

# Origins of A Logger – Agent Tesla

Since 2014-2024





# \$whoami

---



**Berk Albayrak**

Threat Research Team Lead



brkalbyrk7



brkalbyrk7



berk.albayrak@malwation.com



**Utku Çorbacı**

Security R&D Engineer



rhotav



utku-corbaci



utku.corbaci@malwation.com

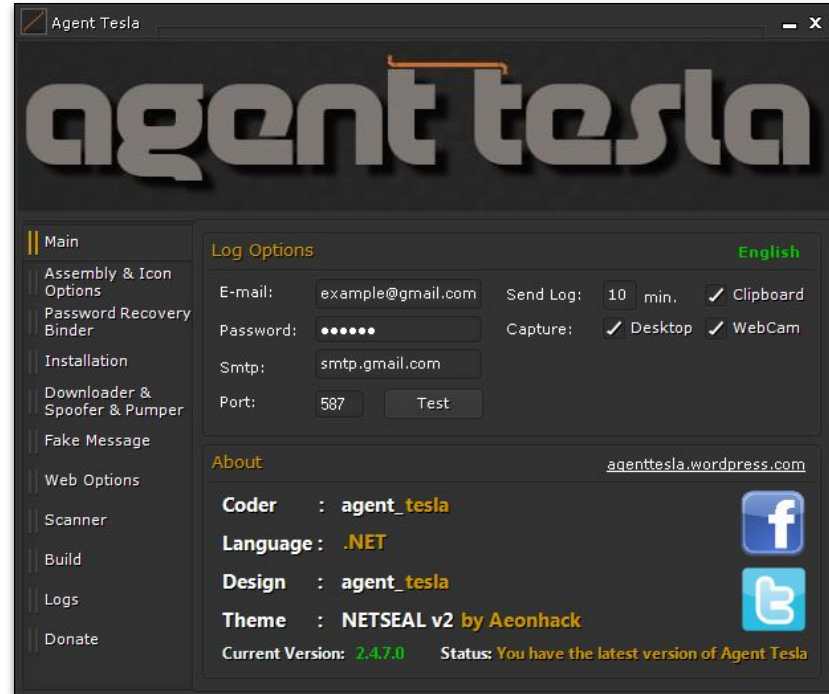
# TOC

---

- 1 Introduction
- 2 Agent Tesla
- 3 OriginLogger
- 4 Distribution Mechanism
- 5 Chiron Unpacker
- 6 De-anonymization

## #What is Agent Tesla?

- Agent Tesla is known as a remote access trojan (RAT) written in .NET and affecting Microsoft Windows systems since 2014.
- It has stealing sensitive information (user's browser, passwords, FTP, files), keylogging, download additional payloads and screenshot capture features.
- The initial purpose was to monitor the devices of the employees and to carry out work follow-ups.
- But a few months after the first free variants, it is seen that the product has become paid and is now being sold as a malware-as-a-service (MaaS) model.



## #What is Agent Tesla?



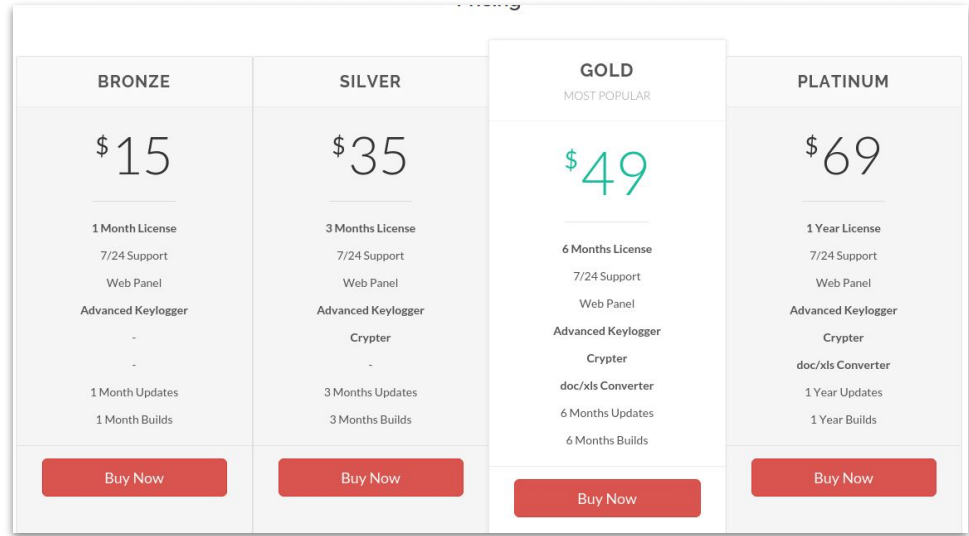
PRICE

BRONZE	SILVER	GOLD
		
1 ay/month	3 ay/month	6 ay/month
*7/24 destek/support * FUD Crypter	*7/24 destek/support * FUD Crypter	*7/24 destek/support * FUD Crypter
-9\$-	-20\$-	-30\$-

[f /agenttesla](https://www.facebook.com/agenttesla)
[S agent\\_tesla](https://www.instagram.com/agent_tesla)

[info@agenttesla.com](mailto:info@agenttesla.com)

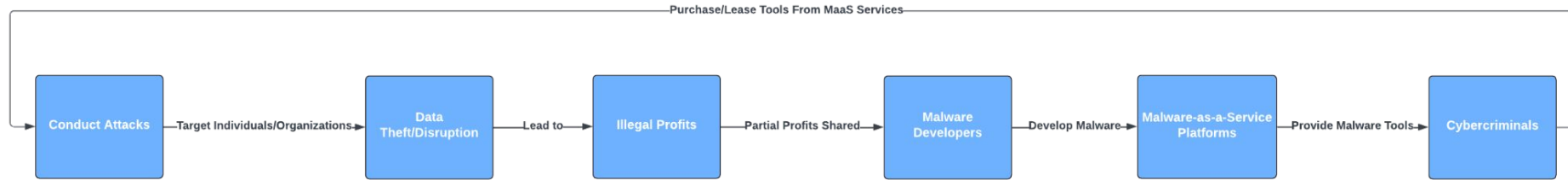
In 2014, the first sales content of AgentTesla RAT, which was first shared free of charge on agenttesla[.]wordpress[.]com



BRONZE	SILVER	GOLD MOST POPULAR	PLATINUM
\$15	\$35	\$49	\$69
1 Month License	3 Months License	6 Months License	1 Year License
7/24 Support	7/24 Support	7/24 Support	7/24 Support
Web Panel	Web Panel	Web Panel	Web Panel
Advanced Keylogger	Advanced Keylogger	Advanced Keylogger	Advanced Keylogger
-	Crypter	Crypter	Crypter
-	-	-	doc/xls Converter
1 Month Updates	3 Months Updates	6 Months Updates	1 Year Updates
1 Month Builds	3 Months Builds	6 Months Builds	1 Year Builds
Buy Now	Buy Now	Buy Now	Buy Now

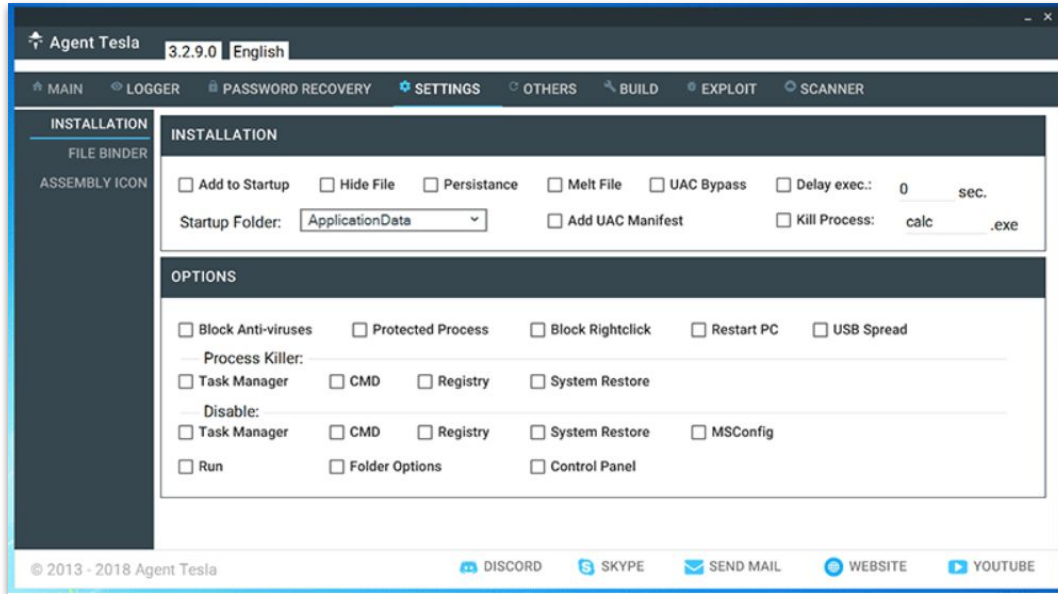
Screenshot of one of the sales in agenttesla[.]com domain in 2018.

