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

Analizë teknike për skedarin keqdashës AgentTesla

Versioni: 1.0
Data: 22/04/2024

PËRMBAJTJA

LISTA E FIGURAVE

Raporti është hartuar për të dokumentuar dhe analizuar tentativa sulmesh kibernetike ndaj infrastrukturave Kritike në Republikën e Shqipërisë. Përmbajtja e këtij raporti bazohet në informacionet e disponueshme deri në datën e përfundimit të analizës.

Përcjellja e këtij raporti ka për qëllim informimin dhe ndërgjegjësimin e palëve të interesuara mbi incidentin kibernetik të dokumentuar. Raporti nuk duhet trajtuar si përfundimtar deri në përditësimin final të tij.

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 malinj 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.

AKCESK rezervon të drejtën për të ndryshuar, përditësuar, ose ndryshuar çfarëdo pjesë të këtij raporti pa lajmërim paraprak.

*Ky raport nuk është një dokument përfundimtar (nxjerrja e detajeve hyr*ëse të aktorëve keqdashës do ju vihet në dispozicion në një moment të dytë*).*

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.

Përmbledhje ekzekutive

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike realizoi një analizë të detajuar teknike të skedarit keqdashës **Agent Tesla Remote Access Trojan (RAT) v4,** i cili synoi infrastrukturën kritike brenda Republikës së Shqipërisë. Ky raport përmbledh gjetjet nga analiza statike dhe dinamike e skedarit keqdashës, duke theksuar treguesit kryesorë të kompromentimit, teknikat e përdorura nga skedari keqdashës bazuar në kornizën ***MITRE ATT&CK*** si dhe ofron rekomandime për të zbutur kërcënimin.

Gjetjet Kyçe:

Skedari keqdashës u identifikua përmes ekipit të monitorimit në formën e *mail phishing* në një nga infrastrukturat kritike që AKCESK monitoron. Analiza konfirmoi që skedarët janë pjesë e familjes **AgentTesla RAT**, një lloj virusi që lejon aktorët keqdashës të përgjojnë në sistemet e kompromentuara dhe të marrin kredencialet e këtyre sistemeve. U kryen ekzaminime të detajuara mbi komponentë të ndryshëm të skedarit keqdashës, duke përfshirë **kugR.exe, Tyrone.dll** dhe skedarë të tjerë të lidhur, duke zbuluar vetitë e tyre dhe metodat e sofistikuara të përdorura për të shmangur zbulimin ndaj sistemeve mbrojtëse ***(antivirus)*** dhe analizën e detajuar.

U identifikuan tregues të kompromentimit, duke përfshirë vlerat hash për skedarë të ndryshëm dhe tregues të rrjetit.

Raporti thekson nevojën për vigjilencë dhe masa proaktive përballë kërcënimeve kibernetike të sofistikuara, duke vënë në pah rëndësinë e përditësimeve të rregullta dhe zbatimit të praktikave të rekomanduara të sigurisë për të mbrojtur infrastrukturën kritike.

Informacione teknike

Referuar raportimit nga ekipi i monitorimit për një email ***Phishing*** në një nga infrastrukturat kritike në Shqipëri, u shkarkuan për analizë më të thelluar disa skedarë të dyshuar si keqdashës. Gjatë analizimit statik dhe dinamik të skedarëve, rezulton që njëri nga skedarët është i familjes ***Trojan*** përkatësisht ***Agent Tesla RAT (remote access trojan) v4,*** ku qëllimi kryesor është marrja e kredencialeve dhe përgjimi i sistemit (spyware). Gjatë analizës u evidentua se ky virus merr kredencialet e ruajtura të SMTP, shfletuesve të ndryshëm (Mozilla, Chrome etj.), Outlook, Discord, NordVPN etj.
Përmes analizës së kodit burim janë gjetur gjithashtu kredenciale të cilat përdoren për të marrë të dhënat përmes SmtpClient. Për një komunikim sa më diskret aktorët keqdashës përdorin emaile të kompromentuara.

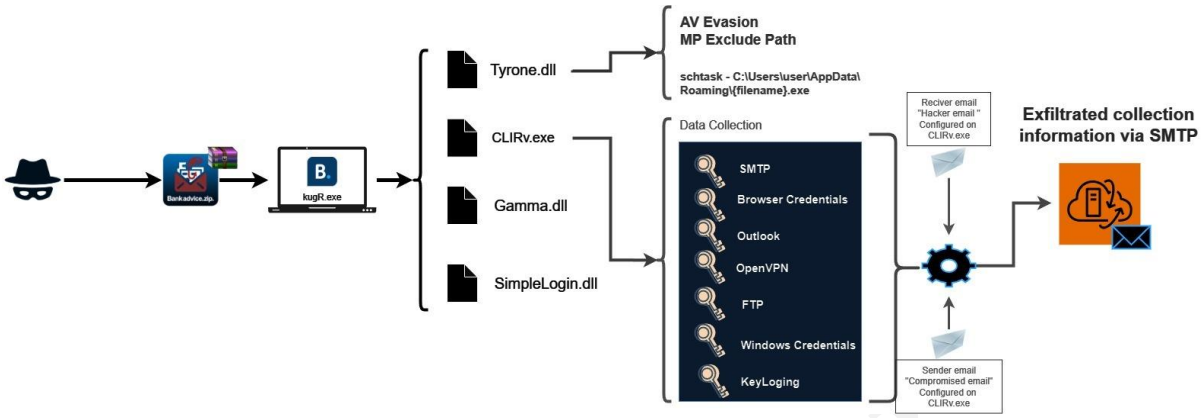

Figura 1: Skema e shpërndarjes së skedarit keqdashës

Analiza e skedarit kugR.exe

Ekzekutuesi **kugR.exe** është një skedar që përdor librarinë .NET i shkruar në gjuhën e programimit C#.

Sha256:
EF171F71804FE96BF375379C691E1F93B3FE38A3535B24F8F19D104E5EECF7AA

Figura 2: kugR.exe

Në figurën e mësipërme në pamje të parë duket se kemi të bëjmë me një aplikacion legjitim që merret me rezervimin e dhomave (Booking), por gjatë analizës statike duke parë kodin shikohet që përveç implementimeve legjitime evidentohet ndër të tjera kod i fshehtë (***obfuscated)*** dhe i paketuar (***packed*** -Teknikë që përdoret nga zhvilluesit e programeve në mënyrë që kodi i tyre të mos jetë i lexueshëm nga zhvilluesit e tjerë).

