كاسبرسكي: برمجية WannaCry ساعدت مرسلي رسائل "سبام" على سرقة أموالا طائلة

الأحد 27 أغسطس 2017 08:08 م

في الربع الثاني من عام 2017، حاول مجرمو الإنترنت المتورطون في توزيع رسائل البريد الإلكتروني غير المرغوب فيها الاستفادة من مخاوف المستخدمين عندما وقعت هجمات الفدية WannaCry في شهر أيار/مايو.

ومع العلم أن هناك الكثير من الناس الذين وقعوا ضحية هجمات الفدية، وسعيًا منهم لاستعادة بياناتهم المشفرة مجددًا، قام المحتالون بإرسال رسائل البريد الإلكتروني غير المرغوب فيها وشن هجمات التصيد الإلكتروني، عرضوا من خلالها على المستخدمين خدمات مختلفة لمكافحة تلك الهجمات الخبيثة والواسعة النطاق.

وكانت هذه واحدة من النتائج الرئيسية التي توصلت إليها كاسبرسكي لاب في تقريرها الصادر بعنوان: "رسائل البريد الإلكتروني غير المرغوب فيها وهجمات التصيد الإلكتروني في الربع الثاني 2017".
أصاب هجوم الفدية WannaCry أكثر من 200,000 جهاز حاسب حول العالم، مما أدى إلى إثارة قدر هائل من الذعر، وسرعان ما استغل مرسلو الرسائل غير المرغوب فيها هذه الفرصة لمصلحتهم.

كما اكتشف الباحثون قدرًا كبيرًا من الرسائل التي تعرض خدمات مختلفة، مثل الحماية من هجمات الفدية WannaCry واستعادة البيانات، بالإضافة إلى تنظيم ندوات تعليمية ودورات توعية للمستخدمين.

وإلى جانب ذلك، تمكن مرسلو الرسائل غير المرغوب فيها بنجاح من تنفيذ مخطط تقليدي ينطوي على تقديم عروض احتيالية لتثبيت تحديثات برمجية على أجهزة الحاسب المصابة. ومع ذلك، كانت الروابط تعيد توجيه المستخدمين إلى صفحات التصيد الاحتيالي حيث كان يتم سرقة البيانات الشخصية للضحايا.

ومن أحد الظواهر الرئيسية التي تم رصدها في الأشهر الثلاثة الماضية هو عدد الرسائل الجماعية الموجهة لشبكات الشركات. واستنادًا إلى أبحاث كاسبرسكي لاب، تفاقم انتشار هذه الرسائل الموجهة منذ بداية العام.

وبدأ مرسلو الرسائل غير المرغوب فيها في إخفاء الرسائل الخبيثة على هيئة قنوات حوار وتواصل بين الشركات، وذلك باستخدام بيانات تعريف خدمات البريد للشركات، بما في ذلك التوقيعات الحقيقية والشعارات، بل حتى المعلومات المصرفية.

كما قام مجرمو الإنترنت بدس وإرسال حزم هجمات ساعة الصفر في الأرشيف المرفق بالبريد الإلكتروني الموجه لسرقة بروتوكول نقل الملفات والبريد الإلكتروني وكلمات المرور الأخرى. ويشير خبراء كاسبرسكي لاب إلى أن معظم الهجمات الموجهة ضد قطاع الشركات تنطوي على أهداف مالية.

وبالإضافة لذلك، توصل الباحثون إلى أن هناك زيادة في عدد الرسائل الجماعية المحملة بأحصنة طروادة الخبيثة التي تم إرسالها نيابة عن خدمات التوصيل الدولية في الربع الثاني من العام. وكان مرسلو الرسائل غير المرغوب فيها يرسلون تقارير شحن تحتوي على معلومات حول عمليات تسليم طرود وهمية وغير موجودة في الأساس.

وبهدف إصابة أجهزة الحاسب أو سرقة بيانات التعريف الخاصة بتسجيل الدخول، تبيّن أن المجرمين يقومون بنشر روابط تحميل ملغّمة بالبرمجيات الخبيثة، بما في ذلك برمجية حصان طروادة Emotet المستهدفة للقنوات المصرفية، والتي تم اكتشافها لأول مرة في العام 2014. وعمومًا، ارتفع حجم الرسائل الجماعية الخبيثة بنسبة 17%، وفقًا لتقرير كاسبرسكي لاب الجديد.

وتقول داريا غودكوفا، خبيرة تحليل الرسائل غير المرغوب فيها في كاسبرسكي لاب: "لقد لاحظنا خلال الربع الثاني من العام بأن الظواهر الرئيسية في هجمات رسائل البريد الإلكتروني غير المرغوب فيها وهجمات التصيد الإلكتروني استمرت في النمو.

ويأتي شن هجمات الفدية WannaCry عن طريق الرسائل الجماعية دليلًا على أن مجرمي الإنترنت منتبهون جدًا وعلى دراية تامة بمجمل الأحداث الدولية. وفضلًا عن ذلك، بدأ مجرمو الإنترنت في التركيز أكثر على قطاع الأعمال من فئة شركة – لشركة B2B-، نظراً لأنه يعود عليهم بأرباح وفيرة. ونتوقع أن تستمر هذه الظواهر في النمو، وبأن تزداد الهجمات الموجهة ضد الشركات من حيث العدد والنوع".

ومن ضمن الاتجاهات والاحصاءات المهمة الأخرى التي حددها باحثوا كاسبرسكي لاب في الربع الثاني 2017: ارتفاع متوسط حجم الرسائل غير المرغوب فيها إلى 56.97% إذ أصبحت فيتنام المصدر الأكثر رواجًا لهجمات الرسائل غير المرغوب فيها، متقدمة على الولايات المتحدة والصين.

وتشمل قائمة الدول العشر الاولى لتلك الهجمات: روسيا والبرازيل وفرنسا وايران وهولندا.
وبحسب التقرير؛ لا تزال شبكة Necurs نشطة. ومع ذلك، رصد الخبراء انخفاضًا في حجم الرسائل غير المرغوب فيها المرسلة من هذه الشبكة وعدم استقرارها.

وتُعد ألمانيا من الدول الأكثر استهدافًا من قبل هجمات البريد الإلكتروني الخبيثة. وجاءت الصين في المرتبة الثانية، تلتها المملكة المتحدة واليابان وروسيا. وتشمل قائمة الأهداف الشائعة الأخرى: البرازيل وإيطاليا وفيتنام وفرنسا والولايات المتحدة.

تم تشغيل نظام كاسبرسكي لاب لمكافحة التصيد الاحتيالي 46,557,343 مرة على أجهزة حاسب مستخدمي حلول كاسبرسكي لاب. واحتضنت البرازيل أكبر نسبة من المستخدمين المتضررين (18.09%). وبشكل عام، تعرض 8.26% من مختلف أنواع مستخدمي منتجات كاسبرسكي لاب في جميع أنحاء العالم لهجمات رسائل التصيّد الإلكتروني.

وفي الربع الأول، بقيت الأهداف الرئيسية لهجمات التصيد الاحتيالي هي نفسها، وكانت تستهدف في المقام الأول القطاع المالي: البنوك وخدمات الدفعات والمتاجر الإلكترونية.