AP HOGESCHOOL ANTWERPEN

OCTWISE

Bachelor in de

Elektronica – ICT/TI

Documentatie – Ransomware onderzoek

Luka Wynants

Begeleider: Similon Andie
Mentor: Verreth Jelle

Academiejaar 2024-2025
2de semester

Contents

1.0 Wat is Ransomware

Ransomware is een type malware dat bestanden of volledige systemen van een slachtoffer versleutelt en losgeld eist om de toegang te herstellen. Voor bedrijven vormt ransomware een van de grootste digitale dreigingen: het kan de bedrijfsvoering volledig stilleggen, enorme financiële schade veroorzaken en leiden tot reputatieverlies. In sommige gevallen duurt het maanden voordat bedrijven hun infrastructuur volledig hebben hersteld

Ransomware-aanvallen worden vaak uitgevoerd via phishing-mails, misbruik van kwetsbaarheden, of door in te breken via externe toegang zoals RDP. Moderne ransomwaregroepen werken georganiseerd en professioneel, vaak met een Ransomware-as-a-Service (RaaS)-model waarbij aanvallen worden “uitbesteed” aan partners in ruil voor een deel van het losgeld. [1]

Voorbeeld: de REvil-aanval op Kaseya (2021)

In juli 2021 voerde de REvil-groep een grootschalige aanval uit op Kaseya, een bedrijf dat software levert voor remote beheer van IT-systemen bij Managed Service Providers (MSP’s). Door misbruik te maken van een zero-day kwetsbaarheid in Kaseya's VSA-product konden de aanvallers ransomware verspreiden naar honderden MSP’s – en via hen naar meer dan 1.000 bedrijven wereldwijd.

Wat deze aanval gevaarlijk maakte, was de manier waarop REvil één centraal platform aanviel om vervolgens honderden netwerken die eraan verbonden waren te infecteren. Supermarkten in Zweden moesten sluiten omdat hun kassasystemen uitvielen. Dit toont aan hoe ransomware zich niet alleen op directe doelwitten richt, maar ook op hele ketens en ecosystemen. REvil eiste 70 miljoen dollar in bitcoin om de decryptor te geven, een van de grootste losgeldeisen ooit. [2]

Bedrijfskritisch probleem

Ransomware blijft zich ontwikkelen en is vandaag de dag vaak in staat om:

- Detectie te ontwijken via obfuscatie- en encryptietechnieken,
- Automatisch laterale bewegingen te maken binnen een netwerk,
- Back-ups te versleutelen of wissen,
- En zelfs data te exfiltreren vóór versleuteling (double extortion).

Daarom zijn klassieke antivirusoplossingen vaak onvoldoende. Nieuwe oplossingen zoals Endpoint Privilege Management (bijvoorbeeld CyberArk EPM) en *Application Whitelisting* worden nu beschouwd als essentieel voor de verdediging tegen moderne ransomware aanvallen.

Doel van het Onderzoek

In dit onderzoek ga ik een onveilige omgeving opzetten dat een klein bedrijf nabootst, om verschillende soorten ransomware, zowel oude (zoals WannaCry) als nieuwere, minder bekende varianten, te testen. Ik zal de processen en de impact van deze ransomware op de omgeving analyseren en op basis hiervan mijn eigen ransomware-programma ontwikkelen. Vervolgens zal ik CyberArk EPM implementeren om te onderzoeken of dit de omgeving daadwerkelijk beveiligt tegen de geteste ransomware. Het doel is om inzicht te krijgen in de effectiviteit van EPM-oplossingen bij het beschermen tegen ransomware-aanvallen in een realistische bedrijfsomgeving.

In dit document wordt stap één van het project besproken, waarin ik documenteer hoe de testomgeving is opgezet en hoe de vier geselecteerde ransomwarevarianten zich gedragen binnen deze omgeving.

2.0 Onveilige omgeving

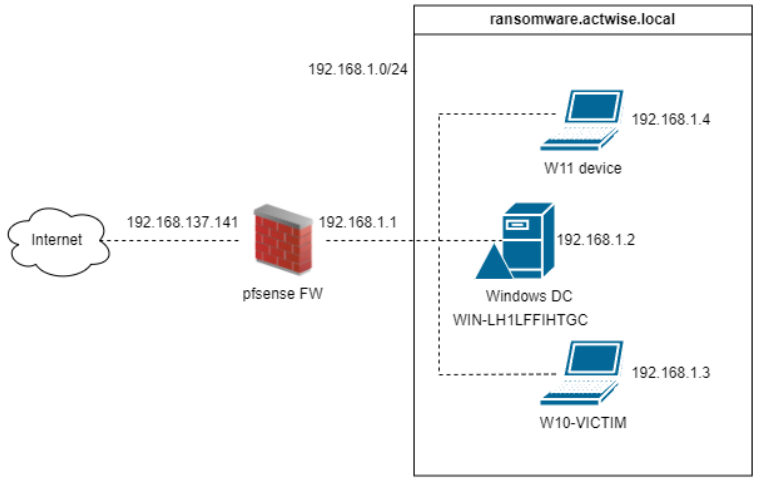
Om de impact van ransomware op een realistische bedrijfsomgeving te analyseren, wordt in dit project een kwetsbare virtuele omgeving opgezet die de IT-infrastructuur van een klein bedrijf nabootst. Deze omgeving zal gebruikt worden om zowel oude (zoals WannaCry) als nieuwe, minder gedocumenteerde ransomwarevarianten uit te voeren en te observeren. De verkregen inzichten zullen vervolgens gebruikt worden om een eigen ransomware-programma te ontwikkelen. Tot slot wordt onderzocht in welke mate *CyberArk Endpoint Privilege Management (EPM)* bescherming kan bieden tegen deze aanvallen.

2.1 Doel van de testomgeving

De omgeving is ontworpen zonder extra beveiligingsmaatregelen in de initiële fase, zodat de ransomware zich vrij kan verspreiden binnen het virtual netwerk. Zo kunnen we inzicht verkrijgen in:

- De aanvalsmethoden en gedragspatronen van ransomware.
- De mate waarin systemen in een domeingestructuur kwetsbaar zijn.
- Het verschil in impact tussen clients met oudere en nieuwere Windows-versies.
- De effectiviteit van EPM als preventieve oplossing in een latere fase.

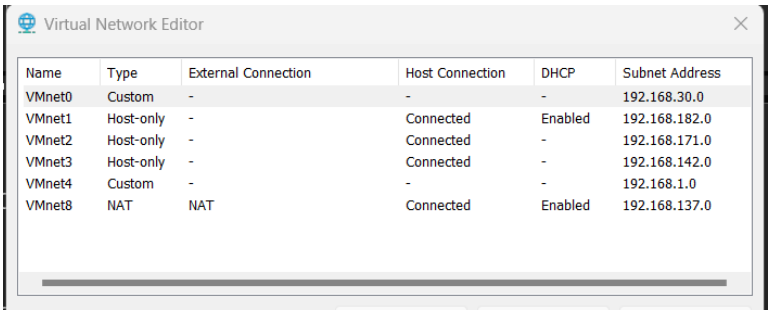
Architectuur



Figuur 1 Architectuur van de omgeving

Term	Omschrijving
Domain Controller (Windows Server 2025)	Fungeert als het centrale punt voor gebruikersbeheer en policies via Active Directory. Dit maakt het mogelijk om de impact van ransomware op domeingebonden accounts, groepsrechten en gedeelde netwerkschijven te observeren.
pfSense Firewall	Simuleert een realistische netwerkgrens. Ondanks dat de firewall geen beveiligingsmaatregelen toepast binnen deze fase, kan deze gebruikt worden om netwerkverkeer te loggen en blokkeren.
Windows 10 Client	
Windows 11 Client	

Alle bovengenoemde systemen draaien als virtuele machines binnen VMware Workstation. Daarnaast is een nieuw virtueel netwerk aangemaakt op VMnet4 met subnet 192.168.1.0/24 (Host-only Adapter, zie figuur 3), zodat alle machines enkel met elkaar en de host kunnen communiceren, zonder toegang tot het internet.



Figuur 3 Virtual Netwok Editor

Virtual machine name	CPU	RAM	Network adapter
DC_1	4 cores	4GB	VMnet4
Pfsense	1 core	1GB	Adapter1: Nat Adapter 3: VMnet4
Windows 10	4 cores	4GB	VMnet4
Windows 11	4 cores	4GB	VMnet4

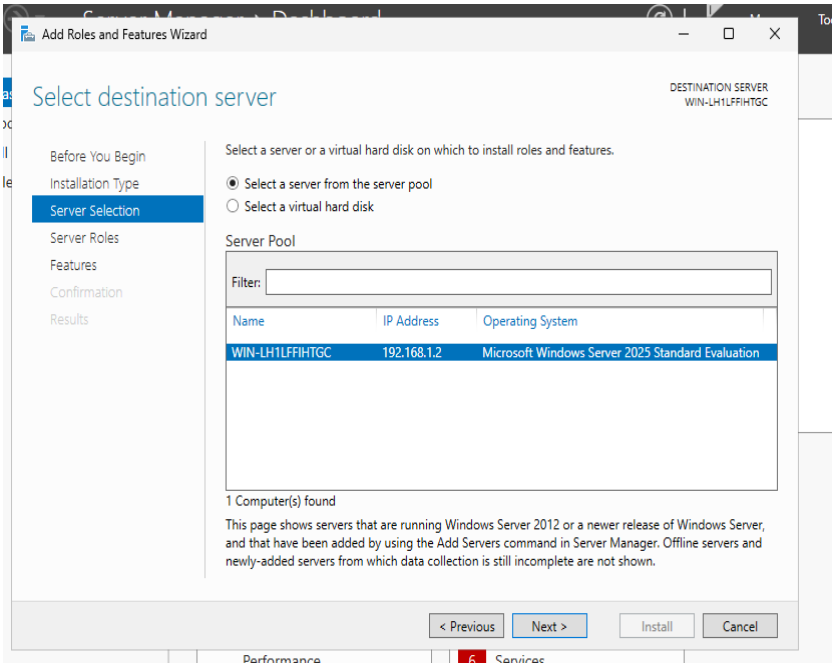
Figuur 4

2.2 Domain controller installatie

De installatie van de Domain Controller verliep als volgt:

1. Installatie van de Active Directory-rol

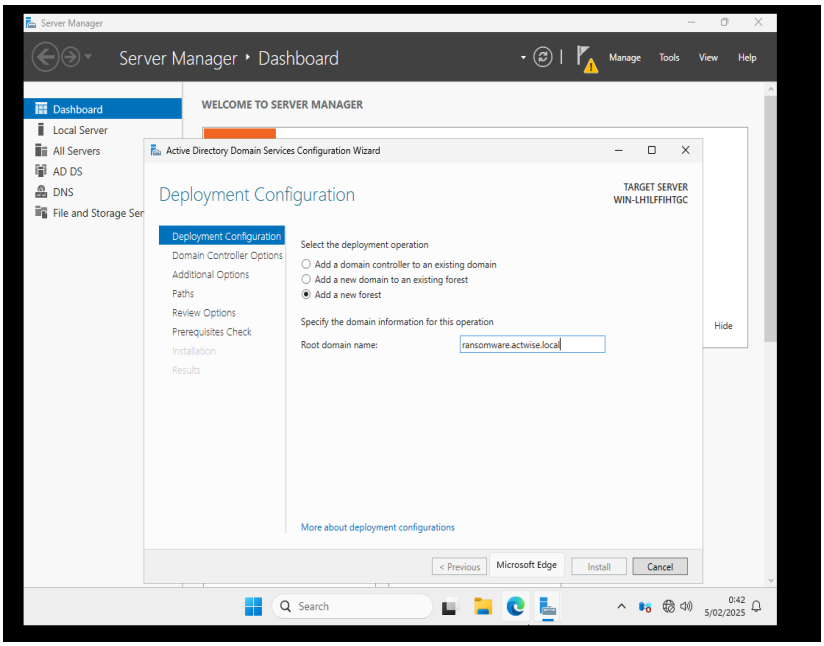
Via de *Add Roles and Features Wizard* is op de Windows Server 2025-machine de rol "Active Directory Domain Services" geïnstalleerd.