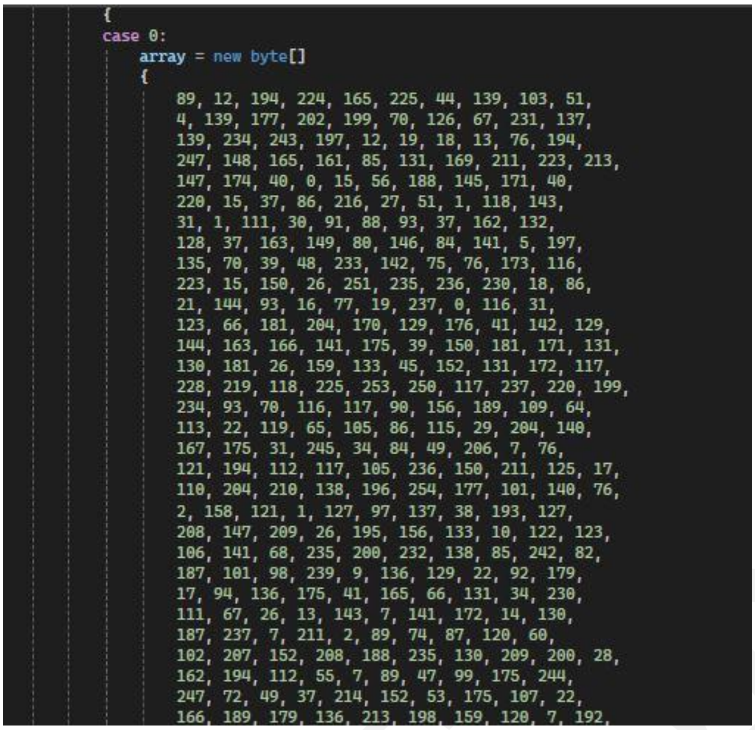

Figura 3: Vektor me byte

Figura 4: Vektor me karaktere

Aktorët kërcënues në raste të tilla përdorin algoritme komplekse të cilat gjatë ekzekutimit të skedarit kryesor këto pjesë kodi i rikthejnë në formate të ekzekutueshme (.exe) të cilat përkthehen në format hexadecimal që nisin me 4D 5A. Në .NET përdoret ***Reflection*** e cila shërben për të thirrur metoda nga formate ***dll*** apo skedarë të ekzekutueshëm. Kjo është një teknikë e përdorur pasi gjatë ekzekutimit të skedarit kryesor jo gjithmonë mund të zbulohen nga antivirusi. Duke qënë se kemi një nivel kaq të lartë fshehje, bëjmë një kontroll nëse kemi ***packers*** të kodit.

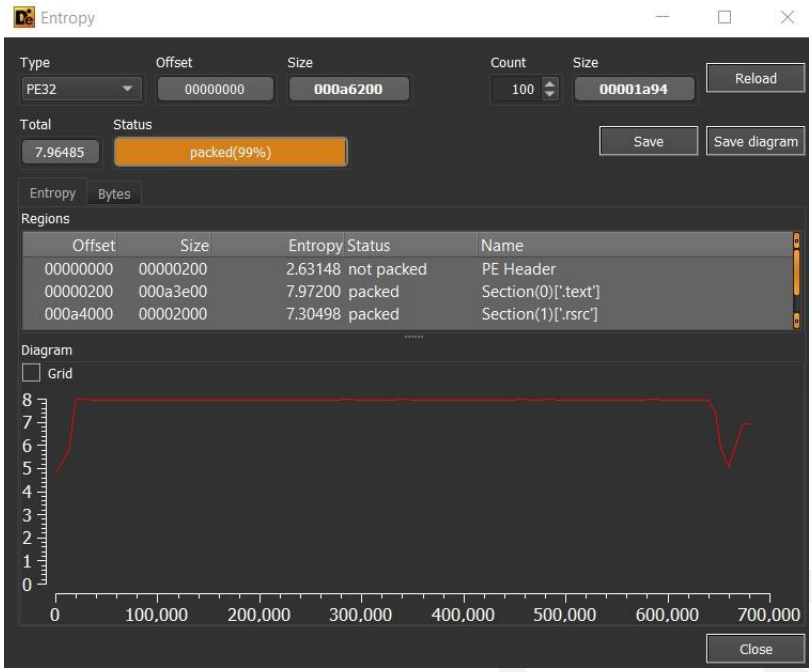

Figura 5: Entropia e skedarit kugR.exe

Evidentohet se kemi në pjesë te ndryshme të skedarit entropi mbi vlerën 5 (pesë), indikator i cili na jep informacion se kemi të bëjmë me kod të paketuar (***packed)***.
Prandaj vijojmë me pjesën e analizës duke tentuar ta kthejmë skedarin në një format sa më të lexueshëm.

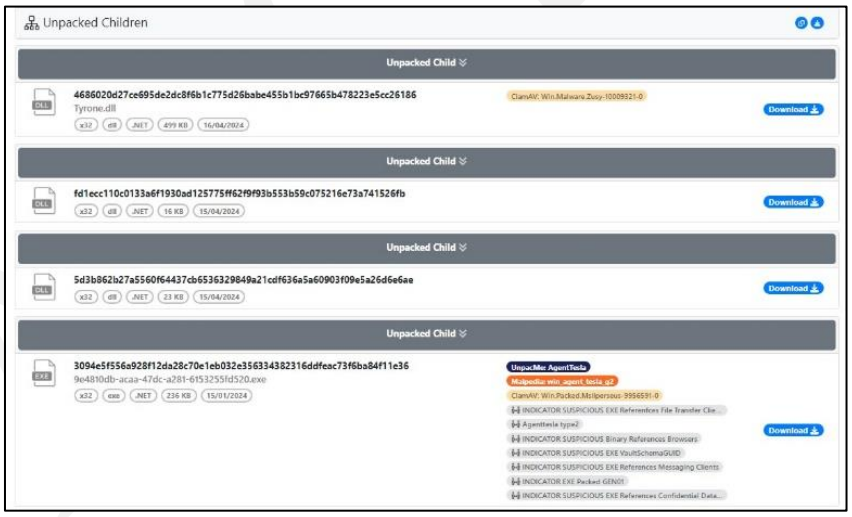

Figura 6: Skedarët e zbërthyer (unpacked)

Nga skedari prind dalin dhe 4 skedarë të tjerë të shkruar në C# me librarinë .NET. Kur i importojmë këto skedarë evidentohet se janë projekte të ndryshme:

