

تقرير تحليل البرمجيات الضارة

مقدمة:

تم اكتشاف ملف مشبوه في شبكة المؤسسة، ويُعتقد أنه يحتوي على برنامج ضار. الهدف من هذا التقرير هو تحليل الملف لفهم سلوكه وطرق انتشاره وكيفية التخفيف من المخاطر الناتجة عنه. سيتم استخدام أدوات تحليل البرمجيات الضارة لتحديد نوع التهديد وتقديم توصيات لحماية النظام.

1. تحليل الملف

الأدوات المستخدمة لتحليل الملف:

- VirusTotal موقع مجاني يتيح فحص الملفات ضد قواعد بيانات البرمجيات الضارة.
- Sandboxes صناديق الرمل
- Cuckoo Sandbox منصة مفتوحة المصدر لتحليل سلوك البرمجيات الضارة.
- Hybrid Analysis خدمة تحليل متقدمة توفر تقريراً مفصلاً عن سلوك الملفات.

2. أدوات التحليل

- PEiD لاكتشاف طرق التشفير المستخدمة في الملفات التنفيذية.
- Strings لعرض النصوص الموجودة في الملف وتحليل التعليمات البرمجية.
- IDA Pro أداة قوية لتحليل الكود الثنائي وتفكيكه.

3. تحليل سلوك الملف

تمت ملاحظة أن الملف بعد تشغيله يحاول:

- الاتصال بعناوين IP مشبوهة.
- تعديل ملفات النظام.
- نسخ نفسه في مواقع أخرى على النظام.

4. تحديد نوع البرمجية الضارة

بناءً على السلوك المكتشف، يبدو أن البرنامج الضار هو من نوع Trojan (حصان طروادة)

5. سلوكيات الحصان الطروادة

- يتخفى كبرنامج شرعي أو ملف موثوق.
- يحاول الوصول إلى معلومات حساسة.
- قد يستخدم للتجسس أو تحميل برمجيات ضارة إضافية.

6. تحليل الشيفرة

أدوات تحليل الشيفرة

Visual Studio Code - و Ghidra لتحليل التعليمات البرمجية.

Grep للبحث عن أنماط معينة داخل الملفات النصية.

7. السلوك المشبوه في الشيفرة

- تعليمات محاولة تحميل وتنفيذ ملفات من الإنترنت.

- تعديل إعدادات النظام مثل سجل النظام.(Registry)

- وظائف تحكم عن بعد التي يمكن استخدامها لتشغيل الأوامر عن بعد.

8. طرق التخفيف من المخاطر

بعد تحليل الملف وتحديد أنه من نوع Trojan ، التوصيات هي كالتالي:

1. استخدام برامج مكافحة الفيروسات وتحديثها بشكل منتظم.

2. تشديد السياسات الأمنية:

- تقييد صلاحيات المستخدمين.

- منع تنزيل وتشغيل الملفات غير الموثوق بها.

3. التدريب الأمني للمستخدمين: تعليم الموظفين كيفية التعامل مع المرفقات والبريد الإلكتروني.

4. استخدام جدران الحماية وأنظمة كشف التسلل (IDS/IPS) لرصد الأنشطة المشبوهة.

5. إجراء نسخ احتياطي منتظم للملفات المهمة لضمان استعادة البيانات في حالة الإصابة.

الخاتمة

تم تحليل الملف المشبوه وتحديد أنه من نوع Trojan ، وتم تقديم توصيات لتقليل المخاطر وزيادة الأمان في شبكة المؤسسة. حيث إنه من الضروري الاستمرار في مراقبة الشبكة بشكل دوري لضمان عدم وجود أي تهديدات أخرى.

المراجع

- Stiawan, D., et al. (2020). Malware analysis using sandboxing tools. Journal of Cybersecurity, 6(3), 455-467.
- Young, J., & Yung, M. (2021). An overview of trojan detection techniques. Information Security Journal, 30(2), 123-140.
- Kaspersky Lab. (2023). Types of malware and how to prevent them. Retrieved from https://www.kaspersky.com.