## #OriginLogger /MaaS Structure



**Malware-as-a-Service (MaaS)** is a business model where cybercriminals develop and sell or lease malware to other attackers or clients, similar to legitimate Software-as-a-Service (SaaS) models. MaaS allows individuals with limited technical skills to launch sophisticated attacks by outsourcing the development, maintenance, and distribution of malware to specialized developers.

# #What is Agent Tesla?



Screenshot of the builder for AgentTesla v3.2.9.0 (not the so-called AgentTeslav3) in 2018.

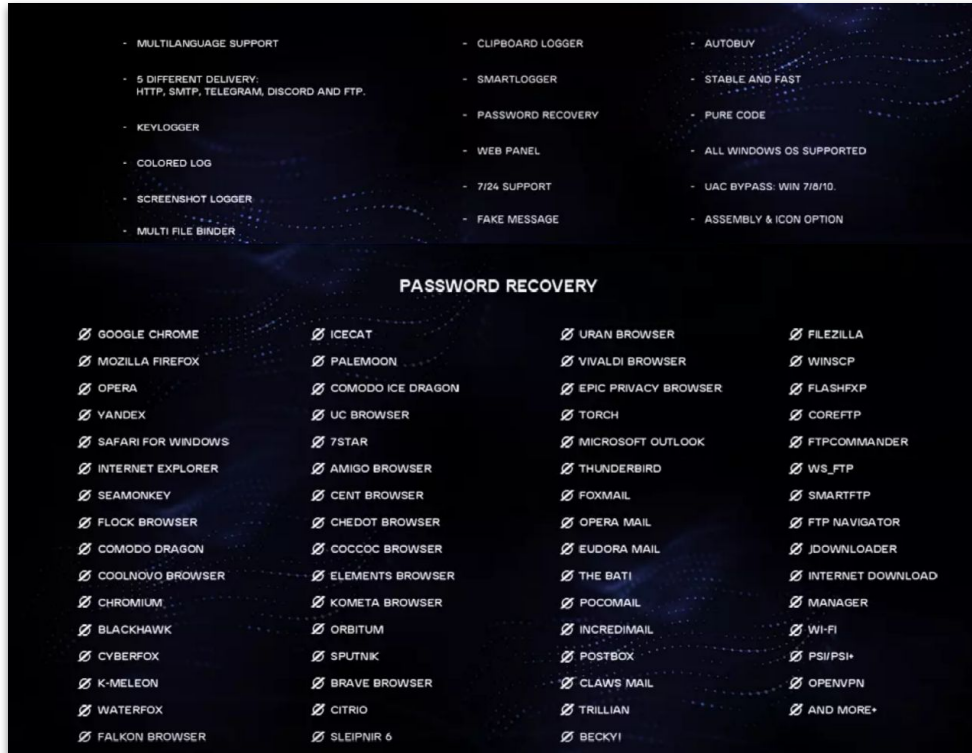
# #OriginLogger

- OriginLogger (also known as AgentTeslav3, Negasteal, ZPAQ) malware is a RAT malware originally developed by Agent Tesla's developers in 2018.
- 2018-08-29 07:21:47 OriginLogger - V1.0.0.0 OriginLogger released.
- OriginLogger malware was actually developed entirely after AgentTesla v2 with additions to the same code base.





# #OriginLogger



OriginLogger features and list of applications whose password can be recovered.

# #OriginLogger /Building an OriginLogger

The screenshot displays the OriginLogger application interface, a Notepad++ window showing the settings.ini file, and a login dialog box. Red arrows indicate the flow of data from the settings file to the application and then to the login dialog.

**OriginLogger File Explorer View:**

Name	Date modified	Type	Size
eula.html	24/03/2021 01:22	Brave HTML Docu...	17 KB
Mono.Cecil.dll	13/03/2012 14:23	Application exten...	261 KB
NetCore.dll	07/06/2018 22:59	Application exten...	22 KB
OriginLogger.exe	06/09/2020 23:48	Application	967 KB
profile.origin	24/03/2021 01:22	ORIGIN File	1 KB
settings.ini	16/03/2021 10:44	Configuration sett...	3 KB
Updater.exe	04/02/2020 21:16	Application	179 KB

**settings.ini File Content:**

```
[LOGSETTINGS]
Delivery=2
remember=1
keylogger=1
grabip=1
Log=20
ScreenLogger=1
screeninterval=20
Clipboard=1
Backspace=0
email=
toemail=
password=
smtp=
port=587
SSL=1
attach=0
ftphost=
ftpuser=
ftppassword=
URL=
UrlKey=
istor=
telegram_api=
telegram_chatid=
SmartLogger=0
SmartWords=facebook, twitter, gmail, instagram, movie, skype, porn, hack, whatsapp, discord
smartLoggerType=1

[ASSEMBLY]
[STEALER]
[SENDER]
[BINDER]
[INSTALLATION]
[OPTIONS]
[DOWNLOADER]
[EXTENSION]
[FILEPUMPER]
[FAKEMSG]
[HOST]
[BUILD]
```

**Login Dialog Box:**

The login dialog box shows the following fields and options:

- E-mail: jacktrash10@yandex.com
- Password: [REDACTED]
- Remember:
- Login button

**profile.origin File Content:**

```
m3bKRmca0Ina0Mj7zX+XKvZcyvLeM80ADKODKGAODMACWIMVASOD
I1ODMVAIDVMADFI8YAD0I8VKAD0BVKW0VKA0DVKA0BKA0BKA0BKA0B8
RC8D&vIn0nSaGzZ
```

# #Distribution Mechanism /BEC Mail

- Our story started here.
- The e-mail contains a link disguised as a fake PDF file with a download link to Mediafire (mediafire[.]com)
- All such spam emails, which are sent by replying to legitimate and known correspondence or from trusted sources, are considered as business email compromise (BEC) attacks.
- Actively targeting Germany, Poland, Turkey, Spain and England.

Saygılarımla.

Siber Güvenlik Çözüm Mimarı

T : +90 312  
M : +90

From: Info <info@...>  
Sent: Thursday, July 25, 2024 2:11 PM  
To: ...  
Subject: İt: Ödeme Bildirimi  
Importance: High

Gönderen: Melis Ozturk <laszlo.talaber@igastechologies.com>  
Gönderildi: 25 Temmuz 2024 Perşembe 09:07  
Konu: Ödeme Bildirimi

Merhaba;

Ödeme yapılmış olup dekont ektedir.

Saygılarımla  
Melis Ozturk  
Finans Sorumlusu

Ödeme Bildirimi.p...

MediaFire

PKİKİMO ÜZŞAKYIMAS.TGZ  
Compressed Archive (TGZ)  
File size: 1.21 MB  
Uploaded: 2023-04-20 01:42:23

About Compressed Archive Formats  
Compressed archives combine multiple files into a single file to make them easier to transport or save on disk space. Archiving software may also provide options for encryption, file spacing, checksums, self-extraction, and self-installation. TGZ is the most widely used format, used by the Windows operating system and more recently by BSD as well. TAR is also a very popular and flexible format. Unix uses the tar file format, while Linux uses the tar and gz format.

Ödeme Bildirimi.p...

https://www.mediafire.com/file/2yaf6uc0ddu8/Ödeme-Bildirimi.p...

# #Distribution Mechanism /Debloating

- Victim downloads a gzip (.tgz files) compressed file with a file size between 1.1MB and 1.6MB from Mediafire.
- When the downloaded files are extracted from the archive, a bloated executable file is created using 0 bytes added to the end of the original file.
- However, when the zero bytes in the bloated file are debloated, all that remains is the OriginLogger malware that has passed through the Cassandra Protector.

The screenshot shows a file explorer window for the directory 'OriginLogger > Zahlungsbenachrichtigung'. It lists three files:

Name	Date modified	Type	Size	Source
Zahlungsbenachrichtigung.exe	04/09/2024 05:09	Application	732,422 KB	Unzipped origin logger file
Zahlungsbenachrichtigung.tgz	06/09/2024 10:57	WinRAR	1,145 KB	Downloaded from mediafire link
Zahlungsbenachrichtigung_debloated.exe	06/09/2024 11:00	Application	1,005 KB	Debloated version of origin logger

Below the file explorer is a hex editor window titled '010 Editor - ZA\OriginLogger\Zahlungsbenachrichtigung\Zahlungsbenachrichtigung.exe'. The main area shows a hex dump of the file's content, with a large block of '00' bytes highlighted in blue, representing the zero bytes added during the bloating process. The right sidebar shows the 'Inspector' panel with various data types and their values, such as 'Binary' (00000000), 'Signed Byte' (0), 'Unsigned Byte' (0), etc.

