017، اكتشفت شركة 360 نت لاب عائلة جديدة من البرمجيات الخبيثة التي أطلقوا عليها اسم ساتوري Satori، المشتقة من برمجية ميراي Mirai الخبيثة، والتي تستهدف ثغرتين أمنيتين، الأولى هي عبارة عن ثغرة أمنية في نص برمجي تنفيذي موجود ضمن خدمة بروتوكول النفاذ إلى الدليل البسيط miniigd SOAP الخاصة براوتر Realtek SDK، والثانية ثغرة أمنية اكتشفت مؤخراً في بوابة الراوتر HG532e المنزلي من هواوي، المصححة في أوائل شهر ديسمبر من العام 2017.

وقد قامت الوحدة 42 التابعة لشركة بالو ألتو نتوركس بالبحث والتحري حول برمجية ساتوري Satori الخبيثة، واستناداً على عمليات استقصاء البيانات التي قمنا بها، تبين لنا وجود ثلاثة صيغ مختلفة لهذه البرمجية الخبيثة، حيث ظهرت أولاها خلال شهر أبريل من العام 2017، أي قبل ثمانية أشهر من موجة الهجمات الأخيرة.

كما عثرت الوحدة 42 أيضاً على دلائل تشير إلى أن صيغة برمجية ساتوري الخبيثة التي تقوم باستغلال الثغرة الأمنية التي كانت نشطة في أواخر شهر نوفمبر 2017، أي قبل أن تقوم شركة هواوي بتصحيح الثغرة الأمنية، ما يشير إلى أن هذه الصيغة من برمجية ساتوري الخبيثة كانت تجسد هجوم اليوم-الصفر التقليدي، وهو هجوم يستهدف ثغرة أمنية غير مكتشفة سابقاً، ولم يتم إصدار أي تصحيح لها بعد ذلك.

وتثبت نتائج عملية التحليل التي قمنا بها حول كيفية تطور برمجية ساتوري الخبيثة صحة نظريتنا القائلة بتطور المزيد من برمجيات إنترنت الأشياء الخبيثة من أجل استغلال إما إحدى الثغرات الأمنية المعروفة، أو حتى استغلال الثغرة الأمنية اليوم-الصفر.

تجدر الإشارة إلى أن الصيغ الأولى من برمجيات إنترنت الأشياء الخبيثة، مثل غافغيت Gafgyt والصيغة الأصلية لبرمجية ميراي، استغلت كلمات السر الافتراضية أو الضعيفة كي تهاجم الأجهزة. ورداً على ذلك، بدأ المستخدمون والمصنعون بتغيير كلمات السر الافتراضية، وتصعيب صيغة كلمات السر بهدف إحباط هذه الهجمات.

وعليه، قام بعض مصممي برمجيات إنترنت الأشياء الخبيثة، على غرار الجهات التي تقف وراء البرمجية الخبيثة أمنسيا Amnesia وآي أو تي_ريبر IoT_Reaper، بتغيير طرق استغلال الثغرات الأمنية المعروفة ضمن بعض أجهزة إنترنت الأشياء IoT. وبطبيعة الحال، استجابت الشركات الموردة لتقنيات إنترنت الأشياء IoT لهذا الأمر بتصحيح الثغرات الأمنية.

أما الخطوة المنطقية التالية والمتوقعة من قبل الجهات المهاجمة فتتمثل في الانتقال إلى استخدام نموذج هجوم اليوم-الصفر التقليدي لاستهداف الثغرات الأمنية غير المعروفة وغير المكتشفة.

وأشارت الوحدة 42 إلى المراحل الرئيسية لتطور برمجية ساتوري الخبيثة، لتصبح فيما بعد من عائلة برمجيات إنترنت الأشياء الخبيثة التي تستهدف ثغرات اليوم-الصفر الأمنية. وعرضت كيف تمكنت برمجية ساتوري الخبيثة، المشتقة من برمجية ميراي الخبيثة، من إعادة استخدام بعض نصوص شيفرة المصدر الخاصة ببرمجية ميراي الخبيثة لتحقيق مسح شامل لبروتوكول الـ وكلمات السر للقيام بهجمة عنيفة تستهدف المهام الوظيفية.