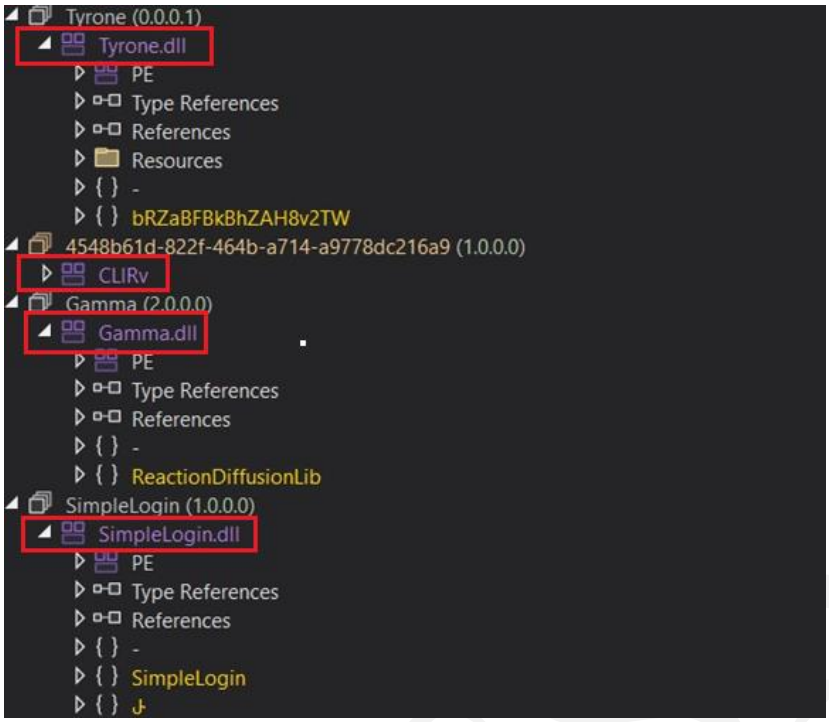

Figura 7: Projektet e zbërthyera (unpacked)

Skedari **Tyrone.dll** është një skedar i tipit **.dll** (dyamic-link-library) i shkruar në C#. Në këtë skedar gjenden disa *namespace* të implementuar ku evidentohet një nivel mjaft i lartë i fshehjes së kodit. Disa nga vlerat e *strings* të zbuluara janë:

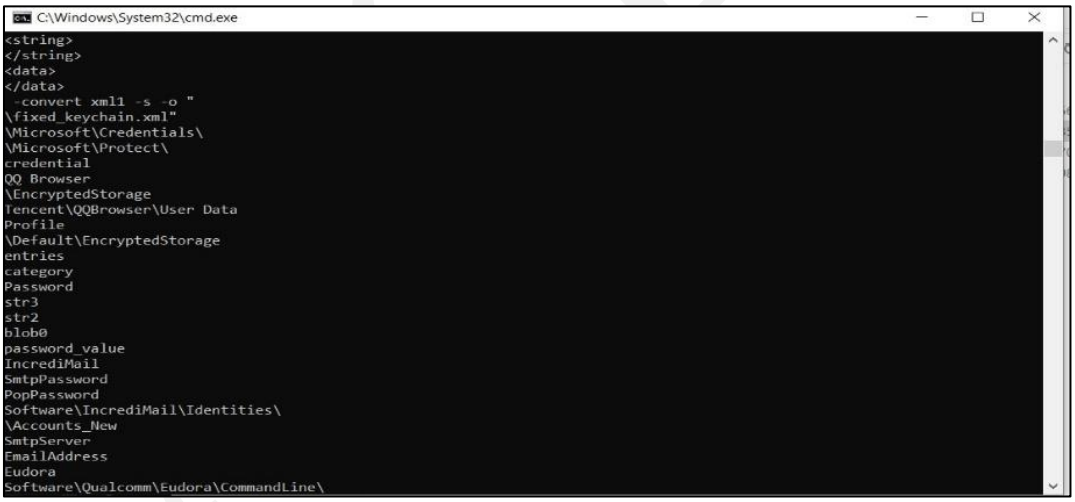

Figura 8: Strings të zbuluar

Për të kuptuar se për cfarë shërben ky skedar krijojmë një projekt të tipit **Console** dhe gjenerojmë një skedar të ekzekutueshëm (.exe) dhe ngarkojmë këtë **dll** duke thërritur metodat që ka të implementuara. Kjo bëhet për arsye sepse vetëm gjatë *run time* mund të marrim vlerat e secilit variabël të funksioneve. Zgjedhim path-in e skedarit **dll**. Ngarkojmë skedarin dhe tentojmë të thërrasim një nga metodat që është e implementuar. Vendosim një *breakpoint* në skedarin ***dll*** dhe shikojmë vlerën e afishuar. Gjatë ekzekutimit evidentohet se në path-in *C:\Users\User_1\AppData\Roaming* krijohet një skedar i ekzekutueshëm i cili është po vetë skedari kryesor por i emërtuar në mënyrë rastësore. Gjithashtu gjatë ekzekutimit, ekzekutohet

skedari ***schtasks.exe.*** Ky skedar shërben për të krijuar një task me emrin **UPDATE**. Kjo bëhet për arsye që të krijohet qëndrueshmëria (***persistence***) nga aktorët keqdashës.