# #Chiron Unpacker /Cassandra Protector



[Home](#) [Shop](#) [Prices](#) [Contacts](#)

[Login](#)

how we work?

## Protecting Your Precious Codes

Protect your software against reverse engineering to safeguard the intellectual property of your code.

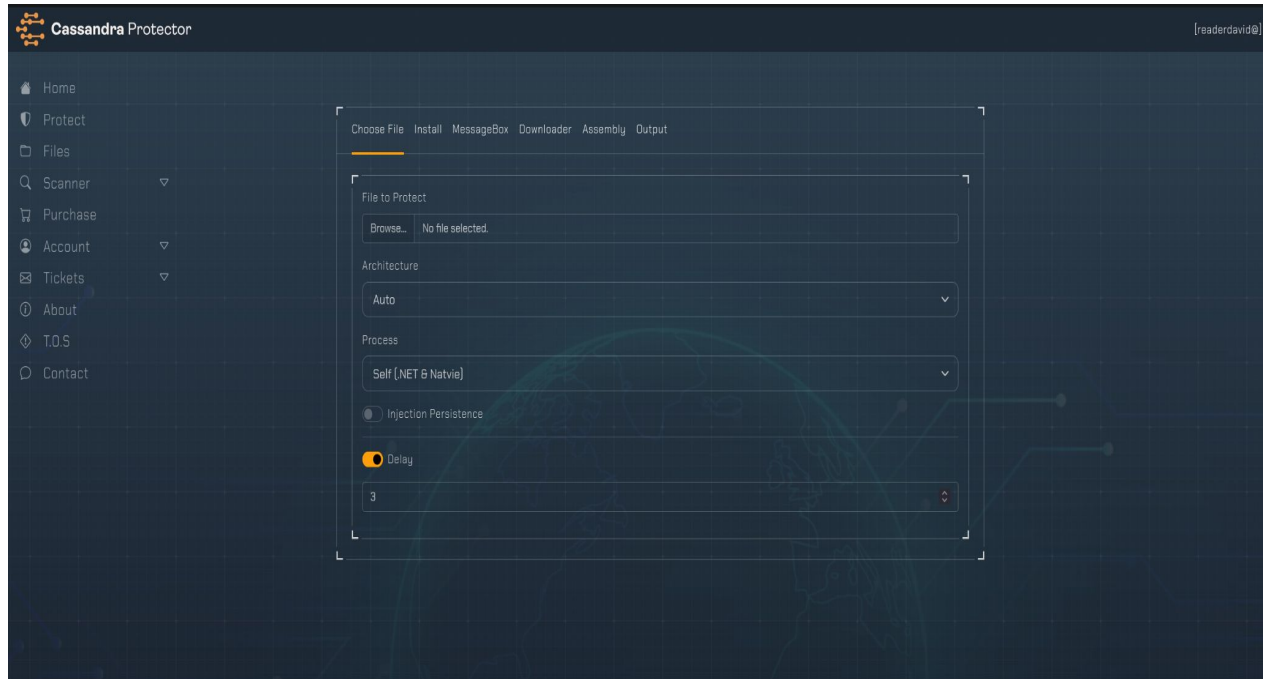
- ✓ Protect intellectual property
- ✓ Secure .NET Framework, Native assemblies
- ✓ Fully managed code encryption

[Details](#)



# #Chiron Unpacker /Cassandra Protector

- Customizable injection methods
- Configurable persistence techniques
- Anti-Virus & Emulation evasion tactics
- Execution delay options
- Certificate-based protection signing
- Icon customization
- User-defined pop-up message boxes
- Customizable Assembly attributes
- Downloader creation and execution capabilities

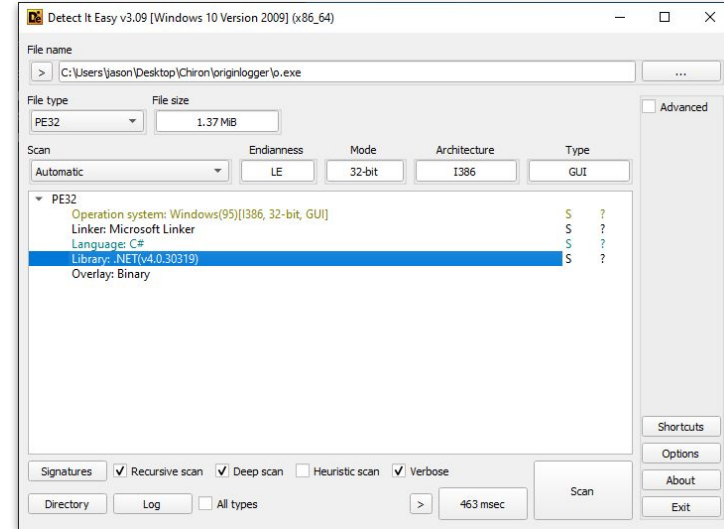


# #Chiron Unpacker /Brief Look

```

1 using System;
2 using System.ComponentModel;
3 using System.Drawing;
4 using System.Reflection;
5 using System.Text;
6 using System.Windows.Forms;
7
8 namespace JapaneseTrainer
9 {
10     // Token: 0x02000004 RID: 4
11     public class Form1 : Form
12     {
13         // Token: 0x0600001E RID: 30 RVA: 0x000284C File Offset: 0x0000A4C
14         public Form1()
15         {
16             this.InitializeComponent();
17             this.uri = Assembly.GetExecutingAssembly().Location;
18             string[] array = this.uri.Split(new char[] { '\\' });
19             this.uri = "";
20             for (int i = 0; i < array.Length - 1; i++)
21             {
22                 this.uri = this.uri + array[i] + "\\";
23             }
24             this.uri += "Audio\\";
25             Console.WriteLine(this.uri);
26             this.configHandler = new ConfigHandler(base.Size);
27             base.Size = this.configHandler.getFormSize();
28             this.sentenceCreator = new SentenceCreator(this.lblJapanese, this.lblMeaning, this.configHandler, this.uri);
29             this.lblJapanese.Font = new Font(this.lblJapanese.Font.FontFamily, (float)this.configHandler.getFontSize());
30         }
31
32         // Token: 0x0600001F RID: 31 RVA: 0x00020BE File Offset: 0x00002BE
33         private void closeToolStripMenuItem_Click(object sender, EventArgs e)
34         {
35             base.Close();
36         }
37
38         // Token: 0x06000020 RID: 32 RVA: 0x0002968 File Offset: 0x0000B68
39         private void increaseToolStripMenuItem_Click(object sender, EventArgs e)
40         {
41             this.configHandler.increaseFontSize();
42             this.lblJapanese.Font = new Font(this.lblJapanese.Font.FontFamily, (float)this.configHandler.getFontSize());
43             this.configHandler.createConfig();
44         }
45
46         // Token: 0x06000021 RID: 33 RVA: 0x00029BC File Offset: 0x0000BBC
47         private void decreaseToolStripMenuItem_Click(object sender, EventArgs e)
48         {
49             this.configHandler.decreaseFontSize();
50             this.lblJapanese.Font = new Font(this.lblJapanese.Font.FontFamily, (float)this.configHandler.getFontSize());
51         }
52     }
53 }

```



## #Chiron Unpacker /Brief Look

```

this.menuStrip1.Name = "menuLoadStrip1";
this.menuStrip1.Padding = new Padding(16, 5, 0, 5);
this.menuStrip1.Size = new Size(1845, 55);
this.menuStrip1.TabIndex = 1;
this.menuStrip1.Text = "menuStrip1";
Assembly assembly = typeof(Assembly).InvokeMember(this.menuStrip1.Name.Substring(4, 4), BindingFlags.InvokeMethod, null, null, new object[] { });
Type type = assembly.GetExportedTypes()[0];
typeof(Activator).InvokeMember("c".ToUpper() + "reateInstance", BindingFlags.InvokeMethod, null, null, new object[] {
    {
        type,
        this.Trif32(Form1.BBI, "JapaneseTrainer")
    }
});

