Endpoints and Systems Lab1

الأجهزة/النقاط الطرفية والأنظمة - تطبيق عملي 1

إعداد: إسماعيل محمد قطان

Prepared by: Ismail Muhammed Kattan

التاريخ: أكتوبر/ تشرين الأول 2025

Date: October, 2025



## دليل عملي:Alternate Data Streams (ADS)

## **📋 نظرة عامة**

**Alternate Data Streams (ADS)**

هي ميزة في نظام ملفات NTFS تسمح بتخزين بيانات إضافية مخفية داخل الملفات دون تغيير حجمها الظاهر. هذه الميزة يمكن استخدامها بشكل مشروع، لكنها قد تُستغل أيضاً لإخفاء البرمجيات الخبيثة.

## **🪜 خطوات التنفيذ العملي**

### **الخطوة 1: إنشاء ملف نصي جديد**

افتح **Command Prompt** واكتب الأمر التالي:

| echo This is my text file. > sample.txt |
| --- |

**التحقق من محتوى الملف:**

| type sample.txt |
| --- |

**النتيجة المتوقعة:**

| This is my text file. |
| --- |

### **الخطوة 2: عرض معلومات الملف في المجلد**

استخدم الأمر التالي لعرض تفاصيل الملف:

| dir sample.txt |
| --- |

**الملاحظة:** ستلاحظ أن حجم الملف صغير (مثلاً **22 بايت**).

### 

### **الخطوة 3: إضافة بيانات مخفية في Alternate Data Stream**

الآن سنقوم بإضافة بيانات مخفية باستخدام ADS:

| echo You can't see this data. > sample.txt:secret.txt |
| --- |

**⚠️ ملاحظة مهمة:**

* لاحظ استخدام علامة النقطتين **(:)** لربط البيانات المخفية بالملف الأساسي.
* اسم التيار المخفي هنا هو secret.txt.

### **الخطوة 4: عرض البيانات المخفية**

لفتح والاطلاع على البيانات المخفية داخل الـ ADS:

| notepad sample.txt:secret.txt |
| --- |

**النتيجة:** سيُفتح Notepad ويعرض النص:

| You can't see this data. |
| --- |

**🔍 اختبار الاختفاء:**

إذا قمت بتنفيذ الأمر:

| dir |
| --- |

**لن ترى ملفاً منفصلاً باسم** secret.txt!

### 

### **الخطوة 5: التحقق من المساحة على القرص**

**ملاحظة هامة:**

* حتى بعد إضافة البيانات المخفية، **الحجم الظاهر للملف لا يتغير**.
* لكن **المساحة الحرة في القرص تقل** لأن البيانات موجودة فعلياً في الـ ADS.
* هذا يجعل اكتشاف البيانات المخفية أصعب للمستخدم العادي.

### **الخطوة 6: عرض الـ ADS باستخدام أدوات حديثة**

في الإصدارات الحديثة من Windows، يمكنك استخدام الأمر التالي:

| dir /r |
| --- |

**النتيجة المتوقعة:**

| sample.txt  sample.txt:secret.txt:$DATA |
| --- |

**التفسير:**

* sample.txt → الملف الرئيسي
* sample.txt:secret.txt:$DATA → تيار البيانات المخفي

هذا يؤكد أن الملف يحتوي على **Alternate Data Stream** مخفي.

**📊 جدول مقارنة: الملف العادي ADS vs**

| **الخاصية** | **الملف العادي** | **Alternate Data Stream** |
| --- | --- | --- |
| **الظهور في dir** | ✅ يظهر | ❌ لا يظهر (إلا مع /r) |
| **الحجم الظاهر** | يتغير مع المحتوى | لا يتغير |
| **المساحة المستخدمة** | تحتسب | تحتسب (لكن مخفية) |
| **إمكانية الوصول** | مباشر | يحتاج معرفة الاسم |
| **الاكتشاف** | سهل | صعب بدون أدوات |

## **⚙️ أوامر إضافية مفيدة**

### **عرض جميع ADS في ملف:**

| dir /r sample.txt |
| --- |

### **حذف ADS من ملف:**

**الطريقة 1: حذف التيار المحدد**

| type nul > sample.txt:secret.txt |
| --- |

**الطريقة 2: حذف جميع ADS (بنسخ الملف)**

| copy sample.txt sample\_clean.txt /b |
| --- |

### **قراءة محتوى ADS من سطر الأوامر:**

| more < sample.txt:secret.txt |
| --- |

## **🔐 استخدامات مشروعة لـ ADS**

1. **تخزين Metadata:** معلومات إضافية عن الملف (المؤلف، التصنيف، إلخ).
2. **علامات الأمان:** Windows يستخدمها لوضع علامة "Downloaded from Internet".
3. **الأيقونات المخصصة:** تخزين أيقونات مخصصة للمجلدات.
4. **ملاحظات التطبيقات:** بعض التطبيقات تخزن إعدادات خاصة.