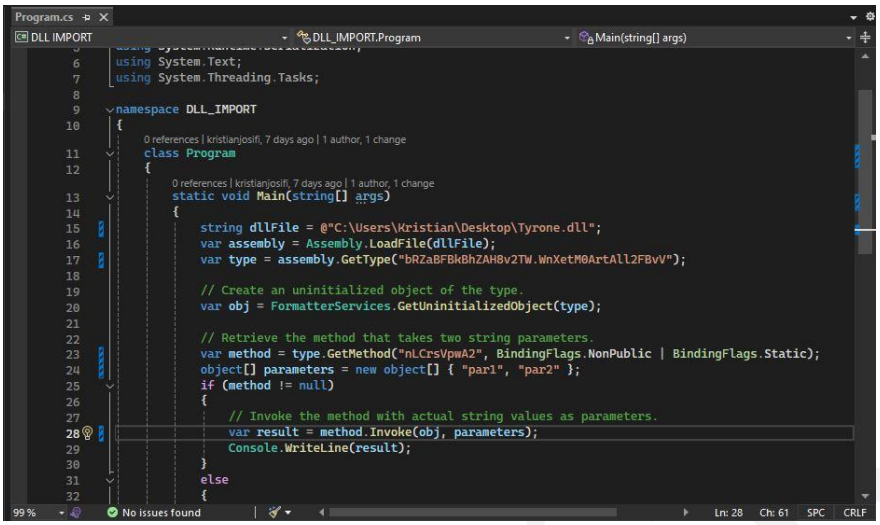

Figura 9: Thirrja e skedarit Tyrone.dll

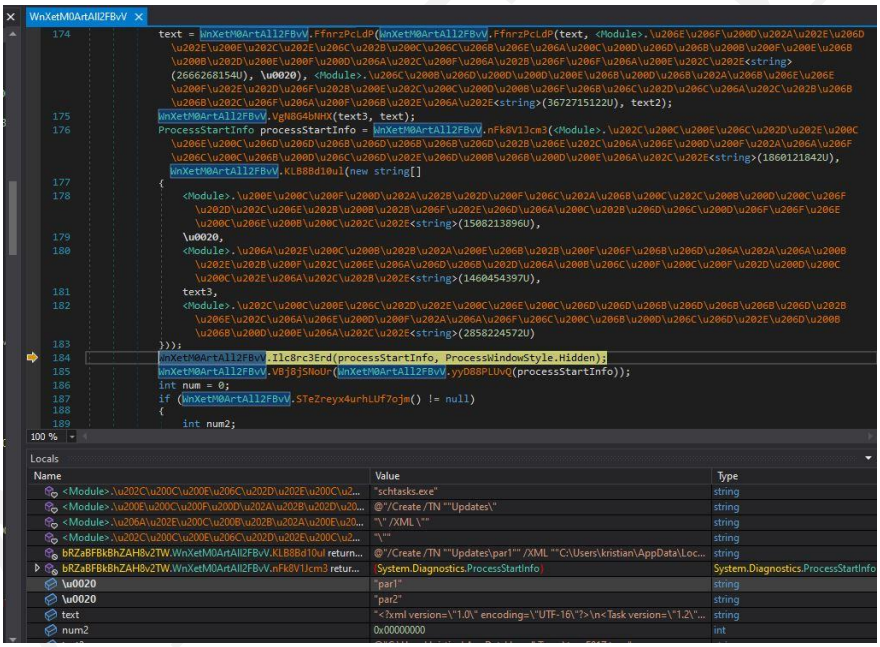

Figura 10: schtasks.exe

Nga kodi burim i skedarit të krijuar duket që tentohet të modifikohen të drejtat, kjo gjë evidentohet pasi një string i enkoduar me *base64* gjatë dekodimit përkthehet në një skedar në formatin **xml**.