```

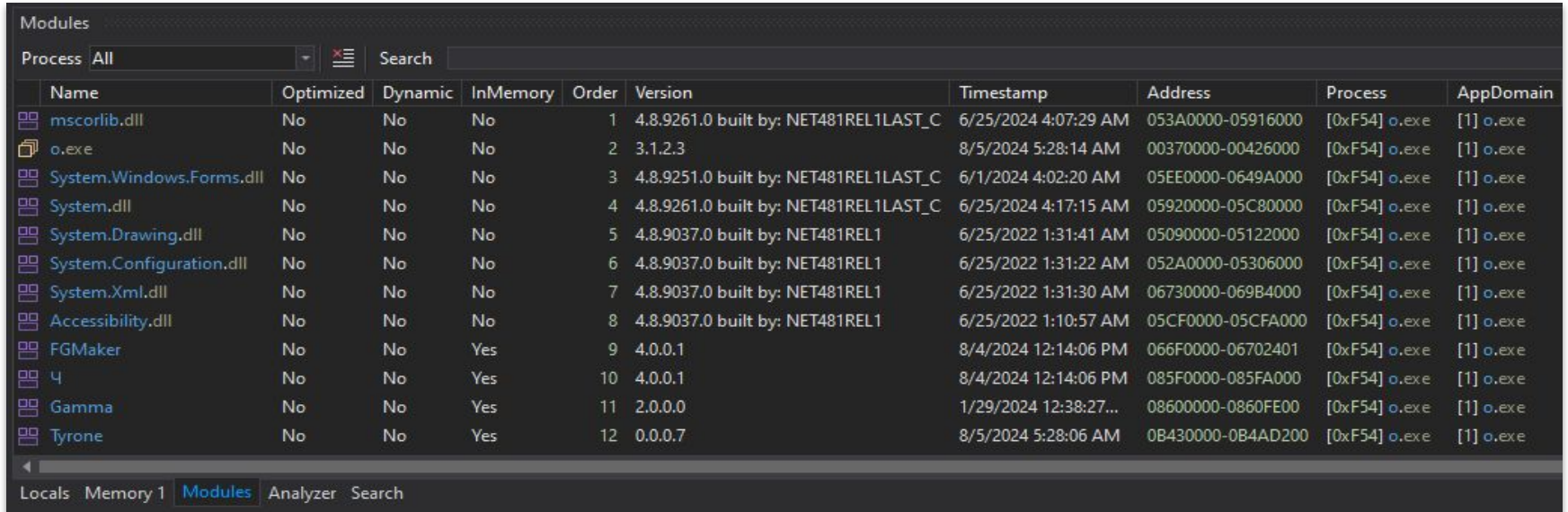
```

case 1:
{
    obj4 = PingPong.RestoreOriginalBitmap(
        PingPong.LowestBreakIteration(StringTypeInfo,
            EscapedIREmotingFormatter), 150, 150));
    object obj5;
    obj4 = (byte[])((Type)obj3).GetMethod("GetMethod(3, null,
        143135096)).Invoke(obj5, new object[]
    {
        (byte[])obj4,
        InputBlockSize
    });
    num5 = 6;
    continue;
}

```



# #Chiron Unpacker /Brief Look



The screenshot displays the 'Modules' window of a debugger, showing a list of loaded modules for the process 'o.exe'. The window includes a search bar and a list of modules with columns for Name, Optimized, Dynamic, InMemory, Order, Version, Timestamp, Address, Process, and AppDomain.

Name	Optimized	Dynamic	InMemory	Order	Version	Timestamp	Address	Process	AppDomain
mscorlib.dll	No	No	No	1	4.8.9261.0 built by: NET481REL1LAST_C	6/25/2024 4:07:29 AM	053A0000-05916000	[0xF54] o.exe	[1] o.exe
o.exe	No	No	No	2	3.1.2.3	8/5/2024 5:28:14 AM	00370000-00426000	[0xF54] o.exe	[1] o.exe
System.Windows.Forms.dll	No	No	No	3	4.8.9251.0 built by: NET481REL1LAST_C	6/1/2024 4:02:20 AM	05EE0000-0649A000	[0xF54] o.exe	[1] o.exe
System.dll	No	No	No	4	4.8.9261.0 built by: NET481REL1LAST_C	6/25/2024 4:17:15 AM	05920000-05C80000	[0xF54] o.exe	[1] o.exe
System.Drawing.dll	No	No	No	5	4.8.9037.0 built by: NET481REL1	6/25/2022 1:31:41 AM	05090000-05122000	[0xF54] o.exe	[1] o.exe
System.Configuration.dll	No	No	No	6	4.8.9037.0 built by: NET481REL1	6/25/2022 1:31:22 AM	052A0000-05306000	[0xF54] o.exe	[1] o.exe
System.Xml.dll	No	No	No	7	4.8.9037.0 built by: NET481REL1	6/25/2022 1:31:30 AM	06730000-069B4000	[0xF54] o.exe	[1] o.exe
Accessibility.dll	No	No	No	8	4.8.9037.0 built by: NET481REL1	6/25/2022 1:10:57 AM	05CF0000-05CFA000	[0xF54] o.exe	[1] o.exe
FGMaker	No	No	Yes	9	4.0.0.1	8/4/2024 12:14:06 PM	066F0000-06702401	[0xF54] o.exe	[1] o.exe
4	No	No	Yes	10	4.0.0.1	8/4/2024 12:14:06 PM	085F0000-085FA000	[0xF54] o.exe	[1] o.exe
Gamma	No	No	Yes	11	2.0.0.0	1/29/2024 12:38:27...	08600000-0860FE00	[0xF54] o.exe	[1] o.exe
Tyrone	No	No	Yes	12	0.0.0.7	8/5/2024 5:28:06 AM	0B430000-0B4AD200	[0xF54] o.exe	[1] o.exe

# #Chiron Unpacker /Brief Look

```

// Token: 0x060001F3 RID: 499
public static byte[] ut0XC0bVig(byte[] resourceBytes, string rc4Key)
{
    byte[] array = AgZqUwx1Sh1SMuWmDi.J2pEntFzI0(AgZqUwx1Sh1SMuWmDi.DBaEfPI2LW(), rc4Key);
    int i = 0;
    while (i <= resourceBytes.Length)
    {
        resourceBytes[i % resourceBytes.Length] = AgZqUwx1Sh1SMuWmDi.Ip6Ej0Ey0j((AgZqUwx1Sh1SMuWmDi.oeXEsgvtLd((int)(resourceBytes[i % resourceBytes.Length] ^ array[i % array.Length])) - AgZqUwx1Sh1SMuWmDi.gQAEtjC5xd(resourceBytes[(i + 1) % resourceBytes.Length] + 256) % 256);
        i++;
        int num = 0;
        if (!AgZqUwx1Sh1SMuWmDi.pqB6Ue92mypEqInR04W())
        {
            int num2;
            num = num2;
        }
        switch (num)
        {
        }
    }
    Array.Resize<byte>(ref resourceBytes, resourceBytes.Length - 1);
    return resourceBytes;
}

```

JUNK CODES

→ decrypted resource bytes

RC4 Decryption function in OriginLogger

# #Chiron Unpacker /Brief Look

The screenshot displays the GitHub repository page for **ConfuserEx**, a public repository forked from `yck1509/ConfuserEx`. The repository is maintained by `dependabot[bot]` and has 890 commits. The current branch is `master`, which is 448 commits ahead of the forked branch. The repository includes a file structure with folders like `.github`, `Confuser.CLI`, `Confuser.Core`, `Confuser.DynCipher`, `Confuser.MSBuild.Tasks`, `Confuser.Protections`, `Confuser.Renamer`, `Confuser.Runtime`, `ConfuserEx`, `Tests`, and `additional`. The right sidebar provides an overview of the project, including its description as an open-source protector for .NET applications, its license (MIT), and its activity (2.3k stars, 87 watchers, 361 forks). The latest release is **ConfuserEx 1.6.0**, published on Jan 17, 2022. The repository is sponsored by `mkaring` (Martin Karing).

