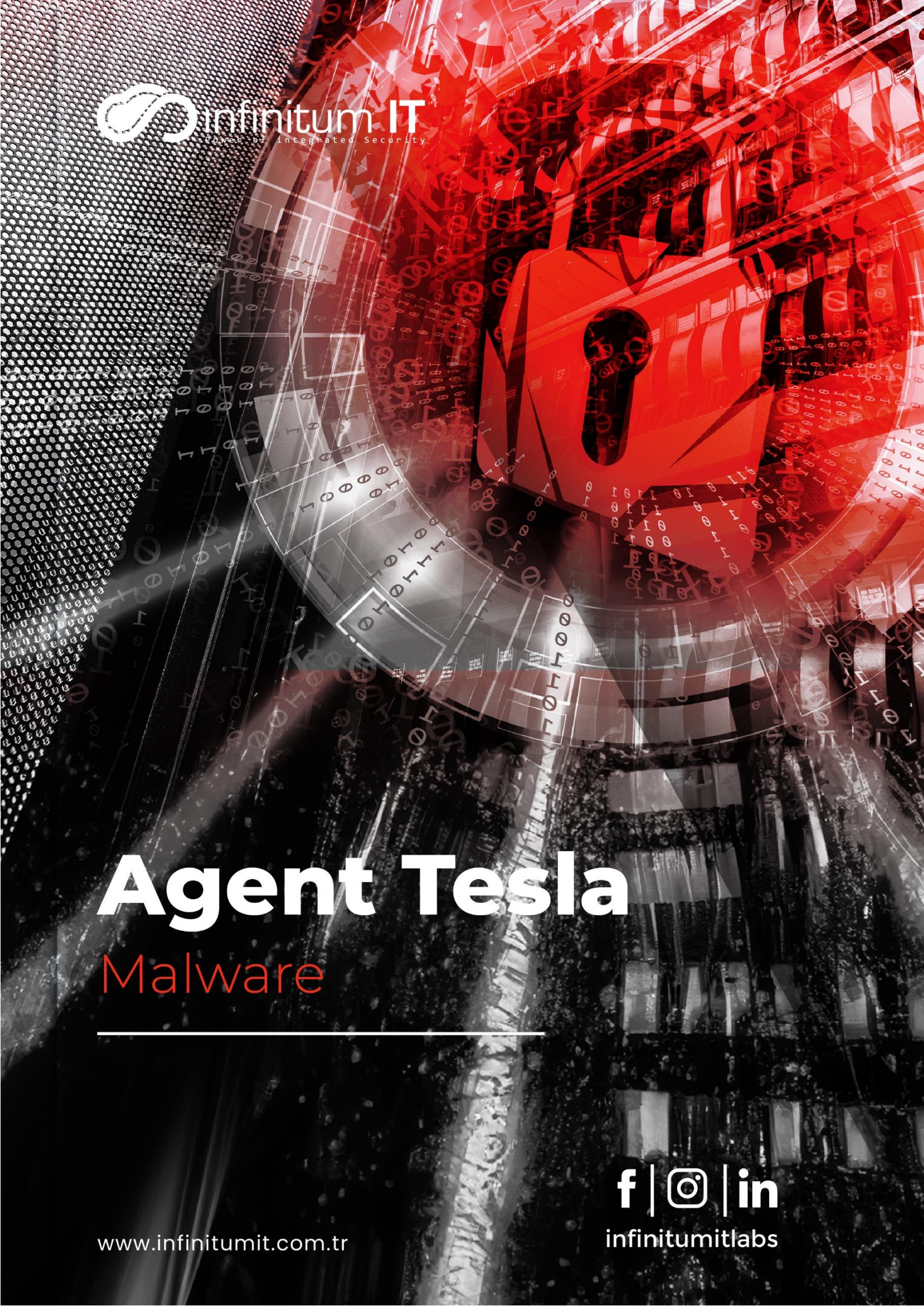

infinitum IT
Power of Integrated Security
Agent Tesla
Malware
www.infinitumit.com.tr
infinitumitlabs

CONTENTS

Overview

On September 29, 2023, an email sent by İş Bankası underwent a detailed examination. The email contained a Swift message with the intention to deceive the user. This Swift message was presented as a zipped file. However, upon opening this zipped file, a file named **"İş_Bankası_Döviz_Transferi_(148038560)_PDF.exe"** was revealed. While it appeared to be a PDF file to avoid suspicion, it was, in fact, a malicious software with a .exe extension. After investigations, it was determined that this email was a phishing attack email.

At this point, the aim was to execute this malicious software without the user noticing. Upon initial access, the .exe file was examined in detail. It was found that this file was actually a malicious version of an original file named **"fbEG.exe."**

It was determined that the malicious file was embedded within another file using a technique known as packing, which is a method often used to bypass security products. The unpacking process revealed that the contained file was a Portable Executable (PE) file, indicating that it was an executable file.

In conclusion, it was determined that this malicious software belonged to the **Agent Tesla Malware Family.** To provide more information about protection from such attacks and security measures, all analysis steps and details are included in the report.

Agent Tesla and What you need to know

What is Agent Tesla ?

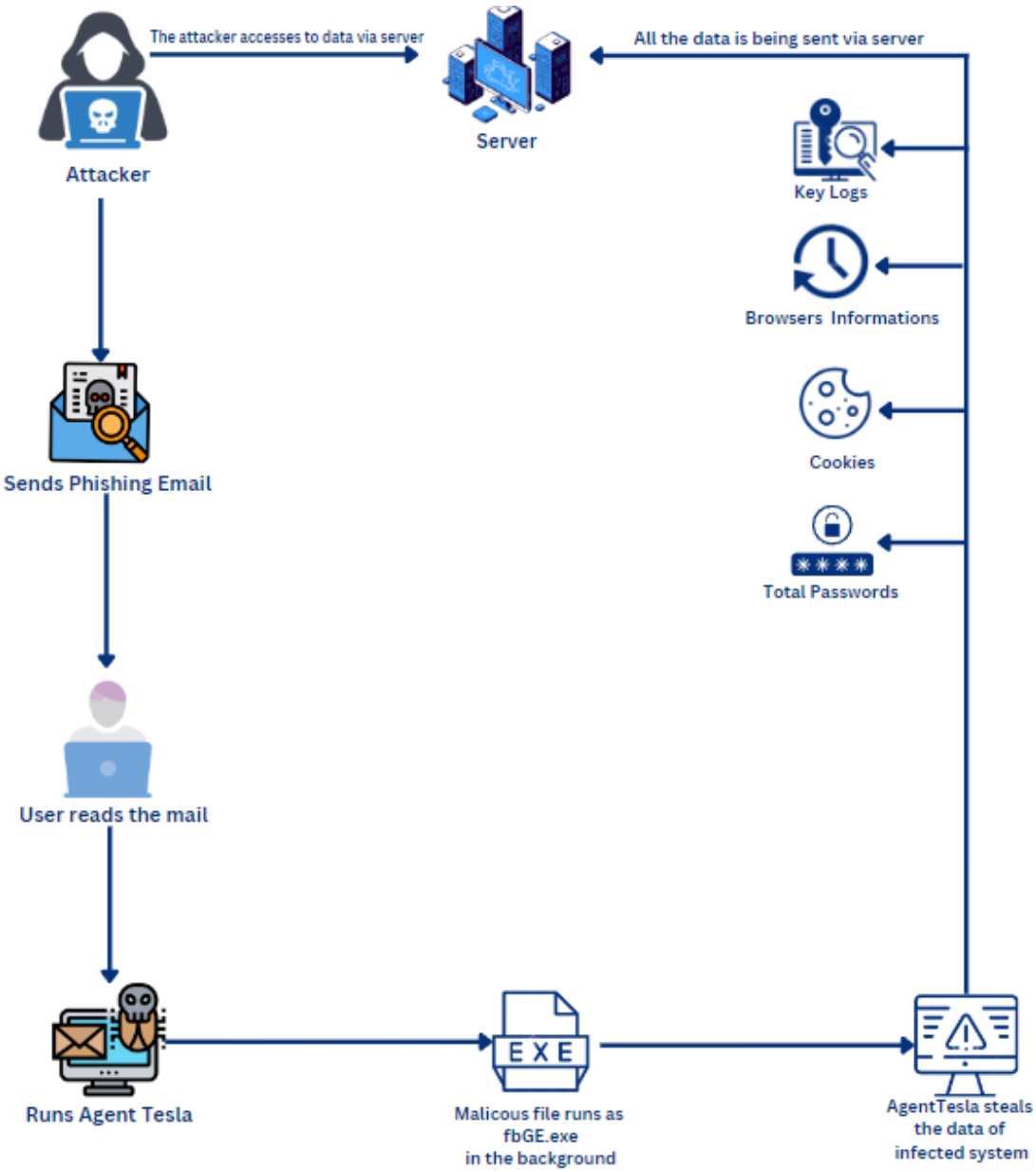
Agent Tesla is known as a .Net-based Remote Access Trojan (RAT) and is commonly used by cybercrime groups that offer Malware as a Service (MaaS). In this type of criminal business model, threat actors, known as Initial Access Brokers (IABs), provide their specialized skills to criminal groups to bypass organizations' security measures and steal information from within. Agent Tesla is used in the initial stages of such cyberattacks. Once the initial access is gained, it is employed to deliver more complex malicious software, such as ransomware, to victim systems.

