xLED برمجيات خبيثة تسرق البيانات باستعمال أضواء جهاز التوجيه

الأربعاء 7 يونيو 2017 10:06 م

تمكن فريق يعمل في مركز أبحاث الأمن السيبراني في جامعة بن غوريون في إسرائيل من إنشاء برمجيات خبيثة تدعى xLED، حيث نجح الفريق سابقاً باستعمال أضواء الليد LED على قرص صلب وطائرة بدون طيار للحصول على البيانات، إلا أن استهداف أجهزة التوجيه والتبديل يسمح لهم بالتقاط بيانات أكبر بكثير لوجود العديد من الأضواء ضمنها.

وتأتي البرمجيات الخبيثة بأشكال كثيرة، إلا أن البرمجيات الخبيثة المسماة xLED تعد أحد أشكال البرمجيات الخبيثة الأكثر غرابة والأحدث التي ظهرت حتى الآن، حيث انها قادرة على إصابة جهاز التوجه (راوتر) أو التبديل (سويتش) ومن ثم سرقة البيانات عن طريق وميض الأضوية LED الذي يحصل ضمن هذه الأجهزة دائماً.

وتعمل هذه البرمجيات الخبيثة xLED على سرقة البيانات عن طريق إصابة الهدف المتمثل بجهاز التوجيه (راوتر) أو التبديل (سويتش) أولاً بهذه البرمجيات، وبمجرد تثبيتها يمكنها أن تسرق البيانات من خلال تحويل البيانات إلى شكل الترميز الثنائي المكون من أصفار وآحاد، بحيث يمكن لكل ضوء موجود على الجهاز نقل رقم ثنائي يضيئ عند الرقم واحد ويطفئ عند الرقم صفر.

ويحتاج المهاجم إلى كاميرا من أجل تسجيل البيانات، ويمكن تركيب هذه الكاميرا على طائرة بدون طيار وجعلها تتابع الجهاز من خلال النافذة أو عن طريق رشوة أحد حراس الأمن لتركيب مثل هذه الكاميرا لتسجيل البيانات ضمن شركة أو دائرة حكومية أو الاستعانة بكاميرا الأمن المثبتة مسبقاً عن طريق اختراقها، حيث يمكن الاعتماد على الإعدادات والوضع.

كما يمكن استعمال أجهزة الاستشعار البصرية للتسجيل مما يعطي نتائج أفضل لأنه بإمكان تلك المستشعرات تسجيل التغييرات التي تحصل لإضاءة أجهزة التوجيه أو التبديل بمعدل أعلى بكثير من حيث دقة العينات المسجلة.

وتمكن الباحثون من تحقيق معدل سرقة بيانات وصل إلى 1000 بت في الثانية الواحدة لكل ضوء ليد LED، ويعد الجزء الأكثر صعوبة للسماح لتلك البرمجيات الخبيثة بالعمل هو إمكانية تثبيتها على جهاز التوجيه أو التبديل بالدرجة الأولى، وقد تتحول هذه البرمجيات الخبيثة إلى المستقبل القادم من طرق سرقة البيانات.

وباستطاعة المصنعين مستقبلاً التفكير في طرق لمواجهة هذه الطريقة عبر اعتبارها ضعف محتمل في الشبكة، ومنع الأشخاص من استعمال هذه الطريقة لنشر هذا النوع من البرمجيات الضارة.