

تحليل الملف :

تم فحص الملف باستخدام أداة VirusTotal ، والتي كشفت عن سلوك مشبوه للملف. تم ملاحظة النقاط التالية:

1. الملف له امتداد .exe ، مما يشير إلى أنه ملف تنفيذي قابل للتشغيل.
2. تم رصد محاولات الملف للوصول إلى مناطق محمية من النظام، بما في ذلك السجلات وملفات النظام.
3. كما تم ملاحظة قيام الملف بإنشاء اتصالات شبكية خارجية، مما يشير إلى احتمالية وجود نشاط مشبوه.

تحديد نوع البرنامج الضار :

بناءً على السلوك المشبوه المكتشف، فإن هذا الملف يُظهر خصائص تروجان. التروجانات هي برامج ضارة تتظاهر بكونها برامج مشروعة لخداع المستخدم والوصول إلى بياناته وموارد النظام دون إذنه. في هذه الحالة، يبدو أن الملف يحاول الوصول إلى مناطق محمية من النظام واستخدام اتصالات الشبكة للاتصال بخوادم خارجية، مما يتوافق مع سلوك التروجان.

طرق الحماية الموصى بها :

1. للحماية من هذا النوع من البرامج الضارة، يوصى باتخاذ الإجراءات التالية:
 - 1. تفعيل برامج الحماية من الفيروسات والتهديدات المتقدمة على النظام وتحديثها باستمرار. هذا سيساعد في اكتشاف ومنع هذا النوع من التروجانات.
 - 2. تطبيق إعدادات الحماية الأساسية على النظام، مثل تمكين جدار الحماية، وتقييد الوصول إلى المناطق الحساسة، وتحديث نظام التشغيل والبرامج بأحدث الإصدارات.
 - 3. توعية المستخدمين بممارسات الأمان السليمة، مثل عدم فتح الملفات أو الروابط المشبوهة، والتحقق من مصدر البرامج قبل تثبيتها.
 - 4. إجراء نسخ احتياطي منتظم للبيانات والتأكد من إمكانية استعادتها في حال وقوع هجوم.

إذا استمرت المشكلة أو لاحظت أي سلوك مشبوه إضافي، فمن المستحسن إجراء مزيد من التحقيقات المتعمقة باستخدام أدوات التحليل المتقدمة.