Agent Tesla is a malicious software that was first detected in 2014 and has been extensively used, especially in the 2020s, in phishing campaigns with COVID-19 pandemic themes. Nowadays, this malware continues its attacks by masquerading as prominent companies. To achieve its objectives, **Agent Tesla delivers malicious attachments through email messages, often with file extensions such as .zip, .gz, .cab, .msi, and .img.** Additionally, it commonly employs malicious Visual Basic Application (VBA) macros while targeting Microsoft Office documents.

One of the distinguishing features of Agent Tesla is its ability to mimic the logos and fonts of legitimate companies in phishing campaigns. This is an effective tactic used to deceive victims and facilitate the further spread of the malware. Agent Tesla is a dangerous threat used to infiltrate computer systems and steal sensitive data.

While not as complex as other malware families in terms of locally operating second-stage capabilities, Agent Tesla can effectively steal various types of sensitive data. Furthermore, it offers an easy-to-use interface for criminals, making it an appealing choice for Initial Access Brokers to direct attacks and gather stolen information.

Infection Chain



Initial Access

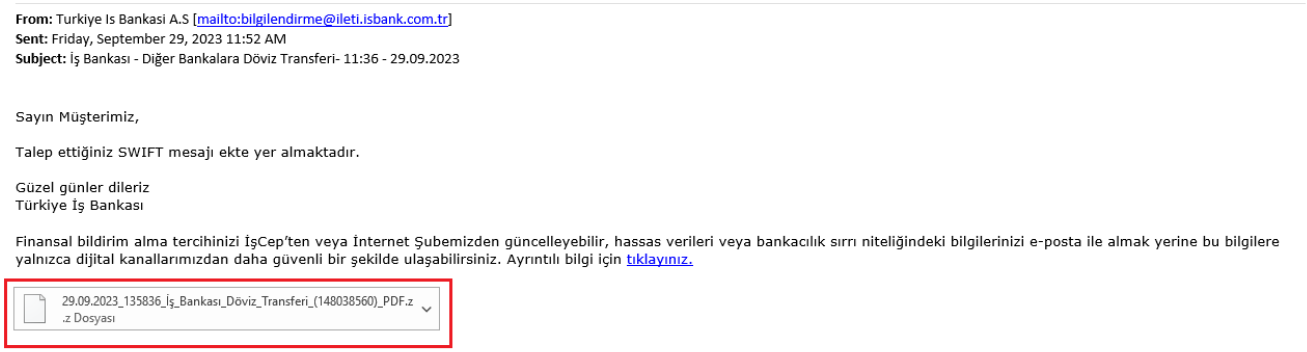


Figure 1- Phishing mail

An e-mail that appears to have been originally sent from İş Bankası is shown in figure 1.

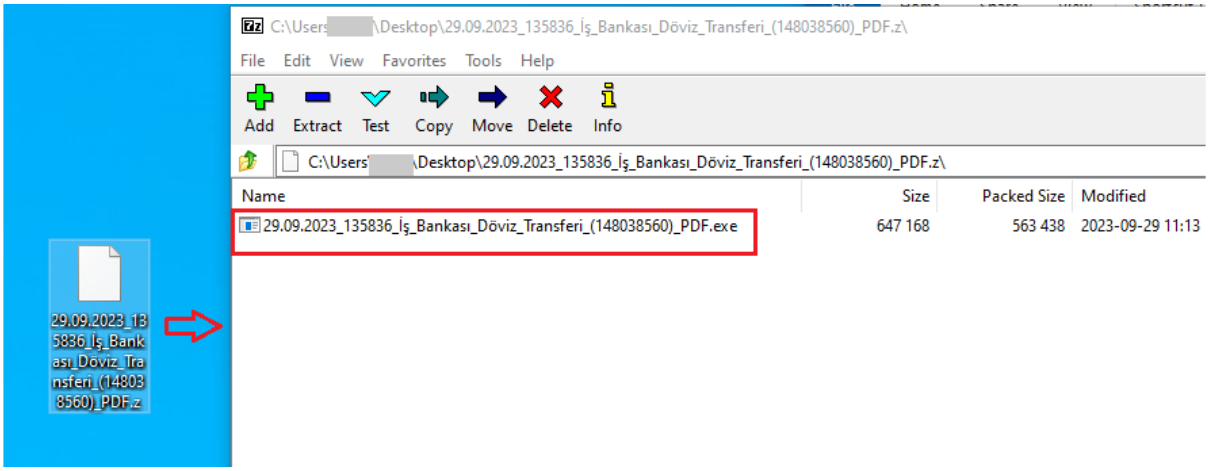


Figure 2- Email attachment content

When the email attachment is downloaded and examined, **İş_Bankası_Döviz_Transferi_(148038560)_PDF.exe** file appears.

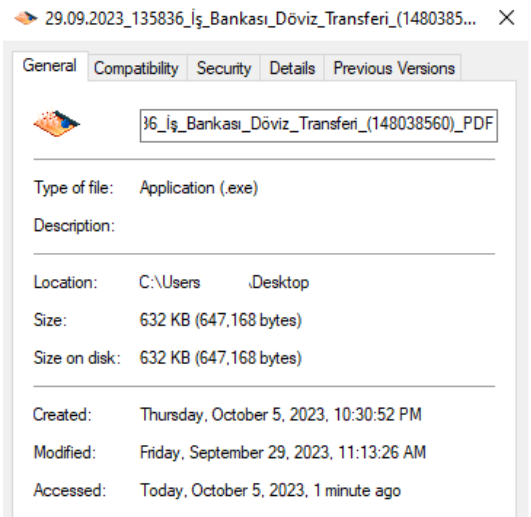


Figure 3- Detailed information of the file

İş_Bankası_Döviz_Transferi_(148038560)_PDF.exe Analysis

Static Analysis

File Name	fbGE.exe
MD5	37404d6df0a039dc790897f52ffc7538
SHA256	a5888a484f812f66cd39e16dbbcbb0891fd7f88e28a02660acfbe95635055696
File Type	PE/32

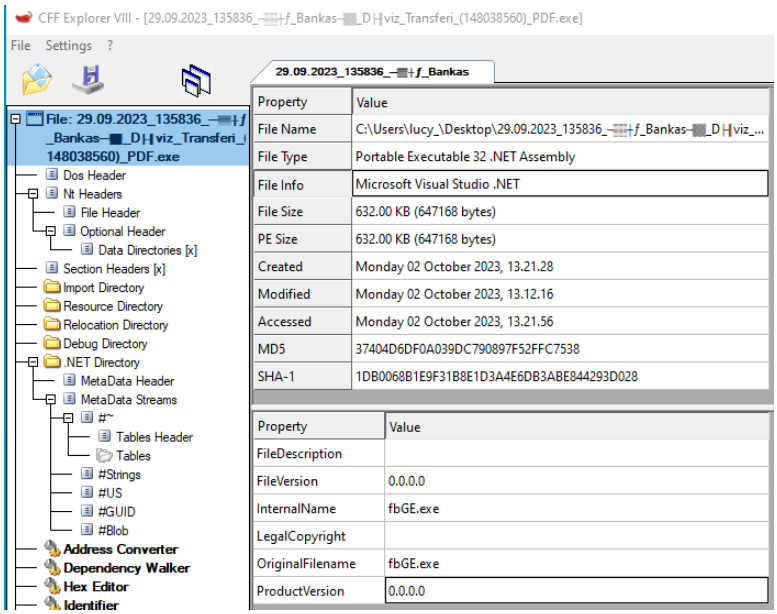


Figure 1- Information about the malicious file

It can be seen that the original file name of the **29.09.2023_135836_İş_Bankası_Döviz_Transferi_(148038560)_PDF file is fbGE.exe**. This file is **written in .NET**.