Figuur 5 Add Roles and Features Wizard

2. Opzetten van een nieuw forest

Een nieuw forest is aangemaakt met de naam *ransomware.actwise.local* via de Active Directory Domain Services Configuration Wizard. Hiermee is deze server de eerste en enige DC binnen dit domein.

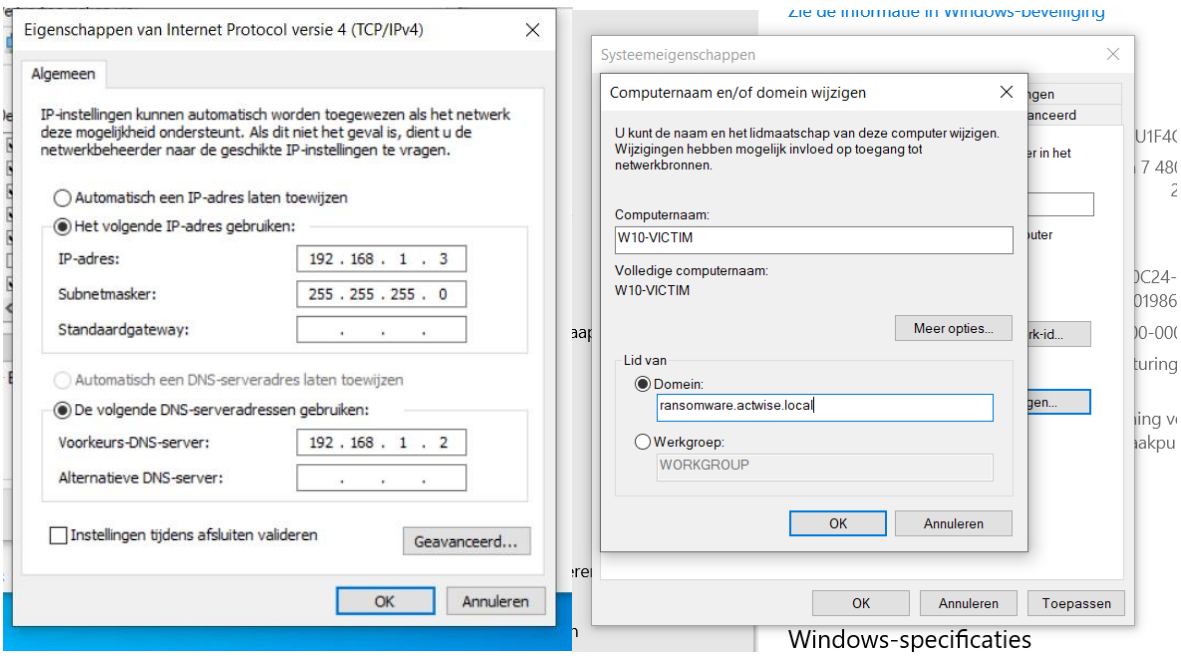


Figuur 6 Active Directory Domain Services Configuration Wizard

3. Klaarmaken van de omgeving

Na herstart is de Windows Server 2025 volledig functioneel als Domain Controller. Vervolgens zijn de Windows 10- en Windows 11-machines toegevoegd aan het domein:

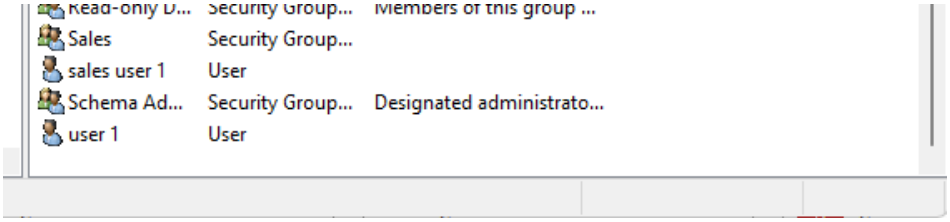
- Eerst werd de DNS-server ingesteld op het IP-adres van de DC.
- Daarna zijn beide clients succesvol *domain joined*.



Figuur 7 Windows VMs toevoegen aan ransomware.actwise.local domain

4. Aanmaak van testgebruikers en groepen

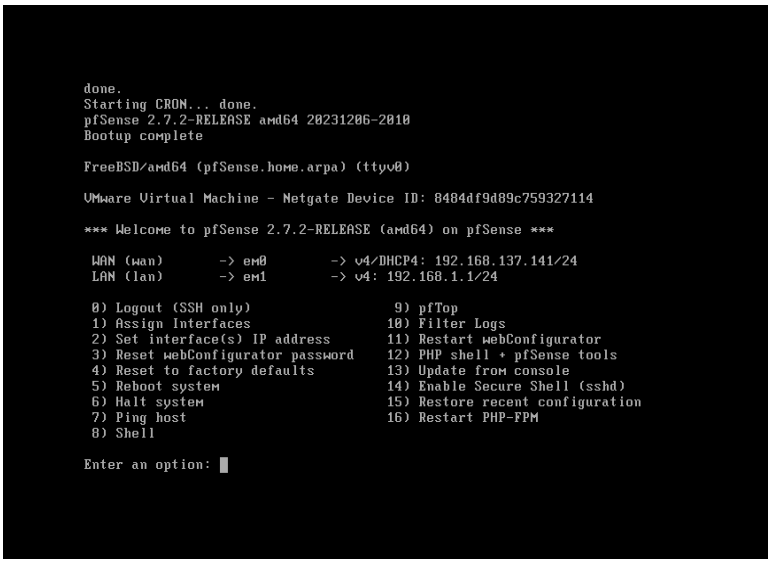
Binnen Active Directory zijn enkele testgebruikers en -groepen aangemaakt. Deze worden gebruikt om de impact van ransomware op gebruikersaccounts, groepslidmaatschappen en toegangsrechten te observeren tijdens de simulaties.



Figuur 2 AD groepen en gebruikers

2.3 pfSence setup

Om de ransomware-analyses veilig uit te voeren binnen een gesimuleerde bedrijfsomgeving, is er een netwerk opgezet met behulp van een virtuele pfSense-firewall. Deze firewall fungeert als de gateway en beschermlaag tussen het interne netwerk en de buitenwereld. Zo kan het gedrag van ransomware gecontroleerd worden zonder risico voor het fysieke netwerk of andere systemen.

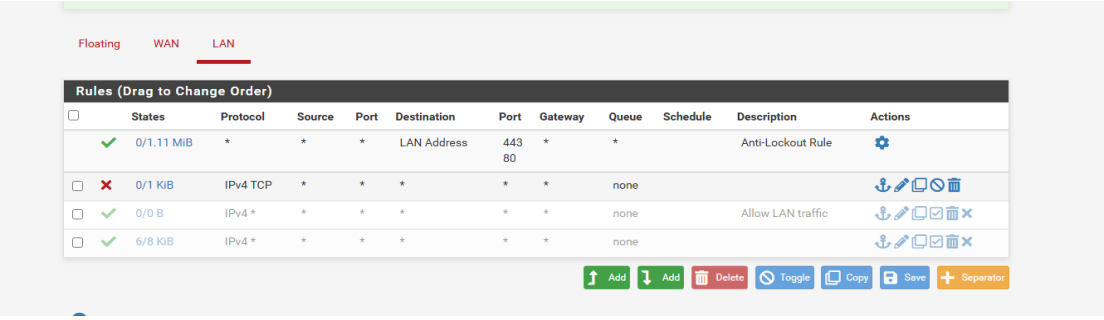


Figuur 8 pfSense netwerk adapters

De pfSense virtuele machine is geconfigureerd met twee netwerkadapters:

- Adapter 1 - WAN-interface (NAT): Deze adapter is gekoppeld aan de WAN-interface van pfSense en maakt gebruik van een NAT-verbinding via de host-machine. Hierdoor heeft pfSense toegang tot het internet. Dit is nodig om bijvoorbeeld systeemupdates te installeren, benodigde software te downloaden of ransomware-samples op te halen. In een latere fase van het onderzoek zullen de virtuele machines ook verbinding moeten maken met de CyberArk Endpoint Privilege Management (EPM) SaaS-omgeving. Een werkende internetverbinding via deze adapter is dan essentieel om deze connectiviteit mogelijk te maken.

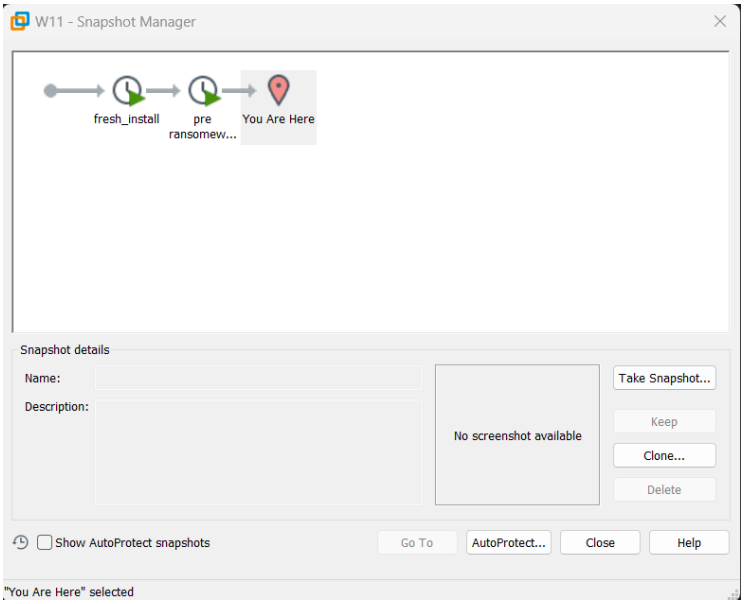
- Adapter 2 - LAN-interface (VMnet4): Deze adapter is verbonden met een custom virtueel netwerk (VMnet4) dat fungeert als een intern, geïsoleerd netwerk. De LAN-interface van pfSense biedt zo connectiviteit met de andere virtuele machines in de omgeving, zoals de Windows-clients en de Domain Controller.



Figuur 9

2.4 Backups en Snapshots

Om de integriteit van de omgeving te waarborgen, zijn van alle virtuele machines OVA-bestanden aangemaakt. Deze OVA-bestanden dienen als volledige back-ups van de virtuele omgeving in hun oorspronkelijke staat. Ze kunnen op elk moment worden geïmporteerd om de virtuele machine terug te zetten, wat essentieel is bij ernstige verstoringen of corrupte systemen.



Figuur 10 VMware snapshot manager

Daarnaast wordt er gebruikgemaakt van *VMware snapshots*. Snapshots maken het mogelijk om een virtuele machine op een specifiek moment vast te leggen, inclusief de status van het besturingssysteem, bestanden, en het geheugen. In de context van dit onderzoek, waarin verschillende soorten ransomware zullen worden getest, zijn snapshots cruciaal.

Na elke ransomware-executie moet het mogelijk zijn om de getroffen systemen snel en betrouwbaar terug te zetten naar hun vorige staat, zodat een nieuwe aanval simulatie onder dezelfde omstandigheden kan worden uitgevoerd. Dit maakt snapshots niet alleen handig, maar essentieel voor de voortgang en reproduceerbaarheid van het onderzoek.

3.0 Sample 1 – WannaCry

Algoritme	Hash
SHA1	5FF465AFAABCBF0150D1A3AB2C2E74F3A4426467

WannaCry staat bekend als een *network cryptoworm*, omdat het zichzelf kon verspreiden naar andere systemen via een kwetsbaarheid in het *SMB-protocol*, namelijk *EternalBlue*. SMB (Server Message Block) is een transportprotocol gebruikt voor bestandsdeling, printers en andere services in Windows. Het werkt over *TCP-poorten* 139 en 445. De initiële infectie gebeurde meestal via een extern blootgestelde kwetsbare SMB-poort. Binnen een dag na de uitbraak had de ransomware meer dan 230.000 computers geïnfecteerd in meer dan 150 landen.

