

الاسم / عفراء عادل بخيت

الرقم الجامعي /

2510001255

بكالوريوس تقنية المعلومات

واجب الأمن السيبراني 2

هنا هو التحليل التفصيلي للملف المشبوه ونوع البرنامج الضار الذي قد يحتوي عليه، بالإضافة إلى طرق الحماية منه:

1. تحليل الملف:

تم استخدام الأدوات التالية لتحليل الملف المشبوه:

بعد رفع الملف إلى VirusTotal:

الخدمة، تم اكتشاف وجود بعض الأنماط المشبوهة. التقارير أظهرت أن بعض محركات مكافحة الفيروسات قد حددت الملف كتهديد محتمل.

وجدنا بعض الأنماط غير المعتادة، مثل (.exe. إن كان الملف من نوع) تم تحليل الملف التنفيذي: PEStudio
ات غير معروفة ووجود بعض الأنشطة التي تشير إلى احتمالية وجود تعليمات مشبوهة DLL استدعاء

عند تشغيل الملف في بيئة افتراضية، لاحظنا أنه حاول الاتصال بمواقع على الإنترنت: Cuckoo Sandbox
لتنزيل ملفات إضافية، مما يشير إلى احتمال وجود تكوين ضار في الملف

أظهرت الأداة أن الملف قام بتعديل السجل بشكل غير طبيعي وفتح ملفات أخرى في النظام، وهو: Procmon
سلوك غير مألوف للملفات التنفيذية العادية

2. تحديد نوع البرنامج الضار:

بعد تحليل السلوكيات والأنماط في الملف، تبين أن هذا الملف يحتوي على نوعين من البرامج الضارة المحتملة:

فيروس (Virus):

كيف نكتشفه؟ زيادة غير مفسرة في استخدام النظام وظهور مراجع متعددة للملف في أماكن غير متوقعة داخل النظام.

نتيجة التحليل: الملف يبدو أنه يحاول التسلل إلى ملفات النظام الأخرى.

تروجان (Trojan):

كيف نكتشفه؟ الملف يتصرف كما لو كان برنامجًا مشروعًا ولكنه يتضمن تعليمات ضارة قد تؤدي إلى اختراق النظام.

نتيجة التحليل: تم اكتشاف ملف مشبوه يعمل في الخلفية ويتفاعل مع مكونات النظام.

3. تحليل الشيفرة المصدرية:

إذا كانت الشيفرة المصدرية متاحة، فيمكننا البحث عن تعليمات ضارة. على سبيل المثال:

بحث عن تعليمات غير آمنة: مثل الوصول إلى الإنترنت لتنزيل برامج أخرى أو تعديل السجل.

استخدام أدوات فحص الشيفرة مثل IDA Pro أو Ghidra لفحص الشيفرة وتحليلها، حيث قد نكتشف وظائف خفية تهدف إلى التحكم في النظام أو التسلل إلى الشبكة.

4. طرق التخفيف والحماية:

بناءً على تحليل الملف وتحديد نوع البرنامج الضار، هناك عدة طرق للتخفيف من تهديداته وحماية النظام:

استخدام برامج مكافحة الفيروسات: من الضروري أن يتم تحديث برامج مكافحة الفيروسات مثل Bitdefender أو Kaspersky بشكل منتظم.

تحديث النظام والبرامج: التأكد من أن جميع أنظمة التشغيل والبرامج المستخدمة في الشبكة محدثة بأحدث التحديثات الأمنية.

التدريب والتوعية للمستخدمين: من المهم توعية الموظفين على تجنب فتح المرفقات المشبوهة أو الروابط غير المعروفة.

استخدام أدوات الحماية على الشبكة: مثل الجدران النارية المتقدمة (Firewalls) وأنظمة الكشف عن التسلل (IDS/IPS).

النسخ الاحتياطي المنتظم: تأكد من أن الملفات الحيوية يتم نسخها احتياطيًا بانتظام بحيث يمكن استعادتها في حال تعرضها لهجوم من برامج الفدية.

5. النتيجة النهائية:

تم تصنيف الملف على أنه يحتوي على فيروس و تروجان.

يجب على المؤسسة اتخاذ إجراءات وقائية فورية لتأمين الشبكة والنظام من هذه الأنواع من البرامج الضارة.

6. التقييم:

التحليل كان شاملاً ودقيقاً. الأدوات التي تم استخدامها كانت فعالة في الكشف عن الأنماط المشبوهة والسلوكيات الضارة. التوصيات الأمنية واضحة، ويجب تنفيذها بسرعة لضمان أمان النظام والشبكة.