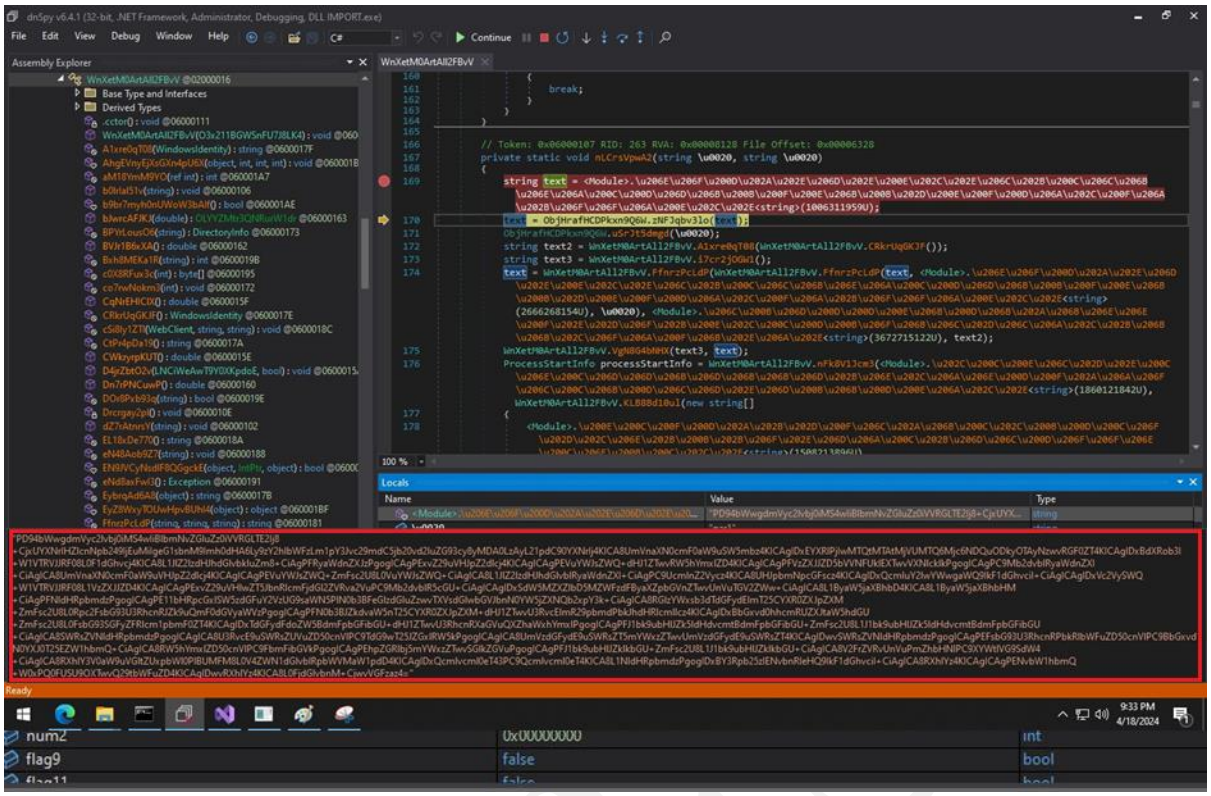

Figura 11: Enkodimi me base64

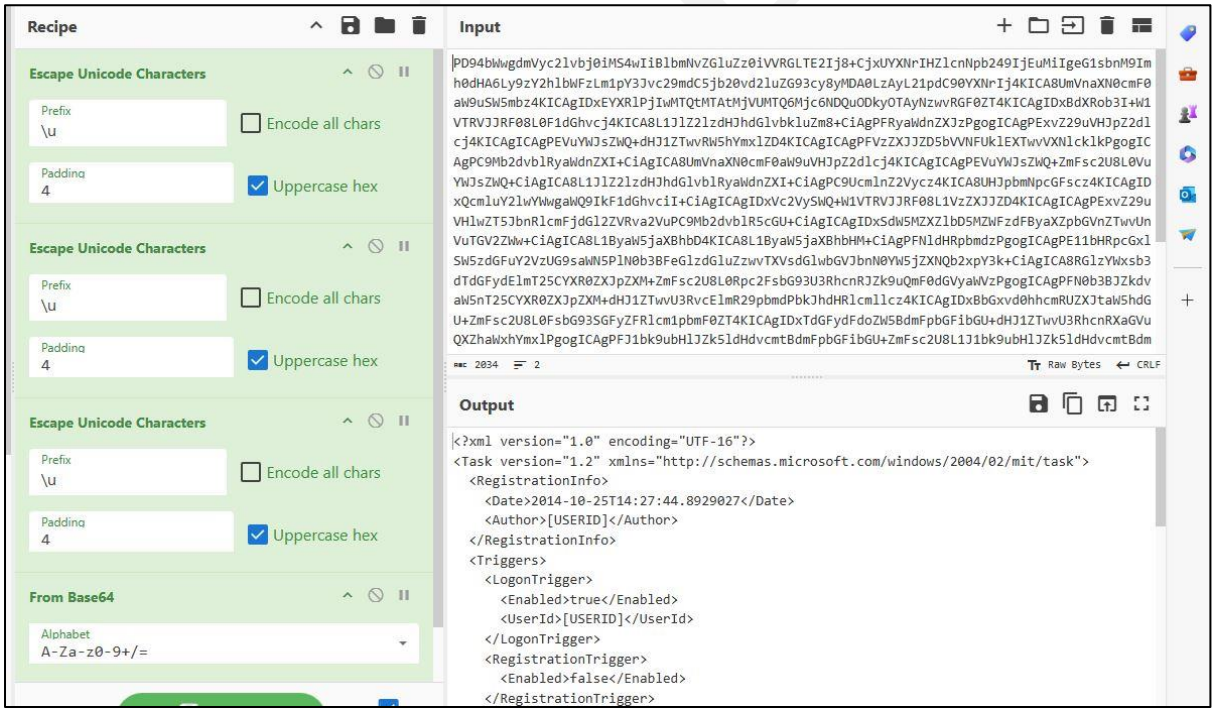

Figura 12: Të drejtat në XML

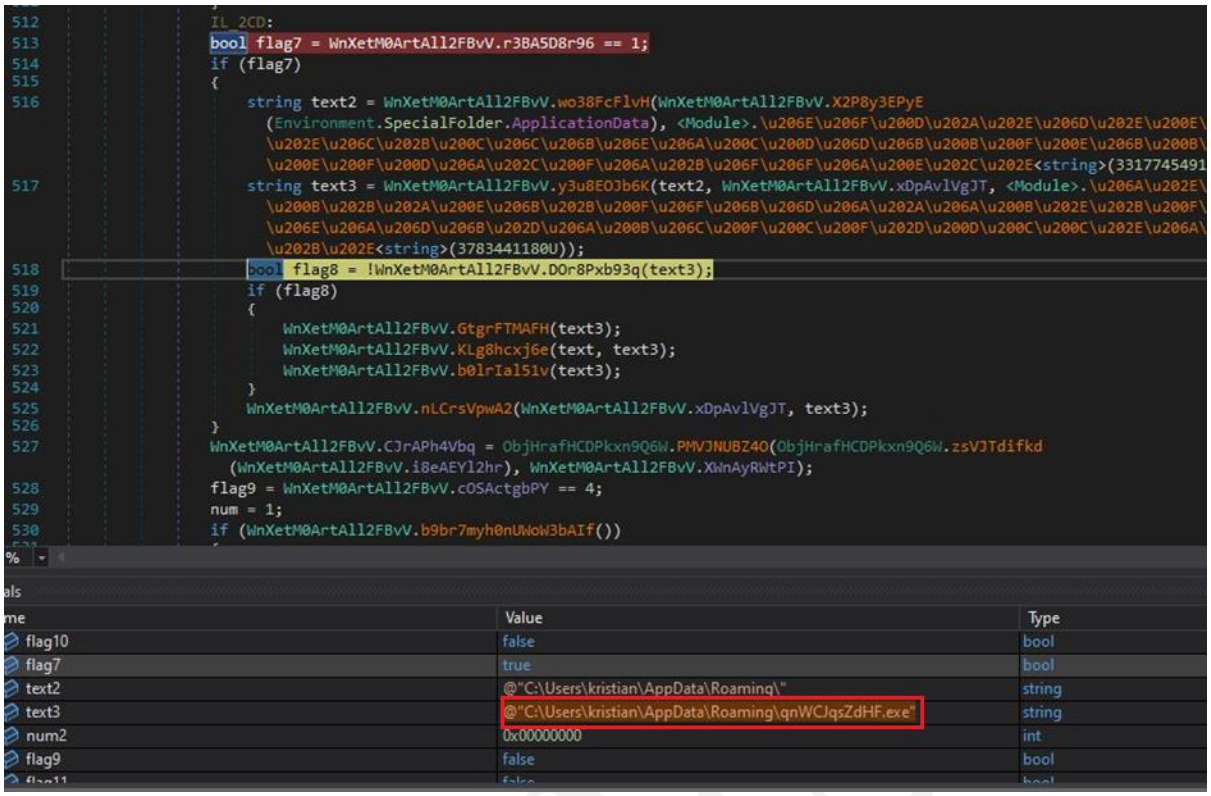

Figura 13: APPDATA

Por gjithashtu evidentohet dhe një komandë e ekzekutuar në Powershell, e cila shërben për të anashkaluar antivirusin.