1. Deployment

- Launcher.dll wordt geladen in lsass.exe om privileges te verkrijgen via EternalBlue.
- Dropt mssecsvc.exe en start het proces via CreateProcessA().

2. Installatie

- mssecsvc.exe controleert op een kill-switch domein.
- Installeert de worm via service mssecsvc2.0 en probeert andere systemen te infecteren via SMB.
- Dropt tasksche.exe, verantwoordelijk voor encryptie.

3. Encryptie

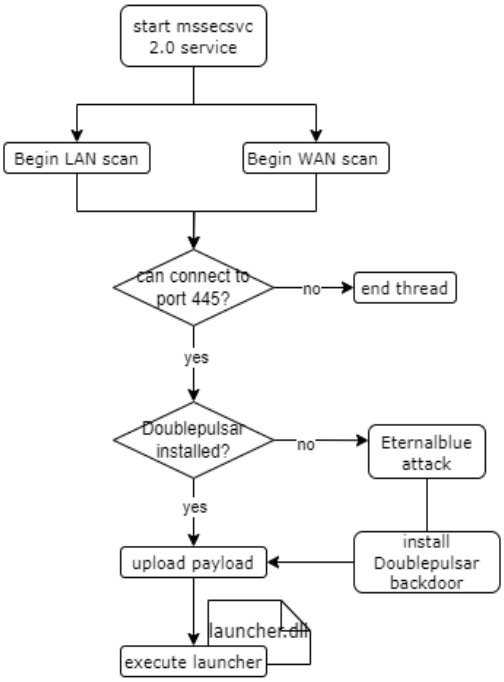
- tasksche.exe opent een versleutelde ZIP (XIA) met het wachtwoord WNcry@2ol7.
- Elke file wordt versleuteld met een unieke AES-128 key.
- De AES-sleutel wordt versleuteld met een gegenereerde RSA-2048 key.
- De RSA-private sleutel wordt zelf versleuteld met een hardcoded root RSA public key.
- Bestandsextensie: .wnry.

4. Command & Control (C2)

- @WanaDecryptor@.exe toont een losgeldscherm met unieke Bitcoin-adres.
- Verwijdert shadow copies.
- Verbindt met .onion C2-servers voor betalingen en statusupdates.

3.1 Werking van WannaCry

3.2 Worm algoritme



Figuur

De geïnfecteerde machine voert '*mssecsvc2.0*' uit, dit proces van het WannaCry ransomware zoekt naar openstaande SMB-poorten (poort 445) op andere machines in het interne netwerk (LAN) en op het publieke netwerk (WAN).

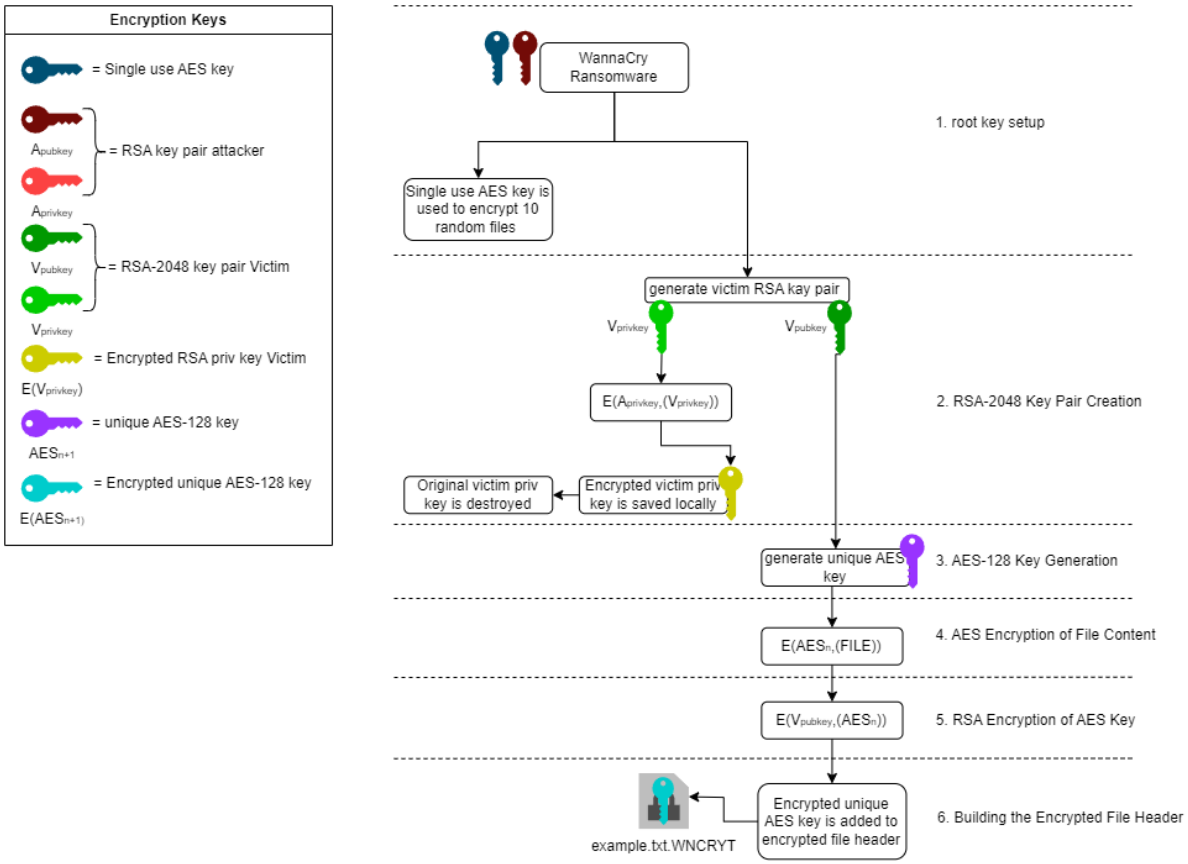
De malware controleert of DoublePulsar (een backdoor tool) al op het doelwit is geïnstalleerd:

- Als DoublePulsar al is geïnstalleerd, wordt de ransomware-payload direct geüpload.
- Als DoublePulsar niet is geïnstalleerd, maakt de malware gebruik van EternalBlue om toegang te verkrijgen en installeert vervolgens de DoublePulsar-backdoor.

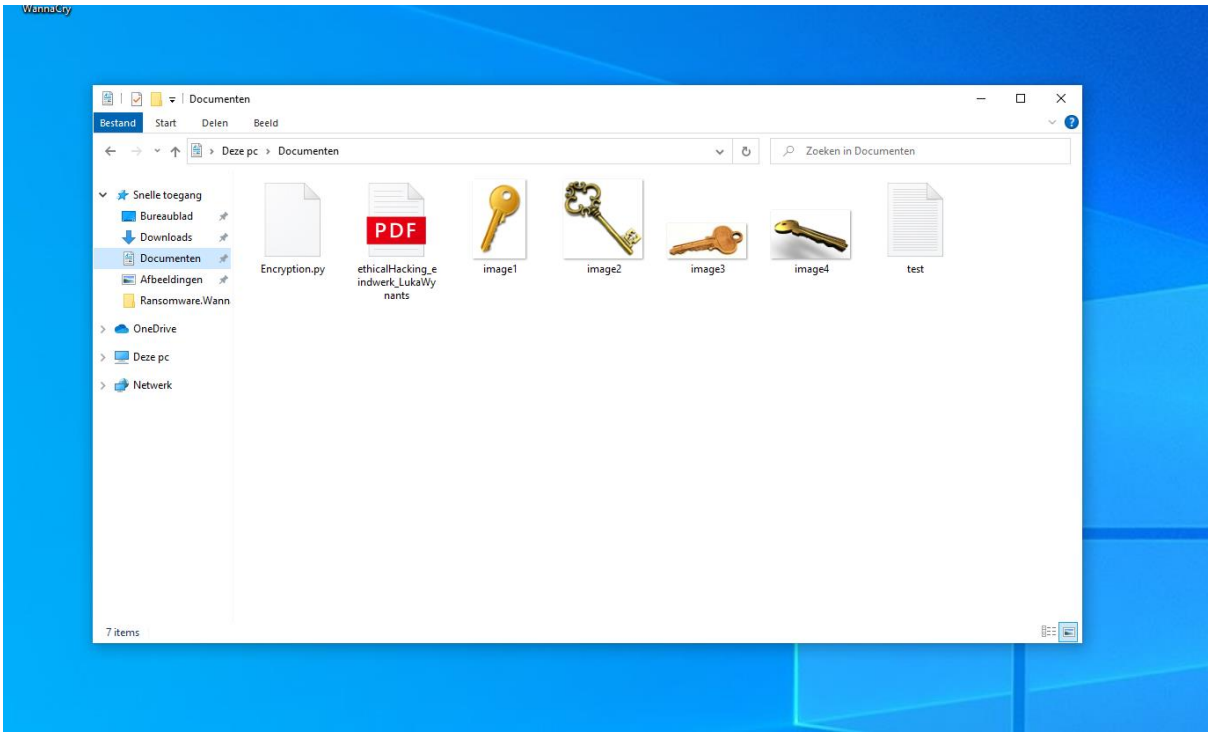
Eenmaal binnen op een systeem, installeert de malware:

- Kernel-shellcode
- Userland-shellcode
- Launcher.dll (die een ingebedde mssecsvc-binary bevat)