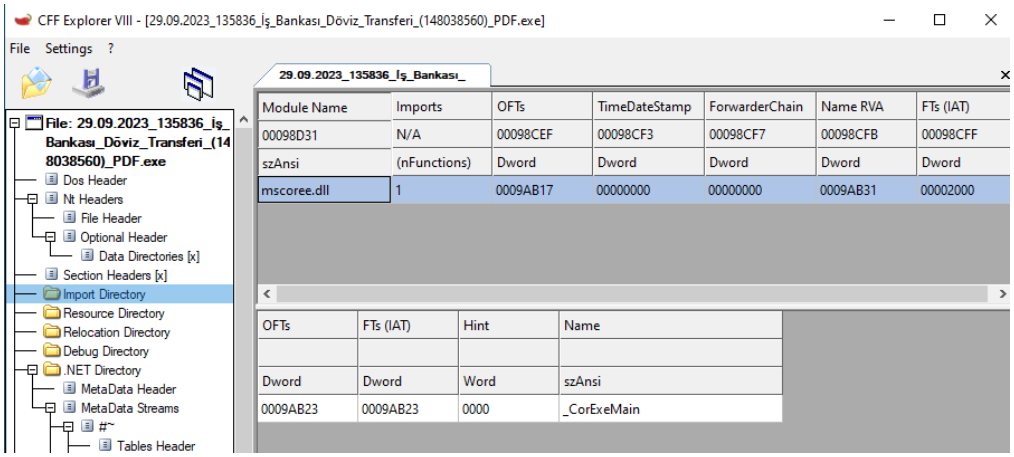


Figure 2- Imported functions

The file uses certain dlls to provide the expected functionality. Only one dll was displayed.

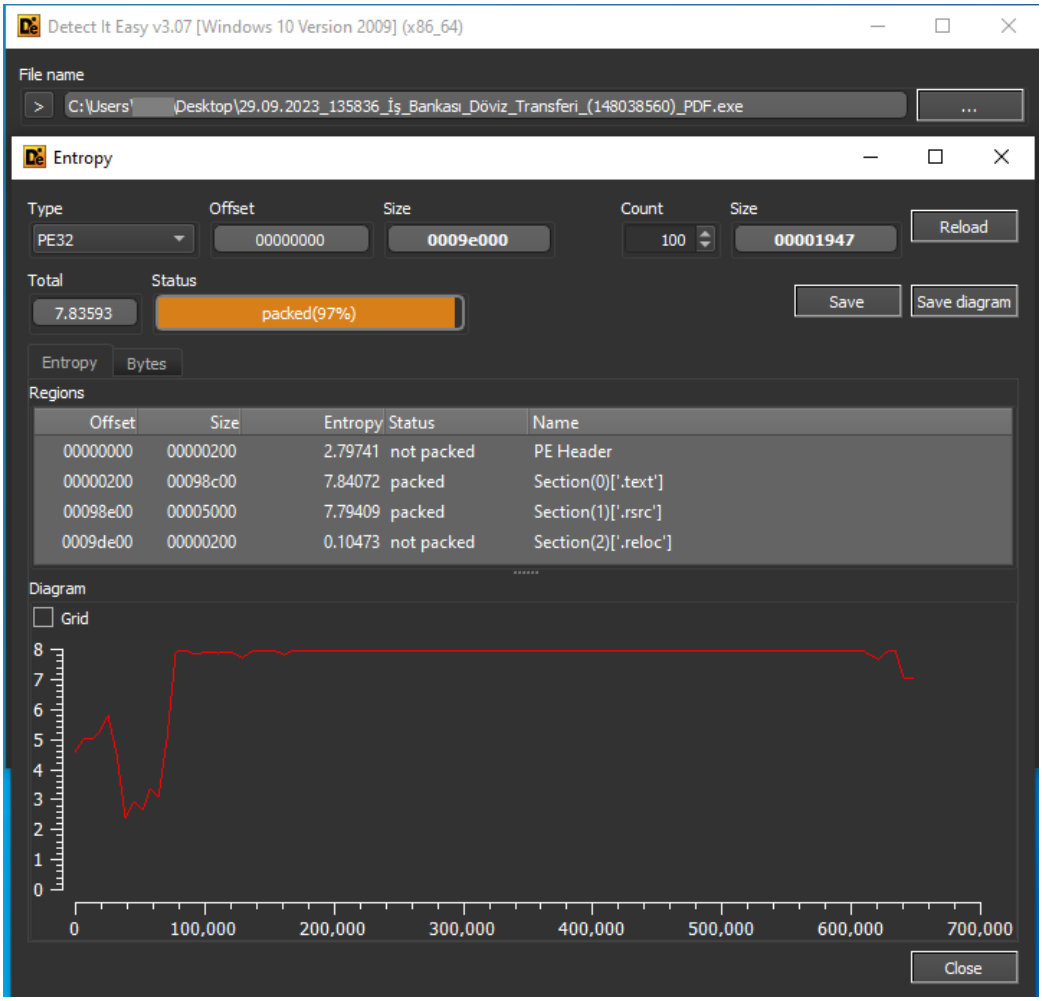


Figure 3- Pack information of the file

It seems that the pack process has been applied to the file with its original name **fbGE.exe.**

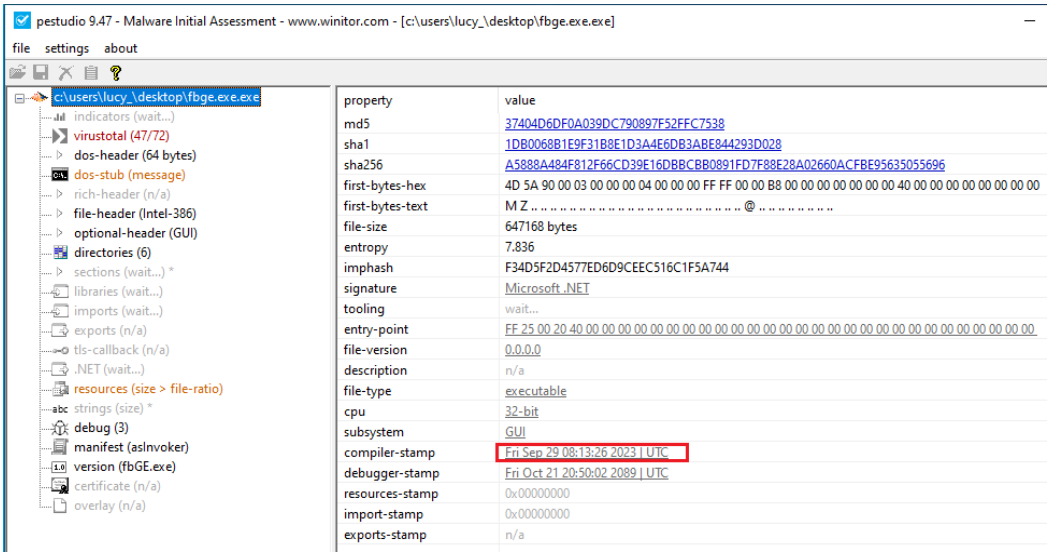


Figure 4- Detailed information about the file

It is seen that the file was compiled on September 29 at 08.13.

