الاتصالات: 7 إرشادات للحماية من فيروس الفدية الإلكتروني

السبت 13 مايو 2017 06:05 م

أكد شريف هاشم، نائب الرئيس التنفيذي للجهاز القومي لتنظيم الاتصالات لشئون الأمن السيبراني، أنه تم التواصل مع مسئولي الأمن السيبراني في كافة قطاعات الدولة الحيوية للتأكيد على اتخاذ كافة الإجراءات الاحترازية لمنع وصول فيروس (الفدية الإلكتروني) إلى تلك القطاعات.

وأضاف هاشم في بيان اليوم السبت، أن أية جهة أو شخص يتعرض لمثل تلك الفيروسات يمكنه التواصل مع المركز المصري للاستجابة للطوارئ المعلوماتية EG CERT، بإرسال رسالة إلى incident@egcert.eg

وقال إنه من المبكر في الوقت الحالي تقدير حجم تأثر مصر بالهجمات الإلكترونية، مشيرا إلى أنه قدم تقريرا للمهندس ياسر القاضي وزير الاتصالات وتكنولوجيا المعلومات ورئيس المجلس الأعلى للأمن السيبراني يتضمن طبيعة الهجمة وإجراءات الأمان والتحصين الجاري اتخاذها في الوقت الحالي.

وأوضح أن الفيروس الإلكتروني ينتشر من خلال رسائل البريد الإلكتروني المرسلة إلى المستخدمين مع مرفق ضار يحتوى على هذا الفيروس، وبعد إصابة جهاز المستخدم فإنه يستغل الثغرة المعروفة باسم MS17-010 لتصيب أجهزة أخرى على نفس الشبكة من أجل تحقيق انتشار سريع للفيروس الإلكتروني.

وأشار هاشم، إلى أنه يمكن لهذا الفيروس أن يصيب الأجهزة الإلكترونية التى تعمل بنظام تشغيل ويندوز من XP إلىR2008 ، وفي حالة إصابة جهاز المستخدم بهذا الهجوم الإلكتروني فإنه يتم تشفير كافة الملفات الموجودة على جهاز الحاسب ويطلب من المستخدم دفع فدية كشريطة استرداد الملفات الخاصة به.

ووجه هاشم مجموعة من الإرشادات للمؤسسات والأشخاص تتمثل في التأكد من أن جميع برامج الحماية الخاصة بالمستخدمين تم تحديثها، والتأكد من وجود حزمة تحديثات (Patch) مايكروسوفت MS17-010 لإغلاق الثغرة المستغلة فى الهجوم الإلكتروني ، كذلك التأكد من إغلاق المنافذ الأتية على الخوادم (135:(no Port445g.

وأوضح أن الهاكرز يستخدمون عناوين بروتوكول الإنترنت IP :

"213.61.66.116, 171.25.193.9, 163.172.35.247, 128.31.0.39, 185.97.32.18, 178.62.173.203, 136.243.176.148, 217.172.190.251, 94.23.173.93, 50.7.151.47, 83.162.202.182, 163.172.185.132, 163.172.153.12, 62.138.7.231".

ولذلك يرجى مراجعة إذا تم اتصال بين حواسب المستخدمين والعناوين السابق ذكرها من خلال البرامج والأدوات المستخدمة لمراقبة وحماية الشبكات من الهجمات الإلكترونية.

وشدد على ضرورة توعية المستخدمين بخطورة هذه النوعية من الهجمات الإلكترونية وعدم فتح مرافق البريد الإلكتروني الضارة وغير الموثوق من مصدرها كما يجب التأكد من خلوها من البرامج الخبيثة من خلال برامج الحماية الخاصة بالمستخدم.

وأكد ضرورة الاحتفاظ بنسخة من الملفات والبيانات الإلكترونية الهامة دوريا على جهاز خارجي منفصل عن الشبكة حتى يتم استعادتها بشكل صحيح في حالة الإصابة.

جدير بالذكر أن عددا من الدول على مستوى أنحاء العالم، من بينها مصر، تتعرض إلى هجمات إلكترونية لفيروس (الفدية الإلكتروني) (Ransomware) الذي يطلق عليه اسم WannaCry وJaff