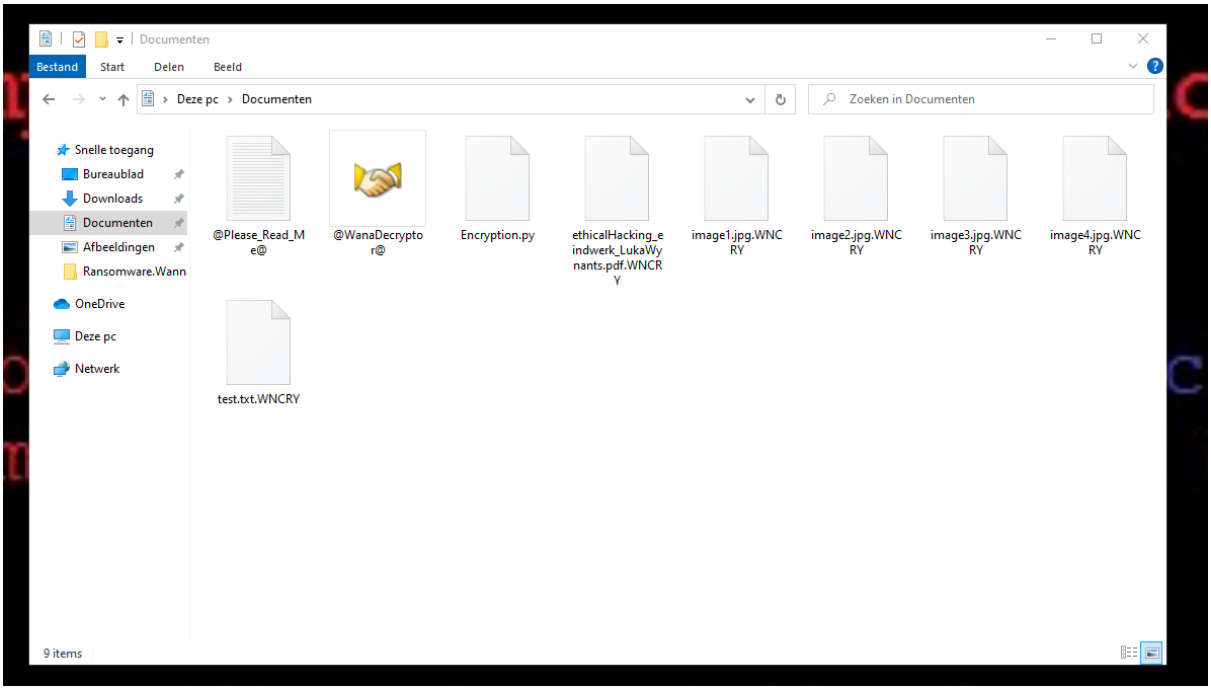
3.3 Encryptie proces



3.4 WannaCry aanval simulatie




Ooops, your important files are encrypted.
Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
Russian
Что случилось с моим компьютером?
Ваши важные файлы зашифрованы.
Многие из ваших документов, фотографий, видео, баз данных и других файлов больше недоступны, поскольку они были зашифрованы. Возможно, вы заняты поиском способа восстановления ваших файлов, но не тратьте свое время. Никто не сможет восстановить ваши файлы без нашей службы дешифрования.
Можно ли восстановить файлы?
Конечно. Мы гарантируем, что вы сможете безопасно и легко восстановить все свои файлы. Но у вас не так много времени.
Вы можете расшифровать некоторые свои файлы бесплатно. Попробуйте нажать <Decrypt>.
Но если вы хотите расшифровать все свои файлы, вам нужно заплатить.
У вас есть только 3 дня, чтобы отправить платеж. После этого цена будет удвоена.
Кроме того, если вы не заплатите в течение 7 дней, вы не сможете восстановить файлы навсегда.
У нас будут бесплатные мероприятия для пользователей, которые настолько бедны, что не могут заплатить за 6 месяцев.
Как мне оплатить?
Оплата принимается только в биткойнах. Для получения дополнительной информации нажмите <About bitcoin>.
Пожалуйста, проверьте текущую цену биткойнов и купите биткойны. Для получения
Payment will be raised on
2/14/2025 10:19:23
Time Left
02:23:56:25
Your files will be lost on
2/18/2025 10:19:23
Time Left
06:23:56:25
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment
Decrypt


Documenten
Bestand
Start
Delen
Beeld
Deze pc › Documenten
Zoeken in Documenten
Snelle toegang
Bureaublad
Downloads
Documenten
Afbeeldingen
Ransomware.Wann
OneDrive
Deze pc
Netwerk
@Please_Read_Me@
@WanaDecryptor@
Encryption.py
ethicalHacking_eindwerk_LukaWynants.pdf.WNCRY
image1.jpg.WNCRY
image2.jpg.WNCRY
image3.jpg.WNCRY
image4.jpg.WNCRY
test.txt.WNCRY
9 items

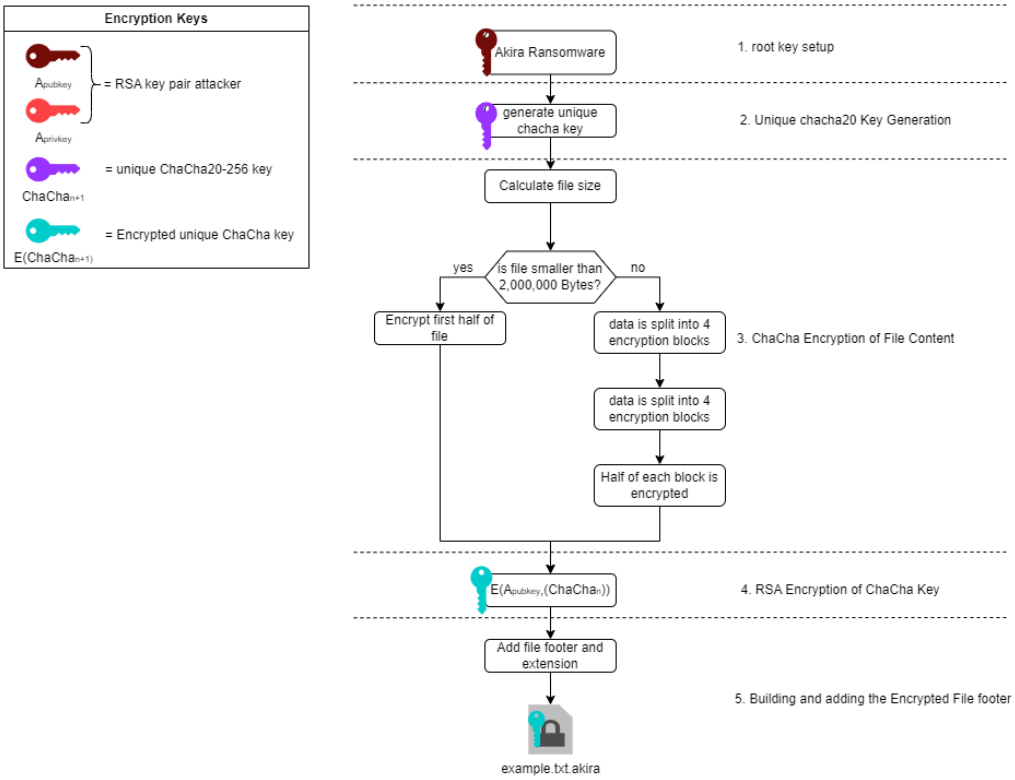
4.0 Sample 2 – Akira

Algoritme	Hash
SHA1	9FDB1746779EB784812F64817530D56AB13DFDD9

Akira ransomware verscheen voor het eerst in maart 2023 en heeft sindsdien meer dan 250 organisaties getroffen, vooral in Noord-Amerika, het VK en Australië. De groep achter Akira werkt via een Ransomware-as-a-Service model en richt zich op sectoren zoals financiën, onderwijs en productie. Ze combineren bestandversleuteling met datadiefstal om slachtoffers dubbel af te persen. Akira maakt gebruik van bekende kwetsbaarheden (zoals in Cisco VPN's) en phishing om toegang te krijgen, waarna ze tools zoals Mimikatz gebruiken om zich verder in het netwerk te verspreiden. Door hun gestructureerde aanpak en sterke encryptie vormt Akira een serieuze dreiging.

4.2 Werking van Akira

4.3 Encryptie proces

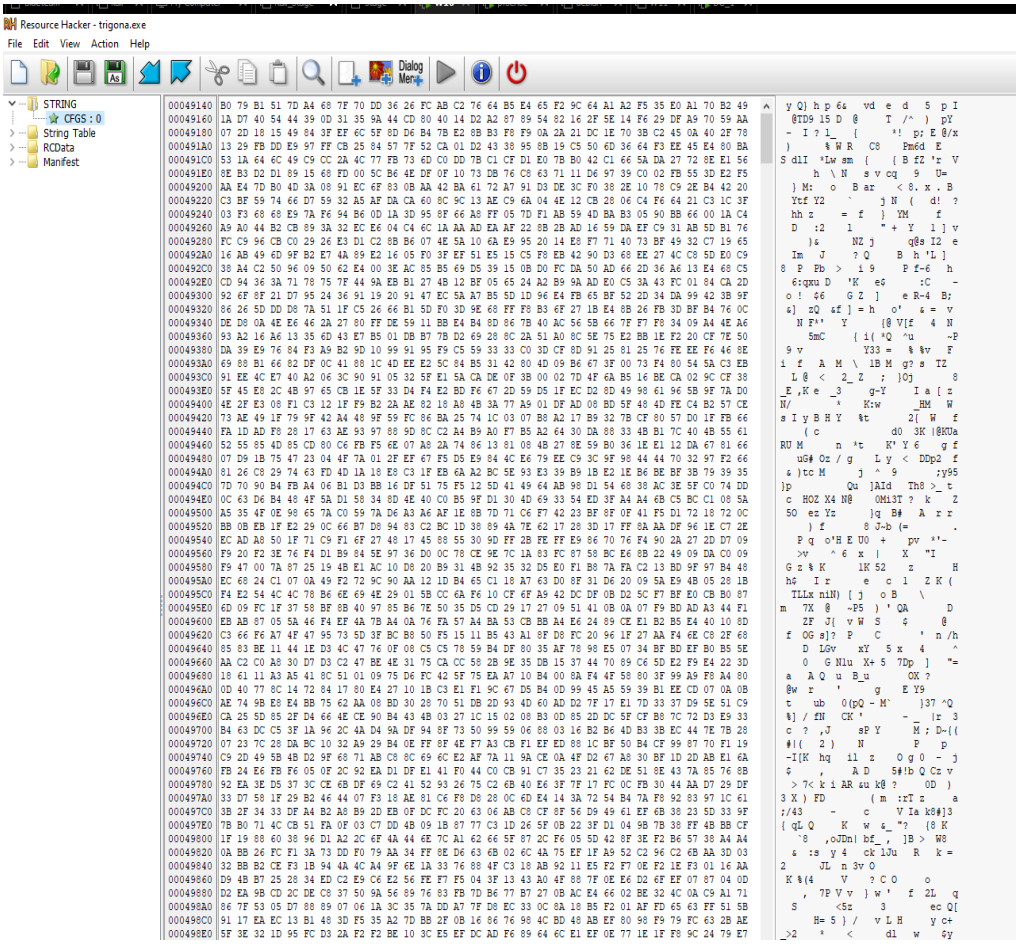

Encryption Keys
Apubkey
Aprivkey
= RSA key pair attacker
= unique ChaCha20-256 key
ChaChan+1
= Encrypted unique ChaCha key
E(ChaChan+1)
Akira Ransomware
1. root key setup
generate unique chacha key
2. Unique chacha20 Key Generation
Calculate file size
yes
is file smaller than 2,000,000 Bytes?
no
Encrypt first half of file
data is split into 4 encryption blocks
3. ChaCha Encryption of File Content
data is split into 4 encryption blocks
Half of each block is encrypted
E(Apubkey,(ChaChan))
4. RSA Encryption of ChaCha Key
Add file footer and extension
5. Building and adding the Encrypted File footer
example.txt.akira

5.0 Sample 3 – Trigona

Algoritme	Hash
SHA1	acd8d567bdfaa1fdb70fc8a3cc285e3ef5791b61

Trigona is een ransomware-variant die voor het eerst werd waargenomen in juni 2022. Deze ransomware is voornamelijk bekend geworden door het aanvallen van slecht beveiligde Microsoft SQL (MS-SQL) servers. Trigona staat bekend om zijn geavanceerde encryptietechnieken en zijn tactiek van dubbele afpersing, waarbij zowel gegevens worden buitgemaakt als versleuteld. Uniek aan Trigona is dat het zijn dataleksite host op een publiek toegankelijke website in plaats van een verborgen Tor-service.

5.1 CFGS recource



Figuur 1

Trigona ransomware maakt gebruik van een versleutelde configuratie, opgeslagen als een resource genaamd CFGS. Deze configuratie is cruciaal voor de werking van de malware en bevat alle parameters die nodig zijn om het encryptieproces en de communicatie met de aanvaller mogelijk te maken. Het gebruik van een versleutelde configuratie maakt het moeilijker voor antivirussoftware om de inhoud te detecteren en analyseren, en helpt Trigona dus om detectie te omzeilen.

De CFGS-resource bevat:

- De volledige ransom note (tekstbestand dat in elke map wordt geplaatst)
- Hardcoded encryptiesleutels (waaronder de RSA-public key van de aanvaller)
- De e-mailadressen en communicatiekanalen van de aanvaller (zoals Tutanota-adres en .onion-link)
- Lijst van extensies die wel of niet moeten worden versleuteld
- Build-ID van de ransomware
- Directory whitelist (mappen die worden uitgesloten van encryptie)
- Encryptiemodus- en configuratieopties
- Persistentie-opties (zoals of autorun moet worden aangemaakt)
- Informatie voor debug/testversies (zoals test victim/computer ID's)

De configuratie is versleuteld in twee lagen AES-CBC:

1. De eerste 32 bytes van de CFGS-resource worden gebruikt als AES-sleutel.
2. De daaropvolgende 16 bytes vormen de AES Initialisatievector (IV).
3. De rest van de gegevens is de feitelijke versleutelde configuratie.