Dynamic Analysis

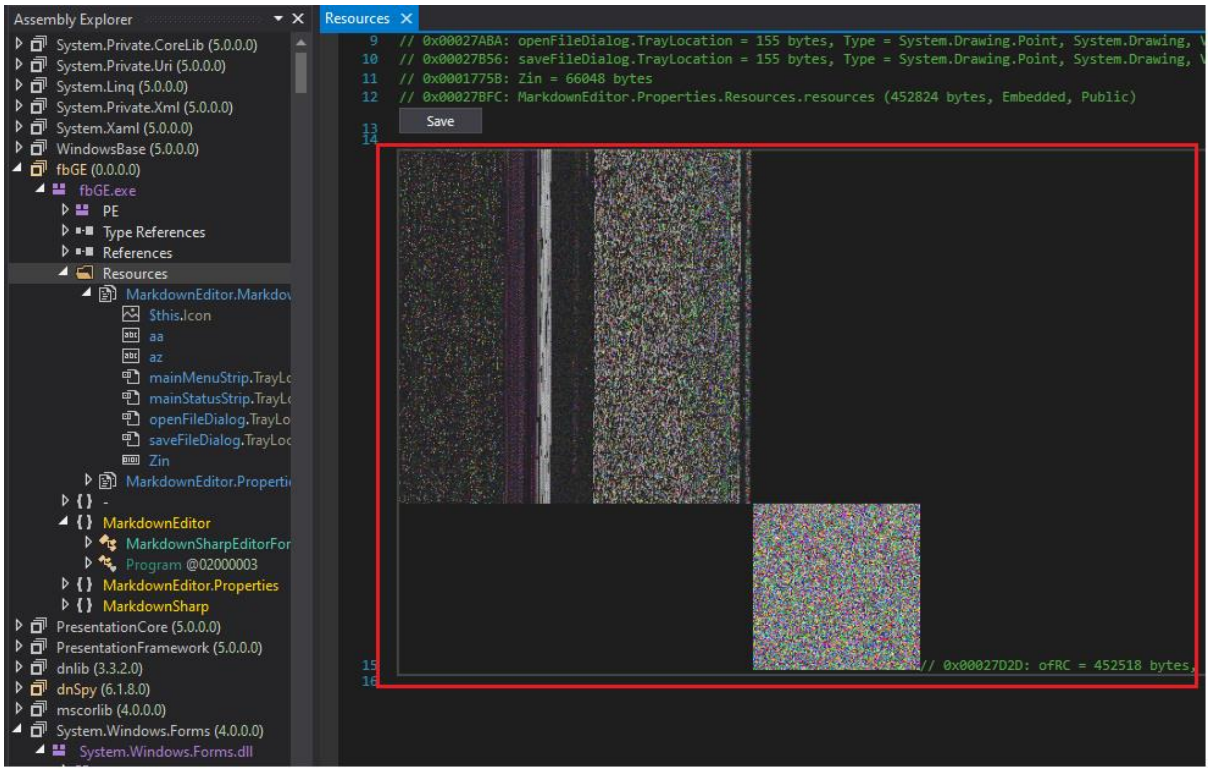


Figure 5- Embedded PE file

This malicious software has embedded a malicious component in the PE (Portable Executable) file format to evade detection and prevention by security products used to identify malicious activities. This PE file contains the main component of the malware or a portion of the malicious code, which it aims to conceal within itself.

```
using System.Windows.Forms;

namespace MarkdownEditor
{
    // Token: 0x02000003 RID: 3
    internal static class Program
    {
        // Token: 0x06000012 RID: 18 RVA: 0x000030E7 File Offset: 0x000012E7
        [STAThread]
        private static void Main()
        {
            Application.EnableVisualStyles();
            Application.SetCompatibleTextRenderingDefault(false);
            Application.Run(new MarkdownSharpEditorForm());
        }
    }
}
```

Figure 6- Main function

The packaged PE file was extracted from this file and the analysis process continued.
The file that performs malicious is named **55d1ae96-5104-40e5-8b90-722f4c79c9a6.exe.**

55d1ae96-5104-40e5-8b90-722f4c79c9a6.exe Analysis

Static Analysis

File Name	55d1ae96-5104-40e5-8b90-722f4c79c9a6.exe
MD5	ec5e9334f65168cce67cd57bc6391d0a
SHA256	1105c0024a2f2173d5bbda6f209168a34ed95d5cdb05f72be075ef301ee0f63c
File Type	PE/32

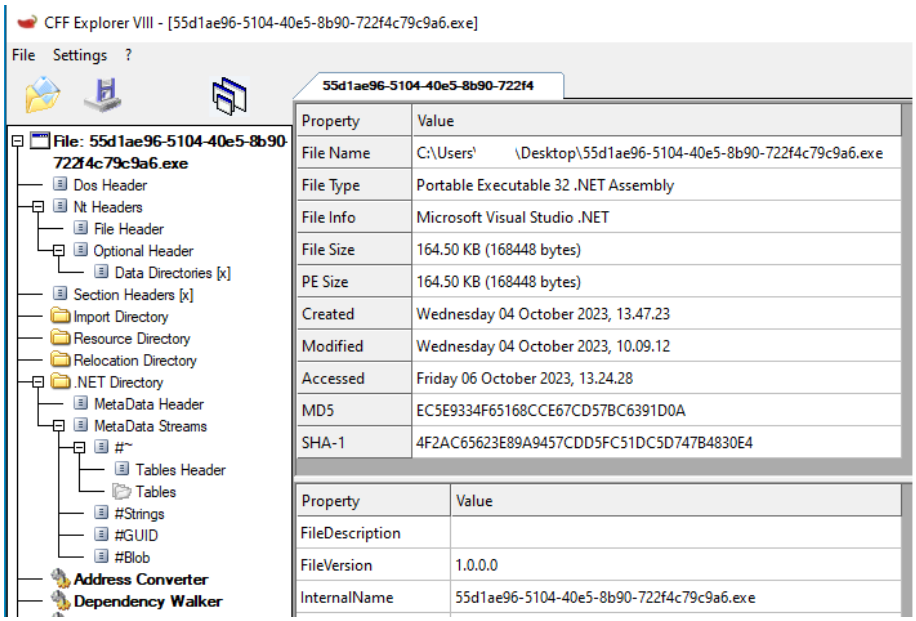


Figure 7- Information of the Extracted File

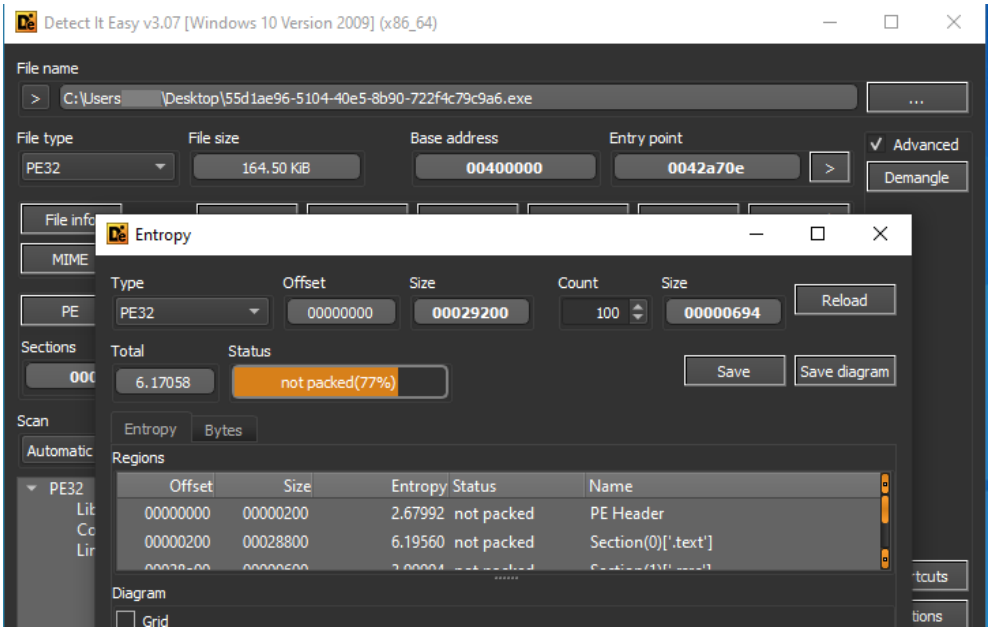


Figure 8- Information of the Extracted File

It appears to be written in **.NET** and no packaging process has been applied.

Dynamic Analysis

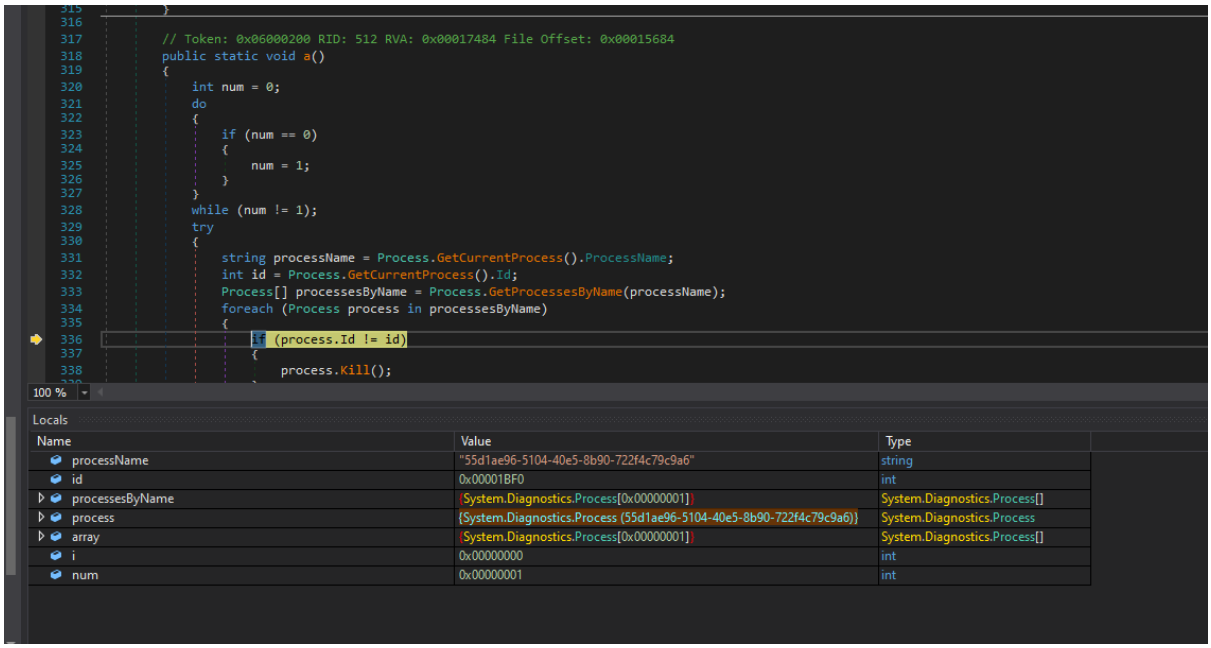


Figure 9- Process Id and Name check

First, it takes the name and id of the process and compares them. If there is a process with that process name, it terminates it.