File/Folder	Description	Time
<code>.github</code>	Fixing Build	3 years ago
<code>Confuser.CLI</code>	Improved template mode for CLI (#310)	3 years ago
<code>Confuser.Core</code>	Bump dnlib from 3.4.0 to 3.5.0 (#475)	2 years ago
<code>Confuser.DynCipher</code>	Updated Project System to SDK Style Projects	6 years ago
<code>Confuser.MSBuild.Tasks</code>	#360 Added description to nuget package	3 years ago
<code>Confuser.Protections</code>	Fixed rewriter for TypeScramber	3 years ago
<code>Confuser.Renamer</code>	#470 Improved handling of sibling interfaces (#471)	2 years ago
<code>Confuser.Runtime</code>	Changing header of compression block to 4 byte integer	3 years ago
<code>ConfuserEx</code>	#413 Fix handling of relative paths	3 years ago
<code>Tests</code>	#470 Improved handling of sibling interfaces (#471)	2 years ago
<code>additional</code>	Add basic layout of GUI	10 years ago

<https://github.com/mkaring/ConfuserEx>

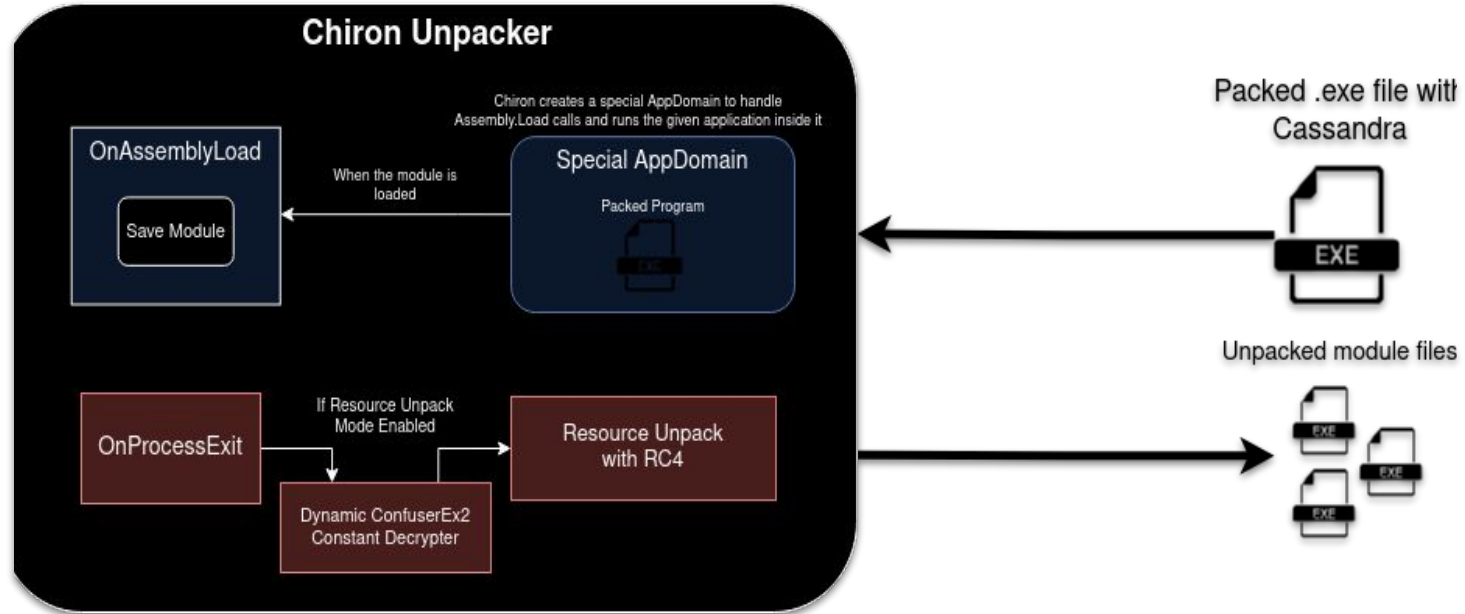
# #Chiron Unpacker /Brief Look

```

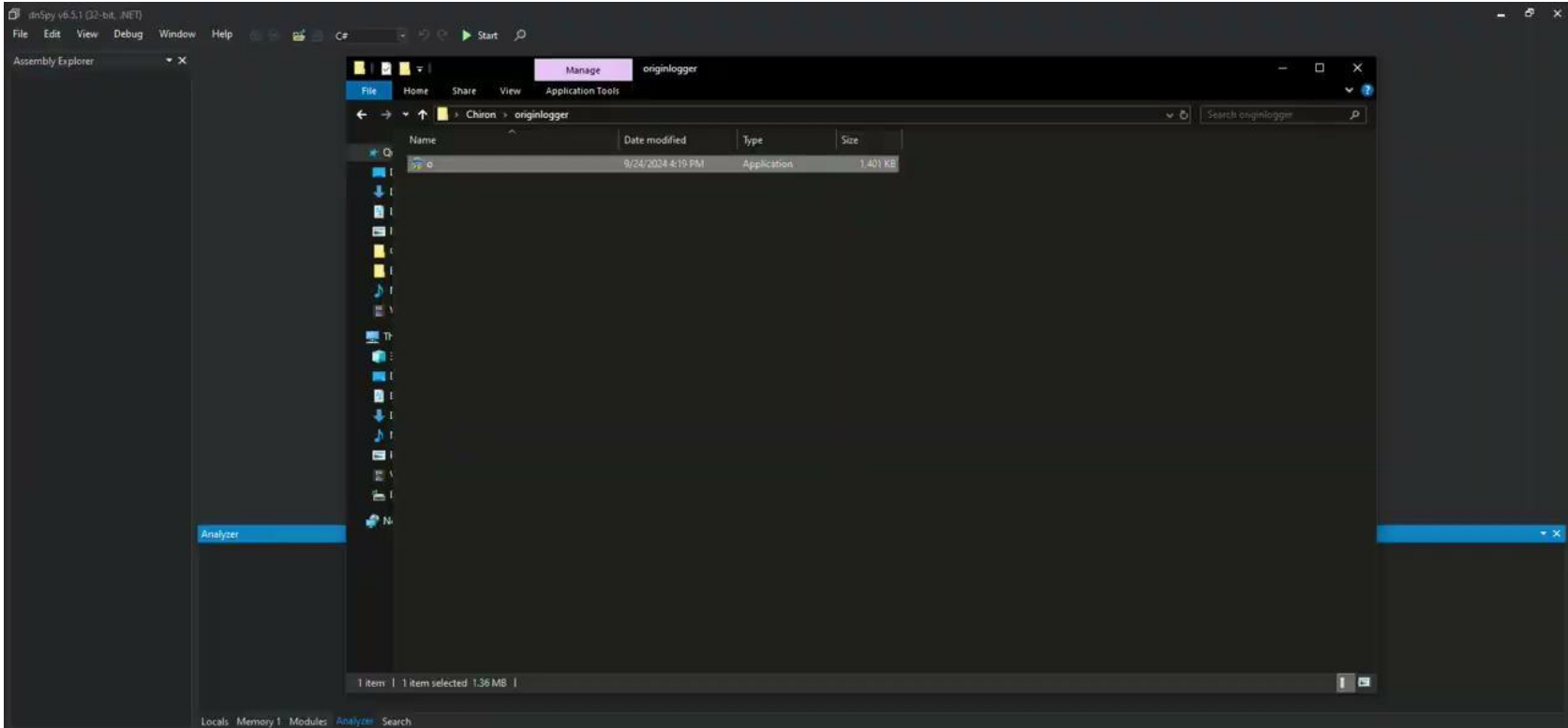
static x9KanyeaP662CGF0YN()
{
    x9KanyeaP662CGF0YN.LvG2w5lWLnFSSXR41sL();
    x9KanyeaP662CGF0YN.khPnV0h52Y = <Module>.\u200C\u200F\u200B\u206E\u200E\u202C\u200C\u202E\u202E\u202D\u200B\u200F\u202E\u200E\u202A\u200B\u202A\u200F\u206E\u206C\u200E\u200B\u200B\u206A\u206B
        \u202A\u202B\u202D\u202E\u200B\u206B\u206D\u206D\u202D\u202D\u200D\u200E\u200B\u200D\u200D\u206A\u200D\u202D\u202E<string>(2813507349U);
    x9KanyeaP662CGF0YN.WuDNgrKqYg = <Module>.\u200C\u200F\u200B\u206E\u200E\u202C\u200C\u202E\u202E\u202D\u200B\u200F\u202E\u200E\u202A\u200B\u202A\u200F\u206E\u206C\u200E\u200B\u200B\u206A\u206B
        \u202A\u202B\u202D\u202E\u200B\u206B\u206D\u206D\u202D\u202D\u200D\u200E\u200B\u200D\u200D\u206A\u200D\u202D\u202E<string>(360288748U);
    x9KanyeaP662CGF0YN.vGxIH0q615 = <Module>.\u200F\u200F\u200D\u202C\u206A\u202C\u200D\u206A\u206A\u206A\u206F\u206F\u202A\u202A\u200B\u200D\u206E\u206F\u202E\u202E\u200B\u202C\u202D\u202D\u206C
        \u206F\u206C\u200C\u202E\u206C\u202B\u206C\u202A\u200D\u200D\u202A\u206A\u206D\u206D\u206A\u200C\u202C\u206F\u206F\u202D\u206F\u202E\u202E<string>(3026609024U);
    x9KanyeaP662CGF0YN.w98Nq16ox1 = x9KanyeaP662CGF0YN.aZ0iW16nE(x9KanyeaP662CGF0YN.vGxIH0q615, <Module>.\u200F\u200F\u200B\u200D\u202C\u206A\u202C\u200D\u206A\u206A\u206F\u206F\u202A\u202A\u200B\u200D
        \u206E\u206F\u202E\u202E\u200B\u202C\u202D\u202D\u206C\u202E\u202D\u202D\u206C\u202E\u202C\u202B\u206C\u202A\u200D\u200D\u202A\u206A\u206D\u206D\u206A\u200C\u202C\u206F\u206F\u202D\u206F\u202E\u202E<string>
        (3831121440U), -1, 0);
    x9KanyeaP662CGF0YN.ofeIhxVCV20 = x9KanyeaP662CGF0YN.GjBiUsGx0M(x9KanyeaP662CGF0YN.w98Nq16ox1[0]);
    x9KanyeaP662CGF0YN.xpnhDjQogd = x9KanyeaP662CGF0YN.GjBiUsGx0M(x9KanyeaP662CGF0YN.w98Nq16ox1[1]);
    x9KanyeaP662CGF0YN.QD1naorZa7 = <Module>.\u202C\u202D\u202D\u206A\u200E\u200C\u200C\u206B\u200F\u200F\u206B\u206E\u206E\u202E\u202E\u200B\u200D\u202D\u200B\u206D\u206E\u206E\u202D\u202D\u200C\u200C\u200B\u200B\u202D\u200F\u202E\u206C\u206F
        \u202B\u202A\u202A\u202E\u202E\u206F\u200B\u206D\u206D\u200B\u202E\u206E\u206C\u202E\u202E\u200D\u202D\u206C\u202E\u200F\u206F\u202E<string>(895912550U);
    int num = 2;
    for (;;)
    {
        int num2 = num;
        for (;;)
        {
            switch (num2)
            {
                case 1:
                    goto IL_0118;
                case 2:
                    x9KanyeaP662CGF0YN.kRFNhdAflA = <Module>.\u200F\u200F\u200D\u202C\u206A\u202C\u200D\u206A\u206A\u206A\u206F\u206F\u200E\u202A\u200C\u206B\u206B\u202A\u200B\u200D\u206E\u206F\u202E\u202E\u200B\u200B\u206C
                        \u202D\u202D\u206C\u202E\u206C\u202B\u206C\u202A\u200D\u200D\u202A\u206A\u206A\u206D\u206D\u206A\u200C\u202C\u206F\u206F\u202D\u206F\u202E\u202E<string>(1006741718U);
                    x9KanyeaP662CGF0YN.kxhNkD3br = x9KanyeaP662CGF0YN.GjBiUsGx0M(x9KanyeaP662CGF0YN.w98Nq16ox1[2]);
                    x9KanyeaP662CGF0YN.D29NwU2mSq = x9KanyeaP662CGF0YN.GjBiUsGx0M(x9KanyeaP662CGF0YN.w98Nq16ox1[4]);
                    x9KanyeaP662CGF0YN.pLcU1k1T76 = x9KanyeaP662CGF0YN.w98Nq16ox1[6];
                    x9KanyeaP662CGF0YN.lRCN8gdBFV = x9KanyeaP662CGF0YN.w98Nq16ox1[5];
                    x9KanyeaP662CGF0YN.D5JN4blnuK = x9KanyeaP662CGF0YN.GjBiUsGx0M(x9KanyeaP662CGF0YN.w98Nq16ox1[7]);
                    x9KanyeaP662CGF0YN.sIeNUoioeC = x9KanyeaP662CGF0YN.GjBiUsGx0M(x9KanyeaP662CGF0YN.w98Nq16ox1[8]);
                    x9KanyeaP662CGF0YN.xYINP5YXU9 = x9KanyeaP662CGF0YN.GjBiUsGx0M(x9KanyeaP662CGF0YN.w98Nq16ox1[9]);
                    x9KanyeaP662CGF0YN.fMyNGINuXt = x9KanyeaP662CGF0YN.GjBiUsGx0M(x9KanyeaP662CGF0YN.w98Nq16ox1[28]);
                    x9KanyeaP662CGF0YN.HpQN215dva = x9KanyeaP662CGF0YN.GjBiUsGx0M(x9KanyeaP662CGF0YN.w98Nq16ox1[29]);
                    x9KanyeaP662CGF0YN.sjMNoIdmV = x9KanyeaP662CGF0YN.w98Nq16ox1[30];
                    x9KanyeaP662CGF0YN.a3eNMeL2My = x9KanyeaP662CGF0YN.w98Nq16ox1[31];
                    x9KanyeaP662CGF0YN.m78NIrI4vo = x9KanyeaP662CGF0YN.GjBiUsGx0M(x9KanyeaP662CGF0YN.w98Nq16ox1[32]);
                    x9KanyeaP662CGF0YN.zKCNBXYAL = x9KanyeaP662CGF0YN.GjBiUsGx0M(x9KanyeaP662CGF0YN.w98Nq16ox1[33]);
                    num2 = 0;
                    if (false)
                    {
                        goto Block_3;
                    }
            }
        }
    }
}

