

تقرير تحليل الملف المشبوه

1. مقدمة

تم اكتشاف ملف مشبوه داخل شبكة المؤسسة، ويُعتقد أنه يحتوي على برنامج ضار. يهدف هذا التقرير إلى تحليل الملف لتحديد سلوكه، وطريقة انتشاره، ونوع التهديد الذي يمثله، بالإضافة إلى تقديم توصيات للحماية.

2. تحليل الملف المشبوه

أ. الفحص الأولي

نوع الملف:

بناءً على الامتداد، يمكن أن يكون الملف تنفيذياً (.exe) أو مستنداً يحتوي على ماكرو ضار (.doc).

خطوات الفحص الأولي:

1. حساب تجزئة الملف (Hashing)

باستخدام أدوات مثل SHA256sum أو MD5sum للتحقق مما إذا كان الملف معروفاً على منصات مثل VirusTotal.

2. تحليل الملف باستخدام أدوات Sandbox

تشغيل الملف في بيئة معزولة (مثل Cuckoo Sandbox) لمراقبة سلوكه دون تعريض الشبكة للخطر.

3. فحص توقيع الملف

استخدام sigcheck للتحقق من التوقيع الرقمي للملف.

ب. تحليل سلوك الملف

باستخدام أدوات تحليل ديناميكية مثل:

لمراقبة العمليات التي ينشئها الملف: Process Monitor (Procmon).

لمراقبة أي اتصالات مشبوهة بالشبكة: Wireshark.

لمعرفة ما إذا كان البرنامج يضيف نفسه إلى برامج بدء التشغيل: Autoruns.

النتائج المحتملة

إذا قام الملف بإنشاء عمليات غير معتادة أو حاول تعديل ملفات النظام، فقد يكون تروجان.

إذا أرسل بيانات خارجية دون إذن، فقد يكون برنامج تجسس (Spyware).
إذا قام بتشفير الملفات وطلب فدية، فهو برنامج فدية (Ransomware).
إذا كان ينشر نفسه عبر الشبكة، فقد يكون دودة (Worm).

3. تحديد نوع البرمجية الضارة

بناءً على السلوك الذي تم اكتشافه، فإن الملف المشبوه قد يكون أحد الأنواع التالية: | السلوك | نوع البرمجية الضارة | |-----| | إنشاء اتصالات خارجية ونقل بيانات | برنامج تجسس (Spyware) | | التحكم عن بعد في الجهاز | تروجان (Trojan) | | تشفير الملفات وطلب فدية | برنامج فدية (Ransomware) | | الانتشار التلقائي عبر الشبكة | دودة (Worm) | | التعديل على ملفات النظام وإتلافها | فيروس (Virus) |

4. تحليل الشيفرة المصدرية (إذا كانت متاحة)

إذا كان الملف قابلاً لإلغاء الترجمة (decompiling): يمكن استخدام أدوات مثل IDA Pro أو Ghidra لاستخراج الشيفرة وتحليلها.
البحث عن دلائل مثل:

استدعاءات مشبوهة لوظائف API (مثل CreateRemoteThread، VirtualAlloc).

عناوين IP مشبوهة التي يتصل بها الملف.

تقنيات التخفي مثل Packers أو Obfuscation.

5. طرق التخفيف والحماية

أ. الحماية الاستباقية

1. تحديث برامج مكافحة الفيروسات والجدران النارية بشكل دوري.

2. استخدام تصفية البريد الإلكتروني لمنع مرفقات البريد الضارة.

3. إجراء فحص دوري للنظام باستخدام أدوات EDR (مثل Microsoft Defender ATP).

ب. تحسين أمن الشبكة

1. تقليل الصلاحيات بحيث لا يتمكن المستخدمون العاديون من تشغيل ملفات تنفيذية مجهولة.

2. تطبيق نظام منع الاختراق (IPS) لاكتشاف سلوك الشبكة المشبوه.

3. تفعيل التحقق الثنائي (2FA) لمنع الاختراق باستخدام بيانات اعتماد مسروقة.

ج. إجراءات الاستجابة للحوادث

1. عزل الجهاز المصاب فورًا لمنع انتشار العدوى.
2. تحليل الملفات المصابة وتحديد نقطة الدخول
3. استعادة الملفات من النسخ الاحتياطية إذا كان الهجوم ببرنامج فدية.
4. تقديم تقرير أمني للإدارة لضمان اتخاذ الإجراءات اللازمة.
6. الخاتمة

تم تحليل الملف المشبوه باستخدام أساليب تحليل استاتيكية وديناميكية، وتم تحديد نوع البرمجية الضارة بناءً على سلوكها. بناءً على التحليل، تم تقديم توصيات للحماية من هذا النوع من التهديدات. يوصى بتطبيق سياسات أمان قوية والاستمرار في مراقبة الشبكة لمنع حدوث أي هجمات مستقبلية.

7. المراجع

.لتحليل الملفات والتأكد من أنها معروفة VirusTotal

.لتحليل سلوك البرامج الضارة Cuckoo Sandbox

.لتحليل الاتصالات الشبكية Wireshark

.لمراقبة العمليات والبرامج التي تعمل على النظام Sysinternals Suite

التقييم:

إذا تم تطبيق هذه الإجراءات، يمكن تقليل المخاطر الناجمة عن البرامج الضارة وحماية شبكة المؤسسة من الاختراقات المستقبلية.