ما الجهاز الذي تعتمده وكالة المخابرات الأمريكية لاختراق نقاط وصول واي فاي؟

ترجمة وتحرير نون بوست

يسمح جهاز "تشيري بلوسوم" لوكالة المخابرات المركزية باختراق جهاز التوجيه واي فاي، ثم الاطلاع على كل المعلومات التي تحتويها حركة مرور شبكة الإنترنت. وبفضل هذه التقنية، يمكن للوكالة التقاط كل حركة جديدة أو استهداف أنواع معينة من الاتصالات أو تنفيذ العديد من الهجمات الأخرى.

يوم الخميس 15 حزيران/ يونيو، نشرت ويكيليكس سلسلة من الوثائق، تمكنت صحيفتا "ميديابار" و"لا ريبوبليكا" من الاطلاع عليها، تتعلق بجهاز "تشيري بلوسوم" الذي يسمح لوكالة المخابرات المركزية باختراق نقاط الإنترنت اللاسلكية، مثل أجهزة التوجيه واي فاي، لرصد وعرقلة حركة المرور داخلها.

في الواقع، يتكون جهاز "تشيري بلوسوم" أو "سي بي" من مجموعة من الأدوات تسمح للمشغل التابع لوكالة المخابرات المركزية بالتحكم في نقاط الوصول اللاسلكية، مثل تلك المستخدمة للاتصال بالواي فاي المعتمدة في الشركات أو حتى في الحانات، أو المطارات، أو الفنادق. وإثر زرع "سي بي" في جهاز الحاسوب، يمكن لوكالة المخابرات المركزية أمره، عن بعد، برصد كل تفاصيل حركة المرور عبر شبكة الإنترنت، أو استهداف أجهزة أخرى أو نوع معين من الاتصالات.

وتجدر الإشارة إلى أن المرحلة الأولى، المتمثلة في إصابة واختراق نقطة الاتصال بالإنترنت، حساسة جدا. ويتم تركيب "تشيري بلوسوم" عن طريق تحديث البرنامج الثابت (فيرم وير) للجهاز. حينها، يجب على وكالة المخابرات المركزية تثبيت نسخة معدلة، تضم برمجياتها الخاصة، دون أن يُلاحظ المستخدمون أي تغيير على مستوى الشبكة.

في الحقيقة، لا يُسبب هذا الأمر أي مشكلة بالنسبة للوكالة. وبعبارة أدق، أكدت هذه الأخيرة في "دليل البدء السريع" الخاص بهذا الجهاز أن "العديد من الأجهزة اللاسلكية تتيح عملية التحديث عبر رابط لاسلكي، الأمر الذي يعني أنه يمكن زرع جهاز لاسلكي دون استخدام معدات مادية".

وبالعودة إلى طريقة تفعيل الجهاز، يشير دليل الاستخدام إلى وجود عدة طرق لإصابة ثم اختراق أجهزة التوجيه. وقد دقق الدليل في "كلايمور"، وهو "أداة مراقبة وجمع وزرع الأجهزة اللاسلكية". كما يُوضح دليل المستخدم أن "وظيفة المراقبة تهدف إلى تحديد النماذج والإصدارات والعلامات التجارية لهذه الأجهزة في أماكن معينة. أما بالنسبة لوظيفة الجمع، فتُمكن من التقاط حركة المرور اللاسلكية، بينما تؤدي وظيفة الزرع إلى تحديث البرامج الثابتة اللاسلكية".

والجدير بالذكر أن لهذا الجهاز ميزات عديدة، حيث يُمكن استخدامه "في بيئة متنقلة" (في جهاز حاسوب محمول على سبيل المثال) أو في بيئة ثابتة مع هوائي ضخم ليعمل على مدى أبعد. "وبمجرد اختراقه، يتحول جهاز التوجيه إلى "صائدة ذباب"، وهو المصطلح الذي اعتمدته وكالة المخابرات المركزية.

وفي ذلك الحين، يُصبح دور الجهاز الرئيسي متمثلا في العمل "كمرشد"، وفي التواصل مع خادم يُعنى "بالقيادة والسيطرة" ويُدعى "تشيري تري". وللتوضيح، يُستعمل هذا النوع من الخادم في إطار الهجمات الإلكترونية، التي تُستخدم فيها "البوت نت" وشبكات من الآلات تلعب دور قيادة وتوجيه هذه الهجمات.

في الحقيقة، هذا هو بالضبط ما يقوم به "تشيري تري"، ذلك أن جهاز التوجيه يقوم بصفة منتظمة، بإرسال "إرشادات" إليه، وهي عبارة عن معلومات تمر عبر نقاط الاتصال بشبكة الإنترنت (أو نقاط التواجد). وردا على ذلك، تصدر هذه الأخيرة أوامرها المحددة بشكل مسبق.

وفي هذا الإطار، يُفسر دليل المستخدم أن "صائدة الذباب" تُرسل إلى "تشيري تري" (عبر نقاط التواجد)، بصفة دورية، معلومة تُخبره بوضع وإعدادات أمان الجهاز. عند ذلك، يرد هذا الخادم بمهمة تكلف "صائدة الذباب" بالبحث عن رسائل البريد الإلكتروني أو مستخدمي الدردشة أو "عناوين ماك" في حركة مرور الشبكة بواسطة هذا الجهاز. وعند الكشف عن الهدف، تُحذر صائدة الذباب الخادم".

