

تقرير تحليل البرمجيات الضارة

مقدمة

تم اكتشاف ملف مشبوه في شبكة المؤسسة، ويعتقد أنه يحتوي على برنامج ضار. يهدف هذا التقرير إلى تحليل الملف لفهم سلوكه، تحديد نوع البرمجية الضارة، وطرق الحماية الموصى بها.

تحليل الملف

لنفترض أن الملف المشبوه هو ملف تنفيذي بامتداد .exe. باستخدام أدوات تحليل مثل:

1. كلاسيك أداة تحليل البرمجيات الضارة (Static Analysis Tools) مثل: PEiD: لفحص نوع الملف إذا كان ملفًا تنفيذيًا عاديًا أو يحتوي على مشغرات.
1. CFF Explorer: لفحص المعلومات الداخلية عن الملف.
2. أدوات التحليل الديناميكي (Dynamic Analysis Tools) مثل: Sandboxie: لتشغيل الملف في بيئة آمنة ومعزولة.
2. Process Monitor: لمراقبة عمليات الملفات والنشاطات التي يقوم بها الملف أثناء تشغيله.

تحديد نوع البرمجية الضارة

بعد إجراء التحليل، لاحظنا سلوكيات غير طبيعية، مثل:

- محاولة الاتصال بخوادم خارجية.
 - إنشاء ملفات جديدة أو تعديل سجل النظام.
 - تنفيذ عمليات ذات صلاحيات مرتفعة.
- بناءً على هذه السلوكيات، يمكن تحديد نوع البرنامج الضار. هناك بعض الأنواع الشائعة:
- فيروس: يعدل أو ينسخ نفسه إلى ملفات أخرى.
 - دودة: تنتشر عبر الشبكة دون حاجة لتدخل المستخدم.
 - تروجان: يتحايل على المستخدم لتثبيته، ثم يقوم بإجراءات ضارة.
 - برنامج فدية: يقوم بتشفير البيانات ويطلب فدية للإفراج عن البيانات.
- إذا كان السلوك يشير إلى التشفير ثم الطلب لفدية، فمن المحتمل أن يكون البرنامج ضارًا من نوع برنامج فدية.

تحليل الشفرة

في حال توفر الشيفرة المصدرية للملف المشبوه، يجب البحث عن تعليمات قد تشير إلى سلوك ضار:

- دالات الأسلوب (Function Calls) مثل CreateProcess و WriteFile: قد تشير إلى إنشاء عمليات جديدة وتعديل الملفات.
 - الوصول غير المصرح به إلى ملفات النظام باستخدام دالات مثل OpenFile أو RegOpenKeyEx يمكن أن يدل على سلوك ضار.
- ### طرق التخفيف

بعد تحليل الملف وتحديد نوع البرمجية الضارة، إليك بعض التوصيات لحماية الشبكة:

1. تحديث البرمجيات: تأكد من تحديث جميع أنظمة التشغيل والبرمجيات لتقليل الثغرات.
2. استخدام برامج الحماية: تثبيت برامج مضادة للفيروسات متقدمة مع تحديثات مستمرة.
3. توعية المستخدمين: إجراء تدريبات دورية للموظفين حول كيفية التعرف على الفيروسات والنقر على الروابط المشبوهة.
4. استخدام جدران الحماية: تأكد من تكوين جدران الحماية لحماية الشبكة ضد الوصول غير المصرح به.
5. عمل نسخ احتياطية دوريًا: من المهم الاحتفاظ بنسخ احتياطية من البيانات لتقليل الأضرار في حال هجوم برنامج

فدية.

خاتمة

من خلال هذا التحليل، قمنا بتحديد سلوك الملف ونوع البرمجية الضارة المحتملة. قدمنا أيضًا مجموعة من التوصيات لحماية النظام والشبكة. يجب على المؤسسة اتخاذ هذه التوصيات بجدية لتعزيز الأمان السيبراني وتقليل المخاطر المستقبلية