وقد قامت برمجية ساتوري الخبيثة أيضاً بتحديد نوع من أجهزة إنترنت الأشياء، حيث أظهر سلوكيات مختلفة وفقاً لاختلاف أنواع هذه الأجهزة. وهو ما يؤكد لنا بأن مصمم برمجية ساتوري Satori الخبيثة بدأ بعكس هندسة البرامج الثابتة في العديد من أجهزة إنترنت الأشياء، وذلك بهدف جمع المعلومات الأصلية للجهاز، واكتشاف ثغرات أمنية جديدة. وفي حال صح هذا الأمر، فقد نشهد في المستقبل

القريب صيغ جديدة لبرمجية ساتوري الخبيثة تستهدف العديد من الثغرات الأمنية غير المعروفة في الأجهزة الأخرى

مراحل تطور برمجية ساتوري الخبيثة
تمكنت الوحدة 42 منذ شهر أبريل من العام 2017 من رصد عدد من الهجمات التي شنتها برمجية ساتوري Satori الخبيثة، ومن خلال تحليل سجلات الهجمات التي قمنا برصدها، واستناداً على نتائج عميلات تحليل العينة، استطاعت الوحدة تحديد ثلاث صيغ رئيسية مختلفة لبرمجية ساتوري الخبيثة، حيث تشير نتائج عمليات التحليل التي قمنا بها إلى أن هذه الصيغ الثلاث تنفذ أوامر مختلفة

الصيغة الأولى تقوم فقط بفحص الإنترنت، والتحقق من عنوان بروتوكول الإنترنت IP لمعرفة أيها يحوي على ثغرة أمنية ضمن تسجيل الدخول إلى بروتوكول الـ Telnet، وذلك عن طريق محاولات تجريب كلمات السر المختلفة وبمجرد نجاحها في تسجيل الدخول فإنها تقوم بتفعيل جدار صد ضد عمليات الوصول، ومن ثم تعمل على تنفيذ الأوامر /bin/busybox satori أو "/bin/busybox SATORI" فقط

أما الصيغة الثانية فإنها محاطة بطبقة حماية وتمويه من أجل تفادي كشفها من قبل عمليات الكشف الثابتة وفي الوقت نفسه، قامت الجهة المهاجمة بإضافة كلمة السر aquario ضمن دليل كلمات المرور، لكي تستخدمها دائماً للدخول من أول محاولة لها، كما أن كلمة السر aquario تعتبر كلمة السر الافتراضية لأجهزة الراوتر الرائجة في دول أمريكا الجنوبية، وهو ما يشير إلى أن الجهة المهاجمة بدأت بالتغلب على البرامج المؤتمتة في أمريكا الجنوبية

في حين قامت الصيغة الثالثة من البرمجية باستغلال ثغرتين أمنيتين لتنفيذ النص البرمجي عن بعد، بما في ذلك ثغرة اليوم-الصفر الأمنية (CVE-2017-17215)، وهو وجه الشبه الذي يربطها ببعض عينات الصيغة الثانية، فهما تحملان نفس الأوامر المدرجة

النتيجة
تظهر برمجية ساتوري الخبيثة أن برمجيات إنترنت الأشياء الخبيثة تتطور باستمرار على نطاق واسع، فهي تبدأ من الهجمات العنيفة لكشف كلمات السر، وصولاً إلى هجمات استغلال الثغرات الأمنية

كما أن شيفرة المصدر المفتوح لبرمجية ميراي الخبيثة وفّر لمصممي برمجيات إنترنت الأشياء الخبيثة نقطة انطلاق جيدة نحو تطوير صيغ جديدة، الأمر الذي قد يصبح من التوجهات السائدة إذا ما واصل مصممو برمجيات إنترنت الأشياء الخبيثة اعتمادهم على استغلال المزيد من الثغرات الأمنية المعروفة، أو اكتشاف ثغرات اليوم-الصفر الأمنية لمهاجمة أجهزة إنترنت الأشياء

تجدر الإشارة إلى أن شركة بالو ألتو نتوركس قامت بإصدار التصحيح رقم (37896) لأنظمة كشف ومنع الاختراق الخاص بثغرة اليوم-الصفر التي تستغله برمجية ساتوري الخبيثة كما تمكنت شركة وايلدفاير أيضاً من تدارك نقاط الكشف عن عينات برمجية ساتوري الخبيثة، في حين قامت شركة سي تو إس بتصنيفها ضمن البرمجيات الخبيثة