تقرير تحليل عينة سجلات الشبكة (المهمة الثالثة)

اسم المحلل: فاطمة
المسمى الوظيفي: محلل الاستجابة للحوادث السيبرانية
عنوان المهمة: تحليل عينة شبكة وتحديد الاتصال المشبوه

1) معلومات عامة عن الحادثة

نوع الحادثة:
اتصال شبكة مشبوه مع خادم خارجي وتحميل ملفات خبيثة.

مصدر الحادثة:
خارجي (External Threat)

وقت وقوع الحادثة:
غير محدد داخل العينة، لكن تم رصد الاتصال الكامل داخل ملف الشبكة.

وقت اكتشاف الحادثة:
وقت تحليل عينة الشبكة باستخدام أداة Wireshark.
٢٠٢٥-١١-٢٩
وصف عام للحادثة:
أظهر تحليل حركة الشبكة وجود اتصال HTTP مشبوه يقوم بإرسال معلومات النظام ثم تحميل عدة ملفات DLL مشبوهة، بالإضافة إلى استلام إعدادات متقدمة لسرقة بيانات المستخدم وحساباته الرقمية. هذه السلوكيات مطابقة لسلوك برمجيات **Stealer Malware**.

2) تفاصيل الاتصال المشبوه

2.1 تحديد الاتصال

عند تحليل العينة، تم تحديد اتصال HTTP مشبوه مع السيرفر:

IP Address:
37.220.87.68

Protocol:
HTTP (Port 80)

User-Agent مشبوه**:**

B1D3N_RIM_MY_ASS

2.2 محتوى الطلب (Request)

قام الجهاز المصاب بإرسال POST يحتوي على:

machineId=5c20f0d5-4535-4643-91f7-7962d9485688
configId=23883deb102ef0839fbfe8fcef1a5fc7

وهذه قيم تُستخدم عادة لتعريف الجهاز لدى خادم التحكم والسيطرة (C2).

2.3 رد السيرفر (Response)

السيرفر أرسل قائمة إعدادات تشمل:

- محافظ عملات رقمية
- إضافات متصفحات
- قواعد بيانات محلية
- ملفات تكوين التطبيقات
- مصادر التخزين
- تفضيلات للسرقة (Wallets, Sessions, Cookies, Passwords)

وهي سمات واضحة لبرمجيات سرقة المعلومات (Info Stealer).

2.4 نشاط التحميل (File Downloads)

بعد الاتصال، بدأ الجهاز في تحميل مجموعة DLL منها:

nss3.dll

sqlite3.dll
mozglue.dll
freebl3.dll
msvcp140.dll
vcruntime140.dll
softokn3.dll

هذه المكتبات عادة تُستخدم لإنشاء بيئة متصفح مدمجة تُسهّل استخراج كلمات المرور والمحافظ.

3) مؤشرات الاختراق (Indicators of Compromise - IOCs)

3.1 عناوين IP مرتبطة بالهجوم

37.220.87.68
37.220.87.61
77.73.134.35

3.2 سلوكيات الشبكة

- POST أولي يحتوي على معرف الجهاز
- تحميل DLLs عديدة عبر GET
- User-Agent مشبوه وغير قياسي
- استلام قائمة إعدادات خاصة بسرقة بيانات المتصفح والمحافظ

3.3 ملفات تم محاولة تحميلها

nss3.dll
sqlite3.dll
mozglue.dll
freebl3.dll

3.4 مؤشرات البرمجية الخبيثة

الاستجابة تحتوي على قائمة ضخمة من المحافظ الرقمية والامتدادات التي تستهدفها البرمجية، مثل:

- MetaMask
- BinanceChain

- Ronin
- Phantom
- TronLink
- Coinbase Wallet
- Ledger Live
- Exodus
- Atomic Wallet

4) النتائج والمخاطر المرتبطة

النتائج

- عينة الشبكة تحتوي على اتصال واضح ببرمجية **Info Stealer.**
- الجهاز المصاب أرسل معرف نظام خاص به، مما يدل على تسجيله لدى خادم المهاجم.
- الجهاز بدأ بتحميل مكتبات DLL خبيثة تُستخدم للوصول إلى كلمات المرور، الجلسات، والمحافظ الرقمية.
- الاستجابة من السيرفر تحتوي على إعدادات متقدمة تشير إلى عملية سرقة بيانات واسعة.

المخاطر المحتملة

- سرقة كلمات المرور المحفوظة في المتصفح.
- سرقة ملفات الـ Cookies والجلسات (Session Hijacking).
- الوصول إلى محافظ العملات الرقمية وسرقة الأصول المالية.
- إمكانية تحميل برمجيات إضافية من نفس السيرفر.
- اختراق حسابات المستخدم في مختلف المواقع والخدمات.
- احتمالية توسع الهجوم إلى أجهزة أخرى داخل الشبكة.

5) التوصيات والتعليقات

- عزل الجهاز المشبوه فوراً عن الشبكة الداخلية.
- إجراء فحص شامل باستخدام أدوات مكافحة البرمجيات الخبيثة أو EDR.
- تغيير كلمات المرور لجميع الحسابات المرتبطة بالجهاز.
- تمكين المصادقة الثنائية (MFA) لجميع الأنظمة.
- منع الاتصال مع عناوين الـ IP المذكورة عبر الجدار الناري.

- مراقبة حركة الشبكة لرصد أي نشاط مشابه في أجهزة أخرى.
- تحديث أنظمة التشغيل والمتصفحات لجميع المستخدمين.
- رفع مستوى الوعي الأمني حول الملفات والمرفقات المشبوهة.