تسريب أكثر من 711 مليون عنوان بريد إلكتروني

الخميس 31 أغسطس 2017 04:08 م

اكتشف باحث أمني فرنسي يدعى بينكو Benkow هذا الأسبوع كمية كبيرة من قوائم البريد المزعج، والتي يصل مجموعها إلى أكثر من 711 مليون عنوان بريد إلكتروني، وقد تمكن الباحث من الكشف عن روبوت ويب Bot للبريد الإلكتروني المزعج مستعمل منذ عام 2016 يدعى "أونلاينر" Onliner، ويستعمل هذا الروبوت صوراً صغيرة بحجم بيكسل مخبأة في رسائل البريد المزعج، والتي تهدف إلى جمع تفاصيل عن أجهزة حاسب المتلقي للبريد، ويتواجد الخادم الذي يحتوي على تلك القوائم ضمن هولندا

وأوضح تروي هانت Troy Hunt الخبير الأمني أن القائمة تحتوي على كمية محيرة للعقل من البيانات المتعلقة بعناوين البريد الإلكتروني وكلمات المرور المخزنة ضمن ملفات نصية عادية، جنباً إلى جنب مع امتلاك روبوت الويب للبريد الإلكتروني المزعج Onliner كمية هائلة من شهادات مصادقة برتوكول SMTP المستعمل في البريد الإلكتروني الصادر، وتستخدم تلك الشهادات من أجل التحايل على مرشحات وفلاتر البريد المزعج، وقد تم الحصول على تلك الشهادات من خلال عمليات تسريب البيانات الأخرى

وتعتبر إمكانية وجود عنوان البريد الإلكتروني الخاص بالمستخدم ضمن تلك البيانات أمر غير مثير للقلق بشكل كبير، إلا انها تعني أنه يجب أن يكون المستخدم اكثر حذراً من رسائل البريد الإلكتروني التي يقوم بفتحها، كما يتواجد ضمن تلك القائمة عدد من الحسابات المعرضة للخطر، بحيث يمكن استعمال تلك الحسابات لإرسال رسائل غير مرغوب فيها إلى المزيد من الأشخاص، وتتعلق بيانات القائمة بسلالة برمجيات خبيثة تسمى أورسنيف Ursnif، وهي عبارة عن تروجان يسرق أسماء المستخدمين وكلمات السر والحساب المصرفي وتفاصيل بطاقة الدفع

وأوضح هانت أن عدد رسائل البريد الإلكتروني الموجودة في الاستخدام أقل قليلاً من العدد الإجمالي لشهادات مصادقة عملية تسجيل الدخول المتواجدة في القائمة، وبإمكان المستخدمين معرفة فيما إذا كانوا قد تعرضوا للاختراق من خلال التوجه إلى موقع الويب have i been pwned، وإدخال عنوان البريد الإلكتروني للحصول على النتيجة، وأضاف الخبير الأمني أنه لا داعي للقلق والخوف بالنسبة للمستخدمين الذين يمتلكون كلمات مرور قوية ويستعملون ميزة التحقق بخطوتين

وبحسب الباحث الأمني Benkow فإن عملية إرسال البريد المزعج تحتاج إلى وجود قائمة ضخمة من شهادات مصادقة بروتوكول SMTP، وهناك خياران فقط للقيام بذلك إما إنشاء تلك القائمة أو شرائها، ويجري ضخ تلك القائمة بعد تجميعها ضمن روبوت الويب للبريد الإلكتروني المزعج، وهو البرمجية الحاسوبية التي تعمل على أتمتة عملية توزيع البريد الإلكتروني، وعلى سبيل المثال فقد اكتشف بينكو حوالي 2 مليون عنوان فيس بوك جرى جمعها من قبل حملات التصيد الاحتيالي