



تحدي الأسبوع ٢ : تحليل البرمجيات الضارة

١. مقدمة

في هذا التقرير، سيتم تحليل ملف مشبوه يشتبه في احتوائه على برنامج ضار. الهدف من هذا التحليل هو تحديد سلوك الملف ونوع البرمجية الضارة وتقديم توصيات لحماية الشبكة.

٢. تحليل الملف

2.1 ملف مشبوه

يمكن أن نفترض أن الملف المشبوه هو ملف تنفيذ (.exe) يُعرف باسم `malicious\_program.exe`.

2.2 أدوات التحليل

استخدمت الأدوات التالية لتحليل الملف:

- **VirusTotal****: لرفع الملف وتحليل ثباته من قبل محركات مكافحة الفيروسات.
- **Cuckoo Sandbox****: لتحليل سلوك الملف في بيئة معزولة.
- **Process Monitor****: لمراقبة العمليات والاتصالات الشبكية الناتجة عن تشغيل الملف.
- **IDA Pro****: أو ****Ghidra**** لتحليل الشيفرة البرمجية إذا كان الملف ثابتاً.

2.3 سلوكيات مشبوهة

خلال التحليل، تم ملاحظة السلوكيات التالية:

- حاول البرنامج إنشاء اتصالات خارجية مع خادم على الإنترنت (IP غير معروف).
- تم تثبيت البرنامج في مجلد النظام (C:\Windows\System32).
- قام البرنامج بتعديل سجل النظام لبدء التشغيل تلقائياً مع Windows.
- حاول الوصول إلى ملفات حساسة، مثل مستندات المستخدم.

3. تحديد نوع البرمجية الضارة

بعد مراجعة السلوكيات، يُعتقد أن هذا البرنامج الضار هو تروجان. وهو لأنه ينفذ سلوكيات خفية مثل تثبيت نفسه دون علم المستخدم وتعديل السجل.

3.1 كيفية التعرف على التروجان

- **التشفير العالي****: غالباً ما يستخدم التروجان تقنية التشفير لإخفاء محتوياته.
- **التواصل مع خادم بعيد****: يتم استخدامه لتحميل وتنفيذ التعليمات البرمجية الضارة.
- **التثبيت الذاتي****: القدرة على تعديل إعدادات النظام وبدء التشغيل تلقائياً.

تحليل الشيفرة

إذا كانت الشيفرة المصدرية متاحة، فسنبحث عن التعليمات التالية القابلة للخطر:

GetProcAddress / LoadLibrary - لمعرفة ما إذا كان يتم استدعاء DLL ضارة.

VirtualProtect - استخدام دوال مثل CreateRemoteThread أو VirtualProtect قد تشير إلى قدرات مثل الحقن في الذاكرة.

تعليمات برمجية تحاول الوصول إلى بيانات المستخدم أو تعديل الملفات.

مثال للتعليمات الضارة:

```
```c
HKEY hKey;
RegOpenKeyEx(HKEY_CURRENT_USER,
"Software\\Microsoft\\Windows\\CurrentVersion\\Run", NULL,
KEY_ALL_ACCESS, &hKey);
RegSetValueEx(hKey, "MaliciousApp", 0, REG_SZ, (BYTE *)path, strlen(path) + 1);
```
```

5. طرق التخفيف

5.1 التوصيات لحماية الشبكة

** - تثبيت برامج مكافحة الفيروسات: يجب التأكد من تحديث برامج مكافحة الفيروسات والحماية الخاصة بالشبكة.

** - تحديث الأنظمة بشكل دوري: للحفاظ على نظام التشغيل والتطبيقات محدثة لحماية الثغرات.

** - التوعية والتدريب: يجب أن يتلقى الموظفون تدريباً حول كيفية التعرف على الملفات المشبوهة والتقنيات المستخدمة في الهجمات.

** - استخدام جدران الحماية: تطبيق جدران الحماية على الشبكة لتحسين الأمان ومنع الاتصالات المشبوهة.

** - التنفيذ في بيئة معزولة: استخدام أجهزة افتراضية أو صناديق رملية (Sandbox) لتحليل الملفات المشتبه بها قبل تشغيلها في النظام الأساسي.

6. الخاتمة

يتطلب تحليل البرمجيات الضارة دقة وانتباهاً كبيرين. من المهم أن تتخذ المؤسسات تدابير أمنية وقائية جيدة، بالإضافة إلى التعليم المناسب للموظفين، لتقليل فرص الإصابة بالبرمجيات الضارة.