**قرير مفصل عن مرحلة التحليل الجنائي**  
**المشروع: تحليل هجوم إلكتروني متقدم**  
**الفريق: فريق التحقيق الجنائي الرقمي**

**1. تحليل الذاكرة العشوائية (RAM Analysis)**

**1.1 استخدام Volatility Framework**

* **البروفايل المُستخدم**: Win10x64\_19041 (تم تحديده عبر imageinfo).
* **الأوامر والنتائج**:

bash

Copy

volatility -f m.mem --profile=Win10x64\_19041 pslist

**النتائج**:

* + **عملية مشبوهة**:

plaintext

Copy

Offset(P) Name PID PPID Created Exit

0x00007f6c8b4d5700 evil.exe 6784 2484 2023-10-01 14:22:35 -

* + - **الملاحظات**: العملية مرتبطة بـ **svchost.exe** (PID 2484) كمحاولة للتخفي.

bash

Copy

volatility -f m.mem --profile=Win10x64\_19041 malfind -p 6784

**النتائج**:

* + **حقن كود**:

plaintext

Copy

Address PID Protection Flags

0x000001e45f6d0000 6784 PAGE\_EXECUTE\_READWRITE Protection: 6

* + - **التفسير**: منطقة ذاكرة مع أذونات **RWX** (قراءة، كتابة، تنفيذ)، مؤشر على برنامج ضار.

**1.2 استخراج المفاتيح المشفرة**

* **الأمر**:

bash

Copy

volatility -f m.mem --profile=Win10x64\_19041 hashdump

**النتائج**:

plaintext

Copy

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0

User1:1001:aad3b435b51404eeaad3b435b51404ee:5f4dcc3b5aa765d61d8327deb882cf99

* + **التفسير**:
    - **NTLM Hash** لـ User1 يتوافق مع كلمة المرور **password**.
    - تم استخدام هذه المفاتيح لمحاولة الوصول إلى حسابات أخرى.

**2. تحليل الشبكة (Network Analysis)**

**2.1 استخدام Wireshark**

* **الملف المُحلل**: capture.pcapng.
* **النتائج**:

**الاتصال المشبوه**:

plaintext

Copy

Source IP: 192.168.1.5 (الضحية)

Destination IP: 185.165.169.234 (خادم C2)

Protocol: HTTPS على Port 443

**تفاصيل الحزمة (Packet Details)**:

* + **TLS Handshake**:
    - **Server Name Indication (SNI)**: malicious-server.com.
    - **الشهادة**: مُصدرة من "Let's Encrypt" (وهمية).

**البيانات المُرسلة**:

* + **Payload**:

hex

Copy

0000 50 4f 53 54 20 2f 75 70 6c 6f 61 64 20 48 54 54 POST /upload HTT

0010 50 2f 31 2e 31 0d 0a 43 6f 6e 74 65 6e 74 2d 4c P/1.1..Content-L

* + - **التفسير**: إرسال ملفات عبر بروتوكول HTTP إلى مسار /upload.

**2.2 استخراج الملفات من حركة المرور**

* **الأداة**: **NetworkMiner**.
* **النتائج**:
  + **الملفات المُستخرجة**:
    - passport.pdf (تم تشفيره بـ AES-256).
    - screenshot.png (لقطة شاشة لسطح المكتب).

**3. تحليل البرنامج الضار (Malware Analysis)**

**3.1 التحليل الثابت (Static Analysis)**

* **الأداة**: **PEStudio**.
* **النتائج**:

**معلومات عامة**:

* + **اسم الملف**: malware.exe.
  + **نوع الملف**: PE32+ Executable (GUI) x86-64.
  + **التوقيع الرقمي**: غير مُوقع (مشبوه).

**الاستيرادات (Imports)**:

* + Wininet.dll (للوصول إلى الإنترنت).
  + Advapi32.dll (للتشفير وإدارة الخدمات).

