

تقرير تحليلي عن تحليل البرمجيات الضارة

أولاً: تحليل الملف المشبوه

أدوات التحليل المستخدمة:

- **VirusTotal** : لفحص الملف باستخدام محركات مكافحة الفيروسات المتعددة.
- **Wireshark** : لمراقبة حركة الشبكة وتحليل الاتصالات الصادرة والواردة من الملف.
- **Process Monitor** : لمراقبة العمليات التي يقوم بها الملف على النظام.
- **Ghidra أو IDA Pro** : لتحليل الشيفرة الثنائية للملف.
- **Cuckoo Sandbox** : لتشغيل الملف في بيئة معزولة ومراقبة سلوكه.

ثانياً: تحديد نوع البرمجية الضارة

نوع البرمجية الضارة:

- **فيروس** : إذا كان الملف يقوم بنسخ نفسه إلى ملفات أخرى.
- **دودة** : إذا كان الملف ينتشر عبر الشبكة بدون تدخل المستخدم.
- **تروجان** : إذا كان الملف يبدو كبرنامج شرعي ولكنه يقوم بأعمال ضارة.
- **برنامج فدية** : إذا كان الملف يقوم بتشفير الملفات ويطلب فدية لفك التشفير.

كيفية التعرف على النوع:

- **الفيروس** : مراقبة سلوك النسخ الذاتي.
- **الدودة** : مراقبة الاتصالات الشبكية ومحاولات الانتشار.
- **التروجان** : تحليل الشيفرة لمعرفة الأوامر الضارة المخفية.
- **برنامج الفدية** : البحث عن عمليات التشفير والرسائل التي تطلب الفدية.

ثالثاً: تحليل الشيفرة

تعليمات مشبوهة:

- **الاتصالات الشبكية غير المصرح بها** : مثل فتح منافذ أو إرسال بيانات إلى خوادم خارجية.
- **تعديل ملفات النظام** : مثل تعديل ملفات النظام أو السجل.
- **تشغيل البيانات** : استخدام خوارزميات التشفير بدون سبب واضح.
- **تحميل وتنفيذ شيفرات إضافية** : مثل تنزيل ملفات من الإنترنت وتنفيذها.

رابعاً: طرق التخفيف

توصيات الحماية:

- استخدام برامج مكافحة الفيروسات :لضمان الكشف المبكر عن البرمجيات الضارة.
- تحديث النظام والبرامج بانتظام :لسد الثغرات الأمنية.
- تدريب الموظفين :على كيفية التعرف على الملفات المشبوهة وتجنب فتحها.
- استخدام جدران الحماية :لمراقبة ومنع الاتصالات غير المصرح بها.
- إجراء نسخ احتياطية منتظمة :لضمان استعادة البيانات في حالة الهجوم ببرنامج فدية.