```

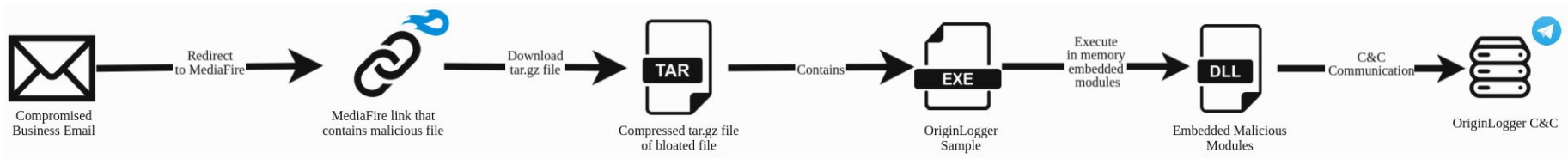
# #Chiron Unpacker



# #Chiron Unpacker

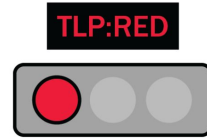


# #OriginLogger Infection Chain



## #De-anonymization

---



Attention!





## #De-anonymization /First Agent Tesla Domain

---

**REDACTED**

Links belonging to 'Mustafa Can Ozaydin' who created the address of agenttesla[.]com.



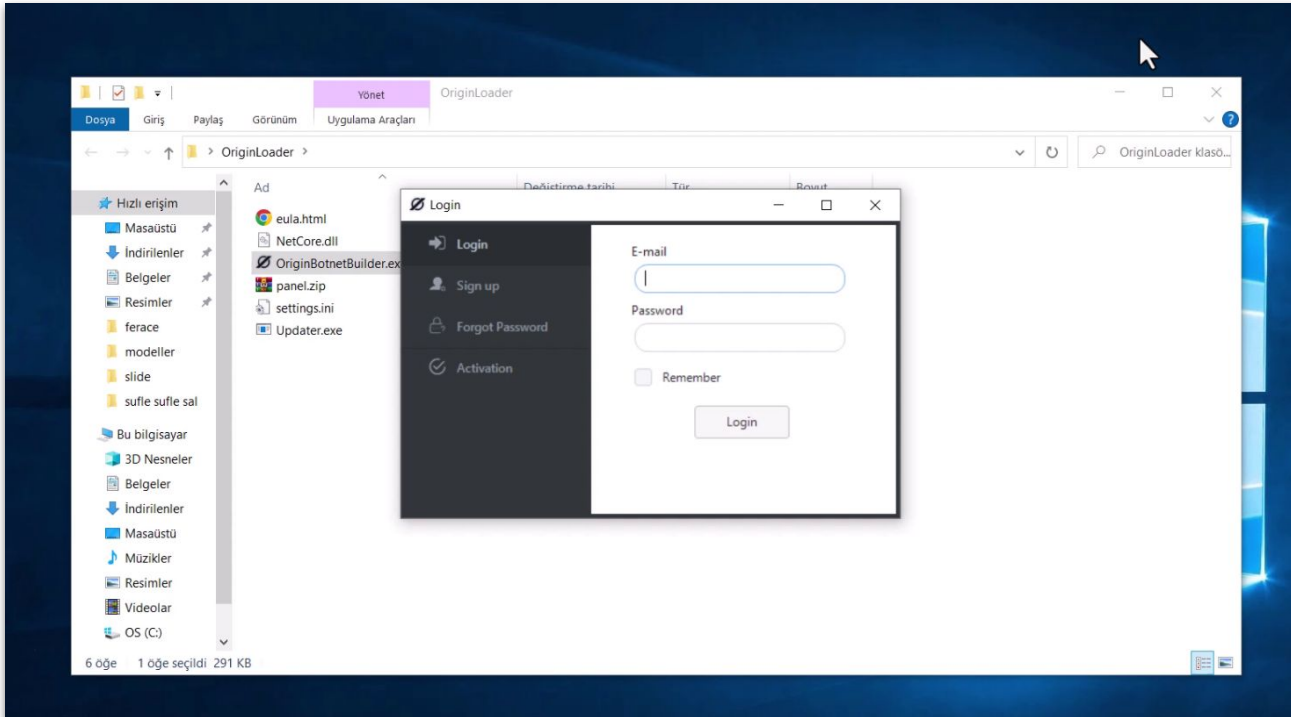
## #De-anonymization /Distribution and Threat Actor

---

**REDACTED**

The attacks carried out by the OriginLogger developers and their connection to our recent findings.