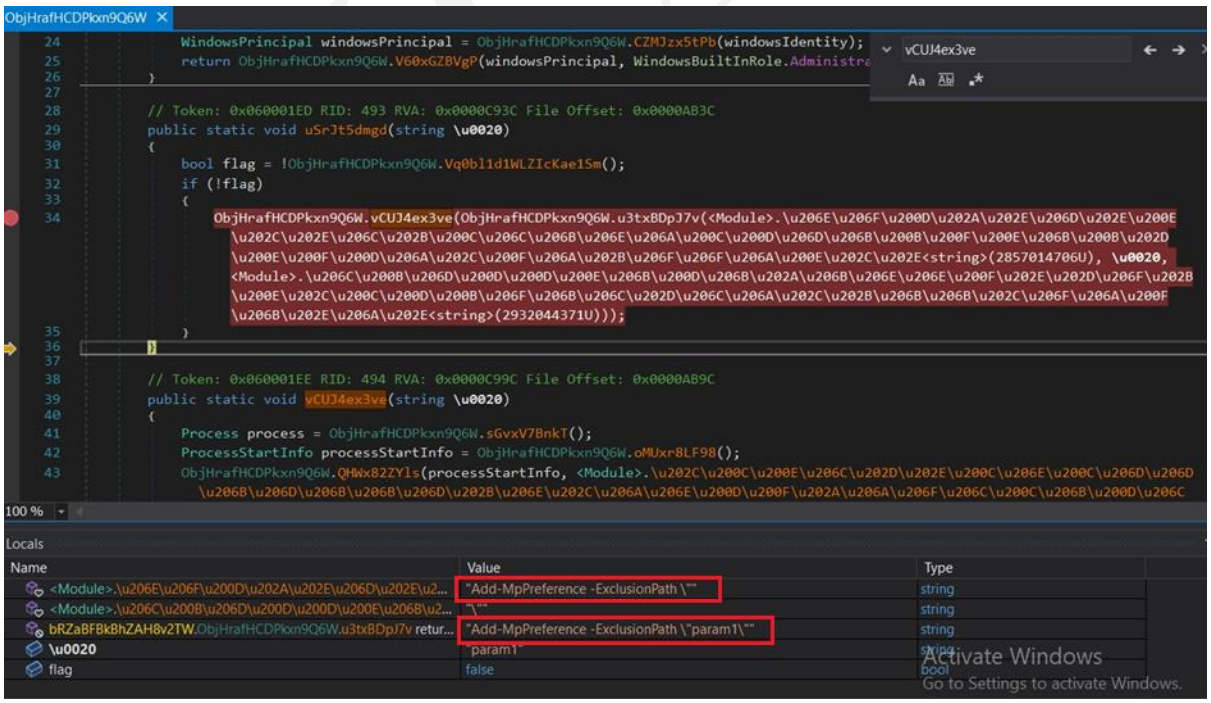

Figura 14: Komanda në Powershell për anashkalimin e antivirusit

Gjatë analizës së skedarit **CLIRv.exe,** evidentohet se ky skedar është një skedar keqdashës **Agent Tesla.**

Sha256:
1403E7C01BF67C9AC15E1D9068FAABDD21C05132CCE0C517C69425DB766FF140

Nga analiza statike e kodit, ky skedar është i shkruar në C# në .NET. Në kodin burim evidentohet se kemi të bëjmë me një **stealer** të kredencialeve. Skedari keqdashës ka të implementuar disa kredenciale të cilat i përkasin një server **smtp** për dërgimin e emaileve.

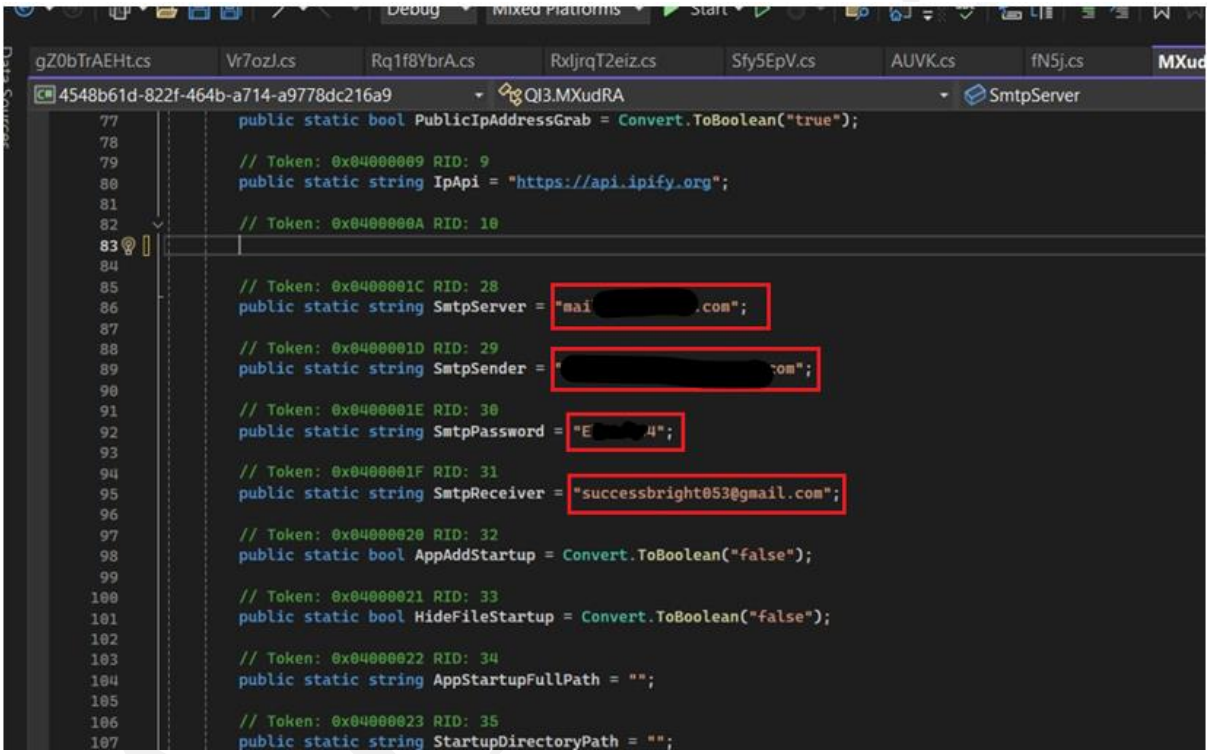

Figura 15: Kredencialet e SMTP

Gjithashtu në këtë skedar evidentohet një klasë (***Class***) me emrin **8WQvgbiWI1.Cs**. Kjo klasë shërben për të krijuar instanca të klasës dhe i mbush ato me të dhëna, përkatësisht me hostin, përdoruesin, password-in, aplikacionin. Kemi të implementuar një ndërfaqe e cila ka si funksion, funksionin **Grab().** Kjo ndërfaqe ka disa implementime brenda në aplikacion, ku çdo implementim i funksionit shërben për të marrë kredenciale nga aplikacione të ndryshme.

