

□ تحدي الأسبوع ٢: تحليل البرمجيات الضارة

الحل

تقرير تحليل البرمجيات الضارة

مقدمة

في هذا التحدي، سنقوم بتحليل ملف مشبوه قد يكون يحتوي على برنامج ضار لتحليل سلوكه وتحديد نوعه، وأخيرًا اقتراح طرق للتخفيف من مخاطره. يتناول التقرير الأدوات المستخدمة في التحليل، والطريقة المستخدمة لتحديد نوع البرنامج الضار، وتحليل الشيفرة إن كانت متاحة، إضافة إلى أساليب الحماية المقترحة.

القسم الأول : تحليل الملف المشبوه

١. أدوات التحليل المستخدمة :

لتحليل هذا الملف المشبوه، سيتم استخدام الأدوات التالية :

- PE Studio : لتحليل الملفات التنفيذية (.exe) واستخراج معلومات حول المكتبات المرتبطة بالملف والتي قد تشير إلى وظائف ضارة.
- VirusTotal : موقع لتحميل وتحليل الملفات باستخدام العديد من محركات مكافحة الفيروسات المعروفة.
- Cuckoo Sandbox : لاختبار الملف المشبوه في بيئة افتراضية وتحليل سلوكه دون تعريض الشبكة للخطر.
- Process Explorer و Process Monitor : لمراقبة العمليات التي ينفذها الملف عند تشغيله.
- Wireshark : لتحليل حركة الشبكة ومعرفة ما إذا كان البرنامج الضار يحاول الاتصال بخادم خارجي.

٢. خطوات التحليل :

١. التأكد من طبيعة الملف : أولاً يتم فحص الملف باستخدام PE Studio و VirusTotal للتحقق مما إذا كانت هناك أي علامات معروفة على البرامج الضارة.
٢. تحليل سلوك الملف : إذا لم يكن هناك استنتاج قاطع، يتم تشغيل الملف في Cuckoo Sandbox لمراقبة سلوكه في بيئة افتراضية وملاحظة أي محاولات لإنشاء عمليات جديدة، أو التواصل مع الخوادم الخارجية، أو محاولات التعديل على ملفات النظام.
٣. تحليل حركة الشبكة : استخدام Wireshark أثناء تشغيل الملف لمراقبة أية محاولات للاتصال بخوادم خارجية أو إرسال بيانات غير مرغوبة.

القسم الثاني : تحديد نوع البرنامج الضار

بناءً على سلوك الملف، يمكننا محاولة تحديد نوع البرنامج الضار. الأنواع الشائعة تشمل:

١. الفيروسات : تقوم بتعديل ملفات النظام أو نسخ نفسها.
٢. الدودة : تعتمد على الشبكة للانتشار وتقوم بإرسال نفسها عبر أجهزة متعددة.
٣. التروجان : يخدع المستخدم ويقوم بتثبيت نفسه لفتح باب خلفي أو سرقة بيانات.
٤. برامج الفدية : تقوم بتشفير ملفات النظام وتطلب فدية لفك التشفير.

استنتاج نوع البرنامج الضار:

- التروجان : إذا كان الملف يحاول إرسال معلومات إلى خادم خارجي أو إنشاء باب خلفي يمكن الوصول إليه.
- برنامج الفدية : إذا لاحظنا أن الملف يقوم بتشفير بيانات النظام وترك رسالة فدية.

القسم الثالث : تحليل الشيفرة

إذا كانت الشيفرة المصدرية متاحة، يمكننا البحث عن التعليمات البرمجية المشبوهة مثل :

- الأوامر المتعلقة بإدارة العمليات : مثل `CreateProcess` و `ShellExecute` ، والتي قد تشير إلى محاولات لفتح باب خلفي.
- أوامر التشفير : مثل `EncryptFile` ، والتي قد تشير إلى برامج الفدية.
- محاولات الاتصال بخوادم خارجية : باستخدام دوال الشبكات مثل `HttpOpenRequest` أو `Socket` والتي قد تشير إلى محاولة اتصال بخادم خارجي.

القسم الرابع : توصيات الحماية

١. التحديثات الأمنية : التأكد من تحديث جميع الأنظمة بشكل دوري لضمان الحماية ضد الثغرات الأمنية.
٢. الحماية عبر الجدران النارية : استخدام جدران نارية تمنع حركة المرور غير المرغوب فيها.
٣. تثقيف الموظفين : زيادة وعي الموظفين حول مخاطر فتح الملفات غير المعروفة.
٤. النسخ الاحتياطي للبيانات : إعداد نظام نسخ احتياطي دوري لجميع البيانات المهمة لمواجهة برامج الفدية.
٥. فحص الملفات قبل فتحها : استخدام حلول مكافحة الفيروسات لفحص الملفات قبل فتحها، خصوصاً ملفات البريد الإلكتروني.

الخاتمة

يوضح هذا التقرير خطوات تحليل ملف مشبوه وتحديد نوع البرنامج الضار الذي قد يحتوي عليه. كما قدمنا توصيات للحد من المخاطر وحماية النظام والشبكة.