أبرز ثلاثة مخاطر تهدد المستخدمين في 2016

الثلاثاء 29 ديسمبر 2015 12:12 م

تتنوع المشاكل الأمنية المتوقع حدوثها عام **2016**، وقد أجمع خبراء أمنيون على ثلاثة مخاطر يجب الحذر منها أكثر من غيرها العام المقبل، وهي الهجمات على الهواتف الذكية، وهجمات الفدية، وتسريب بيانات الأجهزة المتصلة بالإنترنت كالتلفزيونات الذكية.

فمن المنتظر أن يشهد العام المقبل ازديادا في الهجمات الإلكترونية التي تستهدف الأجهزة المحمولة لتظهر أنماطا جديدة من البرمجيات الخبيثة المصنعة خصيصا لأذيتها، وذلك إلى جوار تناقص استهداف الحواسيب المكتبية التقليدية، وفقا لما يرجحه مدير العمليات لدى شركة صناعة البرمجيات الأمنية أفاست، أندريه فالشيك.

أما هجمات الفدية فهي تطلق على ذلك النوع من الهجمات الإلكترونية التي يسلب فيها المعتدي بيانات خاصة بالمستخدم أو يعطل جهازه لإجباره على دفع فدية، ويعطي النظر إلى هذا النوع من الهجمات خلال العامين **2014** و**2015** انطباعا بأنها قد تتضاعف بشكل كبير في العام القادم.

وقد بدأت هجمات الفدية باستهداف الهواتف المحمولة على غرار أجهزة أندرويد، مثل البرمجية الخبيثة "سيمبل لوكر" التي تعد من أوائل البرمجيات الخبيثة الموجهة لاستهداف الهواتف الذكية وقد ظهرت عام **2014.**

وعوضا عن سرقة البيانات أو تدميرها، تقوم هجمات الفدية بتشفير البيانات ومن ثم طلب دفعة مالية من الضحية لفك تشفيرها، الأمر الذي يصفه المدير لدى الشركة الأمنية "بالو ألتو نتوركس"، ريان أولسون، بأنه أكثر حيلة إذا ما قورن بعمليات مثل سرقة بيانات البطاقات الائتمانية، تلك العمليات التي يمكن تعقبها والحد من فاعليتها.

ومن المتوقع -وفقا لأولسون- أن يلجأ المهاجمون في العام القادم إلى استهداف الشركات والشخصيات المهمة، أي الجهات القادرة على دفع مبالغ كبيرة لقاء استعادة بياناتهم الهامة.

إنترنت الأشياء

أما الخطر الثالث فهو التسريبات الناجمة عن استهداف تقنيات إنترنت الأشياء، أي استهداف البيانات الخاصة بالمستخدمين والملتقطة من أجهزتهم الشخصية والمنزلية مثل الأساور الذكية والتلفزيونات الذكية والسيارات المتصلة بالإنترنت وأنظمة ضبط الحرارة الذكية، وفقا لجيوف ويب، نائب الرئيس في شركة أمن المعلومات "مايكرو فوكس" المتخصصة في منع الاختراقات الأمنية.

وفي الحقيقة، تعد تقنيات إنترنت الأشياء عرضة للاستهداف بشكل كبير، خاصة أن مصمميها يهملون في بعض الأحيان الجوانب الأمنية فيها، فكثيرا ما تقوم هذه الأجهزة بإرسال بياناتها دون أي تشفير مما يسهل على المهاجم الوصول إليها وسرقتها، حسب فالشيك.

ولسوء الحظ، فإن ضعف الجوانب الأمنية في موجه الشبكة اللاسلكية المنزلي (الراوتر) من شأنه أن يوفر فرصا أكبر للمخترقين تسمح لهم بالولوج إلى الشبكة المنزلية، وبالتالي إلى بيانات الأجهزة المتصلة بها، وقد تكون الثغرات الأمنية في تلك الموجهات اللاسلكية بسبب عدم تحديث المستخدم لبرمجياتها وفقا لآخر التحديثات التي توفرها الشركة المصنعة.

ويعد استغلال البيانات المسربة من تقنيات إنترنت الأشياء أحد أكبر المخاطر التي تهدد مستخدم التقنية العام القادم، فمن خلالها يمكن للمخترق معرفة معلومات خاصة على غرار موعد نوم المستخدم أو مغادرته منزله للقيام بسرقته، أو الحصول على صور خاصة به وابتزازه ماديا.

المصدر : الجزيرة