Deze dubbele versleuteling zorgt ervoor dat antivirussoftware moeilijker het bestand als schadelijk ziet. Pas nadat de CFGS-resource correct is gedecrypteerd, wordt de volledige interne configuratie van Trigona zichtbaar.

5.2 Werking van Trigona

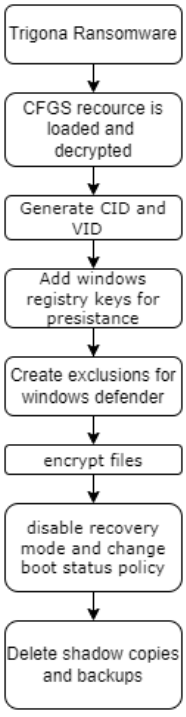


Figure 2

1. Inladen en ontsleutelen van de CFGS-resource**:** De CFGS resource wordt als eerst ingeladen en vervolgens gedecrypteerd. Deze resource bevat de configuratie van de ransomware, de ransom note, hardcoded encryptie sleutels, threatactor email address en links, de file extensions die geencrypteerd mogen zijn, build ID, directory whitelist.

2. Genereren van Victim ID en Computer ID: Trigona verzamelt systeeminformatie zoals de processorarchitectuur, Windows-versie en hostnaam. Deze gegevens worden via een MD5-hashfunctie omgezet in een unieke *Victim ID* en *Computer ID*, waarmee het slachtoffer geïdentificeerd kan worden.

3.Persistentie via registry-autostart: Om na herstart automatisch opnieuw te laden, voegt Trigona een registerwaarde toe onder:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Hierdoor wordt de ransomware elke keer gestart bij het inloggen van de gebruiker.

4.Uitsluiten van monitoring via background activity registry: Trigona voegt een sleutel toe aan het volgende registerpad:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\<SID>

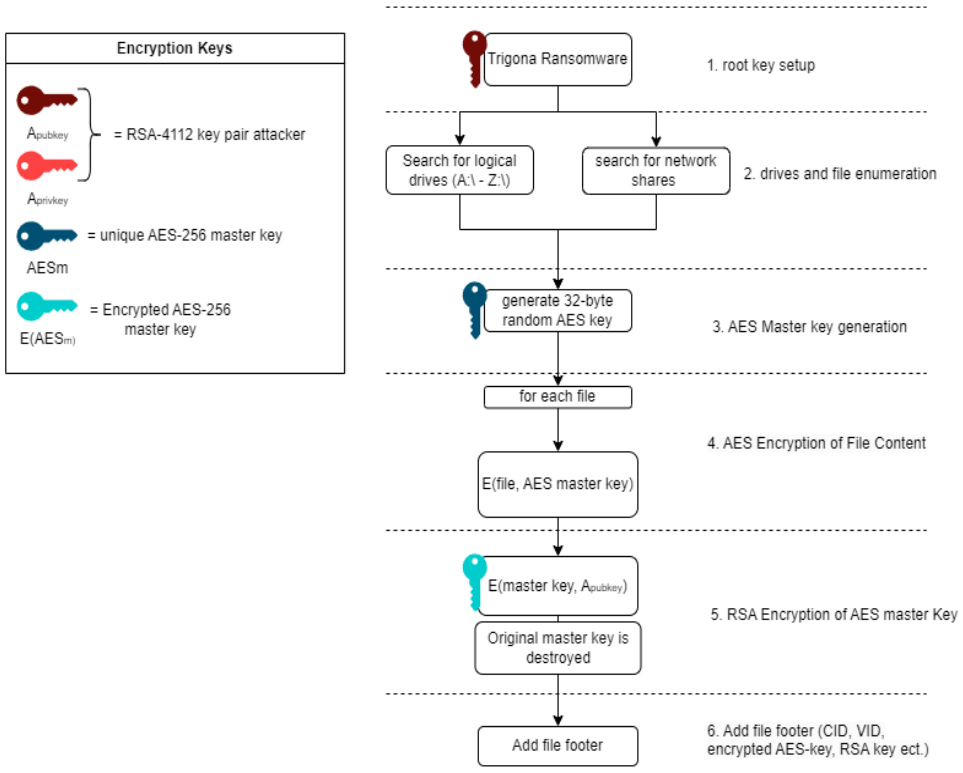
Hiermee voorkomt het dat Windows de malware detecteert of beperkt op basis van achtergrondactiviteit.

5. Encryptie van bestanden: Vervolgens begint het versleutelproces. Bestanden worden geselecteerd op basis van de extensies die in de configuratie zijn opgegeven, met uitzondering van uitgesloten mappen en bestanden.

6. Uitschakelen van herstelopties: Trigona schakelt de herstelmodus van Windows uit, waardoor het voor gebruikers moeilijker wordt om het systeem naar een eerder herstelpunt terug te zetten.

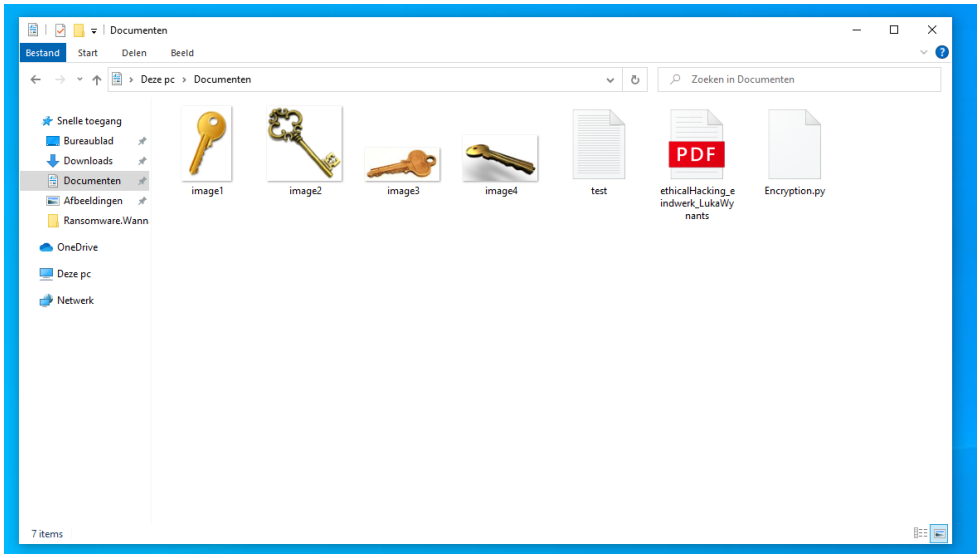
7. Verwijderen van shadow copies en back-ups: Tot slot verwijdert de ransomware Volume Shadow Copies en andere back-upgegevens om herstel van bestanden zonder losgeldbetaling vrijwel onmogelijk te maken.

5.3 Encryptie proces



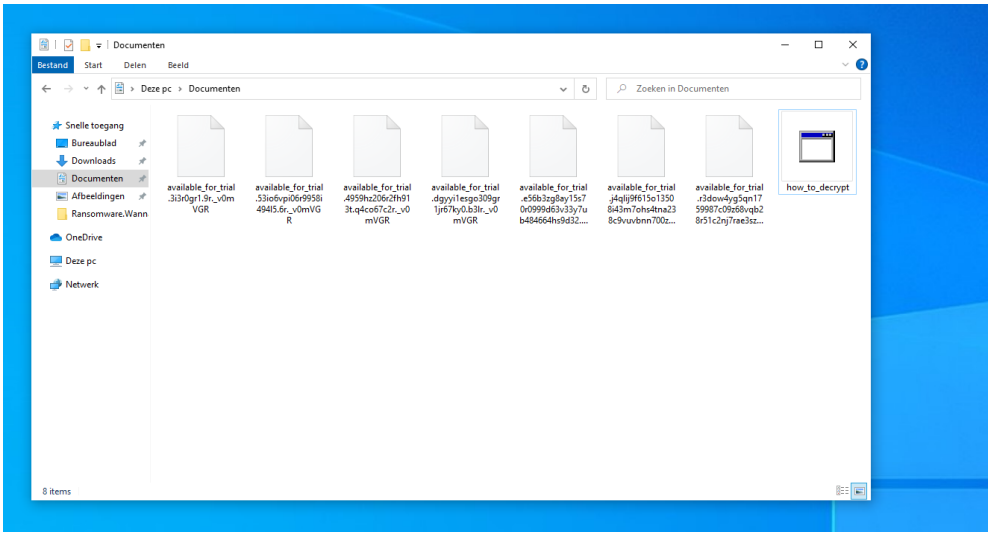
5.4 Trigona aanval simulatie

In deze fase ga ik Trigona uitvoeren op de test omgeving, ik heb enkele bestanden aangemaakt, fotos, pdfs en deze in de documents folder geplaatst,

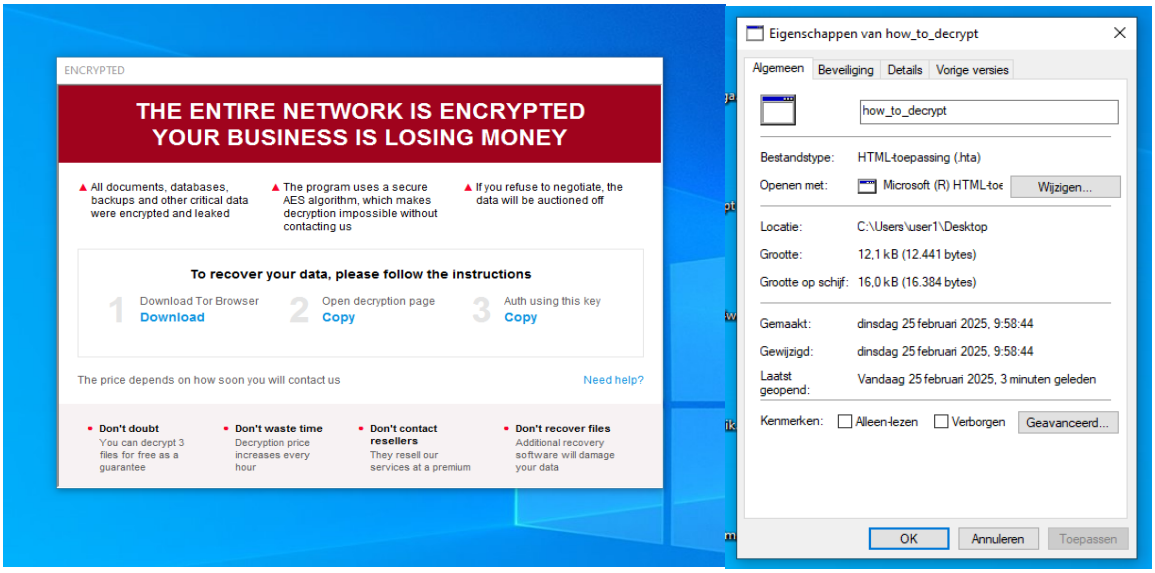


Figuur

Na uitvoering van de ransomware veranderen de bestand extensies en de inhoud wordt geencrypteert, in elke folder wordt er ook een ransomnote gedropped die als popup blijft verschijnen op het scherm



Figuur



Figuur

5.5 Conclusie

6.0 Sample 4 – LockBitV3

Algoritme	Hash
SHA1	C4A6066A02A1FF343CDD5B4DB3FC2FA2481B9D17

LockBitV3, ook wel bekend als LockBit Black, is een geavanceerde ransomware-variant die voortbouwt op de technieken van zijn voorgangers en logica overneemt van andere beruchte families zoals BlackMatter. Ik heb een sample van de LockBitV3 builder gevonden op GitHub:

https://github.com/Tennessene/LockBit

Met deze builder kan ik mijn eigen sample creeren van lockbit, de builder wordt aangebieden als een RaaS waarbij een aanvaller de builder kan kopen en zelf configuraties kan aanpassen om zijn eigen variant van de LockBitV3 ransomware te creeren

6.1 Analyse van de LockBit3 Builder

De LockBit3 builder, te vinden in het bestand LockBit3Builder.7z, bevat de nodige componenten om ransomwarevarianten te genereren:

- build.bat: Script dat encryptie- en decryptieprocessen aanstuurt.
- builder.exe: Bouwt de uitvoerbare ransomware of decryptor.
- config.json: Configuratiebestand met alle instellingen.
- keygen.exe: Genereert asymmetrische sleutelparen.