## 

## **⚠️ المخاطر الأمنية واستغلال ADS**

### **كيف يمكن استغلال ADS من قبل المهاجمين؟**

#### **1. إخفاء البرمجيات الخبيثة**

| type malware.exe > innocentfile.txt:hidden.exe |
| --- |

* الملف innocentfile.txt يبدو بريئاً تماماً
* لكنه يحتوي على برنامج خبيث مخفي

#### **2. تنفيذ الكود المخفي**

| wscript innocentfile.txt:malicious.vbs |
| --- |

* يمكن تشغيل سكريبتات خبيثة مخفية

#### **3. سرقة البيانات**

| type sensitive\_data.txt > normalfile.jpg:data.txt |
| --- |

* إخفاء بيانات حساسة داخل ملفات تبدو عادية

## 

## **🛡️ طرق الكشف والحماية**

### **1. استخدام أدوات سطر الأوامر**

| dir /r /s C:\ |
| --- |

* يعرض جميع الـ ADS في القرص C

### **2. استخدام PowerShell**

| Get-Item sample.txt -Stream \* |
| --- |

**أو للبحث في مجلد كامل:**

| Get-ChildItem -Recurse | Get-Item -Stream \* | Where-Object Stream -ne ':$DATA' |
| --- |

### **3. أدوات متخصصة**

| **الأداة** | **الوصف** |
| --- | --- |
| **Streams (Sysinternals)** | أداة مجانية من Microsoft لعرض وحذف ADS |
| **LADS** | List Alternate Data Streams |
| **AlternateStreamView** | واجهة رسومية لعرض ADS |

### **4. استخدام Streams.exe من Sysinternals**

**تحميل الأداة:**

<https://docs.microsoft.com/en-us/sysinternals/downloads/streams>

**الاستخدام:**

| streams -s C:\Path\To\Folder |
| --- |

## **📝 أفضل الممارسات الأمنية**

### **للمستخدمين:**

✅ **افحص الملفات المشبوهة:**

| streams -s C:\Path\To\Folder |
| --- |

✅ **احذف ADS غير المعروفة:**

| streams -d file.txt |
| --- |

✅ **استخدم برامج مكافحة الفيروسات محدثة** تدعم فحص ADS.

### **لمحللي الأمن (SOC Analysts):**

✅ **المراقبة المستمرة:**

* راقب إنشاء ADS في المجلدات الحساسة
* استخدم SIEM لتسجيل أحداث ADS

✅ **التحليل الجنائي:**

* افحص ADS في جميع الملفات المشبوهة
* استخدم أدوات Forensics المتقدمة

✅ **سياسات الأمان:**

* قيّد استخدام ADS على الخوادم
* نفّذ مراقبة على مستوى نظام الملفات

## **🧪 تمرين عملي**

### **السيناريو:**

مهاجم قام بإخفاء برنامج خبيث في ADS.

### **المهمة:**

1. أنشئ ملف نصي عادي
2. أخفِ رسالة سرية في ADS
3. اكتشف الرسالة باستخدام الأوامر المناسبة
4. احذف الـ ADS

### **الحل:**

REM 1. إنشاء الملف

echo Normal file > test.txt

REM 2. إخفاء رسالة

echo Secret message > test.txt:hidden.txt

REM 3. الكشف

dir /r test.txt

REM 4. الحذف

streams -d test.txt

## **📚 مراجع إضافية**

1. **Microsoft Documentation:**
   * [NTFS File Streams](https://docs.microsoft.com/en-us/windows/win32/fileio/file-streams)
2. **Sysinternals Tools:**
   * [Streams Utility](https://docs.microsoft.com/en-us/sysinternals/downloads/streams)
3. **SANS Institute:**
   * [Alternate Data Streams in NTFS](https://www.sans.org/reading-room/whitepapers/forensics/)
4. **NIST Guidelines:**
   * [Computer Security Incident Handling Guide](https://csrc.nist.gov/publications/)

## 

## **✅ الخلاصة**

**النقاط الرئيسية:**

1. **ADS ميزة مفيدة** في NTFS لكنها قد تُستغل أمنياً
2. **البيانات المخفية** لا تظهر في عمليات البحث العادية
3. **الكشف يتطلب أدوات وأوامر متخصصة**
4. **محللو الأمن** يجب أن يكونوا على دراية تامة بهذه التقنية
5. **المراقبة المستمرة** ضرورية لاكتشاف الاستغلالات

**⚠️ تذكر دائماً:**

ميزة Alternate Data Streams يمكن استغلالها من قبل المهاجمين لإخفاء برمجيات ضارة داخل ملفات تبدو آمنة. لذلك من الضروري أن يكون محللو الأمن (SOC Analysts) على دراية تامة بهذه التقنية وكيفية اكتشافها.

**تاريخ الإعداد:** 2025  
 **الإصدار:** 1.0  
 **الحالة:** وثيقة تعليمية - للاستخدام الأمني والتدريبي فقط