

تحليل البرمجيات الضارة وتحديد نوعها

1. تحليل الملف

1.1 افتراض الملف

تم اختيار ملف بامتداد exe ليمثل عينة مشبوهة. تم الحصول على الملف من مستودع مفتوح المصدر للبرمجيات الضارة يُعرف باسم theZoo، وهو مستودع يحتوي على عينات حقيقية من البرمجيات الضارة لأغراض أكاديمية. تمت هذه الخطوة وفق ضوابط أمنية صارمة لتجنب أي تأثير ضار على الشبكة.

1.2 أدوات التحليل

تم استخدام الأدوات التالية لتحليل الملف:

Wireshark: أداة لتحليل حركة الشبكة، تم استخدامها لمراقبة أي نشاط غير مصرح به للملف.

Process Monitor (Procmon): تم استخدام هذه الأداة لمراقبة العمليات التي يقوم بها الملف داخل النظام، مثل إنشاء وتعديل الملفات.

VirusTotal: موقع على الإنترنت يتيح فحص الملف عبر محركات فحص متعددة لتحديد ما إذا كان الملف يحتوي على سلوك ضار.

1.3 نتائج التحليل

Wireshark: أظهرت نتائج التحليل أن الملف يحاول الاتصال بخادم خارجي باستخدام بروتوكول HTTP. هذا السلوك يُعتبر غير مألوف ويدل على محاولة غير مصرح بها للوصول إلى الشبكة الخارجية، مما يعزز احتمال أن الملف ضار.

Process Monitor: كشف تحليل عمليات النظام أن الملف يقوم بإنشاء وتعديل ملفات داخل مجلد النظام بدون إذن، وهو سلوك ضار يمكن أن يؤدي إلى تغيير إعدادات النظام.

VirusTotal: أظهر الفحص عبر VirusTotal أن عدة محركات فحص تعرفت على الملف كبرنامج ضار من نوع Trojan، مما يؤكد الشكوك حول خطورته.

2. تحديد نوع البرمجية الضارة

بناءً على السلوكيات المرصودة، تم تحديد نوع البرمجية الضارة كـ Trojan. ويعود ذلك إلى أن الملف:

يحاول إجراء اتصال خارجي مشبوه.

يقوم بتعديل ملفات النظام بدون إذن مسبق.

التمييز بين الأنواع الأخرى

يمكن تمييز Trojan عن أنواع البرمجيات الضارة الأخرى، مثل الفيروسات والديدان، بناءً على سلوكياته. ف Trojan يتميز بمحاولاته للتواصل الخارجي أو التحكم عن بعد بالجهاز، بينما تهدف الفيروسات عادة إلى إتلاف الملفات بشكل مباشر، في حين تهدف الديدان إلى الانتشار بين الأجهزة.

3. تحليل الشيفرة (إن أمكن)

في حال توفر الشيفرة المصدرية، يُفضل تحليلها للبحث عن أي تعليمات برمجية مشبوهة تشير إلى نوايا ضارة مثل التحكم عن بعد أو التجسس. لم يكن من الممكن الحصول على الشيفرة المصدرية لهذا الملف، ولكن سلوكه يوحي بوجود تعليمات خبيثة تهدف إلى سرقة البيانات أو التجسس على المستخدم.

4. طرق التخفيف

بناءً على نتائج التحليل وتحديد نوع البرمجية الضارة، نوصي بتنفيذ الإجراءات التالية لتقليل خطر الإصابة مستقبلاً:

- استخدام برنامج حماية موثوق: ينبغي تثبيت برنامج مكافحة الفيروسات قوي يمكنه اكتشاف البرمجيات الضارة من هذا النوع وتعطيلها قبل أن تتمكن من التأثير على النظام.
- تفعيل جدران الحماية: يساعد جدار الحماية في منع محاولات الاتصال الخارجي غير المصرح بها من البرمجيات الضارة.
- التحديث الدوري للنظام: تضمن التحديثات الأمنية إغلاق الثغرات التي قد تستغلها البرمجيات الضارة للوصول إلى النظام.
- التوعية الأمنية: يجب توعية المستخدمين بعدم تحميل أو تشغيل أي ملفات من مصادر غير موثوقة، خاصة الملفات التنفيذية (.exe).