Figuur

```
ckbit > LockBit > Build.bat
1   @echo off
2   echo Press any key to generate the LockBit files (will overwrite existing files)...
3   pause >nul
4   IF exist Build (ERASE /F /Q Build\*.*) ELSE (mkdir Build)
5   echo (1/7) Generating keys
6   keygen -path Build -pubkey pub.key -privkey priv.key
7   echo (2/7) Building decryptor
8   builder -type dec -privkey Build\priv.key -config config.json -ofile Build\LB3Decryptor.exe
9   echo (3/7) Building ransomware executable
10  builder -type enc -exe -pubkey Build\pub.key -config config.json -ofile Build\LB3.exe
11  echo (4/7) Building ransomware executable that requires password
12  builder -type enc -exe -pass -pubkey Build\pub.key -config config.json -ofile Build\LB3_pass.exe
13  echo (5/7) Building ransomware DLL
14  builder -type enc -dll -pubkey Build\pub.key -config config.json -ofile Build\LB3_Rundll32.dll
15  echo (6/7) Building ransomware DLL that requires password
16  builder -type enc -dll -pass -pubkey Build\pub.key -config config.json -ofile Build\LB3_Rundll32_pass.dll
17  echo (7/7) Building reflective DLL
18  builder -type enc -ref -pubkey Build\pub.key -config config.json -ofile Build\LB3_ReflectiveDll_DllMain.dll
19  echo Done.
20  pause >nul
21
```

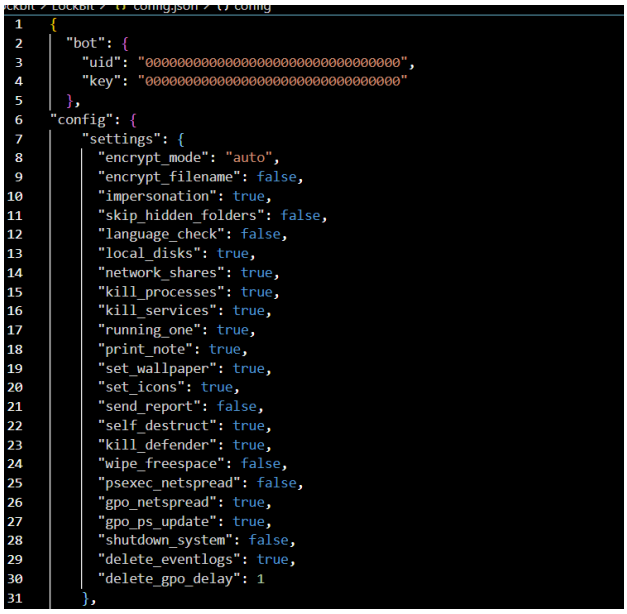
Figuur

In het build.bat-script worden de volgende commando's uitgevoerd:

- keygen: Genereert publieke/private sleutels.
- builder -type dec: Bouwt decryptor.
- builder -type enc -exe: Genereert een uitvoerbare ransomware (EXE).
- builder -type enc -dll: Genereert een DLL ransomware.
- builder -type enc -ref: Genereert een *reflective DLL* ransomware.

Elke gegenereerde variant bevat de publieke sleutel hardcoded, gegenereerd via keygen.exe

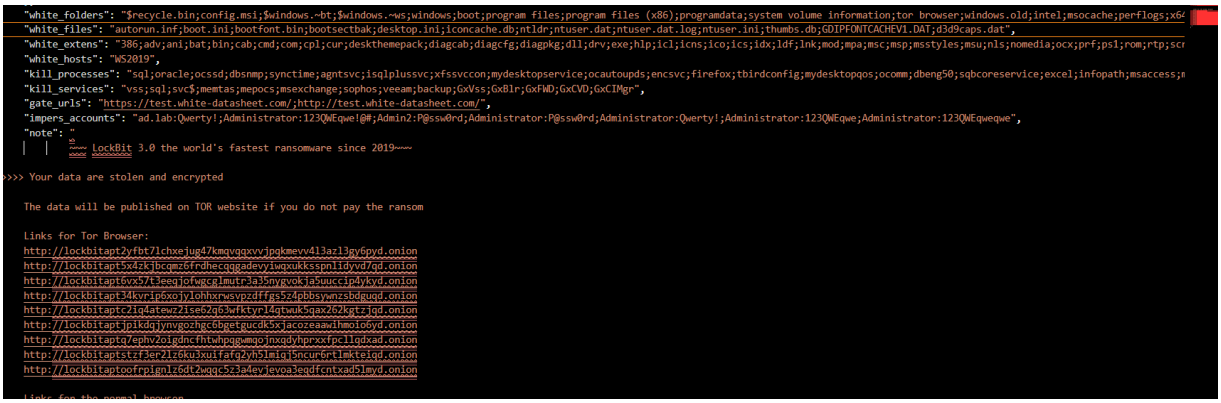
6.2 LockBitV3 configuratie bestand



Figuur

De configuratie woerdt beschreven in de volgende tabel:

Config optie	Beschrijving
encrypt_mode	Bepaalt de manier van encryptie ‘fast’ of ‘auto’
encrypt_filename	Wijzigt bestandsnamen na encryptie (bijv. door extensie toe te voegen of random strings).
impersonation	Probeert administrator-accounts of systeemaccounts te imiteren voor verhoogde rechten.
skip_hidden_folders	Slaat verborgen mappen over tijdens de encryptie.
language_check	Detecteert systeemtaal om bepaalde regio’s te vermijden.
local_disks	Detecteert en encrypteert lokale harde schijven.
network_shares	Detecteert en encrypteert gedeelde netwerkschijven of mappen.
kill_processess	Sluit vooraf bepaalde processen af om toegang tot bestanden te krijgen
kill_services	Sluit vooraf bepaalde *Windows Services* af om toegang tot bestanden te krijgen
print_note	Stuurt de ransom note naar beschikbare printers om af te drukken.
set_wallpaper	Stelt de ransom note in als bureaubladachtergrond.
set_icons	Wijzigt de iconen van geïnfecteerde/geëncrypteerde bestanden.
send_report	Stuurt informatie terug naar de C2-server.
self_destruct	Verwijdert zichzelf na succesvolle uitvoering om detectie te vermijden.
kill_defender	Probeert Windows Defender uit te schakelen of te omzeilen.
wipe_freespace	Overschrijft vrije ruimte op de schijf om herstel van verwijderde bestanden te voorkomen.
psexec_netspread	Verspreidt zichzelf over het netwerk via PsExec en privilege escalation.
gpo_netspread	Verspreiding via aanpassing van Group Policy Object (GPO).
gpo_ps_update	Injecteert PowerShell-scripts in GPO-updates voor verspreiding.
shutdown_system	Herstart het systeem
delete_eventlogs	Herstart of sluit het systeem af na voltooiing van de aanval.
delete_gpo_delay	Verwijdert aangepaste GPO’s na uitvoering om sporen te wissen.



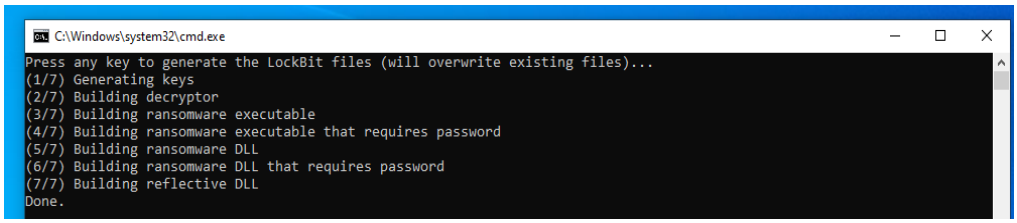
Figuur

Config optie	Beschrijving
white_folders	Een lijst met mappen die niet worden versleuteld.
white_files	Een lijst met bestanden die niet worden versleuteld.
white_extens	Een lijst met bestandsextensies die niet worden versleuteld.
white_hosts	Lijst van hostnamen of IP's die niet worden aangevallen.
kill_processes	Lijst van processen die actief worden beëindigd tijdens uitvoering.
kill_services	Lijst van services die actief worden beëindigd tijdens uitvoering.
gate_urls	C2-domeinen waar de malware mee communiceert.
impers_accounts	Gebruikersaccounts die worden geïmiteerd voor elevated privileges.
note	De tekst van het ransom note dat wordt getoond aan het slachtoffer.

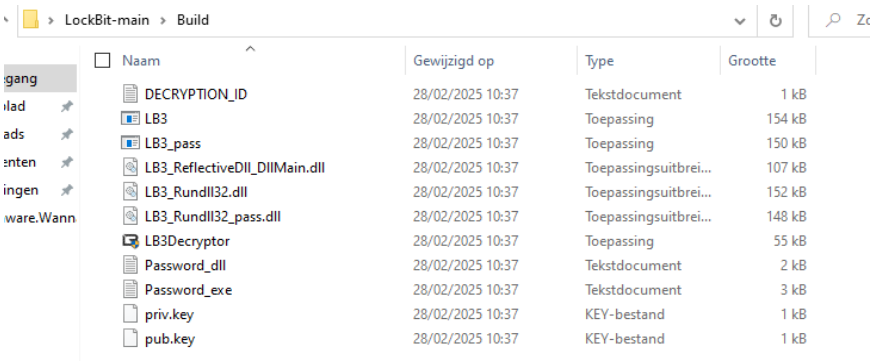
https://www.cybereason.com/hubfs/dam/collateral/reports/Threat-Analysis-Assemble-LockBit-3.pdf

6.3 LockBitV3 Build

Vervolgens heb ik mijn eigen versie van LockBit gegenereerd met behulp van de builder door in command prompt build.bat uit te voeren:



Figuur

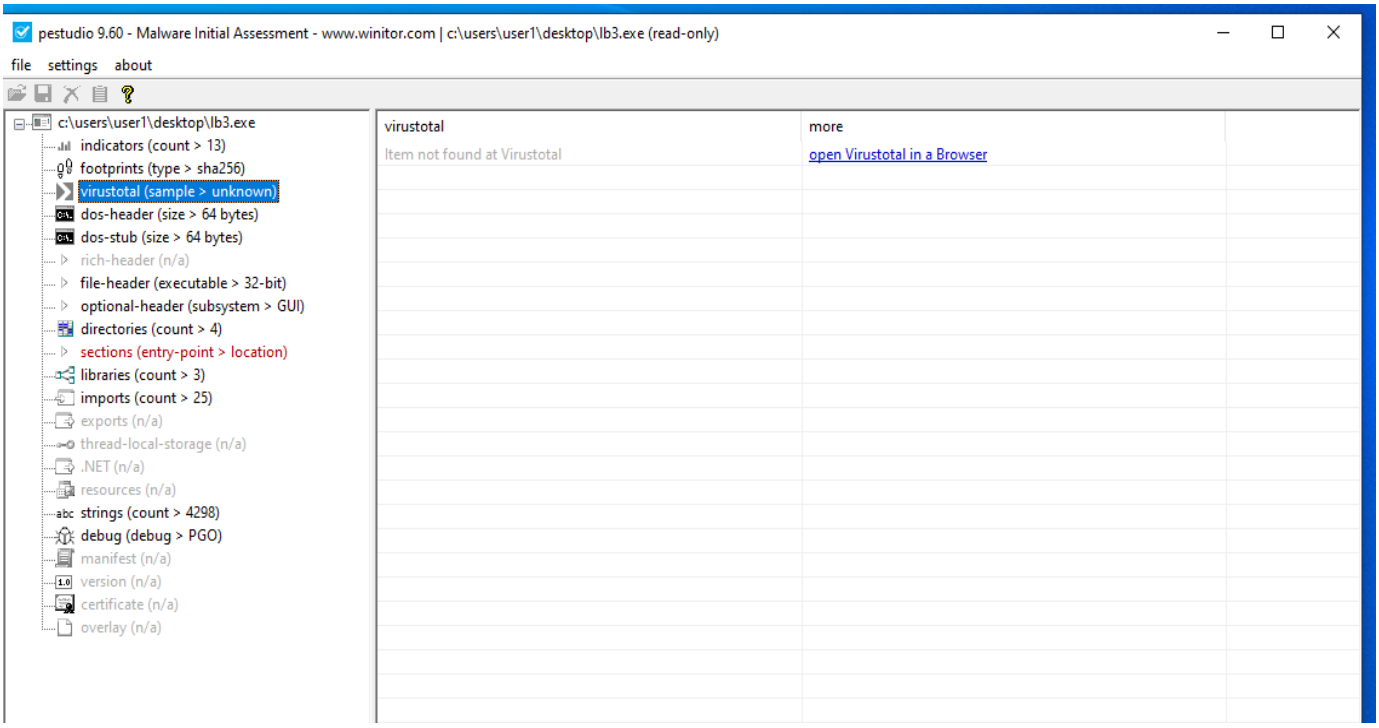


Figuur

Dit genereert de volgende bestanden, te zien in de bovenstaande figuur, en beschreven in het tabel:

