الهيئة الوطنية لأمن وسلامة المعلومات
National Information Security & Safety Authority



فيروسات الفدية

+218 21 361 4115
+218 21 361 4127
+218 21 361 4177
info@nissa.gov.ly
www.nissa.gov.ly
www.cert.gov.ly

إذا حدث الهجوم!

- اعزل الأجهزة المصابة والشبكة فوراً وتعرف على نوع فيروس الفدية.
- قم بتقييم الأضرار والنُسَخ الاحتياطية المتوفرة.
- قم بنشر برمجيات فك التشفير إذا وجدت.
- في حال عدم وجود برامج لفك التشفير، نظِّف الأجهزة واسترجع النسخ الاحتياطية.

أشهر الهجمات

- **PC Cyborg**، أول فيروسات الفدية قام ببرمجته د. جوزيف بوب ونشره بين 20,000 من حضور مؤتمر لمنظمة الصحة العالمية عام 1989. وكانت قيمة الفدية 189$.
- **Cryptolocker**، ظهر في العام 2013 وكان أول من طالب بدفع الفدية بالعملة الرقمية.
- **Locky**، أول من انتشر بشكل واسع من فيروسات الفدية ، ظهر في العام 2016، تم ارسال أكثر 500,000 رسالة تصيد يومياً لنشر الفيروس.
- **Petya**، يستهدف هذا الفيروس سجل الإقلاع الخاص بنظام التشغيل ويندوز ويعطّله عن العمل. له العديد من الأشباه وكان أول ظهور له عام 2016 وانتشر عبر رسائل التصيُّد الإلكتروني.
- **WannaCry**، ظهر في العام 2017 وأصاب ألُوف الأجهزة في أكثر من 150 دولة وانتشر عبر أداة سُميت EternalBlue أنتجتها وكالة الأمن القومي الأمريكية NSA تستغل ثغرةً في نظام التشغيل ويندوز.

فيروسات الفدية

ماهي ؟

هي برمجية خبيثة تقوم بتشفير الملفات والمستندات في حواسيب الضحايا ليطلب المهاجمون بعد ذلك من الضحية دفع الفدية لإرجاع الحواسيب والملفات لأصلها وفك التشفير. ويوجد كذلك طيف منها موجه للهواتف المحمولة. يطلب المهاجمون دفع الفدية بواسطة العملة الرقمية مما يصعّب تعقبهم والتعرف عليهم.

كيف تعمل؟

تبدأ أغلب هجمات فيروس الفدية عَقِب عمليات تصيد الكتروني برسائل ملغمة بمحتويات خبيثة أو عن طريق الدخول لروابط مشبوهة وتنتشر بعدها عن طريق الشبكة أو وسائل نقل الملفات.
تستخدم فيروسات الفدية خوارزميات تشفير (asymmetric encryption algorithms) ذات مفتاحين أحدهما عام والأخر خاص ويقوم المهاجمون بإنشائها بشكل خاص لكل ضحية لحجب الملفات عن المستخدم وتشفيرها بمفتاح لا يملكه إلا المهاجمون.

نشر الفيروس
عن طريق رسائل التصيد والمواقع الملوثة واستغلال نقاط الضعف بالبرمجيات

التنفيذ
تستهدف البرمجية الأنظمة والمستندات والملفات وتنتشر عبر الشبكات

التشفير
يتم اقفال وتشفير الملفات والأنظمة بمفاتيح خاصة يملكها المهاجم

المطالبة
يتم اشعار الضحية بمقدار الفدية وكيفية الدفع مقابل تسليمه مفتاح فك التشفير

الدفع
يطلب المهاجمون الدفع بالعملة الرقمية مقابل تسليم مفاتيح التشفير

وسائل الهجوم

- **رسائل التصيُّد الإلكتروني.**
- **روابط المواقع الخبيثة.**
- **البرمجيات المقرصنة.**
- **شبكات الإنترنت الغير موثوقة.**
- **برتوكولات التحكم بسطح المكتب عن بعد.**
- **وسائل تخزين نقل الملفات الملوثة.**
- **استغلال نقاط الضعف بالبرمجيات.**

أنواعها

- **Locker ransomware**
  يعمل هذا النوع على تعطيل وظائف الجهاز الأساسية مثل الوصول الى سطح المكتب والفأرة.
- **Crypto ransomware**
  يستهدف هذا النوع تشفير الملفات والمستندات في الأساس ولا يُعطل وظائف الجهاز.

الوقاية

- التوقف عن فتح الروابط والرسائل المشبوهة.
- استثمر بقوة في وسائل حماية البريد والأجهزة.
- قم بحفظ المستندات وقواعد البيانات احتياطياً.
- لا تستخدم البرمجيات المقرصنة والمشبوهة.
- لا تغفل وكن حذراً على الدوام.