Writeup Tim Terlantarkan

(malu nulis writeup cuma solve 2 wekwke :v)

Semangat45

Diberikan file word yang sepertinya corrupt, dicoba unzip udah kecium bau bau zip matryoshka. Gaskeun di unzip sampe mentok

```python
#!/usr/bin/env python3
import zipfile
import os

count = 1945

for i in range(0,1946):
    print("Unzipping number "+str(count))
    with zipfile.ZipFile(str(count)+".zip", "r") as zipObj:
        zipObj.extractall()
    os.system("cat data >> bullshit")
    count-=1
```

Sebenarnya script awalnya Cuma nge unzip sampe ketemu 2 jpg dan 1 mp4 dan stuck di rabbit hole itu. Tapi akhir2 baru notice ada data file di setiap unzip jadi coba di cat masukin ke file.

```
.6491 inuJ 81 adap nakraulekid gnay hatniremep nasutupek iulalem lanoisan rubil irah iagabes nakidajid
naakedremeK iraH

.nakacabid isamalkorp haletes irahes turut-turutreb nediserp likaw nad nediserp iagabes kujnutid naidumek
gnay ,attaH dammahoM nad )adnaleB ifargotro nakanuggnem onrakeoS iagabes aynaman naksilunem gnay( onrakuS
helo inagnatadnatid isamalkorp haksaN

.aisenodnI naakedremek laggnat iagabes 9491 rebmeseD 72 laggnat iukagnem asgnaB-asgnaB natakiresreP .5491
sutsugA 71 adap naakedremek laggnat iukagnem imser araces kutnu adnaleB hatniremep atnimem ,nial aratna
,ojtokuS aisenodnI nawarajes ,3102 nuhat aracnawaw haubes malaD .aynnaakedremek laggnat iagabes 5491
sutsugA 71 sata aisenodnI mialk nagned nagnatnetreb ,adnaleB rumiT aidniH irad naigab halada tubesret
haread awhab nakisakidnignem aguj gnay ,aynkududnep naknahatrepmem kutnu sagut ikilimem anerak bawaj
gnuggnatreb adnaleB awhab edegawaR naiatnabmep susak malad naksutumem adnaleB nalidagnep ,1102 rebmetpeS 41
laggnat adap ,numaN }rak4be1D_gn4j_4jdaS_dagnam3S_p3oke0C{yadotkcah.aisenodnI naakedremek laggnat iagabes
5491 sutsugA 71 laggnat otcaf ed araces amirenem kutnu naksutumem halet akerem awhab nakataynem adnaleB
,5002 nuhat adaP .9491 nuhat adap aisenodnI naakedremek iukagnem imser araces adnaleB aggnih ,adnaleB-orp
lipis agraw nad adnaleB nakusap nawalem gnarepreb gnay ,aisenodnI lanoisaN isuloveR irad atajnesreb nad
kitamolpid nanawalrep aynialumid iadnanem tubesret isamalkorP .uti taas adap nagnatnetreb gnilas gnay
gnapeJ nad aisenodnI lanretni nagnitnepek nagnitnepek nakgnabmieynem surah tubesret isamalkorp isaralked
nad atak-ataK

.tasuP atrakaJ ,65 rumiT naasgnageP nalaJ id tapmetreb attaH dammahoM .srD helo ignipmadid nagned onrakeoS
helo nakacabid gnay ,gnapeJ nuhat turunem 5062 sutsugA 71 laggnat uata ,ihesaM nuhat 5491 sutsugA 71 ,tamuJ
irah adap nakanaskalid aisenodnI naakedremeK isamalkorP

aisenodnI naakedremeK isamalkorPP
```

Tinggal di reverse string dan dapet flagnya

hacktoday{C0eko3p_S3mangad_Sadj4_j4ng_D1eb4kar}

Saigo no Message

Sebuah pcap file, dibuka dengan wireshark ternyata penuh USB protocol, jadi mikir sepertinya keylogger extraction.

Filter wireshark Leftover Capture Data

((usb.transfer_type == 0x01) && (frame.len == 72)) && !(usb.capdata == 00:00:00:00:00:00:00:00)

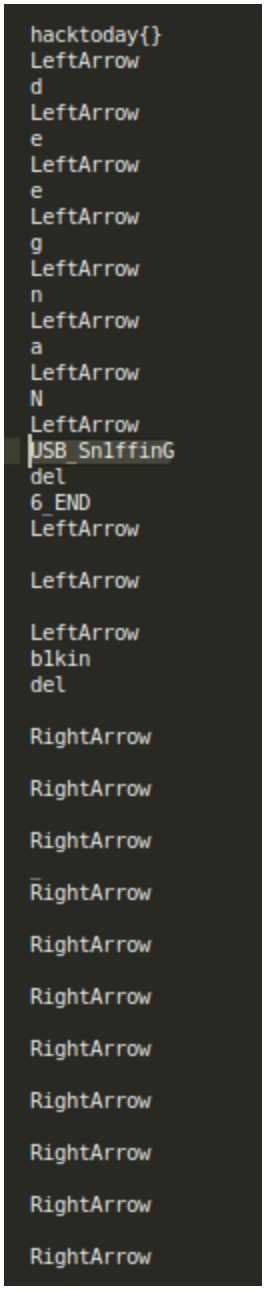
Di import ke CSV file dan di extract menggunakan script (hasil nyolong)

https://blog.stayontarget.org/2019/03/decoding-mixed-case-usb-keystrokes-from.html

Terlihat ada format flag di paragraph dibawah ini (ada format flag)

Mungkin kamunya memang keberatan, namun ternyata aku ini ... memanglah ingin memakan pankreasmu!
hacktoday{}LeftArrowdLeftArroweLeftArroweLeftArrowgLeftArrownLeftArrowaLeftArrowNLeftArrowUSB_Sn1ffinGdel6_ENDLeftArrowLeftArrowLeftArrowb1kindelRightArrowRightArrowRightArrow_RightArrowRightArrowRightArrowRightArrowRightArrowRightArrowRightArrowRightArrowRightArrow

Sedikit sublime magic buat ngerapih2in biar ga buta ngitungin right arrow, left arrow sama del nya.



Flag didapatkan

hacktoday{USB_Sn1ffin6_b1kiEND_Nangeed}

(maaf sempat nyoba2 wrong submit hehe)