Figura 16: Metoda Grab()

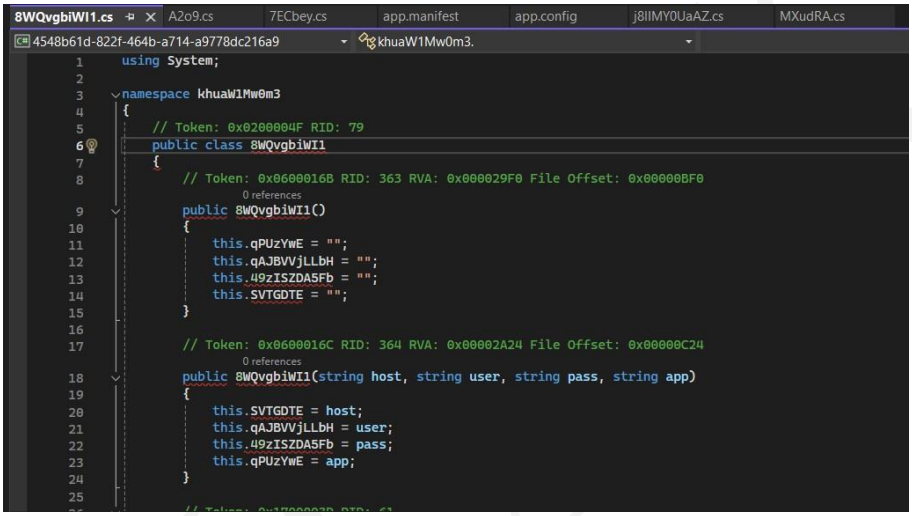

Figura 17: Klasa për marrjen e të dhënave

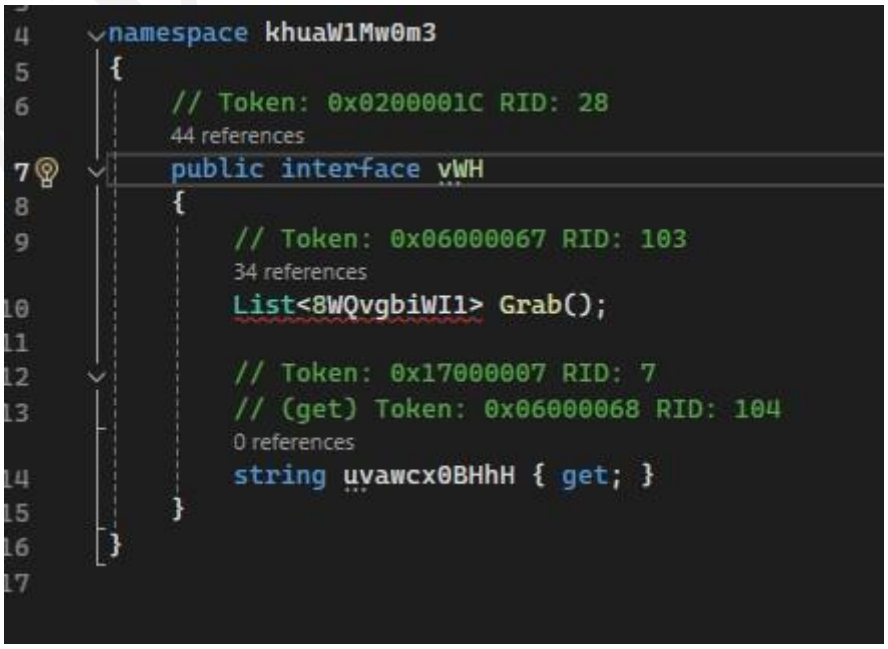

Figura 18: Funksioni Grab()

Nëse shikojmë një nga implementimet e funksionit **Grab()** psh në rastin e Outlook.

- Implementimi ruan një listë të tipit **8WQvgbiWI1**.
- Krijon një vektor me objekte të tipit **Registry key** dhe nis procesin e *enumeration* për të kërkuar informacione mbi regjistrat ***default*** ku ruhen informacione mbi aplikacione të ndryshme.
- Krijon një instancë të **8WQvgbiWI1** dhe mbush variablat me të dhënat si emrin e përdoruesit, passwordin, hostin.
- Çdo instancë e shton në listë dhe më pas i ben return funksionit dhe e rikthen këtë listë. Në kodin burim, skedari ka të implementuar dhe *keylogger* që regjistron tastet e shtypura nga përdoruesi. Përmes disa numrave ***int*** kontrollon gjendjen e keyloggerit duke e bërë enable.

```
                KsQeXu._screenLogger.ovF();
                num = 10;
            }
            if (num == 8)
            {
                KsQeXu._screenLogger = new ztL();
                num = 9;
            }
            if (num == 1)
            {
                XOhttClqJm.1GxB();
                num = 2;
            }
            if (num == 4)
            {
                if (!MXudRA.EnableKeylogger)
                {
                    goto IL_5D;
                }
                num = 5;
            }
            if (num == 6)
            {
                KsQeXu._keyLogger.wMxkzyio();
                num = 7;
            }
            if (num == 0)
            {
                num = 1;
            }
            if (num == 10)
            {
                break;
            }
            continue;
            IL_5D:
            if (MXudRA.EnableScreenLogger)
            {
```

Figura 19: Keylogger

```
// Token: 0x02000039 RID: 57
3 references
public class fN5j : vWH
{
    // Token: 0x060000F4 RID: 244 RVA: 0x000026ED File Offset: 0x000008ED
    1 reference
    public fN5j()
    {
        this.GrLKlf = "Outlook";
    }

    // Token: 0x17000024 RID: 36
    // (get) Token: 0x060000F5 RID: 245 RVA: 0x00002700 File Offset: 0x00000900
    // (set) Token: 0x060000F6 RID: 246 RVA: 0x00002708 File Offset: 0x00000908
    2 references
    public string GrLKlf { get; set; }

    // Token: 0x060000F7 RID: 247 RVA: 0x00010818 File Offset: 0x0000EA18
    1 reference
    public List<8WQvgbiWI1> Grab()
    {
        int num = 0;
        List<8WQvgbiWI1> list;
        do
        {
            if (num == 1)
            {
                list = new List<8WQvgbiWI1>();
                num = 2;
            }
            if (num == 0)
            {
                num = 1;
            }
        }
        while (num != 2);
        try
        {
            string text = "9375CFF0413111d3B88A00104B2A6676";
            RegistryKey[] array = new RegistryKey[]
            {
                Registry.CurrentUser.OpenSubKey("Software\\Microsoft\\Office\\11.0\\Outlook\\Profiles"),
```

Figura 20: Marrja e të dhënave nga Outlook

Në skedar duket dhe implementimi i një funksioni i cili shërben për dërgimin e një emaili. Gjithashtu në kodin burim shikohet dhe një string ***IpApi*** e shërben për të marrë adresën IP të përdoruesit. Informacionet që merren nga kompjuteri i infektuar nisen me email nga përdoruesi *electronics@xxxxx[.]com* (emaili i kompromentuar) drejt përdoruesit *successbright053@gmail[.]com* (emaili i aktorit keqdashës).

Analiza dinamike e Agent Tesla

Analiza dinamike konsiston në ekzekutimin e skedarit keqdashës për të parë se si sillet në një ambient sandbox të mbyllur.Gjatë ekzekutimit u evidentua se emaili që tentohet të dërgohet drejt përdoruesit është i suksesshëm. Në figurën e mëposhtme evidentohen të dhënat e kompjuterit të infektuar së bashku me adresën IP të tij që dërgohen nëpermjet ***smtpclient*** drejt aktorit keqdashës.