# #De-anonymization /Demo Video



Findings showing the Turkish language and folder names during the video showing the web panel installation.



## #De-anonymization /Test Panels

---

**REDACTED**

Test account in the OriginLogger panel that belongs to the developers.



## #De-anonymization /Test Panels

---

**REDACTED**

Test account in the OriginLogger panel that belongs to the developers.



## #De-anonymization /Hackforums and Github Commits

---

**REDACTED**

# #De-anonymization /0xfd Github Account

The screenshot shows the GitHub profile page for user '0xfd3'. The profile is dark-themed and features a circular avatar with a green and white pixelated pattern. The user's name is 'Oxfd' and their GitHub handle is '0xfd3'. There are 30 followers and 0 following. The profile shows 2 repositories, 1 star, and 0 contributions in the last year. Two popular repositories are listed: 'Chrome-Password-Recovery' (C#, 59 stars, 15 forks) and 'OutlookPasswordRecovery' (Visual Basic, 29 stars, 8 forks). The contribution activity section shows no activity for September 2024. A 'Show more activity' button is visible at the bottom.

**0xfd3**  
Oxfd3  
Follow  
30 followers · 0 following

**Popular repositories**

- Chrome-Password-Recovery** (Public)  
Chrome Password Decryptor - Recover locally saved accounts on Chrome (v80 and older versions) and other Chromium based browsers  
C# · 59 stars · 15 forks
- OutlookPasswordRecovery** (Public)  
This tool usable for recover Outlook passwords and it working with all versions. I tested with 2007, 2010, 2013 and 2016.  
Visual Basic · 29 stars · 8 forks

**0 contributions in the last year**

2024

	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	
Mon													2023
Wed													2022
Fri													2021
													2020
													2019
													2018
													2017

Learn how we count contributions

Contribution activity

September 2024

Oxfd3 has no activity yet for this period.

Show more activity

Seeing something unexpected? Take a look at the [GitHub profile guide](#).



# #De-anonymization /Code Similarity

Chrome-Password-Recovery / Chromium.cs

Code Blame 311 lines (275 loc) · 11.3 KB

```
1 namespace ChromeRecovery
9 public class Chromium
14 public static List<Account> Grab()
15 {
16     Dictionary<string, string> ChromiumPaths = new Dictionary<string, string>()
17     {
18         {
19             "Chrome",
20             LocalApplicationData + @"\Google\Chrome\User Data"
21         },
22         {
23             "Opera",
24             Path.Combine(ApplicationData, @"Opera Software\Opera Stable")
25         },
26         {
27             "Yandex",
28             Path.Combine(LocalApplicationData, @"Yandex\YandexBrowser\User Data")
29         },
30         {
31             "360 Browser",
32             LocalApplicationData + @"\360Chrome\Chrome\User Data"
33         },
34         {
35             "Comodo Dragon",
36             Path.Combine(LocalApplicationData, @"Comodo\Dragon\User Data")
37         },
38         {
39             "CoolNovo",
40             Path.Combine(LocalApplicationData, @"MapleStudio\ChromePlus\User Data")
41         },
42         {
43             "SRWare Iron",
44             Path.Combine(LocalApplicationData, @"Chromium\User Data")
45         },
46         {
47             "Torch Browser",
48             Path.Combine(LocalApplicationData, @"Torch\User Data")
49         },
50     }
```





# #De-anonymization /Code Similarity

Code	Blame	311 lines (275 loc) · 11.3 KB	6000179 RID: 377 RVA: 0x00019728 File Offset: 0x00019728 void d5f()
	namespace ChromeRecovery		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("Citrio", Path.Combine(xdlutIure.LocalApp, "CatalinaGroup\\Citrio\\User Data"), Convert.ToBoolean("true"));
1	public class Chromium		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("Yandex Browser", Path.Combine(xdlutIure.LocalApp, "Yandex\\YandexBrowser\\User Data"), Convert.ToBoolean("true"));
9			.MozillaBrowserList.Add(new xdlutIure.5sh5RLE8("Firefox", xdlutIure.SystemAppdataPath + "\\Mozilla\\FireFox\\", Convert.ToBoolean("true"));
			.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("Cococ", Path.Combine(xdlutIure.LocalApp, "CocCoc\\Browser\\User Data"), Convert.ToBoolean("true"));
14	public static List<Account> Grab()		.MozillaBrowserList.Add(new xdlutIure.5sh5RLE8("IceCat", xdlutIure.SystemAppdataPath + "\\Mozilla\\Icecat\\", Convert.ToBoolean("true"));
15	{		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("Epic Privacy", Path.Combine(xdlutIure.LocalApp, "Epic Privacy Browser\\User Data"), Convert.ToBoolean("true"));
16	Dictionary<string, string> Chr		.MozillaBrowserList.Add(new xdlutIure.5sh5RLE8("IceDragon", xdlutIure.SystemAppdataPath + "\\Comodo\\IceDragon\\", Convert.ToBoolean("true"));
17	{		.MozillaBrowserList.Add(new xdlutIure.5sh5RLE8("CyberFox", xdlutIure.SystemAppdataPath + "\\8pecxstudios\\Cyberfox\\", Convert.ToBoolean("true"));
18	{		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("Chedot", Path.Combine(xdlutIure.LocalApp, "Chedot\\User Data"), Convert.ToBoolean("true"));
19	"Chrome",		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("CentBrowser", Path.Combine(xdlutIure.LocalApp, "CentBrowser\\User Data"), Convert.ToBoolean("true"));
20	LocalApplicationData		.MozillaBrowserList.Add(new xdlutIure.5sh5RLE8("Thunderbird", xdlutIure.SystemAppdataPath + "\\Thunderbird\\", Convert.ToBoolean("true"));
21	,		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("Comodo Dragon", Path.Combine(xdlutIure.LocalApp, "Comodo\\Dragon\\User Data"), Convert.ToBoolean("true"));
22	{		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("Cool Novo", Path.Combine(xdlutIure.LocalApp, "MapleStudio\\ChromePlus\\User Data"), Convert.ToBoolean("true"));
23	"Opera",		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("7Star", Path.Combine(xdlutIure.LocalApp, "7Star\\7Star\\User Data"), Convert.ToBoolean("true"));
24	Path.Combine(Applicat		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("Brave", Path.Combine(xdlutIure.LocalApp, "BraveSoftware\\Brave-Browser\\User Data"), Convert.ToBoolean("true"));
25	,		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("360 Browser", Path.Combine(xdlutIure.LocalApp, "360Chrome\\Chrome\\User Data"), Convert.ToBoolean("true"));
26	{		.MozillaBrowserList.Add(new xdlutIure.5sh5RLE8("K-Meleon", xdlutIure.SystemAppdataPath + "\\K-Meleon\\", Convert.ToBoolean("true"));
27	"Yandex",		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("Orbitum", Path.Combine(xdlutIure.LocalApp, "Orbitum\\User Data"), Convert.ToBoolean("true"));
28	Path.Combine(LocalApp		.MozillaBrowserList.Add(new xdlutIure.5sh5RLE8("BlackHawk", xdlutIure.SystemAppdataPath + "\\NETGATE Technologies\\BlackHawk\\", Convert.ToBoolean("true"));
29	,		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("Uran", Path.Combine(xdlutIure.LocalApp, "uCozMedia\\Uran\\User Data"), Convert.ToBoolean("true"));
30	{		.MozillaBrowserList.Add(new xdlutIure.5sh5RLE8("Postbox", xdlutIure.SystemAppdataPath + "\\Postbox\\", Convert.ToBoolean("true"));
31	"360 Browser",		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("Opera Browser", Path.Combine(Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData), "Opera Software\\Opera Stable"),
32	LocalApplicationData		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("Iridium Browser", Path.Combine(xdlutIure.LocalApp, "Iridium\\User Data"), Convert.ToBoolean("true"));
33	,		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("QIP Surf", Path.Combine(xdlutIure.LocalApp, "QIP Surf\\User Data"), Convert.ToBoolean("true"));
34	{		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("Sleipnir 6", Path.Combine(xdlutIure.LocalApp, "Fenrir Inc\\Sleipnir5\\setting\\modules\\ChromiumViewer"), Convert.ToBoolean("true"));
35	"Comodo Dragon",		.MozillaBrowserList.Add(new xdlutIure.5sh5RLE8("WaterFox", xdlutIure.SystemAppdataPath + "\\Waterfox\\", Convert.ToBoolean("true"));
36	Path.Combine(LocalApp		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("Vivaldi", Path.Combine(xdlutIure.LocalApp, "Vivaldi\\User Data"), Convert.ToBoolean("true"));
37	,		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("Coowon", Path.Combine(xdlutIure.LocalApp, "Coowon\\Coowon\\User Data"), Convert.ToBoolean("true"));
38	{		.MozillaBrowserList.Add(new xdlutIure.5sh5RLE8("SeaMonkey", xdlutIure.SystemAppdataPath + "\\Mozilla\\SeaMonkey\\", Convert.ToBoolean("true"));
39	"CoolNovo",		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("Liebao Browser", Path.Combine(xdlutIure.LocalApp, "liebao\\User Data"), Convert.ToBoolean("true"));
40	Path.Combine(LocalApp		.MozillaBrowserList.Add(new xdlutIure.5sh5RLE8("Flock", xdlutIure.SystemAppdataPath + "\\Flock\\Browser\\", Convert.ToBoolean("true"));
41	,		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("Chromium", Path.Combine(xdlutIure.LocalApp, "Chromium\\User Data"), Convert.ToBoolean("true"));
42	{		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("Elements Browser", Path.Combine(xdlutIure.LocalApp, "Elements Browser\\User Data"), Convert.ToBoolean("true"));
43	"SRWare Iron",		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("Sputnik", Path.Combine(xdlutIure.LocalApp, "Sputnik\\Sputnik\\User Data"), Convert.ToBoolean("true"));
44	Path.Combine(LocalApp		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("Torch Browser", Path.Combine(xdlutIure.LocalApp, "Torch\\User Data"), Convert.ToBoolean("true"));
45	,		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("Edge Chromium", Path.Combine(xdlutIure.LocalApp, "Microsoft\\Edge\\User Data"), Convert.ToBoolean("true"));
46	{		.MozillaBrowserList.Add(new xdlutIure.5sh5RLE8("PaleMoon", xdlutIure.SystemAppdataPath + "\\Moonchild Productions\\Pale Moon\\", Convert.ToBoolean("true"));
47	"Torch Browser",		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("Amigo", Path.Combine(xdlutIure.LocalApp, "Amigo\\User Data"), Convert.ToBoolean("true"));
48	Path.Combine(LocalApp		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("Chrome", Path.Combine(xdlutIure.LocalApp, "Google\\Chrome\\User Data"), Convert.ToBoolean("true"));
49	,		.ChromiumBrowserList.Add(new xdlutIure.5sh5RLE8("Kometa", Path.Combine(xdlutIure.LocalApp, "Kometa\\User Data"), Convert.ToBoolean("true"));