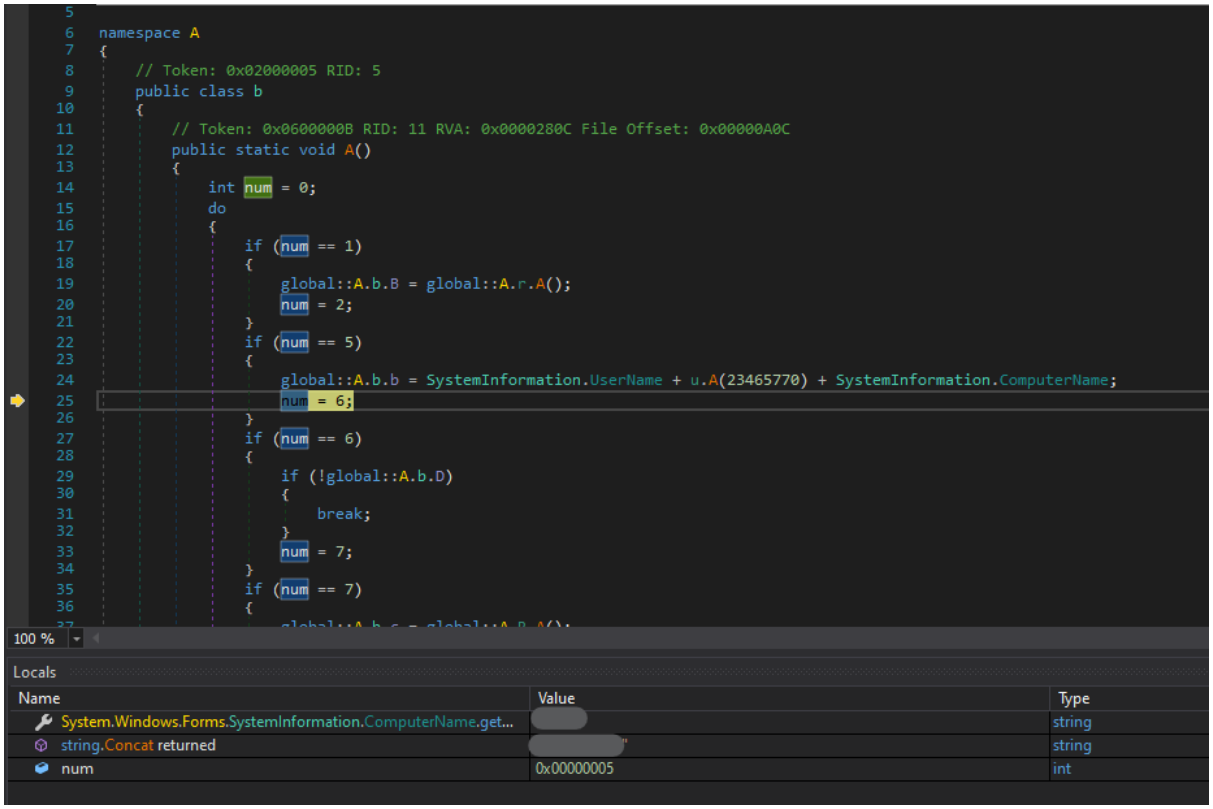


Figure 10- Username and Computer name

It takes the username and computer name.

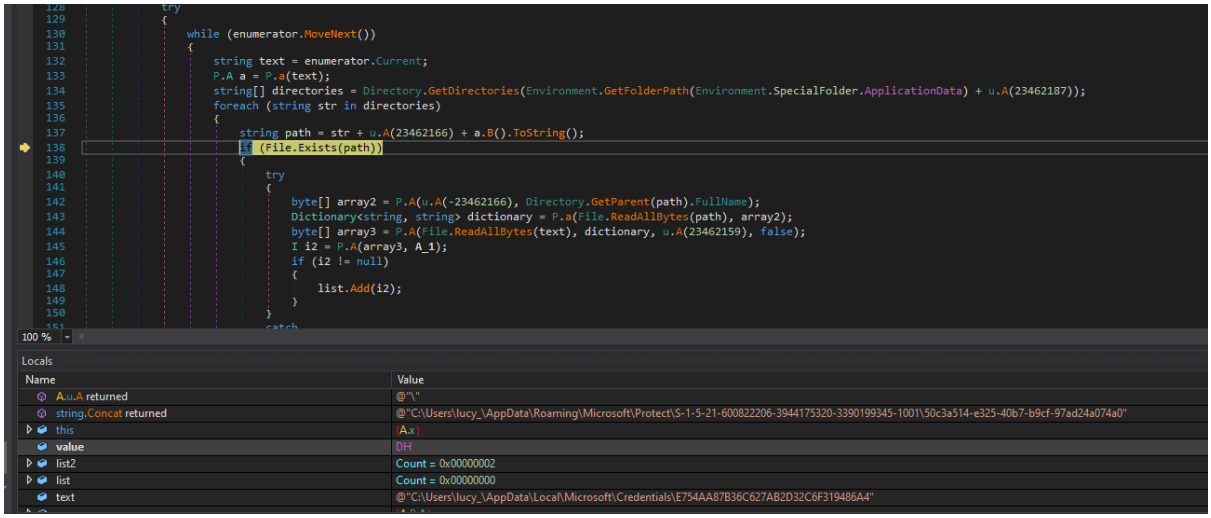


Figure 11- Receiving Data

C:\Users\Admin\AppData\Roaming\Microsoft\Protect\S-1-5-21-600822206-3944175320-3390199345-1001\50c3a514-e325-40b7-b9cf-97ad24a074a0 This directory contains user data (browser history, cookies, contains login information, etc.). The malicious file receives this data.

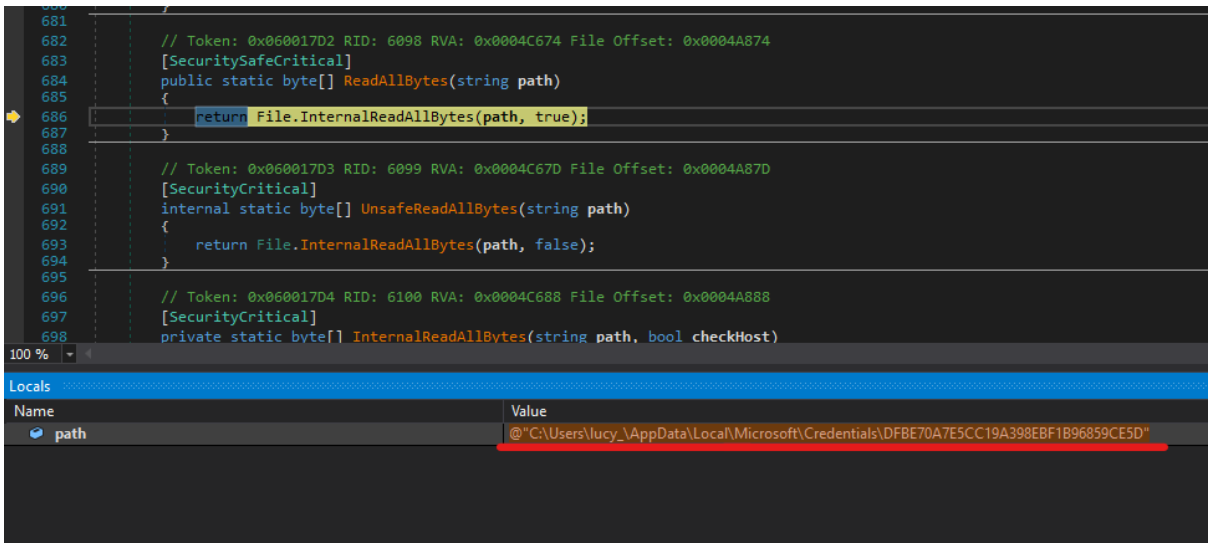


Figure 12- Receiving Sensitive Data

Authentication information and security-related data are stored by the Windows operating system in the **C:\Users\Admin\AppData\Local\Microsoft\Credentials directory. (Credentials, Certificates, System Security Settings, etc.)** The malicious file aims to steal users' sensitive information by accessing this data.