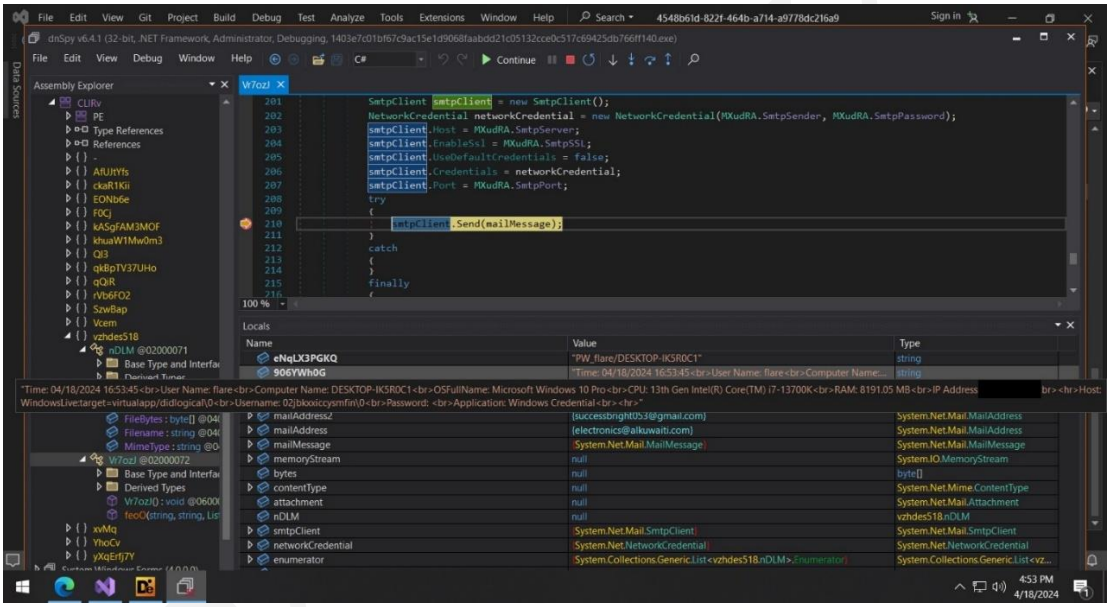

Figura 21: Dërgimi i emailit

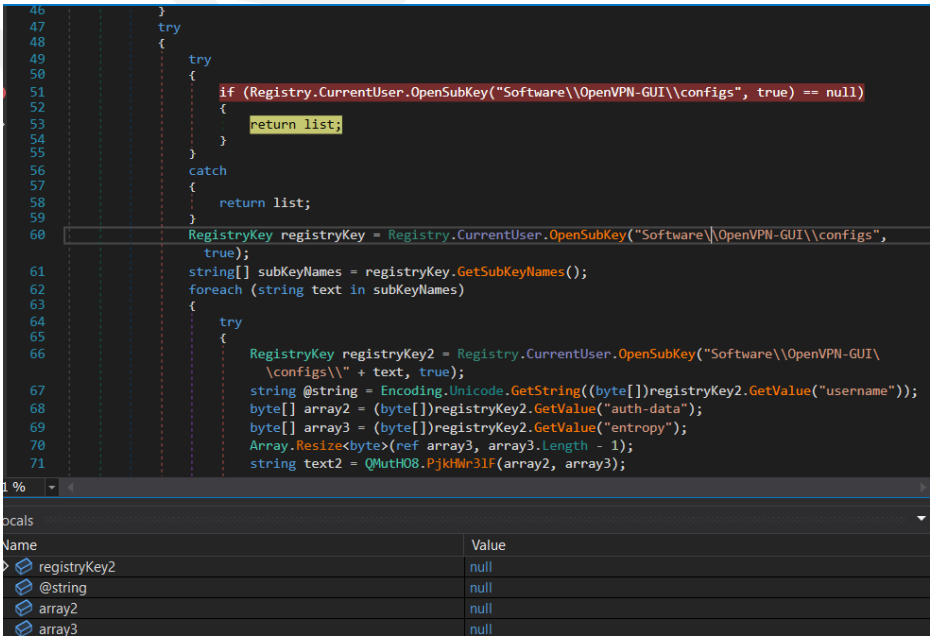

Figura 22: Ekzekutimi i funksionit Grab()

Indikatorët e kompromitetit

HASH-ET :
- *kugR.exe*
ef171f71804fe96bf375379c691e1f93b3fe38a3535b24f8f19d104e5eecf7aa
- *Tyrone.dll*
ead31b8d3cd588c72271e6671c16b7fd310099dbbccb61fe6f272cbc24b77ee8
- *Bank Advice.dll*
22a7e79314c5904ce3a5b0ef9f3ab7dfca2f487acbbb049414f1df7f8f95a3bf
- *CLIRv.exe*
1403E7C01BF67C9AC15E1D9068FAABDD21C05132CCE0C517C69425DB766FF140

Email:
successbright053@gmail[.]com

Teknikat e MITRE ATT&CK

Nr.	Taktika	Teknika
1	Initial Access (TA0001)	T1566: Phishing
		T1566.001: Spear phishing Attachment
2	Execution (TA0002)	T1053.005: Scheduled Task
		T1204.002: Malicious File
3	Persistence (TA0003)	T1547.001: Registry Run Keys/ Startup Folder
		T1053.005: Scheduled Task
4	Privilege Escalation (TA0004)	T1140: Deobfuscation
		T1055.012: Process Hollowing
		T1053.005: Scheduled Task
5	Defense Evasion (TA0005)	T1564.001: Hidden Files and Directories
		TA1562.001: Disable or Modify Tools
		T1055.012: Process Hollowing
		T1564.003: Hidden Window
6	Credential Access (TA0006)	T1555.003: Credentials from WebBrowser
		TA1552.001: Credentials in files
		TA1552.002: Credentials in registry
7	Discovery (TA0007)	T1087.001: Local Account
		T1057: Process Discovery
		T1082: System Information Discovery
6	Collection (TA0009)	T1560: Archive Collect Data

		T1217: Browser Information Discovery
		T1115: Clipboard Data
		T1005: Data from Local System
7	Exfiltration (TA0010)	T1048.003 – Exfiltration Over Unencrypted NON Command-and-Control Protocol
8	Command and Control (TA0011)	T1071.003: Mail Protocols

Rekomandime

AKCESK rekomandon infrastrukturat të zbatojnë praktikat më të mira të mëposhtme për të zvogëluar rrezikun ndaj sulmeve të këtyre aktorëve keqdashës:

- 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".