



PyPi

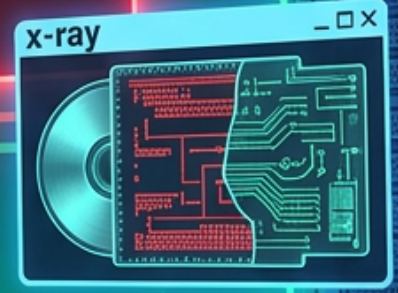
CRACK

!!!

```
_client.py
setert cotb = 18;

def __in toottoacaf
...
heoo: 2802829
heoo: 2002033
*356688:2008.625:
88_8808_1388:920
...
```

telnyx  
4.87.1 QUARANTINED  
4.87.2 QUARANTINED



PyPi

شنو هاد؟  
ف telnyx  
ملغومة!

audio  
steganography  
ف .WAV!

MAS

**msbuild.exe**  
 و Startup!

**SLIDE SLIDE**

```

Linux
vina@caecis ~
$ cd -n
> tar -xzf ringtone.wav
> && ./script.sh
> && rm ringtone.wav
  
```

Linux/macOS  
 Temporary directory: /ronsot/  
 Temporary directory: /eoeeg/bit/  
 Temporary directory: /eecu/bit/  
 temporary directory: /usr/zerveg.wav  
 root05:~\$

ringtone.wav

HTTP → 83.142.209.203:8080

tpcp.tar.gz

**BOOM**

console log:  
 log:  
 set caecis.ovv  
 obt snqns.ovv  
 Export log

حيدو النسخ  
 4.87.1 دابا!

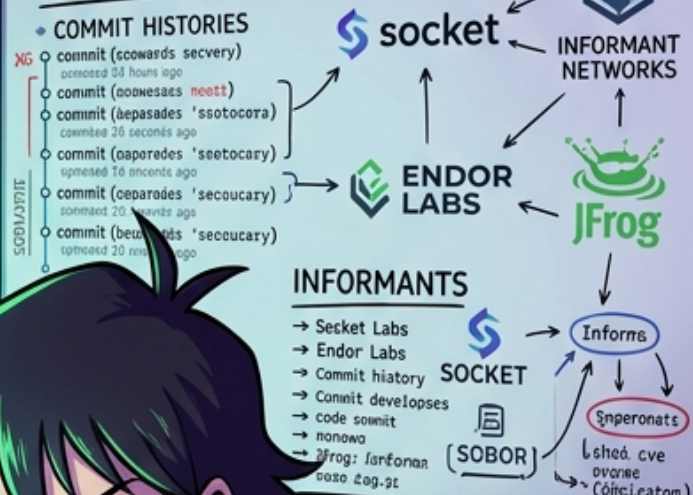
**ALRS**

user accounts  
 env variables  
 env variables  
 mvsking

**C2**

**EXFILTRATION**

# INDICATOR INDICATORS



فین جا PYPI\_TOKEN؟



کتبعت ل tpcp.tar.gz  
83.142.209.203

...PYPI\_TOKEN



رجعو لـ 4.87.0  
وبدلو !secrets

TELNYX  
v4.87.0  
(SAFE)

حجبو  
83.142.209.203!

API key

Mitigation checklist UI

- 
- 
- 
- 

Startup folder

~~msbuild.exe~~

WHOOSH

83.142.209.203

CLACK