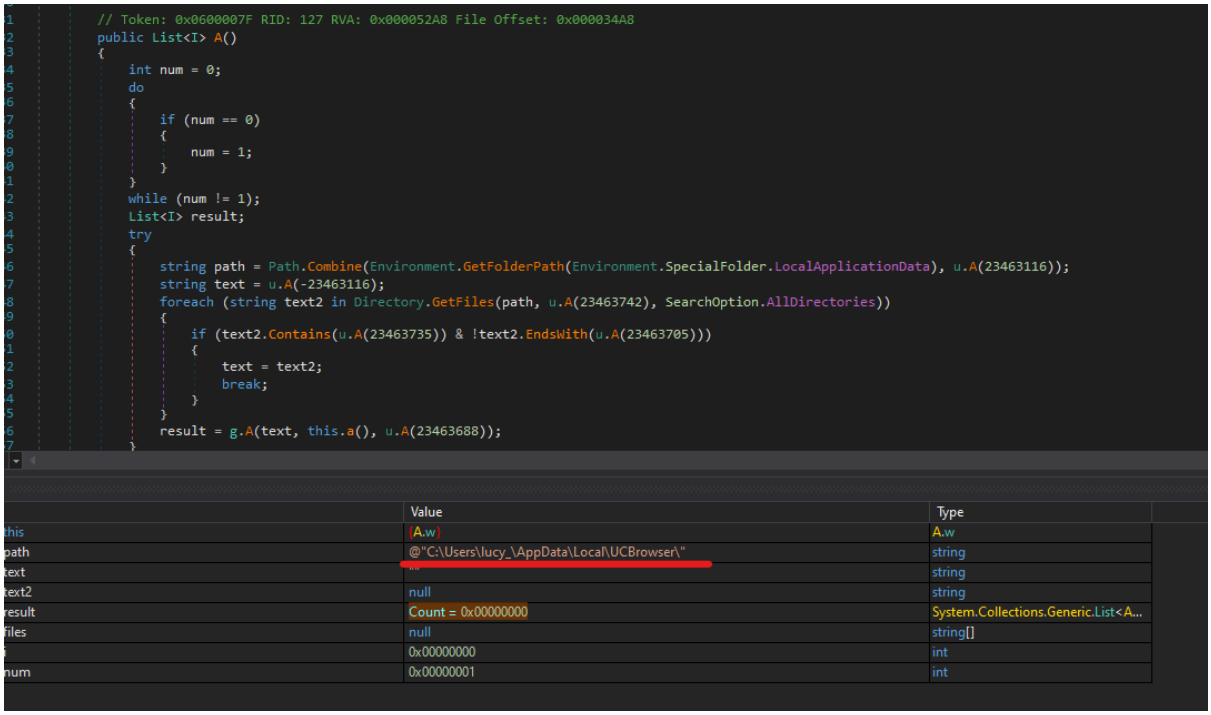


Figure 13- Index control

It sequentially checks the **C:\Users\Admin\AppData\Local** directory using the **GetFolderPath API**. If available, it retrieves the data in these directories. The directories it checks are as in the Table.

Table 1

C:\Users\Admin\AppData\Local\UCBrowser\
C:\Users\Admin\AppData\Local\Tencent\QQBrowser\User Data\Default\EncryptedStorage
C:\Users\Admin\AppData\Local\VirtualStore\Program Files\Foxmail\mail
C:\Users\Admin\AppData\Local\falkon\profiles
C:\Users\Admin\AppData\Local\Microsoft\Credentials\E754AA87B36C627AB2D32C6F319486A4
C:\Users\Admin\AppData\Local\NordVPN
C:\Users\Admin\AppData\Local\VirtualStore\Program Files (x86)\FTP Commander Deluxe\Ftplist.txt

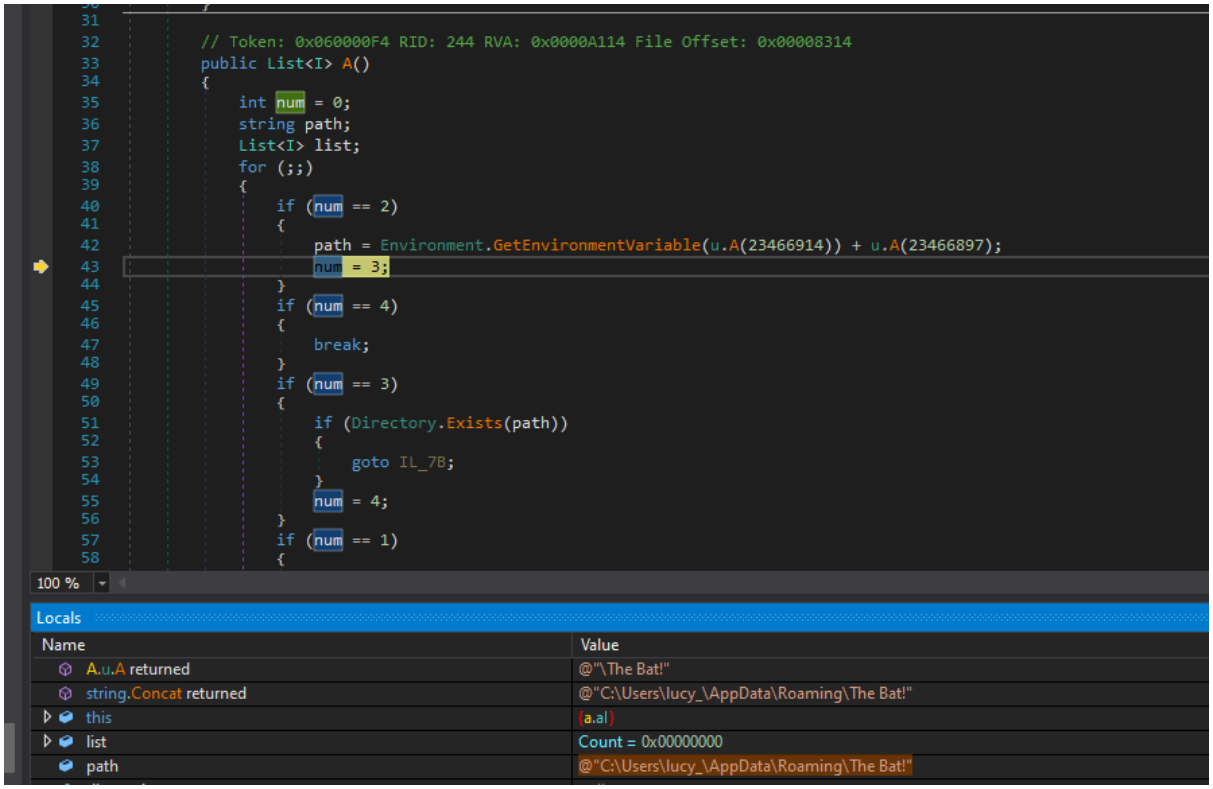


Figure 14- Directory control

Using the **GetEnvironmentVariable** function, it retrieves the variables that store the data of the applications. The variables it takes are shown in Table 2.

Table 2

C:\Users\Admin\AppData\Roaming\The Bat!
C:\Users\Admin\AppData\Roaming\Pocomail\accounts.ini
C:\Users\Admin\AppData\Roaming\eM Client\accounts.dat
C:\Users\Admin\AppData\Roaming\FileZilla\recentservers.xml
C:\Users\Admin\AppData\Roaming\Opera Mail\Opera Mail\wand.dat
C:\Users\Admin\AppData\Roaming\MySQL\Workbench\workbench_user_data.dat
C:\Users\Admin\AppData\Roaming\Claws-mail
C:\Users\Admin\AppData\Roaming\discordcanary"
C:\Users\Admin\AppData\Roaming\Discord
C:\Users\Admin\AppData\Roaming\Apple Computer\Preferences\keychain.plist
C:\Users\Admin\AppData\Roaming\Trillian\users\global\accounts.dat
C:\Users\Admin\AppData\Roaming\FTPGetter\servers.xml