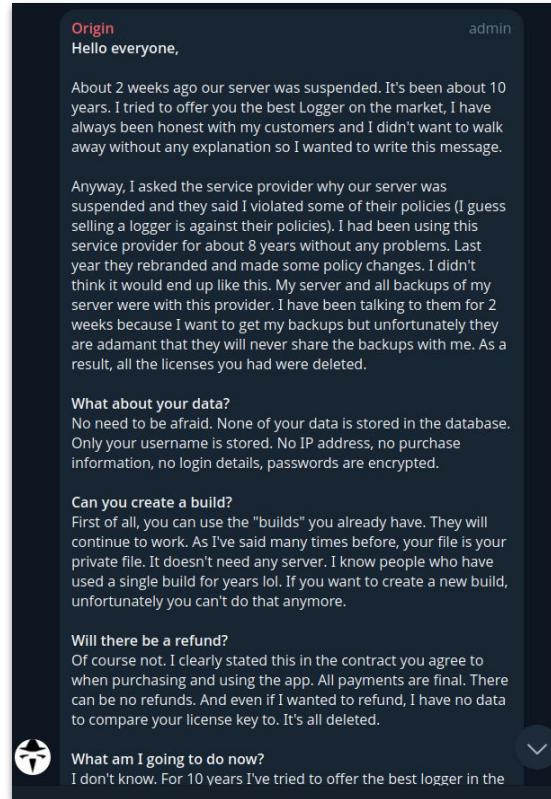
## #De-anonymization /0xfd's Real Identity

---

**REDACTED**

# #Retirement Post /1 July 2024 - End of the story

1 July 2024: Post announcing the retirement of the team that developed OriginLogger (also Agent Tesla) after 10 years.



**Origin** admin

Hello everyone,

About 2 weeks ago our server was suspended. It's been about 10 years. I tried to offer you the best Logger on the market, I have always been honest with my customers and I didn't want to walk away without any explanation so I wanted to write this message.

Anyway, I asked the service provider why our server was suspended and they said I violated some of their policies (I guess selling a logger is against their policies). I had been using this service provider for about 8 years without any problems. Last year they rebranded and made some policy changes, I didn't think it would end up like this. My server and all backups of my server were with this provider. I have been talking to them for 2 weeks because I want to get my backups but unfortunately they are adamant that they will never share the backups with me. As a result, all the licenses you had were deleted.

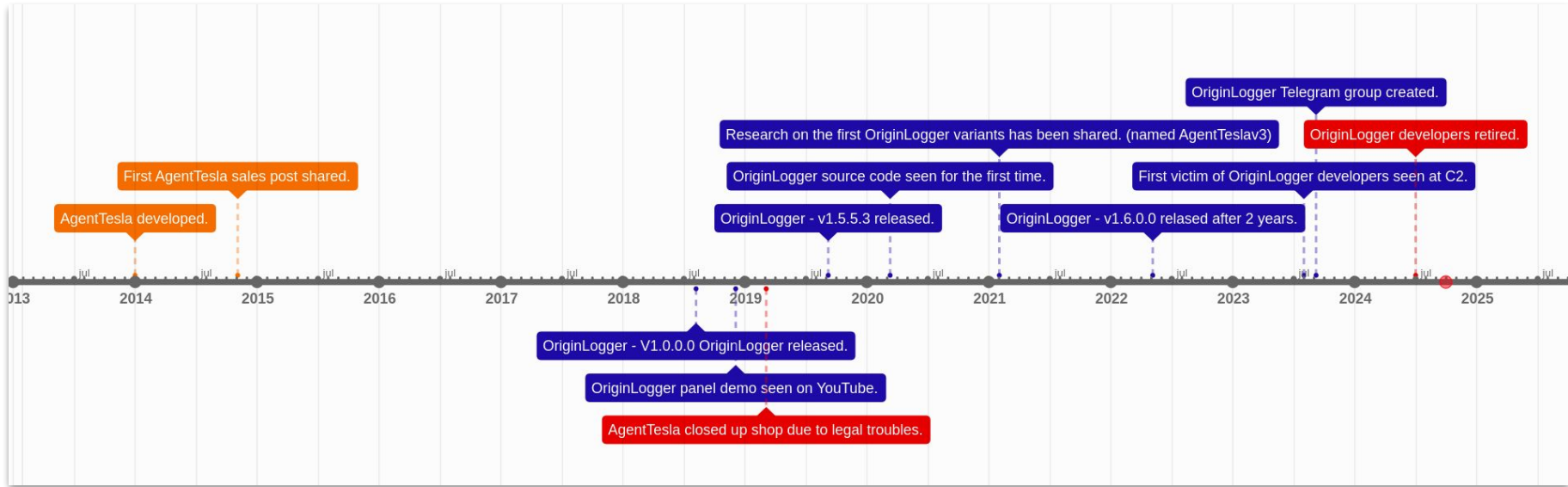
**What about your data?**  
No need to be afraid. None of your data is stored in the database. Only your username is stored. No IP address, no purchase information, no login details, passwords are encrypted.

**Can you create a build?**  
First of all, you can use the "builds" you already have. They will continue to work. As I've said many times before, your file is your private file. It doesn't need any server. I know people who have used a single build for years lol. If you want to create a new build, unfortunately you can't do that anymore.

**Will there be a refund?**  
Of course not. I clearly stated this in the contract you agree to when purchasing and using the app. All payments are final. There can be no refunds. And even if I wanted to refund, I have no data to compare your license key to. It's all deleted.

**What am I going to do now?**  
I don't know. For 10 years I've tried to offer the best logger in the

# #Agent Tesla Group Lifecycle



Timeline diagram of AgentTesla's life cycle.

**THANK YOU!**

[www.malwation.com](http://www.malwation.com)

Twitter:  
[@brkalbyrk7](https://twitter.com/brkalbyrk7)  
[@rhotav](https://twitter.com/rhotav)