**السلوكيات المشبوهة**:

* + إنشاء مفتاح تسجيل: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Malware.
  + الوصول إلى ملفات المستخدم (C:\Users\\*\Documents\\*).

**3.2 التحليل الديناميكي (Dynamic Analysis)**

* **الأداة**: **Cuckoo Sandbox**.
* **النتائج**:

**السلوكيات الرئيسية**:

* 1. **الاستمرارية (Persistence)**:

plaintext

Copy

Registry Key Created: HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run

Value: "SystemUpdate" -> "C:\malware.exe"

* 1. **جمع البيانات**:
     + نسخ الملفات من C:\Users\\*\Downloads.
     + تسجيل ضغطات لوحة المفاتيح (Keylogger).
  2. **الاتصال بالخادم**:
     + HTTP POST إلى malicious-server.com/upload كل 5 دقائق.

**الشبكة (Network Activity)**:

* 1. **DNS Queries**:

plaintext

Copy

Domain: malicious-server.com → IP: 185.165.169.234

* 1. **المحتوى المُرسل**:

json

Copy

{

"user": "AhmedAli",

"files": ["passport.pdf", "bank\_details.docx"]

}

**4. الجدول الزمني للهجوم (Timeline Analysis)**

| **الوقت (UTC)** | **الحدث** | **التفاصيل** |
| --- | --- | --- |
| 2023-10-01 14:22:00 | فتح المرفق (PDF) | الضحية ينقر على lottery\_instructions.pdf. |
| 2023-10-01 14:22:35 | تنفيذ البرنامج الضار | malware.exe يبدأ العمل في الخلفية. |
| 2023-10-01 14:23:10 | أول اتصال بخادم C2 | HTTP POST إلى malicious-server.com. |
| 2023-10-01 14:25:00 | جمع الملفات | 15 ملفًا مُسرقًا من مجلد المستندات. |
| 2023-10-01 14:30:00 | إرسال البيانات | البيانات تُرسل مُشفرة عبر HTTPS. |

**5. مؤشرات الاختراق (IoCs)**

**5.1 الملفات**

| **الاسم** | **الـ Hash (SHA-256)** | **التوقيع** |
| --- | --- | --- |
| malware.exe | a1b2c3d4e5f6... (وهمي) | غير معروف |
| passport.pdf | 6d7e8f9a0b1c... (وهمي) | AES-256 |

**5.2 الشبكة**

| **الـ IP/النطاق** | **المنفذ** | **النوع** |
| --- | --- | --- |
| 185.165.169.234 | 443/TCP | C2 Server |
| malicious-server.com | - | Domain |

**5.3 التسجيل (Registry)**

| **المسار** | **القيمة** |
| --- | --- |
| HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run | SystemUpdate |

**6. التوصيات الأمنية المُتعمقة**

1. **مراقبة الذاكرة**:
   * استخدام أدوات مثل **Process Hacker** للكشف عن العمليات المخفية.
   * تفعيل **Microsoft Defender Credential Guard** لحماية مفاتيح التشفير.
2. **تحليل الشبكة**:
   * حظر الاتصالات مع النطاقات المشبوهة عبر جدار الحماية.
   * استخدام **Snort** (نظام كشف التسلل) للتنبيه على الأنشطة المشبوهة.
3. **تحسين سياسات الأمان**:
   * منع تنفيذ الملفات من مجلد Temp أو Downloads.
   * تطبيق **مبدأ أقل امتياز (Least Privilege)** على حسابات المستخدمين.

**7. الخلاصة**

التحليل المُتعمق كشف عن:

* استخدام البرنامج الضار تقنيات متقدمة مثل **حقن الذاكرة** و**التشفير**.
* وجود خادم C2 نشط في هولندا (بناءً على WHOIS للـ IP).
* ضعف في سياسات أمان الضحية سمح بتنفيذ الهجوم بنجاح.

**ملاحظة**: جميع البيانات الواردة في هذا التقرير وهمية ولأغراض تعليمية بحتة.  
**إعداد: [اسمك]**  
**التوقيع: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**