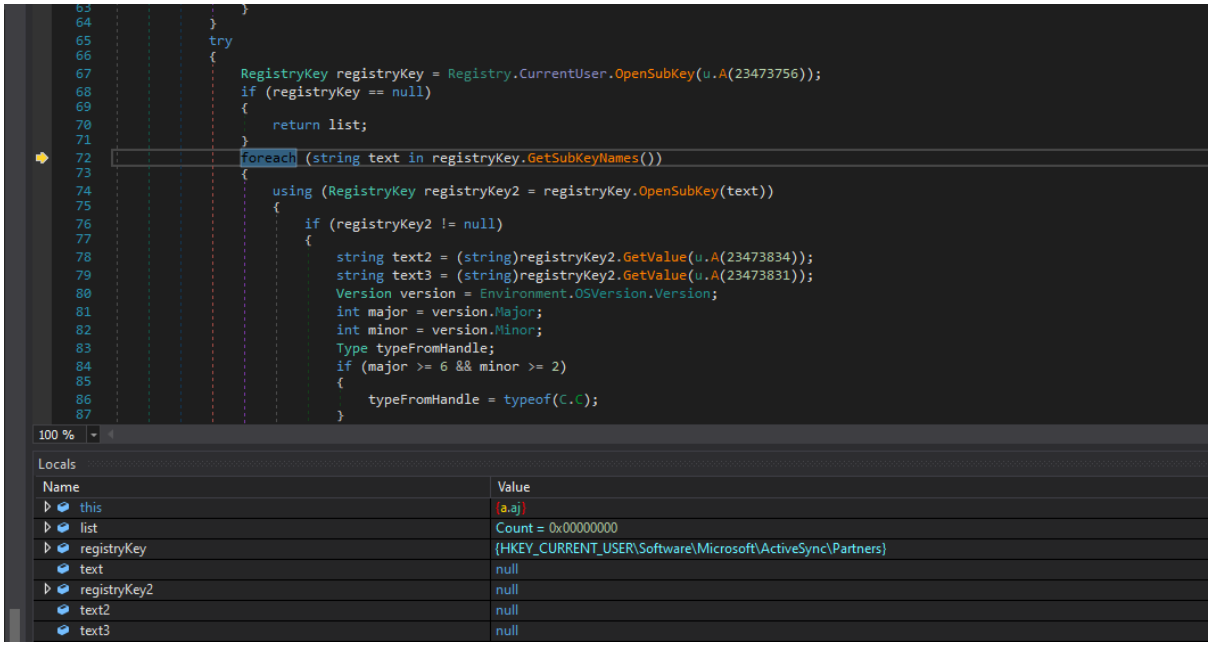


Figure 15- Registry Operations

The malicious file targets Windows registry subkeys to carry out this process, aiming to steal or damage sensitive data from users or systems. The subkeys opened by the malicious file are displayed in Table 3.

Table 3

HKEY_CURRENT_USER\Software\Microsoft\ActiveSync\Partners
HKEY_CURRENT_USER\Software\Aerofox\Foxmail\V3.1
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676
HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging
HKEY_CURRENT_USER\Software\Microsoft\ActiveSync\Partners
HKEY_CURRENT_USER\Software\IncrediMail\Identities\
HKEY_CURRENT_USER\Software\ORL\WinVNC3
HKEY_CURRENT_USER\Software\Qualcomm\Eudora\CommandLine
HKEY_CURRENT_USER\SOFTWARE\Wow6432Node\RealVNC\WinVNC4
HKEY_CURRENT_USER\SOFTWARE\FTPWare\COREFTP\Sites
HKEY_CURRENT_USER\Software\OpenVPN-GUI\configs
HKEY_CURRENT_USER\Software\TightVNC\Server

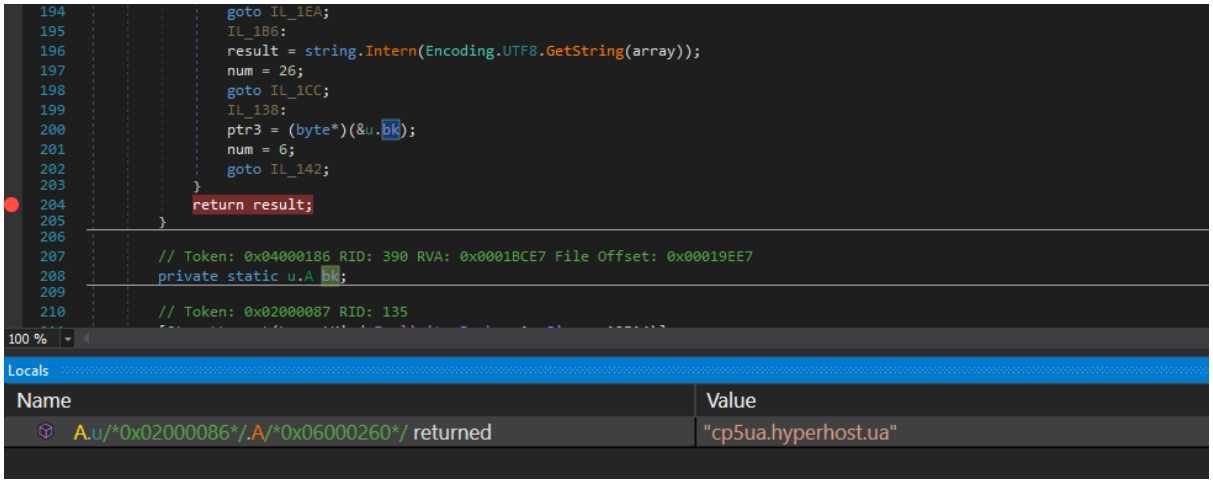


Figure 16- Server address

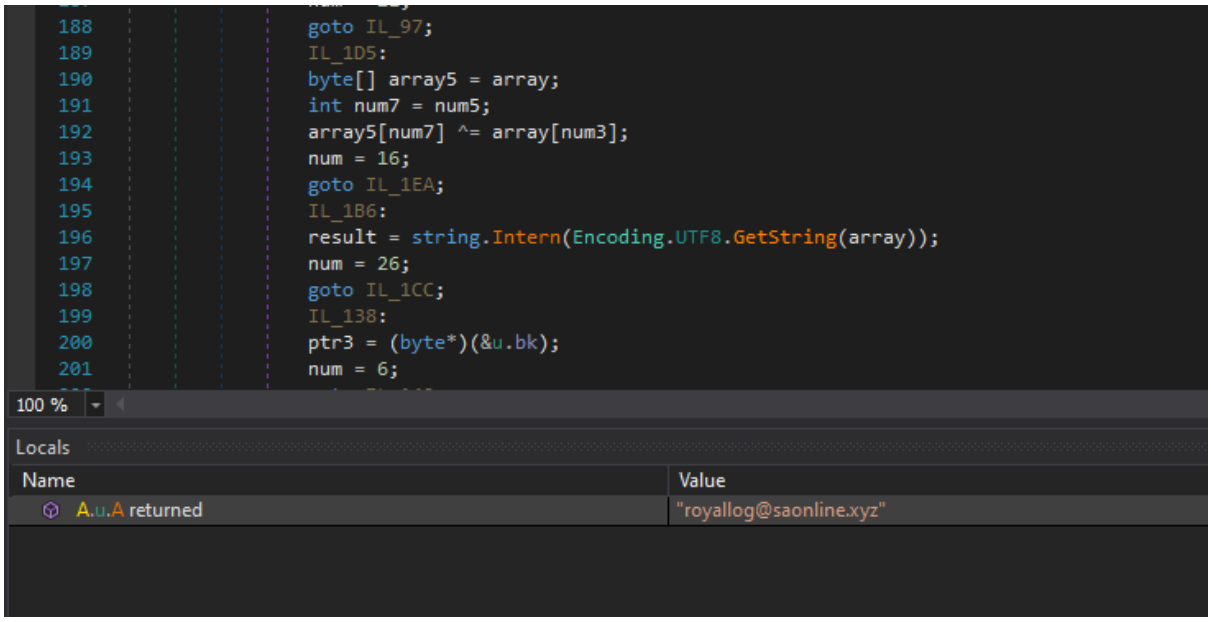


Figure 17- Username info

The malicious file communicates with the server **cp5ua[.]hyperhost[.]ua** to send the stolen data. It specifies the username for the account that will be used to send emails, which is **"royallog@saonline.xyz"** and it provides the password used for this account, which is **"7213575aceACE@#$".**

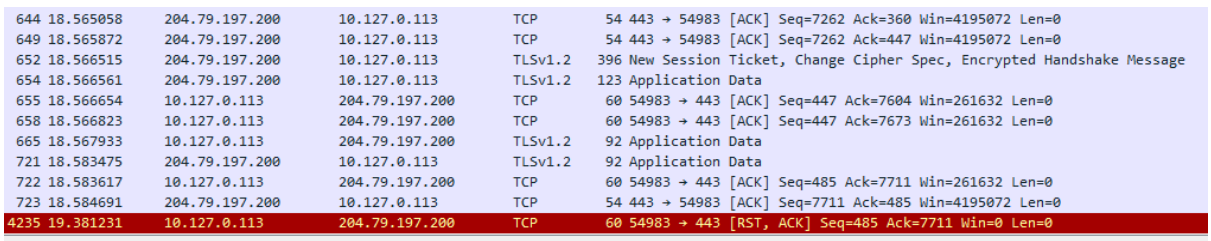


Figure 18-IP informations

The IP address reached by **cp5ua[.]hyperhost[.]ua** in domain name resolution is **204[.]79.197.200.**