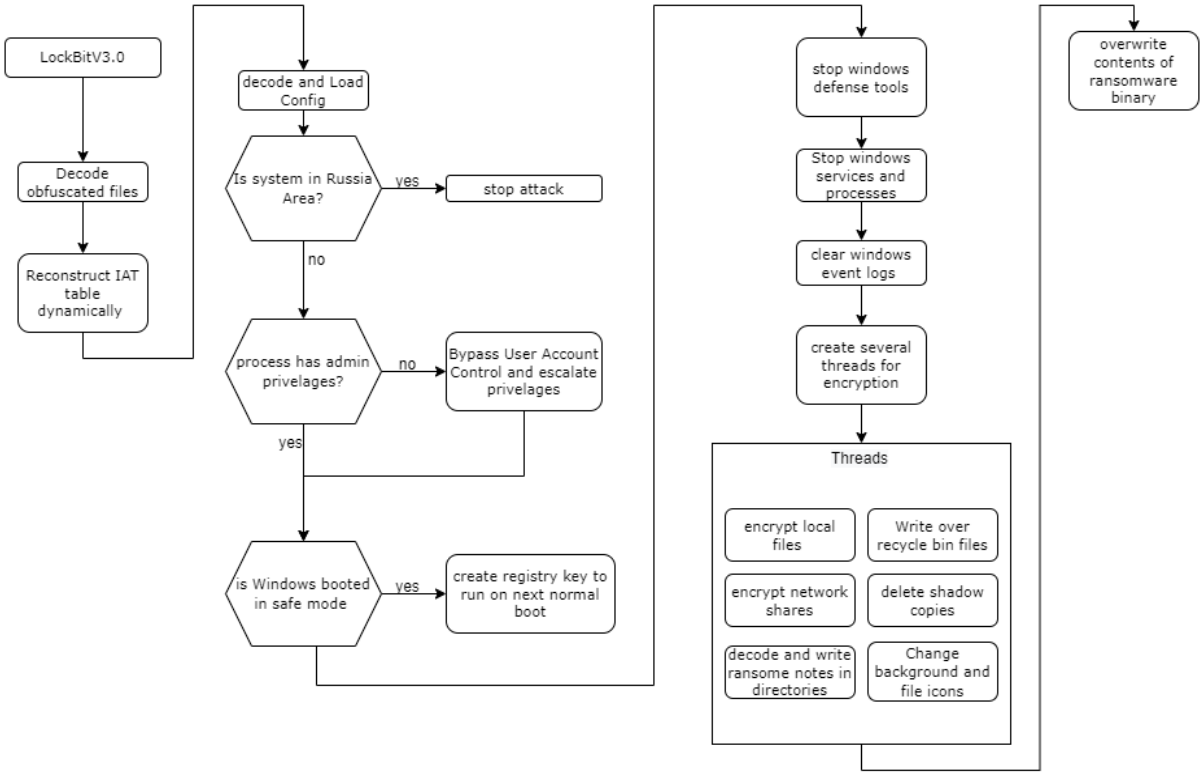
Config optie	Beschrijving
DECRYPTION_ID	Bevat het unieke ID voor decryptie (meestal gekoppeld aan een specifieke build/slachtoffer)
LB3.exe	De uitvoerbare versie van LockBitV3
LB3_rundll32.dll	DLL voor executie via rundll32.exe
LB3_reflectivedll_dllmain.dll	DLL die bedoeld is voor reflective DLL injection (techniek om DLL's in geheugen te injecteren zonder op schijf te schrijven)
LB3Decryptor	Tool die gebruikt wordt om versleutelde bestanden te ontsleutelen met de private key
Password_dll/exe	Bevat de wachtwoorden voor de versleutelde LockBit-versies
priv.key / pub.key	De gegenereerde private en public keys van de ransomware

Bij elke buid van LockBitV3, krijg je een unieke variant, hierdoor is het bijna onmogelijk om de ransomware te herkennen aan de hand van een checksum, zoals een SHA-256-hash, aangezien elke build een andere hash oplevert. Dit blijkt ook uit mijn build: mijn zelfgebouwde LockBitV3-variant werd niet gedetecteerd door VirusTotal:



Figuur

6.4 Werking van LockBitV3



Figuur

In de bovenstaande figuur is een flowchart uitgetekend van de verschillende fases die LockBitV3 onderneemt in deze sectie zal ik deze fases beschrijven:

1. Decode, unpack en reconstructie**:** De LockBitV3 executable is eigenlijk een *dropper*, deze *dropper* bevat de kwaadaardige code en bestanden. Deze code en bestanden zijn geencrypteerd, Hierdoor wordt detectie door statische virusscanners vermijdt. Als eerst worden functies aangeroepen uit kernel32.dll en advapi32.dll om de geëncrypteerde executable te decrypten en uit te voeren, de ransomware is nu actief en de configuratie wordt ingeladen.

2. Privelage escalation en taalcheck: Na het laden van de configuratie controleert LockBit 3.0 de taalinstellingen van het systeem. Als de systeemtaal is ingesteld op Russisch (0x419), Oekraïens (0x22) of Wit-Russisch (0x23), wordt de aanval direct afgebroken.

Als de taalcontrole slaat, probeert de ransomware administratorrechten te verkrijgen. Dit gebeurt door het proces-token van de huidige gebruiker te openen en te controleren of er administrator srechten zijn:

- Als de gebruiker al administrator is, gaat LockBit meteen verder met de infectie.
- Als de gebruiker geen adminrechten heeft, wordt geprobeerd om User Account Control (UAC) te omzeilen en alsnog verhoogde privileges te verkrijgen.

Daarnaast wordt gecontroleerd of het systeem is opgestart in ‘Safe Mode’ dit is omdat het encryptie proces in deze modus niet goed functioneert. LockBit een Windows Registry-key aan die ervoor zorgt dat de ransomware automatisch opnieuw wordt uitgevoerd zodra het systeem opnieuw wordt opgestart.

3. De hoofdactiviteit: uitschakelen, wissen, versleutelen

The modified registry keys are shown below.

Registration key	Software
HKLM\System\CurrentControlSet\Services\SecurityHealthService\Start	Windows Defender Security Center Service
HKLM\System\CurrentControlSet\Services\Sense\Start	Windows Defender 11
HKLM\System\CurrentControlSet\Services\WdBoot\Start	Windows Defender 11
HKLM\System\CurrentControlSet\Services\WdFilter\Start	Windows Defender 11
HKLM\System\CurrentControlSet\Services\WdNisDrv\Start	Windows Defender 11
HKLM\System\CurrentControlSet\Services\WdNisSvc\Start	Windows Defender 11
HKLM\System\CurrentControlSet\Services\WinDefend\Start	Windows Defender 11
HKLM\System\CurrentControlSet\Services\sppsvc\Start	Software Protection
HKLM\System\CurrentControlSet\Services\wscsvc\Start	Security Center Service

Table 7. Windows Defender registry keys

Figuur

In deze fase voert LockBit 3.0 zijn kwaadaardige acties uit. Als eerste probeert LockBitV3 Windows beveiliging uit te schakelen. De ransomware maakt gebruik van *TrustedInstaller-rechten* om antivirussoftware te wijzigen:

- Windows Defender en andere antivirusdiensten worden uitgeschakeld.
- Een vooraf gedefinieerde lijst met processen en services wordt beëindigd.

Vervolgens verwijdert LockBit de Windows Event Logs om detectie en forensische analyse te bemoeilijken. Shadow copies, systeemherstelpunten en de prullenbak worden permanent verwijderd, zodat herstel via standaard Windows-methodes onmogelijk wordt gemaakt. Daarna start het versleutelen van bestanden:

- Hiervoor wordt Salsa20 gebruikt, een snelle symmetrische encryptie-algoritme.
- Zowel lokale schijven als gedeelde netwerkschijven worden gescand. Bestanden worden geselecteerd op basis van hun extensie en locatie.
- Kritieke systeembestanden worden bewust uitgesloten van encryptie om systeemstabiliteit te behouden en detectie te vermijden.
- In elke getroffen map wordt een losgeldbericht (ransom note) geplaatst.
- De iconen van versleutelde bestanden worden aangepast om aan te geven dat ze niet langer toegankelijk zijn.
- De bureaubladachtergrond wordt vervangen door een afbeelding met informatie over de aanval en instructies voor het slachtoffer.

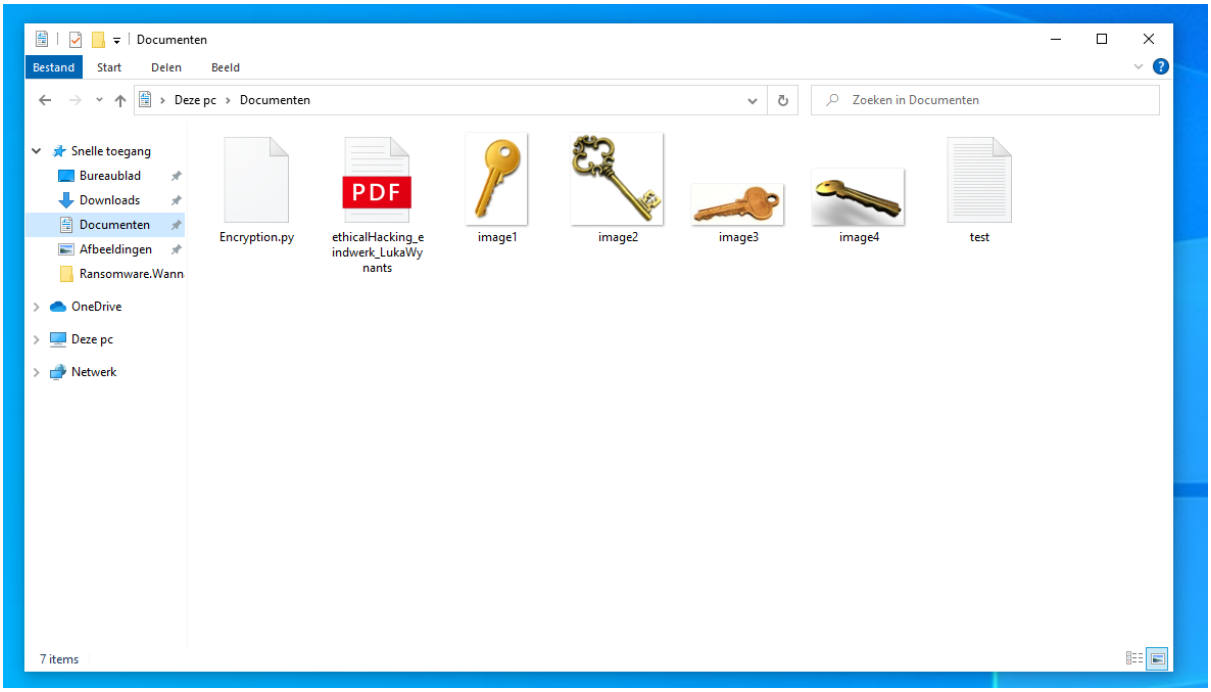
4. Self deletion: Als laatste probeert de ransomware zichzelf volledig van het systeem te verwijderen om detectie en analyse te voorkomen:

- Een tijdelijk proces met een willekeurige naam wordt aangemaakt.
- Dit proces hernoemt en overschrijft de originele ransomware meerdere keren, zodat herstel bijna onmogelijk is.
- Daarna verwijdert het proces zichzelf, waardoor vrijwel geen sporen overblijven.