ومما لا شك فيه يتم تحديد هذه المهمات، أو الأوامر المرسلة إلى جهاز التوجيه، من قبل شخص مادي، يعمل مع وكالة الاستخبارات المركزية بصفة مسبقة. ولهذا، وضعت الوكالة واجهة مخصصة، أطلقت عليها اسم "تشيري ويب". ويُبين دليل بدء التشغيل بعض اللقطات التي تُصورها. ويأخذ "تشيري ويب" شكل موقع متواجد على شبكة الإنترنت، يُمكن من تكوين "صائدات الذباب" وبرمجة "المهمات" ورصد تطور تنفيذها وعمل الجهاز.

والجدير بالذكر أنه من الممكن أن تكون "صائدة الذباب" مبرمجة لاعتراض أو إيقاف جزء من حركة المرور على شبكة الإنترنت، على غرار "عناوين البريد الإلكتروني"، و"أسماء مستخدمي الدردشة" أو "عناوين ماك"، المعروفة أيضا "بالعناوين الفيزيائية"؛ وهي تسمية مسندة لمعرف بطاقة شبكة الكمبيوتر. وبالتالي، يسمح "تشيري بلوسوم" باستهداف كمبيوتر معين متصل بالشبكة المصابة أو المخترقة.

وكما أكدته منظمة ويكيليكس في بيانها، تتموقع "صائدة الذباب" تحديدا بين الهدف ونقطة اتصاله بالإنترنت. ويُطلق مجال أمن المعلومات على هذه الوضعية اسم "الرجل في الوسط"، كما تُعرف أيضا أنها طريقة مثالية لشن هجمات مختلفة. وهكذا، يُمكن للمشغل "نسخ حركة مرور شبكة الهدف" أو إعادة توجيه "متصفحه". ويسمح هذا الخيار الأخير باستبدال موقع إلكتروني بآخر، وإيصال الهدف بصفحة معدة لإيقاعه في الفخ، في الوقت الذي يعتقد فيه أنه متصل، مثلا، بحسابه على جوجل.

علاوة على ذلك، يمكن للمشغل تكليف "صائدة الذباب" "بأعمال ذات صبغة عالمية"، أي بمهمات لا ترتبط بهدف أو بنوع حركة مرور معينة. وفي هذا الإطار، يمكن أن تقوم "بنسخ كل حركات المرور داخل الشبكة" أو "تجميع عناوين البريد الإلكتروني أو أسماء مستخدمي الدردشة، أو أرقام محادثات الصوت عبر ميثاق الإنترنت" (وهي تقنية تمرير الاتصالات الصوتية أو الفيديو عبر الإنترنت وتُستخدم على سبيل

المثال في تطبيقات سكايب أو فايبر). بالإضافة إلى ذلك، يمكن للمشغل إنشاء شبكة خاصة افتراضية، تتيح له فرصة الاتصال المباشر بشبكة الواي فاي المستهدفة لشن هجمات أخرى انطلاقا منها.

وفي شأن ذي صلة، يعود تاريخ الوثائق التي نشرها موقع ويكيليكس إلى الفترة الممتدة بين سنتي 2007 و2012. ولكن، لا يوجد أي تفسير منطقي يوضح سبب تخلي وكالة المخابرات المركزية عن هذه الأدوات. ووفق المعلومات المتوفرة في دليل المستخدم، يتم تثبيت "تشيري بلوسوم" أثناء عملية تحديث قسرية لجهاز التوجيه. ومن ناحية أخرى، يعتبر هذا الجهاز شفافا تماما كما يصعب كشفه تقريبا.

فضلا عن ذلك، لم يتم تطوير العديد من نماذج أجهزة التوجيه منذ تلك الفترة. ومن بين الوثائق المنشورة، نجد قائمة من العلامات والنماذج التي نجح "تشيري بلوسوم" في اختراقها. وركزت صحيفة "لا ريبوبليكا" على قائمة أجهزة التوجيه المتواجدة في السوق إلى يومنا هذا. ومن بينها، يُمكن التعرف على "وي آر تي 54 جي آل"، التابعة لعلامة "لينكسيز" الشعبية. وفي كانون الثاني/ يناير من سنة 2016، كرس موقع "آرس تكنيكا" مقالا لهذه العلامة أشاد فيه بعراقة منتج متوفر منذ 11 عاما، ولازال يواصل درّ الملايين على مُصنّعه.

والجدير بالذكر أن الوثائق المنشورة تندرج ضمن سلسلة "فولت 7" التي كرسها موقع منظمة ويكيليكس لفضح هجمات الكمبيوتر المنظمة التي تشنها وكالة المخابرات المركزية. وفي أوائل شهر آذار/ مارس، أعلنت المنظمة أنها عثرت على 8761 وثيقة وملف تُفصّل الأدوات التي تستعملها الوكالة للتجسس الرقمي. ومنذ ذلك الحين، بادر الموقع بنشر وثيقة كل أسبوع.

المصدر: ميديابار

رابط المقال: https://www.noonpost.com/18485/