IOCs

IPs :

IOC Type	IOC
IPv4	192[.]229.211.108
IPv4	204[.]79.197.200
IPv4	26[.]35.223.20
IPv4	91[.]235.128.141

Domains :

IOC Type	IOC
Domain	https[:]//tse1.mm.bing.net
Domain	cp5ua[.]hyperhost[.]ua

Hashs:

IOC Type	IOC
SHA256	5ab11a933c95891b62f1ba94f38cdf01ded8f19061946601670c430d084dd007
SHA256	1105c0024a2f2173d5bbda6f209168a34ed95d5cdb05f72be075ef301ee0f63c
MD5	ec5e9334f65168cce67cd57bc6391d0a
SHA256	bc6e1487bee00a8fd2b639ee4e60867d7e409bd3cb6be1451f5ddbce26340766

YARA RULES

fbGE.exe Yara Rule

```
import "hash"
rule AgentTesla
{
meta:
        author = "Kerime Gencay"
        description = "AgentTesla Rule"
        file_name = "fbGE.exe"
        hash = "37404d6df0a039dc790897f52ffc7538"
strings:

        $str1 = "CalculateNextDataValue"
        $str2 = "HyperlinkEvaluator"
        $str3 = "fbGE.exe"
        $str4 = "ImageReferenceEvaluator"
        $str5 ="MarkdownEditor"
        $str6 = "AnchorInlineEvaluator"
        $str7 = "MatchEvaluator"
        $str8 = "CodeSpanEvaluator"
        $str9 = "AtxHeaderEvaluator"
        $str10 = "ItalicsEvaluator"

condition:

        uint16(0) == 0x5A4D and (all of ($str*))

}
```

55d1ae96-5104-40e5-8b90-722f4c79c9a6.exe Yara Rule

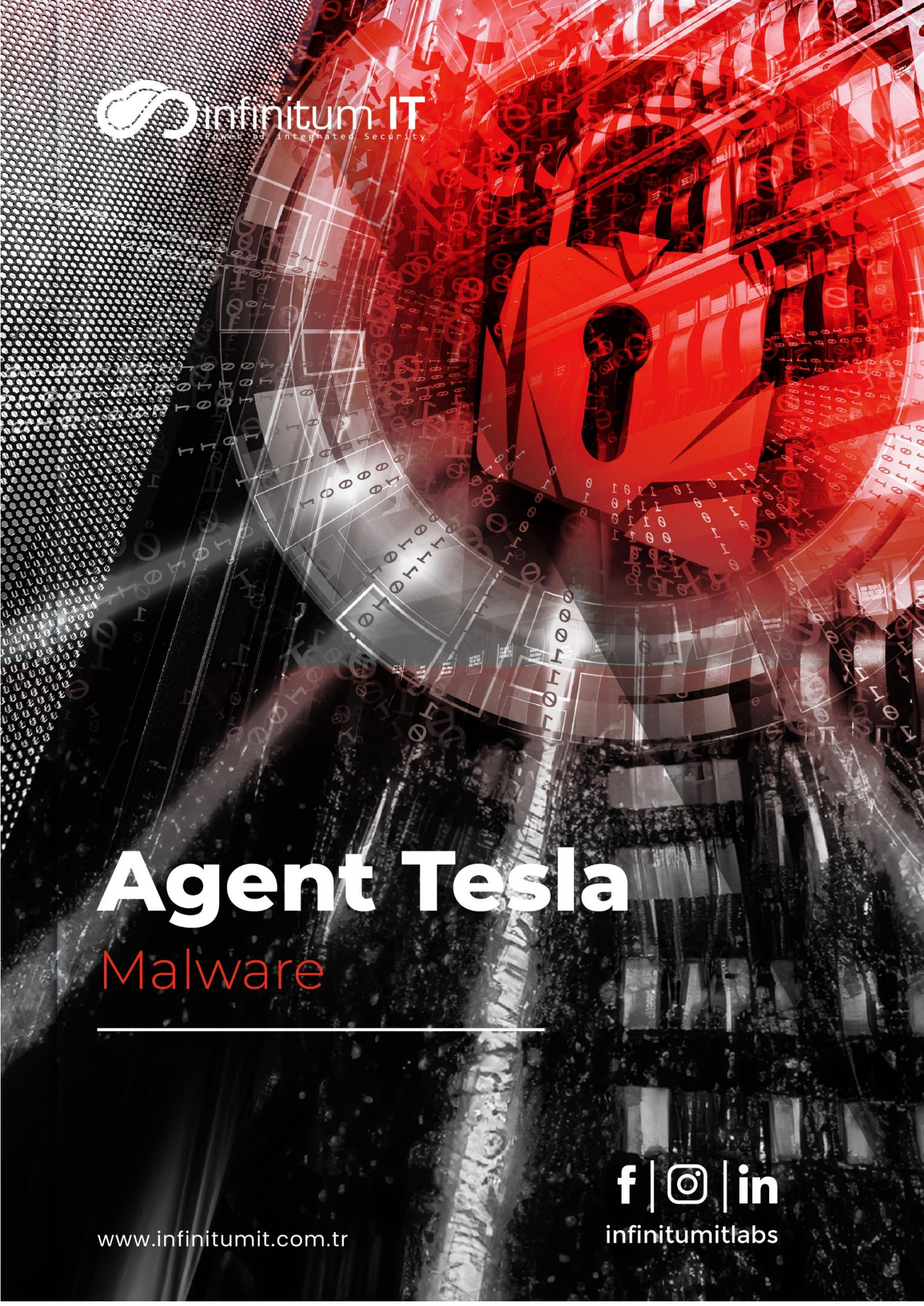
```
import "hash"
rule AgentTesla
{
meta:
        author = "Kerime Gencay"
        description = "AgentTesla Rule"
        file_name = "55d1ae96-5104-40e5-8b90-722f4c79c9a6.exe"
        hash = "ec5e9334f65168cce67cd57bc6391d0a"
strings:

        $str1 = "HMACSHA512"
        $str2 = "SecuritySafeCriticalAttribute"
        $str3 = "set_UseShellExecute"
        $str4 = "Marshal"
        $str5 ="get_InvariantCulture"
        $str6 = "55d1ae96-5104-40e5-8b90-722f4c79c9a6.exe"


      $opc1 = {07 6F AA 00 00 0A 13 28 16 13 29 38 A4 03 00 00 11}
      $opc2 = {0A 0C 08 13 04 16 13 05 2B 1B 11 04 11 05 9A 0D 09}
        $opc3 = {16 0C 2B 28 00 08 17 FE 01 2C 0E 02 28 6B 01 00 06 6F 5F 01
00 0A 0B 18 0C 00 08 16 FE 01 2C 03}
        $opc4 = {00 11 0B 19 FE 01 2C 0B 1F 1A 28 84 00 00 0A 0C 1A 13 0B 00
11 0B 1C FE 01 2C 08 38 72}


condition:

        uint16(0) == 0x5A4D and (any of ($str*,$opc*))

}
```

MITRE ATT&CK TABLE

Discovery	Command and Control	Collections	Defence Evasion	Credential Access	Reconnaissance
T1012 Query Registry	T1102 Web Service	T1005 Data From Local System	T1406.002 Software Packing	T1552 Unsecured Credentials	T1566 Phishing
T1082 Information Discovery		T1564.001 Hidden Files and Directories		T1552.001 Credentials In Files	

MITIGATIONS

- Configure firewalls on your network to block incoming and outgoing connections from suspicious IP addresses. This can prevent RATs from establishing communication with command and control servers.
- Keep your operating system, applications, and security software up-to-date. Updates often include patches that fix vulnerabilities exploited by RATs.
- Install antivirus and anti-malware software. Perform regular scans to detect and remove any RAT infections.
- If not needed, disable remote desktop services. If needed, ensure strong passwords and proper authentication methods are in place.
- Unplug or disable devices such as webcams, microphones, or USB drives when not in use. RATs can abuse these devices for surveillance.
- Whenever possible, enable 2FA for all accounts, including email and cloud services. This can thwart unauthorized access.
- Monitor your system's running processes for any unusual or unfamiliar ones. Use task managers or specialized tools to detect suspicious activity.
- Ensure strong and unique passwords for all accounts. Avoid using easily guessable information.
- Be cautious of unsolicited emails, attachments, or links. RATs can often be delivered through phishing emails.
- Allow only approved applications to run on your system. This can prevent RATs from executing even if they manage to infiltrate.
- Regularly review and update your firewall rules to ensure they're effective against RATs and other malicious traffic.
- Keep an eye on system performance and behavior. Unexpected slowdowns, crashes, or unusual network activity could indicate a RAT


infinitum IT
Power of integrated Security
Agent Tesla
Malware
www.infinitumit.com.tr
infinitumitlabs