وزارة الاتصالات وتكنولوجيا المعلومات
المجلس الأعلى للأمن السيبراني

تعليمات للمستخدمين لمواجهة فيروس "الفدية الإلكتروني"

كيفية الإصابة بهذا الفيروس:

- ينتشر الفيروس الإلكتروني من خلال رسائل البريد الإلكتروني المرسلة إلى المستخدمين مع مرفق ضار يحتوي على هذا الفيروس.
- بعد إصابة جهاز المستخدم، فإنه يستغل الثغرة المعروفة باسم "MS17-010" لتصيب أجهزة أخرى على نفس الشبكة من أجل تحقيق انتشار سريع للفيروس الإلكتروني
- يمكن لهذا الفيروس أن يصيب الأجهزة الإلكترونية التى تعمل بنظم تشغيل ويندوز من XP إلى ٢٠٠٨
- في حالة إصابة جهاز المستخدم بهذا الهجوم الإلكتروني فإنه سيتم تشفير كافة الملفات الموجودة على جهاز الحاسب ويُطلب من مستخدم (مالك) الجهاز دفع مبلغ فدية يتراوح ما بين ٣٠٠-٦٠٠ $ باستخدام عملة البيتكوين وذلك ليكون المستخدم قادر على استرداد الملفات الخاصة به.
- أكثر الدول اصابة بهذا الفيروس هي المانيا وروسيا واسبانيا وسويسرا والمملكة المتحدة والولايات المتحدة.

كيفية الحماية من هذا الهجوم:

- يجب التأكد من أن جميع برامج الحماية الخاصة بالمستخدمين تم تحديثها.
- التأكد من وجود حزمة تحديثات (Patch) مايكروسوفت .MS17-010 لإغلاق الثغرة المستغلة في الهجوم الإلكتروني.
- التأكد من اغلاق المنافذ الآتية على الخوادم (Port no):١٣٥و٤٤٥
- مراجعة اجراءات التامين الالكتروني داخل المؤسسة.

- يستخدم الهاكرز عناوين بروتوكول الأنترنت (IP)التالية:

"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, 62.1
38.7.231",

الإجراءات الوقائية الواجب اتباعها:

- مراجعة ما إذا تم تحقيق أي اتصال بين حواسب المستخدمين والعناوين السابق.ذكرها من خلال البرامج والأدوات المستخدمة لمراقبة وحماية الشبكات من الهجمات الإلكترونية.
- توعية المستخدمين بخطورة هذه النوعية من الهجمات الإلكترونية وعدم فتح مرفقات البريد الإلكتروني غير الموثوق من مصدرها، كما يجب أيضا التأكد من خلوها من البرامج الخبيثة من خلال برامج الحماية الخاصة بالمستخدم.
- يجب الاحتفاظ بنسخة من الملفات والبيانات الإلكترونية الهامة دوريا على جهاز خارجي منفصل عن الشبكة حتى يتم استعادتها بشكل صحيح في حالة الإصابة.
- التحقق من خلو كافة الأجهزة الإلكترونية من **hashes** المتعلقة بهذا الفيروس والموجودة على هذا الرابط: https://gist.github.com/Blevene/42bed05ecb51c1ca0edf846c0153974a
- في حالة اصابة أحد الاجهزة يرجي الاسراع بفصل الجهاز من الشبكة لمنع انتشار الإصابة والتواصل مع المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات عن طريق البريد الإلكتروني **incident@egcert.eg**