Deze self-deletion-routine maakt reverse engineering zeer moeilijk en vormt een grote uitdaging voor cybersecurity-experts die proberen de werking van LockBit 3.0 te analyseren.

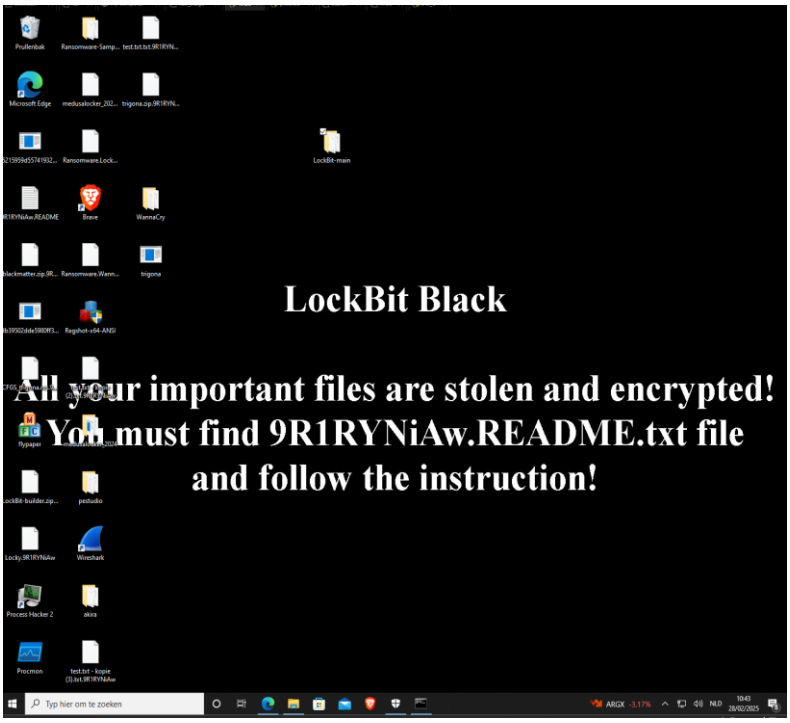
6.5 LockBitV3 aanval simulatie

In deze fase ga ik de ransomware uitvoeren en documenteren wat er gebeurt met mijn systeem. Hiervoor heb ik zeven testbestanden aangemaakt, waaronder enkele foto's, een Python-bestand, een PDF en een testdocument in de Documents-map van *user1*:



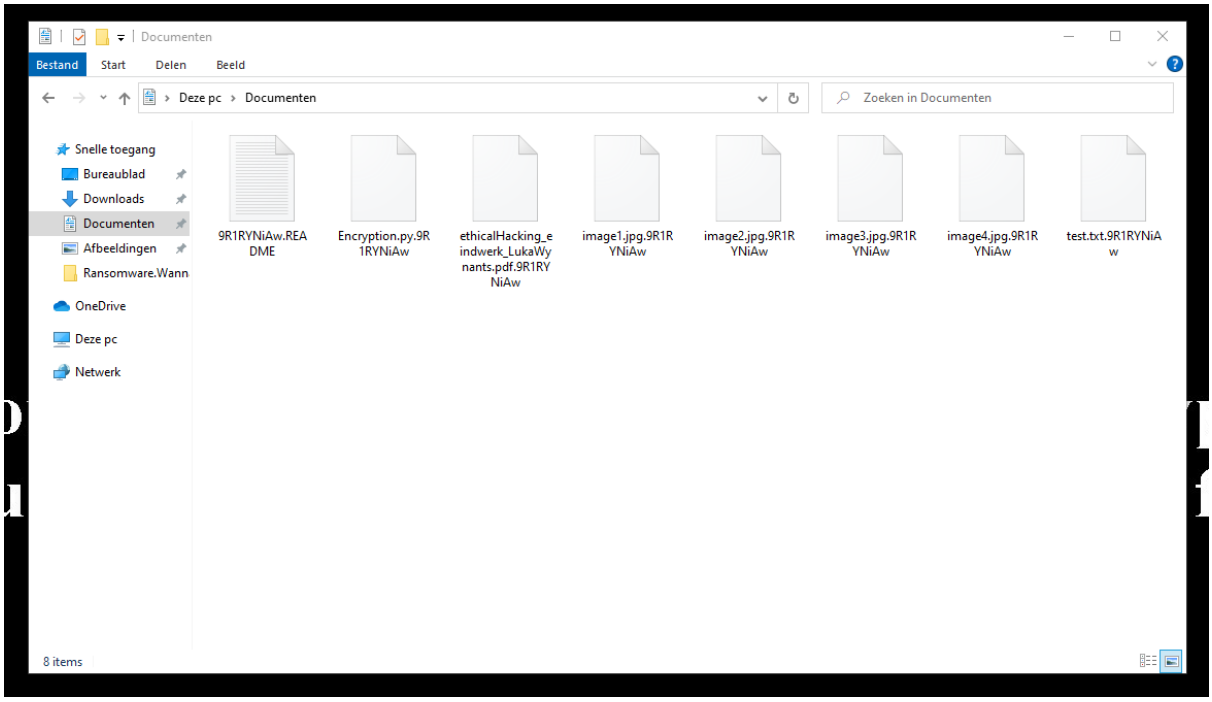
Figuur

Na het uitvoeren van LockBitV3 veranderde de achtergrond van mijn hostmachine. Er verscheen een instructie om een losgeldbericht (ransom note) te lezen. Mijn bureaublad zag er als volgt uit:



Figuur

Bij het openen van de *Documents* folder blijkt dat alle bestanden zijn versleuteld en dat hun extensies zijn aangepast:



Figuur

We zien hier ook dat er een ransom note is achtergelaten met de naam 9R1RYNiAw.README. Wanneer we dit bestand openen, vinden we daarin instructies voor het slachtoffer, samen met links naar de Tor-browser voor verdere communicatie.

```
Bestand  Bewerken  Opmaak  Beeld  Help
>>>> What guarantees that we will not deceive you?

        We are not a politically motivated group and we do not need anything other than your money.

        If you pay, we will provide you the programs for decryption and we will delete your data.
        Life is too short to be sad. Be not sad, money, it is only paper.

        If we do not give you decrypters, or we do not delete your data after payment, then nobody will pay us in the future.
        Therefore to us our reputation is very important. We attack the companies worldwide and there is no dissatisfied victim after payment.

        You can obtain information about us on twitter https://twitter.com/hashtag/lockbit?f=live


>>>> You need contact us and decrypt one file for free on these TOR sites with your personal DECRYPTION ID

        Download and install TOR Browser https://www.torproject.org/
        Write to a chat and wait for the answer, we will always answer you.
        Sometimes you will need to wait for our answer because we attack many companies.

        Links for Tor Browser:
        http://lockbitsupt7nr3fa6e7xyb73lk6bw6rcneqhoyblniiabj4uwvzapqd.onion
        http://lockbitsupuhswh4izvoucoxsbnotkmgq6durg7kficg6u33zfvq3oyd.onion
        http://lockbitsupn2h6be2cnqpvncyhj4rgmnwn44633hnzzmtxdvjoqlp7yd.onion

        Link for the normal browser
        http://lockbitsupp.uz

        If you do not get an answer in the chat room for a long time, the site does not work and in any other emergency, you can contact us in jabber or tox.

        Tox ID LockBitSupp: 3085B89A0C515D2FB124D645906F5D3DA5CB97CEBEA975959AE4F95302A04E1D709C3C4AE9B7
        XMPP (Jabber) Support: 598954663666452@exploit.im 365473292355268@thesecure.biz

>>>> Your personal DECRYPTION ID: B7568014A48684D6D525F3F3722638C4

>>>> Warning! Do not DELETE or MODIFY any files, it can lead to recovery problems!

>>>> Warning! If you do not pay the ransom we will attack your company repeatedly again!
```

Figuur Ransome note

6.6 Conclusie

LockBit 3.0 is waarschijnlijk een van de snelste ransomware-varianten die ik heb getest. Het heeft het vermogen om bestanden binnen vijf seconden te versleutelen, wat extreem snel is vergeleken met andere ransomware-families.

Daarnaast heeft deze ransomware nog steeds een relatief lage detectiegraad, wat betekent dat het in veel gevallen ongehinderd kan worden uitgevoerd zonder dat antivirussoftware of beveiligingsmechanismen direct alarm slaan.

Een opvallend verschil met eerdere ransomware, zoals WannaCry, is dat LockBit 3.0 geen administratorrechten nodig heeft om zijn payload uit te voeren en terwijl SmartScreen bij WannaCry nog een waarschuwing kon geven dat het niet veilig was om het bestand uit te voeren, gebeurt dit bij LockBitV3 niet. Dit toont aan hoe geavanceerd en stealthy deze ransomware is in vergelijking met oudere varianten.

Door de combinatie van snelheid, stealth-technieken en een effectieve encryptieaanpak blijft LockBit 3.0 een van de gevaarlijkste en meest efficiënte ransomware-bedreigingen die momenteel bestaat.

Bronvermelding

[1] Jan, A. (2015-04-12). De titel van dit werk. Opgehaald van https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

[2] https://en.wikipedia.org/wiki/Kaseya_VSA_ransomware_attack.

Wannacry

https://gist.github.com/xpn/facb5692980c14df272b16a4ee6a29d5

https://icact.org/upload/2018/0369/20180369_finalpaper.pdf

https://blog.talosintelligence.com/wannacry/

https://www.microsoft.com/en-us/security/blog/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/?source=mmpc

https://thewebchap.wordpress.com/2017/05/16/wannacry-detailed-analysis-part-1/

Akira

https://news.sophos.com/en-us/2023/12/21/akira-again-the-ransomware-that-keeps-on-taking/

https://news.sophos.com/en-us/2023/05/09/akira-ransomware-is-bringin-88-back/

https://blog.qualys.com/vulnerabilities-threat-research/2024/10/02/threat-brief-understanding-akira-ransomware

https://blog.qualys.com/vulnerabilities-threat-research/2024/10/02/threat-brief-understanding-akira-ransomware

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a

https://www.nomoreransom.org/uploads/User%20Manual%20-%20Akira_Decryptor.pdf

trigona

https://www.acronis.com/en-sg/cyber-protection-center/posts/trigona-a-ransomware-wiper/

https://www.sentinelone.com/anthology/trigona/

https://unit42.paloaltonetworks.com/trigona-ransomware-update/

https://www.csk.gov.in/alerts/Trigona_ransomware.html

https://unit42.paloaltonetworks.com/trigona-ransomware-update/

https://www.zscaler.com/blogs/security-research/technical-analysis-trigona-ransomware

Lockbit

https://www.cybereason.com/hubfs/dam/collateral/reports/Threat-Analysis-Assemble-LockBit-3.pdf [2]

https://www.trendmicro.com/en_be/research/22/g/lockbit-ransomware-group-augments-its-latest-variant--lockbit-3-.html

https://github.com/NorthwaveSecurity/lockbit3/tree/main

https://www.virustotal.com/gui/file/3c304f0319051bfedfbd91caf611cc1a2c66038eee61d43f96c0